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, and fix a rational prime l. A well-known construction of Tate yields a continuous homomorphism $\rho_l\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ such that at each prime $p \neq l$ for which E is unramified, 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 $\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right) \in [0, \pi]$, and let

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

Then the Sato–Tate conjecture (now a theorem) states that the $\{\theta_p\}$ are equidistributed with respect to ST_*, where $* \in \{\text{non-CM}, \text{CM}\}$ describes E.

The Sato–Tate measures here arise because of deep modularity results. 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. He proves 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) set of primes, for which all $\theta_p \in B_\epsilon(\pi/2)$ 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

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

wonder: can Pande's results be strengthened to yield equidistribution? Can the "rate of convergence" of the θ_p to the given measure be specified? 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 empirical measure capturing the set $\{\theta_p\}_{p\leqslant x}$. If μ is some other measure on $[0,\pi]$, the *discrepancy* is

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

In other words, $D_x = \| \operatorname{cdf}_{\mu_x} - \operatorname{cdf}_\mu \|_\infty$. 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 $\mathrm{D}(\mu_x, \mathrm{ST}_{\text{non-CM}}) \ll x^{-\frac{1}{2}+\epsilon}$. Their conjecture implies the Riemann Hypothesis for all $L(\operatorname{sym}^k E, s)$.

Given $\alpha \in (0, 1/2)$ 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 sufficiently close to $p^{-1/2}$, then $\mathrm{D}(\mu_x^{(1)},\mu) \sim \mathrm{D}(\mu_x,\mu)$.

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 $\bar\rho \colon G_\mathbf{Q} \to \mathrm{GL}_2(\mathbf{F}_l)$.
3. Fix a function $h\colon \mathbf{R}^+ \to \mathbf{R}^+$ which decreases rapidly to zero (for example, $h(x) = e^{-x}$ or $h(x) = e^{-e^x}$).
4. Fix a measure μ on $[0,\pi]$ of the form discussed above.
5. Fix $\alpha \in \left(0, \frac{1}{2}\right)$.

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. $\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)\pi(x)$.

3. For each unramified prime p, $a_p = \operatorname{tr}\rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.

4. $\mathrm{D}(\mu_x, \mu) \sim \pi(x)^{-\alpha}$.

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

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.