

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

Daniel Miller

September 6, 2016

1 Motivation

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

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

determines 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 sequence $(\mathrm{sgn} a_p(E))_p$ in fact determines E up to isogeny. Ramakrishna had the insight that this fact means the “strange L -function”

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

determines E up to isogeny. In this note, we define a more general class of strange L -functions, and show that their analytic properties are closely tied to the distribution 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 [BLGHT11], tells us that for any continuous function $f: [0, \pi] \rightarrow \mathbf{C}$, we have

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

as $N \rightarrow \infty$. 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 $L(\mathrm{sym}^k E, s)$

[Ser68, A.1 Th.1]. We take as our starting point the much stronger conjecture, due to Akiyama–Tanigawa [AT99], that

$$\left| \frac{1}{\pi(N)} \sum_{p \leq N} f(\theta_p) - \int_0^\pi f \, d\mu_{\text{ST}} \right| \ll_f N^{-\frac{1}{2} + \epsilon}$$

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

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

where f varies over almost-everywhere continuous functions on $[0, \pi]$.

These results make perfect sense in a much more general context, and we prove them there. In Section ? I set up this context and carefully define strange L -functions. In Section ?, I prove basic analytic properties of the strange L -functions and connect their analytic properties with the equidistribution of a sequence. In Section ?, I apply these results where “everything is known,” i.e. varieties over function fields. Finally, in Section ?, 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 Strange L -functions

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

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

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

wherever this product converges.

Elementary topology tells us that $L : \mathbf{D}^\infty \times \mathbf{C}^{\Re > 1} \rightarrow \mathbf{C}$ is continuous. We will see that for fixed $\mathbf{z} \in \mathbf{D}^\infty$, the analytic properties of $L(\mathbf{z}, s)$ are closely tied to estimates for the sums $A_{\mathbf{z}}(x) = \sum_{p \leq x} z_p$. 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 $\mathbf{x} \in X^\infty$ are of the form $\mathbf{x} = (x_2, x_3, \dots)$. 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 $\mathbf{x} \in \mathbf{D}^\infty$ and $N > 0$, write \mathbf{x}^N for the probability measure on \mathbf{D} given by

$$\int_X f \, d\mathbf{x}^N = \mathbf{x}^N(f) = \frac{1}{\pi(N)} \sum_{p \leq N} f(x_p).$$

Let μ be a Borel measure on X . Recall that \mathbf{x} is μ -*equidistributed* if $\mathbf{x}^N \rightarrow \mu$ weakly, i.e. $\mu(f) = \lim_{N \rightarrow \infty} \mathbf{x}^N(f)$ 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 $f: X \rightarrow \mathbf{C}$ be bounded and measurable. Then f is continuous almost everywhere if and only if $\mu(f) = \lim_{N \rightarrow \infty} \mathbf{x}^N(f)$ for all μ -equidistributed \mathbf{x} .*

Proof. This follows directly from the proof of [Maz96, Th.1]. \square

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

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

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

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

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

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 $\mathbf{x} \in (G^\natural)^\infty = G^{\natural, \infty}$ and function $f \in C^{\text{ae}}(G^\natural)^{\|\cdot\|_\infty \leq 1}$, we can define $L_f(\mathbf{x}, s)$. 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 $\lambda_\rho^1, \dots, \lambda_\rho^{\deg \rho}: G^\natural \rightarrow S^1$, continuous away from the set $\{\det(1 - \rho) = 0\}$, such that for every $x \in G^\natural$, there are angles $\theta_1, \dots, \theta_{\deg \rho} \in [0, 2\pi)$, satisfying $\theta_1 \leq \dots \leq \theta_{\deg \rho}$, 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]. \square

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

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

3 Discrepancy

The rest of our definitions concern discrepancy, which for now we define only in a special context. Let $r \geq 1$ be an integer, and consider the space $[0, 1]^r$. For $x, y \in [0, 1]^r$, we write $x < y$ (resp. $x \leq y$) if $x = (x_1, \dots, x_r)$, $y = (y_1, \dots, y_r)$ and $x_i < y_i$ (resp. $x_i \leq y_i$) for all i . Given $x < y \in [0, 1]^r$, write

$$I_x = \{z \in [0, 1]^r : z < x\}$$

$$I_{x,y} = \{z \in [0, 1]^r : x \leq z < y\}.$$

Definition 3.1. Let μ, ν be probability measures on $[0, 1]^r$. The *star-discrepancy* between μ and ν is

$$\text{disc}^*(\mu, \nu) = \sup_{x \in [0, 1]^r} |\mu(I_x) - \nu(I_x)|,$$

the *discrepancy* between μ and ν is

$$\text{disc}(\mu, \nu) = \sup_{x < y \in [0, 1]^r} |\mu(I_{x,y}) - \nu(I_{x,y})|,$$

and the *isotropic discrepancy* between μ and ν is

$$\text{disc}^{\text{iso}}(\mu, \nu) = \sup_{C \subset [0, 1]^r} |\mu(C) - \nu(C)|,$$

where C ranges over open and closed convex subsets of $[0, 1]^r$.

Let λ be the Lebesgue measure on $[0, 1]^r$, \mathbf{x} a sequence in $[0, 1]^r$. We write $\text{disc}^*(\mathbf{x}^N) = \text{disc}^*(\mathbf{x}^N, \lambda)$ for $*$ in $\{\emptyset, \star, \text{iso}\}$.

Theorem 3.2. *Let \mathbf{x} be a sequence in $[0, 1]^r$. Then*

$$\text{disc}(\mathbf{x}^N) \leq \text{disc}^{\text{iso}}(\mathbf{x}^N) \leq (4r\sqrt{r} + 1) \text{disc}(\mathbf{x}^N)^{1/r},$$

$$\text{disc}^*(\mathbf{x}^N) \leq \text{disc}(\mathbf{x}^N) \leq 2^r \text{disc}^*(\mathbf{x}^N).$$

Proof. The first inequality is Theorem 1.6, and the second is Example 1.2, both from [KN74, Ch.2]. \square

We can use the above to define discrepancy for sequences in G^\natural , the space of conjugacy classes in a compact connected semisimple Lie group.

Let G^{sc} be the simply-connected cover of G . Choose a maximal torus $T \subset G^{\text{sc}}$; let $W = N(T)/T$ be the Weyl group. Let $\mathfrak{t} = \text{Lie}(T)$ and recall that the

kernel of $\exp: \mathfrak{t} \rightarrow T$ is generated by the nodal vectors associated to the root system $R(G^{\text{sc}}, T)$ [Bou05, 9.6 Pr.11]. Write $\{t_1, \dots, t_r\} \subset \mathfrak{t}$ for these vectors. The exponential map $\exp: \mathfrak{t} \rightarrow T$ induces an isomorphism $\mathfrak{t}/(\langle t_i \rangle \rtimes W) \rightarrow G^\natural$. In particular, we can use the basis $\{t_1, \dots, t_r\}$ to identify $\mathfrak{t}/\langle t_i \rangle$ with $[0, 1]^r/W$. Let $p_G: [0, 1]^r \rightarrow G^\natural$ be the surjection $(x_1, \dots, x_r) \mapsto \exp(\sum x_i t_i)$. This is a $\#W$ -to-one map almost everywhere, so for a measure μ on G^\natural the “pullback measure”

$$p_G^* \mu(f) = \mu \left(\frac{1}{\#W} \sum_{w \in W} w^* f \right)$$

makes sense.

Definition 3.3. With the setup as above, let μ, ν be probability measures on G^\natural . The $*$ -discrepancy between μ and ν is

$$\text{disc}^*(\mu, \nu) = \text{disc}^*(p_G^* \mu, p_G^* \nu).$$

Example 3.4. Let $G = \text{SU}(2)$ with maximal torus

$$T = \left\{ \begin{pmatrix} e^{2\pi i t} & \\ & e^{-2\pi i t} \end{pmatrix} : -1 \leq t < 1 \right\}.$$

Then $W = S_2$, whose nontrivial element acts via $t \mapsto -t$.

If ν is the Haar measure on G^\natural , we simply write $\text{disc}(\mu)$ for $\text{disc}(\mu, \text{Haar})$.

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 3.5 (Koksma, Hlawka). *Let G be as above. Let $f: G^\natural \rightarrow \mathbb{C}$ be such that $f \, dx$ is a measure with bounded variation. Then*

$$\left| \mathbf{x}^C(f) - \int f \, dx \right| \leq \text{Var}(f) \text{disc}(\mathbf{x}^C).$$

Proof. This is [Ökt99, Th. 3.2]. □

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

Theorem 3.6. *Let \mathbf{x} be a sequence in $[0, 1]^r$. Then*

$$\text{disc}^{\text{iso}}(\mathbf{x}^N, \mu) = \sup_{P \subset [0, 1]^r} |\mathbf{x}^N(P) - \mu(P)|,$$

where P ranges over all open and closed convex polytopes contained in $[0, 1]^r$.

Proof. We follow the proof of [KN74, Ch.2 Th.1.5]. Clearly the supremum in question is bounded above by isotropic discrepancy, so we only need to show the opposite bound. Let $C \subset [0, 1]^r$ be a convex set. Suppose C contains x_{i_1}, \dots, x_{i_a} . Then C contains P , the convex hull of $\{x_{i_1}, \dots, x_{i_a}\}$.

Use the fact that given a convex set, and a point not in the interior of the set, the two can be separated by a hyperplane. Intersect half-planes, and get $P \subset C \subset Q$, with P and Q polytopes, and $\mathbf{x}^N(P) = \mathbf{x}^N(C) = \mathbf{x}^N(Q)$. This yields (via $a \leq b \leq c$ implies $|b| \leq \max\{|a|, |c|\}$)

$$|\mathbf{x}^N(C) - \mu(C)| \leq \max\{|\mathbf{x}^N(P) - \mu(P)|, |\mathbf{x}^N(Q) - \mu(Q)|\}.$$

□

Theorem 3.7. *Let \mathbf{x} be a sequence in $[0, 1]^r$. Then*

$$\text{disc}^{\text{iso}}(\mathbf{x}^N, \mu) \leq ? \text{disc}(\mathbf{x}^N, \mu)?.$$

Proof. We follow the proof of [KN74, Ch.2 Th.1.6]. First, note that $\mu = f\lambda$ where λ is Lebesgue, thus

$$\mu(S) = \int_S f \, d\lambda \leq \|f\|_\infty \lambda(S).$$

We write this as: $\mu \leq \|\mu\|_\infty \lambda$.

Let P be a convex polytope in $[0, 1]^r$. For any integer $n \geq 1$, we have a partition of $[0, 1]^r$ as follows. Given $h \in \mathbf{Z}^r$ with $|h|_\infty < n$, let

$$I_h^{(n)} = \left\{ x \in [0, 1]^r : \frac{h_i}{n} \leq x_i < \frac{h_i + 1}{n} \right\}.$$

Define:

$$\begin{aligned} P_1^{(r)} &= \bigcup_{I_h^{(r)} \subset P} I_h^{(r)} \\ P_2^{(r)} &= \bigcup_{I_h^{(r)} \cap P \neq \emptyset} I_h^{(r)}. \end{aligned}$$

Then clearly $P_1 \subset P \subset P_2$. Moreover, for each $(h_1, \dots, h_{r-1}) \in \mathbf{Z}^{r-1}$, the set of $m \in \mathbf{Z}$ such that for $h = (h_1, \dots, h_{r-1}, m)$, $I_h^{(r)} \subset P$ (resp. $I_h^{(r)} \cap P \neq \emptyset$) is a sequence with no gaps. This is an easy consequence of the convexity of P . (Prove this.) bla bla bla the rest works. □

4 Main results

Theorem 4.1. *Let $\mathbf{z} \in \mathbf{D}^\infty$. Then $L(\mathbf{z}, s)$ defines a holomorphic function on the region $\{\Re s > 1\}$. Moreover, on that region,*

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

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

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

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 $\log L(\mathbf{z}, s)$ comes from [Apo76, 11.9 Ex.2]. \square

Theorem 4.2. *Assume $A_{\mathbf{z}}(x) \ll x^{\alpha+\epsilon}$, $\alpha \in [\frac{1}{2}, 1]$. Then $\log L(\mathbf{z}, s)$ is holomorphic on $\{\Re > \alpha\}$.*

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

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

For each p , we have

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

Elementary analysis gives

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

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

Corollary 4.3. *Let G be a compact connected semisimple Lie group, $\mathbf{x} \in G^{\natural, \infty}$ satisfy $\text{disc}(\mathbf{x}^C, d\mathbf{x}) \ll C^{-\frac{1}{2}+\epsilon}$. Then for every $f \in C^{\text{ae}}(G^{\natural})^{\|\cdot\| \leq 1}$, $L_f(\mathbf{x}, s)$ 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 $\mathbf{x}^C(f) \ll C^{-\frac{1}{2}+\epsilon}$. Thus the sequence $f(\mathbf{x})$ satisfies $A_{f(\mathbf{x})}(x) \ll x^{\frac{1}{2}+\epsilon}$, and the result follows from Theorem 4.2. \square

5 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 5.1. 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 $G = \overline{\rho_{\mathcal{F}}(\pi_1(U_{\bar{k}}, \infty))}^{\text{Zar}}$. Assume $\rho_{\mathcal{F}}(\pi_1(U, \infty)) \subset G(\overline{\mathbf{Q}}_l)$.

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

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

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

Theorem 5.2. *Let σ be a non-trivial irreducible representation of $\text{ST}(\mathcal{F})$. Then*

$$|\theta_{\mathcal{F}}^C(\text{tr } \sigma)| \ll_{\mathcal{F}} \dim(\sigma) C^{-\frac{1}{2}}.$$

Proof. This is [Kat88, p.39]. □

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

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

For such functions, we have:

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

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

Theorem 5.3. *Let $\mathbf{z} \in \mathbf{D}^{\infty}$, and assume $\log L(\mathbf{z}, s)$ has analytic continuation to $\{\Re > \alpha\}$, $\alpha \in [\frac{1}{2}, 1]$, and that for $\sigma > \alpha$, we have $|\log L(\mathbf{z}, \sigma + it)| \ll |t|^{1-\epsilon}$. Then $|A_{\mathbf{z}}(x)| \ll x^{\alpha+\epsilon}$.*

Proof. Recall that we can write

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

Thus, for any $\epsilon > 0$, our bound on $|\log L(\mathbf{z}, \sigma + it)|$ 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:

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

By [Apo76, Th.11.18],

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

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

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

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

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

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

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

Letting $T \rightarrow \infty$ we obtain the desired result. \square

6 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 $\mu \geq 2$, there is an element ξ_μ of the Cantor set with $\mu(\xi_\mu) = \mu$. Moreover, by [KN74, ?], for every $\epsilon > 0$, the sequence $x_n = n\alpha \bmod 1$ has discrepancy $\text{disc}(\mathbf{x}^C) = \Omega(C^{-\frac{1}{\mu(\alpha)-1}-\epsilon})$.

Theorem 6.1. *Let $X = S^1$ with the natural Haar measure. For every $\eta \in (0, \frac{1}{2})$, there is a sequence $\mathbf{x} = (x_2, x_3, \dots) \in (S^1)^\infty$ such that for all $f \in C^\infty(S^1)^{\|\cdot\|_\infty \leq 1}$, the function $\log L_f(\mathbf{x}, s)$ has analytic continuation to $\{\Re > \frac{1}{2}\}$, but for all $\epsilon > 0$, $|\text{disc}(\mathbf{x}^C)| = \Omega(C^{-\eta-\epsilon})$.*

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

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

□

Theorem 6.2. *Let E/\mathbf{Q} be a non-CM elliptic curve, and put $\theta = \theta(E)$. Assume that $\text{disc}(\theta^C) \ll C^{-\frac{1}{2}+\epsilon}$. Then if $f \in C^{\text{ae}}([0, \pi], \text{ST})^{\|\cdot\|_\infty \leq 1}$, the strange L -function $L_f(\theta, s)$ has analytic continuation to $\{\Re > \frac{1}{2}\}$ and satisfy the Riemann Hypothesis. In particular, this holds for all $L(\text{sym}^k E, s)$.*

Proof. The first conclusion follows from Corollary 4.3. The second part follows from the fact that any $L(\text{sym}^k E, s)$ can be written as a product of L_f 's, namely the $L_{\chi_{\text{sym}^k}^j}$'s in Section ??.

□

Theorem 6.3. *Fix $f \in C^{\text{ae}}([0, \pi], \text{ST})^{\|\cdot\|_\infty \leq 1}$ 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 $f: [0, \pi] \rightarrow \mathbf{C}$ that is not almost everywhere

7 A collection of counterexamples

In [AT99, ?], Akiyama and Tanigawa claim that for E/\mathbf{Q} , the “discrepancy conjecture” $\text{disc}(\theta^C) \ll C^{-\frac{1}{2}+\epsilon}$ 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 7.1. 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

$$\begin{aligned} \max\{|m_0 x_i - m_i|\} &\leq |m|_\infty^{-w} \\ |m_0 + m_1 x_1 + \dots + m_r x_r| &\leq |m|_\infty^{-w} \end{aligned}$$

respectively.

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

Lemma 7.2. *Let $x \in \mathbf{R}^r$ with $|x|_\infty \leq 1$ and $\omega_0(x)$ (resp. $\omega_{r-1}(x)$) is finite. Then*

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

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 7.1 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

$$\begin{aligned} \max\{|m_0x_i - m_i|\} &\geq C_0|m|_\infty^{-\omega_0(x)-\epsilon} \\ |m_0 + m_1x_1 + \cdots + m_rx_r| &\geq C_{r-1}|m|_\infty^{-\omega_{r-1}(x)-\epsilon}. \end{aligned}$$

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 $|(n, m_1, \dots, m_r)| \leq \max\{|n|, |nx_i|\} \leq |n|$. In particular,

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

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 $d(m_1x_1 + \cdots + m_rx_r, \mathbf{Z}) = |m_0 + m_1x_1 + \cdots + m_rx_r|$ for $|m_0| \leq |(m_1, \dots, m_r)| \cdot |x| + 1$. Thus $|(m_0, \dots, m_r)|_\infty \leq 2|x| |(m_1, \dots, m_r)|$, giving us

$$d(m_1x_1 + \cdots + m_rx_r, \mathbf{Z}) \geq C'_{r-1}|(m_1, \dots, m_r)|^{-\omega_{r-1}(x)-\epsilon},$$

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 . \square

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 7.1, 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 $m \in \mathbf{Z}^r$

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

where $\langle m, x \rangle = m_1x_1 + \cdots + m_rx_r$ is the usual inner product.

Theorem 7.3 (Jarník). *Let $w \geq 1/r$. Then there exists $x \in \mathbf{R}^r$ such that $\omega_0(x) = w$ and $\omega_{r-1}(x) = rw + r - 1$.*

Theorem 7.4. *Fix $x \in \mathbf{T}^r$ with $\omega_{r-1}(x)$ finite. Then*

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

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

Proof. First, note the easy bound:

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

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 $\left| \sum_{n \leq N} e^{2\pi i n \langle m, x \rangle} \right| \leq \frac{1}{|\sin(\pi \langle m, x \rangle)|}$. It is easy to check that $|\sin(\pi t)| \geq d(t, \mathbf{Z})$, hence $\left| \sum_{n \leq N} e^{2\pi i n \langle m, x \rangle} \right| \leq \frac{1}{d(\langle m, x \rangle, \mathbf{Z})}$. The final estimate comes from Lemma 7.2. \square

Theorem 7.5. *Assume $\omega_{r-1}(x) < \infty$. Let $f \in L^1(\mathbf{T}^r)$ with $\hat{f}(0) = 0$ and suppose the Fourier coefficients of f satisfy the bound $|\hat{f}(m)| \ll |m|^{-\frac{1}{r-1} - \omega_{r-1} - \epsilon}$. Then*

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

Proof. Write f as a Fourier series:

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

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

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

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

Corollary 7.6. *Assume $\omega_{r-1}(x) < \infty$, and let $f \in C^\infty(\mathbf{T}^r)$ with $\hat{f}(0) = 0$. Then $\left| \sum_{n \leq N} f(nx) \right| \ll_{f,x} 1$.*

Proof. This follows from Theorem 7.5 and the fact that the Fourier coefficients of a smooth function decay faster than $|m|^k$, for any $k \in (-\infty, -1]$. \square

Theorem 7.7. *If $\omega_0(x) < \infty$, then the sequence $\mathbf{x} = (nx)_{n \geq 1}$ in \mathbf{T}^r has discrepancy*

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

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, \dots, m_r) with $q > 0$ such that

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

Since $\max\{q, |m|_\infty\} \geq q$, we derive the stronger statement that for infinitely many $q \rightarrow \infty$, there exists $m = (m_1, \dots, m_r) \in \mathbf{Z}^r$ such that $|qx - m|_\infty \leq q^{-\omega_0(x)+\delta/2}$, or, equivalently, $|x - \frac{m}{q}| \leq q^{-1-\omega_0(x)+\delta/2}$. Pick such a q , and let $N = \lfloor q^{\omega_0(x)-\delta} \rfloor$. Then for $n \leq N$, we have $|nx - \frac{n}{q}m| \leq q^{-1-\delta/2}$. Thus, for $n \leq N$, 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, $q^{-1} - 2q^{-1-\delta/2} \geq 1/2q$, so the (non-star) discrepancy of \mathbf{x}^N is bounded below by $2^{-r}q^{-r}$. Since $q^{\omega_0(x)-\delta} \leq 2N$, the (non-star) discrepancy at N is bounded below by

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

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

The key point in the above theorem is that

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

Theorem 7.8. *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*

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

holds, but for which

$$\text{disc}(\mathbf{x}^N) = \Omega_{\epsilon,r,x} (N^{-\eta-\epsilon}).$$

Proof. Let $w = \frac{r}{\eta} \geq \frac{1}{r}$. By Theorem 7.3, 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 7.6 and Theorem 7.7. \square

Lemma 7.9 (Moser). *Let f be a smooth, nonnegative function on $[0, 1]^r$ such that $\int f = 1$ and f vanishes only on the boundary of $[0, 1]^r$. Then there is a unique factorization*

$$f(x_1, \dots, x_r) = f_1(x_1)f_2(x_1, x_2) \cdots f_r(x_1, \dots, x_r)$$

of f into smooth functions such that

$$\int_0^1 f_i(x_1, \dots, x_{i-1}, t) dt = 1$$

for all $1 \leq i \leq r$.

Proof. We prove this by induction on r . For $r = 1$, the claim is trivial. Otherwise, fix (x_1, \dots, x_{r-1}) . Then we are trying to solve the following problem. Find a factorization $g(t) = \lambda h(t)$, where $\int h = 1$. This has the obvious (unique) solution $h(t) = g(t)/(\int g)$. Thus, we have:

$$\begin{aligned} f_{r-1}(x_1, \dots, x_{r-1}) &= \int_0^1 f(x_1, \dots, x_{r-1}, t) dt \\ f_r(x_1, \dots, x_r) &= f(x_1, \dots, x_r) / f_{r-1}(x_1, \dots, x_{r-1}). \end{aligned}$$

□

Lemma 7.10. *Let λ be the Lebesgue measure on $[0, 1]^r$, and $\mu = f\lambda$ where $f \geq 0$ is smooth, and $f \neq 0$ on the interior of $[0, 1]^r$. Then there is a diffeomorphism $u: [0, 1]^r \rightarrow [0, 1]^r$, identity on the boundary, such that $u_*\lambda = \mu$.*

Proof. We follow [Mos65]. First, use Lemma 7.9 to factor f as a product

$$f(x_1, \dots, x_r) = f_1(x_1)f_2(x_1, x_2) \cdots f_r(x_1, \dots, x_r).$$

Let

$$u_i(x_1, \dots, x_i) = \int_0^{x_i} f_i(x_1, \dots, x_{i-1}, t) dt.$$

Then each u_i is a strictly increasing function, and $u = (u_1, \dots, u_r)$ is a diffeomorphism of the unit square, which is the identity on the boundary. Moreover,

$$\det(\text{Jac } u) = \prod \frac{du_i}{dx_i} = \prod f_i = f.$$

Now, by the change of variables formula,

$$\int \phi du_*^{-1}\lambda = \int \phi \circ u^{-1} d\lambda = \int \phi \det(\text{Jac } u) d\lambda = \int \phi d\mu,$$

i.e. $\mu = u_*^{-1}\lambda$.

□

Theorem 7.11. *Let μ, f be as above. Then there exists a sequence \mathbf{x} in $[0, 1]^r$ such that $\text{disc}(\mathbf{x}^N, \mu) = \Omega(N^{-r\eta-\epsilon})$, but for which $|\sum g(x_n)| \ll_g 1$ for all smooth g with $\mu(g) = 0$.*

Proof. By Lemma 7.10, there exists a boundary-preserving diffeomorphism $u: [0, 1]^r \rightarrow [0, 1]^r$, such that $u_*\lambda = \mu$, where λ is the Lebesgue measure as above.

Start with a sequence $\mathbf{y}_n = ny$, where y is as in Theorem 7.8. Let $\mathbf{x} = u_*\mathbf{y}$, i.e. $x_n = u(y_n)$. Then, if $\phi \in C^\infty([0, 1]^r)$, the composite $\phi \circ u$ is also smooth, so

$$\left| \sum_{n \leq N} \phi(u_*y_n) \right| = \left| \sum_{n \leq N} (\phi \circ u)(y_n) \right| \ll_{\phi \circ u, y} 1.$$

Thus, all we need is a lower bound on the discrepancy. The proof of Theorem 7.7 tells us that for infinitely many $N \rightarrow \infty$, there is an r -ball B_N with volume

$CN^{-\eta-\epsilon}$ (C not depending on N) that does not contain any of y_1, \dots, y_N . By [Pol01, Th.2.1], for N sufficiently large, the set $u(B_N)$ is convex, and moreover $\mu(u(B_N)) = \lambda(B_N)$. Thus, since $\mathbf{x}^N(u(B_N)) = \emptyset$, we have

$$\text{disc}^{\text{iso}}(\mathbf{x}^N, \mu) \geqslant CN^{-\eta-\epsilon},$$

and thus

$$\text{disc}(\mathbf{x}^N, \mu) = \Omega(N^{-r\eta-\epsilon})$$

as desired.

[Need: bounds relating discrepancy and isotropic discrepancy to hold for non-Lebesgue measure.] \square

Theorem 7.12. *Let $[0, 1]^r, \mu$ be as above. Then there exists \mathbf{x} such that for all smooth f , $L_f(\mathbf{x}, s)$ satisfies the Riemann Hypothesis (analytic continuation and no zeros on $\{\Re > \frac{1}{2}\}$, but for which $\text{disc}(\mathbf{x}^N) = \Omega(N^?)$.*

References

- [Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.
- [AT99] Shigeki Akiyama and Yoshio Tanigawa. Calculation of values of L -functions associated to elliptic curves. *Math. Comp.*, 68(227):1201–1231, 1999.
- [BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.
- [Bou05] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 7–9*. Elements of Mathematics. Springer-Verlag, 2005. Translated from the 1975 and 1982 French originals by Andrew Pressley.
- [Bug08] Yann Bugeaud. Diophantine approximation and Cantor sets. *Math. Ann.*, 341(3):677–684, 2008.
- [Eng89] Ryszard Engelking. *General topology*, volume 6 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, second edition, 1989. Translated from the Polish by the author.
- [Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
- [Kat88] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

- [KN74] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], 1974. Pure and Applied Mathematics.
- [KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.
- [Lau09] Michel Laurent. On transfer inequalities in Diophantine approximation. In *Analytic number theory*, pages 306–314. Cambridge Univ. Press, Cambridge, 2009.
- [Maz96] Fernando Mazzone. A characterization of almost everywhere continuous functions. *Real Anal. Exchange*, 21(1), 1995/96.
- [Mos65] Jürgen Moser. On the volume elements on a manifold. *Trans. Amer. Math. Soc.*, 120:286–294, 1965.
- [Ökt99] G. Ökten. Error reduction techniques in quasi-Monte Carlo integration. *Math. Comput. Modelling*, 30(7-8):61–69, 1999.
- [Pol01] B. T. Polyak. Convexity of nonlinear image of a small ball with applications to optimization. *Set-Valued Anal.*, 9(1-2):159–168, 2001.
- [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*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.