The statistics of the signed trace of Frobenius for elliptic curves

Daniel Miller

July 13, 2016

1 Introduction

Let $E_{/\mathbf{Q}}$ be an elliptic curve of conductor N, l a rational prime and $\rho = \rho_{E,l}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ the associated Galois representation coming from the Tate module of E. We have the sequence $\{a_p(E)\}_{p\nmid Nl}$, defined by

$$a_p(E) = \operatorname{tr}\rho(\mathrm{fr}_p).$$

It is well-known that $a_p(E) \in \mathbf{Z}$, are independent of l, and satisfy the *Hasse bound*:

$$|a_p(E)| \leqslant 2\sqrt{p}.$$

Moreover, Faltings proved that the sequence $a(E) = \{a_p(E)\}$ determines the isogeny class of E.

We can define a new sequence, $s(E) = \{s_p = s_p(E)\}_{p\nmid N}$, by $s_p = \operatorname{sgn}(a_p)$. Write $s_{\leqslant X}(E)$ for $\{s_p(E)\colon p \leqslant X\}$. It is known that $s(E)$ determines E, but the proof depends on very deep results coming from Michael Harris and his school. Our goal is to show that, with some elementary input from representation theory, the fact that $s(E)$ determines E follows from the fact that $a(E)$ determines E.

2 Motivation from characteristic zero

Let Γ be a finite group, $\rho\colon \Gamma \to \mathrm{GL}(V)$ a finite-dimensional absolutely irreducible real representation. Put $\chi_\rho = \operatorname{tr}\rho$ and $\sigma_\rho = \operatorname{sgn}(\chi_\rho)$. We conjecture that σ_ρ, not just χ_ρ, determines ρ up to isomorphism. For symmetric groups S_n, all irreducible representations are real, and the conjecture has been checked by the author for S_n up to $n = 17$, D_n up to $n = 20$, A_n up to $n = 11$, and $\mathrm{PGL}(2, \mathbf{F}_p)$ up to $p = 31$. Finally, this can be proved directly.

Theorem 2.1. *Let G be a compact group, ρ_1, ρ_2 two finite-dimensional, continuous, irreducbile complex representations with real traces. If* $\operatorname{sgn}(\operatorname{tr}\rho_1) = \operatorname{sgn}(\operatorname{tr}\rho_2)$*, then* $\rho_1 \simeq \rho_2$*.*

Proof. Representations of a compact group are self-dual, so $\hom_{\mathbf{C}}(\rho_1, \rho_2) = \rho_1 \otimes \rho_2$. For there to be an isomorphism between ρ_1 and ρ_2, we need $\mathrm{H}^0(\rho_1 \otimes \rho_2) \neq 0$. That is, we need

$$\langle 1, \operatorname{tr}(\rho_1 \otimes \rho_2)\rangle = \int_G \operatorname{tr}\rho_1(g)\operatorname{tr}\rho_2(g)\,\mathrm{d}g$$

to be nonzero. Since $\operatorname{sgn}(\operatorname{tr}\rho_1) = \operatorname{sgn}(\operatorname{tr}\rho_2)$, the integrand is nonnegative. Moreover, since $\rho_1(1)\rho_2(1) = 1$, continuity gives us an open neighborhood U of 1 on which $\rho_1, \rho_2 \geqslant 1/2$. We conclude that $\langle 1, \operatorname{tr}(\rho_1 \otimes \rho_2)\rangle > 0$, and the result follows. □

3 The main idea

Let $E_{/\mathbf{Q}}$ be an elliptic curve of conductor N. Since $|a_p| \leqslant 2\sqrt{p}$, if $l > 4\sqrt{p}$, then a_p is determined by its reduction modulo l. In fact, it is given by the function $\overline{\operatorname{sgn}}$, defined by

$$\overline{\operatorname{sgn}}(x) = \begin{cases} 0 & x = 0 \\ 1 & x \equiv 1, \ldots, \frac{l-1}{2} \pmod{l} \\ -1 & x \equiv \frac{l+1}{2}, \ldots, l-1 \pmod{l}. \end{cases}$$

If l is not clear from the context, we write $\overline{\operatorname{sgn}}_l$.

Conjecture. Let Γ be a finite group, $\rho_1, \rho_2 \colon \Gamma \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_l)$ two representations. If $\det\rho_1 = \det\rho_2$ and $\overline{\operatorname{sgn}}\operatorname{tr}\rho_1 = \overline{\operatorname{sgn}}\operatorname{tr}\rho_2$, then $\rho_1 \simeq \rho_2$.

Theorem. If the conjecture is true, then E is determined by the first $O(N\log\log N)$ of the $s_p(E)$.

Proof. Let $E_{/\mathbf{Q}}$ be an elliptic curve with conductor N. It is known that the first $O(N\log\log N)$ of the a_p determine E. Choose a prime l larger than $4\sqrt{p}$ for p the largest of the $O(N\log\log N)$ primes. Then we can recover a_p for all $p < \frac{1}{16}l^2$ from $a_p \mod l$. In other words, $\bar\rho = \rho \mod l$ determines E. If E_1 and E_2 both have conductor $\leqslant N$ and their first $O(N\log\log N)$ of the s_p are equal, then $\overline{\operatorname{sgn}}\operatorname{tr}\bar\rho_{E_1,l} = \overline{\operatorname{sgn}}\operatorname{tr}\bar\rho_{E_2,l}$. By the conjecture, $\bar\rho_{E_1,l} \simeq \bar\rho_{E_2,l}$, hence $a_p(E_1) \equiv a_p(E_2) \mod l$ for $p < \frac{1}{16}l^2$. Together with the Hasse bound, this implies $a_p(E_1) = a_p(E_2)$ for those p, hence E_1 and E_2 are isogenous. □

4 Some ideas

Let $\rho\colon G \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_l)$. We'd like to characterize $N = \ker\rho$ in terms of $\sigma = \overline{\mathrm{sgn}}(\mathrm{tr}\,\rho)$.

For starters, N is a normal subgroup of G with $\sigma(n) = 1$ for all $n \in N$. We claim that N is maximal with respect to that property. It comes down to: are there any normal subgroups of $\mathrm{GL}_2(\mathbf{F}_l)$ on which $\sigma = 1$? The only normal subgroups of $\mathrm{GL}_2(\mathbf{F}_l)$ lie inside $\mathbf{F}_l^\times$. Since $\mathbf{F}_l^\times \simeq \mathbf{Z}/(l-1)$, choose a generator a. Any subgroup of $\mathbf{F}_l^\times$ is of the form $\langle a^r\rangle$ for some r.

Theorem 4.1. *Let $l \geqslant 5$ be prime. If $N \subset \mathbf{F}_l^\times$ is a subgroup with $\overline{\mathrm{sgn}}|_N = 1$, then $N = 1$.*

Proof. [Numeric test up to $l \approx 130$.]

Since $\mathbf{F}_l^\times$ is cyclic, write $N = \langle a\rangle$. □

Theorem 4.2. *Let $\rho\colon G \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_l)$ be a representation. Then $\ker\rho$ is the largest normal subgroup of G on which $\sigma = 1$.*

Proof. Let N be such a subgroup; then $N \cdot \ker\rho$ is also such a subgroup, so without loss of generality we may assume $\ker\rho \subset N$. Then $N/\ker\rho$ is a normal subgroup of $\mathrm{GL}_2(\mathbf{F}_l)$ on which $\overline{\mathrm{sgn}}(\mathrm{tr}) = 1$. Clearly $\mathrm{SL}_2(\mathbf{F}_l) \not\subset N/\ker\rho$, so $N/\ker\rho \subset \mathbf{F}_l^\times$. Applying the previous theorem, we see that $N = \ker\rho$. □

Theorem 4.3. *Let G be a finite group, $\rho_1, \rho_2\colon G \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_l)$ representations with $\det\rho_1 = \det\rho_2$ and $\sigma_1 = \sigma_2$. Then $\rho_1 \simeq \rho_2$.*

Proof. By the previous result, $\ker\rho_1 = \ker\rho_2$, so we can assume that ρ_1 and ρ_2 are isomorphisms. But an automorphism of $\mathrm{GL}_2(\mathbf{F}_l)$ is determined (up to inner automorphism) by its determinant. Thus $\rho_1 \simeq \rho_2$.

[Groupprops wiki: automorphisms of $\mathrm{GL}_2(\mathbf{F}_l)$ are generated by inner automorphisms and twists by a power of the determinant.] □

5 Problems

Not quite so simple. We know that $\mathrm{sgn}(x) = \mathrm{sgn}(y)$ only implies $\overline{\mathrm{sgn}}(x \mod l) = \overline{\mathrm{sgn}}(y \mod l)$ if x and y are in the interval $(-l/2, l/2)$.

Suppose E_1 and E_2 have $s(E_1) = s(E_2)$. Then for l sufficiently large, $\bar\rho_i\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$ are surjective, with the same determinant and $\overline{\mathrm{sgn}}(\mathrm{tr}\,\rho_1) = \overline{\mathrm{sgn}}(\mathrm{tr}\,\rho_2)$ on $\{\rho_i(\mathrm{fr}_p)\}_{p<l^2/16}$. Since $\pi(l^2/16) \ll l^2$ and $\#\,\mathrm{GL}_2(\mathbf{F}_l) \sim l^4$, there is no way we know that $\overline{\mathrm{sgn}}(\mathrm{tr}\,\rho_i)$ are equal on all of $\mathrm{GL}_2(\mathbf{F}_l)$.

Suppose $s(E_1) = s(E_2)$.

6 p-adic Sato–Tate

Let E_1, E_2 be non-isogenous elliptic curves. Let $\rho_{E_1\times E_2}\colon G_{\mathbf{Q}} \to H(\hat{\mathbf{Z}})$ be the associated adelic representation. Its image is an open group we call Γ. Let $\mathrm{tr}\times\mathrm{tr}\colon H(\hat{\mathbf{Z}}) \to \hat{\mathbf{Z}}\times\hat{\mathbf{Z}}$ be the trace function and define

$$\mu_{\mathrm{ST}} = (\mathrm{tr}\times\mathrm{tr})_*\mu_{\mathrm{Haar}(\Gamma)}.$$

Then the pairs $(a_p(E_1), a_p(E_2))$ are equidistributed in $\hat{\mathbf{Z}}^2$ with respect to μ_{ST} in the sense that for any locally constant $f \in C(\hat{\mathbf{Z}}^2)$, we have

$$\int_{\hat{\mathbf{Z}}\times\hat{\mathbf{Z}}} f\,\mathrm{d}\mu_{\mathrm{ST}} = \lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\leqslant x} f(a_p(E_1), a_p(E_2)).$$

Let $s \in C([-2,2])$. Our question is: does $s(a_p/\sqrt{p})$ determine the elliptic curve? To answer this, look at $A_s = \mathbf{C}[s(x), s(y)] \subset C([-2,2]^2)$. This is a commutative ring, and $\mu_{\mathrm{ST}} \in \hom_{\mathbf{C}}(A_s, \mathbf{C})$.

$$\int s(x)s(y) = \int s(x)\int s(y)$$

Conjecture: $\mu_{\mathrm{ST}(E_1\times E_2)} = \mu_{\mathrm{ST}(E_1)} \times \mu_{\mathrm{ST}(E_2)}$. This implies, if $s \in C(\hat{\mathbf{Z}})$ is idempotent, that $\mu_{\mathrm{ST}(E_1\times E_2)} \in \mathrm{Spec}(A_s)$.

Conjecture: on $H(\mathbf{Z}_l)$, the haar measure is

$$\int f = \int f(\gamma,\delta)\frac{\mathrm{d}(\gamma,\delta)}{|\det\gamma|}$$

Then

$$\int R_{g,h}f = \int f(\gamma g, \delta h)\frac{\mathrm{d}(\gamma,\delta)}{|\det\gamma|}$$

7 Ravi's conjecture via Sato–Tate for pairs

Harris proved that if E_1, E_2 are non-CM, absolutely non-isogenous elliptic curves over $\mathbf{Q}$ then the Sato–Tate conjecture holds for $E_1 \times E_2$. Namely, the pairs $(\theta_p(E_1), \theta_p(E_2))$ are equidistributed in $[0,\pi]^2$ with respect to the measure $\frac{4}{\pi^2}\sin^2\theta_1 \sin^2\theta_2 \mathrm{d}\theta_1\mathrm{d}\theta_2$.

Theorem 7.1. *Let $s \in L^2[0,\pi]$ be piecewise continuous and not constant almost everywhere. If $E_{/\mathbf{Q}}$ is a non-CM elliptic curve, then the isogeny class of E is determined by the set $s_\theta(E) = \{s(\theta_p)\}_p$.*

Proof. Suppose by way of contradiction that E_1 and E_2 are non-isogenous and $s_\theta(E_1) = s_\theta(E_2)$. Sato–Tate for pairs of elliptic curves tells us that

$$\begin{aligned}\int_{[0,\pi]^2} |s(x) - s(y)| \, \mathrm{d}\mu_{\mathrm{ST}(E_1 \times E_2)} &= \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p \leqslant x} |s(\theta_p(E_1)) - s(\theta_p(E_2))| \\ &= 0.\end{aligned}$$

But the integrand is not zero almost everywhere, and $\mu_{\mathrm{ST}(E_1\times E_2)} = \mu_{\mathrm{ST}(E_1)} \times \mu_{\mathrm{ST}(E_2)}$ is a positive Borel measure, so the integral is nonzero. This contradiction gives us the proof. □

Now, suppose $s\colon \mathbf{Z}_l \to \mathbf{Z}_l$ is continuous and non-constant. We claim that $s(E) = \{s(a_p(E))\}_p$ determines E up to isogeny. First,

$(*)_l$ For all $(E_1, E_2)_{/\mathbf{Q}}$ non-isogenous and non-CM, the map $\operatorname{tr} \rho_{E_1\times E_2, l}\colon G_{\mathbf{Q}} \to \mathbf{Z}_l \times \mathbf{Z}_l$ is surjective.

Theorem 7.2 (*)**.** *Assume* $(*)_l$*. Then* $s(E)$ *determines the isogeny class of* E*.*

Proof. Again by contradiction. Let

$$\mu_{\mathrm{ST}(l)} = (\operatorname{tr} \times \operatorname{tr})_* \mu_{\mathrm{Haar}(\rho_{E_1\times E_2}(G_{\mathbf{Q}}))},$$

this is a positive Borel measure on $\mathbf{Z}_l^2$. Čebotarev and $(*)_l$ tell us that the $(a_p(E_1), a_p(E_2))$ are equidistributed in $\mathbf{Z}_l^2$ with respect to $\mu_{\mathrm{ST}(l)}$. As above, this yields a contradiction. □

8 Convergence of L-functions

Suppose we have an L-function of the form

$$L(s) = \prod_p \det(1 - \sigma_p p^{-s})^{-1},$$

where the σ_p are matrices. One can show directly that

$$-\frac{L'}{L}(s) = (\log L)'(s) = \sum_{p^\nu} \frac{\log(p) \operatorname{tr}(\sigma_p^\nu)}{(p^\nu)^s},$$

which is again a Dirichlet series with the a_n supported on prime powers.

Now let $E_{/\mathbf{Q}}$ be an elliptic curve, $\eta\colon [0,\pi] \to \mathbf{R}$ piecewise continuous, and put

$$L_\eta(E, s) = \prod_p \frac{1}{1 - \eta(\theta_p) p^{-s}}.$$

Rearrange:

$$\sum_p \log(p) \sum_{\nu \geqslant 1} \left(\frac{\eta(\theta_p)}{p^s} \right)^\nu = \sum_p \log(p) \left(\frac{\eta(\theta_p)}{p^s} \right) \frac{1}{1 - \frac{\eta(\theta_p)}{p^s}}$$
$$= \sum_p \log(p) \frac{\eta(\theta_p)}{p^s - \eta(\theta_p)}$$

Put $s > 0$; then $p^s \to \infty$, while $\eta(\theta_p)$ is bounded. For $p \gg 0$, $|\eta(\theta_p)| < \frac{1}{2} p^s$, so

$$\frac{2}{3p^s} < \frac{1}{p^s - \eta(\theta_p)} < \frac{2}{p^s}.$$

So convergence is equivalent to that of

$$\sum_p \frac{\log(p)\eta(\theta_p)}{p^s} = \sum_p \frac{\log p}{p^s} \eta(\theta_p).$$

The first idea is to apply Dirichlet's test to $a_n = \eta(\theta_p)$, $b_n = \frac{\log p}{p^s}$. Then $b_n \to 0$ from above (for $n \gg 0$) and

$$\sum_{p \leqslant X} \eta(\theta_p) \approx \pi(X) \int_{[0,\pi]} \eta \, \mathrm{d}\mu_{\mathrm{ST}}$$
$$\sum_{p \leqslant X} \frac{\log p}{p^s} \approx \begin{cases} \log X & s = 1 \\ \frac{s}{1-s} X^{1-s} & s < 1 \end{cases}.$$

So Dirichlet's test isn't very helpful.

Instead, we'll try Abel's formula:

$$\sum_{p \leqslant X} a_p \phi(p) = \phi(X) \sum_{p \leqslant X} a_n - \int_1^X \phi'(x) \left(\sum_{p \leqslant x} a_n \right) \mathrm{d}x.$$

where ϕ is any continuously differentiable function. Choose $\phi(x) = \frac{\log x}{x^s}$ and $a_p = \eta(\theta_p)$. Then Abel summation tells us that

$$\sum_{p \leqslant X} \eta(\theta_p) \frac{\log p}{p^s} = \frac{\log X}{X^s} \sum_{p \leqslant X} \eta(\theta_p) - \int_1^X \frac{1 - s \log x}{x^{s+1}} \sum_{p \leqslant x} \eta(\theta_p) \, \mathrm{d}x$$
$$\approx \mu_{\mathrm{ST}}(\eta) X^{1-s} - \mu_{\mathrm{ST}}(\eta) \int_1^X \frac{1 - s \log x}{x^{s+1}} \frac{x}{\log x} \, \mathrm{d}x$$
$$= \mu_{\mathrm{ST}}(\eta) \left(X^{1-s} - \int_1^X \frac{1 - s \log x}{x^s \log x} \, \mathrm{d}x \right).$$

The term X^{1-s} diverges if $s < 1$, and the integrand can be controlled by removing the "1−" term. So we end up studying the convergence of

$$\int_1^\infty \frac{\mathrm{d}x}{x^s},$$

which isn't helpful either as it only converges if $s > 1$. But if $\mu_{\mathrm{ST}}(\eta) = 0$, everything should vanish.

8.1 Some bounds

Let ϑ be Chebyshev's second function:

$$\vartheta(x) = \sum_{p \leqslant x} \log p.$$

Theorem 8.1. *Assume the RH. Then* $|\vartheta(X) - X| = O(\sqrt{X} \log^2 X)$.

Proof. This is [Sch76, Th. 10] □

Conjecture 8.2 (Akiyama–Tanigawa)**.** *Let* $f\colon [0,\pi] \to \mathbf{R}$ *be of bounded variation. For every* $\epsilon > 0$*, we have*

$$\left| \frac{1}{\pi(X)} \sum_{p \leqslant X} f(\theta_p) - \mu_{\mathrm{ST}}(f) \right| < X^{-\frac{1}{2}+\epsilon}$$

for $C \gg 0$.

This is from [AT99]? They conjecture something slightly different. [Show that their conjecture and this is equivalent.]

[Look at functions of bounded variation: it looks like the sequence definition of $\mu_{\mathrm{ST}}(f)$ works if and only if f is of bounded variation.]

9 Riemann Hypothesis

Let $E_{/\mathbf{Q}}$ be an elliptic curve, and let $\theta_p = \theta_p(E)$ be the normalized frobenius eigenvalues. For $\eta\colon [0,\pi] \to \mathbf{R}$ of bounded variation, [AT99] defines the function

$$D_X^{(\eta)} = \sup_{x \in [0,\pi]} \left| \frac{\#\{p \leqslant X : \theta_p \in [0,x)\}}{\pi(X)} - \eta(x) \right|,$$

and conjecture that $D_X^{(\eta)} = O(X^{-\frac{1}{2}+\epsilon})$ for all $\epsilon > 0$. Strictly speaking, [AT99] only conjecture this for $\frac{2}{\pi}\sin^2\theta$.

We need a generalized Koksma–Hlawka inequality.

For now, we imitate the proof of Theorem 2 in [AT99]. Note that

$$\begin{aligned}\log L_\eta(E,s) &= -\sum_p \log(1-\eta(\theta_p)p^{-s}) \\ &= \sum_p \sum_{n\geqslant 1} \frac{\eta(\theta_p)^n}{np^{ns}} \\ &= \sum_p \left(\frac{\eta(\theta_p)}{p^s} + \sum_{n\geqslant 2} \frac{1}{n} \left(\frac{\eta(\theta_p)}{p^s} \right)^n \right)\end{aligned}$$

Assume that η takes values in $B_1(0) = \{z \in \mathbf{C} : |z| \leqslant 1\}$. If $s \geqslant 1/2$, then $|\eta(\theta_p)/p^s| < 1$, so we can sum geometric series

$$\left| \sum_{n\geqslant 2} \frac{1}{n} \left(\frac{\eta(\theta_p)}{p^s} \right)^n \right| \leqslant p^{-2s} \frac{1}{1-p^{-s}} \leqslant 4p^{-2s}.$$

Now $\sum_p p^{-2s}$ is holomorphic on $\Re s > 1/2$. In other words, we know that $\log L_\eta(E,s)$ is holomorphic on $\Re s > 1/2$ (and hence RH holds for $L_\eta(E,s)$) if and only if $\sum_p \frac{\eta(\theta_p)}{p^s}$ converges on that region. Now we apply Abel summation ($1/2 < \Re s < 1$):

$$\sum_{p\leqslant X} \frac{\eta(\theta_p)}{p^s} = X^{-s} \sum_{p\leqslant X} \eta(\theta_p) - s \int_1^X \frac{1}{x^{s+1}} \sum_{p\leqslant x} \eta(\theta_p)\, \mathrm{d}x$$

For convergence we need $\sum_{p\leqslant X} \eta(\theta_p) = O(X^{\frac{1}{2}+\epsilon})$ for any $\epsilon > 0$. Since $\pi(X) \sim \frac{X}{\log X}$, if $\mu_{\mathrm{ST}}(\eta) = 0$, then RH for $L_\eta(E,s)$ is equivalent to

$$\frac{1}{\pi(X)} \sum_{p\leqslant X} \eta(\theta_p) = O(X^{-\frac{1}{2}+\epsilon}).$$

Put $\mathrm{RH}(E,\eta)$ for the associated Riemann Hypothesis for $L_\eta(E,s)$. Can we prove $\mathrm{RH}(E,\mathrm{ST}) \Rightarrow \mathrm{RH}(E,\eta)$?

10 Akiyama–Tanigawa conjecture

We give the precise statement of Conjecture 1 in [AT99]. Let $E_{/\mathbf{Q}}$ be an elliptic curve. Define the *discrepancy*

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

Akiyama and Tanigawa conjecture that $D(X) = O(X^{-\frac{1}{2}+\epsilon})$. We can rewrite:

$$D(X) = \sup_{x\in[0,\pi]} \left| \frac{1}{\pi(X)} \sum_{p\leqslant X} \chi_{[0,x)}(\theta_p) - \mu_{\mathrm{ST}}(\chi_{[0,x)}) \right|$$

Here's some notation. Put

$$\mu_{\mathrm{ST}}^X = \frac{1}{\pi(X)} \sum_{p\leqslant X} \delta_{\theta_p}.$$

Thus $D(X) = \sup_{x\in[0,\pi]} |\mu_{\mathrm{ST}}^X(\chi_{[0,x)}) - \mu_{\mathrm{ST}}(\chi_{[0,x)})|$. Let f be of bounded variation. Then for $\epsilon > 0$, we can choose a_i, x_i such that $\|f - \sum a_i \chi_{[0,x_0)}\|_\infty < \epsilon$.

****

Let (X, μ) be a probability space, $S \subset X$ a finite set, and $\mathcal{F}$ a collection of functions on X. Then

$$D_{\mathcal{F}}^{\mu}(S) = \sup_{f\in\mathcal{F}} \left| \frac{1}{\#S} \sum_{s\in S} f(s) - \int f \,\mathrm{d}\mu \right|.$$

****

Let $S \subset \mathbf{R}$ be finite, let f be a function on $\mathbf{R}$ of bounded variation. Let $\mu = g(t)\,\mathrm{d}t$ be a probability measure. Write $S = \{s_1, \ldots, s_n\}$.

We have

$$\frac{1}{\#S} \sum_{s\in S} f(s) = \frac{1}{n} \sum_{i=1}^{n} f(s_i)$$

$$=$$

[de Bruijn–Post theorem: f is Riemann integrable iff for all equidistributed sequences, "convergence works for f."]

Theorem 10.1. *Let (X, μ) be a compact space with Radon probability measure. Then for $f \in L^1(X, \mu)$,*

$$\lim_{X\to\infty} \left| \frac{1}{X} \sum_{n\leqslant X} f(x_n) - \int_X f \,\mathrm{d}\mu \right| = 0$$

for all μ-equidistributed $\{x_n\}$ if and only if f is continuous almost everywhere.

Proof. Suppose f is a.e. continuous and $\{x_n\}$ is μ-equidistributed. Then for any $\epsilon > 0$, there is open $U \subset X$ such that f is continuous on U and $\mu(U) < \epsilon$. □

****

Basic idea: let μ, ν be Radon measures on X and $\mathcal{F} \subset C(X)$. THen

$$d_{\mathcal{F}}(\mu, \nu) = \sup_{f \in \mathcal{F}} \frac{1}{\|f\|_0} \left| \int f \, \mathrm{d}\mu - \int f \, \mathrm{d}\nu \right| = \sup_{f \in \mathcal{F}} \frac{1}{\|f\|_0} \left| \int f \, \mathrm{d}(\mu - \nu) \right|.$$

Put $|\mu - \nu| = d(\mu, \nu) = d_{C(X)}(\mu, \nu)$.

...

Better, for X a compact space, put

$$|\mu| = \sup_{f \in C(X)} \frac{1}{\|f\|_0} \int f \, \mathrm{d}\mu = \sup_{\|f\|_0 \leqslant 1} \int f \, \mathrm{d}\mu.$$

Theorem 10.2. *Let $E_{/\mathbf{Q}}$ be an elliptic curve. Then the Akiyama–Tanigawa conjecture for E implies*

$$\left| \frac{1}{\pi(X)} \sum_{p \leqslant X} \eta(\theta_p) - \int \eta \, \mathrm{d}\mu_{\mathrm{ST}} \right| = O_\eta(X^{-\frac{1}{2}+\epsilon})$$

for all $\eta \colon [0, \pi] \to [-1, 1]$ continuous almost everywhere.

Proof. Write $\mu = \mu_{\mathrm{ST}}$ and $\mu^X = \frac{1}{\pi(X)} \sum_{p \leqslant X} \delta_{\theta_p}$. Then we wish to show that

$$\sup_{x \in [0,\pi]} |(\mu^X - \mu)(\chi_{[x,\pi]})| = O(X^{-\frac{1}{2}+\epsilon})$$

implies

$$|(\mu^X - \mu)(\eta)| = O_\eta(X^{-\frac{1}{2}+\epsilon}).$$

Let S be the vector space spanned by the $\chi_{[x,\pi]}$. We start by showing that the A–K conjecture implies that for $s \in S$:

$$|(\mu^X - \mu)(s)| = O_s(X^{-\frac{1}{2}+\epsilon}).$$

This follows from an easy computation. Put $s = \sum \lambda_i \chi_{[x_i,\pi]}$. Then

$$\begin{aligned} |(\mu^X - \mu)(s)| &= \left| \sum \lambda_i (\mu^X - \mu)(\chi_{[x_i,\pi]}) \right| \\ &\leqslant \sum |\lambda_i| (\mu^X - \mu)(\chi_{[x_i,\pi]}) \\ &= \left(\sum |\lambda_i| \right) O(X^{-\frac{1}{2}+\epsilon}) \\ &= O_s(X^{-\frac{1}{2}+\epsilon}). \end{aligned}$$

We've proved things for S (the space of all step functions). □

11 Zeta functions and distributions

Let G be a LCA group. If $\chi\colon G \to \mathbf{C}^\times$ is a character, we have the associated representation of C^*-algebras: $\chi\colon L^1(G) \to \mathbf{C}$,

$$\chi(f) = \int_G \chi(x) f(x)\,\mathrm{d}x.$$

Thus we can think of $\chi \in S'(G)$, the space of distributions on G. As a distribution, χ transforms in the following way:

$$\begin{aligned}(g \cdot \chi)f &= \chi(g^{-1} \cdot \phi) \\ &= \chi(x \mapsto f(gx)) \\ &= \int_G \chi(x) f(gx)\,\mathrm{d}x \\ &= \chi(g)^{-1}\chi(f).\end{aligned}$$

In other words, $\chi \in \mathcal{S}'(G)[\chi^{-1}]$. These are the so-called "zeta distributions" from Tate's Thesis.

Lemma 11.1. $\mathcal{S}'(G)[\chi^{-1}] = \mathbf{C} \cdot \chi$.

Proof. We use a tempered distribution $D \in \mathcal{S}'(G)[\chi^{-1}]$ to construct a measure μ on G that transforms by χ. □

[More generally, claim that the $(\mathfrak{g}, K)$-module underlying $S'(G)$ is isomorphic to $\bigoplus \chi$.]

Now let F be a local field. Let $\mathcal{S}(F)$ be the space of Schwartz functions on F, $\chi\colon F^\times \to \mathbf{C}^\times$ a character. Recall that for $\Phi \in \mathcal{S}(F)$, the *zeta function* is

$$\chi(\Phi) = Z(\Phi, \chi) = \int_{F^\times} \chi(x)\Phi(x)\,\mathrm{d}^\times x.$$

Let $\mathcal{S}'(F)$ be the space of continuous linear functionals on $\mathcal{S}(F)$.

Theorem 11.2. $\mathcal{S}'(F)[\chi^{-1}] = \mathbf{C} \cdot Z(-, \chi)$.

Let $\psi\colon F \to \mathbf{C}^\times$ be a non-trivial additive character. It gives an isomorphism $F = \widehat{F}$ and thus an automorphism $\Phi \mapsto \hat{\Phi}$.

$$\hat{\Phi}(x) = \int_F \Phi(y)\psi(xy)\,\mathrm{d}y.$$

Moreover,

$$\begin{aligned}Z(\hat{\Phi}, |\cdot|\chi^{-1}) &= \epsilon_0(\chi, \psi) Z(\Phi, \chi) \\ L(\chi) &= \frac{1}{1 - \chi(p)} \\ L(\chi, s) &= L(\chi|\cdot|^s).\end{aligned}$$

References

[AT99] Shigeki Akiyama and Yoshio Tanigawa. "Calculation of values of L-functions associated to elliptic curves". In: *Math. Comp.* 68.227 (1999), pp. 1201–1231.

[Sch76] Lowell Schoenfeld. "Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$. II". In: *Mathematics of Computation* 30.134 (1976), pp. 337–360.