FROBENIUS DISTRIBUTIONS
(SATO–TATE DISTRIBUTIONS)

COURSE: KIRAN KEDLAYA AND ANDREW SUTHERLAND
NOTES: ROSS PATERSON

Disclaimer. These notes were taken live during lectures. Any errors are the fault of the transcriber and not of the lecturer.

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* $[-2, 2]$.

References

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