1.

Record Nr.	UNINA9910143504203321
Titolo	Algorithmic Number Theory [[electronic resource]] : Third International Symposium, ANTS-III, Portland, Orgeon, USA, June 21-25, 1998, Proceedings / / edited by Joe P. Buhler
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1998
ISBN	3-540-69113-8
Edizione	[1st ed. 1998.]
Descrizione fisica	1 online resource (X, 646 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1423
Disciplina	512/.7
Soggetti	Computers Number theory Computer science—Mathematics Algorithms Data encryption (Computer science) Theory of Computation Number Theory Symbolic and Algebraic Manipulation Algorithm Analysis and Problem Complexity Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Shimura curve computations -- The Decision Diffie-Hellman problem -- Parallel implementation of Schönhage's integer GCD algorithm -- The complete analysis of the binary Euclidean algorithm -- Cyclotomy primality proving — Recent developments -- Primality proving using elliptic curves: An update -- Bounding smooth integers (extended abstract) -- Factorization of the numbers of the form m 3 + c 2 m 2 + c 1 m + c 0 -- Modelling the yield of number field sieve polynomials -- A Montgomery-like square root for the Number Field Sieve -- Robert Bennion's “hopping sieve” -- Trading time for space in prime number sieves -- Do sums of 4 biquadrates have a positive density? -- New experimental results concerning the Goldbach conjecture -- Dense admissible sets -- An analytic approach to smooth polynomials over

finite fields -- Generating a product of three primes with an unknown factorization -- On the performance of signature schemes based on elliptic curves -- NTRU: A ring-based public key cryptosystem -- Finding length-3 positive Cunningham chains and their cryptographic significance -- Reducing ideal arithmetic to linear algebra problems -- Evaluation of linear relations between vectors of a lattice in euclidean space -- An efficient parallel block-reduction algorithm -- Fast multiprecision evaluation of series of rational numbers -- A problem concerning a character sum -- Formal power series and their continued fraction expansion -- Imprimitive octic fields with small discriminants -- A table of totally complex number fields of small discriminants -- Generating arithmetically equivalent number fields with elliptic curves -- Computing the lead term of an abelian L-function -- Timing analysis of targeted hunter searches -- On successive minima of rings of algebraic integers -- Computation of relative quadratic class groups -- Generating class fields using Shimura reciprocity -- Irregularity of prime numbers over real quadratic fields -- Experimental results on class groups of real quadratic fields -- Computation of relative class numbers of imaginary cyclic fields of 2-power degrees -- Formal groups, elliptic curves, and some theorems of Couveignes -- A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve -- An algorithm for approximate counting of points on algebraic sets over finite fields -- S-integral points on elliptic curves and Fermat's triple equations -- Speeding up Pollard's rho method for computing discrete logarithms -- A general method of constructing global function fields with many rational places -- Lattice basis reduction in function fields -- Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves -- Unit computation in purely cubic function fields of unit rank 1 -- An improved method of computing the regulator of a real quadratic function field -- The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Symposium on Algorithmic Number Theory, ANTS-III, held in Portland, Oregon, USA, in June 1998. The volume presents 46 revised full papers together with two invited surveys. The papers are organized in chapters on gcd algorithms, primality, factoring, sieving, analytic number theory, cryptography, linear algebra and lattices, series and sums, algebraic number fields, class groups and fields, curves, and function fields.