Counterexamples related to the Sato–Tate conjecture

Daniel Miller

25 April 2017

Cornell University

Outline

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, l prime, $\rho_l \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$.

Fact: $a_p = \operatorname{tr} \rho_l(\mathrm{fr}_p) = p + 1 - \#E(\mathbf{F}_p)$, $|a_p| \leqslant 2\sqrt{p}$. (Hasse)

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

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

Theorem (Taylor et. al.)

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

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

Use discrepancy (Kolmogorov–Smirnov statistic).

Akiyama–Tanigawa Conjecture

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

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* $\mathrm{sym}^k E$

Related results

Theorem (Bucar–Kedlaya). Assume analytic continuation of Ł$(\mathrm{sym}^k E, s)$, GRH, and functional equation for all $k \geqslant 1$. Then $\mathrm{D}_N \ll N^{-\frac{1}{4}+\epsilon}$.

Theorem (Thorner). Same result (with explicit constants) for a modular form of arbitrary weight .

Theorem (Niederreiter). Let $E_{/F}$, where F is a function field. Then $\mathrm{D}_N \ll N^{-\frac{1}{4}+\epsilon}$.

Theorem (Rosengarten). For $G = \mathrm{ST}(M)$ over a function field, $\mathrm{D}_N \ll N^{-\alpha_G+\epsilon}$, where $\alpha \to 0$ as $\operatorname{rk} G \to \infty$.

Common ingredient. Erdös–Turán–Koksma inequality: from a bound on $\left|\sum_{p\leqslant N} \operatorname{tr}\rho(x_p)\right|$ to a bound on D_N.

Context

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

Theorem (Pande)

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

Theorem (Khare–Rajan)

Any $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ 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 $\pi_{\mathrm{ram}(\rho)}(x)$ be controlled?

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

Answer: Yes! to Q1–Q5.

Discrepancy and Dirichlet series

Discrepancy

Definition

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

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

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

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

Dirichlet series

Definition

For $k \geqslant 1$,

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

Definition

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

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

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

Dirichlet series—basic facts

Theorem

If $\left|\sum_{p\leqslant N} f(\theta_p)\right| \ll N^{\alpha+\epsilon}$, *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

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

Theorem

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

Main theorem

Ingredients

1. Fix a rational prime $l \geqslant 7$.
2. Fix an odd, absolutely, weight 2 representation $\bar{\rho}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$. ρ will be a lift of $\bar{\rho}$.
3. Fix a function $h\colon \mathbf{R}^+ \to \mathbf{R}_{\geqslant 1}$ 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 $\alpha \in \left(0, \frac{1}{3}\right)$. 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 $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ such that

1. $\rho \equiv \bar{\rho} \pmod{l}$.
2. $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)$. (Yes to Q4. $\log x$, $\log^{10^{10}} x$, $A^{-1}(x)$)
3. For each unramified p, $a_p = \operatorname{tr} \rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.
4. $\mathrm{D}_N(\{\theta_p\}, \mu) = \Theta(\pi(x)^{-\alpha})$. (Yes to Q1–Q3.)
5. If $(\theta \mapsto \pi - \theta)_* \mu = \mu$, then for each odd k, $L(\operatorname{sym}^k \rho, s)$ satisfies the Riemann hypothesis. (Yes to Q5.)

Idea of the proof

Prescribing discrepancy decay

Theorem

If $\alpha \in \left(0, \frac{1}{3}\right)$, 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 $\mathrm{D}_N^{(1)} = \Theta(\pi(N)^{-\alpha})$.

Lifting Galois representations

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

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 $\mathrm{H}^i(G_{\mathbf{Q},R}, \mathrm{Ad}^0 \bar{\rho})$, $i = 1, 2$

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

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

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

Controlling ramified primes

Given $\rho_n \colon G_{\mathbf{Q},R_n} \to \mathrm{GL}_2(\mathbf{Z}/l^n)$ and choices of $\operatorname{tr}\rho_{n+1}(\mathrm{fr}_p) \pmod{l^{n+1}}$, 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 $\pi_R(x) \leqslant h(x)\,(\forall x)$, can force this for $\pi_{R\cup N}(x)$.

$\pi_{\mathrm{ram}(\bar\rho)}(x) \leqslant h(x)$ 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 $|a_p| \leqslant 2\sqrt{p}$ and $a_p \equiv \operatorname{tr} \rho_1(\mathrm{fr}_p) \pmod{l}$.

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

For $N \leqslant \max U_1$, $\mathrm{D}_N(\{\theta_p\}, \mu) = \Theta(\pi(N)^{-\alpha})$.

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 $\mathbf{Z}/l^{n+1}$.

Have already chosen a_p for $p \in U_n$. (1–5 hold)

Fix a really huge $U_{n+1} \supset U_n$.

For $p \in U_{n+1} \smallsetminus U_n$, can choose $a_p \in \mathbf{Z}$ subject only to $|a_p| \leqslant 2\sqrt{p}$ and $a_p \equiv \operatorname{tr} \rho_n(\mathrm{fr}_p) \pmod{l^n}$.

We can ensure $\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant \frac{l^n}{2\sqrt{p}}$. ($l^n \ll \log p$).

For $N \leqslant \max U_{n+1}$, $\mathrm{D}_N(\{\theta_p\}, \mu) = \Theta(\pi(N)^{-\alpha})$.

Riemann hypothesis

How can we make $L(\mathrm{sym}^k \rho, s)$, k odd, satisfy the Riemann hypothesis?

$\left|\sum_{p \leqslant N} U_k(\theta_p)\right| \ll N^{\frac{1}{2}+\epsilon}$ implies RH for $L(\mathrm{sym}^k \rho, s)$.

When k is odd, $U_k(\pi - \theta) = -U_k(\theta)$.

Enumerate the primes $p_1 = 2, q_1 = 3, p_2 = 5, q_2 = 7, \ldots$

If $\theta_{q_i} \approx \pi - \theta_{p_i}$, then $U_k(\theta_{q_i}) \approx -U_k(\theta_{p_i})$ (within $p_i^{-1/2}$).

$\left|\sum_{p \leqslant N} U_k(\theta_p)\right| = \left|\sum_{p_i, q_i \leqslant N} \left(U_k(\theta_{p_i}) + U_k(\theta_{q_i})\right)\right| \ll \sum_{n \leqslant N} n^{-1/2}$

$\ll N^{\frac{1}{2}}$.

Consequences

If $f \in C([0,\pi])$, $f \circ \cos^{-1}\colon [-1,1] \to \mathbf{C}$ 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).

For μ any "bump measure," there exits ρ with $\{\theta_p\}$ μ-equidistributed.

Can get equidistribution with respect to μ with non-continuous probability distribution functions.

Questions?