FROBENIUS DISTRIBUTIONS (SATO–TATE DISTRIBUTIONS)

COURSE: KIRAN KEDLAYA AND ANDREW SUTHERLAND
NOTES: ROSS PATERSON

Lecture 1 (Kedlaya)

For $f \in \mathbb{Z}[X]$ squarefree of degree d, define

$$N_f(p) = \#\{x \in \mathbb{F}_p : f(x) \equiv 1 \mod p\}.$$

Note that clearly $0 \leq N_f(p) \leq d$.

Example 1 ([Sut, §1.1])**.**

Definition 2. Let

$$c_i(B) := \frac{\#\{p \leq B \ : \ N_f(p) = i\}}{\#\{p \leq B\}}$$

Claim: We can describe limiting values of $c_i(B)$ for all i.

Let $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ be the splitting field of f over $\mathbb{Q}$, where $f = \prod_{i=1}^{d}(x - \alpha_i)$, and $G = \mathrm{Gal}(L/\mathbb{Q})$ which acts transitively on this set of roots. Then we let

$$\rho : G \to \mathrm{GL}_d(\mathbb{C})$$

be the associated permutation representation. For p prime we have an exact sequence given as follows. Choose a prime $\mathfrak{p} \mid p$ of $\mathcal{O}_L$, and let:

- $D_\mathfrak{p}$ be the associated decomposition group (i.e. the stabiliser of $\mathfrak{p}$ under the action of G on the set of primes above p);
- $I_\mathfrak{p}$ be the ineria subgroup of $D_\mathfrak{p}$.

Then we have

$$1 \longrightarrow I_\mathfrak{p} \longrightarrow D_\mathfrak{p} \longrightarrow \mathrm{Gal}\left(\frac{\mathcal{O}_L}{\mathfrak{p}}/\mathbb{F}_p\right) \longrightarrow 1.$$

Note that $\mathrm{Gal}\left(\frac{\mathcal{O}_L}{\mathfrak{p}}/\mathbb{F}_p\right)$ has a canonical generator, $x \mapsto x^p$, and so we denote by $\mathrm{Frob}_\mathfrak{p}$ a choice of lift of this in $D_\mathfrak{p}$. if p is unramified (which is true of all but finitely many p) then $\mathrm{Frob}_\mathfrak{p}$ is a well defined element of $D_\mathfrak{p}$. As $\mathfrak{p}$ varies amongst primes above p, $\mathrm{Frob}_\mathfrak{p}$ traces out a conjugacy class in G, which we denote by Frob_p.

For unramified p, $N_f(p)$ is counting fixed points of $\mathrm{Frob}_\mathfrak{p}$ on $\{\alpha_1, \ldots, \alpha_d\}$. That is,

$$N_f(p) = \mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})).$$

Applying Chebotaryov density theorem, we see that the conjugacy class of Frob_p is uniformly distributed in the set of conjugacy classes of G, denoted $\mathrm{conj}(G)$, with respect to the measure which weights a conjugacy class C proportionately to its size $\#C$.

Example 3. For $f(x) = x^3 - x + 1$ we have $G = S_3$, so

$$\lim_{B\to\infty} c_i(B) = \begin{cases} \frac{2}{6} & \text{if } i = 0 \\ \frac{3}{6} & \text{if } i = 1 \\ \frac{1}{6} & \text{if } i = 3. \end{cases}$$

Aside. If G is abelian then $L \subseteq \mathbb{Q}(\zeta_n)$ for some n, and then $\mathrm{Frob}_{\mathfrak{p}}$ is determined by $p \mod n$.

Think now of G as a discrete topological group, note that this means that it is compact (also Hausdorff). Any compact topological group has a unique left- and right- invariant probability measure in the Radon sense (i.e. continuous functions $G \to \mathbb{R}$ can be integrated) known as the Haar measure, which we denote by μ_G.

I can then take the pushforward measure on the set of conjugacy classes of G. That is, I evaluate the functional on class functions.

Example 4. Consider $\mathrm{SU}(2) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \ : \ ad - bc = 1, \ A^{-1} = A^* = \overline{A}^T \right\}$. Via the trace map, we have a bijection between the conjugacy classes of $\mathrm{conj}(\mathrm{SU}(2))$ and the set $[-2, 2]$.

Definition 5. Let X be some probability space, and $t : X \to \mathbb{R}$ be a random variable. Then the moment sequence of t is $(\mathbb{E}(t^n))_{n\in\mathbb{Z}_{\geq 0}}$, where we always take $t^0 = 1$.

Here is a comment that we won't expand on for now.

- We could also look at
$$N_f(p^k) = \#\left\{x \in \mathbb{F}_{p^k} \ : \ f(x) = 0\right\},$$
and for fixed p we could package this collection (indexed by k) into a local zeta function (see later in the course). Then
$$N_f(p^k) = \mathrm{tr}(\rho(\mathrm{Frob}_{\mathfrak{p}}^k))$$

1. Arithmetic Schemes

Definition 6. Let X be a scheme of finite type over $\mathbb{Z}$. For each prime number p we define
$$N_X(p) := \#X(\mathbb{F}_p).$$

Question 7. *How does this depend on p?*

Elliptic Curves. Consider $E \subseteq \mathbb{P}^2_{\mathbb{Z}}$ cut out by the affine model $y^2 = x^3 + Ax + B$. Assume that $x^3 + Ax + B$ is squarefree (so the generic fibre $E_{\mathbb{Q}}$ is an elliptic curve), and that $E_{\mathbb{Q}}$ does not have complex multiplication.

Theorem 8 (Hasse)**.** *For each prime number p, write*
$$\#E(\mathbb{F}_p) = p + 1 - t_p.$$
Then, so long as $E_{\mathbb{F}_p}$ is smooth, $|t_p| \leq 2\sqrt{p}$.

This suggests we should look at $\frac{t_p}{\sqrt{p}} \in [-2, 2]$. Looking at these numbers experimentally, there appears to be a clear pattern in their distribution, which is explained by the following theorem.

Theorem 9. *The values* $\frac{t_p}{\sqrt{p}}$ *are equidistributed for the pushforward of the Haar measure on* $\mathrm{conj}(\mathrm{SU}(2))$ *on* $[-2,2]$.

Lecture 2 (Sutherland): Equidistribution

Generalities

Let X be a compact Hausdorff topological space, and let $C(X)$ denote the Banach space of continuous functions $f : X \to \mathbb{C}$ under the sup-norm. For $f, g \in C(X)$ which are $\mathbb{R}$-valued with $f(x) \leq g(x)$ for all $x \in Z$ then we will write $f \leq g$. If we write such an inequality then part of the data is the assertion that the functions are real valued.

Definition 10. a (positive normalised Radon) measure is a continuous $\mathbb{C}$-linear

$$\mu : C(X) \to \mathbb{C}$$

such that for all $f \geq 0$, we have $\mu(f) \geq 0$, and moreover $\mu(1_X) = 1$.

Example 11. Note the dirac measure at a point $x \in X$

$$\delta_X : C(X) \to \mathbb{C}$$

given by $f \mapsto f(x)$.

Notation 12. We denote for $f \in C(X)$

$$\int_X f\mu := \mu(f).$$

Given such a measure, we can define a measure of subsets $S \subset C(X)$

$$\mu(S) := \begin{cases} \sup\{\mu(f) \ : \ 0 \leq f \leq 1_S\} & \text{if } S \text{ is open} \\ 1 - \mu(X - S) & \text{if } S \text{ is closed} \\ 0 & \text{if } \forall \varepsilon > 0 \ \exists \text{ open } U \supset S \text{ with } \mu(U) \leq \varepsilon \\ \mu(\overline{S}) = \mu(S^\circ) & \text{if } \mu(\partial S) = 0,\ \partial S = \overline{s} \backslash S^\circ. \end{cases}$$

Definition 13. A sequence $(x_1, x_2, \dots)$ in X is μ-equidistributed if

$$\mu(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i)$$

for all $f \in C(X)$.

Lemma 14. *Let* (f_j) *be a family of functions in* $C(X)$ *whose* $\mathbb{C}$*-span is dense in* $C(X)$. *If* (x_i) *is a sequence in* X *for which* $\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f_j(x_i)$ *converges for all* f_j *in our family, then there exists a unique measure* μ *on* X *for which* (x_i) *is* μ*-equidistributed.*

Proof. See [Ser68]. □

Definition 15. $S \subseteq C(X)$ is μ-quarrable if $\mu(\partial S) = 0$.

Proposition 16. *If* (x_i) *is* μ*-equidistributed and* S *is* μ*-quarrable, then*

$$\mu(S) = \lim_{n\to\infty} \frac{\#\{x_i \in S \ : \ i \leq n\}}{n}$$

Proof. Exercise. □

Example 17. $X = [0,1]$, μ the Lebesgue measure, then (x_i) is equidistributed if and only if $\forall 0 \leq a < b \leq 1$,

$$\lim_{n\to\infty} \frac{\#\{x_i \in [a,b] \ : \ i \leq n\}}{n} = \mu([a,b]) = b - a$$

Compact Groups

From now on, $X := \mathrm{conj}(G)$ for some compact group G. The Haar measure on G induces a measure μ on X via

$$\mu(f) := \mu(f \circ \mathrm{conj}).$$

In this setting "equidistributed" means μ-equidistributed with respect to this μ.

Proposition 18. *A sequence (x_i) in $X = \mathrm{conj}(G)$ is equidistributed if and only if for every irreducible character $\chi : G \to \mathbb{C}$*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = \mu(\chi)$$

Proof. The Peter–Weyl theorem shows that the irreducible characters χ span a dense subspace of $C(X)$. □

Corollary 19. *(x_i) is equidistributed if and only if for all nontrivial irreducible χ.*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 0$$

Proof. For $\chi = 1$, the $\mu(1) = 1$ is always immediate. For the nontrivial χ,

$$\mu(\chi) = \int_G \chi\mu = \int_G 1 \cdot \chi\mu = 0$$

□

An easy Sato–Tate Result

Let $E/\mathbb{F}_q$ be an elliptic curve with $\#E(\mathbb{F}_q) = q+1-t_q$, where $t_q = \mathrm{tr}(\pi_E) = \alpha+\overline{\alpha}$ for some $\alpha \in \mathbb{C}$ with $|\alpha| = q^{1/2}$. Considering the base change, we have

$$\#E(\mathbb{F}_{q^r}) = q^r + 1 - \mathrm{tr}(\pi_E^r) = q^r + 1 - (\alpha^r + \overline{\alpha}^r).$$

Let $t_{q^r} = q^r + 1 - \#E(\mathbb{F}_{q^r})$.

Proposition 20. *Assume that E is ordinary, and let $x_r := \frac{t_{q^r}}{q^{r/2}}$. The sequence (x_r) is equidistributed in $[-2,2]$ with respect to the measure*

$$\mu := \frac{1}{\pi} \frac{dz}{\sqrt{4-z^2}},$$

where dz is the Lebesgue measure on $[-2,2]$.

Proof. Let $U(1) = \{u \in \mathbb{C}^\times \ : \ |u| = 1\}$. For $u = e^{i\theta}$, θ is uniformly distributed under the Haar measure for $U(1)$. To compute the pushforward of the Haar measure to $z := 2\cos\theta$

$$dz = 2\sin(\theta)d\theta = \sqrt{4-z^2}d\theta,$$

consider $\theta \in [0,\pi]$, $\mu = \frac{d\theta}{\pi} = \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}}$.

Nontrivial irreducible characters $U(1) \to \mathbb{C}^\times$ look like $\phi_a : u \mapsto u^a$ for some $a \in \mathbb{Z}_{\neq 0}$. Then

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \phi_a\left(\frac{\alpha^i}{q^{i/2}}\right) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \phi_a\left(\frac{\alpha^i}{q^{i/2}}\right)$$

□

L-Functions

Let us fix a number field K and consider a sequence $x = (x_\mathfrak{p})$ in $X = \mathrm{conj}(G)$ indexed by primes $\mathfrak{p}$ of K. Order these by $N(\mathfrak{p}) := \#\mathcal{O}_K/\mathfrak{p}$.

Definition 21. For each irreducible representation $\rho : G \to \mathrm{GL}_d(\mathbb{C})$ we define

$$L_X(\rho, s) := \prod_{\mathfrak{p}} \det\left(1 - \rho(x_\mathfrak{p})N(\mathfrak{p})^{-s}\right)^{-1},$$

which converges on $\Re(s) > 1$.

Theorem 22. *Suppose for every irreducible representation ρ, the function $L_x(\rho, s)$ is meromorphic on $\Re(s) \geq 1$ with no zeros or poles away from $s = 1$. Then $x = (x_\mathfrak{p})_\mathfrak{p}$ is equidistributed if and only if $L_x(\rho, 1) \notin \{0, \infty\}$ for every irreducible $\rho \neq 1$.*

Proof. See [Ser68], also Fité's notes from 2015 have a very nice exposition. □

Corollary 23. *L/K finite Galois, then $x = (\mathrm{conj}(\mathrm{Frob}_\mathfrak{p}|_L))_\mathfrak{p}$ is equidistributed.*

Remark 24. This implies the Chebotaryev density theorem.

Proof. If $\rho = 1$ then $L_x(\rho, s) \approx \zeta_K(s)$ which is holomorphic and nonvanishing on $\Re(s) \geq 1$ except simple pole at $s = 1$ (Hecke).

If $\rho \neq 1$ then $L_X(\rho, s) \approx L(\rho, s)$ the Artin L-function and this is holomorphic and nonvanishing on $\Re(s) \geq 1$ (Artin). □

Sato–Tate for CM Elliptic Curves

Definition 25. A Hecke character is a continuous homomorphism $\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ with $K^\times \subseteq \ker(\psi)$.

$$\mathrm{cond}(\psi) := \prod_{\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}},$$

where $e_\mathfrak{p}$ is the least nonnegative integer such that

$$1 + \mathfrak{p}^{e_\mathfrak{p}} \subset \mathcal{O}_{K_\mathfrak{p}}^\times \subseteq \ker(\psi).$$

The L-function is

$$L(\psi, s) := \prod_{\mathfrak{p} \nmid \mathrm{cond}(\psi)} \left(1 - \psi(\pi_\mathfrak{p})N(\mathfrak{p})^{-s}\right)^{-1},$$

where $\pi_\mathfrak{p}$ is any choice of uniformizer for $K_\mathfrak{p}$.

Remark 26. We can unitarise a Hecke characer ψ via

$$\psi := \psi / |\psi|.$$

In particular we can always consider them as functions to $U(1)$.

Lemma 27. *For any unitarized Hecke character ψ, the sequence $(\psi(\mathfrak{p}))_{\mathfrak{p}}$ is equidistributed in $U(1)$.*

Proof. As above, irreducible representaitons of $U(1)$ are $\phi_a(u) = u^a$ for $a \in \mathbb{Z}$, and $\psi_a := \phi_a \circ \psi$ is also a unitarized Hecke character.

If $\psi_a = 1$ then $L(\psi_a, s) \approx \zeta_K(s)$, so all good. If $\psi_a \neq 1$ then $L(\psi_a, s)$ is hoolomorphic and nonvanishing on $\Re(s) \geq 1$. □

Now assume that K is imaginary quadratic, and E/K is an elliptic curve with CM. Then K has a corresponding Hecke character ψ_E for which

$$|\psi_E(\pi_{\mathfrak{p}})| = N(\mathfrak{p})^{1/2},$$

with $t_{\mathfrak{p}} = \mathrm{tr}(\pi_E) = \psi_E(\pi_{\mathfrak{p}}) + \overline{\psi_E(\pi_{\mathfrak{p}})}$. Uniformize to get $x_{\mathfrak{p}} = \psi_E(\pi_{\mathfrak{p}}) + \overline{\psi}(\pi_{\mathfrak{p}}) \in [-2, 2]$.

Proposition 28. *The sequence $(x_{\mathfrak{p}})_{\mathfrak{p}}$ is equidistributed with respect to the measure*

$$\mu_{\mathrm{CM}} = \frac{1}{\pi} \frac{dz}{\sqrt{4 - z^2}}.$$

Proof. μ_{CM} is the pushforward of the Haar measure for $U(1)$ via $u \mapsto u + \overline{u}$ and the proposition then follows from the previous theorem on unitarized Hecke characters. □

Lecture 3 (Kedlaya)

References

[Ser68] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. MR0263823 ↑1, 1

[Sut] A. Sutherland, *Sato–tate distributions*. ↑1