SÉMINAIRES ET CONGRÈS 11

ARITHMETIC, GEOMETRY AND CODING THEORY (AGCT 2003)

edited by

Yves Aubry

Gilles Lachaud

Société Mathématique de France 2005

Y. Aubry
Institut de Mathématiques de Luminy, C.N.R.S., Marseille, France.
E-mail : aubry@iml.univ-mrs.fr

G. Lachaud
Institut de Mathématiques de Luminy, C.N.R.S., Marseille, France.
E-mail : lachaud@iml.univ-mrs.fr

2000 *Mathematics Subject Classification*. — 14H05, 14G05, 11G20, 20M99, 94B27, 11T06, 11T71, 11R37, 14G10, 14G15, 11R58, 11A55, 11R42, 11Yxx, 12E20, 14H40, 14K05.

***Key words and phrases*. —** Zeta functions, abelian varieties, functions fields, curves over finite fields, towers of function fields, finite fields, graphs, numerical semigroups, polynomials over finite fields, cryptography, hyperelliptic curves, p-adic representations, class field towers, Galois groups, rational points, continued fractions, regulators, ideal class number, bilinear complexity, hyperelliptic jacobians.

ARITHMETIC, GEOMETRY AND CODING THEORY (AGCT 2003)

edited by Yves Aubry, Gilles Lachaud

Abstract. — In may 2003, two events have been held in the "Centre International de Rencontres Mathématiques" in Marseille (France), devoted to Arithmetic, Geometry and their applications in Coding theory and Cryptography: an European school "Algebraic Geometry and Information Theory" and the 9-th international conference "Arithmetic, Geometry and Coding Theory". Some of the courses and the conferences are published in this volume. The topics were theoretical for some ones and turned towards applications for others: abelian varieties, function fields and curves over finite fields, Galois group of pro-p-extensions, Dedekind zeta functions of number fields, numerical semigroups, Waring numbers, bilinear complexity of the multiplication in finite fields and class number problems.

Résumé **(Arithmétique, géométrie et théorie des codes (AGCT 2003))**

En mai 2003 se sont tenus au Centre International de Rencontres Mathématiques à Marseille (France), deux événements centrés sur l'Arithmétique, la Géométrie et leurs applications à la théorie des Codes ainsi qu'à la Cryptographie : une école Européenne "Géométrie Algébrique et Théorie de l'Information" ainsi que la 9ème édition du colloque international "Arithmétique, Géométrie et Théorie des Codes". Certains des cours et des conférences font l'objet d'un article publié dans ce volume. Les thèmes abordés furent à la fois théoriques pour certains et tournés vers des applications pour d'autres : variétés abéliennes, corps de fonctions et courbes sur les corps finis, groupes de Galois de pro-p-extensions, fonctions zêta de Dedekind de corps de nombres, semigroupes numériques, nombres de Waring, complexité bilinéaire de la multiplication dans les corps finis et problèmes de nombre de classes.

CONTENTS

RÉSUMÉS DES ARTICLES

Le sujet de cet article est la construction de tours de corps de fonctions sur des corps finis qui sont définies récursivement. Nous donnons un exposé des quelques résultats connus en illustrant la théorie avec plusieurs exemples.

Dans ce travail, nous étudions des objets qui décrivent le comportement de l'addition dans un semi-groupe numérique, tout en montrant qu'ils le déterminent complètement. Ensuite, nous étudions le cas des semi-groupes numériques de type Arf et en donnons quelques résultats spécifiques.

Dans cet article, nous présentons une nouvelle méthode qui permet souvent de calculer la valeur exacte du nombre de Waring ou d'en donner une estimation. Nous améliorons également la borne inférieure relative au problème de Waring pour de grands corps finis.

Les deux systèmes principaux de cryptographie à clef publique sont RSA et le calcul de logarithmes discrets dans un groupe cyclique. Nous nous intéressons aux logarithmes discrets et présentons les faits mathématiques qu'il faut connaître pour apprendre la cryptographie mathématique.

Nous présentons des résultats élémentaires sur les courbes sur les corps finis et leurs points rationnels. Nous avons fait un effort pour donner une présentation aussi simple que possible, la rendant accessible aux non spécialistes.

Parmi ces résultats se trouvent : le théorème de Weil (l'hypothèse de Riemann dans ce contexte), son amélioration donnée par Serre, la borne de Ihara sur le genre pour les courbes maximales, genre et classification des courbes maximales, théorie de Stohr-Voloch des ordres de Frobenius pour les courbes planes, constructions de courbes sur les corps finis ayant beaucoup de points rationnels, les formules explicites de Serre, étude asymptotique des courbes sur les corps finis et des codes correcteurs d'erreurs (la connexion entre elles est un célèbre théorème de Tsfasman-Vladut-Zink), tours récursives de courbes et certaines tours particulièrement intéressantes (atteignant la borne de Drinfeld-Vladut sur des corps finis de cardinal un carré ou atteignant la borne de Zink sur des corps finis de cardinal un cube).

Dans cet article, on examine quelques résultats récents au sujet des groupes de Galois des extensions pro-p modérées des corps des nombres.

Une courbe sur un corps k est appelée *une courbe sans point* si elle n'a aucun point k-rationnel. Nous prouvons qu'il existe des courbes hyperelliptiques de genre trois sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 25$, qu'il existe des quartiques planes sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 23$, $q = 29$ ou $q = 32$, et qu'il existe des courbes de genre quatre sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 49$.

Nous étudions les extensions quadratiques réelles du corps rationnel sur un corps fini de caractéristique 2. On rappelle la forme générale de telles extensions puis on donne une approche géométrique de l'algorithme des fractions continues qui permet de calculer le régulateur. Enfin on s'intéresse aux extensions quadratiques réelles dont le nombre de classes d'idéaux de l'anneau des entiers est égal à un et on donne un grand nombre d'exemples pour lesquels cette situation est réalisée.

Nous donnons une borne supérieure explicite pour le résidu en $s = 1$ de la fonction zêta de Dedekind d'un corps de nombres K totalement réel pour lequel $\zeta_K(s)/\zeta(s)$ est entière. On remarque que c'est conjecturalement toujours le cas, et que c'est vrai si $K/\mathbf{Q}$ est normale ou si K est cubique.

L'objectif de cet article est de présenter la complexité bilinéaire de la multiplication dans les corps finis et de faire un bref tour d'horizon des résultats récents obtenus dans cette partie de la théorie de la complexité algébrique. En particulier, nous présentons les résultats nouveaux qui découlent de l'utilisation de l'algorithme de Chudnovsky-Chudnovsky et de ses généralisations.

Nous étudions les propriétés galoisiennes des points d'ordre fini des variétés abéliennes qui impliquent la simplicité de leur algèbre d'endomorphismes. Nous discutons ceux-ci par rapport aux jacobiennes hyperelliptiques.

ABSTRACTS

On towers of function fields over finite fields
Peter Beelen, Arnaldo Garcia & Henning Stichtenoth 1

The topic of this paper is the construction of good recursive towers of function fields over finite fields. We give an exposition of a number of known results and illustrate the theory by several examples.

Addition behavior of a numerical semigroup
Maria Bras-Amorós 21

In this work we study some objects describing the addition behavior of a numerical semigroup and we prove that they uniquely determine the numerical semigroup. We then study the case of Arf numerical semigroups and find some specific results.

On the calculation and estimation of Waring number for finite fields
Oscar Moreno & Francis N. Castro 29

In this paper we present a new method that often computes the exact value of the Waring number or estimates it. We also improve the lower bound for the Waring problem for large finite fields.

Mathematical background of Public Key Cryptography
Gerhard Frey & Tanja Lange 41

The two main systems used for public key cryptography are RSA and protocols based on the discrete logarithm problem in some cyclic group. We focus on the latter problem and state cryptographic protocols and mathematical background material.

On curves over finite fields
Arnaldo Garcia 75

In these notes we present some basic results of the Theory of Curves over Finite Fields. Assuming a famous theorem of A. Weil, which bounds the number of solutions in a finite field (*i.e.*, number of rational points) in terms of the genus and the cardinality of the finite field, we then prove several other related bounds (bounds of Serre, Ihara, Stohr-Voloch, etc.). We then treat Maximal Curves (classification and genus spectrum). Maximal curves are the curves attaining the upper bound of A. Weil. If the genus of the curve is large with respect to the cardinality of the finite field, Ihara noticed that Weil's bound cannot be reached and he introduced then a quantity $A(q)$ for the study of the asymptotics of curves over a fixed finite field. This leads to towers of curves and we devote special attention to the so-called recursive towers of curves. We present several examples of recursive towers with good asymptotic behaviour, some of them attaining the Drinfeld-Vladut bound. The connection with the asymptotics of linear codes is a celebrated result of Tsfasman-Vladut-Zink, which is obtained via Goppa's construction of codes from algebraic curves over finite fields.

In this paper, we examine some recent results concerning Galois groups of tamely ramified pro-p extensions of numbers fields.

A curve over a field k is *pointless* if it has no k-rational points. We show that there exist pointless genus-3 hyperelliptic curves over a finite field $\mathbb{F}_q$ if and only if $q \leqslant 25$, that there exist pointless smooth plane quartics over $\mathbb{F}_q$ if and only if either $q \leqslant 23$ or $q = 29$ or $q = 32$, and that there exist pointless genus-4 curves over $\mathbb{F}_q$ if and only if $q \leqslant 49$.

We consider real quadratic extensions of the rational field over a finite field of characteristic two. After recalling the equation of such extensions, we present a geometric approach of the continued fraction expansion algorithm to compute the regulator. Finally, we study the ideal class number one problem and give numerous examples for which the ideal class number equals one.

We give an explicit upper bound for the residue at $s = 1$ of the Dedekind zeta function of a totally real number field K for which $\zeta_K(s)/\zeta(s)$ is entire. Notice that this is conjecturally always the case, and that it holds true if $K/\mathbf{Q}$ is normal or if K is cubic.

The aim of this paper is to introduce the bilinear complexity of the multiplication in finite fields and to give a brief exposition of the recent results obtained in this part of algebraic complexity theory. In particular we present the new results obtained using the Chudnovsky-Chudnovsky algorithm and its generalizations.

We study Galois properties of points of prime order on an abelian variety that imply the simplicity of its endomorphism algebra. Applications of these properties to hyperelliptic jacobians are discussed.

PRÉFACE

Sous l'égide de l'*European Science Fondation* et dans le cadre d'un semestre « Arithmétique » de l'*Institut de Mathématiques de Luminy*, nous avons eu le plaisir d'organiser au *Centre International de Rencontres Mathématiques* (Marseille, France) en mai 2003, en collaboration avec Mikhail Tsfasman, une École européenne intitulée « Géométrie Algébrique et Théorie de l'Information » ainsi que la 9ème édition du colloque international « Arithmétique, Géométrie et Théorie des Codes ».

Nous remercions les quatre conférenciers de l'École : Gerhard Frey, Arnaldo Garcia, Gregory Kabatiansky et René Schoof pour la qualité de leur cours. Les cours des deux premiers se trouvent publiés dans ce volume (celui de Gerhard Frey étant coécrit avec Tanja Lange) et constituent une excellente introduction, l'un aux méthodes géométriques employées en cryptographie et l'autre aux courbes et corps de fonctions algébriques à une variable sur un corps fini.

Nous remercions également les conférenciers du colloque dont les exposés furent très variés et d'un grand intérêt ; certains d'entre eux ont donné lieu à un article dans cet ouvrage. Au-delà des conférenciers, c'est l'ensemble des participants à ce colloque qui a également, par sa présence active, contribué à créer un climat à la fois convivial et propice aux échanges : qu'ils en soient tous remerciés.

Outre l'E.S.F. qui nous a permis de financer un tel événement dans le cadre d'un « Exploratory Workshop », nous remercions également le personnel de l'I.M.L. et du C.I.R.M. pour leur aide et leur disponibilité.

Les éditeurs

PREFACE

As an event of the European Science Fondation and also as an "Arithmetic" semester of the "Institut de Mathématiques de Luminy", we had the pleasure in May 2003 to organize at the "Centre International de Rencontres Mathématiques" (Marseille, France), with the help of Mikhail Tsfasman, the European School "Algebraic Geometry and Information Theory" and also the 9-th edition of the international conference "Arithmetic, Geometry and Coding Theory".

We would like to thank the four speakers of the School, Gerhard Frey, Arnaldo Garcia, Gregory Kabatianskii and René Schoof, for the quality of their courses. The first two courses are published in this volume (that of Gerhard Frey is written with Tanja Lange) and constitute an excellent introduction, one for the geometric methods used in cryptography and the other one for the curves and the algebraic functions fields over a finite field.

We also want to thank the speakers of the conference who gave various and very interesting talks, some of which gave rise to articles in these proceedings. Beyond the speakers, we would like to thank all the participants of the conference for their active contribution in creating a convivial and productive climate of exchange.

In addition to the E.S.F. which provided the financial support to organize this event as an "Exploratory Workshop", we also thank the personnel of the I.M.L. and of the C.I.R.M. for their help and availability.

The editors