

# Arithmetic, Geometry, Cryptography and Coding Theory 2011

Yves Aubry

Christophe Ritzenthaler

Alexey Zykin

INSTITUT DE MATHÉMATIQUES DE TOULON, INSTITUT DE MATHÉMATIQUES  
DE LUMINY

*Current address:* Avenue de l'université, 83 957 La Garde Cedex, France; Cam-  
pus de Luminy, Case 907, 13288 Marseille Cedex 9, France

*E-mail address:* [aubry@iml.univ-mrs.fr](mailto:aubry@iml.univ-mrs.fr)

INSTITUT DE MATHÉMATIQUES DE LUMINY

*Current address:* Campus de Luminy, Case 907, 13288 Marseille Cedex 9,  
France

*E-mail address:* [ritzenth@iml.univ-mrs.fr](mailto:ritzenth@iml.univ-mrs.fr)

STATE UNIVERSITY HIGHER SCHOOL OF ECONOMICS, LABORATORY OF AL-  
GEBRAIC GEOMETRY AND ITS APPLICATIONS OF HSE, LABORATOIRE J.-V. PON-  
CELET (UMI 2615), INTITUTE FOR INFORMATION TRANSMISSION PROBLEMS

*Current address:* 117312, Vavilova, 7, Moscow, Russia

*E-mail address:* [alzykin@gmail.com](mailto:alzykin@gmail.com)

2010 *Mathematics Subject Classification.* 11G10, 11G20, 11M38, 11R42, 11T06,  
11T71, 14G10, 14G15, 14G50, 14Q05

## Contents

- Construction of a  $k$ -complete addition law on abelian surfaces  
CHRISTOPHE ARÈNE and ROMAIN COSSET
- Number of points in an Artin–Schreier covering  
RÉGIS BLACHE
- Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents  
ERIC FÉRARD, ROGER OYONO, and FRANÇOIS RODIER
- Rational curves with many rational points over a finite field  
SATORU FUKASAWA, MASA AKI HOMMA, and SEON JEONG KIM
- Enumeration of splitting subspaces over finite fields  
SUDHIR R. GHORPADE and SAMRITH RAM
- The characteristic polynomials of abelian varieties of dimensions 4 over finite fields  
SAFIA HALOUI and VIJAYKUMAR SINGH
- New bounds on the maximum number of points on genus 4 curves over small finite fields  
EVERETT W. HOWE
- Some planar maps and related function fields  
GOHAR M. KYUREGHYAN, FERRUH OZBUDAK,  
and ALEXANDER POTT
- A proof of two conjectures on APN functions  
ELODIE LEDUCQ
- Identities for Kloosterman sums and modular curves  
PETR LISONEK
- Degree growth, linear independence and periods of a class of rational dynamical systems  
ALINA OSTAFE and IGOR SHPARLINSKI
- Computer search for curves with many points among abelian covers of genus 2 curves  
KARL RÖKAEUS
- The groups of points on abelian surfaces over finite fields  
SERGEY RYBAKOV

Computing low-degree isogenies in genus 2 with the Dolgachev–Lehavi method

BENJAMIN SMITH

Hodge classes on certain hyperelliptic Prymians

YURI G. ZARHIN

## Preface

The 13-th AG<sup>2</sup>T conference (Arithmetic, Geometry, Cryptography and Coding Theory) took place at CIRM (Centre International de Rencontres Mathématiques) in Marseille, France, on March 14–18, 2011. This international conference has been a major event in the area of arithmetic geometry and its applications for more than 25 years and more than 80 participants attended it this year. We thank all of them for creating a stimulating research environment. The topics of the talks extended from algebraic number theory to diophantine geometry, curves and abelian varieties over finite fields and applications to codes, boolean functions or cryptography. We especially thank the speakers Bruno Anglès, Stéphane Ballet, Burcu Baran, Régis Blache, Ivan Boyer, Nils Bruin, Alain Couvreur, Frédéric Edoukou, Arnaldo Garcia, Sudhir Ghorpade, Safia Haloui, Marc Hindry, Masaaki Homma, Everett Howe, Kamal Khuri-Makdisi, David Kohel, Aristides Kontogeorgis, Philippe Langevin, Gregor Leander, Elodie Leducq, Petr Lisonek, Kit-Ho Mak, Alina Ostafe, Ferruh Ozbudak, François Rodier, Karl Rökæus, Cécilia Salgado, Jean-Pierre Serre, Vijaykumar Singh, Benjamin Smith, Henning Stichtenoth, Bianca Viray, Gabor Wiese and Yuri Zarhin for their lectures.

For the second time, the AG<sup>2</sup>T conference was twinned with Geocrypt (conference on Geometry and Cryptography) which took place in la Marana near Bastia, Corsica, France, on June 19–24, 2011. This conference focuses on algebraic geometry issues raised by cryptography. We would like to thank Christophe Arene, Xavier Caruso, Luca de Feo, Pierre Dèbes, Oumar Diao, Everett Howe, David Kohel, Reynald Lercier, Pascal Molin, Damien Robert, David Roe, Éric Schost, Benjamin Smith, Peter Stevenhagen, Marco Streng, Emmanuel Thom and Osmanbey Uzunkol for their talks. We also thank the ANR CHIC (Hyperelliptic Curves Isogenies, Point Counting) for its financial support.

The editors would like to thank the staff of CIRM (Olivia Barbarroux, Muriel Milton and Laure Stefanini) and that of the Institut de Mathématiques de Luminy (Aurélia Lozingot and Corinne Roux) for their remarkable professionalism.

Finally, special thanks to the Saint Patrick’s day which gave us an opportunity of a memorable party.