Constructing Galois representations with specified Sato–Tate distributions*

Daniel Miller

24 March 2017

1 Introduction and motivation

Let $E_{/\mathbf{Q}}$ be an elliptic curve, with or without complex multiplication, and fix a rational prime l. The l-adic Tate module yields a continuous representation $\rho_l \colon G_{\mathbf{Q}} = \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_2(\mathbf{Z}_l)$ such that at each prime $p \neq l$ for which E has good reduction, ρ_l is unramified at p and moreover

$$a_p = \operatorname{tr} \rho_l(\mathrm{fr}_p) = p + 1 - \#E(\mathbf{F}_p).$$

It follows that $a_p \in \mathbf{Z}$ satisfies the Hasse bound $|a_p| \leqslant 2\sqrt{p}$. Let $\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right) \in [0, \pi]$ (we think of θ_p as representing the conjugacy class of the matrix $\begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix}$ in $\mathrm{SU}(2)$), and let

$$\begin{aligned} \mathrm{ST}_{\text{non-CM}} &= \frac{2}{\pi} \sin^2 \theta \, \mathrm{d}\theta \\ \mathrm{ST}_{\mathrm{CM}} &= \frac{1}{2}\left(\delta_{\pi/2} + \frac{1}{\pi}\mathrm{d}\theta\right). \end{aligned}$$

Then the Sato–Tate conjecture (now a theorem, of Hecke for CM elliptic curves, and Taylor et. al. for non-CM elliptic curves) states that the $\{\theta_p\}$ are equidistributed with respect to ST_*, where $* \in \{\text{non-CM}, \mathrm{CM}\}$ describes E.

The Sato–Tate measures here arise because of deep modularity results relating L-functions associated to E with Hecke L-functions in the CM case, and automorphic representations in the non-CM case. Aftab Pande's paper *Deformations of Galois representations and the theorems of Sato–Tate and Lang–Trotter* considers the question of whether there might be a purely Galois-theoretic proof of these equidistribution results, and answers no. He proves

*Notes for a talk given in Cornell's Number Theory Seminar.

that for any $\epsilon > 0$, there exist Galois representations $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$, ramified at an infinite (but density zero by results of Khare–Rajan) set of primes, for which $\theta_p \in B_\epsilon(\pi/2)$ at each unramified prime. Pande extensively uses the results and techniques from Khare–Larsen–Ramakrishna's paper *Constructing semisimple p-adic Galois representations with prescribed properties.* It is natural to wonder:

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

Q2 Can the "rate of convergence" of the empirical measures $\{\theta_p\}_{p\leqslant x}$ to the given measure be specified?

Q3 Can the density of the set of ramified primes be controlled?

We will see that all these questions can be answered in the affirmative.

2 Discrepancy

Let $\{\theta_p\}$ be a set of angles in $[0,\pi]$ indexed by a subset U of the rational primes. Given a cutoff x, let $\mu_x = \frac{1}{\pi_U(x)} \sum_{p\leqslant x} \delta_{\theta_p}$ be the discrete empirical measure associated to the set $\{\theta_p\}_{p\leqslant x}$. If μ is some other measure on $[0,\pi]$, the *discrepancy* is

$$\mathrm{D}(\mu_x,\mu) = \sup_{t\in[0,\pi]} |\mu_x[0,t] - \mu[0,t]| = \sup_{t\in[0,\pi]} \left| \frac{\#\{p \leqslant x : \theta_p \leqslant t\}}{\pi_U(x)} - \int_0^t \mathrm{d}\mu \right|.$$

When μ_x is clear, write $D_x = \mathrm{D}(\mu_x,\mu)$. So $D_x = \|\operatorname{cdf}_{\mu_x} - \operatorname{cdf}_\mu\|_\infty$. Weak convergence $\mu_x \to^* \mu$ is equivalent to $D_x \to 0$. Heuristics suggest (and Akiyama–Tanigawa have conjectured) that for $E_{/\mathbf{Q}}$ non-CM, we have

$$\mathrm{D}(\mu_x, \mathrm{ST}_{\text{non-CM}}) \ll x^{-\frac{1}{2}+\epsilon}.$$

Mazur proved that their conjecture implies the Riemann hypothesis for all $L(\operatorname{sym}^k E, s)$. In fact, their conjecture implies that for any $f\colon [0,\pi] \to \mathbf{C}$ of bounded variation having $|f|_\infty \leqslant 1$ and $\int f \,\mathrm{dST}_{\text{non-CM}} = 0$, the Dirichlet series

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

also satisfies the Riemann hypothesis (which we take to mean a non-vanishing analytic continuation of $\log L_f(E,s)$ to $\Re > \frac{1}{2}$). For example, the L-function

$$L_{\text{sgn}}(E,s) = \prod_p \frac{1}{1 - \operatorname{sgn}(a_p)p^{-s}}$$

would satisfy the Riemann hypothesis.

3 Main result

The main theorem involves a number of pieces.

1. Fix a rational prime $l \geqslant 7$.
2. Fix an odd, absolutely irreducible, weight-2 representation $\bar{\rho}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$. Such a representation is modular by results of Khare–Wintenberger, but we don't need their results.
3. Fix a function $h\colon \mathbf{R}^+ \to \mathbf{R}^+$ which decreases rapidly to zero, for example, $h(x) = e^{-x}$ or $h(x) = e^{-e^x}$. This function will control the density of the set of ramified primes.
4. Fix an absolutely measure μ on $[0, \pi]$, of the form $f(\theta)\,\mathrm{d}\theta$, with f bounded.
5. Fix $\alpha \in \left(0, \frac{1}{2}\right)$. This will control the rate of decay of discrepancy.

Then there exists $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$, also of weight 2, such that

1. $\rho \equiv \bar{\rho} \pmod{l}$.
2. $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)\pi(x)$. (Yes! to Q3)
3. For each unramified prime p, $a_p = \operatorname{tr}\rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.
4. $\mathrm{D}(\mu_x, \mu) \sim \pi(x)^{-\alpha}$. (Yes! to Q1 and Q2)
5. If $(\theta \mapsto \pi - \theta)_*\mu = \mu$, then for each odd k, $L(\operatorname{sym}^k \rho, s)$ satisfies the Riemann Hypothesis.

4 Some techniques in the proof

First, some key facts about discrepancy. Given $\alpha \in \left(0, \frac{1}{2}\right)$ and any $\mu = f(t)\,\mathrm{d}t$ for f bounded, there is a sequence of $\{\theta_p\}$ such that $|\,\mathrm{D}(\mu_x, \mu) - \pi(x)^{-\alpha}| \ll x^{-1+\epsilon}$; in particular, $D_x \sim \pi(x)^{-\alpha}$. We can even arrange that the θ_p come from integral a_p (which also satisfy the Hasse bound), though this weakens the bound to $|D_x - \pi(x)^{-\alpha}| \ll x^{-\frac{1}{2}+\epsilon}$. Moreover, if $\{a_p^{(1)}\}$ is any collection of integers satisfying the Hasse bound, and $|a_p^{(1)} - a_p|$ is asymptotically bounded by a multiple of $p^{-1/2}$, then $\mathrm{D}(\mu_x^{(1)}, \mu) \sim \mathrm{D}(\mu_x, \mu)$.

The representation ρ is build as a limit $\rho = \varprojlim \rho_n$, where $\rho_n\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/l^n)$ is chosen so as to ensure the statement of the theorem. We have $\rho_1 = \bar{\rho}$, and further ρ_n are constructed inductively. Enumerate the unramified primes as $\{p_{u_1}, p_{u_2}, \dots\}$. Then the goal is to force each $a_{p_{u_n}} \sim$

$2\sqrt{p_{u_n}}\cos(\widetilde{\theta}_{p_{u_n}})$, where $\{\widetilde{\theta}_p\}$ is a sequence with desired rate of decay of discrepancy. At any given stage, we'll have along with ρ_n, a large finite set U of unramified primes, and choices of a_p for each $p \in U$ such that $a_p \equiv \operatorname{tr}\rho(\mathrm{fr}_p) \pmod{l^n}$. The set of ramified primes R will be very thin. Choose a new $U' \supset U$, large enough that we can enforce the statements of the theorem. Then there exist choices of a_p for $p \in U' \smallsetminus U$ such that the statements about discrepancy continue to hold. The results of Khare–Larsen–Ramakrishna show that there is $R' \supset R$, sufficiently thin, along with a lift $\rho_{n+1}\colon G_{\mathbf{Q},R'} \to \mathrm{GL}_2(\mathbf{Z}/l^{n+1})$, such that $a_p \equiv \operatorname{tr}\rho_p(\mathrm{fr}_p) \pmod{l^{n+1}}$ for all $p \in U'$.

We've seen (very roughly) how to enforce the desired μ and discrepancy, but how can we get the Riemann Hypothesis for $L(\operatorname{sym}^k \rho, s)$, k odd? Let $U_k(\theta) = \frac{\sin((k+1)\theta)}{\sin\theta}$; this is the trace of the k-th symmetric power of $\mathrm{SU}(2) \hookrightarrow \mathrm{GL}_2(\mathbf{C})$ in "theta-space." The Riemann Hypothesis for $L(\operatorname{sym}^k \rho, s)$ follows from bounds of the form

$$\left|\sum_{p\leqslant x} U_k(\theta_p)\right| \ll x^{\frac{1}{2}+\epsilon}.$$

Since $U_k(\pi-\theta) = -U_k(\theta)$ when k is odd, we force $\theta_q \approx \pi - \theta_p$ fr $p < q$ successive unramified primes. We can get $|\theta_q - (\pi - \theta_p)| \ll p^{-1/2}$; since $U_k(\cos^{-1} t)$ is a polynomial in t this gives the desired bound.

In fact, if $\left(\cos^{-1}\right)^* f \in C^2([0,\pi])$ is any function with $|f|_\infty \leqslant 1$ and $f(\pi-\theta) = -f(\theta)$, then an identical argument shows that $L_f(\rho,s)$ satisfies the Riemann hypothesis.