1. Record Nr. UNINA9910484102103321

Titolo	Algorithmic Number Theory : 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings / / edited by Florian Hess, Sebastian Pauli, Michael Pohst
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-36076-X
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 599 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 4076
Altri autori (Persone)	HessFlorian PauliSebastian PohstM
Disciplina	512.7
Soggetti	Number theory Algorithms Computer science - Mathematics Discrete mathematics Cryptography Data encryption (Computer science) Number Theory Discrete Mathematics in Computer Science Cryptology 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	Invited Talks -- Computing Pro-P Galois Groups -- The Elliptic Curve Database for Conductors to 130000 -- On the Computation of the Coefficients of a Modular Form -- Cohen–Lenstra Heuristics of Quadratic Number Fields -- Algebraic Number Theory -- An Algorithm for Computing p-Class Groups of Abelian Number Fields -- Computation of Locally Free Class Groups -- Numerical Results on Class Groups of Imaginary Quadratic Fields -- Cyclic Polynomials Arising from Kummer Theory of Norm Algebraic Tori -- The Totally Real Primitive Number Fields of Discriminant at Most 109 -- A Modular

Method for Computing the Splitting Field of a Polynomial -- Analytic and Elementary Number Theory -- On the Density of Sums of Three Cubes -- The Mertens Conjecture Revisited -- Fast Bounds on the Distribution of Smooth Numbers -- Use of Extended Euclidean Algorithm in Solving a System of Linear Diophantine Equations with Bounded Variables -- The Pseudosquares Prime Sieve -- Doubly-Focused Enumeration of Pseudosquares and Pseudocubes -- Lattices -- Practical Lattice Basis Sampling Reduction -- LLL on the Average -- On the Randomness of Bits Generated by Sufficiently Smooth Functions -- Curves and Varieties over Fields of Characteristic Zero -- Computing a Lower Bound for the Canonical Height on Elliptic Curves over ? -- Points of Low Height on Elliptic Curves and Surfaces I: Elliptic Surfaces over with Small d -- Shimura Curves for Level-3 Subgroups of the (2,3,7) Triangle Group, and Some Other Examples -- The Asymptotics of Points of Bounded Height on Diagonal Cubic and Quartic Threefolds -- Testing Equivalence of Ternary Cubics -- Classification of Genus 3 Curves in Special Strata of the Moduli Space -- Heegner Point Computations Via Numerical p-Adic Integration -- Symmetric Powers of Elliptic Curve L-Functions.-Determined Sequences, Continued Fractions, and Hyperelliptic Curves -- Computing CM Points on Shimura Curves Arising from Cocompact Arithmetic Triangle Groups -- Arithmetic of Generalized Jacobians -- Hidden Pairings and Trapdoor DDH Groups -- Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10 -- Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves -- High Security Pairing-Based Cryptography Revisited -- Efficiently Computable Endomorphisms for Hyperelliptic Curves -- Construction of Rational Points on Elliptic Curves over Finite Fields -- 20 Years of ECM -- Discrete Logarithms -- An Index Calculus Algorithm for Plane Curves of Small Degree -- Signature Calculus and Discrete Logarithm Problems -- Spectral Analysis of Pollard Rho Collisions -- Hard Instances of the Constrained Discrete Logarithm Problem.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Algorithmic Number Theory Symposium, ANTS 2006, held in Berlin, July 2006. The book presents 37 revised full papers together with 4 invited papers selected for inclusion. The papers are organized in topical sections on algebraic number theory, analytic and elementary number theory, lattices, curves and varieties over fields of characteristic zero, curves over finite fields and applications, and discrete logarithms.