Equidistribution and the analytic properties of a strange class of L-functions

Daniel Miller

August 17, 2016

1 Motivation

Let $E_{/\mathbf{Q}}$ be an elliptic curve without complex multiplication. By an old theorem of Faltings [Fal83], the quantities

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

determine E up to isogeny. That is, if E_1 and E_2 satisfy $a_p(E_1) = a_p(E_2)$ for all E, then E_1 and E_2 are isogenous. The starting point of this investigation is the corollary of a theorem of Harris, that the collection $\{\operatorname{sgn} a_p(E)\}_p$ in fact determines E up to isogeny. Ramakrishna had the insight that this fact means the "strange L-function"

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

determines E up to isogeny. In this note, I define a more general class of strange L-functions, and show that their analytic properties are closely tied to the equidistribution of the $a_p(E)$.

Here is a brief discussion of this generalization in the case of a non-CM curve $E_{/\mathbf{Q}}$. It is convenient to repackage the traces of Frobenius as follows:

$$\theta_p(E) = \cos^{-1}(a_p(E)/2\sqrt{p}).$$

The Hasse Bound guarantees that the $\theta_p(E)$ are well-defined angles laying in the interval $[0, \pi]$. Write $\mathrm{dST} = \frac{2}{\pi} \sin^2 \theta \, \mathrm{d}\theta$. Then the Sato–Tate conjecture (now a theorem [BL+11]) tells us that for any continuous function $f \colon [0, \pi] \to \mathbf{C}$, we have

$$\left| \frac{1}{\pi(C)} \sum_{p \leqslant C} f(\theta_p) - \int_0^\pi f \, \mathrm{dST} \right| = o(1)$$

as $C \to \infty$. It is well-known that this follows from the analytic continuation (past $\Re s = 1$) and non-vanishing except at $s = 1$ of all the L-functions

$L(\operatorname{sym}^k E, s)$ [Ser68, A.1, Th.1]. We take as our starting point the much stronger conjecture, due to Akiyama–Tanigawa [AT99], that

$$\left| \frac{1}{\pi(C)} \sum_{p \leqslant C} f(\theta_p) - \int_0^\pi f \, \mathrm{d}\mu_{\mathrm{ST}} \right| = O_f(C^{-\frac{1}{2}+\epsilon})$$

for all continuous f. (Their conjecture is actually more general; we will discuss the precise statement later.) They prove that this conjecture implies the Riemann Hypothesis for E. I prove that not only does their conjecture imply the Riemann Hypothesis for all $L(\operatorname{sym}^k E, s)$, it also does for all the strange L-functions

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

These results make perfect sense in a much more general context, and I will prove them there. In section 2 I set up this context and carefully define strange L-functions. In section 3, I prove basic analytic properties of the strange L-functions and connect their analytic properties with the equidistribution of a sequence. In section 4, I apply these results where "everything is known," i.e. varieties over function fields. Finally, in section 5, I apply the general results to the following cases: a non-CM elliptic curve $E_{/\mathbf{Q}}$, the product $E_1 \times E_2$ of a pair of non-isogenous non-CM elliptic curves over $\mathbf{Q}$, and the Jacobian of a generic genus-2 curve $C_{/\mathbf{Q}}$.

2 Definitions

Let $\mathbf{D} = \{z \in \mathbf{C} : |z| \leqslant 1\}$. Write $\mathbf{D}^\infty$ for the set of sequences in $\mathbf{D}$ indexed by the primes, i.e. $\boldsymbol{z} \in \mathbf{D}^\infty$ is $(z_2, z_3, \dots)$. The space $\mathbf{D}^\infty$ is compact, and comes naturally equipped with the (product) Lebesgue measure, normalized to have mass 1.

Definition 2.1. Let $\boldsymbol{z} \in \mathbf{D}^\infty$. The associated *strange L-function* is given by

$$L(\boldsymbol{z}, s) = \prod_p \frac{1}{1 - z_p p^{-s}},$$

wherever this product converges.

Elementary topology tells us that $L\colon \mathbf{D}^\infty \times \mathbf{C}^{\Re > 1} \to \mathbf{C}$ is continuous. We will see that for fixed $\boldsymbol{z} \in \mathbf{D}^\infty$, the analytic properties of $L(\boldsymbol{z}, s)$ are closely tied to estimates for the sums $A_{\boldsymbol{z}}(x) = \sum_{p \leqslant x} z_p$. One often gets such estimates in the context of equidistribution, which we consider next.

For the remainder of this section, let X be a compact separable metric space with no isolated points. We write X^∞ for the space of sequences in X indexed by rational primes, i.e. points $\boldsymbol{x} \in X^\infty$ are of the form $\boldsymbol{x} = (x_2, x_3, \dots)$. By [Eng89, Cor.2.3.16, Th.4.2.2], the compact space X^∞ is metrizable and separable, also with no isolated points.

Definition 2.2. For $\boldsymbol{x} \in X^\infty$ and $C > 0$, write $\boldsymbol{x}^C$ for the probability measure given by

$$\int_X f \, \mathrm{d}\boldsymbol{x}^C = \boldsymbol{x}^C(f) = \frac{1}{\pi(C)} \sum_{p \leqslant C} f(x_p).$$

Let μ be a Borel measure on X. Recall that $\boldsymbol{x}$ is *μ-equidistributed* if $\boldsymbol{x}^C \to \mu$ weakly, i.e. $\boldsymbol{x}^C(f) \to \mu(f)$ for all $f \in C(X)$. In fact, we can extend this to not-necessarily-continuous functions as follows:

Theorem 2.3 (Mazzone)**.** *Let μ be a Borel measure on X and let $f \colon X \to \mathbf{C}$ be bounded and measurable. Then f is continuous almost everywhere if and only if $\boldsymbol{x}^C(f) \to \mu(f)$ for all μ-equidistributed $\boldsymbol{x}$.*

Proof. This follows directly from the proof of [Maz95, Th.1]. □

Fix a Borel measure μ on X, and write $C^{\mathrm{ae}}(X, \mu)$ for the space of bounded, almost-everywhere continuous functions $f \colon X \to \mathbf{C}$.

Theorem 2.4. *Endowed with the supremum norm $\|f\|_\infty = \sup_{x \in X} |f(x)|$, $C^{\mathrm{ae}}(X, \mu)$ is a Banach space.*

Proof. This is an elementary corollary of the fact that a countable union of measure-zero sets has measure zero. □

Definition 2.5. Let $f \in C^{\mathrm{ae}}(X, \mu)^{\|\cdot\|_\infty \leqslant 1}$, $\boldsymbol{x} \in X^\infty$. The associated *strange L-function* is defined as

$$L_f(\boldsymbol{x}, s) = L(f(\boldsymbol{x}), s) = \prod_p \frac{1}{1 - f(x_p) p^{-s}}$$

for all $s \in \mathbf{C}$ for which the product converges.

Our typical source of a strange L-function is as follows. Let G be a compact connected Lie group and $X = G^\natural$, the space of conjugacy classes of G. Then $G^\natural$ inherits the Haar measure from G. Given any sequence $\boldsymbol{x} \in (G^\natural)^\infty = G^{\natural,\infty}$ and function $f \in C^{\mathrm{ae}}(G^\natural)^{\|\cdot\|_\infty \leqslant 1}$, we can define $L_f(\boldsymbol{x}, s)$. This is related to Serre's L-functions from [Ser68, A.2] as follows.

Theorem 2.6. *Let G be a compact connected Lie group, $\rho \in \widehat{G}$ an irreducible unitary representation of G. Then there exist functions $\lambda_\rho^1, \ldots, \lambda_\rho^{\deg \rho} \colon G^\natural \to S^1$, continuous away from the set $\{\det(1 - \rho) = 0\}$, such that for every $x \in G^\natural$, there are angles $\theta_1, \ldots, \theta_{\deg \rho} \in [0, 2\pi)$, satisfying $\theta_1 \leqslant \cdots \leqslant \theta_{\deg \rho}$, such that $\lambda_\rho^j(x) = e^{i\theta_j}$ and moreover*

$$\det(1 - \rho(x) t) = \prod_{j=0}^{\deg \rho} (1 - \lambda_\rho^j(x) t).$$

Proof. This follows easily from [KS99, Lem.1.0.9]. □

Recall that for $\rho \in \widehat{G}$, Serre defines $L(\rho, s) = \prod_p \det(1 - \rho(x_p) p^{-s})^{-1}$. Using his notation, there is the identity

$$L(\rho, s) = \prod_{j=1}^{\deg \rho} L_{\lambda_\rho^j}(\boldsymbol{x}, s).$$

The rest of our definitions concern discrepancy, which for now we define only in a special context. Let G be a compact connected semisimple Lie group. We will define discrepancy for sequences in $G^\natural$.

Let G^{sc} be the simply-connected cover of G. Choose a maximal torus $T \subset G^{\mathrm{sc}}$; let $W = \mathrm{N}(T)/T$ be the Weyl group. Let $\mathfrak{t} = \mathrm{Lie}(T)$ and recall that the kernel of $\exp\colon \mathfrak{t} \twoheadrightarrow T$ is generated by the nodal vectors associated to the root system $\mathrm{R}(G^{\mathrm{sc}}, T)$ [$\mathrm{Lie}_{7\text{–}9}$, 9.6 Pr.11]. Write $\{t_1, \ldots, t_r\} \subset \mathfrak{t}$ for these vectors. The exponential map $\exp\colon \mathfrak{t} \to T$ induces an isomorphism $\mathfrak{t}/(\langle t_i \rangle \rtimes W) \to G^\natural$. Given $x = (x_1, \ldots, x_r) \in [0,1]^r$, write

$$I_x = \left\{ \sum_{i=1}^r a_i t_i : a_i \in [0, x_i] \right\} \subset \mathfrak{t}.$$

Definition 2.7. With the setup as above, let μ, ν be probability measures on $G^\natural$. The *discrepancy* between μ and ν is

$$\mathrm{disc}(\mu, \nu) = \sup_{x \in [0,1]^r} \left| \mu(\exp I_x) - \nu(\exp I_x) \right|.$$

If $\nu = \mathrm{d}x$, the Haar measure on $G^\natural$, we simply write $\mathrm{disc}(\mu)$ for $\mathrm{disc}(\mu, \mathrm{d}x)$.

The Koksma–Hlawka inequality bounds the difference between the Haar integral and weighted average of a function on $G^\natural$ in terms of the discrepancy of the sequence and the variation of the function.

The following result is essential:

Theorem 2.8 (Koksma, Hlawka)**.** *Let G be as above. Let $f\colon G^\natural \to \mathbf{C}$ be such that $f\,\mathrm{d}x$ is a measure with bounded variation. Then*

$$\left| \boldsymbol{x}^C(f) - \int f\,\mathrm{d}x \right| \leqslant \mathrm{Var}(f)\,\mathrm{disc}(\boldsymbol{x}^C).$$

Proof. This is [Ökt99, Th. 3.2]. □

We will often use the soft version of this inequality. Namely, assume $\int f\,\mathrm{d}x = 0$. Then $|\boldsymbol{x}^C(f)| \ll_f \mathrm{disc}(\boldsymbol{x}^C)$ as $C \to \infty$. Here is another way of putting it. The sequence $f(\boldsymbol{x})$ has $|A_{f(\boldsymbol{x})}(C)| \ll_f \pi(C)\,\mathrm{disc}(\boldsymbol{x}^C)$.

3 Main results

Theorem 3.1. *Let $\boldsymbol{z} \in \mathbf{D}^\infty$. Then $L(\boldsymbol{z}, s)$ defines a holomorphic function on the region $\{\Re s > 1\}$. Moreover, on that region,*

$$\log L(\boldsymbol{z}, s) = \sum_{p^n} \frac{z_p^n}{n p^{ns}}.$$

Proof. Expanding the product for $L(\boldsymbol{z}, s)$ formally, we have

$$L(\boldsymbol{z}, s) = \sum_{n \geqslant 1} \frac{\prod_{p|n} z_p^{v_p(n)}}{n^s}.$$

An easy comparison with Riemann's zeta function tells us that the series expansion is holomorphic on $\{\Re s > 1\}$. By [Apo76, Th. 11.7], the product formula holds on the same region. The formula for $\log L(\boldsymbol{z}, s)$ comes from [Apo76, 11.9 Ex.2]. $\square$

Theorem 3.2. *Assume $A_{\boldsymbol{z}}(x) \ll x^{\alpha+\epsilon}$, $\alpha \in [\frac{1}{2}, 1]$. Then $\log L(\boldsymbol{z}, s)$ is holomorphic on $\{\Re > \alpha\}$.*

Proof. Split the sum for $\log L$ into two pieces:

$$\log L(\boldsymbol{z}, s) = \sum_p \frac{z_p}{p^s} + \sum_p \sum_{n \geqslant 2} \frac{z_p^n}{n p^{ns}}.$$

For each p, we have

$$\left| \sum_{n \geqslant 2} \frac{z_p^n}{n p^{ns}} \right| \leqslant \sum_{n \geqslant 2} p^{-n \Re s} = p^{-2\Re s} \frac{1}{1 - p^{-\Re s}}.$$

Elementary analysis gives

$$1 \leqslant \frac{1}{1 - p^{-\Re s}} \leqslant 2 + 2\sqrt{2},$$

so the second piece of $\log L(\boldsymbol{z}, s)$ converges absolutely when $\Re(s) > \frac{1}{2}$. By [Ten95, II.1 Th.10], our bound on $A_{\boldsymbol{z}}(x)$ yields the holomorphy of $\sum z_p p^{-s}$ on $\{\Re > \alpha\}$. $\square$

Corollary 3.3. *Let G be a compact connected semisimple Lie group, $\boldsymbol{x} \in G^{\natural,\infty}$ satisfy $\operatorname{disc}(\boldsymbol{x}^C, \mathrm{d}x) \ll C^{-\frac{1}{2}+\epsilon}$. Then for every $f \in C^{\mathrm{ae}}(G^\natural)^{\|\cdot\| \leqslant 1}$, $L_f(\boldsymbol{x}, s)$ has analytic continuation to $\{\Re s > \frac{1}{2}\}$, and satisfies the Riemann Hypothesis, for all f bounded and almost-everywhere continuous with $\mu(f) = 0$.*

Proof. Koksma–Hlawka tells that if $\mu(f) = 0$, then $\boldsymbol{x}^C(f) \ll C^{-\frac{1}{2}+\epsilon}$. Thus the sequence $f(\boldsymbol{x})$ satisfies $A_{f(\boldsymbol{x})}(x) \ll x^{\frac{1}{2}+\epsilon}$, and the result follows from Theorem 3.2. $\square$

4 Strange L-functions over function fields

Let k be a finite field of characteristic p and cardinality q. Let $C_{/k}$ be a nice curve in the sense of Poonen (i.e., C is smooth, projective, and geometrically integral). Write $K = k(C)$ for the function field of C. Fix a non-empty open subset $U \subset C$ and a geometric point $\infty \in U(\bar{k})$. Fix a prime $l \neq p$ and an embedding $\overline{\mathbf{Q}_l} \hookrightarrow \mathbf{C}$.

Definition 4.1. An l-adic sheaf $\mathcal{F}$ on U is *good* if the following conditions hold.

1. $\mathcal{F}$ is pure of weight zero.
2. Let $G = \overline{\rho_{\mathcal{F}}(\pi_1(U_{\overline{k}}, \infty))}^{\mathrm{Zar}}$. Assume $\rho_{\mathcal{F}}(\pi_1(U, \infty)) \subset G(\overline{\mathbf{Q}}_l)$.

For any good sheaf $\mathcal{F}$, let $\mathrm{ST}(\mathcal{F})$ be a maximal compact subgroup of $G(\mathbf{C})$.For each $u \in U$, there is a well-defined conjugacy class $\theta(u) = \rho(\mathrm{fr}_u)^{\mathrm{ss}} \in \mathrm{ST}(\mathcal{F})^\natural$. For any $C > 0$, write

$$\boldsymbol{\theta}_{\mathcal{F}}^C = \frac{1}{\#\{u \in U : q_u \leqslant C\}} \sum_{q_u \leqslant C} \delta_{\theta(u)}.$$

Katz proves an equidistribution estimate for the $\theta(u)$'s.

Theorem 4.2. *Let σ be a non-trivial irreducible representation of $\mathrm{ST}(\mathcal{F})$. Then*

$$|\boldsymbol{\theta}_{\mathcal{F}}^C(\operatorname{tr}\sigma)| \ll_{\mathcal{F}} \dim(\sigma) C^{-\frac{1}{2}}.$$

Proof. This is [Kat88, p.39]. □

Now let $C^\natural(\mathrm{ST}(\mathcal{F}))$ be the space of functions $f \colon \mathrm{ST}(\mathcal{F})^\natural \to \mathbf{C}$ satisfying:

$$\|f\|^\natural = \sum_\sigma \dim(\sigma) |\widehat{f}(\sigma)| < \infty.$$

For such functions, we have:

$$|\boldsymbol{\theta}_{\mathcal{F}}^C(f) - \mu(f)| \ll_{\mathcal{F}} \|f\|^\natural C^{-\frac{1}{2}}.$$

Thus for any $f \in C^\natural(\mathrm{ST}(\mathcal{F}))$, the strange L-function $L_f(\boldsymbol{\theta}_{\mathcal{F}}, s)$ has analytic continuation to $\{\Re s > \frac{1}{2}\}$ and satisfies the Riemann Hypothesis.

Theorem 4.3. *Let $\boldsymbol{z} \in \mathbf{D}^\infty$, and assume $\log L(\boldsymbol{z}, s)$ has analytic continuation to $\{\Re > \alpha\}$, $\alpha \in [\frac{1}{2}, 1]$, and that for $\sigma > \alpha$, we have $|\log L(\boldsymbol{z}, \sigma + it)| \ll |t|^{1-\epsilon}$. Then $|A_{\boldsymbol{z}}(x)| \ll x^{\alpha+\epsilon}$.*

Proof. Recall that we can write

$$\log L(\boldsymbol{z}, p) = \sum_p \frac{z_p}{p^s} + \sum_p \sum_{n \geqslant 2} \frac{z_p^n}{np^{ns}} = \sum_p \frac{z_p}{p^s} + O(\zeta(2\Re s)).$$

Thus, for any $\epsilon > 0$, our bound on $|\log L(\boldsymbol{z}, \sigma + it)|$ implies the same bound for $\sum \frac{z_p}{p^s}$ on $\{\Re > \alpha + \epsilon\}$.

Let $\gamma_T = \gamma_{1,T} + \gamma_{2,T} - \gamma_{3,T} - \gamma_{4,T}$ be the following contour:

$$\begin{aligned}
\gamma_{1,T}(t) &= (\alpha + \epsilon) + it \qquad t \in [-T, T] \\
\gamma_{2,T}(t) &= t + iT \qquad t \in [\alpha + \epsilon, 1 + \epsilon] \\
\gamma_{3,T}(t) &= (1 + \epsilon) + it \qquad t \in [-T, T] \\
\gamma_{4,T}(t) &= t - iT \qquad t \in [\alpha + \epsilon, 1 + \epsilon].
\end{aligned}$$

By [Apo76, Th.11.18],

$$\lim_{T\to\infty}\frac{1}{2\pi i}\int_{-\gamma_{3,T}}\sum_p \frac{z_p}{p^s}x^z\,\frac{\mathrm{d}z}{z} =^* \sum_{p\leqslant x} z_p.$$

Let $h(z)$ be the analytic continuation of $\sum z_p p^{-s}$ to $\{\Re > \alpha\}$. Since $\int_\gamma h(z)\frac{\mathrm{d}z}{z} = 0$, we obtain

$$\left|\sum_{p\leqslant z} z_p\right| \ll \left|\int_{\gamma_{T,1}} h(z)x^z\frac{\mathrm{d}z}{z}\right| + \left|\int_{\gamma_{T,2}} h(z)x^z\frac{\mathrm{d}z}{z}\right| + \left|\int_{\gamma_{T,4}} h(z)x^z\frac{\mathrm{d}z}{z}\right|.$$

We know that $|h(\sigma+it)| \ll |t|$, so we can bound:

$$\left|\int_{\gamma_{T,2}} h(z)\frac{\mathrm{d}z}{z}\right| = \left|\int_{\alpha+\epsilon}^{1+\epsilon}\frac{h(t+iT)x^{t+iT}}{t+iT}\,\mathrm{d}t\right| \ll (1+\alpha)x^{1+\alpha}T^{-1},$$

and similarly for $\int_{\gamma_{4,T}}$. Finally, we note that

$$\left|\int_{\gamma_{T,1}} h(z)x^z\frac{\mathrm{d}z}{z}\right| \ll \int_{-T}^{T}|t|^{1-\epsilon}\frac{x^{\alpha+\epsilon}}{(\alpha+\epsilon)^2+t^2}\,\mathrm{d}t \ll x^{\alpha+\epsilon}.$$

Letting $T\to\infty$ we obtain the desired result. □

5 Applications

Recall, following [Bug08] that the *irrationality exponent* $\mu(\alpha)$ a real irrational number α is the supremum of all real numbers μ such that

$$\left|\alpha - \frac{p}{q}\right| < q^{-\mu}$$

for infinitely many $p/q \in \mathbf{Q}$. Bugeaud proves that for any $\mu \geqslant 2$, there is an element ξ_μ of the Cantor set with $\mu(\xi_\mu) = \mu$. Moreover, by [KN74, ?], for every $\epsilon > 0$, the sequence $x_n = n\alpha \mod 1$ has discrepancy $\operatorname{disc}(\boldsymbol{x}^C) = \Omega(C^{-\frac{1}{\mu(\alpha)-1}-\epsilon})$.

Theorem 5.1. *Let $X = S^1$ with the natural Haar measure. For every $\eta \in (0,\frac{1}{2})$, there is a sequence $\boldsymbol{x} = (x_2, x_3, \dots) \in (S^1)^\infty$ such that for all $f \in C^\infty(S^1)^{\|\cdot\|_\infty \leqslant 1}$, the function $\log L_f(\boldsymbol{x}, s)$ has analytic continuation to $\{\Re > \frac{1}{2}\}$, but for all $\epsilon > 0$, $|\operatorname{disc}(\boldsymbol{x}^C)| = \Omega(C^{-\eta-\epsilon})$.*

Proof. Let $\mu > 3$, and let $\boldsymbol{x} = \{x_2, x_3, \dots\}$ be the sequence $x_{p_n} = e^{2\pi i n\xi_\mu}$. To prove that $\log L_f(\boldsymbol{x}, s)$ has analytic continuation to $\{\Re > \frac{1}{2}\}$, we need only to prove that $|A_{\exp(2\pi i m\boldsymbol{x})}(t)| \ll t^{1/2}$, uniformly for each $m \in \mathbf{Z}$. This follows easily from:

$$\left|\sum_{n=1}^{N} e^{2\pi i m n\alpha}\right| \leqslant \frac{|-1+e^{2\pi i M n\alpha}|}{|-1+e^{2\pi i a m}|} \leqslant ? \leqslant \frac{1}{2}m(\eta-1) \ll_\eta m$$

$\square$

Theorem 5.2. *Let $E_{/\mathbf{Q}}$ be a non-CM elliptic curve, and put $\boldsymbol{\theta} = \boldsymbol{\theta}(E)$. Assume that* $\operatorname{disc}(\boldsymbol{\theta}^C) \ll C^{-\frac{1}{2}+\epsilon}$. *Then if $f \in C^{\text{ae}}([0,\pi], \text{ST})^{\|\cdot\|_\infty \leqslant 1}$, the strange L-function $L_f(\boldsymbol{\theta}, s)$ has analytic continuation to $\{\Re > \frac{1}{2}\}$ and satisfy the Riemann Hypothesis. In particular, this holds for all $L(\operatorname{sym}^k E, s)$.*

Proof. The first conclusion follows from Corollary 3.3. The second part follows from the fact that any $L(\operatorname{sym}^k E, s)$ can be written as a product of L_f's, namely the $L_{\lambda^j_{\operatorname{sym}^k}}$'s in section 2. $\square$

Theorem 5.3. *Fix $f \in C^{\text{ae}}([0,\pi], \text{ST})^{\|\cdot\|_\infty \leqslant 1}$ that is not almost everywhere constant.*

Let E_1, E_2 be two non-isogenous, non-CM elliptic curves over $\mathbf{Q}$. Assume the Akiyama–Tanigawa conjecture for the product $E_1 \times E_2$. Then for any $f\colon [0,\pi] \to \mathbf{C}$ that is not almost everywhere

6 A collection of counterexamples

In [AT99, ?], Akiyama and Tanigawa claim that for $E_{/\mathbf{Q}}$, the "discrepancy conjecture" $\operatorname{disc}(\boldsymbol{\theta}^C) \ll C^{-\frac{1}{2}+\epsilon}$ is equivalent to the Riemann Hypothesis for $L(E,s)$. In this section, I construct a collection of examples which show that their conjecture is false for any motive with positive-dimensional Sato–Tate group.

Throughout this section, $|\cdot|_\infty$ is the sup-norm, and $|\cdot|$ can be any of the (commensurable) p-norms on a finite-dimensional real vector space.

Definition 6.1. Let $x \in \mathbf{R}^r$ be such that $x_1, \dots, x_r$ are $\mathbf{Q}$-linearly independent. Following [Lau09], we define r-dimensional *irrationality exponents* as the suprema $\omega_0(x)$ and $\omega_{r-1}(x)$ of the sets of w for which there are infinitely many $m = (m_0, \dots, m_r) \in \mathbf{Z}^{r+1}$ for which

$$\max\{|m_0 x_i - m_i|\} \leqslant |m|_\infty^{-w}$$
$$|m_0 + m_1 x_1 + \cdots + m_r x_r| \leqslant |m|_\infty^{-w}$$

respectively.

Given $x \in \mathbf{R}^r$, write $d(x, \mathbf{Z}^r) = \min_{m \in \mathbf{Z}^r} |x - m|$.

Lemma 6.2. *Let $x \in \mathbf{R}^r$ with $|x|_\infty \leqslant 1$ and $\omega_0(x)$ (resp. $\omega_{r-1}(x)$) is finite. Then*

$$\frac{1}{d(nx, \mathbf{Z}^r)} \ll_{\epsilon,x} n^{\omega_0(x)+\epsilon} \qquad \text{as } n \to \infty, \text{ (resp.)}$$
$$\frac{1}{d(\langle m, x\rangle, \mathbf{Z})} \ll_{\epsilon,x} |m|^{\omega_{r-1}(x)+\epsilon} \qquad \text{as } m \to \infty \text{ in } \mathbf{Z}^r\ .$$

Proof. Let $\epsilon > 0$. Then there are only finitely many $n \in \mathbf{N}$ (resp. $m \in \mathbf{Z}^r$) such that the inequalities in Definition 6.1 hold with $\omega_0(x) + \epsilon$ (resp. $\omega_{r-1}(x) + \epsilon$). In other words, there exist $C_0, C_{r-1} > 0$ such that

$$\max\{|m_0 x_i - m_i|\} \geqslant C_0 |m|_\infty^{-\omega_0(x)-\epsilon}$$
$$|m_0 + m_1 x_1 + \cdots + m_r x_r| \geqslant C_{r-1} |m|_\infty^{-\omega_{r-1}(x)-\epsilon}.$$

for all $m \neq 0$. We consider the first inequality, temporarily setting $|\cdot| = |\cdot|_\infty$. Then $d(nx, \mathbf{Z}^r) = \max\{|nx_i - m_i|\}$ for some m_i such that $|m_i - nx_i| < 1$. Thus $|(n, m_1, \ldots, m_r)| \leqslant \max\{|n|, |nx_i|\} \leqslant |n|$. In particular,

$$d(nx, \mathbf{Z}^r) \geqslant C_0 |n|^{-\omega_0(x)-\epsilon},$$

which implies $\frac{1}{d(nx,\mathbf{Z}^r)} \ll |n|^{\omega_0(x)+\epsilon}$, the implied constant depending on both x and ϵ.

For the second inequality, temporarily set $|\cdot| = |\cdot|_1$, and note that $d(m_1 x_1 + \cdots + m_r x_r, \mathbf{Z}) = |m_0 + m_1 x_1 + \cdots + m_r x_r|$ for $|m_0| \leqslant |(m_1, \ldots, m_r)| \cdot |x| + 1$. Thus $|(m_0, \ldots, m_r)|_\infty \leqslant 2|x||(m_1, \ldots, m_r)|$, giving us

$$d(m_1 x_1 + \cdots m_r x_r, \mathbf{Z}) \geqslant C'_{r-1} |(m_1, \ldots, m_r)|^{-\omega_{r-1}(x)-\epsilon},$$

which implies $\frac{1}{d(\langle m,x\rangle,\mathbf{Z})} \ll |m|^{\omega_{r-1}(x)+\epsilon}$, the implied constant again depending on both x and ϵ. ∎

Let $\mathbf{T}^r = (\mathbf{R}/\mathbf{Z})^r$, with Haar measure normalized to have total mass one. Given $x \in \mathbf{T}^r$, we define $\omega_0(x)$ and $\omega_{r-1}(x)$ as in Definition 6.1, choosing any coset representative of x. This definition is independent of the choice. Recall that for $f \in L^1(\mathbf{T}^r)$, the *Fourier coefficients* of f are, for $m \in \mathbf{Z}^r$

$$\widehat{f}(m) = \int_{\mathbf{T}^r} e^{2\pi i \langle m,x\rangle} \, \mathrm{d}x,$$

where $\langle m, x\rangle = m_1 x_1 + \cdots + m_r x_r$ is the usual inner product.

Theorem 6.3 (Jarník)**.** *Let $w \geqslant 1/r$. Then there exists $x \in \mathbf{R}^r$ such that $\omega_0(x) = w$ and $\omega_{r-1}(x) = rw + r - 1$.*

Theorem 6.4. *Fix $x \in \mathbf{T}^r$ with $\omega_{r-1}(x)$ finite. Then*

$$\left| \sum_{n \leqslant N} e^{2\pi i \langle m, nx\rangle} \right| \ll_{\epsilon,x} |m|^{\omega_{r-1}(x)+\epsilon}$$

as m ranges over $\mathbf{Z}^r \smallsetminus 0$.

Proof. First, note the easy bound:

$$\left| \sum_{n \leqslant N} e^{2\pi i n \langle m,x\rangle} \right| = \left| \frac{e^{2\pi i N \langle m,x\rangle} - 1}{e^{2\pi i \langle m,x\rangle} - 1} \right| \leqslant \frac{2}{|e^{2\pi i \langle m,x\rangle} - 1|}.$$

Since $|e^{2\pi i \langle m,x\rangle} - 1| = \sqrt{2 - 2\cos(2\pi\langle m,x\rangle)}$ and $\cos(2\theta) = 1 - 2\sin^2(\theta)$, we obtain $\left|\sum_{n\leqslant N} e^{2\pi i n\langle m,x\rangle}\right| \leqslant \frac{1}{|\sin(\pi\langle m,x\rangle)|}$. It is easy to check that $|\sin(\pi t)| \geqslant d(t,\mathbf{Z})$, hence $\left|\sum_{n\leqslant N} e^{2\pi i n\langle m,x\rangle}\right| \leqslant \frac{1}{d(\langle m,x\rangle,\mathbf{Z})}$. The final estimate comes from Lemma 6.2. □

Theorem 6.5. *Assume $\omega_{r-1}(x) < \infty$. Let $f \in L^1(\mathbf{T}^r)$ with $\widehat{f}(0) = 0$ and suppose the Fourier coefficients of f satisfy the bound $|\widehat{f}(m)| \ll |m|^{-\frac{1}{r-1}-\omega_{r-1}-\epsilon}$. Then*

$$\left|\sum_{n\leqslant N} f(nx)\right| \ll_{f,x} 1.$$

Proof. Write f as a Fourier series:

$$f(x) = \sum_{m\in\mathbf{Z}^r} \widehat{f}(m) e^{2\pi i(m\cdot x)}.$$

Since $\int f = 0$, we have $\widehat{f}(0) = 0$. Thus we can compute

$$\begin{aligned}
\left|\sum_{n\leqslant N} f(nx)\right| &= \left|\sum_{n\leqslant N}\sum_{m\in\mathbf{Z}^r\smallsetminus 0} \widehat{f}(m) e^{2\pi i n(m\cdot x)}\right| \\
&\leqslant \sum_{m\in\mathbf{Z}^r\smallsetminus 0} |\widehat{f}(m)| \left|\sum_{n\leqslant N} e^{2\pi i n(m\cdot x)}\right| \\
&\ll_{x,\epsilon} \sum_{m\in\mathbf{Z}^r\smallsetminus 0} |m|^{-\frac{1}{r-1}-\omega_{r-1}(x)-\epsilon} |m|^{\omega_{r-1}(x)+\epsilon/2} \\
&\ll_{x,\epsilon} \sum_{m\in\mathbf{Z}^r\smallsetminus 0} |m|^{-\frac{1}{r-1}-\epsilon/2}.
\end{aligned}$$

The sum converges since the exponent is less than $-\frac{1}{r-1}$, and it doesn't depend on N, whence the result. □

Corollary 6.6. *Assume $\omega_{r-1}(x) < \infty$, and let $f \in C^\infty(\mathbf{T}^r)$ with $\widehat{f}(0) = 0$. Then $\left|\sum_{n\leqslant N} f(nx)\right| \ll_{f,x} 1$.*

Proof. This follows from Theorem 6.5 and the fact that the Fourier coefficients of a smooth function decay faster than $|m|^k$, for any $k \in (-\infty, -1]$. □

Theorem 6.7. *If $\omega_0(x) < \infty$, then the sequence $\boldsymbol{x} = (nx)_{n\geqslant 1}$ in $\mathbf{T}^r$ has discrepancy*

$$\operatorname{disc}(\boldsymbol{x}^N) = \Omega\left(2^{-r\left(2+\frac{1}{\omega_0(x)}\right)-\epsilon} N^{-\frac{r}{\omega_0(x)}-\epsilon}\right).$$

Proof. We follow the proof of [KN74, Ch.2, Th.3.3]. First, given $\epsilon > 0$, there exists $\delta > 0$ such that $\frac{r}{\omega_0(x)-\delta} = \frac{r}{\omega_0(x)} + \epsilon$.

By the definition of $\omega_0(x)$, there exist infinitely many $(q, m_1, \ldots, m_r)$ with $q > 0$ such that

$$|qx - m|_\infty \leqslant (\max\{q, |m|_\infty|\})^{-\omega_0(x)+\delta/2}.$$

Since $\max\{q, |m|_\infty\} \geqslant q$, we derive the stronger statement that for infinitely many $q \to \infty$, there exists $m = (m_1, \ldots, m_r) \in \mathbf{Z}^r$ such that $|qx - m|_\infty \leqslant q^{-\omega_0(x)+\delta/2}$, or, equivalently, $|x - \frac{m}{q}| \leqslant q^{-1-\omega_0(x)+\delta/2}$. Pick such a q, and let $N = \lfloor q^{\omega_0(x)-\delta} \rfloor$. Then for $n \leqslant N$, we have $|nx - \frac{n}{q}m| \leqslant q^{-1-\delta/2}$. Thus, for $n \leqslant N$, each nx is within $q^{-1-\delta/2}$ of the grid $\frac{1}{q}\mathbf{Z}^r \subset \mathbf{T}^r$. Thus, they miss a box with side lengths $q^{-1} - 2q^{-1-\delta/2}$. For q sufficiently large, $q^{-1} - 2q^{-1-\delta/2} \geqslant 1/2q$, so the (non-star) discrepancy of $\boldsymbol{x}^N$ is bounded below by $2^{-r}q^{-r}$. Since $q^{\omega_0(x)-\delta} \leqslant 2N$, the (non-star) discrepancy at N is bounded below by

$$2^{-r}\left((2N)^{\frac{1}{\omega_0(x)+\delta}}\right)^{-r} = 2^{-r-\frac{r}{\omega_0(x)+\delta}} N^{-\frac{r}{\omega_0(x)+\delta}} = 2^{-r\left(1+\frac{1}{\omega_0(x)}\right)-\epsilon} N^{-\frac{r}{\omega_0(x)}-\epsilon}.$$

Since r-dimensional star-discrepancy is bounded below by 2^{-r} times non-star discrepancy, we obtain the final result. □

The key point in the above theorem is that

$$\operatorname{disc}(\boldsymbol{x}^N) = \Omega_{x,r,\epsilon}\left(N^{-\frac{r}{\omega_0(x)}-\epsilon}\right).$$

Theorem 6.8. *Let $\eta \in (0,1)$. Then there exists $x \in \mathbf{T}^r$ such that for all $f \in C^\infty(\mathbf{T}^r)$ with $\widehat{f}(0) = 0$, the estimate*

$$\left|\sum_{n\leqslant N} f(nx)\right| \ll_{f,x} 1$$

holds, but for which

$$\operatorname{disc}(\boldsymbol{x}^N) = \Omega_{\epsilon,r,x}\left(N^{-\eta-\epsilon}\right).$$

Proof. Let $w = \frac{r}{\eta} \geqslant \frac{1}{r}$. By Theorem 6.3, there exists $x \in \mathbf{T}^r$ with $\omega_0(x) = w$ and $\omega_{r-1}(x) = rw + r - 1$. The result follows easily from Corollary 6.6 and Theorem 6.7. □

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.

[Apo76] Tom M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[BL+11] Tom Barnet-Lamb et al. "A family of Calabi-Yau varieties and potential automorphy II". In: *Publ. Res. Inst. Math. Sci.* 47.1 (2011), pp. 29–98.

[$\text{Lie}_{7\text{–}9}$] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 7–9.* Elements of Mathematics. Translated from the 1975 and 1982 French originals by Andrew Pressley. Berlin: Springer-Verlag, 2005.

[Bug08] Yann Bugeaud. "Diophantine approximation and Cantor sets". In: *Math. Ann.* 341.3 (2008), pp. 677–684.

[Eng89] Ryszard Engelking. *General topology.* Second. Vol. 6. Sigma Series in Pure Mathematics. Translated from the Polish by the author. Heldermann Verlag, Berlin, 1989.

[Fal83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Invent. Math.* 73.3 (1983), pp. 349–366.

[Kat88] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups.* Vol. 116. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1988.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy.* Vol. 45. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 1999.

[KN74] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences.* Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], 1974.

[Lau09] Michel Laurent. "On transfer inequalities in Diophantine approximation". In: *Analytic number theory.* Cambridge Univ. Press, Cambridge, 2009, pp. 306–314.

[Maz95] Fernando Mazzone. "A characterization of almost everywhere continuous functions". In: *Real Anal. Exchange* 21.1 (1995/96).

[Ökt99] G. Ökten. "Error reduction techniques in quasi-Monte Carlo integration". In: *Math. Comput. Modelling* 30.7-8 (1999), pp. 61–69.

[Ser68] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ten95] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory.* Vol. 46. Cambridge Studies in Advanced Mathematics. Translated from the second French edition (1995) by C. B. Thomas. Cambridge University Press, Cambridge, 1995.