

Algebraic Geometry

Arithmetic and Diophantine Geometry

14Gxx

- [1] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.
- [2] Tatiana Bandman, Gert-Martin Greuel, Fritz Grunewald, Boris Kunyavskiĭ, Gerhard Pfister, and Eugene Plotkin. Identities for finite solvable groups and equations in finite simple groups. *Compos. Math.*, 142(3):734–764, 2006.
- [3] Arthur Baragar and Ronald van Luijk. $K3$ surfaces with Picard number three and canonical vector heights. *Math. Comp.*, 76(259):1493–1498 (electronic), 2007.
- [4] M. Borovoi, J.-L. Colliot-Thélène, and A. N. Skorobogatov. The elementary obstruction and homogeneous spaces. *Duke Math. J.*, 141(2):321–364, 2008.
- [5] Nigel Boston. Reducing the Fontaine-Mazur conjecture to group theory. In *Progress in Galois theory*, volume 12 of *Dev. Math.*, pages 39–50. Springer, New York, 2005.
- [6] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.
- [7] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas. Hyperelliptic curves with compact parameters. *Des. Codes Cryptogr.*, 36(3):245–261, 2005.
- [8] Nils Bruin. Visualising $Sha[2]$ in abelian surfaces. *Math. Comp.*, 73(247):1459–1476 (electronic), 2004.
- [9] Patrick Corn. The Brauer-Manin obstruction on del Pezzo surfaces of degree 2. *Proc. Lond. Math. Soc. (3)*, 95(3):735–777, 2007.

- [10] Patrick Corn. Tate-Shafarevich groups and K3 surfaces. *Math. Comp.*, To appear, 17 pages, 2007.
- [11] Jan Denef and Frederik Vercauteren. An extension of Kedlaya’s algorithm to Artin-Schreier curves in characteristic 2. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 308–323. Springer, Berlin, 2002.
- [12] Claus Diem. The GHS attack in odd characteristic. *J. Ramanujan Math. Soc.*, 18(1):1–32, 2003.
- [13] Xander Faber and Benjamin Hutz. On the number of rational iterated pre-images of the origin under quadratic dynamical systems. [arXiv:0810.1715](https://arxiv.org/abs/0810.1715), 18 pages, 2008.
- [14] Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve. Uniform bounds on pre-images under quadratic dynamical systems. *Math. Res. Lett.*, 16(1):87–101, 2009.
- [15] Tom Fisher. A new approach to minimising binary quartics and ternary cubics. *Math. Res. Lett.*, 14(4):597–613, 2007.
- [16] Tom Fisher. Finding rational points on elliptic curves using 6-descent and 12-descent. *J. Algebra*, 320(2):853–884, 2008.
- [17] E. V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115(4):437–466, 2004.
- [18] David Freeman and Kristin Lauter. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 29–66. World Sci. Publ., Hackensack, NJ, 2008.
- [19] Steven D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology—Asiacrypt 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 495–513. Springer, Berlin, 2001.
- [20] Steven D. Galbraith. Weil descent of Jacobians. *Discrete Appl. Math.*, 128(1):165–180, 2003.

- [21] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In *Advances in Cryptology—Eurocrypt 2002 (Amsterdam)*, volume 2332 of *Lecture Notes in Comput. Sci.*, pages 29–44. Springer, Berlin, 2002.
- [22] Steven D. Galbraith and Xibin Lin. Computing pairings using x -coordinates only. *Des. Codes Cryptogr.*, 50(3):305–324, 2009.
- [23] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
- [24] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology—Eurocrypt 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Berlin, 2000.
- [25] Ralf Gerkmann. Relative rigid cohomology and deformation of hypersurfaces. *Int. Math. Res. Pap. IMRP*, (1):Art. ID rpm003, 67, 2007.
- [26] Josep González and Victor Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.
- [27] Cem Güneri, Henning Stichtenoth, and Ihsan Taşkın. Further improvements on the designed minimum distance of algebraic geometry codes. *J. Pure Appl. Algebra*, 213(1):87–97, 2009.
- [28] Johan P. Hansen. Toric varieties, Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(4):289–300, 2002.
- [29] David Harari and Tamás Szamuely. Galois sections for abelianized fundamental groups. *Math. Ann.*, 344(4):779–800, 2009.
- [30] David Harvey. Kedlaya’s algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.
- [31] F. Hess. Weil descent attacks. In *Advances in Elliptic Curve Cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 151–180. Cambridge Univ. Press, Cambridge, 2005.
- [32] Florian Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math. (Basel)*, 82(1):28–32, 2004.

- [33] Christopher Holden. Mod 4 Galois representations and elliptic curves. *Proc. Amer. Math. Soc.*, 136(1):31–39 (electronic), 2008.
- [34] E. W. Howe and K. E. Lauter. Improved upper bounds for the number of points on curves over finite fields. *Ann. Inst. Fourier (Grenoble)*, 53(6):1677–1737, 2003.
- [35] Everett W. Howe. Supersingular genus-2 curves over fields of characteristic 3. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 49–69. Amer. Math. Soc., Providence, RI, 2008.
- [36] Everett W. Howe, Kristin E. Lauter, and Jaap Top. Pointless curves of genus three and four. In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 125–141. Soc. Math. France, Paris, 2005.
- [37] Nathan Owen Ilten and Hendrik Süß. AG codes from polyhedral divisors. [arXiv:0811.2696](https://arxiv.org/abs/0811.2696), 30 pages, 2008.
- [38] Farzali A. Izadi and V. Kumar Murty. Counting points on an abelian variety over a finite field. In *Progress in Cryptology—Indocrypt 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, pages 323–333. Springer, Berlin, 2003.
- [39] Rafe Jones and Jeremy Rouse. Iterated endomorphisms of Abelian algebraic groups. [arXiv:0707.2384](https://arxiv.org/abs/0707.2384), 34 pages, 2007.
- [40] Samuel Kadziela. Rigid analytic uniformization of curves and the study of isogenies. *Acta Appl. Math.*, 99(2):185–204, 2007.
- [41] Kiran S. Kedlaya. Computing zeta functions via p -adic cohomology. In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 1–17. Springer, Berlin, 2004.
- [42] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.
- [43] Aristides Kontogeorgis and Victor Rotger. On abelian automorphism groups of Mumford curves and applications to Shimura curves. [arXiv:math.AG/0604099](https://arxiv.org/abs/math/0604099), 16 pages, 2006.

- [44] Andrew Kresch and Yuri Tschinkel. Integral points on punctured abelian surfaces. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 198–204. Springer, Berlin, 2002.
- [45] Andrew Kresch and Yuri Tschinkel. On the arithmetic of del Pezzo surfaces of degree 2. *Proc. London Math. Soc. (3)*, 89(3):545–569, 2004.
- [46] Andrew Kresch and Yuri Tschinkel. Effectivity of Brauer-Manin obstructions. *Adv. Math.*, 218(1):1–27, 2008.
- [47] L. Kulesz, G. Matera, and É. Schost. Uniform bounds on the number of rational points of a family of curves of genus 2. *J. Number Theory*, 108(2):241–267, 2004.
- [48] Gilles Lachaud and Christophe Ritzenthaler. On a conjecture of Serre on abelian threefolds. In *Algebraic Geometry and its applications, Proceedings of the First SAGA conference, Papeete, France 2007*, pages 1–28, 2008.
- [49] Alan G. B. Lauder. Counting solutions to equations in many variables over finite fields. *Found. Comput. Math.*, 4(3):221–267, 2004.
- [50] Alan G. B. Lauder. A recursive method for computing zeta functions of varieties. *LMS J. Comput. Math.*, 9:222–269 (electronic), 2006.
- [51] F. Leprévost, M. Pohst, and A. Schöpp. Rational torsion of $J_0(N)$ for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10. *Abh. Math. Sem. Univ. Hamburg*, 74:193–203, 2004.
- [52] John Little and Hal Schenck. Toric surface codes and Minkowski sums. *SIAM J. Discrete Math.*, 20(4):999–1014 (electronic), 2006.
- [53] Adam Logan. The Brauer-Manin obstruction on del Pezzo surfaces of degree 2 branched along a plane section of a Kummer surface. *Math. Proc. Cambridge Philos. Soc.*, 144(3):603–622, 2008.
- [54] Michelle Manes. Q -rational cycles for degree-2 rational maps having an automorphism. *Proc. Lond. Math. Soc. (3)*, 96(3):669–696, 2008.
- [55] David Savitt. The maximum number of points on a curve of genus 4 over F_8 is 25. *Canad. J. Math.*, 55(2):331–352, 2003.

- [56] Éric Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.
- [57] R. Shaw. The polynomial degrees of Grassmann and Segre varieties over $\text{GF}(2)$. *Discrete Math.*, 308(5-6):872–879, 2008.
- [58] Edlyn Teske. An elliptic curve trapdoor system (extended abstract). In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 341–352. Amer. Math. Soc., Providence, RI, 2004.
- [59] Ronald van Luijk. Quartic $K3$ surfaces without nontrivial automorphisms. *Math. Res. Lett.*, 13(2-3):423–439, 2006.
- [60] Ronald van Luijk. Cubic points on cubic curves and the brauer-manin obstruction on $k3$ surfaces. [arXiv:0708.2752v1](https://arxiv.org/abs/0708.2752v1) [[math.NT](https://arxiv.org/html/math)], 17 pages, 2007.
- [61] Anthony Várilly-Alvarado and David Zywina. Arithmetic $E8$ lattices with maximal Galois action. [arXiv:0803.3063](https://arxiv.org/abs/0803.3063), 2008.
- [62] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. Cryptology*, 17(4):277–296, 2004.
- [63] John Voight. Shimura curves of genus at most two. *Math. Comp.*, 78(266):1155–1172, 2009.
- [64] Gabor Wiese. Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133 (electronic), 2004.