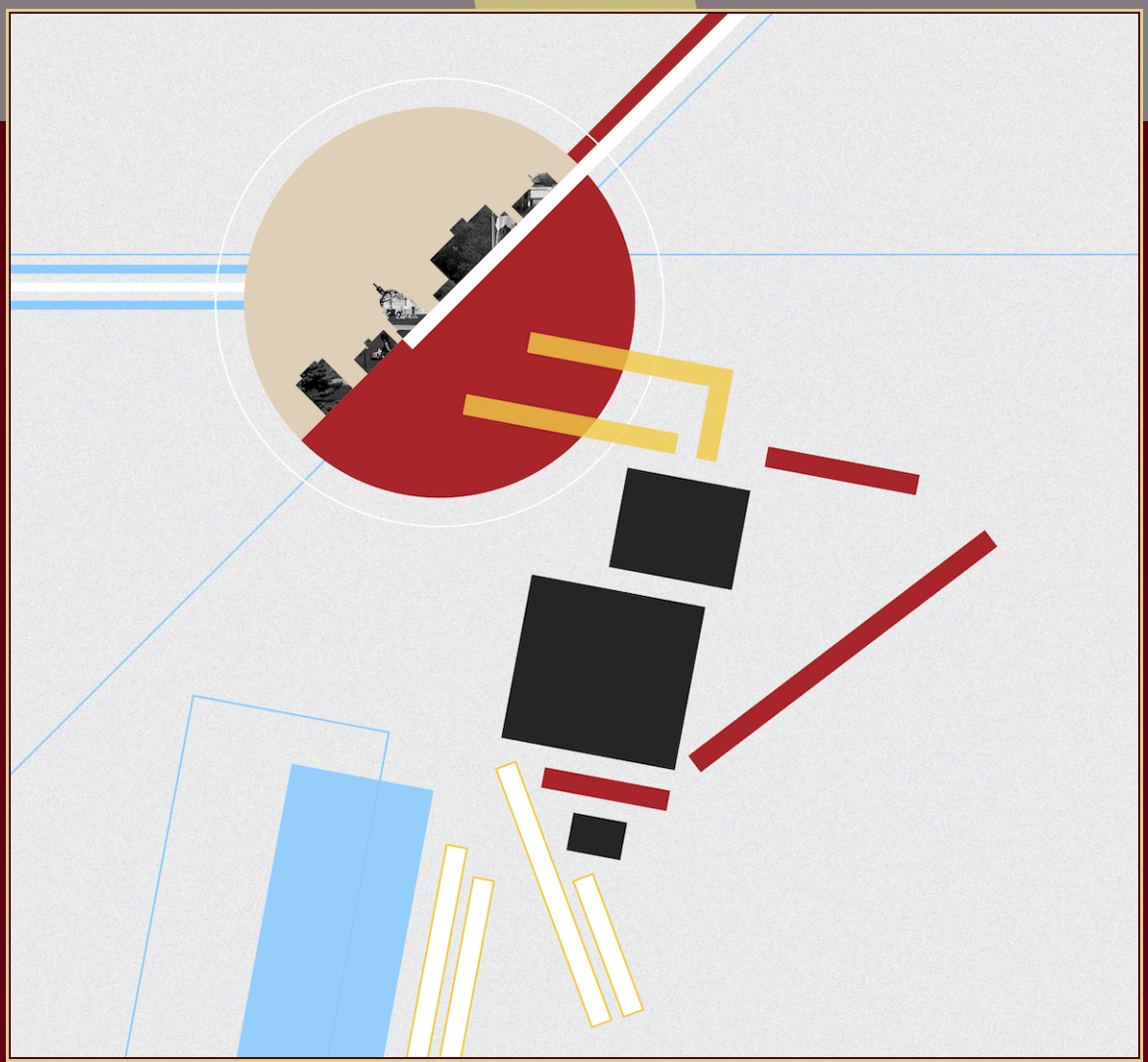
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Preface

Renate Scheidler and Jonathan Sorenson



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.7

Preface

The biennial, international Algorithmic Number Theory Symposium (ANTS) provides the premier international forum for state-of-the-art research in computational and algorithmic number theory. This conference is devoted to algorithmic aspects of all branches of number theory, including elementary number theory, algebraic number theory, analytic number theory, geometry of numbers, arithmetic algebraic geometry, finite fields, and cryptography.

ANTS-XIII, the thirteenth meeting in the Algorithmic Number Theory Symposia series, was held July 16-20, 2018, at the University of Wisconsin-Madison. This volume contains the 28 contributed papers that were presented at the conference; each paper was presented by one of the paper's authors. These 28 papers were selected from 48 submissions through a double-blind refereeing process, where the program committee solicited a minimum of two expert referees for each paper.

In addition to the contributed papers, the conference featured five invited plenary speakers, a poster session on the afternoon of July 17, and a rump session on the afternoon of July 19.

The organizing committee encouraged participation by women and underrepresented minorities. The 109 people who attended represented 13 countries. About 38% of the attendees were graduate or undergraduate students, and about 26% identified as female.

Details about ANTS-XIII, such as the conference schedule, talk slides, abstracts of talks and posters, and more can be found on the conference website at http://www.math.grinnell.edu/~paulhusj/ants2018/.

Plenary speakers

Jennifer Balakrishnan (Boston University, USA)
Noam Elkies (Harvard University, USA)
Steven Galbraith (University of Auckland, New Zealand)
Melanie Matchett Wood (University of Wisconsin-Madison, USA)
Emmanuel Thomé (INRIA, Nancy, France)

Selfridge Prize

At each ANTS meeting since 2006, the Selfridge Prize in Number Theory has been awarded for the best submitted paper as judged by the program committee; the prize carries a cash award funded by the Number Theory Foundation. The winners of the 2018 Selfridge Prize are Michael Musty (Dartmouth College, USA), Sam Schiavone (Dartmouth College, USA), Jeroen Sijsling (Universität Ulm, Germany), and John Voight (Dartmouth College, USA) for their paper "A database of Belyi maps".

Poster Session Prize

The poster session was held Tuesday, July 17 from 2:30 to 3:45 PM. There were 19 poster presentations. Thanks to a generous gift from the American Mathematical Society, the top poster at the conference, as chosen by participant vote, was awarded a US$150 gift certificate to the AMS bookstore. This award went to Travis Scholl (University of Washington, USA), for his poster "Abelian varieties with few isogenies and cryptography."

Organizing Committee

Eric Bach (University of Wisconsin-Madison, USA)
Joshua Holden (Rose-Hulman Institute of Technology, USA)
Jennifer Paulhus (Grinnell College, USA)
Andrew Shallue (Illinois Wesleyan University, USA)

Program Committee

Andrew Booker (University of Bristol, England)
Alina Bucur (University of California San Diego, USA)
John Cremona (University of Warwick, England)
Alyson Deines (Center for Communications Research, USA)
Alex Ghitza (University of Melbourne, Australia)
Mark Giesbrecht (University of Waterloo, Canada)
Everett Howe (Center for Communications Research, USA)
Laurent Imbert (LIRMM, France)
István Gaál (University of Debrecen, Hungary)
Habiba Kadiri (University of Lethbridge, Canada)
David Kohel (Institut de Mathématiques de Marseille, France)
Yoonjin Lee (Ewha Women's University, South Korea)
Alina Ostafe (University of New South Wales, Australia)
Christophe Ritzenthaler (University of Rennes, France)
Damien Robert (INRIA, France)
Renate Scheidler (co-chair) (University of Calgary, Canada)
Jonathan Sorenson (co-chair) (Butler University, USA)
Brigitte Vallée (Caen University, France)
Christelle Vincent (University of Vermont, USA)
Christian Wüthrich (University of Nottingham, England)
Paul Zimmermann (INRIA, France)

Sponsors

American Mathematical Society
National Science Foundation
National Security Agency
Number Theory Foundation
Pacific Institute for the Mathematical Sciences
Grinnell College
Illinois Wesleyan University
Rose-Hulman Institute of Technology
University of Wisconsin-Madison

Acknowledgements

The organizers are very grateful to a variety of generous sponsors who helped make this conference happen. Thanks to the National Science Foundation, the National Security Agency, and the Pacific Institute for the Mathematical Sciences for providing participant travel support. Thanks to the Number Theory Foundation for its continuing support of the Selfridge Prize for best paper at ANTS. Thanks to the American Mathematical Society for supporting a prize for best poster at ANTS. Thanks to Illinois Wesleyan University, Rose-Hulman Institute of Technology, and Grinnell College for their financial support. Finally, thanks to the University of Wisconsin-Madison for hosting ANTS, and in particular the UW Computer Science Department for staff support, and Grainger Hall Conference Services for site support.

The organizers also wish to thank everyone who contributed their time and expertise on a volunteer basis, including members of the program committee, anonymous referees, session chairs, and graduate students who helped with the registration table. Thank you to Daniel J. Bernstein (University of Illinois at Chicago, USA) and Tanje Lange (Technische Universiteit Eindhoven, The Netherlands) for organizing and running the Rump Session. Thanks to all the staff members at the co-organizers' home institutions who provided support.

The cover image is based on a design by Linh Chi Bui.

RENATE SCHEIDLER: rscheidl@ucalgary.ca
University of Calgary, Calgary, AB T2N 1N4, Canada

JONATHAN SORENSON: jsorenso@butler.edu
Butler University, Indianapolis, IN 46208, United States

ANTS History

I	1994	Cornell University (Ithaca, NY, USA)	LNCS 877
II	1996	Université Bordeaux 1 (Talence, France)	LNCS 1122
III	1998	Reed College (Portland, OR, USA)	LNCS 1423
IV	2000	Universiteit Leiden (The Netherlands)	LNCS 1838
V	2002	University of Sydney (Australia)	LNCS 2369
VI	2004	University of Vermont (Burlington, VT, USA)	LNCS 3076
VII	2006	Technische Universität Berlin (Germany)	LNCS 4076
VIII	2008	Banff Centre (Banff, Alberta, Canada)	LNCS 5011
IX	2010	INRIA (Nancy, France)	LNCS 6197
X	2012	University of California (San Diego, CA, USA)	MSP OBS 1
XI	2014	Hotel Hyundai (GyeongJu, Korea)	LMS JCM 17
XII	2016	University of Kaiserslautern (Kaiserslautern, Germany)	LMS JCM 19
XIII	2018	University of Wisconsin-Madison (Madison, USA)	MSP OBS 2

ANTS proceedings have been published through the Springer series *Lecture Notes in Computer Science* (LNCS), the London Mathematics Society *Journal of Computation and Mathematics* (LMS JCM), and Mathematical Sciences Publishers *Open Book Series* (MSP OBS). Each volume from X onwards is freely available at the respective web site.

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine