"COMPUTATIONAL NUMBER THEORY", AN ABSTRACT CONCERNING THE CONTENTS OF FOUR LECTURES (90 MINUTES EACH) TO BE GIVEN IN THE CIMPA SCHOOL ON NUMBER THEORY AND ITS APPLICATIONS, FACULTY OF SCIENCE OF OUJDA, MAY 2015

DANIEL C. MAYER

1. Summary

(1) First Lecture: Lattices, univariate polynomials, and binary quadratic forms
   (a) Hermite and Smith normal forms in linear algebra
   (b) LLL lattice reduction (by A. Lenstra, H. Lenstra, Lovász, 1982)
   (c) Fincke Pohst algorithm for short vectors in lattices
   (d) Resultant and discriminant of a polynomial
   (e) Polynomial factorization, Hensel lift, Zassenhaus and Berlekamp algorithm

   (f) Reduction and composition of positive definite quadratic forms
   (g) Shanks baby-step giant-step strategy
   (h) McCurley's sub-exponential algorithm
   (i) Fundamental unit and regulator via continued fractions
   (j) Shanks' infrastructure and distance function for computing regulators and composita of indefinite quadratic forms
   (k) Buchmann's sub-exponential algorithm for regulators, composition of indefinite quadratic forms, and class group structure

(2) Second Lecture: Local and global fields of algebraic numbers
   (a) Pohst Zassenhaus round 2 and 4 algorithms for maximal orders
   (b) Buchmann Lenstra algorithm for prime ideal decomposition
   (c) Algorithms for determining Galois groups of normal closures
   (d) Unit group and class group structure (by Buchmann, Diaz y Diaz, Cohen, Olivier)
   (e) Principal ideal test, capitulation, and principal factorization

(3) Third Lecture: Elliptic curves and algebraic varieties
   (a) Weierstrass elliptic functions $\wp(z)$ and $\wp'(z)$
   (b) Modular functions g_2, g_3 and Δ of weight 4, 6 and 12
   (c) Periods ω_1 and ω_2 of the lattice L
   (d) Reduction to the standard fundamental domain $\mathcal{F}$ of the torus $\mathbb{C}/L$

Date: August 25, 2013.

2000 *Mathematics Subject Classification.* Primary 11Y40, 11Y65, 14H52, 14K22, secondary 11Y11, 11Y05.

Key words and phrases. algebraic number theory computations, continued fractions, elliptic curves, complex multiplication, primality, factorization.

Research supported by the Austrian Science Fund (FWF): P 26008-N25.

(e) Shanks Mestre algorithm for elliptic curves over $\mathbb{F}_p$
(f) Tate's local reduction mod p, resp. 2 or 3, and global reduction
(g) Rational torsion points
(h) Finite and infinite contribution to the Néron Tate height
(i) L-function of a modular elliptic curve
(j) Elliptic curves with complex multiplication, Klein's modular function $j(\tau)$ of weight 0, Dedekind's η-function, Hilbert and Weber class polynomials
(k) Hyperelliptic cryptosystems

(4) Fourth Lecture: Multiplicative structure of large integers
  (a) Primality tests
    (i) Jacobi sum test, APR test (Adleman, Pomerance, Rumely, 1980), APRCL test (Cohen, Lenstra, 1981)
    (ii) Elliptic curve test, Goldwasser Kilian test, Atkin Morain test, Adleman Huang test
  (b) Factoring methods
    (i) Continued fraction method (by Legendre, Kraitchik, Lehmer, Powers; resp. Brillhart, Morrison)
    (ii) Class group method (by Schnorr, Lenstra; resp. Shanks, Pollard, Atkin, Rickert)
    (iii) ECM: Lenstra's Elliptic Curve Method
    (iv) Quadratic Sieve (QS by Pomerance, Kraitchik), Multiple Polynomial Quadratic Sieve (MPQS by Montgomery)
    (v) Number Field Sieve (NFS by Pollard)

References

[1] H. U. Besche, B. Eick, and E. A. O'Brien, *The SmallGroups Library — a Library of Groups of Small Order*, 2005, an accepted and refereed GAP 4 package, available also in MAGMA.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[3] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.19, Sydney, 2013).
[4] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics **138**, Springer, 1996.
[5] H. Cohen, *Advanced topics in computational number theory*, Graduate texts in mathematics **193**, Springer, 2000.
[6] A. Enge and A. Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp. **71** (2002), no. 239, 1219–1230.
[7] C. Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303.
[8] G. Gamble, W. Nickel, and E. A. O'Brien, *ANU p-Quotient — p-Quotient and p-Group Generation Algorithms*, 2006, an accepted GAP 4 package, available also in MAGMA.
[9] The GAP Group, *GAP – Groups, Algorithms, and Programming — a System for Computational Discrete Algebra*, Version 4.4.12, Aachen, Braunschweig, Fort Collins, St. Andrews, 2008, (`http://www.gap-system.org`).
[10] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.19-8, Sydney, 2013, (`http://magma.maths.usyd.edu.au`).
[11] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.
[12] The PARI Group, *PARI/GP, Version 2.3.4*, Bordeaux, 2008, (`http://pari.math.u-bordeaux.fr`).
[13] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1990.
[14] A. Stein and E. Teske, *The parallelized Pollard kangaroo method in real quadratic function fields*, Math. Comp. **71** (2002), no. 238, 793–814.
[15] A. Stein and E. Teske, *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Math. Comp. **71** (2002), no. 238, 837–861.

Naglergasse 53, 8010 Graz, Austria
E-mail address: `algebraic.number.theory@algebra.at`
URL: `http://www.algebra.at`