CONTEMPORARY MATHEMATICS

722

Arithmetic Geometry: Computation and Applications

16th International Conference
Arithmetic, Geometry, Cryptography, and Coding Theory
June 19–23, 2017
Centre International de Rencontres Mathématiques,
Marseille, France

Yves Aubry
Everett W. Howe
Christophe Ritzenthaler
Editors

AMS
AMERICAN MATHEMATICAL SOCIETY

CONTEMPORARY
MATHEMATICS

722

Arithmetic Geometry: Computation and Applications

16th International Conference
Arithmetic, Geometry, Cryptography, and Coding Theory
June 19–23, 2017
Centre International de Rencontres Mathématiques,
Marseille, France

Yves Aubry
Everett W. Howe
Christophe Ritzenthaler
Editors

AMS
AMERICAN
MATHEMATICAL
SOCIETY

2010 *Mathematics Subject Classification.* Primary 11G20, 11G30, 11G32, 11G40, 11T71, 14G10, 14H40, 14Q05, 20C20, 20G41.

Library of Congress Cataloging-in-Publication Data

Names: International Conference on Arithmetic, Geometry, Cryptography and Coding Theory (16th : 2017 : Marseille, France) | Aubry, Yves, 1965- editor. | Howe, Everett W., editor. | Ritzenthaler, Christophe, 1976- editor.

Title: Arithmetic geometry : computation and applications : 16th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory, June 19-23, 2017, Centre International de Rencontres Mathematiques, Marseille, France / Yves Aubry, Everett W. Howe, Christophe Ritzenthaler, editors.

Description: Providence, Rhode Island : American Mathematical Society, [2019] | Series: Contemporary mathematics ; volume 722 | Includes bibliographical references.

Identifiers: LCCN 2018037194 | ISBN 9781470442125 (alk. paper)

Subjects: LCSH: Coding theory–Congresses. | Geometry, Algebraic–Congresses. | Cryptography–Congresses. | Number theory–Congresses. | AMS: Number theory – Arithmetic algebraic geometry (Diophantine geometry) – Curves over finite and local fields. msc | Number theory – Arithmetic algebraic geometry (Diophantine geometry) – Curves of arbitrary genus or genus $\neq 1$ over global fields. msc | Number theory – Arithmetic algebraic geometry (Diophantine geometry) – Dessins d'enfants, Belyi theory. msc | Number theory – Arithmetic algebraic geometry (Diophantine geometry) – L-functions of varieties over global fields; Birch-Swinnerton-Dyer conjecture. msc | Number theory – Finite fields and commutative rings (number-theoretic aspects) – Algebraic coding theory; cryptography. msc | Algebraic geometry – Arithmetic problems. Diophantine geometry – Zeta-functions and related questions. msc | Algebraic geometry – Computational aspects in algebraic geometry – Curves. msc | Group theory and generalizations – Representation theory of groups – Modular representations and characters. msc | Group theory and generalizations – Linear algebraic groups and related topics – Exceptional groups. msc

Classification: LCC QA268 .I57 2017 | DDC 512.7/4–dc23

LC record available at https://lccn.loc.gov/2018037194

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

DOI: https://doi.org/10.1090/conm/722

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `https://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

Contents

Preface

The 16th edition of the AGC^{2}T conference (Arithmetic, Geometry, Cryptography, and Coding Theory) took place at CIRM (Centre International de Rencontres Mathématiques) in Marseille, France, on June 19–23, 2017. This international conference has been a major event in the area of arithmetic geometry and its applications since 1987, and more than 94 participants joined us to celebrate its 30th anniversary. We thank all of them for creating a stimulating research environment during our week together.

The topics of the talks extended from algebraic number theory to diophantine geometry, and from curves and abelian varieties over finite fields to applications in codes and cryptography. We especially thank the speakers — Jeff Achter, Elise Barelli, Irene Bouw, Nils Bruin, Wouter Castryck, Alina Cojocaru, Mrinmoy Datta, Lucile Devin, Iwan Duursma, Elena Egorova, Sudhir Ghorpade, Marc Hindry, Nathan Kaplan, Valentijn Karemaker, Daniel Katz, Kiran Kedlaya, Pınar Kılıçer, Gilles Lachaud, Philippe Lebacque, Elisa Lorenzo García, Stefano Marseglia, Ivan Pogildiakov, Bjorn Poonen, Rachel Pries, Matthieu Rambaud, Alice Silverberg, Prasant Singh, Andrew Sutherland, Medhi Tibouchi, Andrey Trepalin, Michael Tsfasman, John Voight, Felipe Voloch, Marius Vuille, and Chia-Fu Yu — for their lectures.

As with any anniversary, it was a time for joy and exuberance, and some of the participants' memories of earlier editions of AGC^{2}T were recorded with the kind assistance of Stéphanie Vareilles and Guillaume Hennenfent.[1] It was also a moment for recollection and reflection, as the "AGC^{2}T family" had lost one of its youngest and most brilliant members in the person of Alexey Zykin, who passed away with his wife Tatyana Makarova in a tragic accident a few months before the conference. With Alexey's friends and colleagues, we celebrated one more time his constant enthusiasm in all aspects of his research and life.

Gilles Lachaud, one of the founding fathers of the conference and one of its mainstays, passed away in February 2018. The next edition of the conference will have time set aside for memories of Gilles and for celebrations of his legacy. For now, we are honored to present one of his papers in this volume.

The editors would like to thank the staff of CIRM (Olivia Barbarroux, Muriel Milton, and Laure Stefanini) and of the Institut de Mathématiques de Marseille (Jessica Bouanane and Corinne Roux) for their remarkable professionalism and their friendly and constant help. We would also like to thank Christine Thivierge at the American Mathematical Society for guiding us through the *Contemporary Mathematics* production process. And of course, we give our deepest thanks to the

[1] The video is available at `https://youtu.be/KWklMv4Yya8`.

authors of the papers in this volume for their mathematical creativity and for their patience with the editors.

Toulon, France	Yves Aubry
San Diego, California, U.S.A.	Everett Howe
Rennes, France	Christophe Ritzenthaler
June 2018	

Selected Published Titles in This Series

722 **Yves Aubry, Everett W. Howe, and Christophe Ritzenthaler, Editors,** Arithmetic Geometry: Computation and Applications, 2019

718 **David Ayala, Daniel S. Freed, and Ryan E. Grady, Editors,** Topology and Quantum Theory in Interaction, 2018

717 **Federico Bonetto, David Borthwick, Evans Harrell, and Michael Loss, Editors,** Mathematical Problems in Quantum Physics, 2018

716 **Alex Martsinkovsky, Kiyoshi Igusa, and Gordana Todorov, Editors,** Surveys in Representation Theory of Algebras, 2018

715 **Sergio R. López-Permouth, Jae Keol Park, S. Tariq Rizvi, and Cosmin S. Roman, Editors,** Advances in Rings and Modules, 2018

714 **Jens Gerlach Christensen, Susanna Dann, and Matthew Dawson, Editors,** Representation Theory and Harmonic Analysis on Symmetric Spaces, 2018

713 **Naihuan Jing and Kailash C. Misra, Editors,** Representations of Lie Algebras, Quantum Groups and Related Topics, 2018

712 **Nero Budur, Tommaso de Fernex, Roi Docampo, and Kevin Tucker, Editors,** Local and Global Methods in Algebraic Geometry, 2018

711 **Thomas Creutzig and Andrew R. Linshaw, Editors,** Vertex Algebras and Geometry, 2018

710 **Raphaël Danchin, Reinhard Farwig, Jiří Neustupa, and Patrick Penel, Editors,** Mathematical Analysis in Fluid Mechanics, 2018

709 **Fernando Galaz-García, Juan Carlos Pardo Millán, and Pedro Solórzano, Editors,** Contributions of Mexican Mathematicians Abroad in Pure and Applied Mathematics, 2018

708 **Christian Ausoni, Kathryn Hess, Brenda Johnson, Ieke Moerdijk, and Jérôme Scherer, Editors,** An Alpine Bouquet of Algebraic Topology, 2018

707 **Nitya Kitchloo, Mona Merling, Jack Morava, Emily Riehl, and W. Stephen Wilson, Editors,** New Directions in Homotopy Theory, 2018

706 **Yeonhyang Kim, Sivaram K. Narayan, Gabriel Picioroaga, and Eric S. Weber, Editors,** Frames and Harmonic Analysis, 2018

705 **Graham J. Leuschke, Frauke Bleher, Ralf Schiffler, and Dan Zacharia, Editors,** Representations of Algebras, 2018

704 **Alain Escassut, Cristina Perez-Garcia, and Khodr Shamseddine, Editors,** Advances in Ultrametric Analysis, 2018

703 **Andreas Malmendier and Tony Shaska, Editors,** Higher Genus Curves in Mathematical Physics and Arithmetic Geometry, 2018

702 **Mark Grant, Gregory Lupton, and Lucile Vandembroucq, Editors,** Topological Complexity and Related Topics, 2018

701 **Joan-Carles Lario and V. Kumar Murty, Editors,** Number Theory Related to Modular Curves, 2018

700 **Alexandre Girouard, Dmitry Jakobson, Michael Levitin, Nilima Nigam, Iosif Polterovich, and Frédéric Rochon, Editors,** Geometric and Computational Spectral Theory, 2017

699 **Mark L. Agranovsky, Matania Ben-Artzi, Catherine Bénéteau, Lavi Karp, Dmitry Khavinson, Simeon Reich, David Shoikhet, Gilbert Weinstein, and Lawrence Zalcman, Editors,** Complex Analysis and Dynamical Systems VII, 2017

698 **Alexander M. Blokh, Leonid A. Bunimovich, Paul H. Jung, Lex G. Oversteegen, and Yakov G. Sinai, Editors,** Dynamical Systems, Ergodic Theory, and Probability: in Memory of Kolya Chernov, 2017

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

CONM 722

Arithmetic Geometry: Computation and Applications • Aubry et al., Editors

For thirty years, the biennial international conference AGC^{2}T (Arithmetic, Geometry, Cryptography, and Coding Theory) has brought researchers to Marseille to build connections between arithmetic geometry and its applications, originally highlighting coding theory but more recently including cryptography and other areas as well.

This volume contains the proceedings of the 16th international conference, held from June 19–23, 2017.

The papers are original research articles covering a large range of topics, including weight enumerators for codes, function field analogs of the Brauer–Siegel theorem, the computation of cohomological invariants of curves, the trace distributions of algebraic groups, and applications of the computation of zeta functions of curves. Despite the varied topics, the papers share a common thread: the beautiful interplay between abstract theory and explicit results.

AMS
www.ams.org

ISBN 978-1-4704-4212-5

9 781470 442125
CONM/722

AMS