CONTEMPORARY MATHEMATICS

770

Arithmetic, Geometry, Cryptography and Coding Theory

17th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
June 10–14, 2019
Centre International de Rencontres Mathématiques,
Marseilles, France

Stéphane Ballet
Gaetan Bisson
Irene Bouw
Editors

AMS American Mathematical Society

Arithmetic, Geometry, Cryptography and Coding Theory

CONTEMPORARY MATHEMATICS

770

Arithmetic, Geometry, Cryptography and Coding Theory

17th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
June 10–14, 2019
Centre International de Rencontres Mathématiques,
Marseilles, France

Stéphane Ballet
Gaetan Bisson
Irene Bouw
Editors

AMS American Mathematical Society

2020 *Mathematics Subject Classification.* Primary 11G10, 11G20, 11G25, 11G30, 11T71, 14H45, 14K15, 20C33, 51E20, 94B27.

Library of Congress Cataloging-in-Publication Data

Names: International Conference on Arithmetic, Geometry, Cryptography and Coding Theory (17th : 2019 : Marseille, France). | Ballet, Stéphane, 1971– editor.

Title: Arithmetic, geometry, cryptography and coding theory : 17th International Conference on Arithmetic, Geometry, Cryptography and Coding Theory, June 10–14, 2019, Centre International de Rencontres Mathématiques, Marseille, France / Stéphane Ballet, Gaetan Bisson, Irene Bouw, editors.

Description: Providence, Rhode Island : American Mathematical Society, [2021] | Series: Contemporary mathematics, 0271-4132 ; volume 770 | Includes bibliographical references.

Identifiers: LCCN 2020043187 | ISBN 9781470454265 (paperback) | ISBN 9781470464264 (ebook)

Subjects: LCSH: Coding theory–Congresses. | Geometry, Algebraic–Congresses. | Cryptography–Congresses. | Number theory–Congresses. | AMS: Number theory – Arithmetic algebraic geometry (Diophantine geometry) [See also 11Dxx, 14Gxx, 14Kxx] – Abelian varieties of dimension > 1 [See also 14Kxx]. | Number theory – Arithmetic algebraic geometry (Diophantine geometry) [See also 11Dxx, 14Gxx, 14Kxx] – Curves over finite and local fields [See also 14H25]. | Number theory – Arithmetic algebraic geometry (Diophantine geometry) [See also 11Dxx, 14Gxx, 14Kxx] – Varieties over finite and local fields [See also 14G15, 14G20]. | Number theory – Arithmetic algebraic geometry (Diophantine geometry) [See also 11Dxx, 14Gxx, 14Kxx] – Curves of arbitrary genus or genus $\neq 1$ over global fields [See also 14H25]. | Number theory – Finite fields and commutative rings (number-theoretic aspects) – Algebraic coding theory; cryptography. | Algebraic geometry – Curves – Special curves and curves of low genus. | Algebraic geometry – Abelian varieties and schemes – Arithmetic ground fields [See also 11Dxx, 11Fxx, 11G10, 14Gxx]. | Group theory and generalizations – Representation theory of groups [See also 19A22 (for representation rings and Burnside rings)] – Representations of finite groups of Lie type. | Geometry For algebraic geometry, see 14-XX – Finite geometry and special incidence structures – Combinatorial structures in finite projective spaces [See also 05Bxx]. | Information and communication, circuits – Theory of error-correcting codes and error-detecting codes – Geometric methods (including applications of algebraic geometry) [See also 11T71, 14G50].

Classification: LCC QA268 .I57 2019 | DDC 510–dc23

LC record available at https://lccn.loc.gov/2020043187

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

DOI: https://doi.org/10.1090/conm/770

Color graphic policy. Any graphics created in color will be rendered in grayscale for the printed version unless color printing is authorized by the Publisher. In general, color graphics will appear in color in the online version.

In memory of Gilles Lachaud.

Contents

Preface

Since 1987, the international conference *Arithmetic, Geometry, Cryptography, and Coding Theory* ($\mathrm{AGC}^2\mathrm{T}$) has been held biennially at the *Centre International de Rencontres Mathématiques* in Marseille, France. It brings together the world's best experts on arithmetic and algebraic geometry to foster interactions between pure mathematics and computer science and information theory, specifically error-correcting codes, cryptography and algorithmic complexity.

This volume contains the proceedings of this event's 17^{th} edition, held 10–14 June 2019. It is composed of original research articles which reflect recent developments on a wide range of topics. All share the common goal of connecting arithmetic and algebraic geometry, through explicit aspects, to its many fields of applications.

$\mathrm{AGC}^2\mathrm{T}$-17 welcomed a hundred participants from around the world and we would like to pay special tribute to the speakers: Yves Aubry, Alp Bassa (plenary), Elena Berardini, Frits Beukers, Nils Bruin, Alina Bucur (plenary), Xavier Caruso (plenary), Alain Couvreur, John Cremona (plenary), Iwan Duursma, Bas Edixhoven, Sudhir Ghorpade, Alejandro Giangreco, Richard Griffon, Annamaria Iezzi, Sorina Ionica, Kiran Kedlaya (plenary), Jean Kieffer, Dmitrii Koshelev, Elisa Lorenzo García, Jade Nardi, Fabien Pazuki, Ruud Pellikaan (plenary), Matthieu Rambaud, Hugues Randriambololona, Christophe Ritzenthaler, Sergey Rybakov, Jean-Pierre Serre (plenary), Ben Smith, Andrew Sutherland, Michael Tsfasman, Christelle Vincent, Bianca Viray (plenary), and Serge Vladuts; as well as the chairmen: Peter Beelen, Jean-Marc Couveignes, Marc Hindry, James Hirschfeld, David Kohel, Ruud Pellikaan, Christophe Ritzenthaler, René Schoof, and Serge Vladuts.

The topics of the talks ranged from algebraic number theory to Diophantine geometry, and from curves and abelian varieties over finite fields to applications to codes and cryptography. They highlighted the impact of the most recent advances in computational algebraic geometry as well as algorithmic number theory.

This conference was exceptional in more ways than one. First, it was dedicated to the memory of Gilles Lachaud, one of the founding fathers of the $\mathrm{AGC}^2\mathrm{T}$ series, who passed away in 2018 at the age of seventy. It was an opportunity to celebrate his brilliant career as well as his latest work, with the present volume containing Gilles' last paper. We were also honored by the presence of Jean-Pierre Serre, who presented his latest book extending the notes from his acclaimed Harvard course *Algebraic curves over finite fields*. Finally, we want to pay tribute to our close friend Alexey Zykin, tragically deceased in 2017, while he was a member of the $\mathrm{AGC}^2\mathrm{T}$ organizing committee.

We are grateful to a great number of colleagues for making this conference a successful event. In particular we wish to acknowledge the members of the Steering

Committee, our colleagues in the Program Committee, the many reviewers who carefully evaluated submissions, and most of all the authors for submitting high-quality papers.

We are also indebted to the staff of CIRM (Olivia Barbarroux, Muriel Milton, and Laure Stefanini) and of the Institut de Mathématiques de Marseille (Jessica Bouanane, Eric Lozingot and Corinne Roux) for their remarkable professionalism and invaluable help in organizing this conference. Special thanks are also due to Christine Thivierge from American Mathematical Society, who helped us to publish the present volume in the Contemporary Mathematics series.

Last but not least, we are grateful to the sponsors of AGC^{2}T-17, namely Aix-Marseille University (AMU), the Institute of Mathematics of Marseille (I2M), the LABEX Archimède, the GAATI Laboratory of the University of French Polynesia, and the city of Marseille.

Stéphane Ballet
Gaetan Bisson
Irene Bouw

List of Participants

Samuele Anni
Aix-Marseille Université

Yves Aubry
Aix-Marseille & Toulon Université

Christine Bachoc
Université de Bordeaux

Stéphane Ballet
Aix-Marseille Université

Alp Bassa
Bogazici University

Peter Beelen
Technical University of Denmark

Jean-Robert Belliard
Université de Franche-Comté

Elena Berardini
Aix-Marseille Université

Frits Beukers
Utrecht University

Gaetan Bisson
Université de la Polynésie

Régis Blache
Université des Antilles-Guyane

Alexis Bonnecaze
Aix-Marseille Université

Irene Bouw
Universität Ulm

Nils Bruin
Simon Fraser University

Alina Bucur
University of California, San Diego

Mireille Car
Aix-Marseille Université

Xavier Caruso
CNRS & Université de Bordeaux

Leonardo Colò
Aix-Marseille Université

Jean-Marc Couveignes
Université de Bordeaux

Alain Couvreur
INRIA & École Polytechnique

John Cremona
University of Warwick

Thanh-Hung Dang
Aix-Marseille Université

Luca De Feo
Université de Versailles Saint Quentin

Bogdan Dina
Universität Ulm

Iwan Duursma
University of Illinois

Bas Edixhoven
University of Leiden

Elie Eid
Université de Rennes

Daniel Fiorilli
CNRS & Université d'Orsay

Francesc Fité
Institute for Advanced Study

Sudhir Ghorpade
IIT Bombay

Alejandro Giangreco
Aix-Marseille Université

Heidi Goodson
Brooklyn College (CUNY)

Richard Griffon
University of Basel

Emmanuel Hallouin
Université Toulouse

Johan P. Hansen
Aarhus University

Thierry Henocq
Université Toulouse

Marc Hindry
Université Paris-Diderot

James Hirschfeld
University of Sussex

Annamaria Iezzi
University of South Florida

Sorina Ionica
Université de Picardie Jules Verne

Valentijn Karemaker
University of Pennsylvania

Kiran Kedlaya
University of California, San Diego

Jean Kieffer
INRIA & Université de Bordeaux

Pinar Kilicer
University of Groningen

David Kohel
Aix-Marseille Université

Julien Koperecz
Université de Franche-Comté

Dmitrii Koshelev
Université de Versailles Saint Quentin

Philippe Langevin
Université de Toulon

Julien Lavauzelle
Université de Rennes

Philippe Lebacque
Université de Franche-Comté

Reynald Lercier
Université de Rennes

Elisa Lorenzo García
Université de Rennes

Stéphane Louboutin
Aix-Marseille Université

David Lubicz
Université de Rennes

Jean-François Mestre
Université Paris-Diderot

Fabien Narbonne
Université de Rennes

Jade Nardi
Université Paul Sabatier

Alessandro Neri
University of Zurich

Anca Nitulescu
Aarhus University

Roger Oyono
Université de la Polynésie

Bastien Pacifico
Aix-Marseille Université

Isabella Panaccione
INRIA & École Polytechnique

Fabien Pazuki
University of Copenhagen

Ruud Pellikaan
Technical University Eindhoven

Marc Perret
Université de Toulouse

Julia Pieltant
Conservatoire National des Arts et Métiers

Ivan Pogildiakov
Université de la Polynésie

Bjorn Poonen
MIT

Matthieu Rambaud
Télécom ParisTech

Hugues Randriambololona
Télécom ParisTech

Christophe Ritzenthaler
Université de Rennes

François Rodier
CNRS & Aix-Marseille Université

Robert Rolland
Aix-Marseille Université

Xavier Roulleau
Aix-Marseille Université

Edouard Rousseau
Télécom ParisTech

Sergey Rybakov
IITP & NRU HSE, Moscow

René Schoof
University Roma Tor Vergata

Jean-Pierre Serre
Collège de France

Kaloyan Slavov
ETH Zurich

Benjamin Smith
INRIA & École Polytechnique

Patrick Solé
CNRS & Télécom ParisTech

Katherine Stange
University of Colorado, Boulder

Peter Stevenhagen
University of Leiden

Andrew Sutherland
MIT

Jaap Top
University of Groningen

Michael Tsfasman
CNRS & IITP & IUM

Christelle Vincent
University of Vermont

Bianca Viray
University of Washington

Serge Vladuts
Aix-Marseille Université

Jose Felipe Voloch
University of Canterbury

Selected Published Titles in This Series

770 **Stéphane Ballet, Gaetan Bisson, and Irene Bouw, Editors,** Arithmetic, Geometry, Cryptography and Coding Theory, 2021

769 **Kiyoshi Igusa, Alex Martsinkovsky, and Gordana Todorov, Editors,** Representations of Algebras, Geometry and Physics, 2021

768 **Dražen Adamović, Andrej Dujella, Antun Milas, and Pavle Pandžić, Editors,** Lie Groups, Number Theory, and Vertex Algebras, 2021

767 **Moshe Jarden and Tony Shaska, Editors,** Abelian Varieties and Number Theory, 2021

766 **Paola Comparin, Eduardo Esteves, Herbert Lange, Sebastián Reyes-Carocca, and Rubí E. Rodríguez, Editors,** Geometry at the Frontier, 2021

765 **Michael Aschbacher,** Quaternion Fusion Packets, 2021

764 **Gabriel Cunningham, Mark Mixer, and Egon Schulte, Editors,** Polytopes and Discrete Geometry, 2021

763 **Tyler J. Jarvis and Nathan Priddis, Editors,** Singularities, Mirror Symmetry, and the Gauged Linear Sigma Model, 2021

762 **Atsushi Ichino and Kartik Prasanna,** Periods of Quaternionic Shimura Varieties. I., 2021

761 **Ibrahim Assem, Christof Geiß, and Sonia Trepode, Editors,** Advances in Representation Theory of Algebras, 2021

760 **Olivier Collin, Stefan Friedl, Cameron Gordon, Stephan Tillmann, and Liam Watson, Editors,** Characters in Low-Dimensional Topology, 2020

759 **Omayra Ortega, Emille Davie Lawrence, and Edray Herber Goins, Editors,** The Golden Anniversary Celebration of the National Association of Mathematicians, 2020

758 **Jan Šťovíček and Jan Trlifaj, Editors,** Representation Theory and Beyond, 2020

757 **Kaïs Ammari and Stéphane Gerbi, Editors,** Identification and Control: Some New Challenges, 2020

756 **Joeri Van der Veken, Alfonso Carriazo, Ivko Dimitrić, Yun Myung Oh, Bogdan D. Suceavă, and Luc Vrancken, Editors,** Geometry of Submanifolds, 2020

755 **Marion Scheepers and Ondřej Zindulka, Editors,** Centenary of the Borel Conjecture, 2020

754 **Susanne C. Brenner, Igor Shparlinski, Chi-Wang Shu, and Daniel B. Szyld, Editors,** 75 Years of Mathematics of Computation, 2020

753 **Matthew Krauel, Michael Tuite, and Gaywalee Yamskulna, Editors,** Vertex Operator Algebras, Number Theory and Related Topics, 2020

752 **Samuel Coskey and Grigor Sargsyan, Editors,** Trends in Set Theory, 2020

751 **Ashish K. Srivastava, André Leroy, Ivo Herzog, and Pedro A. Guil Asensio, Editors,** Categorical, Homological and Combinatorial Methods in Algebra, 2020

750 **A. Bourhim, J. Mashreghi, L. Oubbi, and Z. Abdelali, Editors,** Linear and Multilinear Algebra and Function Spaces, 2020

749 **Guillermo Cortiñas and Charles A. Weibel, Editors,** K-theory in Algebra, Analysis and Topology, 2020

748 **Donatella Danielli and Irina Mitrea, Editors,** Advances in Harmonic Analysis and Partial Differential Equations, 2020

747 **Paul Bruillard, Carlos Ortiz Marrero, and Julia Plavnik, Editors,** Topological Phases of Matter and Quantum Computation, 2020

746 **Erica Flapan and Helen Wong, Editors,** Topology and Geometry of Biopolymers, 2020

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

CONM 770

Arithmetic, Geometry, Cryptography and Coding Theory • Ballet, Bisson, and Bouw, Editors

This volume contains the proceedings of the 17th International Conference on Arithmetic, Geometry, Cryptography and Coding Theory (AGC^{2}T-17), held from June 10–14, 2019, at the Centre International de Rencontres Mathématiques in Marseille, France. The conference was dedicated to the memory of Gilles Lachaud, one of the founding fathers of the AGC^{2}T series.

Since the first meeting in 1987 the biennial AGC^{2}T meetings have brought together the leading experts on arithmetic and algebraic geometry, and the connections to coding theory, cryptography, and algorithmic complexity. This volume highlights important new developments in the field.

AMS
www.ams.org

ISBN 978-1-4704-5426-5
9 781470 454265
CONM/770

AMS