

Kılıçer, Pinar; Lauter, Kristin; Lorenzo García, Elisa; Newton, Rachel; Ozman, Ekin; Streng, Marco

A bound on the primes of bad reduction for CM curves of genus 3. (English) Zbl 07204745
Proc. Am. Math. Soc. 148, No. 7, 2843-2861 (2020).

Summary: We give bounds on the primes of geometric bad reduction for curves of genus 3 of primitive complex multiplication (CM) type in terms of the CM orders. In the case of elliptic curves, there are no primes of geometric bad reduction because CM elliptic curves are CM abelian varieties, which have potential good reduction everywhere. However, for genus at least 2, the curve can have bad reduction at a prime although the Jacobian has good reduction. Goren and Lauter gave the first bound in the case of genus 2.

In the cases of hyperelliptic and Picard curves, our results imply bounds on primes appearing in the denominators of invariants and class polynomials, which are important for algorithmic construction of curves with given characteristic polynomials over finite fields.

MSC:

- 11G10 Abelian varieties of dimension > 1
- 11G15 Complex multiplication and moduli of abelian varieties
- 14H45 Special algebraic curves and curves of low genus
- 14K22 Complex multiplication and abelian varieties
- 14J15 Moduli, classification: analytic theory; relations with modular forms
- 14Q05 Computational aspects of algebraic curves

Software:

genus3; RECIPI

Full Text: [DOI](#)

References:

- [1] stacks-project The Stacks~Project Authors. The Stacks project. [\url http://stacks.math.columbia.edu](http://stacks.math.columbia.edu), 2016.
- [2] Balakrishnan, Jennifer S.; Ionica, Sorina; Lauter, Kristin; Vincent, Christelle, Constructing genus-3 hyperelliptic Jacobians with CM, LMS J. Comput. Math., 19, suppl. A, 283-300 (2016) · [Zbl 1404.11085](#)
- [3] Bouw, Irene; Cooley, Jenny; Lauter, Kristin; Lorenzo García, Elisa; Manes, Michelle; Newton, Rachel; Ozman, Ekin, Bad reduction of genus three curves with complex multiplication. Women in numbers Europe, Assoc. Women Math. Ser. 2, 109-151 (2015), Springer, Cham · [Zbl 1397.11102](#)
- [4] BKSW Irene Bouw, Angelos Koutsianas, Jeroen Sijsling, and Stefan Wewers. Conductor and discriminant of Picard curves. Preprint, [\href https://arxiv.org/abs/1902.09624](https://arxiv.org/abs/1902.09624)arXiv:1902.09624, 2019.
- [5] Bouyer, Florian; Streng, Marco, Examples of CM curves of genus two defined over the reflex field, LMS J. Comput. Math., 18, 1, 507-538 (2015) · [Zbl 1397.11103](#)
- [6] Bröker, Reinier; Lauter, Kristin; Streng, Marco, Abelian surfaces admitting an $((1,1))$ -endomorphism, J. Algebra, 394, 374-396 (2013) · [Zbl 1316.14085](#)
- [7] Demazure, Michel, Fibrés tangents, algèbres de Lie. Schémas en Groupes, Sém. Géométrie Algébrique, Inst. Hautes Études Sci., 1963, 40 pp. (1963), Inst. Hautes Études Sci., Paris
- [8] Gaudry, P.; Houtmann, T.; Kohel, D.; Ritzenthaler, C.; Weng, A., The 2-adic CM method for genus 2 curves with application to cryptography. Advances in cryptology-ASIACRYPT 2006, Lecture Notes in Comput. Sci. 4284, 114-129 (2006), Springer, Berlin · [Zbl 1172.94576](#)
- [9] Goren, Eyal Z.; Lauter, Kristin E., Class invariants for quartic CM fields, Ann. Inst. Fourier (Grenoble), 57, 2, 457-480 (2007) · [Zbl 1172.11018](#)
- [10] Goren, Eyal Z.; Lauter, Kristin E., Genus 2 curves with complex multiplication, Int. Math. Res. Not. IMRN, 5, 1068-1142 (2012) · [Zbl 1236.14033](#)
- [11] Habegger, Philipp; Pazuki, Fabien, Bad reduction of genus 2 curves with CM jacobian varieties, Compos. Math., 153, 12, 2534-2576 (2017) · [Zbl 06810459](#)

- [12] Kılıçer, Pinar; Labrande, Hugo; Lercier, Reynald; Ritzenthaler, Christophe; Sijtsing, Jeroen; Streng, Marco, Plane quartics over \mathbb{Q} with complex multiplication, *Acta Arith.*, 185, 2, 127-156 (2018) · [Zbl 1409.14051](#)
- [13] KLS Pinar Kılıçer, Elisa Lorenzo-García, and Marco Streng. Primes dividing invariants of CM Picard curves. *Canadian Journal of Mathematics*, (Published online), 2018. [url https://doi.org/10.4153/S0008414X18000111](https://doi.org/10.4153/S0008414X18000111). · [Zbl 07184219](#)
- [14] Koike, Kenji; Weng, Annegret, Construction of CM Picard curves, *Math. Comp.*, 74, 249, 499-518 (2005) · [Zbl 1049.14014](#)
- [15] LarioSomoza Joan-Carles Lario and Anna Somoza. A note on Picard curves of CM-type. [href https://arxiv.org/abs/1611.02582](https://arxiv.org/abs/1611.02582)arXiv:1611.02582, 2016.
- [16] Lauter, Kristin; Viray, Bianca, An arithmetic intersection formula for denominators of Igusa class polynomials, *Amer. J. Math.*, 137, 2, 497-533 (2015) · [Zbl 1392.11033](#)
- [17] LLLR Reynald Lercier, Qing Liu, Elisa Lorenzo-García, and Christophe Ritzenthaler. Reduction type of smooth quartics. Preprint, [href https://arxiv.org/abs/1803.05816](https://arxiv.org/abs/1803.05816)arXiv:1803.05816, 2018.
- [18] Liu, Qing, Algebraic geometry and arithmetic curves, *Oxford Graduate Texts in Mathematics* 6, xvi+576 pp. (2002), Oxford University Press, Oxford · [Zbl 0996.14005](#)
- [19] Mumford, David, Abelian varieties, *Tata Institute of Fundamental Research Studies in Mathematics* 5, xii+263 pp. (2008), Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi · [Zbl 1177.14001](#)
- [20] Serre, Jean-Pierre; Tate, John, Good reduction of abelian varieties, *Ann. of Math. (2)*, 88, 492-517 (1968) · [Zbl 0172.46101](#)
- [21] Shioda, Tetsuji, On the graded ring of invariants of binary octavics, *Amer. J. Math.*, 89, 1022-1046 (1967) · [Zbl 0188.53304](#)
- [22] Siegel, Carl Ludwig, Lectures on the geometry of numbers, x+160 pp. (1989), Springer-Verlag, Berlin · [Zbl 0691.10021](#)
- [23] StrengImplementation Marco Streng. RECIPI – REpository of Complex multiPIlication SageMath code. [url http://pub.math.leidenuniv.nl/~streng](http://pub.math.leidenuniv.nl/~streng)
- [24] Streng, Marco, Computing Igusa class polynomials, *Math. Comp.*, 83, 285, 275-309 (2014) · [Zbl 1322.11066](#)
- [25] Weng, Annegret, A class of hyperelliptic CM-curves of genus three, *J. Ramanujan Math. Soc.*, 16, 4, 339-372 (2001) · [Zbl 1066.11028](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.