"THÉORIE DES NOMBRES ALGORITHMIQUE", (RESUMÉ DE QUATRE EXPOSÉES À QUATRE-VINGT-DIX MINUTES DANS LE CADRE D'ÉCOLE CIMPA DE THÉORIE DES NOMBRES ET APPLICATIONS, FACULTÉ DES SCIENCES D'OUJDA, MAI 2015)

DANIEL C. MAYER

1. Resumé

(1) Exposé premier: réseaux, polynômes univariates, et formes quadratiques binaires
   (a) Formes normales d'Hermite et Smith dans l'algèbre lineaire
   (b) Réduction LLL de réseaux (par A. Lenstra, H. Lenstra, et Lovász, 1982)
   (c) Algorithme de Fincke et Pohst pour vecteurs brèves dans réseaux
   (d) Résultante et discriminante de polynômes
   (e) Factorisation de polynômes, ascenseur d'Hensel, algorithmes de Zassenhaus et Berlekamp
   (f) Réduction et composition de formes quadratiques positivement definies
   (g) Stratégie de baby steps et giant steps de Shanks
   (h) Algorithme sous-exponentiel de McCurley
   (i) Unité fondamental et régulateur via fractions continues
   (j) Calcul de régulateur et de composé de formes quadratiques indefinies via infrastructure et fonction distance de Shanks
   (k) Algorithme sous-exponentiel de Buchmann pour régulateurs, compositions de formes quadratiques indefinies, et structures de groupes de classes

(2) Exposé deuxième: Corps de nombres algébriques locaux et globaux
   (a) Algorithme Round 2 ou 4 de Pohst et Zassenhaus pour les anneaux des entiers
   (b) Algorithme de Buchmann et Lenstra pour la decomposition des ideaux premiers
   (c) Algorithmes pour la determination de groupes de Galois des clôtures normales
   (d) Structure de groupe d'unités et de groupe de classes à coup d'algorithme de Buchmann, Diaz y Diaz, Cohen, et Olivier
   (e) Test d'ideaux principaux, capitulation, et factorisation principale

(3) Exposé troisième: courbes elliptiques et varietées algébriques
   (a) Fonctions elliptiques $\wp(z)$ et $\wp'(z)$ de Weierstrass
   (b) Fonctions modulaires g_2, g_3 et Δ de poids 4, 6 et 12
   (c) Les périodes ω_1 et ω_2 de réseau L
   (d) Réduction à domaine fondamental standard $\mathcal{F}$ de tore $\mathbb{C}/L$

Date: Août 30, 2013.

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

Key words and phrases. théorie des nombres algébrique algorithmique, fractions continues, courbes elliptiques, multiplication complexe, primalité, factorisation.

Recherche supportée par le Fonds des Sciences d'Autriche (FWF): P 26008-N25.

(e) Algorithme de Shanks et Mestre pour courbes elliptiques sur $\mathbb{F}_p$
(f) Réduction locale mod p, resp. 2 ou 3, et réduction globale de Tate
(g) Points rationnels de torsion
(h) Contributions finies et infinies à l'hauteur de Néron et Tate
(i) Fonction L d'une courbe elliptique modulaire
(j) Courbes elliptiques avec multiplication complexe, fonction modulaire de Klein $j(\tau)$ de poids 0, fonction η de Dedekind, polynômes de classes de Hilbert et Weber
(k) Cryptosystèmes hyperelliptiques

(4) Exposé quatrième: structure multiplicatif des entiers grandes
  (a) Test de primalité
    (i) Test somme de Jacobi, test APR (Adleman, Pomerance, et Rumely, 1980), test APRCL (Cohen et Lenstra, 1981)
    (ii) Test à coup des courbes elliptiques, test de Goldwasser et Kilian, test de Atkin et Morain, test de Adleman et Huang
  (b) Méthodes de factorisation
    (i) Méthode des fractions continues (par Legendre, Kraitchik, Lehmer, et Powers; resp. Brillhart et Morrison)
    (ii) Méthode des groupes de classes (par Schnorr et Lenstra; resp. Shanks, Pollard, Atkin, et Rickert)
    (iii) Méthode des courbes elliptiques (ECM par Lenstra)
    (iv) Crible quadratique (QS par Pomerance et Kraitchik), Crible quadratique avec polynômes multiples (MPQS par Montgomery)
    (v) Crible de corps de nombres (NFS par Pollard)

References

[1] K. Belabas, *Topics in computational algebraic number theory*, J. Théor. Nombres Bordeaux **16** (2004), 19–63.
[2] 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.
[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[4] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.19, Sydney, 2013).
[5] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics **138**, Springer, 1996.
[6] H. Cohen, *Advanced topics in computational number theory*, Graduate texts in mathematics **193**, Springer, 2000.
[7] A. Enge and A. Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp. **71** (2002), no. 239, 1219–1230.
[8] C. Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303.
[9] 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.
[10] 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`).
[11] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.19-8, Sydney, 2013, (`http://magma.maths.usyd.edu.au`).
[12] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.
[13] The PARI Group, *PARI/GP, Version 2.3.4*, Bordeaux, 2008, (`http://pari.math.u-bordeaux.fr`).
[14] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1990.
[15] A. Stein and E. Teske, *The parallelized Pollard kangaroo method in real quadratic function fields*, Math. Comp. **71** (2002), no. 238, 793–814.
[16] 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`