Arithmetic, Geometry, Cryptography and Coding Theory

International Conference
November 5–9, 2007
CIRM, Marseilles, France

Gilles Lachaud
Christophe Ritzenthaler
Michael A. Tsfasman
Editors
Arithmetic, Geometry, Cryptography and Coding Theory
Arithmetic, Geometry, Cryptography and Coding Theory

International Conference
November 5–9, 2007
CIRM, Marseilles, France

Gilles Lachaud
Christophe Ritzenthaler
Michael A. Tsfasman
Editors
Contents

Preface vii

On the fourth moment of theta functions at their central point
   Amadou D. Barry, Stéphane R. Louboutin 1

On the construction of Galois towers
   Alp Bassa, Peter Beelen 9

Codes defined by forms of degree 2 on quadric varieties in \( \mathbb{P}^4(\mathbb{F}_q) \)
   Frédéric A. B. Edoukou 21

Curves of genus 2 with elliptic differentials and associated Hurwitz spaces
   Gerhard Frey, Ernst Kani 33

A note on the Giulietti-Korchmaros maximal curve
   Arnaldo Garcia 83

Subclose families, threshold graphs, and the weight hierarchy of Grassmann
   and Schubert codes
   Sudhir R. Ghorpade, Arunkumar R. Patil, Harish K. Pillai 87

Characteristic polynomials of automorphisms of hyperelliptic curves
   Robert M. Guralnick, Everett W. Howe 101

Breaking the Akiyama-Goto cryptosystem
   Petar Ivanov, José Felipe Voloch 113

Hyperelliptic curves, \( L \)-polynomials, and random matrices
   Kiran S. Kedlaya, Andrew V. Sutherland 119

On special finite fields
   Florian Luca, Igor E. Shparlinski 163

Borne sur le degré des polynômes presque parfaitement non-linéaires
   François Rodier 169

How to use finite fields for problems concerning infinite fields
   Jean-Pierre Serre 183

On the generalizations of the Brauer-Siegel theorem
   Alexey Zykin 195
Preface

The 11th conference on Arithmetic, Geometry, Cryptography and Coding Theory (AGCT 11) was held in Marseilles at the “Centre International de Rencontres Mathématiques” (CIRM), during November 5-9, 2007. This international conference has been a major event in the area of applied arithmetic geometry for more than 20 years and included distinguished guests J.-P. Serre (Fields medal, Abel prize winner), G. Frey, H. Stichtenoth and other leading researchers in the field among its 77 participants.

The meeting was organized by the team “Arithmétique et Théorie de l’Information” (ATI) from the “Institut de Mathématiques de Luminy” (IML). The program consisted of 15 invited talks and 18 communications. Among them, thirteen were selected to form the present proceedings. Twelve are original research articles covering asymptotic properties of global fields, arithmetic properties of curves and higher dimensional varieties, and applications to codes and cryptography. The final article is a special lecture of J.-P. Serre entitled “How to use finite fields for problems concerning infinite fields”.

The conference fulfilled its role of bringing together young researchers and specialists. During the conference, we were also happy to celebrate the retirement of our colleague Robert Rolland with a special day of talks.

Finally, we thank the organization committee of CIRM for their help during the conference and the Calanques for its inspiring atmosphere.
Titles in This Series

489 David Ginzburg, Erez Lapid, and David Soudry, Editors, Automorphic Forms and L-functions II. Local aspects, 2009
488 David Ginzburg, Erez Lapid, and David Soudry, Editors, Automorphic forms and L-functions I. Global aspects, 2009
487 Gilles Lachaud, Christophe Ritzenthaler, and Michael A. Tsfasman, Editors, Arithmetic, geometry, cryptography and coding theory, 2009
486 Frédéric Mynard and Elliott Pearl, Editors, Beyond topology, 2009
485 Idris Assani, Editor, Ergodic theory, 2009
484 Motoko Kotani, Hisashi Naito, and Tatsuya Tate, Editors, Spectral analysis in geometry and number theory, 2009
483 Vyacheslav Futorny, Victor Kac, Iryna Kashuba, and Efim Zelmanov, Editors, Algebras, representations and applications, 2009
482 Kazem Mahdavi and Deborah Koslover, Editors, Advances in quantum computation, 2009
481 Aydin Aytuna, Reinhold Meise, Tosun Terzioglu, and Dietmar Vogt, Editors, Functional analysis and complex analysis, 2009
479 Timothy Y. Chow and Daniel C. Isaksen, Editors, Communicating mathematics, 2008
478 Zongzhu Lin and Jianpan Wang, Editors, Representation theory, 2008
477 Ignacio Luengo, Editor, Recent Trends in Cryptography, 2008
476 Carlos Villegas-Blas, Editor, Fourth summer school in analysis and mathematical physics: Topics in spectral theory and quantum mechanics, 2008
475 Jean-Paul Brasselet, José Luis Cisneros-Molina, David Massey, José Seade, and Bernard Teissier, Editors, Singularities II: Geometric and topological aspects, 2008
474 Jean-Paul Brasselet, José Luis Cisneros-Molina, David Massey, José Seade, and Bernard Teissier, Editors, Singularities I: Algebraic and analytic aspects, 2008
473 Alberto Farina and Jean-Claude Saut, Editors, Stationary and time dependent Gross-Pitaevskii equations, 2008
471 Diego Dominici and Robert S. Maier, Editors, Special functions and orthogonal polynomials, 2008
469 Keith Burns, Dmitry Dolgopyat, and Yakov Pesin, Editors, Geometric and probabilistic structures in dynamics, 2008
468 Bruce Gilligan and Guy J. Roos, Editors, Symmetries in complex analysis, 2008
466 Boo Cheong Khoo, Zhilin Li, and Ping Lin, Editors, Moving interface problems and applications in fluid dynamics, 2008
465 Valery Alexeev, Arnaud Beauville, C. Herbert Clemens, and Elham Izadi, Editors, Curves and Abelian varieties, 2008
TITLES IN THIS SERIES

463 Kristin E. Lauter and Kenneth A. Ribet, Editors, Computational arithmetic geometry, 2008
461 Gary L. Mullen, Daniel Panario, and Igor Shparlinski, Editors, Finite fields and applications, 2008
460 Megumi Harada, Yael Karshon, Mikiya Masuda, and Taras Panov, Editors, Toric topology, 2008
459 Marcelo J. Saia and José Seade, Editors, Real and complex singularities, 2008
456 S. K. Jain and S. Parvathi, Editors, Noncommutative rings, group rings, diagram algebras and their applications, 2008
455 Mark Agranovsky, Daoud Bshouty, Lavi Karp, Simeon Reich, David Shoikhet, and Lawrence Zalcman, Editors, Complex analysis and dynamical systems III, 2008
452 Matthias Beck, Christian Haase, Bruce Reznick, Michèle Vergne, Volkmar Welker, and Ruriko Yoshida, Editors, Integer points in polyhedra, 2008
451 David R. Larson, Peter Massopust, Zuhair Nashed, Minh Chuong Nguyen, Manos Papadakis, and Ahmed Zayed, Editors, Frames and operator theory in analysis and signal processing, 2008
450 Giuseppe Dito, Jiang-Hua Lu, Yoshiaki Maeda, and Alan Weinstein, Editors, Poisson geometry in mathematics and physics, 2008
448 Alberto Corso, Juan Migliore, and Claudia Polini, Editors, Algebra, geometry and their interactions, 2007
447 François Germinet and Peter Hislop, Editors, Adventures in mathematical physics, 2007
445 Laura De Carli and Mario Milman, Editors, Interpolation Theory and Applications, 2007
443 Joseph Stephen Verducci and Xiaotong Shen, Editors, Prediction and discovery, 2007
442 Yi-Zhi Huang and Kailash C Misra, Editors, Lie algebras, vertex operator algebras and their applications, 2007

For a complete list of titles in this series, visit the AMS Bookstore at www.ams.org/bookstore/.
This volume contains the proceedings of the 11th conference AGC$^2$T, held in Marseilles, France in November 2007. There are 12 original research articles covering asymptotic properties of global fields, arithmetic properties of curves and higher dimensional varieties, and applications to codes and cryptography. This volume also contains a survey article on applications of finite fields by J.-P. Serre.

AGC$^2$T conferences take place in Marseilles, France every 2 years. These international conferences have been a major event in the area of applied arithmetic geometry for more than 20 years.