《Primality Testing in》

图书基本信息

书名：《Primality Testing in Polynomial Time多项式时间中的初级测试》

13位ISBN编号：9783540403449

10位ISBN编号：3540403442

出版社：Springer

作者：Dietzfelbinger,Martin

《Primality Testing in》

内容概要

This book is devoted to algorithms for the venerable primality problem: Given a natural number n, decide whether it is prime or composite.

The problem is basic in number theory, efficient algorithms that solve it, i.e., algorithms that run in a number of computational steps which is polynomial in the number of digits needed to write n, are important for theoretical computer science and for applications in algorithmics and cryptology.

This book gives a self-contained account 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 textbook is written for students of computer science, in particular for those with a special interest in cryptology, and students of mathematics, and it may be used as a supplement for courses or for self-study.

《Primality Testing in》

书籍目录

版权说明