

# 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  $\rho_l: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_l)$  such that at each prime  $p \neq l$  for which  $E$  is unramified,  $\rho_l$  is unramified at  $p$  and moreover

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

It follows that  $a_p \in \mathbf{Z}$  satisfies the Hasse bound  $|a_p| \leq 2\sqrt{p}$ . Let  $\theta_p = \cos^{-1} \left( \frac{a_p}{2\sqrt{p}} \right) \in [0, \pi]$ , and let

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

Then the Sato–Tate conjecture (now a theorem) states that the  $\{\theta_p\}$  are equidistributed with respect to  $\mathrm{ST}_*$ , where  $* \in \{\mathrm{non-CM}, \mathrm{CM}\}$  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  $\rho: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_l)$ , 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  $\theta_p$  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  $\mu_x = \frac{1}{\pi_U(x)} \sum_{p \leq x} \delta_{\theta_p}$  be the empirical measure capturing the set  $\{\theta_p\}_{p \leq x}$ . If  $\mu$  is some other measure on  $[0, \pi]$ , the *discrepancy* is

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

In other words,  $D_x = \|\text{cdf}_{\mu_x} - \text{cdf}_{\mu}\|_{\infty}$ . Weak convergence  $\mu_x \rightarrow^* \mu$  is equivalent to  $D_x \rightarrow 0$ . Heuristics suggest (and Akiyama–Tanigawa have conjectured) that for  $E/\mathbf{Q}$  non-CM, we have  $D(\mu_x, \text{ST}_{\text{non-CM}}) \ll x^{-\frac{1}{2}+\epsilon}$ . Their conjecture implies the Riemann Hypothesis for all  $L(\text{sym}^k E, s)$ .

Given  $\alpha \in (0, 1/2)$  and any  $\mu = f(t) dt$  for  $f$  bounded, there is a sequence of  $\{\theta_p\}$  such that  $|D(\mu_x, \mu) - \pi(x)^{-\alpha}| \ll x^{-1+\epsilon}$ ; in particular,  $D_x \sim \pi(x)^{-\alpha}$ . We can even arrange that the  $\theta_p$  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  $\{b_p\}$  is any collection of integers satisfying the Hasse bound, and  $|b_p - a_p|$  is sufficiently close to  $p^{-1/2}$ , then  $D(\nu_x, \mu) \sim D(\mu_x, \mu)$ , where  $\nu_x$  is the empirical measure from the  $\cos^{-1}\left(\frac{b_p}{2\sqrt{p}}\right)$ .

## 3 Main result

The main theorem involves a number of pieces.

1. Fix a rational prime  $l \geq 7$ .
2. Fix an odd, absolutely irreducible, weight-2 representation  $\bar{\rho}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{F}_l)$ .
3. Fix a function  $h: \mathbf{R}^+ \rightarrow \mathbf{R}^+$  which decreases rapidly to zero (for example,  $h(x) = e^{-x}$  or  $h(x) = e^{-e^x}$ ).
4. Fix a measure  $\mu$  on  $[0, \pi]$  of the form discussed above.
5. Fix  $\alpha \in (0, \frac{1}{2})$ .

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

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

## 4 Some techniques in the proof

The representation  $\rho$  is build as a limit  $\rho = \varprojlim \rho_n$ , where  $\rho_n: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Z}/l^n)$  is chosen so as to ensure the statement of the theorem. We have  $\rho_1 = \bar{\rho}$ , and further  $\rho_n$  are constructed inductively.