BASIC NUMBER THEORY: LECTURE 18

WENHAN DAI

We introduce some applications of Čebotarev density theorem.

1. Primes represented by ppdfs

Theorem 1. *Let $f(x,y) = ax^2 + bxy + cy^2$ be a ppdf of discriminant $D < 0$. Let S be the set of all primes represented by f. Then its Dirichlet density*

$$\delta(S) = \begin{cases} \frac{1}{2h(D)} & \text{if } f \text{ is of order} \leqslant 2 \text{ in } C(D), \\ \frac{1}{h(D)} & \text{otherwise.} \end{cases}$$

Proof. Let $\mathcal{O}$ be the order corresponding to D via the isomorphism

$$C(D) \longrightarrow C(\mathcal{O}), \quad f \longmapsto [\mathfrak{a}].$$

Then

$$\begin{aligned} S &\doteq \{p \text{ prime} : p = N(\mathfrak{b}),\ [\mathfrak{b}] = [\mathfrak{a}] \text{ for } \mathcal{O}\text{-ideal } \mathfrak{b}\} \\ &= \{p \text{ prime} : p = N(\mathfrak{b}),\ [\mathfrak{b}] = [\mathfrak{a}\mathcal{O}_K] \text{ for } \mathcal{O}\text{-ideal } \mathfrak{b}\}. \end{aligned}$$

Let f be the conductor of $\mathcal{O}$, then $I_K(f)/P_{K,\mathbb{Z}}(f) \simeq C(\mathcal{O})$. For $K \supseteq \mathcal{O}$ an imaginary quadratic field, and L/K the ring class field of $\mathcal{O}$,

$$\begin{aligned} \varphi : \mathrm{Gal}(L/K) &\xrightarrow{\ \simeq\ } C(\mathcal{O}) \xrightarrow{\ \simeq\ } I_K(f)/P_{K,\mathbb{Z}}(f) \\ \sigma &\longmapsto [\mathfrak{a}\mathcal{O}_K]. \end{aligned}$$

Therefore,

$$\begin{aligned} &\{p \text{ prime} : p = N(\mathfrak{b}),\ [\mathfrak{b}] = [\mathfrak{a}\mathcal{O}_K] \text{ for } \mathcal{O}\text{-ideal } \mathfrak{b}\} \\ &= \{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K : [\mathfrak{p}] = [\mathfrak{a}\mathcal{O}_K]\} \\ &\doteq \left\{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K : \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma\right\}, \end{aligned}$$

where σ is such that $\tau^{-1}\sigma\tau = \sigma^{-1}$, for the complex conjugate τ.

Finally, apply the Čebotarev density theorem to get

$$\delta(S) = \frac{|\langle\sigma\rangle|}{|C(\mathcal{O})| \cdot |\mathrm{Gal}(K/\mathbb{Q})|} = \frac{|\langle\sigma\rangle|}{2h(D)}.$$

Note that f is of order $\leqslant 2$ if and only if $\sigma = \sigma^{-1}$. Hence

$$\delta(S) = \begin{cases} \frac{1}{2h(D)} & \text{if } \sigma = \sigma^{-1}, \\ \frac{1}{h(D)} & \text{otherwise.} \end{cases}$$

□

Date: December 29, 2020.

2. Dirichlet's theorem about primes in arithmetic progression

Let q, ℓ be positive integers such that $(q, \ell) = 1$.

Theorem 2. *There are infinitely many primes of the form $\ell + kq$ for $k \in \mathbb{Z}$.*

We point out that Theorem 2 is equivalent to

Theorem 3. *The following sum diverges:*

$$\sum_{p \equiv \ell \bmod q} \frac{1}{p} = \infty.$$

Here p runs through all prime integers.

For this, we remark that there are two useful identities:

$$\sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}},$$

and

$$\log\left(\prod_p \frac{1}{1-p^{-s}}\right) = -\sum_p \log(1-p^{-s}) = \sum_p p^{-s} + O(1).$$

2.1. Finite Fourier transformation.

For $m \in \mathbb{Z}$, we define

$$\delta_\ell(m) = \begin{cases} 1 & \text{if } m \equiv \ell \bmod q, \\ 0 & \text{otherwise.} \end{cases}$$

(Caution: this is not a character.)

Lemma 4. *Denote χ the Dirichlet character, and χ_0 the trivial character. Then we obtain*

$$\delta_\ell(m) = \frac{1}{\varphi(q)} \sum_{x \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}} \overline{\chi}(\ell)\chi(m).$$

Also,

$$\begin{aligned} \sum_{p \equiv \ell \bmod m} \frac{1}{p^s} = \sum_p \frac{\delta_\ell(p)}{p^s} &= \frac{1}{\varphi(q)} \sum_\chi \overline{\chi}(\ell) \sum_p \frac{\chi(p)}{p^s} \\ &= \frac{1}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi}(\ell) \sum_p \frac{\chi(p)}{p^s}. \end{aligned}$$

Combining these, we see the following Theorem 5 implies Theorem 3.

Theorem 5. *If χ is a nontrivial Dirichlet character, then*

$$\sum_p \frac{\chi(p)}{p^s}$$

is bounded as $s \to 1^+$.

2.2. **Dirichlet L-function.** Let χ be a Dirichlet character. Define

$$L(s,\chi)=\sum_{n=0}^{\infty}\frac{\chi(n)}{n^s}=\prod_{p \text{ prime}}\frac{1}{1-\frac{\chi(p)}{p^s}},\quad s>1.$$

We give some comments on basic properties of $L(s,\chi)$:

- By prime number theorem,

$$\log L(s,\chi)\sim\sum_p\frac{\chi(p)}{p^s}.$$

- Note that if $\chi=\chi_0$, then $L(s,\chi_0)=\zeta(s)$ has a simple pole at $s=1$.
- Consider the Dirichlet character $\chi:(\mathbb{Z}/4\mathbb{Z})^\times\to\{\pm1\}$. It satisfies $\chi(a)=1$ for $a\equiv 1 \bmod 4$ and $\chi(b)=-1$ for $b\equiv -1 \bmod 4$. Also,

$$L(1,\chi)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4}.$$

  For this, we can take $f(x)=1-\frac{x^3}{3}+\frac{x^5}{5}-\cdots$, and then $f'(x)=(1+x^2)^{-1}$. This shows $f(x)=\arctan x$, and $f(1)$ is as desired.

Theorem 6. *If χ is a nontrivial Dirichlet character, then $L(1,\chi)<\infty$, and $L(1,\chi)\neq 0$.*

Note that this implies Theorem 5. So to prove all theorems of this section, it suffices to prove Theorem 6. For $L(1,\chi)<\infty$, it follows from the following lemma.

Lemma 7. *If χ is a nontrivial Dirichlet character, then*

$$\left|\sum_{n=1}^{k}\chi(n)\right|\leqslant q,\quad k\in\mathbb{Z}_{>0}.$$

Proof. Denote $S_k:=\sum_{n=1}^k\chi(n)$. Then $S_q=0$, and

$$\begin{aligned}S_N&=\sum_{k=1}^{N}\frac{\chi(n)}{n^s}=\sum_{k=1}^{N}\frac{S_k-S_{k-1}}{k^s}\\&=\sum_{k=1}^{N-1}\underbrace{S_k\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right)}_{f_k(s)}+\frac{S_N}{N^s}.\end{aligned}$$

We have $|f_k(s)\leqslant q\cdot s\cdot k^{s-1}$. By taking the sum, $L(s,\chi)$ converges if $s>0$. □

The following lemma is for $L(1,\chi)\neq 0$.

Lemma 8. *Whenever $s>1$,*

$$\prod_\chi L(s,\chi)\geqslant 1.$$

Proof. We first compute that

$$\log\left(\prod_\chi L(s,\chi)\right)=\sum_\chi\sum_p\sum_{k=1}^{\infty}\frac{1}{k}\cdot\frac{\chi(p^k)}{p^{ks}}.$$

For this,

$$\sum_{\chi} \frac{1}{k} \cdot \frac{\chi(p^k)}{p^{ks}} = \begin{cases} \frac{\varphi(q)}{p^{ks}}, & p^k \equiv 1 \bmod q, \\ 0, & \text{otherwise.} \end{cases}$$

Hence $\log\left(\prod_{\chi} L(s,\chi)\right) \geqslant 0$, and

$$\prod_{\chi} L(s,\chi) \geqslant 1.$$

□

Proof of Theorem 6. By Lemma 7, it suffices to show $L(1,\chi) \neq 0$ on Lemma 8. Assume χ is a complex character, i.e. $\overline{\chi} \neq \chi$. (The real case would be more complicated.) If $L(1,\chi) = 0$ then $L(1,\overline{\chi}) = 0$. We see $L(s,\chi_0)$ has a simple pole at $s = 1$. Then $\prod_{\chi} L(s,\chi)$ has a zero at $s = 1$. This leads to a contradiction. □

Remark 9 (Idea to prove Čebotarev density theorem). The proof is morally divided into two steps:

(1) Reduce to the case where L/K is abelian.
(2) Note that for some congruence subgroup H of $I_K(\mathfrak{m})$, via the class field theory,

$$I_K(\mathfrak{m})/P_{K,\mathbb{Z}}(\mathfrak{m}) \twoheadrightarrow I_K(\mathfrak{m})/H \simeq \mathrm{Gal}(L/K).$$

Also, we can specialize the case to $K = \mathbb{Q}$ and $L \subseteq \mathbb{Q}(\zeta_n)$ by Kronecker-Weber theorem. In this special case the density theorem is equivalent to Dirichlet's theorem for prime numbers in arithmetic progressions.

Addendum 10 (Dedekind Zeta function)**.** Let K be a number field. Define Dedekind Zeta function as

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

This is a generalization of Riemann Zeta function on $\mathbb{Q}$. When $K = \mathbb{Q}$ we have $\zeta_K = \zeta$ as expected. Moreover, $\zeta_K(s)$ has a simple zero at $s = 1$.

3. Class number

Theorem 11. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K with conductor f. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \cdot f \cdot \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right) \cdot \frac{1}{p}\right).$$

In particular, $h(\mathcal{O}_K) \mid h(\mathcal{O})$.

Recall that $h(d_K) = h(\mathcal{O}_K)$. By Goldfeld and Gross-Zagier,

$$h(d_K) > \frac{\log d_K}{55} \prod_{p \mid d_K,\ p < d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Theorem 12. *Back to the very first theory.*

(1) $h(d_K) = 1$ *if and only if*

$$d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

(2) *Let* $D < 0$ *and* $D \equiv 0, 1 \bmod 4$. *Then* $h(D) = 1$ *if and only if*

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn