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

Preface

Our subject arises out of two of the roots of mathematical thought: fascination with the properties of whole numbers, and the urge to compute. Both number theory and the study of algorithms flowered vividly during the twentieth century, and by the end of the century algorithmic number theory had emerged as an exciting and important field.

In the fall of 2000 the Mathematical Sciences Research Institute (MSRI) in 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 was a dearth of sources for aspiring graduate students in this area, and the idea of collecting written versions of some of the talks arose. At the conference (or shortly thereafter) many of the speakers agreed to write articles, 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 surveys. Many authors (included the editors) dallied. Additional articles were solicited, both for the sake of coherence or fuller treatment, and because newer results could not be ignored (most notably, the polynomial-time primality algorithm due to Manindra Agrawal, Neeraj Kayal, and Nitin Saxena). This led to the usual complications (and then some) that might be expecting when producing a volume with 20 substantial articles, 15 authors, and 600 pages. These have finally run their course; the twists and turns of this process would have been hard to predict, but in any event we are delighted that the volume is finally ready to see the light of day.

We of course have to 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; they are more elementary than their successors and attempt to entice the reader into pursuing the ideas more deeply. The next eight articles provide surveys of key topics, including smooth numbers,

factoring, primality testing, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles pursue specific areas more deeply, including cryptography, computational algebraic number theory, modular forms, and arithmetic geometry.

We remark that the use of "survey" in the title of this volume should not be taken to suggest surveys in the sense of an encyclopedia, where one expects a broad and encompassing viewpoint, and an attempt to capture current thinking. Instead, the articles here are examinations of specific topics, often with a sense of providing an overview, but often from a very distinctive and even non-standard 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 a workshop which 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 energetic work on this volume.

John Voight took notes (by typing nearly real-time TEX into his laptop) at most of the talks at the initial workshop, and these were invaluable to the authors whose talks sprang from the workshop.

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