1.	Record Nr.	UNISA996466151203316
	Titolo	Algorithmic Number Theory [[electronic resource]] : First International Symposium, ANTS-I, Ithaca, NY, USA, May 6 - 9, 1994. Proceedings / / edited by Leonard M. Adleman, Ming-Deh Huang
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1994
	ISBN	3-540-49044-2
	Edizione	[1st ed. 1994.]
	Descrizione fisica	1 online resource (X, 320 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 877
	Disciplina	512/.7
	Soggetti	Data structures (Computer science) Number theory Discrete mathematics Computer science—Mathematics Algorithms Combinatorics Data Structures Number Theory Discrete Mathematics Symbolic and Algebraic Manipulation Algorithm Analysis and Problem Complexity
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	On the difficulty of finding reliable witnesses -- Density computations for real quadratic 2-class groups -- Lattice sieving and trial division -- A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields -- Computing rates of growth of division fields on CM Abelian varieties -- Algorithms for CM-Fields -- Schoof's algorithm and isogeny cycles -- Integer points on rational elliptic curves -- Counting the number of points on elliptic curves over finite fields of characteristic greater than three -- Straight-line complexity and integer factorization -- Decomposition of algebraic functions -- A new modular interpolation algorithm for factoring multivariate polynomials

-- The function field sieve -- Heegner point computations -- Computing the degree of a modular parametrization -- Galois representations from the cohomology of SL(3,?) -- An analysis of the Gaussian algorithm for lattice reduction -- A fast variant of the Gaussian reduction algorithm -- Reducing lattice bases by means of approximations -- Analysis of a left-shift binary GCD algorithm -- The complexity of greatest common divisor computations -- Explicit formulas for units in certain quadratic number fields -- Factorization of polynomials over finite fields in subexponential time under GRH -- On orders of optimal normal basis generators -- Computing in the jacobian of a plane algebraic curve -- Under the assumption of the Generalized Riemann Hypothesis verifying the class number belongs to NP ? co-NP -- Calculating the class number of certain Hilbert class fields -- Efficient checking of computations in number theory -- Constructing elliptic curves with given group order over large finite fields -- Computing ?(x), M(x) and ?(x) -- On some applications of finitely generated semi-groups -- Improved incremental prime number sieves -- Polynomial time algorithms for discrete logarithms and factoring on a quantum computer -- On dispersion and Markov constants -- Open problems in number theoretic complexity, II.

Sommario/riassunto

This volume presents the refereed proceedings of the First Algorithmic Number Theory Symposium, ANTS-I, held at Cornell University, Ithaca, NY in May 1994. The 35 papers accepted for inclusion in this book address many current issues of algorithmic, computational and complexity-theoretic aspects of number theory and thus report the state-of-the-art in this exciting area of research; the book also contributes essentially to foundational research in cryptology and coding. Of particular value is a collection entitled "Open Problems in Number Theoretic Complexity, II" contributed by Len Adleman and Kevin McCurley. This survey presents on 32 pages 36 central open problems and relates them to the literature by means of some 160 references.