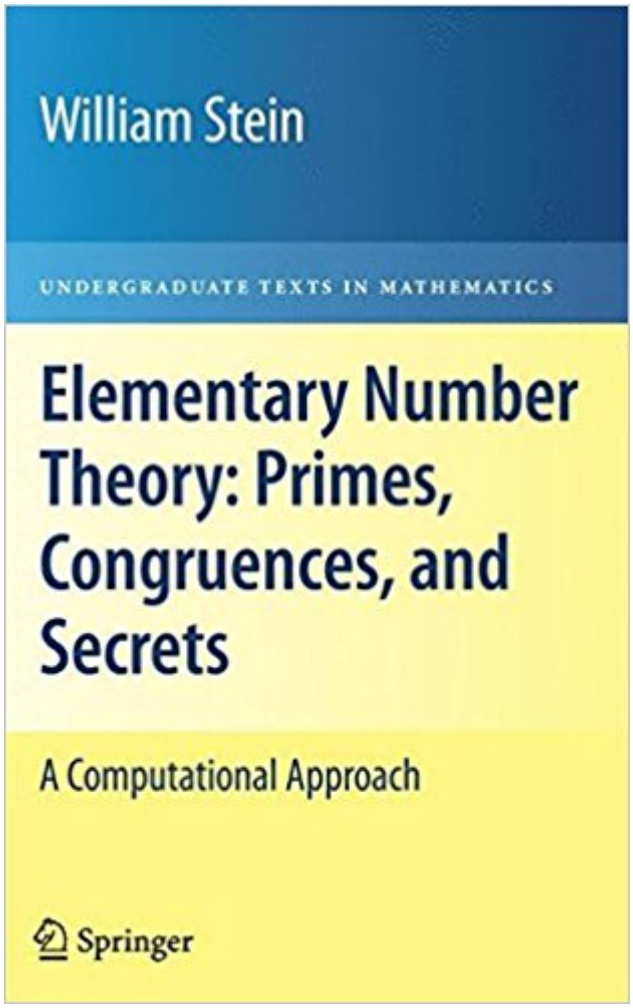
Elementary Number Theory: Primes, Congruences, And Secrets: A Computational Approach (Undergraduate Texts In Mathematics)




PDF
Adobe
DOWNLOAD EBOOK

Synopsis

This is a book about prime numbers, congruences, secret messages, and elliptic curves that you can read cover to cover. It grew out of undergr- uate courses that the author taught at Harvard, UC San Diego, and the University of Washington. The systematic study of number theory was initiated around 300B. C. when Euclid proved that there are in?nitely many prime numbers, and also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over a thousand 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 thousand years later (in 1976), Di?e and Hellman introduced the ?rst ever public-key cryptosystem, which enabled two people to communicate secretely 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, publ- key cryptography, attacks on public-key systems, and playing a central role in Andrew WilesÃ¢â ¬â„¢ resolution of FermatÃ¢â ¬â„¢s Last Theorem.

Book Information

Series: Undergraduate Texts in Mathematics

Hardcover: 168 pages

Publisher: Springer; 2009 edition (December 3, 2008)

Language: English

ISBN-10: 0387855246

ISBN-13: 978-0387855240

Product Dimensions: 6.1 x 0.8 x 9.2 inches

Shipping Weight: 12 ounces (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 1 customer review

Best Sellers Rank: #891,531 in Books (See Top 100 in Books) #152 inÃ Â Books > Science & Math > Mathematics > Geometry & Topology > Algebraic Geometry #298 inÃ Â Books > Science & Math > Mathematics > Pure Mathematics > Number Theory #528 inÃ Â Books > Textbooks > Science & Mathematics > Mathematics > Geometry

Customer Reviews

From the reviews: "This one treats topics that have become standard in recent years Ã¢â ¬Â¦ and it

has exercises with selected solutions. Ã¢â ¬Â¦ it gives the students a tool to do calculations that illustrate even the most abstract concepts, and, simultaneously, introduces them to an open source software that can later be applied profitably for studying research problems. Ã¢â ¬Â¦ introducing the reader to a powerful software system." (Franz Lemmermeyer, Zentralblatt MATH, Vol. 1155, 2009) "The clichÃƒÂ© that number theory, ever the purest mathematics, now yields very practical applications barely tells the story. Teach undergraduate number theory today, and students demand to hear about public-key cryptography and related technologies. Ã¢â ¬Â¦ Stein (Univ. of Washington) serves undergraduates well by Ã¢â ¬Â¦ opening the way by intimating their power. Ã¢â ¬Â¦ he frames the sophisticated Birch and Swinnerton-Dyer conjecture as the new canonical challenge for the future. Summing Up: Recommended. All undergraduates students, professionals, and general readers." (D. V. Feldman, Choice, Vol. 47 (2), October, 2009) "This book is an introduction to elementary number theory with a computational flavor. Ã¢â ¬Â¦ Many numerical examples are given throughout the book using the Sage mathematical software. The text is aimed at an undergraduate student with a basic knowledge of groups, rings and fields. Each chapter concludes with several exercises." (Samuel S. Wagstaff Jr., Mathematical Reviews, Issue 2009 i)

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. Ã Â 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. Ã Â 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.

It is for my number theory class, i just wish there was an answer key somewhere.