

# Number Theory

## Elementary Number Theory

*11Axx except 11A41 and 11A51, 11Cxx*

- [1] David H. Bailey and Jonathan M. Borwein. Experimental mathematics: Examples, methods and implications. *Notices Amer. Math. Soc.*, 52(5):502–514, 2005.
- [2] 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.
- [3] Richard P. Brent and Paul Zimmermann. Ten new primitive binary trinomials. *Math. Comp.*, 78(266):1197–1199, 2009.
- [4] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [5] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [6] J. E. Cremona. Unimodular integer circulants. *Math. Comp.*, 77(263):1639–1652, 2008.
- [7] Graham Everest and Valery Mahe. A generalization of Siegel’s theorem and Hall’s conjecture. *Exp. Math.*, 18(1):1–10, 2009.
- [8] Sharon Anne Garthwaite. Convolution congruences for the partition function. *Proc. Amer. Math. Soc.*, 135(1):13–20 (electronic), 2007.
- [9] Emmanuel Royer. Evaluating convolution sums of the divisor function with quasimodular forms. *Int. J. Number Theory*, 3(2):231–261, 2007.
- [10] J. Sándor and B. Crstici. *Handbook of Number Theory II*. Kluwer Academic Publishers, Dordrecht, 2004.

# Number Theory

## Primality and Factorisation

11A41, 11A51

- [1] Richard P. Brent, Peter L. Montgomery, Herman J.J. te Riele, Henk Boender, Stephania Cavallar, Conrad Curry, Bruce Dodson, Jens Franke, Joseph Leherbauer, George Sassoon, and Robert Silverman. Factorizations of Cunningham numbers with bases 13 to 99: Millennium edition. In *Report – Modelling, Analysis and Simulation*, volume 7, pages i–viii, pp. 1–19. Centrum voor Wiskunde en Informatica, Amsterdam, 2001.
- [2] Graham Everest, Patrick Ingram, and Shaun Stevens. Primitive divisors on twists of Fermat’s cubic. *LMS J. Comput. Math.*, 12:54–81, 2009.
- [3] Stephen McMath. Parallel integer factorization using quadratic forms. *Technical Report*, 132 pages, 2005.
- [4] F. Morain. Primality proving using elliptic curves: An update. In *Algorithmic Number Theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 111–127. Springer, Berlin, 1998.
- [5] 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.

# Number Theory

## Sequences and Sets

11Bxx

- [1] S. Akhtari, A. Togbé, and P. G. Walsh. On the equation  $aX^4 - bY^2 = 2$ . *Acta Arith.*, 131(2):145–169, 2008.
- [2] A. Bremner and N. Tzanakis. Lucas sequences whose 12th or 9th term is a square. *J. Number Theory*, 107(2):215–227, 2004.
- [3] A. Bremner and N. Tzanakis. Lucas sequences whose 8th term is a square. [arXiv:math.NT/0408371](https://arxiv.org/abs/math/0408371) v2, 44 pages, 2004.
- [4] A. Bremner and N. Tzanakis. On squares in Lucas sequences. *J. Number Theory*, 124(2):511–520, 2007.
- [5] Florian Breuer, Ernest Lötter, and Brink van der Merwe. Ducci-sequences and cyclotomic polynomials. *Finite Fields Appl.*, 13(2):293–304, 2007.
- [6] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely. Arithmetic progressions consisting of unlike powers. *Indag. Math. (N.S.)*, 17(4):539–555, 2006.
- [7] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. On Fibonacci numbers with few prime divisors. *Proc. Japan Acad. Ser. A Math. Sci.*, 81(2):17–20, 2005.
- [8] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Sur les nombres de Fibonacci de la forme  $q^k y^p$ . *C. R. Math. Acad. Sci. Paris*, 339(5):327–330, 2004.
- [9] Everett W. Howe. Higher-order Carmichael numbers. *Math. Comp.*, 69(232):1711–1719, 2000.
- [10] J. McLaughlin. Small prime powers in the Fibonacci sequence. [arXiv:math.NT/0110150](https://arxiv.org/abs/math/0110150) v2, 22 pages, 2002.
- [11] A. Stoimenow. Generating functions, Fibonacci numbers and rational knots. *J. Algebra*, 310(2):491–525, 2007.

# Number Theory

## Diophantine Equations

11Dxx

- [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] S. Akhtari, A. Togbé, and P. G. Walsh. On the equation  $aX^4 - bY^2 = 2$ . *Acta Arith.*, 131(2):145–169, 2008.
- [3] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc.* (3), 92(2):273–306, 2006.
- [4] Michael A. Bennett. The Diophantine equation  $(x^k - 1)(y^k - 1) = (z^k - 1)^t$ . *Indag. Math. (N.S.)*, 18(4):507–525, 2007.
- [5] Michael A. Bennett, Kálmán Győry, and Ákos Pintér. On the Diophantine equation  $1^k + 2^k + \dots + x^k = y^n$ . *Compos. Math.*, 140(6):1417–1431, 2004.
- [6] A. Bérczes, A. Pethő, and V. Ziegler. Parameterized norm form equations with arithmetic progressions. *J. Symbolic Comput.*, 41(7):790–810, 2006.
- [7] Attila Bérczes and Attila Pethő. Computational experiences on norm form equations with solutions forming arithmetic progressions. *Glas. Mat. Ser. III*, 41(61)(1):1–8, 2006.
- [8] A. Bremner and N. Tzanakis. Lucas sequences whose 8th term is a square. [arXiv:math.NT/0408371](https://arxiv.org/abs/math.NT/0408371) v2, 44 pages, 2004.
- [9] A. Bremner and N. Tzanakis. On squares in Lucas sequences. *J. Number Theory*, 124(2):511–520, 2007.
- [10] Andrew Bremner. On the equation  $Y^2 = X^5 + k$ . *Experiment. Math.*, 17(3):371–374, 2008.

- [11] Andrew Bremner. A problem of Ozanam. *Proc. Edinburgh Math. Soc.*, 52(1):37–44, 2009.
- [12] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely. Arithmetic progressions consisting of unlike powers. *Indag. Math. (N.S.)*, 17(4):539–555, 2006.
- [13] Nils Bruin. The primitive solutions to  $x^3 + y^9 = z^2$ . *J. Number Theory*, 111(1):179–189, 2005.
- [14] Nils Bruin. Some ternary Diophantine equations of signature  $(n, n, 2)$ . In *Discovering Mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 63–91. Springer, Berlin, 2006.
- [15] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.
- [16] Ralph H. Buchholz. Triangles with three rational medians. *J. Number Theory*, 97(1):113–131, 2002.
- [17] Ralph H. Buchholz and James A. MacDougall. Cyclic polygons with rational sides and area. *J. Number Theory*, 128(1):17–48, 2008.
- [18] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. On perfect powers in Lucas sequences. *Int. J. Number Theory*, 1(3):309–332, 2005.
- [19] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations I: Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3):969–1018, 2006.
- [20] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations II: The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.
- [21] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008.
- [22] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

- [23] Imin Chen. A Diophantine equation associated to  $X_0(5)$ . *LMS J. Comput. Math.*, 8:116–121 (electronic), 2005.
- [24] Imin Chen. On the equation  $s^2 + y^{2p} = \alpha^3$ . *Math. Comp.*, 77(262):1223–1227, 2008.
- [25] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322(3):638–656, 2009.
- [26] C. Chisholm and J. A. MacDougall. Rational and Heron tetrahedra. *J. Number Theory*, 121(1):153–185, 2006.
- [27] C. Chisholm and J. A. MacDougall. Rational tetrahedra with edges in geometric progression. *J. Number Theory*, 128(2):251–262, 2008.
- [28] Mihai Cipu. Gröbner bases and Diophantine analysis. *J. Symbolic Comput.*, 43(10):681–687, 2008.
- [29] Mihai Cipu, Florian Luca, and Maurice Mignotte. Solutions of the Diophantine equation  $x^y + y^z + z^x = n!$ . *Glasg. Math. J.*, 50(2):217–232, 2008.
- [30] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*. Springer, Berlin, 2007.
- [31] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and the Diophantine problem for rings of integers. *J. Théor. Nombres Bordeaux*, 17(3):727–735, 2005.
- [32] Robert S. Coulter, Marie Henderson, and Felix Lazebnik. On certain combinatorial Diophantine equations and their connection to Pythagorean numbers. *Acta Arith.*, 122(4):395–406, 2006.
- [33] A. Bremner and Jean-Joël Delorme. On equal sums of ninth powers. *Math. Comp.*, In Press, 2009.
- [34] Luis V. Dieulefait. Solving Diophantine equations  $x^4 + y^4 = qz^p$ . *Acta Arith.*, 117(3):207–211, 2005.
- [35] Shanshan Ding. Smallest irreducible of the form  $x^2 - dy^2$ . *Int. J. Number Theory*, 7 pages, 2007.

- [36] Konstantinos Draziotis and Dimitrios Poulakis. Practical solution of the Diophantine equation  $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$ . *Math. Comp.*, 75(255):1585–1593 (electronic), 2006.
- [37] Konstantinos Draziotis and Dimitrios Poulakis. Solving the Diophantine equation  $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$ . *Journal of Number Theory*, 129(1):102 – 121, 2009.
- [38] Konstantinos A. Draziotis. Integer points on the curve  $Y^2 = X^3 \pm p^k X$ . *Math. Comp.*, 75(255):1493–1505 (electronic), 2006.
- [39] 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.
- [40] K. Győry and Á. Pintér. Almost perfect powers in products of consecutive integers. *Monatsh. Math.*, 145(1):19–33, 2005.
- [41] K. Győry and Á. Pintér. Correction to the paper: “Almost perfect powers in products of consecutive integers”. *Monatsh. Math.*, 146(4):341, 2005.
- [42] K. Győry and Á. Pintér. On the resolution of equations  $Ax^n - By^n = C$  in integers  $x, y$  and  $n \geq 3$ . I. *Publ. Math. Debrecen*, 70(3-4):483–501, 2007.
- [43] Lajos Hajdu and Szabolcs Tengely. Arithmetic progressions of squares, cubes and  $n$ -th powers. [arXiv:0707.0593](https://arxiv.org/abs/0707.0593), 10 pages, 2007.
- [44] Lajos Hajdu, Szabolcs Tengely, and Robert Tijdeman. Cubes in products of terms in arithmetic progression. *Publ. Math. Debrecen*, 74(1-2):215–232, 2009.
- [45] Robin Hartshorne and Ronald van Luijk. Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on  $K3$  surfaces. *Math. Intelligencer*, 30(4):4–10, 2008.
- [46] Bo He and Alain Togbé. On the number of solutions of Goormaghtigh equation for given  $x$  and  $y$ . *Indag. Math. (N.S.)*, 19(1):65–72, 2008.

- [47] E. Herrmann, I. Járási, and A. Pethő. Note on: “The Diophantine equation  $x^n = Dy^2 + 1$ ” by J. H. E. Cohn. *Acta Arith.*, 113(1):69–76, 2004.
- [48] E. Herrmann, F. Luca, and P. G. Walsh. A note on the Ramanujan-Nagell equation. *Publ. Math. Debrecen*, 64(1-2):21–30, 2004.
- [49] Emanuel Herrmann and Attila Pethő.  $S$ -integral points on elliptic curves. Notes on a paper of B. M. M. de Weger. *J. Théor. Nombres Bordeaux*, 13(2):443–451, 2001.
- [50] Stephen P. Humphries and Kenneth W. Johnson. Fusions of character tables and Schur rings of abelian groups. *Comm. Algebra*, 36(4):1437–1460, 2008.
- [51] L. Hajdu K. Györy and A. Pinter. Perfect powers from products of consecutive terms in arithmetic progression. 145(4):845–864, 2009.
- [52] Tünde Kovács. Combinatorial Diophantine equations—the genus 1 case. *Publ. Math. Debrecen*, 72(1-2):243–255, 2008.
- [53] Shanta Laishram, T. N. Shorey, and Szabolcs Tengely. Squares in products in arithmetic progression with at most one term omitted and common difference a prime power. *Acta Arith.*, 135(2):143–158, 2008.
- [54] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Coleman-Chabauty. [arXiv:math.NT/0005186](https://arxiv.org/abs/math/0005186), 30 pages, 2000.
- [55] F. Luca, P. Stanica, and A. Togbé. On a Diophantine equation of Stroeker. *Bull. Belg. Math. Soc. Simon Stevin*, page 10, 2008.
- [56] F. S. Abu Muriefah, F. Luca, S. Siksek, and S. Tengely. On the Diophantine equation  $x^2 + c = 2y^n$ . *Int. J. Number Theory*, 2008.
- [57] Á. Pintér. On a class of Diophantine equations related to the numbers of cells in hyperplane arrangements. *J. Number Theory*, 129(7):1664–1668, 2009.
- [58] Ákos Pintér. On the power values of power sums. *J. Number Theory*, 125(2):412–423, 2007.

- [59] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$ . *Duke Math. J.*, 137(1):103–158, 2007.
- [60] Samir Siksek and John E. Cremona. On the Diophantine equation  $x^2 + 7 = y^m$ . *Acta Arith.*, 109(2):143–149, 2003.
- [61] N. P. Smart. Thue and Thue-Mahler equations over rings of integers. *J. London Math. Soc. (2)*, 56(3):455–462, 1997.
- [62] Nigel P. Smart. *The Algorithmic Resolution of Diophantine Equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.
- [63] Sz. Tengely. Note on the paper: “An extension of a theorem of Euler” by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman. *Acta Arith.*, 134(4):329–335, 2008.
- [64] Szabolcs Tengely. On the Diophantine equation  $x^2 + a^2 = 2y^p$ . *Indag. Math. (N.S.)*, 15(2):291–304, 2004.
- [65] Szabolcs Tengely. *Effective Methods for Diophantine Equations*. PhD thesis, Leiden University, 2005.
- [66] Szabolcs Tengely. Triangles with two integral sides. *Ann. Math. Inform.*, 34:89–95, 2007.
- [67] P. G. Walsh. On a very particular class of Ramanujan-Nagell type equations. *Far East J. Math. Sci. (FJMS)*, 24(1):55–58, 2007.
- [68] Jahan Zahid. Zeros of  $p$ -adic forms. *J. Number Theory*, 129(10):2439–2456, 2009.
- [69] Huilin Zhu and Jianhua Chen. Integral points on a class of elliptic curve. *Wuhan Univ. J. Nat. Sci.*, 11(3):477–480, 2006.

# Number Theory

## Forms and Linear Algebraic Groups

11Exx

- [1] Kanat Abdukhalikov and Rudolf Scharlau. Unimodular lattices in dimensions 14 and 15 over the Eisenstein integers. *Math. Comp.*, 78(265):387–403, 2009.
- [2] Manjul Bhargava. Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.
- [3] Donald I. Cartwright and Tim Steger. Application of the Bruhat–Tits tree of  $SU_3(h)$  to some  $A_2$  groups. *J. Austral. Math. Soc. Ser. A*, 64(3):329–344, 1998.
- [4] Carlos Castaño-Bernard. Further properties of a function of Ogg and Ligozat. *Ramanujan J.*, 17(1):107–121, 2008.
- [5] Darrin Doud. Supersingular Galois representations and a generalization of a conjecture of Serre. *Experiment. Math.*, 16, 119–128 pages, 2007.
- [6] Jonathan Hanke. Local densities and explicit bounds for representability by a quadratic form. *Duke Math. J.*, 124(2):351–388, 2004.
- [7] Boris Hemkemeier. Algorithmische konstruktionen von gittern. [arXiv:math.MG/0411134](https://arxiv.org/abs/math/0411134), 64 pages, 2004.
- [8] Jeremy Rouse. Zagier duality for the exponents of Borcherds products for Hilbert modular forms. *J. London Math. Soc. (2)*, 73(2):339–354, 2006.
- [9] John Voight. *Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic*. PhD thesis, Berkeley, 2005.
- [10] John Voight. Quadratic forms that represent almost the same primes. *Math. Comp.*, 76(259):1589–1617 (electronic), 2007.

- [11] Tonghai Yang. Local densities of 2-adic quadratic forms. *J. Number Theory*, 108(2):287–345, 2004.
- [12] Dan Yasaki. Hyperbolic tessellations associated to Bianchi groups. [arXiv:0908.1762](https://arxiv.org/abs/0908.1762), 8 pages, 2009.

# Number Theory

## Discontinuous Groups and Automorphic Forms

11Fxx

- [1] Scott Ahlgren. On the irreducibility of Hecke polynomials. *Math. Comp.*, 77(263):1725–1731, 2008.
- [2] Scott Ahlgren and Ken Ono. Arithmetic of singular moduli and class polynomials. *Compos. Math.*, 141(2):293–312, 2005.
- [3] A. O. L. Atkin, Wen-Ching Winnie Li, and Ling Long. On Atkin and Swinnerton-Dyer congruence relations. (II). *Math. Ann.*, 340(2):335–358, 2008.
- [4] Tobias Berger. An Eisenstein ideal for imaginary quadratic fields and the Bloch-Kato conjecture for Hecke characters. [arXiv:math.NT/0701177](https://arxiv.org/abs/math/0701177), 26 pages, 2007.
- [5] Tobias Berger and Krzysztof Klosin. A deformation problem for Galois representations over imaginary quadratic fields. *J. Inst. Math. Jussieu*, To appear:19, 2009.
- [6] 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.
- [7] Jim Brown. Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture. *Compos. Math.*, 143(2):290–322, 2007.
- [8] Jan Hendrik Bruinier and Tonghai Yang.  $CM$ -values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006.
- [9] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008.
- [10] Cecilia Busuioc. The Steinberg symbol and special values of  $L$ -functions. *Trans. Amer. Math. Soc.*, 360(11):5999–6015, 2008.

- [11] Kevin Buzzard. Questions about slopes of modular forms. *Astérisque*, (298):1–15, 2005.
- [12] Kevin Buzzard and Frank Calegari. A counterexample to the Gouvêa-Mazur conjecture. *C. R. Math. Acad. Sci. Paris*, 338(10):751–753, 2004.
- [13] Kevin Buzzard and William A. Stein. A mod five approach to modularity of icosahedral Galois representations. *Pacific J. Math.*, 203(2):265–282, 2002.
- [14] Bryden Cais. Serre’s conjectures. *Preprint*, 21 pages, 2005.
- [15] Frank Calegari and Nathan M. Dunfield. Automorphic forms and rational homology 3-spheres. *Geom. Topol.*, 10:295–329 (electronic), 2006.
- [16] Frank Calegari and William A. Stein. Conjectures about discriminants of Hecke algebras of prime level. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 140–152. Springer, Berlin, 2004.
- [17] I. Chen, I. Kiming, and J. B. Rasmussen. On congruences mod  $p^m$  between eigenforms and their attached Galois representations. [arXiv:0809.3622](https://arxiv.org/abs/0809.3622), 11 pages, 2008.
- [18] C. J. Cummins. Congruence subgroups of groups commensurable with  $\mathrm{PSL}(2, Z)$  of genus 0 and 1. *Experiment. Math.*, 13(3):361–382, 2004.
- [19] Henri Darmon and Robert Pollack. Efficient calculation of Stark-Heegner points via overconvergent modular symbols. *Israel J. Math.*, 153:319–354, 2006.
- [20] Lassina Dembélé. Explicit computations of Hilbert modular forms on  $\mathbf{Q}(\sqrt{5})$ . *Experiment. Math.*, 14(4):457–466, 2005.
- [21] Lassina Dembélé. Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms. *Math. Comp.*, 76(258):1039–1057 (electronic), 2007.
- [22] 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.

- [23] Tobias Dern and Aloys Krieg. Graded rings of Hermitian modular forms of degree 2. *Manuscripta Math.*, 110(2):251–272, 2003.
- [24] Tobias Dern and Aloys Krieg. The graded ring of Hermitian modular forms of degree 2 over  $Q(\sqrt{-2})$ . *J. Number Theory*, 107(2):241–265, 2004.
- [25] Luis Dieulefait and Xavier Taixes i Ventosa. Congruences between modular forms and lowering the level mod  $l^n$ . [arXiv:0801.0104v1](https://arxiv.org/abs/0801.0104v1), 8 pages, 2007.
- [26] Darrin Doud. Three-dimensional Galois representations with conjectural connections to arithmetic cohomology. In *Number Theory for the Millennium I (Urbana, IL, 2000)*, pages 365–375. A K Peters, Natick, MA, 2002.
- [27] Darrin Doud. Distinguishing contragredient Galois representations in characteristic two. *Rocky Mountain J. Math.*, 38(3):835–848, 2008.
- [28] Darrin Doud and Brian Hansen. Explicit Frobenius calculations supporting a generalization of a conjecture of Serre. *JP J. Algebra Number Theory Appl.*, 6(2):381–398, 2006.
- [29] Neil Dummigan, William Stein, and Mark Watkins. Constructing elements in Shafarevich-Tate groups of modular motives. In *Number Theory and Algebraic Geometry*, volume 303 of *London Math. Soc. Lecture Note Ser.*, pages 91–118. Cambridge Univ. Press, Cambridge, 2003.
- [30] Bas Edixhoven. Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. *J. Inst. Math. Jussieu*, 5(1):1–34, 2006.
- [31] Liqun Fang, J. William Hoffman, Benjamin Linowitz, Andrew Rupinski, and Helena Verrill. Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations. [arXiv:0805.2144v1](https://arxiv.org/abs/0805.2144v1) [[math.NT](https://arxiv.org/abs/0805.2144v1)], 37 pages, 2008.
- [32] Julio Fernández, Josep González, and Joan-C. Lario. Plane quartic twists of  $X(5, 3)$ . *Canad. Math. Bull.*, 50(2):196–205, 2007.

- [33] Sharon M. Frechette. A classical characterization of newforms with equivalent eigenforms in  $S_{k+1/2}(4N, \chi)$ . *J. London Math. Soc. (2)*, 68(3):563–578, 2003.
- [34] Eberhard Freitag and Manabu Oura. A theta relation in genus 4. *Nagoya Math. J.*, 161:69–83, 2001.
- [35] Edray Goins. On the modularity of wildly ramified Galois representations. [arXiv:math.NT/0411214](https://arxiv.org/abs/math/0411214), 31 pages, 2004.
- [36] Samar Jaafar and Kamal Khuri-Makdisi. On the maps from  $X(4p)$  to  $X(4)$ . [arXiv:math/0702545](https://arxiv.org/abs/math/0702545), 11 pages, 2007.
- [37] Rafe Jones and Jeremy Rouse. Iterated endomorphisms of Abelian algebraic groups. [arXiv:0707.2384](https://arxiv.org/abs/0707.2384), 34 pages, 2007.
- [38] L. J. P. Kilford. Generating spaces of modular forms with  $\eta$ -quotients. *JP J. Algebra Number Theory Appl.*, 8(2):213–226, 2007.
- [39] L. J. P. Kilford. On mod  $p$  modular representations which are defined over  $F_p$ . *Glas. Mat. Ser. III*, 43(63)(1):1–6, 2008.
- [40] L. J. P. Kilford. On the slopes of the  $U_5$  operator acting on overconvergent modular forms. *J. Théor. Nombres Bordeaux*, 20(1):165–182, 2008.
- [41] L. J. P. Kilford. On the  $U_p$  operator acting on  $p$ -adic overconvergent modular forms when  $X_0(p)$  has genus 1. [arXiv:0810.4788](https://arxiv.org/abs/0810.4788), 10 pages, 2008.
- [42] L. J. P. Kilford and Gabor Wiese. On the failure of the Gorenstein property for Hecke algebras of prime weight. *Experiment. Math.*, 17(1):37–52, 2008.
- [43] Ingo Herbert Klöcker. *Modular Forms for the Orthogonal Group  $O(2, 5)$* . PhD thesis, 2005.
- [44] Elisavet Konstantinou and Kontogeorgis Aristides. Computing polynomials of the Ramanujan  $\mathfrak{t}_n$  class invariants. *Canad. Math. Bull.*, To appear, 12 pages, 2007.

- [45] Aristides Kontogeorgis and Yifan Yang. Automorphisms of hyperelliptic modular curves  $X_0(n)$  in positive characteristic. [arXiv:0811.0876](#), 20 pages, 2008.
- [46] A. Krieg. The graded ring of quaternionic modular forms of degree 2. *Math. Z.*, 251(4):929–942, 2005.
- [47] Dominic Lanphier. Combinatorics of Maass-Shimura operators. *J. Number Theory*, 128(8):2467–2487, 2008.
- [48] Joan-C. Lario and René Schoof. Some computations with Hecke rings and deformation rings. *Experiment. Math.*, 11(2):303–311, 2002.
- [49] Mark Lingham. *Modular Forms and Elliptic Curves over Imaginary Quartic Fields*. PhD Thesis, University of Nottingham, 2005.
- [50] Ling Long. On Atkin and Swinnerton-Dyer congruence relations. III. *J. Number Theory*, 128(8):2413–2429, 2008.
- [51] A. Marschner and J. Müller. On a certain algebra of higher modular forms. *Algebra Colloq.*, 16:371–380, 2009.
- [52] Barry Mazur, William Stein, and John Tate. Computation of  $p$ -adic heights and log convergence. *Doc. Math.*, (Extra Vol.):577–614 (electronic), 2006.
- [53] G. Nebe. Kneser-Hecke-operators in coding theory. *Abh. Math. Sem. Univ. Hamburg*, 76:79–90, 2006.
- [54] Gabriele Nebe. An analogue of Hecke-operators in coding theory. [arXiv:math.NT/05509474 v1](#), 15 pages, 2005.
- [55] Gabriele Nebe and Maria Teider. Hecke actions on certain strongly modular genera of lattices. *Arch. Math. (Basel)*, 84(1):46–56, 2005.
- [56] Ken Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and  $q$ -series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.
- [57] Manabu Oura, Cris Poor, and David S. Yuen. Towards the Siegel ring in genus four. *Int. J. Number Theory*, 4(4):563–586, 2008.

- [58] Ariel Pacetti and Fernando Rodriguez Villegas. Computing weight 2 modular forms of level  $p^2$ . *Math. Comp.*, 74(251):1545–1557 (electronic), 2005.
- [59] Kathleen L. Petersen. One-cusped congruence subgroups of Bianchi groups. *Math. Ann.*, 338(2):249–282, 2007.
- [60] Francesco Dalla Piazza and Bert van Geemen. Siegel modular forms and finite symplectic groups. [arXiv:0804.3769v2](https://arxiv.org/abs/0804.3769v2), 33 pages, 2008.
- [61] Robert Pollack. On the  $p$ -adic  $L$ -function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3):523–558, 2003.
- [62] Alexandru A. Popa. Central values of Rankin  $L$ -series over real quadratic fields. *Compos. Math.*, 142(4):811–866, 2006.
- [63] Jordi Quer. Fields of definition of building blocks. *Math. Comp.*, 78(265):537–554, 2009.
- [64] Jeremy Rouse. Bounds for the coefficients of powers of the Delta-function. *Bull. London Math. Soc.*, 40(6):1081–1090, 2008.
- [65] Emmanuel Royer. Evaluating convolution sums of the divisor function with quasimodular forms. *Int. J. Number Theory*, 3(2):231–261, 2007.
- [66] Michael M. Schein. Weights in Serre’s conjecture for Hilbert modular forms: the ramified case. *Israel J. Math.*, 166:369–391, 2008.
- [67] Mehmet Haluk Şengün. The nonexistence of certain representations of the absolute Galois group of quadratic fields. *Proc. Amer. Math. Soc.*, 137(1):27–35, 2009.
- [68] William Stein. *Modular Forms: A Computational Approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007.
- [69] William A. Stein. *Explicit Approaches to Modular Abelian Varieties*. PhD Thesis, University of California, Berkeley, 2000.
- [70] William A. Stein and Helena A. Verrill. Cuspidal modular symbols are transportable. *LMS J. Comput. Math.*, 4:170–181 (electronic), 2001.

- [71] Helena A. Verrill. Transportable modular symbols and the intersection pairing. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 219–233. Springer, Berlin, 2002.
- [72] John Voight. Computing fundamental domains for Fuchsian groups. [arXiv:math.NT/0802.0196v1](https://arxiv.org/abs/math/0802.0196v1), 16 pages, 2008.
- [73] Gabor Wiese. Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133 (electronic), 2004.
- [74] Gabor Wiese. *Modular Forms of Weight One over Finite Fields*. PhD Thesis, Universiteit Leiden, 2005.
- [75] Gabor Wiese. On the faithfulness of parabolic cohomology as a Hecke module over a finite field. *J. Reine Angew. Math.*, 606:79–103, 2007.
- [76] Gabor Wiese. On projective linear groups over finite fields as Galois groups over the rational numbers. In *Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006*, pages 343–350. Cambridge University Press, Cambridge, 2008.
- [77] Gabor Wiese. On modular symbols and the cohomology of Hecke triangle surfaces. *Int. J. Number Theory*, 5(1):89–108, 2009.
- [78] Dan Yasaki. Integral cohomology of certain Picard modular surfaces. [arXiv:0709.1121v1](https://arxiv.org/abs/0709.1121v1), 14 pages, 2007.
- [79] Dan Yasaki. Elliptic points of the Picard modular group. *Monatsh. Math.*, 156(4):391–396, 2009.

# Number Theory

## Arithmetic Algebraic Geometry

11Gxx

- [1] Amod Agashe, Kenneth Ribet, and William A. Stein. The Manin constant. *Pure Appl. Math. Q.*, 2(2):617–636, 2006.
- [2] Amod Agashe and William Stein. Visibility of Shafarevich-Tate groups of abelian varieties. *J. Number Theory*, 97(1):171–185, 2002.
- [3] Amod Agashe and William Stein. Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. *Math. Comp.*, 74(249):455–484 (electronic), 2005.
- [4] Scott Ahlgren and Matthew Papanikolas. Higher Weierstrass points on  $X_0(p)$ . *Trans. Amer. Math. Soc.*, 355(4):1521–1535 (electronic), 2003.
- [5] Avner Ash, Darrin Doud, and David Pollack. Galois representations with conjectural connections to arithmetic cohomology. *Duke Math. J.*, 112(3):521–579, 2002.
- [6] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.
- [7] Arthur Baragar and Ronald van Luijk.  $K3$  surfaces with Picard number three and canonical vector heights. *Math. Comp.*, 76(259):1493–1498 (electronic), 2007.
- [8] Mark Bauer, Edlyn Teske, and Annegret Weng. Point counting on Picard curves in large characteristic. *Math. Comp.*, 74(252):1983–2005 (electronic), 2005.
- [9] Tobias Berger and Krzysztof Klosin. A deformation problem for Galois representations over imaginary quadratic fields. *J. Inst. Math. Jussieu*, 8(4):669–692, 2009.
- [10] Amnon Besser and Rob De Jeu.  $\text{li}(p)$ -service? an algorithm for computing  $p$ -adic polyalgorithms. *Math. Comp.*, 77(262):1105–1134, 2008.

- [11] Peter Birkner. *Efficient Arithmetic on Low-genus Curves*. Ph D thesis, Technische Universiteit Eindhoven, 2009.
- [12] Nigel Boston and Rafe Jones. Arboreal Galois representations. *Geom. Dedicata*, 124:27–35, 2007.
- [13] M. J. Bright, N. Bruin, E. V. Flynn, and A. Logan. The Brauer-Manin obstruction and Sh[2]. *LMS J. Comput. Math.*, 10:354–377 (electronic), 2007.
- [14] David Brown. The Chabauty-Coleman bound at a prime of bad reduction. [arXiv:0803.0973v2 \[math.NT\]](#), 10 pages, 2008.
- [15] Ezra Brown and Bruce T. Myers. Elliptic curves from Mordell to Diophantus and back. *Amer. Math. Monthly*, 109(7):639–649, 2002.
- [16] N. Bruin and E. V. Flynn.  $n$ -covers of hyperelliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 134(3):397–405, 2003.
- [17] Nils Bruin. Visualising *Sha*[2] in abelian surfaces. *Math. Comp.*, 73(247):1459–1476 (electronic), 2004.
- [18] Nils Bruin. The arithmetic of Prym varieties in genus 3. *Compos. Math.*, 144(2):317–338, 2008.
- [19] Nils Bruin and Noam D. Elkies. Trinomials  $ax^7 + bx + c$  and  $ax^8 + bx + c$  with Galois groups of order 168 and  $8 \cdot 168$ . In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 172–188. Springer, Berlin, 2002.
- [20] Nils Bruin and E. Victor Flynn. Towers of 2-covers of hyperelliptic curves. *Trans. Amer. Math. Soc.*, 357(11):4329–4347 (electronic), 2005.
- [21] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.
- [22] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. [arXiv:0803.2052v1 \[math.NT\]](#), 19 pages, 2008.
- [23] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

- [24] Kevin Buzzard and L. J. P. Kilford. The 2-adic eigencurve at the boundary of weight space. *Compos. Math.*, 141(3):605–619, 2005.
- [25] Robert Carls. Theta null points of 2-adic canonical lifts. [arXiv:math.NT/0509092](#), 18 pages, 2005.
- [26] Robert Carls and David Lubicz. A  $p$ -adic quasi-quadratic time point counting algorithm. *Int. Math. Res. Not. IMRN*, (4):698–735, 2009.
- [27] Antoine Chambert-Loir. Compter (rapidement) le nombre de solutions d'équations dans les corps finis. [arXiv:math.NT/0611584](#), 46 pages, 2006.
- [28] Denis Charles and Kristin Lauter. Computing modular polynomials. *LMS J. Comput. Math.*, 8:195–204 (electronic), 2005.
- [29] Denis Xavier Charles. Complex multiplication tests for elliptic curves. [arXiv:math.NT/0409501 v1](#), 13 pages, 2004.
- [30] Imin Chen. On the equation  $s^2 + y^{2p} = \alpha^3$ . *Math. Comp.*, 77(262):1223–1227, 2008.
- [31] Imin Chen and Chris Cummins. Elliptic curves with nonsplit mod 11 representations. *Math. Comp.*, 73(246):869–880 (electronic), 2004.
- [32] Robert F. Coleman and William A. Stein. Approximation of eigenforms of infinite slope by eigenforms of finite slope. In *Geometric Aspects of Dwork Theory. Vol. I, II*, pages 437–449. Walter de Gruyter GmbH & Co. KG, Berlin, 2004.
- [33] B. Conrad, K. Conrad, and H. Helfgott. Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.
- [34] Brian Conrad, Bas Edixhoven, and William Stein.  $J_1(p)$  has connected fibers. *Doc. Math.*, 8:331–408 (electronic), 2003.
- [35] Caterina Consani and Jasper Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.
- [36] Patrick Kenneth Corn. *Del Pezzo Surfaces and the Brauer-Manin Obstruction*. PhD Thesis, University of California, Berkley, 1998.

- [37] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, Cambridge, second edition, 1997.
- [38] 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.
- [39] J. E. Cremona and M. P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.*, 16(3):303–312, 2007.
- [40] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.
- [41] John Cremona. The elliptic curve database for conductors to 130000. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 11–29. Springer, Berlin, 2006.
- [42] John Cremona, Tom Fisher, Cathy O’Neil, Denis Simon, and Michael Stoll. Explicit  $n$ -descent on elliptic curves II: Geometry. [arXiv:math.NT/0611606](https://arxiv.org/abs/math/0611606), 24 pages, 2006.
- [43] John E. Cremona. A solution for note 84.35. *The Mathematical Gazette*, 86(505):66–68, 2002.
- [44] John Cullinan. A computational approach to the 2-torsion structure of abelian threefolds. *Math. Comp.*, 78(267):1825–1836, 2009.
- [45] C. J. Cummins and S. Pauli. Congruence subgroups of  $\mathrm{PSL}(2, Z)$  of genus less than or equal to 24. *Experiment. Math.*, 12(2):243–255, 2003.
- [46] Samit Dasgupta. Computations of elliptic units for real quadratic fields. *Canad. J. Math.*, 59(3):553–574, 2007.
- [47] Chantal David and Tom Weston. Local torsion on elliptic curves and the deformation theory of Galois representations. *Math. Res. Lett.*, 15(3):599–611, 2008.
- [48] Lassina Dembélé. A non-solvable galois extension of  $q$  ramified at 2 only. *C. R., Math., Acad. Sci. Paris*, 347(3-4), 2009.

- [49] Jan Denef and Frederik Vercauteren. An extension of Kedlaya’s algorithm to Artin-Schreier curves in characteristic 2. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 308–323. Springer, Berlin, 2002.
- [50] Xavier Charles Denis. Complex multiplication tests for elliptic curves. *Preprint*, 13 pages, 2004.
- [51] Claus Diem and Emmanuel Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. *J. Cryptology*, 21(4):593–611, 2008.
- [52] T. Dokchitser and V. Dokchitser. Computations in non-commutative Iwasawa theory. *Proc. Lond. Math. Soc. (3)*, 94(1):211–272, 2007.
- [53] Tim Dokchitser and Vladimir Dokchitser. Root numbers of elliptic curves in residue characteristic 2. *Bull. Lond. Math. Soc.*, 40(3):516–524, 2008.
- [54] Darrin Doud. A procedure to calculate torsion of elliptic curves over  $\mathbf{Q}$ . *Manuscripta Math.*, 95(4):463–469, 1998.
- [55] Andrej Dujella. On Mordell-Weil groups of elliptic curves induced by Diophantine triples. *Glas. Mat. Ser. III*, 42(62)(1):3–18, 2007.
- [56] S. Duquesne. Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem. *Manuscripta Math.*, 108(2):191–204, 2002.
- [57] Sylvain Duquesne. Points rationnels et méthode de Chabauty elliptique. *J. Théor. Nombres Bordeaux*, 15(1):99–113, 2003.
- [58] Sylvain Duquesne. Elliptic curves associated with simplest quartic fields. *J. Théor. Nombres Bordeaux*, 19(1):81–100, 2007.
- [59] 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.
- [60] Bas Edixhoven. On the computation of the coefficients of a modular form. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 30–39. Springer, Berlin, 2006.

- [61] Kirsten Eisentraeger, Dimitar Jetchev, and Kristin Lauter. On the computation of the Cassels pairing for certain Kolyvagin classes in the Shafarevich-Tate group. *5209:113–125*, 2008.
- [62] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. [arXiv:math.NT/0405305v2](https://arxiv.org/abs/math.NT/0405305v2), 16 pages, 2007.
- [63] Noam D. Elkies. Three lectures on elliptic surfaces and curves of high rank. [arXiv:0709.2908v1](https://arxiv.org/abs/0709.2908v1), 14 pages, 2007.
- [64] Noam D. Elkies. Shimura curve computations via K3 surfaces of Neron-Severi rank at least 19. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 2008.
- [65] Noam D. Elkies and Mark Watkins. Elliptic curves of large rank and small conductor. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 42–56. Springer, Berlin, 2004.
- [66] Arsen Elkin. Hyperelliptic Jacobians with real multiplication. *J. Number Theory*, 117(1):53–86, 2006.
- [67] Andreas-Stephan Elsenhans and Jörg Jahnel. K3 surfaces of Picard rank one and degree two. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 212–225. Springer, 2008.
- [68] G. Everest and T. Ward. The canonical height of an algebraic point on an elliptic curve. *New York J. Math.*, 6:331–342 (electronic), 2000.
- [69] Graham Everest, Patrick Ingram, Valéry Mahé, and Shaun Stevens. The uniform primality conjecture for elliptic curves. *Acta Arith.*, 134(2):157–181, 2008.
- [70] Graham Everest, Patrick Ingram, and Shaun Stevens. Primitive divisors on twists of Fermat’s cubic. *LMS J. Comput. Math.*, 12:54–81, 2009.
- [71] Graham Everest and Valery Mahe. A generalization of Siegel’s theorem and Hall’s conjecture. *Exp. Math.*, 18(1):1–10, 2009.

- [72] Xander Faber and Benjamin Hutz. On the number of rational iterated pre-images of the origin under quadratic dynamical systems. [arXiv:0810.1715](#), 18 pages, 2008.
- [73] Reza Rezaeian Farashahi and Ruud Pellikaan. The quadratic extension extractor for (hyper)elliptic curves in odd characteristic. In *Arithmetic of finite fields*, volume 4547 of *Lecture Notes in Comput. Sci.*, pages 219–236. Springer, Berlin, 2007.
- [74] Julio Fernández, Josep González, and Joan-C. Lario. Plane quartic twists of  $X(5, 3)$ . *Canad. Math. Bull.*, 50(2):196–205, 2007.
- [75] Luís R. A. Finotti. Degrees of the elliptic Teichmüller lift. *J. Number Theory*, 95(2):123–141, 2002.
- [76] Luís R. A. Finotti. Minimal degree liftings of hyperelliptic curves. *J. Math. Sci. Univ. Tokyo*, 11(1):1–47, 2004.
- [77] Luís R. A. Finotti. Minimal degree liftings in characteristic 2. *J. Pure Appl. Algebra*, 207(3):631–673, 2006.
- [78] Tom Fisher. The Hessian of a genus one curve. [arXiv:math.NT/0610403](#), 28 pages, 2006.
- [79] Tom Fisher. Testing equivalence of ternary cubics. In *Algorithmic Number Theory (Berlin, 2006)*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 333–345. Springer, Berlin, 2006.
- [80] Tom Fisher. A new approach to minimising binary quartics and ternary cubics. *Math. Res. Lett.*, 14(4):597–613, 2007.
- [81] Tom Fisher. The invariants of a genus one curve. *Proc. Lond. Math. Soc. (3)*, 97(3):753–782, 2008.
- [82] E. V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115(4):437–466, 2004.
- [83] 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.

- [84] E. V. Flynn and J. Wunderle. Cycles of covers. *Monatsh. Math.*, Online first:16, 2008.
- [85] David Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 60–73. Springer, 2008.
- [86] S. D. Galbraith, J. F. McKee, and P. C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields Appl.*, 13(4):800–814, 2007.
- [87] Steven D. Galbraith. Weil descent of Jacobians. *Discrete Appl. Math.*, 128(1):165–180, 2003.
- [88] P. Gaudry and É. Schost. Modular equations for hyperelliptic curves. *Math. Comp.*, 74(249):429–454 (electronic), 2005.
- [89] Pierrick Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. *Preprint*, 13 pages, 2004.
- [90] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya’s point-counting algorithm to superelliptic curves. In *Advances in Cryptology—Asiacrypt 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.
- [91] Pierrick Gaudry and Robert Harley. Counting points on hyperelliptic curves over finite fields. In *Algorithmic Number Theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 313–332. Springer, Berlin, 2000.
- [92] Eknath Ghate, Enrique González-Jiménez, and Jordi Quer. On the Brauer class of modular endomorphism algebras. *Int. Math. Res. Not.*, (12):701–723, 2005.
- [93] Jean Gillibert. Invariants de classes: exemples de non-annulation en dimension supérieure. *Math. Ann.*, 338(2):475–495, 2007.
- [94] Edray Goins. Explicit descent via 4-isogeny on an elliptic curve. [arXiv:math.NT/0411215](https://arxiv.org/abs/math.NT/0411215) v1, 20 pages, 2004.

- [95] Josep González and Jordi Guàrdia. Genus two curves with quaternionic multiplication and modular Jacobian. *Math. Comp.*, 78(265):575–589, 2009.
- [96] Josep González, Jordi Guàrdia, and Victor Rotger. Abelian surfaces of  $GL_2$ -type as Jacobians of curves. *Acta Arith.*, 116(3):263–287, 2005.
- [97] Josep González and Victor Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.
- [98] Enrique González-Jiménez, Josep González, and Jordi Guàrdia. Computations on modular Jacobian surfaces. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 189–197. Springer, Berlin, 2002.
- [99] Eyal Z. Goren and Kristin E. Lauter. The distance between superspecial abelian varieties with real multiplication. *J. Number Theory*, 129(6):1562–1578, 2009.
- [100] Matthew Greenberg. Computing Heegner points arising from Shimura curve parametrizations. *Preprint*, 11 pages, 2006.
- [101] Matthew Greenberg. Heegner point computations via numerical  $p$ -adic integration. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 361–376. Springer Berlin / Heidelberg, 2006.
- [102] Matthew Greenberg. *Heegner Points and Rigid Analytic Modular Forms*. PhD Thesis, McGill University, 2006.
- [103] Grigor Grigorov, Andrei Jorza, Stephan Patrikis, William A. Stein, and Corina Tarnita-Patrascu. Verification of the Birch and Swinnerton-Dyer conjecture for specific elliptic curves. *Preprint*, 26 pages.
- [104] Jordi Guàrdia. Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves. *Ann. Inst. Fourier (Grenoble)*, 57(4):1253–1283, 2007.
- [105] Brian Hansen. *Explicit computations supporting a generalization of Serre’s conjecture*. Master of Science thesis, Brigham Young University, 2005.

- [106] Robin Hartshorne and Ronald van Luijk. Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on  $K3$  surfaces. *Math. Intelligencer*, 30(4):4–10, 2008.
- [107] Ki-ichiro Hashimoto, Katsuya Miyake, and Hiroaki Nakamura, editors. *Galois Theory and Modular Forms*, volume 11 of *Developments in Mathematics*, Boston, MA, 2004. Kluwer Academic Publishers.
- [108] Florian Hess. Computing relations in divisor class groups of algebraic curves over finite fields. *Preprint*, 2003.
- [109] Florian Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math. (Basel)*, 82(1):28–32, 2004.
- [110] Laura Hitt. Families of genus 2 curves with small embedding degree. *J. Math. Cryptol.*, 3(1):19–36, 2009.
- [111] E. W. Howe and K. E. Lauter. Improved upper bounds for the number of points on curves over finite fields. *Ann. Inst. Fourier (Grenoble)*, 53(6):1677–1737, 2003.
- [112] Everett W. Howe. Infinite families of pairs of curves over  $Q$  with isomorphic Jacobians. *J. London Math. Soc. (2)*, 72(2):327–350, 2005.
- [113] Everett W. Howe. Supersingular genus-2 curves over fields of characteristic 3. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 49–69. Amer. Math. Soc., Providence, RI, 2008.
- [114] Everett W. Howe, Kristin E. Lauter, and Jaap Top. Pointless curves of genus three and four. In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 125–141. Soc. Math. France, Paris, 2005.
- [115] Everett W. Howe and Hui June Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory*, 92(1):139–163, 2002.
- [116] Hendrik Hubrechts. Point counting in families of hyperelliptic curves. *Found. Comput. Math.*, 8(1):137–169, 2008.
- [117] Hendrik Hubrechts. Quasi-quadratic elliptic curve point counting using rigid cohomology. *J. Symb. Comput.*, 44(9):1255–1267, 2009.

- [118] Klaus Hulek and Helena Verrill. On modularity of rigid and nonrigid Calabi-Yau varieties associated to the root lattice  $A_4$ . *Nagoya Math. J.*, 179:103–146, 2005.
- [119] Klaus Hulek and Helena A. Verrill. On the motive of Kummer varieties associated to  $\Gamma_1(7)$ — Supplement to the paper: “The modularity of certain non-rigid Calabi-Yau threefolds” by R. Livné and N. Yui. *J. Math. Kyoto Univ.*, 45(4):667–681, 2005.
- [120] Patrick Ingram. Multiples of integral points on elliptic curves. *Journal of Number Theory*, 129(1):182 – 208, 2009.
- [121] Farzali A. Izadi and V. Kumar Murty. Counting points on an abelian variety over a finite field. In *Progress in Cryptology—Indocrypt 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, pages 323–333. Springer, Berlin, 2003.
- [122] Dimitar Jetchev, Kristin Lauter, and William Stein. Explicit Heegner points: Kolyvagin’s conjecture and non-trivial elements in the Shafarevich-Tate group. *Journal of Number Theory*, 129(2):284 – 302, 2009.
- [123] Dimitar P. Jetchev and William A. Stein. Visibility of the Shafarevich-Tate group at higher level. *Doc. Math.*, 12:673–696, 2007.
- [124] Jorge Jimenez-Urroz and Tonghai Yang. Heegner zeros of theta functions. *Trans. Amer. Math. Soc.*, 355(10):4137–4149 (electronic), 2003.
- [125] David Joyner and Amy Ksir. Modular representations on some Riemann-Roch spaces of modular curves  $X(N)$ . In *Computational Aspects of Algebraic Curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 163–205. World Sci. Publ., Hackensack, NJ, 2005.
- [126] Koray Karabina and Edlyn Teske. On prime-order elliptic curves with embedding degrees  $k=3,4$ , and 6. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2008.
- [127] L. J. P. Kilford. Some non-Gorenstein Hecke algebras attached to spaces of modular forms. *J. Number Theory*, 97(1):157–164, 2002.

- [128] L. J. P. Kilford. Slopes of 2-adic overconvergent modular forms with small level. *Math. Res. Lett.*, 11(5-6):723–739, 2004.
- [129] L. J. P. Kilford. On a  $p$ -adic extension of the Jacquet-Langlands correspondence to weight 1. [arXiv:0809.1048v1 \[math.NT\]](#), 17 pages, 2008.
- [130] David R. Kohel. Hecke module structure of quaternions. In *Class Field Theory—Its Centenary and Prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 177–195. Math. Soc. Japan, Tokyo, 2001.
- [131] David R. Kohel. The AGM- $X_0(N)$  Heegner point lifting algorithm and elliptic curve point counting. In *Advances in Cryptology—Asiacrypt 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 124–136. Springer, Berlin, 2003.
- [132] David R. Kohel and William A. Stein. Component groups of quotients of  $J_0(N)$ . In *Algorithmic Number Theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 405–412. Springer, Berlin, 2000.
- [133] David R. Kohel and Helena A. Verrill. Fundamental domains for Shimura curves. *J. Théor. Nombres Bordeaux*, 15(1):205–222, 2003.
- [134] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.
- [135] Elisavet Konstantinou and Kontogeorgis Aristides. Computing polynomials of the Ramanujan  $\mathfrak{t}_n$  class invariants. *Canad. Math. Bull.*, To appear, 12 pages, 2007.
- [136] Aristides Kontogeorgis and Victor Rotger. On the non-existence of exceptional automorphisms on Shimura curves. *Bull. Lond. Math. Soc.*, 40(3):363–374, 2008.
- [137] Andrew Kresch and Yuri Tschinkel. Integral points on punctured abelian surfaces. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 198–204. Springer, Berlin, 2002.

- [138] L. Kulesz, G. Matera, and É. Schost. Uniform bounds on the number of rational points of a family of curves of genus 2. *J. Number Theory*, 108(2):241–267, 2004.
- [139] Dominic Lanphier. The trace of special values of modular  $L$ -functions. *Preprint*, 18 pages.
- [140] Alan G. B. Lauder. Ranks of elliptic curves over function fields. *LMS J. Comput. Math.*, 11:172–212, 2008.
- [141] F. Leprévost, M. Pohst, and A. Schöpp. Rational torsion of  $J_0(N)$  for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10. *Abh. Math. Sem. Univ. Hamburg*, 74:193–203, 2004.
- [142] Franck Leprévost, Michael Pohst, and Andreas Schöpp. Familles de polynômes liées aux courbes modulaires  $X(l)$  unicursales et points rationnels non-triviaux de courbes elliptiques quotient. *Acta Arith.*, 110(4):401–410, 2003.
- [143] Reynald Lercier and David Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. *The Ramanujan Journal*, 12(3):399–423, 2006.
- [144] 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.
- [145] David Loeffler. Explicit calculations of automorphic forms for definite unitary groups. *LMS J. Comput. Math.*, 11:326–342, 2008.
- [146] Adam Logan and Ronald van Luijk. Nontrivial elements of Sha explained through  $K3$  surfaces. *Math. Comp.*, 78(265):441–483, 2009.
- [147] Ling Long and Chris Kurth. On modular forms for some noncongruence subgroups of  $SL_2\mathbb{Z}$  II. [arXiv:0809.0020v1](https://arxiv.org/abs/0809.0020v1) [[math.NT](https://arxiv.org/abs/0809.0020v1)], 13 pages, 2008.
- [148] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Coleman-Chabauty. [arXiv:math.NT/0005186](https://arxiv.org/abs/math.NT/0005186), 30 pages, 2000.

- [149] Kazuo Matsuno. Construction of elliptic curves with large Iwasawa  $\lambda$ -invariants and large Tate-Shafarevich groups. *Manuscripta Math.*, 122(3):289–304, 2007.
- [150] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 461–474. Springer, Berlin, 2002.
- [151] J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the  $l$ -power torsion of an elliptic curve over a finite field. *Math. Comp.*, 78(267):1767–1786, 2009.
- [152] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of  $l$ -isogenies of elliptic curves over finite fields. *Appl. Math. Comput.*, 196(1):67–76, 2008.
- [153] Annika Niehage. *Quantum Goppa Codes over Hyperelliptic Curves*. Diplomarbeit, Universität Mannheim, 2004.
- [154] Mihran Papikian. On the variation of Tate-Shafarevich groups of elliptic curves over hyperelliptic curves. *J. Number Theory*, 115(2):249–283, 2005.
- [155] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques à réduction supersingulière en  $p$ . *Experiment. Math.*, 12(2):155–186, 2003.
- [156] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic Number Theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 283–306. Springer, Berlin, 1996.
- [157] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$ . *Duke Math. J.*, 137(1):103–158, 2007.
- [158] Lisa Marie Redekop. *Torsion Points of Low Order on Elliptic Curves and Drinfeld Modules*. PhD thesis, 2002.

- [159] Guillaume Ricotta and Thomas Vidick. Hauteur asymptotique des points de Heegner. *Canad. J. Math.*, 60(6):1406–1436, 2008.
- [160] Christophe Ritzenthaler. Automorphismes des courbes modulaires  $X(n)$  en caractéristique  $p$ . *Manuscripta Math.*, 109(1):49–62, 2002.
- [161] Christophe Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 379–394. Springer, Berlin, 2004.
- [162] David Savitt. The maximum number of points on a curve of genus 4 over  $F_8$  is 25. *Canad. J. Math.*, 55(2):331–352, 2003.
- [163] Edward F. Schaefer and Michael Stoll. How to do a  $p$ -descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231 (electronic), 2004.
- [164] Jasper Scholten. Weil restriction of an elliptic curve over a quadratic extension. *Preprint*, 6 pages, 2004.
- [165] Andreas M. Schöpp. *Über Torsionspunkte elliptischer und hyperelliptischer Kurven nebst Anwendungen*. PhD thesis, Technische Universität Berlin,, April 2005.
- [166] Samir Siksek. On standardized models of isogenous elliptic curves. *Math. Comp.*, 74(250):949–951 (electronic), 2005.
- [167] Samir Siksek and John E. Cremona. On the Diophantine equation  $x^2 + 7 = y^m$ . *Acta Arith.*, 109(2):143–149, 2003.
- [168] 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.
- [169] Sebastian Karl Michael Stamminger. *Explicit 8-Descent on Elliptic Curves*. PhD thesis, International University Bremen, 2005.
- [170] William Stein. Studying the Birch and Swinnerton-Dyer conjecture for modular abelian varieties using Magma. In *Discovering Mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 93–116. Springer, Berlin, 2006.

- [171] William A. Stein. There are genus one curves over  $Q$  of every odd index. *J. Reine Angew. Math.*, 547:139–147, 2002.
- [172] William A. Stein. Shafarevich-Tate groups of nonsquare order. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 277–289. Birkhäuser, Basel, 2004.
- [173] William A. Stein. Visibility of Mordell-Weil groups. *Doc. Math.*, 12:587–606, 2007.
- [174] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.
- [175] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.
- [176] Michael Stoll. Rational 6-cycles under iteration of quadratic polynomials. *LMS J. Comput. Math.*, 11:367–380, 2008.
- [177] Thotsaphon Thongjunthug. Computing a lower bound for the canonical height on elliptic curves over totally real number fields. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 139–152. Springer, 2008.
- [178] 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.
- [179] Marie-France Vignéras.  $p$ -adic integral structures of some representations of  $GL(2, F)$ . *Preprint*, 23 pages, 2005.
- [180] Bogdan G. Vioreanu. Mordell-Weil problem for cubic surfaces, numerical evidence. [arXiv:0802.0742v1](https://arxiv.org/abs/0802.0742v1) [[math.AG](https://arxiv.org/abs/0802.0742v1)], 22 pages, 2008.
- [181] Mark Watkins. A note on integral points on elliptic curves. *J. Théor. Nombres Bordeaux*, 18(3):707–720, 2006.
- [182] Mark Watkins. Some remarks on Heegner point computations. [arXiv:math.NT/0506325](https://arxiv.org/abs/math.NT/0506325), 14 pages, 2006.

- [183] Mark Watkins. Some heuristics about elliptic curves. *Experiment. Math.*, 17(1):105–125, 2008.
- [184] Rolf Stefan Wilke. On rational embeddings of curves in the second Garcia-Stichtenoth tower. *Finite Fields Appl.*, 14(2):494–504, 2008.
- [185] Christian Wuthrich. The fine Tate-Shafarevich group. *Math. Proc. Cambridge Philos. Soc.*, 142(1):1–12, 2007.
- [186] Chaoping Xing. Applications of algebraic curves to constructions of sequences. In *Cryptography and Computational Number Theory (Singapore, 1999)*, volume 20 of *Progr. Comput. Sci. Appl. Logic*, pages 137–146. Birkhäuser, Basel, 2001.
- [187] Chaoping Xing and Sze Ling Yeo. Construction of global function fields from linear codes and vice versa. *Trans. Amer. Math. Soc.*, 361(3):1333–1349, 2008.
- [188] Huilin Zhu and Jianhua Chen. Integral points on a class of elliptic curve. *Wuhan Univ. J. Nat. Sci.*, 11(3):477–480, 2006.

# Number Theory

## Geometry of Numbers

11Hxx

- [1] Kanat Abdukhalikov. Unimodular Hermitian lattices. *Mathematisches Forschungsinstitut Oberwolfach Report No. 1/2005*, pages 27–30, 2005.
- [2] Kanat Abdukhalikov and Rudolf Scharlau. Unimodular lattices in dimensions 14 and 15 over the Eisenstein integers. *Math. Comp.*, 78(265):387–403, 2009.
- [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 Computer Science*, pages 293–305. Springer, 2008.
- [4] Christine Bachoc and Gabriele Nebe. Classification of two genera of 32-dimensional lattices of rank 8 over the Hurwitz order. *Experiment. Math.*, 6(2):151–162, 1997.
- [5] Christine Bachoc and Boris Venkov. Modular forms, lattices and spherical designs. In *Réseaux Euclidiens, Designs Sphériques et Formes Modulaires*, volume 37 of *Monogr. Enseign. Math.*, pages 87–111. Enseignement Math., Geneva, 2001.
- [6] Werner Backes and Susanne Wetzels. Heuristics on lattice basis reduction in practice. *ACM J. Exp. Algorithmics*, 7:21 pp. (electronic), 2002.
- [7] Robin Chapman, Steven T. Dougherty, Philippe Gaborit, and Patrick Solé. 2-modular lattices from ternary codes. *J. Théor. Nombres Bordeaux*, 14(1):73–85, 2002.
- [8] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999.

- [9] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin. A generalization of Voronoi's reduction theory and its application. *Duke Math. J.*, 142(1):127–164, 2008.
- [10] C. Fieker and M. E. Pohst. On lattices over number fields. In *Algorithmic Number Theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 133–139. Springer, Berlin, 1996.
- [11] Philippe Gaborit. Construction of new extremal unimodular lattices. *European J. Combin.*, 25(4):549–564, 2004.
- [12] Masaaki Harada. On the existence of frames of the Niemeier lattices and self-dual codes over  $\mathbb{F}_p$ . *J. Algebra*, 321(8):2345–2352, 2009.
- [13] Masaaki Harada, Masaaki Kitazume, and Michio Ozeki. Ternary code construction of unimodular lattices and self-dual codes over  $\mathbb{Z}_6$ . *J. Algebraic Combin.*, 16(2):209–223, 2002.
- [14] Boris Hemkemeier. Algorithmische konstruktionen von gittern. [arXiv:math.MG/0411134](https://arxiv.org/abs/math/0411134), 64 pages, 2004.
- [15] G. Nebe. Kneser-Hecke-operators in coding theory. *Abh. Math. Sem. Univ. Hamburg*, 76:79–90, 2006.
- [16] Gabriele Nebe. Finite quaternionic matrix groups. *Represent. Theory*, 2:106–223 (electronic), 1998.
- [17] Gabriele Nebe. Even lattices with covering radius  $< \sqrt{2}$ . *Beiträge Algebra Geom.*, 44(1):229–234, 2003.
- [18] Gabriele Nebe. Strongly modular lattices with long shadow. *J. Théor. Nombres Bordeaux*, 16(1):187–196, 2004.
- [19] Gabriele Nebe and Kristina Schindelar.  $S$ -extremal strongly modular lattices. *J. Théor. Nombres Bordeaux*, 19(3):683–701, 2007.
- [20] Gabriele Nebe and Boris Venkov. The strongly perfect lattices of dimension 10. *J. Théor. Nombres Bordeaux*, 12(2):503–518, 2000.
- [21] Gabriele Nebe and Boris Venkov. Low-dimensional strongly perfect lattices I: The 12-dimensional case. *Enseign. Math. (2)*, 51(1-2):129–163, 2005.

- [22] Gabriele Nebe and Boris Venkov. Low dimensional strongly perfect lattices III: Dual strongly perfect lattices of dimension 14. [arXiv:0809.0593v1 \[math.NT\]](#), 33 pages, 2008.
- [23] Gabriele Nebe and Chaoping Xing. A Gilbert-Varshamov type bound for Euclidean packings. *Math. Comp.*, 77(264):2339–2344, 2008.
- [24] Phong Q. Nguên and Damien Stehlé. Floating-point LLL revisited. In *Advances in Cryptology - Eurocrypt 2005*, Lecture Notes in Computer Science, pages 215–233. Springer Berlin/Heidelberg, 2005.
- [25] Phong Q. Nguyen and Damien Stehlé. LLL on the average. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 238–256. Springer, Berlin, 2006.
- [26] W. Plesken and M. Pohst. Constructing integral lattices with prescribed minimum. I. *Math. Comp.*, 45(171):209–221, S5–S16, 1985.
- [27] E. M. Rains and N. J. A. Sloane. The shadow theory of modular and unimodular lattices. *J. Number Theory*, 73(2):359–389, 1998.
- [28] Achill Schürmann. Perfect, strongly eutactic lattices are periodic extreme. [arXiv:0808.2013v1 \[math.MG\]](#), 18 pages, 2008.
- [29] Achill Schürmann and Frank Vallentin. Local covering optimality of lattices: Leech lattice versus root lattice  $E_8$ . *Int. Math. Res. Not.*, (32):1937–1955, 2005.
- [30] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin. Classification of eight-dimensional perfect forms. *Electron. Res. Announc. Amer. Math. Soc.*, 13:21–32 (electronic), 2007.
- [31] N. J. A. Sloane, R. H. Hardin, T. D. S. Duff, and J. H. Conway. Minimal-energy clusters of hard spheres. *Discrete Comput. Geom.*, 14(3):237–259, 1995.
- [32] Dan Yasaki. Binary Hermitian forms over a cyclotomic field. *J. Algebra*, In Press, 2009.

# Number Theory

## Probabilistic Theory

11Kxx

- [1] Wieb Bosma, Karma Dajani, and Cor Kraaikamp. Entropy quotients and correct digits in number-theoretic expansions. In *Dynamics and Stochastics*, volume 48 of *IMS Lecture Notes Monogr. Ser.*, pages 176–188. Inst. Math. Statist., Beachwood, OH, 2006.

# Number Theory

## Zeta and $L$ -functions: Analytic Theory

11Mxx

- [1] P. Borwein, G. Fee, R. Ferguson, and A. van der Waall. Zeros of partial sums of the Riemann zeta function. *Experiment. Math.*, 16(1):21–39, 2007.
- [2] B. Conrad, K. Conrad, and H. Helfgott. Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.
- [3] M. P. F. du Sautoy, J. J. McDermott, and G. C. Smith. Zeta functions of crystallographic groups and analytic continuation. *Proc. London Math. Soc. (3)*, 79(3):511–534, 1999.
- [4] Marcus du Sautoy and Luke Woodward. Nilpotent groups: Explicit examples. In *Zeta Functions of Groups and Rings*, volume 1925/2008 of *Lecture Notes in Computer Science*, pages 21–68. Springer Berlin / Heidelberg, 2008.
- [5] Ralf Gerkmann. Relative rigid cohomology and deformation of hypersurfaces. *Int. Math. Res. Pap. IMRP*, (1):Art. ID rpm003, 67, 2007.
- [6] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 312–326. 2008.
- [7] Emmanuel Kowalski. The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros. *Int. Math. Res. Not. IMRN*, pages Art. ID rnn 091, 57, 2008.
- [8] Alan G. B. Lauder. A recursive method for computing zeta functions of varieties. *LMS J. Comput. Math.*, 9:222–269 (electronic), 2006.
- [9] Phil Martin and Mark Watkins. Symmetric powers of elliptic curve  $L$ -functions. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 377–392. Springer, Berlin, 2006.

- [10] Christopher Voll. Normal subgroup growth in free class-2-nilpotent groups. *Math. Ann.*, 332(1):67–79, 2005.

# Number Theory

## Multiplicative Number Theory

11Nxx

- [1] 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.
- [2] H. Dubner, T. Forbes, N. Lygeros, M. Mizony, H. Nelson, and P. Zimmermann. Ten consecutive primes in arithmetic progression. *Math. Comp.*, 71(239):1323–1328 (electronic), 2002.

# Number Theory

## Algebraic Number Theory

*11Rxx and 11Sxx*

- [1] Laurent Bartholdi and Michael R. Bush. Maximal unramified 3-extensions of imaginary quadratic fields and  $\mathrm{SL}_2(\mathbb{Z}_3)$ . *J. Number Theory*, 124(1):159–166, 2007.
- [2] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald. The absolute Galois group acts faithfully on the connected components of the moduli space of surfaces of general type. [arXiv:0706.1466v1](#) [[math.AG](#)], 13 pages, 2007.
- [3] 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.
- [4] Amnon Besser and Rob De Jeu.  $\mathrm{li}(p)$ -service? an algorithm for computing  $p$ -adic polyalgorithms. *Math. Comp.*, 77(262):1105–1134, 2008.
- [5] Wieb Bosma. Computation of cyclotomic polynomials with Magma. In *Computational Algebra and Number Theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 213–225. Kluwer Acad. Publ., Dordrecht, 1995.
- [6] 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.
- [7] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2-class groups. *J. Théor. Nombres Bordeaux*, 8(2):283–313, 1996.
- [8] Nigel Boston. Galois  $p$ -groups unramified at  $p$ —a survey. In *Primes and knots*, volume 416 of *Contemp. Math.*, pages 31–40. Amer. Math. Soc., Providence, RI, 2006.
- [9] Nigel Boston. Galois groups of tamely ramified  $p$ -extensions. *J. Théor. Nombres Bordeaux*, 19(1):59–70, 2007.

- [10] Nigel Boston and Rafe Jones. Arboreal Galois representations. *Geom. Dedicata*, 124:27–35, 2007.
- [11] Nigel Boston and Charles Leedham-Green. Counterexamples to a conjecture of Lemmermeyer. *Arch. Math. (Basel)*, 72(3):177–179, 1999.
- [12] M. R. Bush. Computation of Galois groups associated to the 2-class towers of some quadratic fields. *J. Number Theory*, 100(2):313–325, 2003.
- [13] H. Cohen, F. Diaz y Diaz, and M. Olivier. Subexponential algorithms for class group and unit computations. *J. Symbolic Comput.*, 24(3-4):433–441, 1997.
- [14] Henri Cohen. A survey of computational class field theory. *J. Théor. Nombres Bordeaux*, 11(1):1–13, 1999.
- [15] B. de Smit and H. W. Lenstra, Jr. Linearly equivalent actions of solvable groups. *J. Algebra*, 228(1):270–285, 2000.
- [16] Bart de Smit. On arithmetically equivalent fields with distinct  $p$ -class numbers. *J. Algebra*, 272(2):417–424, 2004.
- [17] Darrin Doud. Supersingular Galois representations and a generalization of a conjecture of Serre. *Experiment. Math.*, 16, 119–128 pages, 2007.
- [18] Kirsten Eisenträger and Kristin Lauter. Computing Igusa class polynomials via the chinese remainder theory. [arXiv:math.NT/04053505 v1](https://arxiv.org/abs/math.NT/04053505), 2004.
- [19] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.
- [20] 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.
- [21] Claus Fieker. Sparse representation for cyclotomic fields. *Experiment. Math.*, 16(4):493–500, 2007.

- [22] Claus Fieker. Minimizing representations over number fields ii: Computations in the Brauer group. *J. Algebra*, 322(3):752–765, 2009.
- [23] Claus Fieker and Michael E. Pohst. Dependency of units in number fields. *Math. Comp.*, 75(255):1507–1518 (electronic), 2006.
- [24] Claus Fieker and Michael E. Pohst. A lower regulator bound for number fields. *J. Number Theory*, 128(10):2767–2775, 2008.
- [25] Felix Fontein. The infrastructure of a global field of arbitrary unit rank. [arXiv:0809.1685](#), 36 pages, 2008.
- [26] David Ford, Sebastian Pauli, and Xavier-François Roblot. A fast algorithm for polynomial factorization over  $Q_p$ . *J. Théor. Nombres Bordeaux*, 14(1):151–169, 2002.
- [27] Robert Fraatz. On the computation of integral closures of cyclic extensions of function fields. *LMS J. Comput. Math.*, 10:141–160 (electronic), 2007.
- [28] S. P. Glasby. Generators for the group of units of  $Z_n$ . *Austral. Math. Soc. Gaz.*, 22(5):226–228, 1995.
- [29] Norbert Goeb. Computing the automorphism groups of hyperelliptic function fields. [arXiv:math.NT/0305284](#), 16 pages, 2003.
- [30] Sherry Gong. On a problem regarding coefficients of cyclotomic polynomials. *J. Number Theory*, In Press, 2009.
- [31] 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 \[math.NT\]](#), 24 pages, 2008.
- [32] Emmanuel Hallouin and Christian Maire. Cancellation in totally definite quaternion algebras. *J. Reine Angew. Math.*, 595:189–213, 2006.
- [33] Emmanuel Hallouin and Marc Perret. On the kernel of the norm in some unramified number fields extensions. [arXiv:0706.0417](#), 6 pages, 2007.
- [34] Stephan Hell. *Die Nenner des Kontsevich-Integrals und ein spezieller Drinfeld-Assoziator*. PhD thesis, Freie Universität Berlin, July 2002.

- [35] F. Hess. An algorithm for computing isomorphisms of algebraic function fields. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 263–271. Springer, Berlin, 2004.
- [36] Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548 (electronic), 2003.
- [37] David Hubbard. Dihedral side extensions and class groups. *J. Number Theory*, 128(4):731–737, 2008.
- [38] Jean-François Jaulent, Sebastian Pauli, Michael E. Pohst, and Florence Soriano-Gafiuk. Computation of 2-groups of narrow logarithmic divisor classes of number fields. *Journal of Symbolic Computation*, To appear, 2008.
- [39] 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.
- [40] Henri Johnston. On the trace map between absolutely abelian number fields of equal conductor. *Acta Arith.*, 122(1):63–74, 2006.
- [41] John W. Jones and David P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80–97, 2006.
- [42] John Jossey. Galois 2-extensions unramified outside 2. *J. Number Theory*, 124(1):42–56, 2007.
- [43] Masanari Kida. Kummer theory for norm algebraic tori. *J. Algebra*, 293(2):427–447, 2005.
- [44] Masanari Kida, Yuichi Rikuna, and Atsushi Sato. Classifying Brumer’s quintic polynomials by weak Mordell-Weil groups. [arXiv:math.NT/0802.0054v1](https://arxiv.org/abs/math.NT/0802.0054v1), 10 pages, 2008.
- [45] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.
- [46] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and Picard groups of orders. *J. Algebra*, 292(1):47–64, 2005.

- [47] M. Künzer and H. Weber. Some additive Galois cohomology rings. *Comm. Algebra*, 33(12):4415–4455, 2005.
- [48] Matthias Künzer and Eduard Wirsing. On coefficient valuations of Eisenstein polynomials. *J. Théor. Nombres Bordeaux*, 17(3):801–823, 2005.
- [49] Thorsten Lagemann. *Codes und Automorphismen optimaler Artin-Schreier-Turme*. PhD thesis, Ruprecht-Karls-Universität Heidelberg, April 2006.
- [50] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Experiment. Math.*, 12(2):211–225, 2003.
- [51] Franck Leprévost, Michael Pohst, and Andreas Schöpp. Units in some parametric families of quartic fields. *Acta Arith.*, 127(3):205–216, 2007.
- [52] Aaron Levin. Ideal class groups and torsion in Picard groups of varieties. arXiv:0805.1361v1 [math.NT], 31 pages, 2008.
- [53] Melissa L. Macasieb. Derived arithmetic Fuchsian groups of genus two. *Experiment. Math.*, 17(3):347–369, 2008.
- [54] Kazuo Matsuno. Construction of elliptic curves with large Iwasawa  $\lambda$ -invariants and large Tate-Shafarevich groups. *Manuscripta Math.*, 122(3):289–304, 2007.
- [55] William G. McCallum and Romyar T. Sharifi. A cup product in the Galois cohomology of number fields. *Duke Math. J.*, 120(2):269–310, 2003.
- [56] 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.
- [57] Sebastian Pauli. *Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant*. PhD thesis, Concordia University, June 2001.
- [58] Sebastian Pauli. Constructing class fields over local fields. *J. Théor. Nombres Bordeaux*, 18(3):627–652, 2006.

- [59] Sebastian Pauli and Florence Soriano-Gafiuk. The discrete logarithm in logarithmic  $l$ -class groups and its applications in  $K$ -theory. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 367–378. Springer, Berlin, 2004.
- [60] René Schoof. Arakelov class groups and ideal lattices. *Mathematisches Forschungsinstitut Oberwolfach Report No. 1/2005*, pages 23–24, 2005.
- [61] 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.
- [62] Andreas M. Schöpp. Fundamental units in a parametric family of not totally real quintic number fields. *J. Théor. Nombres Bordeaux*, 18(3):693–706, 2006.
- [63] Romyar T. Sharifi. Iwasawa theory and the Eisenstein ideal. *Duke Math. J.*, 137(1):63–101, 2007.
- [64] Romyar T. Sharifi. On Galois groups of unramified pro- $p$  extensions. *Math. Ann.*, 342(2):297–308, 2008.
- [65] William Stein and Yan Zhang. On power bases in number fields. *Preprint*, 15 pages, 2005.
- [66] Aliza Steurer. On the Galois groups of the 2-class towers of some imaginary quadratic fields. *J. Number Theory*, 125(1):235–246, 2007.
- [67] Mark van Hoeij and John Cremona. Solving conics over function fields. *J. Théor. Nombres Bordeaux*, 18(3):595–606, 2006.
- [68] John Voight. The gauss higher relative class number problem. *Ann. Sci. Math. Québec*, Accepted, 10 pages, 2009.
- [69] Gabor Wiese. On projective linear groups over finite fields as Galois groups over the rational numbers. In *Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006*, pages 343–350. Cambridge University Press, Cambridge, 2008.

- [70] Qingquan Wu and Renate Scheidler. An explicit treatment of bi-quadratic function fields. *Contrib. Discrete Math.*, 2(1):43–60 (electronic), 2007.

# Number Theory

## Finite Fields

11Txx

- [1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang. A trace conjecture and flag-transitive affine planes. *J. Combin. Theory Ser. A*, 95(1):158–168, 2001.
- [2] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O’Keefe. Permutations amongst the Dembowski-Ostrom polynomials. In *Finite fields and applications (Augsburg, 1999)*, pages 37–42. Springer, Berlin, 2001.
- [3] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. [arXiv:0804.4799](https://arxiv.org/abs/0804.4799), 12 pages, 2008.
- [4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields Appl.*, 14(3):703–714, 2008.
- [5] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, 49(1-3):273–288, 2008.
- [6] Mihai Cipu. Dickson polynomials that are permutations. *Serdica Math. J.*, 30(2-3):177–194, 2004.
- [7] Mihai Cipu and Stephen D. Cohen. Dickson polynomial permutations. In *Finite Fields and Applications*, volume 461 of *Contemporary Mathematics*, 79–91 pages. 2008.
- [8] Stephen D. Cohen. Finite field elements with specified order and traces. *Des. Codes Cryptogr.*, 36(3):331–340, 2005.
- [9] Stephen D. Cohen. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.*, 12(3):425–491, 2006.

- [10] Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht's algorithm, the HFE cryptosystem and Ore's  $p^s$ -polynomials. In *Computer Mathematics (Matsuyama, 2001)*, volume 9 of *Lecture Notes Ser. Comput*, pages 36–45. World Sci. Publ., River Edge, NJ, 2001.
- [11] Robert S. Coulter, George Havas, and Marie Henderson. On decomposition of sub-linearised polynomials. *J. Aust. Math. Soc.*, 76(3):317–328, 2004.
- [12] Robert S. Coulter and Marie Henderson. The compositional inverse of a class of permutation polynomials over a finite field. *Bull. Austral. Math. Soc.*, 65(3):521–526, 2002.
- [13] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields and Their Applications*, 15(1):1 – 22, 2009.
- [14] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3(1):59–81, 2009.
- [15] Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang. Gauss sums, Jacobi sums, and  $p$ -ranks of cyclic difference sets. *J. Combin. Theory Ser. A*, 87(1):74–119, 1999.
- [16] Reza Rezaeian Farashahi and Ruud Pellikaan. The quadratic extension extractor for (hyper)elliptic curves in odd characteristic. In *Arithmetic of finite fields*, volume 4547 of *Lecture Notes in Comput. Sci.*, pages 219–236. Springer, Berlin, 2007.
- [17] Kseniya Garaschuk. *On Binary and Ternary Kloosterman Sums*. Ph D thesis, Simon Fraser University, 2007.
- [18] Lenwood S. Heath and Nicholas A. Loehr. New algorithms for generating Conway polynomials over finite fields. In *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999)*, pages 429–437, New York, 1999. ACM.
- [19] Dae San Kim. Codes associated with  $O^+(2n, 2^r)$  and power moments of Kloosterman sums. [arXiv:0807.4671](https://arxiv.org/abs/0807.4671), 9 pages, 2008.
- [20] Dae San Kim. Codes associated with orthogonal groups and power moments of Kloosterman sums. [arXiv:0808.3003](https://arxiv.org/abs/0808.3003), 2008.

- [21] Dae San Kim. Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums. *arXiv:0807.3991*, 7 pages, 2008.
- [22] Douglas A. Leonard. A weighted module view of integral closures of affine domains of type I. *Adv. Math. Commun.*, 3(1):1–11, 2009.
- [23] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arith.*, 132(4):329–350, 2008.
- [24] Ferruh Özbudak. Elements of prescribed order, prescribed traces and systems of rational functions over finite fields. *Des. Codes Cryptogr.*, 34(1):35–54, 2005.
- [25] B. V. Petrenko. On the product of two primitive elements of maximal subfields of a finite field. *J. Pure Appl. Algebra*, 178(3):297–306, 2003.
- [26] B. V. Petrenko. On the sum of two primitive elements of maximal subfields of a finite field. *Finite Fields Appl.*, 9(1):102–116, 2003.
- [27] Håvard Raddum and Igor Semaev. Solving multiple right hand sides linear equations. *Des. Codes Cryptogr.*, 49(1-3):147–160, 2008.

# 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.