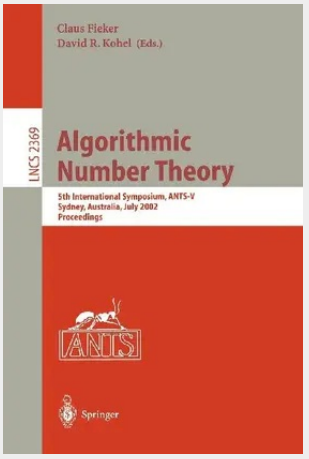
Fieker / Kohel

Algorithmic Number Theory

5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002. Proceedings



. 9 JohnCoates TheWeilandTatePairingsasBuildingBlocks forPublicKeyCryptosystems. 20 AntoineJoux UsingEllipticCurvesofRankOnetowardstheUndecidability ofHilbert'sTenthProblemoverRingsofAlgebraicIntegers. 33 BjornPoonen Onp-adicPointCountingAlgorithmsforEllipticCurves overFiniteFields. 43 TakakazuSatoh NumberTheory OnArithmeticallyEquivalentNumberFieldsofSmallDegree. 67 WiebBosma,BartdeSmit ASurveyofDiscriminantCounting. 80 HenriCohen,FranciscoDiazyDiaz,MichelOlivier AHigher-RankMersenneProblem. 95 GrahamEverest,PeterRogers,ThomasWard AnApplicationofSiegelModularFunctions toKronecker'sLimitFormula. 108 TakashiFukuda,KeiichiKomatsu ComputationalAspectsofNUCOMP. 120 MichaelJ. Jacobson,Jr. ,AlfredJ. vanderPoorten E?cientComputationofClassNumbersofRealAbelianNumberFields. 134 St´ephaneR. Louboutin AnAcceleratedBuchmannAlgorithmforRegulatorComputation inRealQuadraticFields. 148 UlrichVollmer VIII TableofContents ArithmeticGeometry SomeGenus3CurveswithManyPoints. 163 RolandAuer,JaapTop 7 8 Trinomialsax +bx+candax +bx+c withGaloisGroupsofOrder168and8·168. 172 NilsBruin,NoamD. Elkies ComputationsonModularJacobianSurfaces. 189 EnriqueGonz´alez-Jim´enez,JosepGonz ´alez,JordiGu`ardia IntegralPointsonPuncturedAbelianSurfaces. 198 AndrewKresch,YuriTschinkel Genus2Curveswith(3,3)-SplitJacobian andLargeAutomorphismGroup. 205 TonyShaska TransportableModularSymbolsandtheIntersectionPairing. 219 HelenaA. Verrill EllipticCurvesandCM ActionofModularCorrespondencesaroundCMPoints. 234 Jean-MarcCouveignes,ThierryHenocq 2 3 CurvesDy =x ?xofOddAnalyticRank. 244 NoamD. Elkies ComparingInvariantsforClassFieldsofImaginaryQuadraticFields. 252 AndreasEnge,Fran¸coisMorain ADatabaseofEllipticCurves–FirstReport. 267 WilliamA. Stein,MarkWatkins PointCounting IsogenyVolcanoesandtheSEAAlgorithm. 276 MireilleFouquet,Fran¸coisMorain FastEllipticCurvePointCountingUsingGaussianNormalBasis. 292 HaeYoungKim,JungYoulPark,JungHeeCheon,JeHongPark, JaeHeonKim,SangGeunHahn AnExtensionofKedlaya'sAlgorithmtoArtin-SchreierCurves inCharacteristic2. 308 JanDenef,FrederikVercauteren TableofContents IX Cryptography ImplementingtheTatePairing. 324 StevenD. Galbraith,KeithHarrison,DavidSoldera SmoothOrdersandCryptographicApplications. 338 CarlPomerance,IgorE. Shparlinski ChineseRemainderingforAlgebraicNumbersinaHiddenField. 349 IgorE. Shparlinski,RonSteinfeld FunctionFields AnAlgorithmforComputingWeierstrassPoints. 357 FlorianHess NewOptimalTameTowersofFunctionFieldsoverSmallFiniteFields. 372 Wen-ChingW. Li,HirenMaharaj,HenningStichtenoth, NoamD. Elkies PeriodicContinuedFractionsinEllipticFunctionFields. 390 AlfredJ. vanderPoorten,XuanChuongTran DiscreteLogarithmsandFactoring FixedPointsandTwo-CyclesoftheDiscreteLogarithm. 405 JoshuaHolden RandomCayleyDigraphsandtheDiscreteLogarithm. 416 JeremyHorwitz,RamarathnamVenkatesan TheFunctionFieldSieveIsQuiteSpecial. 431 AntoineJoux,ReynaldLercier MPQSwithThreeLargePrimes. 446 PaulLeyland,ArjenLenstra,BruceDodson,AlecMu?ett,SamWagsta? AnImprovedBabyStepGiantStepAlgorithm forPointCountingofHyperellipticCurvesoverFiniteFields. 461 KazutoMatsuo,JinhuiChao,ShigeoTsujii 2 FactoringN=pq withtheEllipticCurveMethod. 475 PeterEbinger,EdlynTeske Gr¨obnerBases ANewSchemeforComputingwithAlgebraicallyClosedFields. 491 AllanSteel X TableofContents Complexity AdditiveComplexityandRootsofPolynomials overNumberFieldsandp-adicFields. 506 J. MauriceRojas AuthorIndex. 517 Gauss Composition and Generalizations ManjulBhargava Clay Mathematics Institute and Princeton University Abstract. We discuss several higher analogues of Gauss

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540438632
Medium: Buch
ISBN: 978-3-540-43863-2
Verlag: Springer
Erscheinungstermin: 26.06.2002
Sprache(n): Englisch
Auflage: 1. Auflage 2002
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1630 g
Seiten: 522
Format (B x H): 155 x 235 mm