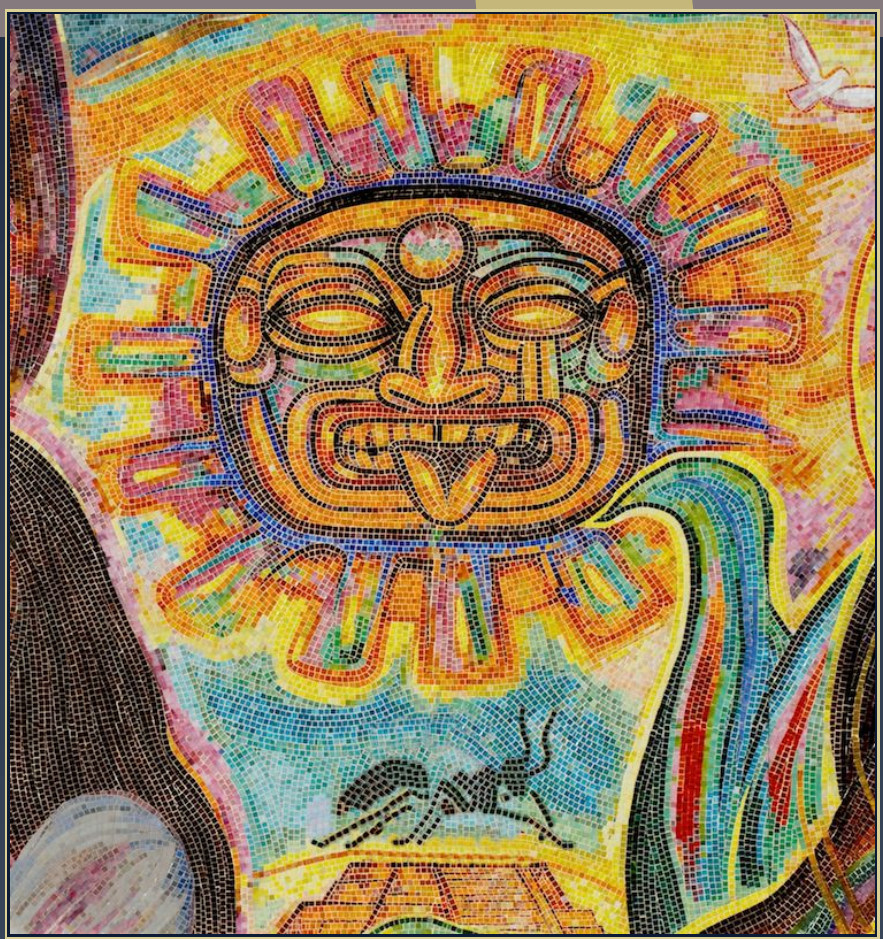
THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Preface

Everett W. Howe and Kiran S. Kedlaya



msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.7

Preface

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 tenth ANTS meeting, held July 9–13, 2012 at the University of California, San Diego. The scientific program of ANTS X consisted of 5 invited lectures, 25 contributed talks, a poster session, and a rump session. The invited speakers were Manjul Bhargava (Princeton University), Nils Bruin (Simon Fraser University), Wen-Ching Winnie Li (Pennsylvania State University), Nils-Peter Skoruppa (Universität Siegen), and Andrew Sutherland (Massachusetts Institute of Technology). Extended abstracts of the presentations of Bruin and Sutherland are included in this volume.

The contributed talks were presentations of papers chosen through a competitive review process. Each of the 55 papers submitted for consideration was reviewed by at least three members of the program committee, often with input from one or more external reviewers as well. Revised and edited versions of the 25 accepted papers are included in this volume.

At each ANTS since 2006, the Number Theory Foundation has sponsored the Selfridge Prize, an award for the best contributed paper, as judged by the program committee. The Selfridge Prize for ANTS X was awarded to Andrew Sutherland for his paper *On the evaluation of modular polynomials*.

Abstracts of all presentations (including invited presentations and posters), PDF slides of many presentations, and the versions of the contributed papers that were presented at the conference can be found on the conference web site:

http://math.ucsd.edu/~kedlaya/ants10/

For each of the previous ANTS conferences, the proceedings volume was produced before the meeting and was available at the meeting. This publication timeline allowed for very little editing and did not permit authors to revise their papers to incorporate insights gained from discussions during the conference. Following a suggestion raised in previous years, the ANTS X organizing committee decided to

produce the proceedings volume *after* the conference. The committee also decided to switch publishers; we are proud to note that this volume is the inaugural volume of the Open Book Series of Mathematical Sciences Publishers.

A word about bibliographic references: The editors tried their best to find online versions of the references that are cited in the ANTS papers. If you are reading a PDF version of one of the papers in this volume, and if one of its references has a title that is colored blue, then the title is a hyperlink to an online copy of the reference. If you are reading a printed copy of an ANTS paper, the hyperlinks will unfortunately no longer work. However, there are still ways to find online versions of cited references. For example, the AMS Digital Mathematics Registry includes a useful list of journal archives:

http://www.ams.org/dmr/JournalList.html

For some of the ANTS references that appear in journals that are not on the AMS list, the editors were nevertheless able to track down online versions. For these references, we spell out the URL of the paper in the bibliographic entry.

The editors are grateful to the authors of the papers in this volume for their flexibility and graciousness during the editing process. The editors are equally grateful to Silvio Levy and Alex Scorpan, our contacts at Mathematical Sciences Publishers, for *their* flexibility and graciousness. We hope that the reader will find the value added by the editing to be sufficient recompense for the extra year's wait for the volume to appear.

Everett Howe and Kiran Kedlaya
San Diego, November 2013

Local organizing committee.

Alina Bucur	University of California, San Diego
Joe Buhler	Center for Communications Research, La Jolla
Dan Gordon	Center for Communications Research, La Jolla
Everett Howe	Center for Communications Research, La Jolla
Kiran Kedlaya	University of California, San Diego
Kristin Lauter	Microsoft Research

Program committee.

Dan Bernstein	University of Illinois, Chicago
Alina Bucur	University of California, San Diego
Joe Buhler	Center for Communications Research, La Jolla
Henri Cohen	Université de Bordeaux 1
Chantal David	Concordia University
Steven Galbraith	University of Auckland

Dan Gordon	Center for Communications Research, La Jolla
Everett Howe (cochair)	Center for Communications Research, La Jolla
Kiran Kedlaya (cochair)	University of California, San Diego
Jürgen Klüners	Universität Paderborn
Kristin Lauter	Microsoft Research
Fernando Rodriguez Villegas	University of Texas, Austin
Peter Stevenhagen	Universiteit Leiden
Michael Stoll	Universität Bayreuth
Bianca Viray	Brown University

Financial sponsors. We are thankful for support from Microsoft Research, the National Science Foundation, the National Security Agency, the Number Theory Foundation, and the University of California, San Diego.

Previous and future ANTS meetings.

	Year	Location	Proceedings
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)	OBS 1
XI	2014	Hotel Hyundai (GyeongJu, Korea)	

Proceedings of the previous ANTS meetings have been published in the Springer Lecture Notes in Computer Science series (LNCS). This volume is the first volume of the Mathematical Sciences Publishers' Open Book Series (OBS).

ANTS XI is planned to be held August 7–11, 2014 in GyeongJu, Korea, as a satellite conference to the International Congress of Mathematicians. The chairs of the program committee are Jung Hee Cheon (Seoul National University) and Hyang-Sook Lee (Ewha Womans University).

EVERETT W. HOWE: however@alumni.caltech.edu
Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1969, United States

KIRAN S. KEDLAYA: kedlaya@ucsd.edu
Department of Mathematics, University of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093-0112, United States

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

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

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

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 1

Tenth 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 tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS