RESEARCH PLAN

LINDA FREY

1. Past research

As a part of my PhD thesis, I made Habegger's 2013 [Hab13] result explicit in the following way.

Theorem 1 ([Fre21a]). *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Let $\alpha \in \mathbb{Q}(E_{\mathit{tors}})^* \setminus \mu_\infty$. Then with $n = 10^7 \max\{985, \frac{1}{12}(18N \log N) + 3\}^2$ we have*

$$h(\alpha) \geq ((8Ne^{\vartheta(n)})^{Ne^{\vartheta(n)}(\log(8Ne^{\vartheta(n)}))^5} 18N \log N)^{-44}$$

where $\vartheta(n) = \sum_{p \leq n} \log p$ and μ_∞ is the set of roots of unity.

As a side result, I also made the result of Elkies [Elk87] on the infinitude of supersingular primes for an elliptic curve explicit.

Theorem 2 ([Fre21a]). *Let E be an elliptic curve with j-invariant j_E and conductor N. Let*

$$B_E = \begin{cases} \left(\frac{\log j_E}{2\pi}\right)^2 & \text{if } j_E > 0, \\ \left(\frac{\log |j_E|}{\pi} + 1\right)^2 & \text{if } j_E < 0, \\ 0 & \text{if } j_E = 0. \end{cases}$$

Let $M \in \mathbb{N}$ and $n = \max(11, M, B_E)$. Then there exists a supersingular prime p of E such that $p \geq n$ and

$$\log p \leq 2 \cdot 10^8 (8Ne^{\vartheta(n)})^{\sqrt{Ne^{\vartheta(n)}}(\log(8Ne^{\vartheta(n)}))^3} (\sqrt{Ne^{\vartheta(n)}}(\log(8Ne^{\vartheta(n)}))^3)^2 \max(h(j_E), \log 2).$$

There are results on the growth of the amount of supersingular primes less than x by Fouvry and Ram Murty [FRM96], but those results do not give an explicit bound for a small supersingular prime.

To get the above result, I followed Elkies' [Elk87] constructive proof of the existence of infinitely many supersingular primes for an elliptic curve and used a result of Bennett, Martin, O'Bryant and Rechnitzer [BMOR18] to bound the prime in the arithmetic progression that resulted from Elkies' proof.

One intermediate result in the proof of the explicit height bound above is the following theorem.

Date: Fall 2022.

Theorem 3 ([Fre21a])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $p \geq 5$ be a supersingular prime of E such that the Galois representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. Then for $\alpha \in \mathbb{Q}(E_{tors})^* \setminus \mu_\infty$ we have*

$$h(\alpha) \geq \frac{(\log p)^5}{10^{31} p^{44}}.$$

In order to prove this result, I had to prove an explicit version of a version of Bilu's Theorem in [Bil97] that can handle a logarithmic singularity that occurs in Habegger's paper. I used an approach with polynomials and bounded their height via a theorem of Mignotte [Mig89].

The following is my generalization of Habegger's 2013 result.

Theorem 4 ([Fre21b])**.** *Let E be an elliptic curve without complex multiplication over $\mathbb{Q}$ and let $L/\mathbb{Q}$ be a Galois extension with uniformly bounded local degrees above all but finitely many primes. Then $L(E_{tor})$ has the Bogomolov property.*

2. Current and future research

2.1. **Heights and Igusa invariants.** In the genus 1 case, the question of integrality of j-invariants of elliptic curves with complex multiplication has been answered by Bilu, Habegger and Kühne clearly [BHK18]: No j-invariant of a CM elliptic curve defined over $\mathbb{C}$ is an algebraic unit. This result was generalized with modular techniques by Li [Li18]. Recently, progress has been made in the direction of S-units (which is a generalization of units) by Campagna [Cam21b], [Cam21a] and Herrero-Menares [HMRL20].

The genus 2 case is more complicated. Here, the space of isomorphism classes (we call it the moduli space) is 3-dimensional, hence we need a triple of invariants to classify these curves. In fact, we define ten invariants and combine them ("projectively weighted") such that we get a suitable triple of invariants and call them Igusa invariants.

For a fixed curve, we call a prime of bad reduction bad prime. Remark that by the work of Serre and Tate ([ST68]), abelian varieties have potential good reduction everywhere. The bad prime is *only* a bad prime of the curve, not of the Jacobian. The point about bad primes is that the *Jacobian* of a CM curve has potential good reduction everywhere, but the *curve itself* can have bad primes. There is a connection between the bad primes of the curve, the integrality of the Igusa invariants and the type of the reduction modulo the bad primes.

A general question is: What can we say about Igusa invariants? More detailed questions and conjectures are:

Question 1. *How many curves of genus two, defined over $\overline{\mathbb{Q}}$, are there such that its jacobian has complex multiplication exist where none/one/two/three of the Igusa invariants are algebraic integers/algebraic units?*

Question 2. *Let C_1 and C_2 be genus two curves over a number field K and let A_1 and A_2, respectively, be their Jacobians. Let $J_1 = (j_1(C_1), j_2(C_1), j_3(C_1))$ be affine Igusa invariants associated with C_1, respectively J_2 for C_2. Assume there is an isogeny f between A_1 and A_2. Can one control $h(J_1) - h(J_2)$ explicitly in terms of $deg(f)$? Can we bound $h(J_1)$?*

Since the absolute Igusa invariants are defined through ten projective invariants and can be combined in several ways (given that the weights match), it does not make much sense asking for units.

Conjecture 1. *There are only finitely many (isomorphism classes of) hyperelliptic curves of genus 2 defined over $\overline{\mathbb{Q}}$ with complex multiplication such that all three Igusa invariants are algebraic integers.*

There are already computational results on bounds on the denominators but since they all come from cryptography, they are upper bounds. We want to find lower bounds or statements on existance of denominators. There is also a formula coming from arithmetic intersection theory, first by Bruinier-Yang and Yang and then generalized by Lauter-Viray which makes it seem promising to use Li's methods in the genus 2 case. In this project I work together with Elisa Lorenzo García (Rennes/Neuchâtel) and Samuel Le Fourn (Grenoble) on the generalization of algebraic techniques and making bounds explicit.

A consequence of the result of Habegger and Pazuki [HP17] is the following:

Theorem 5. *There are infinitely many curves of genus two such that their jacobian has complex multiplication and not all three Igusa invariants are algebraic integers.*

With my coauthors I am writing a paper on results we found on the Igusa invariants. At the moment we are working on an explicit version of the height bound in Habegger's and Pazuki's paper.

We can define the Igusa invariants in terms of modular forms, just like the j-invariant in genus 1. With these techniques, the result of Bilu, Habegger and Kühne is even generalised by Li [Li18] where it is proved that for any two elliptic curves with complex multiplication and an integer m, there always exists a prime p such that the reductions modulo p are m-isogenous.

With my coauthors Elisa Lorenzo García and Samuel Le Fourn I am working on a generalization of this kind: The straightforward generalisation to genus 2 with $m = 1$ would be: given two CM abelian surfaces there exists always a prime such that the reduction are isomorphic. But this is false and it is easy to construct counterexamples. This is related with the fact that the dimension of the moduli space of genus 1 curves is 1 and the dimension of the moduli space of genus 2 curves is 3. So we need to impose more conditions. Real multiplication only lowers the dimension by 1, and 2 is still too big to expect a collision. But if we add the condition of being a product of elliptic curves we could expect the result to be true.

Conjecture 2. *Let A_1 and A_2 CM abelian surfaces that are products of elliptic curves with complex multiplication. Then there always exists a prime number such that they have isomorphic reduction. (A weaker version would be to prove that there exist at most a finite number of exceptions, and a stronger version asking them to be m-isogenous for a fixed integer m.)*

Furthermore, we are almost finished with a preprint that makes height bounds in the Habegger Pazuki paper completely explicit.

2.2. **2-isogenous elliptic curves and their non-isomorphic torsion groups over finite fields.**

This project is the fruit of the workshop Rethinking Number Theory 3 that I attended this summer. It is joint work with John Cullinan, Jorge de Mello, Shanna Dobson, Asimina Hamakiotes, Roberto Hernandez and Gabrielle Scullard.

Consider two 2-isogenous elliptic curves over $\mathbb{Q}$. Being 2-isogenous makes them have the same order of their Mordell-Weil group, but they don't have to be isomorphic. What about the case when they are isomorphic? What happens to extensions? Currently still unpublished work of John Cullinan and Nathan Kaplan proves in some generic setting with fixed E and E' that in $\frac{1}{30}$ of the cases (varying the primes), the Mordell-Weil groups are not isomorphic and then we have that $E(\mathbb{F}_p) \cong E'(\mathbb{F}_p)$, but $E(\mathbb{F}_{p^2}) \cong E'(\mathbb{F}_{p^2})$.

The key how this is tackled is looking at the 2^m-torsion points of the elliptic curves for natural m. Each of the towers of 2-torsion, 2^2-torsion, etc. will have one step where the 2^m-torsion is full, but the 2^{m+1}-torsion is not. Cullinan and Kaplan showed that when the step for E is n, then the step for E' is either $n-1$ or $n+1$. Then we will call $(n, n+1)$ or respectively $(n, n-1)$ the defect. Now we want to look at pairs of 2-isogenous elliptic curves where -1 is contained in the image of the 2-adic Galois representation. This is the setting that Cullinan and Kaplan haven't looked at. There is a database of possible images of 2-adic Galois representations of non-CM elliptic curves over $\mathbb{Q}$. We are - with the help of Magma - computing defects and proportions of primes that give a defect for a given 2-adic Galois image. We are hoping to find regularities in our results and prove them.

2.3. **Transcendence measure for roots of e.**

This project is the fruit of the workshop Women in Numbers Europe 4 that I attended this summer. It is joint work with Anne-Maria Ervnall-Hytönen, Marta Dujella and Bidisha Roy.

Let $m \geq 2$. A transcendence measure for e is a function that upper bounds the expression

$$\left|\lambda_m e^k + \ldots + \lambda_1 e^1 + \lambda_0\right|,$$

where $\lambda_i \in \mathbb{Z}$. Usually, the transcendence measure depends on the height of the λ_i and the degree m of the polynomial. This has been treated in papers [EHMaS19] and [EHLMa15].

In our project we want to look at roots of e instead of e. So we want to find a bound for the expression

$$\left|\lambda_m e^{k/n} + \ldots + \lambda_1 e^{1/n} + \lambda_0\right|.$$

In order to do that, we went through the paper of [EHMaS19] and adapted the strategy from e to $e^{\frac{1}{n}}$. This is still work in progress, but at least a proceedings paper will be ready by February 2023 and a bigger paper is expected for summer 2023.

2.4. **Leopoldt.** Together with Preda Mihăilescu I am writing a paper on a special case of the Leopoldt conjecture.

Let p be a prime and $\mathbb{K}$ a number field. The Leopoldt Conjecture states, in its initial form, that the p-adic regulator of $\mathbb{K}$, if defined, will not vanish. Leopoldt stated this assumption restricted to the case when $\mathbb{K}$ is an abelian extension of $\mathbb{Q}$, in his seminal paper [Leo62] from 1962. The original form of the conjecture was shown by Ax [Ax65] to require some yet unproven results from Diophantine Approximation. These were precisely the result on linear forms in logarithms [Bak67], which brought Alan Baker the Fields medal short time later, in 1964. Based on the indication of Ax and the global result of Baker, A. Brumer proved the p-adic version of Baker's result, which immediately implied the non-vanishing of the p-adic regulator in abelian fields [Bru67].

We shall use here the following formulation of the Theorem of Baker and Brumer on p-adic forms in logarithms:

Theorem 6. *Let $\mathbb{K}/\mathbb{Q}_p$ be a p-adic field and $\alpha_i, \beta_i \in \mathbb{K}; i = 1, 2, \ldots, n$ be algebraic numbers. Assume that $\sum_{i=1} n\beta_i \log_p(\alpha_i) = 0$. Then the linear dependence holds with $\beta_i \in \mathbb{Q}$.*

The applications of Baker theory for proving more general cases of the Leopoldt Conjecture are rare. Here are some of the few examples: Emsalem, Kisilevsky and Wales [EKW84] use group representations and Baker theory for proving the Conjecture for some small non abelian groups; this direction of research has been continued in some further papers by Emsalem or Emsalem and coauthors. In general, hardly any infinite families of non-abelian number fields exist, where the Leopoldt Conjecture was proved. Our result in the present paper considers a special class of metabelian extensions (that is, the commutator subgroup of the Galois group is abelian) and is herewith not a wide generalization either. It has however the interest to provide the proof of a specific fact that implies the Greenberg λ-conjecture for abelian fields.

Theorem 7. *Let $\mathbb{L}/\mathbb{Q}$ be a metabelian extension and $\mathbb{K} \subset \mathbb{L}$ such that $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\mathbb{Q}$ are abelian and $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \ltimes \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Suppose in addition that the primes above the rational prime p are totally split in $\mathbb{L}/\mathbb{K}$. Then the Leopoldt conjecture holds for $\mathbb{L}$ and p.*

2.5. **Generalization of the PhD result.** The results of my PhD have raised the question how they can further be generalized. One can generalize this in several ways: We can generalize the elliptic curve, by looking at a more complicated abelian variety, we can allow larger base fields or we can let the abelian variety be defined over a larger field.

We can also look at the counterpart of $\mathbb{Q}(E_{\text{tor}})$, namely the points $E(\mathbb{Q}(E_{\text{tor}}))$ where we allow the coordinates to be in $\mathbb{Q}(E_{\text{tor}})$, hence get all the possible torsion. There we will look at the Néron-Tate height, which is a height on points of abelian varieties. We can of course also generalize the result: Instead of E we look at curves of higher genus or in general abelian varieties. We can also exchange $/Q$ for larger (number) fields.

Conjecture 3. *Let A be an abelian surface defined over a number field K with complex multiplication. Let L be a Galois extension of K with uniformly bounded local degrees. Then $L(A_{tor})$ has the Bogomolov property.*

We can consider a special case and let A be an elliptic curve. To be able to use Habegger's method, we need Elkies' result on supersingular primes which needs the condition of K having a real embedding. The special case of $K = \mathbb{Q}$ is the main result in [Fre21b].

We still have to find out if we have to put more constraints on A, K and L. Maybe one has to restrict to a subset of the torsion points consisting of points of order not divisible by a fixed prime.

2.6. **Block-chain.** A computer science professor from Algeria, Laid Kahloul, found my YouTube videos on elliptic curves and asked me to collaborate with him on a blockchain paper. He will contribute the computer science and I will contribute the math. The blockchain technology needs - just as cryptography - a trapdoor function. Commonly used trapdoor functions are factorization of large integers, addition of points on elliptic curves and addition of pairs of points on genus 2 curves. Here, my knowledge of genus 1 and 2 curves will be of great help to do research in a more applied direction. The first paper is still in progress (my part is done) and more will follow.

LITERATUR

[Ax65] J. Ax. On the units of an algebraic number field. *Illinois Journal of Mathematics*, 9:584–589, 1965.

[Bak67] A. Baker. Linear forms in the logarithms of algebraic numbers I, II, III. *Mathematika*, 13, 14:204–216; 102–107, 220–228, 1966, 67.

[BHK18] Yu. Bilu, P. Habegger, and L. Kühne. No singular modulus is a unit, 2018.

[Bil97] Y. Bilu. Limit distribution of small points on algebraic tori. *Duke Math. J.*, 89(3):465–476, 1997.

[BMOR18] M. A. Bennett, G. Martin, K. O'Bryant, and A. Rechnitzer. Explicit bounds for primes in arithmetic progressions. *ArXiv e-prints*, January 2018.

[Bru67] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[Cam21a] Francesco Campagna. Effective bounds on differences of singular moduli that are s-units, 2021.

[Cam21b] Francesco Campagna. On singular moduli that are S-units. *Manuscripta Math.*, 166(1-2):73–90, 2021.

[EHLMa15] Anne-Maria Ernvall-Hytönen, Kalle Leppälä, and Tapani Matala-aho. An explicit Baker-type lower bound of exponential values. *Proc. Roy. Soc. Edinburgh Sect. A*, 145(6):1153–1182, 2015.

[EHMaS19] Anne-Maria Ernvall-Hytönen, Tapani Matala-aho, and Louna Seppälä. On Mahler's transcendence measure for e. *Constr. Approx.*, 49(2):405–444, 2019.

[EKW84] M. Emsalem, H. Kisilevsky, and D. Wales. Indépendance linéaire sur $\overline{\mathbb{Q}}$ de logarithmes p - adiques de nombres algébriques et rang p - adique du groupe des unités d'un corps de nombres. *Journal of Number Theory*, 19:384–391, 1984.

[Elk87] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[Fre21a] Linda Frey. Explicit small heights in infinite non-abelian extensions. *Acta Arith.*, 199(2):111–133, 2021.

[Fre21b] Linda Frey. Small heights in large non-abelian extensions. *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, 2021.

[FRM96] E. Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[Hab13] P. Habegger. Small height and infinite nonabelian extensions. *Duke Math. J.*, 162(11):2027–2076, 2013.

[HMRL20] Sebastián Herrero, Ricardo Menares, and Juan Rivera-Letelier. p-adic distribution of CM points and Hecke orbits I: Convergence towards the Gauss point. *Algebra Number Theory*, 14(5):1239–1290, 2020.

[HP17] Philipp Habegger and Fabien Pazuki. Bad reduction of genus 2 curves with CM jacobian varieties. *Compos. Math.*, 153(12):2534–2576, 2017.

[Leo62] H. W. Leopoldt. Zur Artihmetik in Abelschen Zahlkörper. *J. Reine Angew. Math*, 209:54–71, 1962.

[Li18] Yingkun Li. Singular units and isogenies between cm elliptic curves, 2018.

[Mig89] M. Mignotte. Sur un théorème de M. Langevin. *Acta Arith.*, 54(1):81–86, 1989.

[ST68] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

MATHEMATISCHES INSTITUT, BUNSENSTR. 3-5, 37073 GÖTTINGEN, GERMANY
Email address: `linda.frey89@gmail.com`