Distribution of Frobenius Traces

02 Feb

Speaker: Arshay Sheth.

Let $E/\mathbb{Q}$ be an elliptic curve with discriminant $\Delta \in \mathbb{Z}$. For each $p \nmid \Delta$, we let $a_p = p+1 - \#E(\mathbb{F}_p)$

Hasse bound: $|a_p| \leq 2\sqrt{p}$.

Let $N \geq 2$, $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[N]$

$\rightsquigarrow \rho_N : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(E[N]) \cong GL_2(\mathbb{Z}/N\mathbb{Z})$

For each prime $p \nmid N\Delta$, $\text{trace}(\rho_N(\text{Frob}_p)) \equiv a_p \mod N$.

① Sato-Tate conjecture

$a_p = 2\sqrt{p}\cos\theta_p$ for a unique $\theta_p \in [0, \pi]$.

Thm:

$$\lim_{X\to\infty} \frac{\#\{p \leq X : p \text{ prime}, \ \theta_p \in (\alpha,\beta)\}}{\#\{p \leq X : p \text{ prime}\}} = \begin{cases} \frac{\beta-\alpha}{\pi} = \frac{1}{\pi}\int_\alpha^\beta d\theta & \text{if } E \text{ has CM} \\ \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \, d\theta & \text{if } E \text{ has no CM} \end{cases}$$

Where does $\sin^2\theta\, d\theta$ come from?

$$SU_2(\mathbb{C}) \twoheadrightarrow \left\{\begin{matrix}\text{conjugacy classes} \\ \text{of } SU(2,\mathbb{C})\end{matrix}\right\} = X \tilde{=} \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} : \theta \in [0,\pi] \right\}$$

Pushforward of Haar measure is $\mu = \frac{2}{\pi}\sin^2\theta\, d\theta$.

Let f be a cts f^n on $[0,\pi]$

$$\mu(f) = \int_0^\pi \frac{2}{\pi}\sin^2\theta\, f(\theta)\, d\theta$$

↑ measure of f.

Proof of thm requires non-vanishing of certain L-functions, which requires showing analytic continuation (done by Taylor, ...)

② Lang-Trotter conjecture

Qn: What values can a_p take?

Let $P \in E(\mathbb{Q})$ has order $N \geq 2$.

$$E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_p) \quad \forall p \text{ primes } p \nmid \Delta.$$

$$P \longmapsto \tilde{P}$$

$\tilde{P}$ has order $N \Rightarrow N \mid \#E(\mathbb{F}_p)$

$a_p = p+1 - \#E(\mathbb{F}_p) \Rightarrow a_p \equiv p+1 \mod N.$

So if $a_p = 1 \Rightarrow N \mid p \Rightarrow N = p$

<u>Conclusion</u>: If $E(\mathbb{Q})_{tors}$ is not trivial, $a_p = 1$ for only finitely many primes p.

More generally, pick $n \in \mathbb{Z}$. When can $a_p = n$?

Suppose $\mathrm{Im}(\rho_N) \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ contains a matrix whose trace is $m \mod N$.

Chebotarev density thm $\Rightarrow \exists$ are infinitely many primes p s.t $a_p \equiv m \mod N$. $\longrightarrow$ ⊛

<u>Def^n</u>: We say that m has no congruence obstruction if ⊛ is satisfied for $\forall N \geq 2$.

<u>Conjecture</u> (Lang Trotter)

Suppose m has no congruence obstruction. Then $\exists$ are infinitely many primes p s.t $a_p = m$.

Moreover:

$$\lim_{x \to \infty} \#\{p \leq X : a_p = m\} \sim C \frac{\sqrt{x}}{\log x}$$ for some constant C.

E.g. $\mathrm{tr}(\rho_N(\text{complex conj})) = 0$.

Thm (Elkies)

$\exists$ are infinitely many primes p s.t. $a_p = 0$.

E.g. $\mathrm{tr}(\rho_N(\mathrm{Id})) = \mathrm{tr}\begin{pmatrix}1&0\\0&1\end{pmatrix} = 2$.

Conj. $\exists$ are infinitely many primes p for which $a_p = 2$.

Not known for any single elliptic curve!

③ BSD conjecture

Original version of BSD: (modern BSD would be $\asymp$?)

$$\mathrm{OBSD}: \prod_{p \le x} \frac{\#E(\mathbb{F}_p)}{p} \sim C(\log x)^r \qquad r = \mathrm{rank}\, E(\mathbb{Q})$$

OBSD $\Rightarrow$ BSD, OBSD $\Rightarrow$ RH (for this elliptic curve)

(BSD is weaker than OBSD, but a lot of numerical and theoretical evidence to support OBSD)

$$\mathrm{OBSD} \Rightarrow \frac{1}{\log X} \sum_{p \le x} \frac{a_p \log p}{p} = -r + \frac{1}{2}$$

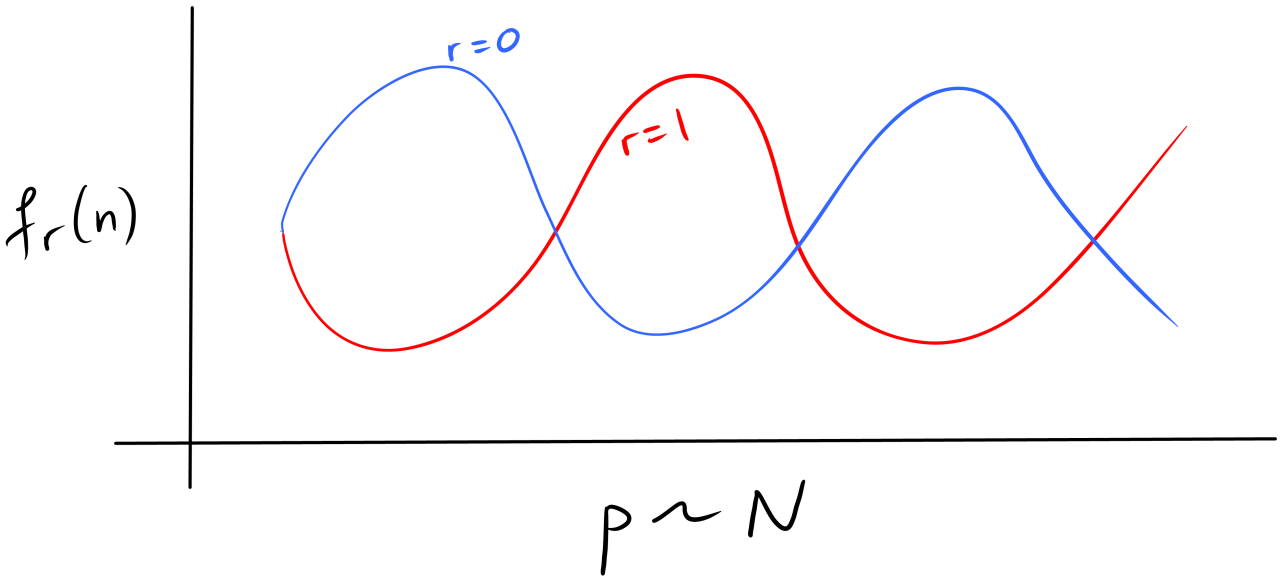
↑ Nagao-Mestre sums

④ Murmurations

Fix some $r \geq 0$ and $N_2 > N_1 \geq 1$.

$$\mathcal{E}_r[N_1, N_2] = \left\{ \begin{array}{l} \text{isogeny classes of elliptic curves} \\ \text{with rank } r \text{ and conductor } \in [N_1, N_2] \end{array} \right\}$$

$$f_r(n) = \frac{1}{\#\mathcal{E}_r[N_1, N_2]} \sum_{E \in \mathcal{E}_r[N_1, N_2]} a_{p_n}(E) \qquad p_n = n^{\text{th}} \text{ prime}.$$



This phenomenon still doesn't have a satisfactory explanation. Peter Sarnak wrote a letter to Andrew Sutherland and Nina Zubrilina giving some wider context.

Sarnak's letter: $\mathcal{F}$ family of L-functions ordered w.r.t. conductor N_π

Def: Let $\Phi : (0, \infty) \longrightarrow \mathbb{R}$ be smooth weight f^n and $f : \mathcal{F} \longrightarrow \mathbb{C}$.

$$A_{\mathcal{F}, \Phi, N}(f) = \sum_{\pi \in \mathcal{F}} \Phi\left(\frac{N_\pi}{N}\right) f(\pi)$$

$$\underset{\pi \in \mathcal{F}}{EXP}_{\Phi, N}(f) = \frac{A_{\Phi, N}(f)}{A_{\Phi, N}(1)}$$

Let $\lambda_\pi(p) = p^{th}$ coefficient of $L(s, \pi)$

$$a_\pi(p) = \lambda_\pi(p)\sqrt{p}$$

Our case: $\underset{\pi \in \mathcal{F}}{EXP}_{\Phi, N}(a_\pi(p))$

Further average over p + explicit formula.

[Formulas which relate coefficients of the L-function to zeroes of the L-function (e.g. Riemann's explicit formula)]

Katz – Sarnak philosophy:

Distribution of zeros of L-functions related to distribution of random matrices.

$$\underset{p\sim N^a}{EXP}\ \underset{\pi\in\mathcal{F}}{EXP_{N,\mathbb{E}}}\left(a_\pi(p)\right) \longrightarrow \begin{cases} \longrightarrow & \text{if } a<1 \\ \longrightarrow & \text{if } a>1 \end{cases}$$

Marmurchian phenomenon is when $a=1$!

(Sami: Double average shouldn't exist for $a=1$?)