

Number Theory

Computational Methods

11-04 and 11Yxx

- [1] Fadwa S. Abu Muriefah, Florian Luca, and Alain Togbé. On the Diophantine equation $x^2 + 5^a 13^b = y^n$. *Glasg. Math. J.*, 50(1):175–181, 2008.
- [2] Fatima K. Abu Salem and Kamal Khuri-Makdisi. Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field. *LMS J. Comput. Math.*, 10:307–328 (electronic), 2007.
- [3] Ali Akhavi and Damien Stehlé. Speeding-up lattice reduction with random projections (extended abstract). In *LATIN 2008: Theoretical informatics*, volume 4957 of *Lecture Notes in Comput. Sci.*, pages 293–305. Springer, Berlin, 2008.
- [4] Bill Allombert. An efficient algorithm for the computation of Galois automorphisms. *Math. Comp.*, 73(245):359–375 (electronic), 2004.
- [5] Roberto Maria Avanzi. Another look at square roots (and other less common operations) in fields of even characteristic. In *Selected Areas in Cryptography*, volume 4876/2007 of *Lecture Notes in Computer Science*, pages 138–154. Springer Berlin / Heidelberg, 2007.
- [6] Eric Bach and Denis Charles. The hardness of computing an eigenform. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 9–15. Amer. Math. Soc., Providence, RI, 2008.
- [7] Werner Backes and Susanne Wetzel. An efficient LLL gram using buffered transformations. In *Computer Algebra in Scientific Computing*, volume 4770/2007 of *Lecture Notes in Computer Science*, pages 31–44. Springer Berlin / Heidelberg, 2007.
- [8] David H. Bailey, Jonathan M. Borwein, Vishaal Kapoor, and Eric W. Weisstein. Ten problems in experimental mathematics. *Amer. Math. Monthly*, 113(6):481–509, 2006.

- [9] Stéphane Ballet. Quasi-optimal algorithms for multiplication in the extensions of \mathbf{F}_{16} of degree 13, 14 and 15. *J. Pure Appl. Algebra*, 171(2-3):149–164, 2002.
- [10] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler. Construction of hyperelliptic function fields of high three-rank. *Math. Comp.*, 77(261):503–530 (electronic), 2008.
- [11] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen. New integer representations as the sum of three cubes. *Math. Comp.*, 76(259):1683–1690 (electronic), 2007.
- [12] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. Optimizing double-base elliptic-curve single-scalar multiplication. In *Progress in Cryptology - INDOCRYPT 2007*, volume 4859/2007 of *Lecture Notes in Computer Science*, pages 167–182. Springer Berlin / Heidelberg, 2007.
- [13] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. ECM using Edwards curves. *IACR eprint:2008:016*, 18 pages, 2008.
- [14] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology - ASIACRYPT 2007*, volume 4833/2007 of *Lecture Notes in Computer Science*, pages 29–50. Springer Berlin / Heidelberg, 2007.
- [15] Amnon Besser and Rob De Jeu. $li(p)$ -service? an algorithm for computing p -adic polyalgorithms. *Math. Comp.*, 77(262):1105–1134, 2008.
- [16] Peter Birkner. Efficient divisor class halving on genus two curves. In *Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Computer Science*, pages 317–326. Springer, Berlin/Heidelberg.
- [17] Werner Bley and Robert Boltje. Computation of locally free class groups. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 72–86. Springer, Berlin, 2006.
- [18] Jonathan Borwein and David Bailey. *Mathematics by Experiment*. A K Peters Ltd., Natick, MA, 2004.

- [19] Wieb Bosma. Some computational experiments in number theory. In *Discovering Mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 1–30. Springer, Berlin, 2006.
- [20] Wieb Bosma, John Cannon, and Allan Steel. Lattices of compatibly embedded finite fields. *J. Symbolic Comput.*, 24(3-4):351–369, 1997.
- [21] Wieb Bosma and Bart de Smit. Class number relations from a computational point of view. *J. Symbolic Comput.*, 31(1-2):97–112, 2001.
- [22] Wieb Bosma and Bart de Smit. On arithmetically equivalent number fields of small degree. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 67–79. Springer, Berlin, 2002.
- [23] Wieb Bosma and Arjen K. Lenstra. An implementation of the elliptic curve integer factorization method. In *Computational Algebra and Number Theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 119–136. Kluwer Acad. Publ., Dordrecht, 1995.
- [24] Wieb Bosma and Peter Stevenhagen. Density computations for real quadratic units. *Math. Comp.*, 65(215):1327–1337, 1996.
- [25] Johan Bosman. On the computation of Galois representations associated to level one modular forms. [arXiv:0710.1237v1](https://arxiv.org/abs/0710.1237v1), 15 pages, 2007.
- [26] Alin Bostan, Pierrick Gaudry, and Éric Schost. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 40–58. Springer, Berlin, 2004.
- [27] Aaron Bradord, Michael Monagan, and Colin Percival. Integer factorization and computing discrete logarithms in Maple. In *Proceedings of the 2006 Maple Conference*, pages 2–13, 2006.
- [28] Richard P. Brent. Factorization of the tenth Fermat number. *Math. Comp.*, 68(225):429–451, 1999.
- [29] Richard P. Brent. Recent progress and prospects for integer factorisation algorithms. In *Computing and Combinatorics (Sydney, 2000)*, volume 1858 of *Lecture Notes in Comput. Sci.*, pages 3–22. Springer, Berlin, 2000.

- [30] Richard P. Brent. Note on Marsaglia’s xorshift random number generators. *J. Stat. Soft.*, 11(5):1–5, 2004.
- [31] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.
- [32] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. [arXiv:0803.2052v1](https://arxiv.org/abs/0803.2052v1) [math.NT], 19 pages, 2008.
- [33] David G. Cantor and Daniel M. Gordon. Factoring polynomials over p -adic fields. In *Algorithmic Number Theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 185–208. Springer, Berlin, 2000.
- [34] Wouter Castryck, Hendrik Hubrechts, and Frederik Vercauteren. Computing zeta functions in families of $C_{a,b}$ curves using deformation. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 296–311. Springer, 2008.
- [35] Antoine Chambert-Loir. Compter (rapidement) le nombre de solutions d’équations dans les corps finis. [arXiv:math.NT/0611584](https://arxiv.org/abs/math.NT/0611584), 46 pages, 2006.
- [36] Hugo Chapdelaine. Computation of p -units in ray class fields of real quadratic number fields. *Math. Comp.*, 78:2307–2345, 2009.
- [37] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll. Explicit n -descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155, 2008.
- [38] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441 (electronic), 2003.
- [39] M. Daberkow. Computing with subfields. *J. Symbolic Comput.*, 24(3-4):371–384, 1997.
- [40] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24(3-4):267–283, 1997.

- [41] Lassina Dembélé. Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms. *Math. Comp.*, 76(258):1039–1057 (electronic), 2007.
- [42] Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 371–386. Springer Berlin / Heidelberg, 2008.
- [43] Francisco Diaz y Diaz, Jean-François Jaulent, Sebastian Pauli, Michael Pohst, and Florence Soriano-Gafiuk. A new algorithm for the computation of logarithmic l -class groups of number fields. *Experiment. Math.*, 14(1):65–74, 2005.
- [44] Claus Diem. Index calculus in class groups of plane curves of small degree. *Preprint*, 43 pages, 2005.
- [45] Claus Diem. An index calculus algorithm for plane curves of small degree. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 543–557. Springer, Berlin, 2006.
- [46] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt. Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field. *Preprint*, 14 pages, 2006.
- [47] Jacques Dubrois and Jean-Guillaume Dumas. Efficient polynomial time algorithms computing industrial-strength primitive roots. *Inform. Process. Lett.*, 97(2):41–45, 2006.
- [48] Sylvain Duquesne. Montgomery ladder for all genus 2 curves in characteristic 2. In *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Computer Science*, pages 174–188. Springer, 2008.
- [49] I. Duursma, P. Gaudry, and F. Morain. Speeding up the discrete log computation on curves with automorphisms. In *Advances in Cryptology—Asiacrypt’99 (Singapore)*, volume 1716 of *Lecture Notes in Comput. Sci.*, pages 103–121. Springer, Berlin, 1999.
- [50] Claus Fieker. Applications of the class field theory of global fields. In *Discovering Mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 31–62. Springer, Berlin, 2006.

- [51] Claus Fieker. Sparse representation for cyclotomic fields. *Experiment. Math.*, 16(4):493–500, 2007.
- [52] Claus Fieker and Willem A. de Graaf. Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras. *LMS J. Comput. Math.*, 10:271–287 (electronic), 2007.
- [53] Claus Fieker and Michael E. Pohst. Dependency of units in number fields. *Math. Comp.*, 75(255):1507–1518 (electronic), 2006.
- [54] Tom Fisher. The Hessian of a genus one curve. [arXiv:math.NT/0610403](https://arxiv.org/abs/math.NT/0610403), 28 pages, 2006.
- [55] Tom Fisher. The invariants of a genus one curve. *Proc. Lond. Math. Soc. (3)*, 97(3):753–782, 2008.
- [56] E. V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *J. Symbolic Comput.*, 43(4):293–303, 2008.
- [57] Felix Fontein. The infrastructure of a global field of arbitrary unit rank. [arXiv:0809.1685](https://arxiv.org/abs/0809.1685), 36 pages, 2008.
- [58] Robert Fraatz. *Computation of Maximal Orders of Cyclic Extensions of Function Fields*. PhD Thesis, Technischen Universität Berlin, 2005.
- [59] David Freeman. Constructing pairing-friendly genus 2 curves with ordinary Jacobians. In *Pairing-based cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 152–176. Springer, Berlin, 2007.
- [60] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology—Eurocrypt 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Berlin, 2000.
- [61] Pierrick Gaudry, Alexander Kruppa, and Paul Zimmermann. A GMP-based implementation of Schönhage-Strassen’s large integer multiplication algorithm. In *ISSAC 2007*, pages 167–174. ACM, New York, 2007.

- [62] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt. Comment on: “A new representation of elements of finite fields $\text{GF}(2^m)$ yielding small complexity arithmetic circuits” by G. Drolet. *IEEE Trans. Comput.*, 51(12):1460–1461, 2002.
- [63] Willi Geiselmann and Rainer Steinwandt. A redundant representation of $\text{GF}(q^n)$ for designing arithmetic circuits. *IEEE Trans Comp*, 52(7):848–853, 2003.
- [64] Willi Geiselmann and Rainer Steinwandt. Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit. In *Advances in cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 466–481. Springer, Berlin, 2007.
- [65] Martine Girard and Leopoldo Kulesz. Computation of sets of rational points of genus-3 curves via the Demjanenko-Manin method. *LMS J. Comput. Math.*, 8:267–300 (electronic), 2005.
- [66] Norbert Goeb. Computing the automorphism groups of hyperelliptic function fields. [arXiv:math.NT/0305284](https://arxiv.org/abs/math.NT/0305284), 16 pages, 2003.
- [67] Edray Goins, Florian Luca, and Alain Togbé. On the diophantine equation $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 430–442. Springer Berlin / Heidelberg, 2008.
- [68] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarnita. Computational verification of the birch and swinnerton-dyer conjecture for individual elliptic curves. *Math. Comp*, 78:2397–2425, 2009.
- [69] Jordi Guardia, Jesus Montes, and Enric Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. [arXiv:0807.4065v3](https://arxiv.org/abs/0807.4065v3) [math.NT], 24 pages, 2008.
- [70] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM.

- [71] Guillaume Hanrot and Damien Stehlé. Improved analysis of Kannan’s shortest lattice vector algorithm (extended abstract). In *Advances in cryptology—CRYPTO 2007*, volume 4622 of *Lecture Notes in Comput. Sci.*, pages 170–186. Springer, Berlin, 2007.
- [72] David Harvey. A cache-friendly truncated FFT. *Theor. Comput. Sci.*, 410(27-29):2649–2658, 2009.
- [73] Lenwood S. Heath and Nicholas A. Loehr. New algorithms for generating Conway polynomials over finite fields. *J. Symbolic Comput.*, 38(2):1003–1024, 2004.
- [74] Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548 (electronic), 2003.
- [75] Hendrik Hubrechts. Point counting in families of hyperelliptic curves. *Found. Comput. Math.*, 8(1):137–169, 2008.
- [76] Hendrik Hubrechts. Quasi-quadratic elliptic curve point counting using rigid cohomology. *J. Symb. Comput.*, 44(9):1255–1267, 2009.
- [77] Jean-François Jaulent, Sebastian Pauli, Michael E. Pohst, and Florence Soriano-Gafiuk. Computation of 2-groups of positive classes of exceptional number fields. *J. Théor. Nombres Bordeaux*, 20(3):715–732, 2008.
- [78] Antoine Joux and Reynald Lercier. Counting points on elliptic curves in medium characteristic. *Preprint*, page 15, 2006.
- [79] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. [arXiv:0808.3833v1 \[math.NT\]](https://arxiv.org/abs/0808.3833v1), 29 pages, 2008.
- [80] Jürgen Klüners. Algorithms for function fields. *Experiment. Math.*, 11(2):171–181, 2002.
- [81] Grégoire Lecerf. Fast separable factorization and applications. *Appl. Algebra Engrg. Comm. Comput.*, 19(2):135–160, 2008.

- [82] Reynald Lercier and Thomas Sirvent. On Elkies subgroups of l -torsion points in elliptic curves defined over a finite field. *J. Théor. Nombres Bordeaux*, 20(3):783–797, 2008.
- [83] J.M. Miret, R. Moreno, J. Pujolas, and A. Rio. Halving for the 2-Sylow subgroup of genus 2 curves over binary fields. *Finite Fields Appl.*, 15(5):569–579, 2009.
- [84] Michael Monagan and Mark van Hoeij. A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions. <http://www.cecm.sfu.ca/CAG/papers/HoeijMonGCD.pdf>, 36 pages.
- [85] I. Morel, D. Stehlé, and G. Villard. Analyse numérique et réduction de reseaux. *Technique et Science Informatiques*, To appear, 29 pages, 2009.
- [86] J.-M. Muller, N. Brisebarre, F. de Dinechin, C.-P. Jeannerod, L. Vincent, G. Melquiond, N. Revol, D. Stehlé, and S. Torres. *Handbook of Floating-point Arithmetic*. Birkhäuser, Boston, MA, 2009.
- [87] Siguna Müller. On the computation of square roots in finite fields. *Des. Codes Cryptogr.*, 31(3):301–312, 2004.
- [88] Phong Q. Nguyen and Damien Stehlé. Floating-point LLL revisited. In *Advances in cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Comput. Sci.*, pages 215–233. Springer, Berlin, 2005.
- [89] Harris Nover. Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group $c_2 \times c_2 \times c_2$. *Journal of Number Theory*, 129(1):231 – 245, 2009.
- [90] Titus Piezas. Solving solvable sextics using polynomial decomposition. *Preprint*, 22 pages, 2004.
- [91] M. E. Pohst. Computational aspects of Kummer theory. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 259–272. Springer, Berlin, 1996.
- [92] Xavier-François Roblot. Polynomial factorization algorithms over number fields. *J. Symbolic Comput.*, 38(5):1429–1443, 2004.

- [93] Tanaka Satoru and Nakamura Ken. More constructing pairing-friendly elliptic curves for cryptography. *arXiv:0711.1942*, 11 pages, 2007.
- [94] René Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.
- [95] Nigel P. Smart. *The Algorithmic Resolution of Diophantine Equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.
- [96] B. Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. *J. Cryptology*, 22(4):505–529, 2009.
- [97] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. In *Advances in Cryptology, Eurocrypt 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 163–180. Springer Berlin/Heidelberg, 2008.
- [98] Damien Stehlé. Floating-point LLL: Theoretical and practical aspects. *Proceedings of LLL+25 Conference, 2007*, 36 pages, 2009.
- [99] Damien Stehlé and Paul Zimmermann. A binary recursive GCD algorithm. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 411–425. Springer, Berlin, 2004.
- [100] Katsuyuki Takashima. A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application. *IEICE Trans. Fundamentals*, E89-A(1):124–133, 2006.
- [101] Hans-Christian Graf v. Bothmer. Finite field experiments (with an appendix by Stefan Wiedmann). In *Higher-Dimensional Geometry over Finite Fields*, volume 16 of *NATO Science for Peace and Security Series, D: Information and Communication Security*, pages 1–62. 2008.
- [102] Mark van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2):167–189, 2002.
- [103] Gilles Villard. Certification of the QR factor R and of lattice basis reducedness. In *ISSAC 2007*, pages 361–368. ACM, New York, 2007.

- [104] P. G. Walsh. On a very particular class of Ramanujan-Nagell type equations. *Far East J. Math. Sci. (FJMS)*, 24(1):55–58, 2007.
- [105] Paul Zimmermann and Bruce Dodson. 20 years of ECM. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 525–542. Springer, Berlin, 2006.