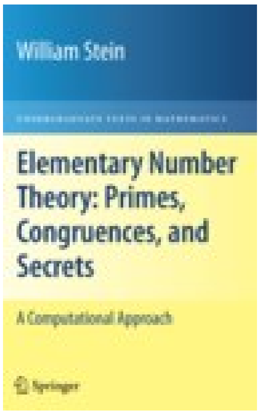
Elementary Number Theory: Primes, Congruences, and Secrets



Elementary Number Theory: Primes, Congruences, and Secrets_下载链接1_

著者:Stein, William

出版者:Springer

出版时间:2009

装帧:Hardcover

isbn:9780387855240

About this textbook

The systematic study of number theory was initiated around 300B.C. when Euclid proved that there are infinitely many prime numbers. At the same time, he also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over 1000 years later (around 972A.D.) Arab mathematicians formulated the congruent number problem that asks for a way to decide whether or not a given positive integer n is the area of a right triangle, all three of whose sides are rational numbers. Then another 1000 years later (in 1976), Diffie and Hellman introduced the first ever public-key cryptosystem, which enabled two people to communicate secretly over a public communications channel with no predetermined secret; this invention and the ones that followed it revolutionized the world of digital communication. In the 1980s and 1990s, elliptic curves revolutionized number theory, providing striking new insights into the congruent number problem, primality testing, public-key cryptography, attacks on public-key systems, and playing a central role in Andrew Wiles' resolution of Fermat's Last Theorem.

Today, pure and applied number theory is an exciting mix of simultaneously broad and deep theory, which is constantly informed and motivated by algorithms and explicit computation. Active research is underway that promises to resolve the congruent number problem, deepen our understanding into the structure of prime numbers, and both challenge and improve our ability to communicate securely. The goal of this book is to bring the reader closer to this world. Each chapter contains exercises, and throughout the text there are examples of calculations done using the powerful free open source mathematical software system Sage. The reader should know how to read and write mathematical proofs and must know the basics of groups, rings, and fields. Thus, the prerequisites for this book are more than the prerequisites for most elementary number theory books, while still being aimed at undergraduates.

William Stein is an Associate Professor of Mathematics at the University of Washington. He is also the author of Modular Forms, A Computational Approach (AMS 2007), and the lead developer of the open source software, Sage.

Written for:

Undergraduate mathematics students, graduate mathematics students, mathematicians, mathematics teachers

作者介绍:

目录:

Elementary Number Theory: Primes, Congruences, and Secrets_下载链接1_

标签

数论

数学

评论

比较注重易读性，有一些用 sage 进行实际计算的例子。

Elementary Number Theory: Primes, Congruences, and Secrets_下载链接1_

书评

Elementary Number Theory: Primes, Congruences, and Secrets_下载链接1_