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

(joint work with Kathrin Bringmann and Ben Kane)

Sudhir Pujahari
National Institute of Science Education and Research (NISER)

International Seminar on Automorphic Forms

17th May, 2022

PLAN OF TALK

PLAN OF TALK

- Part-I: Introduction to theory of equidistribution.

PLAN OF TALK

- Part-I: Introduction to theory of equidistribution.
- Part-II: Introduction to Sato-Tate conjecture.

PLAN OF TALK

- Part-I: Introduction to theory of equidistribution.
- Part-II: Introduction to Sato-Tate conjecture.
- Part-III: Distribution of moments of trace of Frobenius in arithmetic progressions.

Part-I: Introduction to theory of equidistribution.

The story of equidistribution started with the sequence $\{n\theta\}$, θ irrational.

The story of equidistribution started with the sequence $\{n\theta\}$, θ irrational.

(P.G.L. Dirichlet, 1805 – 1859)
(Source: wikipedia.org)

1842 - Dirichlet showed that there are infinitely many elements of this sequence in any neighborhood of 0.

(Leopold Kronecker, 1823 – 1891)
(Source: wikipedia.org)

1884 - Kronecker showed that this sequence is in fact dense throughout the interval [0, 1].

(P. Bohl)
(1865-1921)

(H. Weyl)
(1885-1955)

(W. Sierpinski)
(1882-1969)

(Source: wikipedia.org)

1909 - Piers Bohl.
1910 - Herman Weyl and Waclaw Sierpinski, investigated the following question:

(P. Bohl)
(1865-1921)

(H. Weyl)
(1885-1955)

(W. Sierpinski)
(1882-1969)

(Source: wikipedia.org)

1909 - Piers Bohl.
1910 - Herman Weyl and Waclaw Sierpinski, investigated the following question:
Question How the sequence $\{n\theta\}$ is distributed in the unit interval, when θ is irrational?

General principles of equidistribution

Let $\{x_n\}$ be a sequence of real numbers in the unit interval $[0, 1]$. For a subset I of $[0, 1]$, and for a fixed natural number N, let

$$A_I(N) := \#\{1 \leq n \leq N;\, x_n \in I\}.$$

General principles of equidistribution

Let $\{x_n\}$ be a sequence of real numbers in the unit interval $[0, 1]$. For a subset I of $[0, 1]$, and for a fixed natural number N, let

$$A_I(N) := \#\{1 \leq n \leq N;\ x_n \in I\}.$$

Definition 1

$\{x_n\}$ is said to be **equidistributed** *in the unit interval if for any $I = [a, b] \subset [0, 1]$, we have*

$$\lim_{N\to\infty} \frac{A_I(N)}{N} = b - a.$$

A sequence $\{x_n\}$ of real numbers is said to be **equidistributed** $\Leftrightarrow$ for every $I \subset [0,1]$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_I(x_n) = \int_0^1 \chi_I(x)dx.$$

A sequence $\{x_n\}$ of real numbers is said to be **equidistributed** $\Leftrightarrow$ for every $I \subset [0,1]$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_I(x_n) = \int_0^1 \chi_I(x)dx.$$

$\Leftrightarrow$ for all (complex valued) Riemann integrable functions $f(x)$ of period 1,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx.$$

A sequence $\{x_n\}$ of real numbers is said to be **equidistributed** $\Leftrightarrow$ for every $I \subset [0,1]$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_I(x_n) = \int_0^1 \chi_I(x)dx.$$

$\Leftrightarrow$ for all (complex valued) Riemann integrable functions $f(x)$ of period 1,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx.$$

$\Rightarrow$ For all non-zero $m \in \mathbb{Z}$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i m x_n} = 0.$$

In the year 1916, Weyl investigated the distribution of the sequence $\{n^2\theta\}$, where θ is irrational and proved the following theorem

In the year 1916, Weyl investigated the distribution of the sequence $\{n^2\theta\}$, where θ is irrational and proved the following theorem

Theorem 2 (Weyl, 1916)

$\{n^2\theta\}$ is equidistributed in the unit interval.

In the year 1916, Weyl investigated the distribution of the sequence $\{n^2\theta\}$, where θ is irrational and proved the following theorem

Theorem 2 (Weyl, 1916)

$\{n^2\theta\}$ is equidistributed in the unit interval.

In that paper he gave a criterion for equidistribution in terms exponential sum.

Weyl's Criterion

Theorem 3

Weyl's criterion: *A sequence* $\{x_n\}$ *is e.d if and only if*

$$c_m := \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(mx_n) = 0$$

for every $m \in \mathbb{Z}$, $m \neq 0$, $e(t) = e^{2\pi it}$.

Weyl's Criterion

Theorem 3

Weyl's criterion: *A sequence* $\{x_n\}$ *is e.d if and only if*

$$c_m := \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(mx_n) = 0$$

for every $m \in \mathbb{Z}$, $m \neq 0$, $e(t) = e^{2\pi it}$.

Application: If $\theta \notin \mathbb{Q}$, then $\{n\theta\}$ e.d in $[0, 1]$.

Weyl's Criterion

Theorem 3

Weyl's criterion: *A sequence* $\{x_n\}$ *is e.d if and only if*

$$c_m := \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(mx_n) = 0$$

for every $m \in \mathbb{Z}$, $m \neq 0$, $e(t) = e^{2\pi it}$.

Application: If $\theta \notin \mathbb{Q}$, then $\{n\theta\}$ e.d in $[0, 1]$. If $m \neq 0$,

$$\frac{1}{N} \left| \sum_{n=1}^{N} e(mn\theta) \right|$$

$$= \frac{1}{N} \left| \frac{\sin(\pi mN\theta)}{\sin(\pi m\theta)} \right|$$

$$\to 0 \text{ as } N \to \infty.$$

Definition 4

Consider finite multi sets A_n with $\#A_n \to \infty$ as $n \to \infty$.
$\{A_n\}$ is **set-equidistributed** *with respect to a probability measure μ if for every $[a, b] \subset [0, 1]$,*

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

Definition 4

Consider finite multi sets A_n with $\#A_n \to \infty$ as $n \to \infty$.
$\{A_n\}$ is **set-equidistributed** *with respect to a probability measure μ if for every $[a, b] \subset [0, 1]$,*

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

In particular, if

$$A_n = \{x_1, x_2, ..., x_n\}$$

then the definition is the definition of an equidistributed sequence with respect to μ.

(I.J Schoenberg, 1903 - 1990) (N. Wiener, 1926 - 1964)
(Source: wikipedia.org)

Theorem 5 (Wiener-Schoenberg)

A_n is equidistributed with respect to some positive continuous measure if and only if the Weyl limits exist for every integer m and

$$\lim_{N\to\infty} \frac{1}{N} \sum_{|m|\leq N} |c_m|^2 = 0.$$

(Van der Corput, 1890 – 1975)
(Source: wikipedia.org)

Theorem 6 (Van der Corput,1931)

If for each positive integer s, the sequence $\{x_{n+s} - x_n\}$ is equidistributed (mod 1), then the sequence $\{x_n\}$ is equidistributed (mod 1).

(Ivan Vinagradov, 1891 – 1983)
(Source: wikipedia.org)

1937 - Ivan Vinogradov; $\{p\theta\}$ is equidistributed.

Part-II: Introduction to Sato-Tate conjecture.

Elliptic Curve

- What is an **elliptic curve**?
  For the time being, we define an elliptic curve to be any equation of the form

$$E : y^2 = x^3 + ax^2 + bx + c$$

  with $a, b, c \in \mathbb{Z}$, and such that the polynomial $x^3 + ax^2 + bx + c$ does not have repeated roots.

Theorem 7 (Siegel, 1928)

Let E be an elliptic curve given by an equation $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Then E has only finitely many points $P = (x, y)$ with integer coordinates $x, y \in \mathbb{Z}$, i.e., $E(\mathbb{Z})$ is a finite set

The group $E(\mathbb{F}_p)$ is obviously a finite group. Indeed, it clearly has no more than $2p+1$ points.

Theorem 8 (Hasse, 1922)

Let E be an elliptic curve

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

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

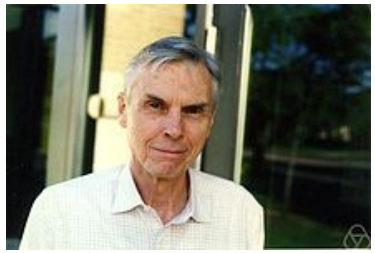
For an elliptic curve E defined over the finite field $\mathbb{F}_{p^r}$ with p^r elements (p prime, $r \in \mathbb{N}$), the *trace of Frobenius* is given by

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

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)

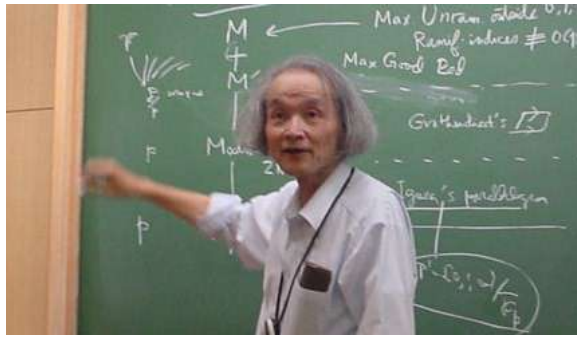
Taking $-1 \leq a \leq b \leq 1$ and a fixed elliptic curve E over $\mathbb{Q}$, it was independently conjectured by Sato and Tate that if E does not have complex multiplication, then

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

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 9 (Birch; 1968)

$\{\frac{tr_p(E)}{\sqrt{p}}\}$ *satisfy the Sato-Tate law in* $[-2, 2]$ *as* $p \to \infty$.

In other words Birch showed that

$$\sum_{E} \left(\frac{tr_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \to \infty,$$

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

In other words Birch showed that

$$\sum_{E} \left(\frac{tr_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \to \infty,$$

where $C_k := \frac{1}{k+1}\binom{2k}{k}$ is the k-th Catalan number.
Extension/Varient of such results are done by
Katz-Sarnak; Yoshida; Deligne; Brock-Granville; Baier-Zhao;
Banks-Shparlinski; .....

In other words Birch showed that

$$\sum_{E} \left(\frac{tr_p(E)}{\sqrt{p}} \right)^{2k} \sim C_k p^k \text{ as } p \to \infty,$$

where $C_k := \frac{1}{k+1}\binom{2k}{k}$ is the k-th Catalan number.
Extension/Varient of such results are done by
Katz-Sarnak; Yoshida; Deligne; Brock-Granville; Baier-Zhao;
Banks-Shparlinski; $\cdots\cdots\cdots$
For $m \in \mathbb{Z}$ and $M \in \mathbb{N}$, we restrict to the set

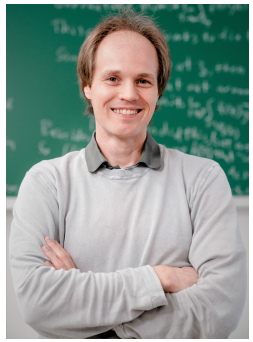
$$\mathcal{E}_{m,M,p^r} := \{E/\mathbb{F}_{p^r} : \text{tr}(E) \equiv m \pmod{M}\}.$$

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

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

Part-III: Distribution of moments of trace of Frobenius in arithmetic progressions.

(K. Bringmann)



(B. Kane)

(Source: webpage)

(S. Pujahari)

Theorem 1

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 $r \to \infty$, we have

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

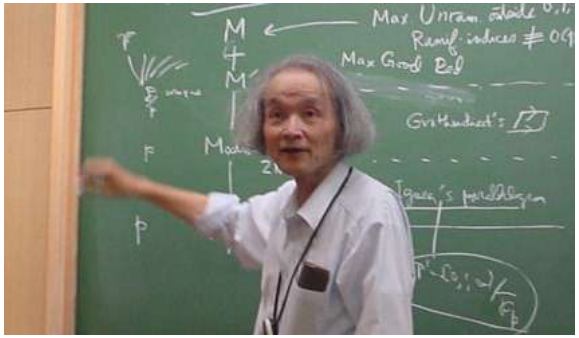
where C_k is the k-th Catlan number.

Theorem 2

Let $m \in \mathbb{Z}$, $M \in \mathbb{N}$ and $\varepsilon > 0$ be given.
For primes $p \to \infty$, we have

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

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



(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 $t \in \{1, 2, \ldots N-1\}$.

(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 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* ($M \in \mathbb{N}$)

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

Here $\mathrm{ord}(P)$ 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

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

and define

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

Corollary 3

Let M be a square free integer.

1. *As $p \to \infty$, 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 3

Let M be a square free integer.

1. *As $p \to \infty$, 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 $r \to \infty$*

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

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

Let $H(n) := \sum_{\substack{d^2 \mid n \\ n/d^2 \equiv 0,1 \pmod 4}} h_w(n/d^2)$ be the nth 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 $H(n) := \sum_{\substack{d^2 \mid n \\ n/d^2 \equiv 0,1 \pmod 4}} h_w(n/d^2)$ be the nth 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 4 (Zagier; 1976)

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

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

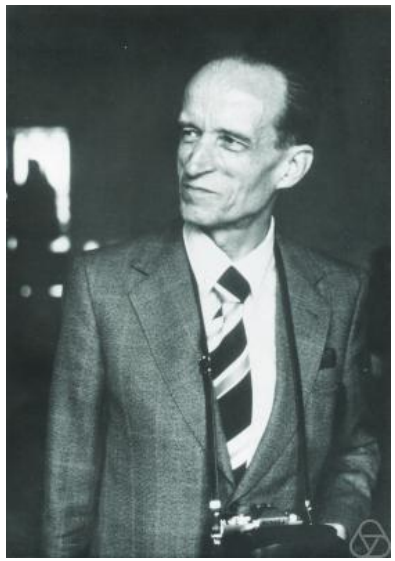
Theorem 4 (Zagier; 1976)

$\mathcal{H}$ 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

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

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



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

Theorem 5 (Eichler; 1956)

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

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

Theorem 6

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

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

and

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

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

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

Sketch of proof

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t,n) H\left(4n - t^2\right)$, where $p_{2k}(t,n)$ denotes the $(2k)$-th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

Sketch of proof

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t,n) H\left(4n - t^2\right)$, where $p_{2k}(t,n)$ denotes the $(2k)$-th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

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

Sketch of proof

Let $G_{k,m,M}(n) := \sum_{t \equiv \pm m \pmod{M}} p_{2k}(t,n) H\left(4n - t^2\right)$, where $p_{2k}(t,n)$ denotes the $(2k)$-th coefficients in the Taylor expansion of $(1 - tX + nX^2)^{-1}$.

- 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

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

continued...

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

continued...

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

- 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 $m \pmod M$.

continued...

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

- 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 $m \pmod M$.

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

Theorem 10

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

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

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

Theorem 11

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 11

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 12

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

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


THANK YOU