Astérisque

AST

Pages préliminaires

Astérisque, tome 61 (1979), p. 1-10

<http://www.numdam.org/item?id=AST_1979__61__1_0>

AVERTISSEMENT

Ce volume rassemble les textes de certains exposés présentés au Colloque International du Centre National de la Recherche Scientifique - Journées Arithmétiques de Marseille - qui s'est tenu au Centre Universitaire de Luminy du 20 au 24 Juin 1978.

La liste des participants ainsi que celle des exposés non rédigés figurent en tête de ce volume.

TABLE DES MATIÈRES

COLLOQUE INTERNATIONAL DU C.N.R.S.

JOURNEES ARITHMETIQUES

MARSEILLE-LUMIGNY

20-24 Juin 1978

Liste des Participants

ALLOUCHE	PARIS-SUD	BOYD David W.	Br. COLUMBIA
AMICE Yvette	PARIS VII	BROWNAWELL W.D.	KOELN
APERY Roger	CAEN	BRUMER Armand	E.P. PALAISEAU
ARCHINARD Gabriel	GENEVE	BUNDSCHUH Peter	COLOGNE
BAKTAVATSALOU	ABIDJAN	CAHEN J-Paul	TUNIS
BANTEGNIE Robert	BESANÇON	CAR MIREILLE	AIX-MARS.3
BARRUCAND Pierre	PARIS VI	CASSOU-NOGUES Ph	BORDEAUX 1
BATUT Christian	BORDEAUX 1	CASSOU-NOGUES P.	"
BAYER Pilar	REGENSBURG	CASTELA Corine	BORDEAUX 1
BECK Bernard	PARIS	CHAIX Henri	PROVENCE
BEJIAN Robert	PROVENCE	CHALK J.H.H.	TORONTO
BERGE A-Marie	BORDEAUX 1	CHALLULAU Michel	PROVENCE
BERNARDI Dominique	E.N.S. PARIS	CHATELET Fr.	BESANÇON
BERNDT Rolf	HAMBOURG	CHOODNOVSKY David	I.H.E.S
BERTIN M-José	PARIS VI	CHOODNOVSKY Grég.	"
BERTRAND Anne	BORDEAUX 1	CHRISTOL Gilles	PARIS VI
BERTRAND Daniel	E.P. PALAIS.	CIRADE Gisèle	ENSJF PARIS
BERTRANDIAS Fce	GRENOBLE 1	COHEN Henri	BORDEAUX 1
BERTRANDIAS J-P	GRENOBLE 1	COHN Harvey	C.C NEW-YORK
BEUKERS Frits	LEIDEN	COLLIOT-THELENE	PARIS-SUD
BILLOT Patrick	PARIS-SUD	COUGNARD Jean	BESANÇON
BIRCH Brian	TORONTO	DABOUSSI Hédi	PARIS-SUD
BLANCHARD André	PROVENCE	DAMEY Pierre	BORDEAUX 1
BLANCHARD Chris.	PROVENCE	DELANGE Hubert	PARIS-SUD
BLANCHET Francis	CONSTANTINE	DESHOUILLERS J-M.	BORDEAUX 1
BOREL J-Pierre	LIMOGES	DIAS Y DIAS Fco	PARIS-SUD
BOUGAUT Bernard	I.N.S.A.RENNES	DRAXL Peter	BIELEFELD
BOUVIER Lyliane	GRENOBLE 1	DRESS François	BORDEAUX 1

DUBOIS Eugène	CAEN
DUMONT J-Marie	AIX-MARSEILLE
DUPAIN Yves	BORDEAUX 1
DUVAL Dominique	GRENOBLE 1
DVORNICICH Roberto	PISE
ELLISON William	BORDEAUX 1
ERDOS Paul	A.Sc. HONGRIE
ESCASSUT Alain	BORDEAUX 1
FARDOUX Gérard	PROVENCE
FAURE Henri	PROVENCE
FONTAINE J-Marc	GRENOBLE 1
FORTI Marco	PISE
FRESNEL Jean	BORDEAUX 1
FREY Gerhard	SARREBRUCK
GILLARD Roland	GRENOBLE 1
GILLET André	PROVENCE
GIRAUD Guy	PROVENCE
GOLDFELD Dorian	M.MIT.CAMBRIDGE
GONDARD Danielle	PARIS VI
GOUT Gérard	GRENOBLE 1
GRAMAIN François	PARIS VI
GRANDET Marc	TOULOUSE III
GRAS Georges	BESANÇON
GRA M-Nicole	BESANÇON
GRAZZINI Fulvio	TUNIS
GREKOS Georges	BORDEAUX 1
HAOUAT Youssef	TUNIS
HARRIS Michaël	Br. University
HENNIART Guy	PARIS
HIBLOT J-Jacques	PARIS-SUD
JAULENT J-Franc.	ENS PARIS
KAPLAN Pierre	NANCY 1
KRASNER Marc	PARIS VI
LABORDE Marc	BORDEAUX 1
LACHAUD Gilles	PARIS VII
LAGRANGE Jean	REIMS
LANGEVIN Michel	ENS St CLOUD
LARDON René	St ETIENNE
LAUBIE François	BORDEAUX 1
LECACHEUX Odile	PARIS VI
LENSTRA Hendrik	I.H.E.S.
LIARDET Pierre	PROVENCE
LIGOZAT Gérard	PARIS-SUD
LOSERT Viktor	WARWICK
MARTEL Bruno	GRENOBLE 1
MARTINET Jacques	BORDEAUX 1
MASSER David	NOTTINGHAM
MASSY Richard	BREST
de MATHAN Bernard	BORDEAUX 1
MATIGNON Michel	BORDEAUX 1
MEYER Jacques	REIMS
MIGNOTTE Maurice	STRASBOURG 1
MONTGOMERY Hugh	MICHIGAN
MOREAU J-Claude	ALGER
MOSER Nicole	GRENOBLE 1
MOTZKIN Elhanan	PARIS
NARKIEWICZ Wladyslaw	WROCLAW
NEUKIRCH Jürgen	REGENSBURG
NEUMANN Olaf	BERLIN
NGUYEN Nhu-Tâm	PARIS-SUD
NICOLAS J-Louis	LIMOGES
NIEDERREITER Harald	ILLINOIS
NORDON Didier	BORDEAUX 1
OESTERLE Joseph	ENS PARIS
OESTREICHER Chris.	GENEVE
de OLIVEIRA Diago	PROVENCE
OLIVIER Michel	BORDEAUX 1
ORIAT Bernard	BESANÇON
PAYSANT-le-ROUX R.	CAEN
PERELLI Alberto	PISE
PERRIN Bernadette	ENSJF PARIS
PHILIBERT Georges	St ETIENNE
PINTZ Jànos	A.Sc.HONGRIE
POITOU Georges	PARIS-SUD

POLZIN Marc BORDEAUX 1
POUSPOURIKAS Evang. AIX-MARS.II
QUEYRUT Jacques BORDEAUX 1
RAUZY Gérard AIX-MARS.II
RAYNER Francis LIVERPOOL
REMOND Paul St ETIENNE
REVERSAT Marc BORDEAUX 1
REYSSAT Eric PARIS VI
RHIN Georges METZ
RIBET Kenneth I.H.E.S.
RINDLER Harald Math. VIENNE
ROBBA Philippe PARIS-SUD
ROBERT Gilles PARIS-SUD
ROBIN Guy LIMOGES
ROUX Dominique BESANÇON
SAFFARI Bahman PARIS-SUD
SALERNO Saverio I.S. SALERNO
SANSUC J-Jacques ENS PARIS
SARMANT M-Claude PARIS VI
SATGE Philippe CAEN
SCHWACH Paul ENS PARIS
SCOURFIELD Eira LONDON
SEBTI Najiba ORSAY
SERRE J-Pierre Coll. FRANCE
SMADJA René AIX-MARS. II
STEINIG John GENEVE
STEWART Cameron L. I.H.E.S
TAYLOR Martin Math. OXFORD
TENENBAUM Gérard BORDEAUX 1
TIJDEMAN Robert Math. LEIDEN
TOFFIN Philippe CAEN
TURK Jan Math. LEIDEN
VAN DER POORTEN Alfred V. New Sth. WALES
VAUGHAN Robert I. Coll. LONDON
VEECH William RICE UNIVERSITY HOUSTON
VELU Jacques Ecole Polytecnique de PALAISEAU
VIGNERAS M-France ENSJF MONTROUGE
WALDSCHMIDT Michel PARIS VI
WALDSPURGER J-Loup CNRS PARIS
WILES Andrew MIT CAMBRIDGE
WILSON Stephen M.J. BORDEAUX 1
WINTENBERGER J-Pier GRENOBLE 1
WIRSING Eduard ULM
ZIMMER Hort G. SARREBRUCK

LISTE DES EXPOSÉS NON RÉDIGÉS

BARRUCAND Pierre	Quelques propriétés des fonctions L pour les corps cubiques et quadratiques.
BEJIAN Robert et FAURE Henri	Discrépance de suites à faible discrépance. R. BEJIAN ET H. FAURE : Discrépance de la suite de Van der Corput. Séminaire DPP. Déc. 1977. N° 13.
BEUKERS Frits	Exponential Diophantine Equations and Recurrences F. BEUKERS : On the generalized Ramanujan-Nagell - equation, part I and II, Acta Arith., to appear. F. BEUKERS : The multiplicity of binary recurrences, Compositio Mathematica, to appear.
CASSOU-NOGUÈS Philippe	Module de Frobenius et structure galoisienne des anneaux d'entiers. Ph. CASSOU-NOGUÈS : Quelques théorèmes de base normale d'entiers, Ann. Inst. Fourier, 3 t. 28 (1978). Ph. CASSOU-NOGUÈS : Structure galoisienne des anneaux d'entiers, Proc. London Math. Soc. à paraître. Ph. CASSOU-NOGUÈS : Module de Frobenius et structure galoisiennes des anneaux d'entiers. (à paraître).
CHRISTOL Gilles	Solutions algébriques des équations différentielles p-adiques. G. CHRISTOL : Systèmes différentiels linéaires p-adiques : structure de Frobenius faible. (à paraître). G. CHRISTOL : Solutions algébriques des équations différentielles p-adiques.
DUPAIN Yves	Discrépance des suites $\{n\alpha\}$.
ESCASSUT Alain	Problèmes de transcendance p-adique. A. ESCASSUT : Proceedings of the Conference on p-adic analysis, Nijmegen, Nederland, janvier 1978. A. ESCASSUT Type de transcendance p-adique, Groupe d'étude d'analyse ultramétrique de 1'I.H.P., 18 Décembre 1977. A. ESCASSUT : Polynômes d'exponentielles p-adiques, Groupe d'étude d'analyse ultramétrique de 1'I.H.P., 22 mai 1978.

GRAZZINI Fulvio et HAOUAT Youssef	Le spectre des polynômes de Barsky. F. GRAZZINI et Y. HAOUAT : C. R. Acad. Sc. Paris, 284, série A, 1977, p. 1171. F. GRAZZINI et Y. HAOUAT : C. R. Acad. Sc. Paris, 286, série A, 1978, p. 273.
KRASNER Marc	Les corpoïdes et leurs applications à la théorie de la ramification dans les extentions finies des corps valués.
De MATHAN Bernard	Sur un ensemble exceptionnel pour un problème de densité modulo 1. B. de MATHAN : Sur un problème de densité modulo 1, C.R. Acad. Sc. Paris, t. 287, (18 Sept. 1978), Série A, p. 277 - 279.
MIGNOTTE Maurice	Une extention du théorème de SKOLEM-MAHLER. M. MIGNOTTE : Intersection des images de certaines suites récurrentes linéaires, Theoretical Computer Science 7(1978)117-122.
MONTGOMERY Hugh	Rapport sur "le grand crible".
MONTGOMERY Hugh	Estimates of character sums.
MOSER Nicole	Contraintes galoisiennes sur le groupe des unités de certaines extensions de Q. N. MOSER : Contraintes galoisiennes sur le groupe des unités de certaines extensions de Q. Applications arithmétiques, thèse d'état, Grenoble, Juin 1978. J.J. PAYAN : Remarques sur la structure galoisienne des unités des corps nombres (à paraître).
NARKIEWICZ Wladyslaw	Finite abelian groups and factorization problems. W. NARKIEWICZ : Finite abelian groups and factorization problems, Colloqium Mathematicum, to appear.
NEUMANN Olaf	On a theorem of Kummer and Hasse.
PINTZ János	Irregularities in the distribution of primes.
PINTZ János	On the remainder term of the prime number formula ; à paraître dans Acta Arithmetica.

SCOURFIELD Eira	A lower bound for a coprimality problem concerning two multiplicative functions.
	E.J. SCOURFIELD : On the coprimality of certain multiplicative functions, Acta Arithmetica, Vol. 38, N° 2, to appear.
TAYLOR Martin	Galois Module structure of integers of relative abelian extensions.
	M. TAYLOR : Galois Module Structure of Integers of Relative abelian extensions, Crelle, to appear.
TIJDEMAN Robert	A number theoretical packing problem.
TURK Jan	Prime factors in small intervals.
VAN DER POORTEN Alfred	On conjectures of Fermat and Abel.
	A. BAKER and D.W. MASSER eds : Transcendance theory - advances and applications. Academic Press, London 1977.
	K. INKERI and A.J. VAN DER POORTEN : Some remarks on Fermat's conjecture, Acta Arithmetica, 1978.
	C.L. STEWART : A note on the Fermat equation, Mathematika 24 (1977) 130-132.
WALDSPURGER Jean-Loup	Engendrement par des séries thêta de certains espaces de formes modulaires.
	J.L. WALDSPURGER : Engendrement par des séries thêta de certains espaces de formes modulaires, Inventiones, à paraître.
WILES Andrew	Explicit reciprocity laws.
WIRSING Eduard	Report on Additive Functions (Characterizing the logarithm).

Astérisque

ROGER APÉRY

Irrationalité de $\zeta 2$ et $\zeta 3$

Astérisque, tome 61 (1979), p. 11-13

<http://www.numdam.org/item?id=AST_1979__61__11_0>

Société Mathématique de France
Astérisque 61 (1979) p. 11-13

IRRATIONALITÉ DE $\zeta 2$ ET $\zeta 3$

par

Roger APÉRY

-:-:-:-

Notre méthode de démonstration de l'irrationalité d'un réel α défini par les sommes partielles σ_n d'une série de rationnels, comporte les étapes suivantes :

1. Remplacer la suite $\sigma_n = u_{o,n}$ par une suite de rationnels à deux indices $u_{k,n}$ avec $0 \leqslant k \leqslant n$ telle que pour chaque k la suite $u_{k,n}$ converge plus rapidement vers α que la suite $u_{k-1,n}$.

2. Poser $u_{k,n} = \dfrac{t_{k,n}}{\binom{n+k}{k}}$.

3. Majorer, en fonction de n exclusivement, le dénominateur de $t_{k,n}$ c'est-à dire montrer qu'il existe une suite d'entiers p_n tels que $p_n\, t_{k,n}$ soit entier et que $p_n \leqslant \mu^{n+\varepsilon}$.

4. Effectuer une même combinaison linéaire (dépendant de n) à cœfficients entiers positifs sur la colonne n du tableau des $t_{k,n}$ et du tableau des $\binom{n+k}{h}$.

5. On obtient ainsi une suite $\dfrac{v_n}{u_n}$ de fractions de numérateur rationnel et de dénominateur entier. On détermine la limite commune λ de $\sqrt[n]{v_n}$ et de $\sqrt[n]{u_n}$.

6. Si on a de la chance, $\lambda > \mu$: on peut conclure l'irrationalité. On peut aussi déduire une mesure d'irrationalité : quels que soient les entiers p,q,

$$\left|\frac{p}{q} - \alpha\right| > \frac{1}{q^{\gamma+\varepsilon}}$$

avec $\gamma = \dfrac{2 \log \lambda}{\log \lambda - \log \mu}$

Pour la construction des $u_{n,k}$, nous utilisons le développement suivant : étant donnée une suite de réels $a_1, a_2 \ldots a_k$, toute fonction analytique $f(x)$ par rapport à la variable $\frac{1}{x}$ qui tend vers 0 avec $\frac{1}{x}$ admet un développement (unique) de la forme

$$f(x) \equiv \sum_{k \geqslant 1} \frac{C_k}{(x+a_1)(x+a_2)\ldots(x+a_k)}$$

(Nous écrivons $\equiv$ au lieu de $=$ pour tenir compte des répugnances des mathématiciens qui considèrent avec Abel, Cauchy et d'Alembert les séries divergentes comme une invention du diable ; en fait, nous n'utilisons jamais qu'une somme finie de termes, mais le nombre de termes croit avec x).

Pour étudier $\zeta 2$, nous posons :

$$\frac{1}{n^2} \equiv \frac{1}{n(n-1)} - \frac{1}{n(n-1)(n-2)} + \ldots \frac{(-1)^{k-1}\, k!}{n(n-1)(n-2)\ldots(n-k-1)} + \ldots$$

$t_{k,n}$ appartient au module

$$\mathbb{Z}(1, \tfrac{1}{4}, \ldots \tfrac{1}{n^2})$$

D'après un résultat classique sur le p.p.c.m. des n premiers entiers, μ est égal à e^2.

La suite u_n s'écrit $(1,3,19,147,1251,11253,\ldots)$
La suite v_n s'écrit $(0,5,\frac{125}{4},\ldots)$

Elles vérifient la récurrence

$$(n+1)^2 u_{n+1} - (11n^2+11n+3)u_n - (n-1)^2 u_{n-1} = 0$$

$$\lambda = \frac{11+5\sqrt{5}}{2}$$

L'irrationalité de $\zeta 2 = \dfrac{\pi^2}{6}$ est connue depuis Euler, mais notre méthode donne une mesure d'irrationalité de π^2.

Pour étudier $\zeta 3$, nous posons :

$$\frac{1}{n^3} \equiv \frac{1}{n(n^2-1)} - \frac{1}{n(n^2-1)(n^2-4)} + \ldots + \frac{(-1)^k\, (k!)^2}{n(n^2-1)\ldots(n^2-(k+1)^2)} + \ldots$$

L'utilisation de la diagonale $u_{n,n}$ donne la série

$$\zeta 3 = \frac{5}{2} \sum_n \frac{(-1)^{n-1}}{n^3 \binom{2n}{n}}$$

qui à défaut de prouver immédiatement l'irrationalité de $\zeta 3$ converge mieux que $\sum \frac{1}{n^3}$.

2. $t_{k,n}$ appartient au module

$$\mathbb{Z}(1, \frac{1}{2^3} \ldots \frac{1}{n^3} \ldots)$$

μ est égal à e^3.

La suite u_n s'écrit $(1,5,73,1445,33001,\ldots)$

La suite v_n s'écrit $(0,6, \frac{351}{4}, \frac{62531}{36}, \ldots)$

Les deux suites vérifient la relation de récurrence

$$(n+1)^3 u_{n+1} - (34n^3+51n^2+27n+5)u_n + n^3 u_{n-1} = 0$$

$$\lambda = 17+12\sqrt{2}$$

Roger APERY
Département de Mathématiques
Esplanade de la Paix
14032 CAEN CEDEX

Astérisque

ANNE-MARIE BERGE

Projectivité des anneaux d'entiers sur leurs ordres associés

Astérisque, tome 61 (1979), p. 15-28

<http://www.numdam.org/item?id=AST_1979__61__15_0>

Société Mathématique de France
Astérisque 61 (1979) p. 15-28

PROJECTIVITÉ DES ANNEAUX D'ENTIERS SUR LEURS ORDRES ASSOCIÉS

par

Anne-Marie BERGÉ

-:-:-:-

Soit F un corps de nombres, et soit N/F une extension galoisienne finie, de groupe de Galois G. Le groupe G opère de façon naturelle sur N, et on peut donc munir N d'une structure de module à gauche sur l'algèbre de groupe $F[G]$. D'après le théorème de la base normale, le $F[G]$-module N est libre, avec un générateur.

Notons $\mathbb{Z}_F$ et $\mathbb{Z}_N$ les anneaux d'entiers de F et N respectivement. Nous savons que $\mathbb{Z}_N$ est un module de rang 1 sur l'algèbre de groupe $\mathbb{Z}_F[G]$, projectif si et seulement si l'extension N/F est modérément ramifiée. Il est donc naturel de chercher si, dans le cas d'une extension non modérément ramifiée, $\mathbb{Z}_N$ vérifie une propriété analogue, à condition naturellement de substituer, à l'ordre $\mathbb{Z}_F[G]$, l'ordre $\mathfrak{O}(\mathbb{Z}_N, F[G])$ formé des $\lambda \in F[G]$ tels que $\lambda \mathbb{Z}_N$ soit inclus dans $\mathbb{Z}_N$.

Nous savons, par un théorème de Leopoldt ([6]), que, dans le cas des extensions abéliennes du corps $\mathbb{Q}$ des rationnels, l'anneau $\mathbb{Z}_N$ est libre sur l'ordre $\mathfrak{O}(\mathbb{Z}_N, \mathbb{Q}[G])$. Nous allons voir que, par contre, l'étude des extensions diédrales de $\mathbb{Q}$ fournit plusieurs types de contre-exemples à la projectivité de $\mathbb{Z}_N$ sur son ordre associé.

Par complétion pour les valuations $\mathfrak{p}$-adiques du corps F, on est immédiatement ramené, pour ce problème, au cas d'une algèbre galoisienne semi-locale sur un corps local. Cette algèbre est induite par une extension galoisienne du

corps local. Nous consacrons donc un premier paragraphe à l'étude de propriétés des ordres d'une algèbre de groupe relatives à l'induction. Nous faisons ainsi apparaître, dans le cas non abélien, des contraintes qui sont à l'origine d'un premier type de contre-exemples. Nous étudions, dans le deuxième paragraphe, les extensions cycliques ou diédrales de corps locaux. Dans le troisième paragraphe, nous appliquons ces résultats aux extensions diédrales de certaines classes de corps de nombres. Nous caractérisons celles pour lesquelles l'anneau d'entiers est projectif sur son ordre associé, par une condition sur la ramification, qui met en évidence l'aspect particulier des extensions de degré $2p$, où p est premier ([7], [1]).

§ .I. - Méthodes locales

Nous conservons les notations de l'introduction. De plus, si R est un anneau intègre, k son corps des fractions, et M un $R[G]$-module de rang 1, nous notons $\mathfrak{O}(M, k[G])$ l'ordre associé à M dans $k[G]$, c'est-à-dire l'ensemble des $\lambda \in k[G]$ vérifiant $\lambda M \subset M$.

1. - Complétion semi-locale

Pour tout idéal premier non nul $\mathfrak{p}$ de $\mathbb{Z}_F$, l'indice $\mathfrak{p}$ désigne la complétion pour la valuation $\mathfrak{p}$-adique.

PROPOSITION 1. - *Soient M un $\mathbb{Z}_F[G]$-module de rang 1, et $\mathfrak{O}$ son ordre associé dans $F[G]$. Alors :*

1) *Pour tout idéal premier $\mathfrak{p}$ de $\mathbb{Z}_F$, on a $\mathfrak{O}(M_{\mathfrak{p}}, F_{\mathfrak{p}}[G]) = \mathfrak{O}_{\mathfrak{p}}$.*

2) *Les conditions suivantes sont équivalentes :*

   i) *M est un $\mathfrak{O}$-module projectif,*

   ii) *Pour tout idéal premier $\mathfrak{p}$ de $\mathbb{Z}_F$, $M_{\mathfrak{p}}$ est projectif sur $\mathfrak{O}_{\mathfrak{p}}$.*

[L'implication (ii) ⇒ (i) résulte du "bon" comportement du foncteur $\mathrm{Ext}^1_{\mathfrak{O}}$ vis-à-vis de la complétion (cf. [3], exercice 11, p. 123).]

2. - Relation avec les complétions locales

Revenons à l'extension galoisienne N/F. Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_F$.

L'algèbre galoisienne $N_\mathfrak{p}$ est composée directe d'extensions galoisiennes de $F_\mathfrak{p}$, sur l'ensemble desquelles le groupe $G = \mathrm{Gal}(N/F)$ opère transitivement. Soient L l'une de ces extensions, et D son groupe de Galois (groupe de décomposition d'un idéal premier au-dessus de $\mathfrak{p}$ dans N). On a $N_\mathfrak{p} = \bigoplus_s sL$, où s décrit un système de représentants de G/D. Autrement dit, $N_\mathfrak{p}$ est de la forme $F_\mathfrak{p}[G] \otimes L$, où le produit tensoriel est pris sur $F_\mathfrak{p}[D]$. De même, si l'on désigne par B l'anneau de valuation de L, on a $\mathbb{Z}_{N,\mathfrak{p}} \simeq \mathbb{Z}_{F,\mathfrak{p}}[G] \otimes B$, où le produit tensoriel est pris sur $\mathbb{Z}_{F,\mathfrak{p}}[D]$.

3. - Propriétés de l'induction

Soient K un corps local d'inégales caractéristiques, A son anneau de valuation, G un groupe fini, et D un sous-groupe de G. Soit enfin M un module de rang 1 sur l'algèbre A[D]. Nous désignons par $\mathfrak{O}$ l'ordre associé à M dans K[D]. Pour tout A[D]-module P de rang 1, nous notons $\mathrm{Ind}_D^G P$ le G-module induit, c'est-à-dire $A[G] \otimes P$, où le produit tensoriel est pris sur A[D].

PROPOSITION 2. - *Si $\mathrm{Ind}_D^G M$ est projectif sur $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$, alors* M *est projectif sur* $\mathfrak{O}$.

Cela résulte de l'inclusion $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G]) \subset \bigoplus_{s \in D\backslash G} \mathfrak{O}s$, grâce au critère suivant ([3]) :

LEMME 1. - *Soit* R *un anneau. Un* R*-module* P *est projectif si, et seulement si, il existe une famille $(x_i)_{i\in I}$ d'éléments de* P*, et une famille $(f_i)_{i\in I}$ de* R*-homomorphismes de* P *dans* R*, tels que, pour tout $x \in P$, on ait $x = \sum_{i\in I} f_i(x)\, x_i$, où presque tous les $f_i(x)$ sont nuls.*

Inversement, si M est libre sur $\mathfrak{O}$, le G-module $\mathrm{Ind}_D^G M$ est isomorphe au G-module $\mathrm{Ind}_D^G \mathfrak{O}$, mais ce dernier n'est généralement pas un anneau. En fait, l'ordre $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$ est l'intersection des conjugués $s(\mathrm{Ind}_D^G \mathfrak{O})s^{-1}$ où s décrit G. Lorsqu'il est induit par un ordre de K[D], on obtient le résultat attendu :

PROPOSITION 3. - *Supposons le sous-groupe* D *distingué dans* G*, et considérons l'ordre $\mathfrak{O}^* = \bigcap_{s\in G} s\mathfrak{O}s^{-1}$ de* K[D]*. Alors :*

1) $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G]) = \mathrm{Ind}_D^G \mathfrak{O}^*$

2) pour que $\mathrm{Ind}_D^G M$ soit projectif sur $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$, il faut et il suffit que M soit projectif sur $\mathfrak{O}^*$.

Ainsi apparaît une contrainte qui s'explicite mieux lorsque l'algèbre $K[D]$ est commutative :

COROLLAIRE. - Supposons le sous-groupe D commutatif et distingué dans G . Alors les conditions suivantes sont équivalentes :

i) $\mathrm{Ind}_D^G M$ est projectif sur son ordre associé dans $K[G]$,

ii) $\mathrm{Ind}_D^G \mathfrak{O}$ est un anneau, et $\mathrm{Ind}_D^G M$ est libre sur $\mathrm{Ind}_D^G \mathfrak{O}$,

iii) M est libre sur $\mathfrak{O}$, et l'on a $s\mathfrak{O}s^{-1} = \mathfrak{O}$ pour tout $s \in G$.

§ .II. - Extension cyclique ou diédrale d'un corps local

1. - Hypothèses et notations

Soit K un corps local, de caractéristique 0 , et de caractéristique résiduelle $p \neq 0$. On note A l'anneau de valuation de K, et on suppose A absolument non ramifié. Soit G un groupe fini. Pour tout sous-groupe J de G , et tout caractère φ de J à valeurs dans K, on introduit l'idempotent de $K[J]$ suivant :

$$e_\varphi = \frac{1}{(J:1)} \sum_{s \in J} \varphi(s^{-1})\, s \ ,$$

noté plus simplement e_J lorsque $\varphi = 1_J$. Lorsque $(J:1) = p^i$, nous écrivons même e_i au lieu de e_J , si aucune confusion n'est possible. Enfin, si $(x_i)_{i \in I}$ est une famille d'éléments de $K[G]$, le symbole $\langle A[G], x_i \rangle_{i \in I}$ désigne la sous-A-algèbre de $K[G]$ engendrée par $A[G]$ et la famille $(x_i)_{i \in I}$.

2. - Algèbre $K[G]$

Nous étudions, lorsque G est cyclique ou diédral, certains ordres de $K[G]$ contenant $A[G]$, et notamment les ordres maximaux.

1) Supposons G cyclique. - On pose alors $G = U.V$, où V est le p-sous-groupe de Sylow de G , d'ordre p^n . Comme A est absolument non ramifié,

les idempotents primitifs centraux de $K[G]$ sont de la forme $e_\chi(e_i - e_{i+1})$, où χ est un caractère irréductible de U à valeurs dans K, et où i varie de 0 à n (avec la convention $e_{n+1}=0$), de sorte que l'ordre $\mathfrak{M} = \langle A[G], e_i \rangle_{1\leq i\leq n}$ est maximal.

PROPOSITION 4.- Soit $0\leq p\leq n$, et soit $\mathfrak{O} = \langle A[G], e_i \rangle_{0\leq i\leq p}$. Soit M un G-module de rang 1, d'ordre associé $\mathfrak{O}$. Alors M est libre sur $\mathfrak{O}$.

En effet, par récurrence sur p à partir de la relation $M = e_1 M \oplus (1-e_1)M$, où l'ordre associé à $(1-e_1)M$ est l'ordre maximal du corps $(1-e_1)K[G]$, on est ramené au cas $p=0$; nous utilisons alors un résultat plus général dû à S.M.J. Wilson :

LEMME 2.- On ne fait ici aucune hypothèse sur l'indice absolu de ramification de A. Soit G un groupe fini abélien. Alors, tout G-module de rang 1, d'ordre associé $A[G]$, est libre sur $A[G]$.

2) Le groupe G est diédral.- Nous désignons par σ et τ deux générateurs de G liés par les relations $\sigma^h = \tau^2 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$, et par H le sous-groupe de G engendré par σ. On pose $H = U.V$, où V est le p-sous-groupe de Sylow de H. Soit Φ l'ensemble des caractères irréductibles de H à valeurs dans K. La famille d'idempotents suivante constitue une base sur K du centre de $K[G]$:

$$\mathcal{B} = \{\tfrac{1}{2}(1\pm\tau)\, e_\varphi\ ,\ \varphi\in\Phi\ ,\ \varphi^2 = 1\} \cup \{e_\varphi\ ,\ \varphi\in\Phi\ ,\ \varphi^2\neq 1\}\ .$$

Soit $e\in\mathcal{B}$. Nous étudions l'ordre $eA[G]$ de la K-algèbre simple $eK[G]$. Lorsque $e = \frac{1}{2}(1\pm\tau)e_\varphi$, cet ordre est l'ordre maximal du corps $eK[G]$. Supposons donc $e = e_\varphi$, et notons K_φ le corps cyclotomique $e_\varphi K[H]$, K'_φ son sous-corps "réel" maximal, A_φ et A'_φ les anneaux de valuation respectifs de K_φ et K'_φ. Si l'on désigne par Γ le groupe de Galois de l'extension K_φ/K'_φ, l'ordre $eA[G]$ est isomorphe au "twisted group ring" $A_\varphi[\Gamma]$, donc est maximal si et seulement si K_φ/K'_φ est non ramifiée. Nous supposons donc l'extension K_φ/K'_φ ramifiée. Il existe alors deux ordres maximaux $\mathfrak{M}_1$ et $\mathfrak{M}_2$ contenant $eA[G]$, lequel est héréditaire si et seulement si la ramification de K_φ/K'_φ est modérée, c'est-à-dire si $p\neq 2$ ([8]).

Soit M un $eA[G]$-module de rang r. Nous allons lui associer deux invariants, de la façon suivante : désignons par σ_V un générateur du groupe V.

Comme $e(\sigma_V - 1)$ est une uniformisante de K_φ, le A-module quotient $(1+\tau)M/(\sigma_V-1)M \cap (1+\tau)M$ est un A/pA-espace vectoriel, de dimension finie $\leq 2r$. On pose :

$$d(M) = \dim_{A/pA}[(1+\tau)M/(\sigma_V-1)M \cap (1+\tau)M] ,$$

et de même, si $p \neq 2$:

$$d'(M) = \dim_{A/pA}[(1-\tau)M/(\sigma_V-1)M \cap (1-\tau)M] .$$

PROPOSITION 5. - Soit $e \in \mathcal{E}$ tel que l'ordre $eA[G]$ ne soit pas maximal, et soit M un $eA[G]$-module de rang r. Alors :

(i) si p est différent de 2, on a $d(M) + d'(M) = 2r$;

(ii) supposons $r = 1$. Le module M est libre sur $eA[G]$ si et seulement si $d(M)$ et $d'(M)$ sont non nuls.

Démonstration. - Il suffit de calculer les invariants d et d' relatifs aux ordres $\mathfrak{M}_1$, $\mathfrak{M}_2$, $\mathfrak{M}_1 \cap \mathfrak{M}_2$ et $eA[G]$. Pour cela, nous utilisons un isomorphisme de $eK[G]$ sur l'algèbre de matrices $M_2(K'_\varphi)$ tel que l'image de $eA[G]$ soit contenue dans l'ordre héréditaire suivant, où $\mathfrak{p}'$ est l'idéal premier de A'_φ :

$$\begin{pmatrix} A'_\varphi & \mathfrak{p}' \\ A'_\varphi & A'_\varphi \end{pmatrix} .$$

3. - Ramification

Pour toute la suite du paragraphe, L/K désigne une extension cyclique ou diédrale, et on pose $q = |A/pA|$.

Notons G_i, $i \geq 0$, les sous-groupes de ramification de $G = Gal(L/K)$. On sait que G_1 est le p-sous-groupe de Sylow du groupe d'inertie G_o ([9]). Posons $r = (G_o : G_1)$. Remarquons que, puisque les groupe G_i/G_{i+1} $(i \geq 1)$ sont de type $(p, p, \ldots, p)$, il nous suffit de préciser les sous-groupes G_i non cycliques, ainsi que la suite $(t_i)_{i \geq 1}$ des indices inférieurs de ramification.

Si le groupe G_1 est cyclique, d'ordre p^n, les t_i vérifient :

$$(1) \qquad t_i = \frac{1}{p-1} rp^i - \left(\frac{rp}{p-1} - t_1\right) \qquad 1 \leq i \leq n .$$

Si de plus G_o est cyclique, on a $t_1 = r$ sauf peut-être lorsque $p = 2$, auquel cas on peut aussi avoir $t_1 = 2r$. En outre r divise $q-1$ ou $q+1$ selon que G est cyclique ou diédral ([2]).

Si G_1 n'est pas cyclique, ce qui suppose $p = 2$, nous utilisons les résultats de Fontaine relatifs aux 2-extensions diédrales ([4]). Résumons les différentes possibilités pour une extension diédrale :

PROPOSITION 6. - On suppose G diédral, et l'on note H (*) le sous-groupe cyclique d'indice 2 de G, et V le p-sous-groupe de Sylow de H. Soit enfin u l'indice de H dans V. Alors u divise $q+1$, et on a $G_o = H$ sauf peut-être lorsque $u \leq 2$, auquel cas on peut aussi avoir la situation suivante :

1) si $p \neq 2$, G_o est diédral d'indice u dans G, $G_1 = H \cap G_o$, et les t_i sont donnés par la formule (1) avec $r = 2$ et $t_1 = 1$ sauf peut être pour $p = 3$ où l'on peut avoir $t_1 = 3$,

2) si $p = 2$, $G_o = G$ sauf peut-être lorsque G est d'ordre 8 (auquel cas G_o peut être diédral d'indice 2), $G_1 = G_o$, et l'un des trois cas suivants :

(I) $G_2 = H \cap G_1$, les t_i vérifient (1) avec $r = t_1 = 1$,

(II) G_2 d'indice 2 dans $H \cap G_1$, et $t_i = 2^{i+1} - 3$ pour $i \geq 1$,

(III) G_2 est diédral d'indice 2 dans G_1, $G_3 = G_2$, $G_4 = H \cap G_2$, et, pour $i \geq 3$, $t_i = 2^i - 3$.

Remarque. - Par la théorie du corps de classes local, on montre que tous les cas énumérés ci-dessus se présentent effectivement. Cependant, si on se limite à $K = \mathbb{Q}_p$, il faut ajouter, lorsque $p = 2$, les restrictions suivantes : lorsque G_o est cyclique, le cas $t_1 = r$ suppose G_1 d'ordre 2. Lorsque G_o est diédral, le cas (II) exige $(G:1) = 8$ et $(G_o:1) = 4$.

Ramification presque-maximale. - Soit J un sous-groupe de G. On note L^J le sous-corps de L fixe par J, B^J son anneau de valuation, et v_J la valuation de L^J. L'idéal fractionnaire $e_J B$ de L^J contient B^J. S'il est entier pour tout sous-groupe J compris entre deux groupes de ramification consécutifs, on dit que la ramification de L/K est presque-maximale ([5]).

(*) lorsque G est d'ordre 4, on suppose H convenablement choisi.

La connaissance de la suite $(G_i)_{i\geq 0}$ permet de calculer les valuations $v_J(e_J B)$, ([9]), et nous obtenons en particulier :

COROLLAIRE. - On suppose l'extension L/K (cyclique ou diédrale) sauvagement ramifiée. La ramification est presque-maximale si et seulement si l'une des conditions suivantes est vérifiée :

(i) le groupe G_o est cyclique d'ordre rp^n (avec r premier à p), et l'on a $r \leq p-1$, ou alors $p=2$ et $t_1 = 2r$,

(ii) le groupe G_o est diédral, et l'on a $p=3$ et $t_1 = 3$, ou alors $p=2$ avec une ramification de type (I).

4. - Structure de B sur son ordre associé $\mathfrak{O}$ dans $K[G]$

Pour déterminer l'ordre $\mathfrak{O}$, on peut supposer l'extension totalement ramifiée, grâce à un résultat de Jacobinski ([5]) :

LEMME 3. - Soit L/K une extension galoisienne finie du corps local K. L'ordre $\mathfrak{O}$ est induit de G_o à G par l'ordre $\mathfrak{O}_o$ associé à B dans l'algèbre $K[G_o]$.

Ainsi, supposons par exemple l'extension L/K cyclique avec une ramification presque-maximale. L'ordre $\mathfrak{O}_o$ est alors l'ordre maximal de $K[G_o]$ (cf. I), et, d'après la proposition 4, B est libre sur $\mathfrak{O} = \langle A[G], e_{G_i} \rangle_{i\geq 1}$.

Nous caractérisons maintenant les extensions diédrales pour lesquelles B est projectif sur $\mathfrak{O}$:

PROPOSITION 7. - On suppose G diédral. Alors le $\mathfrak{O}$-module B est projectif si et seulement si l'une des conditions suivantes est vérifiée :

(i) la ramification est presque-maximale. On a alors :

$$\mathfrak{O} = \langle A[G], e_{G_i} \rangle_{i\geq 1},$$

(ii) la ramification n'est pas presque-maximale, et le groupe G_o est diédral d'ordre 2p. On a alors :

$$\mathfrak{O} = \langle A[G], 2e_{G_o} \rangle.$$

Dans les deux cas, le $\mathfrak{O}$-module B est libre.

Démonstration. - Nous nous bornons au cas où G_o est diédral (pour les autres cas, voir [2]). Nous conservons les notations de I. De plus, si V_i, $0 \leq i \leq n$, désigne le sous-groupe cyclique d'ordre p^i de H, nous écrivons L_i, B_i, v_i au lieu de L^{V_i}, B^{V_i}, v_{V_i}. Supposons d'abord que la ramification est presque-maximale, donc que l'on a $\mathfrak{O} \supset <A[G], e_{G_i}>_{i \geq 1}$. Pour montrer l'égalité, nous supposons $G = G_o$ (lemme 3). Soit $e \in \mathcal{S}$ un idempotent central primitif de $K[G]$; il appartient à $\mathfrak{O}$ sauf peut-être lorsque $p = 2$. Si e appartient à $\mathfrak{O}$, le facteur eB est libre sur $eA[G]$ (proposition 5). En effet, lorsque $eA[G]$ n'est pas maximal, les invariants $d(eB)$ et $d'(eB)$ ne sont pas nuls ($\sigma_V \in G_3$, $\tau \notin G_2$). Lorsque $p = 2$, on a :

$$\bigoplus_{e \notin \mathfrak{O}} e\mathfrak{O} = (e_{n-1} - e_n) A[G] \simeq A[\mathbb{Z}/2\mathbb{Z}],$$

et on conclut grâce au lemme 2. D'après la proposition 5, il reste à étudier, dans le cas $p = 2$ et $G \neq G_o$, les composantes $\frac{1}{2}(1 \pm \tau) e_1 B$, ce qui est immédiat (lemme 2).

Désormais, nous supposons que la ramification n'est pas presque-maximale. Traitons d'abord le cas $p \neq 2$. Le groupe G_o est alors d'ordre $2p^n$. On montre (en utilisant la proposition 6) que :

$$\mathfrak{O} = <A[G], \frac{1+\tau}{2} e_i, (\sigma_V - 1) e_i>_{i \geq 1}.$$

Cet ordre est donc contenu dans l'ordre :

$$\mathfrak{O}^* = <A[G], e_i>_{i \geq 1} = <A[G], e>_{e \in \mathcal{S}}.$$

LEMME 4. - *Soit* M *un* $\mathfrak{O}$*-module projectif de rang* r, *et soit* M^* *le* $\mathfrak{O}^*$*-module* $\mathfrak{O}^* M$. *Soit* $e \in \mathcal{S}$ *tel que l'ordre* $eA[G]$ *ne soit pas maximal. Alors on a* $d(eM^*) = r$.

[Cela étant évident lorsque M est libre sur $\mathfrak{O}$, il suffit de vérifier, pour M projectif sur $\mathfrak{O}$, l'inégalité $d'(eM^*) \geq r$. Soit $M' = \{x \in M ; \sigma_V(x) = x \text{ et } \tau x = -x\}$. On montre, en se ramenant au cas $M = \mathfrak{O}$, que l'application $(1-\tau) ey \longrightarrow (1-\tau) e_n y$ induit une application A/pA-linéaire et surjective de l'espace vectoriel $(1-\tau) eM^* / (\sigma_V - 1) eM^* \cap (1-\tau) eM^*$ sur l'espace M'/pM', qui est de dimension r.] Supposons alors $n > 1$, et montrons que, pour $e = e_{n-1} - e_n$, on a $d(eB^*) = 0$, c'est-à-dire $\frac{1+\tau}{2} eB \subset (\sigma_V - 1) eB$. Il suffit de prouver l'inclusion entre les ensembles de valuations correspondants. Or, puisque $n > 1$, on a $v_{n-1}(e_{n-1} B) = -1$,

et donc tout entier ≥ 0 non congru à 1 modulo p appartient à l'ensemble $v_{n-1}((\sigma_V - 1)eB)$ (car $\sigma_V \in G_1 \setminus G_2$). Par ailleurs, dans $(1+\tau)eB$, les valuations sont paires et non congrues à 1 modulo p (les éléments de eB ont une trace nulle sur L_n). Ainsi, d'après le lemme 4, le $\mathfrak{O}$-module B n'est pas projectif dans le cas $n>1$. Par contre, on montre que, lorsque $n=1$, il est libre (on se ramène au cas $G=G_o$ traité dans [1]). Plaçons-nous désormais dans le cas $p=2$. Le groupe G_o est alors d'ordre 2×2^n. Lorsque $n=1$ (G est alors d'ordre 4 ou 8, et $G_2=(1)$), on vérifie que tout élément $x \in B$ tel que $e_{G_o} x$ ne soit pas entier est une base de B sur l'ordre $\mathfrak{O} = <A[G], 2e_{G_o}>$. Lorsque n est supérieur à 1, B n'est pas projectif sur $\mathfrak{O}$. Montrons-le par exemple lorsque la ramification est de type (II) ($G = G_o = G_1$, $G_2 = V_{n-1}$). Alors on a $2e_G B = 2e_G B_{n-1} = B_n$. On en conclut que tout $\mathfrak{O}$-module M projectif, de rang déterminé, vérifie $e_G M^{V_{n-1}} \subset M$, (et donc que B n'est pas projectif). En effet, il suffit de prouver cette inclusion pour $M = \mathfrak{O}$. Choisissons $x_1 \in B_{n-1}$ tel que $v_n(2e_G x_1) = 0$, et $x_2 \in B$ tel que $v_n(2e_G x_2) > 0$ et $v_{n-1}((1+\tau)e_{n-1}x_2) = 0$. Soit alors $\lambda \in \mathfrak{O}^{V_{n-1}}$: cet élément appartient à l'ordre maximal $Ae_G \oplus A\frac{1-\tau}{2}e_n \oplus A\frac{1+\tau}{2}(e_{n-1}-e_n) \oplus A\frac{1-\tau}{2}(e_{n-1}-e_n)$ de l'algèbre $e_{n-1}K[G]$. En appliquant $(1+\tau)\lambda$ à x_1 et x_2, on prouve qu'en fait $e_G \lambda \in 2Ae_G$. Le cas de la ramification de type (III) se traite de façon analogue (avec $\frac{1}{2}(\sigma_V - 1)$ au lieu de e_G).

§ . 3. - Extension diédrale d'un corps de nombres

Notations et hypothèses

Soit F un corps de nombres, et soit N/F une extension diédrale, de groupe de Galois G. On note $\mathbb{Z}_F$ et $\mathbb{Z}_N$ les anneaux d'entiers de F et N. Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_F$, absolument non ramifié, et non modérément ramifié dans l'extension N/F. On désigne par $(G_i)_{i\geq 0}$ les sous-groupes de ramification d'un idéal premier $\mathfrak{P}$ de $\mathbb{Z}_N$ au-dessus de $\mathfrak{p}$. Soit H le sous-groupe cyclique d'indice 2 de G (lorsque G est d'ordre 4, on suppose H convenablement choisi). On pose $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

THÉORÈME. - *Le complété $\mathbb{Z}_{N,\mathfrak{P}}$ est projectif sur son ordre associé dans $F_{\mathfrak{p}}[G]$ si et seulement si l'une des trois conditions suivantes est vérifiée* :

(i) la ramification est presque-maximale et G_1 est inclus dans H . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], e_{G_i}>_{i\geq 1}$;

(ii) la ramification est presque-maximale, G_1 n'est pas inclus dans H , G_2 est inclus dans H , et l'indice de G_o dans G n'est pas divisible par 4 . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], e_J, e_{G_i}>_{i\geq 2}$ où J est le plus petit sous-groupe distingué de G contenant G_o ;

(iii) la ramification n'est pas presque-maximale, le groupe G_o est d'ordre 2p et d'indice 1 ou 2 dans G . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], 2e_{G_o}>$.

Notons que le cas (ii) suppose $p=2$.

Remarque. - Ainsi, si $\mathbb{Z}_N$ est projectif sur son ordre associé $\mathfrak{O}$, il est localement libre sur $\mathfrak{O}$ (puisque cela est vrai aussi en tout $\mathfrak{p}$ modérément ramifié dans N). On peut conjecturer que ce résultat est général.

Exemples. - Prenons $F=\mathbb{Q}$.

1) Si G est le groupe diédral d'ordre 2ℓ , ℓ premier, alors l'extension $N/\mathbb{Q}$ vérifie, pour tout premier p , les conditions du théorème. En fait, $\mathbb{Z}_N$ est alors libre sur son ordre associé ([2], [7], [6]).

2) Si G est le groupe diédral d'ordre 4ℓ , ℓ premier, il est possible que $\mathbb{Z}_{N,2}$ ne soit pas projectif sur son ordre associé, soit parce que la structure locale n'est pas triviale [exemple (avec $\ell=3$) : $N=\mathbb{Q}(\sqrt[12]{1}, \sqrt{2})$], soit parce que l'induction ne conserve pas la projectivité [citons l'exemple (avec $\ell=2$) $\mathbb{Q}(\sqrt{-7}, \sqrt{\frac{-1+\sqrt{-7}}{2}}, \sqrt{\frac{-1-\sqrt{-7}}{2}})$ dû à S.M.J. Wilson].

3) Soit p un nombre premier impair. On peut construire une extension diédrale $N/\mathbb{Q}$, de degré $2p^n$ par exemple, qui ne vérifie pas, pour p , les conditions du théorème : considérons le corps quadratique imaginaire $k=\mathbb{Q}(\sqrt{-p})$ lorsque $p\neq 3$, $k=\mathbb{Q}(\sqrt{-6})$ lorsque $p=3$, et soit $\mathfrak{p}$ l'idéal premier de k au-dessus de p ; la théorie du corps de classes montre qu'il existe une extension N/k , cyclique de degré p^2 , de conducteur $\mathfrak{p}^{2n}$, qui convient.

La suite du paragraphe est consacrée à la démonstration du théorème. Nous posons $K=F_{\mathfrak{p}}$, $L=N_{\mathfrak{P}}$, et nous reprenons les notations du paragraphe 2 . Notons $\mathfrak{O}_o$ l'ordre associé à B dans $K[G_o]$. Lorsque $\mathbb{Z}_{N,\mathfrak{p}}$ est projectif sur son

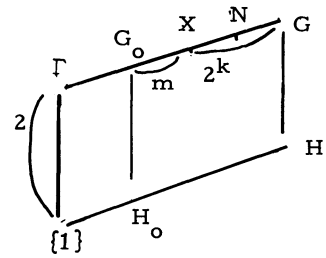
ordre associé dans $K[G]$, il est isomorphe au G-module $\mathrm{Ind}_{G_o}^{G} \mathfrak{O}_o$ (propositions 2 et 7, et lemme 3). Nous allons donc étudier ce module, en nous bornant aux cas où la structure locale est triviale, et où G est d'ordre supérieur à 4. Dans le cas (i), l'ordre $\mathfrak{O}_o$ est engendré, dans $K[G_o]$, par des idempotents e_J tels que J soit distingué dans G. Le G-module $\mathrm{Ind}_{G_o}^{G} \mathfrak{O}_o$ est donc l'anneau engendré dans $K[G]$ par les e_J, ce qui achève l'étude du cas (i). Supposons maintenant que l'extension locale L/K soit cyclique, avec une ramification non presque-maximale. La structure locale peut être triviale (voir [2]), mais l'ordre $\mathfrak{O}_o$ n'est pas invariant par conjugaison par un élément $\tau \in G \setminus H$ (cf. [2], théorème 1 et lemme 5). L'induction ne conserve donc pas la projectivité. Nous supposons désormais G_o non inclus dans H. Il est alors produit semi-direct du groupe $H_o = H \cap G_o$ par un groupe Γ d'ordre 2. D'après la proposition 7, il nous reste à examiner les trois cas suivants :

α) $p=2$ et $\mathfrak{O}_o = \langle A[G_o], e_{G_o}, e_{H'} \rangle_{H' \subset H_o}$

β) $p=2$, $(G_o:1)=4$, et $\mathfrak{O}_o = \langle A[G_o], e_{G_o}, e_\Gamma \rangle$

γ) $(G_o:1)=2p$, et $\mathfrak{O}_o = \langle A[G_o], 2e_{G_o} \rangle$.

Posons $(G:G_o) = m2^k$, où m est impair, et soient X le sous-groupe d'indice 2^k de G contenant G_o, et N le normalisateur de X dans G :



Enfin, nous notons s le plus petit entier tel que $se_{G_o} \in \mathfrak{O}_o$ ($s=1$ ou 2).

a) Etudions l'induction de G_o à X. Dans le cas α), posons $(G_o:1)=2^{n+1}$, et montrons, par récurrence sur $n \geq 0$, que $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ est libre sur l'ordre $\langle A[X], e_X, e_{H'} \rangle_{H' \subset G_o}$: on utilise la relation $\mathfrak{O}_o = e_1 \mathfrak{O}_o \oplus (1-e_1)\mathfrak{O}_o$, où le X-module $\mathrm{Ind}_{G_o}^{X} (1-e_1)\mathfrak{O}_o$ est un ordre de $(1-e_1)K[X]$. On est ainsi ramené au cas $n=0$, pour lequel $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ est égal à l'ordre maximal $\langle A[X], e_X \rangle$ de $K[X]$ (voir II). Dans les cas β) et γ) au contraire, l'idempotent e_{H_o} n'appartient

pas à $\mathfrak{O}_o$. L'ordre $\mathfrak{x}$ associé à $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ dans $K[X]$ possède donc la propriété suivante : $\mathfrak{x}^{G_o} \subset \mathrm{Ams}\, e_X + 2p e_{G_o} A[X]$. Supposons alors que $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ soit projectif sur $\mathfrak{x}$. D'après le lemme 1 , l'élément $s e_{G_o}$ peut s'écrire

$$s e_{G_o} = \sum_{i=1,\ldots,k} \lambda_i x_i \text{ , avec } \lambda_i \in \mathfrak{x}^{G_o} \text{ , } x_i \in \mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o \text{ .}$$

On en déduit que e_{G_o} appartient à $\mathrm{Am}\, e_X + p \sum_{x \in X} A e_{G_o} x$, d'où $X = G_o$.

b) Nous étudions l'induction de X à N de l'ordre $\mathfrak{x}$ égal à $\langle A[X], e_X, e_{H'} \rangle_{H' \subset G_o}$ dans le cas α), à $\langle A[X], e_X, e_\Gamma \rangle$ dans le cas β), et à $\langle A[X], e_X \rangle$ dans le cas γ), le groupe X étant d'ordre $2p$ dans les cas β) et γ). Dans le cas β), le N-module $\mathrm{Ind}_X^N \mathfrak{x}$ n'est projectif sur son ordre associé que lorsque $N = X$, et donc $G = X$ (proposition 3). Dans les cas α) et γ) par contre, $\mathrm{Ind}_X^N \mathfrak{x}$ est un ordre, que nous notons $\mathfrak{N}$, et dont nous étudions l'inductions de N à G .

c) Pour montrer que, si $N \neq G$, $\mathrm{Ind}_N^G \mathfrak{N}$ n'est pas projectif sur son ordre associé, on peut se borner au cas où N est d'indice 2 dans G ; il suffit alors de vérifier que $\mathfrak{N}$ n'est pas projectif sur l'ordre $\mathfrak{N}^* = \bigcap_{s \in G} s \mathfrak{N} s^{-1}$ de $K[N]$. Pour cela, on procède comme dans a), à partir de l'inclusion

$$(\mathfrak{N}^*)^X \subset 2s A e_N + ps e_X A[X] \text{ .}$$

-:-:-:-

BIBLIOGRAPHIE

[1] A.-M. BERGÉ, Sur l'arithmétique d'une extension diédrale, Ann. Inst. Fourier, 22, 2 (1972), 31-59.

[2] A.-M. BERGÉ, Arithmétique d'une extension galoisienne à groupe d'inertie cyclique, Ann. Inst. Fourier, 28, 4 (1978), 17-44.

[3] H. CARTAN and S. EILENBERG, Homological Algebra, Princeton Univ. 1956.

[4] J.-M. FONTAINE, Groupes de ramification et représentations d'Artin, Ann. Scient. Ec. Norm. Sup., 4e série, t. 4 (1971), 337-392.

[5] H. JACOBINSKI, Über die Hauptordnung eines Körpers als Gruppenmodul, J. reine angew. Math. 213 (1963), 151-164.

[6] H.W. LEOPOLDT, Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers, J. reine angew. Math. 201 (1959), 119-149.

[7] J. MARTINET, Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p, Ann. Inst. Fourier, 19 (1969), 1-80.

[8] M. ROSEN, Representations of twisted group rings, Ph. D. Thesis, Princeton Univ., 1963.

[9] J.-P. SERRE, Corps locaux, 2e éd., Hermann, Paris, 1968.

-:-:-:-

Anne-Marie BERGÉ
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX

Astérisque

DANIEL BERTRAND

Fonctions modulaires et indépendance algébrique (II)

Astérisque, tome 61 (1979), p. 29-34

<http://www.numdam.org/item?id=AST_1979__61__29_0>

Société Mathématique de France
Astérisque 61 (1979) p. 29-34

FONCTIONS MODULAIRES ET INDEPENDANCE ALGEBRIQUE (II).

par

Daniel BERTRAND

Soit, pour $k = 1,2$ et 3, E_{2k} la série d'Eisenstein normalisée de poids $2k$:

$$E_{2k}(q) = 1 + (-1)^k (4k/B_k) \sum_{n=1}^{+\infty} n^{2k-1} (q^n/(1-q^n)) \quad ,$$

où B_k désigne le k-ième nombre de Bernoulli . Les récents travaux de G. V. Choodnovsky sur les constantes de la théorie des fonctions elliptiques de Weierstrass fournissent des résultats d'indépendance algébrique concernant les valeurs de ces séries. Nous en établissons ici des versions p-adiques (théorèmes 1 et 3). Nous généralisons et précisons ainsi les résultats de [3].

De même que dans [2] et [3], c'est aux fonctions elliptiques de Tate (cf. [8]) que l'on fait jouer le rôle habituel des fonctions de Weierstrass. Mais ces fonctions admettent deux singularités essentielles, et les majorations analytiques de la théorie des nombres transcendants doivent être adaptées à cette nouvelle situation. Nous ferons ainsi appel au lemme de Schwarz sur les couronnes établi dans [2] et au lemme sur les zéros de "polynômes elliptiques" de [3]. Nous poursuivons ce programme en donnant des estimations analytiques des coefficients de ces polynômes (lemmes 1 et 2), dont le principe remonte aux travaux de Fel'dman et Masser (cf. [6]) . On peut alors calquer les démonstrations sur les méthodes de Choodnovsky.

§ 1. INDEPENDANCE ALGEBRIQUE

Soit Ω un corps ultramétrique complet de caractéristique nulle, et de caractéristique résiduelle non nulle. L'idéal maximal $\mathfrak{M}$ de son anneau d'entiers est le domaine d'analyticité des séries E_{2k} .

Théorème 1 : Soit q un élément non nul de $\mathfrak{M}$. Le degré de transcendance du corps $\mathbb{Q}(E_2(q), E_4(q), E_6(q))$ sur $\mathbb{Q}$ est ≥ 2.

Esquisse de la démonstration : Précisons tout d'abord quelques notations et définitions :

- on désigne par $|\ |$ la valeur absolue (ultramétrique) de Ω ,
- par taille d'un polynôme à coefficients entiers rationnels, on entend le maximum de ses degrés partiels et des logarithmes des valeurs absolues archimédiennes de ses coefficients.
- pour tout entier $n \geq 0$, on note $\mathcal{C}_n$ la couronne $\{z \in \Omega,\ |q|^n \leq |z| \leq |q|^{-n}\}$. Si f est une fonction analytique sur $\mathcal{C}_n$, on pose : $\|f\|_n = \sup_{z \in \mathcal{C}_n} |f(z)|$.
- on note $\ominus$ la fonction thêta fondamentale définie dans [8], formule (6), ζ sa dérivée logarithmique pour l'opérateur de dérivation $D = z(d/dz)$, et $\wp$ la dérivée de $-\zeta$, de sorte que, si K désigne le corps $\mathbb{Q}(E_2(q), E_4(q), E_6(q))$, l'algèbre $K[\zeta, \wp, D\wp]$ est stable par D.
- les lettres $c_1, c_2, \ldots$ désignent des nombres réels > 0 effectivement calculables en fonction de q.

Supposons que, contrairement à la conclusion du théorème 1, le corps K soit une extension algébrique d'une extension transcendante (cf. [2]) $\mathbb{Q}(\omega)$, et soit N un entier $> c_1$. Le principe des tiroirs de Dirichlet permet de construire un polynôme non nul $Q(X,Y)$, de degrés partiels $\leq L = [c_2 N]$, dont les coefficients sont des éléments de $\mathbb{Z}[\omega]$, de degrés $\leq c_3 N$, de tailles $\leq c_4 N \log N$, tel que la fonction $F = Q(\zeta, \wp)$ admette les points $\{-q^n ;\ n = 0, \ldots, N\}$ pour zéros d'ordre $\geq c_3 N$. En vertu du lemme de Schwarz ([2], lemme 2), on a alors : $\|\ominus^{3L} F\|_{c_5 N} \leq \exp(-c_6 N^3)$.

Dans ces conditions, une majoration ([3], lemme) du nombre de zéros de F sur la couronne $\mathcal{C}_{c_5 N}$ assure l'existence d'un élément non nul Q_N de $\mathbb{Z}[X]$, de degré $\leq c_6 N$, de taille $\leq c_7 N \log N$, tel que $|Q_N(\omega)| \leq \exp(-c_8 N^3)$.

L'existence d'une telle suite de polynômes $\{Q_N ; N \geq c_1\}$ contredit le lemme 10 de [1] (analogue p-adique de critère de transcendance

de Gel'fond). ∎

Soient $J(q)$ la fonction modulaire $1728(1-(E_6^2(q)/E_4^3(q))^{-1}$, et θ l'opérateur de Ramanujan $q(d/dq)$. Des formules classiques permettent d'énoncer le théorème 1 sous la forme équivalente suivante : pour tout élément $q \neq 0$ de $\mathcal{M}$, le degré de transcendance du corps $\mathbb{Q}(J(q), \theta J(q), \theta^2 J(q))$ sur $\mathbb{Q}$ est ≥ 2. En particulier (cf. [3], théorème 1), si $J(q)$ est algébrique, les nombres $\theta J(q)$ et $\theta^2 J(q)$ sont algébriquement indépendants. C'est cet énoncé que nous précisons au paragraphe 3. Nous utiliserons à cet effet une mesure de transcendance de $\theta J(q)$.

§ 2. UNE MESURE DE TRANSCENDANCE

L'énoncé suivant est l'analogue p-adique d'un résultat d'E. Reyssat ([7], théorème 1 (12)) sur le quotient par π des périodes des fonctions elliptiques de Weierstrass. Il améliore le théorème 2 de [3], dont la démonstration était fondée sur l'étude des points de torsion des courbes elliptiques. La nouvelle démonstration s'inspire de la démarche de [7].

Théorème 2 : Soit q un élément non nul de $\mathcal{M}$, tel que $J(q)$ soit algébrique. Il existe un nombre réel $C_1 > 0$, effectivement calculable en fonction de q, tel que, pour tout élément non nul P de $\mathbb{Z}[X]$, de taille $\leq t$, on ait :

$$|P(\theta J(q))| > \exp(-C_1 t^2 (\mathrm{Log}\, t)^4) .$$

Esquisse de la démonstration : on reprend les notations du paragraphe 1. De plus :

- l'hypothèse faite sur $J(q)$ amène à normaliser les fonctions de Tate de la façon suivante : on pose $\gamma = (E_4(q)/E_6(q))^{1/2}$ et $\varphi = \gamma^2(\wp + (E_2(q)/12))$. Alors l'équation différentielle algébrique satisfaite par φ, relativement à l'opérateur $\Delta = \gamma D$, est définie sur le corps de nombres $\mathbb{Q}(J(q))$.

- pour tout entier $n \geq 0$, on note $\mathcal{E}_n$ l'ensemble des translatés du disque $-1+\mathcal{M}$ par les éléments $\{ q^\nu, \nu = -n, \ldots, 0\}$ du groupe multiplicatif $\Omega^\times$. Si f est une fonction analytique sur $\mathcal{E}_n$, on pose : $M(f, \mathcal{E}_n) = \sup_{z \in \mathcal{E}_n} |f(z)|$.

Supposons, ce qui revient à contredire la conclusion du théorème 2, qu'il existe un nombre algébrique α, dont le polynôme minimal sur $\mathbb{Z}$ a une taille $t \geq c_1$, tel que $|\gamma - \alpha| \leq \exp(-t^2(\mathrm{Log}\, t)^4)$, et posons :

$L_1 = [t]$, $L_2 = [c_2 \mathrm{Log} t]$. Le principe des tiroirs permet de construire un polynôme non nul $Q(X,Y)$, de degrés partiels $\leq L_1, L_2$ respectivement, dont les coefficients sont des éléments de $\mathbb{Z}[\alpha]$, de degrés majorés par le degré d de α, de tailles $\leq c_3 t (\mathrm{Log} t)((t/d) + \mathrm{Log}\, t)$, tel que la fonction $F(z) = Q(z,\varphi(z))$ vérifie :

$$\| \ominus^{2L_2} F \|_{[t]} \leq \exp(-c_4 t^2 (\mathrm{Log} t)^3) .$$

Cette inégalité permet de majorer $M(F, \mathcal{E}_{[t]})$. Or on a :

Lemme 1 : Soit Q un élément de $\Omega[X,Y]$, de degrés partiels $\leq L_1$, L_2 respectivement. Les coefficients de Q sont, en valeur absolue, majorés par

$$M(Q(z,\varphi(z)), \mathcal{E}_{L_1}) \exp(c(L_1^2 + L_2)),$$

où $c = c(q)$ désigne un nombre réel > 0.

La majoration déduite du lemme 1 est incompatible avec la majoration de la taille des coefficients de Q. ∎

§ 3. UNE MESURE D'INDEPENDANCE ALGEBRIQUE

Dans la démonstration ci-dessous, la construction des polynômes R_N suit la méthode de Gel'fond et Fel'dman ([5], p.498), telle qu'elle a été adaptée au cas elliptique par Choodnovsky. Nous renvoyons à [1] pour les analogues p-adiques des lemmes sur les résultants utilisés dans [5].

Théorème 3 : Soit q un élément non nul de $\mathcal{M}$ tel que $J(q)$ soit algébrique. Il existe un nombre réel $C_2 > 0$, effectivement calculable en fonction de q, tel que, pour tout élément non nul P de $\mathbb{Z}[X,Y]$, de taille $\leq t$, on ait :

$$|P(\theta J(q), \theta^2 J(q))| > \exp(-C_2 t^6 (\mathrm{Log} t)^{24}).$$

Esquisse de la démonstration : On reprend les notations des paragraphes 1 et 2. De plus :

- on pose $\xi = \gamma(\zeta + 1/2)$.

Soit N un entier $\geq c_1$. On commence par construire un polynôme non nul $Q(X,Y)$, de degrés partiels $\leq L = [c_2 N]$, dont les coefficients sont des éléments de $\mathbb{Z}[\theta J(q), \theta^2 J(q)]$, de degrés partiels $\leq c_2 N$, de tailles $\leq c_3 N \operatorname{Log} N$, tel que la fonction $F = Q(\xi, \varphi)$ admette les points $\{-q^n ; n = 0, \ldots, N\}$ pour zéros d'ordre $\geq c_4 N$. On a alors : $\| \ominus^{3L_F} \|_{c_5 N} \leq \exp(-c_6 N^3)$. Par ailleurs :

Lemme 2 : Soit Q un élément de $\Omega[X,Y]$, de degrés partiels $\leq L_1, L_2$. Les coefficients de Q sont, en valeur absolue, majorés par :

$$M(Q(\xi,\varphi), \mathcal{E}_{L_1}) \exp(c'(L_1 \operatorname{Log} L_1 + L_2)),$$

où $c' = c'(q)$ désigne un nombre réel > 0.

Soit alors P un élément non nul de $\mathbb{Z}[X,Y]$ (que l'on peut, sans perte de généralité, supposer irréductible), de taille $\leq t$, et tel que $|P(\theta J(q), \theta^2 J(q))| < \exp(-t^6 (\operatorname{Log} t)^{24})$. Le lemme 2, joint à la majoration du nombre de zéros de F utilisée au paragraphe 1, permet, lorsque l'entier N est $\leq c_7 t^2 (\operatorname{Log} t)^8$, de lui associer un élément non nul R_N de $\mathbb{Z}[X,Y]$, de degrés partiels $\leq c_8 N$, de taille $\leq c_9 N \operatorname{Log} N$, premier à P, et tel que :

$$|R_N(\theta J(q), \theta^2 J(q))| < \exp(-c_{10} N^3).$$

Considérons alors le résultant, par rapport à Y, des polynômes $R_{[c_7 t^2 (\operatorname{Log} t)^8]}$ et P. C'est un élément non nul S de $\mathbb{Z}[X]$, de degré $\leq c_{11} t^3 (\operatorname{Log} t)^8$, de taille $\leq c_{12} t^3 (\operatorname{Log} t)^9$, et tel que

$$|S(\theta J(q))| < \exp(-c_{13} t^6 (\operatorname{Log} t)^{24}).$$

D'après le théorème 2, la taille t de P est donc bornée. ∎

Signalons pour conclure que Choodnovsky a récemment amélioré l'analogue complexe du théorème 3 (cf. [4], théorème 5.7) : il peut ainsi y remplacer l'exposant 6 par 4,2, et même, annonce-t-il, par 3.

***

[1] W. W. Adams : Transcendental numbers in the p-adic domain, Amer. J. Math., 88, 1966, pp.279-308.

[2] D. Bertrand : Séries d'Eisenstein et transcendance, Bull. Soc. Math. France, 104, 1976, pp.309-321.

[3] D. Bertrand : Modular functions and algebraic independence, Proc. Conf. "p-adic Analysis", Nijmegen, 1978.

[4] G. V. Choodnovsky : Algebraic grounds for the proof of algebraic independence... Part I. Preprint (1978).

[5] A. O. Gel'fond, N. I. Fel'dman : Sur une mesure de transcendance mutuelle de certains nombres, Izv. A. N. SSSR, Ser. mat., 14, 1950, pp. 493-500 [en russe].

[6] D. Masser : Elliptic functions and transcendance, Springer 1975, Lecture Notes in Maths. No 437.

[7] E. Reyssat : Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle , à paraître.

[8] P. Roquette : Analytic theory of elliptic functions over local fields, Hamburger Math. Einzel.,1, 1970.

Daniel BERTRAND
Centre de Mathématiques
de l'Ecole Polytechnique
Plateau de Palaiseau
91128 Palaiseau Cedex (France)

Astérisque

DAVID W. BOYD

Pisot sequences, Pisot numbers and Salem numbers

Astérisque, tome 61 (1979), p. 35-42

<http://www.numdam.org/item?id=AST_1979__61__35_0>

Société Mathématique de France
Astérisque 61 (1979) p. 35-42

PISOT SEQUENCES, PISOT NUMBERS AND SALEM NUMBERS

by

DAVID W. BOYD

1. The sets S and H: The well known set S of Pisot (or Pisot-Vijayaraghavan) numbers is the set of algebraic integers $\theta > 1$ all of whose other conjugates lie strictly within the unit circle. The initial interest in S stems from the fact that if $\lambda \in \mathbb{Z}(\theta)$, then $\|\lambda\theta^n\| = \mathrm{dist}(\lambda\theta^n, \mathbb{Z}) \to 0$ as $n \to \infty$. Let us denote by H the set of real $\theta > 1$ for which there is a $\lambda > 0$ such that $\|\lambda\theta^n\| \to 0$. A still unanswered question is whether $S = H$. This was considered by Thue [16] and Hardy [17], who showed that if $\|\lambda\theta^n\| = O(b^n)$ with $b < 1$, then $\theta \in S$. Hardy also pointed out that the only algebraic elements in H are the elements of S. Generalizations of this result were given by Vijayaraghavan in [17].

Until recently Pisot's result [13], that $\sum \|\lambda\theta^n\|^2 < \infty$ implies $\theta \in S$ was essentially the closest approach to a proof that $S = H$, but Cantor [7] has recently given a substantial improvement of this which is somewhat technical to describe here. Salem [14] used Pisot's result to prove that the set S is closed and hence is nowhere dense in $[1,\infty)$.

An interesting fact about H is that it is a countable set. Thus, if H contains any transcendental numbers then it does not do so for trivial reasons. We will see Pisot's [13] proof that H is countable in what follows. It should be mentioned that Vijayaraghavan [18] proved that the set of θ for which $\|\theta^n\| \to 0$ is countable by a somewhat different method.

2. E-sequences: Pisot's method of proof is to examine a certain interesting class of sequences of integers, now called E-sequences or Pisot sequences. To see

how these arise, suppose that $a_n = \lambda\theta^n + \varepsilon_n$, where $\lambda > 0$, $\theta > 1$, $a_n \in \mathbb{Z}$ and ε_n is bounded. We observe that

$$a_{n+1}a_{n-1} - a_n^2 = \lambda\theta^{n-1}(\theta^2\varepsilon_{n-1} - 2\theta\varepsilon_n + \varepsilon_{n+1}) + (\varepsilon_{n+1}\varepsilon_{n-1} - \varepsilon_n^2),$$

so that

$$\limsup |a_{n+1} - a_n^2/a_{n-1}| = \limsup |\theta^2\varepsilon_{n-1} - 2\theta\varepsilon_n + \varepsilon_{n+1}| = \delta \text{ ,say.}$$

If $\delta < 1/2$, then eventually a_{n+1} is determined uniquely by a_n and a_{n-1}. By deleting some initial terms, we have that

$$a_{n+1} = N(a_n^2/a_{n-1}) \quad , \quad n = 0,1,\ldots \quad , \tag{1}$$

where $N(x) = [x + 1/2]$ = "the nearest integer to x". The formula (1) defines the E-sequence $E(a_0,a_1)$ for arbitrary integers $0 < a_0 < a_1$. Pisot showed that the limit $a_{n+1}/a_n \to \theta$ always exists, and this defines a certain set E. Clearly E is countable and contains H, ($\delta = 0$), so H is countable. On the other hand E is dense in $[1,\infty)$ so $E \neq S$, since S is nowhere dense by Salem's result.

One can show that $\lambda = \lim a_n/\theta^n$ exists if $\theta > 1$, and if one defines $\varepsilon_n = a_n - \lambda\theta^n$, then the above discussion shows that E is essentially characterized by the inequality

$$\limsup |\theta^2\varepsilon_{n-1} - 2\theta\varepsilon_n + \varepsilon_{n+1}| \leq 1/2 \quad , \tag{2}$$

in the sense that (2) is necessary for a_n to be an E-sequence, while (2) with strict inequality is sufficient for $\{a_{n-n_0}\}$, $n \geq n_0$ to be an E-sequence for some n_0.

In addition to the set S, E also contains the set T of Salem numbers which are real algebraic integers $\theta > 1$ such that all other conjugates lie within the unit circle, with at least one conjugate on the circle. This in fact implies that θ satisfies a reciprocal equation, so its conjugates are θ^{-1} and a certain set of numbers of modulus one [15]. To see that $E \supset T$, just choose $\lambda \in \mathbb{Z}(\theta)$ so that the other conjugates of λ are small enough so that (2) holds.

3. Recurrent E-sequences: The interesting question now is whether $E = S \cup T$, since this would tell us that T is dense in $[1,\infty)$ and hence that $\inf T = 1$, settling Lehmer's conjecture [12]. It would also imply that $H = S$, settling Pisot's conjecture.

One notes that the proof that $E \supset S \cup T$ shows somewhat more, namely that the corresponding E-sequence satisfies a linear recurrence relation, or equivalently that the generating function of the sequence is rational, so

$$\sum_{n=0}^{\infty} a_n z^n = A(z)/Q(z) \quad , \tag{3}$$

where A and Q are polynomials with integer coefficients, and $Q(0) = 1$. In [9], Flor shows that if $E(a_0,a_1)$ satisfies (3), then θ is in S or in T. We shall refer to these two possibilities as S-recurrence and T-recurrence.

In fact, in [13], Pisot already showed that $E(2,a_1)$ and $E(3,a_1)$ are S-recurrent with $\deg(Q) \leq a_0$. For example $E(3,5) = 3, 5, 8, 13, 21, \ldots$ has degree 2. His proof distinguishes $E(a_0,a_1)$ according to the congruence class $a_1 \pmod{a_0^2}$. Cantor [6] has given the explanation of why this is natural, and has studied the families $E(a_0,ma_0^2 + b)$, giving conditions on a_0 and b in order that this sequence is S-recurrent for all $m \geq m_0$. The corresponding generating function is of the form $A(z)/(Q(z) - mzA(z))$.

However, Cantor and his student Galyean [5], by use of a computer algorithm designed for testing for linear recurrences showed that if $E(4,13)$ is recurrent, then $\deg(Q) \geq 100$, suggesting strongly that no such recurrence exists. In his thesis [10], Galyean found many examples of $E(a_0,a_1)$ satisfying no recurrence of degree ≤ 20, when $4 \leq a_0 \leq 10$.

4. Non-recurrent E-sequences: I was aware only of the example $E(4,13)$ when I proved [1] that indeed there are E-sequences which are non-recurrent, and in fact that the set of θ produced from such sequences is dense in $[(\sqrt{5} + 1)/2,\infty)$. The proof is rather amusing since it concentrates its attention on T-recurrence,

which one might expect to be the difficult case. The point is that, although we have very little quantitative information about T itself, T-recurrent sequences are so distinctive that non-T-recurrence is rather easily detected. In principle, S-recurrence causes no difficulty since one can work in intervals disjoint from S. However, as we shall see later, for specific E-sequences, S-recurrence is more difficult to handle because the intervals in the complement of S are extremely short for even moderately large θ.

To see how T-recurrence is dealt with, suppose then that $E(a_0,a_1)$ is T-recurrent, then, taking into account the structure of the conjugates of θ,

$$a_n = \lambda\theta^n + \mu\theta^{-n} + \delta_n \quad , \quad n \geq n_0, \tag{4}$$

where δ_n is a linear combination of powers of numbers of modulus 1 and hence is almost periodic. Using (2) and the almost periodicity of δ_n, we find that, for all n, including negative n,

$$|\theta^2\delta_{n-1} - 2\theta\delta_n + \delta_{n+1}| \leq 1/2 \, . \tag{5}$$

Furthermore, (4) can be used to define a_n for $n < n_0$, and since Q is reciprocal or antireciprocal, one finds that a_n is an integer for all n. Combining these two facts one then obtains a constructive extimate for n_0 (and this is where the condition $\theta > (\sqrt{5} + 1)/2$ seems unavoidable). For example, if $\theta > 2$ then $n_0 = 0$. Assuming then that $n_0 = 0$ (by shifting the sequence if necessary), the conditions that a_n be an integer for $n < 0$, combined with (5), produce various inequalities which must be satisfied by T-recurrent sequences. As a simple example, the condition that a_{-1} is an integer implies that

$$\|a_0^2/a_1\| \leq (1 + 2\theta)/(2\theta^2) + 1/a_1 \, .$$

This is an extremely restrictive condition for large θ, and shows that non-recurrent E-sequences produce a set of θ dense in $[1 + \sqrt{2}, \infty)$.

Applying this inequality to a family $E(a_0, ma_0^2 + b)$ with $b > 0$, we find that $\|a_0^2/a_1\| = a_0^2/a_1$ if $m \geq 2$, while on the other hand $(1+2\theta)/(2\theta^2) + 1/a_1$

is approximately $(a_0 + 1)/a_1$. Thus, within such a family, T-recurrence can only occur if $m = 0$ or 1. As another example consider $E(2m,7m)$ with $m \equiv 1 \pmod 7$. Then $\|a_0^2/a_1\| = 3/7$ while $(1 + 2\theta)/(2\theta^2) \to 16/49 < 3/7$ as $m \to \infty$. Thus, for sufficiently large m, none of these sequences is T-recurrent. Since $\theta \to 7/2 \notin S$ as $m \to \infty$, and since S is closed, it follows that $\theta \notin S$ for sufficiently large m, so $E(a_0,a_1)$ is not S-recurrent either.

5. Specific cases of non-recurrence: In spite of the ease of producing infinitely many non-recurrent E-sequences, one would still like to be able to answer the question of whether any specific $E(a_0,a_1)$ is recurrent or not. In his thesis [10], Galyean conjectured that if $E(a_0,a_1)$ is recurrent, then the degree of the recurrence is at most a_0. A proof of this would certainly provide the desired criterion. A result of this type seems reasonable when one considers that, in an E-sequence $\lambda \approx a_0$, and in order to make ε_n small enough for (2) to hold, it seems necessary to have the other conjugates of λ small. This in turn forces λ to be fairly large since the product of these numbers is at least as large as $1/\mathrm{disc}(\theta)$.

However, lacking such a quantitative result, we have based our proofs of non-recurrence for specific E-sequences on a different method. Proofs of non-T-recurrence are based on refinements of the ideas discussed above. It seems likely that the infinite set of necessary conditions for T-recurrence so obtained are also sufficient; this has certainly proved to be the case in practice. To prove non-S-recurrence we simply have to show that $\theta \notin S$, a constructively feasible procedure since S is closed and since we can generate arbitrarily good approximations to θ. The practical difficulties grow with θ so our success with this method is confined to $\theta < 2.5$. The main tool is a computer algorithm based on ideas of Dufresnoy and Pisot [8] and described in more detail in [3]. It is capable of finding all the elements in $S \cap (\alpha,\beta)$, provided this number is finite. The idea is that, if P is the minimal polynomial of θ, and $Q(z) = z^{\deg(P)}P(z^{-1})$, then

(6) $f(z) = (\operatorname{sgn} P(0))P(z)/Q(z) = u_0 + u_1 z + \ldots$,

where the u_n are integers and where $|f(z)| = 1$ on $|z| = 1$. The u_n are characterized by inequalities obtained from Schur's algorithm:

(7) $$w_n(u_0,\ldots,u_{n-1}) \le u_n \le w_n^*(u_0,\ldots,u_{n-1}) .$$

If in addition $\alpha \le \theta \le \beta$, then there are additional inequalities

(8) $$v_n(u_0,\ldots,u_{n-1};\alpha) \le u_n \le v_n^*(u_0,\ldots,u_{n-1};\beta) .$$

These lead to the search of a finite tree if $S \cap (\alpha,\beta)$ is a finite set.

An instructive example is the sequence E(10,22), with $\theta = 2.190327956...$ The criteria for T-recurrence are easily shown to be violated. A search of a small interval containing θ shows that $\operatorname{dist}(\theta,S) = .905 \times 10^{-8}$, the closest point of S being a root of the following 32nd degree polynomial:

P = 1 -2 0 0 -1 -2 0 0 -2 0 0 0 -1 2 0 0 1 2 0 0 2 0 0 0 1 -2 0 0-1-1 0 0 -1

(notation: a b c ... means $ax^k + bx^{k-1} + \ldots$). Thus E(10,22) is non-recurrent. From Galyean's thesis, we find that E(10,22) is predicted to a_{21} by the generating function $(10 + 2z + 4z^2 + 9z^3)/(1 - 2z - 2z^4)$. However the polynomial $z^4 - 2z^3 - 2$, in addition to a root $\phi = 2.190327947$, has roots $\gamma,\bar{\gamma}$ with $|\gamma| \simeq 1.0157$. Hence this is not the generating function of an E-sequence. The fact that $|\gamma|^{44} < 2$ makes it clear how this sequence can masquerade as an E-sequence for many terms. Intuitively, it appears that E(10,22) is diverted away from nearby S-numbers of small degree by the presence of this "pseudo"-S-number of degree 4. Since $a_0 = 10$ is apparently too small to allow E(10,22) to satisfy a recurrence of high degree, the sequence is unable to satisfy any recurrence whatsoever.

An extremely interesting example of this type, mentioned in [5], is E(6,16) which is connected with the polynomial $P(z) = z^5 - 3z^4 + z^3 - z - 1$, which has roots at $\phi = 2.699...$ and $\gamma, \bar{\gamma}$ with $|\gamma| \simeq 1.007$. This polynomial turns out to be a limit point of polynomials with the same properties. Since $\operatorname{dist}(\phi,S) < 10^{-46}$, we have as yet been unable to show E(6,16) is not S-recurrent.

There are in addition many other examples of non-recurrence which are not explainable by this mechanism. For example, the non-recurrence of $E(7,15)$ seems to be explained by our arbitrary choice of "rounding up" in the definition of $N(x)$. For details of this and other examples, the reader may consult [3].

6. Concluding Remarks: Space has not permitted a discussion of the new characterization of T given in [2], nor the application of the above-mentioned computer algorithm to questions concerning the distribution of T in the real line, but this is adequately described in [3].

As far as applications of E-sequences to finding T-numbers, as suggested in [5], it seems that a more fruitful type of sequence to use is given by the following non-linear recurrence:

$$a_{n+2} = N(a_{n+1}(a_{n+1} + a_{n-1})/a_n - a_n) \quad , \quad n = 1,2,...$$

If one takes $a_0 = 0$, $a_1 > 0$ and $a_2 \geq 2a_1+1$, then one obtains all Salem numbers as limits of the ratios a_{n+1}/a_n. The criterion for T-recurrence is now valid for all $\theta > 1$, because the inequality (5) is replaced by a more amenable form. Some details concerning these sequences are to be found in [4].

REFERENCES

1. D.W. Boyd, Pisot sequences which satisfy no linear recurrence, Acta Arith. 32(1977),pp.89-98.

2. _____ , Small Salem numbers, Duke Math. Jour. 44(1977),pp.315-328.

3. _____ , Pisot and Salem numbers in intervals of the real line, Math.of Comp. (to appear in 1978).

4. _____ , Some integer sequences related to Pisot sequences, Acta Arith.(to appear).

5. D.G. Cantor, Investigation of T-numbers and E-sequences, in Computers in Number Theory, ed A.O.L. Atkins and B.J. Birch, Academic Press, N.Y. 1971.

6. _____ , On families of Pisot E-sequences, Ann.Sci.Éc.Norm.Sup. 4^e Série, 9(1976),pp.283-308.

7. _____ , On power series with only finitely many coefficients (mod 1): solution of a problem of Pisot and Salem, Acta Arith. 34(1977),pp.43-55.

8. J. Dufresnoy and Ch. Pisot, Étude de certaines fonctions méromorphes bornées sur le cercle unité, application à un ensemble fermé d'entiers algébriques, Ann.Sci.Éc.Norm.Sup. 3^e Série, 72(1955),pp.69-92.

9. P. Flor, Über eine Klasse von Folgen natürlicher Zahlen, Math. Annalen 140 (1960),pp.299-307.

10. P. Galyean, On linear recurrence relations for E-sequences, Thesis, University of California Los Angeles, 1971.

11. G.H. Hardy, A problem of diophantine approximation, Jour.Ind.Math.Soc. 11 (1919),162-166; Collected works I, pp.124-129.

12. D.H. Lehmer, Factorization of certain cyclotomic functions, Ann.Math. 34(1933), pp.461-479.

13. Ch. Pisot, La repartition modulo 1 et les nombres algébriques, Ann. Scuola Norm.Sup. Pisa 7(1938),205-248.

14. R. Salem, A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan, Duke Math. Jour. 11(1944),pp.103-107.

15. _____, Power series with integral coefficients, Duke Math. Jour. 12(1945), pp.153-171.

16. A. Thue, Über eine Eigenschaft die keine transzendente Grösse haben kann, Skrifter Vidensk.I. Kristiania 2(1912), No.20, pp.1-15.

17. T. Vijayaraghavan, On the fractional parts of the powers of a number (II), Proc. Camb. Phil. Soc. 37(1941),pp.349-357.

18. _____, On the fractional parts of the powers of a number (III), Jour. Lond. Math. Soc. 17(1942), pp.137-138.

David W. Boyd
Department of Mathematics
University of British Columbia
Vancouver, B.C., Canada
V6T 1W5

Astérisque

PIERRETTE CASSOU-NOGUES

Analogues p-adiques des fonctions Γ-multiples

Astérisque, tome 61 (1979), p. 43-55

<http://www.numdam.org/item?id=AST_1979__61__43_0>

Société Mathématique de France
Astérisque 61 (1979) p. 43-55

ANALOGUES p-ADIQUES DES FONCTIONS Γ-MULTIPLES

par

Pierrette CASSOU-NOGUÈS

-:-:-:-

Soit M une extension abélienne, réelle, finie d'un corps de nombres K totalement réel, de conducteur $\mathfrak{f}$. Soit $K_{\mathfrak{f}}$ l'ensemble des éléments α de K qui sont totalement positifs et congrus à 1 modulo $\mathfrak{f}$ (c'est-à-dire que $v_{\mathfrak{p}}(\alpha-1) \geq v_{\mathfrak{p}}(\mathfrak{f})$ pour tout idéal $\mathfrak{p}$ divisant $\mathfrak{f}$).

Notons $I_{\mathfrak{f}}$ le groupe des idéaux fractionnaires de K, engendré par les idéaux premiers ne divisant pas $\mathfrak{f}$ et $P_{\mathfrak{f}}$ le sous-groupe des idéaux principaux engendrés par les éléments de $K_{\mathfrak{f}}$. Le groupe quotient $I_{\mathfrak{f}}/P_{\mathfrak{f}}$ est appelé le groupe des classes de rayon $\mathfrak{f}$ et est noté $R_{\mathfrak{f}}$. D'après la théorie du corps de classes, l'application d'Artin : $\mathfrak{a} \in I_{\mathfrak{f}} \longmapsto \sigma_{\mathfrak{a}} \in G(M/K)$ induit un homomorphisme surjectif de $R_{\mathfrak{f}}$ sur $G(M/K)$, le groupe de Galois de M sur K. Soit $\mathfrak{X}$ l'ensemble des caractères primitifs associés aux caractères du groupe de Galois de M sur K.

Pour $\chi \in \mathfrak{X}$, de conducteur $\mathfrak{f}(\chi)$, on définit :

$$L(\chi, s) = \sum_{(\mathfrak{a}, \mathfrak{f}(\chi))=1} \chi(\sigma_{\mathfrak{a}})\, N\mathfrak{a}^{-s} \quad \text{pour } \mathrm{Re}(s)>1$$

où la sommation est prise sur les idéaux entiers $\mathfrak{a}$ de K, premiers à $\mathfrak{f}(\chi)$.
On a encore :

$$L(\chi, s) = \sum_{\sigma \in G(M/K)} \chi(\sigma)\, \zeta_M(\sigma, s)$$

où $\zeta_M(\sigma, s)$ est la fonction zêta partielle associée à σ définie par

$$\zeta_M(\sigma, s) = \sum_{\substack{(\mathfrak{a}, \mathfrak{f}) = 1 \\ \sigma_{\mathfrak{a}} = \sigma}} N\mathfrak{a}^{-s} \quad \text{pour } \mathrm{Re}(s) > 1$$

où la sommation est prise sur les idéaux $\mathfrak{a}$ entiers, premiers à $\mathfrak{f}$, tels que $\sigma_{\mathfrak{a}} = \sigma$. Si M est le corps de classes de rayon $\mathfrak{f}$ on notera

$$\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s) = \zeta_M(\sigma_{\mathfrak{a}^{-1}}, s)$$

Shintani [13] a montré que l'on pouvait écrire

$$(1) \qquad \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s) = N\mathfrak{a}^s \sum_{L_{j,x}} Z(NL_{j,x}, s)$$

où les $L_{j,x}$ sont en nombre fini et de la forme

$$(2) \qquad L_{j,x}(y) = x + v_{j,1} y_1 + \ldots + v_{j,r(j)} y_{r(j)} ,$$

$(v_{j,i} \in \mathfrak{a}, \mathfrak{f}\ ,\ v_{j,i} \gg 0\ ,\ x = \Sigma\, x_i v_{j,i}\ ,\ x_i \in \mathbb{Q}\ ,\ 0 < x_i \leq 1\ ,$ et $x \in \mathfrak{a}\ ,\ x \equiv 1 \mod \mathfrak{f}\ )$
et

$$(3) \qquad Z(NL_{j,x}, s) = \sum_{m_1 = 0}^{\infty} \ldots \sum_{m_{r(j)} = 0}^{\infty} N(L_{j,x}(m))^{-s} .$$

On peut montrer [13] que les fonctions $s \longmapsto Z(NL_{j,x}, s)$ se prolongent à tout le plan complexe en des fonctions méromorphes dont les valeurs aux entiers négatifs sont rationnelles, ce qui prouve la rationnalité de $\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, -k)$ pour tout entier k positif ou nul. Ce résultat avait déjà été démontré par Klingen [9] et Siegel [12] en utilisant la théorie des formes modulaires.

Soit $\mathfrak{c}$ un idéal entier de K possédant la propriété suivante

$$(4) \quad \begin{cases} \text{(i)} & (\mathfrak{c}, \mathfrak{f}) = 1 \ ;\ (\mathfrak{c}, \mathfrak{D}) = 1 \text{ où } \mathfrak{D} \text{ désigne la différente de } K \\ \text{(ii)} & (\mathfrak{c}, (v_{j,i})) = 1 \text{ pour tout } j \in J \text{ et tout } i \in \{1, 2, \ldots, r(j)\} \\ \text{(iii)} & O_K/\mathfrak{c} \simeq Z/cZ \text{ si } c \text{ est un générateur positif de } \mathfrak{c} \cap Z . \end{cases}$$

Considérons

$$(5) \qquad \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = N\mathfrak{c}^{1-s}\, \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}\mathfrak{c}^{-1}, s) - \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s) .$$

Soit ν un élément de K tel que $\mathrm{Tr}_{K/\mathbb{Q}}(\nu) = \frac{b}{c}$ où $(b, c) = 1$. On peut alors montrer que

$$(6)\qquad \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = N\mathfrak{a}^{s} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} (\exp 2\pi i \, \mathrm{Tr}_{K/\mathbb{Q}}(\mu\nu x)) \, Z(NL_{j,x}, \xi^{\mu}, s)$$

où $Z(NL_{j,x}, \xi^{\mu}, s) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_{r(j)}=0}^{\infty} \xi_{j,1}^{\mu m_1} \cdots \xi_{j,r(j)}^{\mu m_{r(j)}} NL_{j,x}(m)^{-s}$ et

$\xi_{j,1}, \ldots, \xi_{j,r(j)}$ sont des racines primitives c-ièmes de 1 .

Nous allons étudier une classe de séries de Dirichlet qui contient les fonctions $Z(NL_{j,x}, \xi^{\mu}, s)$. Ceci nous permet, en particulier, de retrouver (cor. 3) le théorème de Deligne et Ribet [6], sur l'existence d'une fonction p-adique $\zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s)$ telle que pour tout entier $k \geq 0$, $k \equiv -1 \mod \delta$ où $\delta | (p-1)$, $\zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, -k) = \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, -k)$. On peut aussi obtenir l'existence d'analogues p-adiques des fonctions Γ-multiples et une formule remarquable (th. 6), généralisant celle de Ferrero [8], qui exprime $L'_p(\chi, 0)$ à l'aide de ces fonctions.

I. - Théorèmes généraux sur les séries de Dirichlet

Soit K un sous-corps de $\mathbb{R}$.

DÉFINITION. - On dira que le polynôme $P \in K[X_1, \ldots, X_r]$ possède la propriété (*), si

$$P(X) = (P_1(X) + a_1)^{\alpha_1} \ldots\ldots (P_t(X) + a_t)^{\alpha_t}$$

où

i) les P_i sont des polynômes homogènes, de même degré strictement positifs, à r variables, à coefficients dans K positifs ou nuls,

ii) les a_i sont des éléments de K strictement positifs,

iii) les α_i sont des nombres entiers positifs ou nuls tels que $\Sigma \alpha_i \neq 0$.

Considérons un polynôme $P \in K[X_1, \ldots, X_r]$ possédant la propriété (*) et $\xi = (\xi_1, \ldots, \xi_r)$ un r-uple formé de racines de l'unité différentes de 1 . Posons :

$$Z(P, \xi, s) = \sum_{n \in \mathbb{N}^r} P(n)^{-s} \xi_1^{n_1} \ldots \xi_r^{n_r} .$$

Il existe un σ_o tel que cette série converge dans le demi-plan $\mathrm{Re}(s) > \sigma_o$ et on

se propose d'étudier son prolongement. Le résultat est le suivant :

THÉORÈME 1. - La fonction $s \longmapsto Z(P, \xi, s)$ se prolonge à tout le plan complexe en une fonction holomorphe et pour tout entier $k \geq 0$,

$$Z(P, \xi, -k) = R(P^k)(\xi)$$

où $R(P^k)(T) \in K(T_1, \ldots, T_r)$ et $R(P^k)(T) = \sum_{n \in \mathbb{N}^r} P^k(n)\, T^n$.

Remarques. - 1) $R(P^k)(T)$ est une fraction rationnelle de la forme [3]

$$R(P^k)(T) = \sum_{\text{fini}} \frac{\lambda_i(k)}{(1-T)^i}$$

où $(1-T)^i = (1-T_1)^{i_1} \ldots (1-T_r)^{i_r}$, $\lambda_i(k) \in K$.

Elle est donc bien définie pour $T = \xi$ et $R(P^k)(\xi) \in K(\xi_1, \ldots, \xi_r)$.

2) En fait si l'un des ξ_i est égal à 1 , $Z(P, \xi, s)$ admet un prolongement méromorphe à $\mathbb{C}$. Les valeurs aux entiers négatifs appartiennent encore à $K(\xi_1, \ldots, \xi_r)$ mais ne s'expriment plus de la même façon.

On suppose en outre que K est un corps de nombres.

Il est aisé de déduire de ce qui précède le théorème suivant :

THÉORÈME 2. - Si p est un nombre premier, tel que les ξ_i ne soient pas des racines de l'unité d'ordre une puissance de p , alors :

$$|Z(P, \xi, -k)|_\mathfrak{p} \leq \sup |P(n)^k|_\mathfrak{p}$$

pour tout premier $\mathfrak{p}$ de $K(\xi_1, \ldots, \xi_r)$ au-dessus de p .

Soit p un nombre premier impair, $\mathbb{Q}_p$ le corps p-adique élémentaire et $\mathbb{Z}_p$ son anneau de valuation. On note F l'algèbre des fonctions sur $\mathbb{Z}_p$, à valeurs dans un anneau complet $\mathcal{O} \subset \mathbb{C}_p$, et U_1 le sous-groupe de $\mathbb{Z}_p^*$ formé des entiers p-adiques u tels que $u \equiv 1 \pmod p$. Si $u \in U_1$, on note f_u la fonction $s \longmapsto u^s$. Les f_u $(u \in U_1)$ engendrent un sous $\mathcal{O}$-module L de F . Ils forment même une base de L et l'on peut identifier L à l'algèbre $\mathcal{O}[U_1]$ du groupe U_1 . On définit maintenant $\bar{L}$ comme étant l'adhérence de L dans F pour la topologie de la convergence uniforme. Les éléments de $\bar{L}$ sont appelés fonctions d'Iwasawa.

Supposons maintenant $p=2$. Notons U_2 le sous-groupe de $\mathbb{Z}_2^*$, formé des entiers 2-adiques tels que $u \equiv 1 \mod 4$. L est l'algèbre engendré par les fonctions $f_u : s \longmapsto u^s$ avec $u \in U_2$.

Soit p un nombre premier et $\mathfrak{p}$ un idéal premier de K au-dessus de p .

DÉFINITION. - On dira que P possède la propriété $*\mathfrak{p}$ si :

i) P possède la propriété $*$

ii) les coefficients des polynômes P_i appartiennent à $\mathfrak{p}$

iii) les a_i sont congrus à 1 mod $\mathfrak{p}$.

THÉORÈME 3. - Soit p un nombre premier tel que les ξ_i ne soient pas des racines de l'unité d'ordre une puissance de p . Soit $\mathfrak{p}$ un idéal premier de K au-dessus de p et P un polynôme de $K[X_1, \ldots, X_r]$ possédant la propriété $*\mathfrak{p}$.

Alors il existe une fonction d'Iwasawa unique $Z_{\mathfrak{p}}(P, \xi, s)$ telle que pour tout entier $k \geq 0$

$$Z_{\mathfrak{p}}(P, \xi, -k) = Z(P, \xi, -k) .$$

II. - Applications arithmétiques

On reprend ici les notations de l'introduction.

Soient K un corps de nombres totalement réel et $\mathfrak{f}$ un idéal entier de K . Soit $\mathfrak{a}$ un idéal entier de K, premier à $\mathfrak{f}$. On rappelle qu'il existe un nombre fini de $L_{j,x}$ telles que

$$\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s) = N\mathfrak{a}^s \sum_{L_{j,x}} Z(NL_{j,x}, s)$$

où

$$L_{j,x}(y) = x + v_{j,1} y_1 + \ldots + v_{j,r(j)} y_{r(j)}$$

$(v_{j,i} \in \mathfrak{a}\mathfrak{f}, v_{j,i} \gg 0$, $x = \sum x_i v_{j,i}$, $x_i \in \mathbb{Q}$, $0 < x_i \leq 1$, et $x \in \mathfrak{a}$, $x \equiv 1 \mod \mathfrak{f})$

$$Z(NL_{j,x}, s) = \sum_{m \in \mathbb{N}^r} N(L_{j,x}(m))^{-s} .$$

1) Fonctions L p-adiques [3]

Soit $\mathfrak{c}$ un idéal entier de K, possédant la propriété (4). On considère :

$$\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = N\mathfrak{c}^{1-s}\, \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}\mathfrak{c}^{-1}, s) - \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s)$$

alors :

$$\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = N\mathfrak{a}^{s} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} (\exp 2\pi i\, \mathrm{tr}(\mu\nu x))\; Z(NL_{j,x}, \xi_j^{\mu}, s)$$

où :

$$Z(NL_{j,x}, \xi_j^{\mu}, s) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_{r(j)}=0}^{\infty} \xi_{j,1}^{\mu m_1} \cdots \xi_{j,r(j)}^{\mu m_{r(j)}}\, N(L_{j,x}(m))^{-s}$$

et les $\xi_{j,i}$ sont des racines primitives c-ièmes de l'unité. Les propriétés de $L_{j,x}$ permettent alors de dire que le polynôme $NL_{j,x}(X) \in K[X_1, \ldots, X_{r(j)}]$ possède la propriété (*), avec des polynômes P_i homogènes du premier degré et des α_i égaux à 1. Alors le théorème 1 permet d'écrire :

COROLLAIRE 1. - La fonction $s \longmapsto Z(NL_{j,x}, \xi^{\mu}, s)$ se prolonge à $\mathbb{C}$ en une fonction holomorphe et l'on a :

$$Z(NL_{j,x}, \xi^{\mu}, -k) = R(NL_{j,x}^{k})(\xi^{\mu})$$

où

$$R(NL_{j,x}^{k})(T) = \sum_{n \in \mathbb{N}^r} NL_{j,x}(n)^k\, T^n .$$

Remarque. - Shintani [13] a montré que $s \longmapsto Z(NL_{j,x}, \xi^{\mu}, s)$ admettait un prolongement méromorphe à $\mathbb{C}$, mais il a exprimé les valeurs aux entiers négatifs à l'aide de valeurs de polynômes de Bernoulli, sous une forme qui est directement inutilisable pour l'arithmétique.

On peut donc écrire :

$$(7) \qquad \zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, -k) = N\mathfrak{a}^{-k} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} (\exp 2\pi i\, \mathrm{tr}(\mu\nu x))\; R((N L_{j,x})^{k})(\xi_j^{\mu}) .$$

Le théorème 2 donne le résultat suivant :

COROLLAIRE 2. - Si p ne divise pas c, $\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, -k)$ est p-entier pour tout $k \geq 0$.

Supposons que p soit un nombre premier de $\mathbb{Z}$ et que $\mathfrak{f}$ soit divisible par tous les idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ de K au-dessus de p, alors $NL_{j,x}$ possède la propriété $*\mathfrak{p}$ pour tous les idéaux premiers $\mathfrak{p}$, $\mathfrak{p}|(p)$. On en déduit :

COROLLAIRE 3. - Si p est un nombre premier et si $\mathfrak{f}$ est divisible par tous les les idéaux premiers de K au-dessus de p, il existe une fonction d'Iwasawa unique $Z_p(NL_{j,x}, \xi, s)$ telle que pour tout nombre entier k, $k \geq 0$

$$Z_p(NL_{j,x}, \xi, -k) = Z(NL_{j,x}, \xi, -k) .$$

Posons $\exp 2\pi i \operatorname{tr}(\nu x) = \xi_x$. Alors on peut définir :

$$(8) \qquad \zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = \langle N\mathfrak{a}\rangle^{s} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} Z_p(NL_{j,x}, \xi_j^{\mu}, s)$$

qui est une fonction d'Iwasawa (on écrit, si $a \in \mathbb{Z}_p - p\mathbb{Z}_p$, $a = \langle a\rangle \theta(a)$ où $\langle a\rangle \equiv 1 \bmod p$ et $\theta^{p-1}(a) = 1$).

Soit χ un caractère primitif de conducteur $\mathfrak{f}$, on pose :

$$(9) \qquad L_p(\chi, s) = \frac{1}{1 - \chi(\mathfrak{c})\langle N\mathfrak{c}\rangle^{1-s}} \sum_{\mathfrak{a} \in R_{\mathfrak{f}}} \chi(\mathfrak{a}^{-1})\, \zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s)$$

Soit χ un caractère de conducteur $\mathfrak{f}_1$ et soit $\mathfrak{f} = \operatorname{ppcm}(\mathfrak{f}_1, \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ et χ' le caractère induit par χ sur $R_{\mathfrak{f}}$. On définit $L_p(\chi, s)$ par

$$L_p(\chi, s) = L_p(\chi', s) .$$

2) Analogues des fonctions Γ-multiples

Rappelons tout d'abord ce que sont les fonctions Γ-multiples complexes [1], [14].

Pour un r-uple $v = (v_1, \ldots, v_r)$ de nombres positifs et pour un nombre positif a, on note :

$$Z(L_a, s) = \sum_{m \in \mathbb{N}^r} L_a(m)^{-s} \quad \text{où} \quad L_a(m) = a + m_1 v_1 + \ldots + m_r v_r .$$

On définit alors :

$$(11)\qquad -\operatorname{Log}\rho_r(v)=\lim_{a\to+0}\left[\frac{d}{ds}Z(L_a,s)\right]_{s=0}+\operatorname{Log}a\ ;\ \operatorname{Log}\frac{\Gamma_r(a,v)}{\rho_r(v)}=\frac{d}{ds}\left[Z(L_a,s)\right]_{s=0}.$$

On montre que, en tant que fonction de a, $\Gamma_r(a,v)^{-1}$ est une fonction entière d'ordre r. D'autre part, posons $\overset{\vee}{v}(i)=(v_1,\dots,v_{i-1},v_{i+1},\dots,v_r)$. Alors la fonction Γ-multiple satisfait :

$$\operatorname{Log}\frac{\Gamma_r(a+v_i,v)}{\rho_r(v)}-\operatorname{Log}\frac{\Gamma_r(a,v)}{\rho_r(v)}=-\operatorname{Log}\frac{\Gamma_{r-1}(a,\overset{\vee}{v}(i))}{\rho_{r-1}(\overset{\vee}{v}(i))}$$

si $r>1$. Pour $r=1$

$$\operatorname{Log}\frac{\Gamma_1(a,v)}{\rho_1(v)}=\operatorname{Log}\frac{\Gamma(a/v)}{\sqrt{2\pi}}+\left(\frac{a}{v}-\frac{1}{2}\right)\operatorname{Log}v\ .$$

Soit χ un caractère fidèle pair, de conducteur f du groupe de Galois d'une extension abélienne de $\mathbb{Q}$. On sait que la fonction Γ_1 est liée à $L(\chi,s)$ dans les formules suivantes :

$$(12)\qquad L'(\chi,0)=\sum_{a=1}^{f}\chi(a)\operatorname{Log}\frac{\Gamma_1(a,f)}{\rho_1(f)}$$

et

$$(13)\qquad L(\chi,1)=\sum_{a=1}^{f}\chi(a)\frac{d}{dz}\left[\operatorname{Log}\frac{\Gamma_1(z,f)}{\rho_1(f)}\right]_{z=a}$$

Shintani a généralisé (12) de la manière suivante :

Soient $(v_{j,i})(1\le i\le r,\ 1\le j\le n)$ des nombres réels positifs et soit $x=(x_1,\dots,x_r)$ un r-uple de nombres réels positifs. On pose :

$$L_{j,x}(y)=v_{j,1}(y_1+x_1)+\dots+v_{j,r}(y_r+x_r)$$

et

$$Z\Big(\prod_{j=1}^{n}L_{j,x},s\Big)=\sum_{m\in\mathbb{N}^r}\prod_{j=1}^{n}L_{j,x}(m)^{-s}\ .$$

Pour chaque r-uple $\ell=(\ell_1,\dots,\ell_r)$ d'entiers non négatifs, on pose :

$$C_\ell(A)=\sum_{j,k}\int_0^1\left\{\prod_{i=1}^{r}(v_{j,i}+v_{k,i}u)^{\ell_i-1}-\prod_{i=1}^{r}v_{j,i}^{\ell_i-1}\right\}\frac{du}{u}$$

où la sommation sur (j,k) est prise sur toutes les paires (j,k) d'entiers positifs avec $1\le j,k\le n$ et $j\neq k$.

Alors :

$$(14)\qquad \frac{d}{ds} Z\Big(\prod_{j=1}^{n} L_{j,x}, s\Big) = \mathrm{Log}\Big\{\prod_{j=1}^{n} \frac{\Gamma_r(x.v_j, v_j)}{\rho_r(v_j)}\Big\} + \frac{(-1)^r}{n} \sum_{\ell} C_\ell(A) \prod_{i=1} \frac{B_{\ell_i}(x_i)}{\ell_i !}$$

où la sommation sur ℓ est prise sur tous les r-uples d'entiers non négatifs qui satisfont $\ell_1 + \ell_2 + \ldots + \ell_r = r$ et où $x.v_j = \sum x_i v_{j,i}$.

Soient K un corps de nombres totalement réel et $\mathfrak{f}$ un idéal entier de K . Soit $\mathfrak{a}$ un idéal entier de K , premier à $\mathfrak{f}$.

On a vu qu'il existait un nombre fini de $L_{j,x}$ telles que :

$$\zeta_{\mathfrak{f}}(\mathfrak{a}^{-1}, s) = N\mathfrak{a}^s \sum_{L_{j,x}} Z(NL_{j,x}, s) .$$

Ici, on ne va pas définir un analogue p-adique des fonctions Γ-multiples pour chaque x , mais on va directement associer une fonction Γ à l'idéal $\mathfrak{a}$ (pour la construction des fonctions Γ-multiples, associées à x , voir [4]). Posons, pour tout $\sigma \in S$ où S est l'ensemble des n plongements de K dans $\mathbb{R}$.

$$\beta_{\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, s) = \frac{1}{n} N\mathfrak{a}^s \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} Z(L_{j,x}^{\sigma}, \xi_j^{\mu}, ns)$$

où :

$$L_{j,x}^{\sigma}(y) = x^{\sigma} + v_{j,1}^{\sigma} y_1 + \ldots + v_{j,r(j)}^{\sigma} y_{r(j)} .$$

Cette fonction se prolonge en une fonction holomorphe sur $\mathbb{C}$ et pour tout entier $k \geq 0$,

$$\beta_{\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, -k) = \frac{1}{n} N\mathfrak{a}^{-k} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(L_{j,x}^{\sigma\, kn})(\xi_j^{\mu}) .$$

On sait aussi que si p ne divise pas c , $n\beta_{\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, k)$ est p-entier et que si $\mathfrak{f}$ est divisible par (p), il existe une fonction $\beta_{p,\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, s)$ unique telle que, $n\beta_{p,\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, s)$ soit une fonction d'Iwasawa, et pour tout entier $k \geq 0$,

$k \equiv -1 \mod p-1$

$$\beta_{p,\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, -k) = \beta_{\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, -k) .$$

PROPOSITION 4.-

$$\Big[\frac{d}{ds} \zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, s)\Big]_{s=0} = \sum_{\sigma \in S} \Big[\frac{d}{ds} \beta_{p,\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, s)\Big]_{s=0}$$

et

$$\forall \sigma \in S \qquad \zeta_{p,\mathfrak{f}}(\mathfrak{a}^{-1}, \mathfrak{c}, 0) = n\beta_{p,\mathfrak{f}}^{\sigma}(\mathfrak{a}^{-1}, \mathfrak{c}, 0) .$$

Preuve. - Par définition :

$$\zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, -s) = \langle N\mathfrak{a}\rangle^{s} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(NL_{j,x}^{s})(\xi_j^{\mu}) .$$

D'où :

$$-\left[\frac{d}{ds}\zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, -s)\right]_{s=0} = \operatorname{Log}\langle N\mathfrak{a}\rangle\ \zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, 0) + \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(\operatorname{Log}_p NL_{j,x})(\xi_j^{\mu}) .$$

Donc :

$$-\left[\frac{d}{ds}\ \zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, s)\right]_{s=0} = \operatorname{Log}\langle N\mathfrak{a}\rangle\ \zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, 0) + \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \sum_{\sigma} \xi_x^{\mu} R(\operatorname{Log} L_{j,x}^{\sigma})(\xi_j^{\mu}) .$$

D'autre part :

$$\beta_{p,\mathfrak{f}}^{\sigma}(a^{-1}, \mathfrak{c}, -s) = \frac{1}{n}\langle N\mathfrak{a}\rangle^{s} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(L_{j,x}^{\sigma\, ns})(\xi_j^{\mu}) .$$

Alors :

$$-\left[\frac{d}{ds}\ \beta_{p,\mathfrak{f}}^{\sigma}(a^{-1}, \mathfrak{c}, -s)\right]_{s=0} = \operatorname{Log}\langle N\mathfrak{a}\rangle\ \beta_{p,\mathfrak{f}}^{\sigma}(a^{-1}, \mathfrak{c}, 0) + \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(\operatorname{Log} L_{j,x}^{\sigma})(\xi_j^{\mu}) .$$

D'autre part, on a::

$$\zeta_{p,\mathfrak{f}}(a^{-1}, \mathfrak{c}, 0) = \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(1)(\xi_j^{\mu})$$

et

$$\beta_{p,\mathfrak{f}}^{\sigma}(a^{-1}, \mathfrak{c}, 0) = \frac{1}{n} \sum_{\mu=1}^{c-1} \sum_{L_{j,x}} \xi_x^{\mu} R(1)(\xi_j^{\mu}) .$$

Donc la proposition 4 est démontrée.

Supposons maintenant que l'idéal $\mathfrak{c}$, qui vérifie (4) soit tel que $\mathfrak{c} = (\alpha)$ avec $\alpha \equiv 1(\mathfrak{f})$ et $\alpha \gg 0$.

Puisque

$$\zeta_{\mathfrak{f}}(a^{-1}, c, s) = Nc^{1-s}\, \zeta_{\mathfrak{f}}(a^{-1}c^{-1}, s) - \zeta_{\mathfrak{f}}(a^{-1}, s)$$

on a :

$$\zeta_{\mathfrak{f}}(a^{-1}, s) = \zeta_{\mathfrak{f}}(a^{-1}, c, s)/(Nc^{1-s} - 1)$$

et

$$\zeta_{p,\mathfrak{f}}(a^{-1}, s) = \zeta_{p,\mathfrak{f}}(a^{-1}, c, s)/(Nc^{1-s} - 1) .$$

Cette fonction ne dépend plus de l'idéal $c = (\alpha)$ ni de l'idéal a dans sa classe de rayon mod $\mathfrak{f}$.

PROPOSITION 5.-

$$\left[\frac{d}{ds}\, \zeta_{p,\mathfrak{f}}(a^{-1}, s)\right]_{s=0} = \sum_{\sigma \in S} \left[\frac{d}{ds}\, \frac{\beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)}{(Nc^{1-s} - 1)}\right]_{s=0} .$$

Preuve. -

$$\left[\frac{d}{ds}\, \zeta_{p,\mathfrak{f}}(a^{-1}, s)\right]_{s=0} = \frac{Nc\ \mathrm{Log}\, Nc}{(Nc-1)^2}\, \zeta_{p,\mathfrak{f}}(a^{-1}, c, 0) + \frac{1}{Nc-1} \left[\frac{d}{ds}\, \zeta_{p,\mathfrak{f}}(a^{-1}, c, s)\right]_{s=0}$$

$$\frac{d}{ds}\left[\frac{\beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)}{(Nc^{1-s} - 1)}\right]_{s=0} = \frac{Nc\ \mathrm{Log}\, Nc}{(Nc-1)^2}\, \beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, 0) + \frac{1}{Nc-1} \left[\frac{d}{ds}\, \beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)\right]_{s=0}$$

$$\sigma \left[\frac{d}{ds}\, \frac{\beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)}{(Nc^{1-s} - 1)}\right]_{s=0} = \frac{Nc\ \mathrm{Log}\, Nc}{(Nc-1)^2}\, \zeta_{p,\mathfrak{f}}(a^{-1}, c, 0) + \frac{1}{Nc-1} \sum_{\sigma} \left[\frac{d}{ds}\, \beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)\right]_{s=0} .$$

On déduit donc de la proposition 5 que :

$$\sum_{\sigma \in S} \left[\frac{d}{ds}\, \frac{\beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)}{(Nc^{1-s} - 1)}\right]_{s=0}$$

ne dépend plus de c et ne dépend que de la classe de rayon de a mod $\mathfrak{f}$.

DÉFINITION. - On pose :

$$L\Gamma_{p,\mathfrak{f}}(a^{-1}) = \sum_{\sigma \in S} \left[\frac{d}{ds}\, \frac{\beta^{\sigma}_{p,\mathfrak{f}}(a^{-1}, c, s)}{(Nc^{1-s} - 1)}\right]_{s=0} .$$

THÉORÈME 6. - Soient χ un caractère et $\mathfrak{f}$ le ppcm du conducteur de χ et de $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Soit χ' le caractère induit par χ sur $R_{\mathfrak{f}}$. Alors :

$$L'_p(\chi, 0) = \sum_{a \in R_{\mathfrak{f}}} \chi'(a)\, L\Gamma_{p,\mathfrak{f}}(a) .$$

-:-:-:-

BIBLIOGRAPHIE

[1] BARNES E. W., On the theory of the multiple gamma function, Tran. Cambridge Philos. Soc. 19 (1904), 374-425.

[2] CASSOU-NOGUÈS P., Fonctions L p-adiques d'une extension abélienne d'un corps totalement réel, Journées d'analyse ultramétrique 1976, Marseille-Luminy, exposé n° 9.

[3] CASSOU-NOGUÈS P., Valeurs aux entiers négatifs des fonctions zêta et des fonctions zêta p-adiques, (à paraître Inv. Math.).

[4] CASSOU-NOGUÈS P., Fonctions Γ-multiples p-adiques (à paraître).

[5] CASSOU-NOGUÈS P., Etude de certaines séries de Dirichlet (à paraître).

[6] DELIGNE P., RIBET K., Values of abelian L-functions at negative integers (à paraître).

[7] DIAMOND J., The p-adic Log gamma function and p-adic Euler constants (à paraître in Trans. A.M.S.).

[8] FERRERO B. and GREENBERG R., On the behaviour of p-adic L functions at $s=0$ (à paraître).

[9] KLINGEN H., Über die Werte der Dedekindsche Zetafunktion, Math. Annalen, t. 145 (1962), p. 265-272.

[10] MORITA Y., A p-adic analogue of the Γ-function, J. Fac. Science Univ. Tokyo, 22, 1975.

[11] SERRE J.-P., Formes modulaires et fonctions zêta p-adiques "Modular functions of one variable III" (1972) Antwerpen p. 191-268, Berlin, Springer Verlag (1973) (Lecture Notes in Mathematics, 350).

[12] SIEGEL C. L., Über die Fourierschen Koeffizienten von Modulformen, Nachr. Akad. Wiss. Göttingen, Math.-Phys. K 1, t. 3 (1970), p. 15-56.

[13] SHINTANI T., On evaluation of zeta functions of totally real algebraic number at non positive integers, J. of Fac. of Sc., Univ. of Tokyo, section 1, t. 23 (1976), p. 393-417.

[14] SHINTANI T., On values at $s = 1$ of certain L-functions of totally real algebraic number fields, Algebraic Number Theory International Symposium, Kyoto 1976, S Iyanaga Ed.

-:-:-:-

Pierrette CASSOU-NOGUÈS
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX

Astérisque

H. COHEN

Arithmétique et informatique

Astérisque, tome 61 (1979), p. 57-61

<http://www.numdam.org/item?id=AST_1979__61__57_0>

Société Mathématique de France
Astérisque 61 (1979) p. 57-61

ARITHMÉTIQUE ET INFORMATIQUE

par H. COHEN

Le but de mon exposé est d'attirer encore une fois l'attention sur les liens existant entre l'arithmétique et l'informatique, ces liens allant dans les deux sens.

§ 1. UTILISATION DE MOYENS INFORMATIQUES EN ARITHMÉTIQUE.

De nombreux exposés et conférences ont eu lieu à ce sujet. Je voudrais simplement parler de trois problèmes qui m'ont intéressé.

a) Nombres sociables.

Posons $s(n) = \sum_{\substack{d \mid n \\ d \neq n}} d = \sigma_1(n) - n$.

On s'intéresse au comportement des itérés successifs de la fonction s . Ce comportement peut être de trois types :

(i) $s^{(k)}(n)$ converge, c'est-à-dire qu'il existe un k tel que $s^{(k)}(n) = 1$ $\left(s^{(k)}(n) = s\left(s^{(k-1)}(n)\right)\right)$

(ii) $s^{(k)}(n)$ est périodique à partir d'un certain rang

(iii) $s^{(k)}(n)$ est non bornée.

Les exemples de (i) abondent. On ne connaît pas d'exemple de (iii). Le plus petit n qui pourrait être du type (iii) est $n = 276$. Lenstra a toutefois démontré que la suite $s^{(k)}(n)$ peut être arbitrairement longtemps strictement croissante.

Les exemples de (ii) sont les plus intéressants. Si la suite $s^{(k)}(n)$ est purement périodique de période k_o , on appelle $\left(n, s(n), \ldots, s^{(k_o-1)}(n)\right)$ un groupe sociable d'ordre k_o . Les résultats connus sont les suivants :

$k_o = 1$: n est alors dit parfait. On sait que si n est pair, n est de la forme $2^{p-1}(2^p-1)$ où 2^p-1 est premier ; on connaît 25 tels nombres, le plus grand étant $2^{21700}(2^{21701}-1)$. On conjecture qu'il n'y a

pas de nombres parfaits impairs. S'il en existe, ils doivent être supérieurs à 10^{50}.

$k_o = 2$: $(n,s(n))$ est un couple de nombres amiables. On en connaît plus de 1100, le plus petit étant le couple $(220,284)$. Tous les couples pour lesquels $n \leq 10^8$ ont été trouvés (voir [1]).

$k_o > 2$: les seuls exemples connus avant 1968 étaient dus à Poulet avec un groupe sociable d'ordre 5 et un d'ordre 28. En 1968, W. Borho a construit un groupe d'ordre 4, et indépendamment j'ai trouvé 9 groupes d'ordre 4 (voir [1]). Depuis, 5 autres groupes d'ordre 4 ont été trouvés. Les problèmes principaux sur le sujet sont les suivants :

- Existe-t-il un groupe sociable dont la somme des termes soit impair ?
- Existe-t-il un groupe sociable d'ordre 3 ?
- Existe-t-il une infinité de nombres amiables, et si oui peut-on donner une estimation asymptotique ?

b) Fonctions L de caractères quadratiques aux entiers négatifs.

Soit N un entier positif ou nul. Si $r \geq 1$ on pose

$$H(r,N) = \zeta(1-2r) \quad \text{si} \quad N = 0$$

$$H(r,N) = L\left(1-r, \left(\frac{D}{\cdot}\right)\right) \sum_{d|f} \mu(d)\left(\frac{D}{d}\right) d^{r-1}\sigma_{2r-1}(f/d)$$

où on a écrit $(-1)^r N = Df^2$ avec D discriminant de corps quadratique. Ceci est un analogue supérieur de la fonction $H(N) = H(1,N)$ introduite par Hurwitz et comptant le nombre de classes de formes quadratiques de discriminant $-N$ modulo l'ordre de leur groupe d'automorphismes. Ces fonctions $H(r,N)$ interviennent dans différents problèmes (voir [2] et [5]) et j'ai jugé utile d'en faire une table assez étendue, pour $r > 1$ (pour $r = 1$ une telle table existe). Pour cela, j'ai utilisé le fait que la série

$$\mathcal{H}_r(\tau) = \sum_{N\geq 0} H(r,N)e^{2i\pi N\tau} = \sum_{N\geq 0} H(r,N)q^N \qquad (q = e^{2i\pi\tau})$$

est une forme modulaire de poids $r+\frac{1}{2}$ sur $\Gamma_o(4)$. Ceci entraîne que

$\mathcal{H}_r$ est un polynôme en $\theta = \sum_{n\in\mathbb{Z}} q^{n^2}$ et $F_2 = \sum_{\substack{n\geq 1\\ n \text{ impair}}} \sigma_1(n)q^n$ dont les coefficients se déterminent aisément.

Toutefois, le calcul de F_2^2, F_2^3 etc... est très long si on veut aller jusqu'à $N = 1000$. Il a donc fallu employer une méthode (déjà utilisée par Atkin) pour accélérer les calculs. Cette méthode était la suivante :

Posons $\theta_1 = \sum_{n\geq 0} q^{(2n+1)^2}$, $\theta_2 = \sum_{n\in\mathbb{Z}} q^{(2n)^2}$. On démontre que $F_2 = \theta_1\theta_2(\theta_2^2 + 4\theta_1^2)$ et $\theta = 2\theta_1 + \theta_2$ donc on peut exprimer $\mathcal{H}_r$ comme polynôme en θ_1 et θ_2. L'avantage énorme est que les séries θ_1 et θ_2 sont très lacunaires, donc que la multiplication par une telle série est très rapide.

J'ai ainsi pu calculer une table de $H(r,N)$ avec $2 \leq r \leq 11$, $0 \leq N \leq 1020$ en 16 mn d'IRIS 80. Il m'a fallu employer une bibliothèque maison de multiprécision car le plus grand nombre de la table est

$$-3036\,H(11,1020) = 142369924502364047754513095232000 0.$$

Cette table a été déposée aux U.M.T. de Mathematics of Computation [3].

c) Contre-exemple à la conjecture de von Sterneck. (Travail fait en collaboration avec F. Dress)

Posons $M(x) = \sum_{n\leq x} \mu(n)$, où μ est la fonction de Möbius. Von Sterneck a conjecturé que $|M(x)| \leq \frac{\sqrt{x}}{2}$ pour tout $x > 200$. En calculant des valeurs particulières de $M(x)$ Neubauer a montré que cette conjecture était fausse pour $x = 7{,}77 \times 10^9$.

J'ai programmé en assembleur un miniordinateur TI 980 B acheté grâce à l'ATP du CNRS Mathématiques-Informatique, pour faire le calcul systématique de $M(x)$ jusqu'à $7{,}8.10^9$. Le temps de calcul initial pour arriver à $7{,}8.10^9$ aurait été de quelques mois. J'ai réussi en optimisant le programme au maximum à ramener la durée à moins d'une semaine, temps raisonnable. Je dispose ainsi d'une table de $M(x)$ de 10^7 en 10^7 jusqu'à $7{,}8.10^9$ et j'ai trouvé que le plus petit x pour lequel la conjecture de von Sterneck est fausse est $x = 7725038629$ pour lequel on a

$M(7725038629) = 43947$.

Remarque. On conjecture en fait que

$$\overline{\lim} \frac{|M(x)|}{\sqrt{x}} = +\infty$$

et même que

$$\overline{\lim} \frac{|M(x)|}{\sqrt{x}\ \mathrm{Log}\ \mathrm{Log}\ x} > 0 .$$

§ 2. UTILISATION DE L'ARITHMÉTIQUE EN INFORMATIQUE.

Je voudrais ici énoncer un problème non encore résolu à ma connaissance, et qui se trouve dans l'excellent livre de Knuth ([4]) auquel on pourra se référer pour les détails de ce qui suit.

Ce problème est l'analyse de l'algorithme binaire de calcul du PGCD. Cet algorithme est basé sur les remarques suivantes : si u et v sont pairs, $(u,v) = 2(u/2, v/2)$. Si u est pair et v est impair, $(u,v) = (u/2, v)$ (et inversement). Enfin si u et v sont impairs, $(u,v) = (u-v, v)$ et $u-v$ est pair. On peut aisément déduire de ces remarques un algorithme de calcul du PGCD ne nécessitant pas de division (la division par 2 se faisant beaucoup plus rapidement qu'une division arbitraire dans la grande majorité des ordinateurs) et cet algorithme se trouve être en pratique plus rapide que l'algorithme d'Euclide. En ce qui concerne l'algorithme d'Euclide, on sait que le nombre de divisions pour calculer (a,n) est en moyenne de l'ordre de $\frac{12\ \mathrm{Log}\ 2}{\pi^2}\ \mathrm{Log}\ n$. En ce qui concerne l'algorithme binaire, certains calculs heuristiques et des expérimentations ont été faites, mais on ne connaît pas en moyenne le nombre de pas nécessaire pour calculer (a,n) , et ceci pose un problème à mon avis très intéressant aux mathématiciens.

BIBLIOGRAPHIE.

[1] H. COHEN. - On amicable and sociable numbers, Math. Comp. 24 (1970) pp. 423-429.

[2] H. COHEN. - Sums involving the values at negative integers of L functions of quadratic characters, Math. Ann. 217 (1975) pp. 271-285.

[3] H. COHEN. - A table of values at negative integers of L functions of quadratic characters, Math. Comp., UMT file.

[4] D. KNUTH. - The Art of Computer Programming, vol. 2, ch. 4, § 4.5.2 (Addison Wesley, 1969).

[5] D. ZAGIER. - Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields, Lecture Notes n° 627, pp. 106-169.

-:-:-:-

Henri COHEN
Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)

(décembre 1978)

Astérisque

PETER DRAXL

Corps gauches à involution de deuxième espèce

Astérisque, tome 61 (1979), p. 63-72

<http://www.numdam.org/item?id=AST_1979__61__63_0>

Société Mathématique de France
Astérisque 61 (1979) p. 63-72

CORPS GAUCHES À INVOLUTION DE DEUXIÈME ESPÈCE

par Peter DRAXL

§ 1. INTRODUCTION

Soit A une algèbre simple de rang fini sur son centre K à involution I de deuxième espèce (la référence principale dans cette situation est [1],Ch.X). Notons

$$S_I(A) := \{a \in A \mid a^I = a\} \quad \text{et} \quad k := K \cap S_I(A) \quad (^1),$$

alors K/k est une extension quadratique séparable à groupe de Galois $\{1, I|_K\}$, et $S_I(A)$ est un espace vectoriel de dimension $n^2 = |A:K|$ sur k . On définit (J une autre involution du même type)

$$I \sim J \text{ , si et seulement si } I|_K = J|_K \text{ ,}$$

et l'on montre facilement que $I \sim J$ équivaut à l'existence d'un élément $t \in S_I(A)$ tel que l'on ait

$$a^J = ta^I t^{-1} \quad (a \in A).$$

Notons maintenant

$\Sigma_I(A)$:= sous-groupe du groupe multiplicatif A^* engendré par $S_I(A)$,

alors un calcul simple donne

$$\Sigma_I(A) = \Sigma_J(A) \text{ , si } I \sim J \text{ .}$$

(^{1}) La notation := utilisée ici signifie "égale par définition".

En outre on note $\mathrm{Nrd}_{A/K}$ la norme réduite, et l'on démontre (voir p. ex. [7], Prop. 1 pour la première inclusion et [3], (3.3), p. 27 pour la seconde)

$$[A^*,A^*] \subseteq \Sigma_I(A) \subseteq \mathrm{Nrd}_{A/K}^{-1}(k^*) ,$$

donc le groupe

$$\mathrm{USK}_1(A,\tilde{I}) := \mathrm{Nrd}_{A/K}^{-1}(k^*)/\Sigma_I(A)$$

ne dépend que de la classe $\tilde{I}$ de l'involution I modulo la relation $\sim$, et il est appelé (voir [11])

groupe réduit de Whitehead de A par rapport à I .

C'est un analogue du groupe réduit de Whitehead de A

$$\mathrm{SK}_1(A) := \mathrm{Nrd}_{A/K}^{-1}(\{1\})/[A^*,A^*] ,$$

et les deux groupes sont liés par l'homomorphisme

$$(1) \qquad \Omega: \mathrm{SK}_1(A) \longrightarrow \mathrm{USK}_1(A,\tilde{I})$$

qui est induit par l'inclusion.

Quant aux groupes USK_1 les propriétés suivantes sont bien connues:

0° En général on a $\mathrm{USK}_1(A,\tilde{I}) \neq 1$ (voir [8], [5] et [6]) .

1° Soit l/k une extension finie disjointe de K/k, et soit $L := Kl$, alors il existe des homomorphismes

$$\mathrm{USK}_1(A,\tilde{I}) \underset{\pi_L}{\overset{\iota_L}{\rightleftarrows}} \mathrm{USK}_1(A \otimes_K L, \widetilde{I\otimes \mathrm{id}})$$

tels que l'on ait $\pi_L \circ \iota_L = |L:K| \cdot \mathrm{id}$ ([4], Lemma 4).

2° $\mathrm{USK}_1(A,\tilde{I})$ est un groupe de torsion à exposant divisant l'indice $i(A)$ de A (cela résulte de 1°) (^{2}).

3° Soit K/k une extension quadratique séparable, et soit A

(^{2}) $i(A) := \sqrt{|D:K|}$, où D est le corps gauche avec $A = M_r(D)$.

une algèbre simple de rang fini sur son centre K. Pour que A admette une involution I de deuxième espèce avec $K \cap S_I(A) = k$, il faut et il suffit que $\mathrm{cor}_{K/k}(A) = 0$ dans le groupe de Brauer de k (voir p. ex. [9], p.93).

Par conséquent, d'après 2^o et 3^o il n'est pas intéressant de parler de USK_1 sur un corps local (comme la corestriction est toujours injective là; voir p. ex. [10], Ch.XI, Prop.1 et Ch.XIII, Th.1).

4^o Soit $A = M_r(D)$ (D un corps gauche), alors il existe des involutions J de A et i de D telles que l'on ait $I \sim J$ et $(d_{\mu\nu})^J = (d^i_{\nu\mu})$. En outre le déterminant de Dieudonné induit un isomorphisme (voir [4], Lemma 3)

$$USK_1(A,\tilde{I}) \cong USK_1(D,\tilde{i}) \quad .$$

5^o Soit $A \cong A_1 \otimes_K A_2$ avec $\mathrm{pgcd}(i(A_1), i(A_2)) = 1$, alors il existe des involutions I_ν de A_ν telles que l'on ait $I \sim I_1 \otimes I_2$, et l'on a

$$USK_1(A,\tilde{I}) \cong USK_1(A_1,\tilde{I}_1) \times USK_1(A_2,\tilde{I}_2)$$

(c'est une conséquence de 1^o).

6^o Dans le cas "$i(A)$ impair" l'homomorphisme Ω dans (1) est surjectif (en fait, $\mathrm{Nrd}_{A/K}(a) = \mathrm{Nrd}_{A/K}(a)^I$ implique l'existence de $b \in \mathrm{Nrd}^{-1}_{A/K}(\{1\})$ avec $a = a^I b$, donc $a^2 = (aa^I)b$ avec $aa^I \in \Sigma_I(A)$; le reste est clair d'après 2^o).

Nous disons que k vérifie la

condition (∇) ,

lorsque les conditions suivantes sont verifiées:

quel que soit L/k extension finie séparable, quel que soit E corps gauche de rang fini sur son centre L, et si un groupe Γ des automorphismes de L sur k est, ou bien

cyclique d'ordre premier impair, ou bien non-cyclique d'ordre 4 , et tel que $\mathrm{Nrd}_{E/L}(E^*)$ soit stable sous l'opération de Γ , alors

$$H^1(\Gamma, \mathrm{Nrd}_{E/L}(E^*)) = 0 .$$

Si un corps vérifie la condidion C_2^0 (voir p. ex. [4],p.373), alors il vérifie la condition (∇) d'après un théorème classique de Noether et Hilbert. En outre les corps globaux vérifient la condition (∇) d'après un théorème de M. Eichler en arithmétiques (voir [2],p.120,avant-dernière ligne).

Le but de cette conférence est de démontrer simultanément les deux résultats suivants:

THÉORÈME. Soit A une algèbre simple de rang fini sur son centre K à involution I de deuxième espèce, alors

(i) l'exposant de $\mathrm{USK}_1(A,\tilde{I})$ divise $\frac{i(A)}{i(A)'}$, où on a noté $i(A)'$ le plus grand diviseur de $i(A)$ sans facteur carré;

(ii) $\mathrm{USK}_1(A,\tilde{I}) = 1$, si k vérifie la condition (∇) .

Le résultat (i) est une amélioration de 2^o (voir aussi [6],2.8), tandis que le résultat (ii) est une généralisation simultanée d'un théorème de V. I. Jančevskiĭ ([4],Th.1) et d'un théorème de C.T.C. Wall ([12],Th.2). Comme on va prouver (i) et (ii) en même temps, et comme cette démonstration sera très courte (voir § 4.), je pense qu'il est intéressant de démontrer ici ce théorème bien que les résultats n'en soient pas complètement inattendus.

§ 2. SUR LE GROUPE DE KLEIN

Soit $\Gamma = \{1,\sigma_0,\sigma_1,\sigma_2\}$ le groupe de Klein, c'est-à-dire $\sigma_0 = \sigma_1\sigma_2 = \sigma_2\sigma_1$ et $\sigma_1^2 = \sigma_2^2 = 1$. Posons $\Gamma_i := \{1,\sigma_i\}$

(i = 0,1,2), et soit M un Γ-module à droite. Si on note $\hat{H}^r(./.)$ ($r \in \mathbb{Z}$) les groupes de cohomologie au sens de Tate et $\mathfrak{N}: M \longrightarrow M^{\Gamma_0}$ (= sous-module des éléments invariants sous Γ_0) la norme, alors

PROPOSITION 1. <u>On a une suite exacte</u>

$$0 \longrightarrow M^{\Gamma_1} + M^{\Gamma_2} \longrightarrow \mathfrak{N}^{-1}(M^{\Gamma}) \xrightarrow{\alpha} \hat{H}^{-1}(\Gamma/\Gamma_1, M^{\Gamma_1}) \xrightarrow{\beta} \hat{H}^{-1}(\Gamma_2, M) \quad ,$$

<u>induit par</u> $\qquad m \longmapsto m^{(1-\sigma_2)} \qquad m \longmapsto m \quad .$

En fait, à partir de l'identité

$$(2) \qquad (1+\sigma_0)(1-\sigma_1) = (1-\sigma_2)(1-\sigma_1) \quad \text{dans} \quad \mathbb{Z}[\Gamma]$$

on obtient - quel que soit $x \in \mathfrak{N}^{-1}(M^{\Gamma})$ -

$$0 = x^{(1+\sigma_0)(1-\sigma_1)} = x^{(1-\sigma_2)(1-\sigma_1)} \quad ,$$

donc $x^{(1-\sigma_2)} \in M^{\Gamma_1}$ et $\mathfrak{N}_{\Gamma/\Gamma_1}(x^{(1-\sigma_2)}) := x^{(1-\sigma_2)(1+\sigma_2)} = 0$,

c'est-à-dire ceci permet de définir α comme ci-dessus, et l'on en tire immédiatement

$$\beta \circ \alpha = 0 \quad .$$

Réciproquement, soit $\beta(\bar{y}) = \bar{0}$ (avec $y \in M^{\Gamma_1}$ tel que l'on ait $y^{(1+\sigma_2)} = \mathfrak{N}_{\Gamma/\Gamma_1}(y) = 0$), c'est-à-dire il existe $x \in M$ avec $y = x^{(1-\sigma_2)}$, donc - en utilisant (2) encore une fois -

$$0 = y^{(1-\sigma_1)} = x^{(1-\sigma_2)(1-\sigma_1)} = x^{(1+\sigma_0)(1-\sigma_1)} \quad ,$$

ce qui veut dire

$$\bar{y} = \alpha(x) \quad \text{et} \quad \mathfrak{N}(x) \in M^{\Gamma} \quad .$$

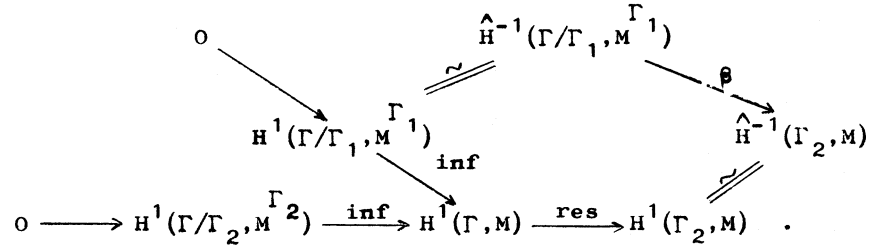
Finalement soit $\alpha(x) = \bar{0}$; il existe donc $y \in M^{\Gamma_1}$ tel que $x^{(1-\sigma_2)} = y^{(1-\sigma_2)}$, par conséquent $x = y + z$ avec $z \in M^{\Gamma_2}$.

Ceci implique

$$\operatorname{Ker} \alpha = M^{\Gamma_1} + M^{\Gamma_2} \quad ,$$

c.q.f.d..

Maintenant on regarde le diagramme suivant:



Le pentagone est commutatif et les deux suites sont exactes (voir p. ex. [10], Ch.VII, §6.). En utilisant convenablement la Prop. 1 ci-dessus on en déduit:

PROPOSITION 2. $\mathfrak{N}^{-1}(M^\Gamma)/(M^{\Gamma_1}+M^{\Gamma_2}) \cong \operatorname{Ker}\beta \cong$

$$\cong \inf\left(H^1(\Gamma/\Gamma_1, M^{\Gamma_1})\right) \cap \inf\left(H^1(\Gamma/\Gamma_2, M^{\Gamma_2})\right) \subseteq H^1(\Gamma, M) \ .$$

COROLLAIRE. $H^1(\Gamma, M) = 0$ <u>implique</u> $\mathfrak{N}^{-1}(M^\Gamma) = M^{\Gamma_1}+M^{\Gamma_2}$.

EXEMPLES.

(A) Soit L/k une extension galoisienne à groupe de Galois Γ ; soient $K_i := L^{\Gamma_i}$ ($i = 0,1,2$), et soit $N := N_{L/K_0}$. Alors, d'après un théorème classique de Noether et Hilbert, le corollaire donne

$$N^{-1}(k^*) = K_1^* \cdot K_2^* \ .$$

(B) Soit L/k comme ci-dessus, et soit E un corps gauche de rang fini sur son centre L tel que $\operatorname{Nrd}_{E/L}(E^*)$ soit stable sous l'opération de Γ . Alors, si k vérifie la condition (∇), on obtient

$$N^{-1}(k^*) \cap \operatorname{Nrd}_{E/L}(E^*) = (K_1^* \cap \operatorname{Nrd}_{E/L}(E^*)) \cdot (K_2^* \cap \operatorname{Nrd}_{E/L}(E^*)) \ .$$

En fait, l'exemple (B) donne la motivation pour la notion "condition (∇)".

§ 3. QUELQUES SUITES EXACTES

Supposons $A = D =$ corps gauche avec $i(A) = i(D) = 2^r$, et

supposons en sus

(3) l'existence d'une extension quadratique séparable l/k telle que $1 \subseteq S_I(D)$, donc $1 \nmid K$.

Posons

$$L := Kl \quad \text{et} \quad E := Z_D(L) = \text{commutant de } L \text{ dans } D,$$

alors L est le centre du corps gauche E avec $i(E) = 2^{r-1}$, et L/k est une extension galoisienne à groupe de Galois Γ (= le groupe de Klein, voir § 2.). Soient $\Gamma_0 = \{1,\sigma_0\} := \mathrm{Gal}(L/K)$ et $\Gamma_1 = \{1,\sigma_1\} := \mathrm{Gal}(L/l)$, alors on obtient $K_0 = K$ et $K_1 = l$ (au sens de l'exemple (A) dans § 2.). D'autre part notre involution I induit sur E une involution $i := I|_E$ de deuxième espèce avec $L \cap S_i(E) = 1 = K_1$, c'est-à-dire $\sigma_1 = i|_L$. Enfin le théorème de Skolem et Noether permet de trouver un élément

$$g \in D^* \quad \text{tel que} \quad \lambda^{\sigma_0} = g\lambda g^{-1} \quad (\lambda \in L \subseteq E \subset D).$$

Maintenant la définition

$$d^{I_0} := gd^I g^{-1}$$

nous donne sur D une involution I_0 de deuxième espèce avec $I_0 \sim I$, et - par restriction - sur E une involution $i_0 := I_0|_E$ de deuxième espèce avec

$$i_0 \neq i \quad \text{et} \quad l_0 := L \cap S_{i_0}(E) = K_2 \quad (\text{au sens de l'exemple (A) dans § 2.}),$$

c'est-à-dire $\sigma_2 = \sigma_1\sigma_0 = \sigma_0\sigma_1 = i_0|_L$.

On va utiliser les abréviations suivantes:

$$NRD := \mathrm{Nrd}_{D/K}, \quad Nrd := \mathrm{Nrd}_{E/L} \quad \text{et} \quad N := N_{L/K}.$$

À partir des formules

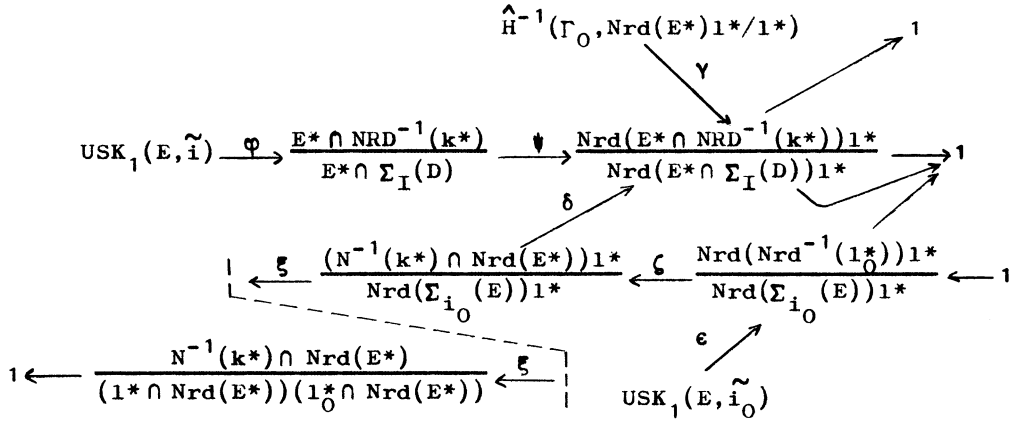
$$NRD|_E = N \circ Nrd \quad (\text{voir } [3], \text{p.28}) \text{ - donc } Nrd(E^* \cap NRD^{-1}(k^*)) =$$

$$Nrd(Nrd^{-1}(1_0^*)) = 1_0^* \cap Nrd(E^*) \subseteq N^{-1}(k^*) \cap Nrd(E^*) = \text{---},$$

$\Sigma_{i_0}(E) \subseteq \Sigma_{I_0}(D) = \Sigma_I(D)$ (c'est clair) , et

$\mathrm{Nrd}(E^*)^{(1-\sigma_0)} \subseteq \mathrm{Nrd}(E^* \cap [D^*,D^*]) \subseteq \mathrm{Nrd}(E^* \cap \Sigma_I(D))$ (voir [3], p.50) ,

on obtient par un calcul simple les cinq suites exactes ci-dessous:



avec:

γ	induit par l'identité	δ	induit par l'identité
φ	induit par l'inclusion	ζ	induit par l'inclusion
ψ	induit par Nrd modulo 1^*	ε	induit par Nrd modulo 1^*
ξ	induit par l'application $\nu\lambda \mapsto \nu$ ($\lambda \in 1^*$ et $\nu \in N^{-1}(k^*) \cap \mathrm{Nrd}(E^*)$) .		

Comme application on en tire:

(4) l'exposant de $\frac{E^* \cap \mathrm{NRD}^{-1}(k^*)}{E^* \cap \Sigma_I(D)}$ divise le double de l'exposant de $\mathrm{USK}_1(E,\tilde{i})$;

(5) $i(A) = i(D) = 2$ (c'est-à-dire $r = 1$ et $E = L$) implique $E^* \cap \mathrm{NRD}^{-1}(k^*) = E^* \cap \Sigma_I(D)$ (voir 2^o et l'exemple (A),§ 2.);

(6) $\mathrm{USK}_1(E,\tilde{i}) = \mathrm{USK}_1(E,\tilde{i}_0) = 1$ implique $E^* \cap \mathrm{NRD}^{-1}(k^*) = E^* \cap \Sigma_I(D)$, si k vérifie la condition (∇) (voir l'exemple (B) dans § 2.).

§ 4. LA DÉMONSTRATION DU THÉORÈME

D'après 4^o,5^o et 6^o dans § 1. on peut se restreindre au cas

$$A = D = \text{corps gauche avec } i(A) = i(D) = 2^r$$

(voir p. ex. (6.10),(6.11) et (6.12) dans [3],p.52/53 , et lignes 12 à 14 sur p.121 dans [2]).

Maintenant, en utilisant convenablement 1^o et 2^o, un résultat classique montre que pour démontrer le théorème il suffit de supposer (3) (voir § 3.) et de démontrer

(7) l'exposant de $\dfrac{E^* \cap \mathrm{NRD}^{-1}(k^*)}{E^* \cap \Sigma_I(D)}$ divise 2^{r-1} ,

et

(8) $E^* \cap \mathrm{NRD}^{-1}(k^*) = E^* \cap \Sigma_I(D)$, si k vérifie la condition (∇) .

Mais pour $r = 1$ les deux assertions sont vraies d'après (5), et pour $r > 1$ on utilise une récurrence sur r , ce qui donne (7) resp. (8) en utilisant (4) resp. (6), c.q.f.d..

RÉFÉRENCES

[1] A.A. ALBERT - Structure of Algebras - AMS Coll. Publ. 24, New York (1939).

[2] P. DRAXL - SK_1 über vollständig diskret bewerteten Körpern und Galoiskohomologie abelscher Körpererweiterungen - J. reine u. angew. Math. 293/294, 116-142 (1977).

[3] P. DRAXL, M. KNESER (éditeurs) - SK_1 von Schiefkörpern - Seminar Bielefeld-Göttingen, SS 1976 (distribué par Math. Inst. d. Univ. Göttingen, Bunsenstr. 3/5, D-3400 Göttingen).

[4] V.I. JANČEVSKIĬ - Simple Algebras with Involution, and Unitary Groups - Math. USSR Sbornik 22, 372-385 (1974).

[5] V.I. JANČEVSKIĬ - On Reduced Unitary K-Theory - Soviet Math.

Dokl. 17, 1220-1223 (1976).

[6] V.I. JANČEVSKIĬ - K-théorie réduite unitaire et corps gauches sur un corps valué henselien à valuation discrète (en russe) - Izv. Akad. Nauk SSSR 42, 879-918 (1978).

[7] V.P. PLATONOV, V.I. JANČEVSKIĬ - The Structure of Unitary Groups and the Commutator Group of a Simple Algebra over Global Fields - Soviet Math. Dokl. 14, 132-136 (1973).

[8] V.P. PLATONOV, V.I. JANČEVSKIĬ - On the Kneser-Tits Conjecture for Unitary Groups - Soviet Math. Dokl. 16, 1456-1460 (1975).

[9] C. RIEHM - The Corestriction of Algebraic Structures - Inventiones math. 11, 73-98 (1970).

[10] J.-P. SERRE - Corps locaux - Paris (1962).

[11] J. TITS - Groupes de Whitehead de groupes algébriques simples sur un corps - Séminaire Bourbaki 505 (1976/77).

[12] C.T.C. WALL - On the Commutator Subgroups of Certain Unitary Groups - J. of Algebra 27, 306-310 (1973).

Peter DRAXL

Universität Bielefeld

Fakultät für Mathematik

Postfach 8640

D-4800 Bielefeld

Astérisque

PAUL ERDÖS

Some unconventional problems in number theory

Astérisque, tome 61 (1979), p. 73-82

<http://www.numdam.org/item?id=AST_1979__61__73_0>

Société Mathématique de France
Astérisque 61 (1979) p. 73-82

SOME UNCONVENTIONAL PROBLEMS IN NUMBER THEORY

by

Paul ERDÖS

I have several papers with a similar title which will be published soon - at least one of them is a joint paper with R.R. Hall. The number of unsolved problems is so large that I can keep the overlap to a minimum.

First of all I state a very old conjecture of mine : the density of integers n which have two divisors d_1 and d_2 satisfying $d_1 < d_2 < 2 d_1$ is 1 . I proved long ago [1] that the density of these numbers exists but I have never been able to prove that it is 1 . I claimed [2] that I proved that almost all integers n have two divisors

$$(1) \qquad d_1 < d_2 < d_1 \left(1 + \left(\frac{e}{3}\right)^{1 - \eta \log\log n}\right)$$

and that (1) is best possible, namely it fails if $1 - \eta$ is replaced by $1 + \eta$. R.R. Hall and I confirmed this later statement but unfortunately we cannot prove (1) . We are fairly sure that (1) is true and perhaps it is not hopeless to prove it by methods of probabilistic number theory which are at our disposal.

Denote by $d^+(n)$ the number of integers k for which n has a divisor d satisfying $2^k < d \leq 2^{k+1}$. I conjecture that for almost all n

$$d^+(n) / d(n) \to 0$$

which of course implies that almost all integers have two divisors satisfying $d_1 < d_2 < 2 d_1$. It would be of some interest to get an asymptotic formula for

$$\sum_{n=1}^{X} d^+(n) = F(X) \quad .$$

It is easy to prove that $F(X) / X \log X \to 1$.

Another interesting and unconventional problem states as follows : let $1 = d_1 < d_2 < \ldots < d_{\tau(n)} = n$ be the set of divisors of n .

Put :

$$G(n) = \sum_{i=1}^{\tau(n)-1} d_i / d_{i+1} \quad .$$

I conjecture that $\varphi(n) \to \infty$ if we disregard a sequence of integers n of density 0. This again would imply the conjecture on $d_1 < d_2 < 2d_1$, but needless to say I cannot prove it.

It would be of interest to determine the normal order of $d^+(n)$ and $\varphi(n)$ (or at least of $\log \varphi(n)$ and $\log d^+(n)$). Also an asymptotic formula for

$$\sum_{n=1}^{x} \varphi(n)$$

would be of interest. It is easy to prove that $\frac{1}{x} \sum_{n=1}^{x} \varphi(n) \to \infty$.

Let $p_1 < \ldots < p_{V(n)}$ be the consecutive prime factors of n. Alladi and I proved that (unpublished):

$$f(n) = \sum_{i=1}^{V(n)-1} p_i/p_{i+1}$$

has a distribution function and a bounded average.

A well-known theorem of Hardy and Ramanujan states that the normal order of $V(n)$ (the number of prime factors of n) is $(1 + o(1))\log\log n$. A special case of our well-known theorem with Kac [3] states that

$$\frac{V(n) - \log\log n}{(\log\log n)^{1/2}}$$

has normal distribution.

More than 40 years ago I proved that if $p_1^{(n)} < \ldots < p_{V(n)}^{(n)}$ are the consecutive prime factors of n, then for almost all n the ν-th prime factor of n satisfies

$$\log\log p_\nu^{(n)} = (1 + o(1))\nu \tag{2}$$

More precisely: the every $\varepsilon > 0$, $\eta > 0$ there is an $\ell_0 = \ell_0(\varepsilon, \eta)$ so that the density of integers n for which for every $\ell_0 < \nu \leq V(n)$

$$\nu(1 - \varepsilon) < \log\log p_\nu^{(n)} < (1 + \varepsilon)\nu \tag{2'}$$

is greater than $1 - \eta$ [4]. I do not prove (2) in [4], I only indicate that it is a special case of a result which can easily be deduced by methods of probabilistic number theory.

(2) seems to me to be interesting and has many applications, thus at the end of this paper I give a direct and simple proof of (2) . A similar proof of (2) is outlined in a forthcoming paper of S. Wagstaff and myself. This paper also deals with an unconventional problem. Let B_n be the n-th Bernoulli number and

$$\frac{a_n}{b_n} = \sum_{p-1 \mid n} \frac{1}{p}$$

its fractional part. Let n be the smallest integer with this fractional part. Then the density d_n of integers m with fractional part a_n/b_n exists and $\sum_n' d_n = \infty$ where the dash indicates that the summation is only extended over the n which have fractional part a_n/b_n and are minimal (our paper will soon appear in Illinois J. of Math.).

Denote by $d_v(p)$ the density of the integers n whose v- th prime factor is n . $d_v(p)$ can easily be calculated by the exclusion - inclusion principle (essentially the sieve of Eratosthenes). By (2), for almost all integers, $p_v^{(n)}$ is about expexp v . On the other hand, it is easy to see that the largest value of $d_v(p)$ is assumed for much smaller values of p , in fact for

$$e^{v(1-\varepsilon)} < p < e^{v(1+\varepsilon)}$$

by more careful computation it would easily be possible to obtain better estimates. The simple explanation for this apparent paradox is that there are very much more values of p at e^{e^v} than at e^v . It is not impossible that $d_v(p)$ is unimodular, i.e. it first increases with p then assumes its maximum and then decreases. I in fact doubt that $d_v(p)$ behaves so regularly but have not disproved it. The same problems arise if $d_v(n)$ denotes the density of the integers m whose v-th divisor is n . Here we obtain that if $D_1 < D_2$ are the consecutive divisors of n then for all but εX integers $n < X$ for $v > v_0(\varepsilon, n)$

$$\exp\left(v^{1/\log 2 - \varepsilon}\right) < D_v < \exp\left(v^{1/\log 2 + \varepsilon}\right) .$$

On the other hand, for fixed v , $d_v(n)$ is maximal for

$$\exp((1-\varepsilon)\log v \log\log v) < D_v < \exp((1+\varepsilon)\log v \log\log v).$$

It can be shown that $d_v(n)$ is not unimodular.

I now state some further results on the prime factors of integers which can be obtained by the methods of probabilistic number theory or also by more elementary but longer computations. Some of these results have been stated in [5].

For almost all integers n :

$$\sum' \frac{1}{v} = (\frac{1}{2} + o(1)) \operatorname{loglog} n$$

where the dash indicates that the summation is extended over the v satisfying $\operatorname{loglog} p_v^{(n)} > v$.

Similarly, for almost all n :

$$\sum_{p_v^{(n)} > p_v^{(n+1)}} \frac{1}{v} = (\frac{1}{2} + o(1)) \operatorname{loglog} n .$$

On the other hand, it is not hard to show that it is not true that for almost all n :

$$\sum' 1 = (\frac{1}{2} + o(1)) \operatorname{loglog} n$$

On the other hand, if $v_{i+1} > (1 + c) v_i$, then for almost all n :

$$(3) \qquad \sum_{\operatorname{loglog} p_{v_i}^{(n)} > v_i} 1 = (\frac{1}{2} + o(1)) \sum_{v_i < \operatorname{loglog} n} 1$$

It easily follows from the methods of [3] that

$$\frac{\operatorname{loglog} p_v^{(n)} - v}{v^{1/2}}$$

has normal distribution, and that if $v_1/v_2 \to \infty$, then

$$\frac{\operatorname{loglog} p_{v_1}^{(n)} - v_1}{v_1^{1/2}} \quad \text{and} \quad \frac{\operatorname{loglog} p_{v_2}^{(n)} - v_2}{v_2^{1/2}}$$

are asymptotically independent. (3) follows from this without too much difficulty.

For further results of this type see [5]. Here we just make two more remarks. (2) does not mean that $p_v^{(n)}$ is really close to e^{e^v}. In fact, the following results hold.

Let $\alpha(v)$ tend to 0 monotonically as v tends to infinity. Denote by $h_\alpha(n)$ the number of v-s for which the v-th prime factor $p_v^{(n)}$ of n satisfies :

$$v - \alpha(v) < \log\log p_v^{(n)} < v + \alpha(v)$$

Then, if $\sum_{v=1}^{\infty} \alpha(v)/v^{1/2} < \infty$, for every k the density β_k of integers n for which $h_\alpha(n) = k$ exists and $\sum_{k=1}^{\infty} \beta_k = 1$ (or roughly speaking $h_\alpha(n)$ is almost always bounded and $h_\alpha(n)$ has a distribution function).

If $\sum_{v=1}^{\infty} \alpha(v)/v^{1/2} = \infty$, then $h_\alpha(n) \to \infty$ for almost all n .

In particular, for almost all n ,

$$\sum{}' 1/v^{1/2} = (1 + o(1))\, c \log\log\log n$$

where the summation is extended over the v for which $v < \log\log p_v^{(n)} < v + 1$. On the other hand, it is not true that for almost all n

$$\sum{}' 1 = (1 + o(1))\, c_1 (\log\log n)^{1/2} \qquad (4)$$

.

The order of magnitude of the left side of (4) is $(\log\log n)^{1/2}$ and with more trouble the distribution function could be calculated.

Let $p_1 < p_2 < \ldots$ be an infinite sequence of primes, it is quite easy to prove that

$$\sum 1/p_i = \infty$$

is the necessary and sufficient condition that almost all integers n should have a prime factor p_i . It seems very difficult to obtain a necessary and sufficient condition that if $a_1 < \ldots$ is a sequence of integers then almost all integers n should be a multiple of one of the a's . I just want to illustrate the difficulty by a simple example : let $n_{i+1} > (1 + c)\, n_i$. Consider the integers m which have a divisor d satisfying $n_k < d < n_k(1 + \eta_k)$.

If $\sum_{h=1}^{\infty} \eta_k < \infty$ then it is easy to see that the density of these integers exists and is less than 1 .

If $\sum_{h=1}^{\infty} \eta_k = \infty$ it seems difficult to get a general result, e.g. if $\eta_k = \frac{1}{k}$ the density in question exists and is less than 1 .

It seems certain that there is an α, $0 < \alpha < 1$ so that if $\beta < \alpha$ and $\eta_k = 1/k^\beta$ the density of the m having a divisor d, $n_k < d < n_k(1 + 1/k^\beta)$ is 1 and if $\beta > \alpha$ it is less than 1.

Denote by $\varepsilon(n, m)$ the density of integers having a divisor d satisfying $n < d < m$ and by $\varepsilon'(n, m)$ the density of integers having precisely one divisor d, $n < d < m$. Besicovitch proved $\liminf \varepsilon(n, 2n) = 0$ and I proved that if $\log m/\log n \to 1$, then $\lim \varepsilon(n, m) = 0$ [6].

It is easy to see that this result is best possible, i.e. $\lim \varepsilon(n, m) = 0$ implies $\log m/\log n \to 1$.

Further, I can prove that :

$$\varepsilon'(n, m) < c/(\log n)^\alpha$$

for a certain $0 < \alpha < 1$. Perhaps $\varepsilon'(n, m)$ is unimodular for $m > n + 1$, but I know nothing about this. I don't know where $\varepsilon'(n, m)$ assumes its maximum.

I am sure that :

$$\varepsilon'(n, m) / \varepsilon(n, m) \to 0$$

for $m = 2n$. If $m - n$ is small, then clearly $\varepsilon'(n, m) / \varepsilon(n, m) \to 1$ and I don't know where the transition occurs.

Some time ago the following question occured to me : let k be given $n > n_0(k)$. Is there an absolute constant α so that for every $n < m < n^k$ there is a t, $0 < t < (\log n)^\alpha$ so that $m + t$ has a divisor in $(n, 2n)$?

More generally : if $n + 1 = a_1 < a_2 < \ldots$ is the sequence of integers which have a divisor d, $n < d < 2n$. Determine or estimate $\max_{a_i < n^k} (a_{i+1} - a_i)$.

Now we prove (2) and (2') . Denote by $V(n)$ the number of prime factors of n and by $V_{T(n)}$ the number of prime factors of n exceeding T. The well known inequality of Turán [7] implies

$$(5) \qquad \sum_{n=1}^{X} (V_T(n) - \log\log T)^2 < C X \log\log T ,$$

where C is an absolute constant. From (5) we immediately obtain by the Tchebicheff inequality that the number of integers $n < X$ satisfying

$$(6) \qquad |V_T(n) - \log\log T| < Z(\log\log T)^{1/2}$$

is less than $C X/Z^2$.

Put $T_i = (\exp\exp i^4)$. From (6) we obtain that the number of integers $n < X$ for which some $i > i_o$

$$(7) \qquad |V_{T_i}(n) - \operatorname{loglog} T_i| > (\operatorname{loglog} T_i)^{3/4}$$

is less than

$$(8) \qquad C X \sum_{i > i_o} \frac{1}{i^2} < \varepsilon X$$

for every $\varepsilon > 0$ if $i_o > i_o(\varepsilon)$. To complete our proof observe that $V_T(n)$ is nondecreasing in T . Thus, if $T_i < T < T_{i+1}$ and n satisfies (7), we have

$$(9) \qquad |V_T(n) - \operatorname{loglog} T| < (\operatorname{loglog} T_i)^{3/4} + \operatorname{loglog} T_{i+1}$$

$$\operatorname{loglog} T_i < 10 (\operatorname{loglog} T)^{3/4} .$$

Thus, from (7), (8) and (9) it follows that (2) and (2') are satisfied for almost all n and our proof is complete.

Finally I state an old problem of mine which is probably very difficult and which seems to be unattackable by the methods of probabilistic number theory : denote by $P(n)$ the greatest prime factor of n . Is it true that the density of integers n satisfying $P(n+1) > P(n)$ is $\frac{1}{2}$? Is it true that the density of integers for which

$$(10) \qquad P(n+1) > P(n)\, n^{\alpha}$$

exists for every α ? Pomerance and I proved (our paper will soon appear in Aequationes Mathematica) that if $\varepsilon_n \to 0$ then the upper density of the integers satisfying

$$n^{-\varepsilon_n} < \frac{P(n+1)}{P(n)} < n^{\varepsilon_n}$$

tends to 0 as n tends to ∞ .

To end this note, I state a few unrelated unconventional problems. Denote by $\Phi(X)$ the number of integers $n < X$ for which $\varphi(m) = n$ is solvable ($\varphi(n)$ is Euler's φ function). The sharpest current bounds for $\Phi(X)$ are due to R.R. Hall and myself [8].

We prove (for every $\varepsilon > 0$ and $X > X_0(\varepsilon)$)

$$(11) \qquad \frac{X}{\log X} \exp\left((\log\log\log X)^2\right) < \Phi(X) < \frac{X}{\log X} \exp\left(C_1 (\log\log X)^{1/2}\right) .$$

It seems to us that the upper bound in (11) is closer to the truth, in fact we believe that for every $\varepsilon > 0$ and $X > X_0(\varepsilon)$

$$\Phi(X) > \frac{X}{\log X} \exp\left(C_2 (\log\log X)^{1/2}\right) .$$

It is not certain that there is a genuine asymptotic formula for $\Phi(X)$ but perhaps $\Phi(CX)/\Phi(X) \to C$ holds for every $C > 0$.

Denote $\Phi_K(X)$ the number of distinct integers n of the form $\varphi(kX + t)$, $1 \le t \le X$. For "small" k all the $\Phi_K(X)$ probably have a similar asymptotic behaviour, but of course I can prove nothing. I have no idea how many new integers appear amongst the $\varphi(kX + t)$, $1 \le t \le X$. In other words : estimate the number of integers $n < X$ for which the smallest solution of $\varphi(m) = n$ satisfies $kX < m \le (k+1)X$. I can at the moment say nothing interesting about this problem.

Denote by m_X the largest integer for which $\varphi(m_X) \le X$ and by m'_X the largest integer for which $\varphi(m'_X) \le X$ and for which there is no $u < m'_X$ with $\varphi(u) = \varphi(m'_X)$. In other words m'_X is the largest integer for which $\varphi(m'_X) \le X$ and which gives a new number of the form $\varphi(m)$. I hope that $m'_X/m_X \to 1$ but I do not see how to prove this. Perhaps $m'_X = m_X$ holds for infinitely many X .

Let $u_1^{(n)} < \ldots < u_t^{(n)}$ be the set of integers (if they exist) for which $\varphi(u_i) = n$, $1 \le i \le t$. An old (and probably hopeless) conjecture of Carmichael states that $t \ge 1$ implies $t > 1$. It would be perhaps interesting to investigate

$$\max_{n < X} u_t^{(n)} / u_1^{(n)} .$$

One final question about the φ - function : let $p^{(n)}$ be the smallest prime $\equiv 1 \pmod n$. By a classical result of Linnik [9] $p^{(n)} < n^{1+C}$. Let u_n be the smallest integer with $\varphi(u_n) \equiv 0 \pmod n$. If $n = p - 1$ we of course have $u_n = p^{(n)}$ and it is easy to show that for infinitely many n $u_n < p^{(n)}$. $u_n/n \to \infty$ stets for almost all n . The proofs are not difficult.
I am sure that $p^{(n)}/u_n \to \infty$ holds for almost all n .

Let $q_1 < q_2 < \dots$ be a sequence of primes for which $q_{i+1} \equiv 1 \pmod{q_i}$. It easily follows from the theorem of Linnik [9] that there is an infinite sequence of such primes satisfying for every i $q_i < (\exp\exp C i)$ for some absolute constant C. In fact, there is little doubt that such a sequence exists with $q_i < \exp(i (\log i)^{1+\varepsilon})$. I am fairly certain that for every such sequence $\lim_{i=\infty} q_i^{1/i} = \infty$ but I have never been able to prove this.

Denote by $h(n)$ the largest integer ℓ for which there is a sequence of prime divisors $p_i^{(n)}$ of n for which

$$p_{i+1}^{(n)} \equiv 1 \pmod{p_i^{(n)}}, \quad 1 \le i \le \ell - 1 = h(n) - 1 .$$

It is easy to see that $h(n)$ tends to infinity for almost all n. Denote by $L(n)$ the smallest integer v for which the v-times iterated logarithm of n is less than e. It seems that the normal order of $h(n)$ is about $L(n)$ but I have not carried out all the details. Denote by $H(n)$ the largest integer u for which there is a sequence of divisors d_i of n, $1 \le i < u - 1$ for which $d_{i+1} \equiv 1 \pmod{d_i}$.

I am not sure if $H(n)/h(n) \to \infty$ holds for almost all n, I am sure that $H(n)$ is not much larger than $L(n)$. The estimation of $H(n)$ is related to the following question: denote by $A(d, \alpha)$ the density of integers n which have a divisor $D \equiv 1 \pmod{d}$, $1 < D < \exp d^{\alpha}$. For $\alpha < 1$, $A(d, \alpha) \to 0$ is trivial. I can prove $A(d, 1) \to 0$ as $d \to \infty$. This last result is not quite trivial since

$$\sum{}' \frac{1}{D} = 1 + o(1)$$

where the dash indicates that $1 < D < \exp d$, $D \equiv 1 \pmod{d}$.

I believe that there is an α, $1 < \alpha < \infty$ so that for $\beta < \alpha$ $\lim_{d=\infty} A(d, \beta) = 0$ and for $\beta > \alpha$ $\lim_{d=\infty} A(d, \beta) = 1$.

REFERENCES

[1] P. Erdös On the density of some sequences of integers, Bull. Amer. Math. Soc. 54 (1948), 685-692.

[2] P. Erdös On some applications of probability to analysis and number theory, J. London Math. Soc. 39 (1964), 692-696.

[3] P. Erdös and M. Kac
The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math. 62 (1940), 738-742.

[4] P. Erdös On the distribution function of additive functions, Annals of Math. 47 (1946), 1-20.

[5] P. Erdös On the distribution of prime divisors, Aequationes Mathematicae 2 (1969), 177-183.

[6] See e.g. the well known book of H.H. Halberstam and K.F. Roth, Sequences, Oxford, Calenron Press 1966, Chapter V.

[7] P. Turán On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934), 274-276.

[8] P. Erdös and R.R. Hall
On the values of Euler's φ function. Acta Arith. 22 (1973), 201-206 and Distinct values of Euler's φ function.

[9] K. Prachar Primzahlverteilung, Springer Verlag, 1957.

Paul ERDÖS
Mathematical Institute of the Academy
BUDAPEST
V. Realtanoda u 13-15
HONGRIE

Astérisque

R. GILLARD

Extensions abéliennes et répartition modulo 1

Astérisque, tome 61 (1979), p. 83-93

<http://www.numdam.org/item?id=AST_1979__61__83_0>

Société Mathématique de France
Astérisque 61 (1979) p. 83-93

EXTENSIONS ABÉLIENNES ET RÉPARTITION MODULO 1

par R. GILLARD

Je me propose d'exposer les importants résultats de B. Ferrero et L. Washington, cf. [2] et [13]. Pour les détails et les démonstrations complètes, je renvoie à leurs articles. Par ailleurs, ceux-ci rappellent les preuves de la plupart des préliminaires utilisés. La différence principale avec la conférence donnée à Luminy est l'unification des démonstrations à l'aide d'un résultat de [13].

§ 1. - RÉSULTATS.

Soient p (resp. ℓ) un nombre premier et k un corps de nombres de degré fini sur $\mathbb{Q}$. Désignons par k_∞/k une $\mathbb{Z}_p$-extension, i.e. une extension galoisienne avec $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_p$. Ainsi on peut écrire

$$k_\infty = \bigcup_{n\in\mathbb{N}} k_n \quad \text{avec} \quad \mathrm{Gal}(k_n/k) \simeq \mathbb{Z}/p^n\mathbb{Z} .$$

Notons h_n le nombre de classes de k_n et $e_n^{(\ell)}$ l'exposant de ℓ dans h_n ; si $\ell = p$, K. Iwasawa a démontré :

THÉORÈME 1, [4]. - *Il existe des entiers* λ, μ, ν *avec* $\lambda \geq 0$, $\mu \geq 0$ *tels que* $e_n^{(p)} = \mu p^n + \lambda n + \nu$ *pour tout* n *assez grand*.

Exemple fondamental : $k = \mathbb{Q}(\zeta_p)$, $k_n = \mathbb{Q}\left(\zeta_{p^{n+1}}\right)$, $k_\infty = \bigcup_{n\in\mathbb{N}} k_n$, avec $p \neq 2$, où pour $m \in \mathbb{N}$, ζ_m désigne une racine primitive $m^{\text{ième}}$ de l'unité. On savait que μ est nul dans les cas suivants :

- $e_o^{(p)} = 0$, i.e. p est régulier.
- $p \leq 4\,000$, cf. [5].
- $p \leq 8\,000$, cf. [7].
- $p \leq 30\,000$, cf. [8].
- $p \leq 125\,000$, cf. [11].

Remarque : Iwasawa a construit des $\mathbb{Z}_p$-extensions dont l'invariant μ est > 0 , cf. [6].

Désignons par $\mathbb{Q}_\infty$ l'unique $\mathbb{Z}_p$-extension de $\mathbb{Q}$. Dans la suite, nous supposons que k est une extension abélienne de $\mathbb{Q}$ et que k_∞ est l'extension composée $k.\mathbb{Q}_\infty$. Notons $\mu(k)$ l'invariant μ pour cette $\mathbb{Z}_p$-extension de k .

THÉORÈME 2, [1]. -
1) Si $e_o^{(p)} = 0$ et k contient ζ_p , alors $\mu(k) = 0$.
2) Si $p = 2$ ou 3 , alors $\mu(k) = 0$.

La partie 2) résulte du fait qu'on a à considérer (cf. plus loin) des sommes sur un 1/2 système de racines de l'unité dans $\mathbb{Z}_p$. Ainsi, pour $p = 2$ ou 3 ces sommes se réduisent à un seul terme et cette simplification permet de conclure.

THÉORÈME 3, [2]. - Pour tout k , on a $\mu(k) = 0$.

La démonstration de ce théorème, comme celle de la partie 1) du théorème 2, utilise des arguments de répartition modulo 1 ; ceux employés dans [2] sont plus forts et plus naturels que ceux de [1].

Soient S un ensemble d'idéaux premiers de k contenant les diviseurs premiers de p et k_S la p-extension de k non ramifiée en dehors de S maximale : k_S contient k_∞ et en est une extension galoisienne.

COROLLAIRE. - Si k contient ζ_p (ζ_4 si $p = 2$) , $\mathrm{Gal}(k_S/k_\infty)$ est un pro-p-groupe libre.

En effet, on sait, [10], que ceci est une conséquence de $\mu(k) = 0$.

THÉORÈME 4, [13]. - Pour k et ℓ fixés, avec $\ell \neq p$, la suite $e_n^{(\ell)}$ est stationnaire.

Remarquons que pour $p = 2$ ou 3 , ce résultat est déjà dans [12] qui utilise la même simplification que pour la partie 2) du théorème 2.

Signalons enfin que les démonstrations des résultats précédents peuvent être rendues effectives (cf. [2] § 4) et peuvent donner pour k , ℓ , p fixés des bornes pour l'invariant λ du théorème 1 et pour le plus petit indice n_o tel que $e_{n_o}^{(\ell)} = e_{n_o+1}^{(\ell)}$.

Notations. - Désignons par Ω_p (resp. Ω_ℓ) une clôture algébrique de $\mathbb{Q}_p$ (resp. $\mathbb{Q}_\ell$) et par $\mathfrak{P}$ (resp. $\mathfrak{L}$) son idéal maximal. Désignons par R un système de représentants des racines de l'unité de $\mathbb{Z}_p$ modulo ± 1 . On suppose dans la suite $p \neq 2$. Si $\alpha \in \mathbb{Z}_p$, on note $t_m(\alpha)$ le $m^{\text{ième}}$ coefficient de son développement p-adique et $s_n(\alpha)$ la $n^{\text{ième}}$ somme partielle :

$$\alpha = \sum_0^\infty t_m(\alpha) p^m \quad \text{avec} \quad 0 \leq t_m(\alpha) < p \ ,$$

$$s_n(\alpha) = \sum_0^n t_m(\alpha) p^m \quad \text{d'où} \quad 0 \leq s_n(\alpha) < p^{n+1} \quad \text{et} \quad s_n(\alpha) \equiv \alpha \bmod p^{n+1} \ .$$

§ 2. - RÉPARTITION MODULO 1 DES $p^{-n-1} s_n(\alpha\eta)$, $\alpha \in \mathbb{Z}_p^*$, $\eta \in R$.

2.1. Introduisons le concept clef de [2] :

DÉFINITION. - *Des entiers p-adiques $\gamma_1, \ldots, \gamma_r$ sont dits conjointement normaux si et seulement si la suite $(p^{-n-1} s_n(\gamma_1), \ldots, p^{-n-1} s_n(\gamma_r))_{n \geq 0}$ est uniformément répartie dans $([0,1[)^r$.*

Cette définition transpose aux nombres p-adiques une définition classique ([9] chap. I, § 8, notes) en répartition modulo 1 pour les nombres réels ; il faut remplacer $1/p$ par p dans les développements p-adiques.

Pour $k \in \mathbb{N}^*$, soit $\mathfrak{M}_k$ l'ensemble des matrices c à r lignes et k colonnes dont les coefficients c_{ij} sont des entiers vérifiant $0 \leq c_{ij} < p$. Pour toute matrice c dans $\mathfrak{M}_k$, désignons par $S(c)$ l'ensemble des entiers $n \geq 1$ vérifiant

$$t_{n+j}(\gamma_i) = c_{ij} \quad \text{pour tout} \quad i = 1, \ldots, r \quad \text{et} \quad j = 1, \ldots, k \ .$$

En traduisant sur les chiffres du développement p-adique la condition

$$p^{-n-1}s_n(\gamma_i) \in [p^{-N}a_i\ ,\ p^{-N}(a_i+1)[\quad ,\ \text{pour}\quad N \in \mathbb{N}^*\ ,$$

on trouve :

PROPOSITION 1. - Les entiers p-adiques $\gamma_1,\ldots,\gamma_r$ sont conjointement normaux si et seulement si pour tout $k \in \mathbb{N}^*$ et tout $c \in \mathfrak{M}_k$, $S(c)$ admet une densité égale à p^{-rk}.

En s'inspirant d'une démonstration classique (cf. [9], théorème 4.1), Ferrero et Washington démontrent :

PROPOSITION 2. - Soient $\gamma_1,\ldots,\gamma_r$ des entiers p-adiques $\mathbb{Q}$-linéairement indépendants, alors pour presque tout $\alpha \in \mathbb{Z}_p$ (au sens de la mesure de Haar), les nombres $\alpha\gamma_1,\ldots,\alpha\gamma_r$ sont conjointement normaux.

2.2. On peut renforcer l'énoncé précédent :

PROPOSITION 3, [13]. - Soient $\beta_1,\ldots,\beta_r$ des entiers p-adiques $\mathbb{Q}$-linéairement indépendants. Donnons-nous un nombre réel $\varepsilon > 0$, des entiers $m,d,g_1,\ldots,g_r$ vérifiant $m > 0$, $d > 0$, d premier à p, et des nombres réels $x_1,\ldots,x_r$ appartenant à $[0,1]$. Alors pour tout n entier assez grand, il existe un entier p-adique α vérifiant :

(1) $\alpha \equiv 1 \mod p^m$

(2) $s_n(\alpha\beta_j) \equiv g_j \mod d$, pour tout $j = 1,\ldots,r$

(3) $|p^{-n-1}s_n(\alpha\beta_j) - x_j| < \varepsilon$ pour tout $j = 1,\ldots,r$

Pour démontrer la proposition 3, Washington utilise la proposition 2 pour trouver un élément β de $\mathbb{Z}_p$ congru à 1 modulo p^m, tels que les nombres $\gamma_j = \beta\beta_j$ soient conjointement normaux ; si $c \in \mathfrak{M}_k$ pour k assez grand, choisissons $n_o \in S(c)$. Avec les données de la proposition 3, soit n entier supérieur ou égal à $n_o + k + m$. Washington construit une

matrice c telle que pour un entier convenable q , $n_o < q \leq n_o + k$, l'entier p-adique $\alpha = \beta(1+p^{n-q})$ vérifie les conditions (1), (2) et (3).

2.3. Nous utiliserons les résultats de 2.1 et 2.2 sous la forme suivante (cf. [13]) dont l'énoncé suppose R convenablement choisi :

PROPOSITION 4. - Soient m et d des entiers > 0 , d premier à p . Pour tout n assez grand, on peut trouver deux entiers p-adiques α_1 et α_2 , congrus à 1 modulo p^m et un élément η_o de R tels que :

(4) $s_{n+m}(\alpha_1\eta) = s_n(\alpha_1\eta) \equiv 0 \mod d$ pour tout $\eta \in R$

(5) $s_{n+m}(\alpha_2\eta) = s_n(\alpha_2\eta) \equiv 0 \mod d$ pour tout $\eta \in R - \{\eta_o\}$

(6) $s_{n+m}(\alpha_2\eta_o) = s_n(\alpha_2\eta_o) + p^{n+1} \equiv 0 \mod d$.

Démonstration : Soient $\eta_1,\ldots,\eta_{(p-1)/2}$ les éléments de R ordonnés de façon à ce que $\eta_1,\ldots,\eta_r$ soient $\mathbb{Q}$-linéairement indépendants ($r=\varphi(p-1)$, φ fonction d'Euler). Pour $j = 1,\ldots,(p-1)/2$, on a

$$\eta_j = \sum_{i=1}^{r} a_{ji}\eta_i \quad \text{pour des } a_{ji} \text{ entiers.}$$

Soient $c_1 > \ldots > c_r$ des éléments de $]0,1]$ et posons

$$c_j = \sum_{i=1}^{r} a_{ji}c_i \quad \text{pour } j = r+1,\ldots,(p-1)/2 .$$

On peut choisir, cf. [2] ou [13], c_2 puis c_3 puis ... puis c_r suffisamment petits pour qu'il existe j_o tel que

$$0 < c_j < c_{j_o} \quad \text{pour tout } j \neq j_o ,$$

si R a été convenablement choisi. Choisissons x_{j_o} dans $]p^{-m},2p^{-m}[$ et posons $x_j = c_j x_{j_o}/c_{j_o}$. Supposons x_{j_o} suffisamment proche de p^{-m} pour avoir $x_j \in]0,p^{-m}[$ si $j \neq j_o$. Posons $g_j = 0$ et prenons ϵ suffisamment petit pour la suite. Soit α_2 un entier p-adique vérifiant les conditions de la proposition 3 avec $\beta_j = \eta_j$ si $j = 1,\ldots,r$ où n est remplacé par $n+m$: la condition (3) implique alors

$$0 < \sum_{i=1}^{r} a_{ji} s_{n+m}(\alpha_2 \eta_i) < p^{n+1} \quad \text{si} \quad j = 1,\ldots,(p-1)/2 \quad \text{et} \quad j \neq j_o$$

$$p^{n+1} < \sum_{i=1}^{r} a_{j_o i} s_{n+m}(\alpha_2 \eta_i) < 2p^{n+1} .$$

On en déduit les égalités

$$s_{n+m}(\alpha_2 \eta_j) = \sum_{i=1}^{r} a_{ji} s_{n+m}(\alpha_2 \eta_i) = s_n(\alpha_2 \eta_j) \quad \text{si} \quad j \neq j_o$$

$$s_{n+m}\left(\alpha_2 \eta_{j_o}\right) = \sum_{i=1}^{r} a_{j_o i} s_{n+m}(\alpha_2 \eta_i) = s_n\left(\alpha_2 \eta_{j_o}\right) + p^{n+1} .$$

Ainsi α_2 vérifie (5) et (6) avec $\eta_o = \eta_{j_o}$. Pour α_1 on procède de même, mais en choisissant x_{j_o} dans $]0, p^{-m}[$. Dans la proposition 4, on peut donc choisir η_o indépendant de n.

§ 3. - DÉMONSTRATION DU THÉORÈME 3 ($\ell = p$).

3.1. Supposons $k = \mathbb{Q}(\zeta_p)$. Rappelons le résultat de [3] §3 :

PROPOSITION 5. - $\mu(k)$ est non nul si et seulement s'il existe $a \in \mathbb{N}$, a impair, tel que pour tout $\alpha \in \mathbb{Z}_p^*$ et $n \in \mathbb{N}$, on ait

(7) $$\sum_{\eta \in \pm R} t_{n+1}(\alpha\eta).\eta^a \equiv 0 \mod \mathfrak{P} .$$

La démonstration d'Iwasawa utilise le théorème de Stickelberger sur l'annulation du groupe des classes. On peut aussi (cf. [2]) utiliser la formule analytique du nombre de classes en interprétant les nombres de Bernoulli avec les séries d'Iwasawa.

En regroupant les termes correspondants à η et $-\eta$, (7) s'écrit :

$$2 \sum_{\eta \in R} t_{n+1}(\alpha\eta).\eta^a - (p-1) \sum_{\eta \in R} \eta^a \equiv 0 \mod \mathfrak{P} .$$

Ainsi si $\mu(k)$ est $\neq 0$, il existe a impair tel que

(8) $$\sum_{\eta \in R} t_{n+1}(\alpha_1\eta)\eta^a \equiv \sum_{\eta \in R} t_{n+1}(\alpha_2\eta)\eta^a \mod \mathfrak{P}$$

pour tout $n \in \mathbb{N}$ et tout α_1, tout $\alpha_2 \in \mathbb{Z}_p^*$. Mais en choisissant α_1 et α_2 comme dans la proposition 4, on trouve

$t_{n+1}(\alpha_1\eta) = 0$ pour tout $\eta \in R$

$t_{n+1}(\alpha_2\eta) = 0$ pour tout $\eta \in R - \{\eta_o\}$, $t_{n+1}(\alpha_2\eta_o) = 1$.

En reportant dans (8), on obtient la contradiction

$$0 \equiv \eta_o^a \mod \mathfrak{P} ,$$

d'où le théorème 3 pour $k = \mathbb{Q}(\zeta_p)$.

3.2. Rappelons le résultat de [1] § 1.8 et 2.4 :

PROPOSITION 6. - Si $\mu(\mathbb{Q}(\zeta_p)) = 0$, alors il existe une extension abélienne finie k de $\mathbb{Q}$ avec $\mu(k) \neq 0$ si et seulement si on peut trouver un caractère de Dirichlet (*) χ , impair, tel que

(9) le conducteur f de χ est égal à d ou $d.p$ avec un entier $d \geq 2$, d premier à p .

(10) Pour tout $\alpha \in \mathbb{Z}_p^*$ et $n \in \mathbb{N}$ on a :
$$\sum_{\eta \in R} \sum_{i=0}^{d-1} i\chi(s_n(\alpha\eta) + p^{n+1}i) \equiv 0 \mod \mathfrak{P} .$$

La démonstration de Ferrero consiste à :

1) remarquer (cf. [12] lemme 1), que sans changer k_n pour n assez grand on peut supposer que p^2 ne divise pas le conducteur de k d'où la condition (9) ci-dessus (sachant que k n'est pas inclus dans $\mathbb{Q}(\zeta_p)$).

2) Montrer (cf. [1] § 1.7), en utilisant l'inégalité "du miroir" (Spiegelungsatz de H. Leopoldt) qu'on peut se limiter aux classes "relatives" i.e. aux caractères de Dirichlet impairs.

3) Utiliser la formule analytique du nombre de classes, en interprétant les nombres de Bernoulli en termes de série d'Iwasawa.

(*) à valeurs dans Ω_p .

Démonstration du théorème 3 : Soit χ un caractère de Dirichlet impair vérifiant (9) et (10). Choisissons n assez grand et vérifiant $p^n \equiv 1 \mod d$. Considérons alors la congruence (10) pour α_1 et α_2 comme dans la proposition 4 : seuls les termes relatifs à $\eta = \eta_o$ diffèrent ; en comparant on obtient :

$$(11) \qquad \sum_{i=0}^{d-1} i\chi(a+ip) \equiv \sum_{i=0}^{d-1} i\chi(a-p+ip) \mod \mathfrak{P} ,$$

où a désigne un entier multiple de d et congru à η_o modulo p. Or,

$$(12) \qquad \sum_{i=0}^{d-1} \chi(a+ip) = 0 .$$

Ceci est clair si tous les termes de la somme sont nuls ou si le conducteur de χ est égal à d. Sinon on se ramène à montrer que

$$\sum_{i=0}^{d-1} \chi(1+ip) = 0 \quad ;$$

la somme porte en fait sur le noyau de l'homomorphisme $(\mathbb{Z}/f\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$: sur ce groupe χ est $\neq 1$ car son conducteur est $\neq p$. En utilisant (12), on peut réécrire (11) sous la forme

$$\sum_{i=0}^{d-1} (i+1)\chi(a+ip) \equiv \sum_{i=0}^{d-1} i\chi(a+(i-1)p) \mod \mathfrak{P} .$$

Après simplification, il ne reste que le terme correspondant à $i = d-1$ dans la somme de gauche, i.e. :

$$(13) \qquad d\chi(a-p) \equiv 0 \mod \mathfrak{P} .$$

Comme $a-p$ est congru à $-p$ modulo d et à η_o modulo p, ce nombre est premier à $f = d$ ou dp ; $\chi(a-p)$, non nul, est donc une racine de l'unité : (13) est donc absurde.

§ 4. - DÉMONSTRATION DU THÉORÈME 4 ($\ell \neq p$) .

4.1. Pour $m \in \mathbb{N}$, soit D_m l'ensemble des caractères de Dirichlet à valeurs dans Ω_ℓ^* dont le conducteur et l'ordre valent respectivement p^m et p^{m+1}. Les éléments de D_m peuvent être prolongés en des fonctions continues de $\mathbb{Z}_p$ dans Ω_ℓ. Si ψ appartient à D_{n+m} et α à $\mathbb{Z}_p$, le nombre $\psi_m(\alpha) = \psi(1+\alpha^{-1}p^{n+1})$ est une racine de 1 d'ordre divisant p^m et ne dépendant de α que modulo p^m.

PROPOSITION 7, [12]. - Supposons qu'il existe une extension abélienne finie k de $\mathbb{Q}$ avec $\lim_{n\to\infty} e_n^{(\ell)} = +\infty$; alors on peut trouver un caractère de Dirichlet (*) χ, impair, tel que

(14) le conducteur de χ est égal à d ou $d.p$ avec $d \in \mathbb{N}$, d premier à p,

(15) pour tout m entier assez grand, il existe une infinité de $n \in \mathbb{N}$ tels que pour au moins un élément ψ de D_{n+m}, on ait :

$$\forall \alpha \in \mathbb{Z}_p^* \quad \sum_{\eta \in R} \sum_{i=0}^{d-1} \psi(\alpha^{-1} s_n(\alpha\eta))\chi(s_n(\alpha\eta) + ip^{n+1}) \frac{\psi_m(\alpha\eta)^i}{\psi_m(\alpha\eta)^d - 1} \equiv 0 \mod \mathfrak{L} .$$

En effet, avec l'hypothèse de la proposition 7, avec la formule analytique du nombre de classes, on peut montrer, [12], qu'il existe un caractère de Dirichlet impair χ vérifiant (14) tel que pour une infinité de n dans $\mathbb{N}$, on ait

$$\frac{1}{2} B_{1,\chi\psi} \equiv 0 \mod \mathfrak{L} \tag{16}$$

pour un élément ψ au moins de D_{n+m} ; ici $B_{1,\chi\psi}$ désigne le nombre de Bernoulli

$$\frac{1}{p^{n+m+1}d} \sum_{a=1}^{dp^{n+m+1}} a(\chi\psi)(a) .$$

Désignons par F_n le corps engendré sur $\mathbb{Q}_\ell$ par l'image de χ et ζ_{p^n}. On suppose dans la suite m assez grand pour avoir $F_m \neq F_{m+1}$. Si (16) est vérifié, on obtient (15) pour $\alpha \in \mathbb{Z}_p^*$ et $n \geq m$ en calculant la trace entre F_{n+m} et F_m de $\psi(\alpha^{-1})B_{1,\chi\psi}/2$.

4.2. Soit χ un caractère de Dirichlet impair vérifiant (14) et (15). Pour n assez grand, choisissons α_1 et α_2 comme dans la proposition 4. Comparons la congruence de (15) pour $\alpha = \alpha_1$ et $\alpha = \alpha_2$: seuls les termes relatifs à $\eta = \eta_o$ diffèrent ; en simplifiant, on obtient :

(*) à valeurs dans Ω_ℓ.

$$\sum_{i=0}^{d-1} \psi(\alpha_1^{-1} s_n(\alpha_1\eta_o))\chi(s_n(\alpha_1\eta_o) + ip^{n+1}) \frac{\psi_m(\alpha_1\eta_o)^i}{\psi_m(\alpha_1\eta_o)^d - 1}$$

$$\equiv \sum_{i=0}^{d-1} \psi(\alpha_2^{-1} s_n(\alpha_2\eta_o))\chi(s_n(\alpha_2\eta_o) + ip^{n+1}) \frac{\psi_m(\alpha_2\eta_o)^i}{\psi_m(\alpha_2\eta_o)^d - 1} \mod \mathfrak{L} .$$

Comme $\alpha_1 \equiv \alpha_2 \equiv 1 \mod p^m$, on a $\psi_m(\alpha_1\eta_o) = \psi_m(\alpha_2\eta_o) = \psi_m(\eta_o)$. Soit a un entier multiple de d et congru à η_o modulo p. En remarquant que

$$\psi(\alpha_1^{-1} s_n(\alpha_1\eta_o)) = \psi(\alpha_1^{-1} s_{n+m}(\alpha_1\eta_o)) = \psi(\eta_o) = 1$$

et $$\psi(\alpha_2^{-1} s_n(\alpha_2\eta_o)) = \psi(\alpha_2^{-1} s_{n+m}(\alpha_2\eta_o) - \alpha_2^{-1} p^{n+1}) = \psi(\eta_o - \alpha_2^{-1} p^{n+1})$$

$$= \psi(\eta_o)\psi(1 - \eta_o^{-1}\alpha_2^{-1} p^{n+1}) = \psi_m(\eta_o)^{-1} ,$$

on déduit

$$\sum_{i=0}^{d-1} \chi(a + ip^{n+1})\psi_m(\eta_o)^i \equiv \sum_{i=0}^{d-1} \chi(a + (i-1)p^{n+1})\psi_m(\eta_o)^{i-1} .$$

Après simplification, il ne reste que le terme correspondant à $i = 0$ (resp. $i = d-1$) dans le terme de droite (resp. de gauche) c'est-à-dire

$$\chi(a + p^{n+1}(d-1))\psi_m(\eta_o)^{d-1} \equiv \chi(a - p^{n+1})\psi_m(\eta_o)^{-1} \mod \mathfrak{L}$$

ou encore

$$(\psi_m(\eta_o)^d - 1)\chi(a - p^{n+1}) \equiv 0 \mod \mathfrak{L} .$$

Comme $a - p^{n+1}$ est congru à $-p^{n+1}$ modulo d et à η_o modulo p, $a - p^{n+1}$ est premier à dp donc $\chi(a - p^{n+1})$ est $\neq 0$ donc est une racine de 1. La contradiction provient du fait que $\psi_m(\eta_o)^d - 1 \not\equiv 0 \mod \mathfrak{L}$, puisque $\psi_m(\eta_o)^d$ est une racine de 1 d'ordre p^m. Le théorème 4 résulte alors du fait que la suite $e_n^{(\ell)}$ est croissante.

BIBLIOGRAPHIE.

[1] B. FERRERO.- Iwasawa invariants of abelian number fields, Math. Ann., 234 (1978).

[2] B. FERRERO et L. WASHINGTON.- The Iwasawa invariant μ_p vanishes for abelian number fields, à paraître aux Ann. of Math.

[3] K. IWASAWA.- On some invariants of cyclotomic fields, Amer. J. Math., 80 (1958).

[4] K. IWASAWA.- On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., 65 (1959).

[5] K. IWASAWA et C. SIMS.- Computations of invariants in the theory of cyclotomic fields, J. Math. Soc. Japan, 18 (1966).

[6] K. IWASAWA. - On the μ invariants of $\mathbb{Z}_\ell$-extensions, in : Number theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1-11, 1973.

[7] W. JOHNSON. - On the vanishing of the Iwasawa invariant μ_p for $p < 8000$, Math. Comp., 27 (1973).

[8] W. JOHNSON. - Irregular primes and cyclotomic invariants, Math. Comp., 29 (1975).

[9] L. KUIPERS et H. NIEDERREITER. - Uniform distribution of sequences, Wiley, 1974.

[10] L. KUZMIN. - Cohomological dimension of some Galois groups, Math. USSR IZV., 9 (1975) = Izv. Akad. Nauk SSSR Ser. Mat., 39 (1975).

[11] S. WAGSTAFF. - The irregular primes to 125 000, Math. Comp., 32, (1978).

[12] L. WASHINGTON. - Class numbers and $\mathbb{Z}_p$-extensions, Math. Ann., 214 (1975).

[13] L. WASHINGTON. - The non p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, Inv. Math., 49 (1978).

-:-:-:-

Roland GILLARD
UNIVERSITE SCIENTIFIQUE ET
MÉDICALE DE GRENOBLE I
Laboratoire de Mathématiques Pures
associé au C.N.R.S. n° 188
B.P. 116
38402 SAINT MARTIN D'HERES

(décembre 1978)

Astérisque

DORIAN GOLDFELD

Analytic and arithmetic theory of Poincaré series

Astérisque, tome 61 (1979), p. 95-107

<http://www.numdam.org/item?id=AST_1979__61__95_0>

Société Mathématique de France
Astérisque 61 (1979) p. 95-107

ANALYTIC AND ARITHMETIC THEORY OF POINCARÉ SERIES

by

Dorian Goldfeld

§1. Define $\Gamma = SL_2(\mathbf{Z})$ to be the modular group, and let

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi inz}, \qquad g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi inz},$$

be cusp forms of weight k for Γ which satisfy the modular relations

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z), \quad g(\frac{az+b}{cz+d}) = (cz+d)^k g(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. We are concerned with the general problem of estimating sums of the type

$$\sum_n a_n \overline{b_{n+m}} \qquad (m \in \mathbf{Z}, \ m \text{ fixed}), \tag{1.1}$$

and shall show that the solution to this problem is invariably based on the analytic and arithmetic properties of Poincaré series.

The special case, $m = 0$, of (1.1) has for the past forty years been the object of rather extensive research and has its origins in the papers of Rankin and Selberg. In [R] and [S1] it is shown that the L-function

$$L_{f,g}(s) = \sum_{n=1}^{\infty} a_n \overline{b_n}\, n^{-s}$$

has a meromorphic continuation to the entire complex s-plane and satisfies the functional equation

$$R_{f,g}(s) = R_{f,g}(2k-1-s)$$

where

$$R_{f,g}(s) = (2\pi)^{-2s}\Gamma(s)\Gamma(s-k+1)\zeta(2s-2k+2)L_{f,g}(s).$$

Moreover, $L_{f,g}(s)$ is regular except for poles corresponding to the complex zeros of $\zeta(2s-2k+2)$ and a simple pole at $s = k$ with residue

$$\alpha = 12 \frac{(4\pi)^{k-1}}{\Gamma(k)} \langle f,g \rangle$$

where

$$\langle f,g \rangle = \iint_D f(z)\overline{g(z)}\, y^k \frac{dxdy}{y^2}$$

is the usual Petersson inner product (over a fundamental domain D for Γ) for forms of weight k.

The functional equation (1.2) was obtained by analyzing the inner product $\langle f, g\overline{E(*,s)} \rangle$ where

$$E(z,s) = \sum_{\sigma \in \Gamma_\infty \backslash \Gamma} (\operatorname{Im} \sigma z)^s, \qquad \Gamma_\infty = \{\sigma \in \Gamma;\ \sigma\infty = \infty\}$$

is the non-holomorphic Eisenstein series which satisfies the properties

(1.3) $\quad E(\sigma z,s) = E(z,s), \qquad$ for all $\sigma \in \Gamma$

(1.4) $\quad \Delta E(z,s) = s(1-s)E(z,s), \qquad \Delta = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$

(1.5) $\quad \pi^{-s}\Gamma(s)\zeta(2s)E(z,s) = \pi^{-(1-s)}\Gamma(1-s)\zeta(2-2s)E(z,1-s).$

It is of course (1.5) which gives the functional equation (1.2).

In [S2], Selberg returned to the general problem (1.1) and very briefly indicated how to obtain the meromorphic continuation of the function

$$\sum_{n=1}^{\infty} a_n \overline{b_{n+m}}\, n^{-s}.$$

Unfortunately, this function does not satisfy a functional equation and a suitable generalization of (1.2) to the case $m \neq 0$ requires the use of the non-holomorphic Poincaré series

$$P_m(z,s) = \sum_{\sigma \in \Gamma_\infty \backslash \Gamma} (\operatorname{Im} \sigma z)^{\frac{1}{2}} I_{s-\frac{1}{2}}(2\pi|m|\operatorname{Im} \sigma z) e^{2\pi i m \operatorname{Re} \sigma z}$$

where

$$I_\nu(y) = \sum_{j=0}^{\infty} (\tfrac{1}{2}y)^{2j+r}/j!\,\Gamma(j+\nu+1)$$

is the modified Bessel function of the first kind which grows exponentially

$$(1.6)\qquad \lim_{y\to\infty} \sqrt{y}\, I_\nu(y) e^{-y} = (2\pi)^{-\frac{1}{2}}.$$

As shown in [NI] and [NE], the Poincaré series $P_m(z,s)$ is similar in behavior to the Eisenstein series $E(z,s)$, and in fact satisfied

$$(1.7)\qquad P_m(\sigma z,s) = P_m(z,s), \qquad \text{for all } \sigma \in \Gamma$$

$$(1.8)\qquad \Delta P_m(z,s) = s(1-s)P_m(z,s)$$

$$(1.9)\qquad P_m(z,s) - P_m(z,1-s) = \frac{2\pi^s |m|^{s-\frac{1}{2}} \sigma_{1-2s}(m)}{(2s-1)\Gamma(s)\zeta(2s)} E(z,1-s)$$

where

$$\sigma_w(m) = \sum_{\substack{d|m \\ d>0}} d^w.$$

On the basis of these properties, one obtains the following generalization of the Rankin-Selberg method. Let

$$Z_m(s) = |\pi m|^{\frac{1}{2}-k} \frac{2^{-s}\Gamma(s)}{\Gamma(s-\frac{3}{2}-k)} \sum_{n=1}^{\infty} a_n \overline{b_{n+m}} \left(\frac{n}{2n+m}\right)^s F\left(\frac{s}{2}, \frac{s+1}{2}, s+\frac{3}{2}-k, \frac{m^2}{(2n+m)^2}\right)$$

where $b_u \equiv 0$ for $u \leq 0$, and

$$F(\alpha,\beta,\eta;w) = \sum_{m=0}^{\infty} \frac{1}{m!} \frac{\Gamma(\alpha+m)\Gamma(\beta+m)\Gamma(\eta)}{\Gamma(\alpha)\Gamma(\beta)\Gamma(\eta+m)} w^m$$

is the Gauss hypergeometric function which in the special case of (1.10) is just a Legendre function since $\beta-\alpha = \frac{1}{2}$. From the expansion

$$F\left(\frac{s}{2}, \frac{s+1}{2}, s+\frac{3}{2}-k; \frac{m^2}{(2n+m)^2}\right) = 1 + \frac{s(s+1)}{4s+6-4k} \frac{m^2}{(2n+m)^2} + \dots$$

it is easily seen that $Z_m(s)$ converges absolutely for $\mathrm{Re}(s) > k$. We show that the function $Z_m(s)$ can be continued to a meromorphic function in the entire s-plane which is regular in $\mathrm{Re}(s) \geq k-\frac{1}{2}$ except for simple poles at the points $s = k - \frac{1}{2} + ir_j$ where $\frac{1}{4} + r_j^2$ is an eigenvalue of the Laplace operator for $L^2(\Gamma\backslash H)$. The eigenvalues are discrete and are characterized by the existence of an orthonormal basis of Maass wave forms $\{e_j(z)\}$ satisfying

$$(1.10)\qquad e_j(z) = \sum_{n\neq 0} c_j(n) \sqrt{y} K_{ir_j}(2\pi|n|y) e^{2\pi i n x},$$

$$\Delta e_j(z) = (\tfrac{1}{4} + r_j^2) e_j(z), \tag{1.11}$$

$$e_j(\sigma z) = e_j(z), \qquad \text{for all } \sigma \in \Gamma, \tag{1.12}$$

where

$$K_v(y) = \int_0^\infty e^{-\frac{1}{2}y(u+u^{-1})} u^{v-1}\, du$$

is the modified Bessel function of the second kind.

THEOREM (1). The function $Z_m(s)$ can be continued to a meromorphic function of order two which is regular in $\mathrm{Re}(s) \geqslant k-\frac{1}{2}$ except for simple poles at the points $s = k - \frac{1}{2} + ir$; with corresponding residues

$$\alpha_j = \frac{c_j(m)}{2ir_j} \langle f, g\overline{e_j} \rangle.$$

Also, $s = k$ is not a pole, and $Z_m(s)$ satisfies the functional equation

$$Z_m(s) - Z_m(2k-1-s) = \frac{2^{k+\frac{1}{2}}\pi^{2k-\frac{3}{2}}}{(2s+1-2k)} G_m(s) R_{f,g}(s)$$

where

$$G_m(s) = \frac{|m|^{k-\frac{1}{2}-s}\sigma_{2s-2k+1}(m)}{\Gamma(k-s)\Gamma(1-k+s)\zeta(2k-2s)\zeta(2-2k+2s)}$$

is invariant for $s \longrightarrow 2k-1-s$.

The proof of Theorem (1) is slightly complicated by the fact that the inner product $\langle f, g\overline{P_m} \rangle$ does not converge absolutely for large m. If we look at the Fourier expansion (see [NI]) of the non-holomorphic Poincaré series

$$P_m(z,s) = \sqrt{y}\, I_{s-\frac{1}{2}}(2\pi|m|y) e^{2\pi imx} + \frac{2\pi^s |m|^{s-\frac{1}{2}} \sigma_{1-2s}(m)}{(2s-1)\Gamma(s)\zeta(2s)} y^{1-s} + \sum_{\substack{\ell=-\infty \\ \ell \neq 0}}^{\infty} B_\ell(s;m) \sqrt{y}\, K_{s-\frac{1}{2}}(2\pi|\ell|y) e^{2\pi i \ell x} \tag{1.13}$$

where

$$B_\ell(s;m) = 2\sum_{c=1}^{\infty} S(\ell,m;c)c^{-1}M_{2s-1}(4\pi c^{-1}(m\ell)^{\frac{1}{2}})$$

$$S(\ell,m;c) = \sum_{\substack{d=1\\(d,c)=1}}^{c} e^{2\pi i\,\frac{a\ell+dm}{c}}, \qquad ad \equiv 1 \pmod{c}$$

is the Kloosterman sum, and

$$M_\nu(y(m\ell)^{\frac{1}{2}}) = \begin{cases} J_\nu(y|m\ell|^{\frac{1}{2}}) & m\ell > 0 \\ I_\nu(y|m\ell|^{\frac{1}{2}}) & m\ell < 0 \end{cases}$$

it easily follows from (1.6) that

$$|P_m(z,s)| \ll e^{2\pi|m|y} \qquad (y \longrightarrow \infty).$$

Consequently

$$|f(z)g(z)P_m(z,s)| \ll e^{2\pi(|m|-2)y} \qquad (y \longrightarrow \infty)$$

if $a_1b_1 \neq 0$; and, therefore, the inner product $\langle f,g\overline{P_m}\rangle$ does not make sense for $|m| > 1$.

In order to get around this difficulty, define for every $Y > 1$

$$D_Y = \{z \in H;\ |z| \geqslant 1,\ \mathrm{Im}(z) \leqslant Y,\ 0 \leqslant \mathrm{Re}(z) \leqslant 1\}$$

$$A = \{z \in H;\ |z| < 1,\ 0 \leqslant \mathrm{Re}(z) \leqslant 1\}$$

$$P_m^*(z,s) = \sum_{\sigma\in\Gamma_\infty\backslash\Gamma}{}' (\mathrm{Im}\,\sigma z)^{\frac{1}{2}}I_{s-\frac{1}{2}}(2\pi|m|\mathrm{Im}(\sigma z))e^{2\pi i m\,\mathrm{Re}(\sigma z)}$$

where the prime on the summation symbol means to omit the identity matrix from the sum. Since

$$A = \bigcup_{\sigma\in\Gamma_\infty\backslash\Gamma}{}' \sigma D$$

it is immediate that

$$I_A(s) = \iint_A f(z)\overline{g(z)}\,y^{k+\frac{1}{2}}I_{s-\frac{1}{2}}(2\pi|m|y)e^{2\pi imx}\,\frac{dxdy}{y^2}$$

$$= \iint_D f(z)\overline{g(z)}\,y^k P_m^*(z,s)\,\frac{dxdy}{y^2}. \tag{1.14}$$

But, for $1 < Y_1 < Y$

$$\iint_A = \int_0^Y \int_0^1 - \int_{Y_1}^Y \int_0^1 = \iint_{D_Y} .$$

Hence

$$(1.15)\quad I_A(s) = \sum_{n=1}^{\infty} a_n \overline{b_{n+m}} \left(\int_0^Y - \int_{Y_1}^Y \right) e^{-2\pi(2n+m)y} I_{s-\frac{1}{2}}(2\pi|m|y) y^{k-\frac{1}{2}} \frac{dy}{y}$$

$$- I_{D_{Y_1}}(s).$$

Using the transform

$$\int_0 e^{-\gamma y} I_{s-\frac{1}{2}}(ay) y^{\rho} \frac{dy}{y} = \left(\frac{a}{2\gamma}\right)^{s-\frac{1}{2}} \gamma^{-\rho} \frac{\Gamma(2-\frac{1}{2}+\rho)}{\Gamma(s+\frac{1}{2})} F\left(\frac{s-\frac{1}{2}+\rho}{2}, \frac{s+\frac{1}{2}+\rho}{2}, s+\tfrac{1}{2}; \left(\frac{a}{\gamma}\right)^2\right),$$

and letting $Y \longrightarrow \infty$ in (1.15), it follows from (1.14) that

$$(1.16)\quad Z_m(s+k-1) = \sum_{n=1}^{\infty} a_n \overline{b_{n+m}} \int_0^{\infty} e^{-2\pi(2n+m)y} I_{s-\frac{1}{2}}(2\pi|m|y) y^{k-\frac{1}{2}} \frac{dy}{y}$$

$$= \iint_D f(z)\overline{g(z)}\, y^k P_m^*(z,s) \frac{dxdy}{y^2} + I_{D_Y}(s)$$

$$+ \sum_{n=1}^{\infty} a_n \overline{b_{n+m}} \int_Y^{\infty} e^{-2\pi(2n+m)y} I_{s-\frac{1}{2}}(2\pi|m|y) y^{k-\frac{1}{2}} \frac{dy}{y}$$

and this holds for any fixed $Y > 1$. Since the second and third terms on the right side of (1.16) are entire functions and $|P_m^*(z,s)| \ll y^{1-\mathrm{Re}(s)}$ as $y \longrightarrow \infty$, it immediately follows that the right side of (1.16) defines an analytic function and gives the analytic continuation of $Z_m(s)$ to the entire complex s-plane.

To determine the poles of $Z_m(s)$, note that if we define

$$\tilde{P}_m(z,s) = \frac{(\pi|m|)^{s-\frac{1}{2}}}{\Gamma(s+\frac{1}{2})} \sum_{\sigma \in \Gamma_\infty \backslash \Gamma} (\mathrm{Im}\ \sigma z)^s e^{2\pi i m \sigma z}$$

then

$$P_m^*(z,s) - \tilde{P}_m(z,s)$$

is regular for $\mathrm{Re}(s) > 0$. The analytic continuation of $\tilde{P}_m(z,s)$ was given by Selberg in [S2] by expanding it in terms of an orthonormal basis of eigenfunctions $\{e_j\}$ satisfying (1.10) - (1.12). The

spectral decomposition of $\widetilde{P}_m(z,s)$ is

$$\widetilde{P}_m(z,s) = \sum_{j=1}^{\infty} \langle \widetilde{P}_m, e_j \rangle e_j(z) + \frac{1}{4\pi i} \int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty} \langle \widetilde{P}_m, E(*,w) \rangle E(z,w)\, dw.$$

One easily computes that

$$\langle \widetilde{P}_m, e_j \rangle = \frac{c_j(m)\Gamma(s-\frac{1}{2}-ir_j)\Gamma(s-\frac{1}{2}+ir_j)}{\Gamma(2s)}$$

$$\langle \widetilde{P}_m, E(*,w) \rangle = \frac{\sigma_{2w-1}(m)\,\Gamma(\frac{s-1-w}{2})\,\Gamma(\frac{s-2+w}{2})}{\pi^{-w}|m|^{w-\frac{3}{2}}\,\Gamma(s-\frac{1}{2})\,\Gamma(w)\,\zeta(2w)}$$

It follows that the only poles of $\widetilde{P}(z,s)$ in $\mathrm{Re}(s) \geqslant \frac{1}{2}$ are at $s = \frac{1}{2} + ir_j$ with corresponding residues

$$\beta_j = \frac{c_j(m)e_j(z)}{2ir_j}.$$

There is no pole at $s = 1$ since the inner product of $\widetilde{P}_m$ with a constant function is identically zero. Putting this information back into (1.16) gives

$$Z_m(s+k-1) = \sum_{j=1}^{\infty} c_j(m)\, \frac{\Gamma(s-\frac{1}{2}-ir_j)\Gamma(s-\frac{1}{2}+ir_j)}{\Gamma(2s)} \langle f, g\overline{e_j} \rangle + H_m(s)$$

where $H_m(s)$ is regular for $\mathrm{Re}(s) \geqslant \frac{1}{2}$.

The functional equation for $Z_m(s)$ can be easily deduced from (1.9) and the identity

$$I_{s-\frac{1}{2}}(2\pi|m|y) - I_{\frac{1}{2}-s}(2\pi|m|y) = \frac{2\sin(\frac{1}{2}-s)\pi}{\pi} K_{s-\frac{1}{2}}(2\pi|m|y).$$

One then obtains from (1.16) that

$$Z_m(s+k-1) - Z_m(k-s) = Q_m(s) \iint_D f(z)\overline{g(z)}\, y^k E(z,1-s)\, \frac{dxdy}{y^2} \tag{1.17}$$

where

$$Q_m(s) = \frac{2\pi^s |m|^{s-\frac{1}{2}} \sigma_{1-2s}(m)}{(2s-1)\Gamma(s)\zeta(2s)}.$$

The Rankin-Selberg method gives

$$\iint_D f(z)\overline{g(z)}\, y^k E(z,1-s)\, \frac{dxdy}{y^2} = \int_0^{\infty}\int_0^1 f(z)\overline{g(z)}\, y^{k-s}\, \frac{dxdy}{y} \tag{1.18}$$

$$= (4\pi)^{s-k}\Gamma(k-s)L_{f,g}(k-s).$$

On combining (1.17) and (1.18) one immediately obtains the functional equation for $Z_m(s)$.

§2. The arithmetic properties of the classical holomorphic Poincaré series of weight k

$$P_m(z) = \sum_{\sigma \in \Gamma_\infty \backslash \Gamma} \frac{e^{2\pi i m z}}{(cz+d)^k}, \qquad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with Fourier expansion

$$(2.1)\quad P_m(z) = \sum_{n=1}^{\infty} \{\delta_{mn} + 2\pi \left(\frac{n}{m}\right)^{\frac{k-1}{2}} i^k \sum_{c=1}^{\infty} s(m,n;c) c^{-1} J_{k-1}\left(\frac{4\pi}{c}\sqrt{mn}\right)\} e^{2\pi i n z}$$

lead to some interesting identities similar in spirit to the functional equation in Theorem (1). Since $P_m(z)$ must be a cusp form, it can be expanded in terms of a basis $f_1, f_2 \ldots f_n$

$$f_j(z) = \sum_{n=1}^{\infty} a_j(n) e^{2\pi i n z}$$

of the space of holomorphic cusp forms of weight k for Γ. Consequently

$$(2.2)\qquad P_m(z) = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}} \sum_{j=1}^{h} \frac{a_j(m)}{\langle f_j, f_j \rangle} f_j(z).$$

Equating Fourier coefficients of (2.1) and (2.2)

$$(2.3)\qquad \frac{\Gamma(k-1)}{(4\pi m)^{k-1}} \sum_{j=1}^{h} \frac{a_j(m)}{\langle f_j, f_j \rangle} a_j(n) = \delta_{mn} + 2\pi (i)^k \left(\frac{n}{m}\right)^{\frac{k-1}{2}} \sum_{c=1}^{\infty} \frac{s(m,n;c)}{c} J_{k-1}\left(\frac{4\pi}{c}\sqrt{mn}\right).$$

Now, using Barnes' representation for the Bessel function

$$J_{k-1}(x) = \frac{1}{4\pi i} \int_{\alpha-i}^{\alpha+i\infty} \frac{\Gamma\left(\frac{k-1+s}{2}\right)}{\Gamma\left(\frac{k+1-s}{2}\right)} \left(\frac{x}{2}\right)^{-s} ds, \qquad (1-k < \alpha < 0)$$

and multiplying both sides of (2.3) by $a_\ell(m) m^{-w}$, and then summing over all positive integers m, it follows that

$$(2.4)\qquad \frac{\Gamma(k-1)}{(4\pi)^{k-1}} \sum_{j=1}^{h} \frac{L_{f_j,f_\ell}(w+k-1)}{\langle f_j,f_j\rangle} a_j(n) - \frac{a_\ell(n)}{n^w} =$$

$$= \frac{(i)^k n^{\frac{k-1}{2}}}{4\pi i} \int_{\alpha-i\infty}^{\alpha+i\infty} \frac{\Gamma(\frac{k-1+s}{2}) n^{-s/2}}{(2\pi)^{s-1}\,(\frac{k+1-s}{2})}$$

$$\sum_{c=1}^{\infty} c^{s-1} \sum_{\substack{d=1\\(d,c)=1}}^{c} e^{\frac{2\pi i d n}{c}} L_\ell(\tfrac{s+k-1}{2}+w;\tfrac{a}{c})\, ds$$

where

$$L_\ell(s;\tfrac{a}{c}) = \sum_{m=1}^{\infty} \frac{a_\ell(m) e^{\frac{2\pi i a m}{c}}}{m^s}, \qquad ad \equiv 1 \pmod{c}.$$

The disadvantage of (2.3) is the appearance of Kloosterman sums on the right hand side. If in (2.4) we apply the functional equation

$$(2.5)\qquad (\tfrac{c}{2\pi})^s \Gamma(s) L_\ell(s;\tfrac{a}{c}) = (i)^k (\tfrac{c}{2\pi})^{k-s} \Gamma(k-s) L_\ell(k-s,\tfrac{-d}{c})$$

then it is easily seen that the Kloosterman sums are transformed into Ramanujan sums which can be evaluated exactly. Ramanujan's identity

$$\sum_{c=1}^{\infty} c^{-2w} \sum_{\substack{d=1\\(d,c)=1}}^{c} e^{\frac{2\pi i d(m-n)}{c}} = \frac{\sigma_{1-2w}(m-n)}{\zeta(2w)}$$

can then be applied to give

$$(2.6)\qquad \sum_{c=1}^{\infty} c^{-2w} \sum_{\substack{d=1\\(d,c)=1}}^{c} e^{\frac{2\pi i d n}{c}} L_\ell(s;\tfrac{-d}{n}) = \frac{1}{\zeta(2w)} \sum_{m=1}^{\infty} \frac{a_\ell(m)\sigma_{1-2w}(m-n)}{m^s}$$

which is valid for $\mathrm{Re}(w) > 1$ and $\mathrm{Re}(s) > \frac{k+1}{2}$.

On combining (2.4), (2.5), and (2.6) we get

$$(2.7)\qquad \frac{\Gamma(k-1)}{(4\pi)^{k-1}} \sum_{j=1}^{h} \frac{L_{f_j,f_\ell}(w+k-1)}{\langle f_j,f_j\rangle} a_j(n)$$

$$= \frac{a_\ell(n)}{n^w} + \frac{(2\pi)^{2w} n^{\frac{k-1}{2}}}{\zeta(2w)} \sum_{m=1}^{\infty} \frac{a_\ell(m)\sigma_{1-2w}(m-n)}{m^{\frac{k+1}{2}-w}} I_w(\tfrac{m}{n})$$

where

$$(2.8)\qquad I_w(x) = \frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty} \frac{\Gamma(\frac{k+1}{2}-w-s)\Gamma(\frac{k-1}{2}+s)}{\Gamma(w+\frac{k-1}{2}+s)\Gamma(\frac{k+1}{2}-s)}\, x^s\, ds.$$

Since $k \geq 12$, the right side of (2.7) converges absolutely for $1 < \mathrm{Re}(w) \leq 2$ and $\alpha < -\mathrm{Re}(w)$, say.

The integral in (2.8) can be computed as follows. If $x < 1$

$$(2.9)\qquad I_w(x) = \sum_{m=0}^{\infty} \frac{(-1)^m}{m!}\frac{\Gamma(k-w+m)}{\Gamma(k+m)\Gamma(w-m)}\, x^{\frac{k+1}{2}-w+m}$$

$$= \frac{\Gamma(k-w)}{\Gamma(k)\Gamma(w)}\, x^{\frac{k+1}{2}-w} F(k-w,1-w,k;x)$$

since $\Gamma(z)$ has poles at $z = -m$ with residue $\frac{(-1)^m}{m!}$. Similarly, for $x > 1$

$$(2.10)\qquad I_w(x) = \frac{\Gamma(k-w)}{\Gamma(k)\Gamma(w)}\, x^{-\frac{k-1}{2}} F(k-w,1-w,k;x^{-1}).$$

Moreover, by continuity, these results are also valid when $x = 1$; and, in fact, using Gauss' formula

$$F(\alpha,\beta,\gamma;1) = \frac{\Gamma(\gamma)\Gamma(\gamma-\alpha-\beta)}{\Gamma(\gamma-\alpha)\Gamma(\gamma-\beta)}$$

we have

$$(2.11)\qquad I_w(1) = \frac{\Gamma(k-w)\Gamma(2w-1)}{\Gamma(2)^2\Gamma(k-1+w)}.$$

It, therefore, follows from (2.7), (2.9), (2.10), (2.11) and the functional equation for the Riemann zeta function that

$$\left(\frac{\pi}{n}\right)^{k-1}\Gamma(k-1)\sum_{j=1}^{h}\frac{R_{f_j,f_\ell}(w+k-1)}{\langle f_j,f_j\rangle}a_j(n) = \Gamma(w+k-1)\zeta(1-2w)\frac{\Gamma(1-2w)}{\Gamma(1-w)}\frac{a_\ell(n)}{n^{w+k-1}}$$

$$+ \Gamma(k-w)\zeta(2w-1)\frac{\Gamma(2w-1)}{\Gamma(w)}\frac{a_\ell(n)}{n^{k-w}}$$

$$+ \frac{\Gamma(w+k-1)\Gamma(k-w)}{\Gamma(k)}\sum_{m<n}\frac{a_\ell(m)\sigma_{1-2w}(m-n)}{n^{k-w}}F(k-w,1-w,k;\tfrac{m}{n})$$

$$+ \frac{\Gamma(w+k-1)\Gamma(k-w)}{\Gamma(k)}\sum_{m>n}\frac{a_\ell(m)\sigma_{1-2w}(m-n)}{m^{k-w}}F(k-w,1-w,k;\tfrac{n}{m}).$$

THEOREM (2). Let $g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi inz}$ be a cusp form of weight k for Γ. Define

$$B_m(s) = \frac{\Gamma(s)\Gamma(2k-1-2s)}{\Gamma(k-1)\Gamma(k-s)}\,\zeta(2k-1-2s)\,\frac{b_m}{m^s}$$

$$Y_m(s) = \sum_{n<m} \frac{b_n\sigma_{2s+1-2k}(m-n)}{m^s}\,F(s,s+1-k,k;\tfrac{n}{m}) + \sum_{n>m} \frac{b_n\sigma_{2s+1-2k}(n-m)}{n^s}\,F(s,s+1-k,k;\tfrac{m}{n})$$

Then

$$(\tfrac{\pi}{m})^{k-1} \sum_{j=1}^{h} \frac{R_{f_j,g}(s)a_j(n)}{\langle f_j,f_j\rangle} = B_m(s) + B_m(2k-1-s) + \frac{\Gamma(s)\Gamma(2k-1-s)}{\Gamma(k)\Gamma(k-1)}\,Y_m(s).$$

The functional equation for $R_{f_j,g}(s)$ immediately implies

$$Y_m(s) = Y_m(2k-1-s),$$

but this could just as easily have been obtained from the Gauss transformation

$$F(\alpha,\beta,\gamma;z) = (1-z)^{\gamma-\alpha-\beta}F(\gamma-\alpha,\gamma-\beta,\gamma;z). \tag{2.12}$$

Curiously, (2.12) can also be used to give a novel proof of (1.2), the functional equation of the Rankin-Selberg zeta function.

As an example of a special case of Theorem (2), we put $k = 12$, $s = 10$ and

$$g(z) = \sum_{n=1}^{\infty} \tau(n)e^{2\pi inz}$$

to be the Ramanujan cusp form of weight twelve. It follows that

$$\frac{10!L_{g,g}(13)}{(4\pi)^{11}\langle g,g\rangle}\,\tau(m) = (\frac{24\zeta(3)}{11}\,m + \frac{1}{m^2})\,\tau(m) + \frac{24m}{11}\sum_{n<m}\tau(n)\sigma_{-3}(m-n)(5-6\tfrac{n}{m}) + \frac{24m}{11}\sum_{n>m}\tau(n)\sigma_{-3}(n-m)(\tfrac{m}{n})^{10}(5-6\tfrac{n}{m}).$$

§3. Using the methods of §1 it is possible to derive explicit formulae relating partial sums of the type (1.1) with sums going over the eigenvalues of the Laplacian. For example, we can obtain

THEOREM (3). Let $x \longrightarrow \infty$ and $\varepsilon > 0$ be fixed. Then

$$\sum_{n=1}^{\infty} a_n \overline{b_{n+m}}\, e^{-\frac{n}{x}} \ll x^{k-\frac{1}{2}+\varepsilon}$$

where the $\ll$-symbol depends only on ε and m.

The proof of Theorem (3) uses the fact that there are no eigenvalues in $(0,\frac{1}{4}]$ for the group Γ. This, however, may not be the case for arbitrary groups; although it is conjectured that there are no eigenvalues in $(0,\frac{1}{4})$ for any congruence subgroup of $SL_2(\mathbf{Z})$.

Let Γ' be any fixed congruence subgroup of $SL_2(\mathbf{Z})$, and let

$$\lambda_j' = \frac{1}{4} + r_j'^2 \qquad (\lambda_0' = 0 < \lambda_1' \leqslant \lambda_2' \leqslant \ldots)$$

be the eigenvalues of the Laplacian in $L^2(\Gamma' \backslash H)$. Put

$$a = \max_j |\mathrm{Re}\ ir_j|.$$

THEOREM (4). Let $x \longrightarrow \infty$ and $\varepsilon > 0$ be fixed. If a_n, b_n are the n^{th} Fourier coefficients, respectively, of two cusp forms of weight k for Γ', then

$$\sum_{n=1}^{\infty} a_n \overline{b_{n+m}}\, e^{-\frac{n}{x}} \ll \begin{cases} x^{k-\frac{1}{2}+a} & a > 0 \\ x^{k-\frac{1}{2}+\varepsilon} & \text{otherwise.} \end{cases}$$

The $\ll$-symbol depends only on ε, m and Γ'.

In the case that $a > 0$, it is possible in many cases to replace the upper bound in Theorem (4) by an asymptotic relation. We also remark that all of our Theorems remain valid if the $\{b_n\}$ are taken to be Fourier coefficients of Eisenstein series.

§4. BIBLIOGRAPHY

[Ne] H. Neunhöffer, Über die analytische Fortsetzung von Poincaréreihen, Sitz. Heidelberger Akad. Wiss., 2. Abhandlung (1973), pp. 33-90.

[Ni] D. Niebur, A class of nonanalytic automorphic functions, Nagoya Math J., Vol. 52 (1973), pp. 133-145.

[R] R. A. Rankin, Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetic functions, Proc. Cambridge Philos. Soc. 35 (1939), pp. 357-372.

[S1] A. Selberg, Bemerkungen über eine Dirichletsche Reihe, die mit der Theorie der Modulformen nahe Verbunden ist, Arch. Math. Naturrid, 43 (1940), pp. 47-50.

[S2] _____, On the estimation of Fourier coefficients of modular forms, Proc. Symp. Pure Math, AMS, Vol. VIII, Theory of Numbers (1965), pp. 1-15.

Dorian GOLDFELD
M.I.T.
Department of Mathematics
Box 2155
CAMBRIDGE
Mass. 02139 U.S.A.

Astérisque

GILLES LACHAUD

Le prolongement analytique d'un type de fonctions zeta généralisées

Astérisque, tome 61 (1979), p. 109-119

<http://www.numdam.org/item?id=AST_1979__61__109_0>

Société Mathématique de France
Astérisque 61 (1979) p. 109-119

LE PROLONGEMENT ANALYTIQUE D'UN TYPE DE FONCTIONS ZETA GÉNÉRALISÉES

par

Gilles LACHAUD

1. C.L. Siegel a démontré en 1925 le résultat suivant (cf. [M2]) : si $F \in \underline{Z}[X,Y]$ est une forme binaire irréductible sur $\underline{Q}$ de degré $d \geq 3$, la série

$$Z_o(s,F) = \Sigma\ |F(x,y)|^{-s}$$

où la sommation porte sur les $(x,y) \in \underline{Z}^2$ tels que $(x,y) \neq (0,0)$, converge pour $\mathrm{Re}\ s > 2/d$, et se prolonge en une fonction méromorphe dans le demi-plan $\mathrm{Res} > 1/(d-1)$, avec un seul pôle au point $s = 2/d$ de résidu

$$V_o = \frac{2}{d} \int |F(1,x)|^{-2/d}\ dx.$$

Ce résultat a été repris et généralisé en 1934 par K. Mahler (cf. encore [M2]). Soit M un ensemble fini de nombres premiers, posons

$$Q(x,y) = \prod_{p \in M} |F(x,y)|_p^{-1}$$

en notant $|x|_p$ la valeur absolue p-adique d'un $x \in \underline{Q}$, et soit $\underline{Z}^2(M)$ l'ensemble des vecteurs $(x,y) \in \underline{Z}^2$ tels que $(x,y,p) = 1$ pour tout $p \in M$. Alors la série

$$Z_M(s,F) = \Sigma\ \{Q(x,y)/|F(x,y)|\}^{-s}$$

où l'on somme sur les $(x,y) \in \underline{Z}^2(M)$, a les mêmes propriétés que la série $Z_o(s,F)$, mis à part que cette fois-ci le résidu au point $2/d$ est égal à

$$V_o \prod_{p \in M} V_p,$$

où on a posé, pour $p \in M$,

$$V_p = \int |F(x,y)|^{-2/d}\ dx\ dy$$

l'intégrale portant sur les $(x,y) \in \underline{Z}_p^2$ tels que $\max(|x|_p, |y|_p) = 1$.

Mahler dit sans préciser que si F est anisotrope sur $\underline{R}$ et sur $\underline{Q}_p$ pour tout $p \in M$, alors la série $Z_M(s,F)$ se prolonge analytiquement à tout le plan complexe, le seul pôle étant en $s = 2/d$, et que pour voir cela on peut utiliser "un vieux théorème de Mellin". Mais ce "vieux théorème de Mellin" avait déjà été repris par Mahler dans [M1], et ne permet pas de traiter le cas où il y a des places ultramétriques (Il fournit seulement le prolongement analytique de $Z_o(s,F)$).

Nous allons démontrer ici un résultat de ce type.

2. On va supposer que $F(X) = F(X_1,\ldots,X_n)$ est un polynôme à n variables et à coefficients entiers, qui est quasi-homogène, ce qui veut dire qu'il existe des entiers $k,k_1,\ldots,k_n$ tels que l'identité formelle

$$(QH) \quad F(T^{k_1}X_1,\ldots,T^{k_n}X_n) = T^k F(X)$$

soit satisfaite.

Dans cette hypothèse, il est naturel de supposer que le pgcd de $k_1,\ldots,k_n$ est égal à 1.

On peut faire la remarque suivante. Supposons que F soit anisotrope sur Q (rappelons qu'un polynôme $F \in K[X]$ est dit anisotrope sur le corps K si les relations $x \in K^n$ et $F(x) = 0$ impliquent $x = 0$). Alors si F vérifie la relation (QH), les nombres $k,k_1,\ldots,k_n$ sont déterminés de façon unique par F. En effet, si on remplace toutes les variables par 0 sauf une, disons X_i, le polynôme $F(0,\ldots,X_i,\ldots,0)$ est non nul ; si d_i est le degré de ce polynôme, la relation (QH) montre que c'est en fait un monôme et implique l'identité $d_i k_i = k$; on voit donc que k est le ppcm de $d_1,\ldots,d_n$, d'où l'assertion. Introduisons les notations suivantes. Si M est un ensemble fini de nombres premiers, on pose, pour $p \in M$ et pour $x \in \underline{Q}_p^n$,

$$\|x\|_p = \mathrm{Max}\,(|x_1|_p,\ldots,|x_n|_p) \ ;$$

et on note $\underline{Z}^n(M)$ l'ensemble des $x \in \underline{Z}^n$ tels que $\|x\|_p = 1$ pour tout $p \in M$, autrement dit tels que

$$(x_1,\ldots,x_n,p) = 1 \quad \text{si} \quad p \in M$$

Si $F \in \underline{Z}[X_1,\ldots,X_n]$ est un polynôme à n variables, on posera, pour $x \in \underline{Q}^n$,

$$F_M(x) = |F(x)|_o \prod_{p \in M} |F(x)|_p$$

On a alors le théorème suivant :

Théorème. Soit $F \in \underline{Z}[X_1,\ldots,X_n]$ vérifiant la relation (QH) et soit M un ensemble fini de nombres premiers. Supposons F anisotrope sur R et sur Q_p lorsque $p \in M$ Alors la série

$$(1) \qquad Z_M(s,F) = \sum_{x \in \underline{Z}^n(M)} F_M(X)^{-s}$$

converge pour $\mathrm{Res} > \kappa = (k_1+\ldots+k_n)/k$ et se prolonge en une fonction méromorphe dans le plan complexe, avec un unique pôle en $s = \kappa$, de résidu égal à

$$(2) \qquad V_M = V_o \prod_{p \in M} V_p \ ,$$

où

$$(3) \qquad V_o = \int e^{-F(x)}\, dx \ ,$$

et où

$$(4) \qquad V_p = \int_{\|x\|_p=1} |F(x)|_p^{-K} \, dx \, .$$

Remarques. 1) Ce résultat est connu lorsque F est homogène et lorsqu'il n'y a pas de places ultramétriques (c'est-à-dire lorsque $M = \phi$). En voici un bref historique sous ces hypothèses. Le cas des formes quadratiques est classique : ce sont des fonctions zêta d'Epstein. Lorsque F est homogène de degré supérieur à 2, ce résultat a été obtenu par Mellin puis généralisé par Mahler, (cf [M1]), en utilisant la formule sommatoire d'Euler-Maclaurin. Ensuite Bochner (cf. [B]), dont l'article a été développé par Randol (cf. [R]), a démontré ce résultat en appliquant la formule de Poisson à la fonction F^{-s} convenablement régularisée. Bochner voit la fonction $Z_o(s,F)$ comme la trace de la fonction Zêta de l'opérateur $F(\partial/\partial x)$ (qui est elliptique puisque F est anisotrope sur $\underline{R}$) sur l'espace compact $\underline{R}^n/\underline{Z}^n$ (Le cas étudié ici, lorsque $M = \phi$, est celui des opérateurs semi-elliptiques). Enfin, An (cf. [A]) a obtenu ce résultat en reprenant la méthode de Riemann : c'est celle que nous allons utiliser.

2) Supposons F homogène de degré d. Si F est anisotrope sur le corps $\underline{F}_p$ pour tout $p \in M$, autrement dit si $x \in \underline{Z}^n(M)$ implique $|F(x)|_p = 1$, alors la fonction $Z_M(s,F)$ s'exprime simplement en fonction de $Z_o(s,F)$; supposons pour simplifier que M soit réduit à un seul nombre premier p. On a alors

$$\begin{aligned} Z_o(s,F) &= \sum_{\underline{Z}^n} F(x)^{-s} = \sum_{k=0}^{\infty} \sum_{X \in \underline{Z}^n(p)} F(p^k x)^{-s} \\ &= (1 - p^{-ds})^{-1} \sum_{X \in \underline{Z}^n(p)} F(x)^{-s} \\ &= (1 - p^{-ds})^{-1} \, Z_p(s,F) \end{aligned}$$

Mais une forme homogène peut être anisotrope sur $\underline{Q}_p$ sans l'être sur $\underline{F}_p$; considérons, par exemple, la forme

$$F(x,y) = x^2 + a\, y^2,$$

avec $a = p^k u$ où $(u,p) = 1$ lorsque $p \neq 2$. Si k est impair, ou bien si k est pair et si $-u$ n'est pas un carré de $\underline{F}_p$, alors F est anisotrope sur $\underline{Q}_p$, mais $|F(0,1)|_p = p^{-k}$.

3) Voici un exemple d'application du théorème. Soit q un nombre entier, notons $\phi_q(X)$ le q-ième polynôme cyclotomique, de degré $\phi(q)$, et posons

$$\Phi_q(X,Y) = X^{\phi(q)} \, \phi_q(Y/X).$$

Puisque ϕ_q n'a aucune racine réelle, la forme Φ_q est anisotrope sur $\underline{R}$; et si $p \not\equiv 1$ (mod. q) elle est aussi anisotrope sur $\underline{Q}_p$. Posons

$$F(X,Y) = \Phi_q(cX^d, Y^{d'})$$

où c, d, d' sont des entiers naturels ; si $p \not\equiv 1$ (mod. q) pour tout $p \in M$, le couple (F,M) satisfait aux hypothèses du théorème.

4) A l'aide du théorème d'Ikehara (cf. [Lg], ch. XV), on déduit immédiatement du théorème le

Corollaire. Posons, pour $t > 0$,

$$N(t) = \#\{x \in \underline{Z}^n(M) \mid F_M(x) \leq t\}.$$

On a alors

$$N(t) \sim \kappa^{-1} V_M t^{\kappa}$$

lorsque t tend vers l'infini.

On peut préciser ce résultat : on renvoie à [L] pour plus de détails sur ce genre d'estimations.

2. Pour démontrer le théorème, on va introduire la série thêta :

$$(5) \qquad \theta_M(t,F) = \sum_{x \in \underline{Z}^n(M)} \exp(-tF_M(x)) \quad (t>0) ;$$

On passe de cette série à la fonction $Z_M(s,F)$ par une transformation de Mellin :

$$(6) \qquad Z_M(s,F) = \int_0^{\infty} t^{s-1} \theta_M(t,F)\, dt ,$$

tous problèmes de convergence mis à part.

Puisque par hypothèse le polynôme F est anisotrope sur $\underline{Q}_p$, il existe un nombre $c_p > 0$ tel que

$$(7) \qquad |F(x)|_p \geq c_p$$

lorsque $x \in \underline{Q}_p^n$ et $\|x\|_p = 1$. En notant c_M le produit des c_p, on a donc, lorsque $x \in \underline{Z}^n(M)$,

$$F_M(x) \geq c_M \, |F(x)|. \tag{8}$$

Posons par ailleurs, pour $x = (x_1,\ldots,x_n) \in \underline{R}^n$,

$$|x|_d = \Sigma \, |x_i|^{d_i}, \tag{9}$$

où $d_i = k/k_i$, les nombres k, $k_1,\ldots,k_n$ étant ceux qui figurent dans la relation (QH). L'ensemble des $x \in \underline{R}^n$ tels que $|x|_d = 1$ est compact. La fonction F ne change pas de signe sur $\underline{R}^n - \{0\}$ puisqu'elle est anisotrope sur $\underline{R}$. On supposera, quitte à changer F en -F, que $F(x) > 0$ si $x \neq 0$. Si on note c_o la borne inférieure de F sur le compact $|x|_d = 1$, qui est strictement positive puisque F est anisotrope sur $\underline{R}$, la relation (QH) implique

$$F(x) \geq c_o \, |x|_d \tag{10}$$

Il s'ensuit que l'on a, avec $c = c_o c_M$,

$$F_M(x) \geq c|x|_d \text{ si } x \in \underline{Z}^n(M). \tag{11}$$

Ceci montre que la série $\theta_M(t,F)$ converge pour $t > 0$, puisque la relation (11) implique

$$\theta_M(t,F) \leq \prod_{i=1}^{n} \sum_{\underline{Z}} \exp\left(-ct|x|^{d_i}\right) \tag{12}$$

En suivant la méthode habituelle, on va couper l'intégrale (6) en deux en posant

$$Z_M^+(s,F) = \int_1^\infty t^{s-1} \, \theta_M(t,F) \, dt \, ,$$

$$Z_M^-(s,F) = \int_0^1 t^{s-1} \, \theta_M(t,F) \, dt \, ;$$

la relation (12) montrant que

$$\theta_M(t,F) << t^{-N}$$

quel que soit $N > 0$ lorsque t tend vers l'infini, on en déduit que la fonction Z_M^+ est une fonction entière. Pour étudier la fonction Z_M^-, on va utiliser le résultat

suivant, en reprenant les notations du théorème :

Lemme 1. Lorsque t tend vers 0, on a, pour tout $N > 0$,

$$(13) \qquad \theta_M(t,F) = t^{-\kappa} V_M + O(t^N)$$

Il s'ensuit que l'intégrale Z_M^- converge pour $\mathrm{Res} > \kappa$ (doù la convergence de la série $Z_M(s,F)$ dans le même domaine) et se prolonge au plan complexe avec un pôle en $s = \kappa$ de résidu V_M ; Le théorème est donc complètement démontré une fois établi le lemme, ce qu'on va faire maintenant.

Pour cela, nous allons écrire la série $\theta(t,F)$ dans le formalisme adélique (cf. [Lg] et [W] .

Pour tout nombre premier p, on note ϕ_p (resp. ψ_p) la fonction caractéristique de l'ensemble $\|x\|_p \leq 1$ de $\underline{Q}_p^n$ (resp. de l'ensemble $\|x\|_p = 1$). Soit $\underline{A}$ l'anneau des adèles de $\underline{Q}$; pour $x = (x_p) \in \underline{A}^n$, on pose

$$\psi_M(x) = \prod_{p \in M} \psi_p(x_p) \prod_{p \notin M} \phi_p(x_p)$$

de telle sorte que

$$\underline{Z}^n(M) = \{x \in \underline{Q}^n \mid \psi_M(x) = 1\}$$

La fonction $F_M(x)$ s'étend naturellement à $\underline{A}^n$ si on pose

$$F_M(x) = |F(x_o)|_o \prod |F(x_p)|_p ,$$

et il vient

$$\theta_M(t,F) = \sum_{x \in Q^n} \psi_M(x)\, e^{-tF_M(x)}$$

Pour obtenir le comportement asymptotique de $\theta(t,F)$ lorsque t tend vers 0, on va appliquer la formule de Poisson à la fonction

$$E_t(x) = \psi_M(x) \exp(-tF_M(x)) \qquad (x \in \underline{A}^n)$$

pour cela vérifions que la fonction E_t satisfait aux conditions qui permettent de lui appliquer cette formule. Pour une fonction f définie sur $\underline{A}^n$, on a la relation

$$\sum_{x \in Q^n} f(x) = \sum_{\xi \in Q^n} \hat{f}(\xi)$$

dès que f satisfait les quatre hypothèses suivantes(cf. [Lg] ch. XIV § 6 , et [W] ch. VII § 2) :

a) f est intégrable ;

b) la série $\sum_{x \in \underline{Q}^n} f(x+y)$ converge uniformément si y est dans un compact de $\underline{A}^n$;

c) $\hat{f}$ est intégrable ;

d) la série $\sum_{\xi \in \underline{Q}^n} |\hat{f}(\xi)|$ converge.

Tout d'abord la fonction E_t est intégrable puisqu'elle est majorée, vu la relation (11), par la fonction décomposable

$$\psi_M(x_f) \cdot \exp(-c t |X_o|_d)$$

en notant x_f la projection d'un $x \in \underline{A}^n$ sur le produit des facteurs ultramétriques ; et cette dernière fonction, qui est dans l'espace des fonctions standard sur $\underline{A}^n$ (cf. [W], loc. cit., déf. 3) vérifie les conditions a) et b) ; il en va donc de même pour la fonction E_t.

Lemme 2. La fonction $\hat{E}_t(\xi)$ est nulle si ξ_f est hors d'un compact ; on a

$$\hat{E}_t(0) = V_M \, t^{-\kappa} \quad ; \tag{14}$$

et pour tout $N > 0$,

$$\hat{E}_t(\xi) \ll t^{N-\kappa} |\xi_o|_d^{-N} \, . \tag{15}$$

Admettons le lemme 2, et soit C la fonction caractéristique du compact hors duquel $\hat{E}_t$ est nulle. On a donc

$$\hat{E}_t(\xi) \ll C(\xi_f) \, |\xi_o|_d^{-N}$$

ce qui prouve que $\hat{E}_t$ est intégrable et que la condition c) d'application de la formule de Poisson est satisfaite.
Vérifions la condition d) : puisque $\hat{E}_t$ n'est non nulle que lorsque ξ_f est dans un compact, elle n'est non nulle pour $\xi \in \underline{Q}^n$ que lorsque ξ est dans un réseau Γ de $\underline{Q}^n$; si w est un entier tel que $\Gamma \subset w\underline{Z}^n$, on a donc, vu la relation (15), et en sommant sur $\xi \neq 0$,

$$(16)\qquad \sum_{\xi\in\underline{Q}^n} \widehat{E}_t(\xi) \ll t^{N-\kappa} \sum_{\xi\in\underline{Z}^n} |w\xi_o|_d^{-N},$$

on peut donc appliquer la formule de Poisson à E_t ; il vient

$$\theta_M(t,F) = \sum_{x\in Q^n} E_t(x) = \sum_{\xi\in Q^n} \widehat{E}_t(\xi) = \widehat{E}_t(0) + \sum_{\xi\neq 0} \widehat{E}_t(\xi)$$
$$= V_M\, t^{-\kappa} + R(t),$$

où R(t) est l'expression de gauche de la formule (16) ; d'où la relation (13) du lemme 1.

Il ne reste donc plus qu'à démontrer le lemme 2. Remarquons tout d'abord que la Formule de Taylor, le fait que F soit anisotrope sur $\underline{Q}_p$, et l'inégalité ultramétrique impliquent qu'il y a un nombre $\varepsilon_p > 0$ tel que, lorsque $x,y \in \underline{Q}_p^n$, on ait

$$|F(x+y)|_p = |F(x)|_p$$

dès que $\|x\|_p = 1$ et $\|y\|_p \leq \varepsilon_p$. Il s'ensuit que la fonction E_t est constante sur les classes x+K, où K est le sous-groupe ouvert compact de $\underline{A}_p^n$ des points $x = (x_p)$ vérifiant $\|x_p\|_p \leq 1$ si $p \notin M$ et $\|x_p\|_p \leq \varepsilon_p$ si $p \in M$. Si $\widehat{K}$ est le sous-espace dual de K, il s'ensuit (cf. la démonstration de la prop. 2 du § 2, ch. VII de [W]), que la fonction $\widehat{E}_t(\xi)$ est nulle si $\xi_f \notin \widehat{K}$, ce qui établit la première assertion du lemme 2. Si les nombres $k,k_1,\ldots,k_n$ sont ceux pour lesquels on a la relation

$$(QH)\qquad F(t^{k_1}x_1,\ldots,t^{k_n}x_n) = t^k F(x),$$

posons $d_i = k/k_i$ et soit D(t) l'application linéaire de $\underline{R}^n$:

$$D(t) : (x_1,\ldots,x_n) \longrightarrow (t^{-1/d_1}x_1,\ldots,t^{-1/d_n}x_n) ;$$

La relation (QH) se réécrit

$$(17)\qquad t\,F(D(t)x) = F(x),$$

et on a, pour toute fonction $f \in \mathcal{S}(\underline{R}^n)$,

$$(18)\qquad \int_{\underline{R}^n} f(x)\,dx = t^{-\kappa} \int_{\underline{R}^n} f(D(t)y)\,dy$$

avec $\kappa = (k_1+\ldots+k_n)/k$, comme on l'a défini dans le théorème

Posons, pour $\xi \in \underline{R}^n$ et $T > 0$,

$$\hat{E}_o(T,\xi) = \int_{\underline{R}^n} \exp - (2i\pi\langle x,\xi\rangle + TF(x))\, dx$$

en notant $\langle,\rangle$ le produit scalaire dans l'espace à n dimensions. Les relations (17) et (18) impliquent que l'on a

$$\hat{E}_o(T,\xi) = T^{-\kappa}\, \hat{E}_o(1,D(T)\xi)\ . \tag{19}$$

Si $\xi = 0$, on a

$$\hat{E}_o(T,0) = T^{-\kappa} \int_{\underline{R}^n} \exp\,(-F(x))\, dx\ ; \tag{20}$$

Si $\xi \neq 0$, la fonction $\exp\,(-F(x))$ est dans $\mathcal{S}(\underline{R}^n)$; on a donc, avec la notation (9),

$$\hat{E}_o(1,\xi) \ll |\xi|_d^{-N} \tag{21}$$

pour tout $N > 0$, et puisque

$$|D(T)\xi|_d = T^{-1}\, |\xi|_d\ ,$$

il vient, vu (19) et (21), l'inégalité

$$\hat{E}_o(T,\xi) \ll T^{-\kappa}(T^N |\xi|_d^{-1})\,. \tag{22}$$

Le calcul de $\hat{E}_t(\xi)$ se ramène à $\hat{E}_o(T,\xi)$. En effet, posons

$$\underline{Q}_M^n = \prod_{p\in M} \underline{Q}_p^n\ ,\quad dx_M = \prod_{p\in M} dx_p\ ;$$

et si $x_M = (x_p) \in \underline{Q}_M$, on écrit

$$\chi(x_M) = \prod_{p\in M} \chi_p(x_p)\,,$$

où χ_p est <u>le caractère de Tate de</u> $\underline{Q}_p$ (cf. la démonstration du thm. 3, ch. IV, § 2 de [W] ou [Lg], ch. XIV, § 1). Posons enfin

$$U_M = \{x \in \underline{Q}_M^n \mid \|x_p\|_p = 1 \quad \text{pour} \quad p \in M\}$$

Avec ces notations, et puisque les fonctions ϕ_p sont leur propres transformées de

Fourier lorsque la transformation de Fourier est définie par le caractère de Tate, il vient

$$\hat{E}_t(\xi) = \prod_{p \notin M} \phi_p(\xi)\, \hat{E}_t(\xi_M, \xi_o)\,, \tag{23}$$

avec

$$\hat{E}_t(\xi_M, \xi_o) = \int_{U_M} \chi(\langle x_M, \xi_M \rangle)\, \hat{E}_o(t\, F_M(x_M), \xi_o)\, dx_M\,. \tag{24}$$

Si $\xi = 0$, on a, vu la relation (20),

$$\begin{aligned} E_t(0,0) &= t^{-K} \int_{U_M} F_M(x_M)^{-K}\, dx_M \int_{\underline{R}^n} \exp(-F(x_o))\, dx_o \\ &= t^{-K} V_o \prod_{p \in M} \int_{\|x\|_p = 1} |F(x_p)|_p^{-1}\, dx_p \\ &= t^{-K} V_M \end{aligned}$$

d'où s'ensuit la relation (14) ; si d'autre part on pose $T = t\, F_M(x_M)^{-1}$, la relation (7) implique que si $x_M \in U_M$, on a $T \leq c_M^{-1} t$ et donc,

$$E_o(t\, F_M(x_M), \xi_o) = E_o(T, \xi_o) \ll t^{N-K}\, |\xi_o|_d^{-N}$$

comme on le déduit de (22) ; cette estimation, jointe à (23) et (24), prouve la relation (15) et le lemme 2 est démontré.

BIBLIOGRAPHIE

[A] C.AN - On the analytic continuation of a certain Dirichlet series, J. of Number Theory, 6 (1974), p. 1-6.

[B] S. BOCHNER - Zeta-functions and Green's functions for linear partial differential operators of elliptic type with constant coefficients, Ann. of Math., 57 (1953), p. 32-56.

[L] G. LACHAUD - Variations sur un thème de Mahler, à paraître aux Inv. Math.

[Lg] S. LANG - Algebraic number theory, Reading, Addison-Wesley, 1970.

[M1] K. MAHLER - Uber einer Satz von Mellin, Math. Ann., 100 (1928), p. 384-395.

[M2] K. MAHLER - Zur Approximation Algebraischer Zahlen, III, Acta Math., 62 (1933), p. 91-166.

[R] B. RANDOL - Generalized zeta-functions, Arkiv för Mat., 5 (1963), p. 101-111.

[W] A. WEIL - Basic Number Theory, Heidelberg, Springer, 1974.

Gilles LACHAUD
U.E.R. de Mathématiques
Université Paris 7
2, place Jussieu
75221 PARIS CEDEX 05

Astérisque

H. W. JUN. LENSTRA

Euclidean ideal classes

Astérisque, tome 61 (1979), p. 121-131

<http://www.numdam.org/item?id=AST_1979__61__121_0>

Société Mathématique de France
Astérisque 61 (1979) p. 121-131

EUCLIDEAN IDEAL CLASSES

par

H.W. Lenstra, jr

Introduction

A classical method, due to Euclid, Stevin and Gauss, to establish that a given commutative ring R is a principal ideal ring consists in showing that R is Euclidean, i.e. that there exists a map φ from $R - \{0\}$ to a well-ordered set, usually $\mathbb{N} = \{0, 1, 2, \ldots\}$, such that for all $a, b \in R$, $b \neq 0$, $a \notin Rb$, there exist $q, r \in R$ such that $a = qb + r$ and $\varphi(r) < \varphi(b)$. Such a map φ is said to be a Euclidean algorithm on R, and R is called Euclidean with respect to φ.

A case of special interest in number theory is the following. Let K be a global field, i.e. a finite extension of $\mathbb{Q}$ or a function field in one variable over a finite field $\mathbb{F}_q$. Denote by P the set of all non-trivial prime divisors of K, and let $S \subset P$ be a finite non-empty subset containing the set S_∞ of archimedean prime divisors of K. For R we take the ring of S-integers in K:

$$R = \{x \in K: |x|_{\underline{p}} \leq 1 \text{ for all } \underline{p} \in P - S\},$$

where $|\ |_{\underline{p}}$, for $\underline{p} \in P$, denotes an absolute value of K corresponding to $\underline{p}$. For $x \in R - \{0\}$, the norm $N(x)$ is the cardinality of the finite ring R/Rx. One is interested in conditions under which the norm N is a Euclidean algorithm on R. Most of the literature on the subject (see [8] for references) restricts to the case that K is a number field, and $S = S_\infty$. Then R is the ring of algebraic integers in K, and N is the absolute value of the field norm $K \to \mathbb{Q}$ (restricted to $R - \{0\}$).

Let the norm N be extended to K by multiplicativity and $N(0) = 0$. Then it is easily seen that N is a Euclidean algorithm on R if and only if

(0.1) for all $x \in K$ there exists $y \in R$ such that $N(x-y) < 1$.

In this paper we investigate a similar property in which the role of the ring R is played by a fractional ideal $\underline{c}$ of R. If $\underline{a} \subset R$ is a non-zero ideal, we define $N(\underline{a})$ to be the cardinality of $R/\underline{a}$, and we extend the definition of $N(\underline{a})$ to fractional ideals by multiplicativity. We are interested in the following property of a fractional ideal $\underline{c}$:

(0.2) for all $x \in K$ there exists $y \in \underline{c}$ such that $N(x-y) < N(\underline{c})$.

For $\underline{c} = R$ this clearly reduces to (0.1). If $\underline{c}$ is principal, $\underline{c} = Rc$, then $N(\underline{c}) = N(c)$ and dividing by c we see that (0.2) and (0.1) are equivalent. Generally, this argument shows that whether or not (0.2) is satisfied only depends on the ideal class $[\underline{c}]$ of $\underline{c}$. If it is satisfied, we say that the ideal class $[\underline{c}]$ is Euclidean for the norm or norm-Euclidean. So the principal ideal class is Euclidean for the norm if and only if N is a Euclidean algorithm on R.

Here is an example of a non-principal Euclidean ideal class. Let $K = \mathbb{Q}(\sqrt{-5})$, $R = \mathbb{Z}[\sqrt{-5}]$ (so $S = S_\infty$) and $\underline{c} = (2, 1 + \sqrt{-5})$. Then $N(\underline{c}) = 2$, and $N(x) = |x|^2$ for $x \in K$ if K is considered as a subfield of $\mathbb{C}$. Drawing a picture (cf. [2]) one finds that

for all $x \in \mathbb{C}$ there exists $y \in \underline{c}$ such that $|x-y| < \sqrt{2}$,

so (0.2) holds. But (0.1) doesn't, because R is no principal ideal ring.

The main result about Euclidean ideal classes is the following theorem.

(0.3) Theorem The ring R has at most one ideal class which is Euclidean for the norm. If there is one, then it generates the ideal class group of R.

In particular, if the principal ideal class is Euclidean, then the class group is trivial and R is a principal ideal ring, as we knew already.

A generalization of theorem (0.3), in an algebraic setting, is proved in section 1. By means of examples we show that the class number can be arbitrarily

large.

Section 2 is devoted to the arithmetic rings discussed above. We shall see in this section that the ring of integers of a quadratic number field K has a non-principal norm-Euclidean ideal class if and only if the discriminant of K over $\mathbb{Q}$ is one of

$$-20, -15, 40, 60, 85,$$

see (2.1) and (2.5). In all five cases, the class number is two (cf. (1.8)).

1. Elementary properties

In this section R is a domain, i.e. a commutative ring, without zero-divisors, with a unit element different from zero. The group of units of R is denoted by R^*, and K denotes its field of fractions. An ideal class of R is a set of the form $\{\underline{d}a: a \in K^*\}$ where $\underline{d} \subset R$ is a non-zero ideal and $\underline{d}a = \{xa: x \in \underline{d}\}$. An element of an ideal class is called a fractional ideal of R. The unique ideal class containing a given fractional ideal $\underline{a}$ is denoted by $[\underline{a}]$. Fractional ideals are multiplied in the usual way, and ideal classes are multiplied by $[\underline{a}].[\underline{b}] = [\underline{a}.\underline{b}]$. If the set $Cl(R)$ of ideal classes of R is a group with respect to this multiplication, then R is called a Dedekind domain, $Cl(R)$ its class group, and the order of $Cl(R)$ its class number. We put

$$E = \{\underline{b}: \underline{b} \text{ is a fractional ideal of } R, \text{ and } \underline{b} \supset R\}.$$

(1.1) Definition Let W be a well-ordered set, $\psi: E \to W$ a map, C an ideal class of R, and $\underline{c} \in C$. We say that ψ is a Euclidean algorithm for C, or that C is Euclidean with respect to ψ, if

(1.2) for all $\underline{b} \in E$ and all $x \in \underline{b}.\underline{c} - \underline{c}$ there exists $z \in x + \underline{c}$ such that $\psi(\underline{b}cz^{-1}) < \psi(\underline{b})$.

We call C Euclidean if there exists a Euclidean algorithm for C.

It is readily verified that the definition does not depend on the choice of

$\underline{c}$ in C, and that, in the given circumstances, we have $z \neq 0$ and $\underline{bc}z^{-1} \in E$.

In the arithmetic case discussed in the introduction we take $\psi(\underline{b}) = N(\underline{b})^{-1}$. The inequality in (1.2) then simplifies to $N(z) < N(\underline{c})$. Using that $\bigcup_{\underline{b} \in E} \underline{bc} = K$, and writing $z = x - y$, we then find that (1.2) is equivalent to (0.2). So C is Euclidean with respect to ψ if and only if it is Euclidean for the norm.

(1.3) Exercise Show that a domain R is Euclidean if and only if the principal ideal class $[R]$ is Euclidean.

In the sequel we suppose that $C = [\underline{c}]$ satisfies the condition

$$\{x \in K: x\underline{c} \subset \underline{c}\} = R. \tag{1.4}$$

This condition is satisfied if $\underline{c}$ is invertible, e.g. if R is Dedekind. If (1.4) does not hold, then in our conclusions R should be replaced by the ring $\{x \in K: x\underline{c} \subset \underline{c}\}$.

In the following lemma we assume that W contains $\mathbb{N}$ as a beginning segment.

(1.5) Lemma Let C satisfy (1.4) and be Euclidean with respect to ψ. Then for every $\underline{b} \in E$, $\underline{b} \neq R$, there exists $n \in \mathbb{N}$ such that

$$[\underline{b}.\underline{c}^n] = [R], \quad 0 < n \leq \psi(\underline{b}).$$

Proof by induction on $\psi(\underline{b})$. From $\underline{b} \neq R$ and (1.4) we find that there exists an element $x \in \underline{bc} - \underline{c}$, and (1.2) then gives us $\underline{a} = \underline{bc}z^{-1} \in E$ with $\psi(\underline{a}) < \psi(\underline{b})$. If $\underline{a} = R$, then $[\underline{bc}] = [R]$ and we can take $n = 1$. If $\underline{a} \neq R$, then by the induction hypothesis $[\underline{ac}^m] = [R]$ for some $m \leq \psi(\underline{a})$, and we can take $n = m + 1$. This proves (1.5).

(1.6) Theorem Let R be a domain, and C a Euclidean ideal class of R satisfying (1.4). Then R is a Dedekind domain with a finite cyclic class group, generated by C.

Proof We may clearly assume that $R \neq K$. Then $Cl(R) = \{[\underline{b}]: \underline{b} \in E, \underline{b} \neq R\}$, so (1.5) shows that every ideal class has an inverse $[\underline{c}^n]$. Therefore R is Dedekind, and $Cl(R) = \{[\underline{c}]^{-n}: n = 1, 2, 3, \ldots\}$. In particular $[R] = [\underline{c}]^{-n}$

for some $n > 0$, so $[\underline{c}]$ has finite order. This proves (1.6).

(1.7) Exercise Let $a \in R - R^*$, $a \neq 0$. Prove that $\#Cl(R) \leq \psi(Ra^{-1})$.

Suppose $\underline{b} \in E$, $\underline{b} \neq R$ is such that $\psi(\underline{b})$ is smallest possible. Then the ideal $\underline{a}$ in the proof of (1.5) must be equal to R, so $n = 1$ and $C = [\underline{b}]^{-1}$. Hence there is at most one ideal class, satisfying (1.4), which is Euclidean with respect to a given ψ. This remark, and theorem (1.6), prove theorem (0.3).

(1.8) Exercise Let K be a Galois extension of degree n of $\mathbb{Q}$, and suppose that its ring of integers has a norm-Euclidean ideal class. Prove that the class number of K divides n.

Many results known about Euclidean rings (cf. [13]) have immediate generalizations for rings possessing a Euclidean ideal class. We list some of them as exercises. Assume, for (1.9) - (1.14), that C satisfies (1.4) and is Euclidean with respect to ψ.

(1.9) Exercise Let $\underline{a}, \underline{b} \in E$. Prove that $\psi(\underline{ab}) \geq \psi(\underline{b})$, with equality if and only if $\underline{a} = R$.

(1.10) Exercise Let $R' \subset K$ be a subring containing R. Prove that R' has a Euclidean ideal class. Prove that R' is Euclidean if and only if R' is a principal ideal domain. Deduce that $\mathbb{Z}[\sqrt{-5}, 1/3]$ is Euclidean (cf. [15]).

In the following exercises we put

(1.11) $$\theta(\underline{b}) = \min\{\psi(\underline{b}): \psi: E \to W \text{ is a Euclidean algorithm for } C\}$$

where W is the set of ordinals of cardinality $\leq \#E$. This map is called the smallest Euclidean algorithm for C; the terminology is easily justified.

(1.12) Exercise Prove that $\theta(\underline{ab}) \geq \theta(\underline{a}) + \theta(\underline{b})$ for $\underline{a}, \underline{b} \in E$.

(1.13) Exercise Let $\underline{b} \in E$ be such that $\theta(\underline{b})$ is finite. Prove that $\underline{b} \in C^{-\theta(\underline{b})}$.

(1.14) Exercise Prove that $\theta(\underline{b}) = 1$ if and only if $\underline{b}^{-1} = \underline{p}$ is a maximal ideal of R such that $\underline{p} \in C$ and the natural map $R^* \to (R/\underline{p})^*$ is surjective.

(1.15) Example Let k be a field, $K = k(t)$ a simple transcendental extension of k, and $f \in k[t]$ an irreducible polynomial. Denote by h the degree of f. Put

$$R = \{a/b \in K: a, b \in k[t], \ b \text{ is a power of } f, \ \deg a \leq \deg b\},$$

$$\underline{c} = \{a/b \in R: \deg a < \deg b\}.$$

Then R is a ring, and $\underline{c}$ is an invertible R-ideal, satisfying (1.4). For a non-zero ideal $\underline{a} \subset R$, put $d(\underline{a}) = \dim_k R/\underline{a}$, and extend the definition to all fractional ideals by $d(\underline{a}\underline{a}^{-1}) = d(\underline{a}) - d(Ra)$. Then $d(\underline{c}) = 1$, and more generally $d(\underline{a}\underline{c}) = d(\underline{a}) + 1$ for all $\underline{a}$; this follows from the invertibility of $\underline{c}$. An easy calculation gives

$$d(Rx) = -\mathrm{ord}_f(x).h \quad \text{for} \quad x \in K^*,$$

where ord_f is the normalized exponential valuation of K corresponding to f.

We claim that $C = [\underline{c}]$ is Euclidean with respect to the map $\psi: E \to \mathbb{N}$ defined by $\psi(\underline{b}) = -d(\underline{b})$. This assertion is equivalent to

for all $x \in K$ there exists $y \in \underline{c}$ such that $d(R(x-y)) < d(\underline{c})$

(cf. (0.2)). To prove it, use the partial fraction expansion of x to write $x = (c/f^n) + z$, with $n \in \mathbb{N}$, $c \in k[t]$, $\deg c < \deg f^n$, $z \in K$, $\mathrm{ord}_f(z) \geq 0$, and choose $y = c/f^n$. Then $d(R(x-y)) = d(Rz) = -\mathrm{ord}_f(z).h \leq 0 < 1 = d(\underline{c})$, as required.

We conclude that R is Dedekind, and that $\mathrm{Cl}(R)$ is generated by C. We calculate the class number. If $\underline{c}^n = Rx$, then $n = d(\underline{c})^n = d(Rx) = -\mathrm{ord}_f(x).h$ so n is divisible by h. Also $\underline{c}^h = Rf^{-1}$, so the class number equals h.

Thus we see that every positive integer occurs as the class number of a ring having a Euclidean ideal class.

If we take $k = \mathbb{F}_q$, then R is of the arithmetic type described in the introduction, and $N(x) = q^{d(x)}$. Hence, in our example, C is also Euclidean for the norm.

2. Arithmetic rings

In this section we let the notations be as in the introduction. In particular, K is a global field, and R is its ring of S-integers.

In the case $\#S = 1$ all examples of Euclidean ideal classes are easily determined.

(2.1) Proposition Let $\#S = 1$, and let C be an ideal class of R. Then C is Euclidean if and only if C is Euclidean for the norm, and if and only if

(a) R is the ring of integers in one of the fields

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{-d}),\ d = 3,\ 4,\ 7,\ 8,\ 11,\ 15,\ \text{or}\ 20$$

and C is the unique generator of $Cl(R)$;

or (b) R is one of the rings described in (1.15), with k finite and $C = [\underline{c}]$.

The proof is similar to the proof in the classical case (cf. [7, sec. 10]). There is an analogous result for function fields over infinite fields of constants.

The class numbers of the rings in (a) are 1, 1, 1, 1, 1, 1, 2, 2, respectively.

(2.2) Proposition Suppose that $\#S \geq 2$, and if K is a number field, assume that for every squarefree integer n the ζ-function of the field $K(\zeta_n, R^{*1/n})$, with ζ_n denoting a primitive n-th root of unity, satisfies the generalized Riemann hypothesis. Then every ideal class C which generates the ideal class group of R is Euclidean.

This proposition generalizes the theorem of Weinberger and Queen in the classical case [16, 12]. The proof of (2.2) uses the methods of [9]. It also yields an explicit description of the map θ defined by (1.11); in most, but not all, cases it is the smallest function having the properties indicated in exercises (1.12), (1.13) and (1.14).

In the rest of this section we are exclusively interested in ideal classes which are Euclidean for the norm.

Let K_S denote the locally compact topological ring

$$K_S = \prod_{\underline{p} \in S} K_{\underline{p}},$$

where $K_{\underline{p}}$ is the $\underline{p}$-adic completion of K. We regard K as being embedded in K_S along the diagonal. Then K is dense in K_S, and every fractional ideal $\underline{a}$ of R is discrete in K_S, with $K_S/\underline{a}$ compact. The norm is extended to a map $N: K_S \to \mathbb{R}_{\geq 0}$ by

$$N(x) = \prod_{\underline{p} \in S} |x_{\underline{p}}|_{\underline{p}}, \quad \text{for} \quad x = (x_{\underline{p}})_{\underline{p} \in S} \in K_S,$$

where the $|\ |_{\underline{p}}$ are normalized in the usual way which makes the formula valid for $x \in K$. For $t \in \mathbb{R}_{>0}$, put

$$V_t = \{z \in K_S : N(z) < t\}.$$

This is an open neighborhood of 0 in K_S. Clearly, the ideal class $C = [\underline{c}]$ is Euclidean for the norm if and only if

$$K \subset \underline{c} + V_{N(\underline{c})} = \{x + y : x \in \underline{c},\ y \in V_{N(\underline{c})}\}.$$

It seems that in all cases in which this condition is known to be satisfied we actually have

$$K_S = \underline{c} + V_{N(\underline{c})}.$$

It is unknown whether both properties are in fact equivalent. The only known result in this direction is:

(2.3) Proposition Suppose that $\#S \leq 2$, and $t \in \mathbb{R}_{>0}$. Then $K \subset \underline{c} + V_t$ implies that $K_S = \underline{c} + V_{t+\varepsilon}$ for every $\varepsilon \in \mathbb{R}_{>0}$; if $\#S = 1$ or K is a function field this is also true for $\varepsilon = 0$.

For the proof, cf. [1, theorem M].

In the case $\#S = 2$, $S = S_\infty$, Davenport [4, nrs 70, 76, 82] proved that only finitely many R, up to isomorphism, are Euclidean with respect to the norm. This result can be generalized as follows.

(2.4) Proposition Suppose that $\#S = 2$. Then R has an ideal class which is

Euclidean for the norm if and only if

(a) K is one of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-d})$, $d = 3, 4, 7, 8, 11, 15, 20$;

or (b) R belongs, up to isomorphism, to a certain finite list of number rings;

or (c) K is a function field of genus zero.

The proof makes use of (2.3) and of ideas of Cassels [3].

The finite list mentioned under (b) is not completely known. It contains at least 107 rings, as we shall see below. We distinguish four cases.

(2.5) $S = S_\infty$, K is real quadratic, and R its ring of integers. This case is completely settled. The principal ideal class is norm-Euclidean if and only if the discriminant of K over $\mathbb{Q}$ has one of the following sixteen values:

$$5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76,$$

cf. [4, nr 74]. By similar methods one can show that there is a non-principal norm-Euclidean ideal class if and only if the discriminant is one of

$$40, 60, 85.$$

In these three cases, the class number is two.

(2.6) $S = S_\infty$, K is complex cubic, and R its ring of integers. If R has a norm-Euclidean ideal class then $-\Delta < 170523$ and $h \leq 4$, where Δ denotes the discriminant of K over $\mathbb{Q}$ and h the class number. The fifty-two known examples all have class number one [14]. It would be of interest to find examples with larger class numbers in this category.

(2.7) $S = S_\infty$, K is totally complex quartic, and R its ring of integers. Here we may restrict attention to fields with $\Delta < 20{,}435{,}007$ and $h \leq 6$. There are thirty-two known K's with $[R]$ norm-Euclidean, see [8] for references. The only other known example in this category is $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$: it has class number two, and the non-principal ideal class is Euclidean for the norm.

(2.8) $S = S_\infty \cup \{\underline{p}\}$, K is a complex quadratic field not mentioned in (2.4)(a), and $\underline{p}$ is a non-archimedean prime of K. The three rings

$$R = \mathbb{Z}[\sqrt{-19}, 1/2],\ \mathbb{Z}[\sqrt{-6}, 1/2],\ \mathbb{Z}[\sqrt{-6}, 1/(1+4\sqrt{-6})]$$

are Euclidean with respect to the norm; the last two are due to G. Cooke (unpublished). Other examples of norm-Euclidean ideal classes are not known in this category, but should not be hard to find. It seems an attractive problem to determine them all. It can be shown that they all have $h \leq 2$.

For higher values of $\#S$ no result comparable to (2.4) is known.

We finish with three unsolved problems.

(2.9) Problem A theorem of O'Meara [11] states that for any global field K there exists a finite subset $S \subset P$, $S \neq \emptyset$, $S \supset S_\infty$, such that the ring R of S-integers is Euclidean with respect to the norm. Can one take S to satisfy $S \cap T = \emptyset$, where T is a given finite subset of P with $S_\infty \cap T = \emptyset$?

(2.10) Problem Do there, in the case $S = S_\infty$, exist infinitely many non-isomorphic rings R with a norm-Euclidean ideal class? See [8, 10] for 312 examples with class number one, and (2.1), (2.5), (2.7) for six examples with class number two.

(2.11) Problem Heilbronn [5, 6] has shown that in certain classes of cyclic number fields there are only finitely many whose ring of integers is Euclidean with respect to the norm. Do his results carry over to rings with a norm-Euclidean ideal class?

Acknowledgement

Research for this paper was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

References

1. E.S. BARNES, H.P.F. SWINNERTON-DYER, The inhomogeneous minima of binary

quadratic forms (II), Acta Math. 88 (1952),279-316.

2. E. CAHEN, Sur une note de M. Fontené relative aux entiers algébriques de la forme $x + y\sqrt{-5}$, Nouv. Ann. Math. (4) 3 (1903), 444-447.
3. J.W.S. CASSELS, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, Proc. Cambridge Philos. Soc. 48 (1952), 72-86, 519-520.
4. The collected works of HAROLD DAVENPORT, vol. I, Academic Press, London 1977.
5. H. HEILBRONN, On Euclid's algorithm in cubic self-conjugate fields, Proc. Cambridge Philos. Soc. 46 (1950), 377-382.
6. H. HEILBRONN, On Euclid's algorithm in cyclic fields, Canad. J. Math. 3 (1951), 257-268.
7. H.W. LENSTRA, Jr., Lectures on Euclidean rings, Bielefeld 1974.
8. H.W. LENSTRA, Jr., Euclidean number fields of large degree, Invent. Math. 38 (1977), 237-254.
9. H.W. LENSTRA, Jr., On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. 42 (1977),201-224.
10. H.W. LENSTRA, Jr., Quelques exemples d'anneaux euclidiens, C. R. Acad. Sci. Paris 286 (1978), 683-685.
11. O.T. O'MEARA, On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.
12. C.S. QUEEN, Arithmetic Euclidean rings, Acta Arith. 26 (1974), 105-113.
13. P. SAMUEL, About Euclidean rings, J. Algebra 19 (1971), 282-301.
14. E.M. TAYLOR, Euclid's algorithm in cubic fields with complex conjugates, J. London Math. Soc. 14 (1976), 49-54.
15. J.H.M. WEDDERBURN, Non-commutative domains of integrity, J. Reine Angew. Math. 167 (1932), 129-141.
16. P.J. WEINBERGER, On Euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (Analytic number theory), 321-332, Amer. Math. Soc. 1973.

Permanent adress

Mathematical Institut
Roetersstraat 15
1018 WB AMSTERDAM
Netherlands

Hendrik Lenstra
Institut des Hautes Études Scientifiques
35, route de Chartres
91440 Bures-sur-Yvette.

Astérisque

VIKTOR LOSERT
HARALD RINDLER

Almost constant sequences

Astérisque, tome 61 (1979), p. 133-143
<http://www.numdam.org/item?id=AST_1979__61__133_0>

Société Mathématique de France
Astérisque 61 (1979) p. 133-143

ALMOST CONSTANT SEQUENCES

by

Viktor LOSERT and Harald RINDLER

Rauzy has characterized all real sequences (c_n) such that for any uniformly distributed sequence (x_n) the sequence $(c_n + x_n)$ is again u.d. modulo 1, [6]. A new proof of this result was given in [10], together with a generalization to uniform distribution in compact metric groups and to R^n. The aim of this paper is to consider the corresponding questions for locally compact Abelian groups with respect to several concepts of uniform distribution. Our methods admit also generalizations to the non-Abelian case. For general references we refer to [1]. For other generalizations see [7] Ch. IV and [2].

1. Definition 1: If G is a locally compact group let M(G) be the set of (Hartman)uniformly distributed sequences (x_n) in G, i.e.:

$$\lim_{N\to\infty} N^{-1} \sum_{n\leq N} U(x_n) = 0$$

hold for all non-trivial irreducible finite-dimensional continuous unitary representations U of G.

Definition 2: a) $C(G) = \{(c_n): x_n \in M(G) \Rightarrow (c_n x_n) \in M(G)\}$

b) $C_0(G) = \{(c_n): \exists a > 1$ such that $c_n = c_m$ if $a^k \leq n,m < a^{k+1}, k = 0,1,2,\ldots\}$

If G is metrizable let $d(x,y)$ be a bounded left-invariant metric on G and define for arbitrary sequences

$$(x_n),(y_n): g(x_n,y_n) = \overline{\lim}\, N^{-1} \sum_{n\leq N} d(x_n,y_n)$$

If A is a family of sequences, A^- will denote the "closure" with respect to the pseudo-metric g. If G is non-metrizable consider the family of all left-invariant pseudo-metrics d_i, $i \in I$, the according pseudo-metrics g_i, $i \in I$ induce a topology on the space of all sequences on G.

Theorem 1: If G is a locally compact separable abelian group then

$$C(G) = C_0(G)^-$$

Remarks: If G is not separable, i.e. there exists no countable dense subset it can easily be seen that M(G) is void. For metric groups Th. 1 has been announced in [11], but our methods admit generalizations to non-Abelian groups.

Proof:

Lemma 1: Let $h: G \to H$ be a continuous group homomorphism, G l.c. separable, H compact metric, such that $h(G)^- = H$. If $(y_n) \in M(H)$ then there exists $(x_n) \in M(G)$ such that lim $d_H(h(x_n), y_n) = 0$ (d_H = metric on H).

Remarks: If h is surjective it is possible to achieve $h(x_n) = y_n$ if G is metric and abelian or compact, [8], in the compact case it is sufficient that G is separable, [3]; if H is only separable even for $G = H \times Z_2$, $Z_2 = \{-1,1\}$ this is no longer true in general, [4], and open even in the case $G = R \times Z_2$, $H = R$. For $G = Z$, $H = R/Z$, $h(z) = za$, a irrational the lemma above cannot be strengthened (e.g.: $(h^{-1}(2az)) = (2z)$ is not u.d. in Z).

Proof: Let (z_n) be an arbitrary u.d. sequence in G (which exists, [9], Th. 1). For $k = 1,2,\ldots$ let (V_{ik}) $(i = 1,2,\ldots,m_k)$ be a partition of H into sets of diameter less than $1/k$ such that the boundary of each V_{ik} has measure 0 and each V_{ik} has positive measure. Put λ for the normalized Haarmeasure on H and C_V for the characteristic function of a set V. We can construct a sequence of indices (N_k) such that $N_{k+1} \geq 2N_k$ and for all $N \geq N_k$ and $i \leq m_k$:

$$|N^{-1} \sum_{n \leq N} C_{V_{ik}}(y_n) - \lambda(V_{ik})| < 1/2^k m_k$$

and

$$|N^{-1} \sum_{n\leq N} C_{V_{ik}}(h(z_n)) - \lambda(V_{ik})| < 1/2^k m_k$$

By induction we define a map $p: N \to N$ in the following way: If $n < N_1$ put $p(n) = n$. If $N_k \leq n < N_{k+1}$, $y_n \in V_{ik}$, let $p(n)$ be the smallest number m such that $h(z_m) \in V_{ik}$ and $m \neq p(s)$ for $s < n$. We put $x_n = z_{p(n)}$. Since $d_H(h(z_{p(n)}), y_n) < 1/k$ for $n \geq N_k$ we have $\lim d_H(h(x_n), y_n) = 0$.

Let $|A|$ be the number of elements of a finite set A, put $D_p(N) = |p([1,N]) \setminus [1,N]|$. If $N > N_k$, it is easily seen that

$$D_p(N) \leq D_p(N_k) + \sum_{i\leq m_k} \Big| \sum_{N_{k+1}\leq n\leq N} C_{V_{ik}}(y_n) - C_{V_{ik}}(h(z_n)) \Big| < D_p(N_k) +$$

$$+ 4Nm_k/2^k m_k = D_p(N_k) + N/2^{k-1}.$$

In particular we get by induction:

$$D_p(N_k) \leq \sum_{2\leq j\leq k} N_j/2^{j-3} \leq N_k \cdot k/2^{k-3}$$

and consequently $D_p(N) \leq N(k+2)2^{k-3} = o(N)$.

Since p is by definition injective, we have $|[1,N] \setminus p([1,N])| = D_p(N)$, i.e. the symmetric difference between the two sets is $2D_p(N) = o(N)$. It follows immediately that the sequence $(x_n) = (z_{p(n)})$ is u.d. like the sequence (z_n). q.e.d.

As any representation U (in Def. 1) is a homomorphism into a compact group and because the homomorphic image of a u.d. sequence is u.d. in the closure of the image (this follows easily from the Definition of u.d.) we obtain

Proposition 1: $(c_n) \in C(G)$ iff $U(c_n) \in U(G)^-$ for any representation U.

Remarks: If G is Abelian, the U's are just the elements of $\hat{G}$ the character group of G; we have $U(G) \subseteq T$ the 1-dimensional torus.

In order to prove that $(c_n) \in C(G)$ it is sufficient to know that $(U(c_n)) \in C(T)$ for all U from a subset of $\hat{G}$ which separates the points of G and is either non meagre or has positive measure. This follows from the observation that $C(T)$ is a group and consequently the set of all U for which $(U(c_n)) \in C(T)$ a subgroup of $\hat{G}$. As a consequence of Proposition 1 we obtain also for non-compact H:

Corollary: If $h: G \to H$ is a continuous epimorphism, $(c_n) \in C(G)$ then $(h(c_n)) \in C(H)$.

In order to prove Theorem 1 it suffices to consider metric groups. (G is the projective limit of metric (even Lie-)groups: G/N_i, $i \in I$, and by the corollary we have for $(c_n) \in C(G)$ and $h_i: G \to G/N_i$: $(h_i(c_n)) \in C(G/N_i)$, and the metrics d_i from G/N_i determine the topology on G).

In order to prove Theorem 1 it is sufficient to prove the following Lemma (see [10], esp. Lemma 4).

Lemma 2: If $(c_n) \in C(G)$ then $\lim N^{-1} \cdot \sum_{n \le N} d(c_n, c_{n+1}) = 0$

Proof: For any $U \in \hat{G}$ we have by Prop. 1 that $U(c_n) \in C(U(G)^-)$. As Th. 1 is known for $U(G)^-$ (already proved by Rauzy, see also [10]) it follows that

$$\lim N^{-1} \sum_{n \le N} |U(c_n) - (c_{n+1})| = 0 \text{ for all } U \in \hat{G}.$$

Take $\varepsilon > 0$ and put $W = \{x \in G: d(x,e) < \varepsilon\}$ W is an open neighbourhood of the unit element of G. If V is an open symmetric neighbourhood of e with $V + V \subseteq W$ then $f = (1/\lambda(V))\, C_V * C_V$ is a positive definite continuous function, satisfies $f(e) = 1$ and vanishes outside W. By Bochner's theorem there exists a probability measure μ on $\hat{G}$ such that

$$f(x) = \int U(x) d\mu(U) \text{ for all } x \in G.$$

By Lebesgue's dominated convergence theorem we conclude that

$$\lim N^{-1} \sum_{n\le N} |f(-c_{n+1}+c_n) - 1| \le \lim \int N^{-1} \sum_{n\le N} |U(-c_{n+1}+c_n) - 1| \, d\mu(U) = 0.$$

It follwos that the set $\{n: -c_{n+1}+c_n \notin W\} = \{n: d(c_n, c_{n+1}) \ge \varepsilon\}$ has density 0 in N. Since d is bounded we get $\overline{\lim}\ 1/N \cdot \sum_{n\le N} d(c_n, c_{n+1}) < \varepsilon$ for all $\varepsilon > 0$. q.e.d.

Remarks: Theorem 1 holds also for non-abelian groups with the property that all irreducible unitary representations are finite dimensional (same proof). If the finite dimensional unitary representations U do not separate points of G, i.e. if there exists $x \neq e$ such that $U(x) = U(e)$ for all U, then the sequence e,x,e,x,e,x,... belongs to $C(G)$ but not to $C_0(G)^-$.

Denote by S_3 the symmetric group and by A_3 the alternating group of 3 elements and consider the discrete group G of all sequences $g = g^{(i)}$, $i = 1,2,\ldots, g^{(i)} \in S_3$, $g^{(i)} \neq e$ for at most finitely many i. If U is a fine-dimensional representation of G, denote by $U^{(i)}$ the restriction to the i-th component. From the fact the $U^{(i)}$ commutes with $U^{(j)}$ $i \neq j$ it can be derived that $U^{(i)}$ restricted to A_i is the trivial representation for all but at most finitely many i ($\le \dim U/2$). It follows that the sequence (c_n) : $c_n^{(i)} = e$ if $i \neq n$, $c_n^{(n)} = (123) \in A_3$ belongs to $C(G)$ but not to $C_0(G)^-$. Nevertheless G has a separating family of 2-dimensional representations.

2. Now we want to consider concepts of uniform distribution connected with infinite dimensional representation. For $1 \le p < \infty$ put $L^p(G) = \{f: (\int |f(x)|^p \, dx)^{1/p} = \|f\|_p < \infty\}$, "dx" denotes a left Haar measure. Consider the left regular representation

$$f \to L_y f, \quad L_y f(x) = f(y^{-1}x), \quad x,y \in G$$

Definition 3: A sequence (x_n) in G is called L^p-uniformly distributed if $\|N^{-1} \cdot \sum_{n \le N} L_{x_n} f\|_p \to 0$ for all $f \in L^1 \cap L^p$ with $\int f = 0$. $M(L^p(G))$ shall denote the set of all L^p-u.d. sequences.

Definition 4: $C(L^p(G)) = \{(c_n) : (x_n) \in M(L^p(G)) \Rightarrow (c_n x_n) \in M(L^p(G))$

Remark: It is known that for compact groups $M(G) = M(L^p(G))$ for all p and $M(L^1(G) \subseteq M(G)$ in general, [9]. $M(L^1(G) \neq \emptyset$ if and only if G is amenable and separable (see [9] and [5]).

Theorem 2: If G is a locally compact separable abelian group then $C(L^1(G)) = C(G)$.

Proof: The same proof as in Lemma 1 shows the following result: if $h: G \to H$ is a continuous group homomorphism onto a dense subgroup of H, and if $(y_n) \in M(H)$ then there exists $(x_n) \in M(L^1(G))$ such that $d_H(h(x_n), y_n) \to 0$ (use the relation $M(L^1(G)) \subseteq M(G)$). It follows that $(c_n) \in C(L^1(G))$ implies $(U(c_n)) \in C(U(G)^-)$ for all $U \in \hat{G}$ and by Proposition 1 that $(c_n) \in C(G)$. On the other hand it follows easily from the characterization of C(G) in Theorem 1 that $C(G) \subseteq C(L^1(G))$. q.e.d.

Remarks: Again the result can be extended to groups having only finite dimensional representations which are known to be amenable. $C(L^1(G) \subseteq C(G)$ for any separable amenable group (same proof as above). In the general non-abelian case several pathologies may appear:

If $G = P_1$ the projective group then $M(L^1(P_1)) = \emptyset$. P_1 is not amenable, $M(P_1) = P_1^{\mathbb{N}}$ the set of all sequences as P_1 is minimal almost periodic i.e. has no non-trivial finite dimensional unitary representation. We have $C(L^1(P_1)) = C(P_1) = P_1^{\mathbb{N}}$!

Let G be the group of all permutations p of an uncountable set such that $E_p = \{x : p(x) \neq x\}$ is finite then it is known that G is amenable and

minimal almost periodic. We have again $M(L^1(G)) \neq \emptyset$ (G is not separable), $M(G) = G^N$, $C(L^1(G)) = C(G) = G^N$. Replacing G by $G \times Z_2$ we obtain $C(L^1(G \times Z_2)) \neq C(G \times Z_2)$.

If G is the group of affine transformations of the line it can be shown that $C(L^1(G))$ contains a sequence (c_n) such that $(x_n c_n) \notin M(L^1(G))$ for some $(x_n) \in M(L^1(G))$, [9], Satz 9.

It can be shown that for a connected separable l.c. group G the set $C(L^1(G))$ coincides with $C(G)$ if and only if either $G \cong R^n \times K$, K compact or G is non amenable and minimal almost periodic. The essential part of the proof is the classical theorem of Freudenthal which implies that the only connected groups such that the finite dim. unitary representations separate points of G are isomorphic to $R^n \times K$.

$G = R$, $G = Z$ are typical for the abelian non-compact case. It should be noted that in both cases $M(L^1(G))$ is a proper subset of $M(G)$. It is already a consequence of results of Weyl that the sequence $(\sqrt{2}n^2+n)$ is u.d. in R and the according sequence of integers (z_n)

$$(z_n < \sqrt{2}\, n^2 + n < z_n + 1)$$

is u.d. in Z. Therefore Theorem 2 does not follow from Theorem 1.

3. In this section we study the case of L^2-uniform distribution which is quite different from the preceding two cases. The results hold for arbitrary locally compact groups ($M(L^p(G)) = M(G)$ if G is compact as mentioned above). For non-compact groups $L^p \cap L^1(G)$ is dense in $L^p(G)$ and we can choose any $f \in L^p(G)$ in Definition 3 ($p > 1$).

Theorem 3: Let (x_n) be a sequence in G (non-compact), K a compact subset of G with nonempty interior. The following statements are equivalent:

a) (x_n) is L^2-uniformly distributed

b) (x_n) is L^p-u.d. for some p with $1 < p < \infty$

c) (x_n) is L^p-u.d. for all p with $1 < p < \infty$

d) For any $\varepsilon > 0$ there exists $N_0(\varepsilon)$ such that

$$1/N\,|\{n: 1 \le n \le N,\ x_n \in xK\}| < \varepsilon \text{ for all } x \in G,\ N \ge N_0(\varepsilon)$$

Proof: Assume a), b) or c) holds and that $1/N\,|\{n: 1 \le n \le N, x_n \in xK\}| \ge \varepsilon$ for arbitrary large N. Put $f = C_{K^{-2}} \in L^p(G)\ (1 < p < \infty)$. If $x_n \in xK$ then $x_n^{-1} y \in K^{-2}$ for all $y \in xK^{-1}$. It follows that $1/N \sum_{n \le N} L_{x_n} f \ge \varepsilon$ on xK^{-1}. Since f is non-negative we conclude that

$$\| 1/N \sum_{n \le N} L_{x_n} f \|_p \ge \varepsilon\ (\lambda(K^{-1}))^{1/p}$$

which contradicts the assumption that (x_n) is L^p-u.d. (note the remark before Th. 3).

Now we assume that d) holds and we will prove c). It is easily seen that d) can be extended to arbitrary compact sets with non-empty interior. Put $f = C_{K^{-1}}$. If $x_n^{-1} \cdot y \in K^{-1}$ then $x_n \in yK$. It follows that

$$1/N \sum_{n \le N} L_{x_n} f(y) = 1/N\,|\{n: 1 \le n \le N,\ x_n \in yK\}| < \varepsilon \text{ for } N \ge N_0(\varepsilon).$$

Consequently: $\| 1/N \sum_{n \le N} L_{x_n} f \|_p \le \varepsilon^{(p-1)/p} \| 1/N \sum_{n \le N} L_{x_n} f \|_1^{1/p} =$

$$= \varepsilon^{(p-1)/p}\ \lambda(K^{-1})^{1/p}.$$

This shows that $\lim \| 1/N \sum_{n \le N} L_{x_n} f \|_p = 0$ for all $f = C_{K^{-1}}$. Since these functions generate a dense subspace of $L^p(G)$ it follows that (x_n) is L^p-u.d.

The first two theorems have shown that (for abelian groups) $C(G)$ and $C(L^1(G))$ consists of all sequences which are "almost constant" in a certain sense (closure of $C_0(G)$). Here the situation is quite different:

Definition 5: $C_f(G) = \{(c_n) \subseteq G, \exists b \in \mathbb{N}: |\{c_n: 2^i < n \leq 2^{i}\}| \leq b$ for $i = 1,2,..$ If d_i, $i \in I$ is the family of all bounded left invariant metrics on G we can define the closure of $C_f(G)$ as before.

Theorem 4: For any non-compact l.c. group $C(L^2(G)) = C_f(G)^-$

Proof: It follows easily from Theorem 3 d) that $C_f(G) \subseteq C(L^2(G))$ and consequently $C_f(G)^- \subseteq C(L^2(G))$.

Conversely assume that (d_n) does not belong to the closure of $C_f(G)$, i.e. there exists $\delta > 0$ and a pseudo-metric g such that $g((c_n),(d_n)) \geq \delta$ for all $(c_n) \in C_f(G)$. Denote by d the corresponding pseudo-metric of G, let U be a compact neighbourhood of e which is contained in

$$\{x: d(x,e) < \delta/2\}$$

and choose a compact symmetric neighbourhood V such that $V^4 \subseteq U$. There exists a sequence (x_n) such that $x_n U$ covers G and $x_n \notin x_i V^2$ for $i < n$. Take b, $i \in \mathbb{N}$. Let $x_{i1}(b)$ be that element x_j such that

$$|\{n: 2^i < n \leq 2^{i+1}, d_n^{-1} \in x_j U\}|$$

is maximal. Similar choose $x_{i2}(b)$ in such a way that

$$|\{n: 2^i < n \leq 2^{i+1}, d_n^{-1} \in x_{i2}(b)U, d_n^{-1} \notin x_{i1}(b)U\}|$$

is maximal, and so on. In this way we get elements $x_{i1}(b),\ldots,x_{ib}(b)$ for $i = 1,2,\ldots$ Now define $c_n = x_{i1}(b)$ for those n such that $2^i < n \leq 2^{i+1}$, $d_n^{-1} \in x_{i2}(b)U$. Similarly define $c_n = x_{i2}(b)$ for those n such that $2^i < n \leq 2^{i+1}$, $d_n^{-1} \in x_{i2}(b)U$, $d_n^{-1} \notin x_{i1}(b)U$ and so on. Let I_1 be the set of indices for which c_n is defined as above. For $n \in I_2 = \mathbb{N} \setminus I_1$ put $c_n = e$. Since we may assume that d is bounded by one we find that $\delta \leq \overline{\lim_{N \to \infty}} 1/N \sum_{n \leq N} d(c_n,d_n) < \delta/2 + \overline{\lim}\ 1/N\ |I_2 \cap [1,N]| = \delta/2 + \bar{d}(I_2)$ ($\bar{d}$ denotes the outer density). It follows that $\bar{d}(I_2) > \delta/2$. We make this construction for each b and find sets $I_2(b)$. Now choose an increasing sequence of indices $N_1 = 0 < N_2 < \ldots$ such that $1/(N_{k+1} - N_k)\ |I_2(k) \cap (N_k, N_{k+1}]| > \delta/2$ and each N_k is of the form 2^{j_k}.

For $n \in I_2(b)$ with $N_b \leq 2^i < n \leq 2^{i+1} \leq N_{b+1}$ choose the smallest number $j \in \mathbb{N}$ such that $d_n^{-1} \in x_j U$ and put $y_n = x_j$. If $x \in G$, $x_j, x_k \in xV$, then $j = k$ by the definition of the sequence (x_n). It follows that $\{n: 2^i < n \leq 2^{i+1}, n \in I_2(b), y_n \in xV\} \subseteq \{n: 2^i < n \leq 2^{i+1}, n \in I_2(b), d_n^{-1} \in x_j U, d_n^{-1} \notin x_k U \ \forall k < j\}$. By construction of the x_j this set has at most $2^i/(b+1)$ elements. Put $\bar{I}_2 = \bigcup_{k=1}^{\infty} (N_k, N_{k+1}] \cap I_2(k)$. The preceding argument shows that for any $\gamma > 0$ and $N \geq N(\gamma)$ we have $1/N |\{n \leq N : n \in \bar{I}_2 : y_n \in xV\}| < \gamma$ for all $x \in G$. Now choose a sequence $\{y_n: n \in \mathbb{N} \setminus \bar{I}_2\}$ such that the sets $\{y_n U: n \in \mathbb{N} \setminus \bar{I}_2\}$ are pairwise disjoint. Then it is easily seen that the sequence (y_n) is L^2-u.d. in G. On the other hand $d_n y_n \in U^{-1}$ for $n \in \bar{I}_2$. Since $\bar{I}_2$ has positive outer density it follows that $(d_n y_n)$ is not L^2-u.d. in G, consequently $(d_n) \notin C(L^2(G))$. q.e.d.

Remarks: Theorem 3 implies that $M(L^2(G)) \neq \emptyset$ for any non compact group. $M(L^2(G)) \subseteq M(G)$ just for compact groups (then equality holds, also in the non-separable case (both sets are empty)). Denote by N(G) the intersection of all kernels of finite dimensional unitary representations then we can show: If $M(G) \neq \emptyset$ then M(G) is not a subset of $M(L^2(G))$ if and only if G is not compact and G/N(G) is compact: If G/N(G) is compact then replacing $(x_n) \in M(G)$ by (y_n) such that $x_n y_n^{-1} \in N(G)$ and that $(y_n) \subseteq K$ compact we have $(y_n) \in M(L^2(G)) \setminus M(G)$ if G is not compact (Th. 3). If G/N is not compact any compact set K in G has measure 0 considered as a subset of the Bohr compactification of G. Then it is easy to see that for $(x_n) \in M(G)$ $1/N \sum_{n \leq N} C_{xK}(x_n) \to 0$ uniformly in $x \in G$ i.e. $(x_n) \in M(L^2(G))$ by Th. 3.

If $(c_n) \in C_f(G)$ then we are able to prove that $(x_n c_n) \in M(L^2(G)$ for any $(x_n) \in M(L^2(G)$ iff there exists a compact neighbourhood of e such that $\bigcup_n c_n V c_n^{-1}$ has compact closure in G. The closure of this subset of $C_f(G)$ consists exactly of these (c_n) such that $(x_n) \in M(L^2(G))$ implies

that $(x_n c_n) \in M(L^2(G))$ (see also [2]). It follows that $(x_n c_n) \in M(L^2(G)$ for any $(c_n) \in C(L^2(G)$, $(x_n) \in M(L^2(G))$ if and only if G has a compact invariant neighbourhood U ($x^{-1}Ux = U$ for all $x \in G$). For M(G) this is true in general, [9] Satz 11. For $C(L^1(G))$ the result above is not true even for groups having a compact invariant neighbourhood (see [9] p. 222) but holds if G has a basis at e of invariant neighbourhoods, [9], Satz 12.

References

[1] Kuipers, L., Niederreiter, H.: Uniform distribution of sequences, John Wiley & Sons, New York (1974).

[2] Losert, V.: Almost constant sequences of transformations, Monatsh. Math. 85, 105-113 (1978).

[3] Losert, V.: Uniformly distributed sequences on compact, separable non metrizable groups, Acta Sci. Math. 40 Fasc. 1-2, 107-110 (1978).

[4] Losert, V., Rindler, H.: Teilfolgen gleichverteilter Folgen, Crelle J., to appear.

[5] Losert, V., Rindler, H.: Uniform distribution and the mean ergodic theorem, Inventiones Math., to appear.

[6] Rauzy, G.: Etude de quelques ensembles de fonction définis par des proprietés de moyenne, Théorie des Nombres, Univ. Bordeaux, 1972/73, Exp. 20.

[7] Rauzy, G.: Propriétés statistiques de suites arithmétiques, Presses Univeritaires de France, le mathematicien 15 (1976).

[8] Rindler, H.: Uniformly distributed sequences in quotient groups, Acta Sci. Math. 38, 153-156 (1976).

[9] Rindler, H.: Gleichverteilte Folgen in lokalkompakten Gruppen, Monatsh. f. Math. 82, 207-235 (1976).

[10] Rindler, H.: Fast konstante Folgen, Acta Arithmetica, to appear.

[11] Rindler, H.: Fast konstante Folgen II, Anzeiger Österr.Akad.Wiss. to appear.

Losert Viktor, Rindler Harald, Inst.f.Math.
Strudlhofgasse 4, A-1090 Wien, Austria

Astérisque

DAVID W. MASSER

Some recent results in transcendence theory

Astérisque, tome 61 (1979), p. 145-154

<http://www.numdam.org/item?id=AST_1979__61__145_0>

Société Mathématique de France
Astérisque 61 (1979) p. 145-154

SOME RECENT RESULTS IN TRANSCENDENCE THEORY

by

David W. MASSER

INTRODUCTION

This article is divided into parts I, II, and III, dealing respectively with elliptic functions, gamma functions, and Siegel E-functions. In each part we describe some recent results and mention a number of open problems.

I - ELLIPTIC FUNCTIONS

M. Anderson [1], [2] has proved several elliptic analogues of A. Baker's inequalities [3] for linear forms in logarithms of algebraic numbers. Let $\wp(z)$ be a Weierstrass elliptic function with algebraic invariants g_2 and g_3. There is a canonical way of choosing a basis ω_1, ω_2 for the period lattice of $\wp(z)$ (see, e.g. [6] p. 421), and we denote by Π the fundamental parallelogram consisting of all points of the form $\theta_1 \omega_1 + \theta_2 \omega_2$ for real θ_1, θ_2 with $0 \leq \theta_1, \theta_2 < 1$. For $n \geq 1$ let $u_1, \ldots, u_n$ be non-zero points of Π such that $\wp(u_1), \ldots, \wp(u_n)$ are algebraic numbers of heights at most $A \geq 4$ and generate over the rational field $\mathbb{Q}$ and algebraic number field F of degree at most $d \geq 2$. Let $\beta_0, \ldots, \beta_n$ be algebraic numbers of heights at most $B \geq 4$ which generate over F an algebraic number field of degree at most $D \geq 2$ (over $\mathbb{Q}$). Put :

$$\Lambda = \beta_0 + \beta_1 u_1 + \ldots + \beta_n u_n$$

and assume $\Lambda \neq 0$.

All Anderson's results need the additional hypothesis of complex multiplication ; thus throughout this section we shall assume that $\wp(z)$ has complex multiplication over a complex quadratic field K. The main results take the form :

$$\log |\Lambda| > -CD^{\lambda} (\log A)^{\mu} \log B (\log \log B)^{\kappa}$$

where $C > 0$ is effectively computable in terms of g_2, g_3, n and the choice of κ, λ, μ. There are three possibilities for this latter choice ; unconditionally we can take any values satisfying either

$$\kappa > n + 1, \quad \lambda > 4n^2 + n + 3, \quad \mu > n^2 + n$$

or

$$\kappa > n + 2\,,\ \lambda > n^2 + 4n + 6,\ \mu > n^2 + n - 1\ ;$$

while if $n \geq 2$ and one of $u_1, \ldots, u_n$ is a half-period we can suppose merely that :

$$\kappa > n + 1\,,\ \lambda > n^2 + 2n + 3\,,\ \mu > n^2 - n - 1\ .$$

Already this presents us with two apparently very difficult problems ; firstly to remove the term $(\log\log B)^{\kappa}$ from these estimates, and secondly to relax the condition on μ to $\mu > n$. Both of these (and much more) have been solved in the case of linear forms in logarithms of algebraic numbers.

Next, suppose that $1, u_1, \ldots, u_n$ are linearly dependent over the field of algebraic numbers. It has been known for some time that then $u_1, \ldots, u_n$ must be linearly dependent over K . Anderson shows in fact that there exist integers $\rho_1, \ldots, \rho_n$ of K , not all zero, with absolute values at most

$$(cn^2 d^4 (\log d)^3 \log A)^{1/2\,(n-1)}\ ,$$

such that

$$\rho_1 u_1 + \ldots + \rho_n u_n = 0\ .$$

Here $c > 0$ is effectively computable in terms of g_2 and g_3 .

For the rest of this section we shall discuss an interesting feature in the proof of this second result. First we consider the exponential case, due to J.H. Loxton and A.J. Van der Poorten [8] . One approach, not quite theirs, leads to the following problem. Let F be an algebraic number field of degree $d \geq 1$, and for any non-zero α in F define

$$h(\alpha) = \sum_{v} \log \max(1, v(\alpha))\ ,$$

where the sum is taken over all normalized valuations v of F . Recall that there are d archimedean valuations v such that $v(\alpha)$ is the absolute value of one of the conjugates of α , and every other valuation is associated with a prime ideal $\mathfrak{P}$ of F . In the latter case $v(\alpha) = (N\mathfrak{P})^{-k}$ where k is the exact power of $\mathfrak{P}$ dividing the principal ideal generated by α in F , and $N\mathfrak{P}$ is the norm of $\mathfrak{P}$.

Now, it is not too hard to prove that $h(\alpha) = 0$ if and only if α is a root of unity ; this is essentially Kronecker's Theorem about algebraic integers on the unit circle. The problem referred to above is to find a good positive lower bound for $h(\alpha)$, depending only on d , as α runs over all non-zero elements of F that are not roots of unity.

This is solved as follows. If α is not an algebraic integer then $v(\alpha) > 1$ for some non-archimedean valuation v, and this implies $v(\alpha) \geq 2$, so that we have the lower bound $h(\alpha) \geq \log 2$. On the other hand, if α is an algebraic integer, then, assuming for the moment that α is of exact degree d with conjugates $\alpha_1, \ldots, \alpha_d$, we see that

$$\exp h(\alpha) = \prod_{i=1}^{d} \max(1, |\alpha_i|) .$$

It is a classical problem to find good lower bounds for the right-hand side of this equation, and until recently the best estimate was due to P.E. Blanksby and H.L. Montgomery [4].
They showed that if α is not a root of unity, then

$$\prod_{i=1}^{d} \max(1, |\alpha_i|) > 1 + (52d \log 6d)^{-1} .$$

We deduce that if $d \geq 2$ then

$$h(\alpha) > c(d \log d)^{-1} \qquad (*)$$

for some absolute constant $c > 0$, and it is easy to check that this remains valid even when α has degree less than d. It follows that (*) is valid for any non-zero α in F that is not a root of unity.

In 1977 C.L. Stewart found a new proof of (*), with a slightly smaller value of c, by applying techniques from transcendence theory (see [12]). Recently, E. Dobrowolski used similar methods to obtain a significant improvement on these estimates, in which the order of magnitude $(d \log d)^{-1}$ is replaced by $(\log \log d / \log d)^3$.

To explain the elliptic analogue, we note that h is a natural height function associated with the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers. This group can be identified with the curve $\mathcal{C}$ of points (x, y) satisfying $xy = 1$, for example. Then h is defined on the subgroup $\mathcal{C}(F) = F^\times$ of points (α, β) on $\mathcal{C}$ with coordinates α, β in F.
Moreover h vanishes exactly at the torsion points of $\mathcal{C}(F)$. Now let $\mathcal{E}$ denote the elliptic curve associated with $\wp(z)$, consisting of points (x, y) satisfying $y^2 = 4x^3 - g_2 x - g_3$ together with the point at infinity ∞.
This curve has an additive group structure, and, provided g_2 and g_3 lie in the algebraic number field F, so has the subset $\mathcal{E}(F)$ of points $P = (\alpha, \beta)$ on $\mathcal{E}$ with coordinates α, β in F (together with $P = \infty$).
There is a natural height function $\hat{h}$ on $\mathcal{E}(F)$ which vanishes exactly at the torsion points of $\mathcal{E}(F)$; this is the Tate height, defined in the following way.

For a finite point $P = (\alpha, \beta)$ of $\mathcal{E}(F)$ let

$$h(P) = \sum_{v} \log \max(1, v(\alpha), v(\beta)) \quad ,$$

where the sum is as before, and put $h(\infty) = 0$. Then for any P in $\mathcal{E}(F)$ the limit

$$\hat{h}(P) = \lim_{m \to \infty} m^{-2} h(mP)$$

can be shown to exist and have the required vanishing properties.

The problem we have to solve for this height function $\hat{h}$ is the same as before ; to find a good positive lower bound for $\hat{h}(P)$, depending only on the degree d of F , as P runs over all non-torsion points of $\mathcal{E}(F)$. The solution seems difficult if the approach of Blanksby-Montgomery is adopted. But by modifying the methods introduced by Stewart, Anderson was able to establish the following result. When $\wp(z)$ has complex multiplication, there is a constant $c > 0$, effectively computable in terms of g_2 and g_3 , such that for any algebraic number field F of degree at most $d \geq 2$ containing g_2 and g_3 we have

$$\hat{h}(P) > c\,(d \log d)^{-3}$$

for any non-torsion point P in $\mathcal{E}(F)$.

It is an interesting problem to extend this result to elliptic curves without complex multiplication. An easy argument shows that always $\hat{h}(P) > \exp(-cd^2)$ for some c independent of d , but it seems hard to prove $\hat{h}(P) > cd^{-\kappa}$ for some absolute constant κ . One might even ask whether $\hat{h}(P)$ is bounded below independently of d . The analogous question for $h(\alpha)$ was asked some time ago by D.H. Lehmer, but it remains unanswered to this day.

II - GAMMA FUNCTIONS

G.V. Chudnovsky's proof [5] of the transcendence of $\Gamma(1/4)$ shows in fact that the numbers π, $\Gamma(1/4)$ are algebraically independent over $\mathbb{Q}$ (see also [14]) . A similar remark applies to $\Gamma(1/3)$. By easy calculations we deduce that $\Gamma(x)$ is transcendental for the following values of x with $0 < x < 1$;

$$1/6\ ,\ 1/4,\ 1/3,\ 1/2,\ 2/3,\ 3/4,\ 5/6\ .$$

Naturally, the next problem is to complete the Farey series of order 6 by adding the values $1/5, 2/5, 3/5, 4/5$ to the list. This problem seems intimately connected, via the Chowla-Selberg relations, to the perhaps no more difficult question of the algebraic independence of periods of abelian varieties with complex multiplication. Recently P. Deligne found an extensive family of new algebraic relations between these periods, thereby substantially reducing the upper bound for the transcendence degree of the field they generate. Chudnovsky in his talk at the Helsinki Congress conjectured that the reduced upper bound is the correct value of the transcendence degree ; this amounts to saying that there are essentially no more algebraic relations. All that is known so far is that the transcendence degree is always at least 2 . This implies, for example, that at least two of the numbers π, $\Gamma(1/5)$, $\Gamma(2/5)$ are algebraically independent over $\mathbb{Q}$.

On a less exciting level, one can consider linear independence. In [9] I asked if the values $B(m/5, n/5)$ of the classical beta function span over the field of algebraic numbers a vector space of dimension 6 as m and n run over all positive integers. Recently I proved that this is so ; writing $\theta = \Gamma(1/5)$, $\Phi = \Gamma(2/5)$ we deduce that the numbers

$$1,\ \pi,\ \theta^2/\Phi,\ \pi\Phi/\theta^2,\ \theta\Phi^2/\pi\ ,\ \pi^2/\theta\Phi^2$$

are linearly independent over the field of algebraic numbers.

Finally let us mention an interesting quantitative sharpening of Chudnovsky's results. A subfield F of $\mathbb{C}$ that is finitely generated over $\mathbb{Q}$ is said to be of finite transcendence type if for any $\theta_1, \ldots, \theta_n$ in F there exist $C > 0$, $\tau > 0$ with the following property. For any polynomial P in $\mathbb{Z}[x_1, \ldots, x_n]$ with degree at most $d \geq 1$ and coefficients at most $H \geq 2$ in absolute value such that $P(\theta_1, \ldots, \theta_n) \neq 0$, we have (+)

$$\log |\, P(\theta_1, \ldots, \theta_n) \,| > - C (d + \log H)^{\tau} \ . \qquad (*)$$

(it suffices to check this for a single transcendence basis $\theta_1, \ldots, \theta_n$ of F over $\mathbb{Q}$) .

(+) It is probably too late to change the nomenclature now, but it would have been nice to define the transcendence type of F as the infimum τ_0 of all numbers τ such that (*) holds. If then (*) happens to hold for $\tau = \tau_0$ we could have said that F has strict transcendence type τ_0 (cf. the order of an entire function).

Classical results show that $\mathbb{Q}(e)$, $\mathbb{Q}(\pi)$, $\mathbb{Q}(e^{\pi})$ are all of finite transcendence type (and much more); but until recently no such field of transcendence degree 2 was known. The work of Chudnovsky provides several examples, including $\mathbb{Q}(\pi, \Gamma(1/4))$ and $\mathbb{Q}(\pi, \Gamma(1/3))$.

III - E-FUNCTIONS

Recall that $f(z) = \sum_{k=0}^{\infty} \alpha_k z^k/k!$ is defined to be an E-function if there is an algebraic number field F and a constant $c > 0$ such that, for each $m \geq 1$, there exists a positive integer $d_m \leq c^m$ such that $d_m \alpha_0, \ldots, d_m \alpha_m$ are algebraic integers of F with all their conjugates of absolute values at most c^m. The fundamental theorem of Siegel-Shidlovsky [11] is as follows. For $n \geq 1$ let $f_1(z), \ldots, f_n(z)$ be E-functions, algebraically independent over $\mathbb{C}(z)$, that satisfy a system of linear differential equations

$$f_i'(z) = q_{i0}(z) + \sum_{j=1}^{n} q_{ij}(z) f_j(z) \qquad (1 \leq i \leq n)$$

with rational functions $q_{ij}(z)$ in $\mathbb{C}(z)$. Then for any non-zero algebraic number α distinct from the poles of the $q_{ij}(z)$, the values $f_1(\alpha), \ldots, f_n(\alpha)$ are algebraically independent over $\mathbb{Q}$.

In 1962, S. Lang obtained a quantitative version of this (see [7]). For brevity put $\theta_i = f_i(\alpha)$ $(1 \leq i \leq n)$. He proved that for any $d \geq 1$ there exist constants $c > 0$, $C > 0$, depending only on d, α, and the functions $f_1(z), \ldots f_n(z)$, with c independent of d, having the following property. For any non-zero polynomial P in $\mathbb{Z}[x_1, \ldots, x_n]$ of degree at most d and coefficients with absolute values at most $H \geq 2$, we have

$$|P(\theta_1, \ldots, \theta_n)| > CH^{-cd^n}.$$

Since C may depend on d, this does not show that the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ has finite transcendence type; and indeed this has not been proved even for the simple example $\mathbb{Q}(e, e^{\sqrt{2}})$.
Recently, Ju. V. Nesterenko [10] published a proof that we can take

$$C^{-1} = \exp\exp(c' d^{2n} \log d)$$

for some c' depending only on α and $f_1(z), \ldots, f_n(z)$.

This relatively weak estimate reflects the fact that Siegel's method is designed to operate with linear independence of power products rather than directly with algebraic independence itself. Incidentally, it does not seem clear from Nesterenko's proof that c' is in fact effectively computable in all cases, and it would be an interesting exercise to verify this point.

The main part of Nesterenko's paper is concerned with estimates for zeroes of functions that are polynomials in $f_1(z), \ldots, f_n(z)$. The arguments are algebraic in nature rather than analytic, and the paper contains techniques from commutative algebra that should be applicable elsewhere in transcendence theory. Recently, Dale Brownawell and myself have obtained similar zero-estimates for solutions of certain non-linear differential equations. Among other things these lead to a quantitative version of the Schneider-Lang Theorem [7], [13].

Let us first recall this result. Let $f_1(z), \ldots, f_n(z)$ be meromorphic functions of finite growth order ρ. Suppose they satisfy differential equations of the form

$$f_i'(z) = P_i(f_1(z), \ldots, f_n(z)) \qquad (1 \leq i \leq n),$$

where $P_1, \ldots, P_n$ are polynomials with coefficients in an algebraic number field F of degree at most $d \geq 1$. Suppose further that at least two of $f_1(z), \ldots, f_n(z)$ are algebraically independent over F. Then if $m > 2\rho d$ and $w_1, \ldots, w_m$ are any distinct points at which $f_1(z), \ldots, f_n(z)$ are analytic, not all the values $f_i(w_j)$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$ can lie in F.

Thus, if β_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq m)$ are elements of F with heights at most $B \geq 1$, the expression

$$\mathcal{U} = \max |f_i(w_j) - \beta_{ij}|$$

never vanishes, and we can ask for a positive lower bound for $\mathcal{U}$ as a function of B. In fact, a further hypothesis is needed before we can give a satisfactory answer.

For, if $\lambda_1, \ldots, \lambda_n$ are complex numbers algebraically independent over $\mathbb{Q}$, the constant functions $f_i(z) = \lambda_i$ $(1 \leq i \leq n)$ satisfy all the conditions of the theorem, and, if also $\lambda_1, \ldots, \lambda_n$ are arbitrarily well approximated by numbers of F, then $\mathcal{U}$ can be an equally arbitrarily small function of B.

However, let us exclude this possibility by assuming that there exists an additional point w_0, at which $f_1(z), \ldots, f_n(z)$ are analytic, such that $f_1(w_0), \ldots, f_n(w_0)$ lie in F. Then we can show that given any $\varepsilon > 0$, there is a constant $c > 0$, depending in a simple way on n and ε, such that if $m > c\rho d$ and $w_1, \ldots, w_m$ are points as above, then

$$\mathcal{U} > C \exp(-B^{\varepsilon})$$

for some $C > 0$ depending only on $f_1(z), \ldots, f_n(z)$, $w_0, \ldots, w_m$, ε, and F.

REFERENCES

[1] M. Anderson Inhomogeneous linear forms in algebraic points of an elliptic function, Transcendence theory : advances and applications (Eds. A. Baker and D.W. Masser), Academic Press, London, (1977), 121 - 143.

[2] M. Anderson Linear forms in algebraic points of an elliptic function, Ph. D. thesis, University of Nottingham, (1978).

[3] A. Baker The theory of linear forms in logarithms, Transcendence theory : advances and applications (Eds. A. Baker and D.W. Masser), Academic Press, London, (1977), 1 - 27.

[4] P.E. Blanksby and H.L. Montgomery
Algebraic integers near the unit circle, Acta Arith. 18, (1971), 355 - 369.

[5] G.V. Chudnovsky
Algebraic independence of constants connected with exponential and elliptic functions (in Russian), Dopovidi Akad. Nauk. USSR, Ser. A, (1976), N° 8.

[6] E.T. Copson An introduction to the theory of functions of a complex variable, Oxford, (1935).

[7] S. Lang Introduction to transcendental numbers, Addison-Wesley, Reading Mass., (1966).

[8] J.H. Loxton and A.J. Van der Poorten
Multiplicative relations in number fields, Bull. Australian Math. Soc. 16, (1977), 83 - 98.

[9] D.W. Masser The transcendence of certain quasi-periods associated with Abelian functions in two variables, Compositio Math. 35, (1977), 239 - 258.

[10] Ju.V. Nesterenko
Bounds on the order of zeroes of a class of functions and their application to the theory of transcendental numbers (in Russian), Izv. Akad. Nauk. USSR, Ser. Mat. 41, (1977), 253 - 284.

[11] A.B. Shidlovsky
On a criterion for the algebraic independence of a class of entire functions (in Russian), Izv. Akad. Nauk. USSR, Ser. Mat. 23, (1959), 35 - 66.

[12] C.L. Stewart Algebraic integers whose conjugates lie near the unit circle, Bull. Soc. Math. France, 106, (1978), 169 - 176.

[13] M. Waldschmidt
Nombres transcendants, Lecture Notes in Math. N° 402, Springer, Berlin, (1974).

[14] M. Waldschmidt
Les travaux de G.V. Chudnovsky sur les nombres transcendants, Sém. Bourbaki, N° 488, (1976).

David MASSER
Department of Mathematics
University of Nottingham
NOTTINGHAM
G. B.

Astérisque

HARALD NIEDERREITER

Nombres pseudo-aléatoires et équirépartition

Astérisque, tome 61 (1979), p. 155-164

<http://www.numdam.org/item?id=AST_1979__61__155_0>

Société Mathématique de France
Astérisque 61 (1979) p. 115-164

NOMBRES PSEUDO-ALÉATOIRES ET ÉQUIRÉPARTITION

par

Harald NIEDERREITER

> Nous voulons, tant ce feu nous brûle le cerveau,
> Plonger au fond du gouffre, Enfer ou Ciel, qu'
> importe? Au fond de l'Inconnu pour trouver du
> *nouveau*!
>
> Baudelaire, *Le Voyage*

La nécessité de produire des "nombres aléatoires" résulte dans le cadre de la simulation de processus complexes et, en particulier, dans la méthode de Monte-Carlo que l'on peut décrire brèvement comme une technique numérique basée sur des procédés d'échantillonnage. Un problème se pose naturellement, à savoir comment mettre à exécution l'échantillonnage concret dans une application spécifique d'une telle méthode. Une définition adéquate d'une suite de nombres aléatoires serait utile pour résoudre cette question pratique.

Il y a plusieurs tentatives bien connues d'arriver à une définition satisfaisante d'une suite de nombres aléatoires (voir [3], [7], [8]). Pour la plupart, ces tentatives sont fondées sur le principe de Venn [21] qui postule qu'une telle suite satisfasse certaines propriétés de distribution. Normalisons les termes d'une suite et supposons désormais qu'ils appartiennent à l'intervalle unité $I = [0, 1]$. Une condition *sine qua non* pour le caractère aléatoire d'une suite

$x_0, x_1, \ldots$ est l'équirépartition dans I. Mais cela ne suffit pas, car il faut aussi avoir égard à l'exigence que les termes successifs de la suite soient indépendants. Ceci nous amène à considérer la "suite-chenille" des s-uplets $\underline{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n = 0, 1, \ldots$, et la condition que cette suite soit équirépartie dans l'hypercube unité $I^s = [0, 1]^s$. Si l'on impose cette condition pour tout entier $s \geq 1$, il revient au même de demander que la suite scalaire $x_0, x_1, \ldots$ soit *complètement équirépartie.*

Par conséquent, on peut regarder une suite complètement équirépartie comme modèle de suite de nombres aléatoires, au moins pour les applications de la méthode de Monte-Carlo dans lesquelles interviennent seulement les propriétés de distribution, par exemple pour l'intégration numérique. On connaît de nombreuses constructions de suites complètement équiréparties, la plus utile du point de vue numérique étant celle de Knuth [2] qui emploie des fractions dyadiques. Rauzy [20] a montré le résultat suivant; si f est une fonction entière non polynomiale qui prend des valeurs réelles sur l'axe réel et verifie la condition de croissance

$$\overline{\lim_{r \to \infty}} \frac{\log \log M(f;r)}{\log \log r} < \frac{5}{4} \quad \text{où} \quad M(f;r) = \sup_{|z| \leq r} |f(z)| ,$$

alors la suite des parties fractionnaires $\{f(1)\}, \{f(2)\}, \ldots, \{f(n)\}, \ldots$ est complètement équirépartie. Levine [6] a construit, pour tout nombre transcendant $\beta > 1$, un nombre $\alpha \in \mathbb{R}$ tel que la suite des parties fractionnaires $\{\alpha\beta\}, \{\alpha\beta^2\}, \ldots, \{\alpha\beta^n\}, \ldots$ est complètement équirépartie. Voir [19] pour les constructions classiques de suites complètement équiréparties.

Quoique les suites complètement équiréparties soient intéressantes en ce qui concerne l'aspect théorique, il est préférable, pour les calculs très étendus de Monte-Carlo, d'utiliser des suites qui sont fabriquées dans l'ordinateur par des algorithmes rapides et simples. Bien entendu, une suite déterministe produite de cette manière ne se qualifie pas de suite de nombres aléatoires. Néanmoins, elle peut respecter plusieurs critères de caractère aléatoire adaptés à des besoins

particuliers. Dans ce cas, les termes d'une telle suite déterministe s'appellent *nombres pseudo-aléatoires*.

L'algorithme le plus efficace et commode pour l'obtention de nombres pseudo-aléatoires est le *générateur multiplicatif (homogène ou mixte)* proposé par Lehmer [5]. Soient m, λ, r et y_0 des entiers avec $m \geq 3$, $2 \leq \lambda < m$, $0 \leq y_0 < m$, λ et m premiers entre eux et $(\lambda - 1)y_0 + r \not\equiv 0 \pmod m$. Alors on engendre une suite d'entiers $y_0, y_1, \ldots$ par la récurrence

$$y_{n+1} \equiv \lambda y_n + r \pmod m, \quad n = 0,1, \ldots,$$

en observant la limitation $0 \leq y_n < m$ pout tout n. Une suite de nombres $x_0, x_1, \ldots$ appartenant à l'intervalle unité I est dérivée en posant $x_n = y_n/m$ pour tout n. Les nombres x_n sont déjà les nombres pseudo-aléatoires engendrés par le générateur multiplicatif. Habituellement, on prend pour m un grand nombre premier ou une grande puissance de 2. On appelle m le *module* et λ le *multiplicateur*.

On peut étudier les propriétés de distribution d'une suite $x_0, x_1, \ldots$ engendrée par le générateur multiplicatif en utilisant un modèle probabiliste. Fixons $\Theta \in \mathbb{R}$ et considérons la récurrence

$$x_{n+1} = \{\lambda x_n + \Theta\}, \quad n = 0,1, \ldots,$$

où $x_0 \in I$ est arbitraire. Or, la transformation

$$T : x \in I \mapsto \{\lambda x + \Theta\}$$

est ergodique par rapport à la mesure de Lebesgue. On en déduit que, pour presque toute valeur de départ $x_0 \in I$, la suite $(x_n) = (T^n x_0)$, $n = 0,1, \ldots$, est équirépartie dans I.

Quant à l'épreuve d'indépendance des termes successifs de la suite $x_0, x_1, \ldots$ ci-dessus, on voit aisément que la suite $\underline{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n = 0,1, \ldots,$

n'est jamais équirépartie dans I^s pour $s \geq 2$. Mais cette suite est en un certain sens presque sûrement "asymptotiquement" équirépartie dans I^s. Écrivons $\underline{x}_n(\lambda)$ au lieu de $\underline{x}_n$ pour souligner que $\underline{x}_n$ dépend de λ. Alors Franklin [1] a montré le résultat suivant: si f est une fonction continue de I^s dans $\mathbb{R}$, on a pour presque tout $x_0 \in I$

$$\lim_{\lambda \to \infty} \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} f(\underline{x}_n(\lambda)) = \int_{I^s} f(\underline{t}) d\underline{t}.$$

Pour $\theta = 0$ le théorème central-limite "asymptotique" de Yermakov [22] précise ce résultat. Soit f une fonction continue de I^s dans $\mathbb{R}$ et dénotons par

$$R_N(f, x_0, \lambda) = \frac{1}{N} \sum_{n=0}^{N-1} f(\underline{x}_n(\lambda)) - \int_{I^s} f(\underline{t}) d\underline{t}$$

l'erreur d'intégration. Alors,

$$\lim_{N \to \infty} \lim_{\lambda \to \infty} \text{mes} \left\{ x_0 \in I : R_N(f, x_0, \lambda) < \frac{\sigma u}{\sqrt{N}} \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} dt$$

pour tout $u \in \mathbb{R}$, où la constante σ désigne un certain écart-type dépendant de f. Ces résultats suggèrent que les nombres pseudo-aléatoires engendrés par un générateur multiplicatif devraient montrer un bon comportement concernant les épreuves de distribution, au moins pour certains grands multiplicateurs λ.

Naturellement, il est plus difficile d'établir des résultats effectifs pour des suites spécifiques de nombres pseudo-aléatoires. Le problème de la répartition dans I des termes d'une telle suite étant déjà étudié en détail (voir [9], [10], [12]), considérons maintenant le problème de répartition pour la dimension $s \geq 2$. L'écart entre la fonction de distribution des points $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_{N-1}$ de la suite-chenille et l'équirépartition sur I^s est mesuré par la *discrépance*

$$D_N^{(s)} = \sup_J |F_N(J) - V(J)|,$$

où le sup est étendu à tous les sous-intervalles J de I^s, $F_N(J)$ est N^{-1} fois le nombre d'entiers n tels que $0 \leq n < N$ et $\underline{x}_n \in J$, et V(J) désigne le volume de J. Il faut remarquer que pour la valeur de départ rationnelle $x_0 = y_0/m$ les suites $x_0, x_1, \ldots$ et $\underline{x}_0, \underline{x}_1, \ldots$ sont périodiques avec la même période τ. À cause de cela, il est évident que l'on n'utilise les terms x_n et $\underline{x}_n$ de ces suites que pour $0 \leq n < \tau$. Par conséquent, on ne considère $D_N^{(s)}$ que pour $1 \leq N \leq \tau$.

Pour estimer $D_N^{(s)}$, il faut établir au préalable une inégalité (voir [14]) qui met en évidence le lien entre la discrépance de certaines suites et les sommes exponentielles associées. Ce résultat améliorera dans ce cas spécial une inégalité de type général (voir [4], [18]). Soit M l'ensemble des treillis $\underline{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ avec $-m/2 < h_j \leq m/2$ pour $1 \leq j \leq s$ et $\underline{h} \neq \underline{0}$. Posons $r(h,m) = m \sin(\pi|h|/m)$ pour $h \neq 0$, $r(0,m) = 1$, $r(\underline{h},m) = r(h_1,m) \ldots r(h_s,m)$, et $e(t) = e^{2\pi i t}$ pour $t \in \mathbb{R}$.

LEMME. - *Pour tout générateur multiplicatif avec module* m *et toute dimension* $s \geq 2$ *on a*

$$D_N^{(s)} \leq \frac{s}{m} + \sum_{\underline{h} \in M} \frac{1}{r(\underline{h},m)} \left| \frac{1}{N} \sum_{n=0}^{N-1} e(\underline{h} \cdot \underline{x}_n) \right|$$

quel que soit l'entier positif N.

Ainsi le problème de l'estimation de $D_N^{(s)}$ est réduit au traitement des sommes exponentielles qui surgissent dans le résultat précédent. Les sommes exponentielles de ce type étaient déjà étudiées par l'auteur (voir [11], [12]). On peut alors donner certaines améliorations de ces résultats antérieurs. Dans le cas d'un générateur multiplicatif homogène (c'est-à-dire $r \equiv 0 \pmod m$) on arrive à l'inégalité suivante.

THÉORÈME 1. - *Soient* μ *l'ordre de* $\lambda + m\mathbb{Z}$ *dans le groupe multiplicatif* $(\mathbb{Z}/m\mathbb{Z})^*$ *et* b *un entier avec* b *et* m *premiers entre eux. Alors on a*

$$\left| \sum_{n=0}^{\mu-1} e(b\lambda^n/m) \right| \leq \sqrt{m} - \frac{\mu}{\phi(m)}(\sqrt{m} - 1)$$

et

$$\left| \sum_{n=0}^{N-1} e(b\lambda^n/m) \right| < \sqrt{m}\left(\frac{2}{\pi}\log \mu + \frac{2}{5}\right) + N\left(\frac{\sqrt{m}}{\mu} - \frac{\sqrt{m}-1}{\phi(m)}\right)$$

pour $1 \leq N < \mu$.

Dans le cas d'un générateur multiplicatif mixte (c'est-à-dire $r \not\equiv 0 \pmod m$) on applique le résultat suivant.

THÉORÈME 2. - *Soient* $y_0, y_1, \ldots$ *la suite d'entiers engendrés par un générateur multiplicatif et* b *un entier avec* b *et* m *premiers entre eux. Alors on a*

$$\left| \sum_{n=0}^{\tau-1} e(by_n/m) \right| \leq \left(\frac{m\tau - \tau^2}{\mu}\right)^{1/2}$$

et

$$\left| \sum_{n=0}^{N-1} e(by_n/m) \right| < \left(\frac{m\tau}{\mu}\right)^{1/2}\left(\frac{2}{\pi}\log \tau + \frac{2}{5}\right) + \frac{N}{\tau}\left(\frac{m\tau - \tau^2}{\mu}\right)^{1/2}$$

pour $1 \leq N < \tau$.

Ces inégalités conduisent à des bornes supérieures de la discrépance $D_N^{(s)}$. On introduit une légère modification d'une définition donnée antérieurement (voir [13], [14]). En effet, posons

$$\rho^{(s)}(\lambda, m) = \min r(\underline{h}),$$

où le minimum est étendu à tous les treillis $\underline{h} = (h_1, \ldots, h_s) \in M$ avec $h_1 + h_2\lambda + \ldots + h_s\lambda^{s-1} \equiv 0 \pmod m$ et $r(\underline{h})$ désigne l'entier positif $r(\underline{h}) = \max(1, 2|h_1|) \ldots$

$\max(1, 2|h_s|)$. Utilisons C_s pour dénoter une constante positive qui dépend seulement de la dimension s, mais qui peut atteindre des valeurs différentes selon le cas.

THÉORÈME 3. - Si le module m est un nombre premier, on a

$$D_\tau^{(s)} \leq \frac{(m-\tau)}{\tau}^{1/2}\left(\frac{2}{\pi}\log m + \frac{7}{5}\right)^s + \frac{C_s \log^s m}{\rho^{(s)}(\lambda,m)}$$

et

$$D_N^{(s)} \leq C_s\left(\frac{m^{1/2}(\log m)^{s+1}}{N} + \frac{\log^s m}{\rho^{(s)}(\lambda,m)}\right) \quad \text{pour} \quad 1 \leq N < \tau.$$

La borne supérieure de $D_\tau^{(s)}$ suggère que l'on choisisse un multiplicateur qui donne la valeur maximale de τ, c'est-à-dire un multiplicateur qui est une racine primitive mod m. Dans ce cas, on obtient

$$D_\tau^{(s)} \leq \frac{C_s \log^s m}{\rho^{(s)}(\lambda,m)}.$$

On en déduit qu'une suite de nombres pseudo-aléatoires engendrés par un générateur multiplicatif pour laquelle s termes successifs sont stochastiquement presque indépendants est obtenue en choisissant un grand module premier m et un multiplicateur λ qui est une racine primitive mod m et donne une grande valeur de $\rho^{(s)}(\lambda,m)$. D'ailleurs, on peut montrer qu'il existe, pour tout $s \geq 2$ et tout module premier m, une racine primitive λ_0 mod m telle que

$$D_\tau^{(s)} \leq C_s\, m^{-1} \log^s m \log\log m,$$

où $\tau = m - 1$. Il est remarquable que cet ordre de grandeur est très proche de la valeur la plus faible connue (et conjecturée) de la discrépance de $m-1$ points de I^s (voir [4], [17]).

On peut établir des résultats analogues pour un module m qui est une puissance d'un nombre premier (voir [14], [15], [17]) ou une puissance de 10 (voir [16]). De plus, il y a une borne inférieure de $D_N^{(s)}$ qui indique que le nombre $\rho^{(s)}(\lambda,m)$ fournit une mesure appropriée de la qualité des paramètres λ et m à l'égard de la dimension s.

THÉORÈME 4. - *Pour tout module* m *et tout multiplicateur* λ *on a*

$$D_N^{(s)} \geq \frac{C_s}{\rho^{(s)}(\lambda,m)}$$

quel que soit l'entier N, $1 \leq N \leq \tau$.

RÉFÉRENCES

[1] J.N. FRANKLIN. - Deterministic simulation of random processes. Math. Comp. 17, 28-59 (1963).

[2] D.E. KNUTH. - Construction of a random sequence. Nordisk Tidskr. Informations-Behandling (BIT) 5, 246-250 (1965).

[3] D.E. KNUTH. - The Art of Computer Programming, Vol.2: Seminumerical Algorithms. Addison-Wesley, Reading, Mass., 1969.

[4] L. KUIPERS et H. NIEDERREITER. - Uniform Distribution of Sequences. Wiley-Interscience, New York, 1974.

[5] D.H. LEHMER. - Mathematical methods in large-scale computing units. Proc. 2nd Sympos. on Large-Scale Digital Calculating Machinery (Cambridge, Mass., 1949), pp. 141-146. Harvard University Press, Cambridge, Mass., 1951.

[6] M.B. LEVINE. - Sur l'équirépartition de la suite $\{\alpha\lambda^x\}$ (en russe). Mat. Sb. 98, 207-222 (1975).

[7] P. MARTIN-LÖF. - The definition of random sequences. Information and Control 9, 602-619 (1966).

[8] M. MENDÈS FRANCE. - Suites de nombres au hasard (d'après Knuth). Sém. Théorie des Nombres 1974-1975, Univ. Bordeaux, Exp. 6.

[9] H. NIEDERREITER. - On the distribution of pseudo-random numbers generated by the linear congruential method. Math. Comp. 26, 793-795 (1972).

[10] H. NIEDERREITER. - On the distribution of pseudo-random numbers generated by the linear congruential method. II. Math. Comp. 28, 1117-1132 (1974).

[11] H. NIEDERREITER. - Some new exponential sums with applications to pseudo-random numbers. Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. János Bolyai, Vol. 13, pp. 209-232. North-Holland, Amsterdam, 1976.

[12] H. NIEDERREITER. - On the distribution of pseudo-random numbers generated by the linear congruential method. III. Math. Comp. 30, 571-597 (1976).

[13] H. NIEDERREITER. - Statistical independence of linear congruential pseudo-random numbers. Bull. Amer. Math. Soc. 82, 927-929 (1976).

[14] H. NIEDERREITER. - Pseudo-random numbers and optimal coefficients. Advances in Math. 26, 99-181 (1977).

[15] H. NIEDERREITER. - The serial test for linear congruential pseudo-random numbers. Bull. Amer. Math. Soc. 84, 273-274 (1978).

[16] H. NIEDERREITER. - Statistical tests for linear congruential pseudo-random numbers. COMPSTAT 1978: Proceedings in Computational Statistics (Leiden, 1978), pp. 398-404. Physica-Verlag, Vienne, 1978.

[17] H. NIEDERREITER. - Quasi-Monte Carlo methods and pseudo-random numbers. Bull. Amer. Math. Soc. 84 (à paraître).

[18] H. NIEDERREITER et W. PHILIPP. - Berry-Esseen bounds and a theorem of Erdös and Turán on uniform distribution mod 1. Duke Math. J. 40, 633-649 (1973).

[19] A.G. POSTNIKOV. - Modelage arithmétique de processus aléatoires (en russe). Trudy Mat. Inst. Steklov. 57 (1960).

[20] G. RAUZY. - Fonctions entières et répartition modulo un, II. Bull. Soc. Math. France 101, 185-192 (1973).

[21] J. VENN. - The Logic of Chance. Macmillan, London, 1876.

[22] S.M. YERMAKOV. - Note sur les suites pseudo-aléatoires (en russe). J.Vyčisl. Mat. i Mat. Fiz. 12, 1077-1082 (1972).

Harald NIEDERREITER
Chair in Pure Mathematics
University of the West Indies
KINGSTON 7
Jamaïque

Ce travail était subventionné par U.S. National Science Foundation Grant MCS-7701699A01.

Astérisque

JOSEPH OESTERLÉ

Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée

Astérisque, tome 61 (1979), p. 165-167

<http://www.numdam.org/item?id=AST_1979__61__165_0>

Société Mathématique de France
Astérisque 61 (1979) p. 165-167

VERSIONS EFFECTIVES DU THÉORÈME DE CHEBOTAREV SOUS L'HYPOTHÈSE DE RIEMANN GÉNÉRALISÉE.

par

Joseph OESTERLÉ

Dans [1], Lagarias et Odlyzko démontrent une version du théorème de Chebotarev avec terme d'erreur. Le but de cet article est d'expliciter les constantes numériques intervenant dans ce terme d'erreur, sous l'hypothèse de Riemann généralisée. Nous nous contenterons d'énoncer les résultats; les démonstrations seront publiées ultérieurement.

Soit E/K une extension galoisienne finie de corps de nombres, de groupe de Galois G. Notons n_E et n_K (resp. d_E et d_K) les degrés absolus (resp. les discriminants absolus) de E et K. Soit χ le caractère d'une représentation complexe de dimension finie τ de G. Notons $n(\chi)$ l'entier $n_K\chi(1)$, $\delta(\chi)$ le nombre de fois qu'intervient dans τ la représentation unité de G , et $A(\chi)$ l'entier $d_K N_{K/\mathbb{Q}}(f(\chi))$ où $f(\chi)$ est le conducteur de χ .

Si $\mathfrak{P}$ est un idéal premier de E au-dessus d'un idéal premier $\mathfrak{p}$ de K , notons $D_{\mathfrak{P}}$ et $I_{\mathfrak{P}}$ ses groupes de décomposition et d'inertie, et $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$ l'élément de Frobenius associé à $\mathfrak{P}$. Si $m \in \mathbb{N}$, et si ε est une fonction centrale sur G , la valeur moyenne de ε sur $\sigma_{\mathfrak{P}}^m$ ne dépend que de $\mathfrak{p}$ et est notée $\varepsilon(\sigma_{\mathfrak{p}}^m)$. Soit $L(s,\chi)$ la série L

d'Artin associée à χ . On a:

$$\frac{L'}{L}(s,\chi) = \sum \chi(\sigma_{\mathfrak{p}}^m) N\mathfrak{p}^{-ms} \mathrm{Log}(N\mathfrak{p}) ,$$

où $\mathfrak{p}$ décrit les idéaux premiers de K et m les entiers $\geqslant 1$.

Si ε est une fonction centrale sur G , posons, pour $x \in \mathbb{R}_+^*$:

$$\psi_\varepsilon(x) = \sum_{N\mathfrak{p} \leqslant x, m \geqslant 1} \varepsilon(\sigma_{\mathfrak{p}}^m) \mathrm{Log}(N\mathfrak{p}) .$$

THÉORÈME 1.- Supposons que $L(s,\chi)$ vérifie A.C. (Conjecture d'Artin) et G.R.H. (Hypothèse de Riemann généralisée). Dans ce cas, on a:

$$\forall x \geqslant 1 , \quad \left|\psi_\chi(x) - \delta(\chi)x\right| \leqslant \sqrt{x}\left[\mathrm{LogA}(\chi)\left(\frac{\mathrm{Log}\, x}{\pi} + 2\right) + n(\chi)\left(\frac{\mathrm{Log}^2 x}{2\pi} + 2\right)\right] .$$

THÉORÈME 2.- Soit C une partie de G stable par conjugaison et ε sa fonction caractéristique. Supposons que la fonction ζ_E vérifie G.R.H. et notons $|C|$ et $|G|$ les cardinaux de C et G . On a:

$$\forall x \geqslant 1 , \quad \left|\psi_\varepsilon(x) - \frac{|C|}{|G|}x\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\left[\mathrm{Log}\, d_E \left(\frac{\mathrm{Log}\, x}{\pi} + 2\right) + n_E\left(\frac{\mathrm{Log}^2 x}{2\pi} + 2\right)\right] .$$

THÉORÈME 3.- Sous les hypothèses du théorème 2 , soit $\pi_C(x)$ le nombre d'idéaux premiers $\mathfrak{p}$ de K, non ramifiés dans E , vérifiant $N\mathfrak{p} \leqslant x$, et tels que la classe de conjugaison des substitutions de Frobenius associées à $\mathfrak{p}$ soit contenue dans C . Pour tout $x \geqslant 2$, on a:

$$\left|\pi_C(x) - \frac{|C|}{|G|}\int_2^x \frac{dt}{\mathrm{Log}\, t}\right| \leqslant \frac{|C|}{|G|}\sqrt{x}\left[\mathrm{Log}\, d_E \left(\frac{1}{\pi} + \frac{5,3}{\mathrm{Log}\, x}\right) + n_E\left(\frac{\mathrm{Log}\, x}{2\pi} + 2\right)\right].$$

THÉORÈME 4.- Sous les hypothèses du théorème 3 , on a $\pi_C(x) \geqslant 1$ si $x \geqslant 70\ \mathrm{Log}^2(d_E)$ et $E \neq \mathbb{Q}$.

Sous les hypothèses des théorèmes 1 , 2 , et 3 respectivement, il est possible de donner des formes simplifiées des termes d'erreur, à savoir:

$$\forall x \geqslant 5 \ , \quad \left| \psi_\chi(x) - \delta(\chi)x \right| \leqslant \sqrt{x}\ \mathrm{Log}\ x\ (\mathrm{Log}\ A(\chi) + 0{,}3\ n(\chi)\mathrm{Log}\ x) \ .$$

$$\forall x \geqslant 5 \ , \quad \left| \psi_\xi(x) - \frac{|C|}{|G|} x \right| \leqslant \frac{|C|}{|G|} \sqrt{x}\ \mathrm{Log}\ x\ (\mathrm{Log}\ d_E + 0{,}3\ n_E \mathrm{Log}\ x) \ .$$

$$\forall x \geqslant 2 \ , \quad \left| \pi_C(x) - \frac{|C|}{|G|} \int_2^x \frac{dt}{\mathrm{Log}\ t} \right| \leqslant \frac{|C|}{|G|} \sqrt{x}\ (2\mathrm{Log}\ d_E + n_E\ \mathrm{Log}\ x) \ .$$

RÉFÉRENCE.- [1] J.C. Lagarias et A.M. Odlyzko, Effective versions of the Chebotarev density theorem, Algebraic number fields, Durham Symposium, Academic Press, 1977 .

Centre de mathématiques de
l'Ecole Normale Supérieure,
E.R.A. n° 07589,
45, rue d'Ulm,
75230 PARIS CEDEX 05

Astérisque

BERNARD ORIAT

Généralisation du "Spiegelungssatz"

Astérisque, tome 61 (1979), p. 169-175

<http://www.numdam.org/item?id=AST_1979__61__169_0>

Société Mathématique de France
Astérisque 61 (1979) p. 169-175

GENERALISATION DU "SPIEGELUNGSSATZ"

par
Bernard Oriat

La propriété qui nous intéresse ici est celle énoncée par Leopoldt dans [3]. Nous la rappelons dans les paragraphes I et II. Dans le paragraphe III nous montrons comment nous avons essayé d'en obtenir une généralisation. Dans le dernier paragraphe un principe analogue est appliqué pour déduire du théorème de Stickelberger une propriété d'annulation de classes d'idéaux réelles.

I Spiegelungsrelation.

Soit L/k une extension galoisienne finie de corps de nombres, de groupe de Galois G. On suppose que L contient toutes les racines n^{eme} de 1. Soit M/L une extension abélienne d'exposant divisant n. C'est une extension de Kummer ; désignons par W son radical, c'est-à-dire l'ensemble des w de L tels que $\sqrt[n]{w}$ appartienne à M. On suppose que W est stable par G, c'est-à-dire que M/k est galoisienne. Le groupe G opère, en tant que groupe de Galois, sur W, donc sur W/L^{*n}. D'autre part on peut le faire opérer par conjugaison sur Gal(M/L). Ainsi les deux groupes W/L^{*n} et Gal(M/L) sont des $(\mathbb{Z}/n\mathbb{Z})[G]$ modules.

D'autre part, soit ζ_n une racine primitive $n^{ème}$ de 1 et $<\zeta_n>$ le groupe multiplicatif qu'elle engendre. On définit un homomorphisme χ^* de G dans $(\mathbb{Z}/n\mathbb{Z})^*$ par l'égalité :

$\zeta_n^{\sigma} = \zeta_n^{\chi^*(\sigma)}$, pour tout σ de G.

Les deux groupes W/L^{*n} et $\mathrm{Hom}\left(\mathrm{Gal}(M/L), <\zeta_n>\right)$, groupe dual de Gal (M/L), sont canoniquement isomorphes. Si α est l'isomorphisme en question, rappelons qu'il est défini par : $\alpha\left(wL^{*n}\right)(u) = w^{u-1}$, pour tout u de Gal (M/L). Nous pouvons maintenant énoncer la "Spiegelungsrelation" [3] :

Théorème : Pour tout w de W, tout τ de G et tout u de Gal (M/L), on a

l'égalité :

$$\alpha\left((wL^{*n})^{\tau}\right)(u) = \alpha(wL^{*n})\left(u^{\chi^*(\tau)\tau^{-1}}\right).$$

Définition de l'involution du miroir. On peut définir dans l'algèbre de groupe $(\mathbb{Z}/n\mathbb{Z})[G]$ une involution en faisant correspondre à $x = \sum_{\tau \in G} a_\tau \tau$, l'élément $\bar{x} = \sum_{\tau \in G} a_\tau \chi^*(\tau)\tau^{-1}$. Nous l'appelons : involution du miroir. Si G est abélien, il s'agit d'un automorphisme de $(\mathbb{Z}/n\mathbb{Z})[G]$. La "Spiegelungsrelation" peut s'écrire à l'aide de cette involution sous la forme :

$$\alpha\left((wL^{*n})^{x}\right)(u) = \alpha(wL^{*n})(u^{\bar{x}}) ;$$

pour tout w de W, tout u de Gal (M/L) et tout x de $(\mathbb{Z}/n\mathbb{Z})[G]$.

Utilisation de la "Spiegelungsrelation" : Dans la suite, la situation décrite ci-dessus est utilisée de la façon suivante : L'extension M/L est non ramifiée. Son groupe de Galois est donc, par la théorie du corps de classes, isomorphe en tant que G-module, à un groupe quotient du groupe des classes de L. Si w appartient à W, alors l'idéal de L qu'il engendre est une puissance $n^{\text{ème}}$ d'un idéal $\mathfrak{a}$ de L. En associant à w la classe de l'idéal $\mathfrak{a}$, on définit une application de W/L^{*n} dans le groupe des classes de L. Le noyau de cet homomorphisme s'exprime alors à l'aide d'un groupe d'unités de L. On dispose ainsi d'un moyen de comparer un quotient du groupe des classes d'idéaux de L (ou d'un sous-corps de L) à un sous-groupe du groupe des classes de L (ou d'un sous-corps de L). De plus, si x annule le premier groupe, alors $\bar{x}$ annule le deuxième.

II Le "Spiegelungssatz" de Leopoldt [3].

Soit ℓ un nombre premier. Dans ce paragraphe on prend $n = \ell$ et on pose l'hypothèse suivante : ℓ ne divise pas le degré $[L : k]$.

Soit ψ un caractère ℓ-adique de G et $1_\psi = \frac{1}{[L : k]} \sum_{\tau \in G} \psi(\tau)\tau^{-1}$ l'idempotent de $\mathbb{Q}_\ell[G]$ associé. Il y a une correspondance biunivoque entre les idempotents de $\mathbb{Q}_\ell[G]$ et les idempotents de $\mathbb{F}_\ell[G]$ déduite de l'application canonique de $\mathbb{Z}_\ell[G]$ sur $\mathbb{F}_\ell[G]$. Si on confond un idempotent avec son résidu modulo ℓ, on voit que l'image $\bar{1}_\psi$ de 1_ψ par l'involution du miroir est un idempotent associé à un caractère $\bar{\psi}$ de G. Ce caractère $\bar{\psi}$ peut être défini de la façon suivante : Soit θ l'unique homomorphisme de G dans $\mathbb{Z}_\ell^*$

défini par $\zeta_\ell^\tau = \zeta_\ell^{\theta(\tau)}$ pour tout τ de G. On a alors $\bar{\psi} = \theta\psi^{-1}$ et l'application $\psi \to \bar{\psi}$ est une involution de l'ensemble des caractères ℓ-adiques de G.

Soit $\mathcal{H}(L)$ le ℓ-groupe des classes de L. A chaque caractère ψ, on associe le groupe $\mathcal{H}(L)^{1_\psi}$. Le "Spiegelungssatz" compare les ℓ-rangs (notés $\dim_\ell$) des groupes $\mathcal{H}(L)^{1_\psi}$ et $\mathcal{H}(L)^{1_{\bar{\psi}}}$. Introduisons encore E(L) groupe des unités de L et $\mathcal{E}(L) = E(L)/E(L)^\ell$.

Théorème : Si ℓ ne divise pas $[L : k]$ et si ψ est un caractère ℓ-adique de G, alors on a l'inégalité :

$$\dim_\ell \mathcal{H}(L)^{1_\psi} - \dim_\ell \mathcal{H}(L)^{1_{\bar{\psi}}} \leq \dim_\ell \mathcal{E}(L)^{1_{\bar{\psi}}}.$$

III Généralisation du Spiegelungssatz [4].

Dans cette généralisation on ne fait plus l'hypothèse : ℓ ne divise pas $[L : k]$, posée dans [3]. Les idempotents 1_ψ ne sont plus des éléments entiers et la notation $\mathcal{H}(L)^{1_\psi}$ n'a plus de sens. Soit maintenant ℓ un nombre premier impair. On désigne par n une puissance de ℓ. L'extension L/k est supposée abélienne de groupe de Galois G. On suppose toujours que L contient toutes les racines $n^{ème}$ de 1.

Les groupes d'idéaux et d'unités considérés sont attachés maintenant, non plus à un caractère ℓ-adique du groupe G, mais à un idéal I de l'algèbre $(\mathbb{Z}/n\mathbb{Z})[G]$. Définissons le corps K_I comme le corps intermédiaire entre L et k tel que $\mathrm{Gal}(L/K_I) = \{\sigma ; \sigma \in G ; \sigma - 1 \in I\}$. Si $\mathcal{H}(K_I)$ est le ℓ-groupe des classes d'idéaux de K_I, le groupe $\mathcal{H}^I$ est défini comme le plus grand quotient de $\mathcal{H}(K_I)/\mathcal{H}(K_I)^n$ annulé par I. De même, si $\mathcal{H}(K_I)^{(n)}$ est le sous-groupe de $\mathcal{H}(K_I)$ formé des éléments h de $\mathcal{H}(K_I)$ tels que $h^n = 1$, $\mathcal{H}_I$ est défini comme le plus grand sous-groupe de $\mathcal{H}(K_I)^{(n)}$ annulé par I.

Remarque : Ces définitions généralisent la définition précédente : en effet si ℓ ne divise pas $[L : k]$ et si ψ est un caractère ℓ-adique de G, soit I l'idéal de $(\mathbb{Z}/n\mathbb{Z})[G]$ engendré par $1 - 1_\psi$. Alors on vérifie que les groupes $\mathcal{H}^I$, $\mathcal{H}_I$ et $\mathcal{H}^{1_\psi}$ ont même ℓ-rang.

De la même façon, désignons par $E(K_I)$ le groupe des unités de K_I, $\mathcal{E}(K_I)$ le quotient $E(K_I)/E(K_I)^n$ et $\mathcal{H}_I$ le plus grand sous-groupe de

$\mathcal{E}(K_\mathfrak{l})$ annulé par 1. Précisons enfin que $\bar{\mathfrak{l}}$ désigne l'image de $\mathfrak{l}$ par l'involution du miroir et que $\dim_m$ désigne le m-rang.

Théorème. Pour toute puissance de ℓ, notée m et comprise entre ℓ et n, on a l'inégalité :

$$\dim_m \mathcal{H}^{\mathfrak{l}} - \dim_m \mathcal{H}_{\bar{\mathfrak{l}}} \leq \dim_\ell \mathcal{E}_{\bar{\mathfrak{l}}} + 1 .$$

De plus, si l'une ou l'autre des hypothèses suivantes est vérifiée :

- Le degré $[L : K_\mathfrak{l}]$ est premier à ℓ,
- Le corps $K_{\bar{\mathfrak{l}}}$ ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1 ; alors

on a plus précisément :

$$\dim_m \mathcal{H}^{\mathfrak{l}} - \dim_m \mathcal{H}_{\bar{\mathfrak{l}}} \leq \dim_\ell \mathcal{E}_{\bar{\mathfrak{l}}}.$$

Remarquons que le changement de $\mathfrak{l}$ en $\bar{\mathfrak{l}}$ ne permute pas $\mathcal{H}^{\mathfrak{l}}$ et $\mathcal{H}_{\bar{\mathfrak{l}}}$. Ainsi, obtenir une minoration de la différence $\dim_m \mathcal{H}^{\mathfrak{l}} - \dim_m \mathcal{H}_{\bar{\mathfrak{l}}}$ est, dans ce cadre plus général, un autre problème. Pour énoncer l'un des résultats obtenus, introduisons un groupe d'unités locales : Soient $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ les idéaux de $K_\mathfrak{l} \cap K_{\bar{\mathfrak{l}}}$ au-dessus de ℓ et D_j le groupe de décomposition de $\mathfrak{l}_j$ dans l'extension L/k. Soit $\bar{\mathfrak{l}}(j) = (\mathbb{Z}/n\mathbb{Z})[D_j] \cap \bar{\mathfrak{l}}$ et U_j le groupe des unités principales du complété de $K_{\bar{\mathfrak{l}}}$ en un idéal au-dessus de $\mathfrak{l}_j$. Soit $\mathcal{U}_{\bar{\mathfrak{l}}(j)}$ le plus grand sous-module de U_j/U_j^n annulé par $\bar{\mathfrak{l}}(j)$. Soit s le nombre de générateurs de l'image de l'idéal $\bar{\mathfrak{l}}$ par l'application restriction de $(\mathbb{Z}/n\mathbb{Z})[G]$ à $(\mathbb{Z}/n\mathbb{Z})[\mathrm{Gal}(K_{\bar{\mathfrak{l}}}/k)]$. Désignons par $(K_\mathfrak{l})_o$ le corps intermédiaire entre $K_\mathfrak{l}$ et $K_\mathfrak{l} \cap K_{\bar{\mathfrak{l}}}$, maximal tel que $[(K_\mathfrak{l})_o : K_\mathfrak{l} \cap K_{\bar{\mathfrak{l}}}]$ soit premier à ℓ.

Théorème. Si aucun idéal, au-dessus de ℓ, n'est totalement décomposé dans $(K_\mathfrak{l})_o / K_\mathfrak{l} \cap K_{\bar{\mathfrak{l}}}$ et si $K_{\bar{\mathfrak{l}}}$ ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1, alors, on a :

$$-\sum_{j=1}^{t} \dim_\ell \mathcal{U}_{\bar{\mathfrak{l}}(j)} - (s-1)\dim_\ell \mathcal{E}(K_{\bar{\mathfrak{l}}}) \leq \dim_m \mathcal{H}^{\mathfrak{l}} - \dim_m \mathcal{H}_{\bar{\mathfrak{l}}},$$

pour toute puissance de ℓ, notée m et comprise entre ℓ et n.

On trouvera dans [4] d'autres inégalités minorant la différence $\dim_m \mathcal{H}^{\mathfrak{l}} - \dim_m \mathcal{H}_{\bar{\mathfrak{l}}}$, valables sous d'autres hypothèses. Mais, en l'absence d'hypothèse, nous ne savons pas minorer cette différence.

IV Annulation de classes d'idéaux réelles.

Nous désignons toujours par ℓ un nombre premier impair. Soit

χ un caractère réel de conducteur f et ψ le caractère ℓ-adique issus de χ. Notons $\mathbb{Q}_\ell^{(\chi)}$ le corps obtenu en adjoignant à $\mathbb{Q}_\ell$ les valeurs prises par χ et $\mathbb{Z}_\ell^{(\chi)}$ l'anneau des entiers de ce corps. On associe à ψ un groupe de classes d'idéaux de la façon suivante :

Soit K_χ le sous-corps de $\mathbb{Q}^{(f)}$ tel que Gal $(\mathbb{Q}^{(f)}/K_\chi)$ soit égal à Ker χ. (Le caractère χ étant considéré comme un homomorphisme de Gal $(\mathbb{Q}^{(f)}/\mathbb{Q})$ dans $\mathbb{Q}_\ell^{(\chi)*}$). Soit $G = \text{Gal}\,(K_\chi/\mathbb{Q})$. On peut encore considérer χ comme un homomorphisme de G dans $\mathbb{Q}_\ell^{(\chi)*}$. Nous notons χ_1 son prolongement $\mathbb{Z}_\ell$-linéaire à $\mathbb{Z}_\ell[G]$. C'est un homomorphisme d'anneaux, de $\mathbb{Z}_\ell[G]$ dans $\mathbb{Z}_\ell^{(\chi)}$ et il est surjectif. Si on considère ψ comme un caractère de G et si 1_ψ est l'idempotent de $\mathbb{Q}_\ell[G]$ associé à ψ, le noyau de χ_1 est égal à $\mathbb{Z}_\ell[G] \cap (1-1_\psi)\mathbb{Q}_\ell[G]$. Si $\mathcal{H}(K_\chi)$ est le ℓ-groupe des classes de K_χ, notons $\mathcal{H}^\psi$ le plus grand quotient de $\mathcal{H}(K_\chi)$ annulé par le noyau de χ_1. Ainsi $\mathcal{H}^\psi$ est un module sur $\mathbb{Z}_\ell^{(\chi)}$.

Le résultat suivant est démontré par G. Gras dans [2] :

Théorème : Si ℓ est un nombre premier impair, si χ est un caractère réel différent de 1 et si ℓ ne divise pas l'ordre de χ, alors $\mathcal{H}^\psi$ est, en tant que $\mathbb{Z}_\ell^{(\chi)}$-module, annulé par $L_\ell(1,\chi)$, valeur en 1 de la fonction L ℓ-adique relative à χ.

Remarque : En fait, le résultat obtenu en [2] est plus précis : Il concerne un groupe de classes généralisées, correspondant par la théorie du corps de classes à une extension non ramifiée, sauf en ℓ, de K_χ.

Nous avons démontré que l'hypothèse "ℓ ne divise pas l'ordre de χ" peut être remplacée par l'hypothèse : "l'ordre de χ n'est pas une puissance de ℓ".

La démonstration de cette propriété utilise toujours les mêmes principes : en voici le résumé : Décomposons le conducteur f de χ sous la forme $f = f_o n_o$ avec f_o premier à ℓ et n_o puissance de ℓ. Soit n une puissance de ℓ, supérieure à n_o. On désigne par L_n le corps obtenu en ajoutant à K_χ toutes les racines $n^{\text{ème}}$ de 1 et on pose $G_n = \text{Gal}\,(L_n/\mathbb{Q})$. On introduit l'extension non ramifiée, M_n/L_n, qui correspond par le corps de classes au groupe de classes $\mathcal{H}^\psi/(\mathcal{H}^\psi)^n$ et on construit comme indiqué au paragraphe I, un homomorphisme de $\mathcal{H}^\psi/(\mathcal{H}^\psi)^n$ dans le ℓ-groupe des

classes de L_n. (Les corps M_n, L_n, $\mathbb{Q}$ correspondent à M, L et k). Comme K_χ est réel, cet homomorphisme est injectif. Le groupe des classes de L_n est annulé par l'idéal de Stickelberger de L_n. On en déduit que l'image par l'involution du miroir (de $L_n/\mathbb{Q}$) de l'idéal de Stickelberger annule le groupe $\mathcal{H}^\psi/(\mathcal{H}\psi)^n$.

Désignons par $(\frac{L_n}{\cdot})$ le symbole d'Artin attaché à L_n et choisissons un entier a_o premier à f_o et à ℓ, tel que $\chi(a_o)$ ne soit pas une racine de 1 d'ordre une puissance de ℓ. Introduisons les éléments suivants de l'algèbre $\mathbb{Q}_\ell[G_n]$:

$$x_n = \frac{1}{f_o n \varphi(n)} \left[1 - \left(\frac{L_n}{a_o}\right) a_o^{\varphi(n)}\right] \sum_{\substack{1 \le a \le f_o n \\ (a, f_o n) = 1}} a^{\varphi(n)} \left(\frac{L_n}{a}\right)$$

et $$y_n = \frac{1}{f_o n} \left[1 - \left(\frac{L_n}{a_o}\right)^{-1} a_o\right] \sum_{\substack{1 \le a \le f_o n \\ (a, f_o n) = 1}} a \left(\frac{L_n}{a}\right)^{-1},$$

où φ désigne l'indicateur d'Euler. On vérifie facilement qu'il s'agit d'éléments de $\mathbb{Z}_\ell[G_n]$ et la démonstration de la proposition suivante est élémentaire :

Proposition. Les résidus modulo n de x_n et y_n sont des éléments de $(\mathbb{Z}/n\mathbb{Z})[G_n]$, images l'un de l'autre par l'involution du miroir attachée à l'extension $L_n/\mathbb{Q}$.

Mais y_n appartient à l'idéal de Stickelberger de L_n et on en déduit donc que x_n annule $\mathcal{H}^\psi/(\mathcal{H}\psi)^n$. Si maintenant on cherche l'image de x_n par χ_1, on voit que cet élément va s'écrire sous la forme d'un produit :

$$\chi_1(x_n) = \left[1 - \chi(a_o) a_o^{\varphi(n)}\right] \left[\frac{1}{f_o n \varphi(n)} \sum_{\substack{1 \le a \le f_o n \\ (a, f_o n) = 1}} a^{\varphi(n)} \chi(a)\right]$$

dont le premier terme est une unité de $\mathbb{Z}_\ell^{(\chi)}$. On reconnaît dans le deuxième l'approximation ℓ-adique de $L_\ell(1, \chi)$ telle qu'elle est donnée dans [1]. Il

reste pour obtenir le résultat annoncé à "faire tendre n vers l'infini".

Bibliographie.

[1] Fresnel J. Nombres de Bernouilli et fonctions L p-adiques, Ann. Inst. Fourier, Grenoble, 17, 2 (1967).

[2] Gras G. Annulation du groupe des ℓ-classes généralisées d'une extension abélienne réelle de degré premier à ℓ. A paraître aux Ann. Inst. Fourier (1979).

[3] Leopoldt H. W. Zur Struktur der ℓ-Klassengruppe galoischer Zahlkörper, Journal für die reine und Angew. Math. 199 (1958).

[4] Oriat B. et Satgé Ph. Un essai de généralisation du "Spiegelungssatz", à paraître.

Bernard Oriat
Mathématiques (ERA 07 06 54)
Faculté des Sciences
25030 BESANCON Cedex

Astérisque

KENNETH A. RIBET

Report on p-adic L-functions over totally real fields

Astérisque, tome 61 (1979), p. 177-192

<http://www.numdam.org/item?id=AST_1979__61__177_0>

Société Mathématique de France
Astérisque 61 (1979) p. 177-192

REPORT ON P-ADIC L-FUNCTIONS OVER TOTALLY REAL FIELDS

by

Kenneth A. Ribet

This report concerns known p-adic properties of values at negative integers of abelian L-functions over totally real fields. These properties were first established by P. Deligne and the author [5], using the theory of p-adic Hilbert modular forms. Recently, techniques found by P. Cassou-Noguès [2] and by D. Barsky [1], based on formulas of Shintani [7], have provided a totally new method for the p-adic study of L-values. The main object of this paper is to compare the congruence results obtained by the two methods

More precisely, the main theorem of [5] is a statement about the existence of p-adic measures with certain properties, or equivalently a theorem asserting generalized Kummer congruences for L-values. The main theorem of [2] establishes certain special congruences introduced (as axioms) by Coates in his study of p-adic L-functions [3]. These congruences are particular cases of the Kummer congruences. Here we shall explain how the congruences of Coates in fact generate *all* Kummer congruences, so that the main results given by the two methods are entirely equivalent. This comparison takes place in the second section of this paper, which follows a preliminary section on the rationality of L-values.

In the third section, we state some 2-adic divisibilities (and a *non*-divisibility) which follow from the modular form technique for studying L-values. These results, obtained in [5], form a complement to the main theorem on Kummer congruences. Some of these divisibilities may be deduced formally from the Kummer congruences, because of the existence of trivial zeros for L-functions attached to abelian characters. It appears, however, that the general divisibility cannot be so obtained. It might be interesting to reprove these divisibilities using the method based on Shintani's formulas.

In the fourth section, we restate the Kummer congruences for conductors which are divisible by p, in terms of measures on Galois groups. Then we review a construction of p-adic L-functions based on these measures. The construction is basically that given by Coates [3], except that the role of measures has been made explicit. In summary, it is the following: the p-adic L-functions, after multiplication by suitable "fudge factors," become the Mellin transforms (in the sense of Mazur) of our measures. In our discussion, we have indicated how one may eliminate constant consideration of the fudge factors by using the *pseudo-measures* recently introduced by Serre [6].

1. *Rationality properties of abelian L-values*

Let K be a totally real field, and set $r = [K:\mathbb{Q}]$. For each (non-zero) integral ideal (or "conductor") f of K, let G_f be the strict ray class group of K modulo f. Recall that G_f is obtained by dividing the set of prime-to-f integral ideals of K by the equivalence:

$$a \sim b \text{ if and only if } ab^{-1} = (\alpha) \text{ for some totally positive } \alpha \in 1 + fb^{-1}.$$

Let $\bar{K}$ be an algebraic closure for K. Class field theory interprets G_f as the Galois group of an abelian extension $K_f \subseteq \bar{K}$ of K, and the union $\bigcup_f K_f$ is the maximal abelian extension K^{ab} of K in $\bar{K}$.

Let f now be a conductor, and let v be an embedding $K \hookrightarrow \mathbb{R}$, i.e., a real

place of K. Let $\alpha \in 1 + \mathfrak{f}$ be an element which is negative at v (i.e., $v(\alpha) < 0$) but positive at each real place of K different from v. The image σ_v in $G_\mathfrak{f}$ of the ideal (α) is independent of the choice of α and has order 1 or 2. It is the (real) Frobenius element of $G_\mathfrak{f}$ attached to v. It may also be described as the automorphism of $G_\mathfrak{f}$ obtained by choosing an embedding $K_\mathfrak{f} \hookrightarrow \mathbb{C}$ compatible with v and applying complex conjugation.

For fixed v, as $\mathfrak{f}$ varies, the elements $\sigma_v \in G_\mathfrak{f}$ form a compatible system in $G = \varprojlim G_\mathfrak{f}$. We again write σ_v for the element of G given by this compatible system. Each $\sigma_v \in G$ has order 2, and the subgroup H of G generated by the σ_v has order exactly 2^r. For each $\mathfrak{f}$, let $H_\mathfrak{f}$ be the subgroup of $G_\mathfrak{f}$ generated by the σ_v in $G_\mathfrak{f}$; this subgroup is the image of H in $G_\mathfrak{f}$.

If $\varepsilon: G_\mathfrak{f} \to \mathbb{C}$ is a complex-valued function mod $\mathfrak{f}$, we set as usual

$$L(s, \varepsilon) = \sum \varepsilon(\mathfrak{x}) N\mathfrak{x}^{-s}, \tag{1.1}$$

the sum being over prime-to-$\mathfrak{f}$ integral ideals $\mathfrak{x}$. (Here N is the norm function, and we view ε as a function on the set of prime-to-$\mathfrak{f}$ ideals in the usual way.) While this sum need converge only for $\operatorname{Re} s > 1$, it is well known that the function $L(s, \varepsilon)$ may be analytically continued to a meromorphic function on $\mathbb{C}$, holomorphic for $s \neq 1$, with at worst a simple pole at $s = 1$. The continuation defines in particular values $L(1 - k, \varepsilon)$ for integral $k \geqslant 1$.

(1.2) THEOREM [7], [8]. *Suppose that the values of* ε *are rational numbers. Then* $L(1 - k, \varepsilon) \in \mathbb{Q}$ *for* $k \geqslant 1$.

For each $a \in G_\mathfrak{f}$, let $1_{a,\mathfrak{f}}$ be the characteristic function of a on $G_\mathfrak{f}$. The L-series $L(s, 1_{a,\mathfrak{f}})$ is the partial zeta function of the class a modulo $\mathfrak{f}$ as considered by Siegel. The theorem asserts that the values of such partial zeta functions at negative integers (including 0) are rational. The formula

$$L(1 - k, \varepsilon) = \sum_{a \in G_\mathfrak{f}} L(1 - k, 1_{a,\mathfrak{f}}) \cdot \varepsilon(a)$$

shows for arbitrary $\varepsilon: G_\mathfrak{f} \to \mathbb{C}$ that the values $L(1 - k, \varepsilon)$ lie in the $\mathbb{Q}$-vector

space spanned by the numbers $\varepsilon(\bar{a})$ in $\mathbb{C}$. It provides the *definition* of values $L(1-k, \varepsilon) \in V$ for any function on G_f with values in a $\mathbb{Q}$-vector space V.

We now consider certain identities which hold among these values. Let $\varepsilon: G_f \to V$ be given. For $a \in G_f$ we write ε_a for the function $x \longmapsto \varepsilon(ax)$, the "twist" of ε by a. For $c \in G$, we write ε_c for the twist of ε by the image of c in G_f. Similarly we define the twist of ε by a prime-to-f integral ideal d.

(1.3) PROPOSITION. *Assume that* $K \neq \mathbb{Q}$ *or that* f *is non-trivial. For each real place* v *of* K *and all* $k \geq 1$, *we have* $L(1-k, \varepsilon_{\sigma_v}) = (-1)^k L(1-k, \varepsilon)$.

The proposition is proved by reduction to the case where ε is a primitive character with values in $\mathbb{C}^*$. It follows in this case from the functional equation for $L(s, \varepsilon)$ (trivial zeros). Note that in the excluded case the proposition would be false for $k = 1$, since the Riemann zeta function does not vanish at 0.

Now let $f' \subset f$ be two conductors. Suppose that d is a divisor of f' which is prime to f. Then f divides the quotient $f'd^{-1}$, so that there is a canonical map $G_{f'd^{-1}} \to G_f$. Let us write ε_d^* for the composite of this canonical map with the twist ε_d of ε by d. The function ε_d^* is thus a function mod $f'd^{-1}$.

(1.4) PROPOSITION. *For* $k \geq 1$ *we have*

$$L(1-k, \varepsilon) = \sum_d L(1-k, \varepsilon_d^*) N d^{k-1},$$

where the sum runs over those divisors d *of* f' *which are prime to* f.

To prove this proposition, it suffices to treat the case $V = \mathbb{C}$. There we decompose the sum (1.1) according to the greatest common divisor d of x and f'. The asserted identity then falls out immediately.

The simplest, and most familiar, case of the identity (1.4) occurs when f and f' have the same prime factors. Then the sum has only one term, corresponding to $d = 1$, and the identity states that $L(1-k, \varepsilon)$ has the same value when we

regard ε as a function modulo f' as when we regard it as a function modulo f.

2. *Congruences for L-values*

Let p be a prime number, fixed in what follows. Let $N : G \to \mathbb{Z}_p^*$ be the p-adic norm character. This map is characterized by each of the following:

(i) The map N is the "Tate" character describing the action of $G = \mathrm{Gal}(K^{ab}/K)$ on the p-power roots of unity in K^{ab},

(ii) The map N factors through the quotient $G_{p^\infty} = \varprojlim G_{p^n}$ of G and coincides with the standard norm map on the dense subset of G_{p^∞} consisting of the prime-to-p integral ideals of K.

In connection with (ii), we note that for $n \geqslant 0$ the map

$$N \bmod p^n;\ G \xrightarrow{N} \mathbb{Z}_p^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$$

already factors across the quotient G_{p^n} of G. Also, we have $N_{\sigma_v} = -1$ for each real place v of K.

Let f be a conductor, and let $\varepsilon : G_f \to V$ take values in a $\mathbb{Q}_p$-vector space. For $c \in G$ we set

$$\Delta_c(1-k, \varepsilon) = L(1-k, \varepsilon) - Nc^k L(1-k, \varepsilon_c) \in V$$

for $k \geqslant 1$. These ε_c are the *twisted L-values* attached to ε. If ε is a *character* with values in an extension field of $\mathbb{Q}_p$, then we have

$$\Delta_c(1-k, \varepsilon) = \{1 - \varepsilon(c)Nc^k\}L(1-k, \varepsilon) :$$

the twisted L-values are the usual L-values corrected by a "fudge factor" depending on c.

Now let $(\varepsilon_k,\ k \geqslant 1)$ be a sequence of $\mathbb{Q}_p$-valued functions on G_f, *only finitely many of which are non-zero*. The Kummer congruences mentioned in the Introduction are given by

(2.1) THEOREM [5]. *Assume that we have*

$$\sum_{k\geqslant 1} \varepsilon_k(x)Nx^{k-1} \in \mathbb{Z}_p$$

for each prime-to-f integral ideal x. *Then for all* $c \in G$ *we have*

$$\sum_{k\geqslant 1} \Delta_c(1-k, \varepsilon_k) \in \mathbb{Z}_p .$$

We note immediately the following *variants* of (2.1):

1. By linearity, we may replace $\mathbb{Z}_p$ by $p^n\mathbb{Z}_p$ for any $n \in \mathbb{Z}$, in the statement of (2.1). Hence (2.1) may be paraphrased: any *congruence* satisfied by a finite sum $\sum \varepsilon_k N^{k-1}$ is again satisfied by the corresponding sum of twisted L-values.

2. We may replace $\mathbb{Z}_p$ by any free $\mathbb{Z}_p$-module R, replacing $\mathbb{Q}_p$ by $E = R \otimes \mathbb{Q}_p$. This applies for example if E is a finite extension of $\mathbb{Q}_p$ and R is its ring of integers.

3. We may replace c by an *integral ideal* d which is prime to pf. The conclusion of (2.1) for a given c is equivalent to the corresponding statement for a given d provided that c and d have the same images in G_f and have norms which are sufficiently p-adically close.

We now turn to the congruences of Coates [3]. We restate them slightly, to make evident that they are special cases of the Kummer congruences (2.1):

A. For all $\varepsilon: G_f \to \mathbb{Z}_p$ *and* $k \geqslant 1$, *we have* $\Delta_c(1-k, \varepsilon) \in \mathbb{Z}_p$ *for all* $c \in G$,

B. Let f *be divisible by* p^n $(n \geqslant 0)$, *and let* $k \geqslant 1$ *be given. Suppose that* $\eta: G_f \to \mathbb{Z}_p$ *is such that* $\eta \equiv N^{k-1} \bmod p^n$, *the two functions being considered as functions on the space of prime-to-f integral ideals. Then for all* $\varepsilon: G_f \to \mathbb{Z}_p$ *we have*

$$\Delta_c(1-k, \varepsilon) \equiv \Delta_c(0, \varepsilon\eta) \bmod p^n .$$

[Note that, in *B*, the function η exists because $N \bmod p^n$ may be viewed as a function on G_{p^n}. Assuming *A*, the assertion *B* is independent of the choice of η.]

(2.2) THEOREM. *Statements* A *and* B *imply* (2.1).

Proof. We first condider the case where f is divisible for all primes dividing p. For $n \geqslant 0$ we have the right to replace f by fp^n in (2.1), replacing ε_k by their composites with the map $G_{fp^n} \to G_f$: The replacement does not change the hypothesis of (2.1), and in light of (1.4) it does not change the conclusion either. Make this replacement, choosing n so that all ε_k take value in $p^{-n}Z_p$. For each $k \geqslant 1$, let η_k be such that $\eta_k \equiv N^{k-1} \bmod p^n$. The function

$$\varepsilon = \sum \varepsilon_k \eta_k$$

is $\mathbb{Z}_p$-valued according to the hypothesis to (2.1). Hence, by *A*, we have $\Delta_c(0, \varepsilon) \in \mathbb{Z}_p$. But by *B* we have

$$\Delta_c(0, \varepsilon_k \eta_k) \equiv \Delta_c(1 - k, \varepsilon_k) \mod \mathbb{Z}_p$$

for each k. Since $\Delta_c(0, \varepsilon) = \sum \Delta_c(0, \varepsilon_k \eta_k)$, this gives the conclusion to (2.1).

We now treat the remaining case, where f is *not* divisible by all primes over p. Each class in G_f is represented by ideals whose norms are arbitrarily highly divisible by p, so that the hypothesis to (2.1) implies that ε_1 takes values in $\mathbb{Z}_p$. Of course, if *all* ε_k are $\mathbb{Z}_p$-valued, then the conclusion to (2.1) is a consequence of *A*. Arguing inductively, we shall assume that (2.1) is known if all ε_k take values in $p^{-n}\mathbb{Z}_p$ but that we are in fact given functions ε_k with values in $p^{-n-1}\mathbb{Z}_p$.

Let $f' = fp$, and decompose each value $L(1 - k, \varepsilon_k)$ as in (1.4). The quantity to be proved integral in (2.1) then breaks up as a sum of quantities $\sum_k \Delta_c(1 - k, \varepsilon^*_{k,d}) N d^{k-1}$, one for each divisor d of f' which is prime to f. It suffices to prove that each such quantity is integral. Fix d, and for each k set $\alpha_k = \varepsilon^*_{k,d} N d^{k-1}$; the problem is then to obtain the conclusion of (2.1) with the ε_k replaced by the α_k. Now for each x prime to $f' d^{-1}$, we have

$$\sum_k \alpha_k(x) N x^{k-1} = \sum_k \varepsilon_k(dx) N(dx)^{k-1},$$

so that the hypothesis of (2.1) for the α_k is just a special case of the same

hypothesis for the ε_k. If $d = 1$, then $f = fp$ is divisible by all primes over p, so we have already obtained the conclusion of (2.1) for the α_k. If $d \neq 1$, then clearly Nd is divisible by p, so that each α_k takes values in $p^{-n}\mathbb{Z}_p$. We again have the desired integrality by induction.

3. *2-adic properties of* L*-values, and "parity"*

In this section we state a strengthening of (2.1) for $p = 2$ in the situation where the functions ε_k satisfy certain parity conditions.

Let f be a conductor. A function ε on G_f with values in a $\mathbb{Q}$-vector space V is said to be *odd* (resp. *even*) if $\varepsilon_{\sigma_v} = -\varepsilon$ (resp. $\varepsilon_{\sigma_v} = \varepsilon$) for each real place v of K. (Here the σ_v are the real Frobenius elements of §1.) Let k be an integer. We say that ε has parity $(-1)^k$ if k is odd and ε is odd or if k is even and ε is even. We shall be considering functions ε_k as in (2.1) where each ε_k has parity $(-1)^k$. Before doing this, we distinguish an *exceptional case*. This is the case where each of the following three conditions is satisfied:

(i) The conductor f is the trivial ideal (1).

(ii) All units of K have norm $+1$.

(iii) The extension L of K obtained by extracting the square roots of all totally positive units of K is *quadratic* over K.

[When (ii) is satisfied, (iii) means that there are units of K of all possible signatures which are compatible with (ii).]

Finally, suppose that $\varepsilon: G_f \to \mathbb{Z}_2$ is either even or odd. Then the reduction

$$\bar{\varepsilon}: G_f \xrightarrow{\varepsilon} \mathbb{Z}_2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})$$

is invariant under the subgroup H_f of G_f generated by the σ_v, so that the sum

$$\sum_{g \in G_f/H_f} \bar{\varepsilon}(g) \in \mathbb{Z}/2\mathbb{Z}$$

is well defined. We let $\delta(\varepsilon)$ denote this sum.

(3.1) THEOREM [5]. *Let* ε_k $(k \geqslant 1)$ *be given as in* (2.1). *Assume that each* ε_k *has parity* $(-1)^k$ *and that* $p = 2$. *Then:*

(a) *For all* $c \in G$ *we have*

$$\Delta_c \overset{\text{def.}}{=} \sum_{k \geqslant 1} \Delta_c(1-k, c_k) \in 2^{r-1}\mathbb{Z}_2 ,$$

(b) *In the non-exceptional case, we have* $\Delta_c \in 2^r\mathbb{Z}_2$.

(c) *In the exceptional case, we have* $\Delta_c \in 2^r\mathbb{Z}_2$ *provided that either* $c \in \mathrm{Gal}(K^{ab}/L)$ *or* $\delta(\varepsilon_1) = 0$.

[Note that in the exceptional case the function ε_1 is $\mathbf{Z}_2$-valued because the conductor $f = (1)$ is not divisible by each prime dividing 2 , as in the proof of (2.2).]

(3.2) THEOREM [5]. *Suppose, in the exceptional case, that* $\delta(\varepsilon_1) = 1$ *and that* $c \notin \mathrm{Gal}(K^{ab}/L)$. *Then* Δ_c *is exactly divisible by* 2^{r-1} .

In connection with these theorems, we now explain why the case where each ε_k has parity $(-1)^k$ is a central one. As in §1, let H be the subgroup of G generated by the real Frobenius elements σ_v . Let $N\colon H \to \{\pm 1\}$ be the homomorphism such that $N\sigma_v = -1$ for each v ; it is the restriction to H of the p-adic norm character $N\colon G \to \mathbb{Z}_p^*$ for any prime p .

Suppose that ε is a function on G_f with values in a $\mathbb{Q}$-vector space. Write

$$\varepsilon^+ = \frac{1}{\#H} \sum_{c \in H} \varepsilon_c ,$$

$$\varepsilon^- = \frac{1}{\#H} \sum_{c \in H} Nc \cdot \varepsilon_c ;$$

these two functions are respectively even and odd. (As we have remarked in §1, one knows in fact that $\#H = 2^r$.)

(3.3) PROPOSITION. *Suppose that either* K *is different from the rational field or that* f *is non-trivial.*

(1) *For* $k \geqslant 1$ *and* $c \in H$ *we have* $L(1-k, \varepsilon_c) = Nc^k L(1-k, \varepsilon)$,

(2) *We have*

$$L(1-k,\varepsilon) = \begin{cases} L(1-k,\varepsilon^+) & \text{if } k \text{ is even} \\ L(1-k,\varepsilon^-) & \text{if } k \text{ is odd,} \end{cases}$$

Proof. The first statement is a variant of (1.3). The second follows directly from the first and the definitions of ε^-, ε^+.

Statement (2) gives a simple expression for an arbitrary L-value in terms of an L-value for a function "with parity." Using it, one shows easily that (2.1), when $p = 2$, is a *consequence* of (3.1). Conversely, given (2.1), the divisibility statement (3.1) may be reinterpreted in terms of divisibilities of values $\Delta_c(0, \varepsilon)$ for *arbitrary* functions $\varepsilon: G_f \to \mathbb{Z}_2$.

4. p-*adic* L-*functions and* p-*adic measures*

Let p be a prime number. In this section we shall outline the construction of p-adic measures on certain Galois groups with the aim of relating our Kummer congruence (2.1) to the theory of p-adic L-functions attached to abelian characters over K.

Let f be a conductor which is divisible by all primes of K dividing p. In this section, we modify our previous notation and let G be the Galois group $G_{fp^\infty} = \varprojlim G_{fp^n}$. The group *previously* denoted by G will now be referred to without abbreviation as $\mathrm{Gal}(K^{ab}/K)$. We shall reformulate in terms of measures on G all Kummer congruences modulo the conductors fp^n $(n \geqslant 0)$.

For each locally constant function $\varepsilon: G \to \mathbb{Q}$, quantities $L(1-k,\varepsilon) \in \mathbb{Q}$ are defined for $k \geqslant 1$. Namely, any such ε is (for sufficiently large n) a map $G_{fp^n} \xrightarrow{\varepsilon_n} \mathbb{Q}$, and the numbers $L(1-k,\varepsilon_n)$ attached to this map as in §1 are independent of the choice of n because of (1.4). For fixed k, the association $\varepsilon \mapsto L(1-k,\varepsilon)$ is thus a distribution on G with values in $\mathbb{Q}$.

For each locally constant $\varepsilon: G \to \mathbb{Q}_p$ and each $c \in \mathrm{Gal}(K^{ab}/K)$, we define

$$\Delta_c(1-k,\varepsilon) = L(1-k,\varepsilon) - Nc^k L(1-k,\varepsilon_c) \in \mathbb{Q}_p$$

as in §2. Since $N: \mathrm{Gal}(K^{ab}/K) \to \mathbb{Z}_p^*$ may be viewed as a function on G, for given ε and k a quantity $\Delta_c(1-k, \varepsilon)$ is well defined for c in G.

For later use, we recall the standard factorization $N = \langle\ \rangle\omega$ of the norm character on G as the product of a character $x \mapsto \langle x \rangle$ with values in $1+2p\mathbb{Z}_p \subseteq \mathbb{Z}_p^*$ and a $\mathbb{Z}_p^*$-valued character of finite order ω, the Teichmüller character. We let $\Gamma \subset \mathbb{Z}_p^*$ be the image of $\langle\ \rangle$; it is (non-canonically) isomorphic to $\mathbb{Z}_p$. The extension of K cut out by the character $\langle\ \rangle$ is the cyclotomic $\mathbb{Z}_p$-extension of K.

Also, we let $A \subseteq G$ be the kernel of $\langle\ \rangle$; it is finite if and only if the Leopoldt conjecture is true for K and p.

(4.1) THEOREM. *For each* $c \in G$, *the distribution* $\varepsilon \longmapsto \Delta_c(0, \varepsilon)$ *is a measure* μ_c *on* G *with values in* $\mathbb{Z}_p$. *For* $k \geq 1$, *the measure* $N^{k-1}\mu_c$ *is the map* $\varepsilon \mapsto \Delta_c(1-k, \varepsilon)$.

Proof. The first statement asserts that if a locally constant function ε on G is $\mathbb{Z}_p$-valued, then $\Delta_c(0, \varepsilon)$ lies in $\mathbb{Z}_p$. This is a special case of (2.1), and indeed is contained in congruence *A* of §2. To check the second statement, it suffices to show for $k \geq 1$ and $n \geq 1$ that

$$\int \varepsilon N^{k-1}\, d\mu_c \equiv \Delta_c(1-k, \varepsilon) \bmod p^n \mathbb{Z}_p$$

for each locally constant $\varepsilon: G \to \mathbb{Z}_p$. For this, let $\eta: G \to \mathbb{Z}_p$ be a locally constant function such that $\eta \equiv N^{k-1} \bmod p^n$. By congruence *B* of §2, we have

$$\Delta_c(1-k, \varepsilon) \equiv \Delta_c(0, \varepsilon\eta) \quad \bmod p^n\mathbb{Z}_p.$$

On the other hand, because μ_c is a measure, we have

$$\Delta_c(0, \varepsilon\eta) = \int \varepsilon\eta\, d\mu_c \equiv \int \varepsilon N^{k-1} d\mu_c \quad \bmod p^n\mathbb{Z}_p.$$

This completes the proof.

Remark. Conversely, we recover the Kummer congruences $\bmod fp^n$ $(n \geq 0)$ from the measures μ_c as follows: if $\sum \varepsilon_k N^{k-1}$ is $\mathbb{Z}_p$-valued, then we have

$$\sum \Delta_c(1-k, \varepsilon_k) = \int \sum \varepsilon_k N^{k-1} d\mu_c \in \mathbb{Z}_p.$$

Since our proof of (4.1) uses only congruences A and B of §2, we find once again that A and B imply the Kummer congruences for any conductor divisible by all primes above p. The proof of this fact provided by the above arguments is essentially the same as that given in §2.

Following [6], it is convenient to renormalize so as to replace $k-1$ by k. Namely, for $c \in G$, let $\lambda_c = N^{-1}\mu_c$. Then λ_c is a measure on G with the property that

$$\int \varepsilon N^k \, d\lambda_c = \Delta_c(1-k, \varepsilon)$$

for $k \geqslant 1$ and ε locally constant (cf. [6, 3.5]).

In the language of [6], the measures λ_c define a *pseudo-measure* λ on G. For each non-trivial continuous character ψ on G with values in the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$, an integral

$$\int \psi \, d\lambda = \frac{\int \psi \, d\lambda_c}{1-\psi(c)} \in \mathbb{C}_p$$

is defined independently of c. When ψ is a character of finite order, we have in particular $\int \psi \, N^k \, d\lambda = L(1-k, \psi)$.

(4.3) Suppose that Leopoldt's conjecture is true for K and p, i.e., that the group $A = \mathrm{Ker}\langle\ \rangle$ is finite. Then by [6, 1.15], λ may be uniquely written as the sum of a $\mathbb{Z}_p$-valued measure μ on G and some $\mathbb{Z}_p$-multiple of a certain "standard" pseudo-measure on G obtianed from Haar measure on A. On the other hand, if Leopoldt's conjecture is false for K and p, then [6, 1.15] states that λ is already a measure. Write $\mu = \lambda$ in this case. Then in both cases we have at least $\int \psi \, d\lambda = \int \psi \, d\mu$ for all characters ψ which are non-trivial on A [6, 1.17].

Now let $H \subseteq G$ be the subgroup of G generated by the real Frobenius elements of G (i.e., the images in G of the real Frobenius elements of $\mathrm{Gal}(K^{ab}/K)$).

(4.4) THEOREM. *Let $\phi : G \to \mathbb{Z}_p$ be a continuous function which is even in the sense that it is invariant under H. Then for all $c \in G$ we have $\int \phi \, d\lambda_c \in 2^r\mathbb{Z}_p$.*

Proof. There is no new assertion if p is odd. If $p = 2$, the result follows immediately from divisibility (b) of (3.1).

Remark. Using (3.3), one may show *a priori* from (4.1) that $\int \phi \, d\lambda_c$ is divisible in $\mathbb{Z}_p$ by the order of H when ϕ is even. This order divides 2^r, and it is equal to 2^r whenever $p = 2$ and Leopoldt's conjecture is true for K and the prime 2. Hence (4.4) asserts the truth of a *consequence* of Leopoldt's conjecture.

(4.5) COROLLARY. *Let* μ *be the measure on* G *introduced in* (4.3). *For all even* $\phi: G \to \mathbb{Z}_p$, we have $\int \phi \, d\mu \in 2^r\mathbb{Z}_p$.

Proof. The divisibility (4.4) asserts that the pseudo-measure on G/H obtained from λ and the projection $G \to G/H$ is divisible by 2^r. The corollary then follows from the uniqueness of the decomposition [6, 1.15].

We close now with remarks on the construction of the p-adic L-function $L_p(s, \varepsilon)$ attached to an even continuous character ε of finite order on G. Let E be the finite extension of $\mathbb{Q}_p$ generated by the values of ε, and let R be the integer ring of E. By definition $L_p(s, \varepsilon)$ is the continuous function (of s) on $\mathbb{Z}_p - \{1\}$ with values in E such that $L_p(1 - k, \varepsilon) = L(1 - k, \varepsilon\omega^{-k})$ for $k \geqslant 1$. The point is to show that $L_p(s, \varepsilon)$ exists, and to derive various "analyticity" properties for it.

For the existence, choose an element c of G such that one of $\varepsilon(c)$, c is different from 1. The expression

$$\frac{\int \langle x \rangle^{1-s} \varepsilon(x) d\lambda_c(x)}{1 - \varepsilon(c)\langle c \rangle^{1-s}} \tag{4.6}$$

then represents a continuous funciton of s having the defining property of $L_p(s, \varepsilon)$. Alternately, $L_p(s, \varepsilon)$ is simply the integral of $\varepsilon\langle\ \rangle^{1-s}$ against the pseudo-measure λ.

The analyticity properties result form the well-known connection between R-valued measures on $\mathbb{Z}_p$ and elements of the power series ring $R[[T]]$, cf. [6, 1.7].

The essential fact for us is a resulting *integral formula.* Choosing a splitting of the projection $G \to \Gamma$, so that G may be viewed as a product $\Gamma \times A$. Also, let $\gamma \in \Gamma$ be a topological generator of Γ over $\mathbb{Z}_p$. If $\alpha : \Gamma \xrightarrow{\sim} \mathbb{Z}_p$ is the resulting isomorphism, we have $x = \gamma^{\alpha(x)}$ for $x \in \Gamma$. We write simply α for the composite of α with the projection $G \to \Gamma$.

Let ψ be a continuous character on G with values in $\mathbb{C}_p^*$. It is the product of a character ψ_A on G which is trivial on Γ and the character $x \mapsto u^{\alpha(x)}$, where $u = \psi(\gamma)$. For $n \geqslant 0$, let a_n be the integral

$$\int_G \psi_A(x) \binom{\alpha(x)}{n} d\mu(x) \in R ,$$

where $\binom{\alpha(x)}{n}$ is the n^{th} binomial function on $\mathbb{Z}_p$, viewed via α as a function on G. Then, by the binomial theorem, we have

$$\int \psi d\mu = \sum_{n \geqslant 0}^{\infty} a_n (u - 1)^n , \tag{4.7}$$

cf. [6, 1.9].

One uses this formula to prove results of *Iwasawa analyticity* for $L_p(s, \varepsilon)$. Namely, let us say that function $\psi : \mathbb{Z}_p \to R$ is Iwasawa analytic if there is a power series $F \in R[[T]]$ such that $F(\gamma^{1-s} - 1) = \phi(s)$. [The power series is unique if it exists, and the property of being analytic in this sense is independent of the choice of the generator γ of Γ.] Here are the main facts concerning $L_p(s, \varepsilon)$:

(4.8) *For each* c, *both the numerator and the denominator in* (4.6) *are Iwasawa analytic function on* $\mathbb{Z}_p$. *The power series representing the numerator is divisible by* 2^r.

(4.9) *If* ε *is non-trivial on* A, *then* $L_p(s, \varepsilon)$ *extends to an Iwasawa analytic function on* $\mathbb{Z}_p$, *and the power series* F_ε *which represents it is divisible by* 2^r.

(4.10) *If* ε *is non-trivial on* A, *but if* $\theta : G \to \mathbb{C}_p^*$ *is a finite character which is trivial on* A, *then* $F_{\theta\varepsilon}(T) = F_\varepsilon(\zeta(1 + T) - 1)$, *where* ζ *is the*

p-power root of unity $\theta(\gamma)$.

Sketches of the proofs. The assertion relative to the denominator of (4.6) is immediate from the definition of the denominator. The Iwasawa analyticity of the numerator follows from (4.7), where we take $\psi = \langle\ \rangle^{1-s}$ and $\mu = \varepsilon\lambda_c$. The divisibility of the coefficients of the power series representing the numerator is a consequence of (4.4) and the hypothesis that ε is an even character. (It is worth noting, in passing, that when ε is a character which is *not* even, the definition of $L_p(s, \varepsilon)$ implies that $L_p(s, \varepsilon)$ is identically 0 .)

The statements in (4.9) may be deduced from (4.8) by an argument involving unique factorization in $R[[T]]$ (cf. [4], 6.5). A more direct approach is to use the expression

$$L_p(s, \varepsilon) = \int \varepsilon \langle\ \rangle^{1-s} d\mu ,$$

valid when ε is non-trivial on A , for $L_p(s, \varepsilon)$ in terms of the measure μ of (4.3). The divisibility of F_ε by 2^r results from (4.5).

Finally, (4.10) is an easy consequence of the integration formula (4.7); we have

$$\begin{aligned} L_p(s, \varepsilon\theta) &= \int (\langle\ \rangle^{1-s}\theta)\varepsilon\, d\lambda \\ &= F_\varepsilon(\gamma^{1-s}\theta(\gamma) - 1) . \end{aligned}$$

BIBLIOGRAPHY

[1] D. BARSKY - Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels. Preprint.

[2] P. CASSOU-NOGUÈS - Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. Preprint.

[3] J. COATES - p-adic L-functions and Iwasawa's theory. In: Algebraic number fields, A. Fröhlich, ed. New York and London: Academic Press 1977.

[4] J. COATES and S. LICHTENBAUM - On ℓ-adic zeta functions. Ann. of Math *98*, 498-550 (1973).

[5] P. DELIGNE and K. RIBET - Values of abelian L-functions at negative integers, To appear.

[6] J.-P. SERRE - Sur le résidu de la fonction zêta p-adique d'un corps de nombres, C.R. Acad. Sc. Paris *287*, 183-188 (1978).

[7] T. SHINTANI - On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. J. Fac. Sci. Univ. Tokyo, Sec. IA *23*, 393-417 (1976).

[8] C.L. SIEGEL - Uber die Fourierschen Koeffizienten von Modulformen. Göttingen Nach. *3*, 15-56 (1970).

Kenneth A. Ribet
Mathematics Dept,
U.C. Berkeley
BERKELEY, CA. 94720
(U.S.A)

Astérisque

PHILIPPE SATGÉ

Divisibilité du nombre de classes de certains corps cycliques

Astérisque, tome 61 (1979), p. 193-203

<http://www.numdam.org/item?id=AST_1979__61__193_0>

Société Mathématique de France
Astérisque 61 (1979) p. 193-203

DIVISIBILITÉ DU NOMBRE DE CLASSES DE CERTAINS CORPS CYCLIQUES

par

Philippe SATGÉ

-:-:-:-

Soient ℓ un nombre premier impair et $n = \ell^r$ une puissance de ℓ ; φ étant l'indicateur d'Euler, nous considérons les extensions cycliques de $\mathbb{Q}$ de degré $\varphi(n)$ qui contiennent le sous-corps réel maximal du n-ème corps cyclotomique. Nous montrons essentiellement qu'il existe une infinité de tels corps (aussi bien réels qu'imaginaires) dont le groupe des classes possède un élément d'ordre n. Dans les cas $n = 3$ et $n = 5$, nous donnons même une caractérisation de tous les corps de ce type dont le nombre de classes est divisible par n. Nous obtenons ces résultats en construisant des extensions non ramifiées.

§ .I. - Construction de corps

I.1. - Notations et définition des ψ-corps

Dans tout cet article, ℓ est un nombre premier impair et $n = \ell^r$ est une puissance de ℓ. On désigne par L un corps cyclique sur $\mathbb{Q}$ dont le degré divise $\varphi(n)$ (φ = indicateur d'Euler), par ζ une racine de l'unité d'ordre n, par L' et N' les corps $N(\zeta)$ et $L(\zeta)$, par ψ un homomorphisme de $\mathrm{Gal}(L'/\mathbb{Q})$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles modulo n dont le noyau est $\mathrm{Gal}(L'/L)$ et par ω l'homomorphisme de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ défini, pour tout σ de $\mathrm{Gal}(L'/\mathbb{Q})$, par $\sigma(\zeta) = \zeta^{\omega(\sigma)}$. On pose $\bar{\psi} = \omega\,\psi^{-1}$, on note K le corps des invariants du noyau de $\bar{\psi}$ et $V(\bar{\psi})$ le sous-groupe de K^* formé des x tels que, pour tout σ de $\mathrm{Gal}(L'/\mathbb{Q})$, le produit $\sigma(x)\,x^{-\bar{\psi}(\sigma)}$ est

une puissance n-ème dans K (ce qui a un sens bien que $\bar{\psi}(\sigma)$ ne soit défini que modulo n). Nous définissons les ψ-corps de la manière suivante :

DÉFINITION I.1.1.- Un corps N est un ψ-corps si N/L est une extension cyclique de degré n , si N est galoisien sur $\mathbb{Q}$ et si l'action par conjugaison de $Gal(L/\mathbb{Q})$ sur $Gal(N/L)$ est l'élévation à la puissance $\psi(\sigma)$.

I.2.- Construction des ψ-corps

Les ψ-corps ont été étudiés dans [1] ; nous donnons ici sans démonstration les résultats de [1] dont nous avons besoin dans la suite.

PROPOSITION I.2.1.- Soit N un ψ-corps ; le corps N' est obtenu en adjoignant à L' la racine n-ème d'un élément x de $V(\bar{\psi})$; de plus, si l'intersection $N \cap L'$ est réduite à L, cet élément n'est pas la puissance ℓ-ème d'un élément de K .

Sous l'hypothèse restrictive que le corps K ne contient pas de racine de l'unité d'ordre ℓ , la proposition précédente admet la réciproque suivante :

PROPOSITION I.2.2.- Si K ne contient pas de racine de l'unité d'ordre ℓ et si x est un élément de $V(\bar{\psi})$ qui n'est pas une puissance ℓ-ème, alors il existe un ψ-corps et un seul N tel que $N' = L'(\sqrt[n]{x})$.

On dira que N est le ψ-corps associé à l'élément x de $V(\bar{\psi})$ ou que x est un élément de $V(\bar{\psi})$ associé à N ; on a la proposition suivante :

PROPOSITION I.2.3.- On suppose toujours que K ne contient pas de racine de l'unité d'ordre ℓ . Soient x_1 et x_2 deux éléments de $V(\bar{\psi})$ qui ne sont pas des puissances ℓ-èmes dans K et soient N_1 et N_2 les ψ-corps associés. On a $N_1 = N_2$ si et seulement si il existe un entier a premier à ℓ et un x de K tels que $x_1 = x_2^a x^n$.

§ .2.- Conditions de non ramification

On conserve les notations introduites en I.1 et l'on suppose que K ne contient pas de racine de l'unité d'ordre ℓ . Comme au § .I, nous donnons ici sans dé-

monstration les résultats de [1] dont nous avons besoin dans la suite.

II.1. - Les ψ-corps non ramifiés

DÉFINITION II.1.1. - Nous dirons que le ψ corps N est non ramifié si l'extension N/L est non ramifiée.

Nous aurons besoin de séparer du cas général un cas spécial que nous définissons ainsi :

DÉFINITION II.1.2. - Le cas spécial est le cas où ℓ est totalement décomposé dans le plus grand sous-corps de L de degré premier à ℓ .

Nous étudions les ψ-corps non ramifiés sous l'une ou l'autre des hypothèses suivantes :

a) ℓ ne divise pas le degré $[L' : L]$ de L'/L ;

b) on n'est pas dans le cas spécial.

II.2. - Générateurs des ψ-corps non ramifiés

DÉFINITION II.2.1. - Soit x un élément de K ; nous disons que x est n-primaire si l'extension $K(\zeta, \sqrt[n]{x})/K(\zeta)$ est non ramifiée.

PROPOSITION II.2.2. - Soit x un élément de $V(\bar{\psi})$; on a :

1) si x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ, alors x est n-primaire ;

2) si b) est vérifiée et si x est n-primaire, alors x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ ; dans ce cas x est une puissance n-ème dans tous les complétés de K au-dessus de ℓ .

PROPOSITION II.2.3. - On suppose a) ou b) vérifiée. Si x est un élément de $V(\bar{\psi})$ qui n'est pas une puissance ℓ-ème et si N est le ψ-corps qui lui est associé, alors les deux assertions suivantes sont équivalentes :

1) N est un ψ-corps non ramifié ;

2) l'idéal principal engendré par x dans K est une puissance n-ème et x est n primaire.

§. III. - Applications

III. 1. - Le cas $K = \mathbb{Q}$

Nous partons de $L = \mathbb{Q}(\zeta)$ et de $\psi = \omega$; on a alors $\bar{\psi} = 1$, donc $K = \mathbb{Q}$ et $V(\psi) = \mathbb{Q}^*$. La proposition II.2.2. montre qu'il n'y a pas de ω-corps non ramifié. En particulier, en prenant $n = \ell$, on retrouve le fait que la partie du ℓ-groupe des classes du ℓ-ème corps cyclotomique associée au caractère ω est triviale.

III. 2. - Le cas K quadratique

On pose $\theta = \cos \frac{2\pi}{n}$ et $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2 - 1)})$ où d est un entier sans facteur carré. Si $d \neq (-1)^{(\ell-1)/2} \ell$, le corps L est une extension quadratique de $\mathbb{Q}(\theta)$ différente de $\mathbb{Q}(\zeta)$ et $L/\mathbb{Q}$ est cyclique de degré $\varphi(n)$ sur $\mathbb{Q}$. Le corps L' est le corps $\mathbb{Q}(\sqrt{d}, \zeta)$ et il y a une injection et une seule de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ telle que $\bar{\psi}$ est l'homomorphisme d'ordre 2 de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$, de noyau $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{d}))$. Pour ces choix de L et de ψ, on a donc $K = \mathbb{Q}(\sqrt{d})$. Dans toute la suite nous nous plaçons dans cette situation ; le cas spécial est alors le cas $\ell = 3$ et $d \equiv -3 \bmod 9$. La démonstration du lemme suivant est évidente.

LEMME III.2.1. - *Un élément de K^* est dans $V(\bar{\psi})$ si et seulement si sa norme sur $\mathbb{Q}$ est la puissance n-ème d'un rationnel.*

Montrons maintenant la proposition suivante :

PROPOSITION III.2.2. - *Soit N un ψ-corps ; une condition suffisante pour que le ψ-corps N soit non ramifié est qu'il existe, dans l'ensemble des éléments de $V(\bar{\psi})$ associé à N, un x vérifiant les trois conditions suivantes :*

1) *x est un entier de K qui n'est divisible par aucun entier rationnel différent de ± 1 ;*

2) *la norme de x sur $\mathbb{Q}$ est la puissance n-ème d'un entier rationnel premier à 2ℓ ;*

3) *x n'est pas une puissance ℓ-ème dans K mais est une puissance ℓ-ème dans un complété de K en une place divisant ℓ.*

De plus, si l'on n'est pas dans le cas spécial, cette condition suffisante est nécessaire.

Démonstration. - Si $\mathfrak{a}$ est un idéal entier de K, nous convenons de noter

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} \tilde{\mathfrak{r}}_k^{\tilde{s}_k}$$

la décomposition de $\mathfrak{a}$ en produit de puissance d'idéaux premiers, les $\mathfrak{p}_i$ étant inertes, les $\mathfrak{q}_j$ ramifiés, les $\mathfrak{r}_k$ décomposés et les $\tilde{\mathfrak{r}}_k$ étant les conjugués des $\mathfrak{r}_k$; de plus, on suppose $s_k \geq \tilde{s}_k$ et l'on note p_i, q_j et r_k les nombres premiers contenus respectivement dans $\mathfrak{p}_i$, $\mathfrak{q}_j$ et $\mathfrak{r}_k$. Soit alors x un élément de $V(\bar{\psi})$ vérifiant 1), 2) et 3) et soit N le ψ-corps associé ; pour prouver la première partie de la proposition, il suffit, compte tenu des propositions II.2.2 et II.2.3, de voir que l'idéal $(x)_K$ engendré par x dans K est la puissance n-ème d'un idéal de K. La condition 1) implique que $(x)_K$ est de la forme :

$$\prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} .$$

La condition 2) montre alors que les m_j et les s_k sont divisibles par n l'idéal $(x)_K$ est donc une puissance n-ème.

Pour prouver la deuxième partie de la proposition, nous supposons que nous ne sommes pas dans le cas spécial. Soient N un ψ-corps non ramifié et y un élément de $V(\bar{\psi})$ qui lui est associé. D'après la proposition II.2.3, l'idéal $(y)_K$ engendré par y dans K est la puissance n-ème d'un idéal et y est n-primaire. Le lemme d'approximation montre qu'il existe un α dans K tel que $z = y\alpha^n$ est un entier de K premier à 2ℓ. Soit $(z)_K$ l'idéal de K engendré par z ; si

$$(z)_K = \prod_i \mathfrak{p}_i^{n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} \tilde{\mathfrak{r}}_k^{\tilde{s}_k} ,$$

on a :

$$z^2 = x \prod_i p_i^{2n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k r_k^{2s_k}$$

où x est un entier de K qui n'est divisible par aucun entier rationnel différent de ± 1. D'autre part, $(z)_K$ est la puissance n-ème d'un idéal, donc n divise les n_i, les m_j et les $\tilde{s}_k$ et donc (proposition I.2.3) x est associé à N et vérifie 1) et 2). Enfin la proposition II.2.2. montre que y, donc z, donc x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ, c'est-à-dire que x vérifie 3) ; cela achève la démonstration.

Rappelons les résultats suivants :

LEMME III.2.3.- Soit $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteur carré et soit x un entier de K. Il existe a et b dans $\mathbb{Z}$ tel que $x = \frac{1}{2}(a+b\sqrt{d})$ et on a l'équivalence :

1) $(a,b) = 1$ ou $(a,b) = 2$ et $d \not\equiv 1 \mod 4$;

2) x n'est divisible par aucun entier rationnel différent de ± 1.

LEMME III.2.4.- Soit x un entier de K ; pour tout entier naturel i on pose $x^i = \frac{1}{2}(a_i+b_i\sqrt{d})$ avec a_i et b_i dans $\mathbb{Z}$. Si la norme de x est première à ℓ, il existe un entier i premier à ℓ tel que ℓ divise $b_i d$ et l'on peut toujours trouver un tel i divisant $\ell - (\frac{d}{\ell})$.

Démonstration.- Si ℓ divise d, c'est clair. Sinon, la norme de l'entier x étant première à ℓ, x lui-même est premier à ℓ ; en conséquence $x^{\ell-(d/\ell)}$ est congru à un rationnel modulo ℓ, ce qui implique le lemme.

On rappelle que $n = \ell^r$; alors :

PROPOSITION III.2.5.- On reprend les notations du lemme III.2.4 et l'on suppose de plus que la norme de x est la puissance n-ème d'un rationnel premier à ℓ. Si i est un entier naturel premier à ℓ tel que ℓ divise $b_i d$, alors x est une puissance n-ème dans un complété de K au-dessus de ℓ si et seulement si :

1) ℓ^{r+1} divise $b_i d$ si l'on n'est pas dans le cas spécial

2) et ℓ^{r+2} divise $b_i d$ si l'on est dans le cas spécial.

Démonstration.- Désignons par $\mathfrak{l}$ un idéal premier de K au-dessus de ℓ, par e son indice de ramification, par $\hat{K}$ le complété de K en ℓ et, pour un entier naturel j, par U^j le groupe des unités de $\hat{K}$ congrues à 1 modulo la puissance j-ème de l'idéal maximal de $\hat{K}$. Le cas spécial correspond à $\hat{K} = \mathbb{Q}_3(\sqrt{-3})$.

LEMME III.2.6.- Un élément u de U^1 est une puissance n-ème si et seulement si :

1) u est dans U^{1+er} si l'on n'est pas dans le cas spécial,

2) u est dans U^{2+er} si l'on est dans le cas spécial.

Revenons à la démonstration de notre proposition. Soit $x^i = \frac{1}{2}(a_i + b_i\sqrt{d})$ de norme m^n avec m entier rationnel premier à ℓ ; on suppose que ℓ divise $b_i d$ et l'on note ℓ^α la plus grande puissance de ℓ qui divise $b_i d$. Supposons tout d'abord que ℓ ne divise pas d ; alors ℓ^α divise b_i et l'égalité $m^n = (a_i^2/4) + (b_i^2 d/4)$ montre que $(a_i/2)$ est une puissance n-ème modulo $l^{2\alpha}$. D'autre part m étant premier à ℓ, a_i est premier à ℓ ; l'égalité $x^i = (a_i/2)(1 + b_i\sqrt{d}/a_i)$ et le lemme III.2.6 montrent alors que x^i, donc x, est une puissance n-ème si et seulement si $\alpha \geq r+1$. Dans le cas où ℓ divise d on conclut à l'aide d'un raisonnement similaire.

Rappelons enfin le résultat suivant démontré dans [2] : soit m un rationnel ; on définit une famille de polynômes en posant $P_o(X;m) = 2$, $P_1(X;m) = X$ et $P_k(X;m) = X P_{k-1}(X;m) - m P_{k-2}(X;m)$; on a alors :

PROPOSITION III.2.7. - Soit x un élément de K dont la norme est m^n avec m rationnel ; x est une puissance ℓ-ème dans K si et seulement si le polynôme $P_\ell(X; m^{n/\ell}) - \mathrm{tr}(x)$ où $\mathrm{tr}(x)$ est la trace de x n'a pas de racine rationnelle.

Les propositions III.2.2, III.2.5, III.2.7 et le lemme III.2.3 se résument dans le théorème suivant :

THÉORÈME III.2.8. - On pose $n = \ell^r$; le corps L et le caractère ψ sont ceux définis au début de ce paragraphe III.2. Alors :

1) si l'on n'est pas dans le cas spécial, l'existence d'un ψ-corps non ramifié est équivalente à l'existence de deux entiers rationnels a et b vérifiant les trois conditions suivantes :

i) $(a,b) = 1$ ou 2 et ℓ^{r+1} divise bd ;

ii) $a^2 - db^2 = 4m^n$ pour un entier rationnel m premier à 2ℓ ;

iii) $P_\ell(X; m^{n/\ell}) - a$ n'a pas de racine rationnelle ;

2) si l'on est dans le cas spécial, alors l'existence de deux entiers rationnels a et b vérifiant, d'une part la condition

i_s) $(a,b) = 1$ et ℓ^{r+2} divise bd

et d'autre part les conditions ii) et iii) de 1) impliquent l'existence d'un ψ-corps non ramifié.

COROLLAIRE III.2.9.- Soient a et m deux entiers rationnels tels que :

1) $(m, 2\ell) = (a, m) = 1$;

2) $a^2 - 4m^n$ n'est pas un carré, est divisible par ℓ^{2r+1} si $\ell \neq 3$ et par 3^{2r+2} si $\ell = 3$;

3) le polynôme $P_\ell(X; m^{n/\ell})$ - a n'a pas de racine rationnelle.

Alors, le groupe des classes du corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ possède un élément d'ordre n .

Démonstration.- L'existence d'un ψ-corps non ramifié implique l'existence d'un quotient cyclique d'ordre n du groupe des classes de L ; si un tel quotient existe, alors il existe une classe d'ordre n .

Remarque III.2.10.- Si $\ell \equiv 3 \mod 4$, alors $L = \mathbb{Q}(\theta, \sqrt{-3(a^2-4m^n)})$. La classe d'ordre n dont le corollaire III.2.9 assure l'existence ne provient pas d'une classe d'ordre n du corps quadratique $\mathbb{Q}(\sqrt{-3(a^2-4m^n)})$: en effet, $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-3(a^2-4m^n)}))$ agit non trivialement sur les groupes de Galois des ψ-corps, donc agit non trivialement sur les classes d'ordre n associées aux ψ-corps non ramifiés.

En s'inspirant d'un raisonnement de Honda ([3]), on peut maintenant montrer le résultat suivant :

PROPOSITION III.2.11.- Il existe une infinité de corps réels et une infinité de corps imaginaires cycliques de degré $\varphi(n)$ sur $\mathbb{Q}$ et contenant le sous-corps réel maximal de $\mathbb{Q}(\zeta)$ qui possèdent une classe d'ordre n .

Démonstration.- Posons $\alpha = 2r+2$ ou $2r+1$ suivant que $\ell = 3$ ou $\ell \neq 3$. Choisissons un entier naturel a qui n'est pas une puissance ℓ-ème et qui est congru à 2 modulo ℓ^α . Considérons le corps $M = \mathbb{Q}(\mu, \sqrt[\ell]{a})$ où μ est une racine de l'unité d'ordre ℓ^α ; M est galoisien sur $\mathbb{Q}$ et les $(\ell-1)$ éléments non triviaux de $\mathrm{Gal}(M/\mathbb{Q}(\mu))$ forment une classe de conjugaison de $\mathrm{Gal}(M/\mathbb{Q})$; nous notons S l'ensemble des nombres premiers dont le Frobenius tombe dans cette classe ; S est infini. Les nombres premiers de S sont congrus à 1 mod ℓ^α et a n'est pas une puissance ℓ-ème modulo ces nombres premiers. Prenons m dans S . Alors $a^2 - 4m^n$ est divisible par ℓ^α ; de plus, $P_\ell(X; m^{n/\ell})$ est

congru à X^ℓ modulo ℓ, donc le polynôme $P_\ell(X; m^{n/\ell})$ n'a pas de racine rationnelle. En conséquence (corollaire III.2.9), le corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ possède une classe d'ordre n si a^2-4m^n n'est pas un carré. Posons $a^2 - 4m^n = y^2\, d(m)$ où $d(m)$ est un entier sans carré. On sait (théorème de Thue) que l'équation $a^2 - 4X^m = Y^2 d$, où X et Y sont les inconnues et a et d sont des constantes entières, n'a qu'un nombre fini de solutions entières. On en déduit que, lorsque m décrit l'ensemble infini S, on obtient une infinité d'entiers $d(m)$; les m étant positifs, presque tous les $d(m)$ sont négatifs, donc on a une infinité de corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ réels et ils possèdent une classe d'ordre n.

En reprenant le même raisonnement avec a congru à -2 modulo ℓ^α et en faisant décrire à m les opposés des éléments de S (i.e. $-m$ est dans S), on trouve une infinité de $d(m)$ positifs, donc une infinité de corps imaginaires L qui possèdent une classe d'ordre n, C.Q.F.D.

Terminons ce travail par quelques exemples particuliers.

Le cas $n = 3$ a été étudié en détail dans [2] ; on y montre qu'il n'y a pas lieu de séparer le cas spécial, i.e. que la partie 1 du théorème III.2.8 est valable sans restriction.

Le cas $n = 5$. Soit d un entier rationnel sans facteur carré et non divisible par 5, soit $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ et soit ψ l'injection de $\mathrm{Gal}(L/\mathbb{Q})$ dans $(\mathbb{Z}/5\mathbb{Z})^*$ telle que $\bar{\psi}$ est l'homomorphisme d'ordre 2 dont le noyau est $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{d}))$. Le corps $\mathbb{Q}(\theta)$ étant le corps $\mathbb{Q}(\sqrt{5})$, les corps $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ et $\mathbb{Q}(\theta, \sqrt{5d(\theta^2-1)})$ coïncident ; il y a donc une injection ψ^* de $\mathrm{Gal}(L/\mathbb{Q})$ dans $(\mathbb{Z}/5\mathbb{Z})^*$ telle que $\bar{\psi}^*$ est l'homomorphisme d'ordre 2 dont le noyau est $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{5d}))$. Soit maintenant H le sous-groupe du groupe des classes de L formé des éléments annulés par 5 ; ce groupe est un $\mathbb{F}_5[\mathrm{Gal}(L/\mathbb{Q})]$- module semi-simple et donc se décompose en une somme $H_1 \oplus H_2 \oplus H_\psi \oplus H_{\psi^*}$ où H_1, H_2, H_ψ et H_{ψ^*} sont les sous-groupes de H correspondant respectivement au caractère unité, au caractère d'ordre 2, à ψ et à ψ^*. Les groupes H_1 et H_2 sont triviaux puisque les nombres de classes de $\mathbb{Q}$ et de $\mathbb{Q}(\sqrt{5})$ sont égaux à 1. La non-trivialité de H_ψ (resp. de H_{ψ^*}) est équivalente à l'existence d'un ψ-corps (resp. d'un ψ^*-corps) non ramifié. Enfin, lorsque d décrit les entiers sans facteur carré non divisibles par 5, les corps $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ décrivent toutes les extensions cycliques de degré 4 de $\mathbb{Q}$ qui contiennent $\mathbb{Q}(\sqrt{5})$; les

résultats établis précédemment donnent donc le critère suivant : un corps cyclique du degré 4 contenant $\mathbb{Q}(\sqrt{5})$ a un nombre de classes divisible par 5 si et seulement si il est de la forme $\mathbb{Q}(\theta, \sqrt{(a^2-4m^5)(\theta^2-1)})$ où a et m sont deux entiers rationnels vérifiant :

1) $(m, 10) = (a, m) = 1$;

2) $a^2 - 4m^5$ est divisible par 125 et n'est pas un carré ;

3) le polynôme $X^5 - 5mX^3 + 5m^2X - a$ n'a pas de racine rationnelle.

On peut remarquer que $\mathbb{Q}(\theta, \sqrt{(a^2-4m^5)(\theta^2-1)}) = \mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(a^2-4m^5)})$ qui est la forme donnée dans [2].

Exemple numérique. - Prenons $m = 11$, alors $4m^5 = 644\,204$ et $644\,204 \equiv (52)^2$ mod. 125 ; par conséquent, si l'on prend $a \equiv \pm 52$ mod 125, alors $a^2 - 4m^5$ est divisible par 125. De plus, si l'on prend $a \not\equiv 0, 1, -1$ mod. 11, on voit, en réduisant modulo 11, que les conditions 1) et 3) sont vérifiées. En prenant $a = 677, 698, 823, 927$ on trouve que les deux corps réels $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(-1487)})$ et $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(-314)})$ et les deux corps imaginaires $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(1721)}$ et $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(53)})$ ont un nombre de classes divisible par 5 .

Le cas $n = 9$. Soient d un entier sans facteur carré, et $L = \mathbb{Q}(\theta, \sqrt{(\theta^2-1)})$; on vérifie que $L = \mathbb{Q}(\theta, \sqrt{-3d})$. Le corollaire III.2.8 entraîne donc le résultat suivant : s'il existe deux entiers rationnels a et m tels que :

1) $(m, 6) = (a, m) = 1$,

2) $a^2 - 4m^9$ est divisible par $3^6 = 729$ et n'est pas un carré,

3) et $X^3 - 3m^3X - a$ n'a pas de racine rationnelle, alors le groupe des classes de $\mathbb{Q}(\theta, \sqrt{-3(a^2-4m^9)})$ a un élément d'ordre 9 .

Exemple numérique. - Prenons $m = 7$, alors $4m^9 = 161\,414\,428$ et $161\,414\,428 \equiv 706$ mod 3^6 ; d'autre part, $706 \equiv (187)^2$ mod 3^6 ; en conséquence, si l'on prend $a \equiv \pm 187$ mod 3^6, alors $a^2 - 4m^9$ est divisible par 3^6 . De plus, si l'on prend $a \not\equiv 0, 1, -1$ mod 7 on voit, en réduisant modulo 7 que 1) et 3) sont vérifiées. En prenant $a = 10\,393, 12\,206$ on trouve que les deux corps réels $\mathbb{Q}(\theta, \sqrt{2\,713})$, $\mathbb{Q}(\theta, \sqrt{12\,786})$ possèdent une classe d'ordre 9 .

-:-:-:-

BIBLIOGRAPHIE

[1] Ph. SATGÉ, Construction de corps résolubles non ramifiés, Séminaire de l'Université de Caen (1977).

[2] Ph. SATGÉ, Corps résolubles et divisibilité de nombre de classes d'idéaux, l'Enseignement Mathématique, à paraître.

[3] T. HONDA, On real quadratic fields whose class numbers are multiples of 3 , J. reine angew. Math. 233 (1968), 101-102.

[4] O. NEUMANN, Relativ-quadratische Zahlkörper, deren Klassenzahlen durch 3 teilbar sind, Math. Nachrichten 56 (1973), 281-306.

-:-:-:-

Philippe SATGÉ
U.E.R. Sciences
Université de Caen
14032 CAEN CEDEX

Astérisque

GÉRALD TENENBAUM

Lois de répartition des diviseurs

Astérisque, tome 61 (1979), p. 205-212

<http://www.numdam.org/item?id=AST_1979__61__205_0>

Société Mathématique de France
Astérisque 61 (1979) p. 205-212

LOIS DE RÉPARTITION DES DIVISEURS

par

Gérald TENENBAUM

-:-:-:-

Une fois défini le concept de densité naturelle des suites d'entiers ([1]), qui peut s'interpréter dans un modèle probabiliste, toute une classe de problèmes trouvant leur origine en théorie des probabilités se pose à l'esprit : étant donnée une fonction f définie sur l'ensemble des entiers naturels, peut-on définir son "espérance" ? admet-elle un comportement déterminé pour "presque tous" les entiers ? peut-on caractériser, en particulier par sa "probabilité", l'ensemble des entiers pour lesquels f prend un ensemble de valeurs fixées ?

Si n désigne un nombre entier, le comportement de la fonction arithmétique $n \mapsto d(n)$ = nombre de diviseurs de n a été beaucoup étudié, notamment par Dirichlet pour sa valeur moyenne et par Hardy et Ramanujan pour son ordre normal - c'est-à-dire intuitivement son ordre de grandeur lorsque n parcourt une suite de densité unité. Nous nous sommes intéressés aux diviseurs des entiers sous un éclairage un peu différent, cherchant des renseignements non plus sur le nombre total des diviseurs d'un entier générique n mais sur leur répartition dans l'intervalle $[1,n]$.

Le premier exemple d'un tel travail se trouve chez Dickman [2] qui, en 1930, a étudié la densité de la suite des entiers n dont tous les diviseurs premiers

---

([1]) si $\mathcal{A}$ désigne une suite d'entiers, on appelle densité (naturelle) de $\mathcal{A}$ la limite, lorsqu'elle existe, de la quantité $x^{-1}\,\mathrm{card}\{n \leq x : n \in \mathcal{A}\}$ pour x infini ; les limites supérieure et inférieure sont appelées densités supérieure et inférieure.

sont inférieurs à $n^{1/t}$. Il montre que cette densité est égale à la valeur $\rho(t)$ d'une fonction continue (appelée depuis par certains auteurs fonction de Dickman) qui vérifie une équation différentielle aux différences :

$$(1) \qquad t\rho'(t) + \rho(t-1) = 0 \ .$$

Nous verrons plus loin que ce type d'équation joue un rôle important dans les problèmes de répartition des diviseurs.

En ce qui concerne la répartition des diviseurs quelconques (c'est-à-dire sans restriction de primalité) le seul résultat dont nous ayons eu connaissance est dû à Kátai, qui donne une condition nécessaire et suffisante pour que, relativement à une fonction additive [1] f, les diviseurs de n soient concentrés au voisinage de $\sqrt{n}$ (voir [5] et [6]) ; plus précisément, Kátai donne une propriété caractéristique des suites (n_k) pour lesquelles on a, pour tout ε positif,

$$\lim_{k\to\infty} \frac{1}{d(n_k)} \operatorname{card}\{d : d \mid n_k \quad \text{et} \quad (\tfrac{1}{2} - \varepsilon) < \frac{f(d)}{f(n)} < (\tfrac{1}{2} + \varepsilon)\} = 1 \ .$$

Si l'on prend pour f la fonction logarithme, on obtient une caractérisation de la suite des entiers n dont, pour tout ε positif, presque tous les diviseurs sont dans l'intervalle $]n^{\frac{1}{2}-\varepsilon}, n^{\frac{1}{2}+\varepsilon}[$.

*

Dans le but d'étudier la répartition des diviseurs des entiers, une idée naturelle consiste à définir pour chaque entier n une variable aléatoire D_n, qui prend les valeurs $\frac{\log d}{\log n}$, lorsque d parcourt les diviseurs de n, avec probabilité uniforme $1/d(n)$ - remarquons au passage que l'un des avantages de cette définition réside en ceci : si la décomposition de n en facteurs premiers est $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, alors D_n est somme des variables indépendantes X_i prenant les valeurs 0, $(\log p_i)/(\log n)$, ..., $\alpha_i(\log p_i)/(\log n)$ avec probabilité uniforme $1/\alpha_i+1$. La fonction de répartition de la variable aléatoire D_n est définie sur $[0,1]$ par

$$\text{Prob}\,(D_n \leq u) = \frac{1}{d(n)} \operatorname{card}\{d : d \mid n \quad \text{et} \quad d < n^u\} \ .$$

---

(1) Une fonction définie sur les entiers est dite additive si elle vérifie la propriété

$$\text{pgcd}(m,n) = 1 \Rightarrow f(mn) = f(m) + f(n) \ .$$

Une première approche du problème de la répartition des diviseurs consiste alors à étudier, pour tout u fixé dans $[0,1]$, la valeur moyenne en n de cette fonction de répartition. Dans un article écrit en commun avec Deshouillers et Dress [1], nous avons montré que, pour x infini, l'on a :

$$(2) \qquad \frac{1}{x} \sum_{n \leq x} \text{Prob}(D_n \leq u) = \frac{2}{\pi} \text{Arc sin}\sqrt{u} + O\left(\frac{1}{\sqrt{\log x}}\right) .$$

On trouve ainsi une nouvelle interprétation de la loi de l'Arcsinus, bien connue en Probabilités notamment parce qu'elle intervient dans les problèmes de marche aléatoire.

La formule (2) incite à se demander si la loi de D_n ne tend pas vers celle de l'Arcsinus lorsque n parcourt une suite de densité unité. La réponse à cette question est négative : nous montrons [9] que, pour toute loi de probabilité μ sur $[0,1]$, la suite des entiers n pour lesquels la loi de D_n tend vers μ est de densité nulle. Qualitativement, cela signifie que la moyenne (2) est obtenue en ajoutant des lois individuelles aux comportements tous différents et qu'il n'existe pas de loi de répartition valable pour une proportion non négligeable d'entiers. Ce résultat est une conséquence facile du fait que la densité supérieure de la suite des entiers n ayant, pour un nombre positif α fixé, au moins un diviseur dans l'intervalle $[n^{\alpha}, n^{\alpha+\varepsilon}]$ tend vers 0 avec ε. Dans [9] nous montrons un résultat plus fort :

Pour tout couple (λ,t) de $[0,1]\times[1,+\infty[$, la suite des entiers n ayant au moins un diviseur dans l'intervalle $[n^{\lambda/t}, n^{1/t}[$ possède une densité $h(\lambda,t)$ qui est une fonction continue pour $(\lambda,t) \neq (1,1)$ et qui vérifie

$$(3) \qquad \forall \varepsilon > 0 \quad \exists c(\varepsilon) \quad \forall t \geq 1+\varepsilon \quad h(\lambda,t) \leq c(\varepsilon)(1-\lambda)^{\delta} \left|\log(1-\lambda)\right|^{-\frac{1}{e}+\varepsilon}$$

où $c(\varepsilon)$ est une constante positive ne dépendant que de ε et où δ est égal à $1 - \frac{\log(e \log 2)}{\log 2} = 0,0860\ldots$.

Cela appelle plusieurs remarques :

tout d'abord, le fait que la densité $h(\lambda,t)$ existe montre que le cadre naturel pour l'étude de la répartition des diviseurs d'un entier n consiste bien à placer les diviseurs relativement aux puissances de n et, cela étant fait, que la répartition présente un certain caractère de régularité

. ensuite, l'exposant δ de la majoration (3) semble être optimal, à la lumière d'un résultat d'Erdös [4] qui montre, dans le cas où l'on choisit $\lambda = 1 - \frac{\log 2}{\log n}$, que le nombre correspondant d'entiers inférieurs à x est minoré pour tout ε positif et x assez grand par :

$$x \log x^{-\delta-\varepsilon}$$

. enfin, le remplacement des variables naturelles (α, β) variant dans $[0,1]\times[0,1]$ pour définir un intervalle $[n^{\alpha}, n^{\beta}[$ par les variables (λ, t) s'explique par le fait que la fonction analogue à $h(\lambda, t)$ n'est pas continue en $(\alpha, \beta) = (0,0)$ - nous verrons d'ailleurs que ces variables (λ, t) jouent un rôle privilégié lors de l'étude de la répartition des facteurs premiers.

La démonstration de l'existence de la densité $h(\lambda, t)$ se conduit en deux étapes : on trouve d'abord une majoration de la densité supérieure du type de (3) -en fait, pour la démonstration d'existence, il suffit d'une majoration qui tend vers 0 lorsque λ tend vers 1 - et on montre ensuite, en utilisant le principe d'inclusion-exclusion, que cette majoration implique l'existence et la continuité de la densité $h(\lambda, t)$. Lorsqu'on doit étudier une suite définie par des conditions sur les diviseurs dépendant d'un ou plusieurs paramètres, ce schéma de démonstration d'existence et continuité se retrouve très fréquemment ; cela méritait d'être souligné.

*

La majoration de la densité supérieure de la suite des entiers n ayant au moins un diviseur dans l'intervalle $[n^{\lambda/t}, n^{1/t}[$ nécessite une étude préalable de la répartition des facteurs premiers.

Levin et Fainleb ont montré [7] que la suite des entiers n ayant exactement k facteurs premiers dans $[n^{\lambda/t}, n^{1/t}[$ possède une densité $f_k(\lambda, t)$ qui est une fonction continue de (λ, t) mais ils ne donnent aucun renseignement sur l'ordre de grandeur de $f_k(\lambda, t)$. Nous redémontrons, par une méthode directe et élémentaire, différente de celle de Levin et Fainleb, l'existence des densités $f_k(\lambda, t)$ et nous établissons l'encadrement suivant [9], valable pour $t \geq k+1$ et $0 \leq \lambda \leq 1$

$$(4) \qquad \frac{\lambda}{k!} \log^k \frac{1}{\lambda} \left\{1 - \frac{2}{\Gamma(t-k)}\right\} \leq f_k(\lambda, t) \leq \frac{\lambda}{k!} \log^k \frac{1}{\lambda} \left\{1 + \frac{2}{\Gamma(t-k)}\right\}$$

où Γ désigne la fonction d'Euler.

Qualitativement, cela signifie que le nombre des facteurs premiers d'un entier n qui appartiennent à l'intervalle $[n^{\lambda/t}, n^{1/t}[$ peut être, en première approximation considéré comme une variable aléatoire qui suit une loi de Poisson de paramètre $\log\frac{1}{\lambda}$ ([1]). D'une certaine manière, ce résultat précise un théorème d'Erdös [3] qui spécifie que, si $p_i(n)$ désigne le i-ème facteur premier distinct de n on a, en moyenne, $\log\log p_i(n) \sim i$: en effet, le nombre moyen de facteurs premiers dans $[n^{\lambda/t}, n^{1/t}[$ est bien égal à la moyenne $\log\frac{1}{\lambda}$ de la loi de Poisson.

L'encadrement (4) est obtenu par une méthode nouvelle pour ce type de problème : on détermine une relation liant $f_{k+1}(\lambda,t)$ et $f_k(\lambda,t)$, soit :

$$(5) \qquad f_{k+1}(\lambda,t) = \frac{1}{k+1}\int_\lambda^1 f_k(\lambda, t-u)\,\frac{du}{u}$$

qu'on interprète comme un produit de convolution ; grâce à la transformation de Laplace, on en déduit des relations intégrales liant $f_k(\lambda,t)$ et la fonction de Dickman $t \longmapsto \rho(t)$, soit :

$$(6) \qquad \int_0^t f_k(\lambda,u)\ \rho(t-u)\ du = \frac{1}{k!}\int_0^t \rho\left(\frac{t-u}{\lambda}\right)\varphi_k(u)\ du$$

avec

$$\varphi_k(u) := \int_{\substack{[\lambda,1]^k \\ \Sigma x_i \le u}} \frac{dx_1}{x_1}\cdots\frac{dx_k}{x_k}\ ;$$

l'encadrement (4) est alors déduit de la combinaison de ces équations intégrales et de certaines équations aux dérivées partielles et aux différences, vérifiées par les f_k, qui dérivent, grâce aux relations (5), de

$$(7) \qquad t\frac{\partial}{\partial t} f_o(\lambda,t) = f_o(\lambda,t-1) - f_o(\lambda,t-\lambda)\ .$$

On notera que l'équation (7) est une généralisation de l'équation (1) car la fonction $(\lambda,t) \longmapsto \rho(\frac{t}{\lambda})$ vérifie (7) pour $t \le 1$.

([1]) Sous la condition $t \ge k+1$ (qui pourrait d'ailleurs être remplacée par $t \ge k+\varepsilon$). Cette condition correspond en fait à l'hypothèse d'indépendance des facteurs premiers $p_1, \ldots, p_k$ dans $[n^{\lambda/t}, n^{1/t}[$ puisque, si $t<k$, la relation $p_1 \ldots p_k \le n$ introduit une restriction supplémentaire.

En faisant tendre t vers l'infini dans (4) on voit que chaque densité $f_k(\lambda,t)$ admet une limite qui est une fonction continue de λ sur $[0,1]$. Pour les diviseurs quelconques, la densité analogue à $f_k(\lambda,t)$ n'est non identiquement nulle que pour $k=0$ [11] ; elle est alors égale à $1-h(\lambda,t)$. Nous montrons [10] que la fonction $h(\lambda,t)$ admet pour t infini une limite $h(\lambda)$ qui est une fonction continue de λ. On a :

$$(8) \qquad (1-\lambda) \leq h(\lambda) \leq 6(1-\lambda)^{\delta} .$$

De plus, $h(\lambda)$ est également la limite, pour y infini, de la valeur $d(\lambda,y)$ de la densité de la suite des entiers ayant au moins un diviseur dans l'intervalle $[y^{\lambda}, y[$.

*

Un autre aspect de la répartition des diviseurs réside dans les propriétés de la fonction arithmétique définie, pour tout couple (λ,t) de $[0,1]\times[1,+\infty[$ par

$$\Delta(\lambda,t,n) := \mathrm{Prob}\left(\frac{\lambda}{t} \leq D_n < \frac{1}{t}\right) .$$

La formule (2) montre que cette fonction possède pour tout couple (λ,t) une valeur moyenne ; nous montrons [11] qu'elle possède une fonction de répartition, c'est-à-dire que, pour tout réel x, la suite des entiers n tels que

$$\Delta(\lambda,t,n) < x$$

possède une densité $H(x)$.

Cette densité a une propriété remarquable : la mesure de Stieljes dH est une combinaison linéaire infinie de mesures de Dirac aux points dyadiques $a2^{-b}$ (a,b entiers) de l'intervalle $[0,1]$. Cela implique en particulier que si l'on se donne une fonction $n \longmapsto \psi(n)$ tendant vers l'infini arbitrairement lentement, il existe une suite d'entiers $\mathcal{A}$ de densité unité telle que, pour tout entier n de $\mathcal{A}$, le nombre des diviseurs dans $[n^{\lambda/t}, n^{1/t}[$ est soit nul, soit supérieur à $\frac{d(n)}{\psi(n)}$ ([1]).

Ce dernier résultat suggère que les diviseurs d'un entier "aléatoire" n sont

([1]) Ce résultat est d'ailleurs optimal en ce sens que, sauf cas triviaux, on ne peut remplacer ψ par une fonction constante.

concentrés au voisinage d'un nombre restreint de diviseurs privilégiés et donc que la répartition des diviseurs possède des trous du type $[n^{\lambda_1}, n^{\lambda_2}[$ ne contenant aucun diviseur de n. Nous étudions [12] la taille maximale de la différence $(\lambda_2 - \lambda_1)$ pour un tel intervalle ; plus précisément, si nous désignons par

$$1 = d_1 < d_2 < \ldots < d_\tau = n$$

la suite croissante des diviseurs de n, nous montrons que la fonction arithmétique

$$n \longmapsto \log^{-1} n \max_{i=1}^{\tau-1} \log \frac{d_{i+1}}{d_i}$$

possède une fonction de répartition $f(x)$ dont l'ordre de grandeur est voisin de x lorsque x tend vers 0. On a :

$$(9) \qquad c_1 x \log^{-1} \frac{1}{x} \leq f(x) \leq c_2 x \log \frac{1}{x}$$

où c_1 et c_2 sont deux constantes absolues positives.

La démonstration de ce résultat utilise des techniques semblables à celles des précédents. La borne inférieure de (9) est obtenue en introduisant une fonction de deux variables $f(x,t)$ qui minore $f(x)$ pour toute valeur de t et qui vérifie la relation

$$(10) \qquad t \frac{\partial}{\partial t} f(x,t) = f(x \frac{t}{t-1}, t-1) .$$

On retrouve ainsi dans ce cas particulier l'importance des équations différentielles aux différences dans les problèmes liés à la répartition des diviseurs.

-:-:-:-

BIBLIOGRAPHIE

[1] J.-M. DESHOUILLERS, F. DRESS, G. TENENBAUM, Lois de répartition des diviseurs, 1, à paraître à Acta Arithm. 36 (n°4).

[2] K. DICKMAN, On the frequency of numbers containing prime factors of a certain relative magnitude, Ark. Mat. Astr. Fys. 22 (1930), 1-14.

[3] P. ERDÖS, On the distribution function of additive functions, Ann. of Math. 47 (1946), 1-20.

[4] P. ERDÖS, Sur une inégalité asymptotique en théorie des nombres, Vestnik Leningrad Univ. 13 (1960), 41-49 (en russe).

[5] I. KÁTAI, On the distribution of solutions of special diophantine equations, Mat. Lapok 20 (1969), 117-122 (en hongrois).

[6] I. KÁTAI, On the distribution of additive fonctions on the set of divisors, Publicationes Math. 24 (1-2) (1977), 91-96.

[7] B. V. LEVIN and A. S. FAINLEB, Applications of some integral equations to problems of number theory, Uspchi Mat. Nauk 22 (1967), n° 3 (135) 199-197) (= Russian Math Surveys 22 (1967), n° 3, 119-204).

[8] G. TENENBAUM, Sur deux fonctions de diviseurs, J. London Math. Soc. (2) 14 (1967), 521-526 et Corrigendum à mon article "sur deux fonctions de diviseurs" J. London Math. Soc. (2) 17 (1978), 212.

[9] G. TENENBAUM, Lois de répartition des diviseurs, 2, à paraître à Acta Arithm. 38 (n° 1).

[10] G. TENENBAUM, Lois de répartition des diviseurs, 3, à paraître à Acta Arithm. 39 (n° 1).

[11] G. TENENBAUM, Lois de répartition des diviseurs, 4, à paraître à Ann. Inst. Fourier.

[12] G. TENENBAUM, Lois de répartition des diviseurs, 5, soumis pour publication à Proc. London Math. Soc.

-:-:-:-

Gérald TENENBAUM
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX

Astérisque

R. C. VAUGHAN

A survey of some important problems in additive number theory

Astérisque, tome 61 (1979), p. 213-222

<http://www.numdam.org/item?id=AST_1979__61__213_0>

Société Mathématique de France
Astérisque 61 (1979) p. 213-222

A SURVEY OF SOME IMPORTANT PROBLEMS IN ADDITIVE NUMBER THEORY

by

R.C. VAUGHAN

-:-:-:-

Since many aspects of additive number theory were covered by Halberstam's adress [27] to the recent meeting on Additive Number Theory in Bordeaux, I shall content myself by adumbrating just two of the principal areas which have interested me particularly. These are problems dealing with

(A) sums of kth powers,

(B) sums of primes.

One of the fascinating aspects of these problems is the interplay between them and other areas of analytic number theory.

A. - The typical problem involving sums of kth powers is

1. - Waring's problem, regarding which there is an excellent survey article by Ellison [24]. Let $g(k)$ denote the smallest s such that for every $n \geq 1$ there exist $x_i \geq 0$ such that $n = x_1^k + \dots + x_s^k$. The problem of evaluating g has been essentially solved for all k except $k = 4$. It is thought that

$$g(k) = 2^k + [(\tfrac{3}{2})^k] - 2 . \tag{1}$$

It is classical that this holds whenever $k \neq 4, 5$ and

$$\{(\tfrac{3}{2})^k\} < 1 - 2^{-k}[(\tfrac{3}{2})^k] . \tag{2}$$

Mahler [38] has shown that (2) has at most a finite number of exceptions, and Stemmler [50] has verified that (2) holds for $k \leq 200\,000$. Incidently, this has lead to interesting questions concerning distribution modulo 1, see Mahler [39].

More recently, Chen [3,4,5] has shown that (1) also holds when $k=5$. This leaves $k=4$. Here there has been considerable recent progress. The upper bound for $g(4)$ has been reduced first to 34, then to 30 and 23 and finally to 22 by Dress [22], Dress [23], Thomas [51] and Thomas [52] respectively. It is trivial that $g(4) \geq 19$.

2. - The more interesting and challenging problem is that of the estimation of $G(k)$, the smallest s such that every sufficiently large integer is the sum of at most s kth powers of positive integers. So far only $G(2)$ and $G(4)$ are known. If one defines $\Gamma(k)$ to be the least s such that for every q, n the congruence $x_1^k + \ldots + x_s^k \equiv n \pmod q$ is soluble, then one has $G(k) \geq \max(k+1, \Gamma(k))$. One might guess that equality occurs. The current of play for small values of k is as follows ;

$G(2) = 4$, Lagrange [34],

$G(3) \leq 7$, Linnik [35], Watson [66],

$G(4) = 16$, Davenport [12],

$G(5) \leq 23$, $G(6) \leq 36$, Davenport [13, 14],

$G(7) \leq 53$, Davenport's method (the claim $G(7) \leq 52$ of Sambasiva Rao [46] is fallacious),

$G(8) \leq 73$, Narasimhamurti [43].

For larger k, the principle results in the last thirty years have been

$G(k) < k(3 \log k + 11)$, Vinogradov [63, 64],

$G(k) < k(3 \log k + 9)$ $(k = 2^m)$, $G(k) < k(3 \log k + 7)$ $(k \neq 2^m)$, } Tong [53],

$G(k) < k(3 \log k + 5.2)$, Chen [2],

$G(k) < k(2 \log k + 4 \log\log k + 2 \log\log\log k + 13)$, Vinogradov [65].

This last result is superior to Chen's only when $k > 6\,103\,975\,350$. More recently, the method described in Vaughan [59] gives $G(9) \leq 91$, $G(10) \leq 107$, $G(11) \leq 122$, $G(12) \leq 137$, $G(13) \leq 153$, $G(14) \leq 168$, $G(15) \leq 184$, $G(16) \leq 200$, $G(17) \leq 216$ and $G(k) < k(3 \log k + 4.2)$.

3. - Homogeneous additive equations. - Davenport and Lewis [15] have shown that there is an $s(k)$ such that if $s \geq s(k)$, then for every $c_1, \ldots, c_s$ (with $c_1 c_2 < 0$

if k is even) the equation $c_1x_1^k+\ldots+c_sx_s^k=0$ has a non-trivial solution in integers $x_1,\ldots,x_s$. They showed that it is possible to take $s(k)\leq k^2+1$ when $k\leq 6$ or $k\geq 18$ giving partial verification of Artin's conjecture that any form of odd degree represents 0 non-trivially whenever $s\geq k^2+1$.

Vaughan [59] has partly filled the gap by showing that $s(k)\leq k^2+1$ is permissible when $11\leq k\leq 17$.

4. - Simultaneous homogeneous additive equations. - Davenport and Lewis [17] have treated the system

$$\begin{cases} c_{11}x_1^k+\ldots+c_{1n}x_n^k=0, \\ \quad\vdots\qquad\qquad\vdots \\ c_{r1}x_1^k+\ldots+c_{rn}x_n^k=0. \end{cases}$$

There are many open questions in connection with this. Earlier [16], they had studied pairs of additive cubics

$$(2)\qquad \begin{cases} c_1x_1^3+\ldots+c_nx_n^3=0, \\ d_1x_1^3+\ldots+d_nx_n^3=0. \end{cases}$$

They showed that if $n\geq 18$, then there is a non-trivial solution of (2), and that there exist $c_1,d_1,\ldots,c_{15},d_{15}$ such that (2) with $n=15$ has only the trivial solution. Cook [10] has replaced the 18 by 17 and Vaughan [57] has reduced this to 16, the best possible.

For related matters see Davenport and Lewis [18].

5. - Vinogradov's mean value theorem. - Let $I(X,s,k)$ denote the number of solutions of

$$\begin{cases} x_1+\ldots+x_s=y_1+\ldots+y_s \\ x_1^2+\ldots+x_s^2=y_1^2+\ldots+y_s^2 \\ \quad\cdots\qquad\cdots \\ x_1^k+\ldots+x_s^k=y_1^k+\ldots+y_s^k \end{cases}$$

with $0<x_i,\ y_i\leq X$. Karatsuba and Korobov [31] have shown that

$$I(X,s,k)<C(k,\ell)\,X^{2s-\frac{1}{2}(k+1)+\delta}$$

with $\delta = \frac{1}{2}k(k+1)(1-\frac{1}{k})^{\ell}$ whenever $s \geq k^2+k\ell$. For an earlier account of this see Vinogradov's book [63, 64]. There are a number of important applications.

The value of $C(k, \ell)$ is not usually very important in additive number theory, but the contrary is true in the applications to multiplicative number theory.

Recently Bombieri has shown that it is possible to take $\delta = \frac{1}{2}k^2(1-\frac{1}{k})^{\ell}$ whenever $s \geq k\ell$.

B. - The archetypal problem concerning sums of primes is Goldbach's problem. This stems from two letters from Goldbach to Euler in 1742 in which he conjectures that every even natural number is the sum of two primes and that every integer greater than 2 is the sum of three primes. He included unity as a prime. There have been three lines of attack on these problems.

1. - Direct applications of sieve methods. - There are excellent surveys of earlier work in Halberstam and Roth [29] and Halberstam and Richert [28]. The most recent result is the celebrated theorem of Chen [6, 7] to the effect that for $n>n_o$ either $2n = p+p_1$ or $2n = p+p_1p_2$. There are shorter proofs by Ding, Pan and Wang [21], and Ross [44]. Ross [45] has also shown that the primes can be restricted in various ways. Graham [26] has made n_o effectively computable.

2. - Indirect applications of sieve methods. - This stems from Shnirel'man [47, 48]. He showed that there exists a constant C such that if $n>n_o$, then $n = p_1+\ldots+p_s$ with $s \leq C$. His C is very large, and the method was later superceded by the more powerful Hardy-Littlewood-Vinogradov method (see below). However, alternative lines of approach are always of interest in connection with difficult problems. In recent times Chechuro and Kuzjashev [1], and Siebert [49] obtained $C = 10$ by this method. This is improved to $C = 6$ in Vaughan [56]. This last paper contains a brief survey of previous work via this method.

Perhaps more interesting is the fact that this method readily yields a C_o such that every $n>1$ can be written as the sum of at most C_o primes. The most recent work in this direction is

$C_o = 6 \times 10^9$, Klimov [32],

$C_o = 115$, Klimov, Pil'tai and Sheptitskaya [33],

$C_o = 75$, Deshouillers [19],

$C_o = 27$, Vaughan [58].

This last paper contains two different methods, in one of which the calculations are easier. However the more difficult method would permit a smaller C_o provided certain calculations could be carried out. Deshouillers [20] has thereby obtained $C_o = 26$.

3. - The Hardy-Littlewood-Vinogradov method. - By obtaining non-trivial estimates for

$$(3) \qquad \sum_{p \le N} e^{2\pi i \alpha p} \quad \text{when} \quad |\alpha - \frac{a}{q}| \le q^{-2}, \ (a,q) = 1, \ (\log N)^A < q \le N (\log N)^{-A},$$

Vinogradov [62] gave an unconditional proof that every sufficiently large odd integer is the sum of at most three primes. Linnik [36, 37] (see also Chudakov [9]), Montgomery [40] and Vaughan [60] have given different ways of estimating (3).

Immediately following Vinogradov's work, Chudakov [8], van der Corput [11] and Estermann [25] all showed that if $E(x) = |\{n \le x : 2n \ne p + p'\}|$, then $E(x) = O_A(x \log^{-A} x)$. Thix was later improved to $O(x \exp(-c\sqrt{\log x}))$ and $O(x^{1-\delta})$ by Vaughan [54] and Montgomery and Vaughan [42] respectively.

For another question connected with Goldbach's problem, see Montgomery and Vaughan [41], and Vaughan [55].

Let me conclude by emphasizing the interaction between this subject and others of analytic number theory. Recently the ideas contained in Vaughan [60] have been used

(a) to give (Vaughan [61]) a new and simple proof of Bombieri's prime number theorem,

(b) by Heath-Brown and Patterson [30] as an aid in their resolution of Kummer's problem concerning cubic Gaussian sums, to the effect that the arguments are uniformly distributed modulo 2π.

-:-:-:-

REFERENCES

[1] E.F. CHECHURO and A.A. KUZJASHEV, The representation of large integers by sums of primes, Studies in Number Theory, n° 3, 45-50, Izdat. Saratov Univ., Saratov 1969.

[2] J.R. CHEN, On Waring's problem for nth powers, Acta Math. Sinica, 8 (1958), 253-257 ; Chinese Math. - Acta 8 (1966), 849-853 (1967).

[3] J.R. CHEN, Waring's problem for g(5), Sci. Record (Peking) (N.S.) 3 (1959), 327-330.

[4] J.R. CHEN, Waring's problem for g(5) = 37, Sci. Sinica 13 (1964), 335.

[5] J.R. CHEN, Waring's problem for g(5) = 37, Sci. Sinica 13 (1964), 1547-1568.

[6] J.R. CHEN, On the representation of a large even integer as the sum of a prime and the product of at most two primes, Kexue Tongbao (Foreign Lang. Ed.) 17 (1966), 385-386.

[7] J.R. CHEN, On the representation of a larger even integer as the sum of a prime and the product of at most two primes, Sci. Sinica 16 (1973), 157-176.

[8] N.G. CHUDAKOV, On the density of the set of even numbers which are not representable as a sum of two odd primes, Izv. Akad. Nauk SSSR Ser. Nat. 2 (1938), 25-40.

[9] N.G. CHUDAKOV, On Goldbach-Vinogradov's theorem, Ann. of Math. (2) 48 (1947), 515-545.

[10] R.J. COOK, Pairs of additive equations, Michigan Math. J. 19 (1972), 325-331.

[11] J.G. van der Corput, Sur l'hypothèse de Goldbach pour presque tous les nombres pairs, Acta Arithmetica 2 (1937), 266-290.

[12] H. DAVENPORT, On Waring's problem for fourth powers, Ann. of Math. 40 (1939), 731-747.

[13] H. DAVENPORT, On sums of positive integeral kth powers, Amer. J. Math. 64 (1942), 189-198.

[14] H. DAVENPORT, On Waring's problem for fifth and sixth powers, Amer. J. Math. 64 (1942), 199-207.

[15] H. DAVENPORT and D.J. LEWIS, Homogeneous additive equations, Proc. Roy. Soc. Ser. A 274 (1963), 443-460.

[16] H. DAVENPORT and D. J. LEWIS, Cubic equations of additive type, Philos. Trans. Roy. Soc. Ser. A 261 (1966), 97-136.

[17] H. DAVENPORT and D. J. LEWIS, Simultaneous equations of additive type, Philos. Trans. Roy. Soc. Ser. A 264 (1969), 557-595.

[18] H. DAVENPORT and D. J. LEWIS, Two additive equations, Number Theory (Proc. Symp. Pure Math., vol. XII, Houston, Texas, 1967), 74-98, Amer. Math. Soc. Providence, R.I., 1969.

[19] J.-M. DESHOUILLERS, Amélioration de la constante de Šnirelman dans le problème de Goldbach, Sém. Delange-Pisot-Poitou 1972/73, Fasc. 2, n° 17, Paris, 1973.

[20] J.-M. DESHOUILLERS, Sur la constante de Šnirel'man, Sém. Delange-Pisot-Poitou 1975/76, Fasc. 2, exp. n° G16, Paris, 1977.

[21] X.-X. DING, C.-D. PAN and Y. WANG, On the representation of every large even integer as a sum of a prime and an almost prime, Sci. Sinica 28 (1975), 599-610.

[22] F. DRESS, Amélioration de la majoration de g(4) dans le problème de Waring : $g(4) \leq 34$, Sém. Delange-Pisot-Poitou 1969/70, fasc. 1, exp. 15, Paris, 1970.

[23] F. DRESS, Sur le problème de Waring pour les puissances quatrièmes, C.R. Acad. Sci. Paris, Sér. A, 272 (1971), 457-459.

[24] W. J. ELLISON, Waring's problem, Amer. Math. Monthly 78 (1971), 10-36.

[25] T. ESTERMANN, On Goldbach's problem : Proof that almost all even positive integers are sums of two primes, Proc. London Math. Soc. (2) 44 (1938), 307-314.

[26] S. W. GRAHAM, Applications of sieve methods, Dissertation, University of Michigan, Ann Arbor, 1977.

[27] H. HALBERSTAM, Additive Number Theory, Proc. Springer Lecture Notes (à paraître).

[28] H. HALBERSTAM and H.-E. RICHERT, Sieve methods, Academic Press, London, 1974.

[29] H. HALBERSTAM and K. F. ROTH, Sequences, vol. 1, Clarendon Press, Oxford, 1966.

[30] D. R. HEATH-BROWN and S. J. PATTERSON, paper in preparation.

[31] A. A. KARATSUBA and N. M. KOROBOV, A mean-value theorem, Dokl. Akad. Nauk SSSR 149 (1963), 245-248.

[32] N.I. KLIMOV, Apropos the computations of Shnirel'man's constant, Volzh. Mat. Sb. Vyp. 7 (1969), 32-40.

[33] N.I. KLIMOV, G.Z. PIL'TAI and T.A. SHEPTITSKAYA, Estimation of the absolute constant in the Goldbach-Shnirel'man problem, Issled. Teor. Chisel, Saratov 4 (1972), 35-51.

[34] J.L. LAGRANGE, Nouv. Mém. Acad. Roy. Soc. Berlin 1770 (1772), 123-133.

[35] Ju. V. LINNIK, On the representation of large numbers as sums of seven cubes, Mat. Sb. 12 (54) (1943), 218-224.

[36] Ju. V. LINNIK, On the possibility of a unique method in certain problems of "additive" and "distributive" prime number theory, Dokl. Akad. Nauk SSSR 48 (1945), 3-7.

[37] Ju. V. LINNIK, A new proof of the Goldbach-Vinogradov theorem, Mat. Sb. 19 (61)(1946), 3-8.

[38] K. MAHLER, On the fractional parts of the powers of a rational number II, Mathematika 4 (1957), 122-124.

[39] K. MAHLER, An unsolved problem on the powers of 3/2, J. Austral. Math. Soc. 8 (1968), 313-321.

[40] H.L. MONTGOMERY, Topics in multiplicative number theory, Lecture Notes in Math. 227 (1971), Berlin and New York.

[41] H.L. MONTGOMERY and R.C. VAUGHAN, Error terms in additive prime number theory, Quart. J. Math. Oxford (2) 24 (1973), 207-216.

[42] H.L. MONTGOMERY and R.C. VAUGHAN, The exceptional set in Goldbach's problem, Acta Arithmetica 27 (1975), 353-370.

[43] V. NARASIMHAMURTI, On Waring's problem for 8th, 9th and 10th powers, J. Indian Math. Soc. 5 1941), 122.

[44] P.M. ROSS, On Chen's theorem that each large even number has the form p_1+p_2 or $p_1+p_2p_3$, J. London Math. Soc. (2) 10 (1975), 500-506.

[45] P.M. ROSS, A short intervals result in additive prime number theory, J. London Math. Soc. (2) 17 (1978), 219-227.

[46] K. SAMBASIVA RAO, On Waring's problem for smaller powers, J. Indian Math. Soc. 5 (1941), 117-121.

[47] L.G. SHNIREL'MAN, On additive properties of numbers, Izv. Donskowo Politeh. Inst., 14 (1930), 3-28.

[48] L.G. SHNIREL'MAN, Über additiven Eigenschaften von Zahlen, Math. Ann. 107 (1933), 649-690.

[49] H. SIEBERT, Darstellung als Summe von Primzahlen (Diplomarbeit, Marburg, 1968).

[50] R.M. STEMMLER, The ideal Waring theorem for exponents 401-200 000, Math. Comp. 18 (1964), 144-146.

[51] H.E. THOMAS Jr., A numerical approach to Waring's problem for fourth powers, Dissertation, University of Michigan, Ann Arbor, 1973.

[52] H.E. THOMAS Jr., Waring's problem for twenty two biquadrates, Trans. Amer. Math. Soc., 193 (1974).

[53] K.-C. TONG, On Waring's problem, Advancement in Math. 3 (1957), 602-607.

[54] R.C. VAUGHAN, On Goldbach's problem, Acta Arithmetica 22 (1972), 21-48.

[55] R.C. VAUGHAN, A new estimate for the exceptional set in Goldbach's problem, Analytic Number Theory (Proc. Symp. Pure Math., vol. XXIV, St. Louis, Missouri, 1972), 315-320, Amer. Math. Soc. Providence, R.I., 1973.

[56] R.C. VAUGHAN, A note on Shnirel'man's approach to Goldbach's problem, Bull. London Math. Soc., 8 (1976), 245-250.

[57] R.C. VAUGHAN, On pairs of additive cubic equations, Proc. London Math. Soc. (3) 34 (1977); 354-364.

[58] R.C. VAUGHAN, On the estimation of Shnirel'man's constant, J. fur Reine Angew. Math., 290 (1977), 93-108.

[59] R.C. VAUGHAN, Homogeneous additive equations and Waring's problem, Acta Arithmetica, 33 (1977), 231-253.

[60] R.C. VAUGHAN, Sommes trigonométriques sur les nombres premiers, C.R. Acad. Sci. Paris, Sér. A, 258 (1977), 981-983.

[61] R.C. VAUGHAN, An elementary method in prime number theory, Acta Arithmetica, to appear.

[62] I.M. VINOGRADOV, Some theorems concerning the theory of primes, Recueil Math. 2 (44), 2 (1937), 179-195.

[63] I.M. VINOGRADOV, The method of trigonometrical sums in the theory of numbers, Trav. Inst. Math. Steklov 23 (1947).

[64] I.M. VINOGRADOV, The method of trigonometrical sums in the theory of numbers, translated from the Russian, revised an annotated by K.F. Roth and A. Davenport, Interscience, London, 1954

[65] I.M. VINOGRADOV, On an upper bound for G(n) , Izv. Akad. Nauk SSSR 23 (1959), 637-642.

[66] G. L. WATSON, A proof of the seven cube theorem, J. London Math. Soc. 26 (1951), 153-156.

-:-:-:-

R.C. VAUGHAN
Mathematics Department
Imperial College
LONDON

Astérisque

WILLIAM A. VEECH

Ergodic theory and uniform distribution

Astérisque, tome 61 (1979), p. 223-234

<http://www.numdam.org/item?id=AST_1979__61__223_0>

Société Mathématique de France
Astérisque 61 (1979) p. 223-234

Ergodic Theory and Uniform Distribution

by
William A. Veech*

1. Introduction. We shall discuss the applications of ergodic theory to two problems in the theory of uniform distribution. The first problem concerns uniform distribution in a general compact group, the second uniform distribution modulo 1.

If K is a compact (Hausdorff, topological) group, a sequence $S = \{s_n\}$ in K is a K-sequence if S generates a dense subgroup of K. S is a K_σ-sequence if it has the additional properties that (i) for every $n > 0$ $(s_1,\dots,s_n) = (s_{k+1},\dots,s_{k+n})$ for infinitely many k, and (ii) $S^{-1}S = \{s_i^{-1}s_j\}$ generates a dense subgroup of K. Any K-sequence may be used to construct a K_σ-sequence.

We recall that a sequence $R = \{r_n\}$ is called a uniformly (resp. well) distributed sequence generator, u.d.s.g. (resp. w.d.s.g.), if for every compact group K and every K-sequence $S \subseteq K$, the sequence $T(R,S) = \{t_n\}$, where

$$t_n = \prod_{j=1}^{n} s_{r_j} \tag{1.1}$$

is uniformly (resp. well) distributed in K ([13], [15], [17]).

Examples of u.d.s.g.'s are given in [13], [15]. One such is $r_1 = 9$, $r_2 = 2$, and in general r_n = the length of the gap between the n^{th} and $(n+1)^{st}$ '1' in the sequence 123456789101112... .

At the present time one knows no example of a w.d.s.g. . However, Losert and Rindler [8] have proved there exist sequences $R \subseteq \mathbb{Z}$ which satisfy a similar condition which we shall not describe

*Research supported by NSF - MCS 78-01858

here . Any Losert-Rindler sequence serves as a "program" (like (1.1)) for writing down a well distributed sequence in terms of a given K-sequence. This is the purpose for which the notion of a w.d.s.g. was introduced, and the Losert-Rindler result suffers only an aesthetic defect of being nonexplicit.

In preparation of the statement of the first theorm, let $\lambda = \{\lambda_1, \lambda_2, \ldots\}$ be a sequence of integers such that $\lambda_n \geq 2$. Also, set $\lambda_0 = 1$. For every $k \in \mathbb{Z}$ such that $k \neq -1$ there is a unique integer $\tau = \tau(k) \geq 0$ such that

$$k+1 = \lambda_0 \lambda_1 \cdots \lambda_\tau (a\lambda_{\tau+1} + b) \tag{1.2}$$

with $a \in \mathbb{Z}$ and $0 < b < \lambda_{\tau+1}$.

Notice in the theorem to follow that the K_σ-sequence begins at 0 (the definition is analogous).

1.3 Theorem. With notations as above, assume the sequence λ is bounded, and define $R = \{\tau(1), \tau(2), \ldots\}$. If K is a compact group, and if $S = \{s_0, s_1, \ldots\}$ is a K_σ-sequence in K, then T(R,S) (see (1.1)) is well distributed in K.

Next, let $X = \mathbb{R}/\mathbb{Z}$, and let $\theta \in X$ be an irrational. Given an "interval" $I \subset X$. whose length is denoted $|I|$, define $S_n(x) = S_n(x, \theta, I)$, $x \in X$, $n > 0$, to be the number of j such that $0 \leq j < n$ and $x + j\theta \in I$.

A theorem of Kesten [7] asserts that there exists $x \in X$ such that $S_n(x) - n|I|$ is bounded (in n) only if $|I| \in \mathbb{Z}\theta$ modulo 1. (The converse is easy and classical.) A simple proof of Kesten's theorem is given by Furstenberg-Keynes -Shapiro [6] (see also [17]). The following is a sharpening of Kesten's theorem:

1.4 Theorem. With notations as above, suppose there exist $x \in X$ and $M < \infty$ such that

$$E_M(x) = \{n \mid |S_n(x) - n|I|| \leq M\} \tag{1.5}$$

has positive upper density. Then modulo 1, $|I| \in \mathbb{Z}\theta$.

2. Monothetic groups. In this section X denotes an infinite compact monothetic group and $\theta \in X$ an element which generates a dense subgroup. X will be written additively. Let μ be normalized Haar measure on X.

Fix a finite set $E \subseteq X$ such that E contains a coset of no subgroup of X other than $\{0\}$. Let K be a compact group, and let there be given a continuous map $\varphi: E^c \to K$ such that φ does not extend to be continuous on X.

Define $X' = E + \mathbb{Z}\theta$, and define a map $X' \to K^{\mathbb{Z}}$ by $m_x(n) = \varphi(x+n\theta)$, $x \in X'$, $n \in \mathbb{Z}$. The closure, M, of the image of X' is invariant under the left shift, $\sigma(\sigma m(n) = m(n+1))$. In addition one has from [16], Section 2, that (a) (σ, M) is minimal (every σ-orbit in M is dense in M), (b) (σ, M) is uniquely ergodic (there is a unique normalized σ-invariant Borel measure on M), and (c) the map $\pi m_x = x$, $x \in X'$, is well defined and extends to a continuous map $M \xrightarrow{\pi} X$ such that $\pi\sigma m = \pi m + \theta$, $m \in M$; moreover, π is one-to-one on $\pi^{-1}X'$. Because of (b) and (c), we shall write μ also for the normalized invariant measure on M.

Next, let $N = M \times K$, and define $T: N \to N$ by

$$T(m,k) = (\sigma m, m(0)k) \quad . \tag{2.1}$$

Let ν be normalized Haar measure on K, and set $\omega = \mu \times \nu$. Clearly, ω is T-invariant.

If (T,N) is uniquely ergodic, a theorem of Oxtoby [9] implies that for each $z \in N$ the sequence $\{T^n z,\ n \geq 1\}$ is ω-well distributed in N. In particular, the sequence of "second coordinates" is well distributed in K. When $z = (m_x, e)$, $x \in X'$, the second coordinate of $T^n z$, $n > 0$, is

$$\varphi^{(n)}(x) = \varphi(x+(n-1)\theta)\varphi(x+(n-2)\theta)\ldots\varphi(x) \quad . \tag{2.2}$$

It is Furstenberg's observation that (T,N) is uniquely ergodic if ω is <u>ergodic</u> for T (if $A \subseteq N$ is measurable, and if $T^{-1}A = A$, then $\omega(A) = 0$ or $\omega(A^c) = 0$)([5]). The necessary and sufficient condition that ω <u>fail</u> to be ergodic is that there exist a nontrivial continuous irreducible unitary representation $\rho: K \to U(d)$ and a nonconstant measurable function $F: X \to \mathbb{C}^d$ such that

$$F(x+\theta) = \rho(\varphi(x))F(x) \quad \text{(a.e. } \mu) \quad . \tag{2.3}$$

(See [5], [14].)

3. Proof of Theorem 1.3. Let λ be as in the introduction, and define $\Lambda_0 = 0$ and $\Lambda_n = \lambda_1\lambda_2\ldots\lambda_n$, $n > 0$. We set $X = \varprojlim^{-1} \mathbb{Z}/\Lambda_n\mathbb{Z}$ and view X as the set of sequences, $x = (x_1, x_2, \ldots)$, such that $0 \leq x_n = x_n(x) < \Lambda_n$ and $x_{n+1} - x_n \in \Lambda_n\mathbb{Z}$ for all $n > 0$. Letting $\theta = (1,1,\ldots)$, the subgroup $\mathbb{Z}\theta$ is dense in X. μ denotes normalized Haar measure on X.

Let $E = \{-\theta\}$. If $x \notin E$, define $\tau(x) = \ell - 1$, where ℓ is the least integer such that $x_\ell \neq \Lambda_\ell - 1$. $\tau(\cdot)$ is continuous on E^c, and $\lim_{x \to -\theta} \tau(x) = \infty$. In terms of the function $\tau(k)$, $k \neq -1$, defined in (1.2), one has (a) $\tau(k\theta) = \tau(k)$, $k \neq -1$, and (b) $\tau(x) = \tau(x_n(x))$ for <u>any</u> n such that $x_n(x) \neq \Lambda_n - 1$.

Define partitions $\mathcal{P}_n = \{P_{nk} | 0 \le k < \Lambda_n\}$ by setting $P_{nk} = \{x | x_n(x) = k\}$. The function $T_n(x) = \Lambda_n - 1 - x_n(x)$ assumes the constant value $\Lambda_n - 1 - k$ on P_{nk} for each k. Remark (b) of the preceding paragraph implies $\tau(x+j\theta)$ is constant on P_{nk} if $j \neq \Lambda_n - 1 - k$. As for the exceptional value of j, define $P_{nk}^{\ell} = \{x \in P_{nk} | \tau(x+(\Lambda_n - 1 - k)\theta) = n+\ell\}$, $\ell \ge 0$. An easy counting argument shows $\mu(P_{nk}^{\ell}) = (\lambda_{n+\ell} - 1)\frac{\Lambda_{n-1}}{\Lambda_{n+\ell}}\mu(P_{nk})$ holds for $\ell \ge 0$. If in particular λ is bounded (by Q), the last inequality implies

$$\mu(P_{nk}^{\ell}) \ge Q^{-(\ell+1)}\mu(P_{nk}) \quad . \tag{3.1}$$

If $x \in X$, write $P_n = P_n(x)$ for the element of $\mathcal{P}$ which contains x. Given an $L^1(\mu)$ function $F:X \to \mathbb{C}^d$, the martingale theorem, together with a standard argument, shows

$$\lim_{n\to\infty} \frac{1}{\mu(P_n)} \int_{P_n} |F(y)-F(x)| \mu(dy) = 0 \tag{3.2}$$

Next, suppose $K \neq \{e\}$ is a compact group, and let $S = \{\psi(0), \psi(1), \ldots\}$ be a K_σ-sequence in K. Using τ and S, we define $\varphi(x) = \psi(\tau(x))$, $x \in E^c$. The facts $K \neq \{e\}$ and S is a K_σ-sequence easily imply φ has no limit at $-\theta$. We shall be interested in $\varphi^{(\Lambda_n)}$ which we denote by φ_n. Our earlier discussion implies there exist $A_{nk}, B_{nk} \in K$, $0 \le k \le \Lambda_n$, such that

$$\varphi_n(x) = A_{nk}\psi(n+\ell)B_{nk} \quad (x \in P_{nk}^{\ell}) \quad . \tag{3.3}$$

Indeed, of the Λ_n factors determining φ_n, all but one are constant on P_{nk}, and that factor is constantly $\psi(n+\ell) = \varphi(\tau(x+T_n(x)\theta))$ on P_{nk}^{ℓ}.

Suppose now that ρ is a nontrivial continuous irreducible unitary representation of K on $\mathbb{C}^d$, and suppose also that (2.3) has a nontrivial measurable solution. We replace K by $\rho(K) \neq \{e\}$, and reletter, so that (2.3) becomes

(2.3′) $$F(x+\theta) = \varphi(x)F(x) \ .$$

Now $\varphi(x) \in U(d)$, and (2.3′) implies $|F(\cdot)|$ is invariant under translation by θ, hence constant a.e. As F is assumed to be nontrivial, we may and shall assume that $|F(x)| = 1$ a.e. This will lead us to a contradiction, assumming λ is bounded (by Q).

Iterating (2.3′), one finds $F(x+m\theta) = \varphi^{(m)}(x)F(x)$, and this, plus the continuity of translation in $L^1(\mu)$, implies

(3.4) $$\lim_{m\theta\to 0} \|\varphi^{(m)}F-F\|_1 = 0 \ .$$

3.5 Lemma. With notations as above, there exists for every pair $\epsilon,q > 0$ a vector $v = v(\epsilon,q)$, $|v| = 1$, such that $|\psi(i)v-\psi(j)v| < 2\epsilon$, $0 \le i, j \le q$.

Proof: S is a K_σ-sequence, and therefore there exists an infinite set Γ such that $\psi(n+j) = \psi(j)$, $0 \le j \le q$, $n \in \Gamma$. Apply (3.4) ($m = \Lambda_n, n \in \Gamma$), and (3.2) to conclude that if $n \in \Gamma$ is large there exist $P_{nk} \in \mathcal{P}_n$, such that $(P_{nk}^\epsilon)^c = \{y \in P_{nk} \mid |\varphi_n(y)F(x)-F(x)| \ge \epsilon\}$ has measure less than $Q^{-(q+1)}\mu(P_{nk})$. From (3.1) one concludes $P_{nk}^\epsilon \cap P_{nk}^\ell \neq \emptyset$, $0 \le \ell \le q$. Finally, (3.3), the definition of P_{nk}^ϵ, and the facts $n \in \Gamma$ and $A_{nk}, B_{nk} \in U(d)$ imply that if $v = B_{nk}F(x)$, then $|v| = 1$ and $|\psi(i)v-\psi(j)v| < 2\epsilon$, $0 \le i, j \le q$. The lemma is proved.

Notice in the above that also $|\psi(i)^{-1}\psi(j)v-v| < 2\epsilon$, $0 \le i, j \le q$, $v = v(\epsilon,q)$. If we let $\epsilon \to 0$, $q \to \infty$ in such a way that $v(\epsilon,q) \to v_0$, then $|v_0| = 1$, and $\psi(i)^{-1}\psi(j)v_0 = v_0$, $i,j \ge 0$. As S is a K_σ-sequence $kv_0 = v_0$, $k \in K$. Irreducibility then implies $d = 1$, $K = \{e\}$, a contradiction. We conclude that (2.3) cannot have a nontrivial measurable solution. The discussion of Section 2 now implies Theorem 1.3. (The second coordinate of $T^n(\theta,\epsilon)$ is $\varphi^{(n)}(\theta) = \psi(\tau(n))\psi(\tau(n-1))\ldots\psi(\tau(1))$, where $\tau(k)$ is defined by (1.2)).

Remark on the case d = 1. Let λ be as in Section 1, possibly unbounded, and let $S = \{\psi(n)\}_{n\geq 0}$ be a sequence of complex numbers of absolute value 1. Define K to be the closed subgroup of U(1) generated by the terms of S. Form $X = X(\lambda)$, and set $\varphi(x) = \psi(\tau(x))$, $x \neq -\theta$. We wish to allow for the possibility that φ has a limit at $-\theta$; this means that $M = M(\lambda,\psi)$, rather than having $X(\lambda)$ for a "factor," may in fact itself be a "factor" of $X(\lambda)$ (more precisely, the quotient of $X(\lambda)$ by the periods of the extended function φ). Let $N = N(\lambda,\psi) = M\times K$ and $T = T(\lambda,\psi)$ be as in Section 2. Also, set $\omega = \omega(\lambda,\psi) = \mu\times\nu$, as in Section 2. Using the above, one may prove

3.6 Theorem. With notations as above, suppose $\sum_{n=0}^{\infty} |\psi(n+1)-\psi(n)| = \infty$. Then (T,N) is uniquely ergodic. Moreover, the point spectrum of T, relative to ω, is contained in $\Gamma(\lambda) = \{\chi(\theta) \mid \chi$ a continuous character on $X(\lambda)\}$.

If $\tilde{\lambda}$ is a second sequence, we write $\tilde{\lambda} \perp \tilde{\lambda}$ if $(\lambda_n, \tilde{\lambda}_n) = 1$ for all n. When $\tilde{\lambda} \perp \lambda$, the Chinese Remainder Theorem implies $\mathbb{Z}(\theta,\tilde{\theta})$ is dense in $X(\lambda)\times X(\tilde{\lambda})$, and this in turn implies $\sigma\times\tilde{\sigma}$ is uniquely ergodic on $M\times M$ for any given $\tilde{\psi}$. Suppose now that both ψ and $\tilde{\psi}$ satisfy the hypothesis of Theorem 3.6. As $\Gamma(\lambda) \cap \Gamma(\tilde{\lambda}) = \{1\}$, the point spectra of $T,\tilde{T}$, relative to $\omega,\tilde{\omega}$, have trivial intersection ($\{1\}$), and so by a well known result in ergodic theory, $T\times\tilde{T}$ is ergodic relative to $\omega\times\tilde{\omega}$. But $\omega\times\tilde{\omega}$ may be viewed as $(\mu\times\tilde{\mu})\times(\nu\times\tilde{\nu})$, $\nu\times\tilde{\nu}$ = Haar measure on $K\times\tilde{K}$, and so Furstenberg's princple (Section 2), plus the unique ergodicity of $\sigma\times\tilde{\sigma}$, implies $T\times\tilde{T}$ in uniquely ergodic.

The sequences $\varphi^{(n)}(0)$, $\tilde{\varphi}^{(n)}(0)$ are "q-muliplicative sequences"

(see [3] for definition and references). An immediate consequence of the above is that when $\lambda \perp \tilde{\lambda}$ and $\Psi, \tilde{\Psi}$ satisfy the hypothesis of Theorem 3.6, one has

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \Phi^{(n)}(0)\tilde{\Phi}^{(n)}(0) = 0 \quad .$$

It would be interesting to know whether other known (and unknown) properties of q-multiplicative sequences can be obtained from such considerations.

4. Irregularities of distribution modulo 1. In this section we suppose $X = \mathbb{R}/\mathbb{Z}$, and we fix $\theta \in X$ irrational. If $I \subseteq X$ is an interval and $\alpha, \beta \in \mathbb{R}$, define $\Phi = (\alpha-\beta)\chi_I - \beta\chi_{I^c}$. We regard Φ as having values in $K = K(\alpha,\beta)$, the closed subgroup of X generated by α and β (modulo 1). We note that $\Phi^{(n)}(x) = S_n(x)\alpha - n\beta$, where $S_n(x) = S_n(x,\theta,I)$ is defined in Section 1.

Let $\{\frac{P_n}{q_n}\}$ be the sequence of convergents to θ, and define $\Gamma^0(\theta) \subseteq X$ to be the set of t which admit a representation $t = \sum_{n=1}^{\infty} b_n q_n \theta$ (in X) such that $b_n \in \mathbb{Z}$ and $\lim_n b_n q_n \|q_n\theta\| = 0$. (Any two such representations agree for large n [16].) If $\alpha \in \mathbb{R}$, we also define $\Gamma^0_\alpha(\theta) = \{t \in \Gamma^0(\theta) \mid \lim_n b_n\alpha = 0 \text{ in } X\}$. As noted in [16], [17] we have (i) if θ has bounded partial quotients, then $\Gamma^0(\theta) = \mathbb{Z}\theta$, and (ii) if $t \notin \mathbb{Z}\theta$, then for almost all α, $t \notin \Gamma^0_\alpha(\theta)$.

The theorem below is proved in [16] for $\alpha = \frac{1}{2}$. Extension to the general case is sketched in [18], [17] and the details are carried out by Stewart in [12].

4.1 Theorem. *Let $\alpha, \beta \in \mathbb{R}$, $\alpha \notin \mathbb{Z}$. If for every k such that $k\alpha \neq 0$ (in X) $|I| \notin \Gamma^0_{k\alpha}(\theta)$ modulo 1, then (T,N) (Section 2) is uniquely ergodic.*

4.2 Corollary. ([17],[12]) *If* $|I| \notin \mathbb{Z}\theta$ *modulo* 1, *then for almost all* $\alpha \in \mathbb{R}$ *the sequence* $\{S_n(x)\alpha - n\beta\}$ *is well distributed modulo* 1 *for any choice of* $x \in X$ *and* $\beta \in \mathbb{R}$.

The corollary may be used to prove Theorem 1.4. To this end, suppose $|I| \notin \mathbb{Z}\theta$ modulo 1 but for some $x \in X$ and $M < \infty$ the set $E_M(x)$ (Section 1) has upper density $2\epsilon > 0$. Corollary 4.2 implies there exists α, $0 < \alpha < \frac{\epsilon}{2M}$ such that $\{S_n(x) - n\beta\}$ is well distributed modulo 1 for all β. Set $\beta = |I|\alpha$, and note for this choice that $\|S_n(x)\alpha - n|I|\alpha\| \leq |S_n(x)\alpha - n|I|\alpha| < \frac{\epsilon}{2}$ if $n \in E_N(x)$. Well distribution implies the set of n such that $\|S_n(x)\alpha - n|I|\alpha\| < \frac{\epsilon}{2}$ has upper density $\frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon < 2\epsilon$, and we have a contradiction. That is, $E_M(x)$ has upper density 0, and the theorem is proved.

When $\varphi = (\alpha - \beta)\chi_I - \beta\chi_{I^c}$ is regarded as taking values in $\mathbb{R}$, it is natural to prevent "drift" by requiring φ to have integral 0. But for a change of scale, this is tantamount to requiring $\varphi = (1-|I|)\chi_I - |I|\chi_{I^c}$. In what follows, $G = G(I)$ is the closed subgroup of $\mathbb{R}$ generated by $|I|$ and $1-|I|$. We assume $0 < |I| < 1$.

Define $T: X \times G \to X \times G$ by $T(x,y) = (x+\theta, y+\varphi(x))$. T preserves Haar measure on $X \times G$, which of course is infinite. Using a topological analogue of K. Schmidt's notion of an "essential value" of a cocycle ([11]), it is not difficult to prove

4.3 Proposition. Assume $|I|$ is rational or else $1, \theta$, and $|I|$ are rationally independent. Then T has a residual set of points with dense orbits. In particular, for a residual set of $x \in X$ the sequence $S_n(x) - n|I|$ is dense in $G(I)$.

One conjectures the conclusion of the proposition holds with

residual set of x replaced by 'measure 1 set of x.' (It does not hold for 'all x'. See Dupain [4].) One way to prove this is to prove T is ergodic (relative to Haar measure). This is so for $|I|=\frac{1}{2}$ (K. Schmidt [10]; Conze-Keane [2]) and also for almost all values of $|I|$ (Conze [1]). In [17] the question was raised whether $|I| \notin \Gamma^0(\theta)$ implies ergodicity. This is proved by M. Stewart [12] when θ has bounded partial quotients, and Stewart now claims a proof for general θ (oral communication). It is open whether any condition on $|I|$ is necessary for ergodicity (save $|I| \in \mathbb{Q}$ or $1,\theta,|I|$ rationally independent).

Stewart's work relies heavily on the work of Schmidt and Conze. The most important ingredients are Schmidt's notion of essential value, the Denjoy-Koksma lemma (used by Conze), and the following

4.4 Theorem (M. Stewart [12]). Assume θ has bounded partial quotients. If $t \notin \mathbb{Z}\theta$ modulo 1, then

$$\limsup_{n\to\infty} (\|q_n t\| - \tfrac{1}{2}q_n\|q_n\theta\|) > 0 \quad .$$

It would be of interest to have a formulation and proof of a nonabelian analogue of Theorem 4.1. At the present time one knows only that if θ has bounded partial quotients, if $|I| \notin \mathbb{Z}\theta$ modulo 1, and if K is a finite group with generators α,β, the homeomorphism (T,N) corresponding to $\varphi(x) = \alpha,\beta$ as $x \in I$, I^c is uniquely ergodic [14].

References

[1] Conze, J. P. "Équirépartition et Ergodicité de Transformations Cylindriques," Preprint, Université de Rennes (1976).

[2] Conze, J. P. and Keane, M. "Ergodicité d'un flot cylindrique," C. R. Acad. Sci. Paris (to appear).

[3] Coquet, J., Kamae, T., and Mendes-France, M. "Sur la mesure spectrale de certaines suites arithmétiques," preprint, l'Universite de Bordeaux.

[4] Dupain, Y. "Intervalles à restes majorés pour la suite $\{n\alpha\}$," Acta. Math. Acad. Sci. Hung., 29(1977), 289-303.

[5] Furstenberg, H. "Strict ergodicity and transformations of the torus," Amer. J. Math. 88(1961), 573-601.

[6] Furstenberg, H., Keynes, H. and Shapiro, L., "Prime flows in topological dynamics," Israel J. Math. 14(1973), 26-38.

[7] Kesten, H. "On a conjecture of Erdös and Szüsz related to uniform distribution mod 1," Acta. Arith. 12(1966/67), 193-212.

[8] Losert, V. and Rindler, H. "Uniform distribution and the mean ergodic theorem," preprint.

[9] Oxtoby, J. C. "Ergodic sets," Bull. Amer. Math. Soc. 58(1952) 116-136.

[10] Schmidt, K. "A Cylinder Flow Arising From Irregularity of Distribution," preprint, University of Warwick, 1975.

[11] Schmidt, K. "Cohomology and Skew Products of Ergodic Transformations," preprint, University of Warwick, 1974.

[12] Stewart, M. "Irregularities of uniform distribution," Ph.D. Thesis, Rice University, 1978.

[13] Veech, W. A. "Applications of ergodic theory to some problems of uniform distribution," Proc. Conf. on Ergodic Theory and Topological Dynamics (Univ. of Kentucky, 1971), Math Dept., Univ. of Kentucky, Lexington, Ky., 26-33.

[14] _____, "Finite group extension of irrational rotations, Israel J. Math. 21(1975) 240-259.

[15] _____, "Some questions of uniform distribution," Ann. of Math. (2)94(1971), 125-138.

[16] _____, "Strict ergodicity in zero dimensional dynamical systems and the Kronecker-Weyl theorem mod 2," Trans. Amer. Math. Soc. 140(1969), 1-33.

[17] _____, "Topological dynamics," Bull. Amer. Math. Soc., 83 (1977), 775-830.

[18] _____, "Well distributed sequences of integers," Trans. Amer. Math. Soc. 161(1971), 63-70.

William A. VEECH
Department of Mathematics
Rice University HOUSTON
U.S.A.

Astérisque

MARIE-FRANCE VIGNÉRAS

L'équation fonctionnelle de la fonction zêta de Selberg du groupe modulaire PSL $(2, \mathbb{Z})$

Astérisque, tome 61 (1979), p. 235-249

<http://www.numdam.org/item?id=AST_1979__61__235_0>

Société Mathématique de France
Astérisque 61 (1979) p. 235-249

L'EQUATION FONCTIONNELLE DE LA FONCTION ZÊTA DE SELBERG DU GROUPE MODULAIRE PSL(2,ℤ)

par
Marie-France VIGNÉRAS

1 - Cette équation est contenue dans la formule des traces de Selberg [21] et l'obtenir nécessite seulement de l'habileté dans le maniement d'intégrales, en suivant les méthodes données par Hejhal [17] pour obtenir l'équation fonctionnelle de la fonction zêta de Selberg des groupes cocompacts, sans éléments elliptiques. La fonction double-gamma définie et étudiée par Barnes [3] , [4] , [5] , [6] joue un rôle essentiel, analogue à celui de la fonction gamma dans l'équation fonctionnelle de la fonction zêta de Riemann. Guidé par le modèle des fonctions L d'Artin, à chaque classe de conjugaison primitive de PSL(2,ℤ), on associe un facteur :

$$Z_p(s) = \prod_{k\geq o} (1 - Np^{-s-k})$$

pour une classe hyperbolique primitive p, de norme Np,

$$Z_{e_2}(s) = [1 + tg(\frac{\pi s}{2} - \frac{\pi}{4})]^{1/2}$$

pour la classe elliptique primitive e_2 d'ordre 2

$$Z_{e_3}(s) = [1 + \sqrt{3}\ tg(\frac{\pi s}{3} - \frac{\pi}{6})]^{2/3}$$

pour la classe elliptique primitive e_3 d'ordre 3

$$Z_{par}(s) = \zeta(2s - 1)$$

où $\zeta(s)$ est la fonction zêta de Riemann, pour la classe parabolique primitive. On introduit ensuite un facteur à l'infini :

$$Z_\infty(s) = [\Gamma_2(s)^2\ \Gamma(s)^{-1}\ (2\pi)^s]^{1/6}$$

où $\Gamma_2(s)$ est la fonction double gamma de Barnes

$$\frac{1}{\Gamma_2(s+1)} = (2\pi)^{s/2} e^{-\frac{1}{2}s(s+1) - \frac{1}{2}\gamma s^2} \prod_{n\geq 1} (1+\frac{s}{n})^n e^{-s+\frac{s^2}{2n}}$$

et vérifiant l'équation $\frac{1}{\Gamma_2(s+1)} = \frac{\Gamma(s)}{\Gamma_2(s)}$ et $\Gamma(1) = 1$.

On définit alors une fonction zêta de Selberg modifiée en posant :

$$Z^*(s) = \prod_{p\in P} Z_p(s)\, Z_{e_2}(s)\, Z_{e_3}(s)\, Z_{par}(s)\, Z_\infty(s) \quad , \quad \text{Re } s > 1$$

où P est l'ensemble des classes hyperboliques de $PSL(2,\mathbb{Z})$; les facteurs elliptiques et paraboliques sont les facteurs exceptionnels. On a alors l'équation fonctionnelle :

(1) $\qquad Z^*(s) = Z^*(1-s).$

Remarques

Les facteurs sont des fonctions analytiques multiformes, les exposants 1/6, 1/2, 2/3 apparaissent dans la formule du genre pour $PSL(2,\mathbb{Z})$ et la fonction zêta de Selberg modifiée est bien définie.

Pour un sous-groupe Γ discret, à covolume fini de $PSL(2,\mathbb{R})$ et une représentation χ unitaire de dimension finie n de Γ, on a aussi une formule des traces. Quelle équation fonctionnelle en déduit-on ? Je ne sais donner qu'une réponse partielle : La valeur du facteur à l'infini s'obtient sans peine :

(2) $\qquad Z_\infty(s,\chi) = [\Gamma_2(s)^2\, \Gamma(s)^{-1}\, (2\pi)^s]^{n\mu}$

où μ est le volume de $\Gamma\backslash H$ pour la mesure $\frac{dx\, dy}{2\pi\, y2}$ sur le demi-plan supérieur H. Les facteurs hyperboliques sont ceux définis par Selberg :

(3) $\qquad Z_p(s,\chi) = \prod_{k\geq o} \det\,(1-\chi(p)\, Np^{-k-s})$

Pour des groupes Γ cocompacts sans éléments elliptiques, en posant $Z^*(s,\chi) = Z_\infty(s,\chi) \prod_{p\in P} Z_p(s,\chi)$, on a donc l'équation fonctionnelle $Z^*(s,\chi) = Z^*(1-s,\chi)$. Soit $\bar{\chi}$ la contragrédiente de χ, définie par $\bar{\chi}(\gamma) = \chi(\gamma^{-1})$; si p est une classe hyperbolique primitive, p^{-1} l'est aussi et $p \to p^{-1}$ définit une

bijection de P, comme $Z_p(s,\chi) = Z_{p^{-1}}(s,\chi)$, on en déduit :

$$Z^*(s,\chi) = Z^*(s,\bar{\chi})$$

L'équation fonctionnelle s'écrit dont aussi :

$$(4) \qquad Z^*(s,\chi) = Z^*(1-s,\bar{\chi})$$

écriture préférable, puisqu'elle reste vraie si Γ contient des éléments elliptiques. Le groupe engendré par une classe elliptique primitive e_m d'ordre m, est un groupe cyclique d'ordre m, et la représentation χ restreinte à ce groupe est une somme de caractères (représentations de degré 1) χ_j, pour $1 \leq j \leq n$ définis par $\chi_j(e_m) = e^{2i\pi x_j/n}$, où $0 \leq x_j \leq m-1$. Le facteur elliptique est égal à

$$(5) \qquad Z_{e_m}(s,\chi) = \prod_{j=1}^{n} Z_{e_m}(s+x_j)\, Z_{e_m}(x_j+\tfrac{1}{2})^{-1}$$

où $Z_{e_m}(s)$ est le facteur elliptique avec caractère trivial.

Enfin, pour les facteurs paraboliques apparaissant si Γ n'est pas cocompact, je n'ai aucun résultat, mis à part le cas où χ est trivial et $\Gamma = \Gamma_o(N)$ image dans $PSL(2,\mathbb{Z})$ de l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ telles que $c \equiv 0 \pmod N$, quand N est sans facteurs carrés, où utilisant la forme explicite de la formule des traces calculée par Hejhal [15] , [16], on obtient :

$$Z_{par}(s) = \left[(2\pi N)^{-s}\, \zeta(2s-1) \prod_{p \mid N} (1-p^{-2s})^{-1/2} \right]^{d(N)}$$

où d(N) est le nombre de diviseurs de N.

Pour des groupes de rang 1, où la formule des traces a été explicitement calculée par Gangolli [12], [13], le facteur à l'infini est un produit de fonctions gamma d'ordre inférieur où égal de l'ordre de la fonction zêta de Selberg, qui se calculent explicitement dans chaque cas.

2 - LA FONCTION DOUBLE GAMMA.

Cette fonction remarquable étudiée par Barnes vers 1900, ne figurant pas dans les tables de fonctions spéciales les plus connues, citée en exercice par Whittaker et Watson [24], a été utilisée récemment par Shintani [23], dans une formule limite de Kronecker pour les corps quadratiques réels. Son prolongement analytique p-adique apparait dans une formule de Cassou-Noguès [9] pour les fonctions L_p-adiques

au point 0.

Avant Barnes, ces fonctions avaient été introduites sous une forme différente par Hölder [18], Alexeiewsky [2], Glaisher [14], Kinkelin [19]. L'exposé de Barnes [3] est remarquable, aussi je me contenterai d'indiquer brièvement leurs principales propriétés :

2.1 - Définition par leur produit de Weierstraß (trois formes) :

$$\Gamma_2(z+1)^{-1} = (2\pi)^{z/2}\, e^{-z/2 - \frac{\gamma+1}{2}z^2} \prod_{k=1}^{\infty} \left[(1+\frac{z}{k})^k\, e^{-z+z^2/2k}\right]$$

$$= (2\pi)^{z/2}\, e^{-z/2 - \frac{\gamma+1}{2}z^2} \prod_{k=1}^{\infty} \left[\frac{\Gamma(k)}{\Gamma(z+k)}\, e^{z\psi(k) + \frac{z^2}{2}\psi'(k)}\right]$$

$$= (2\pi)^{2/2}\, e^{(\gamma-\frac{1}{2})z - (\frac{\pi^2}{6}+1+\gamma)z^2/2}\, \Gamma(z).z \prod_{\substack{n\geq 0\\ m\geq 0\\ n+m\neq 0}} \left[(1+\frac{z}{n+m})e^{-\frac{z}{n+m}+\frac{z^2}{2(n+m)^2}}\right]$$

chaque produit est convergent, γ est la constante d'Euler et $\psi(z) = \frac{\Gamma'}{\Gamma}(z)$.

2.2 - Formule de Stirling : si x est réel et croit indéfiniment, et $a \in \mathbb{C}$,

$$\mathrm{Log}\,\Gamma_2(x+a+1)^{-1} = \frac{x+a}{2}\log 2\pi - \log A + \frac{1}{12} - \frac{3x^2}{4} - ax + (\frac{x^2}{2} - \frac{1}{12} + \frac{a^2}{2} + ax)\log x + 0\,(\frac{1}{x})$$

où A est une constante définie par Kinkelin [19],

$$\mathrm{Log}\, A = \lim_{n\to\infty} [\mathrm{Log}(1^1.2^2\ldots n^n) - (\frac{n^2}{2} + \frac{n}{2} + \frac{1}{12})\,\mathrm{Log}\, n + \frac{n^2}{4}]$$

dont la valeur numérique est A = 1,28 24 27 13 ...

2.3 - Théorème de Gauss

$$\prod_{r=0}^{n-1}\prod_{s=0}^{n-1} \Gamma_2(z+\frac{r+s}{n})^{-1} = K(2\pi)^{n(n-1)z/2}\, n^{-n^2z^2/2 + nz}\, \Gamma_2(nz)^{-1}$$

où

$$K = A^{1-n^2}\, e^{\frac{n^2-1}{12}}\, (2\pi)^{-(n-1)/2}\, n^{-5/12}$$

2.4 - Formule des compléments : On pose $\Phi(z) = \dfrac{\Gamma_2(1+z)^{-1}}{\Gamma_2(1-z)^{-1}}$,

$$\Phi(z) = \frac{\pi}{\sin \pi z} \Phi(z-1)$$

2.5 - Relation de Kinkelin

$$\text{Log } \Phi(z) = z \text{ Log } 2\pi - \int_0^z \pi z \cot g \, \pi z \, dz$$

2.6 - Valeur au point 1/2

$$\Gamma_2(1/2)^{-1} = A^{-3/2} \, \pi^{-1/4} \, e^{1/8} \, 2^{1/24}$$

2.7 - Formule intégrale : si $\text{Re}(z+1) > 0$,

$$\text{Log } \Gamma_2(z+1) = - \int_0^\infty \frac{e^{-t}}{t(1-e^{-t})^2} \left[1 - zt - \frac{z^2 t^2}{2} - e^{-zt} \right] dt$$

$$+ \frac{z^2}{2} (1+\gamma) - \frac{3}{2} \text{ Log } \frac{2\pi}{2}$$

Par analogie avec la fonction gamma, on peut donner pour la fonction double-gamma, et plus généralement pour des fonctions gamma d'ordre n , $n \geq 1$ une définition d'Artin justifiée par la proposition suivante :

2.8 - Proposition : Pour tout $n \geq 1$, il existe une unique fonction $G_n(z)$ méromorphe telle que :

(1) $G_n(z+1) = G_{n-1}(z) \, G_n(z)$ pour $z \in \mathbb{C}$

(2) $G_n(1) = 1$

(3) pour $x \geq 1$, $G_n(x)$ est indéfiniment dérivable et $\frac{d^{n+1}}{dx^{n+1}} \text{ Log } G_n(x) \geq 0$

(4) $G_0(x) = x$

On reconnait la définition d'Artin de la fonction $\Gamma(x)$ pour $n = 1$. On définit ainsi des fonctions gamma d'ordre n en posant

$$\Gamma_n(z) = G_n(z)^{(-1)^{n-1}}$$

Cette proposition est une conséquence immédiate du théorème de Dufresnoy et Pisot [7], [11] qui fournit simultanément l'existence, l'unicité et le développement

en série de Weierstraß.

Théorème 2.9 (Dufresnoy et Pisot) - Soit $\varphi(x)$ une fonction k fois dérivable dont la dérivée $\varphi^{(k)}(x)$ d'ordre k , $k \geq 0$, est décroissante pour $x \geq 0$ et tend vers 0 quand x augmente indéfiniment. L'équation fonctionnelle $f(x+1) - f(x) = \varphi(x)$ admet comme solution la fonction

$$f(x) = f(0) + x(\varphi(0)-S(1)) + \sum_{h=1}^{k-1} \frac{P_h(x)}{h!} (\varphi^{(h)}(0) - S^{(h)}(1)) + S(x)$$

où

$$S(x) = \sum_{n\geq 0} \left[\varphi(n) + \frac{x}{1!} \varphi'(n)+\ldots+ \frac{x^k}{k!} \varphi^{(k)}(n) - \varphi(n+x)\right]$$

où $P_h(x)$, $h \geq 1$ est l'unique polynôme de degré $h + 1$, solution de $f(x+1) - f(x) = x^h$, $x \geq 0$ et $P_h(0) = 0$. Si $f(0)$ est donné, cette solution est la seule qui ait une dérivée $k^{\text{ème}}$ croissante, pour $x \geq 0$.

Les polynômes figurant dans ce théorème, $P_h(x) = 1^h+\ldots+(x-1)^h$ ont été introduits par Bernoulli. Ce que l'on appelle polynômes de Bernoulli sont les dérivés de ceux là (ils vérifient l'équation $f(x+1) - f(x) = h\, x^{h-1}$).

On applique le théorème de Pisot-Dufresnoy en posant $\varphi_o(x) = \text{Log}(x+1)$, de dérivée $\frac{1}{x+1}$ décroissante pour $x \geq 0$ et tendant vers 0 quand x croit indéfiniment. Soit alors $f_1(x)$ l'unique solution convexe de l'équation $f(x+1) - f(x) = \text{Log}(x+1)$ telle que $f(0) = 0$. On pose $\Gamma(x+1) = e^{f_1(x)}$ et on obtient la fonction gamma. On remarque que

$$f_1(x) = -\gamma x + \sum_{n\geq 1} \frac{x}{n} - \text{Log}(1 + \frac{x}{n})$$

et que : $\frac{d^2}{dx^2} f_1(x) = \sum_{n\geq 1} (n+x)^{-2}$

est décroissante pour $x \geq 0$ et tend vers 0 quand x croit indéfiniment. Par récurrence, on définit des fonctions $f_n(x)$ vérifiant :

(a) $f_n(x+1) - f_n(x) = f_{n-1}(x)$

(b) $f_n(0) = 0$

(c) $\frac{d^n}{dx^n} f_n(x) \geq 0$ pour $x \geq 0$

(d) $$f_n(x) = -xE_n(1) + \sum_{h=1}^{n-1} \frac{P_h(x)}{h!}\left[f_{n-1}^{(k)}(0) - E_n^{(k)}(1)\right] + E_n(x)$$

où

$$E_n(x) = \sum_{m\in\mathbb{N}^{n-1}\times\mathbb{N}^*}\left[\frac{1}{n}\left(\frac{x}{L(m)}\right)^n - \frac{1}{n-1}\left(\frac{x}{L(m)}\right)^{n-1} + \ldots + (-1)^{n-1}\frac{x}{L(m)} + (-1)^n \mathrm{Log}\left(1+\frac{x}{L(m)}\right)\right]$$

où

$$L(m) = m_1 + \ldots + m_n \text{ si } m = (m_1, \ldots, m_n)$$

(e) $\frac{d^{n+1}}{dx^{n+1}} f_n(x) = n! \sum_{m\in\mathbb{N}^{n-1}\times\mathbb{N}^*} (x + L(m))^{-n-1}$ est décroissante pour $x \geq 0$ et tend vers 0 quand x croit indéfiniment.

On pose $G_n(x+1) = e^{f_n(x)}$. La relation (d) donne le produit de Weierstraß de $G_n(x)$. La fonction $\Gamma_n(x)^{-1}$ est une fonction d'ordre n, dont tous les zéros sont les entiers négatifs 0, -1, -2,... l'ordre de l'entier négatif -k est égal au nombre de solutions de l'équation $L(m) = k + 1$, $m \in \mathbb{N}^{n-1} \times \mathbb{N}^*$. Le nombre de solutions pour $m \in \mathbb{N}^n$ est le coefficient de X^{k+1} dans le développement en série de Taylor de $(1 - X)^{-n}$, c'est-à-dire $\binom{n+k}{k+1}$. Le nombre de solutions avec $m \in \mathbb{N}^{n-1} \times \mathbb{N}^*$ est égal à $\binom{n+k}{k+1} - \binom{n+k-1}{k+1} = \binom{n+k-1}{n-1}$. L'ordre du zéro au point -k est donc égal à $\binom{n+k-1}{n-1}$.

3 - LA FORMULE DES TRACES DE SELBERG POUR PSL(2,ℤ)

Dasn le cas particulier de PSL(2,ℤ), on peut écrire la formule des traces (sans représentation) sous la forme suivante :

$$\sum_{n=o}^{\infty} h(r_n) = \sum_{p\in P}\sum_{k\geq 1} \frac{\mathrm{Log}\, Np}{Np^{k/2} - Np^{-k/2}}\, g(k \,\mathrm{Log}\, Np)$$

$$+ \frac{1}{12}\int_{-\infty}^{\infty} r\, h(r) \tanh \pi r \, dr$$

$$+ \int_{-\infty}^{\infty} \frac{1}{4} + \frac{1}{3\sqrt{3}}\left(e^{\pi r/3} + e^{-\pi r/3}\right) \frac{h(r)}{e^{\pi r} + e^{-\pi r}}\, dr$$

$$- g(0)\,\mathrm{Log}\, 2\pi + \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{\zeta'}{\zeta}(-2ir)\, h(r)\, dr$$

en donnant comme définitions des différents termes :

a) les nombres complexes r_n sont définis à partir des valeurs propres du spectre discret de l'opérateur de Laplace-Beltrami opérant sur l'espace $L^2(PSL(2,\mathbb{Z})\backslash H)$ soit $0 = \lambda_o \leq \lambda_1 \leq \ldots \leq \lambda_n \ldots$ en posant :

$$\lambda_n = \frac{1}{4} + r_n^2 \quad ; \quad \mathrm{Arg}\,(r_n) = 0 \text{ ou } -\frac{\pi}{2}$$

En fait, $\mathrm{Arg}\,(r_n) = -\pi/2$ ne se produit jamais pour $PSL(2,\mathbb{Z})$, cela se démontre par un argument géométrique élégant donné par Roelcke [20]. C'est équivalent au fait que $\lambda_1 > \frac{1}{4}$, ce que Cartier a vérifié numériquement [8].

b) la formule est valable pour toutes les fonctions paires $h(r)$ holomorphes dans une bande $|\mathrm{Im}\, s| < \frac{1}{2} + \varepsilon$, où $\varepsilon > 0$ et vérifiant dans cette bande la condition de croissance $h(r) = 0\,(1+|r|^2)^{-1-\varepsilon}$ on pose :

$$g(u) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-iru}\, h(r)\, dr$$

en particulier, on a

$$g(0) = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(r)\, dr$$

c) on reconnait quatre types de contribution dans cette formule venant des quatres types de classes de conjugaison : hyperbolique, l'unité, et les types exceptionnels elliptiques et paraboliques. La forme sous laquelle ils figurent coïncide avec celle donnée par Selberg [21] p.74 et p.78, sauf celle de la contribution parabolique qui figure dans Selberg sous l'expression :

$$\int_{-\infty}^{\infty} \{\frac{1}{4\pi} \frac{\phi'}{\phi}\,(\frac{1}{2} + ir) - \frac{1}{2\pi} \frac{\Gamma'}{\Gamma}\,(1 + ir)\}\, h(r)\, dr - \mathrm{Log}\, 2.g(0)$$
$$+ \frac{1}{4}\,(1 - \phi(\tfrac{1}{2}))h(0) \qquad (2)$$

où

$$\phi(s) = \sqrt{\pi}\, \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \sum_{c>0} \frac{\Psi(c)}{c^{2s}}$$

On vérifie que l'on a

$$\phi(s) = \frac{\xi(2s - 1)}{\xi(2s)} \quad , \text{ donc } \phi(\tfrac{1}{2}) = 1$$

où l'on a posé, selon l'habitude usuelle :

(3) $\xi(s) = \pi^{-s/2}\ \Gamma(s/2)\ \zeta(s)$

L'équation fonctionnelle $\xi(1 - s) = \xi(s)$ ou encore $\frac{\xi'}{\xi}(1 - s) = -\frac{\xi'}{\xi}(s)$ permet de transformer la forme (2) en

$$\int_{-\infty}^{\infty} \{\frac{1}{\pi}\frac{\xi'}{\xi}(-2ir) - \frac{1}{2\pi}\frac{\Gamma'}{\Gamma}(1 + ir)\}\ h(r)\ dr \ - \text{Log } 2.\ g(0)$$

On vérifie à l'aide de (3) et de la formule des compléments pour $\Gamma(s)$ que le terme entre accolades est égal à

$$-\frac{\text{Log } 2\pi}{2\pi} - \frac{i}{2}\ \frac{e^{\pi r} + e^{-\pi r}}{e^{\pi r} - e^{-\pi r}} + \frac{1}{\pi}\ \frac{\zeta'}{\zeta}\ (-2ir)$$

En intégrant sur toute la droite réelle, la partie impaire disparait et l'on obtient finalement la contribution parabolique sous la forme

$$-\ g(0)\ \text{Log } 2\pi + \frac{1}{\pi}\ \int_{-\infty}^{\infty} \frac{\zeta'}{\zeta}(-2ir)$$

La démonstration de la formule des traces de Selberg pour $PSL(2,\mathbb{Z})$ est devenue suffisamment classique pour que nous ne la refaisions pas (Duflo-Labesse [10], Hejhal [17], Zagier [25]).

4 - PASSAGE DE LA FORMULE DES TRACES A L'EQUATION FONCTIONNELLE.

Ce passage est fort bien décrit par Hejhal [17] pour des sous-groupes cocompacts sans éléments elliptiques, de $PSL(2,\mathbb{R})$. C'est grâce à cette rédaction, que j'ai fait ce passage pour $PSL(2,\mathbb{Z})$.

On choisit pour fonction $h(r)$, $g(u)$ les fonctions

$$h(r) = \frac{1}{r^2+z^2} - \frac{1}{r^2+\beta^2} \quad \text{où } \frac{1}{2} < \text{Re } z < \text{Re } \beta$$

$$g(u) = \frac{e^{-z|u|}}{2z} - \frac{e^{-\beta|u|}}{2\beta}$$

qui remplissent les conditions nécessaires ; le terme $-\frac{1}{r^2+\beta^2}$ est indispensable pour assurer la condition de croissance. La contribution hyperbolique est égale à ([17] p.66 et p.67 proposition 4.2) :

$$\frac{1}{2z} \sum_{p\in P} \frac{Z'_p}{Z_p}\left(\frac{1}{2}+z\right) - \frac{1}{2\beta}\frac{Z'_p}{Z_p}\left(\frac{1}{2}+\beta\right)$$

Afin de calculer les contributions elliptiques et paraboliques, on utilise les fait suivants, qui sont utilisés par Hejhal pour obtenir la contribution de la classe unité :

Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction intégrable, on a :

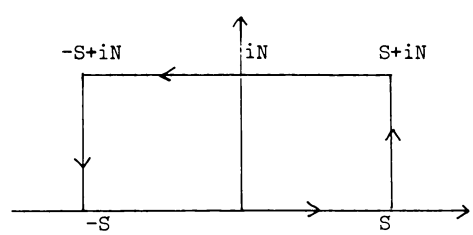
1) $\int_{-\infty}^{\infty} f(r)\,dr = 0$ si f est impaire, et $\int_{-\infty}^{\infty} f(r)\,dr = \int_{-\infty}^{\infty} f(-r)\,dr$

2) si f(r) se prolonge en une fonction méromorphe dans H, sans aucun pôle sur l'axe réel, telle que

A) $\lim_{S\to\infty} \int_{\varepsilon S}^{\varepsilon S+iN} \frac{f(r)}{r^2+z^2}\,dr = 0$ pour $\varepsilon = \pm 1$

B) $\lim_{N\to\infty} \int_{-\infty+iN}^{\infty+iN} \frac{f(r)}{r^2+z^2}\,dr = 0$.

en supposant naturellement que les intégrales écrites aient un sens ; en particulier S et N tendent vers l'infini de sorte que $f(r)/(r^2 + z^2)$ n'ait pas de pôle sur les chemins d'intégration. On choisit alors z, tel que Rez > 0 et que iz ne soit pas un pôle pour f(r). Le théorème de Cauchy appliqué au chemin décrit ci-dessous



suivi d'un passage aux limites nous donne :

(4) $$F(z) = \int_{-\infty}^{\infty} \frac{f(r)}{r^2+z^2}\,dr = \frac{\pi}{z} f(iz) + 2i\pi \sum_{x\in H} \frac{\mathrm{Res}(f,x)}{z^2+x^2}$$

On suppose être arrivé par cette méthode sur une équation du type :

$$\sum_{n=o}^{\infty} h(r_n) = G(z) - G(\beta)$$

L'équation fonctionnelle est alors G(z) = G(-z) ; dans cette équation la partie paire de G(z) disparait, ceci permet dans (4) appliqué en vue de l'équation fonctionnelle de négliger la somme sur les résidus, ainsi que d'éléminer le terme en β. On laissera la vérification des conditions A) et B) non faite, c'est un exercice de routine pour les fonctions simples qui apparaissent dans le cas présent. On décompose G(z) en quatres parties, correspondant à hyperbolique, unité, elliptique, parabolique, que l'on ne considère que modulo les fonctions paires. On obtient :

$$G_p(z) = \frac{1}{2z} \sum_{p\in P} \frac{Z'_p}{Z_p}\left(\frac{1}{2} + z\right)$$

$$G_\infty(z) = \frac{-\pi}{12} \operatorname{tg} \pi z$$

$$G_{ell}(z) = \frac{-\pi}{2z \cos \pi z}\left[\frac{1}{4} + \frac{2\cos(\pi z/3)}{3\sqrt{3}}\right]$$

$$G_{par}(z) = \frac{1}{z} \frac{\zeta'}{\zeta}(2z)$$

On pose alors $H(s) = \exp \int_0^{s-\frac{1}{2}} 2z\, G(z)\, dz$, ce qui transforme l'équation fonctionnelle en H(s) = H(1-s). Les différents termes hyperboliques, paraboliques, unité, elliptiques donnent respectivement :

(5) $$H_p(s) = \prod_{p\in P} Z_p(s)$$

(6) $$H_{par}(s) = \zeta(2s - 1) = Z_{par}(s)$$

(7) $$\frac{H_\infty(s)}{H_\infty(1-s)} = \exp \int_0^{s-\frac{1}{2}} -\frac{\pi}{3}\, z \operatorname{tg} \pi z\, dz = \frac{Z_\infty(s)}{Z_\infty(1-s)}$$

(8) $$\frac{H_{ell}(s)}{H_{ell}(1-s)} = \exp \int_0^{s-\frac{1}{2}} \frac{\pi}{2\cos \pi z}\, dz \times \exp \int_0^{s-\frac{1}{2}} \frac{4}{3\sqrt{3}} \frac{\pi \cos(\pi z/3)}{\cos \pi z}\, dz$$

$$= \frac{Z_{e_2}(s)\, Z_{e_3}(s)}{Z_{e_2}(1-s)\, Z_{e_3}(1-s)}$$

Seuls (7) et (8) sont à démontrer. En l'admettant, on obtient alors l'équation fonctionnelle de la fonction zêta de Selberg (1). La relation de Kinkelin 2.5 montre que

$$\int_0^z \pi v \operatorname{tg} \pi v\, dv = -z \operatorname{Log} 2\pi + \frac{1}{2} \operatorname{Log} \frac{\Gamma(\frac{1}{2} + z)}{\Gamma(\frac{1}{2} - z)} + \operatorname{Log} \frac{\Gamma_2(\frac{1}{2} - z)}{\Gamma_2(\frac{1}{2} + z)}$$

et l'on en déduit (7) sachant que :

$$Z_\infty(s) = [\Gamma_2(s)^2\ \Gamma(s)^{-1}\ (2\pi)^s]^{1/6}$$

Pour obtenir (8), on utilise la formule suivante (Abramowitz-Stegun [1] p.78) :

$$\int \frac{dz}{a+b\cos z} = \frac{1}{\sqrt{b^2-a^2}}\ \mathrm{Log}\left[\frac{(b-a)\mathrm{tg}\,\frac{z}{2} + \sqrt{b^2-a^2}}{(b-a)\ \mathrm{tg}\,\frac{z}{2} - \sqrt{b^2-a^2}}\right] \quad \text{si } b^2 > a^2$$

d'où on déduit :

$$\int \frac{dz}{b^2\cos^2 z - a^2} = \frac{1}{2a\sqrt{b^2-a^2}}\ \mathrm{Log}\left[\frac{1 + \frac{a}{\sqrt{b^2-a^2}}\ \mathrm{tg}\ z}{1 - \frac{a}{\sqrt{b^2-a^2}}\ \mathrm{tg}\ z}\right]$$

On a alors :

$$\exp \int_0^{s-\frac{1}{2}} \frac{\pi\, dz}{2\cos \pi z} = \left[\frac{1 + \mathrm{tg}(\frac{\pi s}{2} - \frac{\pi}{4})}{1 - \mathrm{tg}(\frac{\pi s}{2} - \frac{\pi}{4})}\right]^{1/2} = \frac{Z_{e_2}(s)}{Z_{e_2}(-s)}$$

Enfin l'on a :

$$\exp \int_0^{s-\frac{1}{2}} \frac{4\pi\ \cos(\pi z/3)}{3\sqrt{3}\ \cos \pi z}\, dz = \exp \int_0^{\frac{\pi}{3}(s-\frac{1}{2})} \frac{4\pi}{\sqrt{3}}\ \frac{dz}{4\cos^2\frac{\pi z}{3} - 3}$$

$$= \left[\frac{1 + \sqrt{3}\ \mathrm{tg}\ (\frac{\pi s}{3} - \frac{\pi}{6})}{1 - \sqrt{3}\ \mathrm{tg}\ (\frac{\pi s}{3} - \frac{\pi}{6})}\right]^{2/3} = \frac{Z_{e_3}(s)}{Z_{e_3}(-s)}$$

5 - LE CAS COMPACT.

Pour un sous-groupe discret Γ cocompact de $PSL(2,\mathbb{R})$ et une représentation χ de dimension finie , unitaire de Γ, la formule des traces (Selberg [21]) s'écrit, avec les mêmes notations que précédemment :

$$\sum_{n\geq o} h(r_n) = \sum_{p\in P}\ \sum_{k\geq 1} \frac{\mathrm{tr}(\chi(p^k))\ \mathrm{Log}\ Np}{Np^{k/2} - Np^{-k/2}}\ g\ (k\ \mathrm{Log}\ Np)$$

$$+ \frac{n\mu}{2} \int_{-\infty}^{\infty} r\ \tanh \pi r\ h(r)\ dr$$

$$+ \sum_{e_m} \frac{1}{2m} \sum_{k=1}^{m-1} \frac{\mathrm{tr}\ \chi(e_m^k)}{\sin(k\pi/m)} \int_0^z \frac{e^{-2\ \pi k v/m}}{1+e^{-2\ \pi v}}\ dv$$

où μ est le volume de $\Gamma\backslash H$ pour la mesure $\frac{dx\,dy}{2\pi y^2}$ sur le demi plan supérieur H, et e_m, d'ordre m parcourt <u>toutes</u> les classes elliptiques primitives de Γ (m varie).

Les méthodes précédentes nous donnent sans difficulté une définition convenable pour $Z_\infty(s,\chi)$ et $Z_p(s,\chi)$, voir (2) et (3) dans l'introduction. Comme on l'a dit pour calculer $Z_{e_m}(s,\chi)$ on peut supposer que χ est un <u>caractère</u>

$$\chi(e_m) = e^{-2i\pi \frac{x}{m}} \qquad 0 \le x \le m-1 \ , \ x \in \mathbb{N}$$

L'introduction de χ revient dans (8) écrit pour e_m

$$(9) \qquad \frac{Z_{e_m}(s)}{Z_{e_m}(1-s)} = \exp \frac{2\pi}{m} \sum_{k=1}^{m-1} \frac{\chi^k(e_m)}{\sin \frac{k\pi}{m}} \int_0^{s-\frac{1}{2}} \frac{e^{-2i\pi\, kz/m}}{1+e^{-2i\pi z}}\, dz$$

à remplacer z par z + x sans caractère.

On peut donc choisir comme définition de $Z_{e_m}(s,\chi)$:

$$(10) \qquad Z_{e_m}(s,\chi) = Z_{e_m}(s+x)\, Z_{e_m}(x+\tfrac{1}{2})^{-1}$$

On a alors "l'équation fonctionnelle"

$$(11) \qquad Z_{e_m}(s,\chi) = Z_{e_m}(1-s,\bar{\chi})$$

puisque $\bar{\chi}(e_m) = e^{2i\pi x/m}$.

BIBLIOGRAPHIE

[1] M. ABRAMOWITZ and I.A. STEGUN - Handbook of mathematical functions. Dover Publications (ninth printing, 1970).

[2] W.P. ALEXEIEWSKY - Ueber eine Classe von Functionen die der Gamma Function analog sind. Leipzig Berichte, vol. XLVI p.268-275 (1894).

[3] E.W. BARNES - The Theory of the G-function. Quaterly Journal of Mathematics vol 31, p.264.314, (1899).

[4] E.W. BARNES - Genesis of the Double-Gamma Function. Proccedings of the London Mathematical Society vol 31 p.358.381, (1900).

[5] E.W. BARNES - The Theory of the Double-Gamma Function. Philosophical Transactions of the Royal Society (A) vol.196 (1901) p.265-388.

[6] E.W. BARNES - On the Theory of the Multiple Gamma Function. Philosophical Transactions of the Royal Society (A) vol 19(1904) p.374-439.

[7] CAMPBELL - Les intégrales Eulériennes et leurs applications. Collections universitaires de mathématiques. Dunod (1966).

[8] P. CARTIER - Some numerical computations relating to automorphic functions. Computers in Number Theory, Academic Press, 1971.

[9] P. CASSOU-NOGUES - Analogues p-adiques des fonctions Γ-multiples. Journées arithmétiques de Marseille , 1978.

[10] M. DUFLO et J.P. LABESSE - Sur la formule des traces de Selberg. Annales Scientifiques de l'Ecole Normale Supérieure t.4 (1971) p.193-284.

[11] J. DUFRESNOY et Ch. PISOT - Sur la relation fonctionnelle $f(x+1) - f(x) = \varphi(x)$. Bulletin de la société mathématique de Belgique, t.XV (1963) p.259-270.

[12] R. GANGOLLI - Zeta functions of Selberg's type for compact space forms of symmetric spaces of rank one. Illinois J. Math. vol.21 (1977) p.1-42.

[13] R. GANGOLLI - Zeta functions of Selberg's type for some non compact quotients of symmetric spaces of rank one. Preprint 1978.

[14] J. GLAISHER - On products and series involving prime numbers only, Quaterly Journal of Mathematics, vol.XXVI, p.1-74.

[15] D.A. HEJHAL - The Selberg trace formula for congruence subgroups. Bull. of the A.M.S. vol.81, n° 4 (1975), p.752-755.

[16] D.A. HEJHAL - The Selberg traceformula and the Riemann zeta function. Duke Math. J. vol.43 (1976) p.441-482.

[17] D.A. HEJHAL - The Selberg trace formula for PSL(2,R). Lecture Notes Springer Verlag (1976).

[18] O. HÖLDER - Ueber eine transcendente Function. Göttingen Nächrichten (1886) p.514-522.

[19] KINKELIN - Ueber eine mit der Gamma function verwandte Transcendente und deren anwendung auf die Integral-rechnung. Crelle, LVII p.122-158.

[20] W. ROELCKE - Uber die Wellengleichungen bei grenzkeisgruppen erster Art. Abh. Heidelberg Akad. Wiss.4 (1956) p.159-267.

[21] A. SELBERG - Harmonic Analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series. J. Indian Math. Soc. 20 (1956) p.47-87.

[22] G. SHIMURA - Arithmetic Theory of automorphic functions. Princeton University Press 1971.

[23] T. SHINTANI - On a Kronecker limit formula for real quadratic fields. J. Fac. Tokyo vol.24 (1977) p.167-199.

[24] E.T. WHITTAKER and G.N. WATSON - A Course of Modern Analysis. Cambridge University Press 1965, p.264 exercices 48-49-50.

[25] D. ZAGIER - Eisenstein Series and the Selberg Trace Formula (A paraître).

Marie-France VIGNÉRAS
Ecole Normale Supérieure de Jeunes Filles
1, rue Maurice Arnoux
92120 MONTROUGE