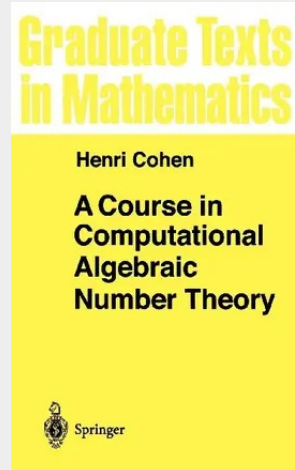


A Course in Computational Algebraic Number Theory

With the advent of powerful computing tools and numerous advances in mathematics, computer science and cryptography, algorithmic number theory has become an important subject in its own right. Both external and internal pressures gave a powerful impetus to the development of more powerful algorithms. These in turn led to a large number of spectacular breakthroughs. To mention but a few, the LLL algorithm which has a wide range of applications, including real world applications to integer programming, primality testing and factoring algorithms, sub-exponential class group and regulator algorithms, etc. Several books exist which treat parts of this subject. (It is essentially impossible for an author to keep up with the rapid pace of progress in all areas of this subject.) Each book emphasizes a different area, corresponding to the author's tastes and interests. The most famous, but unfortunately the oldest, is Knuth's Art of Computer Programming, especially Chapter 4. The present book has two goals. First, to give a reasonably comprehensive introductory course in computational number theory. In particular, although we study some subjects in great detail, others are only mentioned, but with suitable pointers to the literature. Hence, we hope that this book can serve as a first course on the subject. A natural sequel would be to study more specialized subjects in the existing literature.

This book describes 148 algorithms which are essential for serious number-theoretic computations, in particular for computations related to lattices, algebraic number theory, elliptic curves, primality testing and factoring. For each algorithm, a complete theoretical introduction is given so that prerequisites are reduced to a minimum. Many implementation hints and exercises are also provided.



90,94 €
84,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540556404
Medium: Buch
ISBN: 978-3-540-55640-4
Verlag: Springer
Erscheinungstermin: 05.08.1993
Sprache(n): Englisch
Auflage: 1993
Serie: Graduate Texts in Mathematics
Produktform: Gebunden
Gewicht: 1027 g
Seiten: 536
Format (B x H): 160 x 241 mm

