

beta version of Victor Shoups book, "A Computational Introduction to Number Theory and Algebra"

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/1564.html>

From: Mads Rasmussen (*mads_at_SPAMFILTER.opencs.com.br*)

Date: 08/20/03

Date: Wed, 20 Aug 2003 09:06:10 -0300

I think this was announced at crypto 2003 but anyway...

Victor Shoup is writing a new book, he has made a beta version available for download at his site: www.shoup.net

here's the contents as you can see, very interesting:

- 1 Basic Properties of the Integers 1
 - 1.1 Divisibility and Primality
 - 1.2 Ideals and Greatest Common Divisors
 - 1.3 More on Unique Factorization and Greatest Common Divisors
- 2 Congruences 7
 - 2.1 Definitions and Basic Properties
 - 2.2 Solving Linear Congruences
 - 2.3 Residue Classes
 - 2.4 Euler's phi-Function
 - 2.5 Other Arithmetic Functions
- 3 Computing with Large Integers
 - 3.1 Asymptotic Notation
 - 3.2 Machine Models and Complexity Theory
 - 3.3 Basic Integer Arithmetic
 - 3.4 Computing in \mathbb{Z}_n
 - 3.5 Notes
- 4 Euclid's Algorithm
 - 4.1 The Basic Euclidean Algorithm
 - 4.2 The Extended Euclidean Algorithm
 - 4.3 Computing Modular Inverses and Chinese Remaindering
 - 4.4 Speeding up Algorithms via Modular Computation
 - 4.5 Rational Reconstruction and Applications
 - 4.6 Notes
- 5 The Distribution of Primes
 - 5.1 Chebyshev's Theorem on the Density of Primes
 - 5.2 Bertrand's Postulate
 - 5.3 The Sum $\sum_{p \leq x} 1/p$

- 5.4 The Sieve of Eratosthenes
- 5.5 The Prime Number Theorem . . . and Beyond
- 5.6 Notes
- 6 Discrete Probability Distributions
 - 6.1 Finite Probability Distributions: Basic Definitions
 - 6.2 Conditional Probability and Independence
 - 6.3 Random Variables
 - 6.4 Expectation and Variance
 - 6.5 Some Useful Bounds
 - 6.6 The Birthday Paradox
 - 6.7 Statistical Distance
 - 6.8 Measures of Randomness and the Leftover Hash Lemma
 - 6.9 Discrete Probability Distributions
 - 6.10 Notes
- 7 Probabilistic Algorithms
 - 7.1 Basic Definitions
 - 7.2 Approximation of Functions
 - 7.3 Flipping a Coin until a Head Appears
 - 7.4 Generating a Random Number from a Given Interval
 - 7.5 Generating a Random Prime
 - 7.6 Generating a Random Non-Increasing Sequence
 - 7.7 Generating a Random Factored Number
 - 7.8 Notes
- 8 Abelian Groups
 - 8.1 Definitions, Basic Properties, and Some Examples
 - 8.2 Subgroups
 - 8.3 Cosets and Quotient Groups
 - 8.4 Group Homomorphisms and Isomorphisms
 - 8.5 Cyclic Groups
 - 8.6 The Structure of Finite Abelian Groups
- 9 Rings
 - 9.1 Definitions, Basic Properties, and Examples
 - 9.2 Polynomial rings
 - 9.3 Ideals and Quotient Rings
 - 9.4 Ring Homomorphisms and Isomorphisms
- 10 Probabilistic Primality Testing
 - 10.1 Trial Division
 - 10.2 The Structure of Z^*_n
 - 10.3 The Miller–Rabin Test
 - 10.4 Generating Random Primes using the Miller–Rabin Test
 - 10.5 Perfect Power Testing and Prime Power Factoring
 - 10.6 Factoring and Computing Euler's ϕ -Function are Equivalent
 - 10.7 The RSA Cryptosystem
 - 10.8 Notes
- 11 Computing Generators and Discrete Logarithms in Z^*_p
 - 11.1 Finding a Generator for Z^*_p
 - 11.2 Computing Discrete Logarithms Z^*_p
 - 11.3 The Diffie–Hellman Key Establishment Protocol
 - 11.4 Notes
- 12 Quadratic Residues and Quadratic Reciprocity
 - 12.1 Quadratic Residues

- 12.2 The Legendre Symbol
- 12.3 The Jacobi Symbol
- 12.4 Notes
- 13 Computational Problems Related to Quadratic Residues
 - 13.1 Computing the Jacobi Symbol
 - 13.2 Testing Quadratic Residuosity
 - 13.3 Computing Modular Square Roots
- 14 Vector Spaces and Algebras
 - 14.1 Definitions, Properties, and Some Examples
 - 14.2 Subspaces and Quotient Spaces
 - 14.3 Vector Space Homomorphisms and Isomorphisms
 - 14.4 Linear Independence, Bases, and Dimension
 - 14.5 Algebras
- 15 Matrices over Fields
 - 15.1 Basic Definitions and Properties
 - 15.2 Matrices and Linear Maps
 - 15.3 The Inverse of a Matrix
 - 15.4 Gaussian Elimination
 - 15.5 Applications of Gaussian Elimination
 - 15.6 Notes
- 16 Subexponential-time Algorithms for Discrete Logarithms and Factoring
 - 16.1 Smooth Numbers
 - 16.2 An Algorithm for Discrete Logarithms
 - 16.3 An Algorithm for Factoring Integers
 - 16.4 Practical Improvements
 - 16.5 Notes
- 17 More Rings
 - 17.1 The Field of Fractions of an Integral Domain
 - 17.2 Unique Factorization of Polynomials
 - 17.3 Polynomial Congruences
 - 17.4 Polynomial Quotient Algebras
 - 17.5 General Properties of Extension Fields
 - 17.6 Formal Derivatives
 - 17.7 Formal Power Series and Laurent Series
 - 17.8 Unique Factorization Domains
 - 17.9 Constructing the Real Numbers
- 18 Polynomial Arithmetic and Applications
 - 18.1 Basic Arithmetic
 - 18.2 Euclid's Algorithm
 - 18.3 Computing Modular Inverses and Chinese Remaindering
 - 18.4 Rational Function Reconstruction and Applications
 - 18.5 Notes
- 19 Finite Fields
 - 19.1 The Characteristic and Cardinality of a Finite Field
 - 19.2 Some Useful Divisibility Criteria
 - 19.3 The Existence of Finite Fields
 - 19.4 The Subfield Structure and Uniqueness of Finite Fields
 - 19.5 Conjugates, Norms and Traces
- 20 Algorithms for Finite Fields
 - 20.1 Testing and Constructing Irreducible Polynomials
 - 20.2 Factoring Polynomials over Finite Fields: the Cantor-Zassenhaus

sci.crypt: beta version of Victor Shoups book, "A Computational Introduction to Number Theory and Algebra"

Algorithm

20.3 Factoring Polynomials over Finite Fields: Berlekamp's Algorithm

20.4 Notes

21 Deterministic Primality Testing

21.1 The Basic Idea

21.2 The Algorithm and its Analysis

21.3 Notes

A Notation and Useful Facts

Bibliography