Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Bibliography

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves.* International Mathematics Research Notices, 20 (1996) no. 20, 1005-1011

[2] M. Akbas, D. Singerman, *The normalizer of* $\Gamma_0(N)$ *in* $\mathrm{PSL}(2,\mathbf{R})$. Glasgow Mathematical Journal, 32 (1990) no. 3, 317-327

[3] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra.* Addison–Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont. 1969

[4] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Mathematische Annalen, 185 (1970), 134-160

[5] M. Baker, Y. Hasegawa, *Automorphisms of* $X_0^*(p)$. Journal of Number Theory, 100 (2003) no. 1, 72-87

[6] J. Balakrishnan, A. Besser, F. Bianchi, J. Steffen Müller, *Explicit quadratic Chabauty over number fields.* `https://arxiv.org/abs/1910.04653`

[7] J. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski, *Chabauty–Coleman experiments for genus 3 hyperelliptic curves.* Research Directions in Number Theory, Association for Women in Mathematics Series, Vol. 19, Springer, 2019, 67–90.

[8] J. Balakrishnan, N. Dogra, *Quadratic Chabauty and rational points, I: p-adic heights.* With an appendix by J. Steffen Müller. Duke Math. J. 167 (2018), no. 11, 1981–2038.

[9] J. Balakrishnan, N. Dogra, *An effective Chabauty-Kim theorem.* Compos. Math. 155 (2019), no. 6, 1057–1075.

[10] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13.* Ann. of Math. (2) 189 (2019), no. 3, 885–944.

[11] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves.* Journal of Number Theory, 130 (2010) no. 12, 2753-2772

[12] B. Baran, *A modular curve of level 9 and the class number one problem.* Journal of Number Theory, 129 (2009) no. 3, 715-728

[13] B. Baran, *An exceptional isomorphism between modular curves of level 13.* Journal of Number Theory, 145 (2014), 273-300,

[14] F. Bars, *The group structure of the normalizer of* $\Gamma_0(N)$ *after Atkin-Lehner.* Communications in Algebra, 36 (2008) no. 6, 2160-2170

[15] E. Berlekamp, *Factoring polynomials over large finite fields.* Math. Comp. 24 (1970), 713- 735.

[16] D. Bertrand, B. Edixhoven, *Pink's conjecture on unlikely intersections and families of semi-abelian varieties.* `https://arxiv.org/abs/1904.01788`

[17] Y. Bilu, P. Parent, *Serre's uniformity problem in the split Cartan case.* Annals of Mathematics. Second Series, 173 (2011) no. 1, 569-584

[18] Y. Bilu, P. Parent, M. Rebolledo, *Rational points on* $X_0^+(p^r)$. Université de Grenoble. Annales de l'Institut Fourier, 63 (2013) no. 3, 957-984

[19] R. Barbulescu , P. Gaudry, A. Joux, E. Thomé, *A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic.* Annual International Conference on the Theory and Applications of Cryptographic Techniques (2014), 1-16.

[20] A. Besser, *p-adic Arakelov theory.* J. Number Theory, 111 (2005), no. 2, 318—371.

[21] A. Betts, *The motivic anabelian geometry of local heights on abelian varieties.*
`https://arxiv.org/abs/1706.04850`

[22] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 21. Springer-Verlag, Berlin, 1990.

[23] A. W. Bluher, *On $x^{q+1} + ax + b$.* Finite Fields and Their Applications 10 (2004) No. 3, 285–305.

[24] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur á l'unité.* C. R. Acad. Sci. Paris 212 (1941), 882–885.

[25] I. Chen, *The Jacobians of non-split Cartan modular curves.* Proceedings of the London Mathematical Society. Third Series, 77 (1998) no. 1, 1-38

[26] I. Chen, *Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n.* Comptes Rendus Mathématique. Académie des Sciences. Paris, 339 (2004) no. 3, 187-192

[27] Q. Cheng, D. Wan, J. Zhuang, *Traps to the BGJT-algorithm for discrete logarithms.* LMS Journal of Computation and Mathematics 17 (2014), 218-229.

[28] R. Coleman, G. Gross, *p-adic heights on curves.* Algebraic number theory, 73–81 Adv. Stud. Pure Math., 17 (1989).

[29] P. Coupek, D. Lilienfeldt, L. Xiao, Z. Yao, *Geometric quadratic Chabauty over number fields.* `http://www.math.mcgill.ca/lilien/Chabauty-Part1.pdf`

[30] J. M. Couveignes, R. Lercier, *Elliptic periods for finite fields.* Finite Fields and Their Applications, 15 (2009) No. 1, 1–22.

[31] P. Deligne, *La conjecture de Weil II.* Publ. Math. I.H.E.S. 52 (1981), 313-428

[32] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques.* Modular functions of one variable, II, (1972), 143-316

[33] W. Diffie, M. Hellman, *New directions in cryptography.* IEEE Trans. Inform. Theory 22 (1976).

[34] N. Dogra, *Unlikely intersections and the Chabauty-Kim method over number fields.*
`https://arxiv.org/abs/1903.05032`

[35] V. Dose, J. Fernández, J. González, R. Schoof, *The automorphism group of the non-split Cartan modular curve of level 11.* Journal of Algebra, 417 (2014), 95-102

[36] V. Dose, P. Mercuri, C. Stirpe, *Double covers of Cartan modular curves.* Journal of Number Theory, 195 (2019), 96-114

[37] V. Dose, *On the automorphisms of the nonsplit Cartan modular curves of prime level.* Nagoya Mathematical Journal, 224 (2016) no. 1, 74-92

[38] F. Diamond, J. Shurman, *A first course in modular forms.* Graduate Texts in Mathematics (2005), Springer-Verlag, New York, xvi+436

[39] B. de Smit, B. Edixhoven, *Sur un résultat d'Imin Chen.* Mathematical Research Letters, 7 (2000) no. 2-3, 147-153

[40] B. Edixhoven, *Geometric quadratic Chabauty.* Lectures at the Arizona Winter School 2020.
`http://swc.math.arizona.edu/index.html`

[41] A. Grothendieck and J. Dieudonné, *Eléments de Géométrie Algébrique I. Le langage des schémas.* Inst. Hautes Études Sci. Publ. Math. 4 (1960)

[42] N. D. Elkies, *The automorphism group of the modular curve* $X_0(63)$. Compositio Mathematica, 74 (1990) no. 2, 203-208, `http://www.numdam.org/item?id=CM_1990__74_2_203_0`

[43] G. Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349–366.

[44] V. Flynn, *A flexible method for applying Chabauty's theorem.* Compositio Math. 105 (1997), no. 1, 79–94.

[45] A. Fröhlich, *Formal groups.* Vol 74. Springer–Verlag, Berlin–New York, 1957.

[46] S.R. Ghorpade, G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields.* Moscow Mathematical Journal 2 (2002) No. 3, 589-631.

[47] J. González, *Automorphism group of split Cartan modular curves.* Bulletin of the London Mathematical Society, 48 (2016) no. 4, 628-636

[48] J. González, *Constraints on the automorphism group of a curve.* Journal de Théorie des Nombres de Bordeaux, 29 (2017) no. 2, 535-548, `http://jtnb.cedram.org/item?id=JTNB_2017__29_2_535_0`

[49] R. Granger, T. Kleinjung, J. Zumbrägel, *On the discrete logarithm problem in finite fields of fixed characteristic*. Transactions of the American Mathematical Society 370 (2018) No. 5, 3129-3145.

[50] *Database of finite groups of small order*. `http://groupnames.org`

[51] S. Hashimoto, *Cartoon guide to finding $\mathbb{Q}$-points with geometric quadratic Chabauty*. `https://github.com/sachihashimoto/cartoon-guide-gqc`

[52] M. C. Harrison, *A New Automorphism Of $X_0(108)$*. ArXiv preprint 1108.5595 (2011)

[53] Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2*. Proc. Japan Acad. Ser. A Math. Sci. 71 (1995), no. 10, 235–239 (1996).

[54] T. Honda, *On the theory of commutative formal groups*. Journal of the Mathematical Society of Japan Vol. 22 no. 2 (1970). `https://projecteuclid.org/euclid.jmsj/1259942752`

[55] Ivić, A., *Two inequalities for the sum of divisors functions*. Univ. u Novom Sadu Zb. Rad. Prirod.-Mat. Fak., 7 (1997), 17-22

[56] A. Joux, *A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic*. Conference on Selected Areas in Cryptography (2013), 355-379.

[57] A. Joux, C. Pierrot, *Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms*. arXiv preprint 1907.02689 (2019).

[58] N. M. Katz, *Sums of Betti numbers in arbitrary characteristic*. Finite Fields and their Applications 7 (2001) No. 1, 29-44.

[59] N. Katz B. Mazur, *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies, 108 (1985). Princeton University Press,

[60] M. A. Kenku, F. Momose, *Automorphism groups of the modular curves $X_0(N)$*. Compositio Mathematica, 65 (1988) no. 1, 51-80, `http://www.numdam.org/item?id=CM_1988__65_1_51_0`

[61] K. Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*. Math. Comp. 76 (2007), no. 260, 2213–2239.

[62] M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$ *and the theorem of Siegel.* Invent. Math. 161 no. 3 (2005), 629–656.

[63] M. Kim, *The unipotent Albanese map and Selmer varieties for curves.* Publ. Res. Inst. Math. Sci. 45 no. 1 (2009), 89–133.

[64] T. Kleinjung, B. Wesolowski, *A new perspective on the powers of two descent for discrete logarithms in finite fields.* The Open Book Series 2 (2019) No. 1, 343-352.

[65] T. Kleinjung, B. Wesolowski, *Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic.* arXiv preprint:1906.10668 (2019)

[66] H.W. Jr. Lenstra, *Finding isomorphisms between finite fields.* Math. Comp. 56 (1991), 329–347.

[67] G. Lido, *Discrete logarithm over finite fields of small characteristic.* Master's thesis, Universitá di Pisa (2016). Available at https://etd.adm.unipi.it/t/etd-08312016-225452.

[68] Q. Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.

[69] W. Bosma, J. J. Cannon, C. Fieker, A. Steel, *Handbook of Magma functions.* `http://magma.maths.usyd.edu.au/magma/handbook/`

[70] *A Magma script.* `https://github.com/guidoshore/automorphisms_of_Cartan_modular_curves`, last accessed: 2020-08-08

[71] N. Mascot, *Hensel-lifting torsion points on Jacobians and Galois representations.* Math. Comp. 89 (2020), no. 323, 1417–1455.

[72] B. Mazur, *Rational isogenies of prime degree*, Inventiones Mathematicae, 44 (1978) no. 2, 129-162

[73] B. Mazur and J. Tate, *Canonical height pairings via biextensions.* Arithmetic and geometry, Vol. I, 195–237, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.

[74] P. Mercuri, *Equations and rational points of the modular curves* $X_0^+(p)$. Ramanujan Journal, 47 (2018) no. 2, 291-308

[75] P. Mercuri, R. Schoof, *Modular forms invariant under non-split Cartan subgorup.* accepted by Mathematics of Computation (2020)

[76] L. Moret-Bailly, *Métriques permises.* Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). Astérisque no. 127 (1985), 29–87. http://www.numdam.org/article/AST_1985__127__29_0.pdf

[77] L. Moret-Bailly, *Pinceaux de variétés abéliennes.* Astérisque no. 129 (1985). http://www.numdam.org/item/AST_1985__129__1_0/

[78] W. McCallum and B. Poonen, *The method of Chabauty and Coleman.* Explicit methods in number theory, 99–117, Panor. Synthèses, 36, Soc. Math. France, Paris, 2012.

[79] S. Müller, *Applying the Mordell–Weil sieve.* Appendix to [8].

[80] D. Mumford, *Biextensions of formal groups.* In Arithmetic algebraic geometry (proceedings of Purdue conference). Harper, 1965

[81] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Springer Monographs in Mathematics (2004)

[82] J. L. Nicolas, G. Robin, *Majorations explicites pour le nombre de diviseurs de N.* Canadian Mathematical Bulletin, 26 (1983) no. 4, 485-492

[83] A. P. Ogg, *Automorphismes de courbes modulaires.* Séminaire Delange-Pisot-Poitou, Théorie des nombres 16 (1975) no. 1, 1-8

[84] A .P. Ogg, *Diophantine equations and modular forms.* Bulletin of the American Mathematical Society, 81 (1997) no. 1, 14-27

[85] A. P. Ogg, *Über die Automorphismengruppe von* $X_0(N)$. Mathematische Annalen, 228 (1977) no. 3, 279-292

[86] M. Raynaud, *Spécialisation du foncteur de Picard.* Inst. Hautes Études Sci. Publ. Math. 38 (1970), 27-76. http://www.numdam.org/article/PMIHES_1970__38__27_0.pdf

[87] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le k-ième nombre premier et grandes valeurs de la fonction* ω *(n) nombre de diviseurs premiers de n.* Acta Arithmetica, 42 (1998) no. 4, 367-389

[88] G. Robin, *Grandes valeurs de fonctions arithmétiques et problèmes d'optimisation en nombres entiers*. PhD thesis, Université de Limoges ((1998)

[89] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois Journal of Mathematics, 6 (1962) no. 1, 64-94

[90] H. G. Rück, *A Note on Elliptic Curves Over Finite Fields*. Mathematics of Computation Vol. 49 No. 179 (1987), pp. 301–304.

[91] *Groupes de monodromie en géométrie algébrique. I.* Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D.S. Rim. Lecture Notes in Mathematics, Vol 288. Springer–Verlag, Berlin–New York, 1972.

[92] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones Mathematicae, 15 (1972) no. 4, 259-331

[93] J. P. Serre, *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, 3rd ed., Friedr. Vieweg & Sohn, Braunschweig (1997),

[94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press (1971)

[95] G. Shimura, *Class fields over real quadratic fields and Hecke operators*. Annals of Mathematics, 2nd Series, 95 (1972), 130-190

[96] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*. Nagoya Mathematical Journal, 43 (1971), 199-208

[97] J. H. Silverman, *The arithmetic of elliptic curves*. Springer Science and Business Media, Vol. 106 (2009).

[98] P. Spelier, *A geometric approach to linear Chabauty*. MSc thesis, Universiteit Leiden, 2020.
`https://www.universiteitleiden.nl/en/science/mathematics/education/theses`

[99] M. Stoll, *Finite coverings and rational points.* Oberwolfach lecture, 2005–07–19.
`http://www.mathe2.uni-bayreuth.de/stoll/workshop2005/oberwolfach2005.pdf`

[100] D. Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation Vol. 66 No. 129 (1997), 1195–1212.

[101] Y. Zarhin, *Neron coupling and quasicharacters.* Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 497–509.