

# L-function and Dirichlet's theorem, Dirichlet's three works

$LGO$

September 12, 2024

## Contents

<b>1</b>	<b>Introduction (Ye Tian)</b>	<b>1</b>
<b>2</b>	<b>Dirichlet's L-series and Dirichlet's Theorem</b>	<b>2</b>
2.1	$\text{Res}_{s=1} \zeta_K(s)$ . . . . .	2
2.2	$\zeta_K(s)$ and $L(s, \chi)$ . . . . .	5
2.3	the Proof of Dirichlet's Theorem . . . . .	6
2.4	Supplement: Two Direct Ways to Get $\prod_{\chi \neq \chi_0} L(1, \chi) \neq 0$ . . . . .	9
2.4.1	A similar structure of $\zeta_K(s)$ . . . . .	10
2.4.2	A similar proof of $\zeta(1 + i\mathbb{R}) \neq 0$ . . . . .	10
2.5	Why we consider primitive characters . . . . .	11
<b>3</b>	<b>Special Value Formula of L-function</b>	<b>12</b>
3.1	the Gauss Sum $\tau(\chi)$ . . . . .	12
3.2	Clear Form of $L(1, \chi)$ . . . . .	12
<b>4</b>	<b>Class Number Formula for Quadratic Fields</b>	<b>13</b>
<b>5</b>	<b>A Brief (and Naive) Introduction to p-adic L Function</b>	<b>17</b>

# 1 Introduction (Ye Tian)

Three fundamental results of Dirichlet have far-reaching influence. To establish the first one, Dirichlet was led to study the later two ones. Gauss' work on cyclotomy. After he visited Dirichlet, Riemann (1859) did the great work on Riemann zeta function and PNT. Of course, Euler's work on zeta function has influence on Dirichlet L-function.

**Theorem 1.1** (Dirichlet's prime theorem, 1837). *Let  $a, N$  be two coprime integers, then there are infinitely many primes  $p \equiv a \pmod{N}$ .*

**Theorem 1.2** (Special value formula). *Let  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  be a primitive Dirichlet character with conductor  $N > 1$ . Let  $\tau(\chi) = \sum \chi(a)e^{2\pi ia/N}$  be a Gauss sum. Then*

$$L(1, \chi) = \begin{cases} \frac{\pi\tau(\chi)}{N}B_{1,\bar{\chi}}, & \text{if } \chi(-1) = -1, \text{ where } B_{1,\bar{\chi}} = \frac{i}{N} \sum_{a=1}^N \bar{\chi}(a)a, \\ -\frac{\tau(\chi)}{N} \sum_{a=1}^N \bar{\chi}(a) \log |1 - \zeta_N^a|, & \text{if } \chi(-1) = 1, \chi \neq 1. \end{cases}$$

Let  $D$  be a fundamental discriminant of quadratic field with  $|D|$  a prime, then  $L(1, \chi_D) \neq 0$  from Gauss' work on cyclotomy.

**Theorem 1.3** (Class number formula, 1839-1840). *Let  $\chi = \left(\frac{D}{\cdot}\right)$  be the quadratic Dirichlet character associated to a quadratic field  $K = \mathbb{Q}(\sqrt{D})$  with discriminant  $D$ . Let  $h_D$  be the ideal class number of  $K$  and  $\epsilon_D > 1$  the fundamental unit when  $D > 0$ . Then*

$$L(1, \chi_D) = \begin{cases} \frac{2\pi h_D}{w_D \sqrt{|D|}}, & \text{if } \chi(-1) = -1, \\ \frac{2h_D \log |\epsilon_D|}{\sqrt{|D|}}, & \text{if } \chi(-1) = 1, \chi \neq 1. \end{cases}$$

In particular,  $L(1, \chi_D) > 0$ .

**Remark 1.4** (Some reflections on this note).

Just as  $\lim_{s \rightarrow 1^+} \frac{1}{n^s} = \infty$  implies that the number of primes is infy and even the reciprocal sum of all prime numbers is infy,  $L(1, \chi) \neq 0$  when  $\chi$  is not trivial implies that the Dirichlet prime theorem.

The value of  $\zeta(s)$ , or generally, the Dirichlet L-function at special point contains important things in number theory, which we can feel in Dirichlet three works. And we can define different "Riemann zeta functions" for different algebraic objects, each of them integrates a lot of information.

## 2 Dirichlet's L-series and Dirichlet's Theorem

A Dirichlet module  $N$  character is a group homomorphism  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  for some  $N \geq 1$ . We say  $\chi$  is primitive if it can not be induced by any characters of  $(\mathbb{Z}/d\mathbb{Z})^\times$  for  $d \mid N, d \neq N$ , and write the conductor of  $\chi$  is  $f_\chi = N$ . We say  $\chi$  is trivial if  $\chi \equiv 1$  on  $(\mathbb{Z}/N\mathbb{Z})^\times$ , and denoted by  $\chi_0$ . Note that  $\chi$  can be defined on  $\mathbb{Z}$  by setting  $\chi(d) = 0$  if  $\gcd(d, N) > 1$ .

And for Dirichlet module  $N$  character  $\chi$ ,  $\chi$  is induced by a certain Dirichlet module  $f_\chi$  ( $f_\chi \mid N$ ) which is uniquely determined. We denote the latter is  $\chi^*$ .

We put the Dirichlet's L-series:

$$L(s, \chi) = \sum_{n=0}^{+\infty} \frac{\chi(n)}{n^s}$$

As a simple example,  $L(s, \chi_0) = \zeta(s) \prod_{p \mid N} (1 - p^{-s})$  and  $L(s, \chi_0^*) = \zeta(s)$ . Actually we have

$$L(s, \chi) = L(s, \chi^*) \cdot \prod_{p \mid N} (1 - \chi^*(p)p^{-s})$$

which implies that we only need to focus on the primitive Dirichlet characters.

**Fact 2.1.** (i)  $L(s, \chi)$  is absolutely convergence if  $\Re(s) > 1$ , and at this time we have the Euler product:  $L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$ .

(ii) If  $\chi \neq \chi_0$ ,  $L(s, \chi)$  can be analytically extended to a holomorphic function on  $\Re(s) > 0$ .

*Proof.* Actually, (i) comes from  $|L(s, \chi)| \leq \zeta(\Re(s))$  and  $\chi$  is completely multiplicative, (ii) comes from  $\sum_{n \leq t} \chi(n) = O(1)$  when  $t \rightarrow +\infty$  and Remark 2.6.  $\square$

Now we start to proof the Dirichlet's prime theorem. The essential part of the proof is  $L(1, \chi)$  is nonvanishing if  $\chi \neq \chi_0$ . To get this, We need the relation between the Dedekind zeta function  $\zeta_K(s) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$  and  $L(s, \chi)$ , and the residue of  $\zeta_K(s)$  at  $s = 1$ . Moreover, We will give a different method to get the essential part in Section 2.4.

### 2.1 $\text{Res}_{s=1} \zeta_K(s)$

**Lemma 2.2.**  $\zeta_K(s)$  is absolutely convergence if  $\Re(s) > 1$ , and at this time we have the Euler product:  $\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$ .

*Proof.* We just need to consider  $s > 1$  and note that  $N(\mathfrak{p})^{-s} \leq \frac{1}{2}$ , thus  $1 + N(\mathfrak{p})^{-s} < \frac{1}{1 - N(\mathfrak{p})^{-s}} \leq 1 + 2N(\mathfrak{p})^{-s}$ . Then  $\sum_{\mathfrak{p}} (\frac{1}{1 - N(\mathfrak{p})^{-s}} - 1) \leq 2[K : \mathbb{Q}] \sum_{\mathfrak{p}} p^{-s} \leq 2[K : \mathbb{Q}] \sum_n n^{-s}$  is absolutely

convergence. And for a positive series  $a_n$ , we have  $\prod_{n=1}^{\infty} (1 + a_n)$  is absolutely convergence iff  $\sum_{n=1}^{\infty} a_n$  is absolutely convergence, because  $\exp(\sum_{n=1}^{\infty} a_n) \geq \prod_{n=1}^{\infty} (1 + a_n) \geq \sum_{n=1}^{\infty} a_n$ .

Hence  $\prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$  is absolutely convergence and the lemma follows the fact that

$$\prod_{N(\mathfrak{p}) \leq m} \frac{1}{1 - N(\mathfrak{p})^{-s}} = 1 + \sum_{\substack{\mathfrak{a} \in \mathcal{O}_K, N(\mathfrak{p}) \leq m \\ \text{for any } \mathfrak{p} | \mathfrak{a}}} \frac{1}{N(\mathfrak{a})^s}$$

□

To calculate  $\text{Res}_{s=1} \zeta_K(s)$ , we need the following theorem:

**Theorem 2.3.** *Let  $K$  be a number field of degree  $n$  with  $r_1$  real embeddings and  $r_2$  complex embeddings. For a fixed ideal class  $C \in \text{Cl}(K)$  and a number  $t > 0$ , let  $N_C(t) = \#\{\mathfrak{a} \in \mathcal{O}_K \mid N(\mathfrak{a}) \leq t, [\mathfrak{a}] \in C\}$ , we have*

$$N_C(t) = \frac{2^{r_1} (2\pi)^{r_2} R_K}{\omega_K \sqrt{|\Delta_K|}} t + O(t^{1-\frac{1}{n}})$$

where  $\omega_K$  is the number of roots of unity in  $K$ <sup>1</sup>,  $\Delta_K$  is the discriminant of  $K$  and  $R_K$  is the regulator of  $K$ .

**Remark 2.4** (The regulator  $R_K$  of  $K$ ).

Take a fundamental system  $\{u_1, \dots, u_{r_1+r_2-1}\}$  of the unit group  $U_K$  and  $\vec{n} = \frac{1}{r_1+r_2}(1, \dots, 1)$ . Define the map  $\ell$ :

$$\ell : U_K \rightarrow \mathbb{R}^{\times, r_1} \times \mathbb{C}^{\times, r_2} \rightarrow \mathbb{R}^{r_1+r_2}$$

$$x \mapsto (\sigma_i(x))_{r_1+r_2} \mapsto (\log |\sigma_1(x)|, \dots, \log |\sigma_{r_1}(x)|, 2 \log |\sigma_{r_1+1}(x)|, \dots, 2 \log |\sigma_{r_1+r_2}(x)|)$$

Then  $\{\vec{n}, \ell(u_1), \dots, \ell(u_{r_1+r_2-1})\}$  form a basis of  $\mathbb{R}^{r_1+r_2}$ , we define:

$$R_K = |\det(\vec{n}, \ell(u_1), \dots, \ell(u_{r_1+r_2-1}))|$$

Actually,  $\vec{n}$  can be replaced by any vector in  $\mathbb{R}^{r_1+r_2}$  whose components sum up to 1. Regulator measures the density of the group of units: In particular, if the regulator is "small", then there are "lots" of units.

**Proposition 2.5.**  $\zeta_K(s)$  has a meromorphic continuation to  $\Re(s) > 1 - \frac{1}{n}$  with a simple pole at  $s = 1$  and the residue is

$$\kappa := \frac{2^{r_1} (2\pi)^{r_2} R_K}{\omega_K \sqrt{|\Delta_K|}} \cdot h$$

here  $h$  is the class number of  $K$ .

---

<sup>1</sup>the torsion group  $W_K \subset \mathcal{O}_K^\times$  is the group of roots of unity contained in  $K$ , and is a finite cyclic group. As for quadratic fields, we have  $\omega_K = \#W_K = 2$  except  $W_{\mathbb{Q}(\sqrt{-1})} = \langle i \rangle$  and  $W_{\mathbb{Q}(\sqrt{-3})} = \langle \zeta_6 \rangle$ .

*Proof.* By Theorem 2.3, we have  $S_t := \sum_{n \leq t} a_n = \kappa t + O(t^{1-\frac{1}{n}})$  when  $t \rightarrow \infty$ , here  $a_n = \#\{\mathfrak{a} \subset \mathcal{O}_K \mid N(\mathfrak{a}) = n\}$ .

And we put  $g(s) = \zeta_K(s) - \kappa \zeta(s)$  and  $S'_t = \sum_{n \leq t} (a_n - \kappa) = O(t^{1-\frac{1}{n}})$ , we only need to show  $g(s)$  has an analytic continuation to a holomorphic function on  $\Re(s) > 1 - \frac{1}{n} =: 1 - \delta$ . However

$$g(s) = \sum_{n=1}^{\infty} S'_n \left( \frac{1}{n^s} - \frac{1}{(n+1)^s} \right) = \sum_{n=1}^{\infty} S'_n \int_n^{n+1} st^{-s-1} dt$$

so

$$|g(s)| \leq C|s| \sum_{n=1}^{\infty} n^{1-\delta} \int_n^{n+1} t^{-\Re(s)-1} dt \leq C|s| \int_1^{\infty} t^{-\Re(s)-\delta} dt = \frac{C|s|}{\Re(s) + \delta - 1}$$

□

**Remark 2.6.** By the same calculate, we see for  $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$  with  $\sum_{n \leq t} a_n = \kappa t + O(t^{1-\delta})$ ,  $\kappa \in \mathbb{C}$ ,  $0 < \delta \leq 1$ . Then  $f(s)$  can be analytically extended to a meromorphic function on  $\Re(s) > 1 - \delta$  with at most a simple pole at  $s = 1$  with residue  $\kappa$ .

**Corollary 2.7.** Let  $K$  be a number field, then we have

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} \sim \log \frac{1}{s-1} \quad \text{when } s \rightarrow 1^+$$

*Proof.* It follows that:

$$\log \frac{1}{s-1} \sim \log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n N(\mathfrak{p})^{ns}} = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} + \underbrace{\sum_{n \geq 2} \frac{1}{n N(\mathfrak{p})^{ns}}}_{\text{bounded}}$$

□

**Remark 2.8** (The order of  $\zeta_K(s)$  at  $s = 0$ ).

We have

$$\lim_{s \rightarrow 0} s^{-(r_1+r_2-1)} \zeta_K(s) = -\frac{hR_K}{\omega_K}$$

Actually, if we define the complete Dedekind  $\zeta$  function as

$$\widehat{\zeta}_K(s) = |\Delta_K|^{\frac{s}{2}} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_K(s)$$

where  $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2})$  and  $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s)$ , then we have a more brief formula including Proposition 2.5:

$$\lim_{s \rightarrow 1} (s-1) \widehat{\zeta}_K(s) = \lim_{s \rightarrow 0} -s \widehat{\zeta}_K(s) = \frac{2^{r_1+r_2} h R_K}{\omega_K}$$

## 2.2 $\zeta_K(s)$ and $L(s, \chi)$

Let  $K/\mathbb{Q}$  is Abelian extension with Galois group  $G$ , and  $K \subset \mathbb{Q}(\zeta_N)$ .  $\widehat{K} := \widehat{G}$  can be identified with the set of Dirichlet character mod  $N$  which are trivial on  $\text{Gal}(\mathbb{Q}(\zeta_N)/K)$ . We note that the mapping of a  $K/\mathbb{Q}$  to its characteristic group  $\widehat{G}$  maintains the order of the inclusion relationship. Here we consider  $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$  and  $(\mathbb{Z}/N\mathbb{Z})^\times$  as equivalent.

The decomposition of  $N = \prod_{i=1}^n p_i^{e_i}$  induces the decomposition of  $\chi = \chi_{p_1} \cdots \chi_{p_n}$  where  $\chi_{p_i}$  is the character mod  $p_i^{e_i}$ . We denote

$$\widehat{K}_p = \{\chi_p \mid \chi \in \widehat{K}\} \quad Y = \{\chi \in \widehat{K} \mid \chi^*(p) \neq 0\} \quad Z = \{\chi \in Y \mid \chi^*(p) = 1\}$$

Clearly  $\widehat{K}_p, Y, Z$  is group. Let  $[K : \mathbb{Q}] = efg$ , where  $e$  is the ramification index of  $p$ ,  $f$  is the extension degree of residue field of  $\mathbb{F}_p$  and  $g$  is the number of  $\{p|p\}$ , we have the following lemma.

**Lemma 2.9.** (1)  $e = |\widehat{K}_p|$  and  $p$  ramified in  $K \iff \exists \chi \in \widehat{K}$  s.t.  $\chi^*(p) = 0$ .

(2)  $Y, Z$  are the characteristic groups of the inertia field  $K_I$  and decomposition field  $K_D$  of  $p$  with respect to  $K$  respectively.

*Proof.* (1) Let  $N = p^l n$  with  $(p, n) = 1, l \geq 0$ . We denote  $L = K(\zeta_n)$  and then  $\widehat{L} = \langle (\mathbb{Z}/n\mathbb{Z})^\times, \widehat{K} \rangle = (\mathbb{Z}/n\mathbb{Z})^\times \oplus \widehat{K}_p$ . Let  $F$  be the field corresponding to  $\widehat{K}_p$  and then  $F \subset \mathbb{Q}(\zeta_{p^l}), L = \mathbb{Q}(\zeta_n)F$ . Thus we have

$$e = e(K) = e(L) = e(F) = [F : \mathbb{Q}] = |\widehat{F}| = |\widehat{K}_p|$$

and then  $p$  ramified in  $K \iff e > 1 \iff \exists \chi \in \widehat{K}$  s.t.  $\chi_p \neq \chi_0 \iff \exists \chi \in \widehat{K}$  s.t.  $\chi^*(p) = 0$ .

(2) From (1) we see  $Y$  corresponds to the maximal unramified subfield of  $p$  in  $K$ , i.e.  $Y = \widehat{K}_I$ . And for each  $\chi \in Y$ , we note  $f_\chi \mid n$  then there has a unique  $\chi' \in (\mathbb{Z}/n\mathbb{Z})^\times$  s.t.  $(\chi')^* = \chi$  and  $\mathbb{Q} \subset K_D \subset K_I \subset \mathbb{Q}(\zeta_n)$ . Denote  $D, I \subset (\mathbb{Z}/n\mathbb{Z})^\times$  are Galois group correspond to  $K_D, K_I$  respectively.

$$\chi' \in \text{Gal}(\widehat{K_D}/\mathbb{Q}) \iff \chi(D/I) = 1 \iff \chi'(p) = 1 \iff \chi \in Z$$

Hence  $\widehat{K_D} = Z$ . □

The relationship between  $\zeta_K(s)$  and  $L(s, \chi)$  is described in the following proposition.

**Proposition 2.10.** For every abelian number field  $K$ , the Dedekind zeta function is the product of Dirichlet  $L$  functions with primitive character. Namely,

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(s, \chi^*)$$

*Proof.* By the Euler product of  $\zeta_K(s)$  and  $L(s, \chi)$ , it suffices to show

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = \prod_{\chi} (1 - \chi^*(p)p^{-s})$$

On the left side, we have

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = (1 - p^{-fs})^g$$

On the right side (with same notation in Lemma 2.9),

$$\prod_{\chi} (1 - \chi^*(p)p^{-s}) = \prod_{\chi \in Y} (1 - \chi^*(p)p^{-s}) = \prod_{\chi \in Y/Z} (1 - \chi^*(p)p^{-s})^g = (1 - p^{-fs})^g$$

□

**Corollary 2.11** (The nonvanishing of  $L(1, \chi)$  if  $\chi \neq \chi_0$ ).

$$\prod_{\chi \neq \chi_0} L(1, \chi^*) = \frac{2^{r_1} (2\pi)^{r_2} R_K}{\omega_K \sqrt{|\Delta_K|}} \cdot h$$

In particular,  $L(1, \chi) \neq 0$  if  $\chi \neq \chi_0$ .

By using Proposition 2.10 and the function equation of  $L(s, \chi)$ ,  $\zeta_K(s)$ , we can deduce a simple but Interesting relation:

**Corollary 2.12** (Hasse Discriminant-Conductor Formula). *Let  $K$  is an abelian field, then*

$$\prod_{\chi \in \widehat{K}} f_{\chi} = |\Delta_K|$$

*Proof.* Roughly speaking, let  $\Phi$  be the symbol of the extended function equation. We have

$$\left| \frac{\Phi_K(s)}{\prod_{\chi \in \widehat{K}} \Phi(s, \chi)} \right| = \left| \frac{\Delta_K}{\prod_{\chi} f_{\chi}} \right|^{\frac{s}{2}}$$

remaining unchanged when  $s \rightarrow 1 - s$ . The conclusion is drawn. □

## 2.3 the Proof of Dirichlet's Theorem

**Theorem 2.13** (Dirichlet, 1837). *Let  $a, N$  be two coprime integers, then there are infinitely many primes  $p \equiv a \pmod{N}$ .*

*Proof.* We use the orthogonality of characters to extract " $p \equiv a \pmod{N}$ ":

$$\begin{aligned} \sum_{\chi} \bar{\chi}(a) \log L(s, \chi) &= \sum_{\chi} \bar{\chi}(a) \left( \sum_p \sum_{m \geq 1} \frac{\chi(p^m)}{mp^{ms}} \right) \\ &= \varphi(N) \sum_{p \equiv a \pmod{N}} \frac{1}{p^s} + \varphi(N) \sum_{m \geq 2} \left( \sum_{p^m \equiv a \pmod{N}} \frac{1}{mp^{ms}} \right) \text{ for } \Re(s) > 1 \end{aligned}$$

And

$$\sum_{m \geq 2} \left( \sum_{p^m \equiv a \pmod{N}} \frac{1}{mp^{ms}} \right) \leq \sum_p \sum_{m \geq 2} \frac{1}{p^{ms}} \leq \sum_n \frac{1}{n^s(n-1)} < \infty \quad \text{for } \Re(s) > \frac{1}{2}$$

On the left side,

$$L(s, \chi_0) = \zeta(s) \prod_{p|N} (1 - p^{-s}) \sim \frac{1}{s-1} \quad (\text{when } s \rightarrow 1), \quad \prod_{\chi \neq \chi_0} L(1, \chi) \neq 0$$

Hence we have :

$$\sum_{p \equiv a \pmod{N}} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log \frac{1}{s-1} \quad (\text{when } s \rightarrow 1)$$

□

**Remark 2.14** (A more precise form).

*By the Mertens's Second Theorem:*

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + B_1 + O\left(\frac{1}{\log x}\right)$$

*And the Siegel-Walfisz theorem:*

$$\lim_{x \rightarrow \infty} \frac{\#\{p \mid p \leq x \text{ and } p \equiv a \pmod{N}\}}{x} = \frac{1}{\varphi(N)}$$

*We can deduce that:*

$$\sum_{p \leq x, p \equiv a \pmod{N}} \frac{1}{p} = \frac{1}{\varphi(N)} \log \log x + O(1)$$

**Remark 2.15** (The natural density and the Dirichlet density).

*For a subset  $T$  of all prime ideals, we say  $T$  has a Dirichlet density (if exists) :*

$$\rho_D = \lim_{s \rightarrow 1^+} \sum_{\mathfrak{p} \in T} \frac{1}{N\mathfrak{p}^s} / \log \frac{1}{s-1}$$

*and has a (natural) density (if exists):*

$$\rho = \lim_{x \rightarrow \infty} \frac{\#\{\mathfrak{p} \mid N\mathfrak{p} \leq x, \mathfrak{p} \in T\}}{\#\{\mathfrak{p} \mid N\mathfrak{p} \leq x\}}$$

*Generally, if  $\rho$  exists,  $\rho_D$  must exist and equal to  $\rho$ . But if  $\rho_D$  exists,  $\rho$  may do not exist at all<sup>2</sup>.*

*We point out that there is also the concept of logarithmic density<sup>3</sup>, and natural density implies logarithmic density. The later implies Dirichlet.*

<sup>2</sup>The set of positive integers whose decimal expansion starts with digit  $d$  (no leading zeros) has Dirichlet density  $\frac{\ln(d+1) - \ln d}{\ln 10}$ , but no natural density. If we want a example about a set of primes, it suffices to just apply the prime number theorem, we see that the computation is the similar.

<sup>3</sup>See <https://math.stackexchange.com/questions/444419/dirichlet-vs-logarithmic-density>



**Remark 2.16** (generalization: Tchebotarev density theorem).

Let  $K/k$  be Galois with group  $G$ , Let  $\sigma \in G$  and  $C$  be the number of elements in the conjugacy class of  $\sigma$  in  $G$ . Then those primes  $\mathfrak{p}$  of  $k$  which are unramified in  $K$  and for which there exists  $\mathfrak{P}|\mathfrak{p}$  such that  $\sigma = \left(\frac{K/k}{\mathfrak{P}}\right)$  has a density and the density is equal to  $C/[K : k]$ .

If we take  $K/k = \mathbb{Q}(\zeta_N)/\mathbb{Q}$  and  $\sigma = \sigma_a$  with  $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ , this theorem is equivalent to Dirichlet's theorem.

**Remark 2.17** (Analogy: Theorem in the case  $K = \mathbb{F}_p(T)$ ).

As global fields,  $\mathbb{Q}$  and  $\mathbb{F}_p(T)$  has many similar properties. Kornblum consider the following corresponding:

$$\mathbb{F}_p[T] \sim \mathbb{Z} \quad \text{Monic Poly} \sim \mathbb{N} \quad \text{Norm } N(h) = p^{\deg h} \sim N(p) = |p|$$

And consider

$$\zeta_{\mathbb{F}_p[T]}(s) = \prod_{h: \text{monic \& irred}} \frac{1}{1 - N(h)^{-s}} \sim \zeta(s)$$

then (Kornblum)

$$(1) \quad \zeta_{\mathbb{F}_p[T]}(s) = \sum_{f \in \mathbb{F}_p[T] \text{ \& monic}} N(f)^{-s} = \sum_{k=0}^{\infty} \frac{p^k}{p^{ks}} = \frac{1}{1 - p^{1-s}}$$

(2) (Analogy of Dirichlet theorem) If  $a(T), b(T) \in \mathbb{F}_p[T]$  are coprime and nonzero, then there exist infinitely many monic and irreducible polynomials  $h(T)$  s.t.

$$h(T) \equiv b(T) \pmod{a(T)}$$

The proof is similar .

**Remark 2.18** (The Hasse  $\zeta$  function).

It is worth mentioning that we can define  $\zeta$  function on ring  $A$  which is finitely generated on  $\mathbb{Z}$  (more generally, on scheme) , called Hasse  $\zeta$  function:

$$\zeta_A^{\text{Hasse}}(s) := \prod_{\text{maximal ideal } \mathfrak{m} \subset A} \frac{1}{1 - \#(A/\mathfrak{m})^{-s}}$$

And it is easy to see

$$\zeta_{\mathbb{Z}}^{\text{Hasse}}(s) = \zeta(s) \quad \zeta_{\mathbb{F}_p[T]}^{\text{Hasse}}(s) = \zeta_{\mathbb{F}_p[T]}(s) \quad \zeta_{\mathcal{O}_K}^{\text{Hasse}}(s) = \zeta_K(s)$$

**Remark 2.19** (Regarding the least prime in an arithmetic progression).

Dirichlet prime theorem does not predict the gap (or the distribution) in those primes. However, regarding the least prime in an arithmetic progression, Linnik proved a remarkable theorem<sup>4</sup> :

---

<sup>4</sup>This remark refers to:

(i) <https://personal.math.ubc.ca/gerg/teaching/613-Winter2011/LinnikTheorem.pdf> ;

(ii) Barthel, J., & Müller, V. (2022). A Conjecture on Primes in Arithmetic Progressions and Geometric Intervals. The American Mathematical Monthly, 129(10), 979–983.

**Linnik's Theorem (1944):** *There exists an effectively computable and absolute constant  $L > 0$  s.t.*

$$\min\{p : p \text{ prime}, p \equiv a \pmod{N}\} \ll N^L$$

Now the best result is  $L = 5$ , and under GRH one may conclude that any constant  $L > 2$  is admissible (More precisely, the prime we want is less than  $(\varphi(N) \log N)^2$ ).

**Remark 2.20** (A generalization conjecture: Bunyakovsky Conjecture ).

It was stated in 1857 by the Russian mathematician Viktor Bunyakovsky. For a polynomial  $f(x) \in \mathbb{Z}[x]$ , we say it satisfies the “Bunyakovsky conditions” if  $f(x)$  is nonconstant, irreducible, and has no fixed prime divisor (i.e. for each prime  $p$  there is an integer  $n$  s.t.  $p \nmid f(n)$ ). The conjecture states then  $|f(n)|$  is prime for infinite many  $n \in \mathbb{Z}$ .

This conjecture covers many important issues. However, to date, the only case of Bunyakovsky's conjecture that has been proved is that of polynomials of degree 1 which is exactly the Dirichlet's theorem.

## 2.4 Supplement: Two Direct Ways to Get $\prod_{\chi \neq \chi_0} L(1, \chi) \neq 0$

Two methods will use a common key Lemma, which says:

**Lemma 2.21** (Laudau). *Let  $a_n \geq 0$  and  $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$  converges for  $\Re(s) > s_0 \in \mathbb{R}$ , and it extends analytically to an analytic function in a neighborhood around the point  $s_0$ . Then there is an  $\varepsilon > 0$  s.t. the series  $f(s)$  converges for  $\Re(s) > s_0 - \varepsilon$ .*

*Proof.* Without loss of generality, we assume  $s_0 = 0$ .  $f(s)$  is analytic in the  $\{s \mid |s - 1| \leq 1 + \varepsilon\}$  for some  $\varepsilon > 0$ . And in this disk, we give  $f(s)$  the Taylor series around  $s = 1$  and substitutes  $-\varepsilon$ :

$$\begin{aligned} f^{(k)}(1) &= \sum_{n=1}^{\infty} \frac{a_n (-\log n)^k}{n} \\ \Rightarrow f(-\varepsilon) &= \sum_{k=1}^{\infty} \frac{f^{(k)}(1)}{k!} (-\varepsilon - 1)^k = \sum_n \sum_k \frac{a_n}{k!} \cdot \frac{(1 + \varepsilon)^k (\log n)^k}{n} \\ &= \sum_n \frac{a_n \exp[(1 + \varepsilon) \log n]}{n} = \sum_n a_n n^\varepsilon \end{aligned}$$

which shows that the series converges for  $s = -\varepsilon$ .

We claim that if Dirichlet series converges for a particular  $s = s_0$ , then it converges uniformly on the open halfplane  $\Re(s) > \Re(s_0)$ , and furthermore, the sum is analytic in this region. Hence the key Lemma is drawn.

Let  $u_n = \frac{a_n}{n^{s_0}}, v_n = \frac{1}{n^{s-s_0}}, U_n = \sum_{k=1}^n u_k \rightarrow U$ , then

$$\begin{aligned} |v_n - v_{n+1}| &\leq \frac{|s - s_0|}{n^{1+\Re(s-s_0)}} \\ \Rightarrow |\sum u_n v_n| &\leq \sum |U_n| |v_n - v_{n+1}| \leq U \sum \frac{|s - s_0|}{n^{1+\Re(s-s_0)}} \end{aligned}$$

This last expression converges uniformly when  $\Re(s - s_0) > 0$ . The analyticity of the sum follows from the analyticity of each term in the halfplane. □

### 2.4.1 A similar structure of $\zeta_K(s)$

We define  $\zeta_N(s) := \prod_{\chi} L(s, \chi)$ , and we see that  $L(s, \chi_0)$  has a simple pole at  $s = 1$  and all other  $L(s, \chi)$  are analytical for  $\Re(s) > 0$  (See Fact2.1).

Note that  $\chi$  is not necessarily be primitive and  $\zeta_N(s) = \prod_{p \nmid N} (1 - p^{-f(p)s})^{-g(p)}$ , which implies  $\zeta_N(s)$  is a Dirichlet series with positive coefficients.

However, for  $\Re(s) > 1$

$$\zeta_N(s) \geq \prod_{p \nmid N} (1 + p^{-f(p)g(p)s} + p^{-f(p)g(p)2s} + \dots) = \prod_{p \nmid N} \frac{1}{1 - p^{-\varphi(N)s}} = \sum_{\gcd(n, N)=1} \frac{1}{n^{\varphi(N)s}}$$

If there exist some  $L(s, \chi)$  with  $\chi \neq \chi_0$  s.t.  $L(1, \chi) = 0$ , then  $\zeta_N(s)$  would be holomorphic on  $\Re(s) > 0$ . By the Lemma 2.21, the series  $\zeta_N(s)$  should converge for  $\Re(s) > 0$ , but  $\sum_{\gcd(n, N)=1} \frac{1}{n^{\varphi(N)s}}$  only converges for  $\Re(s) > \frac{1}{\varphi(N)}$ , a contradiction.

### 2.4.2 A similar proof of $\zeta(1 + i\mathbb{R}) \neq 0$

Let  $\sigma > 1, s = \sigma + it$ , then

$$\begin{aligned} \log L(s, \chi) &= \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m}{mp^{ms}} \\ \zeta^3(\sigma) L^4(s, \chi) L(\sigma + 2it, \chi^2) &= \exp \left[ \sum_p \sum_{m=1}^{\infty} \frac{3 + 4(\chi(p)p^{-it})^m + (\chi(p)p^{it})^{2m}}{mp^{m\sigma}} \right] \end{aligned}$$

since  $|\chi(p)p^{-it}| = 1$ , let  $|\chi(p)p^{-it}| = e^{i\theta}$ , then

$$\Re [3 + 4(\chi(p)p^{-it})^m + (\chi(p)p^{it})^{2m}] = 2(\cos m\theta + 1)^2 \geq 0$$

which tells us  $|\zeta^3(\sigma) L^4(s, \chi) L(\sigma + 2it, \chi^2)| \geq 1$ .

If  $t \neq 0$  or  $t = 0$  but  $\chi^2 \neq \chi_0$ , then  $L(1 + 2it, \chi^2) \neq \infty$ , so  $L(1 + it, \chi) \neq 0$ .

If  $t = 0$  and  $\chi^2 = \chi_0$ , then

$$\begin{aligned}\zeta(s)L(s, \chi) &= \prod_{\chi(p)=0} (1 + p^{-s} + p^{-2s} + \dots) \prod_{\chi(p)=1} (1 + 2p^{-s} + 3p^{-2s} + \dots) \prod_{\chi(p)=-1} (1 + p^{-2s} + p^{-4s} + \dots) \\ &=: \sum_{n=1}^{\infty} \frac{\rho(n)}{n^s}\end{aligned}$$

We see that  $\rho(n) \geq 0$  and  $\rho(n^2) \geq 1$ . If  $L(1, \chi) = 0$ ,  $\zeta(s)L(s, \chi)$  would be analytic on  $\Re(s) > 0$ , and by the Lemma 2.21,  $\sum \frac{\rho(n)}{n^s}$  would converge on  $\Re(s) > 0$ . However

$$\sum_{n=1}^{\infty} \frac{\rho(n)}{n^{\frac{1}{2}}} \geq \sum_{n=1}^{\infty} \frac{\rho(n^2)}{n} \geq \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

a contradiction.

## 2.5 Why we consider primitive characters

As we have seen, there are some subtle differences in whether  $\chi$  is primitive. In this note, we have made a detailed distinction to avoid confusion. But in this subsection I would like to explain from the perspective of Galois representation why only the primitive case needs to be considered, as is the default in most textbooks.

As we all know, each complex Galois representation  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\mathbb{C})$  factors through  $\mathrm{Gal}(K/\mathbb{Q})$  for some finite Galois extension  $K/\mathbb{Q}$ , by considering the differences of the topology of the two groups (NSS, no small subgroup condition). And let  $L/K$  be Galois,  $\rho : \mathrm{Gal}(L/K) \rightarrow \mathrm{GL}(V)$  for some  $n$  dimensional vector space  $V$  over  $\mathbb{C}$ . We define the local and global Artin L-function:  $L_{\mathfrak{p}}(\rho, T)$ ,  $L(\rho, s)$  as follows

$$L_{\mathfrak{p}}(\rho, T) = \det(1 - \rho^{I_{\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}})T)^{-1} \quad L(\rho, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\rho, N(\mathfrak{p})^{-s})$$

where  $\rho^{I_{\mathfrak{p}}}$  is the representation of  $\mathrm{Gal}(L/K)$  on the subspace of  $V$  fixed by some inertia group  $I_{\mathfrak{p}}$  of  $\mathfrak{p} \in \mathcal{O}_K$  and  $\mathfrak{P} \in \mathcal{O}_L$  over  $\mathfrak{p}$  (You may check two things: one is the  $\rho^{I_{\mathfrak{p}}}$  is unramified at  $\mathfrak{p}$ , the other is the definition of  $L_{\mathfrak{p}}(\rho, T)$  is independent on the choice of  $\mathfrak{P}$ ).

Now let  $\chi$  be a Dirichlet character module  $N$ , then we can define a representation  $\rho_{\chi}$  by considering

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\chi} \mathrm{GL}_1(\mathbb{C})$$

and if we want  $L(\rho_{\chi}, s) = L(\chi, s)$ ,  $\chi$  must be primitive. Then we have a bijection between the set of primitive Dirichlet characters and the set of 1-dimensional complex Galois representations which keep same  $L$ -function.

### 3 Sepcial Value Formula of L-function

#### 3.1 the Gauss Sum $\tau(\chi)$

In this section , we assume  $\chi$  is primitive with conductor  $N \geq 2$  (so  $\chi \neq \chi_0$ ), and denote  $\zeta = \zeta_N$  when there is no ambiguity. Our goal is to compute  $L(1, \chi)$  finely.

$\sum \chi(n)/n^s$  difficult to handle, but a equation of Gauss sum could translate it to  $\sum \zeta^{an}/n^s$ :

**Lemma 3.1.**  $\tau_a(\chi) = \bar{\chi}(a)\tau(\chi)$  for any  $a \in \mathbb{Z}/N\mathbb{Z}$ .

Here  $\tau(\chi) = \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(x)\zeta^x$  and  $\tau_a(\chi) = \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(x)\zeta^{ax}$ .

*Proof.* If  $\gcd(a, N) = 1$ , we have

$$\tau_a(\chi) = \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(x)\zeta^{ax} = \bar{\chi}(a) \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(ax)\zeta^{ax} = \bar{\chi}(a)\tau(\chi)$$

If  $\gcd(a, N) = d > 1$ , we write  $a = a'd$ ,  $N = N'd$ , then

$$\tau_a(\chi) = \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(x)\zeta^{da'x} = \sum_{s=0}^{N'-1} \sum_{t=0}^{d-1} \chi(s+tN')\zeta^{a'd(s+tN')} = \sum_{s=0}^{N'-1} \zeta^{sd} \left( \sum_{t=0}^{d-1} \chi(s+tN') \right)$$

But

$$\sum_{t=0}^{d-1} \chi(s+tN') = \begin{cases} \sum 0 = 0 & \gcd(s, N') > 1 \\ \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times, x \equiv s \pmod{N'}} \chi(x) = \bar{\chi}(s) \sum_{x \in H} \chi(x) = 0 & \gcd(s, N') = 1 \end{cases}$$

where  $H = \ker((\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/N'\mathbb{Z})^\times)$  and  $\chi|_H$  is not trivial.  $\square$

#### 3.2 Clear Form of $L(1, \chi)$

Now we have

$$\begin{aligned} \tau(\bar{\chi})L(s, \chi) &= \sum_n \frac{1}{n^s} \left( \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \bar{\chi}(a)\zeta^{an} \right) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \bar{\chi}(a) \sum_n \frac{\zeta^{na}}{n^s} \\ &\rightarrow \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \bar{\chi}(a)(-\log(1 - \zeta^a)) \quad \text{when } s \rightarrow 1^+ \end{aligned}$$

We can do more things, because:

$$\tau(\chi)\tau(\bar{\chi}) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \tau(\chi)\bar{\chi}(a)\zeta^a = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \tau_a(\chi)\zeta^a = \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \chi(x) \left( \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{a(1+x)} \right) = \chi(-1)N$$

and

$$\log(1 - \zeta^a) = \log|1 - \zeta^a| + \pi i \left( \frac{a}{N} - \frac{1}{2} \right)$$

This encourages us to distinguish two cases<sup>5</sup> of  $\chi$ : odd if  $\chi(-1) = -1$  and even if  $\chi(-1) = 1$ . What follows immediately is

$$(1) \text{ If } \chi \text{ is odd, } \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \bar{\chi}(a) \log |1 - \zeta^a| = 0$$

$$(2) \text{ If } \chi \text{ is even, } \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \bar{\chi}(a) \left( \frac{a}{N} - \frac{1}{2} \right) = 0$$

Hence we get

**Theorem 3.2** (Special value formula). *Let  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  be a primitive Dirichlet character with conductor  $N > 1$ . Let  $\tau(\chi) = \sum \chi(a) e^{2\pi i a/N}$  be a Gauss sum. Then*

$$L(1, \chi) = \begin{cases} \frac{\pi \tau(\chi)}{N} B_{1, \bar{\chi}}, & \text{if } \chi(-1) = -1, \text{ where } B_{1, \bar{\chi}} = \frac{i}{N} \sum_{a=1}^N \bar{\chi}(a) a, \\ -\frac{\tau(\chi)}{N} \sum_{a=1}^N \bar{\chi}(a) \log |1 - \zeta_N^a|, & \text{if } \chi(-1) = 1, \chi \neq 1. \end{cases}$$

## 4 Class Number Formula for Quadratic Fields

Recall that we have a interest result in Proposition 2.10 for Abelian extention  $K/\mathbb{Q}$  with Galois group  $G$ :

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(s, \chi^*)$$

And as a corollary ,we get

$$\prod_{\chi \neq \chi_0} L(1, \chi^*) = \lim_{s \rightarrow 1} \frac{(s-1) \zeta_K(s)}{(s-1) L(1, \chi_0^*)} = \frac{2^{r_1} (2\pi)^{r_2} R_K}{\omega_K \sqrt{|\Delta_K|}} \cdot h$$

So for quadratic fields, in order to get  $h$  on the right hand, we should investigate the nontrivial characters of  $K$  : actually only one , for the reason  $\widehat{K} = \text{Gal}(\widehat{K}/\mathbb{Q})$ . We denote  $\widehat{K} = \{\chi_0, \lambda\}$ , and  $K = \mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_{|D|})$  with discriminant  $\Delta_K = D$ .

Morevoer, we can define a Dirichlet character  $\chi_K$  with conductor  $|D|$  :

- (i)  $\chi_K(-1) = D/|D|$
- (ii)  $\chi_K(2) = (-1)^{\frac{D^2-1}{8}}$  if  $D \equiv 1 \pmod{4}$ , and  $\chi_K(2) = 0$  otherwise.
- (iii)  $\chi_K(p) = \left( \frac{D}{p} \right)$  if  $p$  is a odd prime.
- (iv)  $\chi_K$  is completely multiplicative on  $\mathbb{Z}$ .

**Proposition 4.1.**  $\lambda^* = \chi_K$

<sup>5</sup>We point out a number theoretical significance of the parity of the character  $\chi$ :

- (i) An abelian field  $K$  is real field  $\iff$  All characters of  $K$  is even
- (ii) A imaginary abelian field  $K$  with  $K_+$  being its maximal real subfield , then  $[K : K_+] = 2$  and  $\widehat{K}_+ = \{\chi \in \widehat{K} \mid \chi \text{ is even}\}$ .

*Proof.* We just need to show  $\zeta_K(s) = \zeta(s) \sum_{n=1}^{\infty} \chi_K(n)/n^s$  for  $\Re(s) > 1$ . By Euler product, we only need to show every rational prime  $p$ :

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = (1 - p^{-s})(1 - \chi_K(p)p^{-s})$$

and we have

$$LHS = \begin{cases} 1 - p^{-s} & p \text{ ramified} \\ (1 - p^{-s})^2 & p \text{ splits} \\ (1 - p^{-2s}) & p \text{ inert} \end{cases} \quad \Leftrightarrow \quad \chi_K(p) = \begin{cases} 0 & p \text{ ramified} \\ 1 & p \text{ splits} \\ -1 & p \text{ inert} \end{cases}$$

So we conclude the proposition. □

If  $\chi_K$  is odd, we see  $D < 0$ , and then  $r_1 = 0, r_2 = 1, R_K = 1$ ,

$$L(1, \chi_K) = \frac{2\pi}{\omega_K \sqrt{|D|}} \cdot h$$

If  $\chi_K$  is even, we see  $D > 0$ , and then  $r_1 = 2, r_2 = 0, R_K = \log |\epsilon_K|$ ,

$$L(1, \chi_K) = \frac{2 \log |\epsilon_K|}{\sqrt{|D|}} \cdot h$$

Hence we conclude:

**Theorem 4.2** (Class number formula, 1839-1840). *Let  $\chi = \left(\frac{D}{\cdot}\right)$  be the quadratic Dirichlet character associated to a quadratic field  $K = \mathbb{Q}(\sqrt{D})$  with discriminant  $D$ . Let  $h_K$  be the ideal class number of  $K$  and  $\epsilon_K > 1$  the fundamental unit when  $D > 0$ . Then*

$$L(1, \chi_K) = \begin{cases} \frac{2\pi h_K}{\omega_K \sqrt{|D|}}, & \text{if } \chi(-1) = -1, \\ \frac{2h_K \log |\epsilon_K|}{\sqrt{|D|}}, & \text{if } \chi(-1) = 1, \chi \neq 1. \end{cases}$$

In particular,  $L(1, \chi_K) > 0$ .

We see the Gauss sum occurs in the formula of  $L(1, \chi)$ , which implies it is hard to compute an explicit form of  $\tau_\chi$ . However, in the case of quadratic fields, we have the following theorem<sup>6</sup>, which help us to calculate.

**Theorem 4.3.** *With the notation above,*

$$\tau(\chi_K) = \begin{cases} \sqrt{|D|} & \text{If } \chi \text{ is even} \\ i\sqrt{|D|} & \text{If } \chi \text{ is odd} \end{cases}$$

---

<sup>6</sup>We can easily get a weaker result  $|\tau(\chi)| = \sqrt{|D|}$  by using the fact  $\overline{\tau(\chi)} = \chi(-1)\tau(\chi)$ .

**Remark 4.4** (the class number  $h_K$  for quadratic field).

We have two usual ways to calculate  $h_K$ : one is the Minkowski bound<sup>7</sup> and the other is Theorem 4.2. Take  $K = \mathbb{Q}(\sqrt{-56})$  as a example:

(I) Minkowski Bound.

$r_1 = 0, r_2 = 1, \Delta_K = -56$ , so the Minkowski bound for  $K$  is  $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|} = \frac{4\sqrt{14}}{\pi} \approx 4.76$ .

(2)  $= \mathfrak{p}^2$  with  $\mathfrak{p} = (2, \sqrt{-14})$  and  $N(\mathfrak{p}) = 2$ . From  $a^2 + 14b^2 = 2$  has no integral solutions, we see  $\mathfrak{p}$  is not principal and order is 2; (3)  $= \mathfrak{p}_3 \bar{\mathfrak{p}}_3$  with  $\mathfrak{p}_3 = (3, \sqrt{-14} + 1)$  and  $\mathfrak{p}_3$  is not principal because  $a^2 + 14b^2 = 3$  has no integral solutions. Note that  $\alpha = \sqrt{-14} + 2 \in \mathcal{O}_K$  and  $N(\alpha) = 2 \cdot 3^2$ . But  $\frac{\alpha}{3} \notin \mathcal{O}_K$ , so we may assume  $\mathfrak{p}_3 \mid (\alpha)$  and then  $[\mathfrak{p}\bar{\mathfrak{p}}_3] = [(1)]$ .

Hence  $\mathfrak{p}_3$  has order 4 and  $\text{Cl}(K) = \mathbb{Z}/4\mathbb{Z}$ ,  $h_K = 4$ .

(II) Use the formulas<sup>8</sup> occur in Theorem 3.2, Theorem 4.2, Theorem 4.3, We have

$$h_K = \frac{1}{\Delta_K} \sum_{a=1}^{|\Delta_K|-1} \chi_K(a)a = \frac{2}{-56} \sum_{0 < a < 28} \chi_K(a)a + \sum_{0 < a < 28} \chi_K(a)$$

and

$$\left(\frac{-56}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{p}{7}\right) \Rightarrow \chi_K(p) = \begin{cases} 1 & p = 3, 5, 13, 19, 23 \\ -1 & p = 11, 17 \end{cases} \Rightarrow h_K = \frac{2 \times 112}{-56} + 8 = 4$$

For the class number of quadratic field, Gauss has two famous conjectures:

(i) class-number one problem for complex quadratic fields:  $\#\{d \mid d < 0, h_{\mathbb{Q}\sqrt{d}} = 1\} < \infty$ ;

(ii) class-number one problem for real quadratic fields:  $\#\{d \mid d > 0, h_{\mathbb{Q}\sqrt{d}} = 1\} = \infty$

in 1934, Heilbronn and Linfoot (1934)<sup>9</sup> proved the Gauss Conjecture (i), which says there is at

<sup>7</sup>I searched for information about the refinement work of Minkowski bound, and there are not too much. It is worth mentioning that for real quadratic field, it can be improved to  $1 + \lfloor \frac{\sqrt{\Delta_K}}{3} \rfloor$  and this bound is best possible.

<sup>8</sup>A generalization of the Legendre symbol to get rid of the constraint of  $p$  being an odd prime is the Kronecker symbol. Namely,  $\left(\frac{a}{\pm \prod p^{n_p}}\right) := \left(\frac{a}{\pm 1}\right) \prod \left(\frac{a}{p}\right)^{n_p}$ , and we define:

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & a \equiv \pm 1 \pmod{8} \\ -1 & a \equiv \pm 3 \pmod{8} \\ 0 & a \equiv 0 \pmod{2} \end{cases} \quad \left(\frac{a}{1}\right) = 1 \quad \left(\frac{a}{-1}\right) = \begin{cases} 1 & a \geq 0 \\ -1 & a < 0 \end{cases}$$

A fact is The Kronecker symbol is multiplicative in both variables. So we have

$$\left(\frac{\Delta_K}{p}\right) \left(\frac{\Delta_K}{p^{-1}}\right) = \left(\frac{\Delta_K}{1}\right) = 1 \Rightarrow \bar{\chi}_K(p) = \chi_K(p)$$

<sup>9</sup>H. Heilbronn, E. Linfoot, On the imaginary quadratic corpora of class-number one. Quart. J. Math. Oxford Ser. 5 (1934), pp. 293–301.



most one imaginary quadratic field whose  $h_K = 1$  if  $d < -163$ .<sup>10</sup>

Interestingly, Heilbronn's proof followed a remarkable work of Deuring<sup>11</sup> who proved that if there were infinitely many class-number one complex quadratic fields, then the Riemann Hypothesis would follow! Many authors promptly carried this over to other class-numbers, but Heilbronn realized that Deuring's method would allow one to prove the Generalized Riemann Hypothesis (GRH). Combining with Landau's earlier result which showed that GRH could deduce (i), He proved (i). The interesting thing is that GRH is used as a springboard to complete the proof:

$$(i) \text{ fails. } \xRightarrow{\text{Heilbronn}} \text{GRH} \xRightarrow{\text{Landau}} (i) \text{ holds.}$$

Also in 1934, Heilbronn<sup>12</sup> prove a more general theorem which says  $\lim_{d \rightarrow +\infty} h_{\mathbb{Q}\sqrt{-d}} = \infty$ .

The problem of the class number of real quadratic field is more difficult because the fundamental units are difficult to calculate. Hua Luogeng proved that  $h_{\mathbb{Q}\sqrt{d}, d>0} < \sqrt{d}$  and this is essentially the best outcome.

We recommend H.M.Stark's review<sup>13</sup> to students interested in further understanding related developments.

**Remark 4.5** (Kummer's work on  $h_p := h_{\mathbb{Q}(\zeta_p)}$ ).

In order to study Fermat's Last Conjecture, Kummer systematically investigated a series of profound properties of  $\mathbb{Z}[\zeta_p]$  (such as class number, ideal, analytical properties, etc.), and pioneered theoretical research on the field of cyclotomic field, achieving many profound results. And there are some representative results listed:

(i) Let  $p$  be a odd prime, if  $p \nmid h_p$ , then the Fermat equation  $x^p + y^p = z^p$  has no nontrivial integer solution.

(ii) Denote  $h_p^+ = h_{\mathbb{Q}(\zeta_p + \zeta_p^{-1})}$ , then  $h_p^+ \mid h_p$  and we denote  $h_p^- = h_p / h_p^+$ .

(iii)  $p \mid h_p \iff p \mid h_p^- \iff$  at least one numerator of Bernoulli number  $B_2, B_4, \dots, B_{p-3}$  must be divisible by  $p$ .

<sup>10</sup>Until 1967, the exceptional number field was independently proven by Baker and Stark to be non-existent, which means that there are only nine imaginary quadratic fields with class number one given by Gauss.

<sup>11</sup>M. Deuring – “Imaginäre quadratische Zahlkörper mit der Klassenzahl 1”, Math. Z. 37 (1933), no. 1, p. 405–415.

<sup>12</sup>H. Heilbronn – “On the class-number in imaginary quadratic fields”, Quart. J. Math. Oxford Ser. 5 (1934), p. 150–160.

<sup>13</sup>H.M.Stark, the gauss class-number problems, clay mathematics proceedings volume 7, 2007.

## 5 A Brief (and Naive) Introduction to p-adic $L$ Function

#<sup>14</sup>

We see any Dirichlet character  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  can be seen as a character

$$\chi : \prod_p \mathbb{Z}_p^\times \rightarrow \mathbb{C}^\times$$

via the identification  $\mathbb{Z}_\ell^\times \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times (1 + \ell^n\mathbb{Z}_\ell)$  if  $v_\ell(N) = n > 0$ . And one can view  $\zeta(s)$  as

$$\zeta : \text{Hom}_{\text{cts}}(\mathbb{R}_{>0}, \mathbb{C}^\times) \rightarrow \mathbb{C} \rightarrow \mathbb{C} \quad [x \rightarrow x^s] \mapsto s \mapsto \zeta(s)$$

So for each pair  $(\chi, s)$ , it corresponds to a (unique) continuous character:

$$\kappa_{\chi,s} : \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times \rightarrow \mathbb{C}^\times \quad (x, y) \mapsto x^s \chi(y)$$

All continuous characters on this group are of this form.

Since  $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times = \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times$ , we can consider all Dirichlet  $L$  functions at once via the function  $\widetilde{L}$ :

$$\widetilde{L} : \text{Hom}_{\text{cts}}(\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times, \mathbb{C}^\times) \rightarrow \mathbb{C}^\times \quad \kappa_{\chi,s} \mapsto L(\chi, s)$$

In the framework of Tate, this function  $L$  can be viewed as integrating  $\kappa_{\chi,s}$  against the Haar measure on  $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$ . In his thesis, Tate showed that properties such as the analytic continuation and functional equations of Dirichlet  $L$  functions by using the Poisson formula and the Fourier transformation.

To obtain a p-adic version of  $L$  function, we should consider continuous characters from  $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$  to  $\mathbb{C}_p^\times$  instead of  $\mathbb{C}^\times$ . But  $\mathbb{R}_{>0}$  is connected and  $\mathbb{C}_p^\times$  is totally disconnected, we only need to look at the restriction to  $\mathbb{Z}_p^\times$ .

In the measure-theoretic viewpoint of L-functions, it is then natural to look for an analytic function:

$$\zeta_p : \text{Hom}_{\text{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \rightarrow \mathbb{C}_p$$

**Theorem 5.1** (Kubota-Leopoldt, Iwasawa). *There exists a (pseudo-)measure  $\zeta_p$  on  $\mathbb{Z}_p^\times$  such that for all  $k > 0$ ,*

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \zeta_p := \zeta_p(x \mapsto x^s) = (1 - p^{-(1-k)})\zeta(1 - k)$$

The Kubota-Leopoldt p-adic  $L$  function is the p-adic analogue of the Riemann zeta function. We will see three constructions (analytic, arithmetic and algebraic) of this object, each of a different flavour.

We have much more, and the power of the measure-theoretic approach becomes obvious:

---

<sup>14</sup>Referring to (or, copying) a small part of this lecture: Jacinto, J.R., & Williams, C. (2023). An introduction to p-adic  $L$ -functions. I strongly recommend reading pages 1-13 of this lecture to gain more motivation and general details.

**Theorem 5.2.** *Let  $\chi$  be a Dirichlet character of conductor  $p^n$  ( $n > 0$ ), viewed as a locally constant character on  $\mathbb{Z}_p^\times$ . Then for all  $k > 0$ ,*

$$\int_{\mathbb{Z}_p^\times} \chi(x) x^k \cdot \zeta_p = (1 - \chi(p) p^{-(1-k)}) L(\chi, 1 - k)$$

## References

(Some lecture notes and Internet resource links are attached in the footnotes.)

[1] <http://mcm.amss.cas.cn/faculty/tianyichao/201409/W020140919372982540194.pdf>

[2] 冯克勤. 代数数论 [M]. 哈尔滨: 哈尔滨工业大学出版社, 2018.5.

[3] 加藤和也, 黑川信重, 斋藤毅著; 胥鸣伟, 印林生译. 数论 I, Fermat 的梦想和类域论 [M]. 北京: 高等教育出版社, 2009.6.