Complex multiplication constructions of abelian extensions of quartic fields

Asuncion, J.G.

Bibliography

[1] Karim Belabas. "Topics in computational algebraic number theory". In: *J. Théor. Nombres Bordeaux* 16.1 (2004), pp. 19–63. DOI: 10.5802/jtnb.433. URL: http://jtnb.cedram.org/item?id=JTNB_2004__16_1_19_0.

[2] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2004, pp. xii+635. ISBN: 3-540-20488-1. DOI: 10.1007/978-3-662-06307-1.

[3] Reinier Bröker, David Gruenewald, and Kristin Lauter. "Explicit CM theory for level 2-structures on abelian surfaces". In: *Algebra Number Theory* 5.4 (2011), pp. 495–528. ISSN: 1937-0652. DOI: 10.2140/ant.2011.5.495.

[4] Gabriel Cardona and Jordi Quer. "Field of moduli and field of definition for curves of genus 2". In: *Computational aspects of algebraic curves*. Vol. 13. Lecture Notes Ser. Comput. World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83. DOI: 10.1142/9789812701640_0006.

[5] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993, pp. xii+534. ISBN: 3-540-55640-0. DOI: 10.1007/978-3-662-02945-9.

[6] Henri Cohen. *Advanced topics in computational number theory*. Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+578. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0.

[7] Henri Cohen and Xavier-François Roblot. "Computing the Hilbert class field of real quadratic fields". In: *Math. Comp.* 69.231 (2000), pp. 1229–1244. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-99-01111-4. URL: https://doi.org/10.1090/S0025-5718-99-01111-4.

[8] Henri Cohen and Peter Stevenhagen. "Computational class field theory". In: *Algorithmic number theory: lattices, number fields, curves and cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 497–534.

[9] Romain Cosset. "Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques." Theses. Université Henri Poincaré - Nancy I, Nov. 2011. URL: https://tel.archives-ouvertes.fr/tel-00642951.

[10] David A. Cox. *Primes of the form $x^2 + ny^2$*. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356. ISBN: 978-1-118-39018-4. DOI: 10.1002/9781118400722. URL: https://doi.org/10.1002/9781118400722.

[11] Teresa Crespo. "Embedding problems with ramification conditions". In: *Arch. Math. (Basel)* 53.3 (1989), pp. 270–276. ISSN: 0003-889X. DOI: 10.1007/BF01277064.

[12] Régis Dupont. "Moyenne arithmético-géométrique, suites de Borchardt et applications." PhD thesis. École polytechnique, 2006.

[13] Andreas Enge and Emmanuel Thomé. "Computing class polynomials for abelian surfaces". In: *Exp. Math.* 23.2 (2014), pp. 129–145. ISSN: 1058-6458. DOI: 10.1080/10586458.2013.878675.

[14] Claus Fieker. "Computing class fields via the Artin map". In: *Math. Comp.* 70.235 (2001), pp. 1293–1303. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-00-01255-2.

[15] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. ISBN: 0-387-98975-7; 0-387-98981-1. DOI: 10.1007/978-1-4612-1210-2. URL: https://doi.org/10.1007/978-1-4612-1210-2.

[16] 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. DOI: 10.1007/978-1-4612-5485-0.

[17] Kristin Lauter. "Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields". In: *J. Algebraic Geom.* 10.1 (2001). With an appendix in French by J.-P. Serre, pp. 19–36. ISSN: 1056-3911.

[18] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[19] David Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xiv+272. ISBN: 978-0-8176-4569-4. DOI: 10.1007/978-0-8176-4578-6.

[20] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0.

[21] *PARI/GP version 2.11.2*. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2019.

[22] Hans Richter. "Über die Lösbarkeit des Einbettungsproblems für Abelsche Zahlkörper". In: *Math. Ann.* 112.1 (1936), pp. 700–726. ISSN: 0025-5831. DOI: 10.1007/BF01565438.

[23] Hans Richter. "Über die Lösbarkeit einiger nicht-Abelscher Einbettungsprobleme". In: *Math. Ann.* 112.1 (1936), pp. 69–84. ISSN: 0025-5831. DOI: 10.1007/BF01565404.

[24] Xavier-François Roblot. "Algorithmes de Factorisation dans les Extensions Relatives et Applications de la Conjecture de Stark à la Construction des Corps de Classes de Rayon". PhD thesis. Université Bordeaux I, 1997.

[25] Xavier-François Roblot. "Stark's conjectures and Hilbert's twelfth problem". In: *Experiment. Math.* 9.2 (2000), pp. 251–260. ISSN: 1058-6458. URL: http://projecteuclid.org/euclid.em/1045952349.

[26] Xavier-François Roblot. "Unités de Stark et corps de classes de Hilbert". In: *C. R. Acad. Sci. Paris Sér. I Math.* 323.11 (1996), pp. 1165–1168. ISSN: 0764-4442.

[27] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*. https://www.sagemath.org. 2021.

[28] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998, pp. xvi+218. ISBN: 0-691-01656-9. DOI: 10.1515/9781400883943.

[29] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Reprint of the 1971 original, Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994, pp. xiv+271. ISBN: 0-691-08092-5.

[30] Goro Shimura. “On the class-fields obtained by complex multiplication of abelian varieties”. In: *Osaka Math. J.* 14 (1962), pp. 33–44. ISSN: 0388-0699.

[31] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Vol. 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, Tokyo, 1961, pp. xi+159.

[32] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[33] Marco Streng. “An explicit version of Shimura’s reciprocity law for Siegel modular functions”. In: (2021). arXiv: 1201.0020 [math.NT].

[34] Marco Streng. “Complex multiplication of abelian surfaces”. PhD thesis. Universiteit Leiden, 2010.

[35] Paul van Wamelen. “Equations for the Jacobian of a hyperelliptic curve”. In: *Trans. Amer. Math. Soc.* 350.8 (1998), pp. 3083–3106. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-98-02056-X.

[36] André Weil. *Basic number theory*. Third. Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag, New York-Berlin, 1974, pp. xviii+325.

[37] André Weil. “Zum Beweis des Torellischen Satzes”. In: *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.* 1957 (1957), pp. 33–53. ISSN: 0065-5295.

Acknowledgments

I would like to thank my PhD supervisors – Andreas Enge and Marco Streng – who have both always made sure that my work is the best as it can be given the time constraints. Both of you have been supportive and patient with me through the many questions, requests for comments, and administrative procedures that a cotutelle PhD entails. I would also like to thank my jury for agreeing to read my manuscript and be involved in my defense.

Je voudrais remercier Paul Geniet, et Aurel Page pour corriger les épreuves dans l'introduction français. Graag wil ik Bas Jacobs en Peter Koymans bedanken voor hun hulp bij de Nederlandse samenvatting.

I am happy to be part of the friendly number theory teams of both universities whose members have always answered questions kindly, notably Bill Allombert, Karim Belebas, and Peter Bruin who I'm sure to have asked more than several times!

At the beginning of the PhD, language was a bigger barrier than it is now. Thankfully, I had several good friends who always helped me with bureaucracy, such as Christopher Niesen and Krisztian Benyo.

For all the interesting conversations throughout my PhD, I would like to thank my Leiden officemates Rosa, Ruihua, and Stefan, my Bordeaux lunchmates Abhi, Edo, Emmanuele, and Quentin. For agreeing to be my officemate and for all the chats in and out of the office, I would like to thank Fredrik Johansson.

When I came to visit Leiden at the start of my PhD, I didn't expect I would make friends within that one short week. But I did. Thank you Francesco, for all the crazy adventures all over Europe – mathematical or otherwise, Sebastiano, for geeking out with me when it comes to Linux and open-source, Sergej, for always offering to host whenever I go to The Netherlands, and Matteo for all the board games we've played. I can't wait for the day where we can all hang-out together again!

I would like to thank several people for the online conversations about anything and everything. Without my calls with Giovanni, Goma, Guido, Martina, Miggy, Roberto, and Stevan, I would have probably gone insane from isolating during the lockdowns. I look forward to our future conversations, hopefully some of them in-person.

I would like to thank Corentin Prigent, who has been an all-around good friend and one of the few ones who is consistently within walking distance. I would also like to thank my former-acquaintance now-friend Marco Bravin for helping me find an apartment in Bordeaux, for all the delicious weekend pasta dishes, and for being the best quasi-coloc. See you both in Bordeaux, or anywhere else in the world!

I would have never had considered going to Europe much less enter a PhD programme here if it weren't for the encouragement of Fidel Nemenzo and Peter Stevenhagen during the CIMPA-ICTP Manila Summer School. Thank you for believing in my mathematics and programming skills from the very start.

While my scientific eureka moments came with colleagues, most of my recent life realizations came while I started to be with Pierre Brun. Your patience and support enabled me to be better.

Maraming sa mga kaibigan na game pa ring makipagkita at nagpaparamdam pa rin after all these years kahit wala na ako sa Pilipinas, pati na rin sa yaya, sa kapatid, at sa mga pinsan kong forever supportive.

Kay mom and dad na hindi pa rin tumigil ang suporta kahit umabot na sa point na hindi niyo na naiintindihan o nakikita kung ano'ng ginagawa ko, salamat!

Curriculum Vitae

Jared Asuncion was born in the Philippines in 1992. As a grade school student in Pasig Catholic College, he competed in various spelling bees, writing contests and mathematics competitions. After graduating as valedictorian, he started his high school studies in Ateneo de Manila High School where he joined a student organization which teaches English and Mathematics to Filipino grade school students.

During his undergraduate studies which started in 2008, he joined several ACM-ICPC team programming competitions. He would later help found the Philippines' National Olympiad in Informatics with the friends he met in these competitions.

He wrote his bachelor thesis on ranks of elliptic curves of the form $y^2 = x^3 + px$ for primes $p < 1000$ under the supervision of Fidel Nemenzo and graduated cum laude in 2012 from the University of the Philippines, Diliman.

A year after, he attended the *CIMPA-ICTP school on Algebraic Curves over Finite Fields* held in Quezon City, Philippines. In this school, he met Peter Stevenhagen who encouraged him to apply to the ALGANT Masters Programme.

In 2014, he moved to Leiden for his first year of the ALGANT programme and he wrote his Master thesis *Tower decomposition of Hilbert class fields* in Bordeaux under the supervision of Andreas Enge. He obtained Masters diplomas from both Leiden University and University of Bordeaux in 2016.

After finishing his Masters, he was hired as an engineer in INRIA and implemented the Elliptic Curve Primality Proving (ECPP) algorithm in the open-source computer algebra system PARI/GP.

He started his PhD in 2017 under a cotutelle between Leiden University and University of Bordeaux under the supervision of Andreas Enge and Marco Streng.

After the PhD, he intends to stay in Europe to find a job but also intends to continue helping advance math and programming education in whatever way he can.