RESEARCH STATEMENT

My general research interests lie in (Algebraic) Number Theory. During my PhD I worked on elliptic curves, heights and supersingular primes.

1. Elliptic Curves and Heights

1.1. **Background and past research.** In 1933, Lehmer [Leh33] proposed the question on how the height in a field extension is bounded from below relatively to the degree of the extension. By Northcott's Theorem, zero and roots of unity have height zero. All other elements have positive height which could possibly be bounded from below by a positive constant. A survey article by Smyth on that topic [Smy08] which cites 173 articles shows that this topic is still of great interest.

We will focus on the *Bogomolov* property. A field is said to be *Bogomolov* if there is a positive constant such that all heights of non-zero and non-torsion elements are bounded from below by that constant.

Habegger [Hab13] showed that $\mathbb{Q}(E_{\text{tor}})$ which is the field that contains all coordinates of torsion points of an elliptic curve defined over $\mathbb{Q}$ satisfies the *Bogomolov* property. As a part of my PhD thesis, I made the said result explicit:

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Let $\alpha \in \mathbb{Q}(E_{tors})^* \setminus \mu_\infty$. Then $h(\alpha)$ can be bounded from below explicitly in terms of the conductor of E.*

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

Theorem 2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exists a prime p which is supersingular for E and explicitly bounded from above in terms of the conductor of E.*

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

I proved a generalization of Habegger's 2013 result:

Theorem 3. *Let E be an elliptic curve 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.*

Proving this required Galois theory of local fields and ramification theory.

1.2. **Present and future research.** My key research future are curves of genus two. One of the natural generalizations of the above results is proving the following conjecture:

Conjecture 1. *Let C be a curve of genus two, defined over $\mathbb{Q}$. Let p be a suitable prime. The union of all fields that contain all N-torsion points of the jacobian of C where N is a natural number and not divisible by p has the Bogomolov property.*

One still has to find out which exact properties the prime p has to have. In the genus one case we use supersingularity and surjectivity of the prime. In genus two, there is something similar but further conditions may have to be true. The techniques can probably be adjusted, though we have to take care of the fact that in genus two we can no longer

work on the curve, but have to work on its jacobian. This project is joint work with Valentijn Karemaker (Utrecht).

In genus two, there is an analogue of the j-invariant, the (triple of) Igusa invariants. In genus one there is a recent result of Bilu, Habegger and Kühne ([BHK18])which states that no j-invariants of elliptic curves with complex multiplication can be algebraic units. Later, Li ([Li18]) proved the same result with modular techniques. I want to find out what can be said in the genus two analogue.

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?*

Since the absolute Igusa invariants are defined through ten projective invariants and can be combined in several ways (given that the weights match), it probably does not make much sense asking for units. So I will concentrate on the denominators of the Igusa invariants and a conjectural analogue to the result of Bilu, Habegger and Kühne could be:

Conjecture 2. *There are only finitely many genus 2 curves defined over $\overline{\mathbb{Q}}$ such that their jacobians have complex multiplication and all Igusa invariants are algebraic integers.*

There are already computational results (see [GL07]) 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 ([BY06], [Yan13] and [Yan10]) and then generalized by Lauter-Viray ([LV15]) which makes it sound promising to use Li's methods in the genus 2 case. This project is joint work with Elisa Lorenzo Garcia (Rennes/Neuchâtel) and Samuel Le Fourn (Grenoble).

As a partial answer to the question I proved the following result:

Theorem 4. *There are infinitely many curves of genus two such that their jacobian has complex multiplication and not all three Igusa invariants are algebraic integers.*

REFERENCES

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

[BY06] Jan Hendrik Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006.

[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.

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

[GL07] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007.

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

[Leh33] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.

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

[LV15] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.

[Smy08] Chris Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[Yan10] Tonghai Yang. An arithmetic intersection formula on Hilbert modular surfaces. *Amer. J. Math.*, 132(5):1275–1309, 2010.

[Yan13] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. *Asian J. Math.*, 17(2):335–381, 2013.