Algorithmique arithmtique, N1MA9W11

Jean-Marc Couveignes

5 septembre 2011

Motivation I

Effective methods and issues play an important role in number theory :

- Diophantine equations,
- Agorithmic proofs,
- Proposing, refining and testing conjectures.

Motivation II

Ideas and algorithms from number theory and computer algebra have important practical applications

- Cryptography,
- Error correcting codes,
- Pseudo-random generators,
- Robust networks,
- ...

Topics covered

- Complexity theory, elementary arithmetics, applications to classical cryptography,
- Number fields, class fields, complex multiplication, applications to diophantine equations, factoring, primality proving,
- Algorithmic geometry of curves, applications to diophantine equations and modern cryptography.

Complexity, elementary arithmetics, cryptography

- Languages,Automata,Problems,
- Turing machines,
- Complexity classes (deterministic or not),
- Elementary algorithms for elementary operations on integers and polynomials, fast exponentiation,
- Elementary primality (dis)proving, factoring, discrete logarithms,
- Simple protocols in public key cryptography,
- algorithms for commutative groups, lattices, Hermite normal forms,
- Lattice reduction, LLL algorithm and applications,
- Factoring polynomials,
- The AKS primality testing algorithm.

Number fields, class fields, complex multiplication

- Ring of integers,
- Class groups, group of units, Pell's equation,
- Elliptic curves over $\mathbb{C}$,
- Complex multiplication, and class fields,
- The Elliptic Curve Primality Proving algorithm,
- The Elliptic Curve factoring Method,
- The Number Field Sieve.

Algorithmic geometry of curves

- Algorithms for curves and their jacobians,
- Schoof's algorithm for counting points,
- Canonical lifts,
- Modular curves.