1.	Record Nr.	UNISA996465629503316
	Titolo	Algorithmic Number Theory [[electronic resource]] : Second International Symposium, ANTS-II, Talence, France, May 18 - 23, 1996, Proceedings / / edited by Henri Cohen
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1996
	ISBN	3-540-70632-1
	Edizione	[1st ed. 1996.]
	Descrizione fisica	1 online resource (X, 414 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1122
	Disciplina	512/.7
	Soggetti	Computers Algebra Algorithms Data encryption (Computer science) Computer science—Mathematics Number theory Theory of Computation Algorithm Analysis and Problem Complexity Cryptology Discrete Mathematics in Computer Science Number Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Counting rational points on curves and abelian varieties over finite fields -- Computing cubic fields in quasi-linear time -- Fast ideal arithmetic via lazy localization -- A comparative study of algorithms for computing continued fractions of algebraic numbers -- Computing ray class groups, conductors and discriminants -- Computing l-isogenies using the p-torsion -- On computing Hilbert class fields of prime degree -- On the reduction of composed relations from the number field sieve -- Checking the p-adic stark conjecture when p is archimedean -- A multiple polynomial general number field sieve -- Construction of high-rank elliptic curves over Q and Q(t) with non-trivial 2-torsion -- The height on an abelian variety -- On lattices over

number fields -- Minimum discriminants of primitive sextic fields -- A new algorithm and refined bounds for extended gcd computation -- Application of thue equations to computing power integral bases in algebraic number fields -- Computing S-integral points on elliptic curves -- Probabilistic computation of the Smith normal form of a sparse integer matrix -- Ray class field constructions of curves over finite fields with many rational points -- Computing isogenies in F2n -- A computational technique for determining relative class numbers of CM-fields -- Old and new deterministic factoring algorithms -- Efficient algorithms for computing the Jacobi symbol -- The number field database on the World Wide web server http://hasse.mathematik.tu-muenchen.de/ -- An algorithm of subexponential type computing the class group of quadratic orders over principal ideal domains -- Computational aspects of Kummer theory -- On integral basis reduction in global function fields -- Computational aspects of curves of genus at least 2 -- The complexity of approximate optima for greatest common divisor computations -- Compact representation in real quadratic congruence function fields -- Discrete logarithms: The effectiveness of the index calculus method -- How difficult is it to solve a thue equation? -- Elliptic congruence function fields -- Algebraic geometry lattices and codes -- Computing discrete logarithms with the general number field sieve.

Sommario/riassunto

This book constitutes the refereed post-conference proceedings of the Second International Algorithmic Number Theory Symposium, ANTS-II, held in Talence, France in May 1996. The 35 revised full papers included in the book were selected from a variety of submissions. They cover a broad spectrum of topics and report state-of-the-art research results in computational number theory and complexity theory. Among the issues addressed are number fields computation, Abelian varieties, factoring algorithms, finite fields, elliptic curves, algorithm complexity, lattice theory, and coding.