Isogeny graphs, modular polynomials, and applications

Martindale, C.R.

Bibliography

[Bal+17] S. Ballentine, A. Guillevic, E. Lorenzo-García, M. Massierer, C. Martindale, B. Smith, and J. Top. "Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication". In: *Algebraic Geometry for Coding Theory and Cryptography*. Vol. 9. Association for Women in Mathematics Series. Springer Int. Pub., 2017, pp. 63–94. ISBN: 978-3-319-63931-4.

[BCR] G. Bisson, R. Cosset, and D. Robert. *AVIsogenies: a library for computing isogenies between abelian varieties*. `http://\discretionary{}{}{}avisogenies.gforge.inria.fr`.

[BJW17] E.H. Brooks, D. Jetchev, and B. Wesolowski. "Isogeny graphs of ordinary abelian varieties". In: *Research in Number Theory* 3 (2017). ISSN: 2363-9555.

[BS17] G. Bisson and M. Streng. "On polarised class groups of orders in quartic CM-fields". In: *Math. Res. Lett.* 24.2 (2017), pp. 247–270. ISSN: 1073-2780.

[Can87] D.G. Cantor. "Computing in the Jacobian of a hyperelliptic curve". In: *Math. Comp.* 48.177 (1987), pp. 95–101.

[Car04] R. Carls. "A generalized arithmetic geometric mean". PhD thesis. University of Groningen, The Netherlands, 2004. URL: `http://hdl.handle.net/11370/f47bd074-2c0d-4521-a92b-4e89af5c1840`.

[CE15] J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: *LMS J. Comput. Math.* 18.1 (2015), pp. 555–577.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Vol. 138. Graduate Texts in Mathematics. Spring-Verlag, 1993.

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Invent. Math.* 8 (1969), pp. 238–243. ISSN: 0020-9910.

[Dup06] R. Dupont. "Moyenne Arithmético-géométrique, Suites de Borchant et Applications". PhD thesis. École Polytechnique, 2006. URL: `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`.

[Echidna] D. Kohel. *The Echidna Database*. URL: `https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/index.html`.

[Fly90] E.V. Flynn. "The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field". In: *Math. Proc. Cambridge Philos. Soc.* 107.3 (1990), pp. 425–441.

[Gee88] G. van der Geer. *Hilbert modular surfaces*. Vol. 16. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1988, pp. x+291. ISBN: 3-540-17601-2.

[GH00] P. Gaudry and R. Harley. "Counting Points on Hyperelliptic Curves over Finite Fields". In: *Algorithmic Number Theory, 4th International Symposium, ANTS-IV (Leiden, The Netherlands)*. Ed. by W. Bosma. Vol. 1838. Lecture Notes in Computer Science. Berlin: Springer, 2000, pp. 313–332.

[GKS11] P. Gaudry, D. Kohel, and B. Smith. "Counting Points on Genus 2 Curves with Real Multiplication". In: *Advances in Cryptology—ASIACRYPT 2011 (Seoul, South Korea)*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. Lecture Notes in Computer Science. Heidelberg: Springer, 2011, pp. 504–519.

[GM07] G. van der Geer and B. Moonen. *Abelian varieties*. Book in preparation. 2007.

[Gra90] D. Grant. "Formal groups in genus two". In: *J. Reine Angew. Math.* 411 (1990), pp. 96–121.

[Gro61] A. Grothendieck. "Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes". In: *Inst. Hautes Études Sci. Publ. Math.* 8 (1961), p. 222. ISSN: 0073-8301. URL: http://www.numdam.org/item?id=PMIHES_1961__8__222_0.

[GS12] P. Gaudry and E. Schost. "Genus 2 point counting over prime fields". In: *J. Symbolic Comput.* 47.4 (2012), pp. 368–400. DOI: 10.1016/j.jsc.2011.09.003.

[Gun63] K.-B. Gundlach. "Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $Q(\sqrt{5})$". In: *Math. Ann.* 152 (1963), pp. 226–256. ISSN: 0025-5831.

[Har07] D. Harvey. "Kedlaya's algorithm in larger characteristic". In: *Int. Math. Res. Not. IMRN* 22 (2007), Art. ID rnm095, 29. ISSN: 1073-7928.

[Har12] M.C. Harrison. "An extension of Kedlaya's algorithm for hyperelliptic curves". In: *J. Symbolic Comput.* 47.1 (2012), pp. 89–101. ISSN: 0747-7171.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[How95] E.W. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *Trans. Amer. Math. Soc.* 347.7 (1995), pp. 2361–2401. ISSN: 0002-9947.

[HZ02] E.W. Howe and H.J. Zhu. "On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field". In: *J. Number Theory* 92.1 (2002), pp. 139–163. ISSN: 0022-314X.

[Igu60] J. Igusa. "Arithmetic variety of moduli for genus two". In: *Ann. of Math. (2)* 72 (1960), pp. 612–649. ISSN: 0003-486X.

[Igu67] J. Igusa. "Modular Forms and Projective Invariants". In: *Amer. J. Math.* 89.3 (1967), pp. 817–855.

[IT14] S. Ionica and E. Thomé. *Isogeny graphs of genus 2 curves with Maximal Real Multiplication*. https://eprint.iacr.org/2014/230.pdf. 2014.

[JL01] A. Joux and R. Lercier. ""Chinese & Match", an alternative to Atkin's "Match and Sort" method used in the SEA algorithm". In: *Math. Comp.* 70.234 (2001), pp. 827–836.

[Kat81] N. Katz. "Serre-Tate local moduli". In: *Algebraic surfaces (Orsay, 1976–78)*. Vol. 868. Lecture Notes in Math. Springer, Berlin-New York, 1981, pp. 138–202.

[Ked01] K.S. Kedlaya. "Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology". In: *J. Ramanujan Math. Soc.* 16.4 (2001), pp. 323–338. ISSN: 0970-1249.

[Knu91] M.-A. Knus. *Quadratic and Hermitian forms over rings*. Vol. 294. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With a foreword by I. Bertuccioni. Springer-Verlag, Berlin, 1991, pp. xii+524. ISBN: 3-540-52117-8.

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996, p. 117. ISBN: 978-0591-32123-4.

[Lan78] S. Mac Lane. *Categories for the Working Mathematician*. Vol. 5. Graduate Texts in Mathematics. Springer New York, 1978, p. 317.

[Lan82] S. Lang. *Introduction to Algebraic and Abelian Functions*. Vol. 89. Graduate Texts in Mathematics. New York: Springer-Verlag, 1982.

[Lan83] Serge Lang. *Complex multiplication*. Vol. 255. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1983, pp. viii+184. ISBN: 0-387-90786-6.

[Lan86] S. Lang. *Algebraic Number Theory*. Vol. 16. Graduate Texts in Mathematics. New York: Springer-Verlag, 1986.

[Ler97] R. Lercier. "Algorithmique des courbes elliptiques dans les corps finis". PhD thesis. École Polytechnique, Palaiseau, France, 1997. URL: https://tel.archives-ouvertes.fr/tel-01101949.

[LNY16] K. Lauter, M. Naehrig, and T. Yang. "Hilbert theta series and invariants of genus 2 curves". In: *J. Number Theory* 161 (2016), pp. 146–174. ISSN: 0022-314X.

[LST64] J. Lubin, J.P. Serre, and J. Tate. "Elliptic Curves and Formal Groups". In: (1964). Unpublished skeleton seminar notes.

[LY11] K. Lauter and T. Yang. "Computing genus 2 curves from invariants on the Hilbert moduli space". In: *J. Number Theory* 131.5 (2011), pp. 936–958. ISSN: 0022-314X.

[Mar18] C. Martindale. "Isogeny Graphs, Modular Polynomials, and Applications". PhD thesis. Universiteit Leiden, 2018.

[May07] S. Mayer. "Hilbert Modular Forms for the Fields $Q(\sqrt{5})$, $Q(\sqrt{13})$ and $Q(\sqrt{17})$". PhD thesis. Rheinisch-Westfälischen Technischen Hochschule Aachen, 2007. URL: http://www.matha.rwth-aachen.de/~mayer/homepage/dissertation-S-Mayer-revised-edition.pdf.

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley*. https://webusers.imj-prg.fr/~jean-francois.mestre/lettreGaudryHarley.ps. 2001.

[Mes02] J.-F. Mestre. *Algorithme pour compter des points de courbes en petite caractéristique et petit genre*. https://webusers.imj-prg.fr/~jean-francois.mestre/rennescrypto.ps. Notes from a talk given at the Rennes cryptography seminar. 2002.

[Mes72] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Lecture Notes in Mathematics, Vol. 264. Springer-Verlag, Berlin-New York, 1972, pp. iii+190.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Third. Vol. 34. Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]. Springer-Verlag, Berlin, 1994, pp. xiv+292. ISBN: 3-540-56963-4.

[Mil15a] E. Milio. "A quasi-linear time algorithm for computing modular polynomials in dimension 2". In: *LMS J. Comput. Math.* 18.1 (2015), pp. 603–632.

[Mil15b] E. Milio. "Computing modular polynomials in dimension 2". PhD thesis. Université de Bordeaux, Dec. 2015. URL: https://tel.archives-ouvertes.fr/tel-01240690.

[Mil86] J.S. Milne. "Abelian varieties". In: *Arithmetic Geometry (Storrs, Connecticut, 1984)*. New York: Springer, 1986, pp. 103–150. DOI: 10.1007/978-1-4613-8655-1.

[Mue83] R. Mueller. "Hilbertsche Modulformen und Modulfunktionen zu $\mathbf{Q}(\sqrt{8})$". In: *Math. Ann.* 266.1 (1983), pp. 83–103. ISSN: 0025-5831.

[Mue85] R. Mueller. "Hilbertsche Modulformen und Modulfunktionen zu $\mathbf{Q}(\sqrt{5})$". In: *Arch. Math. (Basel)* 45.3 (1985), pp. 239–251. ISSN: 0003-889X.

[Mum08] D. Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, pp. xii+263. ISBN: 978-81-85931-86-9; 81-85931-86-0.

[Pil90] J. Pila. "Frobenius maps of abelian varieties and finding roots of unity in finite fields". In: *Math. Comp.* 55.192 (1990), pp. 745–763.

[Rap78] M. Rapoport. "Compactifications de l'espace de modules de Hilbert-Blumenthal". In: *Compositio Math.* 36.3 (1978), pp. 255–335. ISSN: 0010-437X.

[Rüc90] H.-G. Rück. "Abelian surfaces and Jacobian varieties over finite fields". In: *Compositio Math.* 76.3 (1990), pp. 351–366. ISSN: 0010-437X.

[Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2)*. http://www.sagemath.org. 2018.

[Sat02] T. Satoh. "On p-adic Point Counting Algorithms for Elliptic Curves over Finite Fields". In: *Algorithmic Number Theory (Sydney, 2002)*. Ed. by C. Fieker and D. R. Kohel. Vol. 2369. Lecture Notes in Computer Science. Berlin: Springer, 2002, pp. 43–66.

[Sch85] R. Schoof. "Elliptic curves over finite fields and the computation of square roots mod p". In: *Math. Comp.* 44.170 (1985), pp. 483–494.

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254.

[Stack-Exchange] Matt E (`https://math.stackexchange.com/users/221/matt-e`). *Why is a smooth connected scheme irreducible?* Mathematics Stack Exchange. eprint: `https://math.stackexchange.com/q/20508`.

[Ste08] P. Stevenhagen. "The arithmetic of number rings". In: *Algorithmic number theory: lattices, number fields, curves and cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 209–266.

[Sut13] A.V. Sutherland. "On the evaluation of modular polynomials". In: *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium (San Diego, California)*. Vol. 1. Open Book Series. Berkeley, CA: Mathematical Sciences Publishers, 2013, pp. 531–555.

[Sut18] A. Sutherland. *Modular Polynomials*. Online database. 2018. URL: `https://math.mit.edu/~drew/~ClassicalModPolys.html`.

[TTV91] W. Tautz, J. Top, and A. Verberkmoes. "Explicit hyperelliptic curves with real multiplication and permutation polynomials". In: *Canad. J. Math.* 43.5 (1991), pp. 1055–1064. ISSN: 0008-414X.

[Was08] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Second. Vol. 50. Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC, 2008.

Index