CONTEMPORARY MATHEMATICS

637

Algorithmic Arithmetic, Geometry, and Coding Theory

14th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
June 3–7, 2013
CIRM, Marseille, France

Stéphane Ballet
Marc Perret
Alexey Zaytsev
Editors

American Mathematical Society

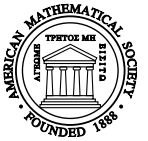
CONTEMPORARY MATHEMATICS

637

Algorithmic Arithmetic, Geometry, and Coding Theory

14th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
June 3–7, 2013
CIRM, Marseille, France

Stéphane Ballet
Marc Perret
Alexey Zaytsev
Editors



American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 11G10, 11G20, 11G25, 11H71, 11Y16, 14G05, 14G15, 14Q05, 14Q15, 94B27.

Library of Congress Cataloging-in-Publication Data

International Conference Arithmetic, Geometry, Cryptography and Coding Theory (14th : 2013 : Marseille, France)

Algorithmic arithmetic, geometry, and coding theory : 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory, June 3-7 2013, CIRM Marseille, France / Stéphane Ballet, Marc Perret, Alexey Zaytsev, editors.

pages cm. – (Contemporary mathematics ; volume 637)

Includes bibliographical references.

ISBN 978-1-4704-1461-0 (alk. paper)

1. Coding theory—Congresses. 2. Geometry, Algebraic—Congresses. 3. Cryptography—Congresses. 4. Number theory—Congresses. I. Ballet, Stéphane, 1971–editor. II. Perret, M. (Marc), 1963– editor. III. Zaytsev, Alexey (Alexey I.), 1976–editor. IV. Title.

QA268.I57 2013

510′–dc23 2014037646

Contemporary Mathematics ISSN: 0271-4132 (print); ISSN: 1098-3627 (online)

DOI: http://dx.doi.org/10.1090/conm/637

Contents

Explicit algebraic geometry

Arithmetic geometry

Preface

The 14th AGCT conference (Arithmetic, Geometry, Cryptography, and Coding Theory) took place at CIRM (Centre International de Rencontres Mathématiques) in Marseille, France, on June 3–7, 2013. This international conference has been a major event in the area of arithmetic geometry and its applications for more than 25 years, 77 participants attended 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 from the theoretical or the algorithmic point of view, and applications to error-correcting codes.

We especially thank the speakers Ekaterina Alekseenko, Nurdagul Ambar, Alp Bassa, Peter Beelen, Jean-Robert Belliard, Ivan Boyer, Niels Bruin, Florian Caullery, Claus Diem, Virgile Ducet, Iwan Duursma, Sudhir Ghorpade, Cécile Gonçalves, Émmanuel Hallouin, Safia Haloui, Johan Peter Hansen, Masaaki Homma, Grigory Kabatiansky, Motoko Kawakita, David Kohel, Dmitry Kubrak, Gilles Lachaud, Kristin Lauter, Winnie Li, Enric Nart, Ferruh Ozbudak, Laurent Poinsot, Hugues Randriambololona, Christophe Ritzenthaler, Damien Robert, Karl Rökaeus, Robert Rolland, Sergey Rybakov, Alexander Schmidt, Jeroen Sijsling, Benjamin Smith, Patrick Solé, and Milakulo Tukumuli for their lectures.

The editors would like to thank the anonymous referees and the staff of CIRM (Olivia Barbarroux, Muriel Milton and Laure Stefanini) for their remarkable professionalism.

Published Titles in This Series

637 **Stéphane Ballet, Marc Perret, and Alexey Zaytsev, Editors,** Algorithmic Arithmetic, Geometry, and Coding Theory, 2015

634 **Steven Dougherty, Alberto Facchini, André Leroy, Edmund Puczyłowski, and Patrick Solé, Editors,** Noncommutative Rings and Their Applications, 2015

633 **Delaram Kahrobaei and Vladimir Shpilrain, Editors,** Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography, 2015

632 **Gohar Kyureghyan, Gary L. Mullen, and Alexander Pott, Editors,** Topics in Finite Fields, 2015

631 **Siddhartha Bhattacharya, Tarun Das, Anish Ghosh, and Riddhi Shah, Editors,** Recent Trends in Ergodic Theory and Dynamical Systems, 2015

630 **Pierre Albin, Dmitry Jakobson, and Frédéric Rochon, Editors,** Geometric and Spectral Analysis, 2014

629 **Milagros Izquierdo, S. Allen Broughton, Antonio F. Costa, and Rubí E. Rodríguez, Editors,** Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces, 2014

628 **Anita T. Layton and Sarah D. Olson, Editors,** Biological Fluid Dynamics: Modeling, Computations, and Applications, 2014

627 **Krishnaswami Alladi, Frank Garvan, and Ae Ja Yee, Editors,** Ramanujan 125, 2014

626 **Veronika Furst, Keri A. Kornelson, and Eric S. Weber, Editors,** Operator Methods in Wavelets, Tilings, and Frames, 2014

625 **Alexander Barg and Oleg R. Musin, Editors,** Discrete Geometry and Algebraic Combinatorics, 2014

624 **Karl-Dieter Crisman and Michael A. Jones, Editors,** The Mathematics of Decisions, Elections, and Games, 2014

623 **Pramod N. Achar, Dijana Jakelić, Kailash C. Misra, and Milen Yakimov, Editors,** Recent Advances in Representation Theory, Quantum Groups, Algebraic Geometry, and Related Topics, 2014

622 **S. Ejaz Ahmed, Editor,** Perspectives on Big Data Analysis, 2014

621 **Ludmil Katzarkov, Ernesto Lupercio, and Francisco J. Turrubiates, Editors,** The Influence of Solomon Lefschetz in Geometry and Topology, 2014

620 **Ulrike Tillmann, Søren Galatius, and Dev Sinha, Editors,** Algebraic Topology: Applications and New Directions, 2014

619 **Gershon Wolansky and Alexander J. Zaslavski, Editors,** Variational and Optimal Control Problems on Unbounded Domains, 2014

618 **Abba B. Gumel, Editor,** Mathematics of Continuous and Discrete Dynamical Systems, 2014

617 **Christian Ausoni, Kathryn Hess, Brenda Johnson, Wolfgang Lück, and Jérôme Scherer, Editors,** An Alpine Expedition through Algebraic Topology, 2014

616 **G. L. Litvinov and S. N. Sergeev, Editors,** Tropical and Idempotent Mathematics and Applications, 2014

615 **Plamen Stefanov, András Vasy, and Maciej Zworski, Editors,** Inverse Problems and Applications, 2014

614 **James W. Cogdell, Freydoon Shahidi, and David Soudry, Editors,** Automorphic Forms and Related Geometry, 2014

613 **Stephan Stolz, Editor,** Topology and Field Theories, 2014

612 **Patricio Cifuentes, José García-Cuerva, Gustavo Garrigós, Eugenio Hernández, José María Martell, Javier Parcet, Keith M. Rogers, Alberto Ruiz, Fernando Soria, and Ana Vargas, Editors,** Harmonic Analysis and Partial Differential Equations, 2014

For a complete list of titles in this series, visit the AMS Bookstore at **www.ams.org/bookstore/conmseries/**.

CONM 637

Algorithmic Arithmetic, Geometry, and Coding Theory • Ballet et al., Editors

This volume contains the proceedings of the 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT), held June 3–7, 2013, at CIRM, Marseille, France.

These international conferences, held every two years, have been a major event in the area of algorithmic and applied arithmetic geometry for more than 20 years.

This volume contains 13 original research articles covering geometric error correcting codes, and algorithmic and explicit arithmetic geometry of curves and higher dimensional varieties. Tools used in these articles include classical algebraic geometry of curves, varieties and Jacobians, Suslin homology, Monsky–Washnitzer cohomology, and L-functions of modular forms.

ISBN 978-1-4704-1461-0

CONM/637

AMS