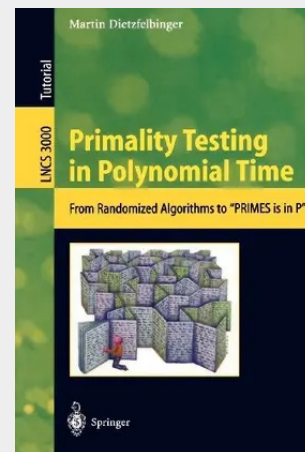


Primality Testing in Polynomial Time

From Randomized Algorithms to "PRIMES Is in P"

A self-contained treatment of theoretically and practically important efficient algorithms for the primality problem, covering the randomized algorithms by Solovay-Strassen and Miller-Rabin from the late 1970s as well as the recent deterministic algorithm of Agrawal, Kayal, and Saxena. The volume is written for students of computer science, in particular those with a special interest in cryptology, and students of mathematics. The text may be used as a supplement for courses or for self-study.

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.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540403449

Medium: Buch

ISBN: 978-3-540-40344-9

Verlag: Springer

Erscheinungstermin: 29.06.2004

Sprache(n): Englisch

Auflage: 1. Auflage 2004

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 260 g

Seiten: 150

Format (B x H): 155 x 235 mm

