CHANTAL DAVID, Concordia University

On the distribution of Frobenius Rings of Elliptic Curves

Let E be an elliptic curve over Q. For each prime p of good reduction, E reduces to a curve over F_p, the Frobenius endormorphism of E/F_p satisfies $x^2 - a_p(E)x + p$, and the Frobenius ring $Z[\sqrt{a_p^2 - 4p}]$ is a subring of the endomorphism ring $\mathrm{End}(E/F_p)$. It is then natural to ask whether the Frobenius ring is the full endomorphism ring, or whether the Frobenius ring is the maximal order in $Q[\sqrt{a_p^2 - 4p}]$.

The second question is a refinement of the first one, and seems to be more difficult. For example, it is not known that there exists infinitely many such primes. For CM curves, the Frobenius ring is the maximal order in $Q[\sqrt{a_p^2 - 4p}]$ if and only if p lies in a quadratic progression.

We will show in this talk that on average, the correct asymptotic holds for the number of primes p such that $a_p^2 - 4p$ is square-free (and then the Frobenius ring is the maximal order). We can also restrict $a_p^2 - 4p$ to an arithmetic progression.

This is joint work with Jorge Jimenez Urroz (UPC, Barcelona).