

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, semi-groupes numériques, nombres de Waring, complexité bilinéaire de la multiplication dans les corps finis et problèmes de nombre de classes.

CONTENTS

Résumés des articles	ix
Abstracts	xiii
Préface	xvii
P. BEELEN, A. GARCIA & H. STICHTENOTH — <i>On towers of function fields over finite fields</i>	
1. Introduction	1
2. The limit of a tower	2
3. Two new non-Galois towers	8
4. Graphs and recursive towers	10
5. The functional equation	16
References	19
M. BRAS-AMORÓS — <i>Addition behavior of a numerical semigroup</i>	
Introduction	21
1. The operation $\oplus$ determines a semigroup	22
2. The sequence (ν_i) determines a semigroup	23
3. Arf case	25
Conclusion	27
References	27
O. MORENO & F.N. CASTRO — <i>On the calculation and estimation of Waring number for finite fields</i>	
1. Review of some results about the divisibility of the number of solutions of a system of polynomials over finite fields	29
2. Review of Applications of Divisibility to Covering Radius	31
3. On the Exact Value of Waring Number	32
4. Previous Estimates for Waring Number of Large Finite Fields	35
5. Calculation of Waring Number for Large Finite Fields	36
References	39