EXPLICIT METHODS IN NUMBER THEORY

RATIONAL POINTS & DIOPHANTINE EQUATIONS

K. Belabas, F. Beukers
P. Gaudry, W. McCallum
B. Poonen, S. Siksek
M. Stoll, M. Watkins

Panoramas et Synthèses

Numéro 36

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique

PANORAMAS ET SYNTHÈSES 36

MÉTHODES EXPLICITES EN THÉORIE DES NOMBRES ÉQUATIONS DIOPHANTIENNES

Karim Belabas
Frits Beukers
Pierrick Gaudry
William McCallum
Bjorn Poonen
Samir Siksek
Michael Stoll
Mark Watkins

Société Mathématique de France 2012
Publié avec le concours du Centre National de la Recherche Scientifique

K. Belabas
Université de Bordeaux, IMB, UMR 5251, F-33400 Talence, France.
CNRS, IMB, UMR 5251, F-33400 Talence, France.
INRIA, F-33400 Talence, France.

F. Beukers
Mathematical Institute, University of Utrecht, P.O.Box 80.010, 3508TA Utrecht, Netherlands.

P. Gaudry
CNRS, INRIA, Université de Lorraine.

W. McCallum
Department of Mathematics, University of Arizona, Tucson, AZ 85718, USA.

B. Poonen
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA.

S. Siksek
Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom.

M. Stoll
Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

M. Watkins
Magma Computer Algebra Group, Department of Mathematics and Statistics, Carslaw Building (F07), University of Sydney, NSW 2006, AUSTRALIA.

***Classification mathématique par sujets* (2000). —** 11D41, 11G05, 11G20, 11G30, 11G40, 11T5, 11Y16, 11Y99, 14G05, 14H52, 14K20.

***Mots clefs*. —** Algorithmes en temps polynomial, Chabauty, corps finis, coubes elliptiques, descente, équation de Fermat généralisée, équations diophantiennes, groupe de Selmer, intégration p-adique, jacobienne, méthodes explicites en théorie des nombres, modularité, points de Heegner, points rationnels, réduction de réseaux, revêtement galoisien, théorème de Fermat, théorie des invariants.

MÉTHODES EXPLICITES EN THÉORIE DES NOMBRES ÉQUATIONS DIOPHANTIENNES

Karim Belabas, Frits Beukers, Pierrick Gaudry, William McCallum, Bjorn Poonen, Samir Siksek, Michael Stoll, Mark Watkins

Résumé. — Ce volume regroupe une sélection de sept cours de théorie des nombres donnés lors d'un trimestre spécial de l'Institut Henri Poincaré (septembre à décembre 2004), centrés sur la résolution effective d'équations diophantiennes. Les cours, du niveau d'une deuxième année de Master, donnent un panorama attrayant des techniques employées et des mathématiques sollicitées.

***Abstract* (Explicit Methods in Number Theory Rational Points. Diophantine Equations)**
This volume contains a selection of seven short courses in number theory taught during a special trimester at Institut Henri Poincaré (from September to December 2004), centered on Diophantine equations and how to effectively solve them. The lectures, targeted at second year graduate students, display an attractive panorama of mathematical ideas and tools, that can be used to reach this goal.

© Panoramas et Synthèses 36, SMF 2012

PRÉFACE

Ce volume regroupe sept cours donnés lors d'un trimestre spécial *Méthodes explicites en théorie des nombres*, qui s'est tenu à l'Institut Henri Poincaré de septembre à décembre 2004. Ce trimestre abordait le vaste champ des aspects effectifs de l'arithmétique, sans se restreindre aux questions purement algorithmiques : une « méthode » peut ne pas fonctionner ; certaines d'entre elles n'ont d'autre intérêt que les problèmes mathématiques qu'elles soulèvent.

Par manque de place et par souci de cohérence, le présent volume laisse de côté des thèmes importants du trimestre comme les conjectures de Stark ou les paramétrisations de Bhargava et se préoccupe essentiellement de la résolution effective d'équations diophantiennes. Les cours qu'il réunit donnent un panorama attrayant des techniques employées et des mathématiques sollicitées. Ils sont du niveau d'une deuxième année de Master, en admettant au besoin quelques résultats plus avancés.

Ce livre n'est pas une introduction à l'algorithmique de $\mathbb{Z}$, des corps de nombres, au calcul formel, ni à l'algorithmique des courbes pour la cryptographie, qui fournissent des outils ou des motivations pour certains cours. Pour plus de détails sur ces sujets, on pourra consulter respectivement *Prime numbers, a computational perspective* de Crandall et Pomerance, *A course in computational algebraic number theory* de Cohen, *Modern computer algebra* de Gerhard et von zur Gathen, et *Hyperelliptic curve cryptography*, édité par Cohen et Frey. Passons maintenant en revue les différentes contributions.

Hendrik Lenstra et Pierrick Gaudry étudient des équations sur des corps finis. Les objets considérés étant tous finis, il suffit de compter. Le problème est donc ici de compter efficacement (Gaudry) ou de s'interroger sur ce que l'on manipule et comment (Lenstra). Les motivations de Gaudry viennent de la cryptographie à clé publique, plus précisément de son utilisation du problème du logarithme discret dans un groupe fini ; celle-ci nécessite de savoir calculer l'ordre du-dit groupe, ici les points de la Jacobienne d'une courbe définie sur un corps fini.

Lenstra s'intéresse à la question suivante : quelle efficacité peut-on atteindre en ne s'autorisant que des constructions déterministes ? Les résultats les plus familiers de la théorie des corps finis, par exemple l'existence mÃłme de $\mathbb{F}_{p^n}$ posent alors

des questions fort intéressantes. (Le lecteur perplexe pourra essayer à ce stade de construire $\mathbb{F}_{p^2}$, c'est-à-dire un résidu non-quadratique dans $\mathbb{F}_p^*$, sans tirer à pile ou face, ni considérer un nombre rédhibitoire d'éléments.)

Les autres cours s'intéressent aux points $\mathbb{Q}$-rationnels, ou plus généralement sur des corps de nombres, de courbes ou de surfaces, et on ne connaît plus maintenant d'algorithme général qui permette de les décrire explicitement.

Michael Stoll et Mark Watkins se restreignent aux courbes elliptiques. Stoll présente un algorithme de descente général qui permet de calculer le groupe de Mordell-Weil si le groupe de Shafarevich-Tate est fini (comme on le conjecture) et en tout état de cause d'obtenir des renseignements sur ces deux groupes. Watkins décrit la méthode des points de Heegner, en supposant la courbe elliptique définie sur $\mathbb{Q}$ et de rang exactement 1, ce qui permet d'obtenir un générateur via une approximation complexe suffisamment précise.

Sur les courbes de genre supérieur, la situation est d'une certaine façon plus favorable puisque d'après le théorème de Faltings (la conjecture de Mordell), il n'y a qu'un nombre fini de points. En contrepartie, contrairement au cas du genre 1, on est encore loin d'une méthode générale, voire de conjectures générales, qui les exhiberaient effectivement. Bill McCallum et Bjorn Poonen présentent la méthode p-adique de Chabauty et Coleman, qui est le point de départ de l'essentiel des succès en genre supérieur ou égal à 2.

Finalement, Frits Beukers et Samir Siksek s'aventurent sur des surfaces, proches de l'équation de Fermat. Le cours de Beukers est une introduction à la théorie classique des invariants (suivant Hilbert) et à son utilisation des syzygies pour résoudre certaines équations diagonales (suivant Mordell). Siksek expose la méthode modulaire, celle de Wiles. En d'autres termes, comment associer concrètement des courbes de Frey aux solutions d'équations de type Fermat, et comment le théorème de Ribet donne des renseignements sur ces solutions, en termes (d'une liste effective) de formes nouvelles de poids 2 et de niveau contrôlé. Dans les cas favorables, ceci suffit pour conclure.

Bonne lecture,

Karim Belabas

TABLE DES MATIÈRES

Préface v

Résumés des articles xi

Abstracts xv

K. Belabas — *Algorithms for finite fields* 1
1. Construction of finite fields 1
2. Preliminaries on finite rings 3
3. Finite commutative $\mathbb{F}_p$-algebras and factorization 4
4. Primitive elements 8
5. The normal basis theorem 9
6. Isomorphisms and field extensions 11
References 17

P. Gaudry — *Algorithmes de comptage de points d'une courbe définie sur un corps fini* 19
1. Introduction : énoncé du problème 19
2. Survol des algorithmes disponibles 20
3. Complexité des opérations algébriques élémentaires 24
4. L'algorithme de Schoof et ses généralisations 25
5. L'algorithme de Satoh et ses généralisations 32
6. L'algorithme de Kedlaya 41
7. Conclusion 45
Références 45

M. Stoll — *Descent on elliptic curves* 51
1. The Selmer Group 53
2. Computation of the Selmer Group as an Abstract Group 66

3. Constructing geometric representations of Selmer group elements ... 73
4. Minimization and Reduction ... 79
References ... 80

M. Watkins — *Some remarks on Heegner point computations* ... 81
1. Introduction ... 81
2. Definitions and Outline of Theory ... 82
3. The Gross–Zagier theorem and an algorithm ... 84
4. Combination with descent ... 90
References ... 95

W. McCallum & B. Poonen — *The method of Chabauty and Coleman* ... 99
1. Rational points on curves of genus ≥ 2 ... 99
2. The Jacobian ... 100
3. A real-analytic method that does not work ... 102
4. Chabauty's idea ... 102
5. Coleman's method ... 104
6. Flynn's method for genus 2 ... 107
7. Effectiveness ... 107
8. Examples ... 108
9. Elliptic Chabauty ... 112
Appendix A. The case of bad reduction ... 112
References ... 115

F. Beukers — *The generalized Fermat equation* ... 119
1. Introduction ... 119
2. A sample solution ... 121
3. Galois covers of $\mathbb{P}^1$ ... 123
4. Lifting points ... 126
5. Galois cocycles ... 129
6. Invariant theory of binary forms ... 131
7. Mordell's approach ... 136
8. Edwards's approach ... 137
9. Reduction of binary forms ... 140
10. An algorithm to solve $x^2 + y^3 = dz^5$ ... 143
11. Appendix A: Parametrizing $X^2 + Y^3 \pm Z^r = 0$ ... 144
12. Appendix B: fourth transvectants ... 147
References ... 148

S. Siksek — *The Modular Approach to Diophantine Equations* ... 151
1. Introduction ... 151
2. Facts about newforms ... 152
3. Correspondence between rational newforms and elliptic curves ... 153
4. Some Useful `MAGMA` Commands ... 153

5. Level-Lowering 156
6. Absence of Isogenies 158
7. Frey Curves or 'How to use Ribet's Theorem?' 159
8. Fermat's Last Theorem 160
9. An Occasional Bound for the Exponent 162
10. An Example of Serre-Mazur-Kraus 163
11. The Method of Kraus 166
12. The Symplectic Method 167
13. 'Predicting Exponents of Constants' 169
14. Recipes for Ternary Diophantine Equations 172
15. Combining the modular approach with quadratic reciprocity 177
References 178

RÉSUMÉS DES ARTICLES

Algorithms for finite fields
Karim Belabas 1

Ce cours traite des algorithmes déterministes relatifs aux corps finis. L'accent n'est pas mis sur des algorithmes efficaces en pratique, mais sur le défi posé par la quête d'algorithmes en temps polynomial à notre compréhension de cette structure élémentaire. Les sujets traités incluent : représenter un corps fini, reconnaître un corps fini, construire un corps fini, construire des applications entre corps finis, et factoriser les polynômes.

Algorithmes de comptage de points d'une courbe définie sur un corps fini
Pierrick Gaudry 19

Le calcul de la fonction Zêta d'une courbe algébrique définie sur un corps fini, communément appelé comptage de points, est une tâche algorithmique dont l'étude a été poussée par d'importantes applications cryptographiques. Dans cet article de survol, nous donnons un aperçu des différentes méthodes disponibles pour s'attaquer à ce problème. Dans la littérature, celles-ci sont traditionnellement illustrées par des calculs records que nous mentionnerons afin de bien mettre en perspective les implications pratiques.

Descent on elliptic curves
Michael Stoll 51

Soit E une courbe elliptique sur $\mathbb{Q}$ (ou, plus généralement, sur un corps de nombres quelconque). On lui associe, d'une part, le groupe abélien de type fini $E(\mathbb{Q})$, et d'autre part, le groupe de Shafarevich-Tate $Ш(\mathbb{Q}, E)$.

La *descente* est une méthode générale pour obtenir des informations sur ces deux objets – idéalement des informations complètes sur le groupe de Mordell-Weil $E(\mathbb{Q})$, et typiquement des informations partielles sur $Ш(\mathbb{Q}, E)$.

Une descente calcule (pour un $n > 1$ donné) le *n-groupe de Selmer* $\mathrm{Sel}^{(n)}(\mathbb{Q}, E)$, qui se trouve dans une suite exacte

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(n)}(\mathbb{Q}, E) \longrightarrow Ш(\mathbb{Q}, E)[n] \longrightarrow 0$$

et qui contient donc des informations combinées sur $E(\mathbb{Q})$ et sur $Ш(\mathbb{Q}, E)$.

Le sujet principal que de ce mini-cours est de rendre explicite cette descente, et en particulier, de représenter les éléments du groupe de Selmer comme des courbes couvrant E. Ces représentations explicites sont utiles à deux égards : elles permettent de chercher des points rationnels (en cas de succès, l'élément est dans l'image de $E(\mathbb{Q})/nE(\mathbb{Q})$) ; et elles fournissent un point de départ pour effectuer des descentes d'ordre plus élevé (par exemple, une p^2-descente suivant une p-descente).

Some remarks on Heegner point computations
Mark Watkins 81

Nous donnons une vue d'ensemble de la théorie des points de Heegner pour les courbes elliptiques, puis décrivons diverses idées nouvelles qui permettent le calcul des points rationnels des courbes de rang 1. En particulier, nous discutons l'idée de Cremona (suivant Silverman) de reconnaître un point rationnel *via* sa hauteur, l'idée de Delaunay d'utiliser les involutions d'Atkin-Lehner lors de la sélection des paramètres auxiliaires, et l'idée d'Elkies combinant descente et réduction de réseau, qui peuvent diminuer drastiquement la précision requise pour mener à bien le calcul.

The method of Chabauty and Coleman
William McCallum & Bjorn Poonen 99

Cet exposé présente une introduction à la méthode de Chabauty et Coleman, une méthode p-adique qui cherche à expliciter l'ensemble des points rationnels d'une courbe de genre $g \geq 2$. Après avoir exposé la méthode, nous donnons quelques exemples de son utilisation en pratique et puis nous discutons sur son efficacité. Une annexe traite le cas où la courbe a mauvaise réduction.

The generalized Fermat equation
Frits Beukers 119

Cet article étudie les généralisations de l'équation de Fermat $x^n + y^n = z^n$. Dès la démonstration du « grand théorème de Fermat » par Wiles et Taylor, on s'est démandé ce qu'il adviendrait si les exposants dans l'équation à trois termes étaient choisis différemment. Ou si l'on plaçait d'autres coefficients que 1 devant les monômes. Nous discutons la réduction de la résolution de telles équations à la détermination des points rationnels d'un ensemble fini de courbes algébriques (définies sur $\mathbb{Q}$ si possible), puis résolvons complètement l'équation d'exposants $2, 3, 5$.

The Modular Approach to Diophantine Equations
SAMIR SIKSEK 151

Le but de cette note est de présenter le théorème de rabaissement du niveau de Ribet et autres idées relatives d'une façon explicite et simplifiée (que nous espérons être toujours aussi précise), et ensuite d'expliquer comment ces idées sont utilisées pour dériver des informations utiles sur les solutions aux équations diophantiennes.