Lecture Notes in Computer Science 3000

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Martin Dietzfelbinger

Primality Testing in Polynomial Time

From Randomized Algorithms to "PRIMES is in P"

Springer

Author

Martin Dietzfelbinger
Technische Universität Ilmenau
Fakultät für Informatik und Automatisierung
98684 Ilmenau, Germany
E-mail: martin.dietzfelbinger@tu-ilmenau.de

Library of Congress Control Number: 2004107785

CR Subject Classification (1998): F.2.1, F.2, F.1.3, E.3, G.3

ISSN 0302-9743
ISBN 3-540-40344-2 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10936009 06/3142 5 4 3 2 1 0

To Angelika, Lisa, Matthias, and Johanna

Preface

On August 6, 2002, a paper with the title "PRIMES is in P", by M. Agrawal, N. Kayal, and N. Saxena, appeared on the website of the Indian Institute of Technology at Kanpur, India. In this paper it was shown that the "*primality problem*" has a "*deterministic algorithm*" that runs in "*polynomial time*".

Finding out whether a given number n is a prime or not is a problem that was formulated in ancient times, and has caught the interest of mathematicians again and again for centuries. Only in the 20th century, with the advent of cryptographic systems that actually used large prime numbers, did it turn out to be of practical importance to be able to distinguish prime numbers and composite numbers of significant size. Readily, algorithms were provided that solved the problem very efficiently and satisfactorily for all practical purposes, and provably enjoyed a time bound polynomial in the number of digits needed to write down the input number n. The only drawback of these algorithms is that they use "*randomization*" — that means the computer that carries out the algorithm performs random experiments, and there is a slight chance that the outcome might be wrong, or that the running time might not be polynomial. To find an algorithm that gets by without randomness, solves the problem error-free, and has polynomial running time had been an eminent open problem in complexity theory for decades when the paper by Agrawal, Kayal, and Saxena hit the web. The news of this amazing result spread very fast around the world among scientists interested in the theory of computation, cryptology, and number theory; within days it even reached The New York Times, which is quite unusual for a topic in theoretical computer science.

Practically, not much has changed. In cryptographic applications, the fast randomized algorithms for primality testing continue to be used, since they are superior in running time and the error can be kept so small that it is irrelevant for practical applications. The new algorithm does not seem to imply that we can factor numbers fast, and no cryptographic system has been broken. Still, the new algorithm is of great importance, both because of its long history and because of the methods used in the solution.

As is quite common in the field of number-theoretic algorithms, the formulation of the deterministic primality test is very compact and uses only very simple basic procedures. The analysis is a little more complex, but astoundingly it gets by with a small selection of the methods and facts taught in introductory algebra and number theory courses. On the one hand, this raises the philosophical question whether other important open problems in theoretical computer science may have solutions that require only basic methods. On the other hand, it opens the rare opportunity for readers without a specialized mathematical training to fully understand the proof of a new and important result.

It is the main purpose of this text to guide its reader all the way from the definitions of the basic concepts from number theory and algebra to a full understanding of the new algorithm and its correctness proof and time analysis, providing details for all the intermediate steps. Of course, the reader still has to go the whole way, which may be steep in some places; some basic mathematical training is required and certainly a good measure of perseverance.

To make a contrast, and to provide an introduction to some practically relevant primality tests for the complete novice to the field, also two of the classical primality testing algorithms are described and analyzed, viz., the "Miller-Rabin Test" and the "Solovay-Strassen Test". Also for these algorithms and their analysis, all necessary background is provided.

I hope that this text makes the area of primality testing and in particular the wonderful new result of Agrawal, Kayal, and Saxena a little easier to access for interested students of computer science, cryptology, or mathematics.

I wish to thank the students of two courses in complexity theory at the Technical University of Ilmenau, who struggled through preliminary versions of parts of the material presented here. Thanks are due to Juraj Hromkovič for proposing that this book be written as well as his permanent encouragement on the way. Thomas Hofmeister and Juraj Hromkovič read parts of the manuscript and gave many helpful hints for improvements. (Of course, the responsibility for any errors remains with the author.) The papers by D.G. Bernstein, generously made accessible on the web, helped me a lot in shaping an understanding of the subject matter. I wish to thank Alfred Hofmann of Springer-Verlag for his patience and the inexhaustible enthusiasm with which he accompanied this project. And, finally, credit is due to M. Agrawal, N. Kayal, and N. Saxena, who found this beautiful result.

Ilmenau, March 2004 *Martin Dietzfelbinger*

Contents