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** (2005), no. 5, 502–514. MR MR2140093

[2] Wieb Bosma, *Some computational experiments in number theory*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 1–30. MR MR2278921

[3] Richard P. Brent and Paul Zimmermann, *Ten new primitive binary trinomials*, Math. Comp. **78** (2009), no. 266, 1197–1199. MR MR2476580

[4] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)

[5] ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR MR1728313 (2000k:11144)

[6] J. E. Cremona, *Unimodular integer circulants*, Math. Comp. **77** (2008), no. 263, 1639–1652. MR MR2398785

[7] Vassil S. Dimitrov and Everett W. Howe, *Lower bounds on the lengths of double-base representations*.

[8] Graham Everest and Valéry Mahé, *A generalization of Siegel's theorem and Hall's conjecture*, Experiment. Math. **18** (2009), no. 1, 1–9. MR MR2548983

[9] Alina Ostafe and Igor E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, 2010.

[10] Emmanuel Royer, *Evaluating convolution sums of the divisor function with quasimodular forms*, Int. J. Number Theory **3** (2007), no. 2, 231–261.

[11] J. Sándor and B. Crstici, *Handbook of Number Theory II*, Kluwer Academic Publishers, Dordrecht, 2004. MR MR2119686 (2005k:11001)

Primality and Factorisation

11A41, 11A51

[1] Wieb Bosma, *Explicit primality criteria for $h \cdot 2^k \pm 1$*, Math. Comp. **61** (1993), no. 203, 97–109. MR MR1197510 (94c:11005)

[2] 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*, Report – Modelling, Analysis and Simulation, vol. 7, Centrum voor Wiskunde en Informatica, Amsterdam, 2001, pp. i–viii, pp. 1–19.

[3] Graham Everest, Patrick Ingram, and Shaun Stevens, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. **12** (2009), 54–81. MR MR2486632

[4] Stephen McMath, *Parallel integer factorization using quadratic forms*, 2005.

[5] F. Morain, *Primality proving using elliptic curves: An update*, Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 111–127. MR MR1726064 (2000i:11190)

[6] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 525–542. MR MR2282947

Sequences and Sets

11Bxx

[1] S. Akhtari, A. Togbé, and P. G. Walsh, *On the equation* $aX^4 - bY^2 = 2$, Acta Arith. **131** (2008), no. 2, 145–169. MR MR2388048

[2] Huseyin Aydin, Ramazan Dikici, and Geoff C. Smith, *Wall and Vinson revisited*, Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 61–68. MR MR1271347 (95f:11009)

[3] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.

[4] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Theory **107** (2004), no. 2, 215–227. MR MR2072385 (2005i:11019)

[5] ———, *Lucas sequences whose 8th term is a square*, 2004.

[6] ———, *On squares in Lucas sequences*, J. Number Theory **124** (2007), no. 2, 511–520. MR MR2321377

[7] Florian Breuer, Ernest Lötter, and Brink van der Merwe, *Ducci-sequences and cyclotomic polynomials*, Finite Fields Appl. **13** (2007), no. 2, 293–304. MR MR2307129 (2008a:11017)

[8] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. (N.S.) **17** (2006), no. 4, 539–555. MR MR2320112 (2008e:11036)

[9] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On Fibonacci numbers with few prime divisors*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 2, 17–20. MR MR2126070 (2005k:11020)

[10] 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** (2004), no. 5, 327–330. MR MR2092057 (2005g:11019)

[11] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.

[12] Everett W. Howe, *Higher-order Carmichael numbers*, Math. Comp. **69** (2000), no. 232, 1711–1719. MR MR1709151 (2001a:11012)

[13] Benjamin Kane, *Representing sets with sums of triangular numbers*, Int. Math. Res. Not. IMRN (2009), no. 17, 3264–3285. MR MR2534998

[14] Tünde Kovács, *Combinatorial numbers in binary recurrences*, Period. Math. Hungar. **58** (2009), no. 1, 83–98. MR MR2487248 (2010a:11024)

[15] J. McLaughlin, *Small prime powers in the Fibonacci sequence*, 2002.

[16] A. Stoimenow, *Generating functions, Fibonacci numbers and rational knots*, J. Algebra **310** (2007), no. 2, 491–525. MR MR2308169 (2008a:05018)

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** (2008), no. 1, 175–181. MR MR2381741 (2008m:11071)

[2] S. Akhtari, A. Togbé, and P. G. Walsh, *On the equation* $aX^4 - bY^2 = 2$, Acta Arith. **131** (2008), no. 2, 145–169. MR MR2388048

[3] Shabnam Akhtari, *The diophantine equation* $ax^4 - by^2 = 1$, 2009.

[4] ———, *The method of Thue-Siegel for binary quartic forms*, 2009.

[5] 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** (2006), no. 2, 273–306. MR MR2205718 (2006k:11046)

[6] Michael A. Bennett, *The Diophantine equation* $(x^k - 1)(y^k - 1) = (z^k - 1)^t$, Indag. Math. (N.S.) **18** (2007), no. 4, 507–525. MR MR2424310 (2009b:11058)

[7] Michael A. Bennett, Kálmán Győry, and Ákos Pintér, *On the Diophantine equation* $1^k + 2^k + \ldots + x^k = y^n$, Compos. Math. **140** (2004), no. 6, 1417–1431. MR MR2098395 (2005g:11042)

[8] A. Bérczes, A. Pethő, and V. Ziegler, *Parameterized norm form equations with arithmetic progressions*, J. Symbolic Comput. **41** (2006), no. 7, 790–810. MR MR2232201 (2007c:11040)

[9] Attila Bérczes and Attila Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, Glas. Mat. Ser. III **41(61)** (2006), no. 1, 1–8. MR MR2242387 (2007g:11040)

[10] A. Bremner and Jean-Joël Delorme., *On equal sums of ninth powers*, Math. Comp **79** (2009), 603–612.

[11] A. Bremner and N. Tzanakis, *Lucas sequences whose 8th term is a square*, 2004.

[12] ———, *On squares in Lucas sequences*, J. Number Theory **124** (2007), no. 2, 511–520. MR MR2321377

[13] Andrew Bremner, *On the equation* $Y^2 = X^5 + k$, Experiment. Math. **17** (2008), no. 3, 371–374. MR MR2455707

[14] ———, *A problem of Ozanam*, Proc. Edinb. Math. Soc. (2) **52** (2009), no. 1, 37–44. MR MR2475879

[15] Andrew Bremner and Nikos Tzanakis, *On the equation* $y^2 = x^6 + k$, Annales des Sciences Mathématiques du Québec **To appear** (2010).

[16] David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, 2009.

[17] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. (N.S.) **17** (2006), no. 4, 539–555. MR MR2320112 (2008e:11036)

[18] Nils Bruin, *The primitive solutions to* $x^3 + y^9 = z^2$, J. Number Theory **111** (2005), no. 1, 179–189. MR MR2124048

[19] ———, *Some ternary Diophantine equations of signature* $(n, n, 2)$, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 63–91. MR MR2278923

[20] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884

[21] Nils Bruin and Michael Stoll, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.

[22] Ralph H. Buchholz, *Triangles with three rational medians*, J. Number Theory **97** (2002), no. 1, 113–131. MR MR1939139 (2003h:11034)

[23] Ralph H. Buchholz and James A. MacDougall, *Cyclic polygons with rational sides and area*, J. Number Theory **128** (2008), no. 1, 17–48. MR MR2382768 (2008m:11061)

[24] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On perfect powers in Lucas sequences*, Int. J. Number Theory **1** (2005), no. 3, 309–332. MR MR2175095

[25] 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** (2006), no. 3, 969–1018. MR MR2215137 (2007f:11031)

[26] ———, *Classical and modular approaches to exponential Diophantine equations II: The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), no. 1, 31–62. MR MR2196761 (2007f:11032)

[27] ———, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), no. 3, 491–519. MR MR2414954 (2009b:11059)

[28] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885. MR MR2457355

[29] I. N. Cangül, M. Demirci, G. Soydan, and N. Tzanakis., *On the diophantine equation* $x^2 + 5^a \cdot 11^b = y^n$, 2011, p. 21 pages.

[30] Imin Chen, *A Diophantine equation associated to* $X_0(5)$, LMS J. Comput. Math. **8** (2005), 116–121 (electronic). MR MR2153792 (2006b:11052)

[31] ———, *On the equation* $s^2 + y^{2p} = \alpha^3$, Math. Comp. **77** (2008), no. 262, 1223–1227. MR MR2373199

[32] Imin Chen and Samir Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), no. 3, 638–656. MR MR2531215

[33] C. Chisholm and J. A. MacDougall, *Rational and Heron tetrahedra*, J. Number Theory **121** (2006), no. 1, 153–185. MR MR2268761 (2007h:11040)

[34] ———, *Rational tetrahedra with edges in geometric progression*, J. Number Theory **128** (2008), no. 2, 251–262. MR MR2380320

[35] Mihai Cipu, *Gröbner bases and Diophantine analysis*, J. Symbolic Comput. **43** (2008), no. 10, 681–687. MR MR2426566

[36] Mihai Cipu, Florian Luca, and Maurice Mignotte, *Solutions of the Diophantine equation* $x^y + y^z + z^x = n!$, Glasg. Math. J. **50** (2008), no. 2, 217–232. MR MR2417617

[37] Henri Cohen, *Number theory: Volume I: Tools and diophantine equations*, Springer, Berlin, 2007.

[38] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR MR2212121 (2006m:11042)

[39] Robert S. Coulter, Marie Henderson, and Felix Lazebnik, *On certain combinatorial Diophantine equations and their connection to Pythagorean numbers*, Acta Arith. **122** (2006), no. 4, 395–406. MR MR2234423 (2007a:11036)

[40] R. de la Bret'che and T.D. Browning, *Manin's conjecture for quartic del Pezzo surfaces with a conic fibration*, 2008.

[41] Luis V. Dieulefait, *Solving Diophantine equations* $x^4 + y^4 = qz^p$, Acta Arith. **117** (2005), no. 3, 207–211. MR MR2139003 (2005k:11059)

[42] Shanshan Ding, *Smallest irreducible of the form* $x^2 - dy^2$, 2007.

[43] 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** (2006), no. 255, 1585–1593 (electronic). MR MR2219047 (2007b:11192)

[44] ———, *Corrigendum to "Solving the Diophantine equation* $y^2 = x(x^2 - n^2)$*" [J. Number Theory 129 (1) (2009) 102–121] [mr2468473]*, J. Number Theory **129** (2009), no. 3, 739–740. MR MR2488600 (2010c:11040)

[45] ———, *Solving the Diophantine equation* $y^2 = x(x^2 - n^2)$, J. Number Theory **129** (2009), no. 1, 102–121. MR MR2468473 (2009j:11047)

[46] Konstantinos A. Draziotis, *Integer points on the curve* $Y^2 = X^3 \pm p^k X$, Math. Comp. **75** (2006), no. 255, 1493–1505 (electronic). MR MR2219040 (2007a:11034)

[47] Edray Goins, Florian Luca, and Alain Togbé, *On the Diophantine equation* $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 430–442. MR MR2467863

[48] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.

[49] K. Győry, L. Hajdu, and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compos. Math. **145** (2009), no. 4, 845–864. MR MR2521247 (2010d:11037)

[50] K. Győry and Á. Pintér, *Almost perfect powers in products of consecutive integers*, Monatsh. Math. **145** (2005), no. 1, 19–33. MR MR2134477 (2006a:11040)

[51] ———, *Correction to the paper: "Almost perfect powers in products of consecutive integers"*, Monatsh. Math. **146** (2005), no. 4, 341. MR MR2191733 (2006i:11036)

[52] ———, *On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$. I*, Publ. Math. Debrecen **70** (2007), no. 3-4, 483–501. MR MR2310662 (2008g:11053)

[53] Lajos Hajdu and Szabolcs Tengely, *Arithmetic progressions of squares, cubes and n-th powers*, Funct. Approx. Comment. Math. **41** (2009), no. 2, 129–138. MR MR2590329

[54] Lajos Hajdu, Szabolcs Tengely, and Robert Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), no. 1-2, 215–232. MR MR2490432 (2009j:11050)

[55] Robin Hartshorne and Ronald van Luijk, *Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on $K3$ surfaces*, Math. Intelligencer **30** (2008), no. 4, 4–10. MR MR2501390

[56] Bo He and Alain Togbé, *On the number of solutions of Goormaghtigh equation for given x and y*, Indag. Math. (N.S.) **19** (2008), no. 1, 65–72. MR MR2466394 (2009i:11042)

[57] 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** (2004), no. 1, 69–76. MR MR2046969 (2004m:11046)

[58] E. Herrmann, F. Luca, and P. G. Walsh, *A note on the Ramanujan-Nagell equation*, Publ. Math. Debrecen **64** (2004), no. 1-2, 21–30. MR MR2035886 (2004k:11033)

[59] 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** (2001), no. 2, 443–451. MR MR1881378 (2003a:11024)

[60] Akinari Hoshi, *On the simplest quartic fields and related Thue equations*, 2010.

[61] Stephen P. Humphries and Kenneth W. Johnson, *Fusions of character tables and Schur rings of abelian groups*, Comm. Algebra **36** (2008), no. 4, 1437–1460. MR MR2406596 (2009b:20008)

[62] Benjamin Kane, *Representing sets with sums of triangular numbers*, Int. Math. Res. Not. IMRN (2009), no. 17, 3264–3285. MR MR2534998

[63] Tünde Kovács, *Combinatorial Diophantine equations—the genus 1 case*, Publ. Math. Debrecen **72** (2008), no. 1-2, 243–255. MR MR2376872 (2008m:11065)

[64] 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** (2008), no. 2, 143–158. MR MR2453529

[65] A. Laradji, M. Mignotte, and N. Tzanakis, *On $px^2+q^{2n}=y^p$ and related Diophantine equations*, 2010.

[66] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Coleman-Chabauty*, 2000.

[67] F. Luca, P. Stanica, and A. Togbé, *On a Diophantine equation of Stroeker*, Bull. Belg. Math. Soc. Simon Stevin (2008), 10.

[68] Florian Luca and Alain Togbé, *On the Diophantine equation $x^2+2^\alpha 13^\beta = y^n$*, Colloq. Math. **116** (2009), no. 1, 139–146. MR MR2504836

[69] Florian Luca and Peter Gareth Walsh, *On a sequence of integers arising from simultaneous Pell equations*, Funct. Approx. Comment. Math. **38** (2008), no. , part 2, 221–226. MR MR2492857 (2010b:11036)

[70] 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).

[71] Á. Pintér, *On a class of Diophantine equations related to the numbers of cells in hyperplane arrangements*, J. Number Theory **129** (2009), no. 7, 1664–1668. MR MR2524187

[72] Ákos Pintér, *On the power values of power sums*, J. Number Theory **125** (2007), no. 2, 412–423. MR MR2332596 (2008g:11052)

[73] 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** (2007), no. 1, 103–158. MR MR2309145

[74] Diana Savin, *About certain prime numbers*, 2009, p. 9.

[75] Samir Siksek, *The modular approach to diophantine equations*, Number Theory (Henri Cohen, ed.), Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007, pp. 495–527.

[76] Samir Siksek and John E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109** (2003), no. 2, 143–149. MR MR1980642 (2004c:11109)

[77] Samir Siksek and Michael Stoll, *On a problem of Hajdu and Tengely*, 2009.

[78] N. P. Smart, *Thue and Thue-Mahler equations over rings of integers*, J. London Math. Soc. (2) **56** (1997), no. 3, 455–462. MR MR1610439 (99d:11031)

[79] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR MR1689189 (2000c:11208)

[80] 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** (2008), no. 4, 329–335. MR MR2449156 (2009h:11050)

[81] Szabolcs Tengely, *On the Diophantine equation* $x^2 + a^2 = 2y^p$, Indag. Math. (N.S.) **15** (2004), no. 2, 291–304. MR MR2071862 (2005f:11045)

[82] ———, *Effective methods for Diophantine equations*, Ph.D. thesis, Leiden University, 2005, p. 85.

[83] ———, *Triangles with two integral sides*, Ann. Math. Inform. **34** (2007), 89–95. MR MR2385428 (2009a:11070)

[84] P. G. Walsh, *On a very particular class of Ramanujan-Nagell type equations*, Far East J. Math. Sci. (FJMS) **24** (2007), no. 1, 55–58. MR MR2281854 (2007k:11213)

[85] Huilin Zhu and Jianhua Chen, *Integral points on a class of elliptic curve*, Wuhan Univ. J. Nat. Sci. **11** (2006), no. 3, 477–480. MR MR2258847 (2007d:11064)

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** (2009), no. 265, 387–403. MR MR2448712

[2] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.

[3] Manjul Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250. MR MR2051392 (2005f:11062a)

[4] Donald I. Cartwright and Tim Steger, *Application of the Bruhat–Tits tree of* $\mathrm{SU}_3(h)$ *to some* A_2 *groups*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 3, 329–344. MR MR1623286 (99i:11026)

[5] Carlos Castaño-Bernard, *Further properties of a function of Ogg and Ligozat*, Ramanujan J. **17** (2008), no. 1, 107–121. MR MR2439528

[6] Darrin Doud, *Supersingular Galois representations and a generalization of a conjecture of Serre*, Experiment. Math. **16** (2007), no. 1, 119–128. MR MR2312982 (2007m:11076)

[7] Paul E. Gunnells and Dan Yasaki, *Perfect forms over totally real number fields*, 2009.

[8] Jonathan Hanke, *Local densities and explicit bounds for representability by a quadratric form*, Duke Math. J. **124** (2004), no. 2, 351–388. MR MR2079252 (2005m:11060)

[9] Boris Hemkemeier, *Algorithmische konstruktionen von gittern*, 2004.

[10] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.

[11] Piotr Maciak, *Primes of the form* $x^2 + n * y^2$ *in function fields*, 2009.

[12] Jeremy Rouse, *Zagier duality for the exponents of Borcherds products for Hilbert modular forms*, J. London Math. Soc. (2) **73** (2006), no. 2, 339–354. MR MR2225490 (2006m:11059)

[13] John Voight, *Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic*, Ph.D. thesis, Berkeley, 2005, p. 98.

[14] John Voight, *Quadratic forms that represent almost the same primes*, Math. Comp. **76** (2007), no. 259, 1589–1617 (electronic). MR MR2299790 (2007m:11055)

[15] Tonghai Yang, *Local densities of 2-adic quadratic forms*, J. Number Theory **108** (2004), no. 2, 287–345. MR MR2098640 (2005i:11048)

[16] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), no. 11, 4132–4142. MR MR2556143

[17] Dan Yasaki, *Hyperbolic tessellations associated to Bianchi groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 385–396.

Discontinuous Groups and Automorphic Forms

11Fxx

[1] Scott Ahlgren, *On the irreducibility of Hecke polynomials*, Math. Comp. **77** (2008), no. 263, 1725–1731. MR MR2398790

[2] Scott Ahlgren and Ken Ono, *Arithmetic of singular moduli and class polynomials*, Compos. Math. **141** (2005), no. 2, 293–312. MR MR2134268 (2006a:11058)

[3] A. O. L. Atkin, Wen-Ching Winnie Li, and Ling Long, *On Atkin and Swinnerton-Dyer congruence relations (II)*, Math. Ann. **340** (2008), no. 2, 335–358. MR MR2368983 (2009a:11102)

[4] Tobias Berger, *An Eisenstein ideal for imaginary quadratic fields and the Bloch-Kato conjecture for Hecke characters*, 2007.

[5] Tobias Berger and Krzysztof Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, J. Inst. Math. Jussieu **To appear** (2009), 19.

[6] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.

[7] Siegfried Boecherer and Gabriele Nebe, *On theta series attached to maximal lattices and their adjoints*, 2009.

[8] Johan Bosman, *On the computation of Galois representations associated to level one modular forms*, 2007.

[9] Jim Brown, *Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture*, Compos. Math. **143** (2007), no. 2, 290–322. MR MR2309988

[10] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288.

[11] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), no. 3, 491–519. MR MR2414954 (2009b:11059)

[12] Cecilia Busuioc, *The Steinberg symbol and special values of L-functions*, Trans. Amer. Math. Soc. **360** (2008), no. 11, 5999–6015. MR MR2425699

[13] Kevin Buzzard, *Questions about slopes of modular forms*, Astérisque (2005), no. 298, 1–15, Automorphic forms. I. MR MR2141701 (2005m:11082)

[14] Kevin Buzzard and Frank Calegari, *A counterexample to the Gouvêa-Mazur conjecture*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 10, 751–753. MR MR2059481 (2005g:11070)

[15] Kevin Buzzard and William A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR MR1897901 (2003c:11052)

[16] Bryden Cais, *Serre's conjectures*, 2005.

[17] Frank Calegari and Nathan M. Dunfield, *Automorphic forms and rational homology 3-spheres*, Geom. Topol. **10** (2006), 295–329 (electronic). MR MR2224458 (2007h:57013)

[18] Frank Calegari and William A. Stein, *Conjectures about discriminants of Hecke algebras of prime level*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 140–152. MR MR2137350

[19] Imin Chen, Ian Kiming, and Jonas B. Rasmussen, *On congruences mod p^m between eigenforms and their attached Galois representations*, J. Number Theory **130** (2010), no. 3, 608–619. MR MR2584844

[20] C. J. Cummins, *Congruence subgroups of groups commensurable with* $\mathrm{PSL}(2, Z)$ *of genus 0 and 1*, Experiment. Math. **13** (2004), no. 3, 361–382. MR MR2103333 (2005i:11058)

[21] C.J. Cummins, *On conjugacy classes of congruence subgroups of* $PSL(2, R)$, LMS J. Comput. Math. **12** (2009), 264–274. MR 2570927

[22] Henri Darmon and Robert Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354. MR MR2254648

[23] Lassina Dembélé, *Explicit computations of Hilbert modular forms on* $\mathbf{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466. MR MR2193808 (2006h:11050)

[24] ———, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057 (electronic). MR MR2291849

[25] Lassina Dembélé, *On the computation of algebraic modular forms on compact inner forms of GSp_4*, 2009.

[26] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 371–386. MR MR2467859 (2010d:11149)

[27] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at* 3 *and* 5, 2009.

[28] Tobias Dern and Aloys Krieg, *Graded rings of Hermitian modular forms of degree 2*, Manuscripta Math. **110** (2003), no. 2, 251–272. MR MR1962537 (2004b:11059)

[29] ———, *The graded ring of Hermitian modular forms of degree 2 over $Q(\sqrt{-2})$*, J. Number Theory **107** (2004), no. 2, 241–265. MR MR2072387 (2005d:11069)

[30] Michael Dewar and Olav K. Richter, *Ramanujan congruences for Siegel modular forms*, arXiv:0910.0787v1 (2009).

[31] Meghan DeWitt and Darrin Doud, *Finding Galois representations corresponding to certain Hecke eigenclasses*, Int. J. Number Theory **5** (2009), no. 1, 1–11. MR MR2499017 (2009k:11091)

[32] Luis Dieulefait, E. Gonzalez-Jimenez, and J. Jimenez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, arXiv:0909.1661v1 (2009).

[33] Luis Dieulefait and Xavier Taixes i Ventosa, *Congruences between modular forms and lowering the level mod l^n*, Journal de Theorie des Nombres de Bordeaux **31** (2009), no. 1, 109–118.

[34] Darrin Doud, *Three-dimensional Galois representations with conjectural connections to arithmetic cohomology*, Number Theory for the Millennium I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 365–375. MR MR1956235 (2003k:11089)

[35] ———, *Distinguishing contragredient Galois representations in characteristic two*, Rocky Mountain J. Math. **38** (2008), no. 3, 835–848. MR MR2426523

[36] Darrin Doud and Brian Hansen, *Explicit Frobenius calculations supporting a generalization of a conjecture of Serre*, JP J. Algebra Number Theory Appl. **6** (2006), no. 2, 381–398. MR MR2283945

[37] Neil Dummigan, William Stein, and Mark Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 91–118. MR MR2053457 (2005g:11071)

[38] 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** (2006), no. 1, 1–34, With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese. MR MR2195943 (2007f:11046)

[39] Liqun Fang, J. William Hoffman, Benjamin Linowitz, Andrew Rupinski, and Helena Verrill, *Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations*, Experiment. Math. **19** (2010), no. 1, 1–27.

[40] Julio Fernández, Josep González, and Joan-C. Lario, *Plane quartic twists of $X(5,3)$*, Canad. Math. Bull. **50** (2007), no. 2, 196–205. MR MR2317442 (2008b:11067)

[41] Sharon M. Frechette, *A classical characterization of newforms with equivalent eigenforms in $S_{k+1/2}(4N,\chi)$*, J. London Math. Soc. (2) **68** (2003), no. 3, 563–578. MR MR2009437 (2004h:11040)

[42] E. Freitag and R. Salvati Manni, *Some Siegel threefolds with a Calabi-Yau model II*, 2010.

[43] Eberhard Freitag and Manabu Oura, *A theta relation in genus 4*, Nagoya Math. J. **161** (2001), 69–83. MR MR1820213 (2002m:11035)

[44] Edray Goins, *On the modularity of wildly ramified Galois representations*, 2004.

[45] Enrique Gonzalez-Jimenez and Xavier Guitart, *On the modularity level of modular abelian varieties over number fields*, J. Number Theory **130** (2010), no. 7, 1560–1570.

[46] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **To appear** (2011).

[47] Xavier Guitart and Jordi Quer, *Modular abelian varieties over number fields*, 2009.

[48] P. E. Gunnells, F. Hajir, and D. Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, 2010.

[49] Jerome W. Hoffman, Ling Long, and Helena Verrill, *On l-adic representations for a space of noncongruence cuspforms*, 2010.

[50] Xavier Taixes i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, arXiv:0909.2724v2 (2009).

[51] Samar Jaafar and Kamal Khuri-Makdisi, *On the maps from $X(4p)$ to $X(4)$*, 2007.

[52] Rafe Jones and Jeremy Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. London Math. Soc. **100** (2010), 763–794.

[53] Hidenori Katsurada, *Exact standard zeta values of Siegel modular forms*, Experiment. Math. **19** (2010), no. 1, 65–77.

[54] L. J. P. Kilford, *Slopes of overconvergent modular forms*, PhD Thesis, Imperial College, University of London, 2002.

[55] L. J. P. Kilford, *Generating spaces of modular forms with η-quotients*, JP J. Algebra Number Theory Appl. **8** (2007), no. 2, 213–226. MR MR2406859 (2009b:11075)

[56] ———, *Modular forms*, Imperial College Press, London, 2008, A classical and computational introduction. MR MR2441106 (2009m:11001)

[57] ———, *On mod p modular representations which are defined over* F_p, Glas. Mat. Ser. III **43(63)** (2008), no. 1, 1–6. MR MR2426658 (2009h:11070)

[58] ———, *On the slopes of the U_5 operator acting on overconvergent modular forms*, J. Théor. Nombres Bordeaux **20** (2008), no. 1, 165–182. MR MR2434162 (2009f:11045)

[59] L. J. P. Kilford, *Experimental finding of modular forms for noncongruence subgroups*, 2009.

[60] L. J. P. Kilford, *On the U_p operator acting on p-adic overconvergent modular forms when $X_0(p)$ has genus 1*, J. Number Theory **130** (2010), no. 3, 586–594. MR MR2584842

[61] L. J. P. Kilford and Gabor Wiese, *On the failure of the Gorenstein property for Hecke algebras of prime weight*, Experiment. Math. **17** (2008), no. 1, 37–52. MR 2410114 (2009c:11075)

[62] L. J. P. Kilford and Gabor Wiese, *On mod p representations which are defined over F_p: Ii*, Glasgow Math. J. **52** (2010), 391–400.

[63] Ian Kiming, Matthias Schuett, and Helena Verrill, *Lifts of projective congruence groups*, J. London Math. Soc **To appear** (2010).

[64] Ingo Herbert Klöcker, *Modular forms for the orthogonal group* $\mathrm{O}(2,5)$, Ph.D. thesis, 2005, p. 142.

[65] Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves $X_0(n)$ in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163.

[66] A. Krieg, *The graded ring of quaternionic modular forms of degree 2*, Math. Z. **251** (2005), no. 4, 929–942. MR MR2190150

[67] Dominic Lanphier, *Combinatorics of Maass-Shimura operators*, J. Number Theory **128** (2008), no. 8, 2467–2487. MR MR2394832

[68] Joan-C. Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311, With an appendix by Amod Agashe and William Stein. MR MR1959271 (2004b:11072)

[69] Mark Lingham, *Modular Forms and Elliptic Curves over Imaginary Quartic Fields*, PhD Thesis, University of Nottingham, 2005.

[70] David Loeffler, *Explicit calculations of automorphic forms for definite unitary groups*, LMS J. Comput. Math. **11** (2008), 326–342. MR MR2452552 (2009i:11062)

[71] David Loeffler and Jared Weinstein, *On the computation of local components of a newform*, 2010.

[72] Ling Long, *On Atkin and Swinnerton-Dyer congruence relations. III*, J. Number Theory **128** (2008), no. 8, 2413–2429. MR MR2394828

[73] A. Marschner and J. Müller, *On a certain algebra of higher modular forms*, Algebra Colloq. **16** (2009), 371–380.

[74] Barry Mazur, William Stein, and John Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic). MR MR2290599

[75] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, 2009.

[76] G. Nebe, *Kneser-Hecke-operators in coding theory*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 79–90. MR MR2293434 (2007m:11090)

[77] Gabriele Nebe and Maria Teider, *Hecke actions on certain strongly modular genera of lattices*, Arch. Math. (Basel) **84** (2005), no. 1, 46–56. MR MR2106404 (2006c:11055)

[78] Ken Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR MR2020489 (2005c:11053)

[79] Manabu Oura, Cris Poor, and David S. Yuen, *Towards the Siegel ring in genus four*, Int. J. Number Theory **4** (2008), no. 4, 563–586. MR MR2441792

[80] Ariel Pacetti and Fernando Rodriguez Villegas, *Computing weight 2 modular forms of level p^2*, Math. Comp. **74** (2005), no. 251, 1545–1557 (electronic), With an appendix by B. Gross. MR MR2137017 (2006a:11053)

[81] Kathleen L. Petersen, *One-cusped congruence subgroups of Bianchi groups*, Math. Ann. **338** (2007), no. 2, 249–282. MR MR2302062 (2008b:20063)

[82] Francesco Dalla Piazza and Bert van Geemen, *Siegel modular forms and finite symplectic groups*, 2008.

[83] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558. MR MR1983040 (2004e:11050)

[84] Alexandru A. Popa, *Central values of Rankin L-series over real quadratic fields*, Compos. Math. **142** (2006), no. 4, 811–866. MR MR2249532

[85] Jordi Quer, *Fields of definition of building blocks*, Math. Comp. **78** (2009), no. 265, 537–554. MR MR2448720

[86] Jeremy Rouse, *Bounds for the coefficients of powers of the Delta-function*, Bull. London Math. Soc. **40** (2008), no. 6, 1081–1090.

[87] Emmanuel Royer, *Evaluating convolution sums of the divisor function with quasi-modular forms*, Int. J. Number Theory **3** (2007), no. 2, 231–261.

[88] Michael M. Schein, *Weights in Serre's conjecture for Hilbert modular forms: the ramified case*, Israel J. Math. **166** (2008), 369–391. MR MR2430440

[89] Mehmet Haluk Şengün, *The nonexistence of certain representations of the absolute Galois group of quadratic fields*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 27–35. MR MR2439421

[90] William Stein, *Modular Forms: A Computational Approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells. MR MR2289048

[91] William A. Stein, *Explicit Approaches to Modular Abelian Varieties*, PhD Thesis, University of California, Berkeley, 2000.

[92] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 641–652. MR MR2467560 (2009k:11085)

[93] William A. Stein and Helena A. Verrill, *Cuspidal modular symbols are transportable*, LMS J. Comput. Math. **4** (2001), 170–181 (electronic). MR MR1901355 (2003m:11074)

[94] Helena A. Verrill, *Transportable modular symbols and the intersection pairing*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 219–233. MR MR2041086 (2005b:11063)

[95] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 469–491. MR MR2541438

[96] Gabor Wiese, *Dihedral Galois representations and Katz modular forms*, Doc. Math. **9** (2004), 123–133 (electronic). MR MR2054983 (2005c:11065)

[97] Gabor Wiese, *Modular Forms of Weight One over Finite Fields*, PhD Thesis, Universiteit Leiden, 2005.

[98] Gabor Wiese, *On the faithfulness of parabolic cohomology as a Hecke module over a finite field*, J. reine angew. Math. **606** (2007), 79–103. MR MR2337642 (2008g:11092)

[99] ———, *On projective linear groups over finite fields as Galois groups over the rational numbers*, Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006, Cambridge University Press, Cambridge, 2008, pp. 343–350. MR)

[100] ———, *On modular symbols and the cohomology of Hecke triangle surfaces*, Int. J. Number Theory **5** (2009), no. 1, 89–108. MR MR2499023

[101] Dan Yasaki, *Integral cohomology of certain Picard modular surfaces*, 2007.

[102] Dan Yasaki, *Elliptic points of the Picard modular group*, Monatsh. Math. **156** (2009), no. 4, 391–396. MR MR2486605

[103] Jahan Zahid, *Zeros of p-adic forms*, J. Number Theory **129** (2009), no. 10, 2439–2456. MR MR2541024

[104] David Zywina, *A refinement of Koblitz's conjecture*, 2009.

Arithmetic Algebraic Geometry

11Gxx

[1] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636. MR MR2251484 (2007c:11076)

[2] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR MR1939144 (2003h:11070)

[3] ———, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur. MR MR2085902 (2005g:11119)

[4] Scott Ahlgren and Matthew Papanikolas, *Higher Weierstrass points on $X_0(p)$*, Trans. Amer. Math. Soc. **355** (2003), no. 4, 1521–1535 (electronic). MR MR1946403 (2003j:11065)

[5] Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579. MR MR1896473 (2003g:11055)

[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** (2005), no. 6, 1325–1387. MR MR2183527

[7] Arthur Baragar and Ronald van Luijk, *$K3$ surfaces with Picard number three and canonical vector heights*, Math. Comp. **76** (2007), no. 259, 1493–1498 (electronic). MR MR2299785

[8] Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005 (electronic). MR MR2164107

[9] Tobias Berger and Krzysztof Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, J. Inst. Math. Jussieu **8** (2009), no. 4, 669–692. MR MR2540877

[10] Amnon Besser and Rob De Jeu, li(p)*-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194

[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** (2007), 27–35. MR MR2318536

[13] Irene I. Bouw and Brian Osserman, *Some* 4*-point Hurwitz numbers in positive characteristic*, 2009.

[14] M. J. Bright, N. Bruin, E. V. Flynn, and A. Logan, *The Brauer-Manin obstruction and Sh[2]*, LMS J. Comput. Math. **10** (2007), 354–377 (electronic). MR MR2342713

[15] David Brown, *The Chabauty-Coleman bound at a prime of bad reduction*, 2008.

[16] ———, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, 2009.

[17] Ezra Brown and Bruce T. Myers, *Elliptic curves from Mordell to Diophantus and back*, Amer. Math. Monthly **109** (2002), no. 7, 639–649. MR MR1917222 (2003d:11080)

[18] N. Bruin and E. V. Flynn, *n-covers of hyperelliptic curves*, Math. Proc. Cambridge Philos. Soc. **134** (2003), no. 3, 397–405. MR MR1981207 (2004b:11089)

[19] Nils Bruin, *Visualising Sha*[2] *in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR MR2047096 (2005c:11067)

[20] ———, *The arithmetic of Prym varieties in genus 3*, Compos. Math. **144** (2008), no. 2, 317–338. MR MR2406115

[21] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with (4,4)-split Jacobians*, arXiv:0902.3480v2 (2010).

[22] Nils Bruin and Noam D. Elkies, *Trinomials* $ax^7 + bx + c$ *and* $ax^8 + bx + c$ *with Galois groups of order 168 and* $8 \cdot 168$, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 172–188. MR MR2041082 (2005d:11094)

[23] Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347 (electronic). MR MR2156713 (2006k:11118)

[24] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884

[25] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, 2008.

[26] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.

[27] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, 2010.

[28] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885. MR MR2457355

[29] Kevin Buzzard and L. J. P. Kilford, *The 2-adic eigencurve at the boundary of weight space*, Compos. Math. **141** (2005), no. 3, 605–619. MR MR2135280 (2005m:11101)

[30] Robert Carls, *Theta null points of 2-adic canonical lifts*, 2005.

[31] ———, *Explicit Frobenius lifts on elliptic curves*, 2009.

[32] ———, *Fast point counting on genus two curves in characteristic three*, 2010.

[33] Robert Carls and David Lubicz, *A p-adic quasi-quadratic time point counting algorithm*, Int. Math. Res. Not. IMRN (2009), no. 4, 698–735. MR MR2480098

[34] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d'equations dans les corps finis*, 2006.

[35] Denis Charles and Kristin Lauter, *Computing modular polynomials*, LMS J. Comput. Math. **8** (2005), 195–204 (electronic). MR MR2166572

[36] Denis Xavier Charles, *Complex multiplication tests for elliptic curves*, 2004.

[37] Imin Chen, *On the equation* $s^2 + y^{2p} = \alpha^3$, Math. Comp. **77** (2008), no. 262, 1223–1227. MR MR2373199

[38] Imin Chen and Chris Cummins, *Elliptic curves with nonsplit mod 11 representations*, Math. Comp. **73** (2004), no. 246, 869–880 (electronic). MR MR2031412 (2004m:11083)

[39] Robert F. Coleman and William A. Stein, *Approximation of eigenforms of infinite slope by eigenforms of finite slope*, Geometric Aspects of Dwork Theory. Vol. I, II, Walter de Gruyter GmbH & Co. KG, Berlin, 2004, pp. 437–449. MR MR2023296 (2005h:11092)

[40] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731. MR MR2183392 (2006m:11080)

[41] Brian Conrad, Bas Edixhoven, and William Stein, $J_1(p)$ *has connected fibers*, Doc. Math. **8** (2003), 331–408 (electronic). MR MR2029169 (2004k:11094)

[42] Caterina Consani and Jasper Scholten, *Arithmetic on a quintic threefold*, Internat. J. Math. **12** (2001), no. 8, 943–972. MR MR1863287 (2002h:11058)

[43] Patrick Kenneth Corn, *Del Pezzo Surfaces and the Brauer-Manin obstruction*, PhD Thesis, University of California, Berkley, 1998.

[44] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm, *Arithmetic equivalence for function fields, the Goss zeta function and a generalisation*, J. Number Theory **130** (2010), no. 4, 1000–1012. MR 2600417

[45] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second ed., Cambridge University Press, Cambridge, 1997. MR MR1628193 (99e:11068)

[46] 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** (2008), 121–155. MR MR2384334

[47] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves, II: Geometry*, J. reine angew. Math **2009** (2009), no. 632, 63–84.

[48] J. E. Cremona, T. A. Fisher, and M. Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra and Number Theory **4** (2010), no. 6, 763–820.

[49] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR MR2367320 (2008k:11057)

[50] J. E. Cremona, M. Prickett, and Samir Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68. MR MR2197860 (2006k:11121)

[51] John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29. MR MR2282912 (2007k:11087)

[52] John E. Cremona, *A solution for note 84.35*, The Mathematical Gazette **86** (2002), no. 505, 66–68.

[53] John Cullinan, *A computational approach to the 2-torsion structure of abelian threefolds*, Math. Comp. **78** (2009), no. 267, 1825–1836. MR MR2501078

[54] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2, Z)$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. MR MR2016709 (2004i:11037)

[55] Samit Dasgupta, *Computations of elliptic units for real quadratic fields*, Canad. J. Math. **59** (2007), no. 3, 553–574. MR MR2319158

[56] Chantal David and Tom Weston, *Local torsion on elliptic curves and the deformation theory of Galois representations*, Math. Res. Lett. **15** (2008), no. 3, 599–611. MR MR2407234 (2009e:11109)

[57] Christophe Delaunay and Christian Wuthrich, *Self-points on elliptic curves of prime conductor*, Int. J. Number Theory **5** (2009), no. 5, 911–932. MR MR2553516

[58] Daniel Delbourgo and Thomas Ward, *The growth of CM periods over false Tate extensions*, Experiment. Math. **19** (2010), no. 2, 195–210. MR 2676748

[59] Daniel Delbourgo and Tom Ward, *Non-abelian congruences between L-values of elliptic curves*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 3, 1023–1055. MR MR2427518 (2009i:11129)

[60] Lassina Dembélé, *A non-solvable Galois extension of Q ramified at 2 only*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 3-4, 111–116. MR MR2538094

[61] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at* 3 *and* 5, 2009.

[62] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)

[63] Xavier Charles Denis, *Complex multiplication tests for elliptic curves*, 2004.

[64] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611. MR MR2438510

[65] Luis Dieulefait, E. Gonzalez-Jimenez, and J. Jimenez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, arXiv:0909.1661v1 (2009).

[66] T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272, With an appendix by J. Coates and R. Sujatha. MR MR2294995 (2008g:11106)

[67] Tim Dokchitser and Vladimir Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 516–524. MR MR2418807

[68] Tim Dokchitser and Vladimir Dokchitser, *A note on the Mordell-Weil rank modulo n*, 2009.

[69] Darrin Doud, *A procedure to calculate torsion of elliptic curves over* $\mathbf{Q}$, Manuscripta Math. **95** (1998), no. 4, 463–469. MR MR1618198 (99c:11067)

[70] Andrej Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42(62)** (2007), no. 1, 3–18. MR MR2332654 (2008e:11062)

[71] S. Duquesne, *Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem*, Manuscripta Math. **108** (2002), no. 2, 191–204. MR MR1918586 (2003e:11067)

[72] Sylvain Duquesne, *Points rationnels et méthode de Chabauty elliptique*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 99–113, Les XXIIèmes Journées Arithmetiques (Lille, 2001). MR MR2019003 (2005a:11074)

[73] ———, *Elliptic curves associated with simplest quartic fields*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 81–100. MR MR2332055 (2008e:11063)

[74] Sylvain Duquesne, *Montgomery ladder for all genus 2 curves in characteristic 2*, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol. 5130, Springer, 2008, pp. 174–188.

[75] ———, *Traces of the group law on the Kummer surface of a curve of genus* 2 *in characteristic* 2, Math. Comput. Sci. **3** (2010), no. 2, 173–183.

[76] Bas Edixhoven, *On the computation of the coefficients of a modular form*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 30–39. MR MR2282913 (2007k:11085)

[77] Kirsten Eisentraeger, Dimitar Jetchev, and Kristin Lauter, *On the computation of the Cassels pairing for certain Kolyvagin classes in the Shafarevich-Tate group*, 2008, pp. 113–125.

[78] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, 2007.

[79] Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007.

[80] ———, *Shimura curve computations via K3 surfaces of Neron-Severi rank at least 19*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 196–211.

[81] Noam D. Elkies and Mark Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 42–56. MR MR2137342 (2006c:11065)

[82] Arsen Elkin, *Hyperelliptic Jacobians with real multiplication*, J. Number Theory **117** (2006), no. 1, 53–86. MR MR2204735 (2006j:11081)

[83] Andreas-Stephan Elsenhans and Jörg Jahnel, *K3 surfaces of Picard rank one and degree two*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 212–225.

[84] G. Everest and T. Ward, *The canonical height of an algebraic point on an elliptic curve*, New York J. Math. **6** (2000), 331–342 (electronic). MR MR1800354 (2001j:11056)

[85] Graham Everest, Patrick Ingram, Valéry Mahé, and Shaun Stevens, *The uniform primality conjecture for elliptic curves*, Acta Arith. **134** (2008), no. 2, 157–181. MR MR2429645

[86] Graham Everest, Patrick Ingram, and Shaun Stevens, *Primitive divisors on twists of Fermat's cubic*, LMS J. Comput. Math. **12** (2009), 54–81. MR MR2486632

[87] Graham Everest and Valéry Mahé, *A generalization of Siegel's theorem and Hall's conjecture*, Experiment. Math. **18** (2009), no. 1, 1–9. MR MR2548983

[88] Graham Everest, Ouamporn Phuksuwan, and Shaun Stevens, *The uniform primality conjecture for the twisted Fermat cubic*, arXiv:1003.2131v2 (2010).

[89] Xander Faber and Benjamin Hutz, *On the number of rational iterated pre-images of the origin under quadratic dynamical systems*, 2008.

[90] Reza Rezaeian Farashahi and Ruud Pellikaan, *The quadratic extension extractor for (hyper)elliptic curves in odd characteristic*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 4547, Springer, Berlin, 2007, pp. 219–236. MR MR2387145 (2009a:11252)

[91] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **To appear** (2010).

[92] Julio Fernández, Josep González, and Joan-C. Lario, *Plane quartic twists of $X(5,3)$*, Canad. Math. Bull. **50** (2007), no. 2, 196–205. MR MR2317442 (2008b:11067)

[93] Luís R. A. Finotti, *Degrees of the elliptic Teichmüller lift*, J. Number Theory **95** (2002), no. 2, 123–141. MR MR1924093 (2003m:11089)

[94] ———, *Minimal degree liftings of hyperelliptic curves*, J. Math. Sci. Univ. Tokyo **11** (2004), no. 1, 1–47. MR MR2044910 (2005a:11087)

[95] ———, *Minimal degree liftings in characteristic 2*, J. Pure Appl. Algebra **207** (2006), no. 3, 631–673. MR MR2265544 (2007g:11068)

[96] ———, *Lifting the j-invariant: Questions of Mazur and Tate*, J. Number Theory **130** (2010), no. 3, 620–638.

[97] Tom Fisher, *The Hessian of a genus one curve*, 2006.

[98] ———, *Testing equivalence of ternary cubics*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 333–345. MR MR2282934 (2007j:11074)

[99] ———, *A new approach to minimising binary quartics and ternary cubics*, Math. Res. Lett. **14** (2007), no. 4, 597–613. MR MR2335986 (2008k:11058)

[100] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246

[101] ———, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138. MR MR2467841 (2009m:11078)

[102] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR MR2103661 (2005j:11047)

[103] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR MR2402033

[104] E. V. Flynn and J. Wunderle, *Cycles of covers*, Monatsh. Math. **Online first** (2008), 16.

[105] David Freeman, Peter Stevenhagen, and Marco Streng, *Abelian varieties with prescribed embedding degree*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 60–73.

[106] S. D. Galbraith, J. F. McKee, and P. C. Valença, *Ordinary abelian varieties having small embedding degree*, Finite Fields Appl. **13** (2007), no. 4, 800–814. MR MR2359321

[107] Steven D. Galbraith, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)

[108] Irene García-Selfa, Enrique González-Jiménez, and José M. Tornero, *Galois theory, discriminants and torsion subgroup of elliptic curves*, J. Pure Appl. Algebra **214** (2010), no. 8, 1340–1346. MR 2593667 (2011b:11076)

[109] P. Gaudry and É. Schost, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), no. 249, 429–454 (electronic). MR MR2085901 (2006b:11062)

[110] Pierrick Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, 2004.

[111] Pierrick Gaudry and Robert Harley, *Counting points on hyperelliptic curves over finite fields*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 313–332. MR MR1850614 (2002f:11072)

[112] Eknath Ghate, Enrique González-Jiménez, and Jordi Quer, *On the Brauer class of modular endomorphism algebras*, Int. Math. Res. Not. (2005), no. 12, 701–723. MR MR2146605 (2006b:11058)

[113] Jean Gillibert, *Invariants de classes: exemples de non-annulation en dimension supérieure*, Math. Ann. **338** (2007), no. 2, 475–495. MR MR2302072 (2008c:11089)

[114] Edray Goins, *Explicit descent via 4-isogeny on an elliptic curve*, 2004.

[115] Josep González and Jordi Guàrdia, *Genus two curves with quaternionic multiplication and modular Jacobian*, Math. Comp. **78** (2009), no. 265, 575–589. MR MR2448722

[116] Josep González, Jordi Guàrdia, and Victor Rotger, *Abelian surfaces of* GL_2*-type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287. MR MR2114780 (2005m:11107)

[117] Josep González and Victor Rotger, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan **58** (2006), no. 4, 927–948. MR MR2276174 (2007k:11093)

[118] Enrique González-Jiménez, Josep González, and Jordi Guàrdia, *Computations on modular Jacobian surfaces*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 189–197. MR MR2041083 (2005c:11074)

[119] Enrique González-Jiménez and Roger Oyono, *Non-hyperelliptic modular curves of genus 3*, J. Number Theory **130** (2010), no. 4, 862–878. MR 2600407

[120] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.

[121] ———, *On symmetric square values of quadratic polynomials*, 2010.

[122] Eyal Z. Goren and Kristin E. Lauter, *The distance between superspecial abelian varieties with real multiplication*, J. Number Theory **129** (2009), no. 6, 1562–1578. MR MR2521493

[123] Eyal Z. Goren and Kristin E. Lauter, *Genus* 2 *curves with complex multiplication*, arXiv:1003.4759v1 (2010).

[124] Matthew Greenberg, *Computing Heegner points arising from Shimura curve parametrizations*, 2006.

[125] ———, *Heegner point computations via numerical p-adic integration*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 4076, Springer Berlin / Heidelberg, 2006, pp. 361–376.

[126] ———, *Heegner Points and Rigid Analytic Modular Forms*, PhD Thesis, McGill University, 2006.

[127] 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.*

[128] Jordi Guàrdia, *Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 4, 1253–1283. MR MR2339331 (2008g:11105)

[129] Brian Hansen, *Explicit computations supporting a generalization of Serre's conjecture*, MSc, Brigham Young University, 2005.

[130] Robin Hartshorne and Ronald van Luijk, *Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on* $K3$ *surfaces*, Math. Intelligencer **30** (2008), no. 4, 4–10. MR MR2501390

[131] Ki-ichiro Hashimoto, Katsuya Miyake, and Hiroaki Nakamura (eds.), *Galois Theory and Modular Forms*, Developments in Mathematics, vol. 11, Boston, MA, Kluwer Academic Publishers, 2004. MR MR2059977 (2004k:11003)

[132] Brendan Hassett, Anthony Vàrilly-Alvarado, and Patrick Varilly, *Transcendental obstructions to weak approximation on general* $K3$ *surfaces*, 2010.

[133] Florian Hess, *Computing relations in divisor class groups of algebraic curves over finite fields*, 2003.

[134] ———, *A note on the Tate pairing of curves over finite fields*, Arch. Math. (Basel) **82** (2004), no. 1, 28–32. MR MR2034467 (2004m:14040)

[135] Laura Hitt, *Families of genus 2 curves with small embedding degree*, J. Math. Cryptol. **3** (2009), no. 1, 19–36. MR MR2524253

[136] 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** (2003), no. 6, 1677–1737. MR MR2038778 (2005c:11079)

[137] Everett W. Howe, *Infinite families of pairs of curves over Q with isomorphic Jacobians*, J. London Math. Soc. (2) **72** (2005), no. 2, 327–350. MR MR2156657 (2006b:11064)

[138] ———, *Supersingular genus-2 curves over fields of characteristic 3*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 49–69. MR MR2459989 (2009j:11103)

[139] Everett W. Howe, Kristin E. Lauter, and Jaap Top, *Pointless curves of genus three and four*, Arithmetic, Geometry and Coding Theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 125–141. MR MR2182840 (2006g:11125)

[140] 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** (2002), no. 1, 139–163. MR MR1880590 (2003g:11063)

[141] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR MR2403533

[142] ———, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.

[143] 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** (2005), 103–146. MR MR2164402

[144] 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** (2005), no. 4, 667–681. MR MR2226624 (2007b:11092)

[145] Patrick Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory **129** (2009), no. 1, 182–208. MR MR2468477 (2010a:11102)

[146] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)

[147] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 219–233.

[148] Dimitar Jetchev, Kristin Lauter, and William Stein, *Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich-Tate group*, J. Number Theory **129** (2009), no. 2, 284 – 302.

[149] Dimitar P. Jetchev and William A. Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696. MR MR2377239

[150] Jorge Jimenez-Urroz and Tonghai Yang, *Heegner zeros of theta functions*, Trans. Amer. Math. Soc. **355** (2003), no. 10, 4137–4149 (electronic). MR MR1990579 (2005e:11070)

[151] Rafe Jones and Jeremy Rouse, *Galois theory of iterated endomorphisms*, Proc. London Math. Soc. **(3) 100** (2010), 763–794.

[152] David Joyner and Amy Ksir, *Modular representations on some Riemann-Roch spaces of modular curves X(N)*, Computational Aspects of Algebraic Curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 163–205. MR MR2182040 (2006k:11112)

[153] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.

[154] Koray Karabina and Edlyn Teske, *On prime-order elliptic curves with embedding degrees k=3,4, and 6*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 102–117.

[155] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, J. Number Theory **97** (2002), no. 1, 157–164. MR MR1939142 (2003j:11046)

[156] ———, *Slopes of 2-adic overconvergent modular forms with small level*, Math. Res. Lett. **11** (2004), no. 5-6, 723–739. MR MR2106238 (2005h:11093)

[157] L. J. P. Kilford, *On a p-adic extension of the Jacquet-Langlands correspondence to weight 1*, 2008.

[158] David R. Kohel, *Hecke module structure of quaternions*, Class Field Theory—Its Centenary and Prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 177–195. MR MR1846458 (2002i:11059)

[159] ———, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)

[160] David R. Kohel and William A. Stein, *Component groups of quotients of $J_0(N)$*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 405–412. MR MR1850621 (2002h:11051)

[161] David R. Kohel and Helena A. Verrill, *Fundamental domains for Shimura curves*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 205–222, Les XXIIèmes Journées Arithmetiques (Lille, 2001). MR MR2019012 (2004k:11096)

[162] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518 (electronic). MR MR2085904 (2005g:11103)

[163] Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 363–374. MR MR2418792

[164] Andrew Kresch and Yuri Tschinkel, *Integral points on punctured abelian surfaces*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 198–204. MR MR2041084 (2005d:11081)

[165] 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** (2004), no. 2, 241–267. MR MR2098638 (2005h:11130)

[166] Dominic Lanphier, *The trace of special values of modular L-functions*.

[167] Alan G. B. Lauder, *Ranks of elliptic curves over function fields*, LMS J. Comput. Math. **11** (2008), 172–212. MR MR2429996

[168] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.

[169] 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** (2004), 193–203. MR MR2112831 (2005h:11131)

[170] 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** (2003), no. 4, 401–410. MR MR2011317 (2004j:11053)

[171] Reynald Lercier and David Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), no. 3, 399–423. MR MR2293798 (2008b:11069)

[172] 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** (2008), no. 3, 783–797. MR MR2523317

[173] Petr Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, Sequences and Their Applications – SETA 2008: Proceedings (Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, eds.), Lecture Notes in Computer Science, vol. 5203, Springer, Berlin Heidelberg, 2008, pp. 182–187.

[174] Adam Logan and Ronald van Luijk, *Nontrivial elements of Sha explained through $K3$ surfaces*, Math. Comp. **78** (2009), no. 265, 441–483. MR MR2448716

[175] Ling Long and Chris Kurth, *On modular forms for some noncongruence subgroups of $SL_2Z)$ II*, 2008.

[176] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Coleman-Chabauty*, 2000.

[177] Álvaro Lozano-Robledo, *On the product of twists of rank two and a conjecture of Larsen*, Ramanujan J. **19** (2009), no. 1, 53–61. MR MR2501236 (2010b:11062)

[178] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304. MR MR2305419

[179] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)

[180] 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** (2009), no. 267, 1767–1786. MR MR2501074

[181] 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** (2008), no. 1, 67–76. MR MR2382590 (2008m:11122)

[182] Josep M. Miret, Jordi Pujolàs, and Anna Rio, *Bisection for genus 2 curves in odd characteristic*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), no. 4, 55–60. MR MR2517297 (2010d:14039)

[183] Jan-Steffen Müller, *Explicit Kummer surface theory for arbitrary characteristic*, London Math. Soc. J. Comput. Math. **13** (2010), 47–64.

[184] Filip Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), no. 9, 1964–1968. MR 2653208

[185] Annika Niehage, *Quantum Goppa codes over hypereliptic curves*, Diplomarbeit, Universität Mannheim, 2004.

[186] Ekin Ozman, *Local points on quadratic twists of $X_0(N)$*, 2009.

[187] Mihran Papikian, *On the degree of modular parametrizations over function fields*, J. Number Theory **97** (2002), no. 2, 317–349. MR MR1942964 (2004c:11104)

[188] ———, *On the variation of Tate-Shafarevich groups of elliptic curves over hyperelliptic curves*, J. Number Theory **115** (2005), no. 2, 249–283. MR MR2180501 (2006g:11111)

[189] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186. MR MR2016704 (2005h:11138)

[190] Bjorn Poonen, *Computational aspects of curves of genus at least 2*, Algorithmic Number Theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 283–306. MR MR1446520 (98c:11059)

[191] 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** (2007), no. 1, 103–158. MR MR2309145

[192] Lisa Marie Redekop, *Torsion Points of Low Order on Elliptic Curves and Drinfeld Modules*, Ph.D. thesis, 2002, p. 95.

[193] Jonathan Reynolds, *Extending Siegel's theorem for elliptic curves*, Phd thesis, University of East Anglia, 2008.

[194] Guillaume Ricotta and Thomas Vidick, *Hauteur asymptotique des points de Heegner*, Canad. J. Math. **60** (2008), no. 6, 1406–1436. MR MR2462452

[195] Christophe Ritzenthaler, *Automorphismes des courbes modulaires $X(n)$ en caractéristique p*, Manuscripta Math. **109** (2002), no. 1, 49–62. MR MR1931207 (2003g:11067)

[196] ———, *Point counting on genus 3 non hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 379–394. MR MR2138009 (2006d:11065)

[197] Christophe Ritzenthaler, *Explicit computations of Serre's obstruction for genus 3 curves and application to optimal curves*, LMS Journal of Computation and Mathematics **13** (2010), 192–207.

[198] Mohammad Sadek, *Counting models of genus one curves*, 2010.

[199] David Savitt, *The maximum number of points on a curve of genus 4 over F_8 is 25*, Canad. J. Math. **55** (2003), no. 2, 331–352, With an appendix by Kristin Lauter. MR MR1969795 (2004i:11059)

[200] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231 (electronic). MR MR2021618 (2004g:11045)

[201] Jasper Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, 2004.

[202] Andreas M. Schöpp, *Über torsionspunkte elliptischer und hyperelliptischer kurven nebst anwendungen*, Ph.D. thesis, Technische Universitaet Berlin,, April 2005, p. 92.

[203] Samir Siksek, *On standardized models of isogenous elliptic curves*, Math. Comp. **74** (2005), no. 250, 949–951 (electronic). MR MR2114657 (2005i:11076)

[204] ———, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236. MR MR2491943 (2010b:11069)

[205] Samir Siksek and John E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109** (2003), no. 2, 143–149. MR MR1980642 (2004c:11109)

[206] Samir Siksek and Michael Stoll, *On a problem of Hajdu and Tengely*, 2009.

[207] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.

[208] ———, *Families of explicit isogenies of hyperelliptic Jacobians*, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 521, AMS, Providence, R.I., 2009, pp. 121–144.

[209] Sebastian Karl Michael Stamminger, *Explicit 8-descent on elliptic curves*, Ph.D. thesis, International University Bremen, 2005, p. 107.

[210] William Stein, *Studying the Birch and Swinnerton-Dyer conjecture for modular abelian varieties using Magma*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 93–116. MR MR2278924

[211] William A. Stein, *There are genus one curves over* Q *of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147. MR MR1900139 (2003c:11059)

[212] ———, *Shafarevich-Tate groups of nonsquare order*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 277–289. MR MR2058655 (2005c:11072)

[213] ———, *Visibility of Mordell-Weil groups*, Doc. Math. **12** (2007), 587–606. MR MR2377241 (2009a:11128)

[214] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR MR1829626 (2002b:11089)

[215] ———, *On the height constant for curves of genus two. II*, Acta Arith. **104** (2002), no. 2, 165–182. MR MR1914251 (2003f:11093)

[216] Michael Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, LMS J. Comput. Math. **11** (2008), 367–380.

[217] Fritz Grunewald Tatiana Bandman, Shelly Garion, *On the surjectivity of engel words on psl(2,q)*, 2010, pp. 1–22.

[218] Thotsaphon Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over totally real number fields*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 139–152.

[219] Hans-Christian Graf v. Bothmer, *Finite field experiments (with an appendix by Stefan Wiedmann)*, Higher-Dimensional Geometry over Finite Fields, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 16, IOS Press, 2008, pp. 1–62.

[220] Anthony Vàrilly-Alvarado and Bianca Viray, *Failure of the Hasse principle for Enriques surfaces*, Advances in Mathematics **226** (2011), 4884–4901.

[221] Marie-France Vignéras, *p-adic integral structures of some representations of GL(2, F)*, 2005.

[222] Bogdan G. Vioreanu, *Mordell-Weil problem for cubic surfaces, numerical evidence*, 2008.

[223] Bianca Viray, *A family of varieties with exactly one pointless rational fiber*, 2009.

[224] Mark Watkins, *A note on integral points on elliptic curves*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 707–720. MR MR2330437 (2008e:11069)

[225] Mark Watkins, *Some remarks on Heegner point computations*, 2006.

[226] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125. MR MR2410120

[227] Rolf Stefan Wilke, *On rational embeddings of curves in the second Garcia-Stichtenoth tower*, Finite Fields Appl. **14** (2008), no. 2, 494–504. MR MR2401990 (2009a:11131)

[228] Christian Wuthrich, *The fine Tate-Shafarevich group*, Math. Proc. Cambridge Philos. Soc. **142** (2007), no. 1, 1–12. MR MR2296386 (2008b:11064)

[229] ———, *Self-points on an elliptic curve of conductor 14*, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007, pp. 189–195. MR MR2402010 (2009e:11112)

[230] Chaoping Xing, *Applications of algebraic curves to constructions of sequences*, Cryptography and Computational Number Theory (Singapore, 1999), Progr. Comput. Sci. Appl. Logic, vol. 20, Birkhäuser, Basel, 2001, pp. 137–146. MR MR1944725 (2004e:11068)

[231] Chaoping Xing and Sze Ling Yeo, *Construction of global function fields from linear codes and vice versa*, Trans. Amer. Math. Soc. **361** (2008), no. 3, 1333–1349.

[232] Huilin Zhu and Jianhua Chen, *Integral points on a class of elliptic curve*, Wuhan Univ. J. Nat. Sci. **11** (2006), no. 3, 477–480. MR MR2258847 (2007d:11064)

Geometry of Numbers

11Hxx

[1] Kanat Abdukhalikov, *Unimodular Hermitian lattices*, Mathematisches Forschungsinstitut Oberwolfach Report No. 1/2005 (2005), 27–30.

[2] Kanat Abdukhalikov and Rudolf Scharlau, *Unimodular lattices in dimensions 14 and 15 over the Eisenstein integers*, Math. Comp. **78** (2009), no. 265, 387–403. MR MR2448712

[3] Christine Bachoc and Gabriele Nebe, *Classification of two genera of 32-dimensional lattices of rank 8 over the Hurwitz order*, Experiment. Math. **6** (1997), no. 2, 151–162. MR MR1474575 (98g:11078)

[4] Christine Bachoc and Boris Venkov, *Modular forms, lattices and spherical designs*, Réseaux Euclidiens, Designs Sphériques et Formes Modulaires, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, pp. 87–111. MR MR1878746 (2003d:11096)

[5] Werner Backes and Susanne Wetzel, *Heuristics on lattice basis reduction in practice*, ACM J. Exp. Algorithmics **7** (2002), 21 pp. (electronic), Fourth Workshop on Algorithm Engineering (Saarbrücken, 2000). MR MR1973646 (2004c:68162)

[6] Siegfried Boecherer and Gabriele Nebe, *On theta series attached to maximal lattices and their adjoints*, 2009.

[7] Robin Chapman, Steven T. Dougherty, Philippe Gaborit, and Patrick Solé, *2-modular lattices from ternary codes*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 73–85. MR MR1925991 (2004g:94091)

[8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR MR1662447 (2000b:11077)

[9] R. Coulangeon, M. I. Icaza, and M. O'Ryan, *Lenstra's constant and extreme forms in number fields*, Experiment. Math. **16** (2007), no. 4, 455–462. MR MR2378486 (2008m:11131)

[10] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin, *A generalization of Voronoi's reduction theory and its application*, Duke Math. J. **142** (2008), no. 1, 127–164. MR MR2397885 (2009a:11141)

[11] C. Fieker and M. E. Pohst, *On lattices over number fields*, Algorithmic Number Theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 133–139. MR MR1446505 (98g:11079)

[12] Philippe Gaborit, *Construction of new extremal unimodular lattices*, European J. Combin. **25** (2004), no. 4, 549–564. MR MR2069381 (2006a:11088)

[13] Paul E. Gunnells and Dan Yasaki, *Perfect forms over totally real number fields*, 2009.

[14] Masaaki Harada, *On the existence of frames of the Niemeier lattices and self-dual codes over F_p*, J. Algebra **321** (2009), no. 8, 2345–2352. MR MR2501524 (2010c:94066)

[15] Masaaki Harada, Masaaki Kitazume, and Michio Ozeki, *Ternary code construction of unimodular lattices and self-dual codes over Z_6*, J. Algebraic Combin. **16** (2002), no. 2, 209–223. MR MR1943589 (2004b:11099)

[16] Boris Hemkemeier, *Algorithmische konstruktionen von gittern*, 2004.

[17] Jacques Martinet and Achill Schürmann, *On classifying Minkowskian sublattices*, 2009.

[18] G. Nebe, *Kneser-Hecke-operators in coding theory*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 79–90. MR MR2293434 (2007m:11090)

[19] Gabriele Nebe, *Finite quaternionic matrix groups*, Represent. Theory **2** (1998), 106–223 (electronic). MR MR1615333 (99f:20085)

[20] ———, *Even lattices with covering radius $< \sqrt{2}$*, Beiträge Algebra Geom. **44** (2003), no. 1, 229–234. MR MR1990996 (2004c:11120)

[21] ———, *Strongly modular lattices with long shadow*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 187–196. MR MR2145580 (2006c:11077)

[22] Gabriele Nebe, *An even unimodular 72-dimensional lattice of minimum 8*, 2010.

[23] Gabriele Nebe and Kristina Schindelar, *S-extremal strongly modular lattices*, J. Théor. Nombres Bordeaux **19** (2007), no. 3, 683–701. MR MR2388794

[24] Gabriele Nebe and Boris Venkov, *The strongly perfect lattices of dimension 10*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 503–518, Colloque International de Théorie des Nombres (Talence, 1999). MR MR1823200 (2002f:11081)

[25] ———, *Low-dimensional strongly perfect lattices I: The 12-dimensional case*, Enseign. Math. (2) **51** (2005), no. 1-2, 129–163. MR MR2154624 (2006b:11069)

[26] Gabriele Nebe and Boris Venkov, *Low dimensional strongly perfect lattices III: Dual strongly perfect lattices of dimension 14*, IJNT **2** (2010), no. 2, 387–409.

[27] Gabriele Nebe and Chaoping Xing, *A Gilbert-Varshamov type bound for Euclidean packings*, Math. Comp. **77** (2008), no. 264, 2339–2344. MR MR2429888

[28] Phong Q. Nguyen and Damien Stehlé, *LLL on the average*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 238–256. MR MR2282928 (2008a:11154)

[29] W. Plesken and M. Pohst, *Constructing integral lattices with prescribed minimum. I*, Math. Comp. **45** (1985), no. 171, 209–221, S5–S16. MR MR790654 (87e:11077)

[30] ———, *Constructing integral lattices with prescribed minimum. II*, Math. Comp. **60** (1993), no. 202, 817–825. MR MR1176715 (93h:11070)

[31] E. M. Rains and N. J. A. Sloane, *The shadow theory of modular and unimodular lattices*, J. Number Theory **73** (1998), no. 2, 359–389. MR MR1657980 (99i:11053)

[32] Achill Schürmann, *Enumerating perfect forms*, Proceedings of the International Conference on Quadratic Forms, Chile 2007, Contemporary Mathematics, vol. To appear, 2009.

[33] ———, *Perfect, strongly eutactic lattices are periodic extreme*, Adv. Math **225** (2010), no. 5, 2546–2564.

[34] Achill Schürmann and Frank Vallentin, *Local covering optimality of lattices: Leech lattice versus root lattice E_8*, Int. Math. Res. Not. (2005), no. 32, 1937–1955. MR MR2173600 (2006i:11076)

[35] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin, *Classification of eight-dimensional perfect forms*, Electron. Res. Announc. Amer. Math. Soc. **13** (2007), 21–32 (electronic). MR MR2300003

[36] 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** (1995), no. 3, 237–259. MR MR1344734 (96m:52033)

[37] Anthony Várilly-Alvarado and David Zywina, *Arithmetic E_8 lattices with maximal Galois action*, LMS J. Comput. Math. **12** (2009), 144–165. MR MR2559115

Probabilistic Theory

11Kxx

[1] Wieb Bosma, Karma Dajani, and Cor Kraaikamp, *Entropy quotients and correct digits in number-theoretic expansions*, Dynamics and Stochastics, IMS Lecture Notes Monogr. Ser., vol. 48, Inst. Math. Statist., Beachwood, OH, 2006, pp. 176–188. MR MR2306199

Zeta and L-functions: Analytic Theory

11Mxx

[1] Peter Borwein, Greg Fee, Ron Ferguson, and Alexa van der Waall, *Zeros of partial sums of the Riemann zeta function*, Experiment. Math. **16** (2007), no. 1, 21–39. MR MR2312975 (2008a:11099)

[2] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731. MR MR2183392 (2006m:11080)

[3] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm, *Arithmetic equivalence for function fields, the Goss zeta function and a generalisation*, J. Number Theory **130** (2010), no. 4, 1000–1012. MR 2600417

[4] 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** (1999), no. 3, 511–534. MR MR1710163 (2000k:11103)

[5] Marcus du Sautoy and Luke Woodward, *Nilpotent groups: Explicit examples*, Zeta Functions of Groups and Rings, Lecture Notes in Computer Science, vol. 1925/2008, Springer Berlin / Heidelberg, 2008, pp. 21–68.

[6] Ralf Gerkmann, *Relative rigid cohomology and deformation of hypersurfaces*, Int. Math. Res. Pap. IMRP (2007), no. 1, Art. ID rpm003, 67. MR MR2334009

[7] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, 2008, pp. 312–326.

[8] Emmanuel Kowalski, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, Int. Math. Res. Not. IMRN (2008), Art. ID rnn 091, 57. MR MR2439552

[9] Alan G. B. Lauder, *A recursive method for computing zeta functions of varieties*, LMS J. Comput. Math. **9** (2006), 222–269 (electronic). MR MR2261044 (2007g:14022)

[10] Phil Martin and Mark Watkins, *Symmetric powers of elliptic curve L-functions*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 377–392. MR MR2282937 (2007i:11087)

[11] Moritz Minzlaff, *Computing zeta functions of superelliptic curves in larger characteristic*, Math. Comput. Sci. **3** (2010), 209–224.

[12] Christopher Voll, *Normal subgroup growth in free class-2-nilpotent groups*, Math. Ann. **332** (2005), no. 1, 67–79. MR MR2139251

[13] Alexey Zaytsev and Gary McGuire, *On the zeta functions of an optimal tower of function fields over F_4*, 2009.

Additive and Multiplicative Number Theory

11Pxx, 11Nxx

[1] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690 (electronic). MR MR2299795 (2007m:11170)

[2] Wieb Bosma and Ben Kane, *The Aliquot constant*, 2009.

[3] Javier Cilleruelo, *The least common multiple of a quadratic sequence*, Compositio Mathematica **To appear** (2010).

[4] H. Dubner, T. Forbes, N. Lygeros, M. Mizony, H. Nelson, and P. Zimmermann, *Ten consecutive primes in arithmetic progression*, Math. Comp. **71** (2002), no. 239, 1323–1328 (electronic). MR MR1898760 (2003d:11137)

[5] Sharon Anne Garthwaite, *Convolution congruences for the partition function*, Proc. Amer. Math. Soc. **135** (2007), no. 1, 13–20 (electronic). MR MR2280169

[6] F. G. Garvan, *Biranks for partitions into 2 colors*, 2009.

[7] David Zywina, *A refinement of Koblitz's conjecture*, 2009.

Algebraic Number Theory

11Rxx and 11Sxx

[1] Avner Ash, Jos Brakenhoff, and Theodore Zarrabi, *Equality of polynomial and field discriminants*, Experiment. Math. **16** (2007), no. 3, 367–374. MR MR2367325 (2008i:11129)

[2] Laurent Bartholdi and Michael R. Bush, *Maximal unramified 3-extensions of imaginary quadratic fields and* $\mathrm{SL}_2(Z_3)$, J. Number Theory **124** (2007), no. 1, 159–166. MR MR2320997 (2008c:11153)

[3] 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*, 2007.

[4] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic). MR MR2353964

[5] Amnon Besser and Rob De Jeu, li(p)*-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194

[6] Wieb Bosma, *Canonical bases for cyclotomic fields*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), no. 2, 125–134. MR MR1325517 (95k:11135)

[7] ———, *Computation of cyclotomic polynomials with Magma*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 213–225. MR MR1344932 (96j:11142)

[8] Wieb Bosma and Bart de Smit, *On arithmetically equivalent number fields of small degree*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR MR2041074 (2005e:11169)

[9] Wieb Bosma and Peter Stevenhagen, *On the computation of quadratic* 2*-class groups*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313. MR MR1438471 (98e:11129a)

[10] Nigel Boston, *Galois p-groups unramified at p—a survey*, Primes and knots, Contemp. Math., vol. 416, Amer. Math. Soc., Providence, RI, 2006, pp. 31–40. MR MR2276134 (2007k:11191)

[11] ———, *Galois groups of tamely ramified p-extensions*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 59–70. MR MR2332053

[12] Nigel Boston and Rafe Jones, *Arboreal Galois representations*, Geom. Dedicata **124** (2007), 27–35. MR MR2318536

[13] Nigel Boston and Charles Leedham-Green, *Counterexamples to a conjecture of Lemmermeyer*, Arch. Math. (Basel) **72** (1999), no. 3, 177–179. MR MR1671275 (99m:11131)

[14] M. R. Bush, *Computation of Galois groups associated to the 2-class towers of some quadratic fields*, J. Number Theory **100** (2003), no. 2, 313–325. MR MR1978459 (2004f:11130)

[15] Nigel P. Byott, James E. Carter, Cornelius Greither, and Henri Johnston, *On the restricted hilbert-speiser and leopoldt properties*, Illinois J. Math **To appear** (2011).

[16] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.

[17] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Subexponential algorithms for class group and unit computations*, J. Symbolic Comput. **24** (1997), no. 3-4, 433–441, Computational algebra and number theory (London, 1993). MR MR1484490 (98m:11138)

[18] Henri Cohen, *A survey of computational class field theory*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 1–13, Les XXèmes Journées Arithmétiques (Limoges, 1997). MR MR1730429 (2000j:11169)

[19] B. de Smit and H. W. Lenstra, Jr., *Linearly equivalent actions of solvable groups*, J. Algebra **228** (2000), no. 1, 270–285. MR MR1760965 (2001f:20069)

[20] Bart de Smit, *On arithmetically equivalent fields with distinct p-class numbers*, J. Algebra **272** (2004), no. 2, 417–424. MR MR2028064 (2005f:11252)

[21] Bart de Smit and Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 2, 213–215. MR MR1260520 (95a:11100)

[22] Daniel Delbourgo and Thomas Ward, *The growth of CM periods over false Tate extensions*, Experiment. Math. **19** (2010), no. 2, 195–210. MR 2676748

[23] Daniel Delbourgo and Tom Ward, *Non-abelian congruences between L-values of elliptic curves*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 3, 1023–1055. MR MR2427518 (2009i:11129)

[24] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at* 3 *and* 5, 2009.

[25] Darrin Doud, *Supersingular Galois representations and a generalization of a conjecture of Serre*, Experiment. Math. **16** (2007), no. 1, 119–128. MR MR2312982 (2007m:11076)

[26] Kirsten Eisenträger and Kristin Lauter, *Computing Igusa class polynomials via the chinese remainder theory*, 2004.

[27] 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** (2006), no. 2, 723–741. MR MR2199231 (2006j:11159)

[28] Claus Fieker, *Applications of the class field theory of global fields*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62. MR MR2278922

[29] ———, *Sparse representation for cyclotomic fields*, Experiment. Math. **16** (2007), no. 4, 493–500. MR MR2378488

[30] ———, *Minimizing representations over number fields II. Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765. MR MR2531221

[31] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518 (electronic). MR MR2219041 (2007a:11168)

[32] ———, *A lower regulator bound for number fields*, J. Number Theory **128** (2008), no. 10, 2767–2775. MR MR2441075

[33] Felix Fontein, *The infrastructure of a global field of arbitrary unit rank*, 2008.

[34] David Ford, Sebastian Pauli, and Xavier-François Roblot, *A fast algorithm for polynomial factorization over Q_p*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 151–169. MR MR1925995 (2003g:11134)

[35] Robert Fraatz, *On the computation of integral closures of cyclic extensions of function fields*, LMS J. Comput. Math. **10** (2007), 141–160 (electronic). MR MR2308855 (2008b:11123)

[36] Irene García-Selfa, Enrique González-Jiménez, and José M. Tornero, *Galois theory, discriminants and torsion subgroup of elliptic curves*, J. Pure Appl. Algebra **214** (2010), no. 8, 1340–1346. MR 2593667 (2011b:11076)

[37] S. P. Glasby, *Generators for the group of units of Z_n*, Austral. Math. Soc. Gaz. **22** (1995), no. 5, 226–228. MR MR1378923 (97a:11199)

[38] Norbert Goeb, *Computing the automorphism groups of hyperelliptic function fields*, 2003.

[39] Ralph Greenberg, *On the structure of certain Galois cohomology groups*, Doc. Math. (2006), no. Extra Vol., 335–391 (electronic). MR MR2290593 (2008b:11112)

[40] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428v1 (2009).

[41] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, 2008.

[42] Lajos Hajdu, *Optimal systems of fundamental S-units for LLL-reduction*, Period. Math. Hungar. **59** (2009), no. 1, 53–79. MR MR2544620

[43] Emmanuel Hallouin and Christian Maire, *Cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **595** (2006), 189–213. MR MR2244802 (2007g:11146)

[44] Emmanuel Hallouin and Marc Perret, *On the kernel of the norm in some unramified number fields extensions*, 2007.

[45] Stephan Hell, *Die nenner des kontsevich-integrals und ein spezieller drinfeld-assoziator*, Ph.D. thesis, Freie Universität Berlin, July 2002, p. 92.

[46] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 263–271. MR MR2137359

[47] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, 1531–1548 (electronic). MR MR1972751 (2004f:11126)

[48] David Hubbard, *Dihedral side extensions and class groups*, J. Number Theory **128** (2008), no. 4, 731–737. MR MR2400036

[49] 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** (2008), no. 3, 715–732. MR MR2523314

[50] ———, *Computation of 2-groups of narrow logarithmic divisor classes of number fields*, J. Symbolic Comput. **44** (2009), no. 7, 852–863. MR MR2522586 (2010d:11133)

[51] Henri Johnston, *On the trace map between absolutely abelian number fields of equal conductor*, Acta Arith. **122** (2006), no. 1, 63–74. MR MR2217325 (2006k:11203)

[52] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR MR2194887 (2006k:11230)

[53] John Jossey, *Galois 2-extensions unramified outside 2*, J. Number Theory **124** (2007), no. 1, 42–56. MR MR2320990

[54] Masanari Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447. MR MR2172348 (2007h:14061)

[55] Masanari Kida, *Descent Kummer theory via Weil restriction of multiplicative groups*, J. of Number Theory **130** (2010), no. 3, 639–659.

[56] ———, *A Kummer theoretic construction of an S_3-polynomial with given quadratic subfield*, Interdisciplinary Information Sciences **16** (2010), no. 1, 17–20.

[57] Masanari Kida, Guénaël Renault, and Kazuhiro Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer and Kummer*, Int. J. Number Theory **5** (2009), no. 4, 555–571. MR MR2532276

[58] Masanari Kida, Yuichi Rikuna, and Atsushi Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*, IJNT **6** (2010), no. 3, 691–704.

[59] Norbert Klingen, *Leopoldt's conjecture for imaginary Galois number fields*, J. Symbolic Comput. **10** (1990), no. 6, 531–545. MR MR1087978 (92e:11124)

[60] Jürgen Klüners and Gunter Malle, *Counting nilpotent Galois extensions*, J. Reine Angew. Math. **572** (2004), 1–26. MR MR2076117 (2005f:11259)

[61] Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), no. 1, 47–64. MR MR2166795

[62] Elisavet Konstantinou and Aristides Kontogeorgis, *Computing polynomials of the Ramanujan* $\mathbf{t_n}$ *class invariants*, Canad. Math. Bull. **52** (2009), no. 4, 583–597. MR MR2567152

[63] M. Künzer and H. Weber, *Some additive Galois cohomology rings*, Comm. Algebra **33** (2005), no. 12, 4415–4455. MR MR2188320 (2006k:11221)

[64] Matthias Künzer and Eduard Wirsing, *On coefficient valuations of Eisenstein polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 801–823. MR MR2212127 (2006m:11151)

[65] Thorsten Lagemann, *Codes und automorphismen optimaler artin-schreier-turme*, Ph.D. thesis, Ruprecht-Karls-Universität Heidelberg, April 2006, p. 92.

[66] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*, Experiment. Math. **12** (2003), no. 2, 211–225. MR MR2016707 (2004j:11143)

[67] Franck Leprévost, Michael Pohst, and Andreas Schöpp, *Units in some parametric families of quartic fields*, Acta Arith. **127** (2007), no. 3, 205–216. MR MR2310343 (2008a:11133)

[68] Aaron Levin, *Ideal class groups and torsion in Picard groups of varieties*, 2008.

[69] Melissa L. Macasieb, *Derived arithmetic Fuchsian groups of genus two*, Experiment. Math. **17** (2008), no. 3, 347–369. MR MR2455706 (2009i:11135)

[70] Piotr Maciak, *Primes of the form* $x^2 + n * y^2$ *in function fields*, 2009.

[71] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa* λ*-invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304. MR MR2305419

[72] William G. McCallum and Romyar T. Sharifi, *A cup product in the Galois cohomology of number fields*, Duke Math. J. **120** (2003), no. 2, 269–310. MR MR2019977 (2004j:11136)

[73] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group* $c2 \times c2 \times c2$, Journal of Number Theory **129** (2009), no. 1, 231 – 245.

[74] Sebastian Pauli, *Efficient enumeration of extensions of local fields with bounded discriminant*, Ph.D. thesis, Concordia University, June 2001, p. 82.

[75] Sebastian Pauli, *Constructing class fields over local fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 627–652. MR MR2330432 (2008f:11135)

[76] Sebastian Pauli and Florence Soriano-Gafiuk, *The discrete logarithm in logarithmic l-class groups and its applications in K-theory*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 367–378. MR MR2138008 (2006a:11155)

[77] Diana Savin, *About certain prime numbers*, 2009, p. 9.

[78] René Schoof, *Arakelov class groups and ideal lattices*, 2005, pp. 23–24.

[79] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR MR2467554

[80] Andreas M. Schöpp, *Fundamental units in a parametric family of not totally real quintic number fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 693–706. MR MR2330436 (2008f:11121)

[81] Romyar T. Sharifi, *Iwasawa theory and the Eisenstein ideal*, Duke Math. J. **137** (2007), no. 1, 63–101. MR MR2309144

[82] ———, *On Galois groups of unramified pro-p extensions*, Math. Ann. **342** (2008), no. 2, 297–308. MR MR2425144

[83] William Stein and Yan Zhang, *On power bases in number fields*, 2005.

[84] Aliza Steurer, *On the Galois groups of the 2-class towers of some imaginary quadratic fields*, J. Number Theory **125** (2007), no. 1, 235–246. MR MR2333129

[85] Mark van Hoeij and John Cremona, *Solving conics over function fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 595–606. MR MR2330429 (2008f:11133)

[86] Stéphane Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de Q*, J. Number Theory **91** (2001), no. 1, 126–152. MR MR1869322 (2002h:11112)

[87] John Voight, *The gauss higher relative class number problem*, Ann. Sci. Math. Québec **Accepted** (2009).

[88] Gabor Wiese, *On projective linear groups over finite fields as Galois groups over the rational numbers*, Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006, Cambridge University Press, Cambridge, 2008, pp. 343–350. MR)

[89] Qingquan Wu and Renate Scheidler, *An explicit treatment of biquadratic function fields*, Contrib. Discrete Math. **2** (2007), no. 1, 43–60 (electronic). MR MR2291883 (2008a:11144)

[90] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), no. 11, 4132–4142. MR MR2556143

[91] Alexey Zaytsev and Gary McGuire, *On the zeta functions of an optimal tower of function fields over F_4*, 2009.

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** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)

[2] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 37–42. MR MR1849077 (2002e:11175)

[3] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *A few more quadratic APN functions*, 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** (2008), no. 3, 703–714. MR MR2435056

[5] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456

[6] Jessica F. Burkhart, Neil J. Calkin, Shuhong Gao, Justine C. Hyde-Volpe, Kevin James, Hiren Maharaj, Shelly Manber, Jared Ruiz, and Ethan Smith, *Finite field elements of high order arising from modular curves*, Des. Codes Cryptogr. **51** (2009), no. 3, 301–314. MR MR2485499 (2010b:11164)

[7] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.

[8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)

[9] Mihai Cipu and Stephen D. Cohen, *Dickson polynomial permutations*, Finite Fields and Applications, Contemporary Mathematics, vol. 461, 2008.

[10] Stephen D. Cohen, *Finite field elements with specified order and traces*, Des. Codes Cryptogr. **36** (2005), no. 3, 331–340. MR MR2163064

[11] ———, *Primitive polynomials with a prescribed coefficient*, Finite Fields Appl. **12** (2006), no. 3, 425–491. MR MR2229326 (2007e:11141)

[12] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's p^s-polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)

[13] ———, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), no. 3, 317–328. MR MR2053506 (2005b:13013)

[14] Robert S. Coulter and Marie Henderson, *The compositional inverse of a class of permutation polynomials over a finite field*, Bull. Austral. Math. Soc. **65** (2002), no. 3, 521–526. MR MR1910505 (2003f:11185)

[15] Jean-Marc Couveignes and Reynald Lercier, *Elliptic periods for finite fields*, Finite Fields Appl. **15** (2009), no. 1, 1–22. MR MR2468989 (2009j:12006)

[16] Yves Edel and Alexander Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), no. 1, 59–81. MR MR2476525 (2010c:11154)

[17] 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** (1999), no. 1, 74–119. MR MR1698269 (2001b:05038)

[18] Reza Rezaeian Farashahi and Ruud Pellikaan, *The quadratic extension extractor for (hyper)elliptic curves in odd characteristic*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 4547, Springer, Berlin, 2007, pp. 219–236. MR MR2387145 (2009a:11252)

[19] Kseniya Garaschuk, *On binary and ternary Kloosterman sums*, Ph D thesis, Simon Fraser University, 2007.

[20] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999) (New York), ACM, 1999, pp. 429–437. MR MR1739972 (2000j:11187)

[21] Dae San Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, 2008.

[22] ———, *Codes associated with orthogonal groups and power moments of Kloosterman sums*, 2008.

[23] ———, *Codes associated with special linear groups and power moments of multidimensional Kloosterman sums*, 2008.

[24] Douglas A. Leonard, *A weighted module view of integral closures of affine domains of type I*, Adv. Math. Commun. **3** (2009), no. 1, 1–11.

[25] Petr Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, Sequences and Their Applications – SETA 2008: Proceedings (Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, eds.), Lecture Notes in Computer Science, vol. 5203, Springer, Berlin Heidelberg, 2008, pp. 182–187.

[26] Marko Moisio, *Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm*, Acta Arith. **132** (2008), no. 4, 329–350. MR MR2413356 (2009f:11149)

[27] Ferruh Özbudak, *Elements of prescribed order, prescribed traces and systems of rational functions over finite fields*, Des. Codes Cryptogr. **34** (2005), no. 1, 35–54. MR MR2126576 (2005k:11239)

[28] B. V. Petrenko, *On the product of two primitive elements of maximal subfields of a finite field*, J. Pure Appl. Algebra **178** (2003), no. 3, 297–306. MR MR1953735 (2004b:11165)

[29] ———, *On the sum of two primitive elements of maximal subfields of a finite field*, Finite Fields Appl. **9** (2003), no. 1, 102–116. MR MR1954786 (2003m:12004)

[30] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 147–160. MR MR2438447

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** (2008), no. 1, 175–181. MR MR2381741 (2008m:11071)

[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** (2007), 307–328 (electronic). MR MR2335723

[3] Ali Akhavi and Damien Stehlé, *Speeding-up lattice reduction with random projections (extended abstract)*, LATIN 2008: Theoretical informatics, Lecture Notes in Comput. Sci., vol. 4957, Springer, Berlin, 2008, pp. 293–305. MR MR2472745

[4] Bill Allombert, *An efficient algorithm for the computation of Galois automorphisms*, Math. Comp. **73** (2004), no. 245, 359–375 (electronic). MR MR2034127 (2004k:11193)

[5] Roberto Maria Avanzi, *Another look at square roots (and other less common operations) in fields of even characteristic*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 138–154.

[6] Eric Bach and Denis Charles, *The hardness of computing an eigenform*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 9–15. MR MR2459985 (2009i:11051)

[7] Werner Backes and Susanne Wetzel, *An efficient LLL gram using buffered transformations*, Computer Algebra in Scientific Computing, Lecture Notes in Computer Science, vol. 4770/2007, Springer Berlin / Heidelberg, 2007, pp. 31–44.

[8] David H. Bailey, Jonathan M. Borwein, Vishaal Kapoor, and Eric W. Weisstein, *Ten problems in experimental mathematics*, Amer. Math. Monthly **113** (2006), no. 6, 481–509. MR MR2231135 (2007b:65001)

[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** (2002), no. 2-3, 149–164. MR MR1904474 (2003b:11133)

[10] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic). MR MR2353964

[11] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690 (electronic). MR MR2299795 (2007m:11170)

[12] Daniel J. Bernstein, *Batch binary edwards*, Advances in Cryptology - CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, Springer, Berlin, 2009, pp. 317–336.

[13] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, Progress in cryptology—INDOCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4859, Springer, Berlin, 2007, pp. 167–182. MR MR2570254

[14] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *ECM using Edwards curves*, 2008.

[15] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 29–50.

[16] Amnon Besser and Rob De Jeu, li(p)*-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194

[17] Peter Birkner, *Efficient divisor class halving on genus two curves*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4356, Springer, Berlin/Heidelberg, pp. 317–326.

[18] Werner Bley and Robert Boltje, *Computation of locally free class groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 72–86. MR MR2282916

[19] Jonathan Borwein and David Bailey, *Mathematics by Experiment*, A K Peters Ltd., Natick, MA, 2004, Plausible reasoning in the 21st century. MR MR2033012 (2005b:00012)

[20] Wieb Bosma, *Some computational experiments in number theory*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 1–30. MR MR2278921

[21] Wieb Bosma, John Cannon, and Allan Steel, *Lattices of compatibly embedded finite fields*, J. Symbolic Comput. **24** (1997), no. 3-4, 351–369, Computational algebra and number theory (London, 1993). MR MR1484485 (99a:11143)

[22] Wieb Bosma and Bart de Smit, *Class number relations from a computational point of view*, J. Symbolic Comput. **31** (2001), no. 1-2, 97–112, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806209 (2002a:11144)

[23] ———, *On arithmetically equivalent number fields of small degree*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR MR2041074 (2005e:11169)

[24] Wieb Bosma and Ben Kane, *The Aliquot constant*, 2009.

[25] Wieb Bosma and Arjen K. Lenstra, *An implementation of the elliptic curve integer factorization method*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 119–136. MR MR1344926 (96d:11134)

[26] Wieb Bosma and Peter Stevenhagen, *Density computations for real quadratic units*, Math. Comp. **65** (1996), no. 215, 1327–1337. MR MR1344607 (96j:11171)

[27] Johan Bosman, *On the computation of Galois representations associated to level one modular forms*, 2007.

[28] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, Finite Fields and Applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 40–58. MR MR2092621

[29] Aaron Bradord, Michael Monagan, and Colin Percival, *Integer factorization and computing discrete logarithms in Maple*, Proceedings of the 2006 Maple Conference, 2006, pp. 2–13.

[30] Richard P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), no. 225, 429–451. MR MR1489968 (99e:11154)

[31] ———, *Recent progress and prospects for integer factorisation algorithms*, Computing and Combinatorics (Sydney, 2000), Lecture Notes in Comput. Sci., vol. 1858, Springer, Berlin, 2000, pp. 3–22. MR MR1866110 (2002h:11138)

[32] ———, *Note on Marsaglia's xorshift random number generators*, J. Stat. Soft **11** (2004), no. 5, 1–5.

[33] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884

[34] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, 2008.

[35] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.

[36] David G. Cantor and Daniel M. Gordon, *Factoring polynomials over p-adic fields*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 185–208. MR MR1850606 (2002f:11175)

[37] Robert Carls, *Explicit Frobenius lifts on elliptic curves*, 2009.

[38] ———, *Fast point counting on genus two curves in characteristic three*, 2010.

[39] Wouter Castryck, Hendrik Hubrechts, and Frederik Vercauteren, *Computing zeta functions in families of $C_{a,b}$ curves using deformation*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 296–311.

[40] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d'equations dans les corps finis*, 2006.

[41] Hugo Chapdelaine, *Computation of p-units in ray class fields of real quadratic number fields*, Math. Comp. **78** (2009), 2307–2345.

[42] 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** (2008), 121–155. MR MR2384334

[43] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441 (electronic). MR MR1972744 (2004a:11137)

[44] M. Daberkow, *Computing with subfields*, J. Symbolic Comput. **24** (1997), no. 3-4, 371–384, Computational algebra and number theory (London, 1993). MR MR1484486 (98k:11185)

[45] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993). MR MR1484479 (99g:11150)

[46] Lassina Dembélé, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057 (electronic). MR MR2291849

[47] Lassina Dembélé, *On the computation of algebraic modular forms on compact inner forms of GSp_4*, 2009.

[48] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 371–386. MR MR2467859 (2010d:11149)

[49] 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** (2005), no. 1, 65–74. MR MR2146520 (2006d:11154)

[50] Claus Diem, *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32. MR MR1966526 (2004a:14030)

[51] ———, *Index calculus in class groups of plane curves of small degree*, 2005.

[52] ———, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557. MR MR2282948

[53] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt, *Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field*, 2006.

[54] Jacques Dubrois and Jean-Guillaume Dumas, *Efficient polynomial time algorithms computing industrial-strength primitive roots*, Inform. Process. Lett. **97** (2006), no. 2, 41–45. MR MR2187046 (2006h:68064)

[55] Sylvain Duquesne, *Montgomery ladder for all genus 2 curves in characteristic 2*, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol. 5130, Springer, 2008, pp. 174–188.

[56] I. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology—Asiacrypt'99 (Singapore), Lecture Notes in Comput. Sci., vol. 1716, Springer, Berlin, 1999, pp. 103–121. MR MR1773225

[57] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **To appear** (2010).

[58] Claus Fieker, *Applications of the class field theory of global fields*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62. MR MR2278922

[59] ———, *Sparse representation for cyclotomic fields*, Experiment. Math. **16** (2007), no. 4, 493–500. MR MR2378488

[60] Claus Fieker and Willem A. de Graaf, *Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras*, LMS J. Comput. Math. **10** (2007), 271–287 (electronic). MR MR2320832 (2008f:11119)

[61] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518 (electronic). MR MR2219041 (2007a:11168)

[62] Tom Fisher, *The Hessian of a genus one curve*, 2006.

[63] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246

[64] ———, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138. MR MR2467841 (2009m:11078)

[65] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR MR2402033

[66] Felix Fontein, *The infrastructure of a global field of arbitrary unit rank*, 2008.

[67] Robert Fraatz, *Computation of maximal orders of cyclic extensions of function fields*, PhD Thesis, Technischen Universtät Berlin, 2005.

[68] David Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing-based cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 152–176. MR MR2423638

[69] David Mandell Freeman and Takakazu Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, 2010, pp. 1–31.

[70] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR MR1880933 (2003b:14032)

[71] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology—Eurocrypt 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34. MR MR1772021

[72] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR MR1934859 (2003h:11159)

[73] Pierrick Gaudry, Alexander Kruppa, and Paul Zimmermann, *A GMP-based implementation of Schönhage-Strassen's large integer multiplication algorithm*, ISSAC 2007, ACM, New York, 2007, pp. 167–174. MR MR2396199

[74] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt, *Comment on: "A new representation of elements of finite fields* $\mathrm{GF}(2^m)$ *yielding small complexity arithmetic circuits" by G. Drolet*, IEEE Trans. Comput. **51** (2002), no. 12, 1460–1461. MR MR2012149

[75] Willi Geiselmann and Rainer Steinwandt, *A redundant representation of* $\mathrm{GF}(q^n)$ *for designing arithmetic circuits*, IEEE Trans. Comp **52** (2003), no. 7, 848–853.

[76] ———, *Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 466–481. MR MR2449226 (2009h:94125)

[77] 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** (2005), 267–300 (electronic). MR MR2193214

[78] Norbert Goeb, *Computing the automorphism groups of hyperelliptic function fields*, 2003.

[79] 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** (2009), 2397–2425.

[80] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428v1 (2009).

[81] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, 2008.

[82] Lajos Hajdu, *Optimal systems of fundamental S-units for LLL-reduction*, Period. Math. Hungar. **59** (2009), no. 1, 53–79. MR MR2544620

[83] G. Hanrot and F. Morain, *Solvability by radicals from an algorithmic point of view*, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 175–182 (electronic). MR MR2049746 (2005a:11200)

[84] Guillaume Hanrot and Damien Stehlé, *Improved analysis of Kannan's shortest lattice vector algorithm (extended abstract)*, Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 170–186. MR MR2419600

[85] David Harvey, *Kedlaya's algorithm in larger characteristic*, Int. Math. Res. Not. IMRN (2007), no. 22, Art. ID rnm095, 29. MR MR2376210

[86] ———, *A cache-friendly truncated FFT*, Theor. Comput. Sci. **410** (2009), no. 27-29, 2649–2658.

[87] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, J. Symbolic Comput. **38** (2004), no. 2, 1003–1024. MR MR2093563 (2005g:11247)

[88] F. Hess, *Weil descent attacks*, Advances in Elliptic Curve Cryptography, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge Univ. Press, Cambridge, 2005, pp. 151–180. MR MR2169214

[89] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, 1531–1548 (electronic). MR MR1972751 (2004f:11126)

[90] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR MR2403533

[91] ———, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.

[92] Xavier Taixes i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, arXiv:0909.2724v2 (2009).

[93] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 219–233.

[94] 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** (2008), no. 3, 715–732. MR MR2523314

[95] Antoine Joux and Reynald Lercier, *Counting points on elliptic curves in medium characteristic*, 2006, p. 15.

[96] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.

[97] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput **39** (2010), no. 5, 1714–1747.

[98] Jürgen Klüners, *Algorithms for function fields*, Experiment. Math. **11** (2002), no. 2, 171–181. MR MR1959261 (2003k:11193)

[99] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.

[100] Grégoire Lecerf, *Fast separable factorization and applications*, Appl. Algebra Engrg. Comm. Comput. **19** (2008), no. 2, 135–160. MR MR2389971 (2009b:13069)

[101] D. Lehavi and C. Ritzenthaler, *An explicit formula for the arithmetic-geometric mean in genus 3*, Experiment. Math. **16** (2007), no. 4, 421–440. MR MR2378484 (2008k:14070)

[102] 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** (2008), no. 3, 783–797. MR MR2523317

[103] Rudolf Lidl, *Computational problems in the theory of finite fields*, Appl. Algebra Engrg. Comm. Comput. **2** (1991), no. 2, 81–89. MR MR1325520 (95m:11134)

[104] J. M. Miret, R. Moreno, J. Pujolàs, and A. Rio, *Halving for the 2-Sylow subgroup of genus 2 curves over binary fields*, Finite Fields Appl. **15** (2009), no. 5, 569–579. MR MR2554040

[105] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, 2009.

[106] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions.*

[107] I. Morel, D. Stehlé, and G. Villard, *Analyse numerique et reduction de reseaux*, 2009.

[108] 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.

[109] Siguna Müller, *On the computation of square roots in finite fields*, Des. Codes Cryptogr. **31** (2004), no. 3, 301–312. MR MR2047886 (2005f:11278)

[110] Phong Q. Nguên and Damien Stehlé, *Floating-point LLL revisited*, Advances in cryptology—EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol. 3494, Springer, Berlin, 2005, pp. 215–233. MR MR2352190 (2008m:94017)

[111] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group* $c2 \times c2 \times c2$, Journal of Number Theory **129** (2009), no. 1, 231 – 245.

[112] Titus Piezas, *Solving solvable sextics using polynomial decomposition*, 2004.

[113] M. E. Pohst, *Computational aspects of Kummer theory*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 259–272. MR MR1446518 (98f:11112)

[114] Xavier-François Roblot, *Polynomial factorization algorithms over number fields*, J. Symbolic Comput. **38** (2004), no. 5, 1429–1443. MR MR2168722

[115] Tanaka Satoru and Nakamula Ken, *More constructing pairing-friendly elliptic curves for cryptography*, 2007.

[116] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR MR2467554

[117] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR MR1689189 (2000c:11208)

[118] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus* 3 *hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529.

[119] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.

[120] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Proceedings of LLL+25 Conference, 2007 (2009).

[121] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Information Security and Cryptography: The LLL Algorithm (Berlin Heidelberg) (David Basin, Ueli Maurer, Phong Q. Nguyen, and Brigitte Vallée, eds.), Information Security and Cryptography, Springer, 2010, pp. 179–213.

[122] Damien Stehlé and Paul Zimmermann, *A binary recursive GCD algorithm*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 411–425. MR MR2138011

[123] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 641–652. MR MR2467560 (2009k:11085)

[124] Katsuyuki Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 124–133.

[125] Nicolas M. Thiéry, *Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis*, Discrete Mathematics and Theoretical Computer Science: 4th International Conference, DMTCS 2003, Dijon, France, July 7-12, 2003: Proceedings (Berlin) (Cristian Calude, Michael J. Dinneen, and Vincent

Vajnovszki, eds.), Lecture Notes in Computer Science, vol. 2731, Springer, 2003, pp. 315–328.

[126] Hans-Christian Graf v. Bothmer, *Finite field experiments (with an appendix by Stefan Wiedmann)*, Higher-Dimensional Geometry over Finite Fields, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 16, IOS Press, 2008, pp. 1–62.

[127] Mark van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory **95** (2002), no. 2, 167–189. MR MR1924096 (2003f:13029)

[128] Gilles Villard, *Certification of the QR factor R and of lattice basis reducedness*, ISSAC 2007, ACM, New York, 2007, pp. 361–368. MR MR2402283

[129] P. G. Walsh, *On a very particular class of Ramanujan-Nagell type equations*, Far East J. Math. Sci. (FJMS) **24** (2007), no. 1, 55–58. MR MR2281854 (2007k:11213)

[130] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.

[131] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 525–542. MR MR2282947