Galois representations of elliptic curves and abelian entanglements

Brau Avila, Julio

Summary

This thesis deals primarily with the study of Galois representations attached to torsion points on elliptic curves. In the first chapter we consider the problem of determining the image of the Galois representation ρ_E attached to a non-CM elliptic curve over the rational number field $\mathbb{Q}$. We give a deterministic algorithm that determines the image of ρ_E as a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, where the output is given as an integer m together with a finite subgroup $G(m) \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The image of ρ_E is then the subgroup of all elements of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose reduction modulo m belongs to $G(m)$.

In the second part we develop a method using character sums that uses the image of ρ_E to describe densities of sets of primes p for which $\tilde{E}(\mathbb{F}_p)$ has certain prescribed properties. If E is an elliptic curve over $\mathbb{Q}$, then it follows by work of Serre and Hooley that, under the assumption of the Generalized Riemann Hypothesis, the density of primes p such that the group of $\mathbb{F}_p$-rational points of the reduced curve $\tilde{E}(\mathbb{F}_p)$ is cyclic can be written as an infinite product $\prod \delta_\ell$ of local factors δ_ℓ reflecting the degree of the ℓ-torsion fields, multiplied by a factor that corrects for the entanglements between the various torsion fields. We show that this correction factor can be interpreted as a character sum, and the resulting description allows us to easily determine non-vanishing criteria for it. We apply our character sum method to a variety of other settings. Among these, we consider the aforementioned problem with the additional condition that the

primes p lie in a given arithmetic progression. We also study the conjectural constants appearing in Koblitz's conjecture, a conjecture which relates to the density of primes p for which the cardinality of the group of $\mathbb{F}_p$-points of E is prime. The unifying theme in all these settings is that the constants we are interested in are completely determined by the image of ρ_E.

The final chapter deals with the classification of non-Serre curves. An elliptic curve over $\mathbb{Q}$ is a *Serre curve* if its attached Galois representation is as large as possible, and it is known that most elliptic curves over $\mathbb{Q}$ are of this type. We exhibit a modular curve of level 6 that completes a set of modular curves which parametrise non-Serre curves. This modular curve also gives an infinite family of elliptic curves with non-abelian "entanglement fields". Exhibiting such a family is naturally motivated by questions arising in the previous chapter regarding the classification of elliptic curves to which we can apply the character sum method described above.