Astérisque

AST

Journées arithmétiques de Genève - 9-13 septembre 1991 : Pages préliminaires

Astérisque, tome 209 (1992), p. 1-16

<http://www.numdam.org/item?id=AST_1992__209__1_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

209 ASTÉRISQUE

1992

JOURNÉES ARITHMÉTIQUES DE GENÈVE

9 - 13 septembre 1991

D.F. CORAY, Y.-F. S. PÉTERMANN, éditeurs

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

A.M.S. Subjects Classification (par article, dans l'ordre de la table des matières) :
• 11D61 (11D57 - 11E76 - 11R09) • 11G (14G) • 11M06 (11M41) • 20G30 (20H05) •11G40 • 11G05 • 11T06 (11P05) • 11H55 • 11J91 • 11C20 (15A36) • 11R33 (14L30) • 11B75 •11G35 (14G25) • 11R34 • 11S20 • 11N13 (11M26) • 11K55 • 11F70 • 11T71 • 11N37 • 11E25 (11E20-11P21) • 22E40 (11E12 - 20H15) • 11J91 • 11A55 (11B25 - 11D09) • 11G25 •

Préface

Les dix-septièmes Journées Arithmétiques ont rassemblé à Genève 213 mathématiciens de 26 pays, du 9 au 13 septembre 1991. Treize conférenciers ont présenté des exposés généraux accessibles à l'ensemble du public; près d'une centaine de communications plus spécialisées ont été réparties en quatre sessions parallèles. Le présent volume contient les textes de quelques-uns de ces exposés.

Ce congrès s'est déroulé sous le patronage de la Société Mathématique Suisse. Il a en outre bénéficié du soutien des institutions suivantes:
Université de Genève; Fonds national suisse de la recherche scientifique; C.N.R.S.; Académie suisse des sciences naturelles; Société Académique (Genève); Etat de Genève; Etat du Valais; 3ème Cycle romand de mathématiques; Association Jan Hus (Lausanne); Caran d'Ache S.A. (Genève); I.B.M. (Suisse) S.A.

En ce qui concerne le présent volume, nous tenons à exprimer notre gratitude aux quelque 40 rapporteurs anonymes, qui avec efficacité et rapidité ont abattu un travail considérable. Leurs remarques et critiques ont formé une contribution essentielle à la composition, la forme, et parfois le fond de la version définitive de ces comptes rendus.

Daniel Coray et Y.-F. S. Pétermann

JA 91 *Genève*

Table des Matières

Préface 1
Table des matières 3
Liste des participants 5
Résumés et dates de réception des manuscrits 11

KÁLMÁN GYŐRY - Some recent applications of S-unit equations 17
MARC HINDRY - Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri) 39
K. RAMACHANDRA - On Riemann zeta-function and allied questions 57
A. RAPINCHUK - Congruence subgroup problem for algebraic groups: old and new 73
A.J. SCHOLL - Modular forms and algebraic K-theory 85
TETSUJI SHIODA - Some remarks on elliptic curves over function fields 99

YVETTE AMICE et BRUNO KAHN - Sommes de puissances dans les corps finis 115
A-M. BERGÉ, J. MARTINET et F. SIGRIST - Une généralisation de l'algorithme de Voronoï pour les formes quadratiques 137
VALÉRIE BERTHÉ - De nouvelles preuves "automatiques" de transcendance pour la fonction zêta de Carlitz 159
GAUTAMI BHOWMIK - Divisor functions of integer matrices: evaluations, average orders and applications 169
TED CHINBURG and BOAS EREZ - Equivariant Euler-Poincaré characteristics and tameness 179
GREGORY A. FREIMAN - On the structure and the number of sum-free sets 195
DAVID HARARI - Groupes de Brauer de certaines hypersurfaces 203
WERNER HÜRLIMANN - A short proof of the Albert-Brauer-Hasse-Noether theorem 215

W. JENKNER - Les corps p-adiques dont les groupes de Galois absolus sont isomorphes 221

J. KACZOROWSKI - The boundary values of generalized Dirichlet series and a problem of Chebyshev 227

A. and J. KNOPFMACHER - Metric properties of algorithms inducing Lüroth series expansions of Laurent series 237

JOAN-C. LARIO - Serre's conjecture on Galois representations attached to Weil curves with additive reduction 247

MIROSLAV LAŠŠÁK - Some remarks on the Pethö public key cryptosystem . 257

TOM MEURMAN - A simple proof of Voronoï's identity 265

B.Z. MOROZ - On representation of large integers by integral ternary positive definite quadratic forms 275

RUDOLF SCHARLAU and CLAUDIA WALHORN - Integral lattices and hyperbolic reflection groups 279

HIRONORI SHIGA - On the transcendency of the values of the modular function at algebraic points 293

S. SRINIVASAN - Two results in number theory 307

V.I. YANCHEVSKIĬ - K-unirationality of conic bundles over large arithmetic fields 311

Abstract 321

Liste des participants

Montserrat ALSINA I AUBACH	Universitat de Barcelona
Hédi AMARA	Université de Tunis
Francesco AMOROSO	Università di Padova
Jannis A. ANTONIADIS	University of Crete
Gabriel ARCHINARD	Université de Genève
Angela ARENAS	Universitat de Barcelona
Maurice ARRIGONI	Université de Besançon
Roland BACHER	Université de Genève
Christine BACHOC	Université de Bordeaux I
U. BALAKRISHNAN	Tata Institute, Bombay
Daniel BARSKY	Université Paris 13
Victor V. BATYREV	Univ. Gesamthochschule Essen
Abdelmejid BAYAD	Université de Bordeaux I
Eva BAYER	Université de Besançon
Anne-Marie BERGÉ	Université de Bordeaux I
Dominique BERNARDI	Université Paris 6
Valérie BERTHÉ	E. N. S. / Univ. Paris 11
Marie-José BERTIN	Université Paris 6
Daniel BERTRAND	Université Paris 6
Gautami BHOWMIK	Jesus & Mary College of New Delhi
Hervé BILLARD	Université Paris 7
Maria Isabel BINIMELIS BASSA	Universitat de Barcelona
Laure BLASCO	Université de Strasbourg
Jacek BOCHŃAK	Vrije Universiteit Amsterdam
Sigrid BÖGE	Universität Heidelberg
Xavier BOICHUT	Université de Paris-Nord
Jean-Pierre BOREL	Université de Limoges
Jan BRINKHUIS	Erasmus University, Rotterdam

Jerzy BROWKIN	Warsaw University
Jörg BRÜDERN	Universität Göttingen
Juliusz BRZEZIŃSKI	Chalmers Univ. of Technology, Göteborg
Peter BUNDSCHUH	Universität zu Köln
Catalina CALDERÓN GARCÍA	Universidad del País Vasco
Philippe CASSOU-NOGUÈS	Université de Bordeaux I
Pierrette CASSOU-NOGUÈS	Université de Bordeaux I
Emmanuel CATELAND	Université de Bordeaux I
Gongliang CHEN	Université de Saint-Étienne
Habib CHÉRIF	Université de Bordeaux I
V. I. CHERNOUSOV	Acad. of Sciences B. S. S. R., Minsk
Henri COHEN	Université de Bordeaux I
Mark David COLEMAN	University of Manchester
Jean-Louis COLLIOT-THÉLÈNE	C. N. R. S. / Université de Paris-Sud
J. Brian CONREY	Oklahoma State University
Daniel CORAY	Université de Genève
Capi CORRALES	Universidad Complutense de Madrid
Anne CORTELLA	Université de Besançon
Teresa DE DIEGO	Université Paris 7
Jean-Marie DE KONINCK	Université Laval
Ilaria DEL CORSO	Scuola Normale Superiore di Pisa
J. R. DELGADO	Universidad Complutense de Madrid
Jean-Marie DELLEY	Université de Genève
Laurent DENIS	Université Paris 6
Jean-Guy DIAZ	Université de Saint-Étienne
Francisco J. DIAZ Y DIAZ	Université de Bordeaux I
Jean-Claude DOUAI	Université Paris 6
François DRESS	Université de Bordeaux I
Eugène DUBOIS	Université de Caen
René DUSSAUD	Chambéry
Roberto DVORNICICH	Università di Pisa
Shalom ELIAHOU	Université de Genève
Carsten ELSNER	Universität Hannover
Michel EMSALEM	Université Paris 7
Boas EREZ	Harvard University
Valérie FLAMMANG	Université de Metz
Vincent FLECKINGER	Université de Besançon
Francois FOUCAULT	Caen

Étienne FOUVRY	Université de Paris-Sud
Günther FREI	E. T. H. Zürich
Gregory FREIMAN	Tel Aviv University
Jean FRESNEL	Université de Bordeaux I
Carlo GASBARRI	Università di Roma "La Sapienza"
Marie-Laure GAUNET	Université de Caen
Jan VAN GEEL	Rijksuniversiteit Gent
Roland GILLARD	Université de Grenoble I
Catherine GOLDSTEIN	Université de Paris-Sud
Marc GRANDET	Université de Toulouse
Georges GRAS	Université de Besançon
Marie-Nicole GRAS	Université de Besançon
Barry W. GREEN	Universität Heidelberg
Cornelius GREITHER	Universität München
Kálmán GYŐRY	University of Debrecen
Franz HALTER-KOCH	Karl-Franzens-Universität Graz
Jaroslav HANČL	University of Ostrava
David HARARI	École Normale Supérieure
G. N. TEN HAVE	University of Leiden
Marc HINDRY	Université Paris 7
Pascal HUBERT	E. N. S. Lyon
Werner HÜRLIMANN	Winterthur
Marc HUTTNER	Université de Lille
Aleksandar IVIĆ	University of Belgrade
Uwe JANNSEN	Universität zu Köln
Piotr JAWORSKI	Warsaw University
Arnaud JEHANNE	Université de Bordeaux I
Wolfgang JENKNER	Karl-Franzens-Universität Graz
Henri JORIS	Université de Lausanne
Jerzy KACZOROWSKI	Adam Mickiewicz University, Poznań
Bruno KAHN	Université Paris 7
Shigeru KANEMITSU	Kinki University in Kyushu
Michel KERVAIRE	Université de Genève
John KNOPFMACHER	University of the Witwatersrand
Michel KOSKAS	Université Paris 6 / E.N.S.
B. È. KUNYAVSKIĬ	Saratov Inst. for Mech. in Agriculture
Gilles LACHAUD	C. N. R. S. Marseille
Erich LAMPRECHT	Universität des Saarlandes

Joan-C. LARIO	Universitat politècnica de Catalunya
Miroslav LAŠŠÁK	Universitas Comenianae, Bratislava
Michel LAURENT	Université Paris 6 / C.N.R.S.
Odile LECACHEUX	Université Paris 6
Günter LETTL	Karl-Franzens-Universität Graz
Armin LEUTBECHER	Technische Universität München
Lutz LUCHT	Technische Universität Clausthal
Maria Dolors MAGRET PLANAS	Universitat politècnica de Catalunya
Yu. I. MANIN	Steklov Institute, Moscow
Constantin MANOIL	Université de Genève
František MARKO	Slovak Academy of Sciences, Bratislava
Roman MARSZALEK	Wroclaw University
Jacques MARTINET	Université de Bordeaux I
Richard MASSY	Université de Valenciennes
Roland MATTHES	Gesamthochschule Kassel
Marcin MAZUR	Warsaw University
Hartmut MENZER	Friedrich-Schiller Universität Jena
Armel MERCIER	Université du Québec à Chicoutimi
Tom MEURMAN	University of Turku
Philippe MICHEL	Université de Paris-Sud
Maurice MIGNOTTE	Université de Strasbourg
Jiří MOČKOŘ	University of Ostrava
Jesús MONTES PERAL	Universitat de Barcelona
Pieter MOREE	University of Leiden
Baruch ben Zelik MOROZ	Max-Planck Institut für Mathematik
Yoichi MOTOHASHI	Nihon University
M. Ram MURTY	McGill University
Kenji NAGASAKA	Hosei University
Shoichi NAKAJIMA	Tokyo University
Thong NGUYEN QUANG DO	Université de Besançon
Jean-Louis NICOLAS	Université de Lyon I
Gerhard NIKLASCH	Technische Universität München
Břetislav NOVÁK	Charles University, Prague
Michel OLIVIER	Université de Bordeaux I
Michel OUELLET	Collège de Sainte-Foy
PATHIAUX-DELEFOSSE	Université Paris 6
Isabelle PAYS	Université de Mons-Hainaut
Roger PAYSANT-LE-ROUX	Université de Caen

Marc PERRET	Université Aix-Marseille II
Bernadette PERRIN-RIOU	Université Paris 6
Y-F. S. PÉTERMANN	Université de Genève
Meinhard PETERS	Universität Münster
Emmanuel PEYRE	École Normale Supérieure
Albrecht PFISTER	Universität Mainz
Thanases PHEIDAS	University of Crete
Georges PHILIBERT	Université de Saint-Étienne
Constantin PIRON	Université de Genève
Carl POMERANCE	University of Georgia
Florian POP	Universität Heidelberg
Dimitrios POULAKIS	Université de Thessalonique
Heinz-Georg QUEBBEMANN	Universität Oldenburg
Jacques QUEYRUT	Université de Bordeaux I
Adolfo QUIRÓS	Universidad Autónoma de Madrid
K. RAMACHANDRA	Tata Institute, Bombay
Olivier RAMARÉ	Université de Bordeaux I
Philippe RAMBOUR	Université de Paris-Sud
A. S. RAPINCHUK	Acad. of Sciences B. S. S. R., Minsk
Winfried RECKNAGEL	Fachhochschule München
Georges RHIN	Université de Metz
Marcello ROBBIANI	E. T. H. Zürich
Guy ROBIN	Université de Limoges
José-Luis RUIZ	Universitat politècnica de Catalunya
Nicolas SABY	Université de Grenoble I
Éric SAIAS	Université Paris 6
Jürgen W. SANDER	Universität Hannover
Philippe SATGÉ	Université de Caen
Fumihiro SATO	Rikkyo University
Volker SCHÄFFER	Universität Hannover
Rudolf SCHARLAU	Universität Bielefeld
Andrzej SCHINZEL	P. A. N., Warsaw
Anthony J. SCHOLL	University of Durham
Rainer SCHULZE-PILLOT	Universität Bielefeld
Jean-Pierre SERRE	Collège de France
Hironori SHIGA	Chiba University
Tetsuji SHIODA	Rikkyo University
François SIGRIST	Université de Neuchâtel

Mariusz SKALBA	Warsaw University
A. N. SKOROBOGATOV	Acad. of Sciences U. S. S. R., Moscow
Abdelhakim SMATI	Université de Limoges
Bouchaïb SODAÏGUI	Université de Valenciennes
David SOLOMON	Université de Bordeaux I
S. SRINIVASAN	Tata Institute, Bombay
John STEINIG	Université de Genève
Peter STEVENHAGEN	Université de Besançon
Noriyuki SUWA	Tokyo Denki University
Sir Peter SWINNERTON-DYER	Cambridge University
Bogdan SZYDLO	Adam Mickiewicz University, Poznań
Jean-Daniel THÉROND	Université de Montpellier
Philippe TOFFIN	Université de Caen
George TOMANOV	Bulgarian Academy of Sciences
Chédly TOUIBI	Université de Tunis
David TRANAH	Cambridge University
Artur TRAVESA	Universitat de Barcelona
Yuri TSCHINKEL	M. I. T.
M. A. TSFASMAN	Acad. of Sciences U. S. S. R., Moscow
Stephen V. ULLOM	University of Illinois at Urbana
Keijo VÄÄNÄNEN	University of Oulu
Michel VÉRANT	Université de Besançon
VERGER-GAUGRY	Université de Grenoble I
Nuria VILA	Universitat de Barcelona
Carlo VIOLA	Università di Pisa
Albert VIOLANT I HOLZ	Universitat de Barcelona
S. G. VLĂDUŢ	Acad. of Sciences U. S. S. R., Moscow
V. E. VOSKRESENSKIĬ	Université de Samara
Michel WALDSCHMIDT	Université Paris 6
Rolf WALLISSER	Universität Freiburg i. Br.
Steve WILSON	University of Durham
Jie WU	Université de Nancy I
V. I. YANCHEVSKIĬ	Acad. of Sciences B. S. S. R., Minsk

Résumés

et dates de réception des manuscrits

Conférences

KÁLMÁN GYŐRY - **Some recent applications of S-unit equations** *26.3.92*

In this survey paper, some new applications of S-unit equations are presented to certain arithmetic graphs and irreducible polynomials, to a conjecture on common polynomial divisors of trinomials, to families of solutions of decomposable form equations, to certain generalized systems of S-unit equations, and to binary forms and decomposable forms of given discriminant. Further, some consequences of a generalization of Baker's type inequalities are discussed for S-unit equations.

MARC HINDRY - **Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)** *4.2.92 (remarque 'dernière minute' 5.5.92)*

I present the new proof of Mordell's conjecture found by Vojta and the generalization proven by Faltings: "a subvariety of an abelian variety has only finitely many points rational over a number field, whenever it contains no translate of subabelian variety". The paper also describes further simplifications due to Bombieri and some applications of these results, especially to the study of algebraic points of given degree on a curve.

K. RAMACHANDRA - **On Riemann zeta-function and allied questions** *13.9.91 (revised 'Postscript' 25.5.92)*

A. RAPINCHUK - **Congruence subgroup problem for algebraic groups: old and new** *5.11.91*

The paper is an up-to-date survey of the congruence subgroup problem. It contains the statement of Serre's conjecture on the congruence subgroup property for S-arithmetic subgroups of simple simply connected groups of S-rank ≥ 2, and most of the results that confirm it. Besides, some new methods of attacking the congruence subgroup problem are described which provide new examples of groups with the congruence subgroup property.

A.J. SCHOLL - **Modular forms and algebraic K-theory** *14.2.92*

This paper is a slightly expanded version of the talk given at the conference. We sketch an example of a non-trivial element of K_2 of a certain threefold, whose existence is related to the vanishing of an *incomplete* L-function of a modular form at $s = 1$. This is preceded with a simple account, for the non-specialist, of some of the conjectures (mostly due to Beilinson) which relate ranks of K-groups and orders of L-functions, supplemented by examples coming from modular forms.

TETSUJI SHIODA - **Some remarks on elliptic curves over function fields** *25.11.91*

As a supplement to my talk 'Mordell-Weil lattices and sphere packings' at JA91 in Geneva, I discuss some basic results on the L-function of an elliptic curve over a function field with a finite constant field, from the viewpoint of Mordell-Weil lattices. Some explicit examples are given.

Autres exposés

YVETTE AMICE et BRUNO KAHN - **Sommes de puissances dans les corps finis** *9.1.92*

The higher levels of a field F, studied among others by Parnami, Agrawal, Rajwade and Revoy, are defined like the ordinary level, as the smallest number of n-th power summands necessary to represent -1, where n is a power of 2. When F is a finite field $\mathbb{F}_q$ (q odd), the increasing sequence of higher levels stabilises from $h(q)$ on, where $h(q)$ is the dyadic valuation of $q-1$; its supremum is denoted here by $s(q)$. It appears that $s(q) = 2$ unless $q = p$ or p^3, with $p =$char F , and $s(p^3) = 2$ or 3. If $q = p$, the Weil (or Jacobi) sums estimates imply that $s(p) = 2$ as soon as $p \geq 2^{4h(p)}$. However, computations performed up to 10^9 hint that this bound is much too big in practice, and at least for small values of $h(p)$ ($h(p) \leq 7$), one has $s(p) = 2$ as soon as $p \geq 2^{2.72h(p)}$. Similarly, computations find no prime p such that $s(p^3) = 3$ up to $p = 101\,711\,873$. We believe that these experimental results exemplify general phenomena, but so far have no theoretical explanation for them.

A-M. BERGÉ, J. MARTINET et F. SIGRIST - **Une généralisation de l'algorithme de Voronoï pour les formes quadratiques** *7.1.92*

Ainsi que Voronoï l'a montré en 1908, les formes quadratiques définies positives *parfaites* de dimension donnée peuvent être classées au moyen d'un algorithme explorant un graphe. Les résultats récents de Jaquet pour la dimension 7 indiquent clairement que cette dimension marque la limite des possibilités actuelles.

Nous montrons dans cet article comment une extension de l'algorithme original permet de traiter des variantes utiles du problème initial, et en particulier de classer les formes parfaites avec groupe d'automorphismes donné.

VALÉRIE BERTHÉ - **De nouvelles preuves "automatiques" de transcendance pour la fonction zêta de Carlitz** *25.11.91*

Carlitz a défini une fonction ζ qui est l'analogue pour le corps fini $\mathbf{F}_q$ de la fonction ζ de Riemann. Yu a montré, en utilisant les modules de Drinfeld, que $\zeta(s)/\Pi^s$ est transcendant pour tout s non divisible par $q-1$, Π étant une série formelle analogue au réel π. Je donne ici une preuve par les automates de la transcendance de $\zeta(s)/\Pi^s$ pour $q \neq 2$ et $1 \leq s \leq q-2$, en utilisant le théorème de Christol, Kamae, Mendès France et Rauzy.

GAUTAMI BHOWMIK - **Divisor functions of integer matrices: evaluations, average orders and applications** *18.11.91*

We extend the concept of divisor functions to matrices over $\mathbb{Z}$ and prove a recursion in the size of the matrix. A special case of the Köcher zeta function helps us obtain average orders.

We give examples of connections of our results with Hecke algebras and partition functions.

TED CHINBURG and BOAS EREZ - **Equivariant Euler-Poincaré characteristics and tameness** *2.12.91*

In this paper we define an Euler-Poincaré characteristic which is the basis for generalizing to tame coverings of schemes the theory of the Galois module structure of rings of algebraic integers. First we define tame G-coverings of schemes $f : X \to Y$, where G is a finite group. Then, under the assumption that the schemes are proper and of finite type over a noetherian ring A and given T a coherent G-sheaf on X, we define the Euler-Poincaré characteristic $\chi R\Gamma^+(f_*((T))$, which is an element of the Grothendieck group $CT(AG)$ of all *finitely generated* AG-modules which are *cohomologically trivial* as G-modules. In fact the definition applies to certain complexes of sheaves on X which occur in applications. In an appendix we include a proof of a variant of the well known Lemma of Abhyankar characterizing tame G-coverings of schemes.

GREGORY A. FREIMAN - **On the structure and the number of sum-free sets** *13.9.91, and in revised form 10.6.92*

A finite set A of positive integers is called sum-free if $A \cap (A+A) = \emptyset$.

For n odd, $\{1, 3, 5, ..., n\}$ and $\left\{\frac{n+1}{2}, \frac{n+3}{2}, ..., n\right\}$ are examples of such sets.

Denote by m and ℓ, respectively, the largest and smallest elements of A and by a the cardinality of A.

We show that if the cardinality of the sum-free set A does not differ much from $\frac{\ell}{2}$, then A does not differ much from one of the two examples mentioned above. More precisely, if $a > \frac{5}{12}\ell + 2$, then either all elements of A are odd or A contains both odd and even integers and $m \geq a$.

It is shown that if $a > \frac{5}{12}\ell + 2$ then the number of such sum-free sets is $O(2^{n/2})$ which proves for such sets the conjecture of P. Cameron and P. Erdös.

DAVID HARARI - **Groupes de Brauer de certaines hypersurfaces** *25.11.91*

Soit k un corps de nombres, V l'hypersurface de $\mathbf{A}_k^n$ d'équation $y^2 - az^2 = f(x_1, ..., x_{n-2})g(x_1, ..., x_{n-2})$, avec $a \in k^* - k^{*2}$, f et g polynômes irréductibles de degré 2 premiers entre eux. Soient ϕ, ψ les formes quadratiques obtenues en homogénéisant f et g ; on suppose que l'intersection de leurs noyaux est réduite à 0. Soit X un modèle projectif lisse de V. Alors, quand $n \geq 6$, X vérifie le principe de Hasse et l'approximation faible. Quand $n = 5$, l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible pour X est la seule, et c'est encore le cas quand $n = 4$ si les coniques définies par ϕ, ψ sont lisses et se coupent transversalement suivant deux paires de points conjugués.

WERNER HÜRLIMANN - **A short proof of the Albert-Brauer-Hasse-Noether theorem** *28.10.91*

We present a short proof of the Albert-Brauer-Hasse-Noether theorem on the Brauer group of a global field. The connection between Galois cohomology and algebraic tori theory is emphasized.

Let K/k be a finite Galois extension of arbitrary fields with group G, then the relative Brauer group is $Br(K/k) \cong H^2(G, K^*) \cong H^1(G, T_1(K))$, where T_1 is the algebraic k-torus associated to the augmentation ideal I_G of G. When k is a global field, we use fundamental facts from algebraic tori theory, Tate-Nakayama duality and modern versions of Grunwald-Wang's lemma to deduce the short exact sequence

$$0 \longrightarrow Br(k) \longrightarrow \oplus Br(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where k_v runs over the completions of k at all places v of k.

W. JENKNER - **Les corps p-adiques dont les groupes de Galois absolus sont isomorphes** *14.11.91*

Soit p un nombre premier quelconque (on remarquera notamment le cas $p = 2$). On considère deux extensions finies K et L de $\mathbb{Q}_p$, contenues dans une clôture algébrique $\bar{\mathbb{Q}}_p$. Si les groupes de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ et $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$ sont des groupes topologiques isomorphes, on démontre que les sous-extensions abéliennes maximales de $K/\mathbb{Q}_p$ et de $L/\mathbb{Q}_p$ sont identiques.

J. KACZOROWSKI - **The boundary values of generalized Dirichlet series and a problem of Chebyshev** *24.9.91*

There is an old conjecture of Chebyshev saying that there are more primes $p \equiv 3 \pmod 4$ than $p \equiv 1 \pmod 4$. S. Knapowski and P. Turán have given a quantitative interpretation of this statement. We prove a theorem about the boudary values of general Dirichlet series and show its relevance to Chebyshev's problem. In particular it turns out that the Knapowski-Turán conjecture is false at least if we accept the Riemann Hypothesis for L-functions $(\mathrm{mod}\, 4)$.

A. and J. KNOPFMACHER - **Metric properties of algorithms inducing Lüroth series expansions of Laurent series** *18.11.91*

We investigate ergodic and metric properties of the polynomial 'digits' occuring in certain Lüroth-type series representations of formal Laurent series over finite fields. In particular, relative to Haar measure on power series with zero constant term, the results stated or derived in detail include the existence almost everywhere of a Khintchine-type constant, and of various other metric conclusions on the frequency or distribution of given 'digit values'.

JOAN-C. LARIO - **Serre's conjecture on Galois representations attached to Weil curves with additive reduction** *15.11.91, and in revised form 21.4.92*

In a joint work with P. Bayer [Ba-La 91] we verify Serre's conjecture (3.2.4$_?$) (in *Duke J.*) for the Galois representation defined by the p-torsion points of p-vertical Weil curves. In this paper our purpose is to emphasize the difference between the p-vertical and the p-horizontal cases in order to check Serre's conjecture. Several numerical examples, collected by computer calculations, lead us to give a conjecture which implies (3.2.4$_?$) for the horizontal case.

MIROSLAV LAŠŠÁK - **Some remarks on the Pethö public key cryptosystem** *18.11.91*

This note aims to point out that under certain conditions the public key cryptosystem introduced by Pethö in [1] can be broken in polynomial time. This gives some additional conditions which should be imposed on the choice of some parameters of the secret part of this system.

TOM MEURMAN - **A simple proof of Voronoï's identity** *1.11.91*

A comparatively simple proof of Voronoï's identity is given. The proof does not depend on the functional equation for the Riemann zeta-function nor on properties of Bessel functions.

B.Z. MOROZ - **On representation of large integers by integral ternary positive definite quadratic forms** *13.9.91, and in revised form 22.10.91*

We prove a conjecture of Heath-Brown to the extent that every sufficiently large integer congruent to 7 modulo 8 is represented by the quadratic form $x^2+y^2+p^3z^2$, where p is a rational prime congruent to 5 modulo 8 (in particular, by the form $x^2+y^2+125z^2$), and discuss some related results.

RUDOLF SCHARLAU and CLAUDIA WALHORN - **Integral lattices and hyperbolic reflection groups** *20.11.91, and in revised form 21.9.92*

The aim of this paper is to study arithmetic groups of isometries of hyperbolic spaces which are generated by hyperplane reflections. This leads to the notion of reflexive Lorenzian lattices.

The main contribution of this paper is to give many new examples of such lattices in dimensions 3 and 4. These lattices give rise to maximal, pairwise non-conjugate arithmetic reflexion groups on hyperbolic 3-space, respectively 4-space. The method belongs to the arithmetic theory of quadratic forms.

HIRONORI SHIGA - **On the transcendency of the values of the modular function at algebraic points** *11.11.91, and in revised form 22.1.92*

In this note we study an abelian variety A defined over $\overline{\mathbb{Q}}$. We characterize the abelian variety of CM type by its property of periods. The obtained result yields the criterion for algebraicity of the values of the Siegel modular function at algebraic points and of various other modular functions.

S. SRINIVASAN - **Two results in number theory** *13.12.91, and in revised form 11.6.92*
Here we present two results which were observed while studying a conjecture from S.K. Zaremba.

V.I. YANCHEVSKIĬ - **K-unirationality of conic bundles over large arithmetic fields** *15.11.91*

We prove that if a conic bundle surface over a rational curve is defined over a pseudo-real closed (or p-adically closed) field K and has a K-rational point then it is K-unirational. We also obtain the corresponding result for the so-called 'large' arithmetic fields K, which are suitable intersections of finitely many Henselizations of $\mathbb{Q}$.

Astérisque

KÁLMÁN GYÖRY

Some recent applications of S-unit equations

Astérisque, tome 209 (1992), p. 17-38

<http://www.numdam.org/item?id=AST_1992__209__17_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SOME RECENT APPLICATIONS OF S-UNIT EQUATIONS

Kálmán GYŐRY *

§ 1. Introduction

In 1988, we published with Evertse, Stewart and Tijdeman [11] a long survey article on S-unit equations and their applications. Since then much progress has been made in this fertile field. The purpose of this paper is to give a survey of some recent developments. In § 2, known finiteness theorems (cf. Theorems A, B) and some recent quantitative results (cf. Theorems 1, 2 and 3) are presented for S-unit equations. The proofs of Theorems A and 1 to 3 depend on the Thue-Siegel-Roth-Schmidt method and its p-adic generalization. §§ 3 to 6 are devoted to recent applications of the mentioned results. In § 3, finiteness theorems are established for certain arithmetic graphs (cf. Theorem 4) and irreducible polynomials of the form $g(f(X))$ (cf. Theorem 5). These are considerable improvements of earlier theorems obtained in this direction, and furnish definitive results in a sense. The results of Schinzel and the author in § 4 (cf. Theorem 6) resolve a conjecture of Posner and Rumsey [28] on common polynomial divisors of trinomials. § 5 is concerned with generalizations for decomposable form equations (cf. Theorem 7, 8) of finiteness theorems of Schmidt [34], Schlickewei [30] and Laurent [25] on families of solutions of norm form equations. Uniform upper bounds are given for the number of families of solutions. As a consequence, bounds are derived for the number of solutions, provided that this number is finite (cf. Corollary 1).

* Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

A further consequence is deduced in § 6 for some generalized systems of S-unit equations (cf. Theorem 9). It provides, over number fields, a quantitative version of a more general result of Laurent [25].

The results treated in §§ 2 to 6 are all ineffective. Baker's effective method and its p-adic analogue made it possible to establish an effective finiteness theorem (cf. Theorem C in § 7) for S-unit equations in two unknowns. As a recent application of Theorem C, in § 8 an effective finiteness theorem (cf. Theorem 10) of Evertse and the author is presented for decomposable forms of given discriminant. It makes effective in a more general form an ineffective theorem of Birch and Merriman [2] on binary forms. Apart from certain particular cases, no effective results are known for S-unit equations in more than two unknowns. In § 7 we state a generalization of Baker's type inequalities (cf. Proposition) whose effective resolution would imply effective versions of all results of this paper.

Theorems A, B and C were already treated in [11], while Theorems 1 to 10 have been obtained since 1988. The complete proofs of Theorems 4 to 8 and 10 will be published in Győry [18, Part II], [14, Part IV], [20], Győry and Schinzel [21] and Evertse and Győry [9], [10].

It is impossible to deal with all recent applications of unit equations within the frame of the present paper. Further applications have recently been obtained for instance to diophantine equations and irreducible polynomials of other type, modular forms, pairs of polynomials and binary forms of given resultant, recurrence sequences, group theory, algebraic number theory and transcendental number theory. Some generalizations and analogues have also been established over finitely generated domains and function fields, respectively.

§ 2. S-unit equations; ineffective results

We introduce some notation which will be used throughout this paper. Let K be an algebraic number field, O_K the ring of integers of K, and O_K^* the unit group[1] of O_K. Further, let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a finite set of prime ideals in O_K, and put

$$O_S = \{\alpha \in K : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \ \text{ for all prime ideals } \mathfrak{p} \text{ of } O_K \text{ with } \mathfrak{p} \notin S\}.$$

Then O_S is a subring of K which is called the ring of S-integers. It contains O_K as a subring. The units of O_S, i.e. the invertible elements are called S-units.

[1] In general, if R is an integral domain then R^* will denote its group of units; thus if R is a field then $R^* = R \setminus \{0\}$.

They form a multiplicative group which is denoted by O_S^*. Put $d = [K : \mathbb{Q}]$ and $s = r + t + 1$ where r denotes the unit rank of O_K^*. Thus $r \leq d - 1$.

Many problems of number theory can be reduced to equations of the form

$$\alpha_1 x_1 + \alpha_2 x_2 = 1 \text{ in } x_1, x_2 \in O_S^* \tag{1}$$

or, more generally,

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in O_S^* \tag{2}$$

where $\alpha_1, \ldots, \alpha_n$ are elements of K^*. Equation (2) is called an *S-unit equation in n unknowns*. For $n > 2$, it can happen that for a solution $x_1, \ldots, x_n$, the left hand side of (2) has a vanishing subsum. In this case the solution is called *degenerate*, otherwise *non-degenerate*. If (2) has a degenerate solution and if O_S^* is infinite then (2) has infinitely many solutions. Denote by $\mu_n(\alpha_1, \ldots, \alpha_n)$ the number of non-degenerate solutions of (2). Several results have been obtained on $\mu_n(\alpha_1, \ldots, \alpha_n)$; for references see [37] and [11]. Using the Thue-Siegel-Roth-Schmidt method, van der Poorten and Schlickewei [26] (see also [27]) and Evertse [3] proved independently of each other the following

THEOREM A. *For $n \geq 2$ we have $\mu_n(\alpha_1, \ldots, \alpha_n) < \infty$.*

The next quantitative result was established by Evertse [4].

THEOREM B. *We have*

$$\mu_2(\alpha_1, \alpha_2) \leq 3 \times 7^{d+2s}. \tag{3}$$

In 1988, we derived with Evertse [7] an upper bound for $\mu_n(\alpha_1, \ldots, \alpha_n)$ which is independent of $\alpha_1, \ldots, \alpha_n$. Recently this has been made explicit by Schlickewei [31] who proved

THEOREM 1. *For $n \geq 2$, we have*

$$\mu_n(\alpha_1, \ldots, \alpha_n) \leq \exp\{2^{36nd!} \cdot s^6 \log(4sd!)\}. \tag{4}$$

Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

The proof is based on Schlickewei's p-adic generalization [32] of the quantitative Subspace Theorem of Schmidt [35]. Very recently Evertse (private communication) has improved (4) in terms of d to

$$\mu_n(\alpha_1,\dots,\alpha_n) \le \exp\{2^{37nd}\cdot s^6\log(8sd!)\}. \tag{5}$$

The dependence on d is much weaker in (4) and (5) than in (3). Probably s^6 can be improved to s.

We call two n-tuples $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ in $(K^*)^n$ (and the corresponding S-unit equations) *S-equivalent* if $\alpha_i'/\alpha_i \in O_S^*$ for $i=1,\dots,n$. If $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ are S-equivalent then $\mu_n(\alpha_1,\dots,\alpha_n) = \mu_n(\alpha_1',\dots,\alpha_n')$. We showed with Evertse, Stewart and Tijdeman [12] (see also [11]) that $\mu_2(\alpha_1,\alpha_2)\le 2$ for all but finitely many S-equivalence classes of pairs $(\alpha_1,\alpha_2)\in(K^*)^2$. Further, we pointed out that if O_S^* is infinite then there are infinitely many S-equivalence classes of pairs (α_1,α_2) for which (1) has two solutions. The proof of the above estimate depends among other things on the fact that $\mu_n := \mu_n(1,1,\dots,1)$ is finite for all $n\le 5$. Following the proof of [12] it is easy to show that apart from at most $\mu_5+12\mu_3+30\mu_2^2$ S-equivalence classes of pairs (α_1,α_2), we have $\mu_2(\alpha_1,\alpha_2)\le 2$ (see e.g. [19] or [21]). Hence, in view of Theorem 1, the above-mentioned result of [12] can be stated in the following quantitative form.

THEOREM 2. *Apart from at most*

$$\exp\{2^{180d!}\cdot s^6\log(2(4sd!))\}$$

S-equivalence classes of pairs $(\alpha_1,\alpha_2)\in(K^*)^2$, we have $\mu_2(\alpha_1,\alpha_2)\le 2$. Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

It was shown in [12] that for $n>2$, there can exist infinitely many S-equivalence classes of equations (2) with "many" non-degenerate solutions. Hence Theorem 2 cannot be generalized in this sense to solutions of (2). There is, however, another possibility for generalization. Denote by $\nu_n(\alpha_1,\dots,\alpha_n)$ the minimal number of $(n-1)$-dimensional linear subspaces of K^n whose union contains all solutions of (2). Theorem 1 implies an upper bound for $\nu_n(\alpha_1,\dots,\alpha_n)$. In 1988, we proved with Evertse [7] that apart from finitely many S-equivalence classes of equations (2), $\nu_n(\alpha_1,\dots,\alpha_n) < 2^{(n+1)!}$ holds. Recently, Evertse [5] improved this bound to $(n!)^{2n+2}$, and applied his estimate to decomposable form equations.

Following the proof of [7], one can derive $\mu_{(n+1)!-1}^{n-1}$ as an upper bound for the number of exceptional S-equivalence classes in question. Together with Theorem 1 this implies that the result of [7] under consideration can now be enunciated in the following quantitative form.

THEOREM 3. *Apart from at most*

$$\exp\{n2^{36(n+1)!d!} \cdot s^6 \log(4sd!)\}$$

S-equivalence classes of n-tuples $(\alpha_1, \ldots, \alpha_n) \in (K^*)^n$, *we have* $\nu_n(\alpha_1, \ldots, \alpha_n) < 2^{(n+1)!}$. *Further, if* K *is a normal extension of* $\mathbb{Q}$ *then* $d!$ *can be replaced by* d.

For $n = 2$, $\nu_2(\alpha_1, \alpha_2) = \mu_2(\alpha_1, \alpha_2)$ holds. Thus, for $n = 2$, Theorem 3 gives a weaker version of Theorem 2. The proof of Theorem 3 will be published in a joint paper with Tijdeman, together with some generalizations and further related results.

It is likely that combining the proof of [5] with Theorem 1, the bound $2^{(n+1)!}$ in Theorem 3 can be improved to $(n!)^{2n+2}$. However, this bound $(n!)^{2n+2}$ is still probably far from being best possible. Theorem 3 and its possible improvements would have applications, e.g. to decomposable form equations (cf. [5]).

§ 3. Applications to irreducible polynomials and arithmetic graphs

Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a finite subset of O_K. For given $N \geq 1$, we denote by $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ the simple graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs $[\alpha_i, \alpha_j]$ such that $\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i - \alpha_j)\right| > N$. The ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ and $\mathcal{A}' = \{\alpha_1', \ldots, \alpha_m'\}$ of O_K are called *equivalent* if $\alpha_i' = \varepsilon\alpha_i + \beta$ for some $\varepsilon \in O_K^*$ and $\beta \in O_K$, $i = 1, \ldots, m$. Then the graphs $\mathcal{G}_K(\mathcal{A}, N)$ and $\mathcal{G}_K(\mathcal{A}', N)$ are isomorphic.

Many diophantine problems, for example related to reducibility of polynomials, pairs of polynomials of given resultant, decomposable form equations or algebraic number theory lead to the study of connectedness properties of graphs $\mathcal{G}_K(\mathcal{A}, N)$ (see [17], [11], [18] and the references given there). Let $m \geq 3$. Using Theorem C of the present paper on S-unit equations in two unknowns, we proved in [17] (see also [11]) in a more precise and effective form that for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ has either

(i) a connected component of order at least $m - 1$,

or

(ii) two connected components of order ≥ 2 which are complete.

This result and its various other variants have been used to solve the diophantine problems mentioned.

For certain applications, for instance to irreducible polynomials (see Theorem 5 below) it is crucial to eliminate the possibility (ii) from the above

statement. Recently, we have proved in [18, Part II] (see also [18, Part I]) a more precise and quantitative version of the following theorem.

THEOREM 4. *Let m be a positive integer different from 4. Then for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ has a connected component of order at least $m-1$.*

In the case $m = 4$, we described in [18] the exceptions having property (ii). In the proof, we used the above-mentioned result of Evertse and myself [7] on S-unit equations. Further, to prove the quantitative version, we needed Theorem 1.

For given $m > 4$, we shall now sketch the proof that apart from finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ cannot have property (ii). In contrast with [18, Part II], here Theorem 2 will be used in a qualitative form. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be an arbitrary ordered subset of O_K for which $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ has two connected components, say $\mathcal{G}_1$ and $\mathcal{G}_2$, with orders ≥ 2 such that both $\mathcal{G}_1$ and $\mathcal{G}_2$ are complete. We may assume without loss of generality that $\{\alpha_1, \ldots, \alpha_k\}$ and $\{\alpha_{k+1}, \ldots, \alpha_{k+l}\}$ are the vertex sets of $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively. Then we have

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i - \alpha_j)\right| \leq N \tag{6}$$

for each i, j with $1 \leq i \leq k$, $k+1 \leq j \leq k+l$. Denote by S the set of all prime ideals in O_K with norm at most N. Then all $\alpha_i - \alpha_j$ satisfying (6) are S-units. For distinct i, i' with $1 \leq i, i' \leq k$, we have

$$\alpha_i - \alpha_{i'} = (\alpha_i - \alpha_j) + (\alpha_j - \alpha_{i'}) \text{ for } j = k+1, \ldots, k+l.$$

Now Theorem 2 implies that apart from an S-unit factor ε, $\alpha_i - \alpha_{i'}$ can assume only finitely many values, say β. But using Theorem B for fixed β, it follows from

$$\beta = (\alpha_i - \alpha_j)/\varepsilon + (\alpha_j - \alpha_{i'})/\varepsilon, \quad j = k+1, \ldots, k+l$$

that $(\alpha_i - \alpha_j)/\varepsilon$ and $(\alpha_j - \alpha_{i'})/\varepsilon$ can assume only finitely many values. Hence the same holds for $(\alpha_p - \alpha_q)/\varepsilon$ for all distinct p, q with $1 \leq p, q \leq m$. Thus $\mathcal{A} = \varepsilon\mathcal{A}' + \alpha_1$ for some ordered subset $\mathcal{A}'$ of O_K whose elements can assume only finitely many values. This proves our claim.

We present now an application of Theorem 4 to irreducible polynomials. I. Schur, A. Brauer, R. Brauer, H. Hopf, I. Seres and others investigated the reducibility of polynomials of the form $f(g(X))$, where f, g are monic polynomials with coefficients in $\mathbb{Z}$, g is irreducible over $\mathbb{Q}$ and the roots of f are

distinct rational integers. For a survey of results obtained in this direction, see [14]. In [14] I extended these investigations to the case when the roots of f are distinct elements of an arbitrary but fixed totally real algebraic number field K of degree d. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be the set of roots of such a monic polynomial $f \in \mathbb{Z}[X]$. Further, suppose that $g \in \mathbb{Z}[X]$ is an irreducible monic polynomial whose splitting field over $\mathbb{Q}$ is a CM-field, i.e. a totally imaginary quadratic extension of a totally real algebraic number field. In this case we say that $g(X)$ is of *CM-type*. If $g(f(X))$ is reducible then so are $g(f(X+a))$ for all $a \in \mathbb{Z}$. Such polynomials $f(X), f(X+a)$ are called *equivalent*. I showed that if the graph $\mathcal{G}_K(\mathcal{A}, N)$ for $N = 2^d|g(0)|^{d/\deg(g)}$ has a connected component with v vertices, then the number of irreducible factors of $g(f(X))$ over $\mathbb{Q}$ is at most $\deg(f)/v$. Further, this estimate is in general best possible (cf. [14, Part II]). Hence it is easy to deduce from Theorem 4 the following

THEOREM 5. *Let $g \in \mathbb{Z}[X]$ be an irreducible monic polynomial of CM-type. There are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[X]$ with degree greater than 4 and with distinct roots in K such that $g(f(X))$ is reducible over $\mathbb{Q}$.*

This theorem is in a certain sense a considerable refinement of Theorem 1 of [14, Part III]. We should, however, remark that this theorem of [14] was established in an effective way and over an arbitrary totally real ground field instead of $\mathbb{Q}$.

Recently, we have obtained in [14, Part IV] a more precise version of Theorem 5. There can exist infinitely many pairwise inequivalent exceptions $f(X)$ of degree 4 for which $g(f(X))$ is reducible for a suitable $g(X)$. We give in [14, Part IV] a precise description of these exceptions. Further, we show that Theorem 5 does not remain valid for any irreducible monic polynomial $g \in \mathbb{Z}[X]$ and for any number field K.

§ 4. Applications to common polynomial divisors of trinomials

Using the terminology of [28], for $i \geq 2$ we shall mean by a monic i-nomial over $\mathbb{Q}$ a polynomial of the form $X^{m_1} + a_2X^{m_2} + \cdots + a_{i-1}X^{m_{i-1}} + a_i$ over $\mathbb{Q}$ with $m_1 > m_2 > \cdots > m_{i-1} > 0$. If $p(X)$ and $s(X)$ are polynomials over $\mathbb{Q}$ with $\deg(s) \leq i-1$ such that $p(X) \mid s(X^r)$ over $\mathbb{Q}$ for some integer $r \geq 1$ then $p(X)$ divides infinitely many i-nomials over $\mathbb{Q}$. Indeed, the vector space of polynomials in $\mathbb{Q}[X]$ modulo $s(X)$ is at most $(i-1)$-dimensional, and hence $s(X)$ divides infinitely many i-nomials $T(X)$ over $\mathbb{Q}$. But then $s(X^r) \mid T(X^r)$ and so $p(X) \mid T(X^r)$ over $\mathbb{Q}$. Conversely, Posner and Rumsey [28] made in 1965 the following conjecture: *If a polynomial with rational coefficients divides*

infinitely many monic i-nomials over $\mathbb{Q}$, then it divides a non-zero polynomial in $\mathbb{Q}[X]$ with degree less than i in X^r for some $r \geq 1$.

For $i = 2$ the conjecture is obvious. For $i = 3$, Posner and Rumsey [28] proved a weaker version of their conjecture. Recently, we have proved with Schinzel [21] that the conjecture is true for $i = 3$ and false for every $i \geq 4$. The disproof for the case $i \geq 4$ is elementary. For $i = 3$, we obtained with Schinzel the following stronger assertion.

THEOREM 6. *Let $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$, k the number of distinct roots of $p(X)$, K the splitting field of $p(X)$ over $\mathbb{Q}$, $d = [K : \mathbb{Q}]$, S the set of places of K consisting of all infinite places and all valuations induced by the prime ideal divisors of the non-zero roots of $p(X)$, and $s = \mathrm{Card}(S)$. If $p(X)$ divides more than*

$$\exp\{(s^6 \cdot 2^{180d} + 8sk)\log(4sd)\}$$

monic trinomials over $\mathbb{Q}$, then it divides a linear or quadratic polynomial in X^r over $\mathbb{Q}$ for some integer $r \geq 1$.

The proof depends on Theorems B and 2 on S-unit equations. We sketch the basic idea of the proof. The details will be published in [21].

Let $T(X) = X^m + aX^n + b$ be a trinomial over $\mathbb{Q}$ which is divisible by $p(X)$. If $p(X)$ is divisible by X or if $ab = 0$, the assertion easily follows. Hence it suffices to deal with the case when $X \nmid p(X)$ and $ab \neq 0$. It is easy to show that $p(X)$ can be written in the form $p(X) = p_1(X) \cdot p_2^2(X)$ where p_1, p_2 are relatively prime squarefree polynomials in $\mathbb{Q}[X]$. Denote by $\xi_1, \ldots, \xi_k$ the distinct roots of $p_1(x) \cdot p_2(x)$, and by S the set of all prime ideal divisors of $\xi_1 \cdots \xi_k$ in O_K. Then, for $j = 1, \ldots, k$, (ξ_j^m, ξ_j^n) is a solution of the S-unit equation

$$(-1/b)x_1 + (-a/b)x_2 = 1 \text{ in } x_1, x_2 \in O_S^*. \tag{7}$$

If (7) has at most 2 solutions, then the assertion can be proved by means of some elementary arguments from algebraic number theory. On the other hand, if $p(X)$ divides trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equation (7) has more than 2 solutions, then one can use Theorem 2 to derive an upper bound for the number of S-equivalence classes of these equations (7). If now there are sufficiently many trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equations (7) are S-equivalent, then one can show by means of Theorem B that there is an integer $r \geq 1$ such that ξ_j^r assumes the same value, say c, for $j = 1, \ldots, k$. Here $c \in \mathbb{Q}^*$ and $p(X) \mid (X^r - c)^2$ over $\mathbb{Q}$, which proves the assertion of Theorem 6.

§ 5. Applications to decomposable form equations

In this section, we present some generalizations to decomposable form equations of well-known finiteness theorems of Schmidt, Schlickewei and Laurent concerning families of solutions of norm form equations.

Let $\mathfrak{M}$ be an O_S-lattice, i.e. a finitely generated O_S-submodule of some K-vector space. Consider a *decomposable form* $F(\mathbf{x})$ on

$$K\mathfrak{M} := \{\lambda \mathbf{x} : \lambda \in K,\ \mathbf{x} \in \mathfrak{M}\}$$

over K, i.e. a function $F\colon K\mathfrak{M} \to K$ for which there are an $\alpha \in K^*$, a finite and normal field extension G/K and K-linear functions $l_1, \ldots, l_f\colon K\mathfrak{M} \to G$ such that $F(\mathbf{x}) = \alpha \prod_{i=1}^{f} l_i(\mathbf{x})$ for all $\mathbf{x} \in K\mathfrak{M}$ (for this general definition, see e.g. [9]). We may assume that G is the splitting field of F, i.e the smallest extension of K over which F factorizes into linear functions. Suppose that $n := \dim_K K\mathfrak{M} \geq 2$ and that $\{l_1, \ldots, l_f\}$ contains n linearly independent functions over G. If in particular $K\mathfrak{M} = K^n$ and $\mathbf{e}_1 = (1, 0, \ldots, 0)^T, \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)^T$ is the standard basis of K^n, we identify $F(\mathbf{x})$ on K^n with the homogeneous polynomial $F(\mathbf{X}) = F(X_1\mathbf{e}_1 + \cdots + X_n\mathbf{e}_n) \in K[X_1, \ldots, X_n]$. This homogeneous polynomial is also called a decomposable form.

Let $\beta \in O_S \setminus \{0\}$ and consider the *decomposable form equation*

$$F(\mathbf{x}) \in \beta O_S^* \ \text{ in } \ \mathbf{x} \in \mathfrak{M}. \tag{8}$$

Put $\mathcal{J} = \{1, \ldots, f\}$. We may assume that $l_i = l_j$ if l_i and l_j are linearly dependent over G and that $\sigma(l_j) = l_{\sigma(j)}$ for all $j \in \mathcal{J}$ and $\sigma \in \mathrm{Gal}(G/K)$, where $(\sigma(1), \ldots, \sigma(f))$ is a permutation of $(1, \ldots, f)$. In the special case when $F(\mathbf{x}) = \alpha \prod_{\sigma \in \mathrm{Gal}(G/K)} \sigma(l_1(\mathbf{x}))$, $F(\mathbf{x})$ is in fact a *norm form* over K, and (8) is a *norm form equation*. Denote by $\mathbf{M}$ the set of tuples $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_f) \in G^f$ for which $\lambda_i = \lambda_j$ if $l_i = l_j$, $i, j \in \mathcal{J}$ and $\sigma(\lambda_i) = \lambda_{\sigma(i)}$ for all $i \in \mathcal{J}$ and $\sigma \in \mathrm{Gal}(G/K)$. Defining the product of $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbf{M}$ componentwise, $\mathbf{M}$ becomes a K-subalgebra of G^f with unit element $\mathbf{1} = (1, \ldots, 1)$. We denote by $\mathbf{M}^*$ the multiplicative group of invertible elements of $\mathbf{M}$, and by $N(\boldsymbol{\lambda})$ the product of components of $\boldsymbol{\lambda} \in \mathbf{M}$. This function $N\colon \mathbf{M} \to K$ is clearly multiplicative. The linear mapping $\Psi\colon K\mathfrak{M} \to G^f\colon \mathbf{x} \mapsto (l_1(\mathbf{x}), \ldots, l_f(\mathbf{x}))$ is injective. Further, $\Psi(K\mathfrak{M})$ is contained in $\mathbf{M}$. Put $\mathcal{M} = \Psi(\mathfrak{M})$. Then $\mathcal{M}$ is an O_S-lattice in $\mathbf{M}$ and Ψ induces an isomorphism betweer $\mathfrak{M}$ and $\mathcal{M}$ (as well as between $K\mathfrak{M}$ and $K\mathcal{M}$). We say that $\mathcal{M}$ is *full* (in [illegible] $K\mathcal{M} = \mathbf{M}$. It will be more convenient to consider (8) in the form

$$\alpha \mathrm{N}(\boldsymbol{\mu}) \in \beta O_S^* \ \text{ in } \ \boldsymbol{\mu} \in \mathcal{M}. \tag{9}$$

If in particular $F(\mathbf{x})$ is a norm form then (9) becomes the norm form equation

$$\alpha \mathrm{N}_{M/K}(\boldsymbol{\mu}) \in \beta O_S^* \text{ in } \boldsymbol{\mu} \in \mathcal{M}, \tag{10}$$

where $\mathcal{M}$ denotes now the O_S-module $\{l_1(\mathbf{x}) : \mathbf{x} \in \mathfrak{M}\}$ and M is a suitable subfield of G containing K and $K\mathcal{M}$.

A partition $\mathrm{I} = \{A_1, \dots, A_h\}$ of $\mathcal{J}$ is called symmetric if $i, j \in \mathcal{J}$ belong to the same subset if $l_i = l_j$, and if $\sigma(A_1), \dots, \sigma(A_h)$ is a permutation of $A_1, \dots, A_h$ for every $\sigma \in \mathrm{Gal}(G/K)$. For a symmetric partition $\mathrm{I} = \{A_1, \dots, A_h\}$ of $\mathcal{J}$, we denote by $\mathbf{L} = \mathbf{L}(\mathrm{I})$ the subset of $\mathbf{M}$ consisting of those elements $\boldsymbol{\lambda} = (\lambda_i)_{i \in \mathcal{J}}$ of $\mathbf{M}$ for which $\lambda_i = \lambda_j$ whenever i and j belong to the same subset in the partition I. Then $\mathbf{L}$ is a K-subalgebra of $\mathbf{M}$ with $\mathbf{1}$. If in particular $\mathrm{I} = \{\mathcal{J}\}$ then we write $\mathbf{K}$ for $\mathbf{L}(\mathcal{J})$. Further, $\mathbf{M} = \mathbf{L}(\mathrm{I}_0)$ for the partition I_0 for which $i, j \in \mathcal{J}$ belong to the same subset if and only if $l_i = l_j$. The subrings of $\mathbf{M}$ with $\mathbf{1}$ are precisely the subalgebras $\mathbf{L}(\mathrm{I})$ where I is a symmetric partition of $\mathcal{J}$.

Let $\mathbf{L} = \mathbf{L}(\mathrm{I})$ with a symmetric partition I of $\mathcal{J}$, and denote by $\mathbf{O}_{S,\mathbf{L}}$ the set of those elements $\boldsymbol{\lambda} = (\lambda_i)_{i \in \mathcal{J}}$ of $\mathbf{L}$ for which all components λ_i are integral over O_S. Then $\mathbf{O}_{S,\mathbf{L}}$ is a subring of $\mathbf{L}$ with unit element $\mathbf{1}$. Its unit group is denoted by $\mathbf{O}_{S,\mathbf{L}}^*$. Let $\mathcal{M}^{\mathbf{L}}$ denote the set of all elements $\boldsymbol{\mu} \in \mathcal{M}$ for which $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in K\mathcal{M}$ for every $\boldsymbol{\lambda} \in \mathbf{L}$. One can show that in this case $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in K\mathcal{M}^{\mathbf{L}}$, that $\mathcal{M}^{\mathbf{L}}$ is an O_S-sublattice of $\mathcal{M}$, that $\mathcal{M}^{\mathbf{K}} = \mathcal{M}$, and that $\mathcal{M}^{\mathbf{M}} = \mathcal{M}$ if $\mathcal{M}$ is full. We say that $\mathbf{L}$ is *admissible* with respect to $\mathcal{M}$ or simply admissible if $\mathcal{M}^{\mathbf{L}} \cap \mathbf{M}^* \neq \varnothing$ and if there is no subalgebra $\mathbf{L}'$ with $\mathbf{1}$ in $\mathbf{M}$ such that $\mathbf{L}' \supsetneq \mathbf{L}$ and $K\mathcal{M}^{\mathbf{L}'} = K\mathcal{M}^{\mathbf{L}}$. We note that if $\mathcal{M}$ is full then $\mathbf{M}$ is admissible. For an admissible subalgebra $\mathbf{L}$ of $\mathbf{M}$, denote by $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$ the set of those $\boldsymbol{\lambda} \in \mathbf{L}$ for which $\boldsymbol{\lambda} \cdot \boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$ for all $\boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$. Then $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$ is a subring of $\mathbf{O}_{S,\mathbf{L}}$ with $\mathbf{1}$ which contains O_S as a subring (identifying the elements λ of O_S with $\boldsymbol{\lambda} = (\lambda, \dots, \lambda)$). Further, $K\mathcal{D}_{\mathcal{M}}^{\mathbf{L}} = \mathbf{L}$. Denote by $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$ the unit group of $\mathcal{D}_{\mathcal{M}}^{\mathbf{L}}$. One can show that $\mathfrak{I}_{\mathbf{L}} := [\mathbf{O}_{S,\mathbf{L}}^* : \mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}]$ is finite. If $\boldsymbol{\mu} \in \mathcal{M}^{\mathbf{L}}$ is a solution of (9) then so is every element of $\boldsymbol{\mu}\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$. Then the set $\boldsymbol{\mu}\mathcal{D}_{\mathcal{M}}^{\mathbf{L}\,*}$ is called a *family of solutions* or more precisely an $(\mathcal{M}, \mathbf{L})$-*family of solutions* of (9). Further, a family of solutions is called *maximal* if it is not properly contained in another family of solutions. Every solution is contained in a maximal family of solutions.

We shall state our results in a quantitative form. Hence we need some further notation. Denote by D the degree of the normal closure of G over $\mathbb{Q}$. Let $m = n$ or $m = n + 1$ according as $\mathfrak{M}$ is free or not. One can show that m is the minimum of the cardinalities of the sets of generators of $\mathfrak{M}$. Assume that F is integral on $\mathfrak{M}$, i.e. that for some set of generators $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ of $\mathfrak{M}$, the polynomial $F(\sum_{j=1}^m X_j \mathbf{a}_j)$ has their coefficients in O_S. This notion of integrality is independent of the choice of $\mathbf{a}_1, \dots, \mathbf{a}_m$. For $\beta \in O_S \setminus \{0\}$, (β) denotes the O_S-ideal generated by β, $\tau_m(\beta)$ is the number of factorizations

of (β) into m integral ideals in O_S, and $\omega(\beta)$ is the number of distinct prime ideal divisors of (β) in O_S. Further, r denotes the maximal number of pairwise linearly independent linear functions in $\{l_i\}_{i\in\mathcal{J}}$ over G, and u is the maximum of the degrees of the irreducible factors of F over K. Throughout this section, let

$$C = \binom{r}{m-1}^{\omega(\beta)} \tau_m(\beta^u).$$

In the non full case, the proof of the next theorem involves among other things Theorem 1 on S-unit equations.

THEOREM 7. *The set of solutions of* (9) *is the union of at most* $\sum_{\mathbf{L}} \mathfrak{I}_{\mathbf{L}}$ *families of solutions, where the sum is taken over at most*

$$C \cdot \exp\{2^{37nD} \cdot s^6 \log(4sD)\} \tag{11}$$

admissible subalgebras $\mathbf{L}$ *of* $\mathbf{M}$ *(for which* (9) *has an* $(\mathcal{M}, \mathbf{L})$*-family of solutions, and among which there can be identical subalgebras* $\mathbf{L}$*). Further, if* $\mathcal{M}$ *is full in* $\mathbf{M}$ *then* $C \cdot \mathfrak{I}_{\mathbf{M}}$ *is an upper bound for the number of families of solutions in question.*

The following theorem can be deduced from Theorem 7.

THEOREM 8. *Equation* (9) *has at most* $\sum_{\mathbf{L}} \mathfrak{I}_{\mathbf{L}}$ *maximal families of solutions, where the sum is taken over at most*

$$Cn^r \exp\{2^{37nD} \cdot s^6 \log(4sD)\} \tag{12}$$

admissible subalgebras $\mathbf{L}$ *of* $\mathbf{M}$ *(for which* (9) *has a maximal* $(\mathcal{M}, \mathbf{L})$*-family of solutions, and among which there can be identical subalgebras* $\mathbf{L}$*). Further, if* $\mathcal{M}$ *is full in* $\mathbf{M}$ *then* (9) *has at most* $C \cdot \mathfrak{I}_{\mathbf{M}}$ *maximal families of solutions and all these are* $(\mathcal{M}, \mathbf{M})$*-families of solutions.*

We remark that in our bounds, the factor $\mathfrak{I}_{\mathbf{L}}$ cannot be omitted. Further, $D \leq (dr)!$

For norm form equations, i.e. for equation (10), the above finiteness theorems were proved in qualitative forms by Schmidt [34] for $K = \mathbb{Q}, S = \varnothing$, by Schlickewei [30] for $K = \mathbb{Q}$, and by Laurent [25] in general. Some qualitative versions of Theorems 7 and 8 have been established independently by Evertse (private communication). He uses different terminology which is however equivalent to ours.

If $\boldsymbol{\mu}$ is a solution of (9) then so is $\boldsymbol{\mu}\,\varepsilon$ for every $\varepsilon \in O_S^*$. A set of solutions of the form $\boldsymbol{\mu}\, O_S^*$ is called an O_S^**-coset of solutions*. For equation (8), O_S^*-cosets of solutions can be defined in a similar way. From Theorem 7 one can deduce

COROLLARY 1. *Suppose that equation* (9) *(or equivalently equation* (8)*) has only finitely many O_S^*-cosets of solutions. Then the number of its O_S^*-cosets of solutions is at most*

$$C \exp\{2^{37nD} \cdot s^6 \log(5sD)\}.$$

We say that $\mathcal{M}$ is *degenerate* if there is a subalgebra $\mathbf{L}$ of $\mathbf{M}$ with $\mathbf{1}$ which is different from $\mathbf{K}$ and is admissible with respect to $\mathcal{M}$, and *non-degenerate* otherwise. Since the O_S^*-cosets of solutions of (9) are precisely the $(\mathcal{M}, \mathbf{K})$-families of solutions, our next corollary is an immediate consequence of Theorem 7.

COROLLARY 2. *If $\mathcal{M}$ is non-degenerate, then the number of O_S^*-cosets of solutions of* (9) *(or, equivalently, of* (8)*) is bounded above by the number occurring in* (11).

Qualitative versions of Corollary 2 were earlier established by Schmidt [33] (in case $K = \mathbb{Q}, S = \varnothing$), Schlickewei [30] (in case $K = \mathbb{Q}$) and Laurent [25] (in the general case) for the norm form equation (10), and by Evertse and Győry [6] for equation (8). In the case $K = \mathbb{Q}$, $S = \varnothing$, Schmidt [36] has recently derived the bound $C \cdot r^{c_1}$ with $c_1 = \min(2^{29n} \cdot r^2, (2n)^{n \cdot 2^{n+4}})$ for the number of solutions of the norm form equation (10) in the non-degenerate case. In terms of r, this bound is better than (11) in the special case under consideration. Very recently Evertse (private communication) has obtained another version of Corollary 2 with a bound which is better than (11) in terms of D but is in general weaker in terms of β. On combining our method of proof with that of Evertse, both Evertse's bound and our bound can be improved. Namely, the factor $\exp\{2^{37nD} \cdot s^6 \log(4sD)\}$ in our bounds (11), (12) can be replaced by

$$\exp\{2^{38nd} \cdot s^6 \log(8sD)\}. \tag{13}$$

The above-presented results will be published with detailed proofs in [20]. The proofs of Theorems 7 and 8 are rather long. The main steps in the proof of Theorem 7 are as follows. *Step* 1. Partition the set of solutions $\boldsymbol{\mu} \in \mathcal{M}$ of (9) into classes $\mathcal{C}$ such that two solutions $\boldsymbol{\mu}_1 = (\mu_{1i})_{i \in \mathcal{J}}$ and $\boldsymbol{\mu}_2 = (\mu_{2i})_{i \in \mathcal{J}}$ belong to the same class if both μ_{1i}/μ_{2i} and μ_{2i}/μ_{1i} are integral over O_S for each $i \in \mathcal{J}$. Generalizing a method of Schmidt [36], one can show that the number of classes $\mathcal{C}$ of solutions of (9) is at most C. *Step* 2. In the non-full case one can prove that the solutions of (9) belonging to a fixed class $\mathcal{C}$ are contained in

the union of at most $\exp\{2^{37nD} \cdot s^6 \log(4sD)\}$ sets of the form $\boldsymbol{\mu}\,\mathbf{L}$, where $\boldsymbol{\mu}$ is a solution and $\mathbf{L}$ is an admissible subalgebra of $\mathbf{M}$. The proof depends among other things on Theorem 1 and some arguments from [6]. *Step* 3. Finally, it is shown that the solutions under consideration which belong to a fixed set $\boldsymbol{\mu} \cdot \mathbf{L}$ are contained in the union of at most $\mathfrak{I}_{\mathbf{L}}$ $(\mathcal{M}, \mathbf{L})$-families of solutions.

§ 6. Applications to generalized systems of S-unit equations

Let $m \geq 2$ be an integer and $\Gamma = (O_S^*)^m$. For any m-tuple $\lambda = (\lambda_1, \ldots, \lambda_m)$ of non-negative integers, put $x^\lambda = x_1^{\lambda_1} \cdots x_m^{\lambda_m}$. Consider the following generalization of equation (2)

$$P_i(x) = \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) x^\lambda = 0 \text{ in } x \in \Gamma \text{ for } i \in \mathrm{I}, \tag{14}$$

where I is a finite index set, $p_i(\lambda) \in K$, and $\mathcal{L}_i$ is the support of P_i (i.e. the set of exponents λ for which the coefficient $p_i(\lambda)$ of x^λ in P_i is non-zero). Denote by $\mathcal{L}$ the disjoint union $\mathcal{L} = \coprod_{i \in \mathrm{I}} \mathcal{L}_i$ of the sets $\mathcal{L}_i$. Let $\mathcal{P}$ be a partition of $\mathcal{L}$; it induces partitions $\mathcal{L}_i = \coprod_{j \in \mathrm{J}_i} \mathcal{L}_{i,j}$ on each $\mathcal{L}_i$. Then $\mathcal{P}$ is said to be *compatible* with a $\gamma \in \Gamma$ if

$$\sum_{\lambda \in \mathcal{L}_{i,j}} p_i(\lambda) \gamma^\lambda = 0 \text{ for each } i \in \mathrm{I} \text{ and } j \in \mathrm{J}_i.$$

Further, we say that $\mathcal{P}$ is *maximal compatible* with γ if $\mathcal{P}'$ is not compatible with γ for any refinement $\mathcal{P}'$ of $\mathcal{P}$. Denote by $H_{\mathcal{P}}$ that subgroup of Γ whose elements γ have the property that for each $\mathcal{L}_{i,j}$, $\gamma^\lambda = \gamma^{\lambda'}$ if $\lambda, \lambda' \in \mathcal{L}_{i,j}$. If γ is a solution of (14), then so is every element of $\gamma H_{\mathcal{P}}$, where $\mathcal{P}$ is a partition of $\mathcal{L}$, compatible with γ. Laurent [25] proved that the set of solutions of (14) is the union of finitely many sets of the form $\gamma H_{\mathcal{P}}$ where γ is a solution and $\mathcal{P}$ is a partition of $\mathcal{L}$ which is maximal compatible with γ. In fact Laurent proved this result in a more general situation, for subgroups Γ of finite rank of $\mathbb{C}^*$. In his proof, he used his more general version of Theorem A (in which the solutions of (2) are taken from an arbitrary but fixed subgroup of finite rank of $\mathbb{C}^*$).

As a consequence of Theorem 8, we get the following quantitative version. Denote by r the cardinality of $\mathcal{L}$, and by k the rank of the matrix $(p_i(\lambda))_{i \in \mathrm{I}, \lambda \in \mathcal{L}}$ formed from the coefficients $p_i(\lambda)$ in (14). Put $n = r - k$.

THEOREM 9. *The set of solutions of* (14) *is the union of at most*

$$n^r \cdot \exp\{2^{37nd!} \cdot s^6 \log(4sd!)\} \tag{15}$$

sets of the form $\gamma H_{\mathcal{P}}$, *where* γ *is a solution of* (14) *and* $\mathcal{P}$ *is a partition of* $\mathcal{L}$ *which is maximal compatible with* γ. *Further, if* $K/\mathbb{Q}$ *is normal then* $d!$ *can be replaced by* d.

In the special case when (14) consists of a single inhomogeneous linear equation, Theorem 9 implies Theorem 1 with a slightly weaker bound. Indeed, in this special case Theorem 9 gives the bound (15) for the number of sets of solutions of the form $\gamma H_{\mathcal{P}_0}$ where $\mathcal{P}_0 = \{\mathcal{L}\}$, and $\mathcal{P}_0$ is maximal compatible with γ. But these solutions γ are just the non-degenerate solutions and $H_{\mathcal{P}_0} = (1, \dots, 1)$, hence our claim follows.

We remark that Theorem 9 can also be proven by combining the proof of Laurent with Theorem 1. Hence, apart from the forms of the bounds, Theorems 9 and 1 are equivalent. Finally, we note that using Theorem 8 with the improved bound (13), the second factor in (15) can be replaced by (13) with the choice $D = d!$

Proof of Theorem 9. If $n \leq 1$ and if (14) has a solution γ then all solutions are contained in $\gamma H_{\mathcal{P}_0}$ with the above $\mathcal{P}_0$, and $\mathcal{P}_0$ is maximal compatible with γ. Next suppose that $n \geq 2$. Put $\widetilde{\Gamma} = (O_S^*)^r$. To each solution $\gamma \in \Gamma$ of (14) we associate the solution $y = (y_\lambda) = (\gamma^\lambda)$ of the system of S-unit equations

$$\widetilde{P}_i(y) = \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) y_\lambda = 0 \text{ in } y = (y_\lambda) \in \widetilde{\Gamma} \text{ for } i \in \mathrm{I}. \tag{16}$$

This is in fact a special equation of the form (14). If $\mathcal{P}$ is a partition of $\mathcal{L}$ which is maximal compatible with γ, then it is at the same time maximal compatible with (γ^λ) in (16), and conversely. We define the subgroup $\widetilde{H}_{\mathcal{P}}$ of $\widetilde{\Gamma}$ in a similar way as $H_{\mathcal{P}}$ above. The solutions of (16) associated to the solutions in $\gamma H_{\mathcal{P}}$ of (14) are contained in $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$. Conversely, it is easy to see that those solutions γ' of (14) for which the associated solutions (γ'^λ) of (16) belong to $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$ are all contained in $\gamma H_{\mathcal{P}}$. Hence it suffices to give an upper bound for the number of sets of solutions of the form $(\gamma^\lambda)\widetilde{H}_{\mathcal{P}}$ of (16).

Let $V = \{\mathbf{y} = (y_\lambda) \in K^r : \sum_{\lambda \in \mathcal{L}_i} p_i(\lambda) y_\lambda = 0 \text{ for each } i \in \mathrm{I}\}$, $\mathfrak{M} = V \cap O_S^r$ and $F(\mathbf{y}) = \prod_{\lambda \in \mathcal{L}} y_\lambda$. Then $\dim_K K\mathfrak{M} = n$. It is easy to show that $\mathbf{y}$ is a solution of (16) if and only if it is a solution of

$$F(\mathbf{y}) \in O_S^* \text{ in } \mathbf{y} \in \mathfrak{M}.$$

This is an equation of type (8), hence it has an equivalent formulation of the form (9), say

$$\mathrm{N}(\boldsymbol{\mu}) \in O_S^* \text{ in } \boldsymbol{\mu} \in \mathcal{M}, \tag{17}$$

where now $\mathbf{M} = K^r$, $\mathcal{M} = \mathfrak{M}$ and $\boldsymbol{\mu} = \mathbf{y}$. It is easily seen that the sets of solutions $(\gamma^\lambda)\widetilde{H}_\mathcal{P}$ of (16) considered above are all maximal families of solutions of (17). By applying now Theorem 8 to (17) with $\beta = 1$, Theorem 9 follows.

§ 7. S-unit equations; effective results

The results presented above are all ineffective. Baker's method for estimating linear forms in logarithms of algebraic numbers and its p-adic analogue enabled one to give explicit bounds for the sizes of the solutions of (1). For a survey of effective results concerning (1), we refer to [37] or [11]. Let h_K and R_K denote the class number and regulator of K, respectively, and let P be the maximum of the rational primes divisible by $\mathfrak{p}_1, \ldots, \mathfrak{p}_{t-1}$ or $\mathfrak{p}_t$ (with the convention that $P = 1$ if $t = 0$). Further, denote by $H(\alpha)$ the height of an algebraic number α, i.e. the maximum absolute value of the coefficients of the minimal defining polynomial of α over $\mathbb{Z}$. By using Baker's method and its p-adic analogue I proved [16] in 1979 the following theorem in a slightly different form.

THEOREM C. *All solutions x_1, x_2 of (1) satisfy*

$$\max_{i=1,2} H(x_i) < \exp\{(c_1 s)^{c_2 s} \cdot P^{d+1} \cdot \log A\}$$

where $A = \max(H(\alpha_1), H(\alpha_2), 2)$ and $c_1 = c_1(d, h_K, R_K)$, $c_2 = c_2(d)$ are effectively computable numbers.

In [16], c_1 and c_2 were given explicitly.

Apart from certain special results concerning the case $n = 3$ (for references see [37] or [11]), for $n > 2$ there are no effective results which would make it possible to determine all non-degenerate solutions of (2). An effective version of Schmidt's Subspace Theorem and its p-adic generalization would yield an effective version of Theorem A. It seems however hopeless to make effective the Subspace Theorem by the present methods. We formulate now a weaker diophantine inequality whose effective resolution would also imply an effective version of Theorem A. Such an effective variant of Theorem A would be of great importance for applications. For instance, it would enable one to make effective all the results presented in §§ 2 to 6 of this paper.

Let $k, l \geq 1$ be integers, $\alpha_0, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$ non-zero elements of K, and $b_{i1}, \ldots, b_{il}$ $(i = 1, \ldots, k)$ rational integers with absolute values at most B such that

(18) $\Lambda = \alpha_0 - \sum_{i=1}^{k} \alpha_i \beta_1^{b_{i1}} \dots \beta_l^{b_{il}}$ has no vanishing subsum containing α_0.

Consider a normalized multiplicative valuation $|\ .\ |_v$ of K, where v is one of the infinite places or the finite places corresponding to the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$.

PROPOSITION. *If*

$$0 < |\Lambda|_v < e^{-\delta B}$$

for some $\delta > 0$, *then* $B < C$, *where* C *is a number depending only on* $\alpha_0, \dots, \alpha_k, \beta_1, \dots, \beta_l, k, l, K, v$ *and* δ.

For $k = 1$, this is a non-effective version of Baker's famous theorem and its p-adic analogue; for a historical survey of Baker's theory, we refer to [1]. For $k \geq 1$, the above Proposition is a straightforward consequence of Theorem 2 of Evertse [3]. Since this result of [3] was derived from Schlickewei's p-adic Subspace Theorem [29], our Proposition is ineffective, i.e. C is not effectively computable for $k > 1$ by the method of proof.

It is easy to see that the assumption (18) is necessary in the above Proposition.

We now show that *an effective version of our Proposition would imply an effective variant of Theorem A.*

In what follows, we use the notation of § 2. c_1 to c_7 will denote numbers depending only on $\alpha_1, \dots, \alpha_n, n, K$ and S. Furthermore, the numbers c_1 to c_5 will be effectively computable.

Suppose that (2) has a non-degenerate solution, and let $x_1, \dots, x_n$ be such a solution. Let $\{v_1, \dots, v_s\}$ be the set of the infinite places of K and of the finite places of K corresponding to the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. It is known (see e.g. [22]) that there are multiplicatively independent S-units $\eta_1, \dots, \eta_{s-1}$ in O_S with $H(\eta_j) \leq c_1$ for $j = 1, \dots, s-1$, such that

$$(19) \qquad \begin{cases} x_i = \gamma_i \eta_1^{b_{i1}} \dots \eta_{s-1}^{b_{i,s-1}} \text{ with some } b_{i1}, \dots, b_{i,s-1} \in \mathbb{Z} \text{ and some} \\ \gamma_i \in O_S^* \text{ for which } H(\gamma_i) \leq c_2 \text{ for } i = 1, \dots, n. \end{cases}$$

Further, the absolute values of the elements of the inverse of the matrix

$$(\log |\eta_j|_{v_p})_{p,j=1,\dots,s-1}$$

is less than c_3. Put $B_i = \max_{1 \leq j \leq s-1} |b_{ij}|$ for $i = 1, \dots, n$. We may suppose that $B = B_1 \geq B_2 \geq \dots \geq B_n$ and that $B > 0$. Fix a q with $1 \leq q \leq s$ for which $|x_1|_{v_q}$ is minimal. Then putting $|\bar{x}_1|_S = \max_{1 \leq p \leq s} |x_1|_{v_p}$, we get by the product formula that

$$|x_1|_{v_q}^{s-1} \leq \frac{1}{|\bar{x}_1|_S}. \tag{20}$$

Further, we have

$$\log |x_1/\gamma_1|_{v_p} = \sum_{j=1}^{s-1} b_{1j} \log |\eta_j|_{v_p} \quad \text{for } p = 1, \ldots, s,$$

whence

$$B < c_4 \max_{1 \leq p \leq s} \left| \log |x_1/\gamma_1|_{v_p} \right| < c_5 \log |\bar{x}_1|_S.$$

Together with (20) this gives

$$|x_1|_{v_q} < e^{-\delta B} \tag{21}$$

with the choice $\delta = ((s-1)c_5)^{-1}$. It follows from (2), (19) and (21) that

$$e^{-\delta B} > |x_1|_{v_q} = \left| (1/\alpha_1) - \sum_{i=2}^{n} (\alpha_i \gamma_i / \alpha_1)\, \eta_1^{b_{i1}} \ldots \eta_{s-1}^{b_{i,s-1}} \right|_{v_q} > 0. \tag{22}$$

Since the solution $x_1, \ldots, x_n$ is non-degenerate, the conditions of the Proposition are fulfilled. By applying now the above Proposition to (22) we obtain $B \leq c_6$ whence $\max_{1 \leq i \leq n} H(x_i) \leq c_7$, where c_6 and c_7 are effectively computable, provided that the corresponding constant C in the Proposition is also effectively computable.

REMARK. For $k = 1$ effective versions of the Proposition are available, hence we gave at the same time a proof for a non-explicit variant of Theorem C.

§ 8. Applications to binary forms and decomposable forms of given discriminant

In this section, we present a recent application of our effective Theorem C on S-unit equations.

Every binary form $F \in \mathbb{Z}[X, Y]$ of degree r can be factorized as $\prod_{i=1}^{r} (\alpha_i X - \beta_i Y)$ over some algebraic number field. The discriminant of F, denoted by $D(F)$, is defined by

$$D(F) = \prod_{1 \leq i < j \leq r} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

$D(F)$ is a rational integer, and is independent of the factorization of F. Further, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ (i.e. A has entries in $\mathbb{Z}$ and determinant 1) and $F_A(X,Y) = F(aX + bY, cX + dY)$ then $D(F_A) = D(F)$. Such binary forms F, F_A are called *equivalent*. It was proved by Lagrange [24] for $r = 2$ and by Hermite [23] for $r = 3$ that for every binary form $F \in \mathbb{Z}[X,Y]$ with degree r and non-zero discriminant, there is an $A \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$H(F_A) \leq c_1 |D(F)|$$

with some effectively computable absolute constant c_1. As usual, $H(P)$ denotes the height of a polynomial P with coefficients in $\mathbb{Z}$. In 1972 Birch and Merriman [2] showed that for every $r \geq 4$ and $D \neq 0$, there exist only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[X,Y]$ of degree r and discriminant D. Here the dependence on r is not necessary because it was shown in 1974 (cf. [15, Part II]) that

$$r \leq 3 + 2 \log |D(F)| / (\log 3) \tag{23}$$

which is already sharp.

The proof of Birch and Merriman is ineffective. Independently of Birch and Merriman, I proved in 1973 (cf. [15, Part I]) an effective version for monic binary forms[2] $F \in \mathbb{Z}[X,Y]$ (i.e. with $F(1,0) = 1$). Further, I used an earlier version of Theorem C to prove (cf. [15, Part IV]) that for every monic binary form $F \in \mathbb{Z}[X,Y]$ with degree r and $D(F) \neq 0$ there is an $A \in \mathrm{SL}_2(\mathbb{Z})$ of the form $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ such that

$$H(F_A) \leq c_2 |D(F)|^{c_3}$$

where c_2, c_3 are effectively computable numbers depending only on r and the discriminant of the splitting field of F over $\mathbb{Q}$. On combining Theorem C with some new ideas, these effective results have recently been extended (cf. Evertse and Győry [8]) to all binary forms, making thereby effective the theorem of Birch and Merriman. Further, some generalizations have also been established for decomposable forms in $n \geq 2$ variables over $\mathbb{Z}$ (cf. Evertse and Győry [9], [10]). To present such a generalization, we have to introduce some further notions and notation.

Let $F(\mathbf{X}) = F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree r with splitting field K over $\mathbb{Q}$. Then it can be written as

[2] Most of the results of [15] were stated for polynomials in $\mathbb{Z}[X]$, but they can be easily reformulated for binary forms.

$F(\mathbf{X}) = l_1(\mathbf{X}) \dots l_r(\mathbf{X})$ where $l_1, \dots, l_r$ are linear forms with coefficients in K. Suppose that F is *squarefree* (i.e., that it is not divisible by the square of a linear form over K). Let $\mathcal{I}(F)$ denote the collection of linearly independent subsets $\{l_{i_1}, \dots, l_{i_n}\}$ of $\{l_1, \dots, l_r\}$ and assume that $\mathcal{I}(F) \neq \varnothing$. Denote by (α) the O_K-ideal generated by $\alpha \in K$, and by (l_i) the O_K-ideal generated by the coefficients of l_i, $i = 1, \dots, r$. Further, let $\det(l_{i_1}, \dots, l_{i_n})$ denote the coefficient determinant of $\{l_{i_1}, \dots, l_{i_n}\}$. Then there is a positive rational integer $D = D_{\mathbb{Z}}(F)$ such that

$$(D) = \prod_{\mathcal{I}(F)} \left\{ \frac{(\det(l_{i_1}, \dots, l_{i_n}))}{(l_{i_1}) \cdots (l_{i_n})} \right\}^2$$

where the product is taken over all sets $\{l_{i_1}, \dots, l_{i_n}\} \in \mathcal{I}(F)$. Further, the integer D does not depend on the choice of $l_1, \dots, l_r$, and $D_{\mathbb{Z}}(aF) = D_{\mathbb{Z}}(F)$ for all $a \in \mathbb{N}$. Hence we may assume that F is *primitive*, i.e. that its coefficients are relatively prime. $D_{\mathbb{Z}}(F)$ is called the *$\mathbb{Z}$-discriminant*[3] of F. For $\mathcal{I}(F) = \varnothing$, we put $D_{\mathbb{Z}}(F) = 0$. If for example F is a primitive, squarefree binary form then $D_{\mathbb{Z}}(F) = |D(F)|$. For $A \in \mathrm{SL}_n(\mathbb{Z})$, the decomposable forms $F(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_n]$ and $F_A(\mathbf{X}) = F(A\mathbf{X})$ are called *equivalent*. Equivalent decomposable forms have the same $\mathbb{Z}$-discriminant.

Recently, we showed with Evertse [9], [10] the following.

THEOREM 10. *Let $F(\mathbf{X}) \in \mathbb{Z}[X_1, \dots, X_n]$ be a primitive, squarefree decomposable form of degree r with $D_{\mathbb{Z}}(F) > 0$ and splitting field K. Then there is an $A \in \mathrm{SL}_n(\mathbb{Z})$ such that*

$$H(F_A) \leq c_4 D_{\mathbb{Z}}(F)^{c_5} \tag{24}$$

where c_4, c_5 are effectively computable numbers which depend only on n, r and the discriminant D_K of K. Further, we have

$$r \leq 2^n - 1 + n \log D_{\mathbb{Z}}(F)/(\log 3). \tag{25}$$

For $n = 2$, (25) gives (23). One can prove (cf. [9]) that $|D_K| \leq c_6$ for some effectively computable number c_6 depending only on n, r and $D_{\mathbb{Z}}(F)$. Hence Theorem 10 implies the following.

[3] For polynomials in several variables there exists also another concept of discriminant; see e.g.[13].

COROLLARY. *For given $n \geq 2$ and $D > 0$, there are only finitely many equivalence classes of primitive, squarefree decomposable forms in $\mathbb{Z}[X_1, \ldots, X_n]$ with $D_{\mathbb{Z}}(F) = D$, and a full set of representatives of these classes can be effectively determined.*

For $n = 2$, this implies an effective version of the theorem of Birch and Merriman.

Both the results of [2], [15] and the theorems of [8], [9] and [10] have been extended to the case when the ground ring is the ring of S-integers of a number field. We note that in our papers [8], [9] and [10], several applications are given for example to algebraic numbers of given discriminant, to discriminant form inequalities, to small values of binary forms and decomposable forms at integral points and to arithmetical properties of discriminants of binary forms and decomposable forms.

The proofs of (24) and (25) will be published in [9] and [10], respectively. In the proof of (24), one of the main tools is Theorem C presented in § 7. The proof of Theorem 10 is long and complicated, hence we shall not outline it here. For instance, the proof of (24) takes about 25 pages.

Finally, we note that in the case $n = 2$, Evertse (private communication) has recently proved (24) with $c_5 = 21/(r-1)$. In his version the constant corresponding to c_4 is not, however, effectively computable.

References

[1] A. BAKER, *Transcendental Number Theory*, 3rd ed., Cambridge University Press, 1990.

[2] B.J. BIRCH and J.R.MERRIMAN, Finiteness theorems for binary forms with given discriminant, *Proc.London Math.Soc.* **25**(1972), 385-394.

[3] J.H. EVERTSE, On sums of S-units and linear recurrences, *Compositio Math.* **53**(1984), 225-244.

[4] J.H. EVERTSE, On equations in S-units and the Thue-Mahler equation, *Invent.Math.* **75**(1984), 561-584.

[5] J.H. EVERTSE, Decomposable form equations with a small linear scattering, to appear.

[6] J.H. EVERTSE and K. GYŐRY, Finiteness criteria for decomposable form equations, *Acta Arith.* **50**(1988), 357-379.

[7] J.H. EVERTSE and K. GYŐRY, On the numbers of solutions of weighted unit equations, *Compositio Math.* **66**(1988), 329-354.

[8] J.H. EVERTSE and K. GYŐRY, Effective finiteness results for binary forms with given discriminant, *Compositio Math.* **79**(1991), 169-204.

[9] J.H. EVERTSE and K. GYŐRY, Effective finiteness theorems for decomposable forms of given discriminant, *Acta Arith.*, to appear.

[10] J.H. EVERTSE and K. GYŐRY, Discriminants of decomposable forms, to appear.

[11] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, S-unit equations and their applications, *New Advances in Transcendence Theory* (A. Baker ed.), pp.110-174. Cambridge University Press, 1988.

[12] J.H. EVERTSE, K. GYŐRY, C.L. STEWART and R. TIJDEMAN, On S-unit equations in two unknowns, *Invent.Math.* **92**(1988), 461-477.

[13] I.M. GELFAND, A.V. ZELEVINSKY and M.M. KARPANOV, On discriminants of polynomials of several variables (Russian), *Functional Anal.and Appl.* **24**(1990), 1-4.

[14] K. GYŐRY, On the irreducibility of a class of polynomials I, II, III, IV, *Publ.Math.Debrecen* **18**(1971), 289-307; **19**(1972), 293-326; *J.Number Theory* **15** (1982), 164-181; *Acta Arith.*, to appear.

[15] K. GYŐRY, On polynomials with integer coefficients and given discriminant I, II, III, IV, V, *Acta Arith.* **23** (1973), 419-426; *Publ.Math.Debrecen* **21** (1974), 125-144; **23** (1976), 141-165; **25** (1978), 155-167; *Acta Math. Hungar.* **32** (1978), 175-190.

[16] K. GYŐRY, On the number of solutions of linear equations in units of an algebraic number field, *Comment.Math.Helv.* **54** (1979), 583-600.

[17] K. GYŐRY, On certain graphs composed of algebraic integers of a number field and their applications I, *Publ.Math.Debrecen* **27** (1980), 229-242.

[18] K. GYŐRY, On arithmetic graphs associated with integral domains I, II, in "*A Tribute to Paul Erdős*" (A.Baker, B.Bollobás, A.Hajnal eds.), Cambridge University Press, 1990, pp.207-222; in "*Sets, Graphs and Numbers*", Coll.Math.Soc.J.Bolyai **59**, North-Holland Publ.Comp., to appear.

[19] K. GYŐRY, Upper bounds for the numbers of solutions of unit equations in two unknowns, to appear.

[20] K. GYŐRY, On the numbers of families of solutions of decomposable form equation systems, to appear.

[21] K. GYŐRY and A. SCHINZEL, On a conjecture of Posner and Rumsey, in preparation.

[22] L. HAJDÚ, Some applications of the effective Dirichlet unit theorem, *Publ. Math. Debrecen*, to appear.

[23] CH. HERMITE, Sur l'introduction des variables continues dans la théorie des nombres, *J. reine Angew. Math.* **41** (1851), 191-216.

[24] J.L. LAGRANGE, Recherches d'arithmétique, *Nouv.Mém.Acad.Berlin*, 1773, pp.265-312. *Oeuvres*, III, pp.693-758.

[25] M. LAURENT, Equations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299-327.

[26] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI, The growth conditions for recurrence sequences, Report 82.0041, Macquarie University, N.S.W.Australia, 1982.

[27] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI, Additive relations in fields, *J.Austral.Math.Soc.*(Series A) **51** (1991), 154-170.

[28] E.C. POSNER and H. RUMSEY, JR., Polynomials that divide infinitely many trinomials, *Michigan Math.J.* **12** (1965), 339-348.

[29] H.P. SCHLICKEWEI, The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt Theorem, *Archiv Math.* **29** (1977), 267-270.

[30] H.P. SCHLICKEWEI, On norm form equations, *J.Number Theory* **9** (1977), 370-380.

[31] H.P. SCHLICKEWEI, S-unit equations over number fields, *Invent. Math.***102** (1990), 95-107.

[32] H.P. SCHLICKEWEI, The quantitative subspace theorem for number fields, to appear.

[33] W.M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191**(1971), 1-20.

[34] W.M. SCHMIDT, Norm form equations, *Annals of Math.* **96** (1972), 526-551.

[35] W.M. SCHMIDT, The subspace theorem in diophantine approximations, *Compositio Math.* **69** (1989), 121-173.

[36] W.M. SCHMIDT, The number of solutions of norm form equations, *Trans. Amer. Math. Soc.* **317** (1990), 197-227.

[37] T.N. SHOREY and R. TIJDEMAN, *Exponential diophantine equations*, Cambridge University Press, 1986.

Kálmán Győry
Mathematical Institute
Kossuth Lajos University
H–4010 Debrecen, Hungary

Astérisque

MARC HINDRY

Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)

Astérisque, tome 209 (1992), p. 39-56

<http://www.numdam.org/item?id=AST_1992__209__39_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR LES CONJECTURES DE MORDELL ET LANG (d'après VOJTA, FALTINGS et BOMBIERI).

Marc HINDRY

1 Introduction

Dans tout le texte, k désigne un corps de nombres, O_k son anneau d'entiers, C une courbe algébrique projective lisse définie sur k et g le genre de C. L'ensemble des points de C rationnels sur k est noté C(k).

On sait que:

si g=0 alors C(k) est ou bien vide ou bien en bijection avec $\mathbf{P}^1(k)$;
si g=1 alors ou bien C(k) est vide ou bien est un groupe de type fini (théorème de Mordell-Weil); la loi de groupe est par ailleurs algébrique;
si g≥2 alors C(k) est fini (Conjecture de Mordell=théorème de Faltings [F1]).
Si U est un ouvert affine de C on peut s'intéresser aux points entiers que je noterai (un peu abusivement) $U(O_k)$; on dispose alors du théorème de Siegel [Si]: $U(O_k)$ est fini sauf (peut-être) si g=0 et C–U possède au plus deux éléments. La preuve de Siegel utilise essentiellement deux ingrédients que j'explicite plus loin: a) la théorie des approximations diophantiennes (Thue-Siegel-Dyson-Gelfond-Roth-Schmidt) et b) le théorème de Mordell-Weil appliqué à la jacobienne de C.
Ces ingrédients n'apparaissent pas dans la preuve de la conjecture de Mordell par Faltings [F1] (Voir aussi les séminaires [Sz1] et [Co-Si]) même si les jacobiennes et les variétés abéliennes y jouent un rôle prépondérant. Vojta a donné une nouvelle preuve de la conjecture de Mordell dans la lignée de Siegel [V1]. Faltings , en développant les idées de Vojta a ensuite prouvé la généralisation suivante, conjecturée par Lang:

THÉORÈME 1(Faltings [F2];voir aussi [Sz2]): *Soit* X *une sous-variété d'une variété abélienne* A *définies sur* k; *on suppose que* X *ne contient aucun translaté de sous-variété abélienne non nulle, alors* X(k) *est fini.*

La preuve de Vojta [V1] utilise des idées et des techniques sophistiquées de géométrie arithmétique "à la Arakelov", notamment [G-S3]; Bombieri [B] a

simplifié cette preuve et donné une version très jolie et "presque élémentaire" du travail de Vojta; c'est un article que tout mathématicien souhaitera lire.
Les liens entre la géométrie et l'approximation diophantienne "à la Siegel" ont été développés dans plusieurs directions: Vojta a annoncé dans [V4] une inégalité plus fine que celle que nous donnons et valable sur toutes les courbes; cette inégalité contient la conjecture de Mordell et le théorème de Roth. Dans [F2] Faltings prouve une généralisation du théorème de Siegel également conjecturée par Serge Lang: un ouvert affine d'une variété abélienne ne contient qu'un nombre fini de points entiers définis sur un corps de nombres donné.
J'explicite dans cette introduction les deux ingrédients fondamentaux mentionnés ci-devant; le paragraphe suivant introduit l'outil de base de la géométrie diophantienne: les hauteurs; je donne dans les paragraphes 3 et 4 une esquisse des preuves respectivement de la conjecture de Mordell selon Vojta et du théorème 1 selon Faltings, il ne saurait donc être question d'originalité ici mais j'espère que cette présentation facilitera à certains la lecture des articles originaux décrivant ces beaux résultats. Le paragraphe 5 complète sur certains points le paragraphe 4 et décrit la conjecture générale de Serge Lang [La1] (maintenant un théorème); le dernier paragraphe raconte une application de ces résultats à l'étude des points algébriques de degré donné sur une courbe.

a)Approximations diophantiennes.
L'idée de Siegel est qu' une suite infinie de points entiers sur une courbe affine doit tendre vers l'un de ses points à l'infini (se rapprocher d'une asymptote) et donc en fournir de très bonnes approximations. Remarquons que cette remarque si simple est en défaut (au moins littéralement) si l'on travaille avec des points rationnels; on a donc longtemps cru qu'elle était inutilisable quand les points ne sont pas entiers, Vojta a montré qu'il n'en était rien.
Je donne un schéma de preuve d'inégalités de ce type (une bonne référence générale est [Sch1]):

THÉORÈME DE ROTH: *Soit* α *un nombre algébrique irrationnel et* $\kappa>2$, *alors il existe un nombre fini de solutions rationnelles à l'inégalité:*

(*) $\qquad |\alpha - \frac{p}{q}| < q^{-\kappa}.$

Premier pas: on fixe m assez grand, et $d_1,\ldots,d_m$ entiers et on construit un polynôme $P \in \mathbf{Z}[X_1\ldots,X_m]$ de degré au plus d_i en X_i, s'annulant beaucoup en $(\alpha,\ldots,\alpha)$ et dont les coefficients sont de taille controlée (Lemme de Siegel ou principe des boites).
Deuxième pas: On suppose qu'il existe $p_1/q_1,\ldots,p_m/q_m$ vérifiant (*); alors on prouve que P et un certain nombre de ses dérivées sont petits en

$\beta=(p_1/q_1,..,p_m/q_m)$ par une simple application de la formule de Taylor.

Troisième pas (difficile): On emploie un théorème de non-annulation, dont je donne ci-après un enoncé ("lemme de Roth à deux variables"). On doit prouver qu'une dérivée d'ordre assez petit est non nulle i.e.:

$\eta := \partial_i P(\beta) \neq 0$ avec $\partial_i = \frac{1}{i_1!..i_m!}(\partial/\partial X_1)^{i_1}..(\partial/\partial X_m)^{i_m}$.

Quatrième pas: comme η est rationnel et non nul on écrit :

$$(\text{Dénominateur}(\eta))^{-1} < |\eta|$$

C'est l''inégalité de Liouville"; elle fournit une contradiction si m est assez grand et si les q_i sont très échelonnés (Cf remarques ci-dessous)

Remarques:

i)Il est vital pour les estimations arithmétiques de diviser par les factorielles.

ii)Les théorèmes d'annulation (Dyson, Roth [Ro], Viola [Vi], Esnault-Viehweg [E–V]) utilisent la notion d'indice, ou ordre d'annulation pondéré; on définit l'indice d'un polynôme P en un point β par rapport aux poids $(d_1,...,d_m)$ par:

$$\text{Indice}_{(d_1,...,d_m)}(\beta)(P) := \min\{ \tfrac{i_1}{d_1}+..+\tfrac{i_m}{d_m} \ / \partial_i P(\beta)\neq 0\}.$$

Dans la pratique les d_i sont effectivement les degrés de P par rapport à X_i. Donnons l'énoncé promis:

LEMME DE ROTH ("À DEUX VARIABLES"): *soit* $\varepsilon>0$, α_1,α_2 *deux nombres algébriques et* $P\in \mathbb{Q}[X,Y]$ *non nul de degré au plus* d_1,d_2 *et supposons que*

1) $d_2/d_1<\varepsilon$

2) $h(P)+4d_1<\varepsilon^2\min(d_1h(\alpha_1),d_2h(\alpha_2))$

alors on a :

$$\text{Indice}_{(d_1,d_2)}(\alpha_1,\alpha_2)(P)<4\varepsilon.$$

Ici, h désigne la hauteur logarithmique usuelle (Cf paragraphe suivant). On pourra lire la preuve dans l'article original de Roth [Ro] ou dans celui de Bombieri [B]; il faut penser pour que le lemme soit utile que ε est petit et donc que d_1 est beaucoup plus grand que d_2 d'après (1) et donc pour majorer efficacement les dérivées de P (deuxième étape) et vérifier l'hypothèse (2) on aura besoin que $d_1h(\alpha_1)$ soit du

même ordre de grandeur que $d_2h(\alpha_2)$ et il faudra supposer:

(**) $h(\alpha_1)/h(\alpha_2) < \varepsilon$ ou encore $\log q_i/\log q_{i+1} < \varepsilon$

(avec les notations de la construction précédente) .

Ceci est la raison de l'ineffectivité congénitale de la méthode: on doit supposer l'existence de bonnes approximations avec des dénominateurs croissant exponentiellement pour montrer que de telles approximations n'existent pas. La preuve de Vojta souffre du même défaut et -tout comme la preuve de Faltings mais pour d'autres raisons- n'est pas effective. Par contre la méthode est très bonne pour borner le nombre des solutions (Cf théorème 2).

b) Jacobienne d'une courbe algébrique.

On définit un plongement de C dans une variété abélienne A=Jac(C) en choisissant un point origine $O \in C$. Sur $\mathbf{C}$ on procède ainsi: on choisit une base $\omega_1,..,\omega_g$ des 1–formes holomorphes sur C et on définit:

$j: C \longrightarrow A=Jac(C)=\mathbf{C}^g/\Omega$

$x \longrightarrow (\int_o^x \omega_1,..,\int_o^x \omega_g)$ modulo périodes.

Cette construction peut se faire algébriquement d'après Weil [W] (voir aussi l'article de Milne dans [Co-Si]). Dans ce cas A est une variété abélienne définie sur k et A(k) est un groupe de type fini. En particulier $A(k)\otimes\mathbf{R}=\mathbf{R}^r$ avec r=rangA(k) et l'application de C(k) dans cet espace est à fibres finies ("finite-to-one"). Ainsi pour prouver que C(k) est fini il suffit de prouver que son image dans $A(k)\otimes\mathbf{R}$ est finie.

Remarque: la description analytique donnée ci-dessus se transcrit mot pour mot à une variété X de dimension quelconque; on obtient ainsi une variété abélienne: sa variété d'Albanese (voir [La2]), mais bien sûr l'application obtenue n'est pas injective en général; en fait cela donne un caractérisation différentielle des sous-variétés de variétés abéliennes: ce sont celles qui ont "suffisamment" de 1-formes régulières.

2 Hauteurs associées à un diviseur.

C'est l'outil de base pour ces questions, des références générales sont [La1], [Se] et [Sz1]; en voici deux définitions donnant des éclairages différents:

1ère définition (Weil):

Si $P=(x_0,\ldots,x_n)\in \mathbf{P}^n(\mathbf{Q})$, on peut supposer $x_i\in \mathbf{Z}$ et $pgcd(x_i)=1$; on pose alors $h(P)=\log\max|x_i|=\Sigma_v \log\max|x_i|_v$

La deuxième somme est prise sur toutes les places de **Q** et d'après la formule du produit est indépendante des coordonnées; de plus sous cette forme la définition se généralise immédiatement aux corps de nombres.

Si D est un diviseur très ample sur une variété X, il correspond à un plongement $\phi_D: X\longrightarrow \mathbf{P}^n$ et on pose $h_D(P):=h(\phi_D(P))$; en général un diviseur est la différence de deux diviseurs très amples D=A–B et on pose $h_D:=h_A-h_B$. La notation est abusive car la hauteur définie ainsi dépend du plongement et en tant que fonction du diviseur n'est définie qu'à une fonction bornée près; il est coutumier d'appeler hauteur de Weil associée à D tout représentant de la classe de h_D modulo les fonctions bornées.

2eme définition (Arakelov):

On étend X en un schéma $\mathfrak{X}$ projectif sur $spec(O_k)$; on pose $\mathfrak{D}$=clôture de Zariski de D dans $\mathfrak{X}$ et on note $\mathfrak{L}$ le fibré en droites associé. On choisit une métrique $\|\ \|_v$ sur $O(D)$ pour chaque place archimédienne. Un point de X(k) correspond dans ce langage à une section du morphisme $\mathfrak{X}\longrightarrow spec(O_k)$ et $P^*\mathfrak{L}$ est alors un fibré en droites (métrisé) sur O_k et si f est un élément non nul (une"section ne s'annulant pas en P") on pose:

$Deg_{Arakelov}(P^*\mathfrak{L})=\log Card(P^*\mathfrak{L}/fO_k)-\Sigma_v \log\|f\|_v$, où la somme est prise sur les places archimédiennes. La définition de la hauteur d'Arakelov est alors:

$[k:Q]h_{\mathfrak{X},\mathfrak{L},\|\ \|}(P)=Deg_{Arakelov}(P^*\mathfrak{L})$

On observe que $h_{\mathfrak{X},\mathfrak{L},\|\ \|}$ est bien une hauteur de Weil pour D, en particulier si $\mathfrak{X}',\mathfrak{L}',\|\ \|'$ désignent un autre modèle de X, un autre prolongement de O(D) et d'autres métriques alors la différence entre $h_{\mathfrak{X},\mathfrak{L},\|\ \|}$ et $h_{\mathfrak{X}',\mathfrak{L}',\|\ \|'}$ est bornée; les propriétés fondamentales sont les suivantes:

H1) h_D ne dépend que de la classe de D (mod O(1))

H2) $h_{D+D'}=h_D+h_{D'}$ mod O(1)

H3) $h_{f^*D}=h_D \circ f$ mod O(1) lorsque f est un morphisme entre deux variétés projectives X et Y.

H4) Si D est effectif, si $P \notin D$, alors $h_D(P) \geq -C^{te}$ ("inégalité de Liouville")

La notation O(1) désigne comme d'habitude la classe des fonctions bornées.

Commentaires: La définition de Weil a bien sûr le mérite d'être naturelle, on a envie de dire incontournable; elle rend clair aussi le fait qu'il n'y ait qu'un nombre fini de points de hauteur bornée (le théorème de Northcott, voir [La1], donne un énoncé un peu plus fort). La définition d'Arakelov enrichit la palette des analogies entre corps de nombres et corps de fonctions (entre géométrie et arithmétique); elle permet aussi en enrichissant la structure de "supprimer les O(1)" ou au moins de leur donner une valeur. En effet les propriétés H1,2,3,4 sont transparentes sur cette définition:

H1) h_D est définie à partir du fibré associé O(D).

H2) Si l'on munit $O(D+D') \equiv O(D) \otimes O(D')$ de la métrique produit tensoriel de celles de O(D) et O(D') on obtient une égalité.

H3) Si l'on choisit des modèles tels que f s'étende en $f: \mathfrak{X} \longrightarrow \mathfrak{Y}$ et si l'on muni O(f*D) de la métrique pullback de celle de O(D) on obtient une égalité.

H4) Si f est une section de O(D) dont le support est D posons $\|f\|_\infty = \sup_v \sup_P \|f(P)\|_v$, alors avec les notations d'Arakelov:

$$h_{\mathfrak{X},\mathfrak{L},\|\ \|}(P) \geq -\log\|f\|_\infty \qquad \text{(il suffit d'écrire } \mathrm{Card}(P^*\mathfrak{X}/fO_k) \geq 1)$$

De plus si X est une variété abélienne et D est ample symétrique alors $h_D(P)=q_D(P)+O(1)$ avec q_D quadratique et même définie positive sur $X(k)\otimes\mathbf{R}$; cette forme quadratique s'appelle la hauteur de Néron-Tate associée à D. On se trouve donc dans une situation "à la Minkovski": on a un réseau (l'image de X(k)) dans un espace vectoriel euclidien $X(k)\otimes\mathbf{R}$.

3 La "conjecture" de Mordell.

On reprend le plongement associé à un point rationnel O fixé:

$j: C \longrightarrow A=Jac(C)$

On dispose du diviseur ample sur A

$\Theta = j(C)+...+j(C)$ (somme g–1 fois)

Je supposerai pour simplifier que Θ est symétrique (cela est toujours vrai pour un translaté de Θ et même dans certains cas on peut choisir O de sorte que cela soit

vrai).
On a donc une norme euclidienne || || sur $A(k)\otimes\mathbf{R}$ telle que:
$q_\Theta(x)=\frac{1}{2}\|x\|^2$. On notera <,> le produit scalaire associé.
On démontre alors les deux inégalités suivantes pour les points de C(k):

INEGALITÉ DE MUMFORD [M1]:*Soit* $\lambda>1/g$, *alors il existe* C_1 *telle que si* $x\neq y\in C(k)$ *et si* $C_1\leq\|x\|\leq\|y\|\leq 2\|x\|$ *alors*

$$\cos(x,y):=\langle x,y\rangle/\|x\|\|y\|\leq\lambda .$$

INEGALITÉ DE VOJTA [V1]:*Soit* $\lambda>1/\sqrt{g}$, *alors il existe* C_2,C_3 *telles que si* $x,y\in C(k)$ *et* $C_2\leq\|x\|\leq C_3\|y\|$ *alors*

$$\cos(x,y):=\langle x,y\rangle/\|x\|\|y\|\leq\lambda .$$

C'est un exercice de géométrie euclidienne de prouver que (en choisissant le même λ dans les deux inégalités, voir [V1] et [B]) on obtient:

THÉORÈME 2(Vojta):*notons* r *le rang du groupe de Mordell-Weil de la jacobienne de* C *et* C_1, C_2, C_3 *les constantes associées à* C *et* λ. *Alors:*

$$\mathrm{Card}\{x\in C(k)/\|x\|\geq\max(C_1,C_2)\}\leq(1+\frac{\log C_3}{\log 2})(1+\frac{1}{\sin(\frac{1}{4}\mathrm{Arcos}(1))})^r$$

Remarque: l'inégalité de Vojta suffit à prouver la conjecture de Mordell mais le résultat obtenu est plus précis .

Preuve de l'inégalité de Mumford [M1]:
On démontre les relations de classes de diviseurs (voir [M1] et [M2]); rappelons que Θ est supposé symétrique:

$j^*(\Theta)=g(O)$

$(j\times j)^*(\mathrm{add}^*(\Theta)-p_1^*(\Theta)-p_2^*(\Theta))=-\Delta'$

où add, p_1, p_2 sont respectivement l'addition et les projections de AxA vers A et $\Delta':=\Delta-Cx(O)-(O)xC$ et Δ est la diagonale de CxC.
Grâce aux propriétés H1,H2,H3 on obtient:

$$h_{(O)}(x)=\frac{1}{2g}\|j(x)\|^2+O(1)$$

$h_{\Delta'}(x,y)=-<j(x),j(y)>+O(1)$

$h_{\Delta}(x,y)=\frac{1}{2g}||j(x)||^2+\frac{1}{2g}||j(y)||^2-<j(x),j(y)>+O(1)$

On observe que la forme quadratique du membre de droite n'est pas définie positive (si $g\geq 2$!!) alors que, d'après la propriété H4 on a $h_{\Delta}(x,y)\geq O(1)$ si $(x,y)\notin\Delta$ i.e. si $x\neq y$. On en tire aisément l'inégalité de Mumford.

Preuve de l'inégalité de Vojta [V1]:

Le point de départ de Vojta est de considérer des diviseurs plus généraux de la forme:

$D=d_1Cx(O)+d_2(O)xC+d_3\Delta'$

(Remarque: si $d_1=d_2=d_3=1$ on retrouve $D=\Delta$)

Ayant fixé une hauteur $h_{(O)}$ associée à (O) sur C et une hauteur $h_{\Delta'}$ associée à Δ' sur $C\times C$ on a une hauteur associée à D définie par $h_D(x,y)=d_1h_{(O)}(x)+d_2h_{(O)}(y)+d_3h_{\Delta'}(x,y)$ et l'on obtient comme précédemment:

$h_D(x,y)=\frac{d_1}{2g}||x||^2+\frac{d_2}{2g}||y||^2-d_3<x,y>+O(d_1+d_2+d_3)$

La forme quadratique qui apparaît n'est pas définie positive dès que:

$$d_1d_2<g^2d_3^2$$

Toute la difficulté réside maintenant dans l'obtention d'une minoration $h_D(x,y)\geq -c(d_1,d_2,d_3)$

Vojta résoud ce problème avec des techniques très similaires à celles de l'approximation diophantienne.

Une première idée est de construire une section f de O(D) de taille controlée et si (par chance!) $f(x,y)\neq 0$ alors l'inégalité de Liouville donnera $h_D(x,y)\geq -\log||f||_\infty$.

Vojta construit f en montrant que D est très ample (sous des conditions explicitées ci-dessous) et en utilisant un théorème de Riemann-Roch arithmétique dû à Gillet-Soulé [G-S1] (voir [G-S2] pour une construction semblable). Bombieri remarque que le théorème de Riemann-Roch classique sur la surface $C\times C$ (l'inégalité, déjà connue des géomètres italiens, suffit) donne l'existence de beaucoup de sections, sous la condition:

$$gd_3<d_1d_2$$

on obtient un espace vectoriel de dimension proportionnelle à d_1d_2 et le lemme de Siegel permet de choisir une section de norme petite.

La deuxième idée est de dériver la section obtenue et de montrer qu'elle ne peut s'annuler avec un ordre trop élevé en (x,y); en effet on ne peut pas garantir $f(x,y)\neq 0$. Plus précisément on définit l'indice de la section f au point (x,y) comme

au paragraphe 1:

$\text{Indice}_{(d_1,d_2)(x,y)}(f):=\min\{\frac{i_1}{d_1}+\frac{i_2}{d_2}/\partial_i f(x,y)\neq 0\}$

Ici $\partial_i=\partial_{i_1,i_2}=\frac{1}{i_1!i_2!}(\frac{\partial}{\partial x_1})^{i_1}(\frac{\partial}{\partial x_2})^{i_2}$ où x_1 et x_2 sont des paramètres locaux en x et y sur la courbe C.

Remarque: dire qu'une dérivée de f s'annule n'a pas vraiment de sens (cela dépend de la trivialisation choisie) mais l'ordre d'annulation est bien défini.

Sous la condition:

$$d_2/d_1 \text{ très petit} \qquad (*)$$

on obtient une bonne borne pour $\text{Indice}_{(d_1,d_2)(x,y)}(f)$; Vojta utilise le "lemme de Dyson" sur CxC qu'il a prouvé pour cela [V2] et Bombieri utilise le lemme de Roth que j'ai enoncé (on commence par projeter CxC sur $\mathbf{P}^1x\mathbf{P}^1$).

Les contraintes explicitées de la preuve forcent pratiquement à choisir des paramètres proportionnels à:

$d_1:=[d/\|x\|^2]$ $d_2:=[d/\|y\|^2]$ et $d_3:=[d/\|x\|\|y\|(\sqrt{g}+\varepsilon)]$

où d est un paramètre qui tendra vers l'infini et ε est suffisament petit pour que $g<(\sqrt{g}+\varepsilon)^2<g^2$. Alors $d_1\|x\|^2$ est presque égal à $d_2\|y\|^2$ et la condition (*) équivaut à $\|x\|/\|y\|$ très petit, ce qui est précisément une des hypothèses. En joignant ces idées à de délicates estimations de la taille des derivées on obtient l'inegalité de Vojta.

4 Les sous-variétés de variétés abéliennes.

Je donne dans ce paragraphe l'esquisse de la preuve du théorème 1: l'extension par Faltings des idées du paragraphe précédent aux variétés de dimension >1, en essayant de faire ressortir le parallélisme des idées.

On considère donc $j:X\longrightarrow A$ une sous-variété d'une variété abélienne A et on appelle encore Θ un diviseur symétrique et ample sur A et $\|.\|$ la norme euclidienne associée à Θ sur $A(k)\otimes\mathbf{R}$. Comme dans la preuve du théorème de Roth on choisit un entier m et un réel ε petit (voir paragraphe suivant pour la "valeur" de m; si dimX=1 alors m=2); on dispose alors sur $A^m=AxAx...xA$ des diviseurs suivants:

$\Theta_i=p_i^*(\Theta)$ (diviseur 'fibre")

$P_{ij}=(p_i+p_j)^*(\Theta)-p_i^*(\Theta)-p_j^*(\Theta)$ (diviseur de Poincaré)
On travaille maintenant avec les diviseurs:
$D':=d_1\Theta_1+\ldots+d_m\Theta_m-e_1P_{12}-\ldots e_{m-1}P_{m-1,m}$ sur $A^m=A\times\ldots\times A$ et $D:=(j\times\ldots\times j)^*(D')$ sur $X^m=X\times\ldots\times X$. On calcule de la même façon $h_D(x_1,..,x_m)$ à partir de $\|x_i\|$ et $\langle x_i,x_j\rangle$; en effet $q_{\Theta_i}(x)=\frac{1}{2}\|x_i\|^2$ et $q_{P_{ij}}(x_1,..,x_m)=\langle x_i,x_j\rangle$ donc :

$$h_D(x_1,..,x_m)=\frac{1}{2}\sum d_i\|x_i\|^2-\sum e_i\langle x_i,x_{i+1}\rangle+O(\sum d_i+e_i)$$

La partie nouvelle et réellement difficile est la minoration de $h_D(x_1,..,x_m)$. Faltings montre que, sous les conditions suivantes:
A1) X ne contient pas de sous-variété abélienne translatée;
A2) m a été choisi assez grand (en fonction de dimX) et ε assez petit (en fonction de m);
A3) $d_i/d_{i+1}>r=r(\varepsilon,m)$ et $d_id_{i+1}=(2-\varepsilon)^2e_i^2$;
on a D ample sur X^m.
Remarques: D' n'est jamais ample sur A^m. La façon dont les deux premières hypothèses sont utilisées ainsi que leur nécessité est discutée au paragraphe suivant. La troisième hypothèse permet l'utilisation d'un outil nouveau qui remplace le lemme de Dyson ou Roth: le théorème du produit, très jolie découverte de Faltings:

THÉORÈME DU PRODUIT (Faltings [F2]).

Soit $x\in\mathbf{P}=\mathbf{P}^{n_1}\times..\times\mathbf{P}^{n_m}$, *et* f *une section de* $L=O(d_1,..,d_m)$ (*i.e. un polynôme multihomogène de degré* $d_1,..,d_m$)
On pose:

$$\text{Indice}_{x,(d_1,\ldots,d_m)}(f):=\max\{\tfrac{i_1}{d_1}+..+\tfrac{i_m}{d_m}\ \textit{/pour tout opérateur différentiel}\ \partial_k\ \textit{d'ordre}\ \le i_k\ \textit{sur}\ \mathbf{P}^{n_k}\ \textit{on a}\ \partial_1\cdots\partial_m f(x)=0\}$$

On note:

$$Z_\sigma:=\{x\in\mathbf{P}/\text{Ind}_{x,d}(f)>\sigma\}$$

Soit $\varepsilon>0$. *Il existe r (dépendant de* ε*) tel que si* $d_i/d_{i+1}>r$ *alors toute composante irréductible* Z *de* $Z_{\sigma+\varepsilon}$ *qui est aussi une composante de* Z_σ *est de la forme* $Z=Z_1\times..\times Z_m$ *avec* Z_i *sous-variété de* $\mathbf{P}^{n_i}$ *de degré borné par une constante dépendant seulement de* ε.

Ce théorème est énoncé sur un corps algébriquement clos; la seule difficulté sur un corps non algébriquement clos provient du fait qu'une composante irréductible peut ne pas être géométriquement irréductible.
Faltings a d'ailleurs montré [F4] comment on pouvait retrouver le théorème de Roth et la généralisation de Schmidt (le "théorème du sous-espace" [Sch2]) en utilisant ce théorème du produit.
Comme pour le théorème de Roth pour montrer qu'il n'existe pas de suite infinie de points rationnels dans X, on choisit m un grand entier et ε un réel petit; il suffit de montrer qu'il n'existe pas de suite $(x_1,..,x_m)$ de points de X(k) vérifiant:

a) $<x_i,x_{i+1}>\geq(1-\varepsilon/4)\|x_i\|\|x_{i+1}\|$ (i.e. les points sont dans un même cône)

b) $\|x_{i+1}\|/\|x_i\|>r=r(\varepsilon)$ et enfin

c) $\|x_1\|$ grand en fonction de ε.

On choisit alors s_i des nombres rationnels très proches de $\|x_i\|^{-1}$ et les paramètres $d_i=s_i^2(2-\varepsilon)$ et $e_i=s_is_{i+1}$ de sorte que les conditions A3) soient remplies; le calcul de la hauteur fournit:
$h_D(x_1,..,x_m)<\frac{1}{2}\sum s_i^2(2-\varepsilon)\|x_i\|^2-\sum s_is_{i+1}\|x_i\|\|x_{i+1}\|(1-\varepsilon/4)+O(\sum s_i^2)$
$<-\varepsilon m/4+O(\|x_1\|^{-2})$

On choisit encore un réel σ disons plus petit que $\varepsilon/4$ et un entier d très grand et suffisamment divisible. L'amplitude et une version raffinée du lemme de Siegel utilisant le théorème des minima successifs de Minkovski permettent de construire une section f de O(dD) ayant un indice $<\sigma$ en x et une norme petite (c'est-à-dire telle que $\log\|f\|_\infty<C\sum ds_i^2$); l'indice est pris par rapport aux poids ds_i^2.

Remarquons que cela renverse un peu l'ordre habituel: le théorème de non annulation, ici le théorème du produit, est déjà inclus dans la construction de la fonction (section) auxiliaire.
On montre ensuite que la norme d'une dérivée de f (ne s'annulant pas en x) vérifie une inégalité du même type et on applique l'inégalité de Liouville pour obtenir $-Cmd/\|x_1\|<-\varepsilon md/2$; d'où une contradiction si $\|x_1\|$ est assez grand!

5 La conjecture générale de Serge Lang.

Lang avait conjecturé un enoncé plus général (voir [La1], [La3] et [La4]) qui peut maintenant être établi. Lang a aussi suggéré que l'énoncé analogue pour les variétés semi-abéliennes devait être vrai; une preuve de cela a été annoncé par Vojta; je me restreint ici à l'énoncé sur les variétés abéliennes:

THÉORÈME 3: *Soit* A *une variété abélienne complexe et* X *une sous variété analytique (fermée), soit* Γ *un sous-groupe de rang fini de* A(**C**). *Alors il existe un nombre fini de points* t_i *de* Γ *et de sous-variétés abéliennes* B_i *(éventuellement nulles) telles que* t_i+B_i *soit contenu dans* X *et:*

$$X(\mathbf{C})\cap\Gamma=\cup t_i+(B_i(\mathbf{C})\cap\Gamma)$$

Cet énoncé contient bien sûr le théorème 1 (appliquer le théorème de Mordell-Weil) mais aussi la conjecture de Manin-Mumford (quand on prend $\Gamma=A_{torsion}$) prouvée auparavant par Raynaud [R1],[R2]. Cet énoncé général est conséquence du théorème suivant, comme cela est prouvé dans [R3] (quand il n'y a pas de sous-variétés abéliennes dans X) et dans [H1] (cas général); bien que l'énoncé semble analytique, on se ramène tout de suite à un corps de type fini sur **Q** et même, par des arguments de spécialisation non triviaux à un corps de nombres; la réduction d'un groupe de rang fini à un groupe de type fini utilise des arguments galoisiens.

THÉORÈME 4 (Faltings [F2]: *Soit* X *une sous-variété d'une variété abélienne* A *définies sur un corps de nombres* k; *il existe un nombre fini de points rationnels* t_i *et de sous-variétés abéliennes* B_i *telles que*

$$X(k)=\cup t_i+B_i(k).$$

Je ne présente pas la preuve assez semblable à la preuve du théorème 1 mais plus compliquée techniquement, toutefois j'explique où interviennent les sous-variétés abéliennes contenues (ou non) dans X et le début de la preuve de l'amplitude du diviseur D du paragraphe précédent. Notons $G_X:=\{a\in A/\ a+X=X\}$ le stabilisateur de X et Z_X l'adhérence de Zariski de l'union des translatés de sous-variétés abéliennes (non nulles, cette fois) contenus dans X; ainsi l'hypothèse du théorème 1 est que Z_X est vide et la conjecture de Lang dit que les points rationnels s'accumulent tous sur Z_X sauf pour un nombre fini d'entre eux.

LEMME 1: *Ou bien* G_X *est de dimension positive (et donc* $Z_X=X$), *ou bien* $Z_X\neq X$ et Z_X *est une union finie de sous-variétés stabilisées par une sous-variété abélienne de dimension positive.*

On peut bien sûr se ramener au cas numéro deux en quotientant par G_X Ce lemme est prouvé explicitement dans [R2] et [H1] et se trouve (caché) dans [Bg] (brièvement: il y a un nombre fini de sous-variété abéliennes maximales [Bg] dans X disons $B_1,..,B_s$ donc $Z_X=\cup(Z_i+B_i)$ où les Z_i sont des sous-variétés de X).

Revenons à la preuve de l'amplitude du diviseur D du paragraphe précédent. Un point essentiel est la considération du morphisme de X^m dans A^{m-1} défini par: $\alpha(x_1,..,x_m)=(t_1x_1-x_2,t_2x_2-x_3,..,t_{m-1}x_{m-1}-x_m)$ où les t_i sont entiers. Remarquons que si x_0+B est inclus dans X et si on pose $x_0 1=(x_0,..x_0)$ et $B(t_1,..,t_m)=\{(x,t_1x,t_1t_2x,..,t_1..t_{m-1}x)/x\in B\}$ alors $\alpha(x_0 1+B(t_1,..,t_m))$ est réduit à un point. Le lemme suivant est une petite généralisation du lemme 4.1 de Faltings [F2]:

LEMME 2: *Il existe* m *tel que si* $t_1\geq..\geq t_{m-1}\geq 2$ *alors le morphisme* α *de* X^m *dans* A^{m-1} *est génériquement fini; plus précisément les composantes de dimension positive des fibres sont de la forme* $x+B(t_1,..,t_m)$ *où* B *est une sous-variété abélienne maximale de* X.
De plus si $t_{m-1}\geq \deg X(2d)^{\dim X}$ *alors on peut choisir* $m=(\dim X+1)!$ (*où* deg X *et* d *désignent respectivement le degré projectif de* X *et le degré d'équations définissant* X *dans* A *dans un plongement projectif).*

Par définition de α l'image réciproque d'un point est formée des m–uplets $(x_1,..,x_m)$ tels que $x_{i+1}=t_ix_i-b'_i$ et donc de la forme $(x,t_1x-b_1,..,t_1..t_{m-1}x-b_{m-1})$ dans laquelle le point x vérifie : $x\in X\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m-1}]^{-1}(X+b_{m-1})$; il faut donc prouver que les composantes de cet ensemble algébrique sont des translatés de sous-variétés abéliennes, si m est assez grand. Supposons prouvé que les composantes non abéliennes de tous les ensembles du type $(X+b_0)\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_m]^{-1}(X+b_m)$ sont de dimension $\leq r$; soit alors $F:=X\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m+k}]^{-1}(X+b_{m+k})$ contenant une composante Z non abélienne de dimension r, alors Z est aussi une composante de:
$F_1=(X+b_0)\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m-1}]^{-1}(X+b_{m-1})$
et $[t_1..t_k](Z)$ est contenu dans:

$F_2=(X+b_k)\cap[t_{k+1}]^{-1}(X+b_{k+1})\cap..\cap[t_{k+1}..t_{m+k}]^{-1}(X+b_{m+k})$
et donc en est une composante. En utilisant la formule $\deg[t](Z)=\deg(Z)t^{2r}/|\mathrm{Ker}[t]\cap G_Z|$ et les autres lemmes de [H1] on obtient:

$$(t_{m+1}..t_k)^{2(r-\dim G_Z)}\leq(t_{k+1}..t_{m+k})^{2(\dim X-r)}\deg X(2d)^{\dim X}$$

ce qui borne visiblement k; on finit facilement la preuve du lemme par récurrence sur r en utilisant les hypothèses sur les t_i.

Considérons Θ'_i l'image réciproque de Θ par la i-ème projection sur A^{m-1}, soit $D_0=\alpha^*(\sum s_{i+1}{}^2\Theta'_i)=\sum(t_i s_{i+1}p_i-s_{i+1}p_{i+1})^*(\Theta)$; alors D_0 est ample si α est fini (et "génériquement ample" si α est génériquement fini). Si on s'arrange pour que $t_i s_{i+1}=s_i$ le diviseur D que nous souhaitons étudier s'écrit $D=D_0-\varepsilon\sum s_i{}^2\Theta_i$ et est donc certainement ample si ε est assez petit (mais dépendant des s_i). Il faut encore beaucoup travailler: Faltings utilise avec brio le théorème de Riemann-Roch, une variante du critère de Nakai-Moishezon (voir [Ha1] et [Ha2]) due à Kleiman et le théorème du produit pour rendre ε indépendant des paramètres.

5 Points algébriques sur les courbes

Le problème est le suivant: on considère une courbe lisse et projective C de genre g et l'on s'intéresse non pas à C(k) mais à l'union de tous les C(L) lorsque L décrit toutes les extensions de degré au plus d; notons cet ensemble $C_d(k)$; on veut savoir quand cet ensemble est fini et éventuellement le paramétrer si il est infini.
Le lien avec la conjecture de Lang est décrit dans [H1]: on commence par observer que les points algébriques de degré au plus d correspondent au points rationnels de $S^dC:=Cx...xC/\Sigma_d$, où Σ_d désigne le groupe symétrique avec son action évidente sur C^d. Plus précisément, à un point $x\in C(\bar{k})$ tel que $[k(x):k]=d$ on associe ses conjugués par Galois $x=x_1,..,x_d$ et le point $\varphi(x):=(x_1)+..+(x_d)\in S^dC(k)$; on identifie implicitement un élément de S^dC avec un diviseur effectif de degré d. Inversement, un point $D=(x_1)+..+(x_d)\in S^dC(k)$ est défini par des $x_i\in C(\bar{k})$ tels que l'ensemble $\{x_1,..,x_d\}$ soit stable par Galois et se décompose donc en orbites de points de degré $d_1,..d_r$ avec $d_1+..+d_r=d$; en particulier $[k(x_i):k]\leq d$. Ces considérations prouvent le lemme suivant:

LEMME 3:

a) $C_d(k)$ *est fini si et seulement si* $S^dC(k)$ *est fini.*

b) *Si* $C_{d-1}(k)$ *est fini alors* φ *définit une bijection entre* $C_d(k)$ *et* $S^dC(k)$ *à un nombre fini d'éléments près.*

Le lien avec la "conjecture" de Lang est établi grâce au théorème d'Abel-Jacobi: on

considère l'application:

ϕ_d: $S^dC \longrightarrow A=Jac(C)$

$(x_1)+..+(x_d) \longrightarrow x_1+..+x_d$ (la somme étant dans A bien sur)

On note classiquement $W_d=W_d(C)$ l'image; alors $\phi_d(D)=\phi_d(D')$ équivaut à $D=D'+(f)$ et si $D\neq D'$ on en déduit l'existence d'un morphisme $f:C \longrightarrow \mathbf{P}^1$ non constant de degré au plus d; inversement l'existence d'un tel morphisme donne des diviseurs $f^*(x)$ (pour x dans $\mathbf{P}^1$) tous linéairement équivalents; en résumé ϕ_d contracte toutes les courbes rationnelles sur S^dC et celles-ci proviennent de morphismes de C sur $\mathbf{P}^1$.

La signification du lemme suivant est éclairée si l'on se souvient qu'une courbe de genre g admet un morphisme de degré d sur $\mathbf{P}^1$ si $d\geq 1+g/2$ (pour une preuve de ce fait, voir par exemple [K-L]).

LEMME 4: $\phi_d: S^dC \longrightarrow W_d$ *est un isomorphisme si et seulement si il n'existe pas de morphisme non constant de degré* $\leq d$ *de* C *sur* $\mathbf{P}^1$.

Le théorème suivant est une conséquence du théoreme 4 (Faltings [F2]) et était conjecturé dans [H1].

THÉORÈME 5: $C_d(k)$ *est fini pour tout corps de nombres si et seulement si* C *n'admet aucun morphisme de degré* $\leq d$ *sur* $\mathbf{P}^1$ *et si* W_dC *ne contient aucun translaté de sous-variétés abéliennes.*

Remarquons que d'après des résultats généraux sur les diviseurs sur les courbes (voir par exemple [K-L]) la condition du théorème est vérifiée pour une courbe de genre g "générale" si $d<1+g/2$. On peut être plus précis par exemple dans le cas d=2; le théorème suivant est conséquence cette fois du théorème 4 (Faltings [F3]) comme cela est expliqué dans [H2].

THÉORÈME 6: $C_2(k)$ *est, à un nombre fini d'éléments près, l'union des points hyperelliptiques (i.e. images réciproques de* $\mathbf{P}^1(k)$ *par* $f:C\rightarrow\mathbf{P}^1$ *de degré* 2) *et surelliptiques ou bi-elliptiques (i.e. images réciproques de* E(k) *par* $f:C\rightarrow E$ *de degré* 2 *avec* E *courbe elliptique*)

Ce problème a été aussi considéré par Frey [Fr] sur les courbes modulaires et Silverman et Harris [Ha-Si]. Il est intéressant de remarquer que Vojta, en poussant

sa méthode obtient dans [V3] des résultats un peu moins précis mais en travaillant uniquement sur les courbes.
On peut donner l'exemple suivant d'une courbe de genre 3 hyperelliptique avec trois revêtements de degré 2 sur des courbes elliptiques:

$$y^2=(x^2-a^2)(x^2-a^{-2})(x^2-b^2)(x^2-b^{-2});$$

mais il est connu qu'une courbe hyperelliptique de genre >3 ne peut avoir un revêtement de degré 2 sur E (Preuve dans [F2] ou dans [A-C-G-H]); par contre la courbe $y^2-(x-a_1)(x-a_2)(x-a_3)=z^2-(x-a_4)...(x-a_{g+2})=0$ a pour genre g (si les a_i sont tous distincts) et est revêtement double de la courbe elliptique d'équation:
$y^2=(x-a_1)(x-a_2)(x-a_3)$; en particulier si g>3 elle n'est pas hyperelliptique.

Harris et Abramovich ont poussé l'analyse plus loin en conjecturant:

CONJECTURE [A-H]
$C_d(k)$ *est fini pour tout corps de nombres* k *si et seulement si* C *ne possède aucun morphisme de degré au plus* d *de* C *sur* $\mathbf{P}^1$ *ou* E.

Il revient au même de conjecturer que si C n'est pas d-gonale, i.e. revêtement de $\mathbf{P}^1$ de degré d, et s'il existe une variété abélienne dans W_dC alors il existe une courbe elliptique dans W_dC et plus précisément C est "d-elliptique"; il s'agit donc d'une conjecture purement géométrique. Harris et Abramovic établissent dans le même article le résultat suivant:

THÉORÈME 7 [A-H]:
La conjecture est vraie si d<5 *sauf (peut-être) si* d=4 *et* g=7.

Ils donnent aussi un joli exemple d'une famille de courbes de genre 5 possédant une surface abélienne dans W_4 sans être un revêtement double d'une courbe de genre 2 (ni d'une courbe de genre 1).

(*ajouté sur épreuve, dernière minute*):
J'apprends que la conjecture de Abramovich et Harris est fausse: lorsque d≥10, Debarre et Fahlaoui ont construit des courbes de genre $g=1+d(d-1)/2$ n'admettant aucun morphisme de degré ≤d sur $\mathbf{P}^1$ ou une courbe elliptique mais telle que leurs W_d contiennent une courbe elliptique.

Dans une autre direction, Frey ("Curves with infinitely many points of fixed degree", à paraître dans Israel J.of Math.) a prouvé que si $C_d(k)$ est infini alors il existe un morphisme de C sur $\mathbf{P}^1$ de degré au plus 2d et défini sur k.

Bibliographie

[A-C-G-H] E. ARBARELLO, M. CORNALBA, P. GRIFFITHS and J. HARRIS. Geometry of curves, vol. I. *Springer* 1985.

[A-H] D. ABRAMOVICH and J. HARRIS. Abelian varieties and curves in W_dC. *Preprint.*

[Bg] F. BOGOMOLOV. Points of finite order on an abelian variety. *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980); *AMS translation Math. USSR Izv.* **17** (1981), *55-72.*

[B] E. BOMBIERI. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Ser. IV* **17** (1990), *615-640;* errata *ibid.* **18** (1991), *473.*

[Co-Si] G. CORNELL and J. SILVERMAN. Arithmetic geometry. *Springer* 1986.

[E-V] H. ESNAULT and E. VIEHWEG. Dyson's lemma for polynomials in several variables. *Inv. Math.* **78** (1984), *445-490.*

[F1] G. FALTINGS. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inv. Math.* **73** (1983), *349-366.*

[F2] G. FALTINGS. Diophantine approximation on abelian varieties. *Annals of Math.* **133** (1991), *549-576.*

[F3] G. FALTINGS. The general case of Lang's conjecture. *Preprint.*

[F4] G. FALTINGS. *Preprint.*

[Fr] G. FREY. A remark on isogenies of elliptic curves over quadratic fields. *Compositio Math.* **58** (1986), *133-134.*

[G-S1] H. GILLET and G. SOULÉ. Un théorème de Riemann-Roch arithmétique. *C. R. Acad. Sci. Paris Sér. I Math.* **309** (1989), *929-932.*

[G-S2] H. GILLET and G. SOULÉ. Amplitude arithmétique. *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), *887-890.*

[G-S3] H. GILLET and G. SOULÉ. Arithmetic intersection theory. *Publ. Math. IHES* **72** (1990), *93-174.*

[Ha1] R. HARTSHORNE. Algebraic geometry. *Springer* 1977.

[Ha2] R. HARTSHORNE. Ample subvarieties of algebraic varieties. *Springer Lecture Notes in Math.* **156** (1970).

[Ha-Si] J. HARRIS and J. SILVERMAN. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.* **112** (1991), *347-356.*

[H1] M. HINDRY. Autour d'une conjecture de Serge Lang. *Inv. Math.* **94** (1988), *575-603.*

[H2] M. HINDRY. Points quadratiques sur les courbes. *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), *219-221*

[K-L] S. KLEIMAN and D. LAKSOV. Another proof of the existence of special divisors. *Acta Math.* **132** (1974), *163-176.*

[La1] S. LANG. Fundamentals of diophantine geometry. *Springer* 1983.

[La2] S. LANG. Abelian varieties. *Interscience, New York* 1959.

[La3] S. LANG. Integral points on curves. *Publ. Math. IHES* **6** (1960), *27-43.*

[La4] S. LANG. Division points on curves. *Ann. Mat. Pura Appl. (4)* **70** (1965), *229-234.*

[M1] D. MUMFORD. A remark on Mordell's conjecture. *Amer. J. Math.* **87** (1965), *1007-1016.*

[M2] D. MUMFORD. Abelian varieties. *Oxford University Press* 1974.

[R1] M. RAYNAUD. Courbes sur une variété abélienne et points de torsion. *Inv. Math.* **71** (1983), *207-233.*

[R2] M. RAYNAUD. Sous-variétés d'une variété abélienne et points de torsion. *Arithmetic and geometry: papers dedicated to I.R. Shafarevich on the occasion of his sixtieth birthday, vol I, M. Artin and J. Tate ed., Birkhäuser* 1983, *327-352.*

[R3] M. RAYNAUD. Around the Mordell conjecture for function fields and a conjecture of Serge Lang. *Algebraic geometry, Springer Lecture Notes* **1016** (1983), *1-19.*

[Ro] F. ROTH Rational approximation to algebraic numbers. *Mathematika* **2** (1955), *1-20.*

[Sch1] W. SCHMIDT. Diophantine approximation. *Springer Lecture Notes* **785** (1980).

[Sch2] W. SCHMIDT. Approximation to algebraic numbers. *Enseign. Math.* **17** (1971), *187-253.*

[Se] J-P. SERRE. Lectures on the Mordell-Weil theorem (translated by M. Brown from notes by M. Waldschmidt). *Vieweg* 1989.

[Si] C. SIEGEL. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.* (1929), *41-69.*

[Sz1] L. SZPIRO. Séminaire sur les pinceaux arithmétiques (la conjecture de Mordell). *Astérisque* **127** (1985).

[Sz2] L. SZPIRO. Sur les solutions d'un système d'équations polynomiales sur une variété abélienne (d'après Faltings et Vojta). *Séminaire Bourbaki, exposé 729, Astérisque* **189-190** (1990), *429-446.*

[Vi] C. VIOLA. On Dyson's lemma. *Ann. Scuola Norm. Sup. Pisa Ser. IV* **12** (1985), *105-135.*

[V1] P. VOJTA. Siegel's theorem in the compact case. *Annals of Math.* **133** (1991), *509-548.*

[V2] P. VOJTA. Dyson's lemma on the product of two curves. *Inv. Math.* **98** (1989), *107-113.*

[V3] P. VOJTA. Arithmetic discriminants and quadratic points on curves. *Arithmetic algebraic geometry, Texel '89, Birkhäuser "Progress in Mathematics"* **89** (1991), *356-376.*

[V4] P. VOJTA. A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing. *J. Amer. Math. Soc.* **5** (1992), *763-804.*

[W] A. WEIL. Sur les courbes algébriques et les variétés qui s'en déduisent. *Hermann, Paris* 1948.

Marc HINDRY
UFR Mathématiques, Université Paris 7
2 Place Jussieu
75251 Paris cedex 05, FRANCE
et
Mathematics, Brown University
Providence RI 02912, U.S.A.

Astérisque

K. RAMACHANDRA

On Riemann zeta-function and allied questions

Astérisque, tome 209 (1992), p. 57-72

<http://www.numdam.org/item?id=AST_1992__209__57_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

ON RIEMANN ZETA-FUNCTION AND ALLIED QUESTIONS

K. RAMACHANDRA

TO PROFESSOR R. BALASUBRAMANIAN
ON HIS FORTIETH BIRTHDAY

§ 1. **Introduction.** I will divide my lecture as follows.

§ 1. Introduction

§ 2. Conjectures 1 and 2.

§ 3. Conjecture 3 and a further question.

§ 4. Balasubramanian-Ramachandra (sufficient) condition for the validity of Conjecture 3.

§ 5. The Balasubramanian-Ramachandra condition is not always satisfied (Counterexample : a power of the Kahane series).

§ 6. Progress towards Conjectures 1 and 2 (Titchmarsh Series-I, Weak Titchmarsh Series, and Titchmarsh Series-II)

§ 7. Applications of Theorems 1 to 4 of § 6.

§ 8. Consequences of Conjectures 1 and 2 without Riemann Hypothesis.

§ 9. Further Conjectures (which would follow from Conjectures 1 and 2 and Riemann Hypothesis).

S. M. F.
Astérisque 209** (1992)

As will be seen in § 7 Conjectures 1 and 2 are more intimately connected with the Riemann zeta-function (and also with zeta and L-functions of algebraic number fields, zeta-functions of ray class fields and so on). But we emphasise only on the Riemann zeta-function.

§ 2. **Conjectures 1 and 2.** For all $N \geq H \geq 1000$ and all N-tuples $a_1 = 1, a_2, \cdots, a_N$ of complex numbers prove (or disprove!) that

Conjecture 1.

$$\frac{1}{H}\int_0^H \Big|\sum_{n\leq N} a_n n^{it}\Big|\, dt \geq 10^{-1000}, \tag{1}$$

Conjecture 2.

$$\frac{1}{H}\int_0^H \Big|\sum_{n\leq N} a_n n^{it}\Big|^2 dt \geq (\log H)^{-1000} \sum_{n\leq M} |a_n|^2 \tag{2}$$

where $M = H(\log H)^{-2}$.

Remark 1. We can formulate conjectures where RHS in (1) and (2) are bigger than the present ones. For example we can replace RHS of (2) by

$$C_1 \sum_{n\leq C_2 H} |a_n|^2$$

where $C_1 > 0$ and $C_2 > 0$ are numerical constants (in fact with any $C_1 < 1$).

Remark 2. Let $1 = \lambda_1 < \lambda_2 < \lambda_3 < \cdots$ be any sequence of real numbers with $\lambda_{n+1} - \lambda_n$ bounded both above and below. Then we can formulate more general conjectures where $\sum_{n\leq N} a_n n^{it}$ is replaced by $\sum_{n\leq N} a_n \lambda_n^{it}$.

§ 3. **Conjecture 3 and a further question.** Let $a_1 = \lambda_1 = 1$, $\lambda_1 < \lambda_2 < \lambda_3 < \cdots$, $\frac{1}{C} \leq \lambda_{n+1} - \lambda_n \leq C$, $\{a_n\}$ $(n = 1, 2, 3, \cdots)$ a sequence of complex numbers such that $F(s) = \sum_{n=1}^{\infty} a_n \lambda_n^{-s}$ is convergent for some $s = \sigma + it$ in the complex plane and can be continued analytically in $(\sigma \geq \beta, T \leq t \leq 2T)$ where β is a positive constant $< \frac{1}{2}$ and there the maximum of $|F(s)| \leq T^A$ where A and C are positive constants ≥ 1. Suppose $\sum_{n\leq x} |a_n|^2 \gg_\varepsilon x^{1-\varepsilon}$ for every $\varepsilon > 0$ and every $x \geq 1$. Then prove (or disprove) the

Conjecture 3. *The number of zeros of* $F(s)$ *in* $(\sigma \geq \beta, T \leq t \leq 2T)$ *is*

$$\gg T \log T. \tag{3}$$

Remark. A simple application of Jensen's Theorem (see $[T]_1$, page 125) shows that the number of zeros of $F(s)$ in $(\sigma \geq (\beta + \frac{1}{2})/2, T + D \leq t \leq 2T - D)$ is $\ll T \log T$, provided D is a large positive constant. Thus speaking roughly,

the order of magnitude of the number of zeros in question is $T \log T$ (if the Conjecture 3 is true).

A further question. *Let $\beta(T) < \frac{1}{2}$ and $\beta(T) \to \frac{1}{2}$ as $T \to \infty$. Then study the lower bound for the number of zeros of $F(s)$ in*

$$(\sigma \geq \beta(T), T \leq t \leq 2T). \tag{4}$$

§ 4. Balasubramanian-Ramachandra (sufficient) condition for the validity of Conjecture 3.

Sufficient Condition. *There should exist a positive constant $\delta < \frac{1}{2} - \beta$ such that*

$$\frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|^2\, dt \ll \left(\frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|\, dt\right)^2. \tag{5}$$

Remark 1. We will show in this section that the condition (5) is sufficient for the validity of Conjecture 3. (Note that the inequality which is the opposite of (5) is always true). From our proof it will be plain that the condition

$$\left(\frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|^g\, dt\right)^h \ll \left(\frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|^h\, dt\right)^g \tag{5'}$$

for some constants g, h with $0 < h < g$ is also sufficient.

Remark 2. A class of examples of $F(s)$ satisfying the condition (5) were studied in $[BR]_3, [BR]_4, [R_5]$, and to some extent $[BR]_5$. We content here by saying that a simple example of $F(s)$ satisfying (5) is $\zeta(s) + \sum_{n=1}^{\infty}(\chi(n)n^{-s})$ where $\chi(n)$ is any sequence of complex numbers with $\sum_{n\leq x}\chi(n) = O(1)$. For the series $\zeta(s) + \sum_{n=1}^{\infty}(\chi(n)n^{-s})$ where $\sum_{n\leq x}\chi(n) = O(x^{\frac{1}{2}-\eta})$ for some constant $\eta > 0$ and further $\chi(n) = O(1)$ the lower bound for the number of zeros in $(\sigma \geq (1-\eta)/2, T \leq t \leq 2T)$ is $\gg T(\log T)(\log\log T)^{-1}$. Both these results have been generalised to generalised Dirichlet series of the form $F(s) = \sum_{n=1}^{\infty}(a_n b_n \lambda_n^{-s})$ where $\{a_n\}$ and $\{b_n\}$ are somewhat general sequences of complex numbers and $\{\lambda_n\}$ is a somewhat general sequence of real numbers (see $[BR]_3, [BR]_4, [R]_5, [BR]_5,$). Less satisfactory results than Conjecture 3 were obtained in $[R]_3$, and $[R]_4$.

Remark 3. For suitable $\beta(t)$ the lower bounds for the number of zeros in (4) of $F(s)$ were studied in $[R]_6, [BR]_6$, and $[BR]_7$. For example in $[R]_6$, it was shown in great generality that $F(s)$ has $\gg T^{1-\varepsilon}$ zeros in $(\sigma \geq \frac{1}{2} - C_0(\log\log T)^{-1}, T \leq t \leq 2T)$. In $[BR]_6$, the functions mentioned in Remark 2 were considered. For example it was proved that the number of zeros of

$F(s) = \zeta(s) + \sum_{n=1}^{\infty}(\chi(n)n^{-s})$ $\left(\text{with } \chi(n) = O(1) \text{ and } \sum_{n\le x}\chi(n) = O\left(x^{\frac{1}{2}-\delta}\right)\right)$ in $(\sigma \ge \frac{1}{2} - C_0(\log\log T)^{\frac{3}{2}}(\log T)^{-\frac{1}{2}}, T \le t \le 2T)$ is $\gg T(\log\log T)^{-1}$. In $[BR]_7$, it was shown that (for $(\log T)^C \le H \le T$ where C is a large constant) in $(\sigma \ge \frac{1}{2} - C_0(\log\log T)(\log H)^{-1}, T \le t \le T+H)$ $\zeta(s)$ has $\gg H(\log\log\log T)^{-1}$ zeros. The interesting fact was that only the Euler product and the analytic continuation (in fact for the lower bound $\gg \cdots$ the upper bound $\log|F(s)| \ll (\log T)^C$ is enough)

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty}\left(n^{-s} - \int_n^{n+1} u^{-s}du\right), (\sigma > 0),$$

were used in the proof. Using these things only it is well known that we can prove that when $H = T$, the number of zeros is $\le T^{\frac{3}{2}-\sigma}(\log T)^C$.

We now resume the Remark 1. We will show that (5) implies that there are points $t_1, t_2, \cdots, t_N$ (where $N \gg T$) with $|t_j - t_{j'}|$ bounded below whenever $j \ne j'$ and further

$$|F(\frac{1}{2} - \delta + it_j)| > T^{\frac{\delta}{10}}, \ (T \le t_j \le 2T). \tag{6}$$

After this we have only to apply Theorem 3 of § 4 in $[BR]_3$ to obtain the proof of Conjecture 3. To deduce (6) from (5) we write

$$\psi(T) = \frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|\,dt. \tag{7}$$

Now RHS of (7) is

$$\frac{1}{T}\sum_I \int_I |F(\frac{1}{2} - \delta + it)|\,dt \tag{8}$$

where $\{I\}$ is a division of $[T, 2T]$ into disjoint (but abutting intervals I of equal length the length being both above and below). Plainly the expression (8) is

$$\le \frac{2}{T}\sum_I{}' \int_I |F(\frac{1}{2} - \delta + it)|\,dt \tag{9}$$

where the accent denotes the restriction of the sum to intervals I for which the integral is not less than $\varepsilon\,\psi(T)$ for a small constant $\varepsilon > 0$. Now

$$\begin{aligned}
\psi(T) &\le \tfrac{2}{T}\sum_I{}' \int_I |F(\tfrac{1}{2} - \delta + it)|\,dt \\
&\le \tfrac{2}{T}\left(\sum_I{}' 1\right)^{\frac{1}{2}}\left(\sum_I{}'\left(\int_I |F(\tfrac{1}{2} - \delta + it)|\,dt\right)^2\right)^{\frac{1}{2}} \\
&\ll \tfrac{1}{T}\left(\sum_I{}' 1\right)^{\frac{1}{2}}\left(\sum_I{}' \int_I |F(\tfrac{1}{2} - \delta + it)|^2\,dt\right)^{\frac{1}{2}}.
\end{aligned}$$

We now sum over all I in the last sum and use (5). We get

$$\psi(T) \ll \frac{1}{T}\left(\sum_I{}'1\right)^{\frac{1}{2}} (T\psi^2)^{\frac{1}{2}}$$

and this in turn gives

$$\sum_I{}'1 \gg T.$$

This gives (6) (which as we have already stated yields the conjecture), provided we prove that $\psi(T) \gg T^{\frac{\delta}{9}}$. By (5) and (7) it suffices to prove that

$$\frac{1}{T}\int_T^{2T} |F(\frac{1}{2} - \delta + it)|^2\, dt \gg T^{\frac{2\delta}{9}}. \tag{10}$$

This will follow unconditionally from Theorem 2 of § 6 of the present paper.

§ 5. **The Balasubramanian-Ramachandra condition is not always satisfied (Counterexample : a power of the Kahane series).** In this section we will show that a suitable (bounded) positive integral power of the "KAHANE SERIES" serves as a counterexample to (5). Kahane series are series of the form

$$K(s) = \sum_{n=1}^{\infty} \varepsilon_n((2n-1)^{-s} - (2n)^{-s}) \tag{11}$$

where ε_n are arbitrary subject to $\varepsilon = \pm 1$. By an ingenious probabilistic argument J.-P. Kahane showed that there exists a sequence $\{\varepsilon_n\}$ for which the Lindelöf function $\mu(\sigma)$ equals $1 - \sigma$ for $0 < \sigma < 1$. In particular given a fixed δ with $0 < \delta < \frac{1}{2}$ there exists a sequence $\{t_n\}$ with $t_n = t_n(\delta) \to \infty$ such that

$$|K(\frac{1}{2} - \delta + it_n)| \gg_{\varepsilon,\delta} t_n^{\delta+\frac{1}{2}-\varepsilon} \tag{12}$$

(For reference see Theorem 2.2 equation (30) on page 139 of [K]). It is not hard to show (whatever be the choice of ε_n) that $K(s)$ is analytic in $\sigma \geq \varepsilon > 0$ and there it is $O(t)$. Also all the derivatives upto any fixed order are $O(t)$ (for instance by Cauchy's theorem). Moreover with some work it is not difficult to show (see for example Theorem 11 of $[R]_5$) that

$$\frac{1}{T}\int_T^{2T} \left|K(\frac{1}{2} - \delta + it)\right|^2 dt \ll T^{2\delta} \tag{13}$$

and so

$$\frac{1}{T}\int_T^{2T} |K(\frac{1}{2} - \delta + it)|\, dt \ll T^{\delta}. \tag{14}$$

By iterating (5) we obtain

$$\frac{1}{T}\int_T^{2T} |K(\frac{1}{2} - \delta + it)|^k\, dt \ll \left(\frac{1}{T}\int_T^{2T} |K(\frac{1}{2} - \delta + it)|\, dt\right)^k \tag{15}$$

for all fixed $k = 2^m$ where m is an integer ≥ 1. Now for $|t - t_n| \leq t_n^{-1} (= \lambda$ say), we have $|K(\frac{1}{2} - \delta + it)| \gg_{\delta,\varepsilon} t^{\delta+\frac{1}{2}-\varepsilon}$ since as remarked above the derivative of $K(\frac{1}{2} - \delta + it)$ is $O(t)$. Hence

$$\int_{t_n-\lambda}^{t_n+\lambda} |K(\frac{1}{2} - \delta + it)|^k \, dt \gg_{\delta,\varepsilon} t_n^{k(\delta+\frac{1}{2}-\varepsilon)-1}. \tag{16}$$

Thus if (15) is true we obtain for $T = t_n - 1$ the estimate

$$T^{k(\delta+\frac{1}{2}-\varepsilon)-2} \ll_{\varepsilon,\delta} \frac{1}{T} \int_T^{2T} \left|K(\frac{1}{2} - \delta + it)\right|^k \, dt \ll T^{k\delta} \tag{17}$$

which is false for $k = 8$. Thus (15) is false for $k = 8$ and so at some stage of iteration (5) is false i.e. (5) is false for $F(s) = K(s), (K(s))^2$ or $(K(s))^4$. We can prove that (5) is false for $(K(s))$ or $(K(s))^2$ by a slight sharpening of the method above.

Remark. The procedure adopted in this section resembles to some extent an argument on page 329 of $[\mathrm{T}]_2$.

§ 6. Progress towards Conjectures 1 and 2 (Titchmarsh Series-I, Weak Titchmarsh Series, and Titchmarsh Series-II)

My paper $[\mathrm{R}]_7$ contains a result which is sufficient for all practical applications. Here we mention six theorems which solved the conjectures proposed by me in $[\mathrm{R}]_7$. These six theorems form further progress towards the conjectures 1 and 2 of § 2 of the present paper. We begin with a definition.

Titchmarsh series. *Let $a_1 = \lambda_1 = 1$, $\{a_n\}$ $(n = 1, 2, 3, \cdots)$ a sequence of complex numbers, $\{\lambda_n\}$ $(n = 1, 2, 3, \cdots)$ a sequence of real numbers with $\frac{1}{C} \leq \lambda_{n+1} - \lambda_n \leq C$, where C (≥ 1) is a constant. Let $H \geq 10$ be a real parameter and $|a_n| \leq (nH)^A$ for all n, where A is a positive integer constant. Suppose $F(s) = \sum_{n=1}^{\infty} (a_n \lambda_n^{-s}), (\sigma \geq A + 2)$ can be continued analytically in $(\sigma \geq 0,\ 0 \leq t \leq H)$. Such a function $F(s)$ is called Titchmarsh series.*

Theorem 1. *Put $u = H^{\frac{7}{8}} + 50(A + 2)\log\log(K + 1)$, where $K \geq 30$ and suppose that there exist T_1 and T_2 with $0 \leq T_1 \leq U, H - U \leq T_2 \leq H$ such that the Titchmarsh series $F(s)$ satisfies the inequality*

$$|F(\sigma + iT_1)| + |F(\sigma + iT_2)| \leq K \tag{18}$$

uniformly in σ for $0 \leq \sigma \leq A + 2$. Also let

$$H \geq (3456000A^2C^3)^{640000A} + (240000A)^{20}\log\log(K + 1). \tag{19}$$

Then, we have,

$$\int_0^H |F(it)|dt \geq H - 8000AH^{\frac{7}{8}} - 240000A^2\log\log(K + 1). \tag{20}$$

Theorem 2. *Suppose that (for some $K \geq 30$) there exist T_1 and T_2 with $0 \leq T_1 \leq H^{\frac{7}{8}}, H - H^{\frac{7}{8}} \leq T_2 \leq H$, such that the Titchmarsh series $F(s)$ satisfies the inequality*

$$|F(\sigma + iT_1)| + |F(\sigma + iT_2)| \leq K \tag{21}$$

uniformly in σ for $0 \leq \sigma \leq A + 2$. Also let

$$H \geq (4C)^{9000A^2} + 520000A^2 \log\log K_1 \tag{22}$$

where $K_1 = (HC)^{12A}K$. Then, we have,

$$\int_0^H |F(it)|^2 dt \geq \sum_{n \leq \alpha H} (H - (3C)^{1000A} H^{\frac{7}{8}} - 130000A^2 \log\log K_1 - 100C^2 n)\, |a_n|^2 \tag{23}$$

where $\alpha = (200C^2)^{-1} 2^{-8A-20}$.

Remark. These theorems are consequences of the second and the third main theorems of the paper $[\mathrm{BR}]_8$. We can get Theorem 1 above by putting $\varepsilon = \frac{1}{2}$, $r = 800A$ in the second main theorem.

Our next two theorems deal with

Weak Titchmarsh Series. *Let $0 \leq \varepsilon < 1, D \geq 1, C \geq 1$ and $H \geq 10$. Put $R = H^{\varepsilon}$. Instead of $|a_n| \leq (nH)^A$ suppose that*

$$\sum_{\lambda_n \leq X} |a_n| \leq D(\log X)^R \tag{24}$$

holds for all $X \geq 3C$. Then, for complex $s = \sigma + it, \sigma > 0$ we refer to $F(s) = \sum_{n=1}^{\infty} (a_n \lambda_n^{-s})$ as a weak Titchmarsh series associated with the parameters occuring in this definition

Theorem 3. *For a weak Titchmarsh series $F(s)$ with $H \geq 36C^2H^{\varepsilon}$, we have*

$$\liminf_{\sigma \to 0+} \int_0^H |F(\sigma + it)|\, dt \geq H - 36C^2H^{\varepsilon} - 12CD. \tag{25}$$

Theorem 4.
For a weak Titchmarsh series $F(s)$ with $\log H \geq 4320C^2(1 - \varepsilon)^{-5}$, we have

$$\liminf_{\sigma \to 0+} \int_0^H |F(\sigma + it)|^2\, dt \geq \sum_{n \leq M} \left(H - \frac{H}{\log H} - 100C^2 n\right) |a_n|^2 - 2D^2 \tag{26}$$

where $M = (36C^2)^{-1} H^{1-\varepsilon} (\log H)^{-4}$.

Remark. The four theorems mentioned above are enough for all applications in the present state of knowledge. For Theorems 3 and 4 see $[\mathrm{R}]_8$.

The next two theorems represent a further progress towards conjectures 1 and 2 although *no new applications* are possible in the present state of knowledge. These two theorems form the subject matter of the paper $[BR]_9$.

Theorem 5. *Let* $0 \leq \varepsilon < 1$, $C \geq 1$, $D \geq 1$, $E = \frac{1}{1-\varepsilon}$, $a_1 = 1 = \lambda_1$, $\frac{1}{C} \leq \lambda_{n+1} - \lambda_n \leq C$ *(for* $n = 1, 2, 3, \cdots$*) and for* $n \geq 2$ *(instead of* $|a_n| \leq (nH)^A$*)*

$$|a_n| \leq \operatorname{Exp}\{(DH^{\varepsilon} - 100C - 1)\log \lambda_n\}$$

where $H \geq 10$. *Let* $F(s) = \sum_{n=1}^{\infty}(a_n \lambda_n^{-s})$ *(convergent absolutely in* $\sigma \geq DH^{\varepsilon}$*) admit an analytic continuation in* $(\sigma \geq 0, 0 \leq t \leq H)$. *Assume that there exist* T_1, T_2 *with* $0 \leq T_1 \leq \frac{1}{8}H$, $\frac{7}{8}H \leq T_2 \leq H$, *such that, for some* $K \geq 30$,

$$|F(\sigma + iT_1)| + |F(\sigma + iT_2)| \leq K$$

holds uniformly in $\sigma \geq 0$. *Let finally*

$$H \geq \max\{100D \log\log K)^E, 100D(100DE)^{3E}\}. \tag{27}$$

Then

$$200 \int_0^H |F(it)|\, dt \geq H. \tag{28}$$

Theorem 6. *Let* $0 \leq \varepsilon < 1$, $C \geq 1$, $D \geq 2560C^2$, $E = \frac{1}{1-\varepsilon}$. *Let* $\{a_n\}$ *and* $\{\lambda_n\}$ *be as in Theorem 5,*

$$H \geq \max\{(256\ D\ \log\log K)^E, (24000\ C^6 DE)^{3E}\}. \tag{29}$$

Suppose $F(s)$ *has the properties stated in Theorem 5 with* K *defined exactly as in Theorem 5. Then, we have,*

$$\frac{10^8}{H} \int_0^H |F(it)|^2\, dt \geq \sum_{n \leq M_1} |a_n|^2 \tag{30}$$

where $M_1 = [(8000C^6 D)^{-1} H^{1-\varepsilon}]$.

§ 7. **Applications of Theorems 1 to 4 of §6.** Theorems 1 to 4 have a lot of applications. We mention only a few.

Theorem 7. *For all integers* $k \geq 1$ *and for all* H *satisfying* $C(k)\log\log T \leq H \leq T$, *we have,*

$$\frac{1}{H} \int_T^{T+H} \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2k} dt \geq C_k' (\log H)^{k^2} \left(1 + O\left(\frac{\log\log T}{H} + \frac{1}{\log H}\right)\right) \tag{31}$$

where $C(k)(> 0)$ *depends only on* k *and*

$$C_k' = (\Gamma(k^2 + 1))^{-1} \prod_p \left\{(1 - p^{-1})^{k^2} \sum_{m=0}^{\infty} \left|\frac{\Gamma(k+m)}{m!\,\Gamma(k)}\right|^2 p^{-m}\right\}.$$

Proof. In Theorem 2 take $F(s) = (\zeta(\frac{1}{2} + s + iT))^k$. Theorem 2 shows that the LHS of (31) is

$$\geq \sum_{n \leq \alpha H} \left(1 + O\left(\frac{\log\log T}{H} + \frac{1}{\log H}\right)\right) \frac{|d_k(n)|^2}{n}. \tag{32}$$

Using the well-known result that $\sum_{n \leq x} (|d_k(n)|^2 n^{-1}) = C_k'(\log x)^{k^2} \left(1 + O\left(\frac{1}{\log x}\right)\right)$ we obtain Theorem 7.

Remark 1. If $C(k, \varepsilon) \leq H \leq C(k) \log\log T$ the only result known is

$$\int_{|t-t_0| \leq C(k,\varepsilon)} \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2k} dt > t_0^{-\varepsilon}.$$

Plainly we can make ε a function of t_0 (and k) which tends to zero as $t_0 \to \infty$ for fixed k. For this and other results see $[\mathrm{BR}]_{10}$.

Remark 2. The result

$$\frac{1}{H} \int_T^{T+H} \left|\frac{d^\ell}{dt^\ell}\left(\zeta\left(\frac{1}{2} + it\right)\right)^k\right| dt \gg (\log H)^{\frac{1}{4}k^2 + \ell}$$

was proved for positive integral k in $[\mathrm{R}]_{10}$. (In $[\mathrm{R}]_9$ a weaker result was proved; but it dealt with positive real k). The result

$$\frac{1}{H} \int_T^{T+H} \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2k} dt \gg (\log H)^{k^2}$$

was proved for all positive rational constants k in $[\mathrm{R}]_{12}$ by using an idea of D.R. Heath-Brown [H]. Later this was extended in $[\mathrm{R}]_{13}$ for positive irrational constants k but with the lower bound $\gg \left(\frac{\log H}{\log\log H}\right)^{k^2}$. In $[\mathrm{R}]_{14}$ this was sharpened (the result involved the s.c.f. expansion of k). For example as a special case of a general result it was shown that

$$\frac{1}{H} \int_T^{T+H} \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2\sqrt{2}} dt \gg (\log H)^2 (\log\log H)^{-1}.$$

The general result contains as a special case the following result. Let k be any real number satisfying $a \leq k \leq b$ where $0 < a \leq b < \infty$. It is easy to prove that there exist integers p, q with $1 \leq q \leq 10 \log\log H$ such that $|k - \frac{p}{q}| \leq (\log\log H)^{-1}$. For any such q we have for $C \log\log T \leq H \leq T$,

$$\frac{1}{H} \int_T^{T+H} \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2k} dt > D\left(\frac{\log H}{q}\right)^{k^2}$$

where C and D are certain positive constants depending only on a and b. When the s.c.f. expansion of k has bounded partial quotients, q can always

be chosen to lie between two constant multiples of $(\log\log H)^{\frac{1}{2}}$. This leads to the special case mentioned above. All the results mentioned in this remark are subject to $T \geq H \gg \log\log T$. See the final remark at the end of the present paper.

Remark 3. Results like

$$\frac{1}{H}\int_T^{T+H}\left|\zeta^{(\ell)}\left(\frac{1}{2}+it\right)\right|dt \ll (\log T)^{\frac{1}{4}+\ell}$$

proved in $[\mathrm{R}]_{11}$ with $H = T^{\frac{1}{2}+\varepsilon}$ perhaps have some relavance here. It was also proved in $[\mathrm{R}]_{11}$ that the same upper bound holds with $H = T^{\frac{1}{4}+\varepsilon}$ if we assume Riemann hypothesis.

Theorem 8. *For C_0 $\log\log T \leq H \leq T$, we have,*

$$\max_{T\leq t\leq T+H}\left|\zeta\left(\frac{1}{2}+it\right)\right| > \mathrm{Exp}\left(\frac{3}{4}\sqrt{\frac{\log H}{\log\log H}}\right), \tag{33}$$

where C_0 is an effective positive constant.

Remark. Factors like $(\log H)^{-1000}$ in place of $\frac{1}{2}$ in (34) below are enough for application to prove Theorem 8. Such results were already available in $[\mathrm{R}]_1, [\mathrm{R}]_7$. In fact we mentioned Theorem 8 in $[\mathrm{R}]_7$. All that was needed was the study of $(\mathrm{RHS})^{\frac{1}{2k}}$ as a function of k in $1 \leq k \leq \log H$ which was done in [B] of course by an ingenious development of $[\mathrm{BR}]_1$. In $[\mathrm{BR}]_1$ a smaller constant than $\frac{3}{4}$ was obtained.

Proof. Put $F(s) = (\zeta(\frac{1}{2}+iT+s))^k$ where $k \geq 1$ is an integer. Then $|a_n| \leq n^2\sum_{m=1}^{\infty}(|a_m|\, m^{-2}) \leq n^2(\zeta(2))^k \leq (nH)^{10}$ if $k \leq \log H$. Note that in $(\sigma \geq 0,\ 0 \leq t \leq H)$ we have $|F(s)| \leq T^{2k}$ so that we can take $K = T^{3k}$. We can take $A = 2$. Notice that for $k \leq \log H$ we have $\log\log\ K_1 \leq 1000(\log\log H + \log\log T)$. This proves that

$$\frac{1}{H}\int_T^{T+H}\left|\zeta\left(\frac{1}{2}+it\right)\right|^{2k}dt \geq \frac{1}{2}\sum_{n\leq\alpha H}(d_k(n))^2 n^{-1} \tag{34}$$

provided $1 \leq k \leq \log H$. Here an asymptotic formula was obtained in [B] for the quantity $\max(\log(\mathrm{RHS})^{\frac{1}{2k}})$ the maximum being taken over $1 \leq k \leq \log H$. In fact the quantity in question is asymptotic to $C_3(\log\ H)^{\frac{1}{2}}(\log\log H)^{-\frac{1}{2}}$ where $C_3 = 0.75\cdots > \frac{3}{4}$. This proves Theorem 8.

Theorem 9. *Let $\frac{1}{2} < \sigma < 1$ and C_0 $\log\log T \leq H \leq T$. Then*

$$\max_{T\leq t\leq T+H}|\zeta(\sigma+it)| > \mathrm{Exp}(C_\sigma(\log H)^{1-\sigma}(\log\log H)^{-1}). \tag{35}$$

Remark. Better inequalities, when we take the maximum over $1 \leq t \leq T$ in Theorem 9 are due to H.L. Montgomery (see [M]) who proved in this case that the maximum $> \mathrm{Exp}\left(\frac{1}{20}\left(\sigma - \frac{1}{2}\right)^{\frac{1}{2}} (\log\ T)^{1-\sigma}(\log\log T)^{-\sigma}\right)$. In [RS] this was improved to $\mathrm{Exp}(C_\sigma(\log T)^{1-\sigma}(\log\log\ T)^{-\sigma})$ where $C_\sigma = C'L^{1-\sigma}(1-\sigma)^{-1}$, C' being a positive numerical constant and $L = \sigma - \frac{1}{2}$ or 1 according as we do not or do assume Riemann hypothesis. The method was a sharpening of the arguments of [M].

Proof. The proof is similar to that of Theorem 8. The study of

$$\max_{1\leq k\leq \log H} \log\left\{\frac{1}{2}\sum_{n\leq \alpha H}((d_k(n))^2 n^{-2\sigma})\right\}^{\frac{1}{2k}}$$

is much simpler. We find that this is $\gg (\log\ H)^{1-\sigma}(\log\log H)^{-1}$, by taking $n_0 = 2.3\cdots p_m \leq \alpha H$ as large possible and ignoring terms with $n \neq n_0$.

Remark. A theorem analogous to Theorems 8 and 9 for $\sigma = 1$ can be proved but we will not state it here. As a corollary to Theorem 4 we prove Theorem 10 which is a much more powerful theorem.

Theorem 10. *Let $z = e^{i\theta} = C + iS$ (C not to be confused with a constant). Put*

$$f(H) = \min_{T\geq 1}\ \max_{T\leq t\leq T+H} |(\zeta(1+it))^z|, \tag{36}$$

and $\lambda(\theta) = \prod_p \lambda_p(\theta)$, where

$$\lambda_p(\theta) = \left(1 - \frac{1}{p}\right)\left(\sqrt{1 - \frac{S^2}{p^2}} - \frac{C}{p}\right)^{-C} \mathrm{Exp}\left(S\ \mathrm{Sin}^{-1}\ \frac{S}{p}\right). \tag{37}$$

Then (for all $H \geq H_0$, a fixed numerical constant), we have,

$$|f(H)e^{-\gamma}(\lambda(\theta))^{-1} - \log\log H| \leq \log\log\log H + O(1). \tag{38}$$

Remark. We give a rough sketch of the proof. For details see $[\mathrm{R}]_2$. The idea in (a) below can be traced to $[\mathrm{BR}]_1$.

Proof. (a) *Lower bound for $f(H)$.* Put $F(s) = (\zeta(1 + iT + s))^z$. The a_n's are multiplicative. To obtain a lower bound for

$$\max_{1\leq k\leq \log H}\left(\frac{1}{2}\sum_{n\leq x}\left|\frac{a_n}{n}\right|^2\right)^{\frac{1}{2k}}$$

write $a_n = a(n)$. We choose $p_1, p_2, \cdots, p_\ell$ (the first ℓ primes) and exponents $b_1, b_2, \cdots, b_\ell$ such that

(i) $p_1^{b_1} \cdots p_\ell^{b_\ell} \leq x$

and where for each fixed p_j, b_j are so chosen that

(ii) $|a(p_j^{b_j})p_j^{-b_j}|^2$

is maximum. This gives the lower bound for $f(H)e^{-\gamma}(\lambda(\theta))^{-1}$. (For details see [BRS]).

(b) *Upper bound for* $f(H)$. For this we use the following Lemma from $[\mathrm{BR}]_2$ which is quoted in $[\mathrm{R}]_2$ (page 29) and we quote it here.

Lemma. *Let* $T = \mathrm{Exp}((\log H)^2)$ *where* H *exceeds a certain positive constant. Then there exists a sub-interval* I *of* $[T, 2T]$ *of length* $H + 2(\log H)^{10}$ *such that the rectangle* $(\sigma \geq \frac{3}{4}, t \in I)$ *does not contain any zero of* $\zeta(s)$ *and moreover*

$$\max |\log \zeta(\sigma + it)| = O((\log H)^{\frac{1}{4}}(\log \log H)^{-\frac{3}{4}})$$

the maximum being taken over the rectangle referred to (and $\log \zeta(s)$ *is the branch for which* $\log \zeta(s) = \log \frac{\pi^2}{6}$ *is real).*

From this lemma the upper bound for $f(H)$ follows with some further arguments (for details see $[\mathrm{R}]_2$).

(a) and (b) complete the sketch of the proof of Theorem 10.

Theorem 11. *Let* $\zeta(s, a) = \sum_{n=0}^{\infty}(n + a)^{-s}$ *where* $0 < a \leq 1$ *be the Hurwitz zeta-function in* $\sigma > 1$. *Consider its analytic continuation in* $\sigma \geq 1$. *Then, we have,*

$$\min_{T \geq 1} \int_T^{T+H} |\zeta(1 + it, a)|\, dt \geq \frac{1}{a}H + O(H). \tag{39}$$

Proof. Follows from Theorem 3 of § 6. For reference see $[\mathrm{R}]_8$.

§ 8. Consequences of Conjectures 1 and 2 without Riemann Hypothesis.

Theorem 12. *We have, for* $C_0 \leq H \leq T$,

$$\frac{1}{H}\int_T^{T+H} |\zeta(\sigma + it)|\, dt \geq C_4, \tag{40}$$

where C_4 *is a positive numerical constant.*

Proof. We approximate to $\zeta(s)$ by $\sum_{n=1}^{\infty}\left(n^{-s}\,\mathrm{Exp}\left(-\frac{n}{X}\right)\right)$, where X is large and apply Conjecture 1. This gives Theorem 12.

Theorem 13. *In Theorems* 7, 8 *and* 9 *the condition on* H *can be relaxed to* $C(k) \leq H \leq T, C_0 \leq H \leq T$ *and* $C_0 \leq H \leq T$ *respectively. The results are still valid.*

Proof. We approximate to $(\zeta(s))^k$ by $\sum_{n=1}^{\infty}(d_k(n)n^{-s}\,\mathrm{Exp}(-\frac{n}{X}))$ where X (a

function of T) is chosen to be large enough. The rest of the proof is the same. We have simply to use Conjecture 2.

§ 9. Further Conjectures which follow from Conjectures 1,2 and Riemann Hypothesis.

Theorem 14. *We have, with* $z = e^{i\theta}$,

$$\max_{T\le t\le T+H}\left|\left(\zeta\left(\frac{1}{2}+it\right)\right)^{z}\right| \ge \operatorname{Exp}\left(\frac{3}{4}\sqrt{\frac{\log H}{\log\log H}}\right) \tag{41}$$

provided $C_0 \le H \le T$. *Also under the same conditions*

$$\max_{T\le t\le T+H}|(\zeta(\sigma+it))^{z}| \ge \operatorname{Exp}\left(C_\sigma\frac{(\log H)^{1-\sigma}}{\log\log H}\right) \tag{42}$$

where σ *is fixed subject to* $\frac{1}{2} < \sigma < 1$.

Remark 1. We interpret $(\zeta(s))^z$ as its analytic continuation from $\sigma \ge 2$ along lines parallel to the real axis which are free from zeros of $\zeta(s)$.

Remark 2. For some unconditional (weaker) results in the direction of Theorem 14 see [BRS], (to appear).

Proof. Put $F(s) = (\zeta(\frac{1}{2}+iT+s))^{zk}$ and proceed as in the proof of Theorem 8. The investigations of [B] necessary for (41) are obviously valid.

Theorem 15. *Theorem 7 is valid for complex constants* k *with* $|(\zeta(\frac{1}{2}+it))^k|^2$ *in place of* $|\zeta(\frac{1}{2}+it)|^{2k}$, *provided in (31) and also in the definition of* C_k' *we replace* k^2 *by* $|k^2|$ *wherever* k^2 *occurs. Moreover the condition on* H *can be relaxed to* $C(k) \le H \le T$.

Final remark. Most of the theorems published earlier depended on the condition $(\log T)^\varepsilon \le H \le T$, (see [I] in particular pages 231-249). But it is a routine matter to change the kernel $\operatorname{Exp}(z^{4\alpha+2})$ to $\operatorname{Exp}((\operatorname{Sin} z)^2)$ and obtain the same results in the wider range $C_0 \log\log T \le H \le T$.

Postscript. The previous history of Theorem 7 is due to J.B. CONREY AND A. GHOSH who proved that if $k > 0$ is real then

$$\frac{1}{T}\int_0^T \left|\zeta(\frac{1}{2}+it)\right|^{2k} dt \ge (C_k' + o(1))(\log T)^{k^2}$$

provided we assume Riemann hypothesis. (See p.181 of $[T]_2$ or [CG]. It should be mentioned that $C_1' = 1$ and $C_2' = (4\pi^2)^{-1}$ and that when $k = 2$, LHS $\sim 2C_2'(\log T)^4$.

Regarding the "further question" figuring after Conjecture 3, R. BALASUBRAMANIAN and K. RAMACHANDRA have made considerable progress

after their paper $[BR]_7$. We can reach $\beta(T) = \frac{c \log\log T}{\log T}$, $\beta(T) = \frac{c \log\log\log T}{\log T}$ and even $\beta(T) = \frac{c}{\log T}$ without assuming an Euler product hypothesis. See the forthcoming papers $[BR]_{11}, [BR]_{12}$ and $[R]_{15}$.

Actually the paper $[BR]_{12}$ deals also with the zeros of a class of generalised Dirichlet series in $\sigma \geq \frac{1}{2} + \delta$ where $\delta(> 0)$ is a constant. The proof of such results makes use of the result of the $[BR]_{13}$.

Continuing the work $[BR]_{12}$, myself and R. BALASUBRAMANIAN have recently succeeded in proving the following two theorems.

Theorem 16. *Let μ be any constant satisfying $0 < \mu < 1$, and let a be any complex constant. Then there exists a constant $\delta > 0$ such that $\zeta'(s) - a$ has $\gg T^{\mu}$ well-spaced zeros in $(\sigma \geq \frac{1}{2} + \delta,\ T \leq t \leq T + T^{\mu})$ for all T exceeding a certain positive constant T_0.*

Remark. The term "well-spaced set of points" means, as usual, that the differences taken positively, between the ordinates of any two points is bounded below by a positive constant.

Theorem 17. *Let δ and μ be any two positive constant satisfying $0 < \delta < 1$ and $0 < \mu < 1$. Let a be any non-zero complex constant. Then $\zeta(s) - a$ has $\gg T^{\mu}$ well-spaced zeros in $(\sigma \geq 1 - \delta,\ T \leq t \leq T + T^{\mu})$ for all T exceeding a certain positive constant T_0.*

Remark. The results in theorems 16 and 17 have actually been proved to hold good for more general Dirichlet series in place of $\zeta'(s) - a$ and $\zeta(s) - a$. The references to these works are respectively $[BR]_{14}$ and $[BR]_{15}$.

Acknowledgements. This paper is the text of an invited one hour talk at Journées Arithmétiques held at Geneva, Switzerland, during 9-13 September 1991. I am very much thankful to the organizers of this conference and in particular to Professor Daniel Coray and Dr. Y-F.S. Pétermann for their kind hospitality and finally to Professor Alan Baker, F.R.S., for presiding over my talk.

SUPPLEMENTARY REFERENCES

[CG] J.B. CONREY and A. GHOSH, *On the mean values of the zeta-function*, Mathematika, 31 (1984), 159-161.

[BR]$_{11}$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series - X* (to appear).

[BR]$_{12}$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series - XI* (to appear).

[BR]$_{13}$ R. BALASUBRAMANIAN and K.RAMACHANDRA, *Proof of some conjectures on the mean-value of Titchmarsh series*-III, (to appear).

[BR]$_{14}$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of* $\zeta'(s) - a$, (to appear).

[BR]$_{15}$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of* $\zeta(s) - a$, (to appear).

[R]$_{15}$ K. RAMACHANDRA, *Application of a Theorem of Montgomery and Vaughan to the zeta-function - II* (to appear).

REFERENCES

[B] R. BALASUBRAMANIAN, *On the frequency of Titchmarsh's phenomenon for* $\zeta(s)$-IV, Hardy-Ramanujan J., vol. 9 (1986), 1-10.

[BR]$_1$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the frequency of Titchmarsh's phenomenon for* $\zeta(s)$-III, Proc. Indian Acad. Sci., Section A, 86 (1977), 341-351.

[BR]$_2$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the frequency of Titchmarsh's phenomenon for* $\zeta(s)$-V, Arkiv för Mathematik, 26 (1) (1988), 13-20.

[BR]$_3$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-III, J. Indian Math. Soc., 41 (1977), 301-315.

[BR]$_4$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-IV, J. Indian Math. Soc., 42 (1978), 135-142.

[BR]$_5$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-VI, Arkiv för Mathematik, 19 (2) (1981), 239-250.

[BR]$_6$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-VIII, Hardy-Ramanujan J., vol. 14 (1991), 21-33.

[BR]$_7$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-IX, Hardy-Ramanujan J., vol. 14 (1991), 34-43.

[BR]$_8$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *Proof of some conjectures on the mean-value of Titchmarsh series*-I, Hardy-Ramanujan J., vol. 13 (1990), 1-20.

[BR]$_9$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *Proof of some conjectures on the mean-value of Titchmarsh series*-II, Hardy-Ramanujan J., vol. 14 (1991), 1-20.

[BR]$_{10}$ R. BALASUBRAMANIAN and K. RAMACHANDRA, *Some local-convexity theorems for the zeta-function-like analytic functions,* Hardy-Ramanujan J., 11 (1988), 1-12.

[BRS] R. BALASUBRAMANIAN, K. RAMACHANDRA and A. SANKARANARAYANAN, *On the frequency of Titchmarsh'sphenomenon for* $\zeta(s)$-VIII, Proc. Indian Acad. Sci. (Math. Sci.), 102 (1992), 1-12.

[H] D.R. HEATH-BROWN, *Fractional moments of the Riemann zeta-function,* J. London Math. Soc., (2) 24 (1981), 65-78.

[I] A. IVIĆ, The Riemann zeta-function, John Wiley and Sons, New York, (1985).

[K] J.-P. KAHANE, *The last problem of Harold Bohr,* J. Austral. Math. Soc., (Series A), 47 (1989), 133-152.

[M] H.L. MONTGOMERY, *Extreme values of the Riemann zeta function,* Comment. Math. Helvitici 52 (1977), 511-518.

[R]$_1$ K. RAMACHANDRA, *On the frequency of Titchmarsh's phenomenon for $\zeta(s)$*-I, J. London Math. Soc., 8 (1974), 683-690.

[R]$_2$ K. RAMACHANDRA, *On the frequency of Titchmarsh's phenomenon for $\zeta(s)$*-IX, Hardy-Ramanujan J., vol. 13 (1990), 28-33.

[R]$_3$ K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-I, J. Reine u. Angew. Math., 273 (1975), 31-40.

[R]$_4$ K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-II, J. Reine u. Angew. Math., 289 (1977), 174-180.

[R]$_5$ K. RAMACHANDRA, *On the zeros of a class of generalised Dirichlet series*-V, J. Reine u. Angew. Math., 303/304 (1978), 295-313.

[R]$_6$ K.RAMACHANDRA, *on the zeros of a clsss of generalised Dirichlet series* - VII, Annales Acad. Sci. Fenn., Ser. A.I. Math. 16 (1991), 391-397.

[R]$_7$ K. RAMACHANDRA, *Progress towards a conjecture on the meanvalue of Titchmarsh series*-I (Proceedings of the Durham Conference July-August (1979)) Recent progress in Analytic number theory, vol. 1 ed. by H. Halberstam and C. Hooley, F.R.S., Academic Press, London, New York, Toronto, Sydney, San Franscisco, (1981), 303-318.

[R]$_8$ K. RAMACHANDRA, *Proof of some conjectures on the mean-value of Titchmarsh series with applications to Titchmarsh's phenomenon,* Hardy-Ramanujan J., vol. 13 (1990), 21-27.

[R]$_9$ K. RAMACHANDRA, *Some remarks on the mean-value of the Riemann zeta-function and other Dirichlet series*-I, Hardy-Ramanujan J., vol. 1 (1978), 1-15.

[R]$_{10}$ K. RAMACHANDRA, *Some remarks on the mean-value of the Riemann zeta-function and other Dirichlet series*-II, Hardy-Ramanujan J., vol. 3 (1980), 1-24.

[R]$_{11}$ K. RAMACHANDRA, *Some remarks on the mean-value of the Riemann zeta-function and other Dirichlet series*-III, Annales Acad. Sci. Fenn. (Ser. AI) Math., 5 (1980), 145-158.

[R]$_{12}$ K. RAMACHANDRA, *Mean-value of the Riemann zeta-function and other remarks*-I, Colloq. Math. Soc. Janós Bolyai, 34, Topics in classical number theory, BUDAPEST, (HUNGARY) (1981), 1317-1347.

[R]$_{13}$ K. RAMACHANDRA, *Mean-value of the Riemann zeta-function and other remarks*-II, Trudy, Mat. Inst. Steklov., 163 (1984), 200-204.

[R]$_{14}$ K. RAMACHANDRA, *Mean-value of the Riemann zeta-function and other remarks*-III, Hardy-Ramanujan J., vol. 6 (1983), 1-21.

[RS] K. RAMACHANDRA and A. SANKARANARAYANAN, *Note on a paper by H,L. Montgomery*, Publ. de L' Institut Math., Novelle Ser. tome 50 (64), Beograd (1991), 51-59.

[T]$_1$ E.C. TITCHMARSH, The Theory of functions, Oxford University Press (1939).

[T]$_2$ E.C. TITCHMARSH, The theory of the Riemann zeta-function, Second edition, (Revised by D.R. Heath-Brown), Clarendon Press, Oxford (1986).

K. Ramachandra
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005, India

Astérisque

A. S. RAPINCHUK

Congruence subgroup problem for algebraic groups: old and new

Astérisque, tome 209 (1992), p. 73-84

<http://www.numdam.org/item?id=AST_1992__209__73_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

CONGRUENCE SUBGROUP PROBLEM FOR ALGEBRAIC GROUPS: OLD AND NEW

A. S. RAPINCHUK*

Let $G \subset \mathrm{GL}_n$ be an algebraic group defined over an algebraic number field K. Let S be a finite subset of the set V^K of all valuations of K, containing the set V_∞^K of archimedean valuations. Denote by $\mathcal{O}(S)$ the ring of S-integers in K and by $G_{\mathcal{O}(S)}$ the group of S-units in G. To any nonzero ideal $\mathfrak{a} \subset \mathcal{O}(S)$ there corresponds the congruence subgroup

$$G_{\mathcal{O}(S)}(\mathfrak{a}) = \{g \in G_{\mathcal{O}(S)} \mid g \equiv E_n \pmod{\mathfrak{a}}\},$$

which is a normal subgroup of finite index in $G_{\mathcal{O}(S)}$. The initial statement of the Congruence Subgroup Problem was:

(1) Does any normal subgroup of finite index in $G_{\mathcal{O}(S)}$ contain a suitable congruence subgroup $G_{\mathcal{O}(S)}(\mathfrak{a})$?

In fact, it was found by F. Klein as far back as 1880 that for the group $\mathrm{SL}_2(\mathbb{Z})$ the answer to question (1) is "no". So a more accurate statement of the problem should be: for which G and S does (1) have an affirmative answer? However, till the mid sixties there were no nontrivial examples of groups for which this is actually true. Only in 1965 did Bass-Lazard-Serre [1] and Mennicke [10] give a positive solution to the congruence subgroup problem for $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. In the course of further investigations, it appeared convenient

* The author wishes to thank the Department of Mathematics in Geneva for editing and retyping the manuscript.

to introduce the object measuring deviation from the positive solution of (1) and then to view the congruence subgroup problem as the problem of its computation. This object (called the congruence kernel) was defined by Serre [27] as follows.

Let us introduce on the group G_K of K-rational points two Hausdorff topologies, τ_a and τ_c, called S-arithmetic topology and S-congruence topology, respectively. The complete system of neighbourhoods of unity for τ_a (resp., τ_c) consists of all normal subgroups of finite index (resp., all congruence subgroups) in $G_{\mathcal{O}(S)}$. It is easy to show that these topologies satisfy all the properties that ensure the existence of the corresponding S-arithmetic and S-congruence completions $\widehat{G}$ and $\overline{G}$. Since τ_a is stronger than τ_c, the identity map

$$(G_K, \tau_a) \to (G_K, \tau_c)$$

is continuous. Therefore it can be extended to a continuous homomorphism $\pi\colon \widehat{G} \to \overline{G}$ of the completions. By definition, $C^S(G) = \operatorname{Ker}\pi$ is the *congruence kernel.*

PROPOSITION 1. *The projection π is surjective and $C^S(G)$ is a profinite group. $C^S(G)$ is trivial if and only if the congruence subgroup problem in the form* (1) *has an affirmative solution for $G_{\mathcal{O}(S)}$.*

Thus, in general, the congruence kernel $C^S(G)$ measures deviation from a positive answer to the congruence subgroup problem. So, by the modern statement of the problem we mean the problem of determination of $C^S(G)$. It is well-known (see for example [23]) that this problem can be reduced to the main case of an (absolutely) simple, simply connected algebraic group G. Here we shall be exclusively concerned with that case. As we have already remarked, the first positive result on the congruence subgroup problem for such groups is due to Bass-Lazard-Serre [1] and Mennicke [10], who studied the case of $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. Then Bass-Milnor-Serre [2] completed the investigation of SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$ over an arbitrary number field K, after obtaining a description of $C^S(G)$ in the following form:

$$C^S(G) = \begin{cases} 1 & \text{if } \exists\, v \in S \text{ such that } K_v \neq \mathbb{C} \\ E(K) & \text{otherwise,} \end{cases} \tag{2}$$

where $E(K)$ is the group of all roots of unity in K. By further developing the methods of [2], Matsumoto [9] extended (2) to all universal Chevalley groups different from SL_2 (the case of twisted Chevalley groups was considered by Deodhar [4]). In the case $G = \mathrm{SL}_2$, first Mennicke [11] gave a positive solution to the congruence subgroup problem for the group $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$, and then Serre

[27] studied the general situation and showed that, provided Card $S > 1$, the answer is of the form (2). On analysing the obtained results, Serre [27] formulated the following congruence subgroup conjecture, which gives sufficient conditions for $C^S(G)$ to be finite or infinite, in terms of the so-called S-rank:

$$\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G,$$

where $\operatorname{rang}_P G$ denotes the rank of the group G over the field P, i.e., the dimension of a maximal P-split subtorus in G.

CONJECTURE 1. *Let G be simple and simply connected. Then in case $\operatorname{rang}_S G \geq 2$ and G is K_v-isotropic for all $v \in S \setminus V_\infty^K$, the congruence kernel $C^S(G)$ should be finite. In case $\operatorname{rang}_S G = 1$, it should be infinite.*

The case of finite $C^S(G)$ is the most interesting and important for applications. In that case, we shall say that the group $\Gamma = G_{\mathcal{O}(S)}$ has the *congruence subgroup property* (*CSP*). In this paper we are going to describe the class of groups for which (*CSP*) is known to hold and outline some new methods of attacking the congruence subgroup problem, which, as we hope, will enable us to enlarge this class considerably.

Let us first describe the general scheme for calculating the congruence kernel $C = C^S(G)$. It follows from our definitions that C can be determined from the exact sequence:

$$1 \to C \to \widehat{G} \xrightarrow{\pi} \overline{G} \to 1 \tag{3}$$

Let us consider the initial segment of the Hochschild-Serre spectral sequence corresponding to (3):

$$H^1(\overline{G}) \xrightarrow{\varphi} H^1(\widehat{G}) \to H^1(C)^{\overline{G}} \xrightarrow{\psi} H^2(\overline{G}), \tag{4}$$

where $H^i(*)$ denotes the i-th continuous cohomology group with coefficients in the one-dimensional torus $\mathbb{R}/\mathbb{Z}$. The term $H^1(C)^{\overline{G}}$ in (4) is connected with C as follows:

$$H^1(C)^{\overline{G}} = \operatorname{Hom}(C/[C, \hat{G}]\,, \mathbb{R}/\mathbb{Z}).$$

So one can reconstruct C from $H^1(C)^{\overline{G}}$ only under the assumption that C is central, i.e., lies in the centre of $\widehat{G}$. Indeed, in this case $H^1(C)^{\overline{G}}$ coincides with the Pontryagin dual C^* of C. Suppose now that C is central. Then we have the following exact sequence:

$$1 \to \operatorname{Coker} \varphi \to C^* \to \operatorname{Im} \psi \to 1.$$

Ignoring the trivial case $\operatorname{rang}_S G = 0$, in which $G_{\mathcal{O}(S)}$ is finite and consequently $C^S(G) = 1$, we immediately obtain from the strong approximation theorem that the group $\overline{G}$ can be identified with the group $G_{A(S)}$ of S-adeles. Then, using the fact that the sequence (3) splits over the group G_K and is the "universal" sequence with this property, one can show that $\operatorname{Im}\psi$ coincides with the so-called *metaplectic kernel*

$$M(G,S) = \operatorname{Ker}\big(H^2(G_{A(S)}) \to H^2(G_K)\big),$$

where G_K is endowed with the discrete topology. On the other hand

$$\operatorname{Coker}\varphi \cong \overline{[G_K, G_K]}/[G_K, G_K],$$

where the bar denotes closure in G_K for the S-arithmetic topology. Taking into account that $M(G,S)$ is always finite (see [17]) and that $[G_K, G_K]$ has finite index in G_K (see [8]), we arrive at the following

PROPOSITION 2. *If C is central then it is finite. If, moreover,* $\operatorname{Coker}\varphi = 1$ *then $C^* \simeq M(G,S)$.*

In fact, at present it is known that $\operatorname{Coker}\varphi$ is indeed trivial for most cases. This depends on the validity for G_K of the following conjecture, which describes the normal structure. (This conjecture was formulated by Platonov [13] in the form of a local-to-global principle for projective simplicity and then by Margulis [8] in the final form).

CONJECTURE 2. *Let $V_f^K = V^K \setminus V_\infty^K$ be the set of nonarchimedean valuations, and let $T = \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic}\}$. Then for any noncentral, normal subgroup $N \subset G_K$ there is an open normal subgroup $W \subset G_T = \prod_{v\in T} G_{K_v}$ such that $N = W \cap G_K$. In other words, any noncentral normal subgroup is open (equivalently, closed) in the T-adic topology.*

If Conjecture 2 is true for G_K then we say that G_K has a *standard description of normal subgroups.* In the situation of Conjecture 1 we have $S \cap T = \varnothing$, and so the triviality of $\operatorname{Coker}\varphi$ is equivalent to saying that Conjecture 2 holds for $N = [G_K, G_K]$. But the latter statement is actually true for all groups, with the possible exception of some anisotropic forms of types ${}^2A_n$, ${}^{3,6}D_4$ and E_6 (see [14]). Thus, in most cases, the calculation of C (provided it is central) reduces to that of $M(G,S)$.

The first computations of the metaplectic kernel had been carried out by Moore [12] and Matsumoto [9]. They obtained the description of $M(G,S)$

for Chevalley groups in the form (2). The case of quasi-split groups was considered by Deodhar [4]. The final result for isotropic groups, due to Prasad-Raghunathan [17], is of the form:

$$M(G,S) = \begin{cases} 1 & \text{if } S \neq V_\infty^K \\ \subset E(K) & \text{otherwise,} \end{cases} \tag{5}$$

where $E(K)$ is the group of all roots of unity in K. The author [20] calculated $M(G,S)$ for a large series of anisotropic groups. Here the description of $M(G,S)$ is of the same nature as (5), but its precise form may differ from (5) by a certain group of exponent 2. The main part of these results is the computation of $M(G,S)$ for the groups of type $\mathrm{SL}_1(D)$. As in the classical case of the group SL_n, we show that any element $x \in M(G,S)$ gives rise to a certain reciprocity law, i.e., to a relation of the form

$$\prod_{w \in V^L} (a,b)_w^{n_w} = 1,$$

where L is a certain maximal subfield in D and $(*,*)_w$ is the norm residue symbol of degree $\mu_w = [E(L_w)]$. But the difference from the classical situation is that this reciprocity law must hold not for all $a, b \in L^*$, but for all a, b of some specific form. Then we prove a certain version of the uniqueness theorem for reciprocity laws of this kind (similar results were obtained by Prasad [16]) and derive from it the desired description of the metaplectic kernel. That is all that is known about the problem of the precise determination of C under the assumption that it is central. Now we shall move on to the methods of proving the centrality of C. This is equivalent (as explained above) to its being finite.

That the congruence kernel is central for the groups SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, was established by Bass-Milnor-Serre in [2]. The case of split and quasi-split groups was considered by Matsumoto [9] and Deodhar [4] respectively. For $G = \mathrm{SL}_2$, Serre [27] proved that $C^S(G)$ is central in the case where $\mathrm{Card}\, S > 1$. Raghunathan [18], [19] completed the discussion of K-isotropic groups by proving that they satisfy Conjecture 1, i.e. in fact that $C^S(G)$ is central for the case $\mathrm{rang}_S G \geq 2$. The argument in all these papers was based on some manipulations with unipotent elements in G_K, and so no version of it can be applied to anisotropic groups. Until recently, the only result which allowed also anisotropic groups was Kneser's theorem [6] for spinor groups of quadratic forms. But then Rapinchuk [21], [22] and Tomanov [29] extended this theorem to all groups having a nice geometric realization.

THEOREM 1. *Let G be a simple, simply connected K-group of one of the following types B_n $(n \geq 2)$, C_n $(n \geq 2)$, D_n $(n \geq 5)$, G_2 or the special unitary groups, $\mathrm{SU}_m(f)$ $(m \geq 4)$, of a nondegenerate hermitian form f over some quadratic extension L/K belonging to the type ${}^2A_{m-1}$. Assume that $\mathrm{rang}_S G \geq 2$ and, moreover, if G is of type C_3 then either S contains a nonarchimedean valuation or such an archimedean valuation v that $\mathrm{rang}_{K_v} G \geq 2$. Then $C^S(G)$ is central.*

Later Tomanov [30] included into the list of groups in Theorem 1 also the unitary groups over the quaternions.

The proof of Theorem 1 is actually independent of the type of the group. It is based on the following two statements.

PROPOSITION 3. *$C^S(G)$ is central if the group G_K is projectively simple and if there is a K-defined subgroup $H \subset G$ with the following properties:*

1) *the natural map $C^S(H) \to C^S(G)$ is surjective;*
2) *for some nontrivial K-defined automorphism $\sigma \in \mathrm{Aut}\, G$, the restriction $\sigma|_H$ is trivial.*

PROPOSITION 4. *Let G act K-rationally on some affine K-variety X, and let $x \in X_K$. Assume that, for any normal subgroup $N \subset G_{\mathcal{O}(S)}$ of finite index, the orbit Nx is open in $G_{\mathcal{O}(S)}x$ for the S-adelic topology (of the space $X_{A(S)}$). Then, if $G(x)$ denotes the stabilizer of the point x, the natural map $C^S(G(x)) \to C^S(G)$ is surjective.*

We apply these statements to the natural realizations of the groups in Theorem 1 as the automorphism groups of some quadratic, hermitian or skew-hermitian forms. In fact, this method is applicable in many other situations besides those described in Theorem 1. For example, it was shown in [23] how it can be used to establish the centrality of the congruence kernel for the group SL_n $(n \geq 3)$. On the other hand, it is inapplicable to the groups which have no nice geometric presentation, in particular to most exceptional groups. Here the solution of the congruence subgroup problem was obtained by Rapinchuk [22] through another approach, using the intrinsic structure of the group.

THEOREM 2. *Let G be a simple, simply connected K-anisotropic group of one of the following types: E_7, E_8, F_4. Assume that:*

1) *if G is of type E_7 or E_8 then $\mathrm{rang}_S G \geq 2$;*
2) *if G is of type F_4 then there is $v \in S$ such that $\mathrm{rang}_{K_v} G \geq 2$.*

Then $C^S(G)$ is central.

A crucial role in the proof of Theorem 2 is played by the fact that all groups of the enumerated types split over some quadratic extension L/K with a special local behaviour. This result is a consequence of the Hasse principle for the Galois cohomology of simply connected groups and the fact that the centres of these groups have order at most 2.

All these results confirm Serre's conjecture for most types of simple groups. However, there is a very important class of groups, viz. the groups of type $\mathrm{SL}_1(D)$ where D is a division algebra, for which these methods fail to work. Even for the case of a quaternion algebra D, until recently there was not a single example of a group of type $\mathrm{SL}_1(D)$ with property (*CSP*). But a few months ago it appeared that such an example can be obtained on the basis of a new approach to the congruence subgroup problem developed in Minsk.

This approach is based on the use of some abstract algebraic concepts. The first step in its foundation was a purely algebraic proof of centrality for the congruence kernel of the groups SL_n ($n \geq 3$) (in fact, for all Chevalley groups of rank ≥ 2) and of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ (see [26]). To be more precise, it was shown that the centrality of the congruence kernel for these groups follows directly from commutator relations. It seems plausible that this argument can be extended to all (or most) isotropic groups where commutator relations of the same type hold. On the other hand, it is inapplicable to groups for which no explicit presentation of a convenient form exists (or is known), i.e. to the most interesting case of anisotropic groups. It is clear that the algebraic approach here should be based not on the analysis of particular relations, but on the specification of some abstract properties of arithmetic groups which would imply the finiteness (or centrality) of the congruence kernel. At present, we know a few properties of this kind, the first of which being the property of bounded generation.

DEFINITION. We say that an abstract group Γ has the property of *bounded generation* (*BG*) if there are elements $\gamma_1, \ldots, \gamma_t \in \Gamma$ such that $\Gamma = \langle\gamma_1\rangle \ldots \langle\gamma_t\rangle$, where $\langle\gamma_i\rangle$ is the cyclic subgroup generated by γ_i.

This property is clearly of a combinatorial nature. However, the author failed to find any mention of it in the works on combinatorial group theory. It should be emphasized that this abstract definition was strongly motivated by a result of Carter and Keller [3], according to which any matrix in $\mathrm{SL}_n(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers in an algebraic number field and $n \geq 3$, is a product of a certain bounded number of elementary matrices. In fact, this paper of Carter and Keller was aimed at the solution of a problem from algebraic K-theory, viz. the question of the triviality of the SK_1-functor for so-

called non-standard models of the rings of integers. Their result quoted above is precisely equivalent to this triviality. However, the technique employed in that paper was borrowed from the works on the congruence subgroup problem (Mennicke symbols, etc.). The analysis of that paper, and also of some other facts, induced the author to formulate the following conjecture.

CONJECTURE 3. *Let G be a simple, simply connected algebraic group over an algebraic number field K, and let $S \subset V^K$ be a finite subset containing V_∞^K. Then for the group $\Gamma = G_{\mathcal{O}(S)}$ of S-integral points the properties (CSP) and (BG) are equivalent.*

Some further evidence in favour of this conjecture appeared when Tavgen' [28] established (BG) for arithmetic and S-arithmetic subgroups of all Chevalley groups of rank ≥ 2, both of normal and of most twisted types. (The (CSP) property for these groups was proved by Matsumoto [9] and Deodhar [4].) There are also some examples of the reverse character. For the groups $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers in an imaginary quadratic field, both properties (CSP) and (BG) fail to hold. In all these cases, (CSP) and (BG) are proved or disproved independently, and somehow it happens that they simultaneously hold or fail to hold. But the real question was whether there is some direct connection between these two properties in the general situation. The first result which established such a connection was the following theorem, proved by the author [24].

THEOREM 3. *Assume that the group G_K admits a standard description of normal subgroups. If $\Gamma = G_{\mathcal{O}(S)}$ has (BG) then the abelianized congruence kernel $C^{ab} = C/[C, C]$ is finite.*

Subsequently it turned out that the technique invented for the proof of Theorem 3 can be pushed further, so that, for S-arithmetic groups of bounded generation, property (CSP) can be proved in full (see Corollary 1 below). This fact was obtained as a consequence of some more general results (to be described a little later), obtained independently by Platonov-Rapinchuk [15] and A. Lubotzky. It is worth mentioning that this enables us to present new examples of S-arithmetic groups with (CSP). Namely, recently F. Grunewald found by computer some explicit examples of groups with (BG) among the groups of the form $G_{\mathbb{Z}(S)}$, where $G = \mathrm{SL}_1(D)$ for some quaternion algebra D over $\mathbb{Q}$ and $S = \{\infty, p\}$ (p prime). This gives the first examples of quaternionic groups with (CSP). Now I would like to formulate a conjecture, the proof of which would provide a proof of Serre's congruence subgroup conjecture.

CONJECTURE 4. *If G is simple and $\operatorname{rang}_S G \geq 2$ then $\Gamma = G_{\mathcal{O}(S)}$ has bounded generation.*

There is no doubt that groups with (BG) (and especially their profinite analogues) deserve some special treatment. They have interesting structural properties and, under additional assumptions, they satisfy an important property from representation theory – the property of finiteness of the representation type (see [25], [26]). However, at present it is not quite clear how to determine in general whether a particular group has bounded generation or not. For this reason we had undertaken a search of other abstract properties of arithmetic groups, which should also ensure (CSP) but be (or at least look) more constructive than (BG). Now, I am going to describe some results in this direction, which have been obtained by Platonov and Rapinchuk [15]. We shall need some new definitions, bearing not on the S-arithmetic group Γ itself but on its profinite completion $\widehat{\Gamma}$.

DEFINITION. Let Δ be a finitely generated profinite group.

1. Δ has *bounded generation as a profinite group* (property $(BG)_{pf}$) if there exist elements $\delta_1, \ldots, \delta_t \in \Delta$ such that $\Delta = \overline{\langle \delta_1 \rangle} \ldots \overline{\langle \delta_t \rangle}$, where $\overline{\langle \delta_i \rangle}$ denotes the closure of the cyclic subgroup generated by δ_i.
2. The *n-th Burnside factor* Δ_n of Δ is the factor group Δ/Δ^n modulo the closed subgroup Δ^n generated by n-th powers of all elements of Δ. (Note that, according to [31], Δ_n is finite for any n.)
3. Δ has *polynomial growth in the orders of its Burnside factors* (property $(PG)_{pf}$) if there are constants c and k such that $|\Delta_n| \leq cn^k$ for all n.
4. Δ has *property* $(PG)'_{pf}$ if, for any integer $n > 0$ and any prime q, there exist c and k such that $\left|\Delta_{nq^i}\right| \leq cq^{ki}$ for all $i > 0$.

It is easy to show that property (BG) for Γ implies $(BG)_{pf}$ for $\widehat{\Gamma}$. On the other hand, for arbitrary Δ we have

$$(BG)_{pf} \Longrightarrow (PG)_{pf} \Longrightarrow (PG)'_{pf}.$$

No other relations between these properties are known. So it would be interesting to find out whether properties $(BG)_{pf}$ and $(PG)_{pf}$ are equivalent or not. (Our results show that this is certainly true for the profinite completions of S-arithmetic groups; see Corollary 2 below. Moreover, as follows from [5] and [7], for a pro-p-group Δ each of the conditions $(BG)_{pf}$, $(PG)_{pf}$, or $(PG)'_{pf}$ is equivalent to analyticity.)

Now we may formulate:

THEOREM 4. *Assume that G_K admits a standard description of normal subgroups and suppose $S \cap T = \varnothing$. If the profinite completion $\widehat{\Gamma}$ of the group $\Gamma = G_{\mathcal{O}(S)}$ satisfies $(PG)'_{pf}$, then Γ has property (CSP).*

Naturally, for the proof we show that $(PG)'_{pf}$ implies that $C = C^S(G)$ is central. It should also be noted that, after the paper [15] had been prepared for publication, A. Lubotzky informed us that he also managed to establish the centrality of C under the condition $(PG)_{pf}$ for $\widehat{\Gamma}$.

COROLLARY 1. *With the assumptions of Theorem 4, if the group $\widehat{\Gamma}$ has property $(BG)_{pf}$ (in particular, if Γ has property (BG)) then Γ has (CSP).*

Now it should be pointed out that the converse statement to Theorem 4 is true without any additional assumptions on the group G. This follows from

THEOREM 5. *Let G be a simple, simply connected K-group, and let $S \subset V^K$ be a finite subset containing V_∞^K. Then the group $G_{A_S(S)}$ of S-integral S-adeles is a profinite group satisfying $(BG)_{pf}$.*

COROLLARY 2. *If G_K has a standard description of normal subgroups and $S \cap T = \varnothing$ then each of the conditions $(BG)_{pf}$, $(PG)_{pf}$, and $(PG)'_{pf}$ for $\widehat{\Gamma}$, is equivalent to (CSP) for Γ.*

Now, to close this survey, we show that, for example in the case of $\Gamma = \mathrm{SL}_m(\mathbb{Z})$ $(m \geq 3)$, the condition $(PG)'_{pf}$ can be straightforwardly checked by purely algebraic means, while condition (BG) requires some rather delicate arithmetic considerations (cf. [3]). (There is no direct proof of condition $(PG)_{pf}$ for this group either.)

It is well-known that $\Gamma = \mathrm{SL}_m(\mathbb{Z})$ $(m \geq 3)$ is generated by elementary matrices e_{ij} $(i, j = 1, \ldots, m;\ i \neq j)$. These satisfy the following commutator relations

$$[e_{ij}^{\alpha}, e_{jk}^{\beta}] = e_{ik}^{\alpha\beta} \tag{6}$$

for all pairwise distinct subscripts i, j, k. Clearly, the profinite Burnside factor $\widehat{\Gamma}_n$ is the maximal finite factor group of the discrete Burnside factor $\Gamma_n = \Gamma/\Gamma^n$, where Γ^n is generated by n-th powers of all elements of Γ. It is known that any noncentral normal subgroup in Γ is of finite index (see [8]). So Γ_n is finite and $|\widehat{\Gamma}_n| = |\Gamma_n|$ for any n. Denote by E_n the normal subgroup in Γ generated by $\{e_{ij}^n\}$. Evidently, we have $E_n \subset \Gamma^n$; so it suffices to estimate

$|\Gamma/E_n|$. Now we fix an integer $n > 0$ and a prime p, and we estimate $|\Gamma/E_{np^\alpha}|$. Assuming $\alpha > 8$ we have

$$|\Gamma/E_{np^\alpha}| = c\,|E_{np^8}/E_{np^\alpha}|,$$

where $c = [\Gamma : E_{np^8}]$. Consider now the profinite group $\Delta = \varprojlim E_{np^8}/E_{np^\alpha}$, the limit being taken over $\alpha > 8$. Using the relations (6), it is easy to show that for any $\alpha > 8$ the group $E_{np^\alpha}/E_{np^{\alpha+2}}$ is an abelian p-group. Thus Δ is a pro-p-group. On the other hand, we have

$$E_{np^{10}} \subset E_{np^8}^{p^2} \subset E_{np^8}.$$

In particular, $[E_{np^8}, E_{np^8}] \subset E_{np^8}^{p^2}$. Applying Lazard's criterion for analyticity (see [7]), or the results on the so-called powerful pro-p-groups (see [5]), we deduce that Δ is analytic. Then it has each of the properties $(BG)_{pf}$, $(PG)_{pf}$, and $(PG)'_{pf}$. This clearly implies that $|E_{np^8}/E_{np^\alpha}|$ grows polynomially in p^α. Hence the same assertion holds for $|\Gamma/E_{np^\alpha}|$, and we are through.

References

[1] H. Bass, M. Lazard & J-P. Serre, Sous-groupes d'indices finis dans $\mathrm{SL}(n, \mathbb{Z})$, *Bull. Amer. Math. Soc.*, 70 (1964), 385–392.

[2] H. Bass, J. Milnor & J-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_n ($n \geq 2$), *Publ. Math. IHES*, 33 (1967), 54–137.

[3] D. Carter & G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$, *Amer. J. Math.*, 105 (1983), 673–687.

[4] V. Deodhar, On central extensions of rational points of algebraic groups, *Amer. J. Math.*, 100 (1978), 303–386.

[5] J.D. Dixon, M.P.F. du Sautoy, A. Mann & D. Segal, Analytic pro-p-Groups, *London Math. Soc. Lecture Note Series*, No. 157, Cambridge Univ. Press, 1991.

[6] M. Kneser, Normalteiler ganzzahliger Spingruppen, *J. reine und angew. Math.*, 311/312 (1979), 191–214.

[7] M. Lazard, Groupes analytiques p-adiques, *Publ. Math. IHES*, 26 (1965), 389–603.

[8] G.A. Margulis, Finiteness of factor groups of discrete groups, *Funct. Anal. and Appl.*, 13 (1979), 28–39 (in Russian).

[9] H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, *Ann. Sci. Ecole Norm. Sup.*, (4) 2 (1969), 1–62.

[10] J. Mennicke, Finite factor groups of the unimodular group, *Ann. of Math.*, 81 (1965), 31–37.

[11] —, On Ihara's modular group, *Invent. Math.*, 4 (1967), 202–228.

[12] C. Moore, Group extensions of p-adic and adelic groups, *Publ. Math. IHES*, 35 (1968), 5–70.

[13] V.P. Platonov, Arithmetic and structural problems for linear algebraic groups, *Proc. Intern. Congr. Math. Vancouver 1974*, vol. 1 (1975), 471–476 (in Russian).

[14] V.P. Platonov & A.S. Rapinchuk, *Algebraic groups and number theory*, Moscow, Nauka, 1991 (in Russian; English translation is being prepared by Academic Press).

[15] —, —, Abstract characterizations of arithmetic groups with the congruence subgroup property, *Dokl. Akad. Nauk SSSR*, 319 (1991), No. 6 (in Russian).

[16] G. Prasad, A variant of a theorem of Calvin Moore, *C.R. Acad. Sci.*, 302 (1986), 405–408.

[17] G. Prasad & M.S. Raghunathan, On the congruence subgroup problem: Determination of the "Metaplectic kernel", *Invent. Math.*, 71 (1983), 21–42.

[18] M.S. Raghunathan, On the congruence subgroup problem, *Publ. Math. IHES*, 46 (1976), 107–161.

[19] —, On the congruence subgroup problem II, *Invent. Math.*, 85 (1986), 73–117.

[20] A.S. Rapinchuk, Multiplicative arithmetic of division algebras over number fields and metaplectic problem, *Izv. Akad. Nauk SSSR, Ser. Mat.*, 51 (1987), 1033–1064 (in Russian).

[21] —, Congruence subgroup problem for algebraic groups and strong approximation in affine varieties, *Dokl. Akad. Nauk BSSR*, 32 (1988), 581–584 (in Russian).

[22] —, On the congruence subgroup problem for algebraic groups, *Dokl. Akad. Nauk SSSR*, 306 (1989), 1304–1307 (in Russian).

[23] —, The congruence subgroup problem for algebraic groups, *Topics in algebra, Banach center publ.*, vol. 26, part 2 (1990), 399–410.

[24] —, The congruence subgroup problem for arithmetic groups with bounded generation, *Dokl. Akad. Nauk SSSR*, 314 (1990), 1327–1331 (in Russian).

[25] —, Representations of groups with bounded generation, *Dokl. Akad. Nauk SSSR*, 315 (1990), 536–540 (in Russian).

[26] —, *Combinatorial theory of arithmetic groups*, Preprint of the Institute of Mathematics of the Byelorussian Acad. Sci., No. 20 (420) (1990).

[27] J-P. Serre, Le problème des groupes de congruence pour SL_2, *Ann. of Math.*, 92 (1970), 489–527.

[28] O.I. Tavgen', Bounded generation of Chevalley groups over the rings of S-integers, *Izv. Akad. Nauk SSSR, Ser. Mat.*, 54 (1990), 97–122 (in Russian).

[29] G. Tomanov, On the congruence subgroup problem for some anisotropic algebraic groups over number fields, *J. reine und angew. Math.*, 402 (1989), 138–152.

[30] —, Remarques sur la structure des groupes algébriques définis sur des corps de nombres, *C.R. Acad. Sci.*, 310 (1990), 33–36.

[31] E.I. Zel'manov, The solution of the restricted Burnside problem for groups of odd exponent, *Izv. Akad. Nauk SSSR., Ser. Mat.*, 54 (1990) (in Russian).

Andreĭ S. Rapinchuk
Institute of Mathematics
of the
Byelorussian Academy of Sciences
ul. Surganova, 11
MINSK 220072 – Byelorussia

Astérisque

A. J. SCHOLL

Modular forms and algebraic K-theory

Astérisque, tome 209 (1992), p. 85-97

<http://www.numdam.org/item?id=AST_1992__209__85_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

MODULAR FORMS AND ALGEBRAIC K-THEORY

A. J. Scholl

In this paper, which follows closely the talk given at the conference, I will sketch an example of a non-trivial element of K_2 of a certain threefold, whose existence is related to the vanishing of an *incomplete* L-function of a modular form at $s = 1$. To explain how this fits into a general picture, we begin with a simple account, for the non-specialist, of some of the conjectures (mostly due to Beilinson) which relate ranks of K-groups and orders of L-functions, supplemented by examples coming from modular forms. The picture presented is in some respects wildly distorted; among the important topics which are given little mention are:

(i) the connection between special values of L-functions and higher regulators, which is at the heart of the Beilinson conjectures;

(ii) the conjectures of Birch and Swinnerton-Dyer, and their generalisation by Beilinson and Bloch;

(iii) the theory of (mixed) motives, which underlies the constructions of the last section.

But I hope that it may be of some use as a gentle introduction to the subject, and to prepare the reader for a more comprehensive account (see for example [**9,17,18,21**] and above all [**1**]).

1. Beginnings

The story begins with Dirichlet's unit theorem: if F is a number field with ring of integers o_F, then

$$\mathrm{rk}\, o_F^* = r_1 + r_2 - 1 = \mathrm{ord}_{s=0}\, \zeta_F(s)$$

and there is the analytic class number formula, which at $s = 0$ reads:

$$\zeta_F^*(0) = -\frac{h_F R_F}{w_F} \tag{1}$$

where $\zeta_F^*(0)$ denotes the leading coefficient in the Taylor series of $\zeta_F(s)$ at $s = 0$. More generally, let S be a finite set of primes of F, and $o_{F,S}$ the ring

of S-integers of F. Then the S-unit theorem says

$$\begin{aligned} \operatorname{rk} \mathfrak{o}_{F,S}^* &= r_1 + r_2 - 1 + \#S \\ &= \operatorname{ord}_{s=0} \zeta_{F,S}(s) \end{aligned}$$

where $\zeta_{F,S}(s)$ is the *incomplete* zeta function:

$$\zeta_{F,S}(s) = \prod_{\mathfrak{p} \notin S} (1 - N\mathfrak{p}^{-s})^{-1}.$$

and the analogue of (1) is the S-class number formula.

Borel found a generalisation of these results to the zeta function at arbitrary negative integers:

Theorem. [5] *Let $l > 0$ be an integer. Then $K_{2l}\mathfrak{o}_F$ is finite, and*

$$\begin{aligned} \operatorname{rk} K_{2l+1}\mathfrak{o}_F &= \begin{cases} r_1 + r_2 & l \text{ even} \\ r_2 & l \text{ odd} \end{cases} \\ &= \operatorname{ord}_{s=-l} \zeta_F(s). \end{aligned}$$

Moreover the leading coefficient $\zeta_F^*(-l)$ is equal, up to a non-zero rational factor, to a "higher regulator".

Remarks: (i) Here $K_i\mathfrak{o}_F$ are the higher K-groups of F, as defined by Quillen (see section 2). This is a natural generalisation of the unit theorem since $K_1\mathfrak{o}_F = \mathfrak{o}_F^*$. The fact that $K_i\mathfrak{o}_F$ are finitely generated was proved by Quillen.

(ii) The higher regulator is the determinant of a certain natural homomorphism

$$K_{2l+1}\mathfrak{o}_F \otimes \mathbf{R} \to \mathbf{R}^{m_l}, \quad m_l = \operatorname{ord}_{s=-l} \zeta_F(s).$$

(iii) The analogue of the S-unit theorem for these higher K-groups is uninteresting; on the one hand, one has

$$K_q\mathfrak{o}_{F,S} \otimes \mathbf{Q} = K_q\mathfrak{o}_F \otimes \mathbf{Q} = K_qF \otimes \mathbf{Q} \tag{2}$$

for every $q > 1$ (cf. section 2); on the other, the individual Euler factors in $\zeta_F(s)$ have no poles at negative integer points, so

$$\operatorname{ord}_{s=-l} \zeta_F(s) = \operatorname{ord}_{s=-l} \zeta_{F,S}(s)$$

for any finite set S of primes and any $l > 0$.

2. K-THEORY

For any scheme X there is a Grothendieck group K_0X. It is defined as the abelian group generated by symbols $[\mathcal{E}]$, where $\mathcal{E}$ runs over all isomorphism classes of vector bundles on X, with relations of the form

$$[\mathcal{E}] = [\mathcal{E}'] + [\mathcal{E}'']$$

for every exact sequence $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$. For a ring R one can define K_0R to be $K_0 \operatorname{Spec} R$, or (which amounts to the same thing) as the Grothendieck group of projective R-modules, with relations $[M \oplus N] = [M] + [N]$.

In a similar way one also has the group $K_0'X$, generated by $[\mathcal{E}]$ for arbitrary coherent sheaves $\mathcal{E}$, with relations from exact sequences of coherent sheaves.

Quillen showed that K_0X and $K_0'X$ are part of an infinite sequence of groups K_qX, $K_q'X$ for $q \geq 0$, constructed as the higher homotopy groups π_{q+1} of certain spaces attached to X. For some of the different ways to define them, see **[10,16,22]**.

Among the important properties of these groups are:

(i) There are cup-products $K_pX \times K_qX \to K_{p+q}X$;
(ii) For X regular (e.g. a smooth variety) $K_q'X = K_qX$;
(iii) For $Y \subset X$ a closed subscheme, there is a long exact sequence (the localisation sequence)

$$\cdots \to K_q'Y \to K_q'X \to K_q'(X - Y) \to K_{q-1}'Y \to \ldots$$

(iv) $\mathcal{O}^*(X)$ injects into K_1X, with equality if $X = \operatorname{Spec} F$ is the spectrum of a field.
(v) The K-groups of finite fields are finite (of known order).

For a number field F the localisation sequence gives

$$\cdots \to K_q\mathfrak{o}_F \to K_q\mathfrak{o}_{F,S} \to \coprod_{\mathfrak{p} \in S} K_{q-1}\mathfrak{o}_F/\mathfrak{p} \to K_{q-1}\mathfrak{o}_F \to \ldots$$

which together with (v) gives (2).

3. L-FUNCTIONS OF AN ALGEBRAIC VARIETY

Consider a smooth, projective algebraic variety X over $\mathbf{Q}$. Since any variety over a number field may be regarded—by restriction of scalars *à la* Grothendieck—as a variety over $\mathbf{Q}$ (in general, not geometrically connected) the restriction to ground field $\mathbf{Q}$ is not serious.

For each integer i in the range $0 \leq i \leq 2\dim X$ there is an L-function $L(h^i(X), s)$, which is an Euler product:

$$L(h^i(X), s) = \prod_p P_p^{(i)}(p^{-s})^{-1}.$$

The polynomials $P_p^{(i)}(t)$ here are defined as follows. Pick a prime $\ell \neq p$, and let $H_\ell^i(X)$ be the ℓ-adic cohomology of $X/\overline{\mathbf{Q}}$, which is a finite-dimensional $\mathbf{Q}_\ell$-vector space on which $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts continuously. Let $I_p \subset D_p \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be inertia and decomposition subgroups at a prime of $\overline{\mathbf{Q}}$ over p, and $\mathrm{Frob}_p = \phi_p^{-1} \in D_p/I_p$ the inverse of the Frobenius substitution. Then

$$P_p^{(i)}(t) = \det\bigl(1 - t\,\mathrm{Frob}_p \mid H_\ell^i(X)^{I_p}\bigr)$$

is the characteristic polynomial of Frob_p (the "geometric Frobenius") acting on the inertia invariants.

If X has a good reduction X_p at p, then $P_p^{(i)}$ has integer coefficients, and does not depend on ℓ, by Deligne's proof of the Weil conjectures [**6**]; moreover in this case the zeroes of $P_p^{(i)}(t)$ all have absolute value $p^{-i/2}$. For general p it is conjectured that $P_p^{(i)}(t)$ has integer coefficients, is independent of ℓ, and that its roots have absolute values $p^{-j/2}$ for various integers $j \leq i$. This is known in very few cases (curves, a class of surfaces and some sporadic higher-dimensional examples). For the conjectures that follow to make sense, we must assume these local properties are true. It is then conjectured that $L(h^i(X), s)$—which is analytic and non-zero for $\Re(s) > i/2 + 1$, by the Euler product—has a meromorphic continuation satisfying a functional equation for the substitution $s \mapsto 1 + i - s$.

4. General conjectures

The part of Beilinson's conjecture related to orders of L-functions can now be approximately stated:

Let m be an integer satisfying $m \leq \frac{1+i}{2}$. Write $q = 1 + i - 2m$. Then the order of $L(h^i(X), s)$ at $s = m$ is equal to the dimension of a certain subspace of $K_q(X)_{\mathbf{Z}} \otimes \mathbf{Q}$. More precisely, for $q > 0$

$$\dim K_q X_{/\mathbf{Z}} \otimes \mathbf{Q} = \sum_{\substack{(i,m) \\ 1+i-2m=q}} \mathrm{ord}_{s=m} L(h^i(X), s).$$

Remarks: (i) The group $K_q X_{/\mathbf{Z}}$ is defined as follows. Let $\mathcal{X}$ be a regular model for X over $\mathbf{Z}$; in other words, $\mathcal{X}$ is a regular scheme, proper over $\mathrm{Spec}\,\mathbf{Z}$, such that $\mathcal{X} \otimes \mathbf{Q} = X$. Then

$$K_q X_{/\mathbf{Z}} = \mathrm{Image}\bigl(K_q \mathcal{X} \to K_q X\bigr).$$

It would be wrong to take K_qX by itself; this can be seen already in the case of $X = \operatorname{Spec} F$, $i = m = 0$ (so that $q = 1$). For then $K_1X = F^*$ has infinite rank, but $K_1F_{/\mathbf{Z}} = \mathfrak{o}_F^*$ has the correct, finite rank. It was Bloch and Grayson who observed that in higher dimensions, and for higher q, it might still be necessary to impose a similar integrality condition (see section 5 below).

(ii) (dimension 0) In the case $X = \operatorname{Spec} F$ the conjecture is a consequence of Borel's theorem; as there is only one L-function ($i = 0$) there is no splitting up of the K-groups. These are essentially the only L-functions for which the conjecture is known to be true.

(iii) (dimension 1) If X is a curve, the conjectural picture is still quite simple. There are three L-functions: $L(h^0(X), s)$ and $L(h^2(X), s)$, which are respectively $\zeta_F(s)$ and $\zeta_F(s-1)$ (if X is irreducible with constant field F), and the Hasse-Weil L-function $L(h^1(X), s)$. There is a parity condition $q \equiv 1 + i \pmod 2$. Therefore the even K-groups K_qX are expected to contribute to the order of the Hasse-Weil L-function at the points $s = 1 - q/2$; whereas the contribution of the odd groups should be to $L(h^0(X), s)$ and $L(h^2(X), s)$, and this should be accounted for by Borel's theorem.

For varieties of higher dimension it becomes necessary to specify a decomposition of the K-groups into pieces corresponding to the various L-functions. There are in fact two (conjecturally equivalent) ways to do this. The first rests on certain conjectures on algebraic cycles (which are only known in a few cases). Suppose that the decomposition of the cohomology $H^*_\ell(X)$ into its graded pieces is algebraic, in the following strong sense: regard the projectors $\pi_i\colon H^*_\ell(X) \to H^i_\ell(X)$ (for $0 \le i \le 2\dim X$) as cohomology classes in $H^{2\dim X}_\ell(X \times X)$. Then one wants algebraic cycles Π_i on $X \times X$ whose cohomology classes are π_i, and whose images in the ring of correspondences $CH^{\dim X}(X \times X) \otimes \mathbf{Q}$ form a complete set of orthogonal idempotents.

This would follow from Grothendieck's standard conjectures; it is the decomposition of the "motive" $h(X)$ into submotives $h^i(X)$. It is known for curves and surfaces: see **[15]** for more details.

The ring $CH^{\dim X}(X \times X) \otimes \mathbf{Q}$ acts on $K_*X \otimes \mathbf{Q}$. So if the projectors Π_i exist, one can write $K_qX \otimes \mathbf{Q} = \oplus K_qh^i(X)$, where $K_qh^i(X) = \Pi_i(K_qX \otimes \mathbf{Q})$. Let $K_qh^i(X)_{/\mathbf{Z}}$ be the image of the composite:

$$K_q\mathcal{X} \otimes \mathbf{Q} \to K_qX \otimes \mathbf{Q} \to K_qh^i(X).$$

The precise conjecture would then be:

$$\dim K_qh^i(X)_{/\mathbf{Z}} = \operatorname{ord}_{s=m} L(h^i(X), s) \quad \text{for } q = 1 + i - 2m > 0.$$

Beilinson actually uses an alternative description of the decomposition, which is not conjectural, and gives a reasonably computable theory (for example, it is compatible with the maps in the localisation sequence when suitably interpreted). There are certain operators ψ^p (Adams operators) acting on the groups K_qX, coming from the exterior power operation on vector bundles. Define $K_q^{(n)}X$ to be the subspace of $K_qX \otimes \mathbf{Q}$ on which ψ^p acts as multiplication by p^n, with $p > 1$. It is known that this is independent of $p > 1$ and that one has a direct sum decomposition:

$$K_qX \otimes \mathbf{Q} = \oplus_{n \geq 0} K_q^{(n)}X.$$

Defining $K_q^{(n)}X_{/\mathbf{Z}}$ to be the image of $K_q\mathcal{X} \otimes \mathbf{Q}$ in $K_q^{(n)}X$, Beilinson's precise conjecture reads:

Conjecture 4.1. [1]

$$\dim K_q^{(n)}X_{/\mathbf{Z}} = \operatorname{ord}_{s=m} L(h^i(X), s)$$

for $q = 1 + i - 2m > 0$ *and* $n = 1 + i - m = q + m$.

Remark: The relation between these two decompositions is almost completely conjectural. It is only over a number field that one expects the two decompositions to be the same—this is apparent even in the case $X = \operatorname{Spec} F$.

To formulate an S-integral version of the conjecture, let S be a finite set of rational primes, and $\mathbf{Z}_S = \mathbf{Z}[\{p^{-1}\}_{p \in S}]$, as in the first section. Let $\mathcal{X}_S = \mathcal{X} \otimes \mathbf{Z}_S$ be the restriction of the regular model to $\operatorname{Spec} \mathbf{Z}_S$, and define

$$K_q^{(n)}X_{/\mathbf{Z}_S} = \operatorname{Image}(K_q\mathcal{X}_S \otimes \mathbf{Q} \to K_q^{(n)}X)$$

Conjecture 4.2. *Let* $L_S(h^i(X), s)$ *be the incomplete L-function (i.e. with the Euler factors for* $p \in S$ *removed). Then:*

$$\dim K_q^{(n)}X_{/\mathbf{Z}_S} = \operatorname{ord}_{s=m} L_S(h^i(X), s)$$

for $q = 1 + i - 2m > 0$ *and* $n = 1 + i - m = q + m$.

Remarks: (i) The order of the incomplete L-function at $s = m$ is the sum of the order of the complete L-function and

$$\sum_{p \in S} \dim \ker\left(\operatorname{Frob}_p - p^m \mid H_\ell^i(X)^{I_p}\right)$$

(assuming that the action of Frob_p is semisimple). In particular, if p is a prime of good reduction, then there will be no contribution to the sum unless $m = i/2$. Thus for $m < i/2$ (ie. $q > 1$) the order of L_S stabilises as soon

as S contains all bad primes. At the same time, $K_q X_{/\mathbf{Z}_S}$ is the kernel of the boundary map in the localisation sequence:

$$K_q X_{/\mathbf{Z}_S} = \ker\bigl(K_q X \to \coprod_{p \notin S} K'_{q-1}\mathcal{X}_{\mathbf{F}_p}\bigr).$$

For a good prime p, $K'_{q-1}\mathcal{X}_{\mathbf{F}_p} = K_{q-1}\mathcal{X}_{\mathbf{F}_p}$ and Parshin has conjectured that this is torsion if $q - 1 \neq 0$. If this conjecture is true, then the left-hand side of conjecture 4.2 also stabilises as soon as S contains all bad primes.

(ii) Conjecture 4.2 was made by Deligne in [**7**]. He also asked for the existence of an S-regulator analogous to the one for units. A general candidate for this has yet to be constructed; for something in this direction see section §4.7 of [**17**].

5. Modular curves

Let Γ be a congruence subgroup of $SL_2(\mathbf{Z})$ of level n, and let U_Γ be the modular curve, whose set of complex points is the non-compact Riemann surface $\Gamma\backslash\mathfrak{H}$. There is the standard compactification

$$X_\Gamma = U_\Gamma \cup (\text{cusps})$$

which has the structure of an irreducible curve over the field $\mathbf{Q}(\zeta_n)$ (although it often can be defined over a smaller field). The Hasse-Weil L-function of X_Γ is a product

$$L(h^1(X_\Gamma), s) = \prod_{i=1}^{g} L(f_i, s)$$

where f_i are certain (not necessarily distinct!) newforms of weight 2 and some level, and $L(f_i, s)$ is the associated Hecke L-series. There is a functional equation relating $L(h^1(X), s)$ and $L(h^1(X), 2 - s)$.

At the point $s = m = (1 + i)/2 = 1$ one has the conjecture of Birch and Swinnerton-Dyer. This fits into the framework of 4.1 because of the relation between K_0 of a curve and its Jacobian. At other points the functional equation determines the order of vanishing of the L-function, and

$$\operatorname{ord}_{s=m} L(h^1(X), s) = g \quad \text{for } m = 0, -1, -2, \ldots$$

Conjecture 4.1 therefore predicts that $K_{2r}X_{\Gamma/\mathbf{Z}}$ will have rank at least g, for every positive integer r.

Remarks: (i) As defined here, g will equal $\phi(n)$ times the genus of the curve X_Γ. If the chosen field of definition is $\mathbf{Q}$, g will be simply the genus.

(ii) The levels of the forms f_i need not equal n, or even divide n; however they always divide n^2.

The simplest case is the point $s = 0$. Here we have the fundamental result of Beilinson:

Theorem. *(a)* [**1**] *There exists a g-dimensional subspace $\mathcal{P}_\Gamma$ of $K_2X_\Gamma \otimes \mathbf{Q}$; its regulator is a non-zero rational multiple of $L^{(g)}(h^1(X_\Gamma), 0)$.*

(b) [**19**] *$\mathcal{P}_\Gamma$ is contained in $K_2X_{\Gamma/\mathbf{Z}} \otimes \mathbf{Q}$.*

The proof of the theorem involves an explicit construction of elements of $K_2X_\Gamma \otimes \mathbf{Q}$. We indicate here the idea of the construction; for details, including the definition and calculation of the regulator, the reader should consult [**1**],[**2**] or [**19**]. The basic tool is:

Theorem (Manin-Drinfeld). *Any divisor of degree zero on X_Γ supported on the cusps is of finite order in the Jacobian of X_Γ.*

This guarantees a good supply of elements of $\mathcal{O}^*(U_\Gamma)$, which are the *modular units*; for example the function $\Delta(nz)/\Delta(z)$ is such a function. Now if g, $g' \in \mathcal{O}^*(U_\Gamma)$, we may form the cup product $g \cup g' \in K_2U_\Gamma$. The localisation sequence gives an exact sequence:

$$0 \to K_2X_\Gamma \otimes \mathbf{Q} \to K_2U_\Gamma \otimes \mathbf{Q} \xrightarrow{\partial} K_1(\text{cusps}) \otimes \mathbf{Q}$$

(it is exact on the left since K_2 of a number field is torsion).

Lemma. *Assume that the cusps are rational over the field of constants of X_Γ. Let W be the subspace of $K_2U_\Gamma \otimes \mathbf{Q}$ generated by elements of the form $c \cup h$, with $h \in \mathcal{O}^*(U_\Gamma)$ and c a constant function. Then $\partial(W) = \partial(K_2U_\Gamma \otimes \mathbf{Q})$.*

Accordingly for any cup-product $g \cup g'$, there are $h_\alpha \in \mathcal{O}^*(U_\Gamma) \otimes \mathbf{Q}$ and constant functions c_α such that

$$g \cup g' + \sum_\alpha c_\alpha \cup h_\alpha \in K_2X_\Gamma \otimes \mathbf{Q}.$$

By varying g, g' one thus obtains a subspace $\mathcal{Q}_\Gamma \subset K_2X_\Gamma \otimes \mathbf{Q}$. For $\Gamma' \subset \Gamma$ there is a direct image map:

$$\theta_{\Gamma,\Gamma'}\colon K_2X_{\Gamma'} \otimes \mathbf{Q} \to K_2X_\Gamma \otimes \mathbf{Q}$$

and the subspace of the theorem is obtained as

$$\mathcal{P}_\Gamma = \bigcup_{\Gamma'} \theta_{\Gamma,\Gamma'}(\mathcal{Q}_{\Gamma'})$$

where Γ' runs over all congruence subgroups $\Gamma' \subset \Gamma$.

The proof that $\dim(\mathcal{P}_\Gamma) \geq g$ is by finding the regulators of these elements, which reduces to the calculation of a certain Rankin-Selberg integral. The

proof that the elements belong to $K_2X_{\Gamma/\mathbf{Z}}$ results from examining the localisation sequence:

$$0 \to K_2X_{\Gamma/\mathbf{Z}} \to K_2X_\Gamma \xrightarrow{\partial} \bigoplus_p K_1'\mathcal{X}_\Gamma \otimes \mathbf{F}_p \tag{3}$$

and using the structure of the reduction modulo p of the modular curves [**8,12**]. The key ingredient is the fact that the action of the Hecke algebra on supersingular points in characteristic p can be expressed in terms of the action on suitable (characteristic zero) cusp forms (see for example [**13**]).

For example, consider the first non-trivial case, the modular curve $X = X_0(11)_{/\mathbf{Q}}$, which has $g = 1$. There are just two cusps 0 and ∞, and their difference has order 5 in the Jacobian of $X_0(11)$, so that the group of modular units has rank 1. If g is a generator, then $g \cup g \in K_2$ is torsion (as the cup-product is skew-symmetric). So $\mathcal{Q}_{\Gamma_0(11)} = 0$, and modular units on $\Gamma_0(11)$ do not suffice to give a non-zero element of K_2. However the covering $X_1(11)$ is an elliptic curve with 5 cusps, all of them rational (it is the Weil curve 11A of the tables in [**3**]). This curve is one of a number studied by Bloch and Grayson in [**4**]. By calculating the regulator (numerically) they determined an element of $\mathcal{Q}_{\Gamma_1(11)}$ of infinite order. Since the isogeny $X_1(11) \to X_0(11)$ induces an isomorphism on $K_2 \otimes \mathbf{Q}$, this produces the desired non-zero element of $K_2(X_0(11)) \otimes \mathbf{Q}$. The integrality of this element was also verified by Bloch and Grayson.

In this setting, conjecture 4.2 states that

$$\operatorname{ord}_{s=0} L_S(X_\Gamma, s) = g + \sum_{p \in S} m_p,$$

where m_p is the number of times $(1 - p^{-s})^{-1}$ occurs in the Euler factor of $L(X_\Gamma, s)$ at p. When $g = 1$, then $m_p = 1$ if the reduction mod p of X_Γ has an ordinary double point with rational tangent directions, and is 0 otherwise. This is also precisely the rank of $K_1'\mathcal{X}_{\Gamma/\mathbf{F}_p}$, suggesting that the boundary map ∂ in (3) is surjective, up to torsion. (For a more detailed analysis of a more general situation, see §4.7 of [**17**].) The calculations of Bloch and Grayson exhibit, in many cases, non-integral elements of $K_2(X_\Gamma)$ in partial confirmation of this result.

Consider for example the case of $X_0(11)$. The only bad prime is $p = 11$, where the reduction is split multiplicative, and conjecture 4.2 therefore predicts that $K_2(X_0(11))$ has rank 2. Bloch and Grayson found two independent elements of K_2 by working with functions with divisors with support in the 5 rational points of $X_0(11)$ (only two of which are cusps). However, unlike the

case of the integral elements (Beilinson's theorem), there is as yet no general construction of the "extra" elements predicted by conjecture 4.2.

6. Generalisations

The results of the previous section have been generalised in various ways. One is by considering the behaviour of $L(X_\Gamma, s)$ at negative integers $s = -l < 0$. Here Beilinson has proved:

Theorem. [2] *There exists a subspace of* $\dim K_{2l+2}(X_\Gamma) \otimes \mathbf{Q}$ *of dimension* $g = \mathrm{ord}_{s=-l} L(X_\Gamma, s)$.

He also proves that elements constructed have the predicted regulators. We should remark that in this case there is, up to torsion, no difference between $K_{2l+2}X_{\Gamma/\mathbf{Z}}$ and $K_{2l+2}X_\Gamma$, since K_j' of a (possibly singular) curve over a finite field is torsion if $j > 1$, by [11]. The construction of the elements uses not just the modular curves themselves but also the "Kuga-Sato varieties" (fibre products of the universal families of elliptic curves).

It is possible to generalise these results to cusp forms of weight $k > 2$. If f is such a cusp form (assumed to be a newform of some level), then its L-series $L(f, s)$ occurs in the L-function of V_k, a Kuga-Sato variety of dimension $k-1$. (For weight two, V_2 is X_Γ.) Corresponding to the simple zero of $L(f, s)$ at the point $s = -l \leq 0$, we can construct a non-zero element of $K_{2l+k}(V_k) \otimes \mathbf{Q}$, and determine its regulator. For a precise statement of this and the previous results, and some indications of the proofs, we refer to §5 of [9].

There are very few examples of evidence in support of conjecture 4.2. Other than the examples of Bloch-Grayson and the example of the next section, there is only the work of Mestre and Schappacher [14]. They consider the symmetric square L-function of an elliptic curve E over $\mathbf{Q}$ at $s = 0$ (where it vanishes to order 2), and exhibit in many cases an experimental relation with $K_3(E \times E)$, generalising all the phenomena observed by Bloch and Grayson.

7. An example

Let $\Gamma < PSL_2(\mathbf{Z})$ be a subgroup of index 7, with two cusps, one of width 5 and another of width two. It is easy to show (by constructing fundamental regions, for example) that up to conjugacy there is exactly one such subgroup: one such is generated by the elements

$$\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

The associated modular curve X_Γ has genus zero, and there is a rational parameter t on X_Γ satisfying the equation

$$j = \frac{(t+18)(t^2+t-26)^3}{(7t+1)^2}$$

where j is the modular invariant. (Similar constructions were made by Klein and Fricke: see [0] for further examples and references.) Let $\phi : E \to X_\Gamma$ be an elliptic surface with invariant j; such a surface may be obtained by taking the affine equation

$$y^2 + xy = x^3 - \frac{36x+1}{j-1728},$$

although there are others. Finally let V be a nonsingular model over $\mathbf{Q}$ for the fibre product $E \times_{X_\Gamma} E$.

Similar fibre varieties were studied in [20], and the same methods can be used to show that the interesting part of the L-function $L(h^3(V), s)$ is a Hecke L-series $L(f, s)$, where f is a certain cusp form on $\Gamma_0(35)$ of weight 4. At the bad primes 5 and 7 the Euler factors of the L-series are $(1+5^{1-s})^{-1}$ and $(1-7^{1-s})^{-1}$.

The functional equation shows $L(f,1) \neq 0$, and so the incomplete L-function $L_S(f,s)$ vanishes at $s=1$ if and only if $7 \in S$. Conjecture 4.2 predicts that there is a non-zero element $\xi \in K_2(V) \otimes \mathbf{Q}$, which is non-integral. We now give the construction of such an element.

Let $\infty \in X_\Gamma$ be the cusp $t = \infty$. The fibre E_∞ of ϕ is a Néron polygon, so there is a canonical (up to sign) inclusion $\mathbb{G}_m \hookrightarrow E_\infty$. Therefore (at any rate if the model V is sufficiently carefully chosen) the fibre V_∞ contains a copy of $\mathbb{G}_m \times \mathbb{G}_m = \operatorname{Spec} \mathbf{Q}[x_1, x_1^{-1}, x_2, x_2^{-1}]$. The element

$$x_1 \cup x_2 \in K_2(\mathbb{G}_m \times \mathbb{G}_m) \otimes \mathbf{Q}$$

can be shown to extend to an element of $K_2'(V_\infty) \otimes \mathbf{Q}$. By the functoriality of K'-theory with respect to the inclusion $V_\infty \hookrightarrow V$ we obtain an element

$$\xi \in K_2'(V) \otimes \mathbf{Q} = K_2(V) \otimes \mathbf{Q}.$$

Theorem. *ξ is non-zero.*

We can only give a vague idea of the proof here. It relies on the existence of the ℓ-adic regulator map

$$K_q(V) \to H^{2j-q}_{\text{ét}}(V, \mathbf{Z}_\ell(j))$$

which takes values in the ℓ-adic cohomology of $V/\mathbf{Q}$ (as distinct from that of $V/\overline{\mathbf{Q}}$). Here as usual $\mathbf{Z}_\ell(j)$ denotes the $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ module which is dual to the module of ℓ-power roots of unity, tensored with itself j times. In

this case we obtain a class in $H^4(V, \mathbf{Q}_\ell(3))$, and from the Hochschild-Serre spectral sequence this maps to an element

$$\xi_\ell \in H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), H^3_\ell(V) \otimes \mathbf{Q}_\ell(3))$$

or equivalently, to a class of extensions of Galois modules

$$0 \to H^3_{\text{ét}}(\overline{V}, \mathbf{Q}_\ell) \to (\text{extension}) \to \mathbf{Q}_\ell(-3) \to 0$$

This extension class is realised by a subquotient of the cohomology of the open variety $V - V_\infty - V'_\infty$ (where V'_∞ is the fibre at the other cusp $t = -1/7$). Using the theory of vanishing cycles, one then shows that the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_7/\mathbf{Q}_7)$ on this cohomology is highly non-trivial, which is enough to prove the non-vanishing of ξ. Full details will appear elsewhere.

Remark: It should be noted that Γ is not a congruence subgroup. Indeed, for congruence subgroups the analogous elements to ξ are always trivial. This is an example of the "Manin-Drinfeld principle", and was proved by Beilinson in [2] by explicitly constructing elements of K-theory of the open varieties, analogous to modular units. I know of *no* examples of non-integral elements of the K-groups of Kuga-Sato varieties for congruence subgroups, and it would be of great interest to have a general construction of them.

References

[0] A. O. L. Atkin, H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups.* Proc. Symp. Pure Math. AMS **19** (1971), 1–25

[1] A. A. Beilinson, *Higher regulators and values of L-functions.* J. Soviet Math. **30** (1985), 2036–2070

[2] A. A. Beilinson, *Higher regulators of modular curves.* Applications of algebraic K-theory to algebraic geometry and number theory (Contemporary Mathematics **5** (1986)), 1–34

[3] B. J. Birch, W. Kuyk (eds), *Modular functions of one variable IV.* Lect. notes in mathematics **476**, 79–88 (Springer, 1975)

[4] S. Bloch, D. Grayson, K_2 *and L-functions of elliptic curves: computer calculations.* Applications of algebraic K-theory to algebraic geometry and number theory (Contemporary Mathematics **55** (1986)), 79–88

[5] A. Borel, *Cohomologie de* SL_n *et valeurs de fonctions zêta.* Ann. Scuola Normale Superiore **7** (1974), 613–616

[6] P. Deligne, *La conjecture de Weil I.* Publ. Math. IHES **43** (1974), 272–307

[7] P. Deligne, *Letter to C. Soulé.* 20–1–1985

[8] P. Deligne, M. Rapoport, *Les schémas de modules des courbes elliptiques.* Modular functions of one variable II. Lect. notes in mathematics **349**, 143–316 (Springer, 1973)

[9] C. Deninger, A. J. Scholl, *The Beilinson Conjectures.* In: *L*-functions and Arithmetic (ed. J. H. Coates, M. J. Taylor), Cambridge University Press (1991), 173–209

[10] H. Gillet, D. Grayson, *On the loop space of the Q-construction.* Illinois J. Math **31** (1987), 574–597

[11] G. Harder, *Die Kohomologie S-arithmetischer Gruppen über Funktionenkörpern.* Inventiones math. **42** (1977), 135–175

[12] N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves.* Ann. of Math. Studies **108** (1985)

[13] J-F. Mestre, *Courbes de Weil et courbes supersingulières.* Séminaire de Théorie de Nombres de Bordeaux 1984–5, exposé 23

[14] J-F. Mestre, N. Schappacher, *Séries de Kronecker et fonctions L des puissances symétriques de courbes elliptiques sur* **Q**. In: Arithmetic algebraic geometry (ed. G. van de Geer, F. Oort, J. Steenbrink), Birkhäuser (1991), 209–245

[15] J. Murre, *The motive of an algebraic surface.* J. reine angew. Math. **409** (1990), 190–204

[16] D. Quillen, *Higher algebraic K-theory I.* Lect. notes in mathematics **341** (1973), 85–147

[17] D. Ramakrishnan, *Regulators, algebraic cycles, and values of L-functions.* Contemporary Mathematics **83** (1989), 183–310

[18] M. Rapoport, N. Schappacher, P. Schneider (ed.), *Beilinson's conjectures on special values of L-functions.* Academic Press (1988)

[19] N. Schappacher, A. J. Scholl, *Beilinson's theorem on modular curves.* In [**18**].

[20] A. J. Scholl, *The ℓ-adic representations attached to a certain noncongruence subgroup.* J. reine angew. Math. **392** (1988), 1–15

[21] C. Soulé, *Régulateurs.* Séminaire Bourbaki, exposé 644. Astérisque **133/134** (1986), 237–253

[22] F. Waldhausen, *Algebraic K-theory of spaces.* Lect. notes in mathematics **1126** (1985), 318–419

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF DURHAM, SOUTH ROAD, DURHAM DH1 3LE, ENGLAND
E-mail address: a.j.scholl@durham.ac.uk

Astérisque

TETSUJI SHIODA

Some remarks on elliptic curves over function fields

Astérisque, tome 209 (1992), p. 99-114

<http://www.numdam.org/item?id=AST_1992__209__99_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SOME REMARKS ON ELLIPTIC CURVES OVER FUNCTION FIELDS

Tetsuji SHIODA

In my lecture at the Journées Arithmétiques in Geneva (entitled "Mordell-Weil lattices and sphere packings"), I talked on
1) a brief survey on lattices and sphere packings,
2) basic results on Mordell-Weil lattices, and
3) application to sphere packings via supersingular surfaces.
For these topics, the following references are available: 1) [CS,Ch.1], 2) [S3], [S4] and 3) [E], [Oe], [S5].

In this note, instead of reporting on these, I would like to treat some related topics on elliptic curves over a function field, especially some results on the L-function of an elliptic curve over a function field with a finite constant field. Most of them must be known to experts, but the approach based on surface theory and Mordell-Weil lattices seems to provide a natural setting for this subject (cf. [T2],[G],[Mc]). In particular, this method enables one to write down explicit examples of such an L-function in some nontrivial cases.

The contents of this paper are as follows:
1. Elliptic surfaces
2. The L-function of an elliptic curve
3. Supersingular case
4. Rational elliptic surfaces

The present work has been done during my visit to Max-Planck-Institut, Bonn and the University of Geneva. I would like to thank Professor F. Hirzebruch and Professor D. Coray for their kind invitation.

1 Elliptic surfaces

Let us review first some basic results on elliptic surfaces, fixing the notation. Let k be an algebraically closed field of arbitrary characteristic and let K/k be a function field of one variable over k, i.e., $K = k(C)$ for some smooth projective curve C over k. Let E/K be an elliptic curve with a K-rational point O, and let $f : S \longrightarrow C$ denote the elliptic surface associated with E/K (the Kodaira-Néron model). The elliptic curve E is recovered from f as its generic fibre and, as is well known, the K-rational points of E can be identified with the sections of f; for each $P \in E(K)$, (P) denotes the image curve in S of the section $P : C \longrightarrow S$. We always assume the condition $(*)$ that f has at least one singular fibre.

Now let $N = \mathrm{NS}(S)$ be the Néron-Severi group of S; it is a free module of finite rank ρ (=the Picard number of S), which is an (indefinite) integral lattice with respect to the intersection pairing. We denote by T or L the trivial or essential sublattice of N; by definition, T is the sublattice generated by the zero-section (O), a fibre and all components of reducible fibres of f, and L is the orthogonal complement of T in N. In particular, we have

$$N \otimes \mathbf{Q} = (T \otimes \mathbf{Q}) \oplus (L \otimes \mathbf{Q}) \tag{1.1}$$

and

$$\rho = \mathrm{rk}\, T + \mathrm{rk}\, L. \tag{1.2}$$

Further we have

$$\mathrm{rk}\, T = 2 + \sum_{v \in C} (m_v - 1) \tag{1.3}$$

where m_v is the number of irreducible components of the fibre $f^{-1}(v)$, and $\mathrm{rk}\, L$ is equal to the Mordell-Weil rank of E/K:

$$r := \mathrm{rk}\, L = \mathrm{rk}\, E(K). \tag{1.4}$$

Actually there is a natural isomorphism

$$L \otimes \mathbf{Q} \simeq E(K) \otimes \mathbf{Q}, \tag{1.5}$$

which takes the intersection pairing on L to the height pairing on the Mordell-Weil group (up to the sign change); indeed this is essentially how we defined the structure of Mordell-Weil lattices (see [S4]).

Next we consider the cycle map

$$\gamma : N \longrightarrow H = H^2(S, \mathbf{Q}_l(1)) \tag{1.6}$$

where H stands for the l-adic cohomology group with a fixed prime number $l \neq \mathrm{char}(k)$ (cf. [T1]). It is injective and takes the intersection pairing of N into the cup-product pairing in H. Let us denote by $\mathrm{Trans}(S)$ the orthogonal complement of $\mathrm{Im}(\gamma)$ in H, whose elements are called transcendental cycles on S, and by W the orthogonal complement of $\gamma(T)$ in H. The space W corresponds to what Weil called the *essential part* in the second homology of S (cf. his comments to the paper [1967a] in [W, III]). Then we have

$$H \simeq (N \otimes \mathbf{Q}_l) \oplus \mathrm{Trans}(S) \simeq (T \otimes \mathbf{Q}_l) \oplus W \tag{1.7}$$

and

$$W \simeq (L \otimes \mathbf{Q}_l) \oplus \mathrm{Trans}(S) \tag{1.8}$$

The Lefschetz number of S is defined as

$$\lambda := \dim \mathrm{Trans}(S) = b_2 - \rho \qquad (b_2 = \dim H^2(S)) \tag{1.9}$$

which is known to be a birational invariant of S.

Proposition 1 *The dimension w of the vector space W is given by*

$$w = r + \lambda = b_2 - \mathrm{rk}\, T. \tag{1.10}$$

If $\mathrm{char}(k) \neq 2, 3$, *then*

$$w = 4g - 4 + \mu + 2\alpha \tag{1.11}$$

where g is the genus of C (or of K) and μ (resp. α) is the number of singular fibres of multiplicative (resp. additive) type.

Proof. The first part is immediate from (1.7) and (1.8). The second part is also well-known (cf.[R],[S1]). Let us briefly recall the idea of the proof. From the standard facts in surface theory, we have

$$b_2 = c_2 + 2b_1 - 2 \qquad (c_2 = \text{ Euler number of } S)$$

where $b_1 = 2g$ since we are assuming the condition $(*)$. On the other hand, we have the following formula for $\mathrm{char}(k) \neq 2, 3$:

$$c_2 = \sum_v e_v \qquad (e_v = \text{ Euler number of } f^{-1}(v)) \tag{1.12}$$

(cf. [K],[Ogg],[Ogu]). Then, by (1.9) and (1.3), we have

$$w = 4g - 4 + \sum_v (e_v - m_v + 1).$$

It remains to check that

$$e_v = m_v \quad \text{or} \quad m_v + 1$$

according as the fibre $f^{-1}(v)$ is of multiplicative or additive type, which can be done using the classification of singular fibres([K],[N],[T3]). *q.e.d.*

It may be worthwhile to mention the following direct consequence. Simply note that we have $\lambda \geq 0$ in general and $\lambda \geq 2p_g$ (p_g: geometric genus of S) in characteristic 0.

Corollary 2 *If* $\mathrm{char}(k) \neq 2, 3$, *then*

(1.13). $$r \leq w = 4g - 4 + \mu + 2\alpha.$$

Corollary 3 *Assume* $\mathrm{char}(k) = 0$. *Then*

(1.14) $$p_g \leq \frac{1}{2}w = 2g - 2 + \frac{1}{2}\mu + \alpha$$

(1.15) $$c_2 = 12(p_g - g + 1) \leq 6(2g - 2 + \mu + 2\alpha)$$

and

(1.13'). $$r \leq 4g - 4 + \mu + 2\alpha - 2p_g.$$

Remark. (a) In case $\mathrm{char}(k) = 2$ or 3, (1.10) is still valid, but (1.11) should be modified by adding an extra term caused by wild ramifications (cf. [Ogg],[R],[Sa]). In other words, each e_v in (1.12) should be replaced by $e_v + \delta_v$ with a well-defined non-negative integer δ_v so that the right hand side of (1.11) should have the term $\sum_v \delta_v$.
(b) The idea behind equality of expressions in (1.10) and (1.11) was first used by Igusa [I] to define a correct Betti number b_2 of an algebraic surface, and later it was formulated in a more general situation as the so-called Ogg-Shafarevich formula (cf. [R]).
(c) The above (1.14) or its equivalent (1.15) seems to have been proved by many authors again and again, though it was explicitly stated in [S1,Cor.2.7] in 1972. In particular, (1.15) is sometimes called Szpiro's conjecture (cf. [Sz,p.10]); note that we make no assumption of semi-stability ($\alpha = 0$) in the above argument.

2 The L-function of an elliptic curve

From now on, we consider the following situation. Let $k_0 = \mathbf{F}_q$ be a finite field with q elements and let k be its algebraic closure. Let $K_0 = k_0(C)$ be the function field of a curve C defined over k_0, and let E be an elliptic curve defined over K_0.

In this section, we shall show that the L-function of E/K_0 is essentially the characteristic polynomial of the Frobenius on the space W introduced above.

The L-function $L(E/K_0, s)$ is defined by the eulerian product

$$L(E/K_0, s) = \prod_v P_v(s)^{-1} \tag{2.1}$$

where v runs over the closed points of C/k_0 (equivalently, over the places of K_0/k_0) whose residue field $\mathbf{F}_v$ is a finite field with q_v elements and where

(2.2)

$$P_v(s) = \begin{cases} 1 - (q_v + 1 - N_v)q_v^{-s} + q_v^{1-2s} & \text{if } f^{-1}(v) \text{ is smooth} \\ 1 - \epsilon_v q_v^{-s} & \text{if } f^{-1}(v) \text{ is of multiplicative type} \\ 1 & \text{if } f^{-1}(v) \text{ is of additive type.} \end{cases}$$

Here N_v is the number of $\mathbf{F}_v$-rational points of the elliptic curve $f^{-1}(v)$, and $\epsilon_v = 1$ or -1 is determined as follows: in the multiplicative reduction case, the minimal Weierstrass model of E at v reduces to a rational curve with a node, and $\epsilon_v = 1$ or -1 according as the tangents at the node are $\mathbf{F}_v$-rational or not (cf. [T3,(5.2)], [Se2]).

On the other hand, regarding E as an elliptic curve over $K = k(C)$, we consider the associated elliptic surface

$$f : S \longrightarrow C$$

as in Section 1. We use the same notation as there unless otherwise mentioned; an exception is that v denotes a closed point of C/k_0 rather than a geometric point.

Note that, in the present situation, the surface S is defined over k_0; namely there is a smooth projective surface, say S_0, over k_0 such that S is equal to the base extension $S_0 \otimes k$.

Now the Galois group $G = \mathrm{Gal}(k/k_0)$ naturally acts on $N = \mathrm{NS}(S)$ and $H = H^2(S, \mathbf{Q}_l(1))$ ($l \neq \mathrm{char}(k)$) and their subspaces T, L, W, etc. appearing in Section 1. It is easy to see that all the maps or the direct sum decompositions there are compatible with the G-action. Letting $\sigma \in G$ be the Frobenius

automorphism of k:

$$\sigma : x \longrightarrow x^q,$$

we can consider the characteristic polynomial of σ or σ^{-1} (called the geometric Frobenius) on these vector spaces.

Theorem 4 *The L-function $L(E/K_0, s)$ of E/K_0 is a polynomial in $x = q^{1-s}$ of degree $w = \dim(W)$ and it is equal to the characteristic polynomial of σ^{-1} on W:*

$$L(E/K_0, s) = \det(1 - x\sigma^{-1} \mid W) \tag{2.3}$$

It satisfies the functional equation (corresponding to $x \to 1/x$):

$$L(E/K_0, 2 - s) = (-1)^w \det(\sigma|W) q^{(s-1)w} L(E/K_0, s).$$

Proof. This is implicit in [T2] where a more general situation is treated. For the convenience of the reader, let us give a complete proof in the case under consideration. First recall that the zeta function of the curve C (or the surface S) over the finite field k_0 is given as follows: letting $u = q^{-s}$, we have

$$\zeta(C/k_0, s) = \frac{P_1(u)}{(1-u)(1-qu)} \tag{2.4}$$

and

$$\zeta(S/k_0, s) = \frac{P_1(u)P_1(qu)}{(1-u)P_2(u)(1-q^2u)} \tag{2.5}$$

where $P_i(u)$ is the characteristic polynomial of the Frobenius endomorphism φ acting on $H^i(S, \mathbf{Q}_l)$. That the same $P_1(u)$ appears both for C and S is a consequence of the fact that the Picard variety of S is isomorphic to the Jacobian of C (cf. [S4,Sect.4]). Now, by a general property of zeta-functions (cf. [Se1]), we have

$$\zeta(C/k_0, s) = \prod_v \frac{1}{1 - q_v^{-s}} \tag{2.6}$$

and

$$\zeta(S/k_0, s) = \prod_v \zeta(f^{-1}(v)/\mathbf{F}_v, s) \tag{2.7}$$

where v runs over the closed points of C/k_0. Note that a closed point v determines and is determined by a G-orbit in $C(k)$, say $\{\bar{v}_1, \ldots, \bar{v}_d\}$ where $d = \deg(v), q_v = q^d$. We put

$$T_v = \sum_{i=1}^{d} T_{\bar{v}_i} \subset N$$

where $T_{\bar{v}_i}$ is the sublattice of N generated by the (k-)irreducible components of $f^{-1}(\bar{v}_i)$ other than the component meeting the zero section. Writing m_v for the common value of $m_{\bar{v}_i}$ (= the number of irreducible components of $f^{-1}(\bar{v}_i)$), we have $\mathrm{rk}\, T_v = \deg(v)(m_v - 1)$.

Lemma 5 *With the above notation, we have*

$$\zeta(f^{-1}(v)/\mathbf{F}_v, s) = \frac{P_v(s)}{(1 - q_v^{-s})(1 - q_v^{1-s})} \frac{1}{\det(1 - u\varphi \mid T_v)} \tag{2.8}$$

where $P_v(s)$ is as defined by (2.2).

Assume this for a moment. By (2.7), (2.6), (2.1) and (2.2), we have

$$\zeta(S/k_0, s) = \frac{\zeta(C/k_0, s)\zeta(C/k_0, s-1)}{L(E/K_0, s) \prod_v \det(1 - u\varphi \mid T_v)} \tag{2.9}$$

In view of (2.4) and (2.5), this implies

$$L(E/K_0, s) = \frac{P_2(u)}{(1 - qu)^2 \prod_v \det(1 - u\varphi \mid T_v)}. \tag{2.10}$$

Since the numerator (resp. denominator) in the right hand side is the characteristic polynomial of φ on $H' = H^2(S, \mathbf{Q}_l)$ (resp. T), the quotient is equal to the characteristic polynomial of φ on the space $W' \subset H'$ corresponding to $W \subset H$. Further, noting that

$$\begin{aligned} P_2(s) &= \det(1 - u\varphi \mid H^2(S, \mathbf{Q}_l)) \\ &= \det(1 - qu\sigma^{-1} \mid H^2(S, \mathbf{Q}_l(1))), \end{aligned} \tag{2.11}$$

(cf. [T1,Sect.3]), we have proven (2.3) by setting $x = qu = q^{1-s}$.

The functional equation for L follows from that of P_2 (which is a consequence of the Poincaré duality for S), since the denominator in (2.10) also satisfies a similar equation (see Lemma 6 below).

To prove Lemma 5, we need

Lemma 6 *Let $m = m_v, d = \deg(v)$ and $x = (qu)^d$. Then*

$$\det(1 - u\varphi \mid T_v) = (1 - x)^{m-1} \tag{2.12}$$

if every irreducible component of $f^{-1}(\bar{v}_i)$ is rational over $\mathbf{F}_v$. Otherwise, let e be the degree of the smallest extension of $\mathbf{F}_v$, say k_1, over which the condition

holds. Then e is either 2 or 3, and the characteristic polynomial of φ on T_v is equal to one of the following :

$$
\begin{array}{lll}
(1-x^2)^{\frac{m-1}{2}} & I_m\ (m:\text{odd}) & e=2 \\
(1-x)(1-x^2)^{\frac{m-2}{2}} & I_m\ (m:\text{even}) & \\
(1-x)^{m-3}(1-x^2) & I_b^*\ (m=b+5) & \\
(1-x^2) & IV\ (m=3) & \\
(1-x)^2(1-x^2)^2 & IV^*\ (m=7) & \\
(1-x)(1-x^3) & I_0^*\ (m=5) & e=3
\end{array} \tag{2.13}
$$

Proof of Lemma 6. By an easy argument (linear algebra), we can reduce the proof to the case $d=1$. Assume $d=1$ (i.e. $v \in C(k_0)$) so that $\mathbf{F}_v = k_0$. Then the first assertion is obvious because then the Frobenius endomorphism φ acts by multiplication by q on T_v. To see the other assertion, recall that the dual graph of a singular fibre (vertices correspond to $m-1$ irreducible components) is a Dynkin diagram of type A_{m-1}, D_{m-1} or E_{m-1}. The Galois group G induces a cyclic automorphism group of this graph, which can be nontrivial only for type A, D or E_6 (cf. [B, Ch.6]), i.e., only for the singular fibre of type I_m, I_b^* or IV^* $(e=2)$ or I_0^* $(e=3)$. If the number of the vertices fixed by G is a, then the characteristic polynomial is equal to $(1-x)^a(1-x^e)^b$ where $b=(m-1-a)/e$. Then, checking case by case, we can verify the above formulas. *q.e.d.*

Proof of Lemma 5. In case $f^{-1}(v)$ is smooth (an elliptic curve), this is well-known. Assume that $f^{-1}(v)$ is a singular fibre. By using Lemma 6, we can assume that v has degree 1 (replace $\mathbf{F}_v$ by k_0 and q_v by q). Let D denote the support of $f^{-1}(v)$ and $\tilde{D}$ its normalization. The latter is a disjoint union of m smooth rational curves, of which $a+1$ are rational over k_0 and the rest are rational over k_1, grouped into e curves conjugate over k_0. (We use the same notation as above.) Therefore we have (cf. (2.6))

$$\zeta(f^{-1}(v)/k_0, s) = \zeta(\mathbf{P}^1/k_0, s)^{a+1}\zeta(\mathbf{P}^1/k_1, es)^b(1-u)^n(1-u^e)^{n'}$$

where n (or n') is the number of closed points of degree 1 (or e) on $\tilde{D}$ which are mapped to singular points of D minus the number of singular closed points of degree 1 (or e) on D. It is easy to count these numbers using the classification of singular fibres, and we can verify the required formula (2.8) by noting that the sign $\epsilon_v = -1$ occurs precisely when we have either $I_m(m>1), e=2$ or I_1 (a rational curve with a node) having irrational tangent lines at the node. *q.e.d.*

This completes the proof of Theorem 4.

Theorem 7 *The L-function of E/K_0 is the product of the characteristic polynomials of σ^{-1} (the geometric Frobenius) on the Mordell-Weil group $E(K)$ and on the space of transcendental cycles* $\mathrm{Trans}(S)$*:*

$$L(E/K_0, s) = \det(1 - x\sigma^{-1} \mid E(K) \otimes \mathbf{Q}) \det(1 - x\sigma^{-1} \mid \mathrm{Trans}(S)). \tag{2.14}$$

The first factor is a polynomial of degree $r = \mathrm{rk}\, E(K)$ in x which is a product of cyclotomic polynomials and whose order of zero at $x = 1$ is equal to the Mordell-Weil rank $r_0 := \mathrm{rk}\, E(K_0)$.

Proof. The first assertion follows from Theorem 4 in view of (1.5) and (1.8). As for the second, let $k_1 \supset k_0$ be the smallest extension such that $E(K) = E(k_1(C))$ (the "splitting field" of $E(K)$). Then the action of $G = \mathrm{Gal}(k/k_0)$ on $E(K)$ factors through the finite cyclic group $\mathrm{Gal}(k_1/k_0)$. Hence the action of σ on $E(K) \otimes \mathbf{C}$ is diagonalizable, and the multiplicity of the eigenvalue 1 is precisely the rank of $E(K_0) = E(K)^G$.

Remark. From the above, one can easily deduce the equivalence of the Birch-Swinnerton-Dyer conjecture for E/K_0:

$$\mathrm{ord}_{s=1} L(E/K_0, s) = r_0 \tag{2.15}$$

and the Tate conjecture for S/k_0:

$$\mathrm{ord}_{u=1/q} P_2(u) = \rho_0 := \mathrm{rk} N_0, \tag{2.16}$$

where we denote by

$$N_0 := \mathrm{NS}(S/k_0) = \mathrm{NS}(S)^G$$

the subgroup of $\mathrm{NS}(S)$ generated by k_0-rational divisors. Indeed, both are equivalent to asserting that the second factor in (2.14) has no zero at $x = 1$, i.e., to the claim $\mathrm{Trans}(S)^G = 0$.

Furthermore the other part of the Birch-Swinnerton-Dyer conjecture involving the Shafarevich-Tate group is equivalent to the Artin-Tate formula for S/k_0 involving the Brauer group, i.e., the statement (d) of [T2] is true in the present case. In fact, in view of Theorem 3.1 in [T2] saying that

$$Ш(E/K_0) \simeq \mathrm{Br}(S/k_0), \tag{2.17}$$

the equivalence reduces to verifying the equality (cf. [T2,(4.4)])

$$\det \mathrm{NS}(S) = \frac{\det(E(K)/(tor))}{[E(K)_{tor}]^2} \det T. \tag{2.18}$$

This can be seen easily from the formalism of Mordell-Weil lattices based on a new definition of the height pairing on $E(K)$ (cf. [S4]).

Finally it is known that the Artin-Tate formula is true provided the Tate conjecture (2.16) holds (see [T2, Th.5.2], [Milne]). Noting that $\mathrm{NS}(S)$ is torsionfree (cf. [S4]), we can state the result as follows:

Theorem 8 *Assume that (2.15) or (2.16) is true and write* $L(E/K_0, s) = (1-x)^{r_0}h(x)$. *Then the value* $h(1)$ *is given by*

$$h(1) = \frac{[\mathrm{Br}(S/k_0)]\det\ \mathrm{NS}(S/k_0)}{q^{\alpha(S)}} \tag{2.19}$$

or, equivalently,

$$h(1) = \frac{[Ш(E/K_0)]\det(E(K_0)/(tor))}{q^{\alpha(S)}[E(K_0)_{tor}]^2}\det T_0\ \ (T_0 = T^G) \tag{2.20}$$

where $\alpha(S) = \chi - 1 + g$, χ *being the arithmetic genus of* S.

3 Supersingular case

A surface S over k is called *supersingular* if

$$\mathrm{Trans}(S) = 0 \tag{3.1}$$

or equivalently if $\lambda = 0$ or $\rho = b_2$. For example, rational surfaces and more generally unirational surfaces are known to be supersingular ([S2, Lem.2]).

(N.B. This notion has nothing to do with that of a "supersingular" elliptic curve.)

Keeping the same notation as before, we first note:

Proposition 9 *Given an elliptic curve* E/K_0, *the L-function is trivial:*

$$L(E/K_0, s) = 1$$

if and only if the associated elliptic surface S *is supersingular and the Mordell-Weil group* $E(K)$ *is finite.*

Proof. By Theorem 4, the L-function is trivial if and only if W is a vector space of dimension 0. By Proposition 1, $w = 0$ is equivalent to $r = 0$ and $\lambda = 0$. *q.e.d.*

(Note that the above condition is a "geometric" one: both S and K are considered over the algebraically closed field k.)

Theorem 10 *For an elliptic curve E/K_0 such that the associated elliptic surface S is supersingular, the L-function $L(E/K_0, s)$ is equal to the characteristic polynomial of the geometric Frobenius on $E(K)/(tor)$, which is a polynomial in $x = q^{1-s}$ of degree $r = \mathrm{rk}\, E(K)$ of the form*

$$L(E/K_0, s) = (1-x)^{r_0} h(x), \quad h(1) \neq 0 \tag{3.2}$$

where $r_0 = \mathrm{rk}\, E(K_0)$ and $h(x)$ is a product of cyclotomic polynomials. The rank r is equal to w given by (1.10) or (1.11), and $h(1)$ satisfies the formula (2.20).

This is obvious from Proposition 1 and Theorems 7, 8.

Thus the Birch-Swinnerton-Dyer conjecture and the Tate conjecture are true for this class of elliptic curves E/K_0 and elliptic surfaces S/k_0. Also it is evident from (3.2) that the sign of the functional equation of the L-function is $(-1)^{r_0}$.

The above theorem applies for instance to unirational (in particular, rational) elliptic surfaces.

Example 1 Consider the elliptic curve

$$E : Y^2 = X^3 + t^m + 1 \tag{3.3}$$

over $K_0 = k_0(t), k_0 = \mathbf{F}_q$, m being a natural number not divisible by $p = \mathrm{char}(k_0)$. Assume for simplicity that $m \equiv 0 \pmod 6$. Then the elliptic surface S has no reducible fibre so that $\mathrm{rk}\, T = 2, \det T = 1$. In this case, we have

$$w = r + \lambda = 2m - 4 \tag{3.4}$$

(cf. [S5, Prop.3.4]).

Now S is unirational (hence supersingular) if $p^e \equiv -1 \pmod m$ for some $e > 0$ (Prop.4.1, *loc.cit.*). Take $q = p^{2e}$. Then we have $E(K) = E(K_0)$ is of rank $r = 2m - 4$ and torsionfree. By (2.20), we have

$$[Ш(E/K_0)] \det(E(K_0)) = (p^e)^{2p_g}, \tag{3.5}$$

since $\alpha(S) = p_g$. This fact was used in Remark 4.5 of [S5].

In general, it is hard to separate the first factor from the second one (called the regulator), but in this case it can be achieved by means of a crystalline method; see Proposition 4.3, *loc.cit.*.

Remark. In characteristic 0, we can show that the rank of the elliptic curve (3.3) over $\mathbf{C}(t)$ for any m is universally bounded by 68 and that the rank is equal to 68 if m is a multiple of 360. As far as we know, this is the largest rank of an elliptic curve over $\mathbf{C}(t)$ at the moment.

Also, in characteristic $p > 0$ not satisfying the condition $p^e \equiv -1 \pmod{m}$, the surface S is not supersingular in general; for example, for p ordinary (i.e. $p \equiv 1 \pmod{m}$), the rank has the same bound as in characteristic 0.

In any case, the L-function of (3.3) can be expressed in terms of certain Jacobi sums. We hope to discuss these elsewhere.

4 Rational elliptic surfaces

Suppose that S is a rational elliptic surface over k. This means that the function field $k(S)$ of S is a purely transcendental extension of dimension 2 over k. Then $K = k(C)$ is also purely transcendental over k, i.e. $K = k(t)$ (a rational function field) and $g = 0$. Further we have $\rho = b_2 = 10$ and $\lambda = 0$ so that S is supersingular. In the statement of Theorem 10, the formula (2.20) reduces to

$$\frac{[Ш(E/K_0)]\det(E(K_0)/(tor))}{[E(K_0)_{tor}]^2} = \frac{h(1)}{\det T_0} \tag{4.1}$$

since $\alpha(S) = p_g = 0$ for a rational elliptic surface S .

On the other hand, by (1.10), we have

$$r = 8 - \sum_v \deg(v)(m_v - 1) \leq 8. \tag{4.2}$$

The structure of $E(K)$ is well understood by the theory of Mordell-Weil lattices (cf. [S4], [OS]). It is especially interesting for relatively large r. For $r = 8, 7$ or 6, it is isomorphic to E_8, E_7^* or E_6^* or D_6^*, where E_r and D_r are the root lattices and $*$ indicates the dual lattices.

The Galois group of k/k_0 preserves the lattice structure in general. Hence, by Theorem 8, the L-function $L(E/k_0(t), s)$ is equal to the characteristic polynomial of some automorphism of these lattices (in fact, of some element in the Weyl group $W(E_r)$, etc.), and it is a product of some cyclotomic polynomials. Can we determine them more explicitly?

Yes! It can be done with the aid of "algebraic equations arising from Mordell-Weil lattices" (cf. [S6], [S7]). Here are some examples.

Example 2 Let us consider the elliptic curve E defined by

$$Y^2 = X^3 + (1 + t^2)X + (1 + t + t^2 + t^4) \tag{4.3}$$

over $K_0 = \mathbf{F}_p(t)$. We have studied this curve over $\mathbf{Q}(t)$ in [S7, Ex.7.4]) and the information below has been obtained in the course of it. The Mordell-Weil group $E(k(t))$ (k:algebraic closure of $\mathbf{F}_p$) is of rank 6 and isomorphic to E_6^* for any $p \neq 2$, 137, 15784603.

In the following table, we determine the L-function $L(E/\mathbf{F}_p(t), s)$ as a product of cyclotomic polynomials in $x = p^{1-s}$ for $2 < p < 137$. We denote by h_n the n-th cyclotomic polynomial; thus

$$h_2 = 1 + x, h_3 = 1 + x + x^2, \ldots, h_9 = 1 + x^3 + x^6, \ldots$$

p	L-function	cycle type	M_1	No.
3,29,41,67,97	h_9	$(9)^3$		14
5,11,23,37,71,73	$(1-x)^2h_5$	$(1)^2(5)^5$		15
7,127	$(1-x)h_2h_3h_6$	$(3)(6)^4$	+1	23
13	$(1-x)^3h_2h_4$	$(1)^5(2)(4)^5$		18
17,61,79	h_3h_{12}	$(3)(12)^2$		13
19,103,109	$(1-x)h_2h_5$	$(2)(5)^3(10)$		25
31	$(1-x)h_2^3h_4$	$(1)(2)^3(4)^5$	-1	19
43,47	$(1-x)h_2h_4h_6$	$(1)(4)^2(6)(12)$		24
53,89	$(1-x)h_2h_8$	$(1)(2)(8)^3$		20
59	$h_2^2h_3h_6$	$(3)(6)^4$	-1	10
83	$(1-x)^2h_2^2h_4$	$(1)(2)^3(4)^5$	+1	5
101	$(1-x)^4h_2^2$	$(1)^7(2)^9$		2
107	$(1-x)^2h_2^2h_6$	$(1)^3(2)^3(6)^3$	+1	7
113	$(1-x)h_2h_3^2$	$(3)^5(6)^2$		22
131	$(1-x)^2h_2^2h_3$	$(1)(2)^4(3)^2(6)^2$		8

To verify this table, we need to determine the Frobenius element σ_p in the Weyl group $W(E_6)$, up to conjugation.

This group, say G, acts naturally on the dual lattice E_6^*, hence on the set of 54 minimal vectors, forming two orbits of 27 elements. In this way, G embeds into the symmetric group S_{27}. It is known that G has 25 conjugacy classes, and they are determined by the cycle type of an element $g \in G$ viewed as an element of S_{27}, plus the knowledge of $tr(g)$ (trace of g on E_6) (in case the cycle type does not uniquely determine the class); see [Sw, Table 1]. In the above table, the 3rd column gives the cycle type of σ_p, the 4th the value of $M_1 = tr(\sigma_p) + 1$ (when necessary) and the 5th the numbering of conjugacy

classes following Swinnerton-Dyer. The characteristic roots for each conjugacy class can be found in his table (*loc.cit.*).

On the other hand, we have an algebraic equation of degree 27 whose roots describe the minimal vectors of $E(K) \simeq E_6^*$, which in the case under consideration is given by Eq. (7.3) of [S7]:

$$F(X) = X^{27} + 12X^{25} + 60X^{23} + \cdots + 5888X - 4096. \tag{4.4}$$

For each p, decomposing $F(X) \bmod p$ into irreducible factors, we get the cycle type of σ_p; for instance, for $p = 3$, $F(X) \bmod p$ splits into a product of 3 irreducible polynomials of degree 9; we denote the corresponding cycle type by $(9)^3$, and similarly for other cases. Further M_1 can be computed by counting the number a_p of $\mathbf{F}_p$-rational points of the surface S:

$$tr(\sigma_p) = (p^2 + 4p + 1 - a_p)/p. \tag{4.5}$$

Once the conjugacy class is determined, we can apply the result of Swinnerton-Dyer to get the characteristic polynomial. In this way, we can verify the table.

Let us derive some consequence from the above table. First observe that the formula (4.1) becomes

$$[Ш(E/K_0)] \det(E(K_0)) = \frac{h(1)}{3} \tag{4.6}$$

since $\det T_0 = \det T = 3$ and $E(K)$ is torsionfree in our case. Also note that $3\det(E(K_0))$ is an integer (=$\det N_0$).

Now, for $p = 3, 29, 41, \cdots$, we have $r_0 = 0$ and $h(1) = 3$. Thus the Mordell-Weil group $E(\mathbf{F}_p(t))$ is trivial. Further, using the general fact that the order of Ш is a square or twice a square (cf. [T2]), we conclude that the Shafarevich-Tate group is also trivial:

$$Ш(E/\mathbf{F}_p(t)) = 0.$$

Also we can see that $N_0 = \mathrm{NS}(S/k_0)$ is an indefinite lattice of rank 4 with $\det = 3$.

Similarly, for $p = 5, 11, 23, \cdots$, we have $r_0 = 2$ and $h(1) = 5$. By the same argument as above, we see

$$Ш(E/\mathbf{F}_p(t)) = 0, \quad \det(E(\mathbf{F}_p(t))) = \frac{5}{3}.$$

We can also give generators of the Mordell-Weil group $E(\mathbf{F}_p(t))$ explicitly. Namely, in this case, the algebraic equation (4.4) has exactly 2 roots in $\mathbf{F}_p$

(look at the cycle type). For example, for $p = 5$, they are given by $X = -1, -2 \bmod p$; by the theory of Mordell-Weil lattices of type E_6 (cf. [S7], [S6]), we see that there are 2 rational points A, B in $E(\mathbf{F}_p(t))$ of the form

$$A = (-t + b, t^2 + dt + e), B = (-2t + b', t^2 + d't + e').$$

To show that these points generate the full Mordell-Weil group $E(\mathbf{F}_p(t))$, we have only to check the Gram matrix to be

$$\begin{pmatrix} < A, A > & < A, B > \\ < A, B > & < B, B > \end{pmatrix} = \begin{pmatrix} 4/3 & -1/3 \\ -1/3 & 4/3 \end{pmatrix},$$

which is an easy exercise in computing the height pairing (cf. [S4]).

In my original plan, this paper should also have included some other type of examples (not necessarily supersingular), for instance, those related to elliptic modular surfaces or to Jacobi sums. Because of space and time limitation, however, I hope to treat them in some other occasion.

References

[B] Bourbaki, N.: Groupes et Algèbres de Lie, Chap. 4,5 et 6, Hermann, Paris (1968).

[CS] Conway, J., Sloane, N.: Sphere Packings, Lattices and Groups, Springer-Verlag (1988).

[E] Elkies, N.: On Mordell-Weil lattices, Arbeitstagung Bonn (1990).

[G] Gordon, W.J.: Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer, Compos. Math. 38, 163-199(1979).

[I] Igusa, J.: Betti and Picard numbers of abstract algebraic surfaces, Proc. N.A.S. 46, 724-726(1960).

[K] Kodaira, K.: On compact analytic surfaces II-III, Ann. of Math. 77, 563-626(1963); 78, 1-40(1963); Collected Works, III, 1269-1372, Iwamami and Princeton Univ. Press (1975).

[Mc] McGuinness, O.: The explicit formula for elliptic curves over function fields, Appendix to A. Brumer, Preprint.

[Mi] Milne, J.: On a conjecture of Artin and Tate, Ann. of Math.102, 517-533(1975).

[N] Néron, A. : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. IHES **21** (1964).

[Oe] Oesterlé, J.: Empilements de sphères, Sém. Bourbaki 1990, $n^0$727.

[Ogg] Ogg, A.P.: Elliptic curves and wild ramification, Am. J. Math. 89, 1-21(1967).

[Ogu] Oguiso, K.: An elementary proof of the topological Euler characteristic formula for an elliptic surface, Comment. Math. Univ. St. Pauli 39, 81-86(1990).

[OS] Oguiso, K., Shioda, T.: The Mordell-Weil lattice of a rational elliptic surface, Comment. Math. Univ. St. Pauli 40, 83-99(1991).

[R] Raynaud, M.: Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, Sém. Bourbaki 1964/65, $n^0$286; In: Dix Exposés ..., 12-30(1968).

[Sa] Saito, T.: Conductor, discriminant, and the Noether formula of arithmetic surfaces, Duke Math. J. 57, 151-173(1988).

[Se1] Serre, J-P.: Zeta and L functions, In: Arithmetical Algebraic Geometry, Harper and Row, New York, 93-110 (1965); Collected Papers, II, 249-259.

[Se2] — : Facteurs locaux des fonctions zêta des variétés algébriques, Sém. DPP 1969/70 $n^0$19; Collected Papers, II, 581-592.

[S1] Shioda, T.: On elliptic modular surfaces, J. Math. Soc. Japan 24, 20-59(1972).

[S2] — : An example of unirational surfaces in characteristic p, Math. Ann. 211, 233-236(1974).

[S3] — : Mordell-Weil lattices and Galois representation, I,II,III. Proc. Japan Acad. **65A**, 268-271; 296-299; 300-303 (1989).

[S4] — : On the Mordell-Weil lattices, Comment. Math. Univ. St. Pauli 39, 211- 240(1990).

[S5] — : Mordell-Weil lattices and sphere packings, Am. J. Math. 113, 931-948(1991).

[S6] — : Construction of elliptic curves with high rank via the invariants of the Weyl groups, J. Math. Soc. Japan 43, 673-719 (1991).

[S7] — : Theory of Mordell-Weil lattices, Proc. ICM Kyoto 1990, Springer, vol.I, 473-489 (1991).

[Sw] Swinnerton-Dyer, H.P.F.: The zeta function of a cubic surface over a finite field, Proc.Cambridge Phil.Soc. 63, 55-71(1967).

[Sz] Szpiro, L.: Discriminant et conducteur des courbes elliptiques, Astérisque 183, 7-18(1990).

[T1] Tate, J.: Algebraic cycles and the pole of zeta functions, In: Arithmetical Algebraic Geometry, 93-110, Harper and Row, New York (1965).

[T2] — : On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki 1965/66, $n^0$306.; In: Dix Exposés ..., 189-214(1968).

[T3] — : Algorithm for determining the type of a singular fiber in an elliptic pencil, LNM 476, 33-52(1975).

[W] Weil, A. : Collected Papers I, II, III, Springer-Verlag (1980).

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171
Japan

Astérisque

YVETTE AMICE
BRUNO KAHN

Sommes de puissances dans les corps finis

Astérisque, tome 209 (1992), p. 115-135
<http://www.numdam.org/item?id=AST_1992__209__115_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Sommes de puissances dans les corps finis

Yvette Amice et Bruno Kahn

Introduction

Soit F un corps fini à q éléments, où q est une puissance d'un nombre premier impair. On note $s(q)$ le plus petit entier s tel que -1 soit somme de s éléments de F* d'ordre (multiplicatif) impair. L'étude de cet entier est motivée par celle des "niveaux supérieurs" d'un corps (§1).

Le but de cet article est de présenter et de commenter le calcul de $s(q)$ pour q premier $< 10^9$ et $q = p^3$ avec p premier $\leq 101\ 711\ 783$ (pour $q = p^n$ avec p premier et $n \neq 1, 3$, on a $s(q) = 2$, *cf* prop. 1, 4)). L'intérêt principal de cette présentation est que les résultats obtenus offrent des caractéristiques inattendues à plusieurs égards. Pour résumer ces caractéristiques, on peut dire qu'en général $s(q)$ est "plus petit" qu'on ne pourrait s'y attendre.

Le paragraphe 1 rappelle la définition des niveaux supérieurs d'un anneau. Les paragraphes 2 et 3 donnent des résultats généraux sur l'entier $s(q)$, notamment les majorations qui ont été utilisées dans les calculs. Le paragraphe 4 décrit les résultats obtenus, et en particulier une série de "phénomènes inexpliqués". Le paragraphe 5 donne quelques questions ouvertes. Enfin, une annexe contient 10 tables extraites de nos calculs, qui illustrent les descriptions données au paragraphe 4.

1. Niveaux supérieurs d'un anneau

Soit A un anneau commutatif de caractéristique différente de 2. Pour tout entier $r \geq 1$, on notera suivant Revoy [R] $s_r(A)$ le plus petit entier s tel que l'équation $-1 = x_1^{2^r} + \ldots + x_s^{2^r}$ ait une solution dans A (ou ∞ si un tel entier n'existe pas). Ainsi, si A est un corps F, $s_1(F)$ n'est autre que le niveau de F étudié notamment par Pfister ([P1], [P2]); $s_2(F)$ a été étudié entre autres dans [PAR1], [PAR2]. Les nombres $s_r(A)$ ont les propriétés évidentes suivantes:

(A) Si A→A' est un homomorphisme d'anneaux, $s_r(A) \geq s_r(A')$.

(B) Si ℓ est un nombre premier impair tel que A contienne une racine primitive ℓ–ième de l'unité ζ telle que $\zeta-1$ ne soit pas diviseur de zéro, on a $s_r(A) \leq \ell-1$ pour tout $r \geq 1$ ([R], prop. 1.6).

L'étude des $s_r(F)$ pour les corps finis est intéressante, d'un part en soi, d'autre part pour les informations qu'elle donne sur les s_r des corps de nombres ([PAR1], [PAR2], [R]).

2. Cas des corps finis: résultats "théoriques"

Supposons que F soit un corps fini à q éléments (q impair); soit $h = h(q)$ le plus grand entier tel que 2^h divise $q-1$. On a alors ([R], th. 2.2):

a) $s_r(F) = 1$ si $r < h$;

b) $1 < s_h(F) = s_r(F) \leq 2^h$ si $r \geq h$.

On note $s(F)$, ou simplement $s(q)$, l'entier $s_h(F)$. Pour un entier s, les conditions suivantes sont équivalentes:

(i) $s \geq s(q)$;

(ii) -1 est somme de s éléments de F, nuls ou d'ordre (multiplicatif) impair;

(iii) l'hypersurface projective d'équation $X_0^{2^h}+\ldots+X_s^{2^h} = 0$ a un point F–rationnel.

La proposition suivante donne quelques renseignements sur le comportement de $s(q)$ en fonction de q. Soit p la caractéristique de F, de sorte que q est une puissance de p.

|| **Proposition 1.** 1) *Si* $\frac{\sqrt{q}^n-\sqrt{q}^{-n}}{\sqrt{q}-\sqrt{q}^{-1}} > (1-2^{-h})[(2^h-1)^n-(-1)^n]$, *on a* $s(q) \leq n$; *en particulier, si* $q \geq 2^{2nh/(n-1)}$, *on a* $s(q) \leq n$.

2) *Si* $q \geq (2^h-1)^2(2^h-2)^2$, *on a* $s(q) = 2$.

3) *Si* $q \geq (2^h-1)(2^{2h}-3\cdot 2^h+3)$, *on a* $s(q) \leq 3$.

4) *Si q n'est pas de la forme p ou* p^3, *on a* $s(q) = 2$.

5) *Si* $q = p^3$, on a $s(q) \leq 3$. *On a* $s(q) = 2$, *sauf peut-être si* $s(p) > 2$ *et* $p < 2^{4h/3}$.

6) *Si p est un nombre premier de Fermat, on a* $s(p) = p-1$.

Démonstration. 6) est évident (*cf* [R], 2.4), et 2) et 3) sont des cas particuliers de 1) (pour 2), *cf* [R] , dém. du lemme 2.3). Supposons $q = p^n$. Si n

est pair, $q-1$ est divisible par 3 donc $s(q) \leq 2$ d'après la propriété (B) rappelée ci-dessus, d'où $s(q) = 2$. Si n est impair, on a $h(q) = h(p)$; si $n \geq 5$, on a donc $q \geq p^5 \geq 2^{5h} \geq 2^{4h}$, d'où $s(q) = 2$ d'après 1); cela démontre 4). En notant que de même 5) est conséquence de 1), il reste à démontrer 1). Pour cela, on minore le nombre de points rationnels de l'hypersurface projective $X_0{}^{2^h}+\ldots+X_n{}^{2^h} = 0$. Une telle minoration peut bien sûr se déduire des conjectures de Weil démontrées par Deligne, mais on peut aussi procéder directement au moyen de sommes de Jacobi généralisées, en reprenant les arguments de Weil, *cf* [L], *pp.* 22–24. Plus généralement, soient d un diviseur de $q-1$ et Y_n l'hypersurface *affine* d'équation $X_0{}^d+\ldots+X_n{}^d = 0$. En suivant Lang (*op. cit.*), on voit que le nombre de points F-rationnels de Y_n est:

$$E_n = \sum_{(a_0,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z})^{n+1}} \sum_{u_0+\ldots+u_n=0} \chi^{a_0}(u_0)\ldots\chi^{a_n}(u_n),$$

où χ est un caractère multiplicatif fixé, d'ordre d. En transformant cette équation comme dans [L] (*loc. cit.*), on trouve:

$$E_n = q^n-(q-1) \sum_{\substack{(a_1,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z}-\{0\})^n \\ a_1+\ldots+a_n\neq 0}} \chi^{a_1+\ldots+a_n}(-1)\, J(\chi^{a_1},\ldots,\chi^{a_n}),$$

où $J(\chi_1,\ldots,\chi_n) = -\sum_{x_1+\ldots+x_n=1} \chi_1(x_1)\ldots\chi_n(x_n)$ est une somme de Jacobi généralisée. Le nombre de points $\overline{E}_n = \dfrac{E_n-1}{q-1}$ de l'hypersurface *projective* est donc:

$$\overline{E}_n = \frac{q^n-1}{q-1} - \sum_{\substack{(a_1,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z}-\{0\})^n \\ a_1+\ldots+a_n\neq 0}} \chi^{a_1+\ldots+a_n}(-1)\, J(\chi^{a_1},\ldots,\chi^{a_n}).$$

Lorsque $\chi_1\ldots\chi_n \neq 1$, on peut écrire $J(\chi_1,\ldots,\chi_n) = \dfrac{S(\chi_1)\ldots S(\chi_n)}{S(\chi_1\ldots\chi_n)}$, où $S(\chi) = \sum_a \chi(a)\lambda(a)$ est la somme de Gauss relative à un caractère additif λ fixé (*cf* [L], *p.* 4). Comme $|S(\chi)| = q^{1/2}$ pour $\chi \neq 1$, cela donne $|J(\chi_1,\ldots,\chi_n)| = q^{\frac{n-1}{2}}$ si χ_1, ..., χ_n, $\chi_1\ldots\chi_n \neq 1$; d'où l'estimation triviale:

$$|\overline{E}_n - \frac{q^n - 1}{q-1}| \leq q^{\frac{n-1}{2}} c_n,$$

où $c_n = Card\{(a_1,\ldots,a_n) \in (\mathbf{Z}/d\mathbf{Z}-\{0\})^n \mid a_1+\ldots+a_n \neq 0\}$.

On a visiblement $c_n = (d-1)^n - c_{n-1}$, d'où

$$c_n = (d-1)^n - (d-1)^{n-1} + \ldots + (-1)^{n-1}(d-1) = (1-\frac{1}{d})[(d-1)^n - (-1)^n].$$

On en conclut que $\overline{E}_n \neq 0$ dès que

$$\frac{q^n - 1}{q-1} > q^{\frac{n-1}{2}}(1-\frac{1}{d})[(d-1)^n - (-1)^n]$$

soit encore:

$$\frac{\sqrt{q}^n - \sqrt{q}^{-n}}{\sqrt{q} - \sqrt{q}^{-1}} > (1-\frac{1}{d})[(d-1)^n - (-1)^n].$$

Pour $n = 3$ et $d = 2^h$, on trouve le premier énoncé de 1). Finalement, on a $\frac{\sqrt{q}^n - \sqrt{q}^{-n}}{\sqrt{q} - \sqrt{q}^{-1}} > \sqrt{q}^{n-1}$ et $(1-2^{-h})[(2^h-1)^n - (-1)^n] < 2^{nh}$, d'où le deuxième énoncé.

Remarque 2.1. On notera que l'estimation de la prop. 1,1) ne donne aucun renseignement tant que $q \leq 2^{2h}$, tandis que le théorème de Chevalley montre que $\overline{E}_n \neq 0$ dès que $n \geq d$.

|| **Corollaire.** *Si n est une puissance de 2, la surface projective d'équation $x_0^n + x_1^n + x_2^n + x_3^n = 0$ a un point rationnel sur tout corps fini non premier.*

Démonstration. Cela résulte de *a*) et *b*) (début de la section) et de la prop. 1, 4) et 5).

Remarque 2.2. Nous baptiserons les inégalités de la prop. 1,1) *majorations de Jacobi-Weil.*

3. Une estimation modulaire

En reprenant la méthode de démonstration du théorème de Chevalley dans les corps finis ([CA], ch. 1), on obtient une formule pour la valeur modulo p du nombre de solutions de l'équation $x^{2^h} + y^{2^h} = -1$. On pourrait en principe l'utiliser pour tester si $s(p^3) = 2$. Toutefois, cette formule est une somme de

$(2^h-1)(2^{h-1}-1)$ termes, ce qui en pratique donne un temps de calcul bien trop long lorsque h devient grand: elle est donc peu intéressante en pratique, à moins qu'on n'arrive à la simplifier encore.

II **Proposition 2.** *Le nombre* N *de solutions dans* $\mathbf{F}_{q^2}$ *de l'équation* $x^{2^h}+y^{2^h} = -1$ *est congru modulo* p *à* $1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \left(\begin{smallmatrix} bi \\ bj \end{smallmatrix}\right)$, *où* $b = (q-1)/2^h$. *Si* $q = p^m$, *avec* m *impair, on a*

$$N \equiv 1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \left(\begin{smallmatrix} b_0 i \\ b_0 j \end{smallmatrix} \right)^m \pmod p,$$

où $b_0 = (p-1)/2^h$.

Démonstration. Soient $F(x,y) = x^{2^h}+y^{2^h}+1$ et $G(x,y) = 1-F(x,y)^{q-1}$. Alors $N \equiv \sum_{x,y \in \mathbf{F}_q} G(x,y)$ [CA], soit:

$$\begin{aligned} N &\equiv - \sum_{x,y \in \mathbf{F}_q} (x^{2^h}+y^{2^h}+1)^{q-1} \\ &\equiv - \sum_{x,y \in \mathbf{F}_q} \sum_{k=0}^{q-1} (-1)^k (x^{2^h}+y^{2^h})^k \\ &\equiv - \sum_{x,y \in \mathbf{F}_q} \sum_{k=0}^{q-1} (-1)^k \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) x^{2^h l} y^{2^h (k-l)} \\ &\equiv \sum_{k=0}^{q-1} (-1)^{k+1} \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) \sum_{x,y \in \mathbf{F}_q} x^{2^h l} y^{2^h (k-l)} \\ &\equiv \sum_{k=0}^{q-1} (-1)^{k+1} \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) \sum_{x \in \mathbf{F}_q} x^{2^h l} . \sum_{y \in \mathbf{F}_q} y^{2^h (k-l)} \pmod p. \end{aligned}$$

La somme $\sum_{x \in \mathbf{F}_q} x^{2^h l}$ (*resp.* $\sum_{y \in \mathbf{F}_q} y^{2^h (k-l)}$) est nulle, sauf si $2^h l \equiv 0 \pmod{q-1}$ et $2^h l > 0$ (*resp.* $2^h(k-l) \equiv 0 \pmod{q-1}$ et $2^h(k-l) > 0$), c'est-à-dire $l \equiv 0 \pmod b$ et $l > 0$ (*resp.* $k-l \equiv 0 \pmod b$ et $k-l > 0$); dans ce cas, elle vaut -1. Comme b est impair, on obtient donc:

$$N \equiv \sum_{i=2}^{2^h} (-1)^{bi+1} \sum_{j=1}^{i-1} \binom{bi}{bj} \equiv \sum_{i=2}^{2^h} (-1)^{i+1} \sum_{j=1}^{i-1} \binom{bi}{bj}.$$

Pour $i = 2^h$, on a $bi = q-1$, donc $\binom{bi}{bj} \equiv (-1)^{bj} \equiv (-1)^j \pmod p$, d'où

$$N \equiv 1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \binom{bi}{bj} \pmod p.$$

Supposons maintenant $q = p^m$, avec m impair. Soient $l \le k < q$: écrivons $k = k_0 + k_1 p + \ldots + k_{m-1} p^{m-1}$ et $l = l_0 + l_1 p + \ldots + l_{m-1} p^{m-1}$, avec $0 \le k_i$, $l_i \le p-1$. On a alors:

$$\binom{k}{l} \equiv \prod_{i=0}^{m-1} \binom{k_i}{l_i} \pmod p;$$

cela résulte de l'identité $(X+Y)^k \equiv \prod_{i=0}^{m-1} (X^{p^i}+Y^{p^i})^{k_i} \pmod p$. On a $b = b_0(1+p+\ldots+p^{m-1})$, donc $ib = ib_0(1+p+\ldots+p^{m-1})$, avec $ib_0 \le p-1$ si $i \le 2^h$. Par conséquent, pour $0 \le j \le i \le 2^h$, on a:

$$\binom{bi}{bj} \equiv \binom{b_0 i}{b_0 j}^m \pmod p.$$

On en déduit l'énoncé.

|| **Corollaire.** *Supposons $q = p^m$, avec m impair. Si* $\sum_{i=2}^{2^h-1} (-1)^i \sum_{j=1}^{i-1} \binom{b_0 i}{b_0 j}^m \not\equiv 1 \pmod p$, *on a $s(q) = 2$.*

4. Cas des corps finis: résultats "expérimentaux"

Nous avons calculé la valeur de $s(p)$ pour tout $p < 10^9$, et celle de $s(p^3)$ pour tout $p < 104\,857\,601$. Ces calculs ont été réalisés sur un Macintosh II à l'aide d'un programme de Lightspeed Pascal et de la bibliothèque multiprécision de Dominique Bernardi. On retrouve ainsi comme cas particuliers les résultats de [PAR1], [PAR2], [PR] et [R] concernant les corps finis.

Les résultats complets, sous forme papier (129 pages) ou informatique, sont disponibles auprès des auteurs.

Phénomènes inexpliqués

Les données obtenues conduisent à un certain nombre d'observations *a priori* inattendues, auxquelles nous n'avons pas trouvé d'explication.

a) Taille de s

La propriété b) du §1, le théorème de Chevalley et la prop. 1,1) montrent qu'une majoration de s est donnée par

$$s \leq \min(l-1, 2^h),$$

et, si $p \geq 2^{2h}$,

$$(S1)\quad s \leq 1 + \left\lceil \frac{1}{\frac{\log(p)}{2h\log(2)} - 1} \right\rceil,$$

où l est le plus petit facteur premier impair de $p-1$, $h = h(p)$ et, pour tout réel a, $\lceil a \rceil$ désigne le plus petit entier $\geq a$.

En fait, hormis le cas des nombres premiers de Fermat (*cf* prop. 1,6)), les calculs montrent que la valeur réelle de s est nettement inférieure à cette majoration (voir table VIII). Pour tous les $p < 10^9$ on a $s \leq 12$ (Fermat exclus). De plus, les p ayant un grand s sont rares: jusqu'à 500 000 (resp. 10^9) il n'y a que 8 (resp. 61) nombres premiers p tels que $s(p) > 4$ (Fermat exclus).

b) Plus grand p pour lequel s > 2

D'après la prop. 1,1), la majoration de Jacobi-Weil affirme que l'on a $s(p) = 2$ dès que $p \geq 2^{4h(p)}$. Soient, pour tout $h \geq 2$, pour tout $s \geq 2$ et pour tout $t \geq 0$, $p_s(h)$ le plus grand nombre premier tel que $h(p) = h$ et $s(p) > s$ et $p_s(h,t)$ le plus grand nombre premier $\leq t$ tel que $h(p) = h$ et $s(p) > s$. Pour $h \leq 7$ on a $2^{4h} \leq 10^9$, donc $p_2(h,10^9) = p_2(h)$. La liste que nous obtenons est donc complète jusqu'à $h = 7$.

En fait, jusqu'à $h = 12$, le plus grand p trouvé est sensiblement inférieur à 10^9 (voir table I). Il est concevable qu'il existe (pour $8 \leq h \leq 12$) un $p > 10^9$ tel que $s(p) > 2$, mais cela impliquerait une forte irrégularité de la croissance des p (*cf* table VI). Les calculs montrent que, pour $4 \leq h \leq 7$, on a $\log(p_2(h))/h\log(2) \leq 2{,}72$ (pour $h = 3$, on a $\log(p_2(h))/h\log(2) = 3{,}19$).

Pour $h \geq 8$, on trouve encore $\log(p_2(h,10^9))/h\log(2) \leq 2{,}72$ (*cf* table I).

Il est curieux de constater que, pour $4 \leq h \leq 12$, les valeurs de $\log(p_2(h,10^9))/h\log(2)$ sont relativement proches, avec un écart-type de 2,7%; leur valeur moyenne est de 2,57, significativement inférieure à 4 (prédit par Jacobi-Weil).

b) Plus grand p pour lequel $s > 3$

La même étude dans ce cas conduit à des observations analogues (table II). Cette fois, la borne de Jacobi-Weil donne $p_3(h) \leq 2^{3h}$; on en déduit que $p_3(h,10^9) = p_3(h)$ pour $h \leq 9$. Pour $h \leq 9$, on trouve $\log(p_3(h))/h\log(2) \leq 1{,}72$; jusqu'à $h = 14$, on a vraisemblablement encore $p_3(h,10^9) = p_3(h)$. Pour ces valeurs de h, on trouve $\log(p_3(h,10^9))/h\log(2) \leq 1{,}74$. De nouveau, ce majorant est nettement inférieur à celui de Jacobi-Weil (3), et l'écart-type des valeurs de $\log(p_3(h,10^9))/h\log(2)$ est faible (1,62%).

c) Plus grand entier p pour lequel $s > 4$

Dans ce cas, les données sont plus partielles mais conduisent aux mêmes observations (table III). La valeur moyenne de $\log(p_4(h,10^9))/h\log(2)$, pour $h \leq 20$, est de 1,45 (les inégalités de Jacobi-Weil donneraient $8/3 = 2{,}66$).

d) Plus petit p pour lequel $s > 2$

Soit $P(h)$ le plus petit nombre premier p tel que $h(p) = h$ et $s(p) > 2$. Les calculs montrent que, pour $h \leq 25$, on a $(P(h)-1)/2^h \leq 749$; on a même $(P(h)-1)/2^h \leq 43$ pour $h \neq 7, 17$ (table IX). Il y a donc "assez tôt" des nombres premiers tels que $h > 2$. Quel est le comportement de $sup\ \{P(h) \mid h \leq H\}$ lorsque $H \to \infty$?

e) Plus petit p pour lequel $s = 3$

Soit $P'(h)$ le plus petit nombre premier p tel que $h(p) = h$ et $s(p) = 3$. Cette fois-ci, la croissance de $P'(h)$ en fonction de h est beaucoup plus rapide (pour $h \leq 17$); toutefois elle ne semble pas obéir à une règle bien déterminée (table X).

f) Valeur de $s(p^3)$

D'après la prop. 1,5), on a $s(p^3) \leq 3$. En fait, nos calculs montrent que,

jusqu'à $p \leq 101\,711\,873$, on a $s(p^3) = 2$. Plus précisément, il y a 21 nombres premiers $\leq 101\,711\,873$ pour lesquels les majorations de Jacobi-Weil autorisent que $s(p^3) = 3$; pour chacun de ces nombres premiers, on trouve en fait $s(p^3) = 2$. (Cette vérification demande un temps de calcul très long.) On a $2^{4h/3} < 10^9$ jusqu'à $h = 22$; on déduit de ceci et de nos calculs:

II **Proposition 3.** *Pour tout p tel que* $h(p) \leq 20$, *on a* $s(p^3) = 2$.

5. Questions ouvertes

5.1. Existe-t-il un nombre premier p tel que $s(p^3) = 3$? La question opposée est équivalente à la suivante (*cf* cor. à la prop. 1):

Si n est une puissance de 2, est-il vrai que la courbe projective d'équation $x^n+y^n+z^n = 0$ *a un point rationnel sur tout corps fini non premier?*

5.2. Les résultats observés en 3 a), b), c) correspondent-ils à un phénomène général? Plus spécifiquement, est-il vrai en général qu'en général, $c(s) := \inf\{\log(p_s(h))/h\log(2) \mid h > 1\}$ est sensiblement inférieur à $\frac{2s}{s-1}$ (donné par la prop. 1)? Nous pensons que oui, mais ne connaissons pas de motivation "théorique" pour ce phénomène hypothétique, et n'avons pas de conjecture sur la valeur de $c(s)$. Les résultats indiqués ci-dessus laisseraient penser que $c(2) < 2{,}8$, $c(3) < 1{,}8$, $c(4) < 1{,}5$. L'absence apparente de p tels que $s(p^3) = 3$ pourrait être liée à un tel phénomène (s'étendant aux corps finis non premiers).

On peut se demander s'il est même vrai que les majorations de Jacobi-Weil peuvent être améliorées dans le cas particulier des hypersurfaces considérées dans la prop. 1; nous n'avons pas fait de calculs dans ce sens. Une meilleure minoration de E_n (*cf* dém. de la prop. 1) n'est en tout cas pas nécessaire *a priori* pour justifier une meilleure majoration de $c(s)$.

On notera que le théorème de Chevalley apporte une information "arithmétique" que ne donnent pas les estimations "analytiques" à la Jacobi-Weil (*cf* remarque 2.2). Une meilleure majoration de $c(s)$ pourrait peut-être être obtenue à partir des congruences de la prop. 2, mais nous n'avons pas réussi à les exploiter dans ce sens.

5.3 (Revoy). Soit $\lambda(h) = \sup_{h(q)=h} s(q)$. D'après la prop. 1, 1), on a $\lambda(h) < +\infty$ pour tout h. Quel est le comportement de $\lambda(h)$ en fonction de h?

Les premières valeurs de $\lambda(h)$ sont données dans la table VIII (nombres premiers de Fermat exclus). S'il y a une infinité de nombres premiers de Fermat, on a $\lambda(h) = 2^h$ pour une infinité de h (prop. 1, 6)). Mais il est probable que $log\lambda(h) = o(h)$. En effet:

Proposition 4. *Soient* $N \geq 1$, $h \geq 2$ *et* p *un nombre premier tel que* $h(p) = h$. *Supposons que* $s(p) \geq 2^{h/N}$. *Alors:*

1) *Tout facteur premier de* $b = \frac{p-1}{2^h}$ *est* $> 2^{h/N}$.

2) *Soient* n_i *les exposants des facteurs premiers de* b. *Supposons* $\sum n_i > N$. *Alors on a* $2^{h/N}-1 \leq \frac{2}{\frac{\sum n_i}{N}-1}$ *et* $h \leq N\log_2(2N+1)$. *Pour* $N \leq 3$, *on a* $\sum n_i \leq N$.

Démonstration. 1) résulte immédiatement de la propriété (B). Supposons 2) faux. On a alors Supposons $\sum n_i > N$. Alors $log_2 p \leq 2\frac{2^{h/N}}{2^{h/N}-1} h$ (prop. 1, 1)). On a donc:

$$\frac{\sum n_i}{N} + 1 \leq 2\frac{2^{h/N}}{2^{h/N}-1}.$$

On en tire la première inégalité de 2). Pour obtenir la deuxième, on minore $\sum n_i$ par N+1. Finalement, supposons $N \leq 3$. Si $\sum n_i > N$ on a $h \leq N\log_2(2N+1) \leq 9$; pour ces valeurs de h on a $s(p) \leq 6$ (à l'exclusion de nombres de Fermat, *cf* table VIII), d'où $h \leq [3\log_2 6] = 7$. Avec cette nouvelle majoration de h, on a $s(p) \leq 5$ (*ibid.*), d'où $h \leq [3\log_2 5] = 6$. On vérifie directement que, pour $h \leq 6$, $(p-1)/2^h$ possède au plus 3 facteurs premiers, comptés avec multiplicité. (Pour $h \leq 6$, l'unique cas où $(p-1)/2^h$ possède 3 facteurs premiers est $p = 4001$, avec $h = 5$ et $s = 3$. Dans ce cas, on n'a donc pas $s(p) \geq 2^{h/N}$.)

Lorsque h est assez grand, le nombre $\frac{p-1}{2^h}$ doit avoir au plus N facteurs premiers (comptés avec multiplicité), tous grands en fonction de h. Il semble peu probable que, N étant fixé, il existe une infinité de h tels qu'un p vérifiant $h(p) = h$ ait cette propriété et vérifie de plus $s(p) \geq 2^{h/N}$.

Une réponse positive à la question 5.2 apporterait sans doute une amélioration importante des résultats de la prop. 4. Par exemple, s'il est vrai que $c(3) < 2$, $s(p) \geq 2^h$ implique $\sum n_i = 0$, *ie* que p est un nombre de Fermat. Si $c(4) < 1{,}5$, $s(p) \geq 2^{h/2}$ implique $\sum n_i \leq 1$. D'autre part, on peut voir que si $\sum n_i = N$, alors au moins un facteur premier de b est $\leq 2^{h/N}+2h\log(2)$. Par le théorème des nombres premiers, l'"espérance mathématique" d'un nombre premier dans l'intervalle $[2^{h/N}, 2^{h/N}+2h\log(2)]$ est 2 pour tout h; ceci laisse à penser que pour h assez grand, $\frac{p-1}{2^h}$ doit en fait avoir au plus N–1 facteurs premiers (comptés avec multiplicité).

5.4 (Revoy). Est-il vrai que $\sup_p s(p) = +\infty$? (De manière équivalente, est-il

vrai que $\lambda(h) \to \infty$, cf question 5.3.)

D'après la prop. 1, 6), cela serait vrai s'il y avait une infinité de nombres premiers de Fermat. On peut espérer que cela ne dépende pas de cette condition (puisqu'on a plutôt tendance à imaginer que les premiers de Fermat sont en nombre fini!). Plus généralement, on peut hasarder la

?? **Conjecture.** *Soient a et b deux entiers premiers entre eux; supposons que l'on n'aie $a \equiv 1 \pmod{l}$ pour aucun facteur premier impair l de b. Alors l'ensemble des $s(p)$, pour $p \equiv a \pmod{b}$, n'est pas borné.*

Dans l'énoncé, la condition sur b est mise pour prendre en considération la propriété (B) du §1. Cette conjecture implique que, si K est un corps quadratique imaginaire différent de $\mathbf{Q}(\sqrt{-3})$ ou un corps abélien de degré impair ne contenant aucune racine de l'unité d'ordre impair > 1, la suite $s_r(K)$ n'est pas bornée. (La condition "de degré impair" sur K est sans doute superflue.)

5.5. Quelle est la taille de $P(h)$ et de $P'(h)$ en général? (*cf* 3 d) et e)).

5.6. Soit $N(h)$ le nombre de p tels que $h(p) = h$ et que $s(p) > 2$; soit $N'(p)$ le nombre de ces p tels que $(p-1)/2^h$ soit premier. Les valeurs de $N(h)$ et $N'(h)$, pour h petit, apparaissent dans la table IV. Quelle est la taille de $N(h)$ et de $N'(h)$ en général, et comment varie la proportion $N'(h)/N(h)$? (L'étude de cette question a été suggérée par Etienne Fouvry.)

Références

[CA] J-P. Serre *Cours d'arithmétique*, P.U.F., Paris, 1970.

[L] S. Lang *Cyclotomic fields*, Graduate texts in Math. **59**, Springer, New York, 1978.

[P1] A. Pfister *Zur Darstellung von -1 als Summe von Quadraten in einem Körper*, J. London Math. Soc **40** (1965), 159-165.

[P2] A. Pfister *Multiplikative quadratische Formen*, Arch. Math. **16** (1965), 363-370.

[PAR1] J.C. Parnami, M.K. Agrawal, A.R. Rajwade, *On the fourth power Stufe of a field*, Rend. del Circ. Matem. di Palermo **30** (1981), 245-254.

[PAR2] J.C. Parnami, M.K. Agrawal, A.R. Rajwade, *On the fourth power Stufe of p-adic completions of algebraic number fields*, Rend. Sem. Mat. Univ. Politecn. Torino **44(1)** (1985), 141-153.

[PR] S. Pall, A.R. Rajwade *Power Stufe of Galois fields*, Bull. Soc. Math. Belg. **35** (1983), 123-130.

[R] P. Revoy *Niveaux supérieurs des corps et des anneaux*, C.R. Acad. Sci. Paris **307** (1988), 203-206.

Annexe: tables

Notations générales:

p: nombre premier
h: valuation dyadique de $p-1$
$s = s(p)$
l: plus petit facteur premier impair de $p-1$
$b = (p-1)/2^h$

I. Plus grandes valeurs de p telles que $s > 2$, pour $h \leq 12$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 4$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$	$\frac{1}{h}\log_2(10^9)$
5	**2**	**4**	**1**	**1,16**	
761	**3**	**3**	**5**	**3,19**	
977	**4**	**3**	**61**	**2,48**	
10 529	**5**	**3**	**7**	**2,67**	
83 009	**6**	**3**	**1297**	**2,72**	
397 697	**7**	**3**	**13**	**2,66**	
1 398 017	8	3	43	2,55	3,74
12 376 577	9	3	23	2,62	3,32
44 858 369	10	3	71	2,54	2,98
140 019 713	11	3	7	2,46	2,71
662 990 849	12	3	13	2,44	2,49

II. Plus grandes valeurs de p telles que $s > 3$, pour $h \leq 17$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 3$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$	$\frac{1}{h}\log_2(10^9)$
5	**2**	**4**	**1**	**1,16**	
41	**3**	**4**	**5**	**1,79**	
113	**4**	**4**	**7**	**1,70**	
353	**5**	**4**	**11**	**1,69**	
1 217	**6**	**4**	**19**	**1,71**	
4 481	**7**	**4**	**5**	**1,73**	
9 473	**8**	**4**	**37**	**1,65**	
45 569	**9**	**4**	**89**	**1,72**	
87 041	10	4	5	1,64	2,99
329 729	11	4	7	1,67	2,72
1 454 081	12	4	5	1,71	2,49
4 513 793	13	4	19	1,70	2,30
21 446 657	14	4	7	1,74	2,13
36 929 537	15	4	7	1,68	1,99
157 745 153	16	4	29	1,70	
410 386 433	17	4	31	1,68	

III. Plus grandes valeurs de p telles que $s > 4$, pour $h \leq 20$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 8/3$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$
449	**6**	**5**	**7**	**1,47**
3 329	**8**	**6**	**13**	**1,46**
13 313	**10**	**8**	**13**	**1,37**
59 393	**11**	**5**	**29**	**1,44**
176 129	12	5	43	1,45
1 073 153	13	5	131	1,54
2 277 377	14	5	139	1,51
4 882 433	15	5	149	1,48
8 716 289	16	5	7	1,44
31 326 209	17	5	239	1,46
64 749 569	18	5	13	1,44
103 284 737	19	5	197	1,40
409 993 217	20	5	17	1,43

IV. Nombre de p tels que $h(p) = h$ et $s(p) > 2$

On note $N(h,x)$ le nombre de $p \leq x$ tels que $h(p) = h$ et $s(p) > 2$, et $N(h) = N(h,\infty)$. Pour $h \leq 7$, on a $N(h,10^9) = N(h)$ par Jacobi-Weil; c'est probablement encore vrai jusqu'à $h = 12$ (cf. tableau I). Pour indiquer ceci, on a écrit $N(h)^*$ à la place de $N(h,10^9)$ pour $8 \leq h \leq 12$.

On note $N'(h,x)$ le nombre de $p \leq x$ tels que $h(p) = h$, $s(p) > 2$ et $(p-1)/2^h$ soit premier, et $N'(h) = N'(h,\infty)$. On a écrit $N'(h)^*$ à la place de $N'(h,10^9)$ pour $8 \leq h \leq 12$.

La fonction $\mathrm{Log}(N(h))/h$ semble croître lentement et irrégulièrement: c'est au moins ce qu'on constate pour $h \leq 12$, avec $\mathrm{Log}(N(h))/h \cong 0,53$.

$h = 2$	$N(h) = 2$	$N'(h) = 2$	$N'(h)/N(h) = 1$
$h = 3$	$N(h) = 5$	$N'(h) = 4$	$N'(h)/N(h) = 0,8$
$h = 4$	$N(h) = 5$	$N'(h) = 3$	$N'(h)/N(h) = 0,6$
$h = 5$	$N(h) = 13$	$N'(h) = 8$	$N'(h)/N(h) = 0,62$
$h = 6$	$N(h) = 23$	$N'(h) = 12$	$N'(h)/N(h) = 0,52$
$h = 7$	$N(h) = 39$	$N'(h) = 16$	$N'(h)/N(h) = 0,41$
$h = 8$	$N(h)^* = 69$	$N'(h)^* = 29$	$N'(h)^*/N(h)^* = 0,42$
$h = 9$	$N(h)^* = 110$	$N'(h)^* = 43$	$N'(h)^*/N(h)^* = 0,39$
$h = 10$	$N(h)^* = 217$	$N'(h)^* = 73$	$N'(h)^*/N(h)^* = 0,34$
$h = 11$	$N(h)^* = 359$	$N'(h)^* = 103$	$N'(h)^*/N(h)^* = 0,29$
$h = 12$	$N(h)^* = 708$	$N'(h)^* = 206$	$N'(h)^*/N(h)^* = 0,29$
$h = 13$	$N(h,10^9) = 1155$		
$h = 14$	$N(h,10^9) = 1163$		
$h = 15$	$N(h,10^9) = 709$		
$h = 16$	$N(h,10^9) = 371$		
$h = 17$	$N(h,10^9) = 171$		
$h = 18$	$N(h,10^9) = 88$		
$h = 19$	$N(h,10^9) = 50$		
$h = 20$	$N(h,10^9) = 28$		
$h = 21$	$N(h,10^9) = 14$		
$h = 22$	$N(h,10^9) = 6$		
$h = 23$	$N(h,10^9) = 4$		
$h = 24$	$N(h,10^9) = 0$		
$h = 25$	$N(h,10^9) = 1$		
$h = 26$	$N(h,10^9) = 1$		

V. Ensemble des $p < 10^9$ tels que $s > 2$ et $p < 2^{4h/3}$

Ces nombres premiers sont les seuls $< 10^9$ pour lesquels les majorations de Jacobi-Weil permettent que $s(p^3) > 2$.

p	h	s	l	$s(p^3)$
17	**4**	**16**	**1**	**2**
257	**8**	**256**	**1**	**2**
40 961	**13**	**4**	**5**	**2**
65 537	**16**	**65 536**	**1**	**2**
114 689	**14**	**6**	**7**	**2**
163 841	**15**	**4**	**5**	**2**
557 057	**15**	**9**	**17**	**2**
2 424 833	**16**	**6**	**37**	**2**
5 767 169	**19**	**10**	**11**	**2**
7 340 033	**20**	**6**	**7**	**2**
11 272 193	**18**	**7**	**43**	**2**
13 631 489	**20**	**12**	**13**	**2**
21 495 809	**19**	**8**	**41**	**2**
23 068 673	**21**	**10**	**11**	**2**
26 214 401	**20**	**4**	**5**	**2**
37 224 449	**19**	**6**	**71**	**2**
40 370 177	**19**	**6**	**7**	**2**
70 254 593	**20**	**6**	**67**	**2**
101 711 873	**20**	**6**	**97**	**2**
104 857 601	22	4	5	
111 149 057	21	7	53	
136 314 881	21	4	5	
155 189 249	22	10	37	
167 772 161	25	4	5	
186 646 529	21	7	89	
199 229 441	21	4	5	
211 812 353	21	6	101	
230 686 721	22	4	5	
249 561 089	21	6	7	
469 762 049	26	6	7	
595 591 169	23	7	71	
645 922 817	23	6	7	
897 581 057	23	7	107	
998 244 353	23	6	7	

VI. Valeurs de s pour $h(p) = 6$

L'entier s_1 est défini par le membre de droite de l'inégalité (S1) du §3, a) (pour $p > 2^{2h} = 4096$).

p	h	s	s_1	l
449	6	5		7
1 217	6	4		19
2 753	6	3		43
3 137	6	3		7
4 289	6	3	182	67
4 673	6	3	65	73
5 441	6	3	31	5
6 977	6	3	17	109
9 281	6	3	12	5
10 433	6	3	10	163
11 969	6	3	9	11
13 121	6	3	9	5
15 809	6	3	8	13
25 409	6	3	6	397
25 793	6	3	6	13
26 177	6	3	6	409
26 561	6	3	6	5
29 633	6	3	6	463
33 857	6	3	5	23
52 289	6	3	5	19
53 441	6	3	5	5
64 577	6	3	5	1009
83 009	6	3	4	1297

VII. Les 12 derniers $p < 10^9$ tels que $h(p) = 12$ et $s(p) > 2$

p	h	s	s_1	l
386 019 329	12	3	7	73
390 270 977	12	3	7	151
398 233 601	12	3	7	5
416 223 233	12	3	7	307
434 040 833	12	3	7	105 967
459 182 081	12	3	7	5
491 696 129	12	3	6	7
502 067 201	12	3	6	5
524 185 601	12	3	6	5
561 246 209	12	3	6	263
588 648 449	12	3	6	137
662 990 849	12	3	6	13

VIII. Valeurs maximales de s en fonction de h trouvées pour $p < 10^9$ (nombres de Fermat exclus)

$W = 2^{sh/(s-1)}$; tant que $W < 10^9$, c'est effectivement la valeur maximale grâce aux majorations de Jacobi-Weil.

h	s	p	W
2	4	5	40
3	4	41	256
4	4	113	1 625
5	4	353	10 321
6	5	449	32 768
7	4	641	416 127
8	6	3 329	602 248
9	4	11 777	16 777 216
10	8	13 313	7 597 760
11	5	59 393	189 812 531
12	6	151 553	467 373 274
13	7	188 417	1 352 829 926
14	6	114 689	13 019 906 170
15	9	557 057	10 822 639 410
16	6	2 424 833	
17	5	19 529 729	
18	7	11 272 193	
19	10	5 767 169	
20	12	13 631 489	
21	10	23 068 673	
22	10	155 189 249	
23	7	595 591 169	
24			
25	4	167 772 161	
26	6	469 762 049	

IX. Plus petite valeur de p pour laquelle $s > 2$

p	h	s	l	b
41	3	4	5	5
17	4	16	1	1
113	4	4	7	7
353	5	4	11	11
449	6	5	7	7
95 873	7	3	7	$749 = 7 \cdot 107$
257	8	256	1	1
3 329	8	6	13	13
11 777	9	4	23	23
13 313	10	8	13	13
59 393	11	5	29	29
151 553	12	6	37	37
40 961	13	4	5	5
114 689	14	6	7	7
163 841	15	4	5	5
65 537	16	65 536	1	1
2 424 833	16	6	37	37
19 529 729	17	5	149	149
11 272 193	18	7	43	43
5 767 169	19	10	11	11
7 340 033	20	6	7	7
23 068 673	21	10	11	11
104 857 601	22	4	5	$25 = 5^2$
595 591 169	23	7	71	71
167 772 161	25	4	5	5
469 762 049	26	6	7	7

X. Plus petite valeur de p pour laquelle $s = 3$

p	h	s	l
89	3	3	11
401	4	3	5
929	5	3	29
4 289	6	3	67
95 873	7	3	7
14 081	8	3	5
17 921	9	3	5
136 193	10	3	7
366 593	11	3	179
643 073	12	3	157
3 383 297	13	3	7
3 260 417	14	3	199
6 258 689	15	3	191
20 512 769	16	3	313
67 502 081	17	3	5

Pour $h \geq 18$, on ne trouve aucun $p < 10^9$ pour lequel $s = 3$.

Yvette AMICE et Bruno KAHN
Université de Paris 7
UFR de Mathématiques
5ème étage, couloir 45–55
2, Place Jussieu
75251 PARIS Cedex 05
FRANCE
adresses électroniques :
amice@mathp7.jussieu.fr
kahn@mathp7.jussieu.fr

Astérisque

A.-M. BERGÉ
J. MARTINET
F. SIGRIST

Une généralisation de l'algorithme de Voronoï pour les formes quadratiques

Astérisque, tome 209 (1992), p. 137-158
<http://www.numdam.org/item?id=AST_1992__209__137_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

UNE GÉNÉRALISATION DE L'ALGORITHME DE VORONOÏ POUR LES FORMES QUADRATIQUES

par A-M. BERGÉ, J. MARTINET et F. SIGRIST

§ 1. **Introduction.** Soit n un entier > 0. On note $\mathcal{Q}_n$ l'espace vectoriel des formes quadratiques sur $\mathbb{R}^n$ que l'on identifie à l'espace vectoriel Sym_n des matrices symétriques d'ordre n à coefficients réels, en associant à $M \in \mathrm{Sym}_n$ la forme $Q(x) = {}^tXMX$ où, pour $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, X désigne la matrice-colonne de composantes $x_1, x_2, \ldots, x_n$ et la notation ${}^tA$ désigne la transposée de la matrice A. Pour une forme Q définie positive, on pose $m(Q) = \min_{x \in \mathbb{Z}^n \setminus \{0\}} Q(x)$ (*le minimum de* Q) et $S(Q) = \{x \in \mathbb{Z}^n \mid Q(x) = m(Q)\}$ (ensemble des *vecteurs minimaux de* Q), et l'on note $\det(Q)$ le déterminant $\det(M)$ de la matrice correspondant à Q (*le discriminant de* Q). *L'invariant d'Hermite de* Q est $\gamma_n(Q) = m(Q)(\det(Q))^{-1/n}$, et *la constante d'Hermite pour la dimension* n est $\gamma_n = \sup_Q \gamma_n(Q)$.

Afin de calculer la constante d'Hermite, Korkine et Zolotareff ont introduit la notion de *forme extrême* (forme qui réalise un maximum local de l'invariant d'Hermite) et démontré le résultat suivant ([K-Z]) :

1.1. Théorème (KORKINE ET ZOLOTAREFF, 1877). *Si Q est une forme extrême, les formes de matrices $Y {}^tY, Y \in S(Q)$ engendrent $\mathcal{Q}_n$. (En particulier, Q possède au moins $\frac{n(n+1)}{2}$ couples de vecteurs minimaux.)*

Les formes vérifiant cette propriété ont été appelées par la suite *formes parfaites* par Voronoï, qui a notamment démontré qu'elles sont en nombre fini à proportionalité et équivalence sous $\mathrm{Gl}_n(\mathbb{Z})$ près. C'est la notion de forme parfaite plutôt que celle de forme extrême qui est importante dans les applications.

mots-clés : Formes quadratiques réelles, Formes parfaites, Réseaux parfaits.

[Noter que, lorsque Y parcourt les vecteurs-colonnes à n composantes, les matrices $Y{}^tY$ parcourent l'ensemble des matrices positives de rang ≤ 1 de Sym_n, alors que ${}^tYY \in \mathbb{R}$ est le carré de la norme de Y.]

Korkine et Zolotareff, à l'aide de méthodes combinatoires, ont classé les formes parfaites jusqu'à la dimension 5, trouvant ainsi la valeur de γ_5 ([K-Z], 1877). L'étude des formes parfaites a été reprise 30 ans plus tard par Voronoï (dans [V], paru en 1908), qui a introduit une méthode entièrement nouvelle qui sera décrite en détail au § suivant. Indiquons simplement ici qu'il associe à toute forme parfaite Q de dimension $n \geq 2$ et de minimum m donné un cône polyédral d'intérieur non vide de $\mathcal{Q}_n$ et à toute face de ce cône une forme parfaite dite contiguë à Q, et qu'il démontre que le graphe de contiguïté ainsi obtenu est *connexe*. La relation de contiguïté étant compatible à l'équivalence, l'ensemble des classes de formes parfaites de minimum donné se trouve muni d'une structure de graphe qui est fini et connexe, ce qui entraîne la validité du procédé de calcul suivant :

1.2. Algorithme (VORONOÏ, 1908)

1. Choisir une forme parfaite Q_0 pour la dimension n.

2. Déterminer ses formes contiguës $Q_1, \ldots, Q_r$.

3. Supprimer de la liste toute forme équivalente à une forme déjà rencontrée.

4. Terminer si aucune forme nouvelle n'a été conservée.

5. Sinon, faire la liste de toutes les formes contiguës à l'une des formes nouvelles et aller en 3.

À l'aide de cet algorithme, Voronoï ([V]) a vérifié les résultats de Korkine et Zolotareff pour les dimensions ≤ 5. Son article indique qu'il a également commencé l'étude de la dimension 6 (et il y annonce aussi diverses autres recherches qu'il serait peut-être intéressant de reprendre). Son décès survenu en 1908 l'a empêché de poursuivre son programme. Le cas de la dimension 6 a été résolu un demi-siècle plus tard par Barnes ([Ba]), et celui de la dimension 7 vient d'être résolu par Jaquet ([J]). Cette dernière étude a nécessité des calculs considérables sur ordinateur, et il ne semble pas possible de traiter la dimension 8 selon les mêmes procédés.

Cela suggère de restreindre l'étude de l'invariant d'Hermite à certaines familles de formes quadratiques pour lesquelles on peut développer un algorithme analogue dans un sous-espace $\mathcal{T}$ de $\mathcal{Q}_n$ de dimension inférieure. Le paragraphe 2 est consacré à la description de cet algorithme. Voici deux exemples qui seront étudiés avec quelques détails dans cet article :

1.3. Exemple. Étant donnée une représentation intégrale $\rho : G \to \mathrm{Gl}_n(\mathbb{Z})$ d'un groupe fini G, on étudie l'ensemble $\mathcal{Q}_\rho$ des formes quadratiques définies positives invariantes par $\rho(G)$; dans ce cas, on peut prendre pour $\mathcal{T}$ l'espace de toutes les formes quadratiques invariantes par $\rho(G)$.

Cet exemple est étudié en détail aux §§ 3, où est justifié le choix fait pour $\mathcal{T}$ en même temps qu'est établi le lien avec la notion de G- réseau développée dans [B-M], et 4, consacré aux résultats effectifs obtenus à l'aide de l'algorithme de Voronoï.

1.4. Exemple. Soit $Q_0 = Q_0(x_1, x_2, \cdots, x_r)$ une forme quadratique définie positive à $r < n$ variables. On étudie les formes quadratiques définies positives $Q \in \mathcal{Q}_n$ de même minimum que Q_0 et telles que $Q(x_1, x_2, \cdots, x_r, 0, 0, \cdots, 0) = Q_0(x_1, x_2, \cdots, x_r)$. On se place alors dans l'espace $\mathcal{T}$ des formes $Q \in \mathcal{Q}_n$ telles que $Q(x_1, \cdots, x_r, 0, \cdots, 0) = 0$. Pour plus de détails, se reporter au § 5.

Le problème de développer un algorithme de Voronoï dans le cas des G-réseaux (exemple 1.3 ci-dessus) est posé dans [B-M]. Il a été résolu indépendamment de nous par Joseph Oesterlé, que nous remercions par ailleurs pour les discussions fructueuses que nous avons eues avec lui.

§ 2. Nouvel algorithme de Voronoï.

On munit Sym_n du produit scalaire $\langle A, B\rangle = \mathrm{Tr}(AB)$. On en déduit un produit scalaire sur $\mathcal{Q}_n$, et par restriction sur tous les sous-espaces de Sym_n et de $\mathcal{Q}_n$. Pour $x \in \mathbb{R}^n$, on note P_x ou P_X la forme de matrice $X^t X \in \mathrm{Sym}_n$. On a alors, pour $x \in \mathbb{R}^n$ et $Q \in \mathcal{Q}_n$, $Q(x) = \langle Q, P_x\rangle = \langle A, P_x\rangle$, où A est la matrice représentant la forme quadratique Q.

2.1. Définition. Soit $\mathcal{T}$ un sous-espace vectoriel de $\mathcal{Q}_n$.

(1) Pour tout $x \in \mathbb{R}^n$ représenté par la matrice-colonne X, on note Ω_x (ou Ω_X) la projection orthogonale de $P_x = P_X$ sur $\mathcal{T}$.

(2) On dit qu'une forme quadratique définie positive Q est *$\mathcal{T}$-parfaite* (ou que la matrice de Q est *$\mathcal{T}$-parfaite*) si les matrices Ω_x engendrent $\mathcal{T}$ tout entier lorsque x décrit l'ensemble $S(Q)$ des vecteurs minimaux de Q.

Si $\mathcal{T}'$ est un sous-espace de $\mathcal{T}$, toute forme $\mathcal{T}$-parfaite est $\mathcal{T}'$-parfaite. Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de forme parfaite introduite par Voronoï. On montre facilement que les vecteurs minimaux d'une forme parfaite engendrent $\mathbb{R}^n$. Nous nous restreindrons aux sous-espaces $\mathcal{T}$ vérifiant une propriété analogue :

2.2. Hypothèse. Désormais, $\mathcal{T}$ désigne un sous-espace vectoriel de $\mathcal{Q}_n$

vérifiant la propriété suivante : *les vecteurs minimaux des formes $\mathcal{T}$-parfaites engendrent $\mathbb{R}^n$.*

La proposition suivante donne d'autres expressions de cette condition :

2.3. Proposition. *Soit Q une forme quadratique définie positive. Les conditions suivantes sont équivalentes :*

(1) *Il existe des coefficients positifs $\lambda_x, x \in S(Q)$ tels que la forme quadratique $\sum_{x\in S} \lambda_x P_x$ soit définie positive.*
(2) *Pour toute famille de coefficients positifs $\lambda_x, x \in S$, la forme quadratique $\sum_{x\in S} \lambda_x P_x$ est définie positive.*
(3) *$S(Q)$ engendre $\mathbb{R}^n$.*

Démonstration. Quel que soit le vecteur $u \in \mathbb{R}^n$ et les coefficients $\lambda_x > 0$, on a

$$\sum_{x\in S(Q)} \lambda_x \langle P_x, P_u\rangle = \sum_{x\in S(Q)} \lambda_x (x.u)^2 \geq 0\,,$$

et l'égalité a lieu si et seulement si u est orthogonal à x pour tout $x \in S(Q)$ (l'espace $\mathbb{R}^n$ étant muni de son produit scalaire canonique). On en déduit tout de suite les équivalences de (1) et (3) d'une part et de (2) et (3) d'autre part, **c.q.f.d.**

2.4. Définition. Soit Q une forme quadratique définie positive. *Le $\mathcal{T}$-domaine de Voronoï $\mathcal{D}_Q$ de Q* est l'enveloppe convexe dans $\mathcal{T}$ des demi-droites fermées portant les formes Ω_x pour $x \in S(Q)$. Si Q a pour matrice A, on écrit aussi $\mathcal{D}_A$ au-lieu de $\mathcal{D}_Q$.

Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de domaine de Q introduite par Voronoï. (En fait, le $\mathcal{T}$-domaine de Q est la projection sur $\mathcal{T}$ du domaine classique).

On a

$$\mathcal{D}_Q = \mathcal{D}_A = \{ \sum_{x\in S(Q)} \lambda_x \Omega_x \mid \lambda_x \geq 0\}\,,$$

et l'intérieur du $\mathcal{T}$-domaine de Voronoï de Q est

$$\mathrm{Int}(\mathcal{D}_Q) = \{ \sum_{x\in S(Q)} \lambda_x \Omega_x \mid \lambda_x > 0\}\,.$$

Dire que Q est $\mathcal{T}$-parfaite revient à dire que $\mathcal{D}_Q$ est d'intérieur non vide dans $\mathcal{T}$.

Dans la suite, on suppose que Q est $\mathcal{T}$-parfaite. (On pourrait se passer de cette restriction, à condition de remplacer dans les énoncés ci-dessous $\mathcal{T}$ par le sous-espace de $\mathcal{T}$ engendré par $\mathcal{D}_Q$.) Soit $\mathcal{F}$ une face de codimension 1 de $\mathcal{D}_Q$ dans $\mathcal{T}$. C'est un cône polyédral contenu dans $\mathcal{D}_Q$ qui engendre un hyperplan $\mathcal{H}$ de $\mathcal{T}$. On a $\mathcal{F} = \mathcal{H} \cap \mathcal{D}_Q$, et $\mathcal{D}_Q$ est contenu dans l'un des demi-espaces fermés définis par $\mathcal{H}$. Il existe une forme $Q_F \in \mathcal{T}$, unique à une homothétie positive près, vérifiant les deux conditions suivantes :

(1) $\langle Q_F, \Omega_x \rangle \geq 0$ quel que soit $x \in S(Q)$.
(2) $\langle Q_F, \Omega_x \rangle = 0 \iff \Omega_x \in \mathcal{F}$.

Une telle forme est appelée *forme de face de Q associée à $\mathcal{F}$*, et l'on note F la matrice correspondante. On a alors

$$\mathcal{D}_Q = \{Q' \in \mathcal{T} \mid \langle Q_F, Q' \rangle \geq 0 \text{ pour toute forme de face } Q_F \text{ de } Q\}.$$

Dans la pratique, on procède de la façon suivante : on commence par choisir une base $\mathcal{B} = (T_1, T_2, \ldots, T_k)$ de $\mathcal{T}$ (des choix commodes sont indiqués dans certains cas aux §§ 4 et 5) ; soit $\mathcal{B}^* = (T_1^*, T_2^*, \ldots, T_k^*)$ sa base duale dans $\mathcal{T}$. Pour tout $x \in S(Q)$, représenté par la matrice-colonne X, on détermine les composantes $\omega_{i,x}$ de Ω_x dans $\mathcal{B}^*$ à l'aide des formules

$$\omega_{i,x} = \langle \Omega_x, T_i \rangle = \langle P_X, T_i \rangle = {}^tXAX = Q_{T_i}(x).$$

La partie algorithmiquement difficile est l'établissement de la liste des faces de $\mathcal{D}_Q$. Comme il n'y a pas de différence de principe avec ce qui se fait dans le cas classique, nous renvoyons le lecteur à la thèse de Jaquet ([J]). La recherche d'une forme de face Q_F pour une face $\mathcal{F}$ se fait en résolvant le système linéaire suivant, qui donne les composantes f_i de Q_F dans la base $\mathcal{B}$:

$$\sum_i \omega_{i,x} f_i = 0 \qquad (x \in \mathcal{F})$$

$$\sum_i \omega_{i,x} f_i > 0 \qquad (x \notin \mathcal{F}).$$

On notera qu'il est inutile de déterminer $\mathcal{B}^*$.

Pour tout nombre réel $\theta \geq 0$, on pose $Q_\theta = Q + \theta Q_F$; c'est une forme quadratique de matrice $A_\theta = A + \theta F$. Les vecteurs X de $S(Q)$ dont l'image Ω_X est dans $\mathcal{F}$ sont de norme m, et ceux dont l'image n'est pas dans $\mathcal{F}$ sont de norme $m + \theta Q_F(X) > m$ dès que θ est > 0. Par ailleurs, les vecteurs

minimaux de Q_θ proviennent de ceux de Q lorsque θ est assez petit. Il en résulte que, pour $\theta > 0$ assez petit, Q_θ est une forme non $\mathcal{T}$-parfaite de même minimum m que Q.

2.5. Définition. On note $\rho \in]0, +\infty]$ la borne supérieure des $\theta \geq 0$ tels que Q_θ soit positive de minimum m. On dit que $\mathcal{F}$ (ou que F) est *une impasse* si $\rho = +\infty$. Lorsque $\mathcal{F}$ n'est pas une impasse, la forme Q_ρ s'appelle *la forme $\mathcal{T}$-contiguë à Q par $\mathcal{F}$* (ou *par F*).

2.6. Proposition.

(1) *Si $\mathcal{F}$ n'est pas une impasse, la forme Q_ρ est $\mathcal{T}$-parfaite.*
(2) *$\mathcal{F}$ est une impasse si et seulement si la forme Q_F est positive.*

Démonstration. Si Q_F est positive, on a $Q_\theta(x) \geq Q(x) \geq m$ pour tout $x \in \mathbb{Z}^n$ non nul, donc $\rho = +\infty$. Dans le cas contraire, il existe $x \in \mathbb{R}^n$ avec $Q_F(x) < 0$. Comme il existe des points de $\mathbb{Z}^n$ arbitrairement proches de la droite $\mathbb{R}x$, il existe $y \in \mathbb{Z}^n$ avec $Q_F(y) < 0$. Alors, $Q_\theta(y)$ est < 0 pour θ assez grand, et un tel θ est un majorant de ρ, d'où (2). En outre, on a $Q_\rho(x) \geq m$ pour tout $x \neq 0$ de $\mathbb{Z}^n$, mais, comme Q_θ prend sur $\mathbb{Z}^n \setminus \{0\}$ des valeurs $< m$ pour tout $\theta > \rho$, il existe $z \in \mathbb{Z}^n$ avec $Q_\rho(z) = m$ et $Q_F(z) < 0$. Le vecteur z est donc un vecteur minimal de Q_ρ qui n'est pas un vecteur minimal de Q. Comme le système des $\Omega_x \in \mathcal{F}$ ($x \in S(Q)$) est de rang $\dim \mathcal{T} - 1$, le système formé par $\Omega_x, x \in \mathcal{F}$ et Ω_z est de rang $\dim \mathcal{T}$, **c.q.f.d.**

Le lemme suivant est énoncé en termes de matrices.

2.7. Lemme. *Soient $A, B \in \mathrm{Sym}_n$ deux matrices définies positives de même minimum m avec $A - B \in \mathcal{T}$.*

(1) *Pour tout $C \in \mathcal{D}_A \cap \mathcal{D}_B$, on a $\langle C, A\rangle = \langle C, B\rangle$.*
(2) *Si $\mathrm{Int}(\mathcal{D}_A) \cap \mathcal{D}_B$ est non vide, alors $\mathcal{D}_A \subset \mathcal{D}_B$.*
(3) *Si de plus A est $\mathcal{T}$-parfaite, alors $B = A$.*

Démonstration. Posons $C = \sum_{x \in S(A)} \lambda_x \Omega_x$ avec des coefficients $\lambda_x \geq 0$. Comme
$A - B \in \mathcal{T}$, on a

$$\langle C, A - B\rangle = \sum_{x \in S(A)} \lambda_x \langle \Omega_x, A - B\rangle = \sum_{x \in S(A)} \lambda_x \langle P_x, A - B\rangle$$
$$= \sum_{x \in S(A)} \lambda_x (m - \langle P_x, B\rangle) \leq 0 .$$

On a de même $\langle C, B - A\rangle \leq 0$, d'où (1).

Lorsque $C \in \mathrm{Int}(A)$, on peut prendre les λ_x strictement positifs. Comme $m - \langle P_x, B\rangle$ est ≤ 0 pour tout $x \in S(A)$, l'égalité $\sum_{x\in S(A)} \lambda_x(m - \langle P_x, B\rangle) = 0$ entraîne que l'on a $\langle P_x, B\rangle = m$ pour tout $x \in S(A)$, d'où $S(A) \subset S(B)$, i.e. $\mathcal{D}_A \subset \mathcal{D}_B$.

Comme $A - B \in \mathcal{T}$, la condition $\langle P_x, A - B\rangle = 0$ pour tout $x \in S(A)$ équivaut à $\langle \Omega_x, A - B\rangle = 0$ pour tout $x \in S(A)$, ce qui, lorsque A est $\mathcal{T}$-parfaite, implique $A - B = 0$, **c.q.f.d.**

L'ensemble des formes $\mathcal{T}$-parfaites est l'ensemble des sommets d'un graphe non orienté dont les arêtes sont les couples de formes contiguës (la relation de contiguïté est clairement symétrique). On s'intéresse à la connexité de ce graphe, que l'on étudie à l'aide du résultat suivant, dont nous laissons comme Voronoï la démonstration au lecteur :

2.8. Lemme. *(*VORONOÏ*) Soit Φ une forme quadratique définie positive, soient m et K deux constantes. L'ensemble des vecteurs minimaux des formes définies positives Q de minimum m et telles que $\langle Q, \Phi\rangle \leq K$ est une partie finie de $\mathbb{Z}^n$.*

On rappelle que $\mathcal{T}$ désigne un sous-espace vectoriel de $\mathcal{Q}_n$ tel que les vecteurs minimaux de toute forme $\mathcal{T}$-parfaite engendrent $\mathbb{R}^n$.

2.9. Théorème. *Soit $Q_0 \in \mathcal{Q}_n$ et soit $\mathcal{E}$ l'ensemble des formes quadratiques Q de même minimum m que Q_0 et telles que $Q - Q_0 \in \mathcal{T}$. Alors, le graphe de $\mathcal{T}$-contiguïté des formes $\mathcal{T}$-parfaites de $\mathcal{E}$ est connexe.*

Démonstration. Soit Q une forme $\mathcal{T}$-parfaite de $\mathcal{E}$. Soient $\lambda_x, x \in S(Q)$ des nombres réels > 0, soit $\Phi_0 = \sum_{x\in S(Q)} \lambda_x \Omega_x$ et soit $\Phi = \sum_{x\in S(Q)} \lambda_x P_x$. Comme Q est $\mathcal{T}$-parfaite, l'hypothèse faite sur $\mathcal{T}$ implique que Φ est définie positive. Si Φ_0 est dans $\mathcal{D}_{Q_0}$, alors le lemme 2.7 montre que $Q_0 = Q$. Sinon, il existe une forme de face F de Q_0 avec $\langle \Phi_0, F\rangle < 0$, ce qui entraîne qu'il existe au moins un $x \in S(Q)$ vérifiant $\langle \Omega_x, F\rangle < 0$. Il existe donc une forme $\mathcal{T}$-contiguë Q_1 à Q_0 par F, et l'on a

$$\langle Q_1, \Phi_0\rangle = \langle Q_0, \Phi_0\rangle + \rho\langle F, \Phi_0\rangle < \langle Q_0, \Phi_0\rangle .$$

Si $\Phi_0 \notin \mathcal{D}_{Q_1}$, on contruit de même une forme $\mathcal{T}$-contiguë Q_2 à Q_1 telle que $\langle Q_2, \Phi_0\rangle < \langle Q_1, \Phi_0\rangle$. On construit ainsi une suite $Q_0, Q_1, \ldots, Q_i$ de formes $\mathcal{T}$-parfaites de même minimum m et telles que

$$\langle Q_0, \Phi\rangle > \langle Q_1, \Phi\rangle > \cdots > \langle Q_i, \Phi\rangle ,$$

car, comme $Q_{i+1} - Q_i$ appartient à $\mathcal{T}$, on a

$$\langle Q_{i+1}, \Phi\rangle - \langle Q_i, \Phi\rangle = \langle Q_{i+1}, \Phi_0\rangle - \langle Q_i, \Phi_0\rangle < 0 .$$

Comme Φ est définie positive, et comme, pour tout i, l'on a $\langle Q_i, \Phi\rangle < \langle Q_0, \Phi\rangle$, il existe une partie finie S de $\mathbb{Z}^n$ telle que, pour tout i, on ait $S(Q_i) \subset S$. La famille des $S(Q_i)$ est donc finie. Soient i et j deux indices tels que $S(Q_i) = S(Q_j)$. Pour tout $x \in S(Q_i)$, on a $\langle Q_i - Q_j, \Omega_x\rangle = \langle Q_i - Q_j, P_x\rangle$ (car $Q_i - Q_j \in \mathcal{T}$), et cette expression est nulle, puisque $\langle Q_i, P_x\rangle = \langle Q_j, P_x\rangle = m$. Comme Q_i est $\mathcal{T}$-parfaite, les $\Omega_x, x \in S(Q_i)$ engendrent $\mathcal{T}$, et les conditions $\langle Q_i - Q_j, \Omega_x\rangle = 0$ pour tout $x \in S(Q_i)$ entraînent donc $Q_i - Q_j = 0$. Par conséquent, la suite $Q_1, Q_2, \ldots$ est finie, et il existe un indice p tel que Φ appartienne à $\mathcal{D}_{Q_p}$, ce qui entraîne par le lemme 2.7 que $Q_p = Q$, **c.q.f.d.**

Dans la théorie classique de Voronoï, on exprime les résultats sur l'ensemble des classes d'équivalence modulo $\mathrm{Gl}_n(\mathbb{Z})$ de formes quadratiques (de minimum donné). Pour étendre la théorie, on doit introduire la définition suivante :

2.10. Définition. On dit que deux formes quadratiques Q et Q' de matrices respectives A et A' sont *$\mathcal{T}$-équivalentes* s'il existe $M \in \mathrm{Gl}_n(\mathbb{Z})$ vérifiant les deux conditions ${}^tMAM = A'$ et ${}^tM\mathcal{T}M \subset \mathcal{T}$.

2.11. Proposition. *La relation de contiguïté est compatible à la $\mathcal{T}$-équivalence.*

[Cela signifie qu'une $\mathcal{T}$-équivalence entre deux formes $\mathcal{T}$-parfaites met en bijection les ensembles de leurs formes contiguës. En particulier, à deux faces $\mathcal{T}$-équivalentes d'une même forme stable par cette équivalence sont associées des formes contiguës $\mathcal{T}$-équivalentes.]

Démonstration. Rappelons que si deux formes quadratiques R et R' sont équivalentes par une transformation de matrice M, on a, pour tout vecteur-colonne X, $R(X) = R'(M^{-1}X)$.

Soit F une matrice de face du domaine D_Q de Q, et soit $F' = {}^tMFM$. C'est un élément de $\mathcal{T}$. Soit $X \in S(Q)$ tel que Ω_X soit dans la face orthogonale à F de $\mathcal{D}_D$. Alors, $M^{-1}X \in S(Q')$ vérifie

$$\langle F', \Omega_{M^{-1}X}\rangle = \langle F', P_{M^{-1}X}\rangle = \langle F, P_X\rangle = \langle F, \Omega_X\rangle = 0\,.$$

Donc, F' est une matrice de face pour $\mathcal{D}_{Q'}$. (Noter cependant que $\mathcal{D}_{Q'}$ est en général distinct de ${}^tM\mathcal{D}_QM$, car l'équivalence n'est pas une transformation orthogonale pour le produit scalaire $\langle .,.\rangle$.)

Pour tout $\theta \in \mathbb{R}$, soit Q_θ la forme de matrice $A_\theta = A + \theta F$. Soit $\rho \in \mathbb{R} \cup \infty$ la borne supérieure des $\theta \geq 0$ tels que Q_θ soit positive de minimum $m(Q)$ sur $\mathbb{Z}^n$, et soit Q'_θ la forme transformée de Q_θ par M. Sa matrice est $A'_\theta = A' + \theta F'$, et l'égalité $Q'_\theta(M^{-1}X)Q_\theta(X)$ montre que ρ est la borne supérieure des $\theta \geq 0$ tels que Q'_θ soit positive de minimum $m(Q) = m(Q')$ sur $\mathbb{Z}^n$, **c.q.f.d.**

La proposition ci-dessus justifie que l'on opère comme dans l'algorithme classique rappelé en 1.2 pour la recherche des formes $\mathcal{T}$-parfaites à partir d'une forme Q_0 donnée. Toutefois, on ne peut pas garantir la finitude du graphe à $\mathcal{T}$-équivalence près sans hypothèses supplémentaires. Du reste, la notion de $\mathcal{T}$-perfection est purement formelle lorsque l'on ne l'applique pas à des formes possédant des propriétés particulières liées à $\mathcal{T}$, comme dans les exemples 1.3 à 1.5.

2.12. Remarque. Dans le cas classique, Voronoï montre que les demi-droites portant les matrices Ω_x (x parcourant l'ensemble des vecteurs minimaux d'une forme parfaite Q) sont toutes des arêtes de de $\mathcal{D}_Q$, et qu'il n'y a pas d'impasse. Ceci ne se généralise pas : des contre-exemples sont signalés au § 4 (ex. 4.3 et 4.2).

§ 3. Actions de groupes. Soit G un groupe fini. Rappelons qu'une *représentation intégrale de rang n* du groupe G est un homomorphisme $\rho : G \to \mathrm{Gl}_n(\mathbb{Z})$; il revient au même de se donner une structure de $\mathbb{Z}[G]$-module sur $\mathbb{Z}^n$. On dit que deux représentations intégrales ρ et ρ' sont *équivalentes* s'il existe $M \in \mathrm{Gl}_n(\mathbb{Z})$ telle que, pour tous $s \in G$, on ait $M^{-1}\rho(s)M = \rho'(s)$.

Soit L un $\mathbb{Z}[G]$-module, libre de rang n sur $\mathbb{Z}$. On associe de façon naturelle à toute base de L une représentation intégrale de G, ce qui met en bijection les classes d'isomorphisme de $\mathbb{Z}[G]$-modules $\mathbb{Z}$-libres de rang n et les classes d'équivalence de représentations intégrales de rang n de G.

Soit E un espace euclidien et soit $\rho : G \to O(E)$ une représentation orthogonale de G. Un *G-réseau* ([B-M], §1) est un réseau stable par G. L'ensemble $\mathcal{R}_G$ des G-réseaux est non vide si et seulement si ρ est rationnelle sur $\mathbb{Q}$ ([B-M], § 2). Un réseau $\Lambda \in \mathcal{R}_G$ définit plus précisément une classe de représentations intégrales. La correspondance entre $\mathbb{Z}[G]$-modules à isomorphismes près et classes de représentations intégrales se traduit ainsi :

3.1. Proposition. *Pour que deux réseaux Λ et Λ' définissent la même classe de représentations intégrales, il faut et il suffit qu'il existe un élément f du commutant de ρ dans $\mathrm{Gl}(E)$ appliquant Λ sur Λ'.*

Pour déterminer les G-réseaux G-parfaits au sens de [B-M], déf. 2.3, à l'aide d'un algorithme de Voronoï du type du § précédent, il sera nécessaire de distinguer les diverses représentations intégrales définissant une même représentation sur $\mathbb{Q}$. Le problème de classification que cela soulève est en général difficile. Nous verrons en fin de § quelques exemples faciles, relatifs au cas d'un groupe G cyclique.

Étant donnés deux bases $\mathcal{B}$ et $\mathcal{B}'$ et un endomorphisme f de E, on note $\mathrm{Mat}(f, \mathcal{B}, \mathcal{B}')$ la matrice de f dans les bases $\mathcal{B}$ et $\mathcal{B}'$, et l'on écrit simplement $\mathrm{Mat}(f, \mathcal{B})$ lorsque $\mathcal{B} = \mathcal{B}'$. Rappelons que la *matrice de* Gram de $\mathcal{B} = (e_1, \ldots, e_n)$ est $\mathrm{Gram}(\mathcal{B}) = (e_i.e_j)$; on a aussi $\mathrm{Gram}(\mathcal{B}) = \mathrm{Mat}(\mathrm{Id}, \mathcal{B}, \mathcal{B}^*)$, où $\mathcal{B}^*$ désigne la base duale de $\mathcal{B}$ pour la structure euclidienne de E.

Soit $\Lambda \in \mathcal{R}_G$, soit $\mathcal{B}$ une base de Λ et soit $A = \mathrm{Gram}\,\mathcal{B}$. Au couple $(\Lambda, \mathcal{B})$, on associe la forme quadratique $Q(X) = {}^tXAX$, de matrice A, ce qui permet d'associer au réseau Λ la classe modulo $\mathrm{Gl}_n(\mathbb{Z})$ de la forme quadratique Q (n est le rang de Λ). Si l'on passe de la base $\mathcal{B}$ à une base $\mathcal{B}'$ à l'aide de la matrice de passage M, la forme Q devient la forme Q' de matrice $A' = {}^tMAM$. Le remplacement de Λ par un réseau qui lui est isométrique ne modifie pas la classe de formes associée à Λ.

Supposons maintenant que Λ soit dans $\mathcal{R}_G$. Au couple $(\Lambda, \mathcal{B})$ correspond alors la forme quadratique Q de matrice A et une représentation intégrale ρ que l'on peut définir par des matrices $U_s, s \in G$ telles que ${}^tU_sAU_s = A$ (ce qui ne fait que traduire l'appartenance de $\rho(s)$ à $O(E)$; on dit que Q (ou que A) est *invariante par* ρ).

Posons

$$\mathcal{T} = \{T \in \mathrm{Sym}_n(\mathbb{R}) \mid \forall s \in G, {}^tU_sTU_s = T\}.$$

3.2. Proposition. *Un G-réseau Λ' définit une représentation intégrale équivalente à $s \mapsto U_s$ si et seulement s'il possède une base dont la matrice de Gram appartient à $\mathcal{T}$.*

Démonstration. Si Λ' possède une base $\mathcal{B}'$ telle que $\mathrm{Mat}(\rho(s), \mathcal{B}') = U_s$, on a $\mathrm{Gram}(\mathcal{B}') = \mathrm{Gram}\,(\rho(s)(\mathcal{B}'))$ (parce que ρ est orthogonale), ce qui exprime l'appartenance de $\mathrm{Gram}(\mathcal{B}')$ à $\mathcal{T}$.

Réciproquement, soit Λ' un réseau et soit $\mathcal{B}'$ une base de Λ' telle que $A' = \mathrm{Gram}(\mathcal{B}')$ soit dans $\mathcal{T}$ (i.e., on a ${}^tU_sA'U_s = A'$ quel que soit $s \in G$). Montrons que Λ' est isométrique à un réseau Λ'' définisant la même classe de représentations intégrales que le réseau Λ de départ.

Soit $f \in \mathrm{Gl}(E)$ tel que $\Lambda' = f(\Lambda)$. Soit $\mathcal{B}$ une base de Λ telle que $\mathrm{Gram}(\mathcal{B}) = A$ et que $U_s = \mathrm{Mat}(s, \mathcal{B})$ (on a donc ${}^tU_sAU_s = A$), de base duale $\mathcal{B}^*$. On a

$$A' = \mathrm{Mat}({}^tff, \mathcal{B}, \mathcal{B}^*) \quad \text{et} \quad {}^tU_sA'U_s = \mathrm{Mat}({}^t\rho(s){}^tff\rho(s), \mathcal{B}, \mathcal{B}^*).$$

La condition ${}^tU_sA'U_s = A'$ équivaut à ${}^t\rho(s){}^tff\rho(s) = {}^tff$. Comme ${}^t\rho(s) = \rho(s)^{-1}$ (parce que ρ est orthogonale), cela signifie que $\rho(s)$ et ${}^tff$

commutent. Il en est donc de même de $\sqrt{{}^t ff}$ et $\rho(s)$ ([B-M], dém. du lemme 2.1). Le réseau $\Lambda'' = \sqrt{{}^t ff}(\Lambda)$ est isométrique à $f(\Lambda)$ (on a $f/\sqrt{{}^t ff} \in O(E)$) et est en outre $\mathbb{Z}[G]$-isomorphe à Λ, **c.q.f.d.**

(Nous avons utilisé le fait qu'un endomorphisme symétrique u à valeurs propres ≥ 0 possède une unique racine carrée à valeurs propres ≥ 0 ; il est immédiat que ce résultat s'applique à ${}^t ff$ quel que soit $f \in \mathrm{End}(E)$.)

Soit $\Lambda \in \mathcal{R}_G$. Les G-réseaux voisins de Λ au sens de la topologie induite par celle de $\mathrm{Gl}(E)$ correspondent à la même classe de représentation intégrale de G que Λ, c'est-à-dire appartiennent à l'orbite de Λ sous l'action du commutant de G. Notons $\mathcal{S}_G$ le sous-espace vectoriel des endomorphismes symétriques de E commutant avec $\rho(s)$ pour tout $s \in G$. On montre dans [B-M] que, si le réseau est *G-extrême*, c'est-à-dire s'il réalise un maximum local de l'invariant d'Hermite dans $\mathcal{R}_G$, il est *G-parfait*, en ce sens que les formes linéaires sur $\mathcal{S}_G$

$$\varphi_x \ : \ h \mapsto h(x).x$$

engendrent, quand x décrit l'ensemble $S(\Lambda)$ des vecteurs minimaux de Λ, le dual $\mathcal{S}_G^*$ de $\mathcal{S}_G$.

3.3 Proposition. *Soit $\mathcal{B}$ une base du G-réseau Λ, soit $A = \mathrm{Gram}(\mathcal{B})$ et soit $\mathcal{T}$ l'espace des matrices invariantes par la représentation intégrale associée à $\mathcal{B}$. Alors le réseau Λ est G-parfait si et seulement si A est $\mathcal{T}$-parfaite.*

Démonstration. Comme on l'a remarqué au cours de la démonstration de la proposition 3.2, on a, pour tout endomorphisme h de E et tout $s \in G$,

$$\mathrm{Mat}\left(\rho(s)h\rho(s^{-1}), \mathcal{B}, \mathcal{B}^*\right) = {}^t U_s H U_s \, ,$$

où $H = \mathrm{Mat}(h, \mathcal{B}, \mathcal{B}^*)$ et $U_s = \mathrm{Mat}(\rho(s), \mathcal{B})$, de sorte que l'endomorphisme h appartient à $\mathcal{S}_G$ si et seulement si sa matrice H appartient à $\mathcal{T}$.

Par ailleurs, si l'on suppose l'une de ces deux conditions vérifiée, on a, pour tout $x \in E$ représenté par la matrice colonne X dans $\mathcal{B}$:

$$\langle \Omega_X, H \rangle = \langle P_X, H \rangle = {}^t XHX = \varphi_x(h) \ ;$$

on voit ainsi que les $(\Omega_X)_{X \in S(A)}$ engendrent $\mathcal{T}$ si et seulement si les $(\varphi_x)_{x \in S(\Lambda)}$ engendrent $\mathcal{S}_G^*$, **c.q.f.d.**

Remarquons que Ω_X ne dépend que de l'orbite de X : cela résulte du calcul suivant (on a $\sigma \in G$ et $T \in \mathcal{T}$, donc ${}^t U_\sigma T = T U_\sigma^{-1}$)

$$\langle P_{\sigma X}, T \rangle = \langle U_\sigma P_X {}^t U_\sigma, T \rangle = \mathrm{Tr}(U_\sigma P_X (t U_\sigma T)) =$$
$$\mathrm{Tr}(U_\sigma P_X T U_\sigma^{-1}) = \mathrm{Tr}(P_X T) = \langle P_X, T \rangle.$$

Toutefois, on peut avoir $\Omega_X = \Omega_{X'}$ pour deux vecteurs minimaux n'appartenant pas à la même orbite. En outre, contrairement à ce qui se passe dans le cas classique, la demi-droite qui porte Ω_X peut ne pas être une arête du domaine de Voronoï pour $\mathcal{T}$, cf. ex. 4.3.

On montre dans [B-M] (prop. 2.9) que les vecteurs minimaux d'une forme G-invariante G-parfaite engendrent $\mathbb{R}^n$, ce qui assure la connexité du graphe de Voronoï (th. 2.9).

Examinons maintenant deux exemples de classifications de représentations intégrales d'un groupe G cyclique, correspondant à une représentation rationnelle ρ donnée de G.

Supposons d'abord que ρ soit $\mathbb{Q}$-irréductible. Soit m l'ordre de G (donc, ρ est de degré $n = \varphi(m)$). Les $\mathbb{Z}[G]$-modules L tels que $\mathbb{Q} \otimes_{\mathbb{Z}} L$ définisse une représentation isomorphe à ρ s'identifient à des $\mathbb{Z}[\zeta_m]$-modules de rang 1, ce qui met en bijection les classes de représentations intégrales associées à ρ et les classes d'idéaux du m-ième corps cyclotomique. (Pour tout entier $k > 0$, on note ζ_k une racine de l'unité d'ordre k dans une clôture algébrique de $\mathbb{Q}$.) En particulier, il n'y a qu'une classe de représentation intégrale lorsque m est < 23.

Supposons maintenant que G soit d'ordre ℓ premier, ρ étant la *représentation régulière*. Plongeons L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L \simeq \mathbb{Q}[G]$, et soit $\mathfrak{O} = \{\lambda \subset \mathbb{Q}[G] \mid \lambda L \in L\}$ *l'ordre associé* à L. L'ordre $\mathfrak{O}$ est égal à $\mathbb{Z}[G]$ ou à l'ordre maximal $\mathfrak{M} \simeq \mathbb{Z} \times \mathbb{Z}[\zeta_l]$ de $\mathbb{Q}[G]$, puisque $[\mathfrak{M} : \mathfrak{O}] = \ell$. On montre (cf. ci-dessous) que, dans le premier cas, L est projectif sur $\mathfrak{O}$. Il en résulte que les représentations intégrales associées à ρ sont classées par deux invariants : leur ordre associé $\mathfrak{O}$ et une classe d'idéaux de $\mathbb{Q}[\zeta_\ell]$, puisque, lorsque $\mathfrak{O} = Z[G]$, le groupe des classes de $\mathbb{Z}[G]$ s'envoie injectivement dans celui de $\mathfrak{M}$ par extension des scalaires (théorème de Dock Sang Rim, [R]).

Indiquons une justification possible du fait qu'un réseau d'ordre associé $\mathbb{Z}[G]$ est $\mathbb{Z}[G]$-projectif, en revenant d'abord au cas général d'une représentation sur $\mathbb{Q}$ d'un groupe cyclique arbitraire G, définie par un $\mathbb{Q}[G]$-module V.

Pour tout sous-groupe H de G et tout sous-$\mathbb{Z}[G]$-module L de V de type fini engendrant V, le *quotient de Herbrand* $h(H, L)$ ([Se], ch. VIII, § 5) est défini et ne dépend que de H et de la classe d'isomorphisme de V : en effet, si L_1, L_2 et L' sont des sous-$\mathbb{Z}[G]$-modules de V de type fini et engendrant V avec $L' \subset L_1 \cap L_2$, on a $h(H, L_1) = h(H, L')$ et $h(H, L_2) = h(H, L')$, puisque L_1/L' et L_2/L' sont des groupes finis ; on le note $h(H, V)$.

3.4. Lemme. *Si V est libre de rang 1 sur $\mathbb{Q}[G]$, $h(H,V)=1$ quel que soit H.*

En effet, on peut calculer $h(H,V)$ en prenant $L=\mathbb{Z}[G]$, qui est libre sur H pour tout sous-groupe H de G.

3.5. Théorème. *Soit G un groupe cyclique, soit V un $\mathbb{Q}[G]$-module libre de rang 1, et soit L un sous-$\mathbb{Z}[G]$-module de V de type fini et engendrant V. Les conditions suivantes sont équivalentes :*

(1) *L'ordre $\mathfrak{O}$ associé à L est égal à $\mathbb{Z}[G]$.*
(2) *Pour tout sous-groupe H de G et tout entier $m>1$, $\frac{1}{m}\sum_{s\in H} s$ ne stabilise pas L.*
(3) *L est projectif sur $Z[G]$.*
(4) *L est localement libre sur $\mathbb{Z}[G]$.*

Démonstration. Il est clair que (1) entraîne (2), car on a l'implication $(\frac{1}{m}\sum_{s\in H} s)L\subset L \Longrightarrow \frac{1}{m}\sum_{s\in H} s\in\mathfrak{O}$. Si (2) est vérifiée, $\hat{H}^0(H,L)$ est nul pour tout sous-groupe H de G. Il en est donc de même de $\hat{H}^1(H,L)$ puisque $h(H,L)=1$. Le module L est alors cohomologiquement trivial, donc projectif sur $\mathbb{Z}[G]$ puisqu'il est libre sur $\mathbb{Z}$ ([Se], ch. IX, th. 6 et 7). L'implication (3)$\Longrightarrow$(4), qui résulte d'un théorème de Swan qui s'applique plus généralement à tous les groupes finis ([Sw]), est également un résultat standard d'algèbre comutative. Enfin, (4)$\Longrightarrow$(1) est immédiat une fois que l'on s'est ramené par localisation au cas d'un module libre, **c.q.f.d.**

§ 4. Algorithme de Voronoï pour un groupe donné. Nous avons au § 3 décrit les représentations intégrales d'un groupe cyclique lorsqu'il s'agit d'une représentation irréductible ou de la représentation régulière d'un groupe d'ordre premier ℓ. Nous explicitons d'abord l'espace $\mathcal{T}$, en nous limitant aux représentations fidèles, ce qui ne nuit pas à la généralité.

Dans tout ce §, G désigne un groupe cyclique d'ordre $m\geq 3$, σ un générateur de G et ζ une racine d'ordre m de l'unité (dans une clôture algébrique donnée de $\mathbb{Q}$). On se donne en outre une représentation intégrale de G de degré n définie par un réseau Λ muni d'une base $\mathcal{B}$. On se limite au cas où Λ est $\mathbb{Z}[G]$-monogène, et l'on écrit $\Lambda=\mathbb{Z}[G]x$.

L'espace $\mathcal{T}$ introduit au § 3 est constitué par les matrices $\mathrm{Mat}(v,\mathcal{B},\mathcal{B}^*)$ où v parcourt le commutant $\mathrm{End}_G^s(E)$ de G dans $\mathrm{End}^s(E)$. Les matrices de $\mathcal{T}$ s'écrivent $(a_{i,j})$ avec

$$a_{i,j}=v(\sigma^{i-1}x).\sigma^{j-1}x=\sigma^{i-j}v(x).x\,,$$

ce qui, en posant $\alpha_i = \frac{1}{2}(\sigma^i + \sigma^{-i})v(x).x$ ($i \bmod m$), s'écrit encore $a_{i,j} = \alpha_{i-j}$ $(= \alpha_{j-i})$:

$$(*) \qquad (a_{i,j}) = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \dots & \alpha_{n-1} \\ \alpha_1 & \alpha_0 & \alpha_1 & \dots & \dots & \alpha_{n-2} \\ \alpha_2 & \alpha_1 & \alpha_0 & \ddots & \dots & \alpha_{n-3} \\ \dots & \dots & \ddots & \ddots & \ddots & \dots \\ \dots & \dots & \dots & \alpha_1 & \alpha_0 & \alpha_1 \\ \alpha_{n-1} & \alpha_{n-2} & \dots & \alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}.$$

Quant aux $\mathcal{T}$-équivalences, on les recherche entre matrices de $\mathcal{T}$ de la forme (*) associées à des suites α_i et α'_i en recherchant dans le module quadratique $\mathbb{Z}[G]x$ tel que $x.\sigma^i x = \alpha_i$ un élément x' vérifiant $x'.\sigma^i x' = \alpha'_i$. La matrice M correspondante est celle des vecteurs $(x', \sigma x', \dots, \sigma^{n-1}x')$ dans la base $(x, \sigma x, \dots, \sigma^{n-1}x)$; c'est une matrice de $\mathcal{T}$-équivalence, car on vérifie tout de suite qu'elle définit un élément du commutant dans $\mathrm{Gl}_n(\mathbb{Z})$ de la représentation considérée.

Occupons-nous d'abord du cas d'une *représentation $\mathbb{Q}$-irréductible* de G, donc de degré $n = \varphi(m)$ pair ; on pose $n = 2p$. Un choix possible pour Λ est alors $\mathbb{Z}[\zeta]$ plongé dans l'espace $\mathbb{R} \otimes \mathbb{Z}[\zeta]$ muni de la forme bilinéaire $1 \otimes \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x\overline{y})$, et rapporté à la base $(1, \zeta, \cdots, \zeta^{n-1}$. Le polynôme cyclotomique (qui est un polynôme réciproque) est de la forme

$$\begin{aligned} \Phi_m(X) &= X^n + a_1 X^{n-1} + \cdots + a_p X^p + \cdots + a_1 X + 1 \\ &= X^p[X^p + X^{-p} + a_1(X^{p-1} + X^{-(p-1)}) + \cdots + a_p], \end{aligned}$$

d'où l'on déduit la matrice représentant σ :

$$U_\sigma = \begin{pmatrix} 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

On montre dans [B-M] que l'espace $\mathcal{T}$ (isomorphe à $\mathrm{End}^s_G(E)$) est dans ce cas de dimension p. Or, dans la forme générale des matrices de $\mathcal{T}$, les coefficients $\alpha_p, \alpha_{p+1}, \cdots, \alpha_{n-1}$ sont maintenant combinaisons linéaires des $p = \frac{n}{2}$ paramètres

$$\alpha_0, \alpha_1, \cdots \text{ et } \alpha_{p-1}.$$

On les calcule de proche en proche à l'aide du polynôme cyclotomique : on a

$$\sigma^p + \sigma^{-p} = -a_1(\sigma^{p-1} + \sigma^{-(p-1)}) - \cdots - a_{p-1}(\sigma + \sigma^{-1}) - a_p\,,$$

d'où

$$\alpha_p = -a_1\alpha_{p-1} - \cdots - a_{p-1}\alpha_1 - \frac{1}{2}a_p\alpha_0\,,$$

puis, pour $i = p+1, \cdots, n-1$, la formule de récurrence

$$\sigma^{i+1} + \sigma^{-(i+1)} = (\sigma^i + \sigma^{-i})(\sigma + \sigma^{-1}) - (\sigma^{i-1} + \sigma^{-(i-1)}).$$

On obtient donc ainsi une description complète de l'espace $\mathcal{T}$ des matrices G-invariantes.

Par exemple, pour $m = 3$, on a $\mathcal{T} = \left\{ \begin{pmatrix} \alpha_0 & -\alpha_0/2 \\ -\alpha_0/2 & \alpha_0 \end{pmatrix} \mid \alpha_0 \in \mathbb{R} \right\}$.

Pour $m = 9$, le polynôme cyclotomique est $\Phi_9(X) = X^3(X^3 + X^{-3} + 1)$, d'où l'on déduit les relations définissant $\mathcal{T}$:
$\alpha_3 = -\frac{1}{2}\alpha_0$ et $\alpha_5 = \alpha_4 = -\alpha_1 + \alpha_2$.

Les relations entre les paramètres α_i sont très faciles à expliciter dans le cas où $m = \ell$ est un nombre premier, et donc $n = \ell - 1$: on a alors
$\alpha_p = -\alpha_{p-1} - \alpha_{p-2} - \cdots - \alpha_1 - \frac{1}{2}\alpha_0$, et, pour $1 \leq i \leq p-1$, $\alpha_{p+i} = \alpha_{p-i+1}$.

Notons que l'étude de la représentation $\mathbb{Q}$-régulière de G représentée en dimension ℓ par l'ordre maximal $\mathbb{Z} \times \mathbb{Z}(\zeta)$ de $\mathbb{Q}[G]$, muni de la base $((1,0),(0,1),(0,\zeta),\cdots,(0,\zeta^{n-1}))$, se ramène directement à la précédente : il suffit de "border" la matrice U_σ et celles de $\mathcal{T}$ par une première ligne $(1,0,\cdots,0)$ et la première colonne transposée de celle-ci.

Considérons maintenant la représentation $\mathbb{Z}$-régulière de G. Cette représentation est donc de degré $n = m$, de polynôme caractéristique $X^m - 1$, et correspond au réseau $\mathbb{Z}[G]$ muni de sa base $(1, \sigma, \sigma^2, \cdots, \sigma^{n-1})$, qui conduit pour σ à la matrice suivante :

$$U_\sigma = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

L'espace $\mathcal{T}$ est constitué des matrices de la forme (*) où les coefficients α_i sont liés par les seules relations $\alpha_i = \alpha_{n-i}\,(= \alpha_{m-i})$: en effet, si l'on pose

$n = 2p$ si n est pair et $n = 2p + 1$ si n est impair, ces matrices dépendent des $p + 1$ paramètres $\alpha_0, \alpha_1, \cdots, \alpha_p$, alors que l'on a vu dans [B-M] que la dimension de $\mathrm{End}_G^s(E)$ est précisément égale à $p + 1$.

4.1. Exemple. $n = 4$, $m = 5$. La représentation s'identifie à celle du groupe G cyclique d'ordre 5 opérant sur $\mathbb{Z}[\zeta_4]$. L'espace $\mathcal{T}$ est de dimension 2. On en considère la base

$$T_1 = \begin{pmatrix} 2 & 0 & -1 & -1 \\ 0 & 2 & 0 & -1 \\ -1 & 0 & 2 & 0 \\ -1 & -1 & 0 & 2 \end{pmatrix} \quad \text{et} \quad T_2 = \begin{pmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 0 \end{pmatrix}.$$

La matrice suivante (qui est la matrice de Gram du réseau A_4 associée au diagramme de Dynkin correspondant) définit une forme $\mathcal{T}$-parfaite :

$$A = T_1 - T_2 = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Les 10 vecteurs minimaux de A se répartissent en 2 orbites auxquelles correspondent les 2 vecteurs de face $F_1 = T_2$ et $F_2 = T_1 - 2T_2$ (il est inutile d'expliciter les faces elles-mêmes). Ces deux vecteurs sont $\mathcal{T}$-équivalents par la matrice

$$M = \begin{pmatrix} -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & -1 \\ -1 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

(trouvée comme matrice dans la base canonique de $\mathbb{R}^4$ d'un élément d'ordre 4 du normalisateur de G dans $\mathrm{Gl}_n(\mathbb{Z})$)).

On est ramené à étudier le premier vecteur de face $F_1 = T_2$. Pour $\rho = 1$, on obtient la forme de matrice $(T_1 - T_2) + 1 \times T_2 = T_1$, $\mathcal{T}$-équivalente à la forme de départ par la matrice

$$M' = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 1 & 0 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

qui correspond au changement de base
$(e_1, \sigma e_1, \sigma^2 e_1, \sigma^3 e_1) \mapsto (e_1+e_2, \sigma(e_1+e_2), \sigma^2(e_1+e_2), \sigma^3(e_1+e_2))$. Il n'y a donc

qu'une seule classe de $\mathcal{T}$-équivalence de formes parfaites (i.e., une seule classe de similitude de G-réseaux parfaits au sens de [B-M]) dans le cas d'un groupe $\mathbb{Q}$-irréductible d'ordre 5 en degré 4 (d'où le fait, trouvé antérieurement par Schoof et Washington, que A_4 réalise le maximum de la constante d'Hermite sur ces G-réseaux).

Le cas des groupes d'ordres 8 et 12 est analogue : on trouve encore une seule classe de réseaux parfaits, en l'occurence semblables à D_4, ce qui donne une nouvelle démonstration du th. 4.3 de [B-M].

4.2. Exemple. $n = 5$, $m = 5$. On s'intéresse dans cet exemple à la représentation régulière sur $\mathbb{Q}$ d'un groupe G cyclique d'ordre 5. Il y a deux classes de représentation intégrale sur $\mathbb{Z}$. L'une est définie par le $\mathbb{Z}$-module $\mathbb{Z} \times \mathbb{Z}[\zeta_4]$, et conduit donc d'après l'exemple précédent à une unique forme parfaite à similitude près, à savoir $A_1 \times A_4$, et l'autre est la représentation régulière sur $\mathbb{Z}$, que nous examinons maintenant.

L'espace $\mathcal{T}$ est de dimension 3 ; c'est l'ensemble de matrices suivant :

$$(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & \beta & \gamma & \gamma & \beta \\ \beta & \alpha & \beta & \gamma & \gamma \\ \gamma & \beta & \alpha & \beta & \gamma \\ \gamma & \gamma & \beta & \alpha & \beta \\ \beta & \gamma & \gamma & \beta & \alpha \end{pmatrix},$$

dont on définit une base (T_1, T_2, T_3) par l'égalité $(\alpha,\beta,\gamma) = \alpha T_1 + \beta T_2 + \gamma T_3$. On vérifie que les deux matrices suivantes

$$M = \begin{pmatrix} 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad M' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

sont des matrices de $\mathcal{T}$-équivalence ; M, d'ordre infini, est dans le commutant de G dans $\mathrm{Gl}_n(\mathbb{Z})$, et M', d'ordre 2, dans son normalisateur. Dans la base (T_1, T_2, T_3), les transformations $\Gamma : X \mapsto {}^tMXM$ et $\Gamma' : X \mapsto {}^tM'XM'$ sont définies par les matrices

$$\Gamma : \begin{pmatrix} 3 & -4 & 2 \\ -2 & 4 & -1 \\ 1 & -1 & 1 \end{pmatrix} \quad \text{et} \quad \Gamma' : \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

La matrice de Gram du réseau A_5 dans une base de Korkine-Zolotareff est de la forme

$$A = (2,1,1) = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix};$$

elle est parfaite donc $\mathcal{T}$-parfaite, et possède 15 vecteurs minimaux, répartis en trois orbites représentées par les vecteurs $(1,0,0,0,0)$, $(1,-1,0,0,0)$ et $(1,0,-1,0,0)$. Les projections sur $\mathcal{T}$ correspondantes ont pour composantes dans la base duale (T_1^*, T_2^*, T_3^*)

$$\Omega_1 = (1,0,0),\ \Omega_2 = (2,0,0) \text{ et } \Omega_3 = (2,0,-2).$$

Les matrices de face $F_{i,j}$ orthogonales aux matrices Ω_i et Ω_j ont pour composantes dans la base (T_1, T_2, T_3)

$$F_{1,2} = (0,0,-1), \quad F_{1,3} = (0,-1,0) \text{ et } F_{2,3} = (1,1,1).$$

Les faces $F_{1,2}$ et $F_{1,3}$ sont échangées par l'involution Γ', et $F_{2,3}$ est une impasse, la forme quadratique qui lui est associée étant $(x_1+x_2+x_3+x_4+x_5)^2$. La forme contiguë à A le long de $F_{1,2}$ est $B = A + F_{1,2}$ (on a $\rho = 1$), qui est équivalente à une matrice de Gram du réseau D_5 (réseau de racines de déterminant 4).

Par des calculs analogues que nous ne reproduirons pas faute de place, on trouve que B a 4 faces : une impasse, deux faces échangées par $\Gamma' \circ \Gamma^{-1}$ et $\mathcal{T}$-équivalentes à A, et une face dont la forme contiguë C s'interprète comme matrice de Gram du réseau A_5^3 de Coxeter, et est équivalente à la forme Z de Korkine-Zolotareff.

La forme C elle-même a 3 faces, dont l'une a pour forme contiguë B et les deux autres, qui se correspondent par $\Gamma' \circ \Gamma^{-1}$, ont pour formes contiguës des formes R et R' équivalentes à la forme notée Λ_5 dans [B-M], th. 5.3, laquelle est égale à $\frac{1}{5}(10T_1 - 5T_2 + T_3)$.

Enfin, la forme R a 3 faces, dont 2 sont $\mathcal{T}$-équivalentes et ont des formes contiguës $\mathcal{T}$-équivalentes à elle-même, et la troisième est bien sûr équivalente à C. Le graphe de contiguïté modulo $\mathcal{T}$-équivalence est le suivant (les formes soulignées ont une impasse, et la forme entourée est contiguë à elle-même) :

$$\boxed{R}\text{—}C\text{—}\underline{B}\text{—}\underline{A}.$$

Le diagramme de contiguïté complet peut se représenter en dimension 2 (dans une section plane du cône de Voronoï). En envoyant à l'infini dans la direction verticale le point $(5, 10, 10)$, sommet commun à toutes les formes équivalentes à R, on obtient la figure suivante limitée vers le bas par les impasses, dans laquelle Γ s'interprète comme la translation transformant $(2, 1, 0)$ en $(2, 0, 1)$, $(2, 1, 1)$ en $(4, -1, 2)$, ... et Γ' comme la symétrie par rapport à l'axe de symétrie vertical du domaine de $(2, 1, 1)$. Ce diagramme est reproduit à la fin du paragraphe.

4.3. Exemple. $n = 6$, $m = 7$ ou 9. Dans ces deux cas, que nous ne détaillons pas, l'espace $\mathcal{T}$ est de dimension 3 et les graphes de contiguïté à $\mathcal{T}$-équivalence près sont réduits à deux formes, que nous donnons dans les notations classiques des réseaux de dimension 6 :

$$A_6 \text{——} P_6 \qquad \text{et} \qquad E_6 \text{——} E_6^* .$$

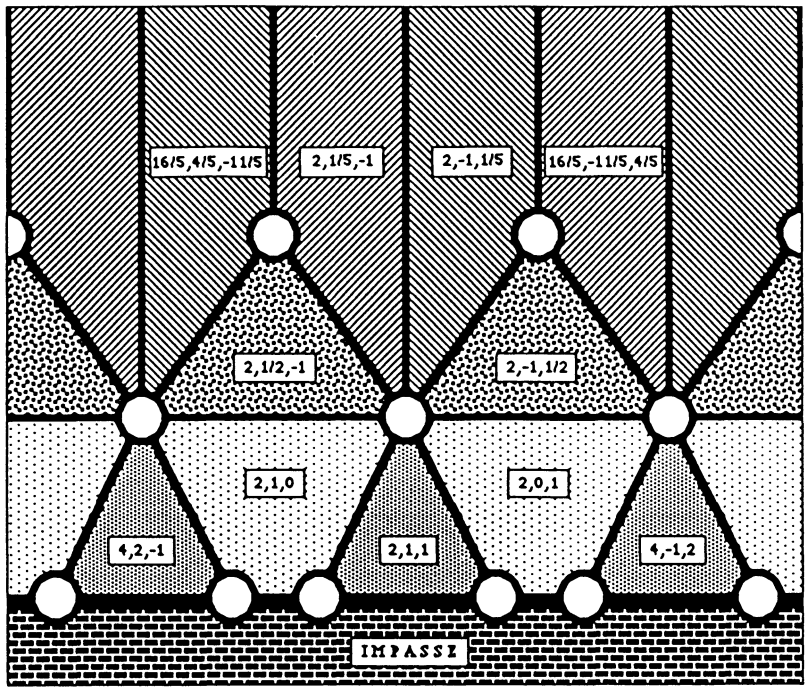
On retrouve encore les résultats de [B-M] (th. 4.6). Signalons que dans le cas de E_6 ($m = 9$), les 36 couples de vecteurs minimaux se répartissent en 4 orbites, mais que seulement 3 des projections associées sur $\mathcal{T}$ sont des arêtes du cône de Voronoï.

4.4 Exemple. $n = 8$, $m = 15$, 16, 20, 24. L'étude n'a été faite qu'à équivalence près, et non pas à $\mathcal{T}$-équivalence près. Les résultats corroborent ceux qui sont annoncés dans [B-M], § 6, et indiquent que dans le cas du groupe d'ordre 20 non traité dans [B-M], E_8 est probablement le seul réseau G-parfait.

[Une erreur typographique s'est glissée dans [B-M] ; dans les données numériques relative à $q = 15$, il faut remplacer $(-1, 0, 0)$ par $(1, 0, 0)$.]

4.5 Exemple. Les calculs effectués en dimension 12 pour le groupe $2A_4$ d'ordre 24 ont permis de trouver 8 réseaux G-parfaits. Parmi ceux-ci se trouve l'exemple connu de $\Lambda_{12}^{\max}$ ([C-S1], ch. 6, [C-S3], § 1), mais aussi un réseau de même déterminant possédant 312 couples de vecteurs minimaux, dont nous avons vérifié qu'il était isométrique à $\Lambda_{12}^{\min}$, prouvant l'existence pour ce réseau d'une structure de module sur l'ordre de Hurwitz. Ces réseaux ont été trouvés indépendamment par M. Laïhem par une méthode de balayage. Les réseaux G- parfaits ont probablement tous été trouvés, mais une démonstration de ce résultat nécessiterait des calculs peut-être trop importants.

Les domaines de Voronoï de l'exemple 4.2.



Dans la figure ci-dessus, les triangles au-dessus de l'impasse sont associés à la forme A, provenant du réseau A_5, et les trapèzes à la forme B, provenant du réseau D_5. Les triangles qui se trouvent au-dessus des domaines décrits ci-dessus sont associés à la forme C, provenant du réseau A_5^3 de Coxeter. Enfin, les domaines du haut de la figure, dont le sommet commun est rejeté à l'infini, sont associés à la forme R, provenant du réseau Λ_5 de [B-M].

§ 5. Indications sur l'algorithme à section donnée. On étudie dans ce § l'exemple 1.4 cité dans l'introduction.

Rappelons que l'on s'est donné une forme Q_0 définie positive à $r < n$ variables et que l'on étudie l'ensemble $\mathcal{E}$ des formes $Q \in \mathcal{Q}_n$ telles que $Q(x_1, \ldots, x_r, 0, \ldots, 0) = Q_0(x_1, \ldots, x_r)$ et $m(Q) = m(Q_0)$. (En termes de réseaux, cela revient à imposer la norme et la section par un sous-espace de dimension r.) On peut montrer que les formes qui réalisent dans $\mathcal{E}$ un maximum local de l'invariant d' Hermite sont $\mathcal{T}$-parfaites pour $\mathcal{T} = \{Q \in \mathcal{Q}_n \mid Q(x_1, \ldots, x_r, 0, \ldots, 0) = 0\}$. Les matrices de $\mathcal{T}$ sont de la

forme

$$\begin{pmatrix} O & M \\ {}^tM & N \end{pmatrix}, \text{ avec } N \text{ symétrique d'ordre } n-r,$$

et la projection Ω_X de

$$P_X = \begin{pmatrix} M_0 & M \\ {}^tM & N \end{pmatrix},$$

est

$$\Omega_X = \begin{pmatrix} O & M \\ {}^tM & N \end{pmatrix},$$

de sorte que les vecteurs minimaux de Q_0 ont une projection nulle. Notons que l'équivalence de deux matrices de $\mathcal{E}$ correspond en termes de réseaux à un endomorphisme de E qui stabilise le réseau et dont la restriction à la section donnée est une isométrie de cette section sur son image. La $\mathcal{T}$-équivalence exige de plus que l'endomorphisme stabilise la section.

On montre facilement que l'hypothèse 2.2 (qui entraîne la connexité du graphe de Voronoï) est vérifiée, et même un peu plus, à savoir que les vecteurs minimaux d'une forme $\mathcal{T}$-parfaite qui ne sont pas dans la section engendrent $\mathbb{R}^n$.

Le cas de la dimension $r = n-1$ est particulièrement simple. L'espace vectoriel euclidien $\mathcal{T}$ est alors de dimension n et peut être identifié à $\mathbb{R}^n$ par

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_1 \\ 0 & 0 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \\ a_1 & a_2 & \dots & 0 & a_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

muni du produit scalaire $X * Y = 2(x_1y_1 + \cdots + x_{n-1}y_{n-1}) + x_ny_n$. Ainsi, une forme $Q \in \mathcal{E}$ est $\mathcal{T}$-parfaite si et seulement si les vecteurs minimaux de Q dont la dernière composante n'est pas nulle engendrent $\mathbb{R}^n$. On montre en outre que s'il en est ainsi et si Q_0 est parfaite, alors Q est elle-même parfaite.

M. Laïhem ([L]) a entrepris à Bordeaux des calculs étendus concernant le cas où Q_0 est l'une des 33 formes parfaites de rang 7, Q elle-même étant de rang 8. Le nombre de classes de formes parfaites contenant une forme Q_0 donnée peut être très important (par exemple, 93 dans le cas de la forme P_7^{11} de [C-S2]). À l'opposé, dans le cas de $Q_0 = P_7^2 \sim E_7^*$ (l'unique forme parfaite entière de norme 3 en dimension 7), on trouve une seule forme parfaite Q, qui n'est entière que pour le minimum 6. Cela montre qu'une forme parfaite de dimension 8, entière et de minimum 3, s'il en existe, ne contient aucune section parfaite de norme 3 (sauf bien sûr en dimension 1).

BIBLIOGRAPHIE

[Ba] E.S. Barnes, *The complete enumeration of extreme senary forms*, Philos. Trans. Roy. Soc. London **249, A** (1957), 461–505.

[B-M] A.-M. Bergé et J. Martinet, *Réseaux extrêmes pour un groupe d'automorphismes*, Astérisque (1991), à paraître.

[C-S1] J. H. Conway et N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, Heidelberg, 1988.

[C-S2] J. H. Conway et N.J.A. Sloane, *Low-dimensional lattices III. Perfect forms*, Proc. R. Soc. Lond. **A 418** (1988), 43–80.

[C-S3] J. H. Conway et N.J.A. Sloane, *Complex and Integral Laminated Lattices*, Trans. Amer. Math. Soc. **280** (1983), 463–490.

[K-Z] A.Korkine et G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. **11** (1877), 242–292.

[J] D.-O. Jaquet, *thèse*, Université de Neuchâtel, 1991.

[L] M. Laïhem, *thèse*, en préparation.

[R] D.S. Rim, *Modules over finite groups*, Ann. of Math. **69** (1959), 700–712.

[Se] J.-P. Serre, *Corps locaux (troisième édition)*, Hermann, Paris, 1980.

[Sw] R.G. Swan, *Induced representations and projective modules*, Ann. of Maths. **71** (1960), 552–578.

[V] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. **133** (1908), 97–178.

A.-M. B. *et* J.M.
CeReMaB
Université Bordeaux I
351, cours de la Libération
F-33405 Talence cedex

F.S.
Dépt. de Mathématiques
Université de Neuchâtel
Chantemerle 20
CH-2007 Neuchâtel

Astérisque

VALÉRIE BERTHÉ

De nouvelles preuves « automatiques » de transcendance pour la fonction zêta de Carlitz

Astérisque, tome 209 (1992), p. 159-168

<http://www.numdam.org/item?id=AST_1992__209__159_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

De nouvelles preuves "automatiques" de transcendance pour la fonction zêta de Carlitz

Valérie BERTHÉ

1 Introduction

Soit $\mathbf{F}_q$ le corps à q éléments, q étant une puissance entière strictement positive de p premier. On note $\mathbf{F}_q[x]$ l'anneau des polynômes à une indéterminée sur $\mathbf{F}_q$ et $\mathbf{F}_q(x)$ le corps des fractions rationnelles en x. Le complété de $\mathbf{F}_q(x)$ pour la valuation $(1/x)$–adique, définie par $v(E) = -d^\circ E$, est le corps $\mathbf{F}_q((1/x))$ des séries formelles de Laurent, c'est-à-dire

$$\mathbf{F}_q((1/x)) = \{a_d x^d + \ldots + a_1 x + a_0 + \frac{a_{-1}}{x} + \ldots \ ; \ \ a_n \in \mathbf{F}_q \ \}.$$

En 1935, Carlitz a défini une fonction ζ, à valeurs dans $\mathbf{F}_q((1/x))$, de la façon suivante:

$$\zeta(m) = \sum_{G \in \mathbf{F}_q[x] \text{ et } G \text{ unitaire}} 1/G^m \ , \quad m \geq 1.$$

La fonction ζ de Carlitz est l'analogue en caractéristique finie de la fonction ζ de Riemann. Carlitz a ainsi établi dans [4] que, pour s divisible par $(q-1)$, $\zeta(s)/\Pi^s \in \mathbf{F}_q(x)$, avec

$$\Pi = \prod_{j=0}^{+\infty} (1 - \frac{x^{q^j} - x}{x^{q^{j+1}} - x}).$$

Cette propriété est l'équivalent du résultat d'Euler sur les valeurs paires de la fonction ζ de Riemann, à savoir $\zeta(2n)/\pi^{2n}$ est rationnel pour n non nul. Notons que le groupe des unités de $\mathbf{F}_q[x]$ est $\mathbf{F}_q^*$, d'ordre $q-1$, alors que le groupe multiplicatif de $\mathbf{Z}$ est de cardinal 2. Les congruences modulo 2 dans le cas complexe sont remplacées ici par des congruences modulo $q-1$.

En 1941, Wade prouve dans [12] la transcendance de Π sur $\mathbf{F}_q(x)$. On en déduit la transcendance de $\zeta(s)$ pour $s \equiv 0\ (q-1)$, (valeurs "paires" de s). En 1986-87, Thakur établit dans [11] des résultats d'irrationalité pour $1 \leq s \leq q^2$ alors que Dammame montre l'irrationalité de $\zeta(s)$ pour $1 \leq s \leq q$, ([7]). En 1988, Dammame et Hellegouarch prouvent la transcendance de $\zeta(s)$ pour $1 \leq s \leq q^2$ par la méthode de Wade, ([10]). Enfin, en 1989, Dammame établit dans [8], voir aussi [9], la preuve de la transcendance de $\zeta(s)$ pour tout s. Parallèlement, Yu prouve en 1988, par une méthode utilisant les modules de Drinfeld, que pour tout entier s non nul, $\zeta(s)$ est transcendant et pour tout entier s non divisible par $q-1$, $\zeta(s)/\Pi^s$ est transcendant, (la preuve est parue dans [13]).

Par ailleurs, en 1989, Allouche donne dans [2] une preuve "élémentaire" de la transcendance de Π , c'est-à-dire qui utilise le théorème de Christol, Kamae, Mendès France et Rauzy, (voir [5]), énoncé ci-dessous:

THÉORÈME **1 (Christol, Kamae, Mendès France et Rauzy)**
Soit $(u(n))_{n\in\mathbf{N}}$ une suite à valeurs dans $\mathbf{F}_q$. Il y a équivalence entre les trois conditions suivantes:
1) la série formelle $\sum_{n\geq 0} u(n)x^{-n}$ est algébrique sur $\mathbf{F}_q(x)$,
2) l'ensemble E des sous-suites de la suite $(u(n))_{n\in\mathbf{N}}$ défini par

$$E = \{(u(q^k n + r))_{n\in\mathbf{N}};\quad k \geq 0;\quad 0 \leq r \leq q^k - 1\}$$

est fini,
3) la suite $(u(n))_{n\in\mathbf{N}}$ est q-automatique.

Seule l'équivalence entre les conditions 1 et 2 intervient dans nos preuves de transcendance. La condition 3 montre le lien qui existe entre le critère d'algébricité donné par la condition 2 et les automates. Rappelons, (voir [1] ou [6]), qu'un q-automate est défini par la donnée de:

- un ensemble fini d'états $S = \{i = a_1, a_2, \ldots, a_d\}$, dont on a privilégié un élément i, appelé état initial,
- q applications ou "flèches" de l'ensemble des états S dans lui-même, notées $0, 1, \ldots, q-1$,
- une application φ de S dans un ensemble Y, dite fonction de sortie.

Une suite $(u(n))_{n\in\mathbf{N}}$ à valeurs dans Y est dite q-automatique si elle est engendrée par un q-automate de la façon suivante: considérons un entier n, écrivons-le en base q en identifiant les chiffres de son développement aux applications $0, 1, \ldots, q-1$; en lisant les chiffres de n de droite à gauche, on obtient

une application composée de S dans lui-même. Soit a_f l'image de l'état initial i par cette application, on pose alors: $u(n) = \varphi(a_f)$.

Allouche étudie, en fait, le quotient α/Π, avec

$$\alpha = \prod_{j=0}^{+\infty}(1 - \frac{x^{q^j}}{x^{q^{j+1}}}).$$

Notons que α est algébrique sur $\mathbf{F}_q(x)$, il suffit de considérer α^q pour s'en convaincre.

M'inspirant du résultat d'Allouche, je donne ici une preuve "automatique" de la transcendance de $\zeta(s)/\Pi^s$ pour $1 \leq s \leq q-2$. Il est, en effet, intéressant de multiplier $\zeta(s)/\Pi^s$ par α^s. On obtient ainsi une expression simple des coefficients du développement en série formelle de $\frac{\zeta(s)}{\Pi^s}\alpha^s$. L'étude des sous-suites de la forme $(u(q^k n + 1 + s(q + q^2 + \ldots + q^{k-1})))_{n\in\mathbf{N}}$, avec $(u(n))_{n\in\mathbf{N}}$ définie par

$$\frac{\zeta(s)}{\Pi^s}\alpha^s = \sum_{n\geq 0} u(n)x^{-n},$$

montre qu'il existe un nombre infini de telles suites. On déduit alors du théorème de Christol, Kamae, Mendès France et Rauzy, les transcendances de $\frac{\zeta(s)}{\Pi^s}\alpha^s$ et de $\zeta(s)/\Pi^s$, α étant algébrique sur $\mathbf{F}_q(x)$.

Je vais dans une première partie de cet article me restreindre au cas où $s = 1$, puis j'indiquerai comment généraliser la méthode employée au cas où s est dans l'intervalle $[1, q-2]$.

2 Preuve de la transcendance de $\zeta(1)/\Pi$

L'objet de ce paragraphe est de démontrer le théorème suivant:

THÉORÈME **2** *Pour $q \neq 2$, $\zeta(1)/\Pi$ est transcendant sur $\mathbf{F}_q(x)$.*

Thakur a établi dans [11] que, pour $1 \leq s \leq q$,

$$\zeta(s) = 1 + \sum_{k=1}^{+\infty}(-1)^{ks}\prod_{j=1}^{k}(\frac{1}{x^{q^j} - x})^s.$$

On obtient alors:

$$\frac{\alpha}{\Pi}\zeta(1) = \frac{\alpha}{\Pi} + \sum_{k=1}^{+\infty}(-1)^k(\frac{1}{x})^{q+\ldots+q^k}\prod_{j=k+1}^{+\infty}(1 - (\frac{1}{x})^{q^j-1}).$$

2.1 Quelques développements en série formelle

Pour appliquer le théorème de Christol, Kamae, Mendès France et Rauzy, nous avons besoin du développement en série formelle de $\frac{\alpha}{\Pi}\zeta(1)$. On remarque que le produit

$$\prod_{j=k+1}^{+\infty}(1-(\frac{1}{x})^{q^j-1})$$

intervient à la fois dans les expressions de $\frac{\alpha}{\Pi}(\zeta(1)-1)$ et de $\frac{\alpha}{\Pi}$, pour $k=0$. Considérons donc le développement en série formelle de

$$\prod_{j=k+1}^{+\infty}(1-(\frac{1}{x})^{q^j-1})$$

On note que, si n s'écrit sous la forme

$$n=\sum_{i=k+1}^{+\infty}\varepsilon_i(q^i-1) \text{ avec } \varepsilon_i=0 \text{ ou } 1, \varepsilon_i=0 \text{ pour } i \text{ assez grand},$$

une telle décomposition est unique.

Par conséquent, soit $(a_k(n))_{n\in\mathbf{N}}$ la suite définie par

$$\prod_{j=k+1}^{+\infty}(1-(\frac{1}{x})^{q^j-1})=\sum_{n\geq 0}a_k(n)x^{-n}$$

Si n s'écrit:

$$n=\sum_{i=k+1}^{+\infty}\varepsilon_i(q^i-1) \text{ avec } \varepsilon_i=0 \text{ ou } 1, \varepsilon_i=0 \text{ pour } i \text{ assez grand},$$

$$\text{alors } a_k(n)=(-1)^{\sum_{i=k+1}^{+\infty}\varepsilon_i},$$

sinon $a_k(n)=0$.

La proposition suivante correspond au cas où $k=0$:

PROPOSITION 1 *Soit* $(a(n))_{n\in\mathbf{N}}$ *la suite définie par*

$$\frac{\alpha}{\Pi}=\sum_{n\geq 0}a(n)x^{-n}$$

Si n *s'écrit:*

$$n=\sum_{k=1}^{+\infty}\varepsilon_i(q^i-1) \textit{ avec } \varepsilon_i=0 \textit{ ou } 1, \varepsilon_i=0 \textit{ pour } i \textit{ assez grand},$$

$$\textit{alors } a(n)=(-1)^{\sum_{i=1}^{+\infty}\varepsilon_i},$$

sinon $a(n)=0$.

On a, en outre,

$$\frac{\alpha}{\Pi}(\zeta(1)-1)=\sum_{k=1}^{+\infty}(-1)^k(\frac{1}{x})^{q+\ldots+q^k}\sum_{n\geq 0}a_k(n)(\frac{1}{x})^n.$$

Par conséquent,

$$\frac{\alpha}{\Pi}(\zeta(1)-1)=\sum_{n\geq 0}(\frac{1}{x})^n\sum_{1\leq k\ \text{tq}\ q+\ldots+q^k\leq n}(-1)^k a_k(n-(q+\ldots+q^k)).$$

Or on montre le lemme suivant:

LEMME 1 *Si n s'écrit sous la forme*

$$n=q+\ldots+q^i+\sum_{j=i+1}^{+\infty}\varepsilon_j(q^j-1) \tag{1}$$

avec $i\geq 1, \varepsilon_j=0$ ou $1, \varepsilon_j=0$ pour j assez grand,

une telle décomposition est unique.

On en déduit la proposition 2:

PROPOSITION 2 *Soit $(b(n))_{n\in\mathbf{N}}$ la suite définie par*

$$\frac{\alpha}{\Pi}(\zeta(1)-1)=\sum_{n\geq 0}b(n)x^{-n}$$

On a:

$b(n)\neq 0$ si et seulement si n s'écrit sous la forme

$$n=q+\ldots+q^i+\sum_{j=i+1}^{+\infty}\varepsilon_j(q^j-1),$$

avec $i\geq 1, \varepsilon_j=0$ ou 1, et $\varepsilon_j=0$ pour j assez grand.

2.2 Schéma de la preuve du théorème 2

Soit $(c(n))_{n\in\mathbf{N}}$ définie par

$$\frac{\alpha}{\Pi}\zeta(1)=\sum_{n\geq 0}c(n)x^{-n}$$

On a

$$(c(n))_{n\in\mathbf{N}}=(a(n))_{n\in\mathbf{N}}+(b(n))_{n\in\mathbf{N}}$$

Nous allons considérer les sous-suites $(c(q^k n+1+q+\ldots+q^{k-1}))_{n\in\mathbf{N}}$ pour $k\geq 3$ et démontrer la proposition suivante:

PROPOSITION **3** *Soit $k \geq 3$. Soit $f(k) = q^k - 1 - (1+q+\ldots+q^{k-1})$. L'indice du premier terme non nul de la sous-suite $(c(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}$ est $n = q + q^2 + \ldots + q^{f(k)}$.*

Cette proposition résulte de deux lemmes concernant les sous-suites $(a(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}$ et $(b(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}$, énoncés ci-dessous:

LEMME **2** *Soit $k \geq 2$. Soit $f(k) = q^k - 1 - (1 + q + \ldots + q^{k-1})$. L'indice du premier terme non nul de la sous-suite $(a(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}$ est $n = q + q^2 + \ldots + q^{f(k)}$.*

LEMME **3** *Soit $k \geq 3$. Soit $g(k) = q^k - 2 - (q^2 + \ldots + q^{k-1})$. L'indice du premier terme non nul de la sous-suite $(b(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}$ est $n = q + q^2 + \ldots + q^{g(k)}$.*

On a $f(k) < g(k)$, $\forall k \geq 3$. On rappelle, de plus, que la suite $(c(n))_{n\in\mathbf{N}}$ est définie comme la somme des suites $(a(n))_{n\in\mathbf{N}}$ et $(b(n))_{n\in\mathbf{N}}$. La proposition 3 résulte donc des lemmes 2 et 3.

Par ailleurs, si $q \neq 2$, la suite $(f(k))_{k\geq 3}$ est strictement croissante. Les sous-suites $(c(q^k n+1+q+\ldots+q^{k-1}))_{n\in\mathbf{N}}$ diffèrent alors par l'indice de leur premier terme non nul. Elles sont donc distinctes et l'ensemble

$$\{(c(q^k n + 1 + q + \ldots + q^{k-1}))_{n\in\mathbf{N}}\}$$

est infini. L'ensemble $\{(c(q^k n + r))_{n\in\mathbf{N}};\ \ k \geq 0;\ \ 0 \leq r \leq q^k - 1\}$ est, à plus forte raison, infini. Selon le théorème de Christol, Kamae, Mendès France et Rauzy, on en déduit la transcendance de $\frac{\alpha}{\Pi}\zeta(1)$ sur $\mathbf{F}_q(x)$ pour $q \neq 2$ et, par conséquent, celle de $\frac{\zeta(1)}{\Pi}$, ce qui achève la preuve du théorème 2.

2.3 Preuve du lemme 2

Nous donnons ici la preuve du lemme 2; on démontre le lemme 3 de manière analogue.
On pose $(\alpha_k(n))_{n\in\mathbf{N}}$ la suite définie par:

$$\alpha_k(n) = a(q^k n + 1 + q + \ldots + q^{k-1}) \quad \forall n \in \mathbf{N}.$$

Soit $k \geq 2$. Soit $n \in \mathbf{N}$ tel que $\alpha_k(n) \neq 0$. Selon la proposition 1,

$$\exists\ (\varepsilon_j)_{j\in\mathbf{N}} \text{ avec } \varepsilon_j = 0 \text{ ou } 1, \varepsilon_j = 0 \text{ pour } j \text{ assez grand, tels que}$$

$$q^k n + 1 + q + \ldots + q^{k-1} = \sum_{j=1}^{+\infty} \varepsilon_j (q^j - 1),$$

c'est-à-dire

$$q^k n + 1 + q + \ldots + q^{k-1} = \sum_{1 \le j \le k-1} \varepsilon_j (q^j - 1) + \sum_{l \ge k} \varepsilon_l (q^l - 1).$$

On pose $\sigma = \sum_{j=1}^{+\infty} \varepsilon_j$. On a

$$q^k n + 1 + q + \ldots + q^{k-1} = \sum_{1 \le j \le k-1} \varepsilon_j q^j + \sum_{l \ge k} \varepsilon_l q^l - \sigma.$$

Par conséquent,

$$\exists \lambda \ge 1 \text{ tel que } \sigma = \lambda q^k + \sum_{1 \le j \le k-1} (\varepsilon_j - 1) q^j - 1.$$

On en déduit que

$$n = (-\lambda + \varepsilon_k) + \sum_{l > k \text{ et } \sum_{l>k} \varepsilon_l = \mathcal{S}} \varepsilon_l q^{l-k}, \tag{2}$$

$$\begin{aligned} \text{avec } \mathcal{S} &= \sigma - \sum_{j \le k} \varepsilon_j \\ &= \lambda q^k + \sum_{j=1}^{k-1} (\varepsilon_j - 1) q^j - \sum_{j \le k} \varepsilon_j - 1. \end{aligned}$$

On vérifie réciproquement que si n s'écrit sous la forme (2), on a alors, selon la proposition 1, $\alpha_k(n) \neq 0$.

Soit $m(k)$ le plus petit m tel que $\alpha_k(m) \neq 0$, c'est-à-dire le plus petit m pouvant s'écrire sous la forme (2). On vérifie que $m(k)$ est obtenu pour

$$\lambda = 1$$

$$\varepsilon_j = 0 \text{ pour } 1 \le j \le k-1$$

$$\varepsilon_k = 1$$

$$\varepsilon_l = 1 \text{ pour } k+1 \le l \le k + q^k - 1 - (1 + \ldots + q^{k-1})$$

$$\varepsilon_l = 0 \text{ pour } l > k + q^k - 1 - (1 + \ldots + q^{k-1})$$

On a alors $m(k) = q + \ldots + q^{f(k)}$ avec $f(k) = q^k - 1 - (1 + \ldots + q^{k-1})$, ce qui achève la preuve du lemme 2.

3 Preuve de la transcendance de $\zeta(s)/\Pi^s$

THÉORÈME 3 *Pour $q \neq 2$ et $1 \leq s \leq q-2$, $\zeta(s)/\Pi^s$ est transcendant sur $\mathbf{F}_q(x)$.*

Nous nous contenterons ici d'esquisser la preuve de ce théorème, qui est faite sur le modèle de la preuve du théorème 2. On peut en trouver une démonstration détaillée dans [3]. On a vu que, pour $1 \leq s \leq q$,

$$\frac{\zeta(s)\alpha^s}{\Pi^s} = \frac{\alpha^s}{\Pi^s} + \sum_{k=1}^{+\infty} (-1)^{ks} \left(\frac{1}{x}\right)^{s(q+\ldots+q^k)} \prod_{j=k+1}^{+\infty} (1 - \left(\frac{1}{x}\right)^{q^j-1})^s.$$

Le produit $\prod_{j=k+1}^{+\infty} (1 - \left(\frac{1}{x}\right)^{q^j-1})^s$ joue ici encore un rôle déterminant. On a ainsi la proposition suivante:

PROPOSITION 4 *Soit $(A(n))_{n\in\mathbf{N}}$ la suite définie par*

$$\frac{\alpha^s}{\Pi^s} = \sum_{n\geq 0} A(n) x^{-n}.$$

Si n s'écrit

$$n = \sum_{j=1}^{+\infty} \mu_j (q^j - 1) \text{ avec } \mu_j \in \{0, 1, \ldots, s\}, \mu_j = 0 \text{ pour } j \text{ assez grand,}$$

$$\text{alors } A(n) = (-1)^{\sum_{j=1}^{+\infty} \mu_j} \prod_{j=1}^{+\infty} \binom{s}{\mu_j} \text{ modulo } p,$$

sinon $A(n) = 0$.

Rappelons que p désigne la caractéristique de $\mathbf{F}_q$.
Les propriétés d'unicité de décomposition sont conservées pour $1 \leq s \leq q-2$. Néanmoins, la présence du terme $\prod_{j=1}^{+\infty} \binom{s}{\mu_j}$ modulo p apporte une difficulté supplémentaire. Ce terme peut être, en effet, éventuellement nul. La proposition 3 devient alors:

PROPOSITION 5 *Soit $(C(n))_{n\in\mathbf{N}}$ définie par*

$$\frac{\alpha^s}{\Pi^s}\zeta(s) = \sum_{n\geq 0} C(n) x^{-n}$$

Soit $k \geq 3$. Soit $F(k) = q^k - 1 - s(1 + q + \ldots + q^{k-1})$. Soient $u(k)$ et $v(k)$ les reste et quotient de la division euclidienne de $F(k)$ par s.
Soit $M(k) = s - 1 + s \sum_{1\leq l\leq u(k)} q^l + v(k) q^{u(k)+1}$.
On a: $\forall\ n < M(k),\ C(q^k n + 1 + s(q + \ldots + q^{k-1})) = 0$.

On ignore donc, a priori, si $C(q^k M(k) + 1 + s(q + \ldots + q^{k-1}))$ est nul ou non.

Notons que les termes $u(k)$ et $v(k)$ apparaissent lors de la minimisation de $\sum_{l>k} \mu_l$ (voir la preuve du lemme 2, section 2.3), les μ_l pouvant prendre au plus la valeur s. Selon la proposition 5, chacune des sous-suites

$$(C(q^k n + 1 + s(q + \ldots + q^{k-1})))_{n \in \mathbf{N}}$$

débute par au moins $M(k)$ zéros, avec $(M(k))_{k \geq 2}$ strictement croissante. Il suffit alors que les suites

$$(C(q^k n + 1 + s(q + \ldots + q^{k-1})))_{n \in \mathbf{N}}$$

soient toutes non nulles pour former un ensemble infini. Or on a la proposition suivante:

PROPOSITION **6**
Supposons $s \not\equiv 0\ (p)$. *Soit* $k \geq 3$. *Soit* $Q(k) = -1 + s \sum_{1 \leq l \leq q^k - k} q^l$. *On a*

$$C(q^k Q(k) + 1 + s(q + \ldots + q^{k-1})) \neq 0.$$

Par conséquent, si $s \not\equiv 0\ (p)$, l'ensemble

$$\{(C(q^k n + r))_{n \in \mathbf{N}};\quad k \geq 0;\quad 0 \leq r \leq q^k - 1\}$$

est infini. On déduit alors du théorème de Christol, Kamae, Mendès France et Rauzy, les transcendances de $\frac{\alpha^s}{\Pi^s}\zeta(s)$ et de $\frac{\zeta(s)}{\Pi^s}$ sur $\mathbf{F}_q(x)$, (pour $1 \leq s \leq q-2$ et $q \neq 2$).

Il reste alors à traiter le cas où $s \equiv 0\ (p)$.
Écrivons $s = p^t r$ avec r non divisible par p. En appliquant le morphisme de Frobenius à $\zeta(r)/\Pi^r$, on obtient que $(\frac{\zeta(r)}{\Pi^r})^{p^t} = \zeta(s)/\Pi^s$. Or $\zeta(r)/\Pi^r$ est transcendant sur $\mathbf{F}_q(x)$.
On a donc démontré le théorème 3, à savoir: $\zeta(s)/\Pi^s$ est transcendant sur $\mathbf{F}_q(x)$ pour tout s tel que $1 \leq s \leq q-2$.

Notons qu'en appliquant le morphisme de Frobenius à $\zeta(1)/\Pi$, on obtient que $\zeta(q^t)/\Pi^{q^t}$ est transcendant sur $\mathbf{F}_q(x)$ pour $q \neq 2$ et pour tout $t \geq 0$.

Il reste à montrer que $\zeta(s)/\Pi^s$ est transcendant sur $\mathbf{F}_q(x)$ pour tout s non divisible par $q-1$. La plus grande complexité de l'expression de $\zeta(s)/\Pi^s$ pour $s > q$ pose alors des problèmes combinatoires. Il semble néanmoins raisonnable d'espérer que la méthode exposée dans cet article puisse permettre de traiter le cas général.

Bibliographie

[1] J. -P. ALLOUCHE *Automates finis en théorie des nombres*, Expo. Math. **5** (1987), 239-266.

[2] J. -P. ALLOUCHE *Sur la transcendance de la série formelle* Π, Sém. de Théorie des Nombres de Bordeaux **2** (1990), 103-117.

[3] V. BERTHÉ *Fonction zêta de Carlitz et automates*, Actes du colloque Thémate, Luminy (mai 1991), à paraître.

[4] L. CARLITZ *On certain functions connected with polynomials in a Galois field*, Duke Math. J. , 1 (1935), 137-168.

[5] G. CHRISTOL, T. KAMAE, M. MENDÈS FRANCE et G. RAUZY *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401-419.

[6] A. COBHAM *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164-192.

[7] G. DAMMAME *Irrationalité de $\zeta(s)$ dans le corps des séries formelles $\mathbf{F}_q((\frac{1}{t}))$*, C.R. Math. Rep. Acad. Sci. Canada **9, 5** (1987), 207-212.

[8] G. DAMMAME *Transcendance de la fonction zêta de Carlitz par la méthode de Wade*, Thèse , Caen, 1990.

[9] G. DAMMAME et Y. HELLEGOUARCH *Transcendence of the values of the Carlitz zeta function by Wade's method*, J. Number Theory, 39, 3 (1991), p. 257- 278.

[10] G. DAMMAME et Y. HELLEGOUARCH *Propriétés de transcendance des valeurs de la fonction zêta de Carlitz*, C.R. Acad. Sci. Paris **307, Série I** (1988), 635-637.

[11] D. S. THAKUR *Gauss functions and Gauss sums for function fields and periods of Drinfeld modules*, Ph. D. thesis, Harvard (Avril 1987).

[12] L. J. WADE *Certain quantities transcendental over $GF(p^n, x)$*, Duke Math. J. , 8 (1941), 701-720.

[13] J. YU *Transcendence and Special Zeta Values in Characteristic p*, Annals of Mathematics, **134** (1991), 1-23.

Valérie BERTHÉ
E. N. S.
45 rue d'Ulm
75005 Paris

Astérisque

GAUTAMI BHOWMIK

Divisor functions of integer matrices: evaluations, average orders and applications

Astérisque, tome 209 (1992), p. 169-177

<http://www.numdam.org/item?id=AST_1992__209__169_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

DIVISOR FUNCTIONS OF INTEGER MATRICES: EVALUATIONS, AVERAGE ORDERS AND APPLICATIONS

Gautami BHOWMIK*

Divisor functions have been extensively studied in classical number theory. We examine the corresponding functions for matrices over the ring of integers. These functions not only are a natural generalisation of historically important concepts, but their study also yields applications and some new interpretations.

We deal only with $r \times r$ nonsingular matrices with entries from the ring of integers. Since there are an infinite number of unimodular matrices, it is necessary to identify *canonical factorisations* of matrices. In his study of arithmetic of matrices, Nanda [8] defines them as follows:

DEFINITION 1. The decomposition of the matrix A as

$$A = A_1 A_2 \dots A_k, \tag{1}$$

where $A_k, A_{k-1}, \dots, A_2$ are matrices in nonsingular Hermite Normal Form (HNF), is said to be a k-order (canonical) factorisation of A.

Since an HNF matrix uniquely represents a class under one-sided equivalence, two factorisations defined as in (1) are *inequivalent*.

* Research supported in part by the Deutscher Akademischer Austauschdienst.

DEFINITION 2. The function $\tau_k^{(r)}$ counts the number of k-order factorisations of an $r \times r$ matrix A, i.e.,

$$\tau_k^{(r)}(A) = \sum_{A=A_1A_2\ldots A_k} 1. \tag{2}$$

When we restrict ourselves to the case $k = 2$, A_2 above is called a *divisor* of A. As in classical theory, we define the functions $\sigma_a^{(r)}$.

DEFINITION 3. For a non-negative integer a, let $\sigma_a^{(r)}(A)$ be the sum of the a^{th} powers of the determinants of divisors of a matrix A, i.e.,

$$\sigma_a^{(r)}(A) = \sum_{A=A_1A_2} (\det A_2)^a. \tag{3}$$

We notice that $\tau_2^{(r)} = \sigma_0^{(r)}$.

Evaluations

For evaluating divisor functions, it is enough to consider A to be in non-singular Smith Normal Form (SNF) with prime-power determinant. We use the notation F_r for the matrix

$$\left(\text{diag}\,[p^{f_1}, p^{f_1+f_2}, \ldots, p^{f_1+f_2+\cdots+f_r}]\right)$$

and may also denote it by $\langle f_1, f_2, \ldots, f_r\rangle$, where $f_1 \geq 1$, $f_i \geq 0$ for $i > 1$, and p is a prime number. We write G_r for the matrix $\langle f_1, f_2, \ldots, f_{r-1}, f_r - 1\rangle$.

It is clear that the evaluation of $\sigma_a^{(r)}$ involves the solving of a system of diophantine equations with rather stringent side conditions and is therefore not easy.

In [4] we proved the result:

$$\tau_2(F_r) - \tau_2(G_r) = \sigma_1(F_{r-1}), \tag{4}$$

which helped us evaluate $\tau_2^{(2)}$ and $\tau_2^{(3)}$. Here we generalise (4) and prove a recurrence between $\sigma_a^{(r)}$ and $\sigma_{a+1}^{(r-1)}$. Thus it becomes possible to reduce the problem to evaluations on F_1 or on *prime matrices* $P_r = \langle 1, 0, \ldots, 0\rangle$. We prove:

THEOREM 1. $\sigma_a(F_r) - p^a\sigma_a(G_r) = \sigma_{a+1}(F_{r-1})$.

Proof. Let $\nu = f_1 + f_2 + \ldots + f_r$. Now

$$F_r = \begin{pmatrix} A_{r-1} & 0 \\ Y & p^t \end{pmatrix} \begin{pmatrix} B_{r-1} & 0 \\ X & p^{\nu-t} \end{pmatrix}, \qquad 0 \le t \le \nu \tag{5}$$

$$G_r = \begin{pmatrix} A_{r-1} & 0 \\ Y & p^t \end{pmatrix} \begin{pmatrix} B_{r-1} & 0 \\ X & p^{\nu-t-1} \end{pmatrix}, \qquad 0 \le t < \nu \tag{6}$$

are factorisations of F_r and G_r whenever B_{r-1} is a divisor of F_{r-1} and $YB_{r-1} + Xp^t = 0$. Then

$$\sigma_a(F_r) = \sum_{\substack{YB_{r-1}+Xp^t=0 \\ 0\le t<\nu}} (\det B_{r-1})^a\, p^{(\nu-t)a} + \sum_{YB_{r-1}+Xp^\nu=0} (\det B_{r-1})^a \tag{7}$$

and

$$\sigma_a(G_r) = \sum_{\substack{YB_{r-1}+Xp^t=0 \\ 0\le t<\nu}} (\det B_{r-1})^a\, p^{(\nu-t-1)a} \tag{8}$$

Thus

$$\sigma_a(F_r) = p^a\sigma_a(G_r) + \sum_{YB_{r-1}+Xp^\nu=0} (\det B_{r-1})^a. \tag{9}$$

But, as in the proof of (4), we can show that the equation $YB_{r-1} + Xp^\nu = 0$ has solutions for all possible choices of X by considering the cases where the matrix

$$\begin{pmatrix} B_{r-1}^{-1}F_{r-1} & 0 \\ -p^\nu X B_{r-1}^{-1} & p^\nu \end{pmatrix}$$

is integral. Since X can be chosen in $\det(B_{r-1})$ ways, we have:

$$\sigma_a(F_r) = p^a\sigma_a(G_r) + \sum_{B_{r-1} \mid F_{r-1}} (\det B_{r-1})^{a+1}.$$

□

It is easy to evaluate $\sigma_a(P_r)$ by generalising Nanda's result [7] for $a = 0$:

THEOREM 2. $\sigma_a(P_r) = \sum_{j=0}^{r} p^{aj} \begin{bmatrix} r \\ j \end{bmatrix}$, *where* $\begin{bmatrix} r \\ j \end{bmatrix}$ *are the Gaussian polynomials in* p.

Proof. Nanda [7] gives a combinatorial argument to show that the number of divisors of P_r with p occurring exactly j times on the diagonal is given by $\begin{bmatrix} r \\ j \end{bmatrix}$. The factor p^{aj} is obviously the a^{th} power of the determinant of the divisor. □

The above theorems give us a method for evaluation, but the calculations involved are cumbersome, as the following example shows.

EXAMPLE.

$$\begin{aligned}\sigma_1(F_3) &= (p^{f_3} + p^{f_3-1} + \ldots + 1)\sigma_2(F_2) \\ &+ p^{f_3+1}(p+1)(\sigma_2\langle f_1, f_2-1\rangle + p^2\sigma_2\langle f_1, f_2-2\rangle + \ldots + p^{2f_2-2}\sigma_2\langle f_1, 0\rangle) \\ &+ p^{f_3+2f_2+1}\sigma_2\langle f_1-1, 1\rangle + p^{f_3+2f_2+2}(p+1)\sigma_2\langle f_1-1, 0\rangle \\ &+ p^{f_3+2f_2+4}\sigma_2\langle f_1-2, 1\rangle + p^{f_3+2f_2+5}(p+1)\sigma_2\langle f_1-2, 0\rangle + \ldots \\ &+ p^{f_3+2f_2+3f_1+2}(p+1)\sigma_2\langle 1, 0\rangle + p^{f_3+2f_2+3f_1+4}\sigma_1\langle 1, 0\rangle,\end{aligned}$$

where

$$\begin{aligned}\sigma_2(F_2) &= (p^{2f_2} + p^{2f_2-2} + \ldots + 1)\sigma_3\langle f_1\rangle + p^{2f_2+2}(p^2+1)\sigma_3\langle f_1-1\rangle \\ &+ p^{2f_2+6}(p^2+1)\sigma_3\langle f_1-2\rangle + \ldots + p^{2f_2+4f_1-6}(p^2+1)\sigma_3\langle 1\rangle \\ &+ p^{2f_2+4f_1-2}\sigma_2\langle 1\rangle.\end{aligned}$$

Average orders

In [3] we evaluated $T(x) = \sum_{\det A \le x} \tau_2^{(2)}(A)$, where A is in SNF. The absence of a zeta function does not allow satisfactory extension of this result.

Here we instead allow A to be in HNF and consider the following *zeta function* [5]:

$$Z_r(s) = \sum_{A \text{ in HNF, } r\times r} (\det A)^{-s} = \sum \alpha_r(n)\, n^{-s}, \qquad s = \sigma + it, \quad \sigma > 1, \tag{10}$$

where $\alpha_r(n)$ is the HNF class-number, i.e., the number of $r \times r$ HNF matrices with determinant n.

Thus

$$Z_r(s) = \zeta(s)\zeta(s-1)\dots\zeta(s-r+1), \tag{11}$$

where $\zeta(s)$ is the Riemann zeta-function. $Z_r(s)$ is a holomorphic function with simple poles at $s = r, r-1, r-2$. It is, in fact, a special case of the Koecher zeta-function [10].

Authors (e.g. [9]) have evaluated $\alpha_r(n)$, and in [3] we obtained an average order for $\alpha_r(n)$ by using elementary methods.

Here we give a few asymptotic results for divisor functions obtained by using $Z_r(s)$ for

$$A_r(x) = \sum_{n \le x} \alpha_r(n), \quad T_k(x) = \sum_{A \text{ in HNF, } \det A \le x} \tau_k(A)$$

and $S_a^{(r)}(x) = \sum_{A \text{ in HNF, } \det A \le x} \sigma_a^{(r)}(A)$. These are only first results. We should be able to prove sharper results in [5].

THEOREM 3.

$$A_r(x) = \frac{1}{r} L_r x^r - \frac{1}{2(r-1)} L_{r-1} x^{r-1} + o(x^{r-1}),$$

where $L_k = \prod_{j=2}^{k} \zeta(j)$.

Proof. From Perron's formula we have:

$$A_r(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{Z_r(s)\, x^s}{s} ds.$$

The main terms can be obtained as residues at $s = r,\ r-1$. □

THEOREM 4. $T_k(x) \sim P_r(x)$,
where $P_r(x)$ *is a polynomial in* x *of degree* r.

Proof. Obvious. □

THEOREM 5.

$$S_a^{(r)}(x) = \frac{1}{a+r} L_r M_{a,0} x^{a+r} - \frac{1}{2(a+r-1)} L_{r-1} M_{a,1} x^{a+r-1} + o(x^{a+r-1}),$$

where

$$M_{b,t} = \prod_{j=1}^{r} \zeta(b+j-t).$$

Proof. Similar to that of Theorem 3. □

Restricted divisor functions

Here we consider factorisations on the subsets
(*a*) $\mathcal{S}_r$, of all $r \times r$ matrices in SNF, and
(*b*) $\mathcal{D}_r$ of all $r \times r$ diagonal matrices,
and show their connection with average orders of functions of integers.

DEFINITION 4. The decompositions

$$\begin{aligned} & S = S_1 S_2 \dots S_k, && S, S_i \in \mathcal{S}_r \\ \text{and} \quad & D = D_1 D_2 \dots D_k, && D, D_i \in \mathcal{D}_r \end{aligned}$$

are said to be k-order SNF (resp., *diagonal*) *factorisations* of S (resp., D).

In [3] we have defined the SNF *zeta function*

$$\widehat{Z}_r(s) = \sum \beta_r(n)/n^s = \zeta(s)\zeta(2s)\dots\zeta(rs) \tag{12}$$

and proved:

THEOREM 6.

$$\sum_{\substack{S \in \mathcal{S}_r \\ \det S \le x}} \widehat{\sigma}_a(r)(S) = \frac{1}{a+1} L_r^{(1)} K_1 x^{a+1} + \frac{1}{a+\frac{1}{2}} L_r^{(1/2)} K_2 x^{a+\frac{1}{2}} + \frac{1}{a+\frac{1}{3}} L_r^{(1/3)} K_3 x^{a+\frac{1}{3}} + O(x^{a+\varepsilon}).$$

where ε is the best known exponent in the error of the three-dimensional divisor problem, and the constants are defined as

$$L_r^{(i)} = \prod_{\substack{j=1 \\ ji \neq 1}}^{r} \zeta(ji), \qquad K_i = \prod_{j=1}^{r} \zeta(j(a+i)).$$

We can similarly define the *diagonal zeta function* as

$$Z_{\mathcal{D}}(s) = \sum_{D \in \mathcal{D}_r} (\det D)^{-s} = \zeta^r(s) \tag{13}$$

and obtain the average order $B_a^{(r)}(x)$ for diagonal divisor functions. For example, when $a = r = 2$, we get

THEOREM 7.

$$B_2^{(2)} = \tfrac{1}{6} x \log^3 x + (2\gamma - \tfrac{1}{2}) x \log^2 x + (6\gamma^2 - 4\gamma + 4\gamma_1 + 1) x \log x + (-1 + 4(\gamma - \gamma_1 + \gamma_2) - 6\gamma^2 + 4\gamma^3 + 12\gamma\gamma_1) x + O(x^{1/2})$$

where the γ's are constants.

Proof. We use the classical estimate for $\zeta^4(s)$. □

Applications

We can interpret some of the above results in different contexts. We give a few illustrations:

a) We consider the set $\Gamma = \mathrm{GL}(r, \mathbb{Z})$ of all $r \times r$ integer unimodular matrices as the unimodular group of degree r over the ring of integers [6]. The divisor functions of matrices then appear in the formal power series over the *Hecke algebra*, which is a polynomial ring over $\mathbb{Z}$ in infinitely many independent indeterminates. Thus, formally,

$$\sum \Gamma A \Gamma (\det A)^{-s} \sum \Gamma A \Gamma (\det A)^{a-s} = \sum \Gamma A \Gamma \sigma_a(A) (\det A)^{-s}, \tag{14}$$

where $A \in \mathcal{S}_r$.

b) We consider Ramanujan's classical formula

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{(2s-a-b)} = \sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s}$$

for the case $a = 1$, $b = 2$, to get

$$Z_4(s) = \zeta(2s-3)\sum_{n=1}^{\infty}\sigma_1(n)\sigma_2(n)/n^s. \tag{15}$$

c) We can evaluate $\sigma_a(P_r)$ in terms of two different *partition functions*. We can show that to get the number of divisors of P_r, we may look at the number of $\underline{0}$'s to the right of each $\underline{1}$ in every string of length r with entries from $\{0,1\}$. This can be expressed in terms of the function $\hat{q}(n,k,r)$, which counts the number of partitions of n into at most k parts (not necessarily distinct) each at most r, i.e.,

$$\sigma_a(P_r) = \sum\sum q(n-ka,k,r-k)p^n. \tag{16}$$

This, we note, agrees with Theorem 2 via Sylvester's generating function for $\widehat{\sigma}$ (see, e.g. Andrews [1]). We can also evaluate $\sigma_a(P_r)$ using the function $q(n,k,r)$ which counts the number of partitions of n into exactly k distinct parts. In [2] we have shown that the number of divisors of P_r that are equivalent to P_k, $k \leq r$, is given by

$$\pi_{k,r} = \sum_{n=\frac{k(k+1)}{2}}^{kr-\frac{k(k-1)}{2}} q(n,k,r)\, p^{kr-\frac{k(k-1)}{2}-n}. \tag{17}$$

Thus we get

$$\sigma_a(P_r) = \sum\sum q\big(kr-\tfrac{k(k-1)}{2}-n-ak,k,r\big)\, p^n. \tag{18}$$

We see that there is no contradiction between these two results, for we can independently show that

$$\hat{q}(n,k,r-k) = q\big(kr-\tfrac{k(k-1)}{2}-n,k,r\big) \tag{19}$$

by writing n as a sum of parts $n_1,n_2,\ldots,n_k$; $r-k \geq n_i \geq n_{i+j} \geq 0$ and replacing n_i by $m_i = r-n_i-i+1$.

As in [2], it is possible to obtain *polynomial* and *partition identities* from these results.

References

[1] G.E. Andrews, The Theory of Partitions, *Encyclopedia of Math. and its Appl.*, vol. 2, Addison-Wesley Publishing Co., 1976.

[2] G. Bhowmik, Completely Multiplicative Arithmetical Functions of Matrices and Certain Partition Identities, *Journal of Indian Mathematical Society*, 56 (1991), 77–83.

[3] –, Average Orders of Certain Functions Connected with Arithmetic of Matrices (to appear in *JIMS*).
[4] –, The Divisor and Summatory Functions of Integer Matrices (to appear).
[5] – and A. Krieg, Manuscript.
[6] A. Krieg, Hecke Algebras, *Memoirs of the AMS*, no. 435, vol. 87, 1990.
[7] V.C. Nanda, Arithmetic Functions of Matrices and Polynomial Identities, *Colloq. Math. Soc. Janos Bolyai*, 34 (1982), 1107–1126.
[8] V.C. Nanda, Arithmetic of Matrices: Manuscript.
[9] M. Newman, *Integer Matrices*, Academic Press, New York-London, 1972.
[10] A. Terras, *Harmonic Analysis on Symmetric Spaces and Applications II*, Springer-Verlag, New York-Berlin-Heidelberg, 1988.

Gautami Bhowmik
Jesus & Mary College
New Delhi – 110 021
India

Astérisque

TED CHINBURG
BOAS EREZ

Equivariant Euler-Poincaré characteristics and tameness

Astérisque, tome 209 (1992), p. 179-194
<http://www.numdam.org/item?id=AST_1992__209__179_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Equivariant Euler-Poincaré Characteristics and Tameness

Ted CHINBURG[†] and Boas EREZ[‡]

Introduction

In this paper we give a reasonably self-contained discussion of the Euler-Poincaré characteristics defined by Chinburg in the first part of [Ch1]. We show how these arise naturally when studying actions of a finite group G on coherent sheaves. More precisely, suppose $f : X \to Y$ is a tame G-covering of schemes which are proper and of finite type over a noetherian ring A. Let T be a coherent sheaf on X which has an action of G compatible with the action of G on O_X. (The construction we will give applies to bounded complexes of sheaves having coherent terms, but for simplicity we will assume in this introduction that T is a single sheaf.) One then has a naive coherent Euler-Poincaré characteristic

$$\chi(G,T) = \sum_i (-1)^i \cdot [H^i(X,T)]$$

in the Grothendieck group $G_0(AG)$ of all finitely generated AG-modules. We will show here how to lift $\chi(G,T)$ in a canonical way to a more refined Euler-Poincaré characteristic $\chi R\Gamma^+(f_*(T))$ in the Grothendieck group $CT(AG)$ of all finitely generated cohomologically trivial AG-modules. The natural forgetful homomorphism $CT(AG) \to G_0(AG)$ is in general neither surjective nor injective. Thus the existence of a canonical $\chi R\Gamma^+(f_*(T))$ in $CT(AG)$ mapping to $\chi(G,T)$ restricts the possibilities for $\chi(G,T)$ and also provides a more subtle invariant of T.

The motivation for defining $\chi R\Gamma^+(f_*(T))$ is to combine the insight into Euler-Poincaré characteristics arising from classical algebraic geometry and

† Partially supported by NSA and NSF grants.

‡ Partially supported by an NSF grant.

from the theory of the Galois module structure of rings of algebraic integers in tame extensions. For example, many results in algebraic geometry have to do with computing the multiplicities of irreducible representations of G in various cohomology groups. The connection of these multiplicities to character functions, such as Gauss sums, becomes clearer when one uses 'Hom-descriptions' of Grothendieck groups, as suggested by work on algebraic integers. Various results about rings of integers have close geometric counterparts, which in turn may suggest new approaches to studying rings of integers. As one example, Taylor's Theorem connects the stable isomorphism class of the ring of integers in a tame finite Galois extension of number fields to the root numbers appearing in the functional equations of L-series. In [Ch1, Ch2], some conjectural generalizations of Taylor's Theorem to tame G-coverings of schemes are discussed, and results in this direction are proved in the case of smooth projective varieties over a finite field. Over finite fields, one has an alternate approach using l-adic cohomology to proving the Galois Gauss sum congruences which are the deepest arithmetic part of the proof of Taylor's Theorem. (See [Ch1, Sect. 8].) This suggests looking for a new, geometric proof of Taylor's Theorem for rings of integers; at this time we know of no such proof.

In this paper we will focus on how to define $\chi R\Gamma^+(f_*(T))$. The generality of the definition makes it possible to consider examples of a widely varied nature. At the same time, we would like to stress that the definition provides a way of calculating $\chi R\Gamma^+(f_*(T))$.

We now give a quick survey of this paper. Sections 1 - 3 are mainly a summary of known results, definitions and examples which prepare the stage for the new results presented in Sections 4 and 5. In Section 1 we recall the two examples which have motivated essentially all research on Galois module theory. Section 2 is an exposition of some well-known applications of Euler-Poincaré characteristics. In Section 3 we recall the notions of G-coverings and Galois G-coverings of schemes and of quasicoherent G-sheaves. In Section 4 we introduce what we call numerically tame G-coverings. These coverings are more general than the ones considered in [Ch1] and [Ch2], and it is for them that we may define $\chi R\Gamma^+(f_*(T))$. The construction of $\chi R\Gamma^+(f_*(T))$ is carried out in Section 5. The Appendix contains a proof –based on Abhyankar's Lemma– that G-coverings which are tame in codimension 1 are numerically tame.

1. Two basic examples

The following examples are included to give the reader an idea of the kind of information on the Galois module structure of G-coverings one should expect to extract from a description of the classes defined in Section 5.

1.1. Galois structure of differentials and generalizations. One of the first uses of character theory outside group theory was Hecke's determination of the Galois module structure of the complex vector space V of cusp forms of weight 2 and level a prime number p. Hecke's goal was to simplify the problem of studying such cusp forms by decomposing V into isotopic components under the natural action of $PSL(2,p)$ (see [He, 1-2]). As is well known V can be identified with the space $H^0(X,\Omega^1)$ of holomorphic differentials on the Riemann surface X which is the compactification of the orbit space of the action by the congruence subgroup $\Gamma(p)$ on the upper half plane (see [L], [Sh, 2.17]): so Hecke was considering the covering $X \to Y = \mathbf{P}^1$ with the group $PSL(2,p)$ acting on X and Ω^1. In [C-W] [W2] Chevalley and Weil generalize part of Hecke's work and deal with G-coverings $X \to Y$ of compact Riemann surfaces with an arbitrary finite group G as group of automorphisms. They give a formula for the multiplicity m_χ of any irreducible character χ of G in $H^0 = H^0(X,\Omega^1)$ in terms of the genus and ramification data. We observe that this can interpreted as follows. The space H^0 is a finite dimensional module over the semisimple algebra $\mathbf{C}G$ and hence determines a class $[H^0]$ in the Grothendieck group $K_0(\mathbf{C}G) = R(G)$ of (projective) $\mathbf{C}G$-modules – this is of course nothing but the group of virtual characters of G. Since $R(G)$ is the free abelian group on the irreducible characters of G, there is a natural isomorphism from $R(G)$ to $\mathrm{Hom}(R(G),\mathbf{Z})$; this isomorphism sends $[H^0]$ to the homomorphism which on an irreducible character χ of G takes the value m_χ.

These results have been considerably generalized in two directions. The first generalization concerns equivariant Euler-Poincaré characteristics of coherent sheaves other than the sheaf of differentials, mainly for covers of varieties which are smooth and proper over an algebraically closed field (see for example [G-G-H], [E-L], [N,1-3], [V-M]). The second generalization concerns Euler-Poincaré characteristics of sheaves for the étale topology. The formulas that have been obtained in this case are generalizations of Weil's interpretation of the fact that in characteristic 0 the determination of the G-action on $H^0(X,\Omega^1)$ determines the action on the space of harmonic forms: this space is dual to the first homology space of X and so we should study the Tate module of the Jacobian of the curve, which plays the role of the first homology group for the étale topology. This leads to a formula for the Artin conductor attached to a G-covering in positive characteristic (see [W1, p. 79],[S1] [Mi],[R]).

1.2. Galois structure of rings of integers. Let N/K be a finite Galois extension of number fields with group G. The ring of integers O_N is a $\mathbf{Z}G$-module and one can show that it is projective if and only if the extension is tamely ramified. Suppose N/K is tamely ramified, so there is a class

(O_N) in the *reduced* Grothendieck group $Cl(\mathbf{Z}G)$ of projective $\mathbf{Z}G$-modules (of rank 0). By results of Fröhlich one can describe $Cl(\mathbf{Z}G)$ in terms of homomorphisms from the group of virtual characters $R(G)$ into the group of idèles of an algebraic closure $(\mathbf{Q}^c)$ of $\mathbf{Q}$. The class (O_N) is then shown to be determined by a homomorphism defined *via* the Galois-Gauss sums of the characters of G (see [F, Ch. 1]).

We observe that most of the results in (1.1) deal with the determination of the actual isomorphism class of the modules involved whereas in (1.2) the emphasis is shifted to the determination of the *stable* isomorphism class. In both cases, however, what one really does when computing the classes is to determine a homomorphism on the virtual characters.

2. Applications of Euler-Poincaré characteristics

In this section we recall some elementary applications of Euler-Poincaré characteristics and of their equivariant generalizations.

2.1. The Riemann Problem. Let X be a projective variety over an algebraically closed field k. The Riemann problem has do to with determining the dimension of the k-vector space $H^0(X,T)$ of global sections of a coherent sheaf T on X. The classical approach to this problem has two steps: (a) Find an expression for the *Euler Poincaré characteristic*

$$\chi(T) = \sum_{i=0}^{\infty} (-1)^i \cdot dim_k H^i(X,T)$$

by means of Generalized Riemann-Roch Theorems, and (b) Prove a Vanishing Theorem which asserts that under suitable hypotheses, $H^i(X,T) = 0$ for $i > 0$. For such T, (a) gives an expression for $\chi(T) = dim_k H^0(X,T)$.

If one has compatible actions of a group G on X and on T, then one can refine the Riemann problem by asking for the kG-module structure of $H^0(X,T)$, as in Sect. (1.1). In step (a), it is then natural to consider the Euler-Poincaré characteristic

$$\chi(G,T) = \sum_{i=0}^{\infty} (-1)^i \cdot [H^i(X,T)]$$

in $G_0(kG)$. (Recall that $G_0(k) = K_0(k)$ can be identified to the ring of integers via the dimension map.) If one cannot accomplish step (b), one may be able nonetheless to restrict the possibilities for the class of $H^i(X,T)$ in $G_0(kG)$ for $i > 0$. For example, one might be able to show that various irreducible representations cannot occur in $H^i(X,T)$ for $i > 0$. In this way one may still deduce from $\chi(G,T)$ information about the class of $H^0(X,T)$ in $G_0(kG)$.

2.2. Group actions on varieties. Euler-Poincaré characteristics are useful in studying the possible actions of a finite group G on a projective variety X. Suppose for example that G acts freely on X, i.e. that there is a quotient morphism of schemes $f : X \to Y = X/G$ which is an (étale) Galois covering with group G, in the sense of Definition 3.3 below. Then for any coherent sheaf T on X which admists a G-action compatible with the one on X, we have the identity

$$\chi(T) = |G| \cdot \chi((f_*(T))^G)$$

where $(f_*(T))^G$ denotes the sheaf on Y of invariants in $f_*(T)$ (see [Mum, Sect. 12, Theorems 1B and 2]). In particular $|G|$ must divide $\chi(T)$. Thus, for example, if the arithmetic genus $\chi(O_X)$ equals 1, then no nontrivial finite group can act *freely* on X. Some interesting X with arithmetic genus 1 are given in [Ha1, Ex. II.8.4(f)].

By [E-L, Theorem 2.4] and [B-K, Prop. 1.2], one can refine the above formula to the equality

$$\chi(G,T) = \chi((f_*(T))^G) \cdot [kG]$$

in $G_0(kG)$ provided that G acts freely on X. Thus $\chi(G,T)$ gives a further obstruction to the freeness of an action of G on X. This is because there may exist non-free actions for which $\chi(G,T)$ is not the class of a free module in $G_0(kG)$ even though $|G|$ divides $\chi(T)$.

Suppose now only that $f : X \to Y$ is a *tame* G-covering of proper schemes of finite type over k. Nakajima shows in [Na2] that while the cohomology groups $H^i(X,T)$ of a coherent G-sheaf T on X need not be projective kG-modules in general, one can always express $\chi(G,T)$ in terms of projective kG-modules. This result will be a consequence of the more general construction in Section 5. For other uses of Euler-Poincaré characteristics, see [B-K] and [N1, Sect. 3].

3. G-covers and G-sheaves ([SGA 1, Ch. I and V], [Mum, Sect. 5 and 12])

In this section we describe the set up for the rest of this paper. Let $S = Spec(A)$ be the spectrum of a noetherian ring A. All the schemes we consider are of finite type over S. Let (X, O_X) be an S-scheme and let G be a finite group. In what follows we will assume that the group G acts admissibly on X by S-automorphisms (on the right)([SGA 1, Ch.I and V]). This means that there is a morphism $f : X \to Y$ of S-schemes such that $O_Y \xrightarrow{\sim} f_*(O_X)^G$. Then $Y = X/G$ is the quotient of X by G. If f is also finite, we will say that f is a *G-covering.*

Definition 3.1. A sheaf T of O_X-modules is a *G-sheaf* on X if G acts on T in a way compatible with its action on O_X and with the action of O_X on T (i.e. $O_X \times T \to T$ is a G-morphism).
Examples: (a) The direct image $f_*(T)$ of a G-sheaf T on X is a G-sheaf on Y. (b) If G acts freely on X then every G-sheaf T on X is the inverse image $f^{-1}(F)$ of some sheaf F on Y (see [Mum, Sect. 12, Theorem 1B]). (c) The structure sheaf O_X and the sheaf $\Omega^1_{X/S}$ of relative differentials are G-sheaves. (d) The sheaf associated to any ambiguous ideal in a Galois extension N/K of number fields with group $G = Gal(N/K)$ is a G-sheaf on $Spec(O_N)$. (e) The invertible sheaf $L(D)$ associated to a G-invariant divisor on X is a G-sheaf. (f) If G acts trivially on X, then the identity morphism $X \to X$ is a G-covering according to our definitions. In this case a G-sheaf on X is simply a sheaf of modules for $O_X - G$, on which the actions of G and O_X commute.
Remark: If each of the cohomology groups $H^i(X,T)$ are finitely generated AG-modules and almost all of these groups vanish, then one may define the Euler-Poincaré characteristic as the alternating sum

$$\chi(G,T) = \sum_i (-1)^i \cdot [H^i(X,T)] \tag{3.2}$$

of the classes $[H^i(X,T)]$ of the AG-modules $H^i(X,T)$ in the Grothendieck group $G_0(AG)$ of all finitely generated AG-modules. This will be the case, for example, if X is proper and of finite type over S and if T is a coherent G-sheaf.

For any scheme Z we denote by G_Z the *constant Z-group scheme*

$$G_Z = \coprod_{g \in G} Z_g$$

where for all $g \in G$, Z_g is isomorphic to Z. The group scheme structure of G_Z is induced by the identity maps $Z_g \times_Z Z_h \to Z_{gh}$ for $g, h \in G$. This shows that an S-action of the group G is the same as an action of the group scheme G_S.
Definition 3.3. A G-covering $f : X \to Y$ is *Galois* if X is a G-torsor over Y, in the sense that X is faithfully flat over Y and the map $(x,g) \mapsto (x, xg)$ defines an isomorphism

$$X \times_Y G_Y \simeq X \times_Y X.$$

A G-covering is Galois if and only if its inertia groups are trivial [SGA1, V.2.6]; in particular, Galois G-coverings are étale.

Examples: (a) $G_Y \to Y$ is called the *trivial* Galois G-covering of Y. (b) Let K be a field. A Galois G-covering X of $Y = Spec(K)$ is necessarily the spectrum of a separable finite dimensional K-algebra N. These algebras are known as *Galois G-algebras.* The trivial G-covering gives the standard Galois G-algebra $\mathrm{Map}(G, K)$ of all set theoretic maps from G to K. If N is a field, then the isomorphism in Definition 3.3 is nothing but the basic isomorphism from Galois theory

$$Map(G, N) \simeq N \otimes_K N.$$

(c) If O_N and O_K are the rings of integers in a G-Galois extension N/K of number fields, then the natural map $Spec(O_N) \to Spec(O_K)$ is a Galois G-covering if and only if O_N is unramified over O_K in the usual sense (observe that $Map(G, O_N)$ is the maximal O_K–order in $Map(G, N)$).

4. Tame G-coverings

We now investigate under which conditions we can ensure that the Euler-Poincaré characteristic defined in (3.2) can be lifted to the group of finitely generated cohomologically trivial AG-modules. Our guiding example will be Example (1.2).

4.1. Cohomologically trivial modules. Recall that a G-module M is *cohomologically trivial* if for every subgroup H of G, the (reduced) Tate cohomology groups $\hat{H}^i(H, M)$ are zero for all i. This is equivalent to the condition that the non-reduced cohomology group $H^i(G, M)$ vanishes for two consecutive values of $i > 0$. If M is an A-module, then $H^i(H, M)$ and $\hat{H}^i(H, M)$ are A-modules. If B is a flat A-algebra, then

$$H^i(H, B \otimes_A M) = B \otimes_A H^i(H, M)$$

for all $i \geq 0$. Thus if B is faithfully flat over A, then M is cohomologically trivial if and only if $B \otimes_A M$ is. We also see that M is cohomologically trivial if and only if each of the localizations of M at prime ideals of A are cohomologically trivial.

We now recall a well-known sufficient condition for an AG-module to be cohomologically trivial.

Lemma 4.2. *Suppose H is a subgroup of G of order prime to the residue characteristics of A , i.e. the order of H is a unit in every localization of A at a prime ideal. Suppose that M is isomorphic to the induced AG-module $Ind_H^G(M')$ associated to some AH-module M'. Then M is cohomologically trivial for G.*

Proof. By Shapiro's Lemma and Mackey's formula, it will suffice to show that M' is cohomologically trivial for H. Let H' be a subgroup of H and let A_P

be a localization of A at a prime ideal P. Then the order of H' is a unit of A_P which annihilates

$$H^i(H', A_P \otimes_A M') = A_P \otimes_A H^i(H', M')$$

for all $i > 0$. It follows that M' is cohomologically trivial for H', as required.

4.3. Čech cohomology. Recall now that we can compute the cohomology of a *quasicoherent* sheaf F on a separated scheme Y by means of the Čech complex. Choose a finite open affine covering $\mathcal{U} = \{U_i\}_i$ of Y and consider the family of abelian groups

$$C^p(\mathcal{U}, F) = \prod_{i_0 < \cdots < i_p} F\left(U_{i_0} \cap \cdots \cap U_{i_p}\right) .$$

These form a complex the i-th homology group of which is the group $H^i(Y, F)$ (see [Ha1, III 4]). Suppose now that G acts trivially on (Y, O_Y) and that F is a G-sheaf on Y. Since Y is separated, the intersections $U_{i_0} \cap \cdots \cap U_{i_p}$ are affine. Hence to show that the $C^p(\mathcal{U}, F)$ are cohomologically trivial AG-modules, it is sufficient to show – say – that for any affine open subset $U \subset Y$ the module $F(U)$ is cohomologically trivial. By the preceding remarks this is equivalent to showing that the stalks of F at every point of Y are cohomologically trivial (see also Prop. 4.7 below).

Consider the case of a G-covering $f : X \to Y$ and a sheaf F which is the direct image $f_*(T)$ of a (quasicoherent) G-sheaf T on X. Then the study of the stalk of F at any point y of Y can be done by base change. More precisely, we will use the following. Let $\alpha : Y' \to Y$ be a *flat* base change containing y in its image and let $f' : X' \to Y'$ and T' be the base change of f and T respectively. Then f' is again a G-covering and for $y' \in Y'$ such that $\alpha(y') = y$ we have

$$(f'_* T')_{y'} = O_{Y',y'} \otimes_{O_{Y,y}} (f_* T)_y .$$

In particular—since $O_{Y',y'}$ is faithfully flat over $O_{Y,y}$ —$(f_* T)_y$ is cohomologically trivial if and only if $(f'_* T')_{y'}$ is.

4.4. Tame extensions of D.V.R.'s. Let R be a discrete valuation ring with field of fractions K and residue field k. A finite Galois extension L/K with group G is said to be *tamely ramified* (or simply *tame*) if for any maximal ideal of the integral closure W of R in L the inertia group has order prime to the characteristic of k and the residue field extension is separable ([SGA 1, XIII 2], [G-M]). If R is *strictly henselian*, i.e. if all of its connected étale extensions are trivial, then the situation is very simple: L/K is tame if and

only if the degree $[L : K]$ is prime to the residue characteristic. Moreover since in this case the decomposition group equals the inertia group, we see that L/K is cyclic. It is shown in [SGA 1,XIII 2.0.2] and [G-M, 2.2.8] that tameness for any extension W/R of D.V.R.'s can be detected by going over to the extension $\hat{W}/\hat{R}$ of the strict henselizations. Recall that $W \to \hat{W}$ is faithfully flat ([EGA IV] [Ra, Chap. VIII.4]).

Proposition 4.5. ([Ra, X Lemma 1]) *Let R be any strictly henselian ring and let G be a finite group. Let W be a (finite) R-algebra on which G acts in such a way that $R = W^G$. Choose a maximal ideal q of W. Then*

$$W \simeq Map_H(G, C)$$

where C is the localization of W at q, and where the algebra $Map_H(G, C)$ is the algebra of elements in the standard algebra $Map(G, C)$ invariant under the inertia group $H = I_q$.

Thus for example a tame G-extensions of a strictly henselian discrete valuation ring is induced from a subgroup of order prime to the residue characteristic (compare with the structure of the semilocalization of a ring of integers in tame G-extensions of number fields). Observe that in the situation of the proposition any WG-module M is isomorphic as an RG-module to a module $\mathrm{Ind}_H^G(M')$ induced from some RH-module M' (see the proof of Prop. 4.7).

We now make a geometric definition motivated by the above discussion.

Definition 4.6. Let $f : X \to Y$ be a G-covering. We say that f is *numerically tame* if for every point y of Y there is a flat morphism $Y' \to Y$ having y in its image and a Y'-scheme Z for which the following conditions are satisfied.

(a) The structure morphism $Z \to Y'$ is an H-covering for some group H of order prime to the residue characterics of Y', and

(b) There is a homomorphism from H to G for which there is a G-equivariant isomorphism of Y'-schemes

$$X \times_Y Y' \simeq (Z \times_{Y'} G_{Y'})/H.$$

Remarks: (a) We do not require the group H to be abelian, we are only imposing a condition on its order (this is a "numerical" condition). (b) A surjective Galois covering $f : X \to Y$ is clearly numerically tame (take $Y' = X = Z$ and $H = 1$). (c) By (4.4) any tame finite Galois extensions of number fields defines a numerically tame $Gal(N/K)$-covering $Spec(O_N) \to Spec(O_K)$. (d) If G has order prime to all of the residue characteristics of Y, then $f : X \to Y$ is numerically tame, since we can let $Y' = Y, Z = X$ and $H = G$. (e) In the Appendix we relate numerical tameness to a more ramification theoretic notion of tameness, thereby giving many examples of numerically tame G-coverings.

The following result was proved in [Ch1] under the more restrictive hypothesis that $f : X \to Y$ is a tame G-covering in the sense of [G-M, 2.2.2] (see also A.1 of the Appendix).

Proposition 4.7. *Let $f : X \to Y$ be a numerically tame G-covering of S-schemes where $S = Spec(A)$ and let $F = f_*(T)$ be the direct image of a quasicoherent G-sheaf T on X. Then the following two equivalent conditions are satisfied*
(a) all the stalks of F are cohomologically trivial AG-modules
(b) for every open affine subset U of Y, $F(U)$ is a cohomologically trivial AG-module.

Proof. If $U = Spec(B)$ in (b), then $F(U)$ is a BG-module which is cohomologically trivial if and only if for all $y \in U$, the localization $F(U)_y$ of $F(U)$ at y is cohomologically trivial. Hence the equivalence of (a) and (b) follows from the fact that $F(U)_y$ is the stalk F_y of F at y.

By the remarks in (4.3), to show that F_y is cohomologically trivial, we are free to make a base change by a flat morphism $Y' \to Y$ whose image contains y. Thus in view of Definition 4.6, we can assume that $X = (Z \times_Y G_Y)/H$ for some finite group H mapping homomorphically to G and for some H-cover $Z \to Y$. By [G-M, Lemma 1.5.2(iii)] we can replace H by its image in G and Z by its image in X so as to be able to assume that H is a subgroup of G. Choose a set $\mathcal{S}$ of representatives for the cosets $H\backslash G$ which contains the identity element e of G. Over Y we have an isomorphism of schemes

$$(Z \times_Y G_Y)/H = \coprod_{s \in \mathcal{S}} Z \cdot s. \tag{4.8}$$

This is a G-isomorphism when we let G act on the right hand side according to our choice of coset representatives $\mathcal{S}$ and according to the (right) action of H on Z.

Let T_Z be the restriction of the G-sheaf T on $X = (Z \times_Y G_Y)/H$ to the component $Z \cdot e$ on the right hand side of (4.8). Let $\alpha : Z \cdot e \to Y$ be the restriction of $f : X \to Y$. Then we find that the stalk $f_*(T)_y = F_y$ at y is isomorphic as a left $O_{Y,y}[G]$-module to the induced module $Ind_H^G \alpha_*(T_Z)_y$, where $\alpha_*(T_Z)_y$ is a left $O_{Y,y}[H]$-module. Because of condition (a) of Definition 4.6, we can now conclude from Lemma 4.2 that F_y is cohomologically trivial, which completes the proof.

5. Equivariant Euler-Poincaré characteristics for numerically tame coverings

In this section we carry out the construction of equivariant Euler-Poincaré characteristics for numerically tame coverings. In particular, we deal with the

problem of producing bounded complexes of finitely generated cohomologically trivial AG-modules which compute sheaf cohomology. As will be seen, we consider a slightly more general situation than the one we have considered so far, in that we replace the G-sheaf T by a bounded complex of sheaves. The additional freedom this allows is useful in applications, where one considers complexes which arise from truncating the de Rham complex $\Omega^{\bullet}_{X/A}$ (see [Ch1, Ch2]).

As in Section 3, let $f : X \to Y = X/G$ be a G-covering of schemes of finite type over a noetherian ring A, where G is a finite group. Let $K^+(Y, A, G)$ be the category whose objects are complexes $F^{\bullet}$ of sheaves of AG-modules on Y which are bounded below. Morphisms between consecutive terms of $F^{\bullet}$ are assumed to respect the AG-module structure, where the actions of A and G commute. Note that we do not assume that O_Y acts on the terms of $F^{\bullet}$. Morphisms in $K^+(Y, A, G)$ are homotopy classes of morphisms of complexes.

Let $K^+(A, G)$ be the (homotopy) category of complexes of AG-modules which are bounded below. A morphism between two such complexes is a quasi-isomorphism if it induces an isomorphism in cohomology. The derived category $D^+(A, G)$ of $K^+(A, G)$ is the localization of $K^+(A, G)$ with respect to quasi-isomorphisms (see [Ha2, p.37] or [K-S, Chap. 1 and 2]). Since there are enough injectives in the category of sheaves of AG-modules, the construction given in [Ha1, Prop. III.2.2] shows that there are enough injectives in the category of sheaves of AG-modules on Y. Hence by e.g. [Ha2, Cor. I.5.3] the global section functor has a right derived functor $R\Gamma^+ : K^+(Y, A, G) \to D^+(A, G)$. The basic fact that we will need to know about $R\Gamma^+$ is that under suitable assumptions on Y and $F^{\bullet}$, one can compute $R\Gamma^+(F^{\bullet})$ by a Čech hypercohomology complex $\mathbf{H}(\mathcal{U}, F^{\bullet})$. In the case of a complex reduced to the term F in degree 0, this is the usual Čech complex. More precisely we will need the

Facts 5.1. [EGA III, 0.12.4.7] Let $\mathcal{U} = \{U_\alpha\}$ be a finite open affine cover of Y and let

$$C^i(\mathcal{U}, F^j) = \prod_{k_0 < \cdots < k_i} F^j\left(U_{k_0} \cap \cdots \cap U_{k_i}\right) .$$

One can define differentials on the $C^i(\mathcal{U}, F^j)$ so as to get a double complex $C^{\bullet}(\mathcal{U}, F^{\bullet})$. Let $\mathbf{H}(\mathcal{U}, F^{\bullet})$ be the total complex of this double complex. Suppose now that Y is separated over A. Suppose further that the terms of $F^{\bullet}$ are quasicoherent O_Y-modules, and that the A-module structure given on each of these terms is compatible with the structure morphism $Y \to \mathrm{Spec}(A)$. Then $\mathbf{H}(\mathcal{U}, F^{\bullet})$ is isomorphic in $D^+(A, G)$ to $R\Gamma^+(F^{\bullet})$.

The following result was proved in [Ch1] under the more restrictive hypothesis that $f : X \to Y$ is a tame G-covering in the sense of [G-M, 2.2.2] and A.1 of the Appendix.

Theorem 5.2. *Let $f : X \to Y$ be a numerically tame G-covering of schemes which are proper and of finite type over A. Suppose $T^\bullet$ is a bounded complex of sheaves of abelian groups on X which has the following properties. Each term of $T^\bullet$ is assumed to be a coherent O_X-module which has an action of G compatible with the action of G on O_X. The structure morphism $X \to Spec(A)$ then makes each term of $T^\bullet$ an AG-module. The morphism between consecutive terms of $T^\bullet$ are assumed to respect the AG-module structure (but not necessarily the O_X-structure). Under these assumptions, $f_*(T^\bullet)$ is an object in $K^+(Y, A, G)$. Furthermore, there is a bounded complex $M^\bullet = (M^i)$ of finitely generated cohomologically trivial AG-modules wich is isomorphic to $R\Gamma^+(f_*(T^\bullet)$ in $D^+(A, G)$. Let $CT(AG)$ be the Grothendieck group of all finitely generated AG modules which are cohomologically trivial as G-modules. The (equivariant) Euler-Poincaré characteristic*

$$\chi R\Gamma^+(f_*(T^\bullet)) = \sum_{i=-\infty}^{\infty} (-1)^i \cdot [M^i]$$

in $CT(AG)$ depends only on $T^\bullet$ and not on the choice of $M^\bullet$.

Proof. Since $f : X \to Y$ is finite, the complex $F^\bullet = f_*(T^\bullet)$ is a bounded complex of coherent O_Y-modules. The A-module and G-module structure of the terms of $T^\bullet$ make $F^\bullet$ into an object in $K^+(Y, A, G)$. The action of O_Y on each term of $F^\bullet$ commutes with the action of G, and is compatible with the A-module structure of this term via the structure morphism $Y \to \mathrm{Spec}(A)$. In light of the Facts 5.1, as a first approximation to the complex $M^\bullet$ we may take the Čech hypercohomology complex $M_0^\bullet = \mathbf{H}(\mathcal{U}, F^\bullet)$. By our assumptions on $T^\bullet$ and $\mathcal{U}$, $M_0^\bullet$ is bounded. Since the G-covering $f : X \to Y$ is numerically tame and the intersections $U_{k_0} \cap \cdots \cap U_{k_i}$ are affine, we know by Proposition 4.7 that all the $F^j(U_{k_0} \cap \cdots \cap U_{k_i})$ are cohomologically trivial AG-modules. So the terms of $M_0^\bullet$ are cohomologically trivial. We now use the assumption that the terms of $T^\bullet$ are coherent to get a complex with the same properties as $M_0^\bullet$, but with finitely generated terms. There is a standard way of doing this (see [Ha, III 12.3] [EGA III, 0.11.9.1] [Mum, Sect. 5 Lemma 1] [SGA 6, I 1.4]). The idea is as follows. Suppose that $L^\bullet = (L^i)$ and $N^\bullet = (N^i)$ are complexes with terms in some nice category and let $u : L^\bullet \to N^\bullet$ be a morphism of complexes inducing an isomorphism in cohomology for $i > n$ and an epimorphism for $i = n$. Suppose also that the n-th cohomology of the mapping cone complex of u satisfies some reasonable finiteness condition. Then one can modify u in degree n so as to get an isomorphism in cohomology for $i = n$ and an epimorphism for $i = n - 1$ (i.e. we move one step to the left). Moreover the modification simply consists of adding to L^n an object of the category satisfying the same finiteness condition as the cohomology of

the cone. We will apply this with $L^\bullet = M_0^\bullet$, $N^\bullet = R\Gamma^+(F^\bullet)$ and proceed by descending induction to get a complex $M_1^\bullet$ with finitely generated cohomologically trivial terms and with the same cohomology as $R\Gamma^+(F^\bullet)$: the assumption on the mapping cone is satisfied since we are considering complexes with coherent cohomology sheaves. The complex $M_1^\bullet$ is not necessarily bounded below. We get the complex $M^\bullet$ of the statement by truncating $M_1^\bullet$ in degree 0 so as not to change its cohomology, i.e. we let $M^i = M_1^i$ for $i \geq 1$ and $M^0 = M_1^0/\mathrm{im}(M_1^{-1})$. It follows from the fact that we have isomorphisms in cohomology that M^0 is also cohomologically trivial. Suppose now that $M'^\bullet$ is another bounded complex of finitely generated AG-modules which are cohomologically trivial for G, and that there is an isomorphism between $M^\bullet$ and $M'^\bullet$ in the derived category. This isomorphism is represented by a pair of quasi-isomorphisms of complexes $N^\bullet \to M^\bullet$ and $N^\bullet \to M'^\bullet$, where $N^\bullet$ is bounded below. Applying the construction above, we can replace $N^\bullet$ by a complex of finitely generated AG-modules which are cohomologically trivial as G-modules. Thus to prove $\chi(M) = \sum_{i=0}^{\infty}(-1)^i \cdot [M^i]$ equals $\chi(M')$ in $CT(AG)$, we can reduce to the case in which there is a quasi-isomorphism of complexes $\tau : M^\bullet \to M'^\bullet$. The mapping cone complex $L^\bullet$ of τ is now acylic and consists of finitely generated cohomologically trivial AG-modules. Hence $0 = \chi(L^\bullet) = \chi(M^\bullet) - \chi(M'^\bullet)$, as claimed. This concludes the proof of the theorem.

Appendix: A variant of Abhyankar's Lemma

We define G-coverings of normal schemes which are tame in codimension 1 and show that they are numerically tame. The statement comes form [G-M]. The proof is based on Abhyankar's observation that under suitable regularity assumptions one can "eliminate ramification from a tame covering by a tame base change which is completely determined by the covering".

Definition A.1. [G-M, 2.2.2] Let $f : X \to Y$ be a G-covering and suppose X and Y are *normal.* Let D be a divisor with normal crossings on Y which is of codimension at least 1. Write $U = Y \setminus D$. The covering f is said to be *tamely ramified in codimension 1* with respect to D if

a) $X \times_Y U$ is Galois over U with group G (see (3.3));
b) every irreducible component of X dominates an irreducible component of Y;
c) f is tamely ramified at every $y \in D$ of codimension 1 in the following sense. The local ring $O_{Y,y}$ is a discrete valuation ring by our assumptions on Y and y. Let $K = Q(O_{Y,y})$ be its quotient field. Then we want every field component of the function ring of the fiber $f^{-1}(y)$ to be tamely ramified over K (as in (4.4)).

The assumption on D implies that the local rings of all the points in the support of D are regular and that at any point we have nice local equations for the components of D after making an étale base change. The functions defining these equations together with the orders of the relevant inertia groups are the crucial elements needed for Abhyankar's method to work.

Theorem A.2. *A G-covering $f : X \to Y$ of normal schemes which is tame in codimension 1 (with respect to some divisor with normal crossings D) is numerically tame.*

Proof. We just string a number of propositions from [G-M] and [SGA 1] (note that a proof of the theorem is not given in [G-M] nor in [SGA 1, XIII]). For every $y \in Y$ it suffices to construct an étale neighborhood $g : Y' \to Y$ of y and a covering Z of Y' satisfying the conditions of Definition 4.6. We choose Y' to be the spectrum of the strict henselization of the local ring at y. The base change $f' : X' = X \times_Y Y' \to Y'$ of f is again a G-covering ([SGA 1, V 1.9]). Applying Proposition 4.5 to the covering f' we can replace X' by one of its connected components and G by the inertia group of the closed point of this component, so as to be able to assume that X' is the spectrum of a strictly henselian local ring. The G-covering f' is tame with respect to a divisor D' on Y' having normal crossings ([G-M, p. 27 and 2.2.8]).

Next we consider the Y'-scheme Y''

$$Y'' = \mathrm{Spec}\,(O_{Y'}[(T_i)]_{i\in I})/\left((T_i^{n_i} - a_i)_{i\in I}\right) .$$

Here $\underline{a} = \{a_i\}$ is the finite family of non-unit global sections of $O_{Y'}$ defining the local equations of the divisor D' at the closed point y' of Y' and $\underline{n} = \{n_i\}$ is a family of integers determined by the orders of the inertia groups attached to f' (see [SGA 1, XIII 5.2]). The covering $Y'' \to Y'$ comes with an action of $\mu_{\underline{n}} = \prod_i \mu_i$ and is a Kummer covering in the sense of [G-M, 1.2]. Furthermore Y'' is the spectrum of a strictly henselian local ring (see the proof of [G-M, Lemma 1.8.6]). The main idea of the proof – which goes back to Abhyankar (see e.g. [S2]) – is to show that $X'' = X' \times_{Y'} Y''$ is étale over Y''; then since Y'' is strictly henselian, it will follow that $X'' \to Y''$ has a section. Composing this section with the natural projection $X'' \to X'$, exhibits $X' \to Y'$ as a quotient of the covering $Y'' \to Y'$. (To check this it is useful to apply Proposition 4.5 to the coverings $X'' \to X'$ and $X'' \to Y'$.)

To show that $X'' \to Y''$ is étale one reduces to the classical Abhyankar Lemma as stated in [SGA 1, X 3.6] by using the Theorem on the Purity of the Branch Locus [SGA 2, X 3.4] (see [SGA 1, XIII 5.3.0] for the reduction). The rest is all downhill. Since f' is a quotient of a Kummer covering it is a generalized Kummer covering (X', G). Then by [G-M, Prop. 1.6.2] there is

a generalized Kummer covering (Z, H) such that $(X', G) \simeq ((Z \times G)/H, G)$. Here Z is the connected component of X' and H is the stabilizer of Z in G; compare Proposition 4.5. This concludes the proof.

References

[B-K] Browder, W., Katz, N.M. : Free actions of finite groups on varieties, II. Math. Ann. **260** (1982), 403-412.

[C-W] Chevalley, C., Weil, A. : Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers, Abh. aus den Math. Sem. der Hamb. Univ. **10** (1934), 358-361 (= Weil, Oeuvres [1934a])

[Ch1] Chinburg, T. : Galois structure of de Rham cohomology of tame covers of schemes, preprint 1991.

[Ch2] Chinburg, T. : Galois structure of de Rham cohomology, to appear in Sém. de Théorie des Nombres, Bordeaux.

[EGA III] Grothendieck, A., Dieudonné, J. : Étude cohomologique des faisceaux cohérents (EGA III), Publ. Math. IHES **11** (1961) and **17** (1963).

[EGA IV] Grothendieck, A., Dieudonné, J. : Étude locale des schémas et des morphismes de schémas (EGA IV), Publ. Math. IHES **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[E-L] Ellingsrud, G. , Lønsted, K. : An equivariant Lefschetz formula for finite reductive groups, Math. Ann. **251** (1980), 253-261.

[F] Fröhlich, A. : Galois module structure of algebraic integers, Ergebnisse der Math. (3) 1. Berlin, New York: Springer-Verlag, 1983.

[G-G-H] Glazebrook, J.F., Grayson, D.R., Hewitt, P.R. : Galois representations on holomorphic differentials, Comm. in Algebra, **19** (1991), 1375-1386.

[G] Grothendieck, A. : Sur quelques points d'algèbre homologique, Tôhoku Math. J. **9** (1957), 119-221.

[G-M] Grothendieck, A., Murre, J.P. : The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme, Lect. Notes in Math. 208. Berlin, New York : Springer-Verlag, 1971.

[Ha1] Hartshorne, R. : Algebraic Geometry, Grad. Texts in Math. 52. New York, Heidelberg, Berlin : Springer-Verlag, 1977.

[Ha2] Hartshorne, R. : Residues and duality, Springer Lecture Notes in Math. 20. New-York, Heidelberg, Berlin : Springer-Verlag, 1966.

[He1] Hecke, E. : Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen, Abh. aus dem Math. Sem. der Hamb. Univ. **6** (1928), 235-257 (= Math. Werke **28**).

[He2] Hecke, E. : Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen, Abh. aus dem Math. Sem. der Hamb. Univ. **8** (1930), 271-281 (= Math. Werke **29**).

[K-S] Kashiwara, M., Shapira, P. : Sheaves on manifolds, Grundl. der math. Wiss. 292. Berlin, New York: Springer-Verlag, 1990.

[L] Lang, S. : Introduction to modular forms. Berlin, New York : Springer-Verlag, 1976.

[Mi] Milne, J.S. : Étale cohomology. Princeton: Princeton University Press, 1980.

[Mum] Mumford, D. : Abelian varieties. London: Oxford University Press, 1974.

[N1] Nakajima, S. : On Galois module structure of the cohomology groups of an algebraic variety, Invent. Math. **75** (1984), 1-8.

[N2] Nakajima, S. : Galois module structure of cohomology groups for tamely ramified coverings of algebraic varieties, J. Number Theory **22** (1986), 115-123.

[N3] Nakajima, S. : Action of an automorphism of order p on cohomology groups of an algebraic curve, J. Pure and Appl. Alg. **42** (1986), 85-94.

[R] Raynaud, M. : Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abeliennes, (d'après Ogg-Shafarevitch et Grothendieck), Sém. Bourbaki 1964/65, no. 286 (also in : Dix exposés sur la cohomologie des schémas : J. Giraud, et al., Amsterdam, North-Holland Publ., 1968).

[Ra] Raynaud, M. : Anneaux locaux henseliens, Lect. Notes in Math. 169. Berlin, Heidelberg, New York: Springer-Verlag, 1970.

[SGA 1] Grothendieck, A. et al. : Revêtements étales et groupe fondamental (SGA 1), Lect. Notes in Math. 224. Heidelberg: Springer-Verlag, 1971.

[SGA 2] Grothendieck, A. et al. : Cohomologie locale des faisceaux cohérents et théorèmes des Lefschetz locaux et globaux (SGA 2). Amsterdam: North-Holland, 1968.

[SGA 6] Grothendieck, A. et al. : Théorie des intersections et théorème de Riemann-Roch, Lect. Notes in Math. 225. Heidelberg: Springer-Verlag, 1971.

[S1] Serre, J.-P. : Sur la rationalité des représentations d'Artin, Ann. of Math. **72** (1960), 405-420.

[S2] Serre, J.-P. : Revêtements ramifiés du plan projectif (d'après Abhyankar), Sém. Bourbaki 1959/60 no. 204.

[Sh] Shimura, G. : Introduction to the arithmetic theory of automorphic functions, Princeton University Press, 1971.

[V-M] Valentini, R.C., Madan, M.L. : Automorphisms and holomorphic differentials in characteristic p, J. Number Theory **13** (1981), 106-115.

[W1] Weil, A. : Sur les courbes algébriques et les variétés qui s'en déduisent. Paris: Hermann, 1948.

[W2] Weil, A. : Über Matrizenringe auf Riemannschen Flächen und den Riemann-Rochschen Satz, Abh. aus dem Math. Sem. der Hamb. Univ. **11** (1935), 110-115 (= Weil, Oeuvres (1935a)).

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104.
Department of Mathematics, Harvard University, Cambridge, MA 02138.

Astérisque

GREGORY A. FREIMAN

On the structure and the number of sum-free sets

Astérisque, tome 209 (1992), p. 195-201

<http://www.numdam.org/item?id=AST_1992__209__195_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

ON THE STRUCTURE AND THE NUMBER OF SUM-FREE SETS

Gregory A. FREIMAN

1. Introduction

A finite set A of positive integers is called *sum-free*, if $A \cap (A+A) = \emptyset$. In this note we study the structure of sum-free sets. For n odd, $\{1, 3, 5, \ldots, n\}$ and $\left\{\frac{n+1}{2}\ \frac{n+3}{2}, \ldots, n\right\}$ are important examples of such sets.

For any non-empty finite set $K \subset \mathbf{Z}$, we denote by $\ell(K)$ and $m(K)$, respectively, the largest and smallest element of K, by $d(K)$ the greatest common divisor of the elements of K, and by $|K|$ the cardinality of K. For the sets A considered below, we set $m := m(A)$, $\ell := \ell(A)$, $a := |A|$, $2A := A+A$ and $A - m := \{x - m \mid x \in A\}$, $\ell - A := \{\ell - x \mid x \in A\}$. Denote $[m, n] = \{x \in \mathbf{Z} \mid m \leq x \leq n\}$. There is a general property of sum-free sets (from [CE], page 63) which we will use later: If B is a sum-free subset of $\{1, \ldots, n\}$ then B contains at most one of i and $\ell(B) - i$, for each positive integer $i < \ell(B)$; and if $\ell(B)$ is even, then $\frac{1}{2}\ell(B) \notin B$. Hence

$$|B| \leq \left\lceil \frac{1}{2}\ell(B) \right\rceil \leq \left\lceil \frac{1}{2}n \right\rceil . \tag{1}$$

We will show that if the cardinality of a sum-free set A does not differ much from $\frac{1}{2}\ell(A)$, then A does not differ much from one of the two examples mentioned above. More precisely, we will prove

Theorem 1. *Let A be a sum-free set of positive integers for which $a \geq \frac{5}{12}\ell + 2$. Then either*

1) *All elements of A are odd, or*
2) *A contains both odd and even integers, $m \geq a$, and for $A_1 := A \cap \left[1, \frac{1}{2}\ell\right]$ we have*

$$|A_1| \leq \frac{\ell - 2a + 3}{4} .$$

Let $f(n)$ denote the number of sum-free subsets of $\{1, \ldots, n\}$.

P.J. Cameron and P. Erdös in their talk at the First Conference of the Canadian Number Theory Association [CE, page 64] conjectured that

$$f(n) = O(2^{\frac{n}{2}}) .$$

P. Erdös and A. Granville, and independently N. Calkin as well as N. Alon [Al] showed that

$$f(n) = 2^{\left(\frac{1}{2} + o(1)\right)n} .$$

The proof in [Al] is more general and in particular applies to any group.

As a simple corollary of Theorem 1 we will prove that the number of sum-free sets $A \subset [1, n]$ for which $a \geq \frac{5}{12}\ell + 2$ has the bound $O\left(2^{\frac{n}{2}}\right)$.

2. The Structure of Sum-Free Sets of Large Cardinality

As a main tool in the proof of Theorem 1 we will use the following two theorems from [F1].

Let M and N be finite sets of non-negative integers such that $m(M) = m(N) = 0$.

Theorem 2. *If $\ell(M) = \max(\ell(M), \ell(N))$ and $\ell(M) \leq |M| + |N| - 3$, then $|M + N| \geq \ell(M) + |N|$.*

Theorem 3. *If $\max(\ell(M), \ell(N)) \geq |M| + |N| - 2$ and $d(M \cup N) = 1$, then*

$$|M + N| \geq |M| + |N| - 3 + \min(|M|, |N|) .$$

We shall also use the following result from [F2]:

Lemma. *If $A \subset \mathbb{Z}$ is finite, then*

$$|2A| \geq 2|A| - 1 . \tag{2}$$

Proof of Theorem 1. Let us call a set A difference-free if $A \cap (A-A) = \emptyset$. Note first that the notions of sum-free set and of difference-free set coincide. For if $x, y, z \in A$, then $x = y + z \iff y = x - z$. Thus if A is not sum-free then A is not difference-free and conversely.

In the set $A - A$, to each positive difference $x - y$ there corresponds the negative difference $y - x$. Denote by $(A-A)_+$ and $(A-A)_-$, respectively, the set of positive and negative differences.

Since $A - A = (A-A)_+ \cup (A-A)_- \cup \{0\}$ and $|(A-A)_+| = |(A-A)_-|$, we have

$$|A - A| = 2|(A-A)_+| + 1 \ . \tag{3}$$

The sets A and $(A-A)_+$ are both contained in the interval $[1, \ell]$. Since A is difference-free, it follows that

$$|A| + |(A-A)_+| \leq \ell \ . \tag{4}$$

This inequality is very restrictive for large $a = |A|$, and we will use it in conjunction with a lower bound for $|(A-A)_+|$ to be obtained from Theorems 2 and 3, to prove Theorem 1.

Let us study various cases according to the value of $d(A - m)$.

We first observe that $d(A-m) \leq 2$, for if $d(A-m) \geq 3$ then $a \leq \frac{\ell}{3} + 1$ which contradicts the condition $a \geq \frac{5}{12}\ell + 2$.

In case $d(A-m) = 2$ first consider the subcase when m is odd. Then all the numbers of A are odd and we have Case 1 of Theorem 1.

If $d(A-m) = 2$, then m cannot be even, under the hypothesis of Theorem 1. Indeed, if m is even and $d(A-m) = 2$ then all the integers in A are even and the set $\frac{A}{2} := \{x \mid x = \frac{a}{2},\ a \in A\}$ is sum-free, with largest element $\ell_1 = \frac{\ell}{2}$. Also if $a \geq \frac{5}{12}\ell + 2$ then (1), applied to $B = \frac{A}{2}$, would yield $\frac{5}{12}\ell + 2 \leq a = |A| = |\frac{A}{2}| = |B| \leq \frac{\ell_1 + 1}{2} = \frac{\ell + 2}{4}$, which is absurd.

The only case left is that in which $d(A-m) = 1$. Clearly the elements of A cannot then all be of the same parity. We define sets M and N by $M := A - m$ and $N := \ell - A$. Then $m(M) = m(N) = 0$, $\ell(M) = \ell(N) = \ell - m$, $|M| = |N| = a$, $|M+N| = |A-A|$; and $d(M \cup N) = 1$ since $d(M) = 1$. If we had

$$\ell - m \geq 2a - 2 \ , \tag{5}$$

Theorem 3 would apply, giving $|A-A| = |M+N| \geq 3a - 3$, whence $|(A-A)_+| \geq \frac{3a}{2} - 2$ by (3). Using this in (4) together with $a \geq \frac{5}{12}\ell + 2$ would yield the absurd

$$\ell \geq |(A-A)_+| + a \geq \frac{5a}{2} - 2 > \frac{25}{24}\ell \ .$$

Hence (5) is impossible: $\ell - m < 2a - 2$ if $d(A - m) = 1$ and $a \geq \frac{5}{12}\ell + 2$.

Theorem 2 applies, and gives $|A - A| \geq \ell - m + a$, whence $|(A - A)_+| \geq \frac{1}{2}(\ell - m + a - 1)$ by (3).

Using this inequality, (4) and $a \geq \frac{5}{12}\ell + 2$, we get

$$m > \frac{\ell}{4} . \tag{6}$$

Having obtained this lower bound for m, we can strengthen it as follows.

For any positive integer i, the integers i and $m + i$ cannot both belong to A($m \in A$ and A is sum-free). Hence the union $[\ell - 2m + 1, \ell]$ of the intervals $I = [\ell - 2m + 1,\ \ell - m]$ and $I + m$ contains at most m elements of A. Recall that $A_1 = A \cap \left[1, \frac{\ell}{2}\right]$. Let $A_2 = A \setminus A_1 = A \cap \left[\frac{\ell+1}{2}, \ell\right]$. Then by (6), $A_2 \subset \left[\frac{\ell+1}{2}, \ell\right] \subset [\ell - 2m + 1, \ell]$, and therefore

$$|A_2| \leq m . \tag{7}$$

Now $2A_1 \cap A_2 = \emptyset$($A_2 \subset A$, and $2A_1 \cap A = \emptyset$ since A is sum-free) and by (6), $2A_1 \subset \left[\frac{\ell+1}{2}, \ell\right]$. Hence

$$|2A_1| + |A_2| \leq \left| \left[\frac{\ell + 1}{2}, \ell\right] \right| \leq \frac{\ell + 1}{2} .$$

By adding this inequality to (7) and using (2) and $|A_1| + |A_2| = a$ we get $2a \leq \frac{1}{2}(\ell + 3) + m$. Hence with $a \geq \frac{5}{12}\ell + 2$ we get

$$m > \frac{\ell}{3} + 2 . \tag{8}$$

From (8) we have $A \subset [m, \ell] \subset [\ell - 2m + 1, \ell]$. We have seen that this last interval contains at most m integers from A; it follows that $m \geq a$, which proves the first inequality in Case 2 of Theorem 1.

To establish the second inequality of Case 2, we observe that $\ell - A_1$, $2A_1$, and A_2 are pairwise disjoint subsets of $\left[\frac{\ell+1}{2}, \ell\right]$. We have already verified this for $2A_1$ and A_2. Also, $(\ell - A_1) \cap A_2 = \emptyset$ since A is sum-free and $(\ell - A_1) \cap 2A_1 = \emptyset$ because $\ell - A_1 \subset [0, \ell - m]$, $2A_1 \subset [2m, \ell]$ and $\ell - m < 2m$ by (8). Finally, $\ell - A_1 \subset \left[\frac{\ell}{2},\ \ell - 1\right]$ since $A_1 \subset \left[1,\ \frac{\ell}{2}\right]$; and $\frac{\ell}{2} \notin A$ if ℓ is even, because A is sum-free.

It now follows that $|\ell - A_1| + |2A_1| + |A_2| \leq \frac{\ell+1}{2}$, whence by (2), $3|A_1| + |A_2| - 1 \leq \frac{\ell+1}{2}$, or $|A_1| \leq \frac{\ell}{4} - \frac{a}{2} + \frac{3}{4}$. This completes the proof of Theorem 1.

3. Maximal Sum-Free Sets

We will call a sum-free subset of $[1,n]$ *maximal* if it is of maximal cardinality.

We will now prove the following theorem, stated without proof in [CE] on page 63.

Theorem 2. *For $n \geq 24$, the only maximal sets are*
(i) the set C of all odd numbers in $[1,n]$;
(ii) the set D of all numbers in $[1,n]$ which are greater than $\frac{n}{2}$,
(iii) if n is even, the set $E = D - 1 = \left[\frac{n}{2},\ n-1\right]$.

Proof: Clearly, the sets C, D and E are sum-free of cardinality $\lceil \frac{n}{2} \rceil$. Hence, by (1), a sum-free set A is maximal if and only if $|A| = \lceil \frac{n}{2} \rceil$. Let A be any maximal set. Then $a = |A| = \lceil \frac{n}{2} \rceil \geq \frac{n}{2} \geq \frac{5}{12}n + 2$ (if $n \geq 24$) $\geq \frac{5}{12}\ell + 2$, so the condition of Theorem 1 is satisfied.

In Case 1, $A \subseteq C$, so $A = C$.

In Case 2, $m \geq a$, so $A \subseteq \left[\lceil \frac{n}{2} \rceil,\ n\right] = F$, say. If n is odd, then $F = D$, so that $A = D$. If n is even, then $F = \left\{\frac{n}{2},\ \frac{n}{2}+1, \ldots, n\right\}$ which is a set of cardinality $\lceil \frac{n}{2} \rceil + 1$, so precisely one of its elements does not belong to A. If $\frac{n}{2} \notin A$, then $A = D$, and if $\frac{n}{2} \in A$, then $n \notin A$, therefore, $A = E$.

4. Some Examples of Sum-Free Sets

We now give two examples to show that each of the inequalities in Theorem 1 is best possible.

Example 1. Let us consider positive integers m and n such that $n \geq 36$ and $5n + 24 \leq 12m < 6n$ ($n \geq 36$ ensures the existence of at least one such m). Then define the set $A = ([n-m+1, n] \cup \{m\}) \setminus \{2m\}$. Then one has

1) A is a sum-free set,
2) $|A| = m$ and $\ell(A) = n$ so that the condition $a \geq \frac{5\ell}{12} + 2$ is fulfilled,
3) A contains an even number (because we have $n > 24$, so that $m > 12$ and $[n-m+1, n]$ contains at least two even numbers),
4) $m = a$.

Example 2. Let us consider two positive integers m and n satisfying $11n + 18 \leq 24m \leq 12n - 12$. (such that n is odd and $n \geq 53$), and let us define

$$A = \left[m, \frac{n-1}{2}\right] \cup ([n-m+1, n] \setminus [2m, n-1]) \ .$$

Then one has

1) A is a sum-free set,
2) $|A| = \frac{4m-n+1}{2}$ and $\ell(A) = n$, so that condition $a \geq \frac{5\ell}{12} + 2$ is fulfilled,

3) A contains an even number (because $[n-m+1,\ 2m-1]$ contains at least one even number),
4) therefore, we have $A \cap [1,\ \frac{\ell}{2}] = [m,\ \frac{n-1}{2}]$ so that $|A \cap [1,\ \frac{\ell}{2}]| = \frac{\ell}{4} - \frac{a}{2} + \frac{3}{4}$.

It can be shown that when m is sufficiently large, both equalities $m = a$ and $|A_1| = \frac{\ell}{4} - \frac{a}{2} + \frac{3}{4}$ cannot hold at the same time; and indeed deeper results can be established correlating the lower bound of m and the upper bound of $|A_1|$.

The hypothesis $a \geq \frac{5}{12}\ell + 2$ in Theorem 1 cannot be replaced by $a \geq \frac{2}{5}\ell$, as is seen from the example (for $n \in \mathbb{N}$ divisible by 5) of the set $[\frac{n}{5}+1,\ \frac{2n}{5}] \cup [\frac{4n}{5}+1, n]$. Furthermore, this set is locally maximal in the sense of the following definition.

Definition. A set A in $[1,n]$ is *locally maximal* if A is sum-free, but if $A \subseteq A' \subseteq [1,n]$ and $A' \neq A$, then A' is not sum-free.

There naturally arises the problem of determining all locally maximal sets.

5. On the Number of Sum-Free Sets

Theorem 1 immediately gives an upper bound for the number of sum-free sets for which $a \geq \frac{5}{12}\ell + 2$.

In Case 1 the number of sum-free sets with $|A| = a$ is less than or equal to $\binom{[\frac{n+1}{2}]}{a}$.

In Case 2 the number of sum-free sets is less than or equal to $\binom{n-a+1}{a}$. These upper bounds confirm the conjecture of Cameron and Erdös for the number of sum-free sets for which $a \geq \frac{5}{12}\ell + 2$.

It may be conjectured that the number of sum-free sets in $[1,n]$ of cardinality a is $O\left(\binom{\frac{n}{2}}{a}\right)$.

In conclusion, I am pleased to express my gratitude to Professor John Steinig, the referee of this paper, who has spent much of his time clarifying and making more precise an exposition of this paper.

References

[Al] N. Alon, Independent sets in regular graphs and sum-free subsets of finite groups, Israel J. Math. 73(1991), 247-256.

[CE] P.J. Cameron and P. Erdös, On the Number of Sets of Integers with Various Properties, Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association held at the Banff Center, Banff, Alberta, April 17-27, 1988, ed. by Richard A. Molin.

[F1] Freiman, G.A. Inverse problems in additive number theory. VI. On the addition of finite sets. III. (Russian) Izv. Vysš. Učebn. Zaved. Matematika, 1962, no. 3 (28), 151-157.

[F2] Freiman, G.A., Foundations of a Structural Theory of Set Addition, A.M.S. Translations of Mathematical Monographs, Volume 37, Providence, 1973.

Gregory A. FREIMAN
Raymond and Beverly Sackler
Faculty of Exact Sciences
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv, 69978 Israel

Astérisque

DAVID HARARI

Groupe de Brauer de certaines hypersurfaces

Astérisque, tome 209 (1992), p. 203-214

<http://www.numdam.org/item?id=AST_1992__209__203_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

GROUPE DE BRAUER DE CERTAINES HYPERSURFACES

David HARARI

1. Rappels et notations

Dans toute la suite, k désignera un corps de nombres, Ω_k l'ensemble de ses places, $\bar{k}$ une clôture algébrique fixée de k, $G = \mathrm{Gal}(\bar{k}/k)$. Soit X une k-variété algébrique lisse. On dit que X vérifie le principe de Hasse si la condition $X(k_v) \neq \emptyset$ pour toute place v de k implique $X(k) \neq \emptyset$. On dit que X vérifie l'approximation faible si la condition $X(k) \neq \emptyset$ implique que $X(k)$ est dense dans $\prod_{v \in S} X(k_v)$, muni de sa topologie produit, pour tout ensemble fini S inclus dans Ω_k.

Nous considérerons ici les hypersurfaces V de $\mathbf{A}^n_k$ d'équation:

$$y^2 - az^2 = P(x_1, \ldots, x_{n-2}) \tag{1}$$

avec $n \geq 3$, $a \in k^* - k^{*2}$ et P polynôme non nul de degré total au plus 4. On se pose deux types de problèmes pour ces variétés:

- problème arithmétique: Quand les modèles projectifs lisses X de V vérifient-ils le principe de Hasse et l'approximation faible (cette propriété ne dépend en fait pas du modèle lisse X choisi [1], c'est une propriété qui ne dépend que du corps des fonctions $k(V)$ de la variété V) ?
- problème algébrique: Calculer le groupe de Brauer $\mathrm{Br}\, X$ d'un modèle projectif lisse X de V.

Les deux problèmes sont liés par le fait suivant [2]:

[1] voir appendice 1

[2] voir appendice 2

Proposition 1. *Soit X une k-variété propre, lisse, géométriquement intègre, qui a des points dans tous les complétés de k. Alors, la condition:*

$$(\forall (P_v) \in \prod_{v\in\Omega_k} X(k_v)) \quad (\exists A \in \mathrm{Br}\, X) \quad (\sum_{v\in\Omega_k} \mathrm{inv}_v A(P_v) \neq 0 \text{ dans } \mathbf{Q}/\mathbf{Z})$$

$$(\text{resp. } (\exists A \in \mathrm{Br}\, X) \quad (\exists (P_v) \in \prod_{v\in\Omega_k} X(k_v)) \quad (\sum_{v\in\Omega_k} \mathrm{inv}_v A(P_v) \neq 0 \text{ dans } \mathbf{Q}/\mathbf{Z}))$$

est une obstruction, dite obstruction de Brauer-Manin, au principe de Hasse (resp. à l'approximation faible) pour X.

La conjecture principale que nous faisons pour les modèles projectifs lisses X des variétés V d'équation (1) est que l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible est la seule. Il s'agit d'une conjecture standard pour beaucoup de classes de variétés rationnelles (c'est à dire dont le corps des fonctions devient transcendant pur sur la clôture algébrique). Dans le cas que nous considérons ici, notons que Colliot-Thélène, Sansuc, et Swinnerton-Dyer ont montré que la réponse est affirmative quand le polynôme P qui intervient dans l'équation (1) est irréductible ou bien produit d'un facteur irréductible de degré 3 et d'un facteur linéaire, ou bien quand $n = 3$ (cf. [3]).
Nous considérerons dans la suite le cas où $n \geq 4$ et $P = fg$ avec f, g, irréductibles sur $k(\sqrt{a})$, de degré 2, premiers entre eux [3]. Si φ, ψ sont les formes quadratiques obtenues en homogénéisant f, g, nous supposerons toujours que l'intersection de leurs noyaux est réduite à 0, ce qui traduit qu'on ne peut pas, par changement de variables, se ramener à n plus faible.

2. Cas simples

Théorème 1. *Soit $V : y^2 - az^2 = f(x_1, \ldots, x_{n-2})g(x_1, \ldots, x_{n-2})$ une hypersurface du type (1). On garde les hypothèses et notations de la fin du paragraphe précédent. Alors, un modèle projectif lisse X de V satisfait le principe de Hasse et l'approximation faible dans les cas suivants:*

- $n \geq 6$
- $n = 5$ *et toute forme du pinceau* $\lambda\varphi + \mu\psi, (\lambda, \mu) \in \bar{k}^2 - (0,0)$ *est de rang au moins* 3.

[3] Pour les autres cas, qui découlent assez simplement des résultats de [8], voir [5]

PREUVE: La variété V est k-birationnelle à:

$$Y : (y^2 - az^2)f(x_1, \ldots, x_{n-2}) = g(x_1, \ldots, x_{n-2})$$

Or, Y peut se voir comme fibrée en quadriques, via (y, z), au-dessus de $\mathbf{A}_k^2$.

- Pour $n \geq 6$, il y a deux cas:
  - Si le discriminant de la forme $\lambda\varphi + \mu\psi$ n'est pas identiquement nul, la fibre générique est lisse et les fibres sont des quadriques de dimension ≥ 3. On conclut alors avec le lemme suivant, que l'on trouve dans [3]:

    Lemme 1. *Soient Y, Z, deux k-variétés et $p : Y \to Z$ un fibré en quadriques de dimension relative $d \geq 3$. On suppose la fibre générique lisse. Alors, si Z_{lisse} vérifie le principe de Hasse et l'approximation faible, il en est de même de Y_{lisse}.*

    PREUVE DU LEMME 1: La preuve de ce lemme est assez simple; soit $(P_v)_{v \in \Omega_k}$ une famille de points locaux lisses de Y, S un ensemble fini de places de k. Quitte à élargir S, on peut supposer qu'il contient toutes les places archimédiennes. Soit $M_v = p(P_v)$. On peut supposer que les M_v sont des points locaux lisses de Z (quitte à bouger légèrement les P_v, grâce au théorème des fonctions implicites v-adiques). Comme Z_{lisse} satisfait le principe de Hasse et l'approximation faible, on peut trouver un point dans $Z_{\text{lisse}}(k)$, qui est en plus arbitrairement proche des M_v pour $v \in S$. Par le théorème des fonctions implicites, pour M assez proche des M_v pour $v \in S$, la fibre en M (qu'on note Y_M) aura des points dans tous les k_v tels que $v \in S$. Comme la fibre générique est lisse, on peut de plus supposer que Y_M est lisse. Maintenant, Y_M a des points dans tous les k_v pour $v \notin S$ car Y_M est une quadrique définie par l'annulation d'une forme quadratique de rang ≥ 5 et une telle forme quadratique a un zéro non trivial dans tout k_v pour v non archimédienne. Il ne reste plus alors qu'à appliquer principe de Hasse et approximation faible pour la quadrique Y_M pour démontrer le lemme.

  - Si maintenant le discriminant de la forme $\lambda\varphi + \mu\psi$ est identiquement nul, φ et ψ ont un point k-rationnel M commun (lemme 1.14 de [3]). Maintenant, la fibre générique admet M comme point rationnel non conique (à cause de l'hypothèse $N(\varphi) \cap N(\psi) = 0$), elle est donc birationnelle à $\mathbf{P}^{n-3}$ et Y est k-birationnelle à $\mathbf{P}_k^{n-3} \times \mathbf{A}_k^2$ (la projection sur $\mathbf{A}_k^2$ admettant une section via M). D'où le résultat.

- Dans le cas $n = 5$, il faut utiliser le lemme suivant, dont la preuve, que l'on peut trouver dans [9], est plus difficile:

  Lemme 2. *Soit Y une k-variété géométriquement intègre, $f : Y \to Z$ un morphisme projectif, surjectif dont les fibres sont géométriquement intègres, avec Z ouvert de $\mathbf{A}^r_k$ dont le complémentaire est de dimension au plus $r-2$. On fait de plus l'hypothèse géométrique (*) que sur $\bar{k}$, $Y_{\eta,\text{lisse}}(\eta) \neq \emptyset$ pour un ouvert de Zariski non vide de la variété des droites affines de $\mathbf{A}^r$, $\eta \subset \mathbf{A}^r$ étant le plongement du point générique de $\mathbf{A}^1$ associé . Alors, si les fibres de f sur un ouvert de Z vérifient le principe de Hasse et l'approximation faible, il en va de même de Y.*

  On applique alors ce lemme, quand le discriminant de la forme $\lambda\varphi + \mu\psi$ n' est pas identiquement nul, avec $Z = \mathbf{A}^2_k$. L'hypothèse (*) est automatiquement vérifiée d'après [9] car les fibres, sur un ouvert de Zariski non vide de Z, sont des quadriques lisses et toutes les fibres sont géométriquement intègres à cause de l'hypothèse que toute forme du pinceau $\lambda\varphi + \mu\psi, (\lambda,\mu) \in \bar{k}^2 - (0,0)$ est de rang au moins 3. Quand le discriminant de la forme $\lambda\varphi + \mu\psi$ est identiquement nul, le même argument de k-rationalité de Y que dans le cas $n \geq 6$ fonctionne encore.

REMARQUE: Pour les cas simples que recouvre le théorème 1, on n'a donc pas besoin de faire intervenir le groupe de Brauer de X: une méthode de fibration permet de résoudre directement le problème arithmétique.

3. Cas plus difficiles

Quand on n'est pas dans les cas favorables examinés dans la section précédente, on peut espérer traiter le problème arithmétique en utilisant des méthodes de descente, selon la théorie développée par Colliot-Thélène et Sansuc dans [4]. Il faut pour cela d'abord résoudre le problème algébrique du calcul de $\mathrm{Br}\, X$. C'est l'objet du théorème suivant:

Théorème 2. *Soit $V : y^2 - az^2 = f(x_1,\ldots,x_{n-2})g(x_1,\ldots,x_{n-2})$ une hypersurface du type (1). On garde les hypothèses et notations de la fin du paragraphe 1. Soit X un modèle projectif lisse de V. Alors:*

- *Pour $n = 5$, $\mathrm{Br}\, X/\mathrm{Br}\, k = \mathbf{Z}/2$ s'il existe une forme $Q = \lambda\varphi + \mu\psi$ du type (T), avec $(\lambda,\mu) \in k^2 - (0,0)$, telle que les restrictions de φ, ψ au noyau de Q soient encore du type (T). Sinon, $\mathrm{Br}\, X/\mathrm{Br}\, k = 0$.*

- *Pour $n = 4$, on fait de plus l'hypothèse que les coniques projectives associées à φ, ψ sont lisses et en position transverse* [4] *. Soient R_1, R_2, R_3, R_4 leurs quatre points d'intersection. Alors,* $\operatorname{Br} X/\operatorname{Br} k = \mathbf{Z}/2$ *si les R_i sont conjugués et tels que l'extension de degré quatre associée contienne $k(\sqrt{a})$, ou bien si les R_i forment deux paires de points conjugués dans $k(\sqrt{a})$. Sinon,* $\operatorname{Br} X/\operatorname{Br} k = 0$.

(On dira qu'une k-forme quadratique de rang 2 est du type (T) si elle est isomorphe sur k à une forme proportionnelle à $\langle 1, -a \rangle$).

IDÉES DE LA PREUVE: La méthode est différente selon que $n = 5$ ou $n = 4$.

- Pour $n = 5$, on remarque que la variété V est K-rationnelle ($K = k(\sqrt{a})$). On utilise alors le lemme fondamental suivant (cf. [1]) qui permet de relier le groupe de Brauer de X aux fonctions dont les diviseurs sont des normes pour l'extension K/k:

  Lemme 3. *Soit $\mathbf{F}/k$ une extension finie cyclique de corps de nombres, de groupe $\mathcal{G}$. Soit X une k-variété géométriquement intègre, propre et lisse, $\mathbf{F}$-rationnelle (c'est-à-dire que $\mathbf{F}(X)$ est transcendant pur sur $\mathbf{F}$), qui a des points dans tous les complétés de k. Alors,* $\operatorname{Br} X/\operatorname{Br} k$ *est égal au noyau de la flèche $\phi : k(X)^*/k^* N\mathbf{F}(X)^* \to \operatorname{Div} X/N\operatorname{Div} X_{\mathbf{F}}$. Si I est un système de générateurs de ce groupe et $\{f_i\}_{i \in I}$ un système de représentants de I dans $k(X)^*$, il y a obstruction de Brauer-Manin au principe de Hasse (resp. à l'approximation faible) pour X si et seulement si:*

$$(\forall (P_v) \in \prod_{v \in \Omega_k} X(k_v)) \quad (\exists i \in I) \quad (\sum_{v \in \Omega_k} j_v(f_i(P_v)) \neq 0 \text{ dans } \mathbf{Q}/\mathbf{Z})$$

$$(\text{resp. } (\exists (P_v) \in \prod_{v \in \Omega_k} X(k_v)) \quad (\exists i \in I) \quad (\sum_{v \in \Omega_k} j_v(f_i(P_v)) \neq 0 \text{ dans } \mathbf{Q}/\mathbf{Z}) \ )$$

  (Où j_v désigne le plongement: $k_v^*/N\mathbf{F}_v^* \hookrightarrow \mathbf{Q}/\mathbf{Z}$ donné par la théorie du corps de classe local. On note $\mathbf{F}_v^* = k_v^* \otimes_k \mathbf{F}$).

  Le grand intérêt de ce résultat est qu'il permet de calculer $\operatorname{Br} X$ sans avoir à construire explicitement un modèle lisse X de V puisque seul intervient le corps des fonctions de X (qui est le même que celui de V). Notons encore $Y \subset \mathbf{A}_k^n$ le modèle de V d'équation $(y^2 - az^2) f(x_1, \ldots, x_{n-2}) = g(x_1, \ldots, x_{n-2})$ et $K = k(\sqrt{a})$. D'abord, $\operatorname{Br} X/\operatorname{Br} k$ est inclus dans le sous-groupe de $k(X)^*/k^* NK(X)^*$ engendré par la classe de f: il résulte

[4] les autres cas se traitent simplement, cf. [5]

en effet facilement du fait que Y est fibrée en coniques au-dessus de $\mathbf{A}_k^{n-2}$ par $x_1, \ldots, x_{n-2}$ que si F est une fonction sur Y dont le diviseur est une norme de l'extension K/k, F est égale modulo $k^*NK(Y)^*$ à une fonction constante en tant que fonction sur le corps $k(x_1, \ldots, x_{n-2})$, c'est à dire à une fonction $h(x_1, \ldots, x_{n-2})$ ne dépendant plus de (y, z). Si r est un facteur irréductible sur K de h, $r = f$ ou $r = g$ sinon en considérant le diviseur intègre (au niveau $k(\sqrt{a})$) sur Y défini par $r = 0$, on voit que le diviseur de $h(x_1, \ldots, x_{n-2})$ ne peut etre une norme. Ainsi, comme fg est une norme, F est égale modulo $k^*NK(Y)^*$ à f. Ceci nous donne déjà que $\mathrm{Br}\, X/\mathrm{Br}\, k$ s'injecte dans $\mathbf{Z}/2$.

Reste à voir à quelle condition le diviseur de f est une norme. Il faut considérer les différentes possibilités pour la décomposition du cycle $[\overline{W}]$, où W est l'intersection dans $\mathbf{P}_k^3$ des quadriques définies par φ et ψ. La condition nécessaire s'obtient alors en utilisant notamment les lemmes du chapitre 1 de [3], et en faisant intervenir des anneaux de valuation discrète A, avec $k \subset A \subset k(X) = \mathrm{Frac}\, A$, qui restent de valuation discrète au niveau K (le diviseur de f étant une norme si et seulement si sa valuation par rapport à tous les anneaux de ce type est paire). On montre que la condition trouvée est suffisante en écrivant explicitement la forme que doivent avoir f et g pour qu'elle soit vérifiée, ce qui permet de prouver que la valuation de f par rapport à tous les anneaux A comme ci-dessus est paire.

- Dans le cas $n = 4$, la méthode précédente ne fournit qu'un résultat partiel; on a donc intérêt ici à calculer $\mathrm{Br}\, X/\mathrm{Br}\, k$ via $H^1(G, \mathrm{Pic}\, \overline{X})$ (ces deux groupes sont isomorphes car X est une k-variété rationnelle et k est un corps de nombres, cf. [4]). Pour cela, on construit d'abord un modèle projectif lisse X de Z, où Z est la k-variété fibrée en produit de deux coniques au-dessus de $\mathbf{P}_k^1$ définie par:

$$y^2 - az^2 = \lambda, \qquad f(x_1, x_2) = \lambda g(x_1, x_2)$$

(Z est k-birationnelle à V). Ensuite, on calcule $H^1(G, \mathrm{Pic}\, \overline{X})$ en utilisant une suite exacte du type:

$$0 \to A \to B \to \mathrm{Pic}\, \overline{X} \to \mathrm{Pic}\, \overline{X}_{\bar{k}(\eta)} \to 0$$

où A, B sont des G-modules de permutation (la suite exacte est similaire à celle qui intervient pour les fibrés en coniques, cf. [4]).

Pour les détails de la preuve du théorème 2, cf. [5].

Nous pouvons maintenant énoncer le résultat arithmétique:

Théorème 3. *Avec les hypothèses et notations du théorème précédent, l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible pour X est la seule dans les cas suivants:*

- $\operatorname{Br} X/\operatorname{Br} k = \mathbf{Z}/2$.
- $n = 5$.
- $n = 4$ *et les* R_i *forment deux paires de points conjugués.*

PREUVE: On utilise des méthodes de descente. Nous ne traiterons ici en détail que le premier cas qui est le plus simple. Puis, nous indiquerons brièvement par quelle méthode on traite les deux autres (pour les détails de ces deux derniers cas, cf. [5]).
Si $\operatorname{Br} X/\operatorname{Br} k = \mathbf{Z}/2$, f/g étant une norme, les diviseurs de f et g sont par hypothèse des normes de l'extension K/k. Soit $(M_v)_{v\in\Omega}$ une famille de points locaux. S'il n'y a pas obstruction de Manin au principe de Hasse et à l'approximation faible on a, d'après le lemme fondamental 3, en notant $m = n-2$ et $M_v = (x_1^v, \ldots, x_m^v, y^v, z^v)$:

$$\sum_v j_v(f(M_v)) = \sum_v j_v(g(M_v)) = 0 \quad \text{dans } \mathbf{Z}/2$$

Or, on a la suite exacte, issue de la théorie du corps de classes global (cf. [6]):

$$0 \longrightarrow k^*/NK^* \longrightarrow \coprod_v k_v^*/NK_v^* \xrightarrow{\sum j_v} \mathbf{Z}/2 \longrightarrow 0$$

Où l'on note j_v le plongement donné par la théorie du corps de classe local et $K_v = k_v \otimes_k K$. Ainsi, il existe c_1 et c_2 dans k^* vérifiant $c_1 = f(x_1^v, \ldots, x_m^v)$ et $c_2 = g(x_1^v, \ldots, x_m^v)$ dans k_v^*/NK_v^*. Considérons alors la variété de descente T suivante:

$$\begin{aligned} f(x_1, \ldots, x_m) &= c_1(u_1^2 - av_1^2) && \neq 0 \\ g(x_1, \ldots, x_m) &= c_2(u_2^2 - av_2^2) && \neq 0 \\ y^2 - az^2 &= f(x_1, \ldots, x_m)g(x_1, \ldots, x_m) && \neq 0 \end{aligned}$$

D'après le choix de c_1, c_2, il existe $(P_v)_{v\in\Omega}$, famille de points locaux de T, dont la projection $p(P_v)$ est M_v, c'est-à-dire que

$$P_v = (x_1^v, \ldots, x_m^v, y^v, z^v, u_1^v, u_2^v, v_1^v, v_2^v).$$

Il nous suffit donc pour conclure de montrer que T satisfait le principe de Hasse et l'approximation faible.

Effectuons le changement de variables:

$$\begin{cases} u_3 + \sqrt{a}v_3 = (y + \sqrt{a}z)/(u_1 + \sqrt{a}v_1)(u_2 + \sqrt{a}v_2) \\ u_3 - \sqrt{a}v_3 = (y - \sqrt{a}z)/(u_1 - \sqrt{a}v_1)(u_2 - \sqrt{a}v_2) \end{cases}$$

On est ramené à la variété T_1:

$$\begin{array}{rll} u_3^2 - av_3^2 & = c_1c_2 & \neq 0 \\ f(x_1, \ldots, x_m) & = c_1(u_1^2 - av_1^2) & \neq 0 \\ g(x_1, \ldots, x_m) & = c_2(u_2^2 - av_2^2) & \neq 0 \end{array}$$

Soit Z la k-variété de $\mathbf{P}_k^r$ $(r = n + 2)$ d'équation:

$$\begin{cases} \varphi(x_1, \ldots, x_m, t) = c_1(u_1^2 - av_1^2) \\ \psi(x_1, \ldots, x_m, t) = c_2(u_2^2 - av_2^2) \end{cases}$$

C'est l'intersection de deux quadriques dans $\mathbf{P}_k^r$, avec $r \geq 6$, qui n'est pas un cône (toujours parce que l'intersection des noyaux des formes quadratiques φ et ψ est réduite à 0) et qui contient une paire de droites gauches conjuguées, soit $(x_1 = \ldots = x_m = t = 0,\ u_1 = \varepsilon\sqrt{a}v_1,\ u_2 = \varepsilon\sqrt{a}v_2), \varepsilon \in \{-1, 1\}$. D'après le théorème 13.2 de [3], un modèle projectif lisse de Z vérifie le principe de Hasse et l'approximation faible. Il en va donc de même de T_1 (qui est k-birationnelle au produit de Z et d'une conique). D'où le résultat.

Les deux autres cas utilisent la théorie générale de la descente qui est développée dans [4]: à partir d'une résolution de $\operatorname{Pic}\overline{X}$ par des G-modules de permutation, on obtient des équations de variétés de descente. Dans le cas $n = 4$, le fait que l'on suppose les R_i deux à deux conjugués permet encore de se ramener à une intersection de deux quadriques pour laquelle on sait conclure avec les résultats de [3]. Dans le cas $n = 5$, on sait montrer le principe de Hasse et l'approximation faible pour les variétés de descente par un théorème de fibration voisin du lemme 2. Pour plus de détails, nous renvoyons à [5].

CONCLUSION: La conjecture énoncée au paragraphe 1 admet donc une réponse affirmative quand le groupe de Brauer de X est non trivial, quand $n \geq 5$, quand $n = 3$, et dans certains cas pour $n = 4$. Le cas a priori encore ouvert est celui où $n = 4$ et où les deux coniques définies par φ et ψ se coupent suivant quatre points conjugués, avec $\operatorname{Br} X/\operatorname{Br} k = 0$. La méthode qui fonctionne quand leur intersection consiste en deux paires de points conjugués conduit à des variétés de descente qui sont des intersections non plus de deux, mais de trois quadriques, pour lesquelles on ne dispose guère de résultats.
Toutefois, il se trouve qu'une hypersurface cubique (géométriquement intègre, non conique) de $\mathbf{P}_k^n$ qui possède un ensemble globalement rationnel de deux

points singuliers conjugués est k-birationnelle à une hypersurface V de $\mathbf{A}^n_k$ dont l'équation est du type (1) ([3], proposition 9.8.). Dans ce cas particulier, on sait encore (sans hypothèse supplémentaire) démontrer que la conjecture est vraie pour V ([5]): la preuve combine méthode de fibrations et méthode de descente, elle utilise les calculs de groupe de Brauer de cet article, ainsi que des résultats analytiques de la théorie du corps de classes.

4. Contre-exemples au principe de Hasse et à l'approximation faible

Nous présentons ici trois exemples où l'on a obstruction de Brauer-Manin. Nous nous contenterons détudier en détail le premier exemple, les autres s'analysant de la même manière.

Proposition 2. *Soit X la $\mathbf{Q}$-hypersurface de $\mathbf{A}^4_{\mathbf{Q}}$ d'équation:*

$$y^2 + z^2 = (28(x_1^2+1) + 79(x_2^2+1))(95(x_1^2+1) + 268(x_2^2+1))$$

Alors X ne vérifie pas le principe de Hasse

Posons $\alpha = 28$, $\beta = 79$, $\gamma = 95$, $\delta = 268$. On a $\alpha\delta - \beta\gamma = -1$ et $\alpha = 4(4k-1)$, $\beta = 4l-1$, $\gamma = 4k'-1$, $\delta = 4(4l'-1)$ avec $(k,l,k',l') \in \mathbf{N}$ (ces deux propriétés sont en fait essentiellement les seules dont on va se servir dans la preuve). On notera encore $f(x_1,x_2) = (\alpha(x_1^2+1) + \beta(x_2^2+1))$ et $g(x_1,x_2) = (\gamma(x_1^2+1) + \delta(x_2^2+1))$ et U l'ouvert de X défini par $y^2+z^2 = f(x_1,x_2)g(x_1,x_2) \neq 0$. Nous utiliserons deux lemmes:

Lemme 4. *Soit $M_p \in U(\mathbf{Q}_p)$ un point local avec p premier, $p \notin \{2,\infty\}$. Alors l'image $\varphi_p(M_p)$ de $f(M_p)$ dans $\mathbf{Q}_p^*/NK_p^*$ est triviale (où $K_p = \mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(i)$).*

PREUVE DU LEMME 4: Soit p premier inerte dans l'extension $\mathbf{Q}(i)/\mathbf{Q}$ (si p n'est pas inerte, $\mathbf{Q}_p^*/NK_p^*$ est trivial), c'est-à-dire p tel que -1 n'est pas un carré dans $\mathbf{Q}_p^*$, ou encore $p \equiv -1\,[4]$. Supposons $v_p(f(x_1,x_2)) = 2r+1$ avec $(y,z,x_1,x_2) \in U(Q_p)$. Alors, $v_p(g(x_1,x_2)) = 2s+1$ avec par exemple $s \geq r$. De $v_p(\alpha g(x_1,x_2) - \gamma f(x_1,x_2)) \geq 2r+1$, on tire $v_p(x_2^2+1) \geq 2r+1$ et de même, de $v_p(\beta g(x_1,x_2) - \delta f(x_1,x_2)) \geq 2r+1$, on tire $v_p(x_1^2+1) \geq 2r+1$. Comme la valuation p-adique d'une norme est paire, on en déduit $v_p(x_1^2+1) \geq 2r+2$ et $v_p(x_2^2+1) \geq 2r+2$ ce qui contredit $v_p(f(x_1,x_2)) = 2r+1$. Ainsi, pour tout p inerte, $v_p(f(x_1,x_2))$ est paire et on a le résultat voulu (cf. [7]).

Lemme 5. *Soit $M_2 \in U(\mathbf{Q}_2)$ un point local 2-adique. Alors $f(M_2)$ est non trivial dans $\mathbf{Q}_2^*/NK_2^*$.*

PREUVE DU LEMME 5: Posons $M_2 = (y, z, x_1, x_2) \in \mathbf{Q}_2^4$. Comme (x_1^2+1) et (x_2^2+1) sont des normes, on peut (cf. [7]) écrire $(x_1^2+1) = 2^u(4r+1)$ et $(x_2^2+1) = 2^v(4s+1)$ avec u, v dans $\mathbf{Z}$ et r, s dans $\mathbf{Z}_2$. Si $u \geq v$, $\alpha(x_1^2+1)+\beta(x_2^2+1) = 2^v(\alpha 2^{(u-v)}(4r+1)+\beta(4s+1))$. Comme $\alpha = 4(4k-1)$ et $\beta = 4l-1$, $(\alpha 2^{(u-v)}(4r+1)+\beta(4s+1))$ est un élément de $\mathbf{Z}_2$ de la forme $4t-1$ avec $t \in \mathbf{Z}_2$ donc $f(x_1, x_2)$ n'est pas une norme 2-adique (cf. [7]). De même, si $v \geq u$, c'est $g(x_1, x_2)$ qui ne peut être une norme 2-adique, d'où le résultat.

PREUVE DE LA PROPOSITION 2: Pour tout point réel M_∞, on a trivialement $f(M_\infty)$ positif. Ainsi, d'après les deux lemmes précédents, pour toute famille de points locaux (M_p) $(M_p \in U(\mathbf{Q}_p))$, $\sum_p j_p(\varphi_p(M_p))$ n'est pas trivial dans $\mathbf{Z}/2$; il suffit donc (cf. lemme fondamental 3) pour conclure de montrer que X a des points dans tous les complétés de $\mathbf{Q}$. Or en faisant $x_1 = x_2 = 0$, on obtient un point 2-adique puisque $(\alpha+\beta)(\gamma+\delta) = 107.3.11^2$ est une norme 2-adique. De même, en faisant $x_1 = x_2 = 0$, on obtient un point p-adique pour $p \notin \{3, 11, 107\}$ et en faisant $x_1 = 1/p, x_2 = 0$, on obtient un point p-adique pour $p \in \{3, 11, 107\}$. Ceci achève la preuve.

Les deux contre-exemples à l'approximation faible suivants (pour lesquels le principe de Hasse est vérifié) se traitent de façon analogue (cf. [5]): pour toute famille de points locaux M_p, $\varphi_p(M_p)$ est trivial dans $\mathbf{Z}/2$, sauf pour $p = 2$ où $\varphi_2(M_2)$ peut etre trivial ou non trivial (selon le point M_2).

Proposition 3. *Soit X la $\mathbf{Q}$-hypersurface de $\mathbf{A}_\mathbf{Q}^4$ d'équation:*

$$y^2 + z^2 = ((x_1-2)^2 + x_2^2 - 3)((x_1+2)^2 + x_2^2 - 3)$$

Alors X ne vérifie pas l'approximation faible.

Proposition 4. *Soit X la $\mathbf{Q}$-hypersurface de $\mathbf{A}_\mathbf{Q}^5$ d'équation:*

$$y^2 + z^2 = f(x_1, x_2, x_3)g(x_1, x_2, x_3)$$

avec $f(x_1, x_2, x_3) = (x_1^2+1) + (x_2^2 + x_3^2 + 3)$, $g(x_1, x_2, x_3) = x_2^2 + x_3^2 + 3$. Alors X ne vérifie pas l'approximation faible.

Appendice 1 : invariance birationnelle du principe de Hasse et de l'approximation faible

Rappelons d'abord un lemme classique (cf. [1]), dû à Nishimura et Lang :

LEMME. *Soit X une k-variété intègre lisse, Y une k-variété propre, $\varphi : X \to Y$ une application rationnelle. Alors, si $X(k) \neq \varnothing$, on a : $Y(k) \neq \varnothing$.*

Maintenant, une application immédiate de ce lemme, combiné avec le théorème des fonctions implicites v-adiques, permet de déduire la proposition suivante, annoncée dans l'introduction :

PROPOSITION. *Soit V une k-variété. Si un modèle propre lisse X de V vérifie le principe de Hasse (resp. l'approximation faible), il en est de même de tout modèle propre lisse de V. Ainsi, ces propriétés ne dépendent que du corps des fonctions $k(V)$ de la variété V. Il suffit de les vérifier pour le lieu lisse V_{lisse} de V.*

Appendice 2 : obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible

Soit X une k-variété algébrique, géométriquement intègre, propre et lisse, qui a des points dans tous les k_v. Alors, pour tout A dans $\operatorname{Br} X$, on a le diagramme commutatif suivant (cf. [4]) :

$$\begin{array}{ccccc} X(k) & \longrightarrow & X(A_k) & & \\ {\scriptstyle A}\downarrow & & {\scriptstyle A}\downarrow & \searrow^{i_A} & \\ \operatorname{Br} k & \longrightarrow & \bigoplus_v \operatorname{Br} k_v & \xrightarrow{\sum_v \operatorname{inv}_v} & \mathbf{Q}/\mathbf{Z} \end{array}$$

où $X(A_k) = \prod_{v \in \Omega_k} X(k_v)$. Maintenant, ce diagramme montre que pour un point global P dans $X(k)$ dont l'image dans k_v est P_v, on a :

$$\sum_{v \in \Omega_k} \operatorname{inv}_v A(P_v) = 0 \text{ dans } \mathbf{Q}/\mathbf{Z}$$

Si $X(k) \neq \varnothing$, il existe donc des point locaux (P_v) avec $\sum_{v \in \Omega_k} \operatorname{inv}_v A(P_v)$ nul dans $\mathbf{Q}/\mathbf{Z}$ et si $X(k)$ est dense dans $\prod_{v \in S} X(k_v)$, l'égalité précédente est vraie pour tout élément de $X(A_k)$ qui est l'image d'un point de $X(k)$, donc par densité pour tout élément de $X(A_k)$. Ainsi, les conditions de la proposition 1 du paragraphe 1 sont bien des obstructions au principe de Hasse et à l'approximation faible.

Bibliographie

[1] J.-L. Colliot-Thélène, D. Coray, J.-J. Sansuc: *Descente et principe de Hasse pour certaines variétés rationnelles*, J. reine angew. Math. **320** (1980) 150-191.

[2] J.-L. Colliot-Thélène, P. Salberger: *Arithmetic on singular cubic hypersurfaces*, Proc. London Math. Soc. (3) **58** (1989), 519-549.

[3] J.-L. Colliot-Thélène, J.-J. Sansuc, Sir P. Swinnerton-Dyer: *Intersection of two quadrics and Châtelet surfaces*, J. reine angew. Math. **373** (1987), 307-107; **374** (1987), 72-168

[4] J.-L. Colliot-Thélène, J.-J. Sansuc: *La descente sur les variétés rationnelles* II, Duke Math. J. **54** (1987), 375-492.

[5] D. Harari: *Principe de Hasse et approximation faible sur certaines hypersurfaces*, preprint 1992

[6] S. Lang: *Algebraic number theory*, Springer Verlag 1986

[7] J.-P. Serre: *Cours d'arithmétique*, PUF 1970

[8] A.-N. Skorobogatov: *Arithmetic on certain quadric bundles of relative dimension 2*, J. reine angew. Math. **407** (1990), 57-74.

[9] A.-N. Skorobogatov: *On the fibration method for proving the Hasse principle and weak approximation*, Séminaire de théorie des nombres de Paris 1988-1989, 205-219.

David HARARI
E. N. S., Département de
mathématiques et informatique
45 rue d'Ulm
75005 Paris, France

Astérisque

WERNER HÜRLIMANN

A short proof of the Albert-Brauer-Hasse-Noether theorem

Astérisque, tome 209 (1992), p. 215-220

<http://www.numdam.org/item?id=AST_1992__209__215_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

A SHORT PROOF OF THE ALBERT-BRAUER-HASSE-NOETHER THEOREM

Werner Hürlimann *

We present a short proof of the Albert-Brauer-Hasse-Noether theorem on the Brauer group of a global field. The connection between Galois cohomology and algebraic tori theory is emphasized. Let K/k be a finite Galois extension of arbitrary fields with group G, then the relative Brauer group is $Br(K/k) \cong H^2(G,K^*) \cong H^1(G,T_1(K))$, where T_1 is the algebraic k-torus associated to the augmentation ideal I_G of G. When k is a global field, we use fundamental facts from algebraic tori theory, Tate-Nakayama duality and modern versions of Grunwald-Wang's lemma to deduce the short exact sequence

$$0 \longrightarrow Br(k) \longrightarrow \bigoplus_v Br(k_v) \longrightarrow Q/Z \longrightarrow 0,$$

where k_v runs over the completions of k at all places v of k.

* This work was done in great part at the Max-Planck-Institut für Mathematik in Bonn during a visit in 1982/83. Financial support from the Swiss National Foundation for scientific research is gratefully acknowledged.

1. Preliminaries.

Since the seminal work by Manin(1970), the Brauer group plays an increasingly important role in Number Theory and especially in questions related to the existence of rational points on algebraic varieties (see Lang(1991), chap. X). A recent introduction to the Brauer group over a field is Kersten(1990).

Besides the original proofs of the classical theorem of Albert-Brauer-Hasse-Noether, one finds proofs fitting the context of Diophantine Geometry in Shatz(1972) and Artin/Tate(1968). Thus the topic discussed in this note is well-known, only the conceptual presentation may be new. As pointed out by Serre(1962) for C_1-fields, the Brauer group of fields may be computed via algebraic tori theory. This follows also from our Theorem 1 in the special case n=2. Indeed the relative Brauer group of a Galois extension with finite group G is

$$Br(K/k) \cong H^2(G,K^*) \cong H^1(G,T_1(K)),$$

where T_1 is the algebraic k-torus associated to the augmentation ideal I_G of G.

Let K/k be a finite Galois extension of arbitrary fields with group G. The category of finitely generated ZG-modules which are free as abelian groups is denoted by L_G. The Z-dual of a ZG-module M is the ZG-module $M^\circ=Hom(M,Z)$. One knows that L_G is in duality with the category T(K/k) of algebraic tori defined over k and split by K (see Borel(1969) for example). A k-torus $T \in T(K/k)$ corresponds in this duality to the dual $X(T)^\circ$ of the character module $X(T)=Hom(T,G_m)$. Under the K-rational points of T, one understands the group $T(K)=Hom(X(T),K^*)$. Two algebraic k-tori T_1 and T_2 are called ***k-stably birationally equivalent*** if the k-varieties $T_1 x_k A^r(k)$ and $T_2 x_k A^s(k)$ are k-birationally equivalent for appropriate choices of the integers r and s. For an arbitrary ZG-module M, one denotes by $H^n(G,M)$ the Tate cohomology groups defined for all integers n. A ZG-module M is called a ***flasque module*** if $H^{-1}(H,M)=0$ for all subgroups $H \subset G$. It is shown in Colliot-Thélène/Sansuc(1977), Prop. 5 and 6, that there exists an ***invariant*** ρ, defined on T(K/k) with values in a "semigroup of similarity classes of flasque ZG-modules", and which characterizes the equivalence classes of k-stably birational equivalent tori. For a precise construction, the interested reader is referred to the mentioned work.

Let us link now Galois cohomology with algebraic tori theory. From the standard free resolution of Z, one obtains the short exact sequences

$$\begin{array}{l} 0 \longrightarrow X(T_1):=I_G \longrightarrow ZG \longrightarrow X(T_0):=Z \longrightarrow 0, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \varepsilon_n \\ 0 \longrightarrow X(T_{n+1}):=Ker(\varepsilon_n) \longrightarrow \bigoplus_{r \in G^n} ZG\cdot u(\mathbf{r}) \longrightarrow X(T_n) \longrightarrow 0, \quad n \geq 1, \end{array} \tag{1.1}$$

where the $u(\mathbf{r})=u(r_1,...,r_n)$, $r_i \in G$, are symbols such that the $s.u(\mathbf{r})$, $s \in G$, form a Z-basis of $\bigoplus_{r \in G^n} ZG\cdot u(\mathbf{r})$. The action of G on $u(\mathbf{r})$ is trivial and ε_n is the ZG-homomorphism defined by $\varepsilon_n(u(\mathbf{r}))=(d_{n-1}u)(\mathbf{r})$, where d_{n-1} is the usual coboundary in

the cohomology theory of groups. To the ZG-module $X(T_n)$ corresponds by duality the algebraic k-tori T_n split by K. For n negative one defines T_n by specifying its character module $X(T_n)=X(T_{-n})^\circ$. Then one applies the functor $\mathrm{Hom}(\cdot,K^*)$ to the sequence (1.1). Since $\mathrm{Hom}(ZG,K^*)=ZG\otimes K^*$ is G-induced, one has $H^n(G,\mathrm{Hom}(ZG,K^*))=0$ for all n. From the associated long exact sequences of cohomology one derives the following result (mentioned by Opolka in Schappacher/Scholz(1992), p. 18).

THEOREM 1. *For all finite Galois extensions of arbitrary fields K/k with group G and for all positive integers i, n such that* $1 \le i \le n$, *one has* $H^n(G,K^*) \cong H^i(G,T_{n-i}(K))$, *and a similar result holds for negative integers.*

Recall now some standard facts from algebraic number theory. Assume in the following that K and k are global fields. By A_K, J_K and $C_K=J_K/K^*$, one denotes respectively the ***adele ring*** of K, the ***idele group*** of K and the ***idele classgroup*** of K. For $T \in T(K/k)$ one defines $T(A_K)=\mathrm{Hom}(X(T),J_K)$ and $T(C_K)=T(A_K)/T(K)=\mathrm{Hom}(X(T),C_K)$. The set of all places v of k is denoted by P.

The following result is the generalization of one of the main theorems in classfield theory, which states that the finite Galois extensions K/k build up a ***classformation*** with respect to the idele classgroup C_K.

THEOREM 2. (**Tate-Nakayama duality**) *Let K/k be a finite Galois extension of global fields with group G. For every integer n and for any* $T \in T(K/k)$, *there is a (non-canonical) isomorphism* $H^n(G,T(C_K)) \cong H^{2-n}(G,X(T))$.

Proof. See the work of Tate and Nakayama or Ono(1963), 2.2.1.

As a ***special case*** when $T=G_m$, one gets $H^n(G,C_K)\cong H^{2-n}(G,Z)$, which is a main theorem in classfield theory.

By application of the functor $\mathrm{Hom}(\cdot,J_K)$ to the sequences (1.1) and by passing to the long exact sequences of cohomology using that $H^n(G,\mathrm{Hom}(ZG,J_K))=0$ for all n (since $\mathrm{Hom}(ZG,J_K)=ZG\otimes J_K$ is G-induced!), one gets the analogue of Theorem 1.

THEOREM 3. *For all finite Galois extensions of global fields K/k with group G and for all positive integers i, n such that* $1 \le i \le n$, *one has* $H^n(G,J_K)\cong H^i(G,T_{n-i}(A_K))$.

Finally for a torus $T \in T(K/k)$ one denotes by $Ш^n(T)$ the kernel of the natural map $H^n(G,T(K)) \longrightarrow H^n(G,T(A_K))$. The group $Ш^1(T)$, simply written $Ш(T)$, is the so-called Shafarevich-Tate group of T. The cokernel of the map $H^1(G,T(K)) \longrightarrow H^1(G,T(A_K))$ is denoted by $Ч(T)$.

2. Computation.

Let us evaluate the ***Brauer group*** Br(k) of a global field k. Let K/k be a finite Galois extension of global fields with group G. By Theorem 1 one has $H^2(G,K^*)=H^1(G,T_1(K))$ and by Theorem 3 one has $H^2(G,J_K)=H^1(G,T_1(A_K))$. By definition of the groups $Ш(\cdot)$ and $Ч(\cdot)$ one gets the exact sequence

$$(2.1) \qquad 0 \longrightarrow Ш(T_1) \longrightarrow H^2(G,K^*) \longrightarrow H^2(G,J_K) \longrightarrow Ч(T_1) \longrightarrow 0.$$

The evaluation of the ρ-invariant of T_1 yields $\rho(T_1)=\rho(I_G)=0$ (see Colliot-Thélène/Sansuc(1977), prop. 5 and 6). From the same work, prop. 18, it follows that $Ш(T_1)=0$. On the other hand from the long exact sequence associated to the sequence

$$1 \longrightarrow T_1(K) \longrightarrow T_1(A_K) \longrightarrow T_1(C_K) \longrightarrow 1,$$

one derives the exact sequence

$$(2.2) \qquad 0 \longrightarrow Ч(T_1) \longrightarrow H^1(G,T_1(C_K)) \longrightarrow Ш^2(T_1) \longrightarrow 0.$$

By Tate-Nakayama duality, that is Theorem 2, one has

$$H^1(G,T_1(C_K)) = H^1(G,X(T_1)) = H^1(G,I_G) = H^0(G,Z) = Z/nZ,$$

where n is the ***order*** of the group G. Moreover applying Theorems 1 and 3 one gets

$$\begin{aligned} Ш^2(T_1) &= \mathrm{Ker}(\, H^2(G,T_1(K)) \longrightarrow H^2(G,T_1(A_K))\,) \\ &= \mathrm{Ker}(\, H^3(G,K^*) \longrightarrow H^3(G,J_K)\,) \\ &= H^3(G,K^*), \end{aligned}$$

the last equality following since $H^3(G,J_K)=0$ by classfield theory (see for example Neukirch(1969), III, (3.5) in the case of number fields, or Iyanaga(1975), chap. V, Theorem 1.4, in the general case). Furthermore the third cohomological group $H^3(G,K^*)$ is cyclic of order n/m where $m=m_{K/k}$ (depending on the extension K/k) is the least common multiple of the local degrees (see for example Cassels/Fröhlich(1967), p. 199). Introduced in (2.2) these two results provide the equality

$$(2.3) \qquad Ч(T_1) = Z/m_{K/k}Z.$$

Introduced in (2.1) together with $Ш(T_1)=0$ this generates a whole class of exact sequences whose members are

$$(2.4) \qquad 0 \longrightarrow H^2(G,K^*) \longrightarrow H^2(G,J_K) \longrightarrow Z/m_{K/k}Z \longrightarrow 0.$$

This class defines a ***directed system*** of exact sequences of abelian groups with respect

to inflation on cohomology groups and the divisibility property of the integer symbols $m_{K/k}$. For L/K, L/k and K/k all Galois extensions the ***partial ordering*** of this system, formally written $K/k \preceq L/k$, is provided by the existence of inflation homomorphisms $\mathrm{Inf} : H^2(G_{K/k},K^*) \longrightarrow H^2(G_{L/k},L^*)$ and $\mathrm{Inf} : H^2(G_{K/k},J_K) \longrightarrow H^2(G_{L/k},J_L)$ and the fact that $m_{K/k}$ divides $m_{L/k}$. Moreover since $H^1(G_{L/k},L^*)=H^1(G_{L/k},J_L)=0$ the inflation maps are actually injective. Therefore the partial ordering of this system can be viewed as ***inclusion*** of exact sequences. The system is ***directed.*** Indeed given Galois extensions K/k, L/k such that $K/k \preceq L/k$, there always exists a Galois extension M/k such that $M \supset K \supset k$, $M \supset L \supset k$ are all Galois extensions, hence also $K/k \preceq M/k$ and $L/k \preceq M/k$. Now the integer symbols $m_{K/k}$ take on all values of $\mathbb{N}$. In fact this is already true for cyclic extensions (for example Neukirch(1969), III, (3.7) in the case of number fields and the generalized Grunwald-Wang theorems of Saltman(1982) in the general case). The functor ***direct limit*** yields from (2.4) the exact sequence

$$(2.5)\quad 0 \longrightarrow \varinjlim_{K/k} H^2(G_{K/k},K^*) \longrightarrow \varinjlim_{K/k} H^2(G_{K/k},J_K) \longrightarrow \varinjlim_{K/k} Z/m_{K/k}Z \longrightarrow 0.$$

In view of the inclusion interpretation of the above inflation maps and completing with the necessary details (for example Neukirch(1969), III, p. 244), one obtains the desired famous result.

THEOREM 4. (**Albert-Brauer-Hasse-Noether**) *Let k be a global field. The following sequence*

$$0 \longrightarrow Br(k) \longrightarrow \bigoplus_{v \in P} Br(k_v) \xrightarrow{inv} Q/Z \longrightarrow 0$$

is exact, where $inv=\sum inv_v$ *is the sum of the local invariant maps.*

References

Artin, E., Tate, J.(1968), Class field theory, Benjamin.
Borel, A.(1969), Linear Algebraic Groups, New York.
Cassels, J.W.S, Fröhlich, A.(1967) (editors), Algebraic Number Theory, Thompson, Washington.
Colliot-Thélène, J.-L., Sansuc, J.-J.(1977), La R-équivalence sur les tores, Ann. Scient. Ecole Norm. Sup. (4), 10, 175-229.
Iyanaga, S.(1975), The Theory of Numbers, North-Holland Publ. Co., Amsterdam.
Kersten, I.(1990), Brauergruppen von Körpern, Aspekte der Mathematik, D6.
Lang, S.(1991) (Ed.), Number Theory III, Diophantine Geometry, Encyclopaedia of Mathematical Sciences, vol. 60, Springer.
Manin, J.(1970), Le groupe de Brauer-Grothendieck en géométrie diophantienne, Actes du Congrès International Math., tome 1, 401-11.

Neukirch, J.(1969), Klassenkörpertheorie, BI-Hochschulskripten, Mannheim.
Ono, T.(1963), On the Tamagawa number of algebraic tori, Ann. Math. 78, 47-73.
Saltman, D.J.(1982), Generic Galois extensions and problems in field theory, Advances in Mathematics 43, 250-83.
Schappacher, N., Scholz, E.(1992), Oswald Teichmüller - Leben und Werk, Jahresbericht der Deutschen Mathematiker-Vereinigung 94, 1-39.
Serre, J.-P.(1962), Corps locaux, Hermann, Paris (engl. transl. appeared as "Local fields", Graduate Texts in Mathematics 67, Springer).
Shatz, S.(1972), Profinite groups, arithmetic, and geometry, Annals of Mathematical Studies 67, Princeton Univ. Press.

Hürlimann Werner
Allgemeine Mathematik
Winterthur-Leben
Römerstr. 17
CH-8401 Winterthur

Astérisque

WOLFGANG JENKNER

Les corps p-adiques dont les groupes de Galois absolus sont isomorphes

Astérisque, tome 209 (1992), p. 221-226

<http://www.numdam.org/item?id=AST_1992__209__221_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

LES CORPS p-ADIQUES DONT LES GROUPES DE GALOIS ABSOLUS SONT ISOMORPHES

Wolfgang JENKNER

Soit p un nombre premier quelconque. Pour toute extension finie $K/\mathbb{Q}_p$, soit $K^0/\mathbb{Q}_p$ la sous-extension abélienne maximale de $K/\mathbb{Q}_p$. De plus, on désignera par $\bar{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$, et par G_K le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$.

THÉORÈME.– *Soient* $K/\mathbb{Q}_p$ *et* $L/\mathbb{Q}_p$ *deux extensions finies. Alors* $G_K \simeq G_L$ *entraîne* $K^0 = L^0$.

Dans [3] M. Jarden et J. Ritter ont donné une démonstration de l'énoncé du théorème en faisant l'hypothèse supplémentaire que K et, par conséquent, L contiennent une racine de l'unité d'ordre $2p$. C'est là une restriction que J. Ritter a su enlever lorsque $p \neq 2$ ([6]).

D'un autre côté, tout en restant très proche des idées exposées dans [3], on peut montrer que le résultat reste encore vrai si l'extension de K engendrée par une racine de l'unité d'ordre $2p$ n'a pas de ramification sauvage (sur K), ce qui permet d'obtenir les résultats de [6] d'une manière quelque peu différente et, en même temps, d'aller un peu plus loin si $p = 2$.

D'ailleurs, c'est en supposant vérifiée cette condition-là que U. Jannsen, K. Wingberg ([2]) et V. Diekert ([1]) ont donné une description de G_K, à partir de laquelle on déduit les résultats susmentionnés d'une manière assez directe.

Or, pour ce qui concerne le but de cet article, les écueils de la ramification sauvage (dans le cas $p = 2$) seront tournés dans la proposition 2.

D'abord, fixons quelques notations : Pour toute extension finie $K/\mathbb{Q}_p$, soit n_K le degré, f_K le degré résiduel et e_K l'indice de ramification de cette extension. Si K'/K est une extension finie, on pose $f(K'/K) = f_{K'}/f_K$ et de même $e(K'/K) = e_{K'}/e_K$.

Pour tout $m \in \mathbb{N}$, on désigne par ζ_m une racine de l'unité d'ordre m (contenue dans $\bar{\mathbb{Q}}_p$).

De plus, soit $r_K = \max\{\nu \in \mathbb{N} \mid \zeta_{p^\nu} \in K(\zeta_{2p})\}$ et soit

$$d_K = \max\{\nu \in \mathbb{N} \mid K(\zeta_{p^{r_K+\nu}})/K(\zeta_{2p}) \text{ est non ramifiée }\}.$$

On voit facilement que $f_K = f_{K^0}$, $r_K = r_{K^0}$ et $d_K = d_{K^0}$ (cf. [3]).

PROPOSITION 1.- *Soit $K/\mathbb{Q}_p$ une extension finie telle que $\zeta_{2p} \in K$. Alors*

$$\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) \subset K^0 \subset \mathbb{Q}_p(\zeta_{(p^{fp^d}-1)p^{r+d}}) = K^0(\zeta_{p^{r+d}})$$

où f, d et r désignent respectivement f_K, d_K et r_K.

Preuve. – On utilisera des résultats de la théorie du corps de classes local ([7] XI, §4). Pour toute extension finie $K'/\mathbb{Q}_p$, soit $\mathcal{N}K'$ le groupe de normes (dans $\mathbb{Q}_p^\times$). Alors il est bien connu que $\mathcal{N}\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) = \langle p^f \rangle \times U^{(r)}$, où $U^{(0)} = \mathbb{Z}_p^\times$ et $U^{(r)} = 1 + p^r\mathbb{Z}_p$ pour $r \geq 1$.

Soient $k \in \mathbb{N}_0$ et $u \in \mathbb{N}$ tels que $p \nmid u$ et $p^k u = [K^0 : \mathbb{Q}_p(\zeta_{(p^f-1)p^r})]$. Alors on a aussi $p^k u = (\mathcal{N}\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) : \mathcal{N}K^0)$. On en déduit que

$$\mathcal{N}K^0 \supset (\langle p^f \rangle \times U^{(r)})^{p^k u} = \langle p^{fp^k u} \rangle \times U^{(r+k)} = \mathcal{N}\mathbb{Q}_p(\zeta_{(p^{fp^k u}-1)p^{r+k}}).$$

Il s'ensuit que le corps K^0 est contenu dans $\mathbb{Q}_p(\zeta_{(p^{fp^k u}-1)p^{r+k}})$. Étant donné que

$$p^k = e(\mathbb{Q}_p(\zeta_{(p^{fp^k u}-1)p^{r+k}})/\mathbb{Q}_p(\zeta_{(p^f-1)p^r})) = p^k u e(\mathbb{Q}_p(\zeta_{(p^{fp^k u}-1)p^{r+k}})/K^0),$$

on obtient $u = 1$, donc $K^0 \subset \mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}})$. De plus, il en résulte que $\mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}})/K^0$ n'est pas ramifiée.

Puis on a

$$\begin{aligned} p^{2k} &= [\mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}}) : \mathbb{Q}_p(\zeta_{p^f-1)p^r})] \\ &= [\mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}}) : K^0]\,[K^0 : \mathbb{Q}_p(\zeta_{(p^f-1)p^r})], \end{aligned}$$

ce qui donne $[\mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}}) : K^0] = p^k$.

Évidemment, le corps $K^0(\zeta_{p^{r+k}})$ est contenu dans $\mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}})$. Comme toutes les sous-extensions de $\mathbb{Q}_p(\zeta_{p^{r+k}})/\mathbb{Q}_p(\zeta_{p^r})$ sont de la forme $\mathbb{Q}_p(\zeta_{p^{r+\nu}})/\mathbb{Q}_p(\zeta_{p^r})$, il s'ensuit $[K^0(\zeta_{p^{r+k}}) : K^0] = p^k$, donc $K^0(\zeta_{p^{r+k}}) = \mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}})$. Puisque $K^0(\zeta_{p^{r+k}})/K^0$ est non ramifiée, on a $k \leq d$. D'autre part, comme $K^0(\zeta_{p^{r+k+1}}) = \mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k+1}})$ est une extension ramifiée de $K^0(\zeta_{p^{r+k}}) = \mathbb{Q}_p(\zeta_{(p^{fp^k}-1)p^{r+k}})$, on a $k \geq d$. □

Pour lier l'action de G_K sur des racines de l'unité à la structure même du groupe, on se servira du lemme suivant.

LEMME 1.– *Soit* k *un corps et soit* D *le corps de décomposition du polynôme* $x^n - a \in k[x]$, *que l'on suppose irréductible sur* $K = k(\zeta_n)$.

Soit le caractère $\chi : \mathrm{Gal}(K/k) \to \mathbb{Z}/(n)^\times$ *donné par* $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$. *Alors pour tout* $\sigma \in \mathrm{Gal}(K/k)$ *et pour tout* $\tau \in \mathrm{Gal}(D/K)$, *on a* $\tau^\sigma = \tau^{\chi(\sigma)}$.

Preuve. –Tous les caractères de $\mathrm{Gal}(D/K)$ sont de la forme $\phi : \tau \mapsto \frac{\tau(\alpha)}{\alpha}$ pour tout $\tau \in \mathrm{Gal}(D/K)$, où α est une racine de $x^n - a$. On voit aussitôt que $\phi(\tau^\sigma) = \sigma\phi(\tau)$. Il suffit de choisir l'automorphisme τ et le caractère ϕ tels que $\phi(\tau) = \zeta_n$. □

Remarque. On peut prouver un résultat plus général : Soit D/k une extension galoisienne finie et K/k une sous-extension galoisienne telle que D/K soit abélienne. Soient $G = \mathrm{Gal}(D/k)$ et $H = \mathrm{Gal}(D/K)$. Alors

$$(D^\times/K^\times)^G \to \mathrm{Hom}_G(H, K^\times)$$
$$\alpha K^\times \mapsto (\tau \mapsto \frac{\tau(\alpha)}{\alpha})$$

est un isomorphisme.

Esquissons brièvement une preuve de cette proposition : La suite exacte de Hochschild-Serre, appliquée au G-module $K^\times$ donne un isomorphisme $H^1(G, K^\times) \xrightarrow{res} H^1(H, K^\times)^G = \mathrm{Hom}_G(H, K^\times)$, tandis que

$$1 \to K^\times \to D^\times \to D^\times/K^\times \to 1$$

donne l'isomorphisme $(D^\times/K^\times)^G \xrightarrow{\delta} H^1(G, K^\times)$. □

Donc, pour appliquer le lemme, il faudra construire des extensions appropriées.

PROPOSITION 2.– *Soit* $K/\mathbb{Q}_p$ *une extension finie et soit* π *un élément premier de* K. *Alors, pour tout* $n \in \mathbb{N}$, *on a*

$$K(\pi^{p^{-n}}) \cap K(\zeta_{p^{r+d}}) = K.$$

(*Ici* $\pi^{p^{-n}}$ *désigne une racine dans* $\bar{\mathbb{Q}}_p$ *du polynôme* $X^{p^n} - \pi$, *et* $r = r_K$, $d = d_K$.)

Preuve. – Si $p \neq 2$, il suffit de comparer les indices de ramification : $e(K(\pi^{p^{-n}})/K) = p^n$, alors que $e(K(\zeta_{p^{r+d}})/K) \mid p - 1$.
Si $p = 2$, on s'appuie sur les deux propositions auxiliaires suivantes :

(i) On a toujours $\sqrt{\pi} \notin K(\zeta_4)$.
(ii) Si $d \geq 1$, on a $\sqrt{\pi} \notin K(\zeta_{2^{r+1}})$.

Preuve de **(i)**. Supposons $\zeta_4 \notin K$ et soient a, $b \in K$ tels que $\zeta_4 = a + b\sqrt{\pi}$, alors $-1 = a^2 + b^2\pi + 2ab\sqrt{\pi}$ et, par conséquent, $a^2 = -1$ ou $b^2\pi = -1$, ce qui est une contradiction.

Preuve de **(ii)**. Si $K(\sqrt{\pi}) \subset K(\zeta_{2^{r+1}})$, l'extension $K(\zeta_4)/K$ doit être ramifiée, puisque $K(\zeta_{2^{r+1}})/K(\zeta_4)$ ne l'est pas. Alors, il se trouve trois sous-extensions ramifiées de l'extension $K(\zeta_{2^{r+1}})/K$ de degré 4, que voici:

$$K(\zeta_4)/K, \quad K(\sqrt{\pi})/K, \quad K(\zeta_4\sqrt{\pi})/K.$$

Ces extensions de degré 2 sont différentes deux à deux grâce à l'assertion **(i)**, pourtant il en existe une autre non ramifiée. Cela n'est pas possible.

Maintenant, pour prouver la proposition, on pourrait procéder par induction, mais il est plus facile d'utiliser un critère connu ([4], ch. VIII, 9). □

Revenons aux données du théorème. Soient $K/\mathbb{Q}_p$ et $L/\mathbb{Q}_p$ deux extensions finies. Soit $\varphi : G_K \to G_L$ un isomorphisme de groupes topologiques.

Pour tout ce qui suit on fait la supposition que K'/K *et* L'/L *sont des extensions finies telles que* $G_{L'} = \varphi(G_{K'})$.

Les hypothèses entraînent que l'on a un isomorphisme $G_K^{ab} \simeq G_L^{ab}$ des groupes quotient abéliens maximaux. Du fait qu'un tel groupe est isomorphe au produit direct de $\hat{\mathbb{Z}}$ avec le groupe des unités du corps, on déduit facilement que $f_K = f_L$, $r_K = r_L$, $d_K = d_L$ et, de plus, si $K' = K(\zeta_n)$ on a $L' = L(\zeta_n)$ ([3]).

LEMME 2.– *S'il existe des extensions* $K' = K(\alpha)$ *et* $L' = L(\beta)$ *de degré n respectivement sur K et sur L telles que* $\alpha^n \in K$, $\beta^n \in L$ *et que* $K(\alpha) \cap K(\zeta_n) = K$, *alors, quel que soit* $\sigma \in G_K$, *on a* $\varphi(\sigma)(\zeta_n) = \sigma(\zeta_n)$.

Preuve. – C'est une conséquence du lemme 1 (compte tenu du fait que l'on a aussi $L(\beta) \cap L(\zeta_n) = L$). □

PROPOSITION 3.– *Soit* $n \in \mathbb{N}$ *tel que* $p \nmid n$. *Alors, pour tout* $\sigma \in G_K$, *on a* $\varphi(\sigma)(\zeta_n) = \sigma(\zeta_n)$.

Preuve. – Soit π_K un élément premier de K et soit α une racine n-ième quelconque de π_K. Alors $K' = K(\alpha)$ est une extension modérément et totalement ramifiée de K et, par conséquent, L' l'est aussi de L. Comme une telle extension peut être engendrée par une racine n-ième d'un élément premier de L, toutes les conditions du lemme précédent sont satisfaites. □

Rappelons que les éléments du groupe de Weil W_K^{ab} sont les automorphismes appartenant à G_K^{ab} dont les restrictions à l'extension non ramifiée maximale de K sont des puissances (à exposant entier) de l'automorphisme de Frobenius associé à K.

COROLLAIRE 1.– $\varphi(W_K^{ab}) = W_L^{ab}$.

Preuve. – L'extension non ramifiée maximale est engendrée par toutes les racines de l'unité ζ_n telles que $p \nmid n$. □

On désigne par $\varphi_{K',L'}$ la restriction $\varphi\,|_{W_{K'}}: W_{K'}^{ab} \to W_{L'}^{ab}$. De même, si $\psi = \varphi^{-1}$, on a un isomorphisme $\psi_{L',K'}$, de sorte que $\psi_{L',K'} = (\varphi_{K',L'})^{-1}$. En utilisant l'isomorphisme de réciprocité ([7] XIII, §4)

$$(\cdot, K^{ab}/K) : K^\times \to W_K^{ab},$$

et de même pour L, on obtient un isomorphisme $\bar{\varphi}_{K,L} : K^\times \to L^\times$ défini par $\bar{\varphi}_{K,L} = (\cdot, L^{ab}/L)^{-1} \circ \varphi_{K,L} \circ (\cdot, K^{ab}/K)$ (et de même pour K' et L').

PROPOSITION 4.– **(i)** $\bar{\varphi}_{K',L'}\,|_{K^\times} = \bar{\varphi}_{K,L}$.

(ii) $\bar{\psi}_{L',K'} = (\bar{\varphi}_{K',L'})^{-1}$.

(iii) *Soit* $M \subset \bar{\mathbb{Q}}_p^\times$ *tel que* $K' = K(M)$. *Alors* $L' = L(\bar{\varphi}_{K',L'}(M))$.

(iv) *Soit* π_K *un élément premier de* K. *Alors* $\bar{\varphi}_{K,L}(\pi_K)$ *est un élément premier de* L.

Preuve. – L'assertion **(i)** résulte de propriétés connues du *transfert* ([7] XI, §3 et XIV, §6 Ex 1.). La propriété **(ii)** est banale, alors que **(iii)** n'est qu'une conséquence de **(i)** et **(ii)**. Pour ce qui concerne **(iv)**, il suffit de remarquer que $(\pi_K, K^{ab}/K)$ est un prolongement de l'automorphisme de Frobenius ([7] XIII, Prop.13). □

COROLLAIRE 2.– *Si* π_K *est un élément premier de* K *tel que* $K' = K(\sqrt[n]{\pi_K})$, *alors il y a un élément premier* π_L *de* L *tel que* $L' = L(\sqrt[n]{\pi_L})$, *quel que soit* $n \in \mathbb{N}$.

PROPOSITION 5.– *Posons* $r = r_K = r_L$, $d = d_K = d_L$. *Alors, pour tout* $\sigma \in G_K$ *on a* $\varphi(\sigma)(\zeta_{p^{r+d}}) = \sigma(\zeta_{p^{r+d}})$.

Preuve. – C'est là une conséquence immédiate des lemme 2, corollaire 2 et proposition 2. □

Achevons la démonstration du théorème: Soit $F = \mathbb{Q}_p(\zeta_{(p^{fp^d}-1)p^{r+d}})$. On obtient un isomorphisme $\mathrm{Gal}(K(\zeta_{p^{r+d}})/K) \to \mathrm{Gal}(L(\zeta_{p^{r+d}})/L)$ et, par conséquent, un isomorphisme $\mathrm{Gal}(F/K^0) \to \mathrm{Gal}(F/L^0)$ donné par $\sigma|F \mapsto \varphi(\sigma)|F$ pour tout $\sigma \in G_K$ (Prop. 1); mais ces restrictions sont identiques d'après la prop. 3 et la prop. 5. □

Bibliographie

[1] V. Diekert, *Über die absolute Galoisgruppe dyadischer Zahlkörper*, J. Reine Angew. Math. **350** (1984), 152 – 172.

[2] U. Jannsen et K. Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper*, Invent. Math. **70** (1982), 71 – 98.

[3] M. Jarden et J. Ritter, *On the characterization of local fields by their absolute Galois groups*, J. Number Th., Vol 11, No 1 (1979).

[4] S. Lang, *Algebra*, Addison-Wesley 1984.

[5] J. Neukirch, *Class field theory*, Springer-Verlag, Berlin ... 1986.

[6] J. Ritter, *p-adic fields having the same type of algebraic extensions*, Math. Ann. **238** (1978), 281 – 288.

[7] J.-P. Serre, *Local fields*, Springer-Verlag, New York ... 1979.

Wolfgang Jenkner
Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36/IV
A-8010 Graz, Autriche

Astérisque

J. KACZOROWSKI

The boundary values of generalized Dirichlet series and a problem of Chebyshev

Astérisque, tome 209 (1992), p. 227-235

<http://www.numdam.org/item?id=AST_1992__209__227_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

The boundary values of generalized Dirichlet series and a problem of Chebyshev

J. KACZOROWSKI*

1. Introduction and statement of results

In 1853 Chebyshev asserted in a letter to M. Fuss that there are more primes $p \equiv 3 \pmod 4$ than $p \equiv 1 \pmod 4$. S. Knapowski and P. Turán in their well-known series of papers on comparative prime number theory [5] write, after quoting Littlewood's result that $\pi(x,4,1) - \pi(x,4,3)$ changes sign infinitely many times as $x \to \infty$, the following lines: *one feels that Chebyshev's vague formulation could also be interpreted so as*

$$\lim_{Y \to \infty} N(Y)/Y = 0, \tag{1.1}$$

where $N(Y)$ denotes the number of integers $m \leq Y$ with the property

$$\pi(m,4,1) \geq \pi(m,4,3) \tag{1.2}$$

(cf. also [6], page 26). They support this conjecture by referring to Shanks [7], who found that (1.2) is not fulfilled for $m \leq 26860$, is then fulfilled for $m = 26861$ and $m = 26862$, and is again false for $26863 \leq m \leq 616768$. They also ask the following general question ([5], Problem 7).

* The work is partially supported by KBN grant no. 2 1086 91 01.

For fixed positive integers a, b and q such that $(a,q)=(b,q)=1$, $a \not\equiv b \pmod q$, what is the asymptotical behaviour of $N_{a,b}(Y)$ for $Y \to \infty$, where $N_{a,b}(Y)$ denotes the number of integers $m \leq Y$ with

$$\pi(m,q,a) \geq \pi(m,q,b) \quad ?$$

Our aim is to prove a general result concerning boundary values of Dirichlet series and to show its relevance to Chebyshev's problem. As a corollary we obtain the following theorem.

THEOREM 1. *Suppose a and q are positive integers satisfying $(a,q)=1$, $a \not\equiv 1 \pmod q$ and let the Generalized Riemann Hypothesis (G.R.H.) be true for Dirichlet L-series $\pmod q$. Then there exist two constants $0 < c_1 < c_2 < 1$ such that the inequalities*

$$c_1 Y \leq N_{a,1}(Y) \leq c_2 Y$$

hold for all sufficiently large Y.

This shows that the Knapowski-Turán conjecture (1.1) is false at least when we accept the G.R.H.

The basic tool used in the proof of Theorem 1 is a result concerning generalized Dirichlet series which seems to be of an independent interest. For the sake of brevity, let $\mathcal{A}$ denote the set of all functions

$$F(z) = \sum_{n=1}^{\infty} a_n e^{iw_n z}, \quad z = x+iy, \quad y > 0 \tag{1.3}$$

satisfying the following conditions:

1. $0 \leq w_1 < w_2 < \dots$ are real numbers.
2. $a_n \in \mathbb{C}$, $n = 1,2,3,\dots$
3. There exists a non-negative integer B such that

$$\sum_{n=2}^{\infty} |a_n| w_n^{-B} < \infty. \tag{1.4}$$

4. There exists a non-negative number L_0 such that for every x, $|x| \geq L_0$, the limit

$$P(x) = \lim_{y \to 0+} \operatorname{Re} F(x+iy)$$

exists and represents a locally bounded function of $x \in \mathbb{R} \setminus [-L_0, L_0]$.

Moreover, let

$$\alpha(F) = \inf_{\substack{y>0 \\ x\in\mathbb{R}}} \operatorname{Re} F(x+iy), \qquad \beta(F) = \sup_{\substack{y>0 \\ x\in\mathbb{R}}} \operatorname{Re} F(x+iy).$$

It was proved in [4] that if $F \in \mathcal{A}$ and $\alpha(F) < u < \beta(F)$ then there exists a positive number $l = l(u, F)$ such that

$$\inf_{x\in I} P(x) < u < \sup_{x\in I} P(x) \tag{1.5}$$

for every interval $I \subset \mathbb{R} \setminus [-L_0, L_0]$ of length $\geq l$.

This result is of importance to the prime number theory being a substitute for Ingham's method [1], [2]. Now we impose somewhat stronger conditions on F and we estimate the measure of the set of x satisfying (1.5).

THEOREM 2. *Let $F \in \mathcal{A}$ and suppose that*

$$\|P\|^2 = \sup_{|t|>L_0+1} \int_0^1 |P(x+t)|^2\, dx < \infty. \tag{1.6}$$

Then for every real number u satisfying $\alpha(F) < u < \beta(F)$ there exist positive constants $l = l(u, F)$ and $d_1 = d_1(u, F)$ such that

$$|\{x \in I \,:\, P(x) > u\}| \geq d_1 \tag{1.7}$$

and

$$|\{x \in I \,:\, P(x) < u\}| \geq d_1 \tag{1.8}$$

for every interval $I \subset \mathbb{R} \setminus [-L_0, L_0]$ of length $\geq l$ (where $|A|$ denotes the Lebesgue measure of a set $A \subset \mathbb{R}$).

We apply this theorem to the function

$$\begin{aligned} F_{a,b}(z) = -2e^{-z/2}\frac{1}{\phi(q)} &\sum_{\chi \pmod q} (\overline{\chi(a)} - \overline{\chi(b)})\, K(z, \chi') \\ &-\frac{2}{\phi(q)} \sum_{\chi \pmod q} (\overline{\chi(a)} - \overline{\chi(b)})\, m(\tfrac{1}{2}, \chi), \end{aligned} \tag{1.9}$$

where $q \geq 2$, $0 < a, b < q$, $(a, q) = (b, q) = 1$, $a \not\equiv b \pmod q$ are integers, K denotes the K-function as introduced in [3]:

$$K(z, \chi') = \sum_{\gamma>0} e^{\rho z}, \quad z = x + iy, \quad y > 0$$

(the summation being taken over all non-trivial $L(s,\chi')$ zeros ρ with positive imaginary parts γ); χ' is the primitive Dirichlet character induced by χ, and $m(\frac{1}{2},\chi)$ is the multiplicity of a zero of $L(s,\chi)$ at $s=\frac{1}{2}$ (we put $m(\frac{1}{2},\chi)=0$ when $L(s,\chi)\neq 0$). We obtain the following corollaries.

COROLLARY 1. *Suppose the G.R.H. is true for Dirichlet L-functions* (mod q). *Then for every real number u satisfying $\alpha(F_{a,b}) < u < \beta(F_{a,b})$ there exist positive constants $c_0 = c_0(u,q)$ and $d_0 = d_0(u,q)$ such that*

$$\left|\left\{T \le t \le c_0 T \ : \ \psi(t,q,a) - \psi(t,q,b) > u\sqrt{t}\right\}\right| \ge d_0 T \tag{1.10}$$

and

$$\left|\left\{T \le t \le c_0 T \ : \ \psi(t,q,a) - \psi(t,q,b) < u\sqrt{t}\right\}\right| \ge d_0 T \tag{1.11}$$

for sufficiently large T.

COROLLARY 2. *Suppose the G.R.H. is true for Dirichlet L-functions* (mod q) *and let $(a,q)=1$, $a \not\equiv 1 \pmod q$. Then for every positive u there exist $c_1 = c_1(u,q) > 0$ and $d_1 = d_1(u,q) > 0$ such that*

$$\#\left\{Y \le m \le c_1 Y \ : \ \psi(m,q,a) - \psi(m,q,1) > u\sqrt{m}\right\} \ge d_1 Y, \tag{1.12}$$

$$\#\left\{Y \le m \le c_1 Y \ : \ \psi(m,q,a) - \psi(m,q,1) < -u\sqrt{m}\right\} \ge d_1 Y, \tag{1.13}$$

$$\#\left\{Y \le m \le c_1 Y \ : \ \pi(m,q,a) - \pi(m,q,1) > u\sqrt{m}/(\log m)\right\} \ge d_1 Y, \tag{1.14}$$

and

$$\#\left\{Y \le m \le c_1 Y \ : \ \pi(m,q,a) - \pi(m,q,1) < -u\sqrt{m}/(\log m)\right\} \ge d_1 Y, \tag{1.15}$$

for all sufficiently large Y.

Let us remark that our Theorem 1 follows at once from Corollary 2; it is sufficient therefore to prove this corollary only.

Applying Theorem 2 to the function

$$F_a(z) = -2e^{-z/2}\frac{1}{\phi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\,K(z,\chi') - \frac{2}{\phi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\,m(\tfrac{1}{2},\chi),$$

$$(z = x+iy, \quad y>0, \quad (a,q)=1)$$

in place of $F_{a,b}$, we can prove results analogous to Corollaries 1 and 2 for the remainders $\psi(t,q,a) - t/\phi(q)$, $\psi(m,q,1) - m/\phi(q)$, and $\pi(m,q,1) - \operatorname{li} x/\phi(q)$.

2. Proof of Theorem 2

For a real $\delta > 0$ we consider the subsidiary function

$$F_\delta(z) = \sum_{n=1}^{\infty} a_n S^N(\delta w_n) e^{iw_n z}, \quad z = x + iy, \quad y > 0,$$

where

$$S(\nu) = \begin{cases} (\sin \nu)/\nu, & \nu \neq 0, \\ 1, & \nu = 0 \end{cases}$$

and $N = B + 2$. Since $S(\nu) \leq \min(1, 1/|\nu|)$, the sum F_δ is absolutely convergent for $y \geq 0$. Moreover, $F_\delta \to F$ as $\delta \to 0$ almost uniformly on the upper half-plane and thus $\alpha(F_\delta) \to \alpha(F)$ and $\beta(F_\delta) \to \beta(F)$ as $\delta \to 0$. Let us fix a δ_0, $0 < \delta_0 < \frac{1}{2}$, so small that $\alpha(F_{\delta_0}) < u < \beta(F_{\delta_0})$.

From (1.4) it follows that the sum in (1.3) absolutely and uniformly converges in every closed half-plane $y \geq y_0$ with $y_0 > 0$. Hence we can integrate $F(z)$ term by term. Thus for $y > 0$

$$F_{\delta_0}(z) = \frac{1}{(2\delta_0)^N} \int_{-\delta_0}^{\delta_0} \cdots \int_{-\delta_0}^{\delta_0} F(z + t_1 + \ldots + t_N)\, dt_1 \ldots dt_N.$$

We take real parts and make $y \to 0+$. Using the Lebesgue bounded integration theorem we obtain

$$\operatorname{Re} F_{\delta_0}(x) = \frac{1}{(2\delta_0)^N} \int_{-\delta_0}^{\delta_0} \cdots \int_{-\delta_0}^{\delta_0} P(x + t_1 + \ldots + t_N)\, dt_1 \ldots dt_N \tag{2.1}$$

for $|x| > L_0 + N\delta_0$.

Let us consider now the following two cases.

Case 1. $\alpha(F)\beta(F) < 0$. Then of course $\alpha(F) < 0$ and $\beta(F) > 0$. Obviously it suffices to prove (1.7) for positive u only. Moreover, (1.8) follows from (1.7) by considering $-F$ instead of F. Let hence u be positive and let us fix u_1 satisfying

$$u < u_1 < \alpha(F_{\delta_0}). \tag{2.2}$$

$\operatorname{Re} F_{\delta_0}(x)$ is almost periodic in the sense of Bohr. Hence there exists a positive constant $l_1 = l_1(u_1, F, \delta_0)$ such that every interval of length $\geq l_1$ contains a real number x such that

$$\operatorname{Re} F_{\delta_0}(x) \geq u_1. \tag{2.3}$$

Let now $I \subset \mathbb{R} \setminus [-L_0, L_0]$ be an interval of length $\geq l_1 + N\delta_0$. Let x_0 be its middle point and let x satisfying (2.3) be such that $|x - x_0| \leq l_1/2$. Let

$$\mathbf{A} = \{t \in I \,:\, P(t) > u\}$$

$$\mathbf{B} = \{(t_1, \ldots, t_N) \,:\, |t_j| < \delta_0 \ (j = 1, 2, \ldots, N),\ x + t_1 + \ldots + t_N \in \mathbf{A}\}$$

$$\mathbf{C} = [-\delta_0, \delta_0]^N \setminus \mathbf{B}.$$

Using (2.1) and the Cauchy-Schwarz inequality we get

$$\begin{aligned}
u_1 &\leq \operatorname{Re} F_{\delta_0}(x) \\
&= \frac{1}{(2\delta_0)^N} \left(\int\limits_{\mathbf{B}} \cdots \int + \int\limits_{\mathbf{C}} \cdots \int \right) P(x + t_1 + \ldots + t_N)\, dt_1 \ldots dt_N \\
&\leq u + \frac{1}{(2\delta_0)^N} \int\limits_{-\delta_0}^{\delta_0} \cdots \int\limits_{-\delta_0}^{\delta_0} \int\limits_{\substack{\mathbf{A} - (x + t_1 + \ldots + t_{N-1}) \\ |t_N| < \delta_0}} P(x + t_1 + \ldots + t_N)\, dt_N \ldots dt_1 \\
&\leq u + \frac{1}{(2\delta_0)^N} \int\limits_{-\delta_0}^{\delta_0} \cdots \int\limits_{-\delta_0}^{\delta_0} \int\limits_{\substack{\mathbf{A} - (x + t_1 + \ldots + t_{N-1}) \\ |t_N| < \delta_0}} |\mathbf{A}|^{\frac{1}{2}} \, \|P\|\, dt_1 \ldots dt_N \\
&= u + |\mathbf{A}|^{\frac{1}{2}} \, \|P\| / (2\delta_0).
\end{aligned}$$

Hence

$$|\mathbf{A}| \geq \left(2\delta_0 (u_1 - u) \|P\|^{-1} \right)^2.$$

Hence it is enough to take

$$d(u, F) = \left(2\delta_0 (u_1 - u) \|P\|^{-1} \right)^2$$

and

$$l(u, F) = l_1(u_1, F, \delta_0) + N\delta_0. \tag{2.4}$$

Case 2. $\alpha(F)\beta(F) \geq 0$. Replacing if necessary F by $-F$ we can assume that $\alpha(F) \geq 0$. Then (1.7) can be proved exactly in the same way as in Case 1. To prove (1.8) let us fix u_1 satisfying $\max(\alpha(F), \alpha(F_{\delta_0})) < u_1 < u$. Let l_1, I and x have the same meaning as previously with (2.3) replaced by

(2.3)′ $$\operatorname{Re} F_{\delta_0}(x) \leq u_1.$$

Let moreover

$$\mathbf{A}_1 = \{t \in I \,:\, P(t) < u\}$$

$$\mathbf{B}_1 = \{(t_1, \ldots, t_N) \,:\, |t_j| < \delta_0 \ (j = 1, 2, \ldots, N),\ x + t_1 + \ldots + t_N \in \mathbf{A}_1\}$$

$$\mathbf{C}_1 = [-\delta_0, \delta_0]^N \setminus \mathbf{B}_1.$$

Then

$$\begin{aligned} u_1 \geq \operatorname{Re} F_{\delta_0}(x) &\geq \frac{1}{(2\delta_0)^N} \int\limits_{\mathbf{C}_1} \cdots \int P(x + t_1 + \ldots + t_N)\, dt_1 \ldots dt_N \\ &\geq u(2\delta_0)^{-N} \mu(\mathbf{C}_1) \\ &= u(2\delta_0)^{-N} \left((2\delta_0)^N - \mu(\mathbf{B}_1)\right), \end{aligned}$$

μ being the N-dimensional Lebesgue measure. Hence

$$\mu(\mathbf{B}_1) \geq (2\delta_0)^N (1 - u_1/u).$$

But

$$\begin{aligned} \mu(\mathbf{B}_1) &= \int\limits_{-\delta_0}^{\delta_0} \cdots \int\limits_{-\delta_0}^{\delta_0} \int\limits_{\substack{\mathbf{A}_1 - (x + t_1 + \ldots + t_{N-1}) \\ |t_N| < \delta_0}} dt_N \ldots dt_1 \\ &\leq |\mathbf{A}_1|\, (2\delta_0)^{N-1} \end{aligned}$$

and consequently

$$|\mathbf{A}_1| \geq 2\delta_0 (1 - u_1/u).$$

We obtain (1.8) with the same $l(u, F)$ as in (2.4) and

$$d_1(u, F) = 2\delta_0 (1 - u_1/u).$$

The proof is complete.

3. Proof of the corollaries

We apply Theorem 2 to the function $F_{a,b}$ defined by (1.9). It belongs to the class $\mathcal{A}$; condition 4. is satisfied with $L_0 = 0$ (cf. [3]). Condition (1.6) can be proved as follows. For positive y we have by term-by-term integration

$$\begin{aligned}\int_0^1 |\mathrm{Re}\, F_{a,b}(x+t+iy)|^2\, dx &\ll 1 + \sum_{\gamma>0}\sum_{\gamma'>0} \frac{1}{\gamma}\frac{1}{\gamma'} e^{-(\gamma+\gamma')y} \left| \int_0^1 e^{i(\gamma-\gamma')x}\, dx \right| \\ &\ll 1 + \sum_{\gamma>0}\sum_{\gamma'>0} \frac{1}{\gamma}\frac{1}{\gamma'} \min(1, |\gamma-\gamma'|^{-1}) \ll 1\end{aligned}$$

uniformly in $t \in \mathbb{R}$ (γ and γ' denote imaginary parts of non-trivial zeros of all Dirichlet L-functions $\pmod q$); (1.6) therefore follows making $y \to 0+$ and using the Lebesgue bounded integration theorem. Finally it is proved in [4], page 242, that

$$P(x) = e^{-x/2}(\psi(e^x, q, a) - \psi(e^x, q, b)) + O(x\, e^{-x/2}).$$

Hence (1.10) and (1.11) follow from (1.7) and (1.8) by the change of variable $t = e^x$; this proves Corollary 1.

To prove Corollary 2 observe that by (3.3), (4.3) and (8.11) of [3] we have

$$\mathrm{Re}\, F_{1,a}(re^{i\phi}) = \frac{1}{\pi}(\phi - \pi/2)\log r + O(1) \quad \text{for} \quad 0 < r < 1,\ 0 < \phi < \pi,$$

and hence $\alpha = -\infty$ and $\beta = +\infty$. Using this, Corollary 1 and the obvious remark that $\psi(t, q, a) - \psi(t, q, 1) = \psi([t], q, a) - \psi([t], q, 1)$ we obtain (1.12) and (1.13). Inequalities for $\pi(x, q, a) - \pi(x, q, 1)$ follow from what we have just proved and the partial summation.

References

[1] A. E. INGHAM, A note on the distribution of primes, *Acta Arithmetica*, 1 (1936), 201–211.

[2] A. E. INGHAM, On two conjectures in the theory of numbers, *Amer. J. Math.*, 64 (1942), 313–319.

[3] J. KACZOROWSKI, The k-functions in multiplicative number theory, I; On complex explicit formulae, *Acta Arithmetica*, 56 (1990), 195–211.

[4] J. KACZOROWSKI, The k-functions in multiplicative number theory, IV; On a method of A. E. Ingham, *Acta Arithmetica*, 57 (1991), 231–244.

[5] S. KNAPOWSKI, P. TURÁN, Comparative prime number theory, I; *Acta Mathematica Hungarica*, 13 (1962), 299–314.

[6] S. KNAPOWSKI, P. TURÁN, Further developments in the comparative prime number theory, I; *Acta Arithmetica*, 9 (1964), 23–40.

[7] D. SHANKS, Quadratic residues and the distribution of primes, *Math. Tables and other aids to computation*, 13 (1959), 272–284.

Jerzy Kaczorowski
Institute of Mathematics
Adam Mickiewicz University
ul. Matejki 48/49
Poznań, Poland

Astérisque

JOHN KNOPFMACHER
ARNOLD KNOPFMACHER

Metric properties of algorithms inducing Lüroth series expansions of Laurent series

Astérisque, tome 209 (1992), p. 237-246
<http://www.numdam.org/item?id=AST_1992__209__237_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

METRIC PROPERTIES OF ALGORITHMS INDUCING LÜROTH SERIES EXPANSIONS OF LAURENT SERIES

John KNOPFMACHER & Arnold KNOPFMACHER

1. Introduction

Recently the present authors [8] introduced and studied some properties of various unique expansions of formal Laurent series over a field F, as the sums of reciprocals of polynomials, involving "digits" $a_1, a_2, \ldots$ lying in a polynomial ring $F[X]$ over F. In particular, one of these expansions (described below) turned out to be analogous to the so–called *Lüroth* expansion of a real number, discussed in Perron [15] Chapter 4.

In a partly parallel way, Artin [1] and Magnus [11,12] had earlier studied a Laurent series analogue of simple *continued fractions* of real numbers, involving "digits" $x_1, x_2, \ldots$ in a polynomial ring as above. In addition to sketching elementary properties of an n–dimensional "Jacobi–Perron" variant of this, Paysant–Leroux and Dubois [13, 14] also briefly outlined certain "metric" theorems analogous to some of Khintchine [7] for real continued fractions, in the case when F is a finite field. The main aim of this paper is to state or derive some similar metric or ergodic results for the Laurent series Lüroth–type expansion referred to above. (These results were introduced at the Geneva conference by the first–named author, and are *partly* based on his forthcoming paper [9]. For analogous results concerning Lüroth expansions of *real* numbers, see Jager and de Vroedt [5] and Salát [16].)

In order to explain the conclusions, we first fix some notation and describe the inverse–polynomial Lüroth–type representation to be considered:

Let $\mathcal{L} = F((z))$ denote the field of all *formal Laurent series* $A = \sum_{n=v}^{\infty} c_n z^n$ in an indeterminate z, with coefficients c_n all lying in a given field F. Although the main case of importance usually occurs when F is the field $\mathbb{C}$ of complex numbers, certain interest also attaches to other ground fields F and most of the results of [8] hold for arbitrary F. It will be convenient to write $X = z^{-1}$ and also consider the ring $F[X]$ of *polynomials* in X, and the field $F(X)$ of *rational functions* in X, with coefficients in F.

If $c_v \neq 0$, we call $v = v(A)$ the *order* of A above, and define the *norm* (or *valuation*) of A to be $\|A\| = q^{-v(A)}$, where initially $q > 1$ may be an arbitrary constant, but *later will be chosen* as $q = \text{card}(F)$, if F is finite. Letting $v(0) = +\infty$, $\|0\| = 0$, one then has (cf. Jones and Thron [6] Chapter 5):

$$\|A\| \geq 0 \text{ with } \|A\| = 0 \text{ iff } A = 0,$$

(1.1)

$$\|AB\| = \|A\| \cdot \|B\|, \text{ and}$$

$\|\alpha A + \beta B\| \leq \max(\|A\|, \|B\|)$ for non–zero $\alpha, \beta \in F$, with equality when $\|A\| \neq \|B\|$. By (1.1), the norm $\| \ \|$ is non–Archimedean, and it is well known that $\mathcal{L}$ forms a *complete* metric space relative to the metric ρ such that $\rho(A, B) = \|A - B\|$.

In terms of the notation $X = z^{-1}$ above, we shall make frequent use of the polynomial $[A] = \sum_{v \leq n \leq 0} c_n X^{-n} \in F[X]$, and refer to $[A]$ as the *integral part* of $A \in \mathcal{L}$. Then $v = v(A)$ is the *degree* $\deg[A]$ of $[A]$ relative to X, and the same function $[\ ]$ was used by Artin [1] and Magnus [11, 12] for their continued fractions. (For a recent application of Artin's algorithm, F finite, see Hayes [4].)

Given $A \in \mathcal{L}$ now note that $[A] = a_0 \in F[X]$ iff $v(A_1) \geq 1$ where $A_1 = A - a_0$. As in [8], if $A_n \neq 0 (n > 0)$ is already defined, we then let $a_n = \left[\frac{1}{A_n}\right]$ and put $A_{n+1} = (a_n - 1)(a_n A_n - 1)$. If some $A_m = 0$ or $a_n = 0$, this recursive process stops. It was shown in [8] that this algorithm leads to a finite or convergent (relative to ρ) *Lüroth–type* series expansion

$$A = a_0 + \frac{1}{a_1} + \sum_{r \geq 2} \frac{1}{a_1(a_1 - 1) \ldots a_{r-1}(a_{r-1} - 1)a_r}, \tag{1.2}$$

where $a_r \in F[X]$, $a_0 = [A]$, and $\deg(a_r) \geq 1$ for $r \geq 1$. Furthermore this expansion is *unique* for A subject to the preceding conditions on the "digits" a_r.

If I denotes the ideal in the power series ring $F[[z]]$, consisting of all power series x such that $x(0) = 0$, then another way of looking at this expansion algorithm is in terms of operators $a : I-\{0\} \to F[X]$, $T : I \to I$ such that $a(x) = \left[\frac{1}{x}\right]$, $T(0) = 0$ and otherwise $T(x) = \big(a(x) - 1\big)\big(xa(x) - 1\big)$. Then, for $x = A_1 \in I$, $a_1 = a_1(x) = a(x)$, and more generally $a_n = a_n(x) = a_1(T^{n-1}x)$ if $0 \neq T^{n-1}x \in I$.

From now on it will be *assumed* that $F = \mathbb{F}_q$ is a *finite* field with exactly q elements. For that case it was shown in [**9**] that $T : I \to I$ is *ergodic* relative to the Haar measure μ on I such that $\mu(I) = 1$, and that this fact implies in particular:

Theorem 1. (i) *For any given polynomial $k \in \mathbb{F}_q[X]$, $\deg(k) \geq 1$, and all $x \in I$ outside a set of Haar measure 0, the digit value k has asymptotic frequency*

$$\lim_{n\to\infty} \frac{1}{n} \#\{r \leq n : a_r(x) = k\} = \|k\|^{-2} = q^{-2\deg(k)}.$$

(ii) *For all $x \in I$ outside a set of Haar measure 0 there exists a single asymptotic mean–value*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{n} \deg\big(a_r(x)\big) = \frac{q}{q-1}.$$

(iii) *For all $x \in I$ outside a set of Haar measure 0,*

$$\|x - w_n\| = q^{\left(-\frac{2q}{q-1}+o(1)\right)n} \quad \text{as} \quad n \to \infty,$$

where

$$w_n = w_n(x) := \sum_{r=1}^{n} \frac{\lambda_{r-1}}{a_r}, \ \lambda_0 = 1, \ \lambda_r = \frac{1}{a_1(a_1-1)\dots a_r(a_r-1)}.$$

Regarding (iii), a similar but more elementary algebraic conclusion [**8**] states that

$$\|x - w_n\| \leq q^{-2n-1} \quad \text{for all} \quad x.$$

Our main aim in the present article will be to state and prove various further metric results concerning polynomial "digits" $a_r(x)$ and their limiting distributions.

2. Sharper Metric Conclusions

A useful description of the Haar measure μ on I is given in Sprindžuk [17]. In particular $\mu(C) = q^{-r}$ for any "circle", "disc" or "ball"

$$C = C(x, q^{-r-1}) := \left\{ y \in \mathcal{L} : \|x - y\| \leq q^{-r-1} \right\}.$$

Using this, the proof of Theorem 1 (i) in [9] includes:

$$\mu\left\{ x \in I : a_r(x) = k \right\} = \|k\|^{-2} \tag{2.1}$$

for any $k \in \mathbb{F}_q[X]$, $\deg(k) \geq 1$, and $r \geq 1$, and

(2.2) the Lüroth–type digits $a_r(x)$ define identically–distributed independent random variables a_r relative to μ on I.

More precisely, by Theorem 3.16 and the law of the iterated logarithm (Theorem 3.17) in Galambos [3], we obtain:

Theorem 2. *Let* $A_{n,k}(x) = \#\{r \leq n : a_r(x) = k\}$. *Then for almost all* $x \in I$

$$\limsup_{n\to\infty} \frac{A_{n,k}(x) - n\|k\|^{-2}}{\sqrt{n \log\log n}} = \sqrt{2\|k\|^{-2}(1 - \|k\|^{-2})}.$$

Further, for any real s,

$$\lim_{n\to\infty} \mu \left\{ x \in I : A_{n,k}(x) - n\|k\|^{-2} < \frac{s}{\|k\|} \sqrt{\frac{n}{(1 - \|k\|^{-2})}} \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{s} e^{-u^2/2} du.$$

Next we note that Theorem 1 (ii) is equivalent to the existence of a *Khintchine–type* constant

$$\lim_{n\to\infty} \left\| a_1(x) a_2(x) \dots a_n(x) \right\|^{1/n} = q^{q/(q-1)} \ a.e.$$

This conclusion can be refined to:

Theorem 3. *For almost all $x \in I$,*

$$\limsup_{n\to\infty} \frac{\sum_{r=1}^{n} \deg(a_r(x)) - c_1 n}{\sqrt{n \log\log n}} = \sqrt{2c_2},$$

where $c_1 = q/(q-1)$, $c_2 = q/(q-1)^2$. Hence as $n \to \infty$

$$\left\| a_1(x)a_2(x)\dots a_n(x) \right\|^{1/n} = q^{q/(q-1)} + O\left(\sqrt{\frac{\log\log n}{n}}\right) \text{ a.e.}$$

Proof. Define a sequence (t_n) of independent random variables t_n on I by

$$t_n(x) = \begin{cases} \deg(a_n(x)) & \text{if } \|a_n(x)\| \le n^2, \\ 0 & \text{otherwise.} \end{cases}$$

Then the expected value

$$E(t_n) = \sum_{q^r \le n^2} q^{-2r} r(q-1)q^r = E\Big(\deg(a_n(\cdot))\Big) + O\left(\frac{\log n}{n^2}\right),$$

and

$$E(t_n^2) = \sum_{q^r \le n^2} q^{-2r} r^2(q-1)q^r = E\Big(\deg^2(a_n(\cdot))\Big) + O\left(\frac{\log^2 n}{n^2}\right).$$

Hence the variance

$$\operatorname{var}(t_n) = \operatorname{var}\Big(\deg(a_n(\cdot))\Big) + O\left(\frac{\log^2 n}{n^2}\right),$$

and

$$B_n := \sum_{r=1}^{n} \operatorname{var}(t_r) = \frac{qn}{(q-1)^2} + O(1).$$

Next, since

$$t_n(x) \le 2\log_q n = o\left(\sqrt{\frac{B_n}{\log\log B_n}}\right),$$

the law of the iterated logarithm implies:

$$\limsup_{n\to\infty} \frac{\sum_{r=1}^{n} t_r - \sum_{r=1}^{n} E(t_r)}{\sqrt{2B_n \log\log B_n}} = 1 \ a.e.$$

Hence

$$\limsup_{n\to\infty} \frac{\sum_{r=1}^{n} t_r - \sum_{r=1}^{n} E\Big(\deg\big(a_r(\cdot)\big)\Big)}{\sqrt{2\frac{q}{(q-1)^2} n \log\log n}} = 1 \ a.e.$$

Now let $U_n = \Big\{x \in I : t_n(x) \neq \deg\big(a_n(x)\big)\Big\}$. Then

$$\mu(U_n) = \sum_{\|k\|>n^2} \|k\|^{-2} < \frac{1}{n^2},$$

and the Borel–Cantelli lemma yields $\mu\big(\limsup_{n\to\infty} U_n\big) = 0$. Thus, for almost all $x \in I$, there exists $n_0(x)$ with

$$t_n(x) = \deg\big(a_n(x)\big) \ \text{ for } \ n \geq n_0(x),$$

and hence Theorem 3 follows.

The next theorem sharpens part (iii) of Theorem 1 above:

Theorem 4. *If $w_n = w_n(x)$ is defined as in Theorem* 1 (iii), *then*

$$\limsup_{n\to\infty} \frac{\deg(x - w_n) + \frac{2qn}{q-1}}{\sqrt{n \log\log n}} = \frac{\sqrt{8q}}{q-1} \ a.e.$$

Hence

$$\frac{1}{n}\deg(x - w_n) = -\frac{2q}{q-1} + O\left(\sqrt{\frac{\log\log n}{n}}\right) \ a.e.$$

Proof. From Theorem 3, by symmetry as in Feller [**2**] page 205, we have

$$\liminf_{n\to\infty} \frac{\sum_{r=1}^{n} \deg\big(a_r^2(x)\big) - \frac{2qn}{q-1}}{\sqrt{n \log\log n}} = -2\sqrt{2c_2} \ a.e.$$

Also [**9**] shows that

$$1 - \sum_{r=1}^{n+1} \deg\left(a_r^2(x)\right) \leq \deg(x - w_n) \leq -1 - \sum_{r=1}^{n} \deg\left(a_r^2(x)\right),$$

which then leads to Theorem 4.

The next theorem sharpens the conclusion [9] that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{n} \left\|a_r(x)\right\| = \infty \text{ a.e.}$$

Theorem 5. *For any fixed* $\varepsilon > 0$,

$$\lim_{n\to\infty} \mu\left\{x \in I : \frac{1}{n \log_q n} \left|\sum_{r=1}^{n} \left\|a_r(x)\right\| - (q-1)\right| > \varepsilon\right\} = 0,$$

i.e. $\dfrac{1}{n \log_q n} \sum_{r=1}^{n} \left\|a_r(x)\right\| \to q - 1$ *in probability over* I.

Proof. We write $s = \log_q y$ iff $y = q^s$, and use the truncation method of Feller [2], Chapter 10, §2, applied to the random variables U_r, V_r $(r \leq n)$ defined by

$$\begin{aligned} U_r(x) &= \left\|a_r(x)\right\|, V_r(x) = 0 && \text{if } \left\|a_r(x)\right\| \leq n \log_q n, \\ U_r(x) &= 0, \qquad V_r(x) = \left\|a_r(x)\right\| && \text{if } \left\|a_r(x)\right\| > n \log_q n. \end{aligned}$$

Then

$$\begin{aligned} &\mu\left\{x \in I : \frac{1}{n \log_q n} \left|\sum_{r=1}^{n} \left\|a_r(x)\right\| - (q-1)\right| > \varepsilon\right\} \\ &\quad \leq \mu\left\{x : \left|U_1 + \cdots + U_n - (q-1) n \log_q n\right| > \varepsilon n \log_q n\right\} + \\ &\qquad + \mu\left\{x : V_1 + \cdots + V_n \neq 0\right\}, \end{aligned}$$

and

$$\begin{aligned} \mu\left\{x : V_1 + \cdots + V_n \neq 0\right\} &\leq n\mu\left\{x : \left\|a_1(x)\right\| > n \log_q n\right\} \\ &= n \sum_{\|k\| > n \log_q n} \|k\|^{-2} < \frac{1}{\log_q n} = o(1). \end{aligned}$$

Now note that

$$E(U_1 + \cdots + U_n) = nE(U_1),\ \operatorname{var}(U_1 + \cdots + U_n) = n \operatorname{var}(U_1),$$

where

$$\begin{aligned} E(U_1) &= \sum_{\|k\| \le n \log_q n} \|k\|^{-1} = \sum_{q^r \le n \log_q n} q^{-r}(q-1)q^r \\ &= (q-1)\log_q([n \log_q n]), \end{aligned}$$

and

$$\begin{aligned} \operatorname{var}(U_1) < E(U_1^2) &= \sum_{\|k\| \le n \log_q n} 1 = \sum_{q^r \le n \log_q n} (q-1)q^r \\ &< qn \log_q n. \end{aligned}$$

Chebyshev's inequality then yields

$$\begin{aligned} &\mu\left\{x : \left|U_1 + \cdots + U_n - nE(U_1)\right| > \varepsilon n E(U_1)\right\} \\ &\quad \le \frac{n \operatorname{var}(U_1)}{(\varepsilon n E(U_1))^2} < \frac{qn^2 \log_q n}{\left(\varepsilon(q-1)n \log_q([n \log_q n])\right)^2} = o(1). \end{aligned}$$

Since $E(U_1) \sim (q-1)\log_q n$ as $n \to \infty$, Theorem 5 follows.

Remark. Since a theorem in Galambos [**3**, p. 46], implies that **either**

$$\limsup_{n\to\infty} \frac{1}{n \log_q n} \sum_{r=1}^{n} \|a_r(x)\| = \infty \text{ a.e. or } \liminf_{n\to\infty} \frac{1}{n \log_q n} \sum \|a_r(x)\| = 0 \text{ a.e.},$$

the conclusion of Theorem 5 does not carry over to validity with probability one.

3. Estimates for Individual Digits

Without attempting to be exhaustive, we conclude this article with two asymptotic results emphasizing the sizes of individual digits $a_n(x)$ *a.e.* as $n \to \infty$.

Theorem 6. *Let $\psi(n)$ be a positive increasing function of n. Then*

$$\|a_n(x)\| = O(\psi(n)) \text{ a.e.} \iff \sum_{n=1}^{\infty} \frac{1}{\psi(n)} < \infty.$$

In fact $\|a_n(x)\| = O(\psi(n))$ is false a.e. if the series diverges.

Proof. Let $V_n = \{x \in I : \|a_n(x)\| > \psi(n)\}$. Since $\mu\{x : a_n(x) = k\} = \|k\|^{-2}$, it follows that

$$\mu(V_n) = \sum_{\|k\| > \psi(n)} \|k\|^{-2} = \sum_{q^r > \psi(n)} q^{-2r}(q-1)q^r \leq \frac{1}{\psi(n)}.$$

If $\sum_{n=1}^{\infty} \psi(n)^{-1} < \infty$, then the Borel–Cantelli lemma (cf. [**3**], page 36) now yields $\mu(\limsup V_n) = 0$. Hence $\|a_n(x)\| > \psi(n)$ for at most finitely many n, for almost all $x \in I$. Thus $\|a_n(x)\| = O(\psi(n))$ *a.e.*

If $\sum_{n=1}^{\infty} \psi(n)^{-1}$ diverges, the Abel–Dini theorem (Knopp [**10**], page 290) implies that there exists a positive increasing function $\theta(n)$ with $\theta(n) \to \infty$ as $n \to \infty$, such that $\sum_{n=1}^{\infty} \psi(n)^{-1}\theta(n)^{-1}$ also diverges. Then let $W_n = \{x \in I : \|a_n(x)\| > \psi(n)\theta(n)\}$. The independence of the random variables a_n implies the independence of the sets W_n. Also

$$\sum_{n=1}^{\infty} \mu(W_n) = \sum_{n=1}^{\infty} \sum_{\|k\| > \psi(n)\theta(n)} \|k\|^{-2} > \frac{1}{q} \sum_{n=1}^{\infty} \frac{1}{\psi(n)\theta(n)} = \infty.$$

Thus the Borel–Cantelli lemma yields $\mu(\limsup W_n) = 1$, and so $\|a_n(x)\| > \psi(n)\theta(n)$ holds with probability one, for infinitely many n. Thus $\|a_n(x)\| = O(\psi(n))$ is false *a.e.*

Theorem 6 implies for example that $\|a_n(x)\| = O(n(\log n)^{\alpha})$ *a.e.* for any $\alpha > 1$, while $\|a_n(x)\| = O(n(\log n)^{\beta})$ is false *a.e.* for any $\beta \leq 1$. This leads to the

Corollary. *For almost all $x \in I$*

$$\limsup_{n \to \infty} \frac{\log\|a_n(x)\| - \log n}{\log\log n} = 1.$$

Remark. The corresponding lower limit is not finite *a.e.*, since (2.1) earlier shows that $\|a_n(x)\|$ can take any particular constant value q^N $(N \geq 1)$ for all n, and all x in a set of positive measure.

References

[1] E. ARTIN, Quadratische Körper im Gebiete der höheren Kongruenzen, I–II. *Math. Z.* **19**(1924), 153—246.

[2] W. FELLER, *An Introduction to Probability Theory and its Applications,* Vol. 1 (3rd Ed.). J. Wiley, 1968.

[3] J. GALAMBOS, *Representations of Real Numbers by Infinite Series.* Springer–Verlag, 1976.

[4] D.R. HAYES, Real quadratic function fields. *Canadian Math. Soc. Conf. Proceedings,* **7**(1987), 203—236.

[5] H. JAGER and C. de VROEDT, Lüroth series and their ergodic properties. *Proc. K. Nederl. Akad. Wet.,* **A 72**(1969), 31—42.

[6] W.B. JONES and W.J. THRON, *Continued Fractions.* Addison–Wesley, 1980.

[7] A.Y. KHINTCHINE, Metrische Kettenbruchprobleme, *Compositio Math.,* **1** (1935), 361—382.

[8] A. KNOPFMACHER and J. KNOPFMACHER, Inverse polynomial expansions of Laurent series, I–II. *Constr. Approx.,* **4**(1988), 379—389, and *J. Comp. Appl. Math.,* **28**(1989), 249—257.

[9] J. KNOPFMACHER, Ergodic properties of some inverse polynomial series expansions of Laurent series; accepted by *Acta Math. Hungarica.*

[10] K. KNOPP, *Theory & Application of Infinite Series,* Dover, 1990.

[11] A. MAGNUS, Certain continued fractions associated with the Padé table. *Math. Z.,* **78**(1962), 361—374.

[12] A. MAGNUS, p-fractions and the Padé table. *Rocky Mtn. J. Math.,* **4**(1974), 257—259.

[13] R. PAYSANT–LEROUX and E. DUBOIS, Algorithme de Jacobi–Perron dans un corps de séries formelles. *C.R. Acad. Sci. Paris,* **A 272**(1971), 564—566.

[14] R. PAYSANT–LEROUX and E. DUBOIS, Étude métrique de l'algorithme de Jacobi–Perron dan un corps de séries formelles. *C.R. Acad. Sci. Paris,* **A 275**(1972), 683—686.

[15] O. PERRON, *Irrationalzahlen.* Chelsea Publ. Co., 1951.

[16] T. SALÁT, Zur Metrischen Theorie der Lüroschen Entwicklungen der reellen Zahlen, *Czech. Math. J.,* **18**(1968), 489—522.

[17] V.G. SPRINDŽUK, *Mahler's Problem in Metric Number Theory.* American Math. Soc., 1969.

J. Knopfmacher
Department of Mathematics
University of the Witwatersrand
Johannesburg, 2050
South Africa.

A. Knopfmacher
Dept. of Computational &
Applied Mathematics
University of the Witwatersrand
Johannesburg, 2050
South Africa.

Astérisque

JOAN-C. LARIO

Serre's conjecture on Galois representations attached to Weil curves with additive reduction

Astérisque, tome 209 (1992), p. 247-255

<http://www.numdam.org/item?id=AST_1992__209__247_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Serre's conjecture on Galois representations attached to Weil curves with additive reduction

Joan-C. LARIO

1. Introduction: terminology and facts.– Let E be an elliptic curve defined over $\mathbb{Q}$ which is supposed to be modular, i.e. E is a Weil curve, and denote by $F(z) = \sum A_n e^{2\pi i n z}$ the weight 2 newform attached to E by the Eichler-Shimura congruences.

Fix a prime $p > 7$. We shall be interested in which cases E has additive reduction at p, excluding the Kodaira reduction types I_ν^* ($\nu \geq 0$) which are related to the potentially semi-stable case. Thus p divides exactly twice the geometric conductor N_E of the elliptic curve E.

After [Ed 89] we say that E is p-vertical if E has bad but potentially good ordinary reduction at p, and that E is p-horizontal if E has bad but potentially good supersingular reduction at p. Recall that these conditions can be given in terms of the Hasse invariant (cf. [Hu 87], pag.248) of E and, moreover, one gets:

$$E \text{ is } p\text{-vertical} \iff p \equiv 1 \pmod{e},$$

where e is the least common multiple of the multiplicities of the irreducible components of the special fibre of the stable model; that is

$$e = \begin{cases} 6 & \text{if } p\text{-type}(E) = II, II^*; \\ 4 & \text{if } p\text{-type}(E) = III, III^*; \\ 3 & \text{if } p\text{-type}(E) = IV, IV^*. \end{cases}$$

The Galois module E_p of the p-torsion points of E gives rise to a continuous and odd representation

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \backsimeq \mathrm{GL}_2(\mathbb{F}_p),$$

which is almost always absolutely irreducible (cf. [Ma 78]).

Serre's conjecture $(3.2.4_?)$ in [Se 87] predicts, in this case, the existence of a Hecke cusp form $(\mathrm{mod}\, p)$

$$f(q) = \sum a_n q^n$$

of type $(N_\rho, k_\rho, \varepsilon_\rho)$ satisfying

$$a_n \equiv A_n \pmod{p}, \quad \text{for all } n \text{ prime to } N_E .$$

The level N_ρ, the weight k_ρ and the character ε_ρ are given by a precise recipe in [Se 87] and, depending on the Néron model of E, they have been computed, for instance in [Ba-La 91].

In [Ba-La 91], we verify $(3.2.4_?)$ for the Galois representations defined by the p-torsion points of the p-vertical Weil curves. In this paper our purpose is to emphasize the difference between the p-vertical and the p-horizontal cases in order to check Serre's conjecture. Several numerical examples, collected by computer calculations, lead us to give a conjecture which implies $(3.2.4_?)$ for the horizontal case.

2. Lowering the level (ordinary case).– First, we shall consider a general situation. Let

$$F(z) = \sum_{n=1}^{\infty} A_n e^{2\pi i n z}$$

be a newform of type (N, k, ε), defined over $\overline{\mathbb{Q}}$. If $\alpha : (\mathbb{Z}/M\mathbb{Z})^* \to \mathbb{C}^*$ is a Dirichlet character modulo M, then the twisted form

$$F \otimes \alpha\,(z) = \sum_{n=1}^{\infty} A_n\, \alpha(n) e^{2\pi i n z} \qquad (\alpha(n) = 0 \text{ if g.c.d. } (n, M) \neq 1)$$

is a Hecke cusp form of type $(N', k, \varepsilon\, \alpha^2)$, where

$$N' = \text{l.c.m.}\,(N, M \cdot \text{conductor}\,(\varepsilon), M^2) .$$

If M is prime to the level N, then $F \otimes \alpha$ is a newform of type $(NM^2, k, \varepsilon\, \alpha^2)$; otherwise, the form $F \otimes \alpha$ can either be or not be a newform! The question is to decide when it is.

After Li's work [Li 75], one has a nice criterion to decide whether a Hecke cusp form is new or not. More precisely, consider the operators K and H_N defined by

$$G|H_N = G|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \quad \text{and} \quad G|K(z) = \overline{G(-\bar{z})},$$

for each cusp form $G(z) = \sum_{n=1}^{\infty} B_n e^{2\pi i n z}$ of type (N, k, ε). We have

PROPOSITION. (cf. [Li 75]). *Let $G \in S_k(N, \varepsilon)$ be a Hecke cusp form. Then G is a newform of type (N, k, ε) if and only if the functional equation $G|K|H_N = \gamma G$ holds for a certain complex constant γ of absolute value 1.*

Let us go back to the case of elliptic curves. Let F be the newform attached to the Weil curve E as above and let $N_E = Np^2$ be the conductor of E. Choose an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ and let $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{Q}}$ be the Dirichlet character which satisfies

$$\psi(n)\, n \equiv 1 \pmod{\mathfrak{P}},$$

where $\mathfrak{P}$ is the place of $\overline{\mathbb{Q}}$ dividing p fixed by our embedding.

We ask for which values of $j \in \{0, \ldots, p-2\}$ the twisted form $F \otimes \psi^j$ fails to be new. Prof. D. B. Zagier suggested to us to apply the following test which is an immediate consequence of Li's result.

COROLLARY. *Keep the above notations. If there exist a complex number $z \in \mathbb{H}$ such that*

$$\left| \frac{\sum_{n=1}^{\infty} \overline{A}_n \overline{\psi}^j(n)\, e^{-2\pi i n / N_E z}}{N_E\, z^2 \sum_{n=1}^{\infty} A_n \psi^j(n)\, e^{2\pi i n z}} \right| - 1 \neq 0,$$

then $F \otimes \psi^j$ is not new.

On a VAX 8600 at the Facultat d'Informàtica de Barcelona we have obtained the following numerical examples, by taking $z = 2i/\sqrt{N_E} \in \mathbb{H}$ and a few number (around 500) of Fourier coefficients for $F \otimes \psi^j$.

For the elliptic curve 338 **A1** (cf. [Cre 91]),

$$E : y^2 + xy = x^3 - x^2 + x + 1$$

of conductor $N_E = 2 \cdot 13^2$, we get the following data:

j	TEST
0	0.0000000000
1	0.0000000000
2	2.6699959395
3	0.0000000000
4	0.0000000000
5	0.0000000000
6	0.0000000000
7	0.0000000000
8	0.0000000000
9	0.0000000000
10	2.6699959395
11	0.0000000000

Observe that the Hecke cusp forms $F \otimes \psi^2$ and $F \otimes \psi^{10}$ don't seem to be newforms. Indeed, as we shall see later, they are not newforms.

Another example is provided by the elliptic curve

$$E : y^2 + xy + y = x^3 - 39x - 27$$

of conductor $N_E = 43^2$ (cf. [Ed-Gr-To 90]). In this case we get:

j	TEST
14	5.5513673695
28	5.5513673695 ,

and zero for all the others values of j. Now, the Hecke cusp forms $F \otimes \psi^{14}$ and $F \otimes \psi^{28}$ are not newforms.

In the previous examples E is vertical at $p = 13, 43$, respectively; indeed, in both cases we have $p \equiv 1 \pmod 3$ and, following Tate's algorithm [Ta 75], we find that p-type (E) is equal to II and IV, respectively.

Actually, we are able to say what happens in the general p-vertical case. If ℓ denotes a prime which does not divide the conductor of E, then one can prove that the restriction to an inertia group I_p at p of the ℓ-adic representation ρ_ℓ attached to $F \otimes \psi^{\frac{p-1}{e}}$ is given by

$$\rho_\ell(I_p) = \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} .$$

Therefore, we obtain

PROPOSITION . (cf. [Ba-La 91]) . *If E is a p-vertical Weil curve as above, there exists a newform*

$$G(z) = \sum B_n e^{2\pi i n z} \in S_2(Np, \psi^{2\frac{p-1}{e}}) ,$$

having the same eigenvalue system as the twisted form $F \otimes \psi^{\frac{p-1}{e}}$.

Similar arguments do not work when E is p-horizontal. Consider the following example: the elliptic curve 605 **A1**, in [Cre 91],

$$E : y^2 + xy = x^3 - x^2 - 1414x - 44027$$

of conductor $N_E = 5 \cdot 11^2$ has 11-type IV^*. Since $11 \equiv 2 \pmod 3$, E is 11-horizontal. Running our program we get:

j	TEST
0	0.00000000000
1	0.00000000000
2	0.00000000000
3	0.00000000000
4	0.00000000000
5	0.00000000000
6	0.00000000000
7	0.00000000000
8	0.00000000000
9	0.00000000000

Actually, all the twisted forms $F \otimes \psi^j$ are newforms.

3. Lowering the level (supersingular case).– Keep the notations as above and let $v^{ss} = \frac{p+1}{e}$. Since we are interested in Serre's conjecture (3.2.4?), we shall assume without loss of generality that p-type $(E) = II, III, IV$. Indeed, the exclusion of the cases with asterisk remain justified by considering the minimal or companion representations as in [La 91].

CONJECTURE (ss.?). *If E is a p-horizontal Weil curve as above, there exists a newform*

$$G(z) = \sum B_n e^{2\pi i n z} \in S_2(Np, \psi^{2\frac{p+1}{e}}),$$

having the same eigenvalue system $(\mathrm{mod}\ \mathfrak{P})$ *as the twisted form $F \otimes \psi^{\frac{p+1}{e}}$; i.e., such that for all n prime to N_E we have*

$$B_n \equiv A_n \psi^{v^{ss}}(n) \pmod{\mathfrak{P}}.$$

Moreover, G is $\mathfrak{P}$-ordinary if and only if $\rho|_{D_p}$ is not irreducible. Here D_p denotes a decomposition group for p.

First of all, we are going to show a numerical example of the lowering of the level predicted by the conjecture.

Consider the elliptic curve E given by the Weierstraß model

$$y^2 + xy = x^3 + 3x + 1;$$

it is the curve 242 **A1** in [Cre 91] and has conductor $N_E = 2 \cdot 11^2$. The special fibre of the Néron model over the local ring $\mathbb{Z}_{11}$ has reduction type II; therefore, E is 11-horizontal. Moreover, E has no $\mathbb{Q}$-rational isogenies of degree 11, and then

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_{11}) \backsimeq \mathrm{GL}_2(\mathbb{F}_{11})$$

is irreducible; since $v_{11}(c_4) = 1$, we find that $\rho|D_{11}$ is reducible.

Choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{11}$ such that the character

$$\psi : (\mathbb{Z}/11\mathbb{Z})^* \to \overline{\mathbb{Q}}^*, \quad \psi(2) = e^{2\pi i/10},$$

satisfies

$$\psi(2) \equiv 2^{-1} \pmod{\mathfrak{P}_{11}},$$

where $\mathfrak{P}_{11}$ is the place of $\overline{\mathbb{Q}}$, over 11, determined by the embedding.

Our conjecture (ss.?) predicts the existence of a cusp form

$$G(q) = \sum B_n q^n \in S_2(22, \psi^4)$$

satisfying the congruences

$$B_n \equiv A_n \psi^2(n) \pmod{\mathfrak{P}_{11}}$$

for all odd integers n prime to 11.

In this case, we find

$$\dim S_2(22, \psi^4) = 1.$$

The Eichler-Selberg trace formula (cf. [Hij-Pi-She 90]) allows us to obtain the Fourier coefficients of the unique normalized newform of this type.

An efficient implementation of this formula is due to J. Quer; its program, written in UBASIC, find the first coefficients of the newform $G(q) = \sum_{n\geq 1} B_n q^n$ in $S_2(22, \psi^4)$:

$$\begin{aligned}
B_3 &= -\zeta^4 - \zeta^2 - 2\zeta - 2 \\
B_5 &= -2\zeta^3 - 2 \\
B_7 &= -2\zeta^4 - 2\zeta^3 - 4\zeta^2 - 2\zeta \\
B_{13} &= -2\zeta^2 - 2\zeta - 2 \\
B_{17} &= -4\zeta^4 - 4\zeta^3 - 5\zeta^2 - 5\zeta - 4 \\
B_{19} &= -2\zeta^4 - 6\zeta^3 - 2\zeta^2 - 5\zeta - 5 \\
&\ldots
\end{aligned}$$

where $\zeta = e^{2\pi i/5}$. The coefficients B_n can be rewritten taking into account that $\cos \pi/5$ is the unique positive (double) root of the polynomial $16X^5 - 20X^3 + 5X + 1$ and that

$$i \cos \frac{\pi}{10} = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5} - \frac{\sqrt{5}-1}{4}.$$

On the other hand, computing the first coefficients of the L-series of the elliptic curve E, we find the following:

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43
A_ℓ	–	-2	-3	-2	–	-5	-3	-2	6	3	2	-7	-3	-8

Finally, since $\sqrt{5} \equiv 4 \pmod{11}$ and

$$\cos\frac{\pi}{5} + i\sin\frac{\pi}{5} = e^{2\pi i/10} \equiv 2^{-1} \equiv 6 \pmod{\mathfrak{P}_{11}},$$

we get

ℓ	$\psi^2(\ell)$	B_ℓ	$A_\ell\psi^2(\ell) - B_\ell \pmod{\mathfrak{P}_{11}}$
2	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	–	–
3	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$-\frac{\sqrt{5}+1}{2}(\psi^4(3)+1)$	0
5	$\cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$	$(\sqrt{5}-1)(\psi^8(5)+1)-2$	0
7	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$-(\sqrt{5}-1)\psi^6(7)+2$	0
11	–	–	–
13	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	$-(\sqrt{5}-1)\psi^2(13)$	0
17	$\cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$	$-\frac{\sqrt{5}+1}{2}\psi^8(17)+1$	0
19	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$(2\sqrt{5}-5)(\psi^4(19)+1)$	0
23	1	$-(\sqrt{5}+1)$	0
29	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$(\sqrt{5}-5)\psi^6(29)+2\sqrt{5}$	0
31	$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$	$2\psi^2(31)$	0
37	$\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$	$6\psi^6(37)-3(\sqrt{5}+1)$	0
41	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$\frac{7-5\sqrt{5}}{2}(\psi^4(41)+1)$	0
43	1	$\frac{3}{2}(3\sqrt{5}+1)$	0
47	$\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$	$(2\sqrt{5}-6)(\psi^4(47)+1)$	0

Since a modular form of given weight and level $(\mathrm{mod}\, p)$ cannot start with a very high power of q (cf. [Gr 90], pag.499), note that in this case we have truly proved the congruences $B_n \equiv A_n\psi^2(n) \pmod{\mathfrak{P}_{11}}$ for all n.

4. Galois representations attached to Weil curves.–

We deduce Serre's conjecture (3.2.4?) for the remaining case of p-horizontal Weil curves from our conjecture (ss.?).

THEOREM. *Assume conjecture (ss.?) is true. Then Serre's conjecture* (3.2.4?) *is true for all irreducible representations*

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\,(E_p)$$

provided that E is a p-horizontal Weil curve as above.

PROOF. Consider the twisted representation

$$\rho(\frac{p+1}{e}) : = \rho \otimes \chi^{-\frac{p+1}{e}},$$

where χ is the pth cyclotomic character. It is easy to see that if $\rho(\frac{p+1}{e})$ satisfies Serre's conjecture so does ρ.

The reason to consider $\rho(\frac{p+1}{e})$ instaed of ρ is that the invariant weight for $\rho(\frac{p+1}{e})$ is less than $p+1$. Namely (cf. [Ba-La 91]),

$$k_{\rho(\frac{p+1}{e})} = \begin{cases} \frac{p+1}{e}(e-2) & \text{if } \rho|_{D_p} \text{ reduces;} \\ p+1-2\frac{p+1}{e} & \text{if } \rho|_{D_p} \text{ is irreducible .} \end{cases}$$

Let $G(z) = \sum B_n e^{2\pi i n z} \in S_2(Np, \psi^{2\frac{p+1}{e}})$ be the newform attached to E as in conjecture (ss.?). We have (cf. Lemma 4, [Ba-La 91]) that

$$\mathrm{Tr}\,(G\,E_{1,\psi}^{-2\frac{p+1}{e}+(p-1)}) \in S_{k_{\rho(\frac{p+1}{e})}}(N,1)$$

with $\mathrm{Tr}\,(G\,E_{1,\psi}^{-2\frac{p+1}{e}+(p-1)}) \equiv G \pmod{\mathfrak{P}}$ if $\rho|_{D_p}$ is reducible, and

$$\mathrm{Tr}\,(G\,E_{1,\psi}^{-2\frac{p+1}{e}+2(p-1)}) \in S_{k_{\rho(\frac{p+1}{e})}}(N,1)$$

with $\mathrm{Tr}\,(G\,E_{1,\psi}^{-2\frac{p+1}{e}+2(p-1)}) \equiv G \pmod{\mathfrak{P}}$ if $\rho|_{D_p}$ is irreducible, where Tr denotes the trace operator and $E_{1,\psi}$ denotes the Eisenstein series of weight one attached to ψ.

Now, we see that the twisted representation $\rho(\frac{p+1}{e})$ arises from a Hecke cusp form (mod p) of type $(N, k_{\rho(\frac{p+1}{e})}, 1)$. If necessary, since N is prime to p, the results in [Jo-Li 89] bring the level N to N_ρ.

REFERENCES

[Ba-La 91] Bayer, P; Lario, J.C. (1991). Galois representations defined by torsion points of modular elliptic curves. To appear in *Compositio Math.*

[Ca 86] Carayol, H. (1986). Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Nor. Sup.*, **19**, 409-468.

[Cr 91] Cremona, J.E. (1991). Computation of modular elliptic curves and the Birch–Swinerton-Dyer conjecture. *University of Exeter*, preprint.

[Ed 89] Edixhoven , B. (1989). Stable models of modular curves and applications. *Faculteit der Wiskunde en Informatica. Rijksuniversiteit te Utrecht.* Thesis.

[Ed-Gr-To 90] Edixhoven , B.; de Groot, A.; Top, J. (1990). Elliptic curves over the rationals with bad reduction at only one prime. *Math. of Computation*, **54**, 413-419.

[Gr 90] Gross, B.H. (1990). A tameness criterion for Galois representations associated to modular forms. *Duke Math. Journal*, **61**, 445-517.

[Hi-Pi-She 90] Hijikata, H.; Pizer, A.; Shemanske, T. (1990). Twist of newforms.

[Hu 87] Husemöller, D. (1987). Elliptic Curves. *GTM Springer-Verlag*, **111**.

[Jo-Li 89] Jordan, B.;Livné, R. (1989). Conjecture "epsilon" for weight $k > 2$. *Bull. of the AMS*, **21**, 51-56.

[La 91] Lario, J.C. (1991). Representacions de Galois i corbes el·líptiques. *Universitat de Barcelona.* Thesis.

[Li 75] Li, W. (1975). Newforms and functional equations. *Math. Ann.*, **212**, 285-315.

[Se 87] Serre, J.-P. (1987). Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. Journal*, **54**, 179-230.

[Ma 78] Mazur, B. (1978). Rational isogenies of prime degree. *Invent. Math.*, **44**, 129-162.

[Ta 75] Tate, J. (1975). Algorithm for determining the type of a singular fibre in an elliptic pencil. *Springer LN in Math.*, **476**, 33-52.

Joan-C. Lario
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Pau Gargallo, 5
E-08028 Barcelona (Spain)

Astérisque

MORISLAV LASSAK

Some remarks on the Pethő public key cryptosystem

Astérisque, tome 209 (1992), p. 257-264

<http://www.numdam.org/item?id=AST_1992__209__257_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Some remarks on the Pethő public key cryptosystem

Miroslav Laššák, Bratislava

In [1] Pethő introduced a public key cryptosystem. In its definition (see below for more details) an essential role is played by a monic polynomial $g(t)$ of degree n and a modulus M, which belong to the nonpublic part of this cryptosystem. The aim of this note is to show that if the greatest common divisor of the nth power of the constant term of g and M is too "small", then the cryptosystem can be broken in polynomial time. The crucial role in our cryptoanalysis is played by a system of congruences (9) whose solution can be found under the above mentioned condition.

1 Pethő public key cryptosystem

For the convenience of the reader, we describe in this section the main ingredients of the public key cryptosystem suggested by A. Pethő in [1].

Let $g(t) = t^n + g_{n-1}t^{n-1} + \cdots + g_1 t + g_0 \in \mathcal{Z}[t]$, where $\mathcal{Z}$ denotes the ring of integers and $\mathbf{G}$ the companion matrix of the polynomial $g(t)$. Further, let $\mathbf{x}_i \in \mathcal{Z}^n$ for $i \geq 0$ be the sequence of vectors defined by

$$\begin{aligned} \mathbf{x}_0 &= (1, 0, \ldots, 0) \\ \mathbf{x}_{i+1} &= \mathbf{x}_i \mathbf{G} \quad \text{for} \quad i \geq 0. \end{aligned} \tag{1}$$

Given a finite subset $\mathcal{N}$ of $\mathcal{Z}$, $\mathcal{A}_\mathcal{N}$ will denote the set of all finite words over $\mathcal{N}$ satisfying the property that if $0 \in \mathcal{N}$ and $l > 0$ then $w_l \neq 0$. If $l(w) = l+1$ denotes the length of the word $w = w_0 w_1 \ldots w_l$, then $\mathcal{A}_\mathcal{N}^L$ will denote the set of all words of $\mathcal{A}_\mathcal{N}$ of length not exceeding $L+1$.

DEFINITION 1.1 *A pair* $\{g(t), \mathcal{N}\}$ *is called a* weak number system *if the map* $T : \mathcal{A}_\mathcal{N} \to \mathcal{Z}^n$ *defined by*

$$T(w_0 \ldots w_l) = w_0 \mathbf{x}_0 + \cdots + w_l \mathbf{x}_l \tag{2}$$

is injective.

One sufficient condition for weak number systems is contained in the next result [1]:

PROPOSITION 1.1 *If $|g_0| \geq 2$ and $\mathcal{N}$ consists of pairwise incongruent integers modulo g_0, then the pair $\{g(t), \mathcal{N}\}$ is a weak number system.*

This weak number system enables us to construct a private key cryptosystem. To do this take $g(t) = t^n + g_{n-1}t^{n-1} + \cdots + g_1 t + g_0 \in \mathcal{Z}[t]$ with $|g_0| \geq 2$ and a set $\mathcal{N}$ of pairwise incongruent integers modulo g_0.

For encryption of a plaintext $w = w_0 \dots w_r \in \mathcal{A}_\mathcal{N}$ choose integers $l_1, l_2, \dots, l_h$ with $l_1 + l_2 + \cdots + l_h = r + 1$. Then cut the word w into subwords $W_1, \dots, W_h$ of $\mathcal{A}_\mathcal{N}$ in such a way that $w = W_1 \dots W_h$ and $l(W_i) = l_i$. Then application of the map T gives the cryptogram $Y_1, \dots, Y_h \in \mathcal{Z}^n$, where $Y_i = T(W_i)$ for $i = 1, \dots, h$. The knowledge of the corresponding secret keys $g(t)$ and $\mathcal{N}$ may be used to decrypt the received message. For more details about the corresponding algorithm consult [1].

Unfortunately, this cryptosystem cannot be used as the public key cryptosystem, therefore Pethő suggested the following modification:

Let $\{g(t), \mathcal{N}\}$ be a weak number system constructed by proposition 1.1 such that $0 \in \mathcal{N}$.

Let the height $m(w)$ of the word $w \in \mathcal{A}_\mathcal{N}$ be defined by

$$m(w) = \max\{|y_0|, \dots, |y_{n-1}|\},$$

where $T(w) = (y_0, \dots, y_{n-1}) \in \mathcal{Z}^n$. Then take an integer M such that

$$M > 2\max\{m(w) : w \in \mathcal{A}_\mathcal{N}^{n+L}\} \tag{3}$$

and a regular matrix $\mathbf{C}$ over $\mathcal{Z}_M$ satisfying

$$\mathbf{CG} \neq \mathbf{GC} \quad \text{over } \mathcal{Z}_M. \tag{4}$$

Finally, define the vectors $\widehat{\mathbf{x}}_i$ for $i = 0, 1, \dots, L$ by

$$\widehat{\mathbf{x}}_i \equiv \mathbf{x}_{n+i}\mathbf{C} \pmod{M} \tag{5}$$

and the map $\widehat{T} : \mathcal{A}_\mathcal{N}^L \to \mathcal{Z}^n$ by

$$\widehat{T}(w_0 \dots w_l) = w_0\widehat{\mathbf{x}}_0 + \cdots + w_l\widehat{\mathbf{x}}_l \quad \text{for } l \leq L. \tag{6}$$

The public part of the Pethő public key cryptosystem consists of the chosen weak number system, $\mathcal{N}$ and vectors $\widehat{\mathbf{x}}_0, \widehat{\mathbf{x}}_1, \dots, \widehat{\mathbf{x}}_L$. To encrypt a plaintext $w = w_0 \dots w_i$ an analogous algorithm can be used, but based on $\widehat{T}(w_0 \dots w_i)$ instead on $T(w_0 \dots w_i)$.

Knowing the secret keys $\mathbf{C}, M$ one can determine the matrix $\mathbf{C}^{-1}$ over $\mathcal{Z}_M$. We have

$$\widehat{T}(w_0 \dots w_l) = w_0\widehat{\mathbf{x}}_0 + \dots + w_l\widehat{\mathbf{x}}_l \equiv (w_0\mathbf{x}_n + \dots + w_l\mathbf{x}_{n+l})\mathbf{C} \pmod{M}$$

and consequently

$$(y_0, \dots, y_{n-1}) = T(\underbrace{0 \dots 0}_{n} w_0 \dots w_l) \equiv \widehat{T}(w_0 \dots w_l)\mathbf{C}^{-1} \pmod{M}. \quad (7)$$

Furthermore, using (3) we obtain

$$2|y_i| \leq 2m(\underbrace{0 \dots 0}_{n} w_0 \dots w_l) < M,$$

which implies

$$|y_i| < M/2 \quad \text{for} \quad i = 0, 1, \dots, n-1 \quad (8)$$

and $y_0, \dots, y_{n-1}$ are uniquely determined. Using the algorithm for decryption (see [1]) we get $0 \dots 0 w_0 \dots w_l$ and then $w_0 \dots w_l$.

This cryptosystem is correct in the sense that the plaintext may be uniquely determined from the encrypted text.

2 A possibility of decryption

We write $\mathbf{A} \equiv \mathbf{B} \pmod{m}$ or $\mathbf{A} \overset{(m)}{\equiv} \mathbf{B}$ for the matrices $\mathbf{A}, \mathbf{B}$ congruent modulo m.

DEFINITION 2.1 *The square matrices $\mathbf{A}, \mathbf{B}$ of order n are called* similar modulo m *if there exist two square matrices $\mathbf{P}, \mathbf{Q}$ of order n such that $\mathbf{PQ} \overset{(m)}{\equiv} \mathbf{QP} \overset{(m)}{\equiv} \mathbf{I}$ and $\mathbf{B} \equiv \mathbf{PAQ} \pmod{m}$. We write $\mathbf{A} \sim \mathbf{B} \pmod{m}$.*

PROPOSITION 2.1 *Let $\mathbf{A}, \mathbf{B}$ be square matrices of order n and $\operatorname{char}(\mathbf{A}) = t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0, \operatorname{char}(\mathbf{B}) = t^n + b_{n-1}t^{n-1} + \dots + b_1 t + b_0$ be their characteristic polynomials. If $\mathbf{A} \sim \mathbf{B} \pmod{m}$, then*

$$a_i \equiv b_i \pmod{m} \quad \textit{for } i = 0, 1, \dots, n-1.$$

Now we return to the Pethő public key cryptosystem. Consider the following system of congruences

$$\widehat{\mathbf{x}}_i \equiv \widehat{\mathbf{x}}_{i-1}\mathbf{A} \pmod{M} \quad \text{for} \quad i = 1, 2, \dots, L, \quad (9)$$

where $\mathbf{A}$ is a (unknown) matrix of order n and M, $\widehat{\mathbf{x}}_0, \widehat{\mathbf{x}}_1, \dots, \widehat{\mathbf{x}}_L$ are public keys.

It is not hard to see that the matrix $\mathbf{C}^{-1}\mathbf{GC}$ is a solution of the system of congruences (9) for

$$\begin{aligned}\widehat{\mathbf{x}}_i &\overset{(M)}{\equiv} \mathbf{x}_{n+i}\mathbf{C} = \mathbf{x}_{n+i-1}\mathbf{GC} \\ &\overset{(M)}{\equiv} \mathbf{x}_{n+i-1}\mathbf{C}\mathbf{C}^{-1}\mathbf{GC} \overset{(M)}{\equiv} \widehat{\mathbf{x}}_{i-1}(\mathbf{C}^{-1}\mathbf{GC}) \quad \text{for} \quad i = 1, 2, \ldots, L.\end{aligned}$$

In the rest of the paper we shall find conditions under which it is possible to find M and a solution matrix $\mathbf{A}_0$ of the system (9). The following observations show that this is sufficient to break the Pethő cryptosystem in polynomial time. To see this note:

1. If $\mathbf{A}_0 \equiv \mathbf{C}^{-1}\mathbf{GC} \pmod{M}$, then by definition 2.1 the matrices $\mathbf{A}_0$ and $\mathbf{G}$ are similar modulo M. Therefore, if $\operatorname{char}(\mathbf{A}_0) = t^n + g'_{n-1}t^{n-1} + \cdots + g'_1 t + g'_0$ is the characteristic polynomial of the matrix $\mathbf{A}_0$, then by proposition 2.1 we have

$$g'_i \equiv g_i \pmod{M}. \tag{10}$$

Furthermore, we have

$$M > 2|g_i| \cdot |w'| \geq 2|g_i|, \tag{11}$$

where w' is a nonzero element of $\mathcal{N}$, since $\mathbf{x}_n = (-g_0, \ldots, -g_{n-1})$. Consequently, $|g_i| < M/2$ for $i = 0, 1, \ldots, n-1$ and this together with (10) implies that the coefficients $g_0, g_1, \ldots, g_{n-1}$ of the polynomial $g(t)$ are uniquely determined. Thus we can derive the polynomial $g(t)$, the matrix $\mathbf{G}$ and the vectors $\mathbf{x}_i$ $(i = 0, 1, \ldots, n+L)$ from knowledge of M and $\mathbf{A}_0$.

2. Let $\mathbf{R}_0$ be an arbitrary solution of the system of congruences

$$\widehat{\mathbf{x}}_i\mathbf{R} \equiv \mathbf{x}_{n+i} \pmod{M} \quad \text{for } i = 0, 1, \ldots, L \tag{12}$$

with an unknown matrix $\mathbf{R}$. This system is solvable, because $\mathbf{C}^{-1}$ solves it. But it is not necessary to find just the matrix $\mathbf{C}^{-1}$, because any solution matrix $\mathbf{R}_0$ can be used for determining $y_0, \ldots, y_{n-1}$ since

$$\begin{aligned}\widehat{T}(w_0 \ldots w_l)\mathbf{R}_0 &= (w_0\widehat{\mathbf{x}}_0 + \cdots + w_l\widehat{\mathbf{x}}_l)\mathbf{R}_0 \\ &\overset{(M)}{\equiv} w_0\mathbf{x}_n + \cdots + w_l\mathbf{x}_{n+l} \\ &= T(0 \ldots 0 w_0 \ldots w_l) = (y_0, \ldots, y_{n-1})\end{aligned}$$

Due to (8) the numbers $y_0, \ldots, y_{n-1}$ are uniquely determined. Now we know all that is necessary for decryption. Applying the decryption algorithm to $(y_0, \ldots, y_{n-1}) = T(0 \ldots 0 w_0 \ldots w_l)$ we get $0 \ldots 0 w_0 \ldots w_l$ and consequently $w_0 \ldots w_l$.

Thus knowing M and the matrix $\mathbf{A}_0$ we are able to decrypt intercepted messages in polynomial time.

3 How to solve system (9)

Put

$$\mathbf{X} = \begin{pmatrix} \widehat{\mathbf{x}}_0 \\ \vdots \\ \widehat{\mathbf{x}}_{L-1} \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} \widehat{\mathbf{x}}_1 \\ \vdots \\ \widehat{\mathbf{x}}_L \end{pmatrix}$$

and rewrite the system of congruences (9) into the matrix form

$$\mathbf{XA} \equiv \mathbf{Y} \pmod{M}. \tag{13}$$

We can suppose $L \geq n$. In the opposite case (i. e. if $L < n$) this system would reduce to a system of equations, which is easy to solve and we immediately obtain the plaintext.

Reduce the matrix $\mathbf{X}$ of order $L \times n$ over $\mathcal{Z}$ to Smith canonical form. Then we obtain invertible matrices $\mathbf{P}, \mathbf{Q}$ over $\mathcal{Z}$ such that

$$\mathbf{PXQ} = \mathbf{D},$$

where $\mathbf{D} = \mathrm{diag}_{L,n}(a_0, \ldots, a_{n-1})$ is the matrix of order $L \times n$ with $a_0, \ldots, a_{n-1}$ on the main diagonal and $a_i | a_j$ for $i < j$. We may suppose that $a_i \geq 0$ for $i = 0, 1, \ldots, n-1$ (in the opposite case multiply the row by -1).

The system (13) can be equivalently rewritten into the form

$$\mathbf{DB} = \mathbf{PXQB} \equiv \mathbf{PY} \pmod{M}, \tag{14}$$

with an unknown matrix $\mathbf{B}$ such that $\mathbf{A} = \mathbf{QB}$.

Note that we do not need to know M in order to be able to reduce the matrix $\mathbf{X}$ to Smith canonical form.

If $\mathbf{B} = \|y_{ij}\|$ and $\mathbf{PY} = \|b_{ij}\|$, then the system (14) can be replaced by two systems

$$\begin{aligned} a_0 y_{0,j} &\equiv b_{0,j} \pmod{M} \\ &\vdots \\ a_{n-1} y_{n-1,j} &\equiv b_{n-1,j} \pmod{M} \quad \text{for} \quad j = 0, \ldots, n-1 \end{aligned} \tag{15}$$

and

$$\begin{aligned} 0 &\equiv b_{n,j} \pmod{M} \\ &\vdots \\ 0 &\equiv b_{L-1,j} \pmod{M} \quad \text{for} \quad j = 0, \ldots, n-1. \end{aligned} \tag{16}$$

System (16) is solvable, because e. g. the matrix $\mathbf{Q}^{-1}\mathbf{C}^{-1}\mathbf{GC}$ is its solution. Thus the following condition must be true:

$$M | b_{k,j} \quad \text{for} \quad k = n, \ldots, L-1; j = 0, \ldots, n-1.$$

If we write d for the greatest common divisor of $b_{k,j}$ for all $k = n, \ldots, L-1$; $j = 0, \ldots, n-1$, then $M|d$.

Similarly, system (15) has also a solution, therefore

$$(a_i, M) = (a_i, M, b_{i,j}) \quad \text{for} \quad i = 0, \ldots, n-1; j = 0, \ldots, n-1$$

and this gives a further restriction on M of the type $M|d'$, where $d' \leq d$.

Now we may gradually substitute for M divisors of d'. However, this is possible only provided $d \neq 0$, otherwise the congruences (5) become equalities, i. e. $\widehat{\mathbf{x}}_i = \mathbf{x}_{n+i}\mathbf{C}$ for $i = 0, \ldots, L$.

Now we suppose that we know M. Put $d_i = (a_i, M)$, $m_i = M/d_i$ for $i = 0, 1, \ldots, n-1$. Since $a_i|a_j$ for $i < j$, we have $d_i|d_j$ and $m_j|m_i$ for $i < j$.

The congruence $a_i y_{ij} \equiv b_{ij} \pmod{m_i}$ has exactly d_i solutions incongruent modulo M for all $i, j \in \{0, \ldots, n-1\}$. Therefore there are $d_0^n d_1^n \cdots d_{n-1}^n$ solutions incongruent modulo M of the system (14) and also the same number of the system (13).

4 Conclusions

Now we prove the following theorem.

THEOREM 4.1 *Let* $\mathbf{X}$ *be the matrix of order* $L \times n$ *defined in section 3 and* $L \geq n$. *Let the matrix* $\mathbf{D} = \operatorname{diag}_{L,n}(a_0, \ldots, a_{n-1})$ *be its Smith canonical form with* $a_i|a_j$ *for* $i < j$ *and* $a_i \geq 0$ *for* $i = 0, 1, \ldots, n-1$. *Then*

(a) $(a_0, M) = d_0 = (M, g_0, \ldots, g_{n-1})$

(b) $(a_0 \cdots a_{n-1}, M) = (M, g_0^n)$.

Proof: The following property of the Smith canonical form will be used.

Let $\Delta_k(\mathbf{A})$ be the greatest common divisor of all minors of k-th order of a matrix $\mathbf{A}$. Given a matrix $\mathbf{A}$ of order $l \times m$, write $\mathbf{D} = \operatorname{diag}_{l,m}(a_0, \ldots, a_{n-1})$ for its Smith canonical form. Then (see [2] chapter 16)

$$\begin{aligned} a_0 &= \Delta_1(\mathbf{A}) \\ a_0 a_1 &= \Delta_2(\mathbf{A}) \\ &\vdots \\ a_0 a_1 \cdots a_{n-1} &= \Delta_n(\mathbf{A}). \end{aligned} \tag{17}$$

(a) Put $s = (M, g_0, \ldots, g_{n-1})$. We show by induction on i that there is a vector $\mathbf{x}'_{n+i}$ such that $\mathbf{x}_{n+i} = s\mathbf{x}'_{n+i}$ for all $i = 0, 1, \ldots, L$. The case $i = 0$ is trivial, because $\mathbf{x}_n = (-g_0, \ldots, -g_{n-1})$. Suppose therefore that our assertion is true for $i-1$. The induction hypothesis implies $\mathbf{x}_{n+i} = \mathbf{x}_{n+i-1}\mathbf{G} = s\mathbf{x}'_{n+i-1}\mathbf{G} =$

$s\mathbf{x}'_{n+i}$. Furthermore, we have $\widehat{\mathbf{x}}_i \overset{(M)}{\equiv} \mathbf{x}_{n+i}\mathbf{C} = s\mathbf{x}'_{n+i}\mathbf{C}$. Since $s|M$, there exists a vector $\widehat{\mathbf{x}}'_i$ over $\mathcal{Z}$ such that $\widehat{\mathbf{x}}_i = s\mathbf{x}'_i$ for all $i = 0, 1, \ldots, L$. Consequently $s|d_0$. There exists a vector $\widehat{\mathbf{x}}''_0$ over $\mathcal{Z}$ with $\mathbf{x}_n\mathbf{C} \overset{(M)}{\equiv} \widehat{\mathbf{x}}_0 = d_0\widehat{\mathbf{x}}''_0$. The matrix $\mathbf{C}$ is regular over $\mathcal{Z}_M$, $d_0|M$, thus necessarily there exists a vector $\mathbf{x}''_n$ such that $\mathbf{x}_n = d_0\mathbf{x}''_n$, i. e. $d_0|s$ as claimed.

(b) We have

$$\left|\begin{pmatrix} \widehat{\mathbf{x}}_0 \\ \vdots \\ \widehat{\mathbf{x}}_{n-1} \end{pmatrix}\right| \overset{(M)}{\equiv} \left|\begin{pmatrix} \mathbf{x}_n \\ \vdots \\ \mathbf{x}_{2n-1} \end{pmatrix}\mathbf{C}\right| =$$
$$= |\mathbf{I}\mathbf{G}^n\mathbf{C}| = |\mathbf{G}|^n|\mathbf{C}| = (-1)^n g_0^n|\mathbf{C}|.$$

Determine now the value of another minor of n-th order of the matrix $\mathbf{X}$. Let $0 \le i_0 < \cdots < i_{n-1} < L$, then

$$\left|\begin{pmatrix} \widehat{\mathbf{x}}_{i_0} \\ \vdots \\ \widehat{\mathbf{x}}_{i_{n-1}} \end{pmatrix}\right| \overset{(M)}{\equiv} \left|\begin{pmatrix} \mathbf{x}_{n+i_0} \\ \vdots \\ \mathbf{x}_{n+i_{n-1}} \end{pmatrix}\mathbf{C}\right| =$$
$$= \left|\begin{pmatrix} \mathbf{x}_{i_0} \\ \vdots \\ \mathbf{x}_{i_{n-1}} \end{pmatrix}\mathbf{G}^n\mathbf{C}\right| = \left|\begin{pmatrix} \mathbf{x}_{i_0} \\ \vdots \\ \mathbf{x}_{i_{n-1}} \end{pmatrix}\right| (-1)^n g_0^n|\mathbf{C}|.$$

This implies

$$a_0 a_1 \cdots a_{n-1} = \Delta_n(\mathbf{X}) = g_0^n|\mathbf{C}|,$$

and since the matrix $\mathbf{C}$ is regular over $\mathcal{Z}_M$ we have $(|\mathbf{C}|, M) = 1$ and in turn

$$(a_0 a_1 \cdots a_{n-1}, M) = (\Delta_n(\mathbf{X}), M) = (M, g_0^n)$$

and the proof is finished.

In section 3 we obtained $d_0^n d_1^n \cdots d_{n-1}^n$ solutions incongruent modulo M of the system (13). But we need one such $\mathbf{A}_0$ for which $\mathbf{A}_0 \equiv \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{M}$. Thus we arrive at the problem to determine which one among the solutions of (13) satisfies this additional condition.

If $d_{n-1} = 1$, then the system (13) has only one solution and we are able to decrypt. Thus $d_{n-1} = 1$ is a sufficient condition for the determination of the matrix $\mathbf{A}_0$. But there is also a weaker condition for this conclusion.

All the solutions of the system (13) are congruent modulo m_{n-1}. Let $\mathbf{Z}$ be one of them, then $\mathbf{Z} \equiv \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{m_{n-1}}$. Since $m_{n-1}|M$ and $\mathbf{C}\mathbf{C}^{-1} \overset{(M)}{\equiv} \mathbf{C}^{-1}\mathbf{C} \overset{(M)}{\equiv} \mathbf{I}$, we have $\mathbf{C}\mathbf{C}^{-1} \overset{(m_{n-1})}{\equiv} \mathbf{C}^{-1}\mathbf{C} \overset{(m_{n-1})}{\equiv} \mathbf{I}$. According to definition 2.1

we obtain $\mathbf{Z} \sim \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{m_{n-1}}$. If $\mathrm{char}(\mathbf{Z}) = t^n + g'_{n-1}t^{n-1} + \cdots + g'_1 t + g'_0$ is the characteristic polynomial of the matrix $\mathbf{Z}$, then $g_i \equiv g'_i \pmod{m_{n-1}}$ for $i = 0, 1, \ldots n-1$ as proposition 2.1 shows. Put $k = \max\{|w| : w \in \mathcal{N}\}$, then we have $M > 2k|g_i|$ for $i = 0, \ldots, n-1$ by (11), whence

$$|g_i| < \frac{M/k}{2} \quad \text{for} \quad i = 0, 1, \ldots, n-1.$$

Thus if

$$m_{n-1} \geq M/k, \quad \text{resp.} \quad d_{n-1} \leq k, \tag{18}$$

then the coefficients of $g(t)$ are uniquely determined, since

$$|g_i| < \frac{M/k}{2} \leq \frac{m_{n-1}}{2} \quad \text{for} \quad i = 0, \ldots, n-1.$$

And now we can decrypt by the same way as in section 2.

According to assertion (b) of theorem 4.1 we have

$$d_{n-1} \leq (a_0 \cdots a_{n-1}, M) = (g_0^n, M).$$

Thus the Pethő public key cryptosystem cannot be used securely if $(g_0^n, M) \leq k$ and therefore it is necessary to choose M in such a way that (g_0^n, M) is sufficiently large.

References

[1] A. PETHŐ, *On a polynomial transformation to the construction of a public key cryptosystem*, Proceedings of the Colloquium on Computational Number Theory held at Kossuth Lajos University, Debrecen (Hungary), September 4-9, 1989.

[2] K. A. RODOSSKIJ, *Euclid algorithm*, Moscow, Nauka, 1988 (in Russian).

Miroslav Laššák
Department of Algebra
and Number Theory
Faculty of Mathematics and Physics
Comenius University
Mlynská dolina
842 15 Bratislava
Czechoslovakia

Astérisque

TOM MEURMAN

A simple proof of Voronoi's identity

Astérisque, tome 209 (1992), p. 265-274

<http://www.numdam.org/item?id=AST_1992__209__265_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

A SIMPLE PROOF OF VORONOI'S IDENTITY

Tom MEURMAN

1 Introduction

Denote by $d(n)$ the number of divisors of n. Consider the function $\Delta(x)$ satisfying

$$\sum_{n<x} d(n) + \frac{1}{2}d(x) = x\log x + (2\gamma - 1)x + \frac{1}{4} + \Delta(x), \tag{1.1}$$

where $d(x) = 0$ unless x is an integer, and γ is Euler's constant. We have the following well-known and remarkable theorem:

THEOREM. *The function $\Delta(x)$ defined by (1.1) satisfies*

$$\Delta(x) = \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{d(n)}{n}\int_0^{\infty}\cos(2\pi u)\sin(2\pi\frac{nx}{u})du. \tag{1.2}$$

Moreover, the series here is boundedly convergent in any interval $[x_1, x_2] \subset (0, \infty)$, and uniformly convergent in any such interval free from integers.

This was proved originally by Voronoi [16], and later by many others, e.g. [1], [3] (or [4, Ch. VIII]), [5] (or [13, Ch. 1]), [6] and [7] combined, [10, Ch. I], [11], [14], [15]. The proofs are usually long and difficult. Most of them depend on the functional equation for the Riemann zeta-function, and the simplest of these is due to Jutila [10]. The simplest proof not depending on the functional equation is due to Landau [11]. Jutila uses the method of Dixon and Ferrar [5] except for the case when x is an integer, where he introduces a substantial simplification. Landau uses Poisson's summation formula and only real analysis. The detailed proof takes about 20 pages.

My purpose is to give a comparatively simple proof not depending on the functional equation. It has some features in common with Landau's proof, but it is shorter and the principle is different. Indeed, the principle can be used (as I shall show in a subsequent paper) in the analogous problem where

$d(n)$ is replaced by $a(n)$, the nth Fourier coefficient of a holomorphic modular cusp form. Landau's method fails here.

The method of this paper works also when $d(n)$ is replaced by $d(n)\exp(2\pi iqn)$ or by $r(n)\exp(2\pi iqn)$, where q is rational and $r(n)$ signifies the number of ways of representing n as the sum of two squares. It probably works also for $a(n)\exp(2\pi iqn)$. Moreover, there are other more obvious generalizations. This may be of some interest, since the modern theory of generalizations is based invariably on the functional equations for the relevant Dirichlet series (see e.g. Berndt [2]).

As to the significance, generalizations or analogues of Voronoi's identity the reader may consult [9, Chapters 3, 13, 15], [10, Ch. I], [12], [2] and [8]. The last two papers contain many references to the literature of the subject.

The integral in (1.2) is usually expressed in terms of the Bessel functions Y_1 and K_1 as follows (see Watson [17]):

$$-\sqrt{nx}(K_1(4\pi\sqrt{nx}) + \frac{\pi}{2}Y_1(4\pi\sqrt{nx})).$$

It is of practical value that this admits sharp approximations involving elementary functions. However, I prefer (1.2) as it stands, since, as will be shown, it is quite easy to obtain such approximations for the integral in (1.2). It would be an unnecessary detour to invoke Watson. This appears not to have been observed before. Landau evaluates the integral in (1.2) within an error $O(1)$ only, and this is not enough for practical purposes.

The principle of the proof of the theorem will be explained in the following section. The most important new idea lies in the use of the weight function $\exp(-v(u + nx/u))$.

2 The principle

For $0 \le v \le \frac{1}{2}$ define

$$\Delta(x,v) = \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{d(n)}{n}F(nx,v), \tag{2.1}$$

where

$$F(t,v) = \int_0^{\infty} e^{-v(u+t/u)}\cos(2\pi u)\sin(2\pi t/u)du. \tag{2.2}$$

Fix t for a moment. Since $\frac{d}{du}(e^{-v(u+t/u)}\sin(2\pi t/u)) \ll u^{-2}$, it follows easily by partial integration that $F(t,v)$ is uniformly convergent in $[0,\frac{1}{2}]$. Moreover, for any $\varepsilon > 0$ we have $\lim_{v\to 0+} e^{-v(u+t/u)} = 1$ uniformly in $[\varepsilon, 1/\varepsilon]$. Hence

$$\lim_{v\to 0+} F(t,v) = F(t,0). \tag{2.3}$$

Suppose that the following lemma holds:

LEMMA. *For $t \geq t_0 > 0$ and $0 \leq v \leq \frac{1}{2}$ we have*

$$F(t,v) = \frac{1}{2\sqrt{2}} t^{\frac{1}{4}} e^{-2v\sqrt{t}} \cos(4\pi\sqrt{t} - \frac{\pi}{4}) + O(t^{-\frac{1}{4}}), \tag{2.4}$$

where the implied constant in the O-term may depend on t_0 only.

Fix x for a moment. If $\Delta(x,0)$ is convergent then, since $e^{-2v\sqrt{nx}}$ is monotonic, it follows by partial summation that

$$\sum_{n=1}^{\infty} \frac{d(n)}{n} F(nx,0) e^{-2v\sqrt{nx}}$$

is uniformly convergent in $[0, \frac{1}{2}]$. By the lemma,

$$F(nx,v) = F(nx,0) e^{-2v\sqrt{nx}} + O(n^{-\frac{1}{4}}).$$

Hence also the series $\Delta(x,v)$ is uniformly convergent in $[0, \frac{1}{2}]$. By (2.3) this implies that

$$\lim_{v \to 0+} \Delta(x,v) = \Delta(x,0).$$

Then $\Delta(x) = \Delta(x,0)$, i.e. (1.2) holds, if

$$\lim_{v \to 0+} \Delta(x,v) = \Delta(x). \tag{2.5}$$

Therefore, to prove the theorem, we must prove the lemma, the statement (2.5) and the assertions concerning the convergence of $\Delta(x,0)$.

3 Proof of the lemma

The argument to be given here could easily be refined to yield an asymptotic series.

Suppose first that $v > 0$ in (2.2). Clearly

$$F(t,v) = \sqrt{t} \int_0^{\infty} e^{-v\sqrt{t}(u+1/u)} \cos(2\pi\sqrt{t}u) \sin(2\pi\sqrt{t}/u) du.$$

The main term will come from the values of u near 1. Since

$$\cos(\alpha)\sin(\beta) = \frac{1}{2}\mathrm{Im}(e^{i(\alpha+\beta)} - e^{i(\alpha-\beta)}),$$

it follows that

$$F(t,v) = \frac{1}{2}\sqrt{t}\,\mathrm{Im}(F^+ - F^-),$$

where

$$F^{\pm} = \int_0^{\infty} e^{(-v(u+1/u)+2\pi i(u\pm 1/u))\sqrt{t}} du.$$

Consider F^- and denote $g(u) = -v(u+1/u) + 2\pi i(u-1/u)$. Integrating twice by parts one gets

$$F^- = \frac{1}{t}\int_0^{\infty} \left(\frac{1}{g'(u)}\left(\frac{1}{g'(u)}\right)'\right)' e^{g(u)\sqrt{t}} du,$$

since, as $v > 0$, the integrated terms vanish at each step. We have

$$\left(\frac{1}{g'}\left(\frac{1}{g'}\right)'\right)' = -\left(\frac{g''}{(g')^3}\right)' \ll \left|\frac{g'''}{(g')^3}\right| + \left|\frac{(g'')^2}{(g')^4}\right| \ll \frac{u^2}{(u^2+1)^3} \ll \frac{1}{u^4+1}.$$

Hence $F^- = O(t^{-1})$ uniformly in v.

Consider F^+ and substitute $y = \operatorname{sgn}(u-1)\sqrt{u+1/u-2}$. Then

$$F^+ = e^{-2a}\int_{-\infty}^{\infty} f(y)e^{-ay^2} dy,$$

where $f(y) = y + \sqrt{y^2+4} - 2/\sqrt{y^2+4}$ and $a = (v - 2\pi i)\sqrt{t}$. Replace $f(y)$ by its Maclaurin polynomial $f_3(y)$, say, of degree 3, and estimate the error in the way F^- was estimated. This gives $O(t^{-1})$ uniformly in v, since

$$\left(\frac{1}{y}\left(\frac{f(y)-f_3(y)}{y}\right)'\right)' \ll \frac{1}{y^2+1}.$$

The terms of $f_3(y)$ of odd degree may clearly be omitted. The integral corresponding to the term of degree 2 is integrated (once) by parts. This gives

$$F^+ = e^{-2a}(1 + O(t^{-\frac{1}{2}}))\int_{-\infty}^{\infty} e^{-ay^2} dy + O(t^{-1}).$$

It is well-known that the integral here equals $\sqrt{\pi/a}$. Hence

$$F^+ = (\frac{\pi}{a})^{\frac{1}{2}} e^{-2a} + O(t^{-\frac{3}{4}}).$$

We have

$$(\frac{\pi}{a})^{\frac{1}{2}} - \frac{1}{\sqrt{2}} t^{-\frac{1}{4}} e^{\pi i/4} = O(vt^{-\frac{1}{4}}) = O(t^{-\frac{3}{4}} e^{v\sqrt{t}}).$$

Hence

$$F^+ = \frac{1}{\sqrt{2}} t^{-\frac{1}{4}} e^{-2v\sqrt{t} + (4\pi\sqrt{t} + \pi/4)i} + O(t^{-\frac{3}{4}}).$$

Hence, uniformly in v,

$$F(t,v) = \frac{1}{2\sqrt{2}} t^{\frac{1}{4}} e^{-2v\sqrt{t}} \sin(4\pi\sqrt{t} + \frac{\pi}{4}) + O(t^{-\frac{1}{4}}).$$

However, by (2.3) this holds even for $v = 0$.

4 $\Delta(x,v)$ as an integral

Suppose that $v > 0$. From the lemma it follows that the series in (2.1) is absolutely convergent. Hence, and by (2.2), it may be represented as the double series

$$\sum_{m=1}^{\infty}\sum_{k=1}^{\infty}\frac{1}{mk}\int_0^{\infty} e^{-v(u+mkx/u)}\cos(2\pi u)\sin(2\pi mkx/u)du$$

$$= \sum_{m=1}^{\infty}\sum_{k=1}^{\infty}\frac{1}{k}\int_0^{\infty} e^{-v(mu+kx/u)}\cos(2\pi mu)\sin(2\pi kx/u)du = \sum\sum\int f_{m,k}(u),$$

say. This is absolutely convergent, since

$$|f_{m,k}(u)| \le \exp(-\frac{1}{2}v(u + x/u + \sqrt{mkx})).$$

Moreover, the double series $\sum\sum f_{m,k}(u)$ is absolutely and uniformly convergent in any interval $[u_1,u_2] \subset (0,\infty)$. Therefore the summations may be taken behind the integral sign. This gives (as Im(log) = arg)

$$\Delta(x,v) = \frac{2}{\pi}\int_0^{\infty}\mathrm{Re}\left(\frac{1}{e^{pu}-1}\right)\arg(1-e^{-px/u})du,$$

where

$$p = v + 2\pi i.$$

5 Truncation and decomposition

Let N be an integer, $N > 2x$ and $R = N + \frac{1}{2}$. Denote

$$\Delta_1 = -\frac{1}{\pi}\int_0^R \arg(1-e^{-px/u})du,$$

$$\Delta_2 = \frac{1}{\pi}\int_0^R \mathrm{Re}\left(\frac{2}{e^{pu}-1}+1\right)\arg(1-e^{-px/u})du$$

and $\Delta_3 = \Delta(x,v) - \Delta_1 - \Delta_2$. We estimate Δ_3 by partial integration. We have

$$\int \mathrm{Re}\left(\frac{1}{e^{pu}-1}\right)du = \mathrm{Re}\left(\frac{1}{p}\log(1-e^{-pu})\right). \tag{5.1}$$

In any case this is $O(1)$. But for $u = R$ it is $O(v)$. Hence

$$\Delta_3 = \frac{2}{\pi}\int_R^{\infty}\mathrm{Re}\left(\frac{1}{e^{pu}-1}\right)\arg(1-e^{-px/u})du \ll v + \int_R^{\infty}|\frac{d}{du}\arg(1-e^{-px/u})|du.$$

The last integrand is $O(xu^{-2})$, since for $t > 0$ we have

$$\frac{d}{dt}\arg(1-e^{-pt}) = \operatorname{Im}\left(\frac{p}{e^{pt}-1}\right), \tag{5.2}$$

and for $\operatorname{Re}(z) \geq 0$ and $|\operatorname{Im}(z)| \leq \pi$ we have

$$\operatorname{Im}\left(\frac{z}{e^z-1}\right) = \operatorname{Im}\left(\frac{z+1-e^z}{e^z-1}\right) \ll |z|. \tag{5.3}$$

It follows that $\Delta_3 \ll v + x/R$, or equivalently,

$$\Delta(x,v) = \Delta_1 + \Delta_2 + O(v + xR^{-1}).$$

6 The integral Δ_1

Denote $\psi(t) = t - [t] - \frac{1}{2}$. Writing $\arg(1-e^{-2\pi it})$ as a power series we recognize the Fourier series of $\psi(t)$. Thus $\arg(1-e^{-2\pi it}) = -\pi\psi(t)$ for $t \notin \mathbf{Z}$. For $t > 0$ we have

$$\frac{d}{dv}\arg(1-e^{-pt}) = \operatorname{Im}\left(\frac{t}{e^{pt}-1}\right) \ll \frac{t}{\| t \|},$$

where $\| t \|$ denotes the distance of t from the nearest integer. Hence,

$$\arg(1-e^{-pt}) + \pi\psi(t) \ll \min(\frac{vt}{\| t \|}, 1) \ll (\frac{vt}{\| t \|})^{\frac{3}{4}} \tag{6.1}$$

for $t \notin \mathbf{Z}$ and $t > 0$. Then an easy calculation gives (as $R > x$)

$$\begin{aligned}\Delta_1 &= x\int_{x/R}^{\infty}\psi(t)t^{-2}dt + O\left(x\int_{x/R}^{\infty}(\frac{vt}{\| t \|})^{\frac{3}{4}}t^{-2}dt\right)\\ &= x(\log(\frac{R}{x}) + 1 - \gamma) - \frac{R}{2} + O(Rv^{\frac{3}{4}}).\end{aligned}$$

7 The integral Δ_2

Since $Re((e^{pu}+1)(e^{\bar{p}u}-1)) = e^{2vu} - 1 \ll vu$ for $vu \ll 1$, and since $|e^{pu}-1|^2 \gg (vu)^2 +$
$\| u \|^2 \gg (vu)^{\frac{1}{2}} \| u \|^{\frac{3}{2}}$, it follows that

$$Re\left(\frac{2}{e^{pu}-1}+1\right) = Re\left(\frac{e^{pu}+1}{e^{pu}-1}\right) = \frac{e^{2vu}-1}{|e^{pu}-1|^2} \ll (vu)^{\frac{1}{2}} \| u \|^{-\frac{3}{2}}. \tag{7.1}$$

Trivially $\arg(1-e^{-px/u}) \ll e^{-vx/u} \ll (vx/u)^{-\frac{1}{4}}$. Hence the subintegral $\int_0^{1/2}$ of Δ_2 is $O((v/x)^{\frac{1}{4}})$. Hence (recall that $R = N + \frac{1}{2}$)

$$\Delta_2 = \frac{1}{\pi}\sum_{n=1}^{N}\int_{-\frac{1}{2}}^{\frac{1}{2}} Re\left(\frac{2}{e^{p(n+u)}-1}+1\right)A_p(u)du + O\left((\frac{v}{x})^{\frac{1}{4}}\right),$$

where

$$A_q(t) = \arg(1 - e^{-qx/(n+t)}).$$

CASE 1: $x/n \notin \mathbf{Z}$. For $|u| \leq \frac{1}{2}$ we have

$$A_p(u) = A_p(0) + O\left((\| \frac{x}{n} \|^{-1} N|u|)^{\frac{3}{4}}\right). \tag{7.2}$$

To prove this, suppose that $4N|u| \leq \|x/n\|$ (the other case being trivial). Suppose that $|t| \leq |u|$. Then

$$|\frac{x}{n+t} - \frac{x}{n}| \leq 2x|t| \leq 2N|u| \leq \frac{1}{2} \| \frac{x}{n} \| .$$

Hence $\|x/(n+t)\| \gg \|x/n\|$. Using (5.2) we get

$$A_p'(t) \ll \| \frac{x}{n+t} \|^{-1} n^{-2}x \ll \| \frac{x}{n} \|^{-1} N.$$

Hence $A_p(u) - A_p(0) \ll \| x/n \|^{-1} N|u|$, and (7.2) follows.

CASE 2: $x/n \in \mathbf{Z}$. Put $q = v - 2\pi iu/n$. For $|u| \leq \frac{1}{2}$ we have

$$A_p(u) = A_q(0) + O\left((N|u|)^{\frac{3}{4}}\right). \tag{7.3}$$

To prove this, suppose that $4N|u| \leq 1$ (the other case being trivial). Suppose that $|t| \leq |u|$. Then $|\mathrm{Im}(qx/(n+t))| \leq \pi$. Hence we may use (5.2) and (5.3) to get

$$A_q'(t) \ll |q|n^{-2}x \ll n^{-2}x \ll N,$$

since(5.2) holds also when p is replaced by q. Hence $A_q(u) - A_q(0) \ll N|u|$. But $A_p(u) = A_q(u)$, since $(p-q)x/2\pi i(n+u) \in \mathbf{Z}$. Hence (7.3) follows.

Denote

$$Q_x = \begin{cases} \| x \| & for \quad x \notin \mathbf{Z}, \\ 1 & for \quad x \in \mathbf{Z}. \end{cases} \tag{7.4}$$

To estimate the contribution of the O-terms in (7.2) and (7.3) we use (7.1) and the fact that $\| x/n \| \geq Q_x/n$ if $x/n \notin \mathbf{Z}$. This gives

$$\ll v^{\frac{1}{2}} N^{\frac{3}{4}} \left(\sum_{x/n \notin \mathbf{Z}} n^{\frac{1}{2}} \| \frac{x}{n} \|^{-\frac{3}{4}} + \sum_{x/n \in \mathbf{Z}} n^{\frac{1}{2}} \right) \ll v^{\frac{1}{2}} N^3 Q_x^{-\frac{3}{4}}.$$

Consider the contribution of $A_q(0)$. The function $A_q(0)$ is odd in u, while

$$Re((e^{p(n+u)-vu} - 1)^{-1})$$

is even. Moreover,

$$\left(e^{p(n+u)} - 1\right)^{-1} - \left(e^{p(n+u)-vu} - 1\right)^{-1} \ll \frac{vu}{(vn)^2 + u^2} \ll \left(\frac{v}{n|u|}\right)^{\frac{1}{2}}.$$

It follows that

$$\sum_{x/n\in\mathbf{Z}}\int_{-\frac{1}{2}}^{\frac{1}{2}} Re\left(\frac{2}{e^{p(n+u)}-1}+1\right)A_q(0)du \ll (Nv)^{\frac{1}{2}}.$$

Consider the contribution of $A_p(0)$. We have

$$\sum_{x/n\notin\mathbf{Z}} A_p(0)\int_{-\frac{1}{2}}^{\frac{1}{2}} Re\left(\frac{2}{e^{p(n+u)}-1}\right)du \ll Nv,$$

since by (5.1) the integral in the summand equals

$$2Re(\frac{1}{p})\log\left(\frac{1+e^{-v(n+\frac{1}{2})}}{1+e^{-v(n-\frac{1}{2})}}\right) \ll Re(\frac{1}{p}) \ll v.$$

Finally, (6.1) with $t = x/n$ implies that

$$\frac{1}{\pi}\sum_{x/n\notin\mathbf{Z}} A_p(0) = -\sum_{x/n\notin\mathbf{Z}}\psi(\frac{x}{n}) + O(v^{\frac{3}{4}}N^{\frac{7}{4}}Q_x^{-\frac{3}{4}}),$$

and we have

$$\begin{aligned}\sum_{x/n\notin\mathbf{Z}}\psi(\frac{x}{n}) &= \sum_{n=1}^{N}\psi(\frac{x}{n}) - \sum_{x/n\in\mathbf{Z}}\psi(\frac{x}{n})\\ &= x\sum_{n=1}^{N}\frac{1}{n} - \sum_{n=1}^{N}\sum_{m\le x/n}1 - \frac{N}{2} + \frac{1}{2}d(x)\\ &= x(\log N+\gamma) - \sum_{n<x}d(n) - \frac{1}{2}d(x) - \frac{N}{2} + O(\frac{x}{N}).\end{aligned}$$

Collecting the relevant formulas in this and the two previous sections and using (1.1) we get

$$\Delta(x,v) = \Delta(x) + O(xN^{-1} + v^{\frac{1}{4}}N^3Q_x^{-\frac{3}{4}}) \tag{7.5}$$

for $N > x$, $N \in \mathbf{Z}$. This implies (2.5).

8 Convergence of $\Delta(x,0)$

Denote

$$f(n,x) = x^{\frac{1}{4}}n^{-\frac{3}{4}}\cos(4\pi\sqrt{nx} - \frac{\pi}{4})$$

and

$$S = \sum_{a<n\le b} d(n)f(n,x),$$

where $2 \leq a < b$. By (2.1) and (2.4) it is sufficient to consider S. Let $0 < \varepsilon < \frac{1}{4}$. We set out to prove that

$$S \ll x^{\frac{3}{4}}a^{-\frac{1}{4}+\varepsilon} + x^{\frac{1}{2}+\varepsilon}a^{-\frac{1}{2}}Q_x^{-1}, \tag{8.1}$$

$$S \ll x^{\frac{3}{4}}. \tag{8.2}$$

The symbol Q_x was defined by (7.4).

By partial summation and (1.1) we find that S equals

$$-\int_a^b \left(\frac{\partial}{\partial t}f(t,x)\right)\Delta(t)dt + \int_a^b f(t,x)(\log t + 2\gamma)dt + \left[f(t,x)(\Delta(t) + \frac{1}{2}d(t))\right]_a^b. \tag{8.3}$$

The integrated term is $O(x^{\frac{1}{4}}a^{-\frac{1}{4}})$, since $\Delta(t) \ll t^{\frac{1}{2}}$. The second integral is $O((xa)^{-\frac{1}{4}}\log a)$, by partial integration.

Consider the first integral in (8.3). We have

$$\frac{\partial}{\partial t}f(t,x) = -2\pi x^{\frac{3}{4}}t^{-\frac{5}{4}}\sin(4\pi\sqrt{tx} - \frac{\pi}{4}) + O(x^{\frac{1}{4}}t^{-\frac{7}{4}}).$$

The error term here contributes $\ll x^{\frac{1}{4}}a^{-\frac{1}{4}}$. Then replace $\Delta(t)$ by $\Delta(t,v)$, where $v = b^{-28}$. This gives an error $O(x^{\frac{3}{4}}a^{-\frac{5}{4}})$, since (7.5) with $N = [b^2]$ implies that

$$\int_a^b |\Delta(t) - \Delta(t,v)|dt \ll 1.$$

Then replace $\Delta(t,v)$ by

$$\frac{1}{\pi\sqrt{2}}\sum_{n=1}^{\infty} d(n)f(n,t)e^{-2v\sqrt{nt}} = \Delta^*(t,v),$$

say, which in view of (2.4) differs from $\Delta(t,v)$ by $\ll t^{-\frac{1}{4}}$. This difference gives an error $O(x^{\frac{3}{4}}a^{-\frac{1}{2}})$.

We are now left with

$$x^{\frac{3}{4}}\int_a^b t^{-\frac{5}{4}}\sin(4\pi\sqrt{tx} - \frac{\pi}{4})\Delta^*(t,v)dt.$$

This is, on integrating Δ^* term-by-term,

$$\ll x^{\frac{3}{4}}\sum_{n=1}^{\infty} d(n)n^{-\frac{3}{4}}\left|\int_a^b t^{-1}\sin(4\pi\sqrt{tx} - \frac{\pi}{4})\cos(4\pi\sqrt{nt} - \frac{\pi}{4})e^{-2v\sqrt{nt}}dt\right|.$$

Here $\sin(\ldots)\cos(\ldots)$ is a linear combination of

$$\sin(4\pi\sqrt{t}(\sqrt{x} - \sqrt{n})) \quad \text{and} \quad \cos(4\pi\sqrt{t}(\sqrt{x} + \sqrt{n})),$$

so that, integrating by parts, the integral is $\ll a^{-\frac{1}{2}}|\sqrt{x} \pm \sqrt{n}|^{-1}$. Therefore, excluding the term involving $\sqrt{x} - \sqrt{n}$, in which n is the (or a) positive integer minimizing $|n - x|$, the rest of the expression is $\ll x^{\frac{1}{2}+\varepsilon}a^{-\frac{1}{2}}$.

Denote by I_x the integral in the excluded term. If $x \notin \mathbf{Z}$ then $I_x \ll x^{\frac{1}{2}} a^{-\frac{1}{2}} \|x\|^{-1}$. Otherwise $I_x = 0$. This completes the proof of (8.1).

To finish the proof of (8.2) we may assume, by (8.1), that $0 < \|x\| < a^{-\frac{1}{2}}$. Split up I_x at $c = \min(b, \|x\|^{-2})$. Then, estimating as before, $\int_c^b \ll x^{\frac{1}{2}}$, and by the general inequality $|\sin y| \leq |y|$, we have $\int_a^c \ll x^{-\frac{1}{2}}$.

References

1. B.C. Berndt, Identities involving the coefficients of a class of Dirichlet series I, Trans. Amer. Math. Soc. 137 (1969), 345–359.
2. B.C. Berndt, The Voronoi summation formula, in "The theory of arithmetic functions," Lect. Notes Math. 251, pp. 21–36, Springer, 1972.
3. K. Chandrasekharan and R. Narasimhan, Functional equations with multiple gamma factors and the average order of arithmetical functions, Ann. Math. 76 (1962), 93–136.
4. K. Chandrasekharan, "Arithmetical functions," Springer, 1970.
5. A.L. Dixon and W.L. Ferrar, Lattice point summation formulae, Quart. J. Math. 2 (1931), 31–54.
6. G.H. Hardy, On the expression of a number as the sum of two squares, Quart. J. Math. 46 (1915), 263–283.
7. G.H. Hardy, On Dirichlet's divisor problem, Proc. London Math. Soc. 15 (1916), 1–25.
8. D.A. Hejhal, A note on the Voronoi summation formula, Mh. Math. 87 (1979), 1–14.
9. A. Ivić, "The Riemann zeta-function," John Wiley & Sons, 1985.
10. M. Jutila, "Lectures on a method in the theory of exponential sums," Tata Institute of Fundamental Research, Lectures on mathematics and physics 80, Springer, 1987.
11. E. Landau, Über das Konvergenzgebiet einer mit der Riemannschen Zetafunktion zusammenhängenden Reihe, Math. Ann. 97 (1927), 251–290.
12. T. Meurman, On exponential sums involving the Fourier coefficients of Maass wave forms, J. reine angew. Math. 384 (1988), 192–207.
13. Y. Motohashi, "Lectures on the Riemann–Siegel formula," Ulam. Seminar, Dept. Math., Colorado Univ., Boulder, 1987.
14. A. Oppenheim, Some identities in the theory of numbers, Proc. London Math. Soc. 26 (1927), 295–350.
15. W. Rogosinski, "Neue Anwendung der Pfeifferschen Methode bei Dirichlets Teilerproblem," Thesis, Göttingen, 1922.
16. M.G. Voronoi, Sur une fonction transcendante et ses applications à la sommation de quelques séries, Ann. Ecole Norm. Sup. 21 (1904), 207–267, 459–533.
17. G.N. Watson, "A treatise on the theory of Bessel functions (2nd ed.)," Cambridge Univ. Press, 1951.

Department of Mathematics, University of Turku, SF–20500 Turku, Finland

Astérisque

B. Z. Moroz

On the representation of large integers by integral ternary positive definite quadratic forms

Astérisque, tome 209 (1992), p. 275-278

<http://www.numdam.org/item?id=AST_1992__209__275_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

On the Representation of Large Integers by Integral Ternary Positive Definite Quadratic Forms

B. Z. MOROZ

A few years after the famous work of C. L. Siegel [17] on representation of integers by a genus of quadratic forms had appeared, Yu. V. Linnik [10] initiated a study of representation of integers by an individual ternary quadratic form. Due to the efforts of many authors (cf., for instance, [1], [3], [9], [11], [12], [15], [19], and references therein), we may now claim a success. Let $f(x) = \frac{1}{2} \sum_{1 \leq i,j \leq 3} a_{ij} x_i x_j$ be a positive definite quadratic form with integral rational coefficients, so that $a_{ij} = a_{ji}$, $a_{ij} \in \mathbb{Z}$, $2 \mid a_{ii}$ for $1 \leq i, j \leq 3$, and let $r_f(n) = \operatorname{card}\{u \mid u \in \mathbb{Z}^3, f(u) = n\}$ be the representation number of n by f; let $D = \det(a_{ij})$.

THEOREM 1. *Suppose that $n \in \mathbb{Z}$, $n \geq 1$ and $\gcd(n, 2D) = 1$. Then $r_f(n) = r(n, \operatorname{gen} f) + O(n^{\frac{1}{2}-\gamma})$ for $\gamma < \frac{1}{28}$, where $r(n, \operatorname{gen} f)$ denotes the number of representations of n by the genus of f averaged in accordance with Siegel's prescription* [17]. *Moreover, if n is primitively represented by f over the ring of p-adic integers for each rational prime p then $r(n, \operatorname{gen} f) \gg_{f,\varepsilon} n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$.*

Proof. Let N be a positive integer such that $2D \mid N$ and $8 \mid N$, and let $\varphi \in S_0(\frac{3}{2}, N, \chi)$ with $\chi(d) = \left(\frac{2D}{d}\right)$, suppose furthermore that $\varphi \in \mathcal{U}^{\perp}$, in the notation of [15]. Thus φ is a 'good' cusp-form of weight $\frac{3}{2}$ (and character χ) that does not come from a θ-series. Therefore an argument due to H. Iwaniec [9] and W. Duke [3], supplemented by the considerations going back to G. Shimura [16] and B. A. Cipra [2], leads to an estimate for the

Fourier coefficients of φ (cf. also [7]), and on writing $\varphi(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi inz}$ we obtain: $a(n) \ll_{\varphi,\gamma} n^{\frac{1}{2}-\gamma}$ as soon as $(n, 2D) = 1$ and $\gamma < \frac{1}{28}$. By [15, Korollar 3], it follows then that $r_f(n) = r(n, \operatorname{spn} f) + O(n^{\frac{1}{2}-\gamma})$ for $(n, 2D) = 1$ and $\gamma < \frac{1}{28}$, where $r(n, \operatorname{spn} f)$ denotes the representation number of n averaged over the spinor genus containing f (cf. [15]). On the other hand, by [15, Korollar 2], if $(n, 2D) = 1$ then $r(n, \operatorname{spn} f) = r(n, \operatorname{gen} f)$. Finally, the estimate $r(n, \operatorname{gen} f) \gg n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$ is a consequence of Siegel's work [17, 18] (cf. also [14, Satz (3.1)]), as soon as n is primitively representable by f over the p-adic integers. This completes the proof.

REMARK 1. The condition $(n, 2D) = 1$ in Theorem 1 has been used in the proof twice, to ensure the estimate $a(n) \ll n^{\frac{1}{2}-\gamma}$ and to deduce the identity $r(n, \operatorname{spn} f) = r(n, \operatorname{gen} f)$. The former use of this condition is due to the fact that $\varphi \in S(\frac{3}{2}, N, \chi)$ with $\chi = \left(\frac{2D}{d}\right)$ (see [13] for the details). It is an interesting question to what extent one can weaken the condition $(n, 2D) = 1$ in Theorem 1. The work of R. Schulze-Pillot [15] (cf. also [19] and references therein) is pertinent to this question.

THEOREM 2. *Let q be a rational prime congruent to 5 modulo 8 and let $f(x) = x_1^2 + x_2^2 + q^3x_3^2$. Then $r_f(n) \gg_{q,\varepsilon} n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$ and $n \equiv 7 \pmod 8$.*

Proof. Let $n = q^\ell n_1$, $q \mid n_1$ and suppose that $n \equiv 7 \pmod 8$. Consider the quadratic form $g(x) = x_1^2 + x_2^2 + q^m x_3^2$, where $m = 3 - \ell$ when $\ell \leq 3$ and $m = 0$ when $\ell \geq 3$; let $n_2 = nq^{m-3}$. Since $n_2 \equiv 3 \pmod 8$ if $\ell \geq 3$ and $n_2 \not\equiv 0 \pmod q$ when $\ell < 3$, it follows from Theorem 1 that $r_g(n_2) \gg n_2^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$. On writing $x_1^2 + x_2^2 = q^{3-m}(n_2 - q^m y_3^2)$ one notes that to each solution of the equations: $n_2 = g(y)$ with $y \in \mathbb{Z}^3$, $q^{3-m} = z_1^2 + z_2^2$ with $z_1 \in \mathbb{Z}$, $z_2 \in \mathbb{Z}$ there corresponds a unique solution of the equation $n = f(x)$ with $x \in \mathbb{Z}^3$. Since $q \equiv 1 \pmod 4$ it follows, in particular, that $r_f(n) \gg n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$. This completes the proof.

REMARK 2. Theorem 2 confirms a conjecture of D. R. Heath-Brown [8, p. 137–138], that every large integer congruent to 7 modulo 8 is represented by the form $x_1^2 + x_2^2 + q^3x_3^2$ when $q \equiv 5 \pmod 8$ and q is a rational prime.

DEFINITION. Let $n \in \mathbb{Z}$. We say that n is square-full if $n > 0$ and $p \mid n \Rightarrow p^2 \mid n$ for each rational prime p.

COROLLARY. *Every sufficiently large positive integer is a sum of at most three square-full numbers.*

Proof. By a classical theorem of Gauß, each positive integer n is either a sum of three squares or it is of the shape $n = 4^\ell(8k+7)$ with $\ell \in \mathbb{Z}$, $k \in \mathbb{Z}$. In the latter case, however, Theorem 2 shows that the integer n is represented, for instance, by the form $x_1^2 + x_2^2 + 125x_3^2$ if k is sufficiently large. Other possibilities are also easily eliminated since the form $x^2 + y^2 + 2z^2$ is easily seen to represent n as soon as $n \equiv 4 \pmod 8$, cf. [8, p. 137]. This completes the proof.

REMARK 3. This corollary has been first proved by D. R. Heath-Brown [8], by a different method; according to [8, p. 137], it answers a question posed by P. Erdős and A. Ivić.

REMARK 4. This note contains the text of my lecture at the 16$^{\text{th}}$ Journées Arithmétiques (Marseilles, July 1989). Since then a new important paper by W. Duke and R. Schulze-Pillot [5] has appeared, which allows, in particular, to weaken the condition $(n, 2D) = 1$ in Theorem 1 of this note (cf. also Remark 1). Unfortunately, the authors suppress the details of the proof of their crucial Lemma 2 [5, p. 50–51]; following [7], where incidentally the proof of the corresponding assertion is also omitted, we are content with a weaker statement [13, p. 17–19] that leads to the results described above. Finally, we cite here two articles [4], [6], throwing further light on our subject.

ACKNOWLEDGEMENT. It is my pleasant duty to thank Professor W. Duke for a few useful conversations during the conference, relating to his work [3]; I am grateful also to Professor R. Schulze-Pillot for a private communication, allowing me to reconstruct the proof of Lemma 2 in [5] mentioned above.

References

[1] Cassels, J.W.S.: Rationale quadratische Formen. Jahresbericht der Deutschen Mathematiker-Vereinigung, 82 (1980), 81–93.

[2] Cipra, B.A.: On the Niwa-Shintani theta-kernel lifting of modular forms. Nagoya Mathematical Journal, 91 (1983), 49–117.

[3] Duke, W.: Hyperbolic distribution problems and half-integral weight Maass forms. Inventiones Mathematicae, 92 (1988), 73–90.

[4] Duke, W.: Lattice points on ellipsoids. Séminaire de Théorie des Nombres de Bordeaux, le 20 mai 1988, Année 1987–88, Exposé no. 37.

[5] Duke, W. & Schulze-Pillot, R.: Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. Inventiones Mathematicae, 99 (1990), 49–57.

[6] Fomenko, O.M.: Estimates of the norms of cusp-forms and arithmetic applications. Zapiski LOMI, 168 (1988), 158–179.

[7] Fomenko, O.M. & Golubeva, E.P.: Asymptotic distribution of integral points on a two-dimensional sphere. Zapiski LOMI, 160 (1987), 54–71.

[8] Heath-Brown, D.R.: Ternary quadratic forms and sums of three square-full numbers; in: Séminaire de Théorie des Nombres, Paris 1986/87 (edited by C. Goldstein), Birkhäuser, 1988; pp. 137–163.

[9] Iwaniec, H.: Fourier coefficients of modular forms of half-integral weight. Inventiones Mathematicae, 87 (1987), 385–401.

[10] Linnik, Yu. V.: On the representation of large integers by positive definite quadratic forms. Izvestiya Akademii Nauk SSSR (ser. mat.), 4 (1940), 363–402.

[11] Linnik, Yu. V.: Ergodic properties of algebraic fields. Springer-Verlag, 1968.

[12] Malyshev, A.V.: Yu. V. Linnik's ergodic method in number theory. Acta Arithmetica, 27 (1975), 555–598.

[13] Moroz, B. Z.: Recent progress in analytic arithmetic of positive definite quadratic forms. Max-Planck-Institut für Mathematik, preprint, 1989.

[14] Peters, M.: Darstellungen durch definite ternäre quadratische Formen. Acta Arithmetica, 34 (1977), 57–80.

[15] Schulze-Pillot, R.: Thetareihen positiv definiter quadratischer Formen. Inventiones Mathematicae, 75 (1984), 283–299.

[16] Shimura, G.: On modular forms of half-integral weight. Annals of Mathematics, 97 (1973), 440–481.

[17] Siegel, C.L., Über die analytische Theorie der quadratischen Formen; in: Gesammelte Abhandlungen, Bd. I. Springer-Verlag, 1966; 326–405.

[18] Siegel, C.L., Über die Klassenzahl quadratischer Zahlkörper; in: Gesammelte Abhandlungen, Bd. I. Springer-Verlag, 1966; 406–409.

[19] Teterin, Yu. G.: Representations of integers by spinor genera of translated lattices. Zapiski LOMI, 151 (1986), 135–140.

B. Z. Moroz
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D–5300 Bonn 3, Deutschland

Astérisque

RUDOLF SCHARLAU
CLAUDIA WALHORN

Integral lattices and hyperbolic reflection groups

Astérisque, tome 209 (1992), p. 279-291
<http://www.numdam.org/item?id=AST_1992__209__279_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

INTEGRAL LATTICES AND HYPERBOLIC REFLECTION GROUPS

Rudolf SCHARLAU and Claudia WALHORN

1. Reflective lattices and their groups

In this paper we wish to contribute to the problem of giving a full, explicit classification of all arithmetic groups of isometries of hyperbolic space which are generated by reflections in hyperplanes.

We consider integral quadratic lattices L, that is, L is a free $\mathbb{Z}$-module of finite rank, $L \cong \mathbb{Z}^r$, together with a symmetric bilinear form. The value of the form at vectors $x, y \in V := \mathbb{R}L$ is denoted by $(x, y) \in \mathbb{R}$. "Integral" means that $(x, y) \in \mathbb{Z}$ for all $x, y \in L$. We shall deal with the following two cases: L is **Euclidean**, i.e. the form is positive definite, or L is **Lorentzian**, i.e. the form is of signature $(n, 1)$, $n + 1 = r$.

For $v \in V$ with $(v, v) \neq 0$, the reflection

$$s_v : x \longmapsto x - \frac{2(v,x)}{(v,v)} v$$

is an isometry of the quadratic vector space V. A primitive vector $v \in L$ (that is, $v/m \notin L$ for all integers $m > 1$) is called a **root** of L if $(v, v) > 0$ and if s_v maps L into itself. By the above formula, this holds if and only if $(v, L) \subseteq \mathbb{Z}(v, v)/2$. In particular, $(v, v)/2$ divides the exponent of the finite group $L^\# / L$, where $L^\# = \{y \in V \mid (L, y) \subseteq \mathbb{Z}\}$ is the dual lattice. Notice that a vector v with $(v, v) = 1$ or 2 always is a root, but if L is not unimodular, then other values may occur. In the Lorentz case, the restriction to vectors with $(v, v) > 0$ is made for the following reason. The set of vectors $x \in V$ such that $(x, x) = -1$ falls into two connected components. If $O^+(V)$ denotes the subgroup of index 2 of the orthogonal group $O(V)$ mapping each of these into itself, then $(v, v) > 0$ is equivalent to $s_v \in O^+(V)$. Each of the connected

components is a model of hyperbolic n-space H^n, and $O^+(V)$ induces the full isometry group of H^n. Notice that if $(v,v) > 0$, then the orthogonal complement $v^\perp$ is of signature $(n-1,1)$. Thus the fixed point set of s_v really "is" a hyperbolic subspace (hyperplane) in our hyperbolic space.

A basic (though trivial) observation now is that in the Euclidean case, the set $R(L)$ of all roots of L is a root system in the usual sense of Lie algebra theory. Indeed, if $v, v' \in R(L)$, then $s_v v' \in R(L)$ since $s_{s_v v'} = s_v s_{v'} s_v$. The "crystallographic condition" $2(v,v')/(v,v) \in \mathbb{Z}$ also holds; we have just seen that it holds for all $v' \in L$. Strictly speaking, $R(L)$ should be considered as a root system R together with a fixed quadratic form invariant under the Weyl group $W(R) = \langle s_v \mid v \in R \rangle$, and the notion of isomorphism is that of an isometric bijection. Thus, $R(L)$ is even a finer invariant than a usual root system.

We now come to the basic definition of this paper, which was first introduced explicitly by E. Vinberg [Vi2].

1.1. **Definition.** A quadratic lattice L is called **reflective** if

a) in the Euclidean case: $R(L)$ has the maximum possible rank $\dim L$,

b) in the Lorentz case: the normal subgroup $W(L)$ of $O^+(L)$ generated by all reflections s_v, v a root, is of finite index.

See [BS] for general results about the structure of reflective Euclidean lattices and for a full classification in small dimensions. If the signature is $(n,1)$, any group $W(L)$ acts as a discrete group, generated by reflections in hyperplanes, on hyperbolic n-space. By definition, $W(L)$ is "crystallographic" in the sense that it has a fundamental domain of finite volume if and only if L is reflective. (Recall that $O^+(L)$ always has a fundamental domain of finite volume.) Like in the case of reflection groups on the sphere or on Euclidean space, these "hyperbolic reflection groups" satisfy the axioms of abstract Coxeter groups (after one has fixed a fundamental domain and thus a fundamental set of generating reflections) and are described by Coxeter diagrams; see [Vi1]. Contrary to the spherical or Euclidean case, a full classification of hyperbolic reflection groups is not known, not even in the case of "arithmetic" groups $W(L)$.

A basic lemma of Vinberg's [Vi2] relates the two notions of reflectiveness of lattices to each other:

1.2. VINBERG'S LEMMA. *A necessary condition for a Lorentzian lattice L to be reflective is that, for all primitive isotropic vectors $c \in L$, the Euclidean lattice $c^\perp/\mathbb{Z}c$ is reflective.*

In particular, if L is of the form $L = \mathbb{H} \perp M$, $\mathbb{H} = (\mathbb{Z}^2, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right))$ the hyperbolic plane and M a positive definite lattice, then L is reflective only if M is reflective. (Take $c = (1,0) \in \mathbb{H}$ in Vinberg's lemma.) Now notice that a lattice of the form $\mathbb{H} \perp M$ of dimension ≥ 3 has only one class in its genus (since it is indefinite and has at least one two dimensional Jordan component at each prime; we refer for instance to [OM] for general facts about quadratic forms). Thus $\mathbb{H} \perp M$ only depends on the genus $\mathcal{G}(M)$, and Vinberg's lemma automatically sharpens to the following statement:

1.3. LEMMA. *If a lattice $L = \mathbb{H} \perp M$, where M is positive definite of rank at least 2 is reflective, then the genus $\mathcal{G}(M)$ (which only depends on L) is* **totally reflective** *in the sense that every lattice $M' \in \mathcal{G}(M)$ is reflective.*

It is true under quite general circumstances that L of signature $(n,1)$ is of the shape $\mathbb{H} \perp M$. In particular, this holds if $n \geq 4$ and L is **strongly square free** in the following sense: The exponent of $L^\#/L$ is square free (we say that L itself is **square free** for short), and the p-exponent of $\det L$ is at most half the dimension of L, for all p. In terms of Jordan decompositions, this means that for each p, the localized lattice has only a unimodular and a p-modular component $L_{0,p}$ resp. $L_{1,p}$, and $\dim(L_{1,p}) \leq \dim(L_{0,p})$. It is well known that to any lattice M (of whatever signature), one can associate a strongly square free lattice $\widetilde{M}$ (on the same space, but possibly scaling the quadratic form) such that $O(M) \subseteq O(\widetilde{M})$. In particular, if M is reflective, then $\widetilde{M}$ is reflective. The genus of $\widetilde{M}$ only depends on the genus of M, and (in the positive definite case) the mapping $M \mapsto \widetilde{M}$ induces a surjection of genera. This technique has been used by many people and goes back at least to Watson [Wa]. The construction of $\widetilde{M}$ breaks into two parts. One first makes the lattice square free by (iterated) application of the substitution $M \mapsto p^{-1}(M \cap p^2 M^\#) + M$, for the prime divisors p of $\det M$; then one applies, if necessary, the "local dualizing" operation $M \mapsto D_p M := {}^p(M^\# \cap p^{-1}M)$ to interchange the unimodular and the p-modular component of a Jordan decomposition.

The following theorem is an immediate consequence of an unpublished result of J. Biermann [Bie].

1.4. THEOREM. *There are only finitely many totally reflective genera of positive definite lattices of dimension ≥ 3.*

Proof: It is well known and easy to prove that any genus (w.l.o.g. strongly square free) of large enough dimension $n \geq n_0$ contains a non-reflective lattice. (It suffices to embed a lower-dimensional non-reflective lattice M_0 as an orthogonal summand; for $n_0 = 57$, the Leech lattice always works.) For

lattices of fixed dimension $n \geq 3$, the main result of [Bie] says that any genus of sufficiently large determinant contains a lattice with trivial automorphism group which *a fortiori* is non-reflective. □

Remark 1. The result of Biermann's we have just referred to depends on the mass formula as well as on various algebraic reduction techniques and requires a long and complicated proof. Only a part of the arguments is actually needed if one only wants to prove the existence of a non-reflective lattice in a genus. In the case of signature $(4,1)$, we shall come back to this question in Section 3 below.

Remark 2. The first good upper bound $n_0 = 30$ has been given (implicitly) by Vinberg [Vi4], §4. Recently F. Esselmann [Es] proved that 20 is the precise value of the largest dimension of totally reflective genera, and $n = 21$ is the largest value for which a reflective lattice of signature $(n,1)$ exists; R. Borcherds had proved already several years ago that the unique even lattice of this signature and determinant 4 is reflective; [Bor], §8, Example 5.

We now observe that Theorem 1.4 together with Vinberg's lemma gives a new and –modulo the use of Biermann's result– very short proof of the following finiteness result for arithmetic hyperbolic reflection groups due to V.V. Nikulin.

1.5. COROLLARY. *There are only finitely many strongly square free reflective lattices of signature* $(n,1)$, $n \geq 4$.

This is a special case of [Ni], Theorem 5.2.1. The result holds without the assumption that the lattices should be strongly square free. (Of course one must then restrict to primitive lattices.) In fact, for Nikulin's proof it is irrelevant whether or not they are. In the above proof, one could avoid the assumption with some additional technical effort. More important is that Nikulin proves the result also for $n = 2, 3$ where our method completely breaks down for the following trivial reason: If $L = \mathbb{H} \perp M$ is strongly square free of dimension 3 or 4, then M is not necessarily primitive but can be scaled by an arbitrary square free factor, of course without affecting the reflectiveness.

Nikulin's proof of the finiteness result is geometrical, dealing with combinatorial and metrical properties of the fundamental polytopes of hyperbolic reflection groups. It also applies to lattices (with the appropriate signatures) over number fields. However, it gives only poor bounds on the discriminants of reflective lattices and apparently no other arithmetical restrictions. .

2. Normal forms for lattices

Apart from Vinberg's basic general work and Nikulin's fundamental finiteness result, the existing literature on hyperbolic reflection groups and reflective lattices deals mainly with examples. Complete classifications have been obtained only under very restrictive assumptions (e.g. for unimodular lattices [Vi3]). In this and the next section we want to show that our knowledge of reflective Lorentzian lattices can be considerably improved by making a systematic use of the arithmetic theory of integral quadratic forms. In this article, we shall restrict ourselves to the (hyperbolic) dimensions $n = 3, 4$. If $n = 3$, we shall only treat the case of isotropic forms, where $H^n/W(L)$ is non-compact. A third general condition is that we require the groups $W(L)$ to be maximal among groups of this kind. Under these assumptions, we now want to give certain normal forms for our lattices. (The term "normal form" is not to be understood in a completely rigorous sense.) The main ingredient of these normal forms will be a fact which was already mentioned above: we can assume the lattices to be strongly square free, and if the unimodular and the p-modular component have the same dimension, for some prime p, then we can interchange them by the operation D_p not affecting the group.

We first deal with the case $n = 3$. Here we shall drop the assumption of square freeness in certain cases for the benefit of dealing only with even lattices, i.e. $(v, v) \in 2\mathbb{Z}$ for all $v \in L$. The quadratic form on $\mathbb{Z}^4$ in the following proposition is $f(v) = (v, v)/2$, not (v, v). A left upper index means scaling the quadratic form.

2.1. PROPOSITION. *If L is a lattice of signature $(3,1)$ with $O(L)$ maximal, then we may assume that L has the shape $L = \mathbb{H} \perp {}^s[a,b,c]$, where $\mathbb{H}$ denotes the hyperbolic plane $(\mathbb{Z}^2, xy)$, ${}^s[a,b,c]$ the binary lattice $(\mathbb{Z}^2,\ s(az^2 + bzw + cw^2))$, the discriminant $-D_0 = -(4ac - b^2)$ of $[a,b,c]$ is a fundamental discriminant (discriminant of a quadratic field), and s is a square free natural number relatively prime to D_0.*

Proof: We may start with an L which is strongly square free. The main aim of the proof is to embed the hyperbolic plane $\mathbb{H}$ into L (after possibly replacing L by a lattice with the same or a larger group). Once this is proved, the precise shape as given in the proposition will be obvious from the fact that L is strongly square free or equal to the even sublattice $L^\circ = \{x \in L \mid (x, x) \in 2\mathbb{Z}\}$ of a strongly square free lattice. It is sufficient to embed $\mathbb{H}$ locally for all primes p. Choose a Jordan decomposition $\mathbb{Z}_p L = L_0 \perp^p L_1$, L_0, L_1 unimodular. First consider the case $p \neq 2$. If $\dim L_0 \geq 3$, it is clear that $\mathbb{H}$ embeds into L_0. If $\dim L_0 = \dim L_1 = 2$, then one of L_0, L_1 is isotropic, since $L_0 \perp^p L_1 = L$ is isotropic. After possibly interchanging L_0 and L_1, we may assume that

$L_0 \cong \mathbb{H}$.

Now we consider the case $p = 2$. There are various cases according to the dimensions and the parity even/odd of L_0, L_1. In some cases, we pass from L to the even sublattice $L^\circ = \{x \in L \mid (x,x) \in 2\mathbb{Z}_2\}$. We give the details only in the case where $\dim L_0 = \dim L_1 = 2$. If L_0, L_1 are both even, then the same proof as for $p \neq 2$ applies. If one of them is even and the other odd, then we may assume that L_0 is even and L_1 is odd, that is, L_1 is a diagonal form $\langle a, b\rangle$, a, b odd. We claim that the Jordan decomposition can be chosen such that $L_0 \cong \mathbb{H}$. Indeed, if $L_0 \ncong \mathbb{H}$, then $L_0 \cong A_2$, the A_2-root-lattice with quadratic form [1,1,1]. But since A_2 over $\mathbb{Z}_2$ represents primitively any odd number, in particular $-a$, it is clear that already $A_2 \perp \langle 2a\rangle$ contains a primitive isotropic vector and thus splits off a hyperbolic plane. (In fact $A_2 \perp \langle 2a\rangle \cong \mathbb{H} \perp \langle 2(a+4)\rangle$.) If finally L_0, L_1 are both odd, then we may pass to the even sublattice L°, which is of the shape ${}^2M$, for M odd, unimodular and thus can be replaced by the odd unimodular lattice M. □

For the signature $(4,1)$, we have chosen the following normal form which, for reasons to be explained later, restricts the positive definite ternary constituent to a determinant not divisible by 4.

2.2. PROPOSITION. *If L is a lattice of signature $(4,1)$ with $O(L)$ maximal, then we may assume that L has the shape $L = \mathbb{H} \perp M$ or ${}^2\mathbb{H} \perp M$, where M is obtained from a ternary lattice $\widetilde{M}$ of square free determinant d which is odd in the case ${}^2\mathbb{H}$, by applying the dualizing operators D_p for some set of odd prime divisors $p \mid d$.*

Proof: First notice that the condition on M just means that M is primitive and square free (not necessarily strongly square free) and of determinant not divisible by 4, resp. odd determinant. We have chosen the formulation with the D_p to emphasize that we have essentially only to deal with square free determinants. The proof amounts to showing that L which we assume to be strongly square free splits off $\mathbb{H}$ if $4 \nmid \det L$ and splits off ${}^2\mathbb{H}$ if $4 \mid \det L$. This must be shown locally for each p. The claim is obvious for $p \neq 2$ since the unimodular Jordan component is of dimension at least 3 and therefore isotropic.

Now consider the case $p = 2$ and assume first that $4 \nmid \det L$. Let v be a primitive isotropic vector; it exists because $\dim L = 5$. Then $(L, v) = \mathbb{Z}_2$ or $2\mathbb{Z}_2$, since L is square free; $2\mathbb{Z}_2$ is impossible since the 2-modular Jordan component is at most one-dimensional and thus is anisotropic. Therefore, L splits off $\mathbb{H}$ or $\langle -1, 1\rangle$. We have to show that the case $\langle -1, 1\rangle$ can be reduced to the case $\mathbb{H}$. The only situation where there could be a problem occurs when L is odd, of the form $\langle -1, 1\rangle \perp M$ for an even lattice M. Over $\mathbb{Z}_2$, the

lattice M is of the shape $B \perp \langle 2a \rangle$, where a is an odd number and the binary lattice is $\mathbb{H}$ or A_2, the unique anisotropic binary even unimodular lattice over $\mathbb{Z}_2$. We have already observed in the proof of 2.1 that in this situation we can always assume that $B = \mathbb{H}$, (i.e. M is isotropic over $\mathbb{Z}_2$). But then it is clear that we can replace M locally and hence also globally by an odd lattice M' of the same determinant on the same space. The lattices $L = \langle -1, 1 \rangle \perp M$ and $L' := \mathbb{H} \perp M'$ are both odd, hence in the same genus and therefore isometric over $\mathbb{Z}$.

Now we treat the case where $4 \mid \det L$. We claim that there exists a primitive isotropic vector v with $(L, v) = 2\mathbb{Z}_2$. If not, such a vector satisfies $(L, v) = \mathbb{Z}_2$ and L, being odd, is locally of the shape $\langle -1, 1 \rangle \perp \langle a \rangle \perp {}^2B$ for a binary unimodular lattice B. The lattice $2\langle a \rangle \perp {}^2B \cong \langle 4a \rangle \perp {}^2B$ certainly represents primitively some number $4b$, b odd. But $\langle -1, 1 \rangle$ represents every odd number, in particular $-b$, and we finally arrive at a primitive isotropic vector $v \in 2L^{\#}$, as desired. We now know that L splits off either ${}^2\mathbb{H}$ or $\langle -2, 2 \rangle$ (and there is no choice for a given L, since the parity of a 2-modular Jordan component is unique). In the case $\langle -2, 2 \rangle$, we replace L first by $D_2 L$ which locally is of the form $\langle -1, 1 \rangle \perp {}^2M$ for some ternary unimodular M and then by the even sublattice $(D_2 L)^\circ$ which is ${}^2\mathbb{H} \perp {}^2M$. Scaling by $1/2$ we finally arrive at a unimodular lattice L' (which by the way carries the original, unscaled form) such that $O(L) \subseteq O(L')$. Thus we may remove L from the list of lattices to be considered. We want to remark that in fact $O(L) \neq O(L')$ and thus $O(L)$ is not maximal and eliminating L in this case is not only a matter of normalization. To verify the last claim one equivalently shows that $O(D_2 L) \subset O((D_2 L)^\circ)$ (proper inclusion). To see this, one checks that $(D_2 L)^\circ$ has further odd integral over-lattices (in addition to $D_2 L$ itself) and these are necessarily permuted transitively by $O(L)$. □

3. On the classification of reflective Lorentzian lattices in dimensions 3 and 4

The following proposition considerably extends the list of hyperbolic reflection groups in dimensions 3 and 4 known previously. In particular, we have found quite a few new maximal groups.

3.1. PROPOSITION. *The* $49 + 42$ *quadratic lattices in tables* 1 *and* 2 *below are all reflective and give rise to maximal, pairwise non-conjugate arithmetic reflection groups on hyperbolic* 3*-space, resp.* 4*-space.*

More detailed information about the $49 + 42$ groups is given in [SW]. The data collected in that paper were obtained, on the basis of our normal forms, by implementing Vinberg's algorithm for finding fundamental roots on a computer; they in particular set in evidence that the lattices listed in our tables 1 and 2 really are reflective.

We do not prove here that the groups are maximal within this class of groups.

Table 1. Reflective lattices of signature $(3,1)$.

$L = \mathbb{H}\perp {}^s[a,b,c] = (\mathbb{Z}^4, f)$, where $f(v) = (v,v)/2 = x_0x_1 + s(ax_2^2 + bx_2x_3 + cx_3^2)$

$D = s^2(4ac - b^2)$ is the (negative of the) discriminant

r is the number of fundamental roots

No.	D	${}^s[a,b,c]$	r	No.	D	${}^s[a,b,c]$	r
1.	3	$[1,1,1]$	4	26.	72	${}^3[1,0,2]$	8
2.	4	$[1,0,1]$	4	27.	75	${}^5[1,1,1]$	6
3.	7	$[1,1,2]$	6	28.	84	$[1,0,21]$	11
4.	8	$[1,0,2]$	5	29.	84	$[3,0,7]$	8
5.	11	$[1,1,3]$	6	30.	84	$[5,4,5]$	11
6.	12	${}^2[1,1,1]$	4	31.	100	${}^5[1,0,1]$	6
7.	15	$[1,1,4]$	8	32.	120	$[1,0,30]$	11
8.	15	$[2,1,2]$	6	33.	120	$[2,0,15]$	14
9.	19	$[1,1,5]$	7	34.	120	$[3,0,10]$	13
10.	20	$[1,0,5]$	6	35.	120	$[5,0,6]$	14
11.	20	$[2,2,3]$	6	36.	132	$[1,0,33]$	15
12.	24	$[1,0,6]$	6	37.	140	${}^2[3,1,3]$	11
13.	24	$[2,0,3]$	6	38.	147	${}^7[1,1,1]$	6
14.	28	${}^2[1,1,2]$	8	39.	168	$[3,0,14]$	18
15.	35	$[3,1,3]$	8	40.	168	$[6,0,7]$	18
16.	36	${}^3[1,0,1]$	5	41.	180	${}^3[1,0,5]$	15
17.	39	$[1,1,10]$	10	42.	196	${}^7[1,0,1]$	9
18.	40	$[1,0,10]$	9	43.	200	${}^5[1,0,2]$	13
19.	40	$[2,0,5]$	7	44.	300	${}^{10}[1,1,1]$	7
20.	44	${}^2[1,1,3]$	7	45.	360	${}^3[1,0,10]$	20
21.	52	$[1,0,13]$	10	46.	360	${}^3[2,0,5]$	20
22.	56	$[1,0,14]$	9	47.	507	${}^{13}[1,1,1]$	12
23.	60	${}^2[1,1,4]$	10	48.	588	${}^{14}[1,1,1]$	12
24.	63	${}^3[1,1,2]$	10	49.	900	${}^{15}[1,0,1]$	18.
25.	68	$[1,0,17]$	13				

Table 2. Reflective lattices of signature $(4,1)$.

$\langle a_1, ..., a_r \rangle$ denotes a diagonal form

$\langle a_b c \rangle$ denotes the binary form $(v,v) = ax^2 + 2bxy + cy^2$

$-D$ is the determinant

r is the number of fundamental roots

No.	D	bilinear form	r
1.	1	$\mathbb{H}\perp\langle 1,1,1\rangle$	5
2.	3	$\mathbb{H}\perp\langle 1\rangle\perp\langle 2_1 2\rangle$	6
3.	3	$\mathbb{H}\perp\langle 1,1,3\rangle$	7
4.	4	$^2\mathbb{H}\perp\langle 1,1,1\rangle$	5
5.	5	$\mathbb{H}\perp\langle 1,1,5\rangle$	7
6.	5	$\mathbb{H}\perp\langle 1\rangle\perp\langle 2_1 3\rangle$	8
7.	6	$\mathbb{H}\perp\langle 1,1,6\rangle$	7
8.	6	$\mathbb{H}\perp\langle 2\rangle\perp\langle 2_1 2\rangle$	6
9.	7	$\mathbb{H}\perp\langle 1,1,7\rangle$	10
10.	9	$\mathbb{H}\perp\langle 3\rangle\perp\langle 2_1 2\rangle$	7
11.	9	$\mathbb{H}\perp\langle 1,3,3\rangle$	7
12.	11	$\mathbb{H}\perp\langle 1\rangle\perp\langle 2_1 6\rangle$	9
13.	12	$^2\mathbb{H}\perp\langle 1\rangle\perp\langle 2_1 2\rangle$	6
14.	14	$\mathbb{H}\perp\langle 1,2,7\rangle$	13
15.	14	$\mathbb{H}\perp\langle 2\rangle\perp\langle 2_1 4\rangle$	8
16.	15	$\mathbb{H}\perp\langle 3\rangle\perp\langle 2_1 3\rangle$	10
17.	15	$\mathbb{H}\perp\langle 1,3,5\rangle$	15
18.	15	$\mathbb{H}\perp\langle 1,1,15\rangle$	12
19.	15	$\mathbb{H}\perp\langle 5\rangle\perp\langle 2_1 2\rangle$	10
20.	18	$\mathbb{H}\perp\langle 2,3,3\rangle$	8
21.	18	$\mathbb{H}\perp\langle 6\rangle\perp\langle 2_1 2\rangle$	7
22.	20	$^2\mathbb{H}\perp\langle 1,1,5\rangle$	7
23.	21	$\mathbb{H}\perp\langle 7\rangle\perp\langle 2_1 2\rangle$	14
24.	21	$\mathbb{H}\perp\langle 1,3,7\rangle$	18
25.	25	$\mathbb{H}\perp\langle 1,5,5\rangle$	9
26.	25	$\mathbb{H}\perp\langle 5\rangle\perp\langle 2_1 3\rangle$	14
27.	30	$\mathbb{H}\perp\langle 1,2,15\rangle$	19
28.	30	$\mathbb{H}\perp\langle 2\rangle\perp\langle 2_1 8\rangle$	11
29.	30	$\mathbb{H}\perp\langle 10\rangle\perp\langle 2_1 2\rangle$	10
30.	36	$^2\mathbb{H}\perp\langle 3\rangle\perp\langle 2_1 2\rangle$	7
31.	42	$\mathbb{H}\perp\langle 14\rangle\perp\langle 2_1 2\rangle$	11
32.	45	$\mathbb{H}\perp\langle 15\rangle\perp\langle 2_1 2\rangle$	16
33.	45	$\mathbb{H}\perp\langle 3\rangle\perp\langle 2_1 8\rangle$	21
34.	60	$^2\mathbb{H}\perp\langle 3\rangle\perp\langle 2_1 3\rangle$	11
35.	60	$^2\mathbb{H}\perp\langle 5\rangle\perp\langle 2_1 2\rangle$	12
36.	75	$\mathbb{H}\perp\langle 1\rangle\perp\langle 10_5 10\rangle$	14
37.	75	$\mathbb{H}\perp\langle 1,5,15\rangle$	51
38.	84	$^2\mathbb{H}\perp\langle 7\rangle\perp\langle 2_1 2\rangle$	15
39.	100	$^2\mathbb{H}\perp\langle 1,5,5\rangle$	11
40.	150	$\mathbb{H}\perp\langle 10\rangle\perp\langle 2_1 8\rangle$	33
41.	180	$^2\mathbb{H}\perp\langle 15\rangle\perp\langle 2_1 2\rangle$	17
42.	300	$^2\mathbb{H}\perp\langle 1\rangle\perp^5\langle 2_1 2\rangle$	19

It is likely that our list of maximal (arithmetic, non-cocompact) reflection groups in dimensions 3 and 4 is complete. We now want to give a brief sketch of what we can prove so far in this direction. The complete determination of all reflective lattices (with maximal group, say) in some fixed dimension breaks up into two steps, which, although they are logically not strictly separate from each other, turn out to require quite different methods. In the first step one has to produce a finite (and not too large) list of lattices which one can show contains all the reflective lattices. In particular, this list of candidates should only contain lattices which satisfy the conclusion of Vinberg's lemma. In an intermediate step one applies Vinberg's algorithm to each lattice in

the list. This shows immediately (at least in principle, in small dimensions also in practice) that a number of the candidates from the list are indeed reflective. In a second step one must show that all remaining lattices are non-reflective. For this, Vinberg's algorithm can only give numerical evidence, but no proof. Of course, the task of the second step depends on how good, that is, how small the list from the first step was. One can hope that for larger dimensions, starting with about 10, any lattice satisfying the necessary condition of Vinberg's lemma is indeed reflective and thus the second step completely disappears.

We now have to treat the dimensions 3 and 4 separately. For $n = 3$ we do not say anything about the first step here except that it is of an essentially geometric nature; the arithmetic theory of quadratic forms does not seem to help much here. Vinberg's lemma does for $n = 3$ not even imply the finiteness of the number of reflective lattices: the number s ocurring in the normal form cannot be bounded. The solution of the second step is given for $n = 3$ by the theorem below which is a consequence of the following two propositions. We refer to the normal form and notation for the lattices as introduced in Proposition 2.1.

3.2. PROPOSITION. *If D_0 is odd or if $8 \nmid D_0$ and $f(v)$ is even, then any two roots v, v' such that $f(v) = f(v') > 0$ are conjugate under $O^+(L)$. In any case, there are at most two conjugacy classes of roots v for fixed $f(v) > 0$.*

This proposition which by the way is of obvious independent interest is proved along lines which are essentially known: using strong approximation, one reduces to the local case; the local situation has been studied for instance in [Kn,Tr]. A special case of 3.2 has been treated (with a different proof) in [EGM], Theorem 11.3.

3.3. PROPOSITION. *Each of the following conditions on the lattice L and the value q implies that two distinct fundamental roots v, v' s.th. $f(v) = f(v') = q$ are never conjugate under $W(L)$:*

i) $D_0 \neq 3$, *and there exists a prime number* $p \neq 2$ *such that* $p \mid q$, $p \mid D_0$.

ii) *There exists a prime number* $p \neq 2$ *such that* $p \mid q$, $p \mid s$, *and* $(\frac{3D_0}{p}) \neq 1$.

iii) $2 \mid q$, $2 \mid D_0$.

iv) $D_0 = 3$, $q \not\equiv s(3)$.

v) $D_0 = 4$, *there exists a prime number* $p \neq 2$ *such that* $p \mid q$, $p \equiv \pm 5\ (12)$.

The proof of this proposition combines arithmetical facts with properties of abstract, combinatorial Coxeter groups [Ti]. Detailed proofs of the last two results will appear elsewhere. The next theorem is an obvious consequence of the two previous propositions, taking into account the fact that the stabilizer

$A = A(L)$ in $O^+(L)$ of any fundamental domain for $W(L)$ is a complement to $W(L)$ in $O^+(L)$.

3.4. THEOREM. *Suppose that L and q satisfy one of the conditions stated in Proposition 3.3. Let $o(L,q) = 1,2$ be the number of orbits of $O^+(L)$ on roots v with $f(v) = q$. If L has more than $4 \cdot o(L,q)$ fundamental roots v with $f(v) = q$, then L is non-reflective.*

The number 4 in the last proposition is an upper bound for the order of A which comes from the fact that any rotation of order 3 or 4 in $O^+(L)$ is a product of two reflections in $O^+(L)$. This last result will also be published elsewhere; it was suggested by an unpublished result of Mennicke who treated rotations of order 3 for lattices $L = \mathbb{H}\perp[1,0,d]$, d square free. Modulo extensive use of a computer the trivial bound $|A| \leq 24$ is by the way sufficient for most applications of 3.4.

We now turn to dimension $n = 4$ and outline the first step of the general procedure, the compilation of a list of candidates containing lattices for all maximal groups. In all dimensions $n \geq 4$, this step relies basically on Vinberg's lemma and the finiteness of totally reflective genera (Theorem 1.4). The task is to give strong bounds on the determinant (even better: on the largest prime factor of the determinant) of totally reflective genera of dimension $m = n - 1$ which are square free and without essential loss of generality even strongly square free. For $n = 4$, the verification of the existence of at least one non-reflective lattice in almost every genus in question is facilitated by the following result.

3.5. LEMMA. *Let M be a ternary lattice of determinant not divisible by 4. If M is indecomposable, then M is even non-reflective.*

Recall that by Proposition 2.2 it is really sufficient to deal with lattices of determinant d with $4 \nmid d$, and even d square free. Lemma 3.5 is completely false for lattices of determinant divisible by 4. There is no reason to prove the lemma here; it is an immediate consequence (verifying case-by-case) of the full classification of all ternary reflective lattices in dimension 3 given in [BS]. The existence of indecomposable lattices in each genus of sufficiently large determinant is a consequence of the mass formula. The mass of the decomposable lattices is a sum of essentially binary masses which grows more slowly than the whole mass. The determination of an upper bound for the determinant of a "totally decomposable" genus finally amounts to comparing certain values of L-series. Once one has obtained such a bound, the determination of all totally reflective genera will reduce to checking all genera up to this bound by computer.

For the second step in the proof of the completeness of table 2, we use a method of Bugaenko [Bu]. If a lattice L obtained in the first step is such that Vinberg's algorithm appears not to stop, one tries to find involutionary symmetries $\sigma_1, ..., \sigma_m$, $m \geq 2$, between appropriate subsets of the set of fundamental roots, extending to the whole lattice L and to H^4, such that their common fixed point set in H^4 is empty. Then the group $S = \langle \sigma_1, ..., \sigma_m \rangle$ must be infinite. On the other hand, this group preserves a fundamental domain of $W(L)$ and thus injects into $O(L)/W(L)$. Thus, the lattice is non-reflective.

Acknowledgement. This work was partly supported by the Wissenschaft and Forschung Ministry of the State Government of Nordrhein–Westfalen.

Literature

[Bie] J. Biermann: Gitter mit kleiner Automorphismengruppe in Geschlechtern von $\mathbb{Z}$-Gittern mit positiv-definiter quadratischer Form. Dissertation, Göttingen 1981.

[BS] B. Blaschke and R. Scharlau: Reflective integral quadratic forms. In preparation.

[Bor] R. Borcherds: Automorphism Groups of Lorentzian Lattices. J. Algebra **111** (1987), 133–153.

[Bu] V.O. Bugaenko: Arithmetic crystallographic groups generated by reflections, and reflective hyperbolic lattices. Advances in Soviet Mathematics **8** (1992), 33–55.

[EGM] J. Elstrodt, F. Grunewald, and J. Mennicke: Discontinuous Groups on Three-dimensional Hyperbolic Space: Analytical Theory and Arithmetic Applications. Russian Math. Surveys **38** (1983), 137–168.

[Es] F. Esselmann: Über die maximale Dimension von Lorentz-Gittern mit coendlicher Spiegelungsgruppe. Universität Bielefeld, Sonderforschungsbereich 343, Preprint No. 1992 – 23.

[Kn] M. Kneser: Witts Satz für quadratische Formen über lokalen Ringen. Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse (1972), 195–203.

[Ni] V. V. Nikulin: On the Classification of Arithmetic Groups Generated by Reflections in Lobachevsky Spaces. Math. USSR Izvestija **18** (1982), 99–123.

[OM] O. T. O'Meara: *Introduction to quadratic Forms.* Springer Verlag, Berlin, Heidelberg, New York 1971.

[SW] R. Scharlau and C. Walhorn: Tables of hyperbolic reflection groups. Universität Bielefeld, Ergänzungsreihe des Sonderforschungsbereichs 343, Heft 1992 – 01.

[Ti] J. Tits: Le problème des mots dans les groupes de Coxeter. Istituto Nazionale die Alta Matematica, Symposia Mathematica **I** (1968), 175–185.

[Tr] A. Trojan: The Integral Extension of Isometries of Quadratic Forms over Local Fields. Canadian J. of Math. **18** (1966), 920–942.

[Vi1] E. B. Vinberg: Discrete Groups Generated by Reflections in Lobačevskiĭ Spaces. Math. USSR Sbornik **1** (1967), 429–444.

[Vi2] E. B. Vinberg: On Unimodular Integral Quadratic Forms. Functional Anal. Appl. **6** (1972), 24–31.

[Vi3] E. B. Vinberg: On Groups of Unit Elements of Certain Quadratic Forms. Math. USSR Sbornik **16** (1972), 17–35.

[Vi4] E. B. Vinberg: The Absence of Crystallographic Groups of Reflections in Lobachevsky Spaces of Large Dimension. Trans. Moscow Math. Soc. **47** (1985), 75–112.

[Wal] C. Walhorn: Reflektive Gitter der Signatur (4,1) und hyperbolische Spiegelungsgruppen. Diplom thesis, Bielefeld 1990.

[Wa] G. L. Watson: Transformations of a quadratic form which do not increase the class-number. Proc. London Math. Soc. **12** (1962), 577–587.

Rudolf Scharlau & Claudia Walhorn
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31
D–4800 Bielefeld 1
Germany

electronic mail:
scharlau@mathematik.uni-bielefeld.de

Astérisque

HIRONORI SHIGA

On the transcendency of the values of the modular function at algebraic points

Astérisque, tome 209 (1992), p. 293-305

<http://www.numdam.org/item?id=AST_1992__209__293_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

On the transcendency of the values of the modular function at algebraic points

Hironori SHIGA

Dedicated to Professor Toshio Nishino on his 60th birthday

In this note we study an abelian variety A defined over $\overline{\mathbf{Q}}$. We shall characterize the abelian variety of CM type by its property of periods. The obtained result brings the criterion for algebraicity of the values of the Siegel modular function at algebraic points and of other various modular functions.

Our result can be regarded as the extension of the well known algebraicity criterion (so called Schneider's theorem) for the value of the elliptic modular function (cf. Theorem A-0). The author wishes to express many thanks for valuable advices given by D. Bertrand, F. Beukers and J. Wolfart.

§1 Characterization of the abelian variety of CM type.

We use the following notations.

A: g-dimensional abelian variety defined over $\overline{\mathbf{Q}}$ with a polarization χ.

$End_0\, A = (End\, A) \otimes \mathbf{Q}$,

$\omega_1, \cdots, \omega_g$: a basis system of holomorphic 1-forms on A defined over $\overline{\mathbf{Q}}$,

$\gamma_1, \ldots, \gamma_{2g}$: a basis system of $H_1(A, \mathbf{Z})$,

$\mathfrak{S}_g$: the Siegel upper half space of degree g.

We may change the period matrix ${}^t(\Omega_2, \Omega_1)$ by $M\,{}^t(\Omega_2, \Omega_1)$ with a transformation M of $\mathrm{GL}(2g, \mathbf{Z})$. By this procedure we may suppose the polarization χ is given by a $2g \times 2g$ matrix

$$\begin{pmatrix} O & \Delta \\ -\Delta & O \end{pmatrix}$$

with a certain integral diagonal $g \times g$ matrix Δ. Concerning this polarization the period relation is expressed as

$$ {}^t\begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} \chi \begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} = O $$

$$ \sqrt{-1}\,{}^t\begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} \chi \begin{pmatrix}\bar{\Omega}_2\\ \bar{\Omega}_1\end{pmatrix} > 0. $$

Hence we obtain a point $\Omega = \Omega_2(\Delta\Omega_1)^{-1}$ of $\mathfrak{S}_g$. The modular group

$$ \Gamma = \mathrm{Sp}(2g, \mathbf{Z}, \Delta) = \{M \in M(2g, \mathbf{Z}) |\, {}^t g \chi g = \chi\} \tag{1.1} $$

acts on $\mathfrak{S}_g$ by

$$ M \circ \Omega = (A\Omega + B\Delta^{-1})(C\Omega + D\Delta^{-1})^{-1}\Delta^{-1}, \tag{1.2} $$

where $M = \begin{pmatrix}A & B\\ C & D\end{pmatrix} \in \mathrm{Sp}(2g, \mathbf{Z}, \Delta)$. In the following we regard the Γ-equivalence class represented by Ω as the reduced period matrix of A. Our main theorem is stated as the following.

Theorem M.

Let A be a g-dimensional polarized abelian variety defined over $\overline{\mathbf{Q}}$, and let Ω be the reduced period matrix of A. If Ω is an algebraic point of $\mathfrak{S}_g$, then A is an abelian variety of CM type.

We also have the following analogous result.

Theorem M'.

Let A be a g-dimensional polarized abelian variety defined over $\overline{\mathbf{Q}}$. Let ω_i and γ_j $(1 \le i \le 1, 1 \le j \le 2g)$ be as above. Suppose the ratio

$$ \frac{\int_{\gamma_i} \omega_k}{\int_{\gamma_j} \omega_k} $$

is an algebraic number for any indices i, j and k whenever the denominator does not vanish. Then A is an abelian variety of CM type.

Remark 1.1. A simple abelian variety A is said to be of CM type if $End_0 A$ is isomorphic to a certain number field of degree $2 \times \dim A$. When A is not simple, A is said to be of CM type if every simple component is of CM type.

Remark 1.2. When A is simple and defined over $\overline{\mathbf{Q}}$, the period $\int_{\gamma_i} \omega_k$ does not vanish for every i and k (cf. [W-W]).

Remark 1.3. Let Ω be a reduced period matrix of a polarized abelian variety (A, χ). The abelian variety A is of CM type if and only if Ω is an isolated fixed point of a certain element of $\mathrm{Sp}(2g, \mathbf{Q}, \Delta)$,(cf.[H-I]).

Proof of Theorem M. The following theorem, due to Wüstholz (cf. [Wü]), plays the essential role in our argument.

Theorem W. *Let A be an abelian variety defined over $\overline{\mathbf{Q}}$, and let $T_A \cong \mathbf{C}^g$ be its tangent space. Let* exp *be the exponential map from T_A to $A = \mathbf{C}^g/\Omega_2\mathbf{Z} + \Omega_1\mathbf{Z}$. Let W be a linear subspace of T_A defined over $\overline{\mathbf{Q}}$. If W contains a point $\vec{v}(\neq 0)$ with $\exp(\vec{v}) \in A(\overline{\mathbf{Q}})$, then there exists an algebraic subgroup G of A with the following properties:*

(i) G is defined over $\overline{\mathbf{Q}}$

(ii) the tangent space T_G is a subspace of W and contains $\vec{v}$

(iii) dim G *is positive*

We need the following lemma also.

Lemma 1.

Let A be a simple abelian variety over $\overline{\mathbf{Q}}$. Suppose $A \times A$ contains an algebraic subgroup H defined over $\overline{\mathbf{Q}}$. If we have dim $H =$ dim A *and $p_i(H) = A$ (p_i is the projection to the i-th component), then H determines an element of $End_0\, A$. Moreover H corresponds to a trivial endomorphism (namely the one identified with a rational number) if and only if the tangent space T_H of H is given by the form*

$$\{(\vec{z}, \vec{w}) \in \mathbf{C}^g \times \mathbf{C}^g | m\vec{z} = n\vec{w}\}$$

for certain integers m and n.

We proceed our argument in three steps:

(i) We reduce the problem to the simple case

(ii) $D = End_0\, A$ is a $2g$-dimensional vector space over $\mathbf{Q}$,

(iii) D is a commutative division algebra.

Step (i).

Let A and A' be polarized abelian varieties defined over $\overline{\mathbf{Q}}$. Let ${}^t(\Omega_2, \Omega_1)$ and ${}^t(\Omega_2', \Omega_1')$ be the period matrix of A and A', respectively. Let $\Omega(A)$ and $\Omega(A')$ be the reduced period matrix of A andA', respectively. Suppose these two abelian varieties are isogenous, and let φ be the isogeny from A and A'. Then φ is induced from a certain invertible linear transformation U of $\mathbf{C}^g$. Moreover this linear transformation induces a homomorphism of the lattices represented by the form

$$\begin{pmatrix} \Omega_2' \\ \Omega_1' \end{pmatrix} = M \begin{pmatrix} \Omega_2 \\ \Omega_1 \end{pmatrix} \tag{1.3}$$

for a certain element $M = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ of $M(2g, \mathbf{Z})$. By (1.1) we have

$$\Omega(A) = \Omega_2 \Delta (\Omega_1)^{-1}, \Omega(A') = \Omega_2' \Delta' {\Omega_1'}^{-1}, \tag{1.4}$$

where Δ and Δ' indicate the polarizations of A and A', respectively. Using (1.4) we obtain

$$\Omega(A') = (P\Omega(A) + Q)(R\Omega(A) + S)^{-1}\Delta'$$

Hence $\Omega(A')$ is an algebraic point of $\mathfrak{S}$ provided $\Omega(A)$ is an algebraic point of $\mathfrak{S}$. This argument shows that it is sufficient to study only the simple case.

Step (ii)

Let A be a simple abelian variety defined over $\overline{\mathbf{Q}}$. Suppose the reduced period matrix

$$\Omega(A) = (\lambda_{ij})_{1 \leq i,j \leq g}$$

is an algebraic point of $\mathfrak{S}$. Set

$$\begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix} = \begin{pmatrix} \int_{\gamma_{g+1}} \vec{\omega} \\ \cdot \\ \cdot \\ \cdot \\ \int_{\gamma_{2g}} \vec{\omega} \end{pmatrix}, \qquad \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix} = \begin{pmatrix} \int_{\gamma_1} \vec{\omega} \\ \cdot \\ \cdot \\ \cdot \\ \int_{\gamma_g} \vec{\omega} \end{pmatrix}.$$

Then we have $\Omega_1 = \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix}$ and $\Omega_2 = \begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix}$, hence it holds

$$\begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix} = \Omega \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix}. \tag{1.5}$$

Set

$$G = \underbrace{A \times \cdots \times A}_{2g \text{ times}},$$

and let $\vec{u}_i$ and $\vec{z}_i$ $(i = 1, \cdots, g)$ be the coordinate for the tangent space T_A of i-th and $g + i$ th component of G, respectively. We regard them as row vectors. We suppose the exponential map is given by the projection

$$\mathbf{C}^g \longrightarrow \mathbf{C}^g/\Omega_2\mathbf{Z}^g + \Omega_1\mathbf{Z}^g.$$

Set the linear subspace

$$W = \{(\vec{z}_1, \cdots \vec{z}_g, \vec{u}_1, \cdots \vec{u}_g) \Big| \begin{pmatrix} \vec{u}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{u}_g \end{pmatrix} = \Omega \begin{pmatrix} \vec{z}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{z}_g \end{pmatrix} \} \tag{1.6}$$

in $\mathbf{C}^{2g} = T_G$. It is a g^2-dimensional linear subspace. By (1.5) W contains a point

$$P_0 = (\vec{\alpha}_1, \cdots, \vec{\alpha}_g, \vec{\beta}_1, \cdots, \vec{\beta}_g).$$

Let us note that $\exp(P_0) = (0, \ldots, 0)$ in G, especially this is an algebraic point on G. By virtue of Theorem W we can find an algebraic subgroup H of G defined over $\overline{\mathbf{Q}}$. Also the tangent space T_H of H has the property:

$$P_0 \in T_H \subset W. \tag{*}$$

Set $h = \dim H$. Because A is simple the projection map p_i from G to the i-th component A is always surjective. By considering the following exact sequence

$$O \longrightarrow \ker p_i \longrightarrow H \xrightarrow{p_i} A \longrightarrow O$$

we know $\ker p_i$ is $(h - g)$-dimensional. By the iteration of this argument we know that $h = kg$ for a certain positive integer k.

Let π_k be the projection of T_H to the $(\vec{z}_1, \ldots, \vec{z}_k)$-space (the first k-components of T_G). After an appropriate change of order in $\vec{z}_1, \ldots, \vec{z}_g$, if necessary, it becomes surjective. Therefore T_H is represented by $g - k$ relations of the form

$$\begin{cases} \vec{z}_{k+1} = c_{1,k+1}\vec{z}_1 + \cdots + c_{k,k+1}\vec{z}_k \\ \qquad\qquad \cdots\cdots \\ \qquad\qquad \cdots\cdots \\ \qquad\qquad \cdots\cdots \\ \vec{z}_g = c_{1,g}\vec{z}_1 + \cdots + c_{k,g}\vec{z}_k \end{cases} \tag{1.7}$$

together with (1.6).

If we recall Lemma 1 we can show that every coefficient c_{ij} in (1.7) determines a $\mathbf{Q}$-endomorphism of A. Set $D = End_0 A$, it is an algebra over $\mathbf{Q}$. We claim that D is a $2g$-dimensional vector space over $\mathbf{Q}$. So we assume the contrary, namely

$$(**) \qquad \dim_{\mathbf{Q}} D \leq g$$

If it holds $k = g$, there is no relation of the form (1.7). By using Lemma 1 we can find every λ_{ij} belongs to D.

Then we obtain a number field of degree at most g by attaching λ_{ij}'s to $\mathbf{Q}$. According to the following Lemma 2 it contradicts the simpleness of A.

Lemma 2.

Let $\Omega = (\lambda_{ij})$ be an element of $\mathfrak{S}_g$. If every λ_{ij} belongs to a certain number field of degree at most g, then the corresponding abelian variety A is not simple.

Proof. By the assumption we can find the linear relation

$$(+) \qquad b_{i0} + b_{i1}\lambda_{i1} + \cdots + b_{ig}\lambda_{ig} = 0 \quad (i = 1, \ldots, g)$$

over $\mathbf{Q}$. By considering the transformation

$$I_{2g} + (E_{ij} - E_{g+j,g+i})$$

of $\mathrm{Sp}(g, \mathbf{Z})$ we can assume $b_{ii} \neq 0 \quad (i = 1, \ldots, g)$, where E_{ij} indicates the matrix element with the (i, j)-element is equal to 1.

Set

$$A_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & \cdots & b_{1g} \\ 0 & 1 & & & \\ & & \cdots & \cdots & 0 \\ 0 & & & & 1 \end{pmatrix},$$

$$B_1 = C_1 = O, D_1 = {}^t A_1^{-1}$$

and set

$$A_2 = D_2 = I_g, B_2 = b_{10}E_{11}, C_2 = O.$$

By putting

$$M_i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix},$$

we obtain two elements M_1 and M_2 of $\mathrm{Sp}(g, \mathbf{Q})$. Put

$$\Omega' = M_2 M_1(\Omega).$$

So we find

$$\begin{pmatrix} b_{10} + b_{11}\lambda_{11} + \ldots + b_{1g}\lambda_{1g} \\ \lambda_{2g} \\ \cdot \\ \cdot \\ \lambda_{gg} \end{pmatrix}$$

as the g-th column vector of Ω'. By (+) it means the $(1, g)$-element (and the $(g, 1)$-element) of Ω' is equal to 0. By the iteration of this procedure Ω is deformed to a matrix of $\mathfrak{S}_g$ with a direct sum decomposition. This contradicts the simpleness of A. q.e.d.

Next we suppose $k = g - 1$. In this case we get one relation of the form (1.7):

$$\vec{z}_g = c_1\vec{z}_1 + \cdots + c_{g-1}\vec{z}_{g-1} \tag{1.7'}$$

$c_i \in D$. By substituting it in (1.6) we obtain

$$\begin{cases} \vec{u}_1 = (\lambda_{11} + c_1\lambda_{1g})\vec{z}_1 + \cdots + (\lambda_{1,g-1} + c_{g-1}\lambda_{1,g})\vec{z}_{g-1} \\ \cdots \\ \vec{u}_g = (\lambda_{g1} + c_1\lambda_{gg})\vec{z}_1 + \cdots + (\lambda_{g,g-1} + c_{g-1}\lambda_{g,g})\vec{z}_{g-1} \end{cases} \tag{1.8}$$

The coefficients in (1.8) are also $\mathbf{Q}$-endomorphisms. Namely every $\lambda_{ij} + c_j\lambda_{ig}$ belongs to D. By using the fact $\lambda_{ij} = \lambda_{ji}$ we know that every λ_{ij} is contained in the D-module $D \oplus \lambda_{gg}D$. On the other hand we have a certain $\mathbf{Q}$-linear relation

$$b_0 + b_1(\lambda_{11} + c_1\lambda_{1g}) + \cdots + b_g(\lambda_{g1} + c_1\lambda_{gg}) = 0$$

between $g + 1$ endomorphisms

$$1, \lambda_{11} + c_1\lambda_{1g}, \ldots, \lambda_{g1} + c_1\lambda_{gg},$$

for we assumed (**). Therefore λ_{gg} itself belongs to D. So we find that every λ_{ij} is also an element of D. Hence it occurs a linear relation of the form (+) over $\mathbf{Q}$ between

$$1, \lambda_{11}, \ldots, \lambda_{1g}.$$

It is a contradiction again.

Even for the case $k \leq g-2$ we can proceed this argument.

Step (iii). By the same argument in Step (ii) we can find every λ_{ij} belongs to D, and they constitute a generator system of D. So the commutativity is obvious. q.e.d.

§2. Applications.

0) Transcendency of $j(\tau)$.

We have a new proof of the following well-known fact.

Theorem A-0. *Let $j(\tau)$ be the elliptic modular function. Suppose $\tau \in \overline{\mathbf{Q}}$, then $j(\tau)$ is an algebraic number if and only if τ is an imaginary quadratic number.*

Proof.

If part is the conclusion from the classical complex multiplication theory. Only if part is immediate from Theorem M for $g=1$. q.e.d.

1) The transcendency of the Igusa-Rosenhain modular mapping on $\mathfrak{S}_2$.

Let $\lambda : \mathfrak{S}_2 \longrightarrow \mathbf{P}^3$ be the Igusa-Rosenhain modular mapping defined by

$$\lambda(\Omega) = [\xi_0, \cdots, \xi_3]$$

$$= [\vartheta^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \vartheta^2 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \vartheta^2 \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

$$\vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}],$$

where the thetas indicate the Jacobi theta constants (cf. [I]). It is a modular mapping with respect to $\Gamma(2)$, the principal congruence subgroup of $\mathrm{Sp}(2, \mathbf{Z})$ with level 2. Moreover λ gives a birational correspondence between $\mathfrak{S}_2/\Gamma(2)$ and $\mathbf{P}^2$.

Theorem A-1. *Suppose Ω is an algebraic point of $\mathfrak{S}_2$, then $\lambda(\Omega)$ is an algebraic point of $\mathbf{P}^3$ if and only if Ω is a CM-point.*

Remark 2.1. The mapping λ is the inverse of the period mapping for the family of the curves of genus 2 given by the Legendre normal form

$$C(\xi) : y^2 = x \prod_{i=0}^{3} (x - \xi_i),$$

where $[\xi_0, \cdots, \xi_3]$ is a parameter on $\mathbf{P}^3$.

Proof of Theorem A-1.

If part is the consequence of the complex multiplication theory (cf. [S-T]), so we consider only if part. Let $A = Jac(C)$ be the jacobian variety of $C(\xi)$. By the assumption $C(\xi)$ is defined over $\overline{\mathbf{Q}}$. So A is also defined over $\overline{\mathbf{Q}}$. According to Theorem M A must be of CM type. Recalling Remark 1.3 we know the period $\Omega(A)$ is a CM point of $\mathfrak{S}_2$. q.e.d.

2) The Picard modular mapping.

We use the following notations in this argument.

$\zeta = \exp(2\pi i/3)$, $K = \mathbf{Q}(\zeta)$, $\mathcal{O}_K = \mathbf{Z} \bigoplus \mathbf{Z}\zeta$,

$$H = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let D be the domain defined by

$$D = \{\eta \in \mathbf{P}^2(\mathbf{C}) : {}^t\bar{\eta} H \eta < 0\} = \{(u, v) \in \mathbf{C}^2 : 2\,\Re v + |u|^2 < 0\}$$

(by putting $v = \eta_1/\eta_0, u = \eta_2/\eta_0$), this is biholomorphically equivalent to the 2 dimensional hyperball. Let Γ be the modular group defined by

$$\Gamma = U(H, \mathcal{O}_K) = \{g \in M(3, \mathcal{O}_K) : {}^t\bar{g} H g = H\}.$$

We also consider the modular group with the level structure by $\sqrt{-3}$

$$\Gamma(\sqrt{-3}) = \{g \in \Gamma : g \equiv 1_3 \mod (\sqrt{-3})\}.$$

Set

$$\Omega = \Omega(u, v)$$

$$= \begin{pmatrix} (u^2 + 2\omega^2 v)/(1-\omega) & \omega^2 u & (\omega u^2 - \omega^2 v)/(1-\omega) \\ \omega^2 u & -\omega^2 & u \\ (\omega u^2 - \omega^2 v)/(1-\omega) & u & (u^2 + 2v)/(\omega - \omega^2) \end{pmatrix}.$$

This Ω gives an embedding of D into $\mathfrak{S}_3$. Using above notations we define the mapping $\lambda : D \longrightarrow \mathbf{P}^2$ by $\lambda(u, v) = [\xi_0, \xi_1, \xi_2] =$

$$[\vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ 0 & \frac{1}{6} & 0 \end{bmatrix}(\Omega), \vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{3} \end{bmatrix}(\Omega), \vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ \frac{2}{3} & \frac{1}{6} & \frac{2}{3} \end{bmatrix}(\Omega)].$$

Remark 2.2. The mapping λ is the inverse of the period mapping for the following family of algebraic curves of genus 3 (cf. [S])

$$C(\xi) : y^3 = x\prod_{i=0}^{2}(x-\xi_i),$$

where $[\xi_i]$ is a parameter in

$$\mathbf{P}^2 - \{\prod_{i=0}^{2}\xi_i \prod_{j,k=0}^{2}(\xi_j - \xi_k) \neq 0\}.$$

Moreover λ induces the biholomorphic correspondence between the compactification of $D/\Gamma(\sqrt{-3})$ and $\mathbf{P}^2$.

Theorem A-2. *Suppose the point $P = (u, v)$ varies on the algebraic points of D. Then $\lambda(u, v)$ is an algebraic point if and only if P is an isolated fixed point of an element in*

$$U(H, K) = \{g \in M(3, K) : {}^t\bar{g}Hg = H\}.$$

Proof. We can obtain the above conclusion by the similar argument as 1).
q.e.d.

3) The inverse of the Schwarz function for the Gauss hypergeometric differential equation.

Let $F(\alpha, \beta, \gamma)$ be the Gauss hypergeometric function and $D(\alpha, \beta, \gamma)$ be the corresponding hypergeometric differential equation:

$$x(x-1)y'' + \{\gamma + (1+\alpha+\beta)x\}y' - \alpha\beta y = 0 \tag{2.1}$$

Always the parameters α, β and γ are supposed to be rational numbers. Set

$$\lambda = 1-\gamma, \quad \mu = \beta - \alpha, \quad \nu = \gamma - \alpha - \beta$$

Let N be the least common multiplier of the denominators of α, β and γ. Put

$$1-\alpha = A/N, \quad \alpha + 1 - \gamma = B/N, \quad \beta = C/N$$

We assume the following condition for λ, μ and ν

$$\begin{cases} 1/\lambda,\ 1/\mu,\ 1/\nu \in \mathbf{Z} \cup \{0\}, \\ |\lambda| + |\mu| + |\nu| < 1. \end{cases} \tag{2.2}$$

Set

$$I(\infty, z) = \Gamma(\gamma)\{\Gamma(\alpha)\Gamma(\beta)\}^{-1} \int_0^\infty x^{\alpha-1}(1-x)^{\gamma-\alpha-1}(1-zx)^{-\beta}dx \tag{2.3}$$

$$I(1, z) = \Gamma(\gamma)\{\Gamma(\alpha)\Gamma(\beta)\}^{-1} \int_0^1 x^{\alpha-1}(1-x)^{\gamma-\alpha-1}(1-zx)^{-\beta}dx. \tag{2.3'}$$

Under the condition (2.2) $I(\infty, z)$ and $I(1, z)$ are independent solutions of (2.1). Moreover the Schwarz function

$$\sigma(z) = I(\infty, z)/I(1, z)$$

has a single valued inverse function, say $\lambda(\tau)$, defined on a bounded domain D (namely it is biholomorphically equivalent to the upper half plane H).

Here we use the notations according to [Wo]. The hypergeometric function $F(\alpha, \beta, \gamma : z) = I(\infty, z)$ can be considered as a period integral on the algebraic curve

$$X(N, z) : y^N = x^A(1-x)^B(1-zx)C.$$

Let us denote its Jacobian variety by $Jac(X(N, z))$. Set

S= the system of linearly independent differential forms of the form $\omega_n = \frac{P(x)dx}{y^n}$ for a certain positive integer n.

Then we have $r = \sharp S = \varphi(N)$. So we put $S = \{\omega^{(1)}, \cdots, \omega^{(r)}\}$ and $\omega^{(i)} = \omega_{n_i}$.

Let ζ be the primitive N-th root of unity, and set $K = \mathbf{Q}(\zeta)$. We obtain a lattice Λ in $\mathbf{C}^r$ by putting

$$\Lambda = \{(\rho_i(a) \int_0^1 \omega^{(i)} + \rho_i(b) \int_0^\infty \omega^{(i)})_{1 \le i \le r} : a, b \in \mathcal{O}_K\},$$

where $\mathcal{O}_K$ is the ring of integers in K and ρ_i is the automorphism of K with $\rho_i(\zeta) = \zeta^{n_i}$. Then we obtain an abelian variety $T = \mathbf{C}^r/\Lambda$. According to Wolfart $Jac(X(N, z))$ is isogenous to

$$T \oplus \sum_{D|N, D \neq N} Jac(X(D, z)).$$

Theorem A-3. *Suppose τ is algebraic. Then $\lambda(\tau)$ is an algebraic number if and only if T is an abelian variety of CM type.*

Proof.

i) The case T is simple. Let us consider $G = T \times T$. In the tangent space $T_G \cong \mathbf{C}^r \times \mathbf{C}^r$ of G we define the linear subspace

$$W = \{(\vec{z}, \vec{w}) \in \mathbf{C}^r \times \mathbf{C}^r : z_1 \int_0^\infty \omega_1 = w_1 \int_0^1 \omega_1\}$$

We have a natural action of the cyclotomic field $\mathbf{Q}(\zeta)$, where ζ indicates the N-th primitive root of unity, on the lattice Λ. Therefore $End_0 T$ contains the algebraic number field $\mathbf{Q}(\zeta)$ of degree $r = \phi(N) = \dim T$. So it is sufficient to show that $End_0 T$ contains a $\mathbf{Q}$-endomorphism which is not contained in $\mathbf{Q}(\zeta)$.

The subspace W contains a point

$$P_0 = (\vec{z}, \vec{w}) = \begin{pmatrix} \int_0^1 \omega_1 & \int_0^\infty \omega_1 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \int_0^1 \omega_r & \int_0^\infty \omega_r \end{pmatrix}$$

which is sent to $0 \in G(\overline{\mathbf{Q}})$ by the exponential map. According to Theorem W there exists an algebraic subgroup H satisfying the three conditions in the statement. Because T is simple H must be r-dimensional. Obviously H does not coincide with the component of T. By Lemma 1 we can find a $\mathbf{Q}$-endomorphism, say σ.

Suppose σ is contained in $\mathbf{Q}(\zeta)$. On multiplying by a certain integer, σ can be supposed to lie in the ring of integers of $\mathbf{Q}(\zeta)$. By the definition of the lattice Λ the endomorphism σ carries the vector $\int_0^1 \vec{\omega}$ to a certain $\mathbf{Z}$-linear combination of

$$\alpha_1 \int_0^1 \vec{\omega}, \ldots, \alpha_r \int_0^1 \vec{\omega}$$

where $\{\alpha_1, \ldots, \alpha_r\}$ is the generator system of the ring of integers. On the other hand if we examine the construction of σ, it carries the vector $\int_0^1 \vec{\omega}$ to $\int_0^\infty \vec{\omega}$. This is a contradiction.

ii) The case T is not simple.

Suppose we have the decomposition $T = A_1 \times \cdots \times A_k$, where every A_i is the same simple abelian variety A. By the same arguments as in i) also in this

case we have a certain subvariety H in $G = T \times T$. If we restrict it to a certain product $A_i \times A_j$ in $T \times T$, we can find a $\mathbf{Q}$-endomorphism σ of $End_0 A$. So we can proceed the same discussion as the first case.

q.e.d.

REFERENCES

[B] Bertrand, D., *Lemme de zéros et nombres transcendants*, Seminaire Bourbaki, (1985-86).

[B-W] Beukers, F., Wolfart, J., *Algebraic values of hypergeometric functions*, Proceedings of Durham conference on transcendental numbers 1986.

[H-I] Hashimoto, K., Ibukiyama, T., *On class numbers of positive definite binary quaternion hermitian forms*, J. Fac. Sci. Univ. Tokyo **27** (1980), 549-601.

[I] Igusa, J., *On Siegel Modular forms of genus two*, Amer. J. Math. **84** (1962), 175-200.

[Mo] Morita, Y., *On transcendency of special values of arithmetic automorphic functions*, J. Math. Soc. Japan **24** (1972), 268-274.

[Mu] Mumford, D., *Tata lectures on theta I.*

[S-T] Shimura, G., Taniyama, Y., *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. Japan (1975).

[S] Shiga, H., *On the representation of the Picard modular function by theta constants I-II*, Pub. Research Inst. Kyoto Univ. **24** (1988), 311-360.

[T] Takeuchi, K., *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), 600-612.

[W-W] Wolfart, J., Wüstholz, G., *Der Überlangerungsradius gewisser algebraischer Kurven und die Werte der Betafunktion an rationalen Stellen*, Math. Ann. **273** (1985), 1-15.

[Wo] Wolfart, J., *Werte Hypergeometrischer Funktionen*, Inv. Math. **92** (1988), 187-216.

[Wü] Wüstholz, G., *Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen*, Ann. Math. (1989), 501-517.

Hironori Shiga
Department of Mathematics,
Chiba University
Yayoi-cho 1–33,
Chiba-City, Japan

Astérisque

HIRONORI SHIGA

On the transcendency of the values of the modular function at algebraic points

Astérisque, tome 209 (1992), p. 293-305

<http://www.numdam.org/item?id=AST_1992__209__293_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

On the transcendency of the values of the modular function at algebraic points

Hironori SHIGA

Dedicated to Professor Toshio Nishino on his 60th birthday

In this note we study an abelian variety A defined over $\overline{\mathbf{Q}}$. We shall characterize the abelian variety of CM type by its property of periods. The obtained result brings the criterion for algebraicity of the values of the Siegel modular function at algebraic points and of other various modular functions.

Our result can be regarded as the extension of the well known algebraicity criterion (so called Schneider's theorem) for the value of the elliptic modular function (cf. Theorem A-0). The author wishes to express many thanks for valuable advices given by D. Bertrand, F. Beukers and J. Wolfart.

§1 Characterization of the abelian variety of CM type.

We use the following notations.

A: g-dimensional abelian variety defined over $\overline{\mathbf{Q}}$ with a polarization χ.

$End_0\, A = (End\, A) \otimes \mathbf{Q}$,

$\omega_1, \cdots, \omega_g$: a basis system of holomorphic 1-forms on A defined over $\overline{\mathbf{Q}}$,

$\gamma_1, \ldots, \gamma_{2g}$: a basis system of $H_1(A, \mathbf{Z})$,

$\mathfrak{S}_g$: the Siegel upper half space of degree g.

We may change the period matrix ${}^t(\Omega_2, \Omega_1)$ by $M\,{}^t(\Omega_2, \Omega_1)$ with a transformation M of $\mathrm{GL}(2g, \mathbf{Z})$. By this procedure we may suppose the polarization χ is given by a $2g \times 2g$ matrix

$$\begin{pmatrix} O & \Delta \\ -\Delta & O \end{pmatrix}$$

with a certain integral diagonal $g \times g$ matrix Δ. Concerning this polarization the period relation is expressed as

$$ {}^t\begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} \chi \begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} = O $$

$$ \sqrt{-1}\,{}^t\begin{pmatrix}\Omega_2\\ \Omega_1\end{pmatrix} \chi \begin{pmatrix}\bar{\Omega}_2\\ \bar{\Omega}_1\end{pmatrix} > 0. $$

Hence we obtain a point $\Omega = \Omega_2(\Delta\Omega_1)^{-1}$ of $\mathfrak{S}_g$. The modular group

$$ \Gamma = \mathrm{Sp}(2g, \mathbf{Z}, \Delta) = \{M \in M(2g, \mathbf{Z}) |\, {}^t g \chi g = \chi\} \tag{1.1} $$

acts on $\mathfrak{S}_g$ by

$$ M \circ \Omega = (A\Omega + B\Delta^{-1})(C\Omega + D\Delta^{-1})^{-1}\Delta^{-1}, \tag{1.2} $$

where $M = \begin{pmatrix}A & B\\ C & D\end{pmatrix} \in \mathrm{Sp}(2g, \mathbf{Z}, \Delta)$. In the following we regard the Γ-equivalence class represented by Ω as the reduced period matrix of A. Our main theorem is stated as the following.

Theorem M.

Let A be a g-dimensional polarized abelian variety defined over $\overline{\mathbf{Q}}$, and let Ω be the reduced period matrix of A. If Ω is an algebraic point of $\mathfrak{S}_g$, then A is an abelian variety of CM type.

We also have the following analogous result.

Theorem M'.

Let A be a g-dimensional polarized abelian variety defined over $\overline{\mathbf{Q}}$. Let ω_i and γ_j $(1 \le i \le 1, 1 \le j \le 2g)$ be as above. Suppose the ratio

$$ \frac{\int_{\gamma_i} \omega_k}{\int_{\gamma_j} \omega_k} $$

is an algebraic number for any indices i, j and k whenever the denominator does not vanish. Then A is an abelian variety of CM type.

Remark 1.1. A simple abelian variety A is said to be of CM type if $End_0 A$ is isomorphic to a certain number field of degree $2 \times \dim A$. When A is not simple, A is said to be of CM type if every simple component is of CM type.

Remark 1.2. When A is simple and defined over $\overline{\mathbf{Q}}$, the period $\int_{\gamma_i} \omega_k$ does not vanish for every i and k (cf. [W-W]).

Remark 1.3. Let Ω be a reduced period matrix of a polarized abelian variety (A, χ). The abelian variety A is of CM type if and only if Ω is an isolated fixed point of a certain element of $\mathrm{Sp}(2g, \mathbf{Q}, \Delta)$,(cf.[H-I]).

Proof of Theorem M. The following theorem, due to Wüstholz (cf. [Wü]), plays the essential role in our argument.

Theorem W. *Let A be an abelian variety defined over $\overline{\mathbf{Q}}$, and let $T_A \cong \mathbf{C}^g$ be its tangent space. Let* exp *be the exponential map from T_A to $A = \mathbf{C}^g/\Omega_2\mathbf{Z} + \Omega_1\mathbf{Z}$. Let W be a linear subspace of T_A defined over $\overline{\mathbf{Q}}$. If W contains a point $\vec{v}(\neq 0)$ with $\exp(\vec{v}) \in A(\overline{\mathbf{Q}})$, then there exists an algebraic subgroup G of A with the following properties:*

(i) G is defined over $\overline{\mathbf{Q}}$

(ii) the tangent space T_G is a subspace of W and contains $\vec{v}$

(iii) dim G *is positive*

We need the following lemma also.

Lemma 1.

Let A be a simple abelian variety over $\overline{\mathbf{Q}}$. Suppose $A \times A$ contains an algebraic subgroup H defined over $\overline{\mathbf{Q}}$. If we have dim $H =$ dim A *and $p_i(H) = A$ (p_i is the projection to the i-th component), then H determines an element of $End_0\, A$. Moreover H corresponds to a trivial endomorphism (namely the one identified with a rational number) if and only if the tangent space T_H of H is given by the form*

$$\{(\vec{z}, \vec{w}) \in \mathbf{C}^g \times \mathbf{C}^g | m\vec{z} = n\vec{w}\}$$

for certain integers m and n.

We proceed our argument in three steps:

(i) We reduce the problem to the simple case

(ii) $D = End_0\, A$ is a $2g$-dimensional vector space over $\mathbf{Q}$,

(iii) D is a commutative division algebra.

Step (i).

Let A and A' be polarized abelian varieties defined over $\overline{\mathbf{Q}}$. Let ${}^t(\Omega_2, \Omega_1)$ and ${}^t(\Omega_2', \Omega_1')$ be the period matrix of A and A', respectively. Let $\Omega(A)$ and $\Omega(A')$ be the reduced period matrix of A andA', respectively. Suppose these two abelian varieties are isogenous, and let φ be the isogeny from A and A'. Then φ is induced from a certain invertible linear transformation U of $\mathbf{C}^g$. Moreover this linear transformation induces a homomorphism of the lattices represented by the form

$$\begin{pmatrix} \Omega_2' \\ \Omega_1' \end{pmatrix} = M \begin{pmatrix} \Omega_2 \\ \Omega_1 \end{pmatrix} \tag{1.3}$$

for a certain element $M = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ of $M(2g, \mathbf{Z})$. By (1.1) we have

$$\Omega(A) = \Omega_2 \Delta (\Omega_1)^{-1}, \Omega(A') = \Omega_2' \Delta' {\Omega_1'}^{-1}, \tag{1.4}$$

where Δ and Δ' indicate the polarizations of A and A', respectively. Using (1.4) we obtain

$$\Omega(A') = (P\Omega(A) + Q)(R\Omega(A) + S)^{-1}\Delta'$$

Hence $\Omega(A')$ is an algebraic point of $\mathfrak{S}$ provided $\Omega(A)$ is an algebraic point of $\mathfrak{S}$. This argument shows that it is sufficient to study only the simple case.

Step (ii)

Let A be a simple abelian variety defined over $\overline{\mathbf{Q}}$. Suppose the reduced period matrix

$$\Omega(A) = (\lambda_{ij})_{1 \leq i,j \leq g}$$

is an algebraic point of $\mathfrak{S}$. Set

$$\begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix} = \begin{pmatrix} \int_{\gamma_{g+1}} \vec{\omega} \\ \cdot \\ \cdot \\ \cdot \\ \int_{\gamma_{2g}} \vec{\omega} \end{pmatrix}, \qquad \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix} = \begin{pmatrix} \int_{\gamma_1} \vec{\omega} \\ \cdot \\ \cdot \\ \cdot \\ \int_{\gamma_g} \vec{\omega} \end{pmatrix}.$$

Then we have $\Omega_1 = \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix}$ and $\Omega_2 = \begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix}$, hence it holds

$$\begin{pmatrix} \vec{\beta}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\beta}_g \end{pmatrix} = \Omega \begin{pmatrix} \vec{\alpha}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{\alpha}_g \end{pmatrix}. \tag{1.5}$$

Set

$$G = \underbrace{A \times \cdots \times A}_{2g \text{ times}},$$

and let $\vec{u}_i$ and $\vec{z}_i$ $(i = 1, \cdots, g)$ be the coordinate for the tangent space T_A of i-th and $g + i$ th component of G, respectively. We regard them as row vectors. We suppose the exponential map is given by the projection

$$\mathbf{C}^g \longrightarrow \mathbf{C}^g/\Omega_2\mathbf{Z}^g + \Omega_1\mathbf{Z}^g.$$

Set the linear subspace

$$W = \{(\vec{z}_1, \cdots \vec{z}_g, \vec{u}_1, \cdots \vec{u}_g) \Big| \begin{pmatrix} \vec{u}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{u}_g \end{pmatrix} = \Omega \begin{pmatrix} \vec{z}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{z}_g \end{pmatrix} \} \tag{1.6}$$

in $\mathbf{C}^{2g} = T_G$. It is a g^2-dimensional linear subspace. By (1.5) W contains a point

$$P_0 = (\vec{\alpha}_1, \cdots, \vec{\alpha}_g, \vec{\beta}_1, \cdots, \vec{\beta}_g).$$

Let us note that $\exp(P_0) = (0, \ldots, 0)$ in G, especially this is an algebraic point on G. By virtue of Theorem W we can find an algebraic subgroup H of G defined over $\overline{\mathbf{Q}}$. Also the tangent space T_H of H has the property:

$$P_0 \in T_H \subset W. \tag{*}$$

Set $h = \dim H$. Because A is simple the projection map p_i from G to the i-th component A is always surjective. By considering the following exact sequence

$$O \longrightarrow \ker p_i \longrightarrow H \xrightarrow{p_i} A \longrightarrow O$$

we know $\ker p_i$ is $(h - g)$-dimensional. By the iteration of this argument we know that $h = kg$ for a certain positive integer k.

Let π_k be the projection of T_H to the $(\vec{z}_1, \ldots, \vec{z}_k)$-space (the first k-components of T_G). After an appropriate change of order in $\vec{z}_1, \ldots, \vec{z}_g$, if necessary, it becomes surjective. Therefore T_H is represented by $g - k$ relations of the form

$$\begin{cases} \vec{z}_{k+1} = c_{1,k+1}\vec{z}_1 + \cdots + c_{k,k+1}\vec{z}_k \\ \qquad\qquad \cdots\cdots \\ \qquad\qquad \cdots\cdots \\ \qquad\qquad \cdots\cdots \\ \vec{z}_g = c_{1,g}\vec{z}_1 + \cdots + c_{k,g}\vec{z}_k \end{cases} \tag{1.7}$$

together with (1.6).

If we recall Lemma 1 we can show that every coefficient c_{ij} in (1.7) determines a $\mathbf{Q}$-endomorphism of A. Set $D = End_0 A$, it is an algebra over $\mathbf{Q}$. We claim that D is a $2g$-dimensional vector space over $\mathbf{Q}$. So we assume the contrary, namely

$$(**) \qquad \dim_{\mathbf{Q}} D \leq g$$

If it holds $k = g$, there is no relation of the form (1.7). By using Lemma 1 we can find every λ_{ij} belongs to D.

Then we obtain a number field of degree at most g by attaching λ_{ij}'s to $\mathbf{Q}$. According to the following Lemma 2 it contradicts the simpleness of A.

Lemma 2.

Let $\Omega = (\lambda_{ij})$ be an element of $\mathfrak{S}_g$. If every λ_{ij} belongs to a certain number field of degree at most g, then the corresponding abelian variety A is not simple.

Proof. By the assumption we can find the linear relation

$$(+) \qquad b_{i0} + b_{i1}\lambda_{i1} + \cdots + b_{ig}\lambda_{ig} = 0 \quad (i = 1, \ldots, g)$$

over $\mathbf{Q}$. By considering the transformation

$$I_{2g} + (E_{ij} - E_{g+j,g+i})$$

of $\mathrm{Sp}(g, \mathbf{Z})$ we can assume $b_{ii} \neq 0 \quad (i = 1, \ldots, g)$, where E_{ij} indicates the matrix element with the (i, j)-element is equal to 1.

Set

$$A_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & \cdots & b_{1g} \\ 0 & 1 & & & \\ & & \cdots & \cdots & 0 \\ 0 & & & & 1 \end{pmatrix},$$

$$B_1 = C_1 = O, D_1 = {}^t A_1^{-1}$$

and set

$$A_2 = D_2 = I_g, B_2 = b_{10}E_{11}, C_2 = O.$$

By putting

$$M_i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix},$$

we obtain two elements M_1 and M_2 of $\mathrm{Sp}(g, \mathbf{Q})$. Put

$$\Omega' = M_2 M_1(\Omega).$$

So we find

$$\begin{pmatrix} b_{10} + b_{11}\lambda_{11} + \ldots + b_{1g}\lambda_{1g} \\ \lambda_{2g} \\ \cdot \\ \cdot \\ \lambda_{gg} \end{pmatrix}$$

as the g-th column vector of Ω'. By (+) it means the $(1, g)$-element (and the $(g, 1)$-element) of Ω' is equal to 0. By the iteration of this procedure Ω is deformed to a matrix of $\mathfrak{S}_g$ with a direct sum decomposition. This contradicts the simpleness of A. q.e.d.

Next we suppose $k = g - 1$. In this case we get one relation of the form (1.7):

$$\vec{z}_g = c_1\vec{z}_1 + \cdots + c_{g-1}\vec{z}_{g-1} \tag{1.7'}$$

$c_i \in D$. By substituting it in (1.6) we obtain

$$\begin{cases} \vec{u}_1 = (\lambda_{11} + c_1\lambda_{1g})\vec{z}_1 + \cdots + (\lambda_{1,g-1} + c_{g-1}\lambda_{1,g})\vec{z}_{g-1} \\ \cdots \\ \vec{u}_g = (\lambda_{g1} + c_1\lambda_{gg})\vec{z}_1 + \cdots + (\lambda_{g,g-1} + c_{g-1}\lambda_{g,g})\vec{z}_{g-1} \end{cases} \tag{1.8}$$

The coefficients in (1.8) are also $\mathbf{Q}$-endomorphisms. Namely every $\lambda_{ij} + c_j\lambda_{ig}$ belongs to D. By using the fact $\lambda_{ij} = \lambda_{ji}$ we know that every λ_{ij} is contained in the D-module $D \oplus \lambda_{gg}D$. On the other hand we have a certain $\mathbf{Q}$-linear relation

$$b_0 + b_1(\lambda_{11} + c_1\lambda_{1g}) + \cdots + b_g(\lambda_{g1} + c_1\lambda_{gg}) = 0$$

between $g + 1$ endomorphisms

$$1, \lambda_{11} + c_1\lambda_{1g}, \ldots, \lambda_{g1} + c_1\lambda_{gg},$$

for we assumed (**). Therefore λ_{gg} itself belongs to D. So we find that every λ_{ij} is also an element of D. Hence it occurs a linear relation of the form (+) over $\mathbf{Q}$ between

$$1, \lambda_{11}, \ldots, \lambda_{1g}.$$

It is a contradiction again.

Even for the case $k \leq g-2$ we can proceed this argument.

Step (iii). By the same argument in Step (ii) we can find every λ_{ij} belongs to D, and they constitute a generator system of D. So the commutativity is obvious. q.e.d.

§2. Applications.

0) Transcendency of $j(\tau)$.

We have a new proof of the following well-known fact.

Theorem A-0. *Let $j(\tau)$ be the elliptic modular function. Suppose $\tau \in \overline{\mathbf{Q}}$, then $j(\tau)$ is an algebraic number if and only if τ is an imaginary quadratic number.*

Proof.

If part is the conclusion from the classical complex multiplication theory. Only if part is immediate from Theorem M for $g=1$. q.e.d.

1) The transcendency of the Igusa-Rosenhain modular mapping on $\mathfrak{S}_2$.

Let $\lambda : \mathfrak{S}_2 \longrightarrow \mathbf{P}^3$ be the Igusa-Rosenhain modular mapping defined by

$$\lambda(\Omega) = [\xi_0, \cdots, \xi_3]$$

$$= [\vartheta^2 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \vartheta^2 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \vartheta^2 \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

$$\vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \vartheta^2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}],$$

where the thetas indicate the Jacobi theta constants (cf. [I]). It is a modular mapping with respect to $\Gamma(2)$, the principal congruence subgroup of $\mathrm{Sp}(2, \mathbf{Z})$ with level 2. Moreover λ gives a birational correspondence between $\mathfrak{S}_2/\Gamma(2)$ and $\mathbf{P}^2$.

Theorem A-1. *Suppose Ω is an algebraic point of $\mathfrak{S}_2$, then $\lambda(\Omega)$ is an algebraic point of $\mathbf{P}^3$ if and only if Ω is a CM-point.*

Remark 2.1. The mapping λ is the inverse of the period mapping for the family of the curves of genus 2 given by the Legendre normal form

$$C(\xi) : y^2 = x \prod_{i=0}^{3} (x - \xi_i),$$

where $[\xi_0, \cdots, \xi_3]$ is a parameter on $\mathbf{P}^3$.

Proof of Theorem A-1.

If part is the consequence of the complex multiplication theory (cf. [S-T]), so we consider only if part. Let $A = Jac(C)$ be the jacobian variety of $C(\xi)$. By the assumption $C(\xi)$ is defined over $\overline{\mathbf{Q}}$. So A is also defined over $\overline{\mathbf{Q}}$. According to Theorem M A must be of CM type. Recalling Remark 1.3 we know the period $\Omega(A)$ is a CM point of $\mathfrak{S}_2$. q.e.d.

2) The Picard modular mapping.

We use the following notations in this argument.

$\zeta = \exp(2\pi i/3)$, $K = \mathbf{Q}(\zeta)$, $\mathcal{O}_K = \mathbf{Z} \bigoplus \mathbf{Z}\zeta$,

$$H = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let D be the domain defined by

$$D = \{\eta \in \mathbf{P}^2(\mathbf{C}) : {}^t\bar{\eta} H \eta < 0\} = \{(u, v) \in \mathbf{C}^2 : 2\,\Re v + |u|^2 < 0\}$$

(by putting $v = \eta_1/\eta_0, u = \eta_2/\eta_0$), this is biholomorphically equivalent to the 2 dimensional hyperball. Let Γ be the modular group defined by

$$\Gamma = U(H, \mathcal{O}_K) = \{g \in M(3, \mathcal{O}_K) : {}^t\bar{g} H g = H\}.$$

We also consider the modular group with the level structure by $\sqrt{-3}$

$$\Gamma(\sqrt{-3}) = \{g \in \Gamma : g \equiv 1_3 \mod (\sqrt{-3})\}.$$

Set

$$\Omega = \Omega(u, v)$$

$$= \begin{pmatrix} (u^2 + 2\omega^2 v)/(1-\omega) & \omega^2 u & (\omega u^2 - \omega^2 v)/(1-\omega) \\ \omega^2 u & -\omega^2 & u \\ (\omega u^2 - \omega^2 v)/(1-\omega) & u & (u^2 + 2v)/(\omega - \omega^2) \end{pmatrix}.$$

This Ω gives an embedding of D into $\mathfrak{S}_3$. Using above notations we define the mapping $\lambda : D \longrightarrow \mathbf{P}^2$ by $\lambda(u, v) = [\xi_0, \xi_1, \xi_2] =$

$$[\vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ 0 & \frac{1}{6} & 0 \end{bmatrix}(\Omega), \vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{3} \end{bmatrix}(\Omega), \vartheta^3 \begin{bmatrix} 0 & \frac{1}{6} & 0 \\ \frac{2}{3} & \frac{1}{6} & \frac{2}{3} \end{bmatrix}(\Omega)].$$

Remark 2.2. The mapping λ is the inverse of the period mapping for the following family of algebraic curves of genus 3 (cf. [S])

$$C(\xi) : y^3 = x\prod_{i=0}^{2}(x-\xi_i),$$

where $[\xi_i]$ is a parameter in

$$\mathbf{P}^2 - \{\prod_{i=0}^{2}\xi_i \prod_{j,k=0}^{2}(\xi_j - \xi_k) \neq 0\}.$$

Moreover λ induces the biholomorphic correspondence between the compactification of $D/\Gamma(\sqrt{-3})$ and $\mathbf{P}^2$.

Theorem A-2. *Suppose the point $P = (u, v)$ varies on the algebraic points of D. Then $\lambda(u, v)$ is an algebraic point if and only if P is an isolated fixed point of an element in*

$$U(H, K) = \{g \in M(3, K) : {}^t\bar{g}Hg = H\}.$$

Proof. We can obtain the above conclusion by the similar argument as 1).
q.e.d.

3) The inverse of the Schwarz function for the Gauss hypergeometric differential equation.

Let $F(\alpha, \beta, \gamma)$ be the Gauss hypergeometric function and $D(\alpha, \beta, \gamma)$ be the corresponding hypergeometric differential equation:

$$x(x-1)y'' + \{\gamma + (1+\alpha+\beta)x\}y' - \alpha\beta y = 0 \tag{2.1}$$

Always the parameters α, β and γ are supposed to be rational numbers. Set

$$\lambda = 1-\gamma, \quad \mu = \beta - \alpha, \quad \nu = \gamma - \alpha - \beta$$

Let N be the least common multiplier of the denominators of α, β and γ. Put

$$1-\alpha = A/N, \quad \alpha + 1 - \gamma = B/N, \quad \beta = C/N$$

We assume the following condition for λ, μ and ν

$$\begin{cases} 1/\lambda,\ 1/\mu,\ 1/\nu \in \mathbf{Z} \cup \{0\}, \\ |\lambda| + |\mu| + |\nu| < 1. \end{cases} \tag{2.2}$$

Set

$$I(\infty, z) = \Gamma(\gamma)\{\Gamma(\alpha)\Gamma(\beta)\}^{-1} \int_0^\infty x^{\alpha-1}(1-x)^{\gamma-\alpha-1}(1-zx)^{-\beta}dx \tag{2.3}$$

$$I(1, z) = \Gamma(\gamma)\{\Gamma(\alpha)\Gamma(\beta)\}^{-1} \int_0^1 x^{\alpha-1}(1-x)^{\gamma-\alpha-1}(1-zx)^{-\beta}dx. \tag{2.3'}$$

Under the condition (2.2) $I(\infty, z)$ and $I(1, z)$ are independent solutions of (2.1). Moreover the Schwarz function

$$\sigma(z) = I(\infty, z)/I(1, z)$$

has a single valued inverse function, say $\lambda(\tau)$, defined on a bounded domain D (namely it is biholomorphically equivalent to the upper half plane H).

Here we use the notations according to [Wo]. The hypergeometric function $F(\alpha, \beta, \gamma : z) = I(\infty, z)$ can be considered as a period integral on the algebraic curve

$$X(N, z) : y^N = x^A(1-x)^B(1-zx)C.$$

Let us denote its Jacobian variety by $Jac(X(N, z))$. Set

S= the system of linearly independent differential forms of the form $\omega_n = \frac{P(x)dx}{y^n}$ for a certain positive integer n.

Then we have $r = \sharp S = \varphi(N)$. So we put $S = \{\omega^{(1)}, \cdots, \omega^{(r)}\}$ and $\omega^{(i)} = \omega_{n_i}$.

Let ζ be the primitive N-th root of unity, and set $K = \mathbf{Q}(\zeta)$. We obtain a lattice Λ in $\mathbf{C}^r$ by putting

$$\Lambda = \{(\rho_i(a) \int_0^1 \omega^{(i)} + \rho_i(b) \int_0^\infty \omega^{(i)})_{1 \le i \le r} : a, b \in \mathcal{O}_K\},$$

where $\mathcal{O}_K$ is the ring of integers in K and ρ_i is the automorphism of K with $\rho_i(\zeta) = \zeta^{n_i}$. Then we obtain an abelian variety $T = \mathbf{C}^r/\Lambda$. According to Wolfart $Jac(X(N, z))$ is isogenous to

$$T \oplus \sum_{D|N, D \neq N} Jac(X(D, z)).$$

Theorem A-3. *Suppose τ is algebraic. Then $\lambda(\tau)$ is an algebraic number if and only if T is an abelian variety of CM type.*

Proof.

i) The case T is simple. Let us consider $G = T \times T$. In the tangent space $T_G \cong \mathbf{C}^r \times \mathbf{C}^r$ of G we define the linear subspace

$$W = \{(\vec{z}, \vec{w}) \in \mathbf{C}^r \times \mathbf{C}^r : z_1 \int_0^\infty \omega_1 = w_1 \int_0^1 \omega_1\}$$

We have a natural action of the cyclotomic field $\mathbf{Q}(\zeta)$, where ζ indicates the N-th primitive root of unity, on the lattice Λ. Therefore $End_0 T$ contains the algebraic number field $\mathbf{Q}(\zeta)$ of degree $r = \phi(N) = \dim T$. So it is sufficient to show that $End_0 T$ contains a $\mathbf{Q}$-endomorphism which is not contained in $\mathbf{Q}(\zeta)$.

The subspace W contains a point

$$P_0 = (\vec{z}, \vec{w}) = \begin{pmatrix} \int_0^1 \omega_1 & \int_0^\infty \omega_1 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ \int_0^1 \omega_r & \int_0^\infty \omega_r \end{pmatrix}$$

which is sent to $0 \in G(\overline{\mathbf{Q}})$ by the exponential map. According to Theorem W there exists an algebraic subgroup H satisfying the three conditions in the statement. Because T is simple H must be r-dimensional. Obviously H does not coincide with the component of T. By Lemma 1 we can find a $\mathbf{Q}$-endomorphism, say σ.

Suppose σ is contained in $\mathbf{Q}(\zeta)$. On multiplying by a certain integer, σ can be supposed to lie in the ring of integers of $\mathbf{Q}(\zeta)$. By the definition of the lattice Λ the endomorphism σ carries the vector $\int_0^1 \vec{\omega}$ to a certain $\mathbf{Z}$-linear combination of

$$\alpha_1 \int_0^1 \vec{\omega}, \ldots, \alpha_r \int_0^1 \vec{\omega}$$

where $\{\alpha_1, \ldots, \alpha_r\}$ is the generator system of the ring of integers. On the other hand if we examine the construction of σ, it carries the vector $\int_0^1 \vec{\omega}$ to $\int_0^\infty \vec{\omega}$. This is a contradiction.

ii) The case T is not simple.

Suppose we have the decomposition $T = A_1 \times \cdots \times A_k$, where every A_i is the same simple abelian variety A. By the same arguments as in i) also in this

case we have a certain subvariety H in $G = T \times T$. If we restrict it to a certain product $A_i \times A_j$ in $T \times T$, we can find a $\mathbf{Q}$-endomorphism σ of $End_0 A$. So we can proceed the same discussion as the first case.

q.e.d.

REFERENCES

[B] Bertrand, D., *Lemme de zéros et nombres transcendants*, Seminaire Bourbaki, (1985-86).

[B-W] Beukers, F., Wolfart, J., *Algebraic values of hypergeometric functions*, Proceedings of Durham conference on transcendental numbers 1986.

[H-I] Hashimoto, K., Ibukiyama, T., *On class numbers of positive definite binary quaternion hermitian forms*, J. Fac. Sci. Univ. Tokyo **27** (1980), 549-601.

[I] Igusa, J., *On Siegel Modular forms of genus two*, Amer. J. Math. **84** (1962), 175-200.

[Mo] Morita, Y., *On transcendency of special values of arithmetic automorphic functions*, J. Math. Soc. Japan **24** (1972), 268-274.

[Mu] Mumford, D., *Tata lectures on theta I.*

[S-T] Shimura, G., Taniyama, Y., *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. Japan (1975).

[S] Shiga, H., *On the representation of the Picard modular function by theta constants I-II*, Pub. Research Inst. Kyoto Univ. **24** (1988), 311-360.

[T] Takeuchi, K., *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), 600-612.

[W-W] Wolfart, J., Wüstholz, G., *Der Überlangerungsradius gewisser algebraischer Kurven und die Werte der Betafunktion an rationalen Stellen*, Math. Ann. **273** (1985), 1-15.

[Wo] Wolfart, J., *Werte Hypergeometrischer Funktionen*, Inv. Math. **92** (1988), 187-216.

[Wü] Wüstholz, G., *Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen*, Ann. Math. (1989), 501-517.

Hironori Shiga
Department of Mathematics,
Chiba University
Yayoi-cho 1–33,
Chiba-City, Japan

Astérisque

S. SRINIVASAN

Two results in number theory

Astérisque, tome 209 (1992), p. 307-310

<http://www.numdam.org/item?id=AST_1992__209__307_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

TWO RESULTS IN NUMBER THEORY

S. Srinivasan

In memory of my friend
Mr. Ellis Martin Richstone

§1. Introduction. Let $N \geq 1$ be an integer and, for a reduced fraction a/N, let $K(a/N)$ denote the largest partial quotient in the continued fraction expansion of a/N. Set $K_0(N) = \min K(a/N)$ for $1 \leq a \leq N, (a,N) = 1$. Let, for a sequence B of integers, $B(x)$ denote the number of b in B, but not exceeding x. With this notation, a conjecture of S.K. Zaremba can be stated as $K_0(N) \leq 5$, for all N (cf., p.76 of [4]). There has also been some numerical evidence for this conjecture (cf., p.989 of [2]).

Now considering for given integer $\ell \geq 2$, the sequence A_ℓ consisting of N with $K_0(N) \leq \ell$, it has been shown in [3] that

$$A_\ell(x) > \frac{1}{\sqrt{2\ell}}\, x^{\frac{1}{2}(1-\ell^{-2})}, \text{ for } x \geq 1. \tag{1}$$

In this context, we observe the following proposition, which also leads to a qualitative result of type (1). For a given collection of a.p.s (i.e., arithmetic progressions) of (positive) integers, let $\alpha(m)$ denote the number of a.p.s containing m (but not as the smallest) and, $\delta(m)$ denote the number of a.p.s with common difference m.

Proposition 1. *Let $k(\geq 2)$ be an integer, β and β' some positive constants. Suppose A is the union of a collection of a.p.s, each consisting of k integers, satisfying (i) $\alpha(m) \leq \beta\delta(m)$ for all m and (ii) the smallest member of each a.p. is $\leq \beta'$ times its common difference. Then, for any b such that $\alpha(b) > 0$ and for all sufficiently large x, we have*

$$A(x) \geq \frac{\sqrt{\beta}}{k-1}\left(\frac{x}{b}\right)^{\theta}, \quad \textit{for some} \quad \theta = \theta(\beta,\beta',k) > 0, \tag{2}$$

provided $(k-1)$ exceeds β. (An expression for θ is given in (4) below.)

Our second observation gives the following

Proposition 2. *Any solution in integers of the equation*

$$(\xi^2+\eta^2-1)=t(\xi u+\eta v)(\xi v-\eta u) \tag{3}$$

satisfies $tuv=0$.

In § 3, we shall give an example from R.Tijdeman in connection with Proposition 1. And in § 4, we have some remarks about these results.

§2. Proofs. We start with the proof of Proposition 1. Consider

$$T(x):=\sum_{m\le x}\alpha(m)\le\beta\sum_{m\le x}\delta(m).$$

Since every a.p. counted by the last sum, in view of the assumption (ii), consists of members not exceeding $(k-1+\beta')x$, we see that it occurs $(k-1)$ times in $T((k-1+\beta')x)$ and so,

$$(k-1)T(x)\le\beta T((k-1+\beta')x).$$

On letting $x_r=(k-1+\beta')^r b$, we obtain

$$T(x_r)\ge(\frac{k-1}{\beta})^r,\quad r=1,2,3,\cdots.$$

From here, after a short calculation, (2) is obtained on noting that $T(x)\le(k-1)(A(x))^2$. To see the last inequality observe that every a.p. counted in $\alpha(m)$ determines the pair (a,m), a being its smallest member and, each such pair arises from at most $(k-1)$ of the a.p.s. Also, we may take

$$\theta=\frac{1}{2}\{\log(\frac{k-1}{\beta})/\log(k-1+\beta')\}. \tag{4}$$

Now we give a proof of Proposition 2. Let $tuv\neq 0$. First, observe that, after changing notations if necessary, we can assume that

$$(u,v)=1,\quad \min(\xi,\eta,t,x,y)>0, \tag{5}$$

where $x:=\xi u+\eta v, y:=\xi v-\eta u$. Now, since $(x,y)\mid(\xi^2+\eta^2)$, we can conclude, by (5), that $(x,y)=1$. Then (3) can be rewritten as

$$(x^2+y^2)=d(1+txy),\quad d:=u^2+v^2>1.$$

Next we obtain from this

$$w\ge\varphi(x,y):=(x^2+y^2-wxy)=d>1,\quad w:=dt. \tag{6}$$

We have here

$$\varphi(x,y) = y^2 - xz = \varphi(y,z); \quad z := wy - x.$$

Thus starting with a solution (x,y) of (6), we obtain another solution (y,z) through $z = wy - x$. Now we observe that if $x \geq y > 1$ and $\gcd(x,y) = 1$, then $y > z > 0$, and obviously $\gcd(y,z) = 1$ so that, on iteration, we finally get a solution of (6) with $y = 1$, whereas (6) has no such solution and therefore $tuv = 0$, which proves Proposition 2.

§3. About β. The following example illuminates the significance of β occurring in Proposition 1: Let $k > 2$, and let r be a positive integer such that $r+1, \ldots, r+k-2$ are all composite. (We can take $r < k$!) Consider the sequence A of positive integers composed of primes at most r. Take any element $m > 1$ of A. Then m is divisible by a prime p which is at most r. The numbers $p-1, p, \ldots, p+k-2$ are all smaller than $r+k-1$ and therefore composed of primes at most r. Thus m is the second element of the following a.p. of length k with entries from A: $(p-1)m/p, m, (p+1)m/p, \ldots, (p+k-2)m/p$. Now it is easily seen that

$$A(x) < 2(\log x)^t,$$

where t is the number of primes at most r. Hence t is a constant depending only on k.

This example satisfies all conditions of Proposition 1, except the last one. For, we have $\delta(m) = t$ and $\alpha(m) \leq t(k-1)$ and further, $\alpha(m) = t(k-1)$ for all m belonging to A and which are multiples of K, defined as the product of $(p+j)$, as p runs through all of the t primes not exceeding r, and j takes values $0, 1, \ldots, (k-2)$. So, $\beta = k-1$.

§4. Some remarks. It can easily be seen that the conjecture of Zaremba (in §1) may also be stated as follows: Let $V_q := \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$ and Z_ℓ denote the semigroup of matrices generated by $V_1, \cdots, V_\ell$. Then every $N \geq 1$ occurs as an entry of some element in Z_5. It is this formulation involving substitutions like $x_{j+1} = qx_j + x_{j-1}$ which links Propositions 1 and 2 with the conjecture; in fact, in Proposition 1 this connection comes by considering members of an a.p., with least element a and common difference m, as values of $qm + a$ $(0 \leq q < k)$, whereas in Proposition 2 this is more explicit through the substitution $z = wy - x$.

For obtaining a result of the form (1), from (2), we need only observe that A_ℓ can be considered as a sequence A of Proposition 1, with $k = \ell + 1$,

$\beta = 1 = \beta'$. (Here, with regard to $N \in A_\ell$, $N \geq 2$ and a/N with $K(a/N) \leq \ell$ we consider the a.p.s (of length $\ell+1$): (i) with smallest member b and common difference a, where $N = aj + b$ $(0 \leq b < a, 1 \leq j \leq \ell)$, and (ii) with smallest member a and common difference N.)

Also, it is apparent from the proof that for an estimate like (2) it suffices to have (i), in Proposition 1, for all sufficiently large values of m.

Incidentally, it may be noted that the argument subsequent to (6) would lead to all solutions of the simultaneous congruences

$$\xi^2 \equiv 1 \pmod{\eta}, \quad \eta^2 \equiv 1 \pmod{\xi}. \tag{7}$$

This is because (7) implies that $\xi^2 + \eta^2 - 1 = w\xi\eta$ for some positive integer w and so we obtain (6), but instead with $d = 1$. Now starting with any solution (ξ, η) of (7) we can iterate the passage from (ξ, η) to $(\eta, w\eta - \xi)$ from the proof following (6) until, after only finitely many steps, we reach $(w, 1)$. It is obvious that $(w, 1)$ is a solution of (7) for every positive integer w. Hence we obtain a complete parametrization of the set of solutions of (7). Congruences of the type (7) were earlier considered in [1].

§5. Acknowledgement. The author thanks Professor R.Tijdeman, for his kind permission to include his construction in this paper and for suggesting the parameter β' (instead of the earlier 1) in Proposition 1. Also the author would like to thank the referee for helpful suggestions.

References

[1] Gupta, H. and Srinivasan, S.: *Cycles of Quadratic Congruences,* Res. Bull. (N.S.) of the Panjab University, **22** (1971),401–404.

[2] Niederreiter, H.: *Quasi Monte-Carlo methods and pseudo-random numbers*, Bull. of A.M.S., **84** (1978), 957–1041.

[3] Sander, J.W.: *On a Conjecture of Zaremba,* Mh. Math., **104** (1987), 133–137.

[4] Zaremba, S.K.: *La méthode des »bons treillis« pour le calcul des intégrales multiples*, Application of Number Theory to Numerical Analysis (S.K. Zaremba, ed.), pp.39–119, New York; Academic Press (1972).

Seshadri SRINIVASAN
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005, India

Astérisque

VYACHESLAV I. YANCHEVSKIJ

K-unirationality of conic bundles over large arithmetic fields

Astérisque, tome 209 (1992), p. 311-320

<http://www.numdam.org/item?id=AST_1992__209__311_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

K-UNIRATIONALITY OF CONIC BUNDLES OVER LARGE ARITHMETIC FIELDS

Vyacheslav I. YANCHEVSKIĬ

In the study of rational surfaces a major role is played by Del Pezzo surfaces and by conic bundles over curves. There are some interesting open questions about their properties. Most important among them is the problem of K-unirationality for conic bundles having a K-rational point. For a more precise exposition of this problem we need some definitions and conventions.

Let K be a field of characteristic $\neq 2$, X an absolutely irreducible variety defined over K, and $\overline{K}$ the algebraic closure of K.

Recall that X is said to be K-rational (respectively, K-unirational) if its function field $K(X)$ is (respectively, is contained in) a purely transcendental extension of K. One says that X is rational if $\overline{X} = X \times_K \overline{K}$ is $\overline{K}$-rational.

DEFINITION 1. A rational K-surface X is called a *conic bundle* over a rational curve C if there exists a K-morphism $f: X \to C$ whose generic fibre is a rational curve.

The problem of K-unirationality for conic bundles without a K-rational point clearly has a negative solution. So the following question is natural: are rational conic bundle surfaces with a K-rational point K-unirational? This question is not only of arithmetic interest. Its algebraic significance lies in the connection with the problem of existence of splitting fields of special type for some quaternion algebras. More precisely, V. A. Iskovskikh [8] has established that a conic bundle is K-unirational if and only if the corresponding quaternion algebra over a K-rational field has a K-rational splitting field

(here a 'K-rational field' means some rational function field $K(z)$). Thus our K-unirationality question can be formulated as a problem in the theory of central simple algebras.

Further, this problem generalizes to arbitrary finite-dimensional central simple algebras. For a strict formulation we shall need the following definitions.

Let v be a valuation (or a place) of a field F. We shall denote by F_v the completion of F with respect to v (or at v).

DEFINITION 2. Let A be a finite-dimensional central simple algebra over a K-rational field L. Then one says that A *has a K-rational point* if there exist two elements, $k \in K$ and $x \in L$, such that $L = K(x)$ and the algebra $A \otimes_{K(x)} K(x)_{(x-k)}$ (where $(x-k)$ denotes the valuation of $K(x)$ corresponding to $x - k$ with trivial restriction to K) is trivial (i.e. a total matrix algebra over $K(x)_{(x-k)}$).

With the above notation (and definitions), the problem of existence of rational splitting fields for quaternion algebras generalizes as follows.

PROBLEM. *Let A be a finite-dimensional central simple algebra over a K-rational field, and suppose it has a K-rational point. Does A have a K-rational splitting field?*

For some classes of fields this problem has a positive answer. This is trivial in the case of an algebraically closed field K. Actually, in this case, $K(x)$ is a C_1-field (for definitions see e.g. [15]), and the Brauer group of $K(x)$ is trivial (see [15]). Hence any extension of $K(x)$ (in particular, any K-rational field) is a splitting field for any central simple algebra over $K(x)$. The first nontrivial case is that of local fields (i.e. real closed and p-adically closed fields). The case where $K = \mathbb{R}$ was first considered by Iskovskikh [8]. Real closed fields were considered later by the author. As to p-adically closed fields, the author [18] proved that the above problem has a positive solution for Henselian fields K and hence for p-adically closed fields (see [14]). The next natural case for consideration is when K is 'pseudo-closed'. The aim of this paper is an exposition of results on the above problem in this case and of the analogous result for the so-called large arithmetic fields. These results were obtained recently by Yu. Drakokhrust and the author.

The author would like to thank the referee for some useful suggestions (see the Appendix).

§1. The case of pseudo-closed fields

In this section we shall prove that if a central simple algebra over a K-rational field has a K-rational point, then it has a K-rational splitting field, provided K is 'pseudo-closed'. We recall some definitions.

DEFINITION 3. A field K is said to be *formally real* if it has at least one ordering (for details see e.g. [11] and [12]).

DEFINITION 4. A field K is said to be *real closed* if it is formally real and does not admit any proper formally real algebraic extension.

Any real closed field has a unique ordering, and any formally real field is contained in some real closed one. Moreover, if L_1 and L_2 are two real closed algebraic field extensions of K whose orderings induce the same ordering v on K, then L_1 and L_2 are K-isomorphic and one says that L_1 is a real closure of K (with respect to v). Let us denote by S_K the set of all orderings on K (we do not rule out the possibility that S_K may be empty) and by K_v the real closure of K for each $v \in S_K$.

DEFINITION 5. A field K is called *pseudo-real closed (prc)* if any absolutely irreducible affine K-variety X has a K-rational point if and only if it has a simple K_v-point for every $v \in S_K$.

These definitions imply that the class of pseudo-algebraically closed (pac-) fields K is contained in that of prc-fields. This is a case where S_K is empty. (Pac-fields were introduced by J. Ax and have been systematically investigated in [4], [9], and [17]. As to prc-fields, see e.g. [13].)

The class of p-adically closed fields can be defined in a similar fashion.

DEFINITION 6. Let K be a field of characteristic zero with valuation v, valuation ring Ω, and maximal ideal $\Sigma \subset \Omega$. Suppose the field Ω/Σ is of characteristic p and $\dim_{\mathbb{Z}/p\mathbb{Z}} \Omega/\Sigma = d$. Then K is called a *p-valued field* of p-rank d.

DEFINITION 7. Let K be a p-valued field of p-rank d. Then K is said to be *p-adically closed* if K does not admit any proper p-valued algebraic extension with the same p-rank.

If K is a p-valued field with valuation v, then there exists a maximal p-valued algebraic extension of K having the same p-rank. Any such field K_v is called a *p-adic closure* of K.

DEFINITION 8. Let K be a p-valued field and let M_K be the set of all non-K-isomorphic p-adic closures of K. Then K is said to be *pseudo-p-adically closed (ppc)* if every absolutely irreducible affine K-variety has a K-rational point provided it has a simple L-rational point for every element L of M_K.

REMARK 1. The Brauer groups of prc-fields can be finite but, contrary to the case of pac- and real closed fields, their orders are not uniformly bounded and can even be infinite.

From now on, pac-, prc- and ppc-fields will be called *pseudo-closed fields* for short. The main result of this section is as follows.

THEOREM 1. *Let K be a pseudo-closed field. If a finite-dimensional central simple algebra A over a K-rational field $K(x)$ has a K-rational point, then it has a K-rational splitting field.*

REMARK 2. In the case of pac-fields K, this theorem was proved earlier by I. I. Voronovich [16].

Before proving the theorem, it is convenient to formulate the main result of [18].

THEOREM (*). *Let A be a central simple (finite-dimensional) algebra over a K-rational field $K(x)$. We assume that A has a K-rational point. If K is Henselian and its characteristic does not divide the index of A, then A has a K-rational splitting field $K(z)$. Furthermore,*

$$x = h(z)/\pi,$$

where $h(z) \in K[z]$ is an irreducible monic polynomial and π is a suitable element in the valuation ideal of K. In addition, a root α of $h(z)$ generates a Galois extension of K, and $K(\alpha)(x)$ is a splitting field of A.

Proof of Theorem 1. Let A be a central division algebra over $K(x)$ and let $\dim_{K(x)} A = n^2$. We denote by P the algebraic closure of $K(t)$ in $K\langle t\rangle$, where $K\langle t\rangle$ is the field of formal power series in t over K. Then P is a Henselian field [2]. By Theorem (*) the algebra $B = A \otimes_{K(x)} P(x)$ has a P-rational splitting field $P(z)$ such that

$$x = h(z)/t^m.$$

Here n divides m, and $h(z) \in K[z]$ is an irreducible monic polynomial with the property: if $h(\alpha) = 0$ then $K(\alpha)$ is a Galois extension of K and $K(\alpha)(x)$ is a splitting field of A.

Let us fix ourselves a $K(x)$-basis $\{u_1, u_2, \ldots, u_{n^2}\}$ for A. Then the elements of the standard matrix basis $\{e_{11}, e_{12}, \ldots, e_{nn}\}$ of the total matrix algebra $B \otimes_{P(x)} P(z)$ are $P(z)$-linear combinations of $u_1, u_2, \ldots, u_{n^2}$. We write $\varphi_i = a_i(z)/b_i(z)$ $(i = 1, 2, \ldots, n^4)$ for the coefficients of all these combinations $(a_i(z), b_i(z) \in P[z])$, and $\Phi(z) = S(z)/R(z)$ for the determinant of the matrix N (with $S(z), R(z) \in P[z]$), where $[e_{11}, e_{12}, \ldots, e_{nn}] = [u_1, u_2, \ldots, u_{n^2}]\, N$. Finally, we write

$$a_i(z) = a_{0i} z^{\deg a_i(z)} + a_{1i} z^{\deg a_i(z)-1} + \ldots + a_{\deg a_i(z)\, i},$$

with $a_{0i}, \ldots, a_{\deg a_i(z)\, i} \in P$. In quite the same way, we define elements $b_{0i}, \ldots, b_{\deg b_i(z)\, i}$; $s_0, \ldots, s_{\deg S(z)}$; and $r_0, \ldots, r_{\deg R(z)}$. Let L be the extension of K generated by the elements $a_{0i}, \ldots, a_{\deg a_i(z)\, i}$, $b_{0i}, \ldots, b_{\deg b_i(z)\, i}$ $(i = 1, 2, \ldots, n)$ and by t. Then L is a regular extension of K. Since L is algebraic over $K(t)$ and $\operatorname{char} K = 0$, then $L = K(t, s)$, where $f(t, s) = 0$ for some absolutely irreducible polynomial $f(X, Y) \in K[X, Y]$. Now let $\Gamma = \{(\alpha, \beta) \in \mathbb{A}^2 \mid f(\alpha, \beta) = 0\}$. Without loss of generality we may assume that all of $a_{ki}, b_{ki}, r_k, s_k \in K[\Gamma]$, where $K[\Gamma]$ is the ring of regular functions on Γ. Let $g(t, s)$ be the product of all those $a_{ki}, b_{ki}, r_k, s_k, t$ which are not identically zero on Γ, and let E be the affine curve defined by the equations $f(X, Y) = 0$ and $Z\, g(X, Y) = 1$. Since E is isomorphic to an open subset of the absolutely irreducible curve Γ, it is also absolutely irreducible. Further, $L = K(\Gamma) \cong K(E)$, where $K(\Gamma)$ (resp. $K(E)$) is the field of K-rational functions on Γ (resp. on E).

Now, an ordering v of a prc-field K $(v \in S_K)$ can be extended (see [12]) to an ordering w of $K_v\langle t\rangle$. And it is clear that the restriction of w to L induces an extension of v to an ordering of L. Similarly, a valuation v of a ppc-field K can, according to [14], be extended to a p-adic valuation w of $K_v\langle t\rangle$. Hence its restriction to L is a p-adic valuation extending v. Thus we find, according to [13] (resp. [14]), that Γ has a simple K_v-point for every real (resp. p-adic) closure K_v. Hence E has a K-rational point $(a, b) \in \mathbb{A}^2$ such that $a \neq 0$. Further, for every $b_i(z)$ not all $b_{ki}(a, b)$ can vanish, for $S(z)$ not all $s_k(a, b)$, and the same is true for $R(z)$ and the $r_k(a, b)$.

We now consider the extension $K(y)$ of $K(x)$, where $x = h(y)/a^m$, and the algebra $C = A \otimes_{K(x)} K(y)$. There exists a place μ of $K(x)(t, s)$ to $K(x)$, which is trivial on $K(x)$ and such that $\mu(t) = a$, $\mu(s) = b$ (see e.g. [3]). Let ν be a place of $K(z)(t, s)$ to $K(y)$ extending μ and such that $\nu(z) = y$. The construction of E and the choice of (a, b) imply:

$$\nu(S(z)) \neq 0, \quad \nu(R(z)) \neq 0, \quad \nu(b_i(z)) \neq 0 \quad (i = 1, 2, \ldots, n^4).$$

Let $[v_{11}, v_{12}, \ldots, v_{nn}] = [u_1, u_2, \ldots, u_{n^2}]\, \nu(N)$. Then the matrix $\nu(N)$ is non-singular and $\{v_{11}, v_{12}, \ldots, v_{nn}\}$ is a basis for C. Finally, on comparing the

structure constants of the algebras B and C with respect to $\{e_{11}, e_{12}, \ldots, e_{nn}\}$ and $\{v_{11}, v_{12}, \ldots, v_{nn}\}$, we are led to the conclusion that the triviality of B implies that of C. □

COROLLARY 1. *Let X be a conic bundle defined over a pseudo-closed field K. Then X is K-unirational if and only if X has a K-point.*

§2. The case of large arithmetic fields

In this section a 'closed field' means an algebraically closed, real closed or p-adically closed field.

Let $\mathbb{Q}$ be the field of rational numbers, $\overline{\mathbb{Q}}$ its algebraic closure, and let $\mathbb{Q}_v^{\mathrm{alg}} = \mathbb{Q}_v \cap \overline{\mathbb{Q}}$ be the p-adic closure of $\mathbb{Q}$ if $v = p$, and the real closure of $\mathbb{Q}$ if v is real. We denote by $G(\mathbb{Q})$ the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$.

Let $v_1, v_2, \ldots, v_r$ be a finite set of (not necessarily distinct) absolute values of $\mathbb{Q}$. We write: $\bar{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in G(\mathbb{Q})^r$ and

$$\mathbb{Q}_{\bar{\sigma}} = \sigma_1(\mathbb{Q}_{v_1}^{\mathrm{alg}}) \cap \sigma_2(\mathbb{Q}_{v_2}^{\mathrm{alg}}) \cap \ldots \cap \sigma_r(\mathbb{Q}_{v_r}^{\mathrm{alg}}). \qquad (*)$$

For two elements $\bar{\sigma}, \bar{\lambda} \in G(\mathbb{Q})^r$ we now define $\overline{\sigma\lambda}$ to be the element $(\sigma_1\lambda_1, \ldots, \sigma_r\lambda_r)$. In what follows, we use the term 'almost all' in the sense of the Haar measure on $G(\mathbb{Q})^r$. With the above notation, one has the following two lemmas, which are analogous to Lemmas 12.4 and 12.5 of [7].

LEMMA 1. *Let $\bar{\tau} \in G(\mathbb{Q})^r$ and let $L \subset \mathbb{Q}_{\bar{\tau}}$ be a finite extension of $\mathbb{Q}$. Then, for almost all $\bar{\lambda} \in G(\mathbb{Q})^r$, the following holds: if $f(X,Y) \in L[X,Y]$ is an absolutely irreducible polynomial such that, for every $i = 1, 2, \ldots, r$, there exists a point $(a_{0i}, b_{0i}) \in (\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}}))^2$ with $f(a_{0i}, b_{0i}) = 0$ and $\frac{\partial f}{\partial Y}(a_{0i}, b_{0i}) \neq 0$, then the curve $f(X,Y) = 0$ has a $\mathbb{Q}_{\overline{\lambda\tau}}$-rational point.*

Proof. Let $\tau_1(\mathbb{Q}_{v_1}^{\mathrm{alg}}), \ldots, \tau_m(\mathbb{Q}_{v_m}^{\mathrm{alg}})$ $(m \leq r)$ be all L-nonisomorphic closed fields from $(*)$. Using [5], since L is a Hilbertian field, one has sequences $\{a_j\}, \{b_j\}$ $(a_j \in L, b_j \in \overline{\mathbb{Q}})$ such that

i) a_j lies near a_{0i} in $\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$, $i = 1, 2, \ldots, m$;

ii) $f(a_j, Y)$ is irreducible over L and we have: $\deg f(a_j, Y) = \deg_Y f(X,Y)$ and $f(a_j, b_j) = 0$;

iii) for $L_j = L(b_j)$ the sequence $L_1, L_2, \ldots$ is linearly disjoint over L.

Condition i), Krasner's lemma, Sturm's theorem [11] and the condition $f(a_{0i}, b_{0i}) = 0$ imply that $f(a_j, Y)$ has a root in $\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$, $i = 1, 2, \ldots, r$. Then there exist $\lambda_{j1}, \lambda_{j2}, \ldots, \lambda_{jr} \in G(\mathbb{Q})$ such that $\lambda_{ji}(L_j) \subset \tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$, $i = 1, 2, \ldots, r$.

Let $\bar{\lambda}_j = (\lambda_{j1}, \ldots, \lambda_{jr})$. Condition iii) implies (see [10]) that, for almost all $\bar{\lambda} \in G(\mathbb{Q})^r$, there exists j such that $\overline{\lambda\lambda_j} \in G(L_j)^r$. Then $\lambda_i^{-1}(L_j) = \lambda_{ji}(L_j) \subset \tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$ $(i = 1, 2, \ldots, r)$, i.e. $L_j \subset \lambda_i\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$ $(i = 1, 2, \ldots, r)$. Hence $L_j \subset \mathbb{Q}_{\overline{\lambda\tau}}$, and (a_j, b_j) is a $\mathbb{Q}_{\overline{\lambda\tau}}$-rational point of the curve $f = 0$.

LEMMA 2. *For almost all $\bar{\sigma} \in G(\mathbb{Q})^r$ one has: if $f(X, Y)$ is an irreducible polynomial in $\mathbb{Q}_{\bar{\sigma}}[X, Y]$ and there exists, for every $i = 1, 2, \ldots, r$, a $\sigma_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$-rational point (a_{0i}, b_{0i}) such that $f(a_{0i}, b_{0i}) = 0$ and $\frac{\partial f}{\partial Y}(a_{0i}, b_{0i}) \neq 0$, then the curve $f = 0$ has a $\mathbb{Q}_{\bar{\sigma}}$-rational point.*

Proof. Let T be a countable dense subset of $G(\mathbb{Q})^r$ and let $L \subset \mathbb{Q}_{\bar{\sigma}}$ be the finite extension of $\mathbb{Q}$ generated by all coefficients of $f(X, Y)$. We consider the element $\bar{\tau} \in T \cap G(\mathbb{Q})^r\,\bar{\sigma}$. Since the fields $\sigma_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$, $\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$ are isomorphic over L, we see that $f(X, Y)$ has $\tau_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$-rational points (c_{0i}, d_{0i}) such that $\frac{\partial f}{\partial Y}(c_{0i}, d_{0i}) \neq 0$ $(i = 1, 2, \ldots, r)$. Then by Lemma 1 we see that $f(X, Y)$ has a $\mathbb{Q}_{\bar{\sigma}}$-point, unless $\bar{\sigma}$ belongs to a zero subset of $G(L)^r\bar{\tau}$. Since the set of all polynomials $f(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ is countable and a countable union of zero sets is again a zero set, the lemma is proved.

Using the above two lemmas we can prove the following

THEOREM 2. *For almost all $\bar{\sigma} \in G(\mathbb{Q})^r$, if a finite-dimensional central simple algebra over a $\mathbb{Q}_{\bar{\sigma}}$-rational field has a $\mathbb{Q}_{\bar{\sigma}}$-rational point, then it has a $\mathbb{Q}_{\bar{\sigma}}$-rational splitting field.*

Proof. Let M be a curve similar to the one occurring in the proof of Theorem 1. In fact it is enough to establish that, for almost all fields $\mathbb{Q}_{\bar{\sigma}}$, the curve M has a $\mathbb{Q}_{\bar{\sigma}}$-rational point. Then $L = \mathbb{Q}_{\bar{\sigma}}(\Gamma) \cong \mathbb{Q}_{\bar{\sigma}}(E)$ is contained in $\mathbb{Q}_{\bar{\sigma}}\langle t\rangle$. Since $\mathbb{Q}_{\bar{\sigma}} \subset \sigma_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$, it has an absolute value v_i. By [12] and [14], v_i extends to an absolute value w_i on $\sigma_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})\langle t\rangle$ and the restriction of w_i to L yields an extension of v_i to L. Hence we see that Γ has a $\sigma_i(\mathbb{Q}_{v_i}^{\mathrm{alg}})$-rational point (a_{0i}, b_{0i}) for each v_i, $i = 1, 2, \ldots, r$. By Lemma 2 it follows that, for almost all $\bar{\sigma} \in G(\mathbb{Q})^r$, the curve Γ given by the equation $f(X, Y) = 0$ has a $\mathbb{Q}_{\bar{\sigma}}$-rational point. Now, the existence of a $\mathbb{Q}_{\bar{\sigma}}$-rational point on M follows from the proof of Lemma 1. Indeed, its statement remains true if we exclude from the infinite sequence of fields L_j a finite number of fields, which correspond to points (a_j, b_j) lying on Γ but not on M. The end of the proof of our theorem is similar to that of Theorem 1.

COROLLARY 2. *For almost all $\bar{\sigma} \in G(\mathbb{Q})^r$, the $\mathbb{Q}_{\bar{\sigma}}$-unirationality of a conic bundle X is equivalent to the existence of a $\mathbb{Q}_{\bar{\sigma}}$-rational point on X.*

REMARK 3. A field of the form $\mathbb{Q}_{\bar{\sigma}}$ is not pseudo-closed in general. In fact, let m, n be two distinct odd prime numbers. By the Chinese Remainder Theorem we can find two integers u_m, u_n such that $(u_m/m) = (u_n/n) = -1$ and $(u_m/n) = (u_n/m) = 1$ (where $(../..)$ denotes the Legendre symbol). Besides, for any odd prime number $p \neq m, n$ there exists $v_p \in \mathbb{Z}$ such that $(v_p/p) = 1$ and $(v_p/m) = -1$. Finally, let $a \in \mathbb{Z}$ be such that $a \equiv 1 \pmod 8$ and $(a/n) = -1$. Let us consider the absolutely irreducible quadrics defined by the polynomials: $f_m(X,Y) = X^2 - u_m Y^2 - m$, $f_n(X,Y) = X^2 - u_n Y^2 - n$, $f_p(X,Y) = X^2 - v_p Y^2 - p$, and $f_a(X,Y) = X^2 - aY^2 - n$. Then the quadric $f_m = 0$ has simple points over $\mathbb{Q}_n$ and over the real closure of $\mathbb{Q}$, but it has no points over $\mathbb{Q}_m$. Hence, $\mathbb{Q}_{(m,n)}$ is neither a prc- nor a pnc-field. The same argument with $f_n = 0$ shows that $\mathbb{Q}_{(m,n)}$ is not a pmc-field either. Now the quadric $f_p = 0$ has no simple points over $\mathbb{Q}_m$, so $\mathbb{Q}_{(m,n)}$ is not a ppc-field. Finally, the quadric $f_a = 0$ has no simple points over $\mathbb{Q}_n$, so $\mathbb{Q}_{(m,n)}$ is not a p2c-field.

REMARK 4. Let K be a finite extension of $\mathbb{Q}$ and let Σ be a finite subset of the set $P(K)$ of all inequivalent places (or valuations) of K. For any $g \in \Sigma$ let $K_g^{\mathrm{alg}} = K_g \cap \overline{\mathbb{Q}}$ and $K^{\Sigma} = \bigcap_{g\in\Sigma}\big(\bigcap_{\sigma\in G(K)}(\sigma(K_g^{\mathrm{alg}}))\big)$, where $G(K)$ is the Galois group of $\overline{\mathbb{Q}}$ over K. Let Ω be an algebraic extension of K^{Σ} (for instance, K^{Σ}). Recently F. Pop informed me that he proved the following

THEOREM. *An absolute irreducible variety V defined over Ω has an Ω-rational point if and only if V has a simple Ω_v-rational point for all inequivalent extensions v of the elements of Σ to Ω.*

Using this fact and modifying the proof of Theorems 1 and 2 one can prove the following

THEOREM. *Let Ω be as above. If a finite-dimensional central simple algebra over an Ω-rational field has an Ω-point, then it has an Ω-rational splitting field.*

COROLLARY. *Any conic bundle defined over Ω is Ω-unirational if and only if it has an Ω-rational point.*

Appendix

By using the language of finitely presented morphisms, one can give another nice form to the arguments in §1. Here is a brief exposition of this

point of view, which I owe to Per Salberger. (Most facts on finitely presented morphisms can be found in [6].)

PROPOSITION. *Let K be a pseudo-closed field and P the algebraic closure of $K(t)$ in $K\langle t\rangle$. Let $f: X \to Y$ be a proper dominant K-morphism between smooth projective geometrically connected K-varieties. Suppose there exists a finitely presented P-morphism $s_P: Y_P \to X_P$ such that the composition $f_P \circ s_P: Y_P \to Y_P$ with the induced P-morphism $f_P: X_P \to Y_P$ is finite and surjective. Then there exists a K-morphism $s: Y \to X$ such that $f \circ s: Y \to Y$ is finite and surjective.*

Sketch of proof. Using standard results on finitely presented morphisms [6], we see that there exists a finite extension field L of $K(t)$ in $K\langle t\rangle$ such that $s_P: Y_P \to X_P$ is defined over L. In this way we obtain an L-morphism $s_L: Y_L \to X_L$ with $f_L \circ s_L: Y_L \to Y_L$ finite and surjective. Since $L \subset K\langle t\rangle$ and $[L : K(t)] < \infty$, it is further clear that L is the function field of a smooth projective geometrically connected K-curve C. Once more we apply the standard results in [6] on finitely presented morphisms and extend s_L to a U-morphism $s_U: Y_U \to X_U$ such that $f_U \circ s_U: Y_U \to Y_U$ is finite and surjective for some open K-subset U of C. Now $U(K)$ is nonempty since K is pseudo-closed and $L = K(U) \subset K\langle t\rangle$ (extend orderings and valuations as in §1). So we may specialize s_U at some K-point on U to obtain the desired K-morphism.

COROLLARY. *Let K, P be as above and let X be a smooth K-variety. Let $f: X \to \mathbb{P}^1_K$ be a proper dominant K-morphism whose generic fibre is a Severi-Brauer variety over the function field of $\mathbb{P}^1_K$ (e.g. a conic bundle surface). Then X is K-unirational if and only if X_P is P-unirational.*

Proof. X is K-unirational if and only if there exists a K-morphism $g: \mathbb{P}^1_K \to X$ such that $f \circ g: \mathbb{P}^1_K \to \mathbb{P}^1_K$ is finite and surjective, i.e. if and only if there exists a P-morphism $g_P: \mathbb{P}^1_P \to X_P$ such that $f_P \circ g_P: \mathbb{P}^1_P \to \mathbb{P}^1_P$ is finite and surjective, i.e. if and only if X_P is P-unirational.

It is known that any Severi-Brauer variety over the function field of $\mathbb{P}^1_K$ extends to a proper morphism $f: X \to \mathbb{P}^1_K$ from a smooth K-variety X (cf. [1]). So there is no reason to restrict our unirationality results to the case where f is of relative dimension one. The splitting field result for central simple algebras is equivalent to the existence of $g: \mathbb{P}^1_K \to X$ with $f \circ g$ finite and surjective.

References

[1] M. Artin, Brauer Severi varieties, in: *Lecture Notes in Math.*, 917 (1982).

[2] N. Bourbaki, *Éléments de mathématique. Algèbre commutative.* Paris 1965.

[3] C. Chevalley, *Introduction to the theory of algebraic functions of one variable.* New York 1951.

[4] G.-J. Frey, Pseudo-algebraically closed fields with non-archimedean real valuations. *J. Algebra* 26 (1973), 202–207.

[5] W.-D. Geyer, Galois groups of intersections local fields, *Israel J. of Math.* 30 (1978) 382–396.

[6] A. Grothendieck, Éléments de Géométrie Algébrique, IV, P. 1, *Publ. Math. IHES* 20 (1964).

[7] D. Haran, M. Jarden, The absolute Galois group of a pseudo p-adically closed, *J. reine und angew. Math.* 383 (1988), 147–206.

[8] V.A. Iskovskikh, Rational surfaces with a pencil of curves, *Mat. Sbornik* 74 (1967), 608–638 (= *Math. USSR–Sbornik* 3 (1967), 563–587).

[9] M. Jarden, Elementary statements over large algebraic fields, *Trans. Amer. Math. Soc.* 164 (1972), 67–91.

[10] M. Jarden, The elementary theory of large e-fold ordered fields, *Acta mathematica* 149 (1982), 240–260.

[11] S. Lang, *Algebra*, Addison-Wesley Publishing Company, Reading, Mass. 1965.

[12] A. Prestel, *Lectures on formally real fields*, IMPA, Rio de Janeiro 1975.

[13] A. Prestel, Pseudo real closed fields, in: *Lecture Notes in Math.* 872 (1981), 127–156.

[14] A. Prestel, P. Roquette, Formally p-adic fields, *Lecture Notes in Math.* 872 (1984).

[15] J-P. Serre, *Cohomologie galoisienne*, Springer, Berlin-Göttingen-Heidelberg-New York 1964.

[16] I.I. Voronovich, On splitting fields of central simple algebras over rational function fields, *Dokl. Akad. Nauk BSSR* (1986), 773–775 (in Russian).

[17] W. Wheeler, Model-complete theories of pseudo algebraically closed fields, *Ann. Math. Logic* 17 (1979), 205–226.

[18] V.I. Yanchevskiĭ, K-unirationality of conic bundles and splitting fields of central simple algebras, *Dokl .Akad. Nauk BSSR* 29 (1985), 1061–1064 (in Russian).

Vyacheslav I. Yanchevskiĭ
Institute of Mathematics
of the
Byelorussian Academy of Sciences
ul. Surganova, 11
MINSK 220072 – Byelorussia

Astérisque

AST

Abstract

Astérisque, tome 209 (1992), p. 321

<http://www.numdam.org/item?id=AST_1992__209__321_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Abstract

The "Journées Arithmétiques" offer every other year a wide panorama of the latest advances in Number Theory.

The present volume contains six surveys on recent progress in arithmetic algebraic geometry (S-units, Mordell and Lang conjectures, modular forms and K-theory, elliptic curves), on linear algebraic groups, and on the Riemann zeta-function, as well as nineteen other contributions.