

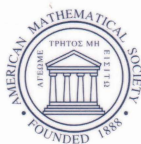
CONTEMPORARY MATHEMATICS

463

Computational Arithmetic Geometry

AMS Special Session
April 29–30, 2006
San Francisco State University
San Francisco, California

Kristin E. Lauter
Kenneth A. Ribet
Editors



Computational Arithmetic Geometry



Special Session at the San Francisco AMS meeting, April 29-30, 2006.

Front group: Iftikhar Burhanuddin, Tong Hai Yang, Ken Ono, Alina Cojocaru, Kristin Lauter, Kenneth Ribet, René Schoof, Loïc Merel, Peter Stevenhagen

Back group: Everett Howe, David Freeman, Jordan Ellenberg, Kate Stevenson, Jayce Getz, Nils Bruin, Dimitar Jetchev, Bjorn Poonen, David Grant, Denis Charles, Ronald van Luijk, William McCallum, Kiran Kedlaya, David Zywina, Jared Weinstein, William Cherry, David Brown, Lassina Dembele, Byungchul Cha

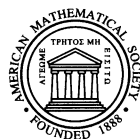
CONTEMPORARY MATHEMATICS

463

Computational Arithmetic Geometry

AMS Special Session
April 29–30, 2006
San Francisco State University
San Francisco, California

Kristin E. Lauter
Kenneth A. Ribet
Editors



American Mathematical Society
Providence, Rhode Island

Editorial Board

Dennis DeTurck, managing editor

George Andrews Abel Klein

2000 *Mathematics Subject Classification*. Primary 14G05, 14G10, 14G15, 14G50, 14H45, 11G50, 11G15, 11G20, 11Y16, 11F11.

Photo courtesy of Kenneth A. Ribet

Library of Congress Cataloging-in-Publication Data

AMS Special Session on Computational Arithmetic Geometry (2006 : San Francisco, Calif.)

Computational arithmetic geometry : AMS Special Session on Computational Arithmetic Geometry, April 29–30, 2006, San Francisco State University, San Francisco, CA / Kristin E. Lauter, Kenneth A. Ribet, editors.

p. cm. — (Contemporary mathematics, ISSN 0271-4132 ; v. 463)

ISBN 978-0-8218-4320-8 (alk. paper)

1. Arithmetical algebraic geometry—Congresses. 2. Algebraic number theory—Congresses. I. Lauter, Kristin E. (Kristin Estella), 1969– II. Ribet, Kenneth.

QA242.5.A48 2008
516.3'5—dc22

2008010326

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2008 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Copyright of individual articles may revert to the public domain 28 years
after publication. Contact the AMS for copyright status of individual articles.

Printed in the United States of America.

∞ 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 <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 13 12 11 10 09 08

To Tom, Joyce, and Josephine
To Lisa, Caroline and Stephanie

Contents

Preface	ix
Schedule of talks	xi
Results of Cohen–Lenstra type for quadratic function fields JEFFREY D. ACHTER	1
The hardness of computing an eigenform ERIC BACH and DENIS CHARLES	9
Constructing elliptic curves of prime order REINIER BRÖKER and PETER STEVENHAGEN	17
Space-time codes and non-associative division algebras arising from elliptic curves ABDULAZIZ DEAJIM and DAVID GRANT	29
Points of low height on \mathbb{P}^1 over number fields and bounds for torsion in class groups JORDAN S. ELLENBERG	45
Supersingular genus-2 curves over fields of characteristic 3 EVERETT W. HOWE	49
Search techniques for root-unitary polynomials KIRAN S. KEDLAYA	71
Yet more elements in the Shafarevich–Tate group of the jacobian of a Fermat Curve BENJAMIN LEVITT and WILLIAM MCCALLUM	83
Stable reduction of $X_0(81)$ KEN MCMURDY	91
Isomorphism types of commutative algebras of finite rank over an algebraically closed field BJORN POONEN	111
A short guide to p -torsion of abelian varieties in characteristic p RACHEL PRIES	121

Preface

This volume is the record of the special session on computational aspects of arithmetic geometry at the April, 2006 regional meeting of the American Mathematical Society at San Francisco State University. Our session attracted a large number of outstanding researchers in the field, many of whom presented talks at the session and contributed manuscripts to this volume.

In planning our gathering, we decided to stress computational issues because of recent and ongoing increases in computing power. These increases have enabled computational breakthroughs in any number of areas of arithmetic geometry. For example, Cremona's tables of elliptic curves now go up to conductor 120,000 instead of just conductor 1,000; tables of Hilbert class fields are known for discriminant up to at least 5,000; and special values of Hilbert and Siegel modular forms can be calculated to extremely high precision. In many cases, these experimental capabilities have led to new observations and ideas for progress in the field. They have also led to natural algorithmic questions on the feasibility and efficiency of many computations, especially for the purpose of applications in cryptography.

As our gathering took shape, we were able to identify themes that united clusters of talks: modular abelian varieties; Tate–Shafarevich groups of elliptic curves; Stark's conjectures; Hilbert modular varieties; curves with complex multiplication. In scheduling the lectures, we grouped these clusters together whenever possible.

A thread that ran through a number of the talks was the application of number theory and algebraic geometry to cryptography and coding theory. Potential applications in these areas have suggested interesting mathematical questions and computational challenges that are addressed by articles in this volume. For example, the article by Bach and Charles addresses hardness of computing eigenforms and relates it to breaking RSA cryptosystems based on the hardness of factoring integers. The contribution by Bröker and Steinhagen addresses the issue of generating elliptic curves for use in cryptography by finding an efficient algorithm for generating good parameters for using the CM (complex multiplication) method. The contribution by Deajim and Grant uncovers interesting number theory questions when constructing good space-time codes. Two papers relate to zeta functions of curves and surfaces, one providing algorithms for computing zeta functions and one answering the question of which zeta functions of supersingular genus 2 curves are possible over finite fields of characteristic 3. We hope that this collection will interest number theorists, algebraic geometers and cryptographers and that its contents will contribute to the ongoing interaction among these groups.

Kristin Lauter
Ken Ribet

Schedule of talks

Saturday morning, April 29:

Heegner points and Tate-Shafarevich Groups

8:00am–8:30am: William McCallum

Yet more nontrivial elements in Shafarevich-Tate groups of Fermat curves.

8:30am–9:00am: Byungchul Cha

Vanishing of some cohomology groups and bounds for Shafarevich–Tate groups of elliptic curves.

9:00am–9:30am: Samit Dasgupta

Shintani zeta-functions and Gross-Stark units for totally real fields.

9:30am–10:00am: Ken McMurdy

Heegner Points on $X_0(p^n)$.

10:00am–10:30am: Nils Bruin

Solvability of small curves of genus 2.

10:30am–11:00am: William Stein

SAGE — Software for Algebra and Geometry Experimentation.

Saturday afternoon, April 29:

Hilbert modular surfaces

3:00pm–3:30pm: Tonghai Yang

A basic intersection problem on Hilbert modular surfaces.

3:30pm–4:00pm: Lassina Dembele

Examples of automorphic forms on the unitary group in three variables.

4:00pm–4:30pm: Amod Agashe

Rational torsion of elliptic curves and the cuspidal subgroup.

4:30pm–5:00pm: Jayce Getz

Hilbert modular forms, intersection homology base change.

5:00pm–5:30pm: Ken Ono

Traces of singular moduli on Hilbert surfaces.

Sunday morning, April 30:

Curves I

8:00am–8:30am: Kiran Kedlaya

Computing zeta functions of surfaces using p -adic cohomology.

- 8:30am–9:00am: Jeff Achter
Divisibility of function field class numbers.
- 9:00am–9:30am: Alina Cojocaru
Frobenius fields for Drinfeld modules of rank 2
- 9:30am–10:00am: Denis Charles
Some applications of the graph of supersingular elliptic curves.
- 10:00am–10:30am: Everett Howe
Jacobians in isogeny classes of supersingular surfaces over finite fields.
- 10:30am–11:00am: Peter Stevenhagen
Constructing elliptic curves in almost polynomial time

Sunday afternoon, April 30:

Curves II

- 3:00pm–3:30pm: Rachel Pries
The p -torsion of curves in characteristic p .
- 3:30pm–4:00pm: Kate Stevenson
Local Galois theory in dimension two.
- 4:00pm–4:30pm: David Grant
Number Theoretic Aspects of Space-Time Codes.
- 4:30pm–5:00pm: Bjorn Poonen
Gonality of modular curves in characteristic p .
- 5:00pm–5:30pm: Jordan Ellenberg
Reflection principles and l -parts of class groups.
- 5:30pm–6:00pm: Rene Schoof
Modular curves and semistable abelian varieties over \mathbb{Q} .

Titles in This Series

- 463 **Kristin E. Lauter and Kenneth A. Ribet, Editors**, Computational arithmetic geometry, 2008
- 462 **Giuseppe Dito, Hugo García-Compeán, Ernesto Lupercio, and Francisco J. Turrubiates, Editors**, Non-commutative geometry in mathematics and physics, 2008
- 461 **Gary L. Mullen, Daniel Panario, and Igor Shparlinski, Editors**, Finite Fields and Applications, 2008
- 460 **Megumi Harada, Yael Karshon, Mikiya Masuda, and Taras Panov, Editors**, Toric topology, 2008
- 459 **Marcelo J. Saia and José Seade, Editors**, Real and complex singularities, 2008
- 458 **Jinho Baik, Thomas Kriecherbauer, Luen-Chau Li, Kenneth D. T-R McLaughlin, and Carlos Tomei, Editors**, Integrable systems and random matrices, 2008
- 457 **Tewodros Amdeberhan and Victor H. Moll, Editors**, Tapas in experimental mathematics, 2008
- 456 **S. K. Jain and S. Parvathi, Editors**, Noncommutative rings, group rings, diagram algebras and their applications, 2008
- 455 **Mark Agranovsky, Daoud Bshouty, Lavi Karp, Simeon Reich, David Shoikhet, and Lawrence Zalcman, Editors**, Complex analysis and dynamical systems III, 2008
- 454 **Rita A. Hirschweiler and Thomas H. MacGregor, Editors**, Banach spaces of analytic functions, 2008
- 453 **Jacob E. Goodman, János Pach, and Richard Pollack, Editors**, Surveys on Discrete and Computational Geometry—Twenty Years Later, 2008
- 452 **Matthias Beck, Christian Haase, Bruce Reznick, Michèle Vergne, Volkmar Welker, and Ruriko Yoshida, Editors**, Integer points in polyhedra, 2008
- 451 **David R. Larson, Peter Massopust, Zuhair Nashed, Minh Chuong Nguyen, Manos Papadakis, and Ahmed Zayed, Editors**, Frames and operator theory in analysis and signal processing, 2008
- 450 **Giuseppe Dito, Jiang-Hua Lu, Yoshiaki Maeda, and Alan Weinstein, Editors**, Poisson geometry in mathematics and physics, 2008
- 449 **Robert S. Doran, Calvin C. Moore, and Robert J. Zimmer, Editors**, Group representations, ergodic theory, and mathematical physics: A tribute to George W. Mackey, 2007
- 448 **Alberto Corso, Juan Migliore, and Claudia Polini, Editors**, Algebra, geometry and their interactions, 2007
- 447 **François Germinet and Peter Hislop, Editors**, Adventures in mathematical physics, 2007
- 446 **Henri Berestycki, Michiel Bertsch, Felix E. Browder, Louis Nirenberg, Lambertus A. Peletier, and Laurent Véron, Editors**, Perspectives in Nonlinear Partial Differential Equations, 2007
- 445 **Laura De Carli and Mario Milman, Editors**, Interpolation Theory and Applications, 2007
- 444 **Joseph Rosenblatt, Alexander Stokolos, and Ahmed I. Zayed, Editors**, Topics in harmonic analysis and ergodic theory, 2007
- 443 **Joseph Stephen Verducci and Xiaotong Shen, Editors**, Prediction and discovery, 2007
- 442 **Yi-Zhi Huang and Kailash C Misra, Editors**, Lie algebras, vertex operator algebras and their applications, 2007
- 441 **Louis H. Kauffman, David E. Radford, and Fernando J. O. Souza, Editors**, Hopf algebras and generalizations, 2007

TITLES IN THIS SERIES

- 440 **Fernanda Botelho, Thomas Hagen, and James Jamison, Editors**, Fluids and Waves, 2007
- 439 **Donatella Danielli, Editor**, Recent developments in nonlinear partial differential equations, 2007
- 438 **Marc Burger, Michael Farber, Robert Ghrist, and Daniel Koditschek, Editors**, Topology and robotics, 2007
- 437 **José C. Mourão, João P. Nunes, Roger Picken, and Jean-Claude Zambrini, Editors**, Prospects in mathematical physics, 2007
- 436 **Luchezar L. Avramov, Daniel Christensen, William G Dwyer, Michael A Mandell, and Brooke E Shipley, Editors**, Interactions between homotopy theory and algebra, 2007
- 435 **Krzysztof Jarosz, Editor**, Function spaces, 2007
- 434 **S. Paycha and B. Uribe, Editors**, Geometric and topological methods for quantum field theory, 2007
- 433 **Pavel Etingof, Shlomo Gelaki, and Steven Shnider, Editors**, Quantum groups, 2007
- 432 **Dick Canary, Jane Gilman, Juha Heinonen, and Howard Masur, Editors**, In the tradition of Ahlfors-Bers, IV, 2007
- 431 **Michael Batanin, Alexei Davydov, Michael Johnson, Stephen Lack, and Amnon Neeman, Editors**, Categories in algebra, geometry and mathematical physics, 2007
- 430 **Idris Assani, Editor**, Ergodic theory and related fields, 2007
- 429 **Gui-Qiang Chen, Elton Hsu, and Mark Pinsky, Editors**, Stochastic analysis and partial differential equations, 2007
- 428 **Estela A. Gavosto, Marianne K. Korten, Charles N. Moore, and Rodolfo H. Torres, Editors**, Harmonic analysis, partial differential equations, and related topics, 2007
- 427 **Anastasios Mallios and Marina Haralampidou, Editors**, Topological algebras and applications, 2007
- 426 **Fabio Ancona, Irena Lasiecka, Walter Littman, and Roberto Triggiani, Editors**, Control methods in PDE-dynamical systems, 2007
- 425 **Su Gao, Steve Jackson, and Yi Zhang, Editors**, Advances in Logic, 2007
- 424 **V. I. Burenko, T. Iwaniec, and S. K. Vodopyanov, Editors**, Analysis and geometry in their interaction, 2007
- 423 **Christos A. Athanasiadis, Victor V. Batyrev, Dimitrios I. Dais, Martin Henk, and Francisco Santos, Editors**, Algebraic and geometric combinatorics, 2007
- 422 **JongHae Keum and Shigeyuki Kondō, Editors**, Algebraic geometry, 2007
- 421 **Benjamin Fine, Anthony M. Gaglione, and Dennis Spellman, Editors**, Combinatorial group theory, discrete groups, and number theory, 2007
- 420 **William Chin, James Osterburg, and Declan Quinn, Editors**, Groups, rings and algebras, 2006
- 419 **Dinh V. Huynh, S. K. Jain, and S. R. López-Permouth, Editors**, Algebra and Its applications, 2006
- 418 **Lothar Gerritzen, Dorian Goldfeld, Martin Kreuzer, Gerhard Rosenberger, and Vladimir Shpilrain, Editors**, Algebraic methods in cryptography, 2006
- 417 **Vadim B. Kuznetsov and Siddhartha Sahi, Editors**, Jack, Hall-Littlewood and Macdonald polynomials, 2006
- 416 **Toshitake Kohno and Masanori Morishita, Editors**, Primes and knots, 2006

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

With the recent increase in available computing power, new computations are possible in many areas of arithmetic geometry. To name just a few examples, Cremona's tables of elliptic curves now go up to conductor 120,000 instead of just conductor 1,000, tables of Hilbert class fields are known for discriminant up to at least 5,000, and special values of Hilbert and Siegel modular forms can be calculated to extremely high precision. In many cases, these experimental capabilities have led to new observations and ideas for progress in the field. They have also led to natural algorithmic questions on the feasibility and efficiency of many computations, especially for the purpose of applications in cryptography. The AMS Special Session on Computational Arithmetic Geometry, held on April 29–30, 2006, in San Francisco, CA, gathered together many of the people currently working on the computational and algorithmic aspects of arithmetic geometry. This volume contains research articles related to talks given at the session. The majority of articles are devoted to various aspects of arithmetic geometry, mainly with a computational approach.

ISBN 978-0-8218-4320-8



CONM/463

AMS *on the Web*
www.ams.org