ELLIPTIC CURVES AND THE DISTRIBUTION OF PRIMES

KEVIN JAMES

ABSTRACT. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$. Then the trace of the Frobenius map of E for the prime p is denoted $a_E(p)$ and satisfies the equation $a_E(p) = p+1-\#E(\mathbb{F}_p)$. By theorems of Hasse and Deuring, we know that for a fixed prime p, $a_E(p)$ takes on every integer value in $(-2\sqrt{p}, 2\sqrt{p})$ as E varies over all elliptic curves defined over $\mathbb{F}_p$. It is natural to consider the complementary question of how often $a_E(p)$ takes on a given value as p varies and E is fixed.

As a corollary of the Cebotarev density theorem, one has for all $r \in \mathbb{Z}$ and $M \in \mathbb{N}$ there exists a constant $C_{E,r,M}$ such that

$$\#\{p < X |\ p \text{ is prime and } a_E(p) \equiv r \bmod M\} \sim C_{E,r,M} \frac{X}{\log X}$$

The Sato-Tate conjecture asserts that if E does not have complex multiplication and if $-1 < \alpha < \beta < 1$, then

$$\#\left\{p < X |\ p \text{ is prime and } 2\alpha\sqrt{p} < a_E(p) < 2\beta\sqrt{p}\right\} \sim \left(\frac{2}{\pi}\int_\alpha^\beta \sqrt{1-t^2}\, dt\right) \frac{X}{\log X}$$

Lang and Trotter have made the more precise conjecture that if $r \in \mathbb{Z}$ and E does not have complex multiplication or if $r \neq 0$ then

$$\#\{p < X | p \text{ is prime and } a_E(p) = r\} \sim C_{E,r} \frac{\sqrt{X}}{\log X}.$$

where $C_{E,r}$ is an explicit constant depending only on E and r. Richard Taylor has recently proved the Sato-Tate conjecture for an elliptic curve defined over any totally real number field which satisfies a mild hypothesis. The more precise conjecture of Lang and Trotter remains open.

In this talk we will briefly discuss a potential refinement of the Sato-Tate conjecture and a generalization of the Lang-Trotter conjecture. We will also discuss some averaging results related to these conjectures. We will devote most of our attention to averaging results related to the following generalization of the Lang-Trotter conjecture to the setting of number fields. If K is a number field and E is an elliptic curve defined over K we define

$$\pi_E^{r,f}(X) = \#\{\mathfrak{P} \subset \mathcal{O}_K |\ \mathfrak{P} \text{ is a prime ideal; } N\mathfrak{P} < X; \deg(\mathfrak{P}) = f;\ a_E(\mathfrak{P}) = r\},$$

where $\deg(\mathfrak{P})$ denotes the dimension of $\mathcal{O}_K/\mathfrak{P}$ over $\mathbb{F}_p$ (p is the rational prime lying beneath $\mathfrak{P}$) and $a_E(\mathfrak{P})$ denotes $|\mathcal{O}_K/\mathfrak{P}| + 1 - \#E(\mathcal{O}_K/\mathfrak{P})$. It is conjectured that there is a constant $C_{E,r,f}$ such that

$$\pi_E^{r,f}(X) \sim C_{E,r,f} \cdot \begin{cases} \frac{\sqrt{X}}{\log X} & \text{if } f = 1, \\ \log\log X & \text{if } f = 2, \\ 1 & \text{otherwise} \end{cases}$$

We show that if K is an Abelian extension of $\mathbb{Q}$ then this conjecture is true in an average sense if one averages over all elliptic curves defined over K.