Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Stellingen

behorende bij het proefschrift getiteld

Geometric quadratic Chabauty and other topics in number theory

I. The projective hyperelliptic curve defined by the equation $y^2+y = x^6-3x^5+x^4+3x^3-x^2-x$ has exactly 14 rational points. This can be shown using the geometric quadratic Chabauty method.

II. In characteristic zero, all formal commutative biextensions are isomorphic to an additive biextension.

III. If p^e be a prime power greater than 12 and different from $3^3, 2^4, 2^5, 2^6$, then all the automorphisms of a Cartan modular curve of level p^e are modular. The same statement is false when $p^e \leq 11$, while the cases $3^3, 2^4, 2^5, 2^6$ are open, in the author's knowledge.

IV. If p is a prime number and $e > p$ is an integer, then the discrete logarithm problem in the group $\mathbb{F}_{p^e}^{\times}$ can be solved in $(\log(p^e))^{O(\log\log(p^e))}$ operations.

V. The article [1] is one of the most important articles about automorphisms of modular curves. Yet, as shown in [2], there are some mistakes in the statements of Lemma 1.6, Lemma 2.15 there contained (the main theorem of the article is true, up to excluding the case $N = 108$).

VI. The geometric quadratic Chabauty method described in chapter 1 can be generalised to arbitrary number fields. See the ongoing project [3] by Pavel Čoupek, David Lilienfeldt, Luciena Xiao and Zijian Yao.

VII. Interestingly, the implementation details of discrete logarithm algorithms based on elliptic basis have been already studied in [4]

VIII. Chapter 1 uses geometric methods, that can and should be visualised. A cartoon guide to it is available at [5]

Guido Maria Lido,
Leiden ??-??-????

References

[1] M. A. Kenku, F. Momose, *Automorphism groups of the modular curves $X_0(N)$*. Compositio Mathematica, 65 (1988)

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

[3] https://www.math.mcgill.ca/lilien/Chabauty-Part1.pdf

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

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