

Counterexamples related to the Sato–Tate conjecture

Daniel Miller

25 April 2017

Cornell University

Motivation and background

Discrepancy and Dirichlet series

Main theorem

Idea of the proof

Motivation and background

Sato–Tate Conjecture

E/\mathbf{Q} non-CM elliptic curve, $a_p = \text{tr } \rho_l(\text{fr}_p) \in \mathbf{Z}$, $|a_p| \leq 2\sqrt{p}$.

Satake parameter: $\theta_p = \cos^{-1} \left(\frac{a_p}{2\sqrt{p}} \right)$.

Sato–Tate measure: $\text{ST} = \frac{2}{\pi} \sin^2 \theta \, d\theta$ (Haar measure on $\text{SU}(2)^{\natural}$).

Theorem (Taylor et. al.)

$\{\theta_p\}$ is equidistributed with respect to ST.

Quantify rate of convergence of $\frac{1}{\pi(N)} \sum_{p \leq N} \delta_{\theta_p}$ to ST.

Use discrepancy (Kolmogorov–Smirnov statistic).

Akiyama–Tanigawa Conjecture

$$D_N = \sup_{x \in [0, \pi]} \left| \frac{1}{\pi(N)} \sum_{p \leq N} 1_{[0, x)}(\theta_p) - \int 1_{[0, x)}(\theta) \, dST(\theta) \right|.$$

Conjecture (Akiyama–Tanigawa)

$$D_N \ll N^{-\frac{1}{2} + \epsilon}.$$

There is a variant of this conjecture for CM elliptic curve.

Theorem (Akiyama–Tanigawa)

Akiyama–Tanigawa conjecture \Rightarrow Riemann hypothesis for E .

Theorem (Mazur)

Akiyama–Tanigawa conjecture \Rightarrow Riemann hypothesis for $\text{sym}^k E$

A. Pande: is the Sato–Tate conjecture a Galois-theoretic result?

Theorem (Pande)

Let $\epsilon > 0$. Then there exists an infinitely ramified representation $\rho: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_l)$ such that $\theta_p \in B_\epsilon(\pi/2)$ for a density one set of primes.

Theorem (Khare–Rajan)

Any $\rho: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_l)$ is ramified at a density zero set of primes.

Question (Serre): can you *a priori* control the ratio $\frac{\pi_{\mathrm{ram}(\rho)}(x)}{\pi(x)}$?

Answer (Khare–Larsen–Ramakrishna): no!

Questions

Q1. Can Pande's results be strengthened to yield equidistribution?

Q2. If so, can the measure be specified?

Q3. Can the rate of convergence of empirical measures to the true measure be specified?

Q4. Can the growth of $\pi_{\text{ram}(\rho)}(x)$ be controlled?

Q5. Can anything be said about the L -functions associated with ρ ?

Answer: Yes! to Q1–Q5.

Discrepancy and Dirichlet series

Definition

Let $\{\theta_p\}$ be a sequence in $[0, \pi]$, μ a measure on $[0, \pi]$. The *discrepancy* is

$$D_N(\{\theta_p\}, \mu) = \sup_{x \in [0, \pi]} \left| \frac{1}{\pi(N)} \sum_{p \leq N} 1_{[0, x)}(\theta_p) - \int_0^x d\mu \right|.$$

Fact: $\{\theta_p\}$ are μ -equidistributed if and only if $D_N \rightarrow 0$.

Fact: $\frac{\log N}{N} \ll D_N$. The *van der Corput sequence* achieves this.

Definition

For $k \geq 1$,

$$L(\text{sym}^k \rho, s) = \prod_p \det \left(1 - \text{sym}^k \begin{pmatrix} e^{i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{pmatrix} p^{-s} \right)^{-1}$$

Definition

For $f: [0, \pi] \rightarrow \mathbf{C}$ of bounded variation with $\mu(f) = 0$,

$$L_f(s) = \prod_p (1 - f(\theta_p) p^{-s})^{-1}$$

Example (Ramakrishna): $L_{\text{sgn}}(s) = \prod_p (1 - \text{sgn}(a_p) p^{-s})^{-1}$.

Dirichlet series—basic facts

Theorem

If $\left| \sum_{p \leq N} f(\theta_p) \right| \ll N^{\alpha+\epsilon}$, then $L_f(s)$ admits a nonvanishing analytic continuation to $\Re > \alpha$.

Corollary

If $D_N \ll N^{-\alpha+\epsilon}$, then $L_f(s)$ admits a nonvanishing analytic continuation to $\Re > \alpha$.

Definition

$$U_k(\theta) = \frac{\sin((k+1)\theta)}{\sin \theta} = \text{tr sym}^k \begin{pmatrix} e^{i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{pmatrix}.$$

Theorem

If $\left| \sum_{p \leq N} U_k(\theta_p) \right| \ll N^{\alpha+\epsilon}$, then $L(\text{sym}^k \rho, s)$ admits a nonvanishing analytic continuation to $\Re > \alpha$.

Main theorem

Ingredients

1. Fix a rational prime $l \geq 7$.
2. Fix an odd, absolutely, weight 2 representation $\bar{\rho}: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{F}_l)$. ρ will be a lift of $\bar{\rho}$.
3. Fix a function $h: \mathbf{R}^+ \rightarrow \mathbf{R}_{\geq 1}$ which increases slowly to infinity. We will have $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)$.
4. Fix an absolutely continuous measure μ on $[0, \pi]$, with bounded probability density function. The angles $\{\theta_p\}$ will be μ -equidistributed.
5. Fix $\alpha \in (0, \frac{1}{3})$. The discrepancy D_N will decay like $\pi(N)^{-\alpha}$.

Theorem

Let l , $\bar{\rho}$, h , μ , and α be as above. Then there exists $\rho: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_l)$ such that

1. $\rho \equiv \bar{\rho} \pmod{l}$.
2. $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)$. (Yes to Q4.)
3. For each unramified p , $a_p = \mathrm{tr} \rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.
4. $D_N(\{\theta_p\}, \mu) = \Theta(\pi(x)^{-\alpha})$. (Yes to Q1–Q3.)
5. If $(\theta \mapsto \pi - \theta)_* \mu = \mu$, then for each odd k , $L(\mathrm{sym}^k \rho, s)$ satisfies the Riemann hypothesis. (Yes to Q5.)

Idea of the proof

Prescribing discrepancy decay

Theorem

If $\alpha \in (0, \frac{1}{3})$, there exists a sequence (x_2, x_3, x_5, \dots) in $[-1, 1]$ such that $|D_N - \pi(N)^{-\alpha}| \ll \pi(N)^{-1}$.

(Can have $x_p = \frac{a_p}{2\sqrt{p}}$ for $a_p \in \mathbf{Z}$ satisfying the Hasse bound.)

Fact: Discrepancy is invariant under pushforward by \cos and \cos^{-1} .

Idea: Construct ρ so that $\frac{a_p}{2\sqrt{p}} \approx x_p$.

Fact: If $(x_p^{(1)})$ is a sequence with $|x_p - x_p^{(1)}| \ll p^{-1/2+\epsilon}$, then $D_N^{(1)} = \Theta(\pi(N)^{-\alpha})$.

Lifting Galois representations

Construct ρ as $\varprojlim \rho_n$, where $\rho_n: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}/l^n)$.

For all n , require $\det \rho_n \equiv \kappa \pmod{l^n}$ (l -adic cyclotomic character)

Passage from ρ_n to ρ_{n+1} is governed by $H^i(G_{\mathbf{Q},R}, \mathrm{Ad}^0 \bar{\rho})$, $i = 1, 2$

Theorem (K–L–R). Fix a finite set U of primes. Then there exists a finite set N of primes such that

$$H^1(G_{\mathbf{Q},R \cup N}, \mathrm{Ad}^0 \bar{\rho}) \xrightarrow{\sim} \prod_{p \in R} H^1(G_{\mathbf{Q}_p}, \mathrm{Ad}^0 \bar{\rho}) \times \prod_{p \in U} H^1_{\mathrm{nr}}(G_{\mathbf{Q}_p}, \mathrm{Ad}^0 \bar{\rho})$$

Corollary: Given $\rho_n: G_{\mathbf{Q},R_n} \rightarrow \mathrm{GL}_2(\mathbf{Z}/l^n)$, can choose $\mathrm{tr} \rho_{n+1}(\mathrm{fr}_p)$ for all p in a finite set. (Finitely many more ramified primes.)

Controlling ramified primes

Given $\rho_n: G_{\mathbf{Q}, R_n} \rightarrow \mathrm{GL}_2(\mathbf{Z}/l^n)$ and choices of $\mathrm{tr} \rho_{n+1}(\mathrm{fr}_p) \pmod{l^{n+1}}$, need to add finite set N to R_n .

Each $p \in N$ is chosen from a positive-density set of primes.

So p can be arbitrarily large!

If $\pi_R(x) \leq h(x) \ (\forall x)$, can force this for $\pi_{R \cup N}(x)$.

$\pi_{\mathrm{ram}(\bar{\rho})}(x) \leq h(x)$ may not hold—scale h to make this true!

Fact: constant in $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)$ only depends on $\bar{\rho}$.

Lifting Galois representations—first stage

Lift from \mathbf{Z}/l to \mathbf{Z}/l^2 .

Fix a **large** finite set U_1 of primes.

For $p \in U_1$, can choose $a_p \in \mathbf{Z}$ subject only to $|a_p| \leq 2\sqrt{p}$ and $a_p \equiv \text{tr } \rho_1(\text{fr}_p) \pmod{l}$.

We can ensure $\left| \frac{a_p}{2\sqrt{p}} - x_p \right| \leq \frac{l}{2\sqrt{p}}$.

For $N \leq \max U_1$, $D_N(\{\theta_p\}, \mu) = \Theta(\pi(N)^{-\alpha})$.

Make U_1 so large that for $p > \max U_1$, $l^2 < \log p$.

Lifting Galois representations—inductive step

Lift from \mathbf{Z}/l^n to \mathbf{Z}/l^{n+1} .

If $f \in C([0, \pi])$, $f \circ \cos^{-1}: [-1, 1] \rightarrow \mathbf{C}$ is Lipschitz, and $f(\pi - \theta) = -f(\theta)$, then $L_f(\rho, s)$ has a nonvanishing analytic continuation to $\Re > \frac{1}{2}$ (Riemann hypothesis).

Questions?