Introduction to Algebraic Number Theory
Lecture 25

Andrei Jorza

10 ζ-functions and L-functions

(10.7) Density (continued).

Definition 1. Suppose $\mathcal{P}$ is a set of prime ideals of $K/\mathbb{Q}$. The set $\mathcal{P}$ is said to have **natural density** $\delta(\mathcal{P})_{\text{nat}}$ if

$$d(\mathcal{P}) = \lim_{x\to\infty} \frac{|\{\mathfrak{p}\in\mathcal{P} | |\mathfrak{p}|| < x\}|}{|\{\mathfrak{p}||\mathfrak{p}|| < x\}|}$$

exists.

The set $\mathcal{P}$ is said to have **Dirichlet density** $\delta(\mathcal{P})$ if

$$\delta(\mathcal{P}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{P}} ||\mathfrak{p}||^{-s}}{\sum_{\mathfrak{p}} ||\mathfrak{p}||^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{P}} ||\mathfrak{p}||^{-s}}{-\log(s-1)}$$

exists.

Note that, if they exist, then $\delta(\mathcal{P}) \leq 1$ and $\delta(\mathcal{P})_{\text{nat}} \leq 1$.

Proposition 2. *1. If $\mathcal{P}$ is finite then $d(\mathcal{P}) = \delta(\mathcal{P}) = 0$.*

2. If $\mathcal{P} \subset \mathcal{Q}$ then $\delta(\mathcal{P}) \leq \delta(\mathcal{Q})$.

3. Have $\delta(\mathcal{P}\cup\mathcal{Q}) \leq \delta(\mathcal{P}) + \delta(\mathcal{Q})$ with equality when $\delta(\mathcal{P}\cap\mathcal{Q}) = 0$ (e.g., when the intersection is finite or empty).

4. If $d(\mathcal{P})$ exists and equals $\alpha \in [0,1]$ then $\delta(\mathcal{P}) = d(\mathcal{P}) = \alpha$.

Proof. The only part requiring work is the last one, but we'll skip that since it reduces to basic, but unenlightening calculus. □

(10.8) Counting primes in arithmetic progression. The goal of this section is the following theorem.

Theorem 3 (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let $n \geq 2$ and a coprime to n. The set $\mathcal{P}_{a,n}$ of primes $p \equiv a \pmod n$ has density (either natural or Dirichlet) equal to $1/\varphi(n)$. In particular the set $\mathcal{P}_{a,n}$ is infinite.*

Proof. We will only show that the Dirichlet density is $1/\varphi(n)$, which already implies that $\mathcal{P}_{a,n}$ is infinite.

First, writing $G = (\mathbb{Z}/n\mathbb{Z})^\times$ note that

$$\sum_{\chi\in\widehat{G}} \chi(a^{-1}p) = \begin{cases} \varphi(n) & p \equiv a \pmod n \\ 0 & p \not\equiv a \pmod n \end{cases}$$

for any prime p. Thus

$$\varphi(n) \sum_{p\in\mathcal{P}_{a,n}} \frac{1}{p^s} = \sum_p \sum_{\chi\in\widehat{G}} \frac{\chi(a^{-1}p)}{p^s}$$

For $s \to 1^+$ we have

$$\begin{aligned}\sum_{\chi \in \widehat{G}} \chi(a^{-1}) \log(L(\chi, s)) &= -\sum_{\chi \in \widehat{G}} \sum_p \chi(a^{-1}) \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_{\chi, p} \sum_{n \geq 1} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}} \\ &= \varphi(n) \sum_{p \in \mathcal{P}_{a,n}} \frac{1}{p^s} + \sum_{\chi, p} \sum_{n \geq 2} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}}\end{aligned}$$

using the previous identity. The term $\sum_{\chi, p} \sum_{n \geq 2} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}}$ is holomorphic around $s = 1$ by an argument similar to the estimate from the previous section.

We conclude that for $s \to 1^+$ we have

$$\begin{aligned}\varphi(n) \sum_{p \in \mathcal{P}_{a,n}} \frac{1}{p^s} &= \sum_{\chi \in \widehat{G}} \chi(a^{-1}) \log(L(\chi, s)) + O(1) \\ &= \log(L(1, s)) + \sum_{\chi \neq 1} \chi(a^{-1}) \log(L(\chi, s))\end{aligned}$$

Now

$$\log(\zeta(s)) = \log(L(1, s)) - \sum_{p | n} \log\left(1 - \frac{1}{p^s}\right) = \log(L(1, s)) + O(1)$$

around $s = 1$ and so

$$\begin{aligned}\delta(\mathcal{P}_{a,n}) &= \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{P}_{a,n}} p^{-s}}{-\log(s-1)} \\ &= \lim_{s \to 1^+} \frac{\varphi(n)^{-1} \log(\zeta(s)) + \varphi(n)^{-1} \sum_{\chi \neq 1} \log(L(\chi, s)) + O(1)}{-\log(s-1)} \\ &= \lim_{s \to 1^+} \frac{\varphi(n)^{-1} \log(\zeta(s)) + O(1)}{-\log(s-1)} \\ &= \frac{1}{\varphi(n)}\end{aligned}$$

Here we used that for $\chi \neq 1$, $L(\chi, 1) \neq 0$ and so $\log(L(\chi, 1)) = O(1)$.

□

(10.9) The Chebotarëv density theorem.

Let L/K be a finite Galois extension of number fields. Recall that for $\mathfrak{q} \mid \mathfrak{p}$ prime ideals of L and K one has $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G_{L/K}$ well-defined up to an element of inertia $I_{\mathfrak{q}/\mathfrak{p}}$. If $\mathfrak{q}/\mathfrak{p}$ is unramified then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is uniquely defined. Moreover, if $\mathfrak{q}' = \sigma(\mathfrak{q})$ is some other prime ideals above $\mathfrak{p}$ where $\sigma \in G_{L/K}$ then $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma \,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\, \sigma^{-1}$ and so one gets a well-defined conjugacy class

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G_{L/K} | \mathfrak{q} \mid \mathfrak{p}\}$$

Theorem 4 (The Chebotarëv density theorem)**.** *Suppose $C \subset G_{L/K}$ is a conjugacy class. Then the set $\mathcal{P}_C$ of prime ideals $\mathfrak{p}$ of K such that the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ is C has both natural and Dirichlet density*

$$\delta(\mathcal{P}_C) = \frac{|C|}{|G_{L/K}|}$$

Proposition 5. *The Dirichlet theorem on primes in arithmetic progressions is equivalent to Chebotarev for* $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Proof. Indeed, taking $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}$ then $G_{L/K}$ is abelian $\cong (\mathbb{Z}/n\mathbb{Z})^\times$ and so every conjugacy class consists of one element. Taking $C = a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we deduce that the density of primes p such that $\mathrm{Frob}_p = a$ is $1/\varphi(n)$. But Frob_p is $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Proposition 6. *1. If Chebotarev is true for abelian Galois extensions (i.e., where the Galois group is abelian) then it is true for all Galois extensions.*

2. If Chebotarev is true for the abelian Galois extension M/K then it is true for L/K for any $M/L/K$.

Proof. Part one: Let $L^{\mathrm{ab}} \subset L$ be the subfield fixed by the commutator $[G_{L/K}, G_{L/K}] = \{aba^{-1}b^{-1} | a, b \in G_{L/K}\}$. Then L^{ab}/K is abelian and $G_{L^{\mathrm{ab}}/K} \cong G_{L/K}/[G_{L/K}, G_{L/K}] = G_{L/K}^{\mathrm{ab}}$ is the largest abelian quotient of $G_{L/K}$. Moreover, if $C \subset G_{L/K}$ is a conjugacy class with image $c \in G_{L/K}^{\mathrm{ab}}$ then the preimage of c under the projection $G_{L/K} \twoheadrightarrow G_{L/K}^{\mathrm{ab}}$ is C. Finally, if $\mathfrak{p}$ is a prime ideal of K then the image of the conjugacy class $\mathrm{Frob}_\mathfrak{p} \subset G_{L/K}$ in $G_{L/K}^{\mathrm{ab}} \cong G_{L^{\mathrm{ab}},K}$ is the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ since both are lifts of the same map on residue fields.

By Chebotarev for abelian Galois extensions

$$\delta(\{\mathfrak{p} | \operatorname{Frob}_\mathfrak{p} = c\} = \frac{1}{|G_{L/K}^{\mathrm{ab}}|}$$

and so

$$\delta(\{\mathfrak{p} | \operatorname{Frob}_\mathfrak{p} = C\} = \frac{|C|}{|G_{L/K}|}$$

Part two: Let $c \in G_{L/K}$ with preimage $\{c_1, \ldots, c_d\} \subset G_{M/K}$ where $d = [M : L]$. Then

$$\begin{aligned}
\delta(\{\mathfrak{p} | \operatorname{Frob}_\mathfrak{p} = c\}) &= \delta(\{\mathfrak{p} | \operatorname{Frob}_\mathfrak{p} \in \{c_1, \ldots, c_d\}\}) \\
&= \sum \delta(\{\mathfrak{p} | \operatorname{Frob}_\mathfrak{p} = c_i\}) \\
&= \frac{d}{|G_{M/K}|} \\
&= \frac{1}{|G_{L/K}|}
\end{aligned}$$

as desired. □