1. Record Nr. UNINA9910812157303321

Autore	Cohen Henri
Titolo	A Course in Computational Algebraic Number Theory / / by Henri Cohen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1993
ISBN	3-662-02945-6
Edizione	[1st ed. 1993.]
Descrizione fisica	1 online resource (XXI, 536 p.)
Collana	Graduate Texts in Mathematics, , 2197-5612 ; ; 138
Disciplina	512.7
Soggetti	Number theory Algebra Computer science Algorithms Computer science - Mathematics Number Theory Theory of Computation Symbolic and Algebraic Manipulation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Fundamental Number-Theoretic Algorithms -- 2. Algorithms for Linear Algebra and Lattices -- 3. Algorithms on Polynomials -- 4. Algorithms for Algebraic Number Theory I -- 5. Algorithms for Quadratic Fields -- 6. Algorithms for Algebraic Number Theory II -- 7. Introduction to Elliptic Curves -- 8. Factoring in the Dark Ages -- 9. Modern Primality Tests -- 10. Modern Factoring Methods -- Appendix A. Packages for Number Theory -- Appendix B. Some Useful Tables -- B.1. Table of Class Numbers of Complex Quadratic Fields -- B.2. Table of Class Numbers and Units of Real Quadratic Fields -- B.3. Table of Class Numbers and Units of Complex Cubic Fields -- B.4. Table of Class Numbers and Units of Totally Real Cubic Fields -- B.5. Table of Elliptic Curves.
Sommario/riassunto	With the advent of powerful computing tools and numerous advances in math- ematics, 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 al- gorithms. 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 appli- cations, 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.