Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Summary

Geometric quadratic Chabauty and other topics in number theory

This thesis consists of three parts.

In the first part we describe a generalization of Chabauty's method which, in certain cases, computes the set of rational points on a curve C of genus $g > 1$. Chabauty's method is to intersect, for a prime number p, in the p-adic Lie group of p-adic points of the jacobian J, the closure of the Mordell-Weil group with the p-adic points of the curve. If the Mordell-Weil rank r is less than the genus, this method produces a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$. In our method, we substitute J with a product T of $\mathbb{G}_{\mathrm{m}}$-torsors over it. We take these torsors to be pull backs of the Poincaré torsor of the jacobian, and we use the biextension structure on it to parametrize the integral points on T. When $r-g+1$ is smaller than the rank of the Néron-Severi group of the jacobian, our method produces a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$.

The second part of this thesis is devoted to the study of automorphisms of Cartan modular curves. In the literature we usually hit Cartan curves of prime level p, because their non-cuspidal points give elliptic curves E such that the natural Galois representation on the p-torsion of E is not surjective. We also study Cartan curves of composite level and we prove that, if the level is large enough, these curves only have the "expected" automorphisms, namely those automorphisms that lift to the upper half plane $\mathbb{H}$. In particular, we show that, when the level p is prime, this result holds for $p > 11$. The main novelty of our proof is a thorough study, for a wide class of modular curves, of the action of Hecke operators on elliptic points and cuspidal points. Then, we generalize classical methods to bound the field of definition of an automorphism u and we deduce that the u almost commutes with the Hecke operators. We conclude that u preserves both the set of elliptic points and the set of cuspidal points. Basic topological properties of covers imply that u lifts to the upper half plane $\mathbb{H}$.

The last part deals with the discrete logarithm problem in finite fields of small characteristic: given a finite field K of characteristic p and order larger than p^p, given a generator g of the group $K^\times$ and given another element $h \in \mathbb{K}^\times$, the problem is to determine an integer z such that $h = g^z$. In the last chapter of our thesis we describe a probabilistic algorithm that solves this problem in quasi-polynomial time, that is $\log(\#K)^{O(\log\log \#K)}$. A *heuristically quasi-polynomial* algorithm was already proposed by Joux, Barbulescu, Gaudry and Thomé, whose main idea is to look for an element of K on which the Frobenius automorphism acts in a "simple" way. We use this idea but we look for two elements of K on which the Frobenius acts in a "simple" way. In particular, we want these two elements to be the coordinates of a point on an elliptic curve E and we define "simple" using the group structure on E. Because of the abundance of elliptic curves, it is easy to prove that each finite field of small characteristic can be embedded in a slightly larger field containing two such elements. This makes our approach rigorous.