A joint distribution theorem with applications to extremal primes

Neha Prabhu

University of Pune

(Joint with Amita Malik)

Equidistribution of a sequence

A sequence of real numbers $\{x_n\}$ in $[0,1]$ is said to be uniformly distributed, or equidistributed in $[0,1]$ if, for every subinterval $[a,b] \subseteq [0,1]$, the following holds.

$$\lim_{N\to\infty} \frac{\#\{n \leq N : a_n \in [a,b]\}}{N} = b - a.$$

- The sequence of fractional parts of $\{n\alpha\}$, where α is a fixed irrational number, is an equidistributed sequence.
- The sequence of fractional parts of $\{\log n\}$ is not uniformly distributed.

More generally, a sequence $\{x_n\}$ is equidistributed w.r.t the measure μ if

$$\lim_{N\to\infty} \frac{\#\{n \leq N : a_n \in [a,b]\}}{N} = \int_a^b \, d\mu.$$

Sato-Tate conjecture

For $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $\Delta(a, b) = 4a^3 + 27b^2 \neq 0$, let $E(a, b)$ be the elliptic curve given in Weierstrass form by

$$y^2 = x^3 + ax + b.$$

Reducing a, b mod p, where p is a prime not dividing the discriminant $\Delta(a, b)$, the number of $\mathbb{F}_p$ points is given by

$$\#E_p = p + 1 - a_E(p).$$

Hasse's theorem:

$$\frac{a_E(p)}{\sqrt{p}} \in [-2, 2].$$

$\sim$ 1960: M. Sato and J. Tate independently conjectured the distribution of this sequence.

Theorem (Sato-Tate for elliptic curves)

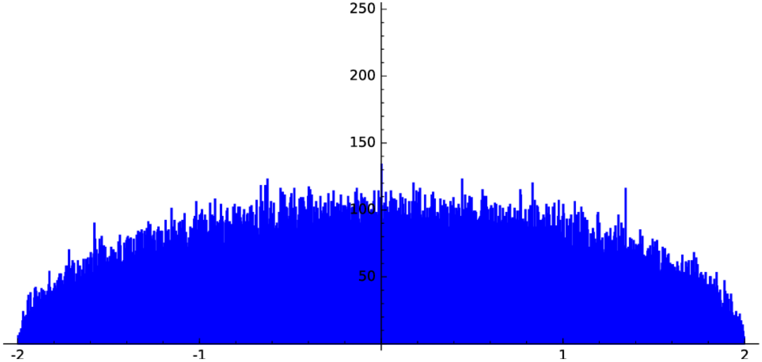
For $I \subseteq [-2, 2]$ *and a non-CM elliptic curve* E*, Let*

$$N_I(E, x) = \#\{p < x : p \text{ prime},\ p \nmid N_E,\ \tilde{a}_E(p) \in I\},$$

where $\tilde{a}_E(p) = \frac{a_E(p)}{\sqrt{p}}$*. Then*

$$\lim_{x \to \infty} \frac{N_I(E, x)}{\pi(x)} = \frac{1}{2\pi} \int_I \sqrt{4 - t^2}\, dt.$$

Proved by L. Clozel, M. Harris, N. Shepherd-Barron and R. Talyor. (2008-2010)



Histogram plot showing the distribution of $a_E(p)/\sqrt{p}$ for the curve $y^2 = x^3 + x + 1$ for $p \leq 10^6$.

It is evident from the graph that there are fewer primes at the ends of the interval, so it is interesting to see if we can say something precise.

Definition

An **extremal prime** for an elliptic curve E is a prime of good reduction satisfying

$$a_E(p) = \pm[2\sqrt{p}].$$

Extremal primes were first studied by Kevin James et al, who conjectured that, as $x \to \infty$,

$$\#\{p \leq x \ : \ a_E(p) = \pm[2\sqrt{p}]\} \sim \begin{cases} \dfrac{8}{3\pi}\dfrac{x^{1/4}}{\log x} & \text{if } E \text{ does not have complex multiplication (CM)}, \\ \dfrac{2}{3\pi}\dfrac{x^{3/4}}{\log x} & \text{if } E \text{ has complex multiplication.} \end{cases}$$

(An elliptic curve has CM if its endomorphism ring is bigger than $\mathbb{Z}$.)

Progress towards conjecture

1. The asymptotic for CM curves was proven by James and Pollack in 2017.
2. For non-CM curves, the asymptotic was shown to hold on average by Giberson in 2017.
3. Upper bound of $x^{1/2}$ under GRH by C. David, A. Gafni, A. Malik, N. Prabhu, and
   C. Turnage-Butterbaugh in 2020.
4. An unconditional upper bound of $\frac{x(\log\log x)^2}{(\log x)^2}$ by Gafni-Thorner-Wong in 2021.
5. (Prabhu, in preparation) An unconditional upper bound of

$$x^{3/4}e^{-c\sqrt{\log x}}.$$

We investigate a related quantity. For ℓ prime, what can we say about

$$\#\{p \leq x : p \nmid N_E, a_E(p) \equiv [2\sqrt{p}] \bmod \ell\}?$$

We prove

Theorem (Malik-Prabhu, preprint)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. Assume that GRH holds for the Dedekind zeta functions of the ℓ-torsion fields $\mathbb{Q}(E[\ell])/\mathbb{Q}$. For $\ell \ll (x^{1/18} \log^{-8/9} x)$, as $x \to \infty$

$$\# \{x < p \leq 2x \ : \ p \nmid N_E, \ a_E(p) \equiv [2\sqrt{p}] \bmod \ell\}$$
$$= \frac{x}{\ell \log x} + O\left(\frac{x}{\ell(\log x)^2} + \ell^{5/4} x^{7/8} (\log x)^{3/2} + \ell^{7/2} x^{3/4} (\log x)^3 \right).$$

Here, $\mathbb{Q}(E[\ell])$ is the field obtained by adjoining the coordinates of all the ℓ-torsion points of E to $\mathbb{Q}$.

Proof outline

$$
\begin{aligned}
&\{p \le x \ : \ a_E(p) \equiv [2\sqrt{p}] \bmod \ell\} \\
&= \sum_{a \bmod \ell} \# \{p \le x \ : \ a_E(p) \equiv a \bmod \ell \text{ and } [2\sqrt{p}] \equiv a \bmod \ell\}
\end{aligned}
$$

where $2\sqrt{p} = [2\sqrt{p}] + \{2\sqrt{p}\}$.

The condition $[2\sqrt{p}] \equiv a \bmod \ell$ translates to $\left\{\frac{2\sqrt{p}}{\ell}\right\} \in \left(\frac{a}{\ell}, \frac{a+1}{\ell}\right)$.

If $[2\sqrt{p}] = k\ell + a$, then

$$
2\sqrt{p} = k\ell + a + \{2\sqrt{p}\} \iff \frac{2\sqrt{p}}{\ell} = k + \frac{a}{\ell} + \frac{\{2\sqrt{p}\}}{\ell}
$$

Unpacking the condition $a_E(p) \equiv a \bmod \ell$ is less straightforward.

Let $E[\ell]$ denote the ℓ-torsion subgroup of $E(\overline{\mathbb{Q}})$. The action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Aut}(E[\ell])$ can be expressed using a Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_\ell}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

- (Serre, '81): The map $\rho_{E,\ell}$ is surjective for all but finitely many primes ℓ.
- The field $\mathbb{Q}(E[\ell])$ is the fixed field in $\overline{\mathbb{Q}}$ of $\mathrm{Ker}\rho_{E,\ell}$.

Recall: If $H \leq G = \mathrm{Gal}(E/F)$ is a normal subgroup, then

$$\mathrm{Gal}(E^H/F) \cong \mathrm{Gal}(E/F)/H.$$

Thus for a large enough prime ℓ, it follows that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$.

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_\ell}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

For each rational prime $p \in \mathbb{Q}$, there is a distinguished automorphism in $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$, called the Frobenius automorphism σ_p. It turns out that the characteristic polynomial of $\rho_{E,\ell}(\sigma_p)$ is given by

$$x^2 - a_E(p)x + p \pmod{\ell}.$$

That is, $a_E(p)$ mod ℓ is the trace of the Frobenius automorphism σ_p. Therefore, for $a \in \mathbb{F}_\ell$, if $C_\ell(a)$ denotes the union of conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of elements of trace a mod ℓ, then

$$a_E(p) \equiv a \bmod \ell \iff \sigma_p \in C_\ell(a).$$

So we have

$$
\begin{aligned}
&\#\{p \le x \ :\ a_E(p) \equiv [2\sqrt{p}] \bmod \ell\} \\
&= \sum_{a \bmod \ell} \#\left\{ p \le x \ :\ \sigma_p \in C_\ell(a) \text{ and } \left\{\frac{2\sqrt{p}}{\ell}\right\} \in \left[\frac{a}{\ell}, \frac{a+1}{\ell}\right] \right\}
\end{aligned}
$$

Recall:

1. $C_\ell(a)$ is the union of conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of trace a.
2. $\{\cdot\}$ denotes the fractional part.

Now,
The quantity

$$\#\{p \le x \ : \ \sigma_p \in C_\ell(a)\}$$

can be computed using the Chebotarev Density Theorem:

Theorem (Lagarias-Odlyzko, 1977)

Let L/K be a finite Galois extension of number fields with Galois group G and C be a conjugacy class in G. If $\zeta_L(s)$ satisfies GRH, then

$$\#\{p \le x : \sigma_p = C\} = \frac{|C|}{|G|}\pi(x) + Error.$$

On the other hand, the quantity $\#\left\{p \le x \ : \ \left\{\frac{2\sqrt{p}}{\ell}\right\} \in \left[\frac{a}{\ell}, \frac{a+1}{\ell}\right]\right\}$ can be computed using the equidistribution of fractional parts of αp^θ:

Theorem (Balog, Harman, etc.)

Fix $\theta, \delta \in (0,1)$. Then

$$\#\{p \le x : \{p^\theta\} < \delta\} = \delta\pi(x) + Error.$$

We require a theorem that combines the above two, i.e., a joint distribution theorem.
Roughly, we prove

$$\#\{x < p \leq 2x : \sigma_p \in C \text{ and } \{\alpha p^\theta\} < \delta\} = \delta \frac{|C|}{|G|}\pi(x) + \text{Error}.$$

More precisely,
Consider a finite Galois extension $L/\mathbb{Q}$, with Galois group G, and $n_L = [L : \mathbb{Q}]$. Let $\alpha > 0$ and $[\delta_1, \delta_2] \subseteq [0, 1]$ be an interval of length δ. Let $\theta \in [0, 1]$ be fixed. Define

$$\pi(x, C, G) := \#\{x < p \leq 2x : \gcd(p, d_L) = 1, \sigma_p \in C\}$$

where C is a union of conjugacy classes in G.

Theorem (Malik-Prabhu, preprint)

Assume that GRH holds for $\zeta_{L/K}(s)$ *and the condition*

$$\alpha^{\frac{1}{4}}\delta^{\frac{-1}{2}}n_L^{\frac{1}{2}}(\log x)^2 \ll x^{\frac{1-\theta}{4}}$$

is satisfied. Then, the following holds.

$$\#\{x < p \leq 2x : \sigma_p \in C \text{ and } \delta_1 < \{\alpha p^\theta\} < \delta_2\} - \delta\pi(x, C, G)$$

$$\ll \frac{|C|}{|G|}n_L(\log x)^3\left(\frac{\delta^{\frac{1}{2}}\alpha^{\frac{1}{4}}}{n_L^{\frac{1}{2}}(\log x)^{\frac{3}{2}}}x^{\frac{3+\theta}{4}} + \frac{\delta}{\alpha^{\frac{1}{2}}}x^{1-\frac{\theta}{2}}\right) + \delta^{\frac{1}{2}}\alpha^{\frac{1}{4}}n_L^{\frac{1}{2}}x^{\frac{1+\theta}{4}}(\log x)^{\frac{3}{2}} + \frac{|C|}{|G|}\frac{\delta x}{(\log x)^2}. \quad (1)$$

uniformly for L/K, δ *and* α. *Here, the implied constant may depend on* θ.

(from previous slide)

$$\#\{x < p \leq 2x : \sigma_p \in C \text{ and } \delta_1 < \{\alpha p^\theta\} < \delta_2\} = \delta\pi(x, C, G) + E_{n_L, \frac{|C|}{|G|}, \alpha, \delta}$$

Applying this to our case:

$$L/K = \mathbb{Q}(E[\ell])/\mathbb{Q}$$

$$G = \mathrm{GL}_2(\mathbb{F}_\ell)$$

$$\frac{|C|}{|G|} = \frac{|C_\ell(a)|}{|G|} = \frac{1}{\ell} + O\left(\frac{1}{\ell^2}\right)$$

$$n_L = (\ell^2 - 1)(\ell^2 - \ell)$$

$$\{\alpha p^\theta\} = \left\{\frac{2}{\ell} p^{1/2}\right\}$$

$$[\delta_1, \delta_2] = [a/\ell, (a+1)/\ell] \text{ so } \delta = 1/\ell$$

Using the above joint distribution theorem with these substitutions, we deduce (under GRH)

$$
\begin{aligned}
&\#\{p \le x \ : \ a_E(p) \equiv [2\sqrt{p}] \bmod \ell\} \\
&= \sum_{a \bmod \ell} \# \left\{ p \le x \ : \ \sigma_p \in C_\ell(a) \text{ and } \left\{ \frac{2\sqrt{p}}{\ell} \right\} \in \left[\frac{a}{\ell}, \frac{a+1}{\ell} \right) \right\} \\
&= \sum_{a \bmod \ell} \frac{1}{\ell} \pi\left(x, C_\ell(a), G_\ell\right) \\
&\quad + O\left(\frac{x}{\ell^2 (\log x)^2} + x^{7/8} \ell^{1/4} (\log x)^{3/2} + x^{3/4} \ell^{5/2} \log^3 x. \right) \\
&= \frac{x}{\ell \log x} \\
&\quad + O\left(\frac{x}{\ell (\log x)^2} + \ell^{5/4} x^{7/8} (\log x)^{3/2} + \ell^{7/2} x^{3/4} (\log x)^3 \right).
\end{aligned}
$$

Remarks on the joint distribution result

Recall that the joint distribution result studied the quantity

$$\#\{x < p \leq 2x : \sigma_p \in C \textit{ and } \delta_1 < \{\alpha p^\theta\} < \delta_2\}.$$

- A *Carmichael number* is a composite number n such that $b^n \equiv b \bmod n$ for all integers b.
  In 2013, Banks-Gulöglu-Yeager showed that there are infinitely many Carmichael numbers n solely composed of primes p satisfying a Chebotarev condition.
- A *Piatetski-Shapiro prime* is a prime number of the form $\lfloor n^c \rfloor$ with $c > 0$ and $n \in \mathbb{N}$.
  In 2015, Gulöglu-Yildirim proved a joint distribution of Piatetski-Shapiro primes satisfying a Chebotarev condition.

Thank you for your attention!