

Sato-Tate conjecture in arithmetic progressions for certain families of elliptic curves

(joint work with Kathrin Bringmann and Ben Kane)

Sudhir Pujahari
NISER

36th Automorphic form workshop
Oklahoma State University

May 20-24, 2024

Let E be an elliptic curve over the finite field \mathbb{F}_p and $E(\mathbb{F}_p)$ be the set of points on E with coordinates in \mathbb{F}_p . The group $E(\mathbb{F}_p)$ is obviously a finite group. Indeed, it clearly has no more than $2p + 1$ points.

Theorem (Hasse, 1922)

Let E be an elliptic curve

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$. Then $|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$.

For an elliptic curve E defined over the finite field \mathbb{F}_{p^r} with p^r elements (p prime, $r \in \mathbb{N}$), the *trace of Frobenius* is given by

$$\mathrm{tr}(E) = \mathrm{tr}_{p^r}(E) := p^r + 1 - \#E(\mathbb{F}_{p^r}).$$

Here $E(\mathbb{F}_{p^r})$ is the set of points on the elliptic curve over the finite field \mathbb{F}_{p^r} .

Sato-Tate conjecture



(Mikio Sato)

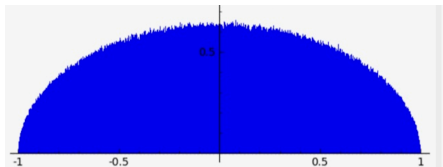


(John Tate)

(Source: wikipedia.org)

Taking $-1 \leq a \leq b \leq 1$ and a fixed elliptic curve E over \mathbb{Q} , it was independently conjectured by Sato and Tate that if E does not have complex multiplication, then

$$\lim_{N \rightarrow \infty} \frac{\#\{p \leq N : 2a\sqrt{p} \leq \text{tr}(E) \leq 2b\sqrt{p}\}}{\#\{p \leq N\}} = \frac{2}{\pi} \int_a^b \sqrt{1-x^2} dx.$$



$$\stackrel{?}{\implies} y = \frac{2}{\pi} \cdot \sqrt{1 - x^2}$$

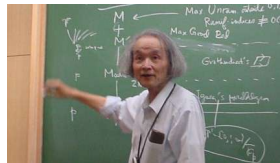
$$(E : y^2 - y = x^3 - x^2 \text{ for } p < 10^9)$$

In a series of papers by Richard Taylor, Michael Harris, Nick Shepherd-Barron, David Geraghty, Laurent Clozel and Tom Barnet-Lamb, this conjecture is now a theorem.

In a series of papers by Richard Taylor, Michael Harris, Nick Shepherd-Barron, David Geraghty, Laurent Clozel and Tom Barnet-Lamb, this conjecture is now a theorem.



(B.J. Birch)



(Y. Ihara)

(Source: wikipedia.org)

Theorem (Birch; 1968)

$\left\{ \frac{\text{tr}_p(E)}{\sqrt{p}} \right\}$ satisfy the Sato-Tate law in $[-2, 2]$ as $p \rightarrow \infty$.

In other words Birch showed that

$$\sum_E \left(\frac{\text{tr}_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \rightarrow \infty,$$

where $C_k := \frac{1}{k+1} \binom{2k}{k}$ is the k -th Catalan number.

In other words Birch showed that

$$\sum_E \left(\frac{\text{tr}_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \rightarrow \infty,$$

where $C_k := \frac{1}{k+1} \binom{2k}{k}$ is the k -th Catalan number.

Extension/Variation of such results are done by
Katz-Sarnak; Yoshida; Deligne; Brock-Granville; Baier-Zhao;
Banks-Shparlinski;

In other words Birch showed that

$$\sum_E \left(\frac{\text{tr}_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \rightarrow \infty,$$

where $C_k := \frac{1}{k+1} \binom{2k}{k}$ is the k -th Catalan number.

Extension/Variation of such results are done by
Katz-Sarnak; Yoshida; Deligne; Brock-Granville; Baier-Zhao;
Banks-Shparlinski;

For $m \in \mathbb{Z}$ and $M \in \mathbb{N}$, we restrict to the set

$$\mathcal{E}_{m,M,p^r} := \{E/\mathbb{F}_{p^r} : \text{tr}(E) \equiv m \pmod{M}\}.$$

Understanding the distribution of the numbers $\text{tr}(E)$ in this arithmetic progression is closely related to investigating the *weighted κ -th moment with respect to $\text{tr}(E)$* (for $\kappa \in \mathbb{N}_0$)

$$S_{\kappa, m, M}(p^r) := \sum_{\substack{E/\mathbb{F}_{p^r} \\ \text{tr}(E) \equiv m \pmod{M}}} \frac{\text{tr}(E)^\kappa}{\# \text{Aut}_{\mathbb{F}_{p^r}}(E)} = \sum_{E \in \mathcal{E}_{m, M, p^r}} \frac{\text{tr}(E)^\kappa}{\# \text{Aut}_{\mathbb{F}_{p^r}}(E)}.$$

Distribution of moments of trace of Frobenius in arithmetic progressions.



(K. Bringmann)



(B. Kane)
(Source: webpage)



(S. Pujahari)

Theorem

Let $m \in \mathbb{Z}$, $M \in \mathbb{N}$ and $\varepsilon > 0$ be given. Let $p > 3$ be a prime for which $p \nmid \gcd(m, M)$ and $k \in \mathbb{N}$. As $r \rightarrow \infty$, we have

$$\frac{S_{2k,m,M}(p^r)}{p^{rk} S_{m,M}(p^r)} = C_k + O_{k,p,M,\varepsilon} \left(p^{(-\frac{1}{2}+\varepsilon)r} \right),$$

where C_k is the k -th Catalan number.

Theorem

Let $m \in \mathbb{Z}$, $M \in \mathbb{N}$ and $\varepsilon > 0$ be given.

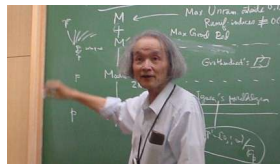
For primes $p \rightarrow \infty$, we have

$$\frac{S_{2k,m,M}(p)}{p^k S_{m,M}(p)} = C_k + O_{k,M,\varepsilon} \left(p^{-\frac{1}{2}+\varepsilon} \right),$$

$$\frac{S_{2k,m,M}(p^r)}{p^{rk} S_{m,M}(p^r)} = C_k + O_{k,M,r,\varepsilon} \left(p^{-1+\varepsilon} \right) \quad (r \geq 2).$$



(B.J. Birch)



(Y. Ihara)

(Source: wikipedia.org)

For $M = 1$, these sums were studied by Birch and implicitly appear in the work of Ihara. They obtained a formula for these sums in terms of the trace of Hecke operators that yields the asymptotic like above.



(Wouter Castryck)



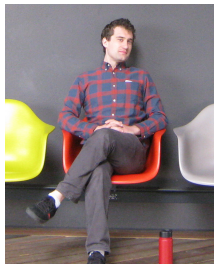
(Hendrik Hubrechts)

(Source: wikipedia.org)

They studied the distribution of $\{tr_q(E) \equiv t \pmod{N}\}$, $N \in \mathbb{N}$ and $t \in \{1, 2, \dots, N-1\}$.



(N. Kaplan)



(I. Petrow)

(Source: webpage)

For $M = 2$, formulas for $S_{2k,m,2}$ were obtained by Kaplan and Petrow.

A special case of above theorem yields a result about elliptic curves with *M-torsion points* ($M \in \mathbb{N}$)

$$E[M] := \{P \in E : \text{ord}(P) \mid M\}.$$

Here $\text{ord}(P)$ means the order of the point under the group law defined on elliptic curves.

A special case of above theorem yields a result about elliptic curves with *M-torsion points* ($M \in \mathbb{N}$)

$$E[M] := \{P \in E : \text{ord}(P) \mid M\}.$$

Here $\text{ord}(P)$ means the order of the point under the group law defined on elliptic curves. We denote the subset of torsion points of precise order M by

$$E^*[M] := \{P \in E : \text{ord}(P) = M\}$$

and define

$$S_{\kappa, M}^*(p^r) := \sum_{\substack{E/\mathbb{F}_{p^r} \\ E^*[M] \neq \emptyset}} \frac{\text{tr}(E)^\kappa}{\# \text{Aut}_{\mathbb{F}_{p^r}}(E)}.$$

Corollary

Let M be a square free integer.

① As $p \rightarrow \infty$, we have

$$\frac{S_{2k,M}^*(p)}{p^k S_M^*(p)} = C_k + O_{k,M,\varepsilon} \left(p^{-\frac{1}{2}+\varepsilon} \right),$$

$$\frac{S_{2k,M}^*(p^r)}{p^{rk} S_M^*(p^r)} = C_k + O_{k,M,r,\varepsilon} \left(p^{-1+\varepsilon} \right) \quad (r \geq 2).$$

Corollary

Let M be a square free integer.

- ① As $p \rightarrow \infty$, we have

$$\frac{S_{2k,M}^*(p)}{p^k S_M^*(p)} = C_k + O_{k,M,\varepsilon} \left(p^{-\frac{1}{2}+\varepsilon} \right),$$
$$\frac{S_{2k,M}^*(p^r)}{p^{rk} S_M^*(p^r)} = C_k + O_{k,M,r,\varepsilon} \left(p^{-1+\varepsilon} \right) \quad (r \geq 2).$$

- ② If $p > 3$ is a prime we have, as $r \rightarrow \infty$

$$\frac{S_{2k,M}^*(p^r)}{p^{rk} S_M^*(p^r)} = C_k + O_{k,p,M,\varepsilon} \left(p^{(-\frac{1}{2}+\varepsilon)r} \right).$$

Now we consider moments of sums of Hurwitz class numbers that are of independent interest. Let $h(d)$ denote the class number.

Let $H(n) := \sum_{\substack{d^2 | n \\ n/d^2 \equiv 0,1 \pmod{4}}} h_w(n/d^2)$ be the n th Hurwitz class number, where

$$h_w(d) := \begin{cases} h(d)/3 & \text{if } d = -3; \\ h(d)/2 & \text{if } d = -4; \\ h(d) & \text{else.} \end{cases}$$

Now we consider moments of sums of Hurwitz class numbers that are of independent interest. Let $h(d)$ denote the class number.

Let $H(n) := \sum_{\substack{d^2 | n \\ n/d^2 \equiv 0,1 \pmod{4}}} h_w(n/d^2)$ be the n th Hurwitz class number, where

$$h_w(d) := \begin{cases} h(d)/3 & \text{if } d = -3; \\ h(d)/2 & \text{if } d = -4; \\ h(d) & \text{else.} \end{cases}$$

Let

$$\mathcal{H}(\tau) := \sum_{n \in \mathbb{Z}} H(n) q^n$$

be the generating function for the Hurwitz class numbers.



(D. Zagier)
(Source: wikipedia.org)

Theorem (Zagier; 1976)

\mathcal{H} is a Mock modular forms of weight $\frac{3}{2}$.



(D. Zagier)
(Source: wikipedia.org)

Theorem (Zagier; 1976)

\mathcal{H} is a Mock modular forms of weight $\frac{3}{2}$.

Sums of moments of these Hurwitz class numbers analogous to $S_{\kappa, m, M}$ are given by

$$H_{\kappa, m, M}(n) := \sum_{\substack{t \in \mathbb{Z} \\ t \equiv m \pmod{M}}} t^{\kappa} H(4n - t^2).$$

Sums of this type have occurred throughout the literature and satisfy many nice identities.



(M. Eichler)
(Source: wikipedia.org)

Theorem (Eichler; 1956)

For $M = 1$, $\kappa = 0$, and $n = p$ prime we have the famous identity

$$H_{0,1}(p) = 2p.$$

Theorem

Let $m, M, k \in \mathbb{N}$ be given. As $n \rightarrow \infty$, we have

$$\frac{H_{2k,m,M}(n)}{n^k H_{m,M}(n)} = C_k + O_{k,M,\varepsilon} \left(n^{-\frac{1}{2} + \varepsilon} \right).$$

Let

$$\mathcal{E}_{p^r,t} := \{E/\mathbb{F}_{p^r} : \text{tr}(E) = t\}$$

and

$$N_A(p^r; t) := \sum_{E \in \mathcal{E}_{p^r,t}} \frac{1}{\#\text{Aut}_{\mathbb{F}_{p^r}}(E)}.$$

Then, for a prime $p > 3$ and $r \in \mathbb{N}$ we have

$$2N_A(p^r; t) = \begin{cases} H(4p^r - t^2) & \text{if } t^2 < 4p^r, \ p \nmid t, \\ H(4p) & \text{if } t = 0 \text{ and } r \text{ is odd,} \\ \frac{1}{2} \left(1 - \left(\frac{-1}{p}\right)\right) & \text{if } t = 0 \text{ and } r \text{ is even,} \\ \frac{1}{3} \left(1 - \left(\frac{-3}{p}\right)\right) & \text{if } t^2 = p^r, \\ \frac{1}{12} (p - 1) & \text{if } t^2 = 4p^r, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

Let $k \in \mathbb{N}$, $m \in \mathbb{Z}$, and $M \in \mathbb{N}$ be given.

(1) For a fixed prime $p > 3$, as $r \rightarrow \infty$ we have

$$S_{2k+1,m,M}(p^r) = O_{k,M,\varepsilon} \left(p^{(k+1+\varepsilon)r} \right).$$

(2) For $r \in \mathbb{N}$ fixed, as $p \rightarrow \infty$ we have

$$S_{2k+1,m,M}(p^r) = O_{k,M,\varepsilon} \left(p^{(k+1+\varepsilon)r} \right).$$

Theorem

Let $k \in \mathbb{N}_0$ be given. Then

$$\frac{H_{2k+1,m,M}(n)}{n^{k+\frac{1}{2}}H_{m,M}(n)} = O_{k,M,\varepsilon}\left(n^{-\frac{1}{2}+\varepsilon}\right), \quad H_{2k+1,m,M}(n) = O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right).$$

Theorem

Let $k \in \mathbb{N}_0$ be given. Then

$$\frac{H_{2k+1,m,M}(n)}{n^{k+\frac{1}{2}}H_{m,M}(n)} = O_{k,M,\varepsilon}\left(n^{-\frac{1}{2}+\varepsilon}\right), \quad H_{2k+1,m,M}(n) = O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right).$$

Theorem

Let $m \in \mathbb{Z}$ and $M \in \mathbb{N}$ be given. The x_E for $E \in \mathcal{E}_{m,M}(p^r)$ are equidistributed with respect to the Sato–Tate measure.

Specifically, we have

$$\lim_{p \rightarrow \infty} \Pr_{\text{Aut}} \left(a \leq \frac{\text{tr}_q(E)}{\sqrt{q}} \leq b : E \in \mathcal{E}_{m,M}(p^r) \right) = \int_a^b \mu(x) dx.$$

Sketch of proof for even moments:

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t, n) H(4n - t^2)$, where

$p_{2k}(t, n)$ denotes the $(2k)$ -th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

Sketch of proof for even moments:

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t, n) H(4n - t^2)$, where

$p_{2k}(t, n)$ denotes the $(2k)$ -th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

- The n -th Fourier coefficient of $[\mathcal{H}, \theta_{m,M}]_k | U_4$ equals $\left(\frac{(2k)!}{2 \cdot k!} G_{k,m,M}(n) \right)$.

Sketch of proof for even moments:

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t, n) H(4n - t^2)$, where

$p_{2k}(t, n)$ denotes the $(2k)$ -th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

- The n -th Fourier coefficient of $[\mathcal{H}, \theta_{m,M}]_k | U_4$ equals $\left(\frac{(2k)!}{2 \cdot k!} G_{k,m,M}(n) \right)$.
- For $m \in \mathbb{Z}$ and $k, M \in \mathbb{N}$, we have
$$H_{2k,m,M}(n) = \frac{k!}{(2k)!} G_{k,m,M}(n) - \sum_{\mu=1}^k (-1)^\mu \frac{(2k-\mu)!}{\mu!(2k-2\mu)!} n^\mu H_{2k-2\mu,m,M}(n).$$

We argue by induction.

- Since $C_0 = 1$, the claim holds trivially for $k = 0$.

We argue by induction.

- Since $C_0 = 1$, the claim holds trivially for $k = 0$.
- For $k \geq 1$,

$$G_{k,m,M}(n) + \frac{1}{2^{2k} \cdot k!} \lambda_{2k+1,m,M}(4n)$$

is the n -th coefficient of a weight $2k + 2$ cusp form, where

$$\lambda_{\ell,m,M}(n) := 2 \sum_{\pm} \sum_{\substack{t > s \geq 0 \\ t^2 - s^2 = n \\ t \equiv \pm m \pmod{M}}} (t - s)^{\ell}.$$



$$\lambda_{\ell,m,M}(n) \leq n^{\frac{\ell}{2}} \lambda_{m,M}(n) \ll_{\varepsilon} n^{\frac{\ell}{2} + \varepsilon}.$$



$$\lambda_{\ell,m,M}(n) \leq n^{\frac{\ell}{2}} \lambda_{m,M}(n) \ll_{\varepsilon} n^{\frac{\ell}{2}+\varepsilon}.$$

- By Deligne's bound it thus may be bound against $O_{k,M,\varepsilon}(n^{k+\frac{1}{2}+\varepsilon})$. The implied constant in the error term a priori depends on m as well, but by taking the maximum over all of the choices of $m \pmod{M}$.

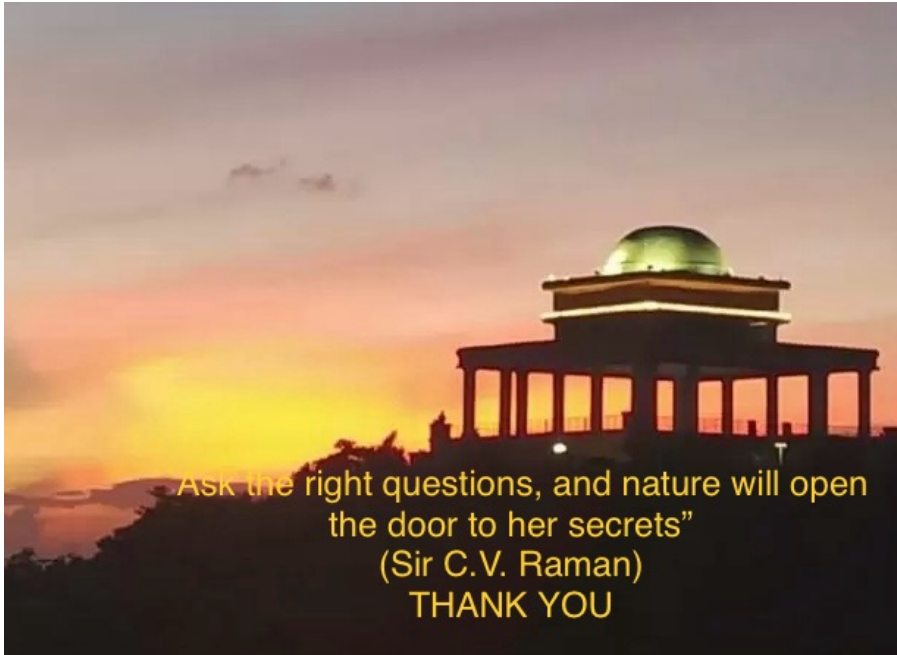


$$\lambda_{\ell,m,M}(n) \leq n^{\frac{\ell}{2}} \lambda_{m,M}(n) \ll_{\varepsilon} n^{\frac{\ell}{2}+\varepsilon}.$$

- By Deligne's bound it thus may be bound against $O_{k,M,\varepsilon}(n^{k+\frac{1}{2}+\varepsilon})$. The implied constant in the error term a priori depends on m as well, but by taking the maximum over all of the choices of $m \pmod{M}$.



$$G_{k,m,M}(n) \ll_{k,M,\varepsilon} n^{k+\frac{1}{2}+\varepsilon}.$$



Ask the right questions, and nature will open
the door to her secrets”
(Sir C.V. Raman)
THANK YOU