Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Preface

Our subject arises out of two roots of mathematical thought: fascination with properties of whole numbers and the urge to compute. Number theory and computer science flowered vividly during the last quarter of the twentieth century, and the synergy at their intersection was striking. Algorithmic number theory emerged as an exciting field in its own right, containing deep insights, and having surprising applications.

In the fall of 2000 the Mathematical Sciences Research Institute Berkeley hosted a one-semester program on algorithmic number theory. Its opening workshop, cosponsored by the Clay Mathematics Institute, featured many foundational and survey talks. During the meeting, it was noted that there was a dearth of sources for newcomers to the field. After the conference, some of the speakers agreed to write articles based on their talks, and we were drafted to edit the volume.

A few authors turned in drafts promptly, some retaining the tutorial focus and tone of the original talks, while others were full-blown tutorials or surveys. Many authors (including the editors) dallied. Additional articles were solicited, to provide more coherence and to incorporate newer results that couldn't be ignored (most notably, the polynomial-time primality algorithm due to Manindra Agrawal, Neeraj Kayal, and Nitin Saxena). This led to complications that might have been expected for a volume with 20 substantial articles, 15 authors, and 650 pages. These have finally run their course, and we are delighted that the volume is ready to see the light of day.

We do apologize to the authors who responded promptly, and can only hope that they will be compensated by the greater breadth and interest of the volume in which their contributions appear.

The articles in the volume can be loosely categorized as follows. The first two articles are introductory, and are more elementary than their successors — they attempt to entice the reader into pursuing the ideas more deeply. The next eight articles provide surveys of central topics, including smooth numbers, factoring, primality testing, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles study specific topics more deeply,

including cryptography, computational algebraic number theory, modular forms, and arithmetic geometry.

Although the articles in this volume are surveys in the broadest sense, the word should not be taken to mean an encyclopedic treatment that captures current conventional wisdom. We prefer the term overviews, and the articles have a distinctive and in some cases even nonstandard perspective.

It remains our pleasant duty to thank a number of institutions and people. Most obviously, the authors have produced many fascinating pages, sure to inspire others to pursue the subject. We thank the Clay Institute and MSRI for their generous funding for the workshop that provided the initial spark for this volume. We thank Cambridge University Press and MSRI for their support and patience during the production of this volume, and we especially thank Silvio Levy for his extensive efforts on this volume. John Voight took notes (by typing nearly real-time TEX into his laptop) at most of the talks at workshop, and these were valuable to some of the authors.

Finally, Hendrik Lenstra has long been a source of pervasive and brilliant inspiration to the entire field of algorithmic number theory, and this volume is no exception: in addition to two distinctive articles, he has provided much-appreciated advice over the years to the editors and to virtually all of the other authors.

Joe Buhler
Peter Stevenhagen
San Diego, May 2008