CONTEMPORARY MATHEMATICS

686

# Arithmetic, Geometry, Cryptography and Coding Theory

15th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
May 18–22, 2015
CIRM, Luminy, France

Alp Bassa
Alain Couvreur
David Kohel
Editors


American Mathematical Society

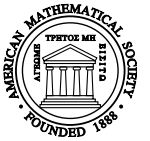
# CONTEMPORARY MATHEMATICS

686

# Arithmetic, Geometry, Cryptography and Coding Theory

15th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
May 18–22, 2015
CIRM, Luminy, France

Alp Bassa
Alain Couvreur
David Kohel
Editors




**American Mathematical Society**
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 11T71, 11G20, 11G25, 14G15, 14H40, 94A60, 94B27.

---

**Library of Congress Cataloging-in-Publication Data**

Names: International Conference Arithmetic, Geometry, Cryptography and Coding Theory (15th : 2015 : Marseille, France) | Bassa, Alp, 1982- editor. | Couvreur, Alain, 1981- editor. | Kohel, David R., 1966- editor.

Title: Arithmetic, geometry, cryptography and coding theory : 15th International Conference on Arithmetic, Geometry, Cryptography and Coding Theory, May 18-22, 2015, CIRM, Marseille, France / Alp Bassa, Alain Couvreur, David Kohel, editors.

Description: Providence, Rhode Island : American Mathematical Society, [2017] | Series: Contemporary mathematics ; volume 686 | Includes bibliographical references.

Identifiers: LCCN 2016041988 | ISBN 9781470428105 (alk. paper)

Subjects: LCSH: Coding theory–Congresses. | Geometry, Algebraic–Congresses. | Cryptography–Congresses. | Number theory–Congresses. | AMS: Number theory – Finite fields and commutative rings (number-theoretic aspects) – Algebraic coding theory; cryptography. msc | Number theory – Arithmetic algebraic geometry (Diophantine geometry) – Curves over finite and local fields. msc | Number theory – Arithmetic algebraic geometry (Diophantine geometry) – Varieties over finite and local fields. msc | Algebraic geometry – Arithmetic problems. Diophantine geometry – Finite ground fields. msc | Algebraic geometry – Curves – Jacobians, Prym varieties. msc | Information and communication, circuits – Communication, information – Cryptography. msc | Information and communication, circuits – Theory of error-correcting codes and error-detecting codes – Geometric methods (including applications of algebraic geometry). msc

Classification: LCC QA268 .I57 2015 | DDC 510–dc23

LC record available at https://lccn.loc.gov/2016041988

DOI: http://dx.doi.org/10.1090/conm/686

---

## Contents

# Preface

The $15^{\text{th}}$ edition of the conference Arithmetic Geometry Cryptography and Coding Theory took place at the *Centre International de Rencontres Mathématiques* (CIRM) in Luminy from May 18 to 22, 2015. It gathered together nearly one hundred researchers from eighteen different countries, all working on aspects of algebraic geometry over finite fields, number theory, cryptography and coding theory. Reaching 28 years since the first edition of the conference in 1987, the community remains extremely active. In particular, the significant participation of young researchers in the conference shows the high dynamism of the domain reflects well on its future prospect.

Four plenary speakers were invited to give an overview on problems connected to the main themes of the conference. Alena Pirutka gave a talk on cycle class maps and surveyed known results and open questions related to Tate conjectures. Ernst-Ulrich Gekeler presented a construction of families of curves with many points from higher-rank Drinfeld modular varieties. Antoine Joux discussed the discrete logarithm problem in multiplicative groups of finite fields following his recent breakthrough. Finally Bernard Le Stum gave an introductory talk on rigid cohomology.

In addition to the invited speakers, there were more than forty talks covering a wide range of topics, such as estimates of the number of rational points of curves or higher dimensional varieties over finite fields, towers of global fields, algebraic geometric coding theory, abelian varieties, and public key cryptography. Certain topics, such as algebraic geometry codes, are among the historical themes of the conference, while others, such as the arithmetic of abelian varieties and curve based cryptography have appeared more recently in the scope of the conference. This emphasizes the continual evolution of the community. The articles of the present volume represent a selection of research presented at this conference.

We warmly thank all the speakers of the conference for their participation and the high quality of their presentations. We also express a deep gratitude to the CIRM's team Olivia Barbaroux, Muriel Milton and Laure Stefanini for their remarkable efficiency.

# Published Titles in This Series

686 **Alp Bassa, Alain Couvreur, and David Kohel, Editors,** Arithmetic, Geometry, Cryptography and Coding Theory, 2017

681 **Shiferaw Berhanu, Nordine Mir, and Emil J. Straube, Editors,** Analysis and Geometry in Several Complex Variables, 2017

680 **Sergei Gukov, Mikhail Khovanov, and Johannes Walcher, Editors,** Physics and Mathematics of Link Homology, 2016

679 **Catherine Bénéteau, Alberto A. Condori, Constanze Liaw, William T. Ross, and Alan A. Sola, Editors,** Recent Progress on Operator Theory and Approximation in Spaces of Analytic Functions, 2016

678 **Joseph Auslander, Aimee Johnson, and Cesar E. Silva, Editors,** Ergodic Theory, Dynamical Systems, and the Continuing Influence of John C. Oxtoby, 2016

677 **Delaram Kahrobaei, Bren Cavallo, and David Garber, Editors,** Algebra and Computer Science, 2016

676 **Pierre Martinetti and Jean-Christophe Wallet, Editors,** Noncommutative Geometry and Optimal Transport, 2016

675 **Ana Claudia Nabarro, Juan J. Nuño-Ballesteros, Raúl Oset Sinha, and Maria Aparecida Soares Ruas, Editors,** Real and Complex Singularities, 2016

674 **Bogdan D. Suceavă, Alfonso Carriazo, Yun Myung Oh, and Joeri Van der Veken, Editors,** Recent Advances in the Geometry of Submanifolds, 2016

673 **Alex Martsinkovsky, Gordana Todorov, and Kiyoshi Igusa, Editors,** Recent Developments in Representation Theory, 2016

672 **Bernard Russo, Asuman Güven Aksoy, Ravshan Ashurov, and Shavkat Ayupov, Editors,** Topics in Functional Analysis and Algebra, 2016

671 **Robert S. Doran and Efton Park, Editors,** Operator Algebras and Their Applications, 2016

670 **Krishnendu Gongopadhyay and Rama Mishra, Editors,** Knot Theory and Its Applications, 2016

669 **Sergiĭ Kolyada, Martin Möller, Pieter Moree, and Thomas Ward, Editors,** Dynamics and Numbers, 2016

668 **Gregory Budzban, Harry Randolph Hughes, and Henri Schurz, Editors,** Probability on Algebraic and Geometric Structures, 2016

667 **Mark L. Agranovsky, Matania Ben-Artzi, Greg Galloway, Lavi Karp, Dmitry Khavinson, Simeon Reich, Gilbert Weinstein, and Lawrence Zalcman, Editors,** Complex Analysis and Dynamical Systems VI: Part 2: Complex Analysis, Quasiconformal Mappings, Complex Dynamics, 2016

666 **Vicenţiu D. Rădulescu, Adélia Sequeira, and Vsevolod A. Solonnikov, Editors,** Recent Advances in Partial Differential Equations and Applications, 2016

665 **Helge Glöckner, Alain Escassut, and Khodr Shamseddine, Editors,** Advances in Non-Archimedean Analysis, 2016

664 **Dihua Jiang, Freydoon Shahidi, and David Soudry, Editors,** Advances in the Theory of Automorphic Forms and Their $L$-functions, 2016

663 **David Kohel and Igor Shparlinski, Editors,** Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures, 2016

662 **Zair Ibragimov, Norman Levenberg, Sergey Pinchuk, and Azimbay Sadullaev, Editors,** Topics in Several Complex Variables, 2016

CONM 686

AGCT • Bassa et al., Editors

This volume contains the proceedings of the 15th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT), held at the Centre International de Rencontres Mathématiques in Marseille, France, from May 18–22, 2015.

Since the first meeting almost 30 years ago, the biennial AGCT meetings have been one of the main events bringing together researchers interested in explicit aspects of arithmetic geometry and applications to coding theory and cryptography. This volume contains original research articles reflecting recent developments in the field.

ISBN 978-1-4704-2810-5


CONM/686

AMS on the Web
www.ams.org

AMS