Note on

Dirichlet's Theorem

of primes in arithmetic progressions

(Spring 2016, Nankai)

Dr.Hanbin Zhang, Syu Gau

Last update:May 27, 2016

Contents

Notations

For any integer n, we will use $n \bmod m$ or simply $\overline{n}$ to denote its image in the quotient $\mathbb{Z}/m$. We use $v_p(n)$ to denote the p-adic valuation of n, which is the maximal integer v such that $p^v \mid n$.

We will use $\Re(z)$ to denote the real part of the complex number z.

We will also use the capital O notation. The standard notation $f = O(g)$ means there exists a constant $c > 0$ such that $|f| \leqslant cg$. Note that if $f = O(g)$, we can always replace f in right side of an equality by $O(g)$. To extend the replacement to inequality, we also use the non-standard notation $f \leqslant O(g)$ (resp. $f \geqslant O(g)$), which means there exists a constant $c > 0$ such that $f \leqslant cg$ (resp. $-f \leqslant cg$).

§ 1 Statement of the theorem

The aim of this note is to prove the following theorem which is conjugated by Ledgered and proved by Dirichlet.

Dirichlet's Theorem *Let m and a be two relatively prime integers. Then there exist infinitely many primes in the arithmetic progression $\{km + a\}$.*

To prove this, recall how Euler prove that there exist infinitely many primes. The key ideal is to show the summand

$$\sum_p \frac{1}{p}$$

is actually a divergent series.

How to show this? Recall the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{(1 - \frac{1}{p^s})}$$

diverges at $s = 1$ and we have

$$\begin{aligned} \log \zeta(s) &= -\sum_p \log(1 - \frac{1}{p^s}) = \sum_{k \geqslant 1, p} \frac{1}{kp^{ks}} \\ &= \sum_p \frac{1}{p^s} + \sum_{k \geqslant 2, p} \frac{1}{kp^{ks}}. \end{aligned}$$

Note that when $s \geqslant 1$,

$$\begin{aligned} \sum_{k \geqslant 2, p} \frac{1}{kp^{ks}} &\leqslant \frac{1}{2} \sum_{k \geqslant 2, p} \frac{1}{p^k} \\ &\leqslant \sum_p \frac{\frac{1}{p^2}}{1 - \frac{1}{p}} = \sum_p \frac{1}{(p-1)p} \\ &< \sum_n \frac{1}{n(n-1)} < 1. \end{aligned}$$

Therefore $\sum_p \frac{1}{p^s}$ diverges at $s = 1$.

Dirichlet character and L-series

Now we want to analogy the above strategy. To give a summand of the form

$$\sum_{p \equiv a \pmod m} \frac{1}{p^s},$$

we need some characters to sieve primes in $a \bmod m$.

A ***Dirichlet character*** of m is a class function χ on $\mathbb{Z}$ such that $\chi(n) = 0$ for any integers n which is not relative prime to m and that it induces a group homomorphism from $\mathbb{G}(m) := (\mathbb{Z}/m)^\times$ to S^1. We use $\widehat{\mathbb{G}(m)}$ to denote the dual group of $\mathbb{G}(m)$ and identify it with the group of Dirichlet characters of m. We use $\mathbf{1}$ to denote the identity (called the ***principal character***).

We now define the ***L-series*** for a Dirichlet character χ to be

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

It is easy to see that

$$L(s,\chi) = \sum_{(m,n)=1} \frac{\chi(n)}{n^s} = \prod_{p\nmid m} \frac{1}{1-\frac{\chi(p)}{p^s}}.$$

Therefore

$$\begin{aligned}\log L(s,\chi) &= \sum_{p\neq m} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \\ &= \sum_{p\neq m} \frac{\chi(p)}{p^s} + \sum_{k\geqslant 2, p\neq m} \frac{\chi(p^k)}{kp^{ks}}.\end{aligned}$$

Note that

$$\sum_{\chi\in\widehat{\mathbb{G}(m)}} \chi(-a)\chi(n) = \begin{cases}\phi(m) & a\equiv n \pmod m,\\ 0 & a\not\equiv n \pmod m.\end{cases}$$

Therefore

$$(1)\quad \frac{1}{\phi(m)} \sum_{\chi} \chi(-a)\log L(s,\chi) = \sum_{p\equiv a \,(\mathrm{mod}\ m)} \frac{1}{p^s} + \sum_{k\geqslant 2, p^k\equiv a \,(\mathrm{mod}\ m)} \frac{1}{kp^{ks}}.$$

To show the divergence of $\sum\limits_{p\equiv a \,(\mathrm{mod}\ m)} p^{-s}$ at $s=1$, it suffices to show

1. $\dfrac{1}{\phi(m)} \sum\limits_{\chi} \chi(-a)\log L(s,\chi)$ diverges at $s=1$;

2. $\sum\limits_{k\geqslant 2, p^k\equiv a \,(\mathrm{mod}\ m)} \dfrac{1}{kp^{ks}}$ converges at $s=1$.

The later one is clear since for $s\geqslant 1$,

$$\sum_{k\geqslant 2, p^k\equiv a \,(\mathrm{mod}\ m)} \frac{1}{kp^{ks}} \leqslant \sum_{k\geqslant 2, p} \frac{1}{kp^{ks}} < 1.$$

It remains to prove 1.

Note that

$$L(s,\mathbf{1}) = (1-m^{-s})\zeta(s),$$

thus $L(s, \mathbf{1})$ diverges at $s = 1$. Since $\sum_{k=1}^{m-1} \chi(n+k) = 0$, by Dirichlet's test for convergence, every $L(s, \chi)$ converges at $s = 1$. If we can furthermore show that none of them converges to 0, then the sum

$$\frac{1}{\phi(m)} \sum_{\chi} \chi(-a) \log L(s, \chi)$$

must diverges at $s = 1$.

Complex characters

In this subsection, we will show that $L(s, \chi)$ does not converge to 0 if χ is not a real character.

First, for any $s > 1$, from eq. (1), we see that

$$\sum_{\chi} \log L(s, \chi) \geqslant 0.$$

Hence

$$\prod_{\chi} L(s, \chi) \geqslant 1. \tag{2}$$

Before, going foreword, we should point out that, by Dirichlet's test, the L-series $L(s, \chi)$ does not only converges at $s = 1$, but uniformly converges in $\Re(s) > \epsilon$, where $\Re(s)$ is the real part of s and ϵ is an arbitrary positive real number. In this way, $L(s, \chi)$ defines a continuous functions in $\Re(s) > 0$. We will still use $L(s, \chi)$ to denote this function. Consider the series

$$L'(s, \chi) = \sum_{n=1}^{\infty} -\chi(n)(\log n) n^{-s}.$$

By Dirichlet's test again, we see this series also defines a a continuous functions in $\Re(s) > 0$ and hence $L(s, \chi)$ is differential in $\Re(s) > 0$.

Assume there is a complex character χ such that $L(1, \chi) = 0$, then so

does its conjugate $\overline{\chi}$. For $1 < s < 2$, we have

$$\begin{aligned}
L(s, \mathbf{1}) &= (1 - m^{-s})\zeta(s) \\
&< (1 - m^{-s}) \left(1 + \int_1^{\infty} \frac{1}{x^s} \mathrm{d}x\right) \\
&= \frac{(1 - m^{-s})s}{s - 1} < \frac{s}{s - 1} < \frac{2}{s - 1}, \\
L(s, \chi) &= L(s, \chi) - L(1, \chi) \\
&\leqslant (s - 1) \max_{1 < s' \leqslant s} L'(s', \chi) \\
&\leqslant (s - 1) \max_{1 < s' \leqslant 2} L'(s', \chi), \\
L(s, \overline{\chi}) &\leqslant (s - 1) \max_{1 < s' \leqslant 2} L'(s', \overline{\chi}).
\end{aligned}$$

From the above, we see that

$$\lim_{s \to 1} \prod_{\chi} L(s, \chi) = 0,$$

which contradicts to eq. (2).

§ 2 Dirichlet's elementary proof for prime case

By the discussion before, we see that to prove , it suffices to prove $L(1, \chi) \neq 0$ for any real character χ.

In the case m is an odd prime q, the only real non-principal character is precisely the *Legendre symbol* $\chi_{-1}(n) = \left(\frac{n}{q}\right)$. Then,

$$L(s, \chi_{-1}) = \sum_{n=1}^{\infty} \left(\frac{n}{q}\right) n^{-s},$$

It remains to show

$$L(1, \chi_{-1}) = \sum_{n=1}^{\infty} \left(\frac{n}{q}\right) n^{-1} \neq 0 \tag{3}$$

Gauss sum

To achieve our goal, we need some technology to translate multiplicative characters to additives. To do this, we invite the ***Gauss sum***

$$G(n) = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) e_q(kn),$$

where

$$e_q(kn) = e^{2\pi i \frac{kn}{q}}.$$

Note that $\left(\frac{n}{q}\right)$ is multiplicative while $e_q(n)$ is additive.

First, we show that $G(1)$ is never 0.

2.1 Lemma $G(1)^2 = \begin{cases} q & q \equiv 1 \pmod 4, \\ -q & q \equiv 3 \pmod 4. \end{cases}$

Proof: We have

$$G(1)^2 = \sum_{k_1=1}^{q-1} \sum_{k_2=1}^{q-1} \left(\frac{k_1}{q}\right) \left(\frac{k_2}{q}\right) e_q(k_1 + k_2).$$

Replacing $k_1^{-1}k_2$ by its residue mod q, saying n, we get

$$\left(\frac{k_1}{q}\right) \left(\frac{k_2}{q}\right) = \left(\frac{k_1^2}{q}\right) \left(\frac{n}{q}\right) = \left(\frac{n}{q}\right).$$

Then

$$G(1)^2 = \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \sum_{k=1}^{q-1} e_q(k(n+1)).$$

Note that for any n with $q \nmid n$, we have

$$\sum_{k=1}^{q-1} e_q(kn) = 1.$$

Therefore

$$G(1)^2 = \left(\frac{-1}{q}\right)(q-1) - \sum_{n=1}^{q-2} \left(\frac{n}{q}\right).$$

Since

$$\sum_{n=1}^{q-1} \left(\frac{n}{q}\right) = 0,$$

we have

$$\begin{aligned} G(1)^2 &= \left(\frac{-1}{q}\right)(q-1) - \sum_{n=1}^{q-2} \left(\frac{n}{q}\right) \\ &= q\left(\frac{-1}{q}\right) = \begin{cases} q & q \equiv 1 \pmod 4, \\ -q & q \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

□

Now we introduce a formula which represents the Legendre symbol by an additive character.

2.2 Lemma $\left(\frac{n}{q}\right) = \frac{1}{G(1)} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) e_q(kn)$.

Proof: Let $k' \equiv kn \pmod q$. Then

$$G(n) = \sum_{k'=1}^{q-1} \left(\frac{k'n^{-1}}{q}\right) e_q(k') = \left(\frac{n}{q}\right) G(1).$$

As $G(1) \neq 0$ (by Lemma 2.1), we conclude. □

Use this formula, the $L(1, \chi_{-1})$ can be written as

$$\begin{aligned} L(1, \chi_{-1}) &= \frac{1}{G(1)} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{n=1}^{\infty} \frac{e_q(kn)}{n} \\ &= \frac{1}{G(1)} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{n=1}^{\infty} \frac{e_q(k)^n}{n} \\ &= \frac{1}{G(1)} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) (-\log(1 - e_q(k))). \end{aligned}$$

Note that, for $z = e^{\mathrm{i}\theta}$, we have

$$\begin{aligned} 1 - z &= 1 - \cos\theta - \mathrm{i}\sin\theta \\ &= 2\sin\frac{\theta}{2}\left(\cos(\frac{\theta}{2} - \frac{\pi}{2}) + \mathrm{i}\sin(\frac{\theta}{2} - \frac{\pi}{2})\right). \end{aligned}$$

Therefore

$$L(1, \chi_{-1}) = \frac{1}{G(1)} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) (-\log(2\sin\frac{\pi k}{q}) - \mathrm{i}(\frac{\pi k}{q} - \frac{\pi}{2})).$$

Note that $L(1, \chi_{-1})$ must be a real number since χ_{-1} is real.

By Lemma 2.1, we have the following inferences.

1. When $q \equiv 1 \pmod 4$, $G(1)$ is either $q^{\frac{1}{2}}$ or $-q^{\frac{1}{2}}$. Therefore, in this case, to show $L(1, \chi_{-1}) \neq 0$, it suffices to show

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \log(2\sin\frac{\pi k}{q}) \neq 0. \tag{4}$$

2. When $q \equiv 3 \pmod 4$, $G(1)$ is either $\mathrm{i}q^{\frac{1}{2}}$ or $-\mathrm{i}q^{\frac{1}{2}}$. Therefore, in this case, to show $L(1, \chi_{-1}) \neq 0$, it suffices to show

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) (\frac{\pi k}{q} - \frac{\pi}{2}) \neq 0. \tag{5}$$

The case $q \equiv 3 \pmod 4$ is easy to prove. Indeed, we have

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) (\frac{\pi k}{q} - \frac{\pi}{2}) = \frac{\pi}{q} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) k.$$

Since

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) k \equiv \sum_{k=1}^{q-1} k = \frac{q(q-1)}{2} \not\equiv 0 \pmod 2,$$

The conclusion (5) follows.

Cyclotomy

In the case $q \equiv 1 \pmod 4$, we divide the set $[q-1] := \{1, 2, \cdots, q-1\}$ to the following two parts:

$$\mathcal{R} = \left\{ r \in [q-1] \middle| \left(\frac{r}{q}\right) = 1 \right\},$$
$$\mathcal{N} = \left\{ n \in [q-1] \middle| \left(\frac{n}{q}\right) = -1 \right\}.$$

Then, we have

$$\begin{aligned} &\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \log(2 \sin \frac{\pi k}{q}) \\ =& \sum_{r \in \mathcal{R}} \log(2 \sin \frac{\pi r}{q}) - \sum_{n \in \mathcal{N}} \log(2 \sin \frac{\pi n}{q}) \\ =& \log \frac{\prod_{r \in \mathcal{R}} \sin \frac{\pi r}{q}}{\prod_{n \in \mathcal{N}} \sin \frac{\pi n}{q}}. \end{aligned}$$

Therefore, to show (4), it suffices to show

$$\prod_{r \in \mathcal{R}} \sin \frac{\pi r}{q} \neq \prod_{n \in \mathcal{N}} \sin \frac{\pi n}{q}. \tag{6}$$

To do this, we consider the ***q-th cyclotomic polynomial***

$$\Phi_q(t) := \prod_{k=1}^{q-1} (t - e_q(k))$$

as well as

$$\Phi_{\mathcal{R}}(t) = \prod_{r \in \mathcal{R}} (t - e_q(r)), \qquad \Phi_{\mathcal{N}}(t) = \prod_{n \in \mathcal{N}} (t - e_q(n)).$$

Note that

$$\prod_{r\in\mathcal{R}}(1-e_q(r)) = \prod_{r\in\mathcal{R}} e_q(\frac{r}{2})(-\mathfrak{i}\sin\frac{\pi r}{2})$$
$$= (-\mathfrak{i})^{\frac{q-1}{2}} e_q(\frac{1}{2}\sum_{r\in\mathcal{R}} r)\prod_{r\in\mathcal{R}}\sin\frac{\pi r}{2}.$$

and similarly,

$$\prod_{n\in\mathcal{N}}(1-e_q(n)) = (-\mathfrak{i})^{\frac{q-1}{2}} e_q(\frac{1}{2}\sum_{n\in\mathcal{N}} n)\prod_{n\in\mathcal{N}}\sin\frac{\pi n}{2}.$$

Since $\left(\frac{-1}{q}\right) = 1$, we have

$$\left(\frac{-k}{q}\right) = \left(\frac{k}{q}\right).$$

Then,

$$\sum_{r\in\mathcal{R}} r = \sum_{r\in\mathcal{R}}(q-r) = \frac{q(q-1)}{2} - \sum_{r\in\mathcal{R}} r.$$

Hence

$$\sum_{r\in\mathcal{R}} r = \sum_{n\in\mathcal{N}} n = \frac{1}{4}q(q-1).$$

Now, we see that, to show (6), it suffices to show

$$\Phi_{\mathcal{R}}(1) \neq \Phi_{\mathcal{N}}(1). \tag{7}$$

To do this, we will show

2.3 Lemma *There exist $\mathbb{Z}$-polynomials $Y(t)$ and $Z(t)$ such that*

$$\Phi_{\mathcal{R}}(t) = \frac{1}{2}(Y(t) - q^{\frac{1}{2}}Z(t)),$$
$$\Phi_{\mathcal{N}}(t) = \frac{1}{2}(Y(t) + q^{\frac{1}{2}}Z(t)).$$

Note that

$$Y(t)^2 - qZ(t)^2 = 4\Phi_{\mathcal{R}}(t)\Phi_{\mathcal{N}}(t) = 4\Phi_q(t) = 4(t^{q-1} + t^{q-2} + \cdots + 1).$$

Then

$$Y(1)^2 - qZ(1)^2 = 4q.$$

Since q is a prime, $Z(1) \neq 0$ and therefore (7) follows.

Gauss periods

To prove Lemma 2.3, we introduce the *Gauss periods*.
Note that in our case, q is prime, thus

$$\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1).$$

For any n with $q \nmid n$, we use $v(n)$ to denote the image of $\overline{n}$ in $\mathbb{Z}/(q-1)$.

For any $s \mid q-1$, those $v(n)$ can be classified by $\bmod s$. Then, the ***Gauss periods*** for s are defined to be

$$\eta_j := \sum_{v(n)\equiv j \pmod s} e_q(n), \quad j = 0, \cdots, s-1.$$

For conversion, we denote $e_q(1)$ by ξ.

We first prove the following useful lemma

2.4 Lemma *Let A be a free $\mathbb{Z}$-algebra. Let $F(t)$ be a A-polynomial such that $F(\xi^n) = F(\xi)$ whenever $v(n) \equiv 0 \pmod s$. Then there exist $b_0, \cdots, b_{s-1} \in A$ such that*

$$F(\xi) = b_0\eta_0 + \cdots + b_{s-1}\eta_{s-1}.$$

Proof: Since $1 + x + \cdots + x^{q-1}$ is the minimal polynomial of ξ over $\mathbb{Z}$ and furthermore over A, any A-polynomial on ξ can be uniquely written in the form

$$a_1\xi + \cdots + a_{q-1}\xi^{q-1}.$$

Thus we may assume

$$F(x) = \sum_{k=1}^{q-1} a_k x^k.$$

Since $F(\xi^n) = F(\xi)$ whenever $v(n) \equiv 0 \pmod s$, we have

$$a_k = a_l, \quad k \equiv nl \pmod q.$$

Note that for such k, l, we have

$$v(k) \equiv v(n) + v(l) \pmod s.$$

Since $v(n) \equiv 0 \pmod s$, we get

$$v(k) \equiv v(l) \pmod s.$$

Therefore we can write $F(\xi)$ as

$$F(\xi) = b_0\eta_0 + \cdots + b_{s-1}\eta_{s-1},$$

where $b_0, \cdots, b_{s-1} \in A$. □

Now, let $s = 2$ and consider the polynomial

$$F(x) = \prod_{r \in \mathcal{R}} (t - x^r).$$

In this case, $v(n) \equiv 0 \pmod 2$ is equivalent to say $\left(\frac{n}{q}\right) = 1$. Then, up to $\bmod q$, $n\mathcal{R}$ equals $\mathcal{R}$ and therefore

$$F(\xi^n) = \prod_{r \in \mathcal{R}} (t - \xi^r) = \prod_{r \in \mathcal{R}} (t - \xi^{nr}) = F(\xi).$$

Hence, by Lemma 2.4, there exist $b_0(t), b_1(t) \in \mathbb{Z}[t]$ such that

$$\Phi_{\mathcal{R}}(t) = F(\xi) = b_0(t)\eta_0 + b_1(t)\eta_1.$$

Let g be a ***primitive root*** $\bmod q$, which means $\overline{g}$ generates $\mathbb{F}_q^\times$. Then, up to $\bmod q$, $g\mathcal{R}$ equals $\mathcal{N}$ and therefore

$$\Phi_{\mathcal{N}}(t) = F(\xi^g).$$

Since the map $\xi \mapsto \xi^g$ exchanges η_0 and η_1, we have

$$\Phi_{\mathcal{N}}(t) = b_1(t)\eta_0 + b_0(t)\eta_1.$$

Now, it remains to determine η_0 and η_1. First, we have

$$\eta_0 = \sum_{r \in \mathcal{R}} \xi^r, \qquad \eta_1 = \sum_{n \in \mathcal{N}} \xi^n.$$

Thus

$$\eta_0 - \eta_1 = G(1).$$

On the other hand, we have

$$\eta_0 + \eta_1 = -1.$$

Therefore

$$\eta_0 = \frac{1}{2}(-1 + G(1)), \qquad \eta_1 = \frac{1}{2}(-1 - G(1)).$$

Write $\epsilon = G(1)|G(1)|^{-1}$ and

$$Y(t) = -b_0(t) - b_1(t), \qquad Z(t) = (-b_0(t) + b_1(t))\epsilon.$$

Note that in the case $q \equiv 1 \pmod 4$, $G(1)^2 = q$, thus $\epsilon \in \mathbb{Z}$ and we finish proving Lemma 2.3.

Determine $G(1)$

Although it is not necessary to determine the value of $G(1)$, we still put it here.

First, note that

$$\begin{aligned} G(1) &= \sum_{r\in\mathcal{R}} e_q(r) - \sum_{n\in\mathcal{N}} e_q(n) \\ &= 2\sum_{r\in\mathcal{R}} e_q(r) - \sum_{k=1}^{q-1} e_q(k) \\ &= 1 + 2\sum_{r\in\mathcal{R}} e_q(r) \\ &= \sum_{k=0}^{q-1} e_q(k^2). \end{aligned}$$

We will show more generally that

2.5 Lemma *For any positive integer n, we have*

$$S = \sum_{k=0}^{n-1} e_n(k^2) = \begin{cases} (1+\mathfrak{i})n^{\frac{1}{2}} & n \equiv 0 \pmod 4, \\ n^{\frac{1}{2}} & n \equiv 1 \pmod 4, \\ 0 & n \equiv 2 \pmod 4, \\ \mathfrak{i}n^{\frac{1}{2}} & n \equiv 3 \pmod 4. \end{cases}$$

To prove this, we need the Poisson's formula.

Recall the *Poisson's formula* says that if $f(x)$ belongs to the *Schwartz space*, then

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}(n),$$

where

$$\widehat{f}(n) = \int_{-\infty}^{\infty} f(x) e^{2\pi i n x} \mathrm{d}x.$$

But what we need is

2.6 Lemma *If $f(x)$ is a monotonic continuous function on $[A, B]$, then*

$$\sum_{n=A}^{B}{}' f(n) = \sum_{v=-\infty}^{\infty} \int_A^B f(x) e^{2\pi i v x} \mathrm{d}x,$$

where $\sum\limits_{n=A}^{B}{}' f(n) = \frac{f(A)}{2} + \frac{f(B)}{2} + \sum\limits_{n=A+1}^{B-1} f(n)$.

Proof: Let $f_1(x) = f(x)$ when $x \in [0,1)$ and $f_1(x) = f_1(x+n)$ for any $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then, $f_1(x)$ is continuous in $(0,1)$ and

$$\lim_{x\to 0^+} f_1(x) = f(0), \quad \lim_{x\to 0^-} f_1(x) = f(1).$$

The *Fourier series* of $f_1(x)$ is

$$f_1(x) \sim \frac{1}{2}a_0 + \sum_{v=1}^{\infty}(a_v \cos 2\pi vx + b_v \sin 2\pi vx),$$

where

$$\frac{1}{2}a_v = \int_0^1 f(x)\cos 2\pi vx \mathrm{d}x, \quad \frac{1}{2}b_v = \int_0^1 f(x)\sin 2\pi vx \mathrm{d}x.$$

Then the series converges to $f_1(x)$ when $x \in (0,1)$ and $\frac{f(0)+f(1)}{2}$ at $x = 0$.

Thus

$$\begin{aligned}\frac{f(0)+f(1)}{2} &= \frac{1}{2}a_0 + \sum_{v=1}^{\infty} a_v \\ &= \frac{1}{2}a_0 + 2\sum_{v=1}^{\infty}\int_0^1 f(x)\cos 2\pi vx \mathrm{d}x \\ &= \sum_{-\infty}^{\infty}\int_0^1 f(x)\cos 2\pi vx \mathrm{d}x.\end{aligned}$$

For general A, B. Define $f_k(x) = f(x+A+k-1)$ when $x \in [0,1)$ and $f_k(x) = f_k(x+n)$ for any $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then for each $f_k(x)$,

$$\frac{1}{2}a_v = \int_{A+k-1}^{A+k} f(x)\cos 2\pi vx \mathrm{d}x.$$

Thus the formula follows. □

Proof (Lemma 2.5): Note that

$$S = \sum_{x=0}^{n-1} e_n(x^2) = \sum_{x=0}^{n-1}(\cos\frac{2\pi x^2}{n} + \mathrm{i}\sin\frac{2\pi x^2}{n}).$$

Thus we have

$$\begin{aligned}\sum_{x=0}^{n-1}\cos\frac{2\pi x^2}{n} &= \sum_{x=0}^{n}{}'\cos\frac{2\pi x^2}{n} = \sum_{v=-\infty}^{\infty}\int_0^n \cos\frac{2\pi x^2}{n}e^{2\pi \mathrm{i}vx}\mathrm{d}x, \\ \sum_{x=0}^{n-1}\sin\frac{2\pi x^2}{n} &= \sum_{x=0}^{n}{}'\sin\frac{2\pi x^2}{n} = \sum_{v=-\infty}^{\infty}\int_0^n \sin\frac{2\pi x^2}{n}e^{2\pi \mathrm{i}vx}\mathrm{d}x.\end{aligned}$$

Therefore

$$\begin{aligned}
S &= \sum_{v=-\infty}^{\infty} \int_0^n e^{\frac{2\pi \mathfrak{i} x^2}{n}} e^{2\pi \mathfrak{i} v x} \mathrm{d}x \\
&= n \sum_{v=-\infty}^{\infty} \int_0^1 e^{2\pi \mathfrak{i} n x^2} e^{2\pi \mathfrak{i} v n x} \mathrm{d}x \\
&= n \sum_{v=-\infty}^{\infty} \int_0^1 e^{2\pi \mathfrak{i} n (x^2 + v x)} \mathrm{d}x \\
&= n \sum_{v=-\infty}^{\infty} \int_{\frac{v}{2}}^{\frac{v}{2}+1} e^{2\pi \mathfrak{i} n (x^2 - \frac{v^2}{4})} \mathrm{d}x \\
&= n \sum_{v=-\infty}^{\infty} e^{-\frac{\pi \mathfrak{i} n v^2}{2}} \int_{\frac{v}{2}}^{\frac{v}{2}+1} e^{2\pi \mathfrak{i} n x^2} \mathrm{d}x \\
&= n \sum_{2 \nmid v} (-\mathfrak{i})^n \int_{\frac{v}{2}}^{\frac{v}{2}+1} e^{2\pi \mathfrak{i} n x^2} \mathrm{d}x + n \sum_{2 | v} \int_{\frac{v}{2}}^{\frac{v}{2}+1} e^{2\pi \mathfrak{i} n x^2} \mathrm{d}x \\
&= n((-\mathfrak{i})^n + 1) \int_{-\infty}^{\infty} e^{2\pi \mathfrak{i} n x^2} \mathrm{d}x = n^{\frac{1}{2}}((-\mathfrak{i})^n + 1) \int_{-\infty}^{\infty} e^{2\pi \mathfrak{i} x^2} \mathrm{d}x.
\end{aligned}$$

By Cauchy's test, $\int_{-\infty}^{\infty} e^{2\pi \mathfrak{i} x^2} \mathrm{d}x$ converges. Let it be C. Let $n = 1$, then

$$C = \frac{1}{1 - \mathfrak{i}}.$$

Therefore

$$S = \frac{n^{\frac{1}{2}}((-\mathfrak{i})^n + 1)}{1 - \mathfrak{i}}.$$

□

Poisson's summand formula

We can also prove Lemma 2.5 by using the Poisson's summand formula on S^1.

Let G be a locally compact abelian group and Γ a discrete subgroup of it. For $f(x)$ a L^1-function on G, its ***Fourier transformation*** is the continuous function on $\widehat{G}$ by

$$\hat{f}(\xi) = \int_G \overline{\langle x, \xi \rangle} f(x) \mathrm{d}x, \quad \forall \xi \in \widehat{G}.$$

Here the pairing is defined as

$$\langle x, \xi \rangle := \xi(x).$$

Let

$$F(x) = \sum_{g\in\Gamma} f(gx),$$

Then, we have Fourier expansion

$$F(x) \sim \int_{\widehat{G/\Gamma}} \hat{f}(\xi)\langle x,\xi\rangle \mathrm{d}\xi.$$

It remains to show the above series converges to $F(x)$.

§ 3 Proofs on Landau's lines

In this section, we introduce three proofs on the general lines in Landau's 1905 proof. The general process is like the following.

Setp 1. Construct a meromorphic function $f(s)$ on $\Re(s) > \sigma$ such that $f(s)$ is holomorphic on $\Re(s) > \sigma$ if there exists some character such that $L(1,\chi) = 0$.

Setp 2. Show that the function $f(s)$ has an expansion in Dirichlet series.

Setp 3. Show that however the Dirichlet series diverges at some point in the domain $\Re(s) > \sigma$.

Basic analytic property of L-functions

By the Fundamental Theorem of Dirichlet series, each Dirichlet series define a meromorphic function on the half-plane $\Re(s) \geqslant \sigma_c$ with poles in the line $\Re(s) = \sigma_c$ of *abscissa of convergence*. This function can still be extended analytically and obtained a meromorphic function which admits no analytic continuation. In particular, each L-series $L(s,\chi)$ defines such a maximal analytical continuation, namely the ***L-function***. We will still use $L(s,\chi)$ to denote the L-function extending the L-series for χ. in particular, we use $\zeta(s)$ to denote the ***zeta function***.

3.1 Lemma *The zeta function $\zeta(s)$ is meromorphic on $\Re(s) > 0$ with a simply pole at $s = 1$.*

Proof: Since

$$\frac{1}{s-1} = \int_1^\infty t^{-s}\mathrm{d}t,$$

we have

$$\begin{aligned}\zeta(s) &= \frac{1}{s-1} + \sum_{n\geqslant 1}\frac{1}{n^s} - \frac{1}{s-1}\\ &= \frac{1}{s-1} + \sum_{n\geqslant 1}\int_n^{n+1}(\frac{1}{n^s} - \frac{1}{t^s})\mathrm{d}t.\end{aligned}$$

Let $\varphi_n(s) = \int_n^{n+1}(\frac{1}{n^s} - \frac{1}{t^s})\mathrm{d}t$. Then

$$|\varphi_n(s)| \leqslant \sup_{n\leqslant t\leqslant n+1}\left|\frac{1}{n^s} - \frac{1}{t^s}\right| \leqslant \left|\frac{s}{n^{s+1}}\right|.$$

Therefore $\sum_n \varphi_n(s)$ locally converges uniformly on $\Re(s) > 0$ and thus defines a holomorphic function on $\Re(s) > 0$. □

Note that the result of the above lemma also applies to $L(s, \mathbf{1})$ since

$$L(s, \mathbf{1}) = \prod_{p|m}(1 - p^{-s})\zeta(s).$$

3.2 Lemma *For $\chi \neq \mathbf{1}$, $L(s, \chi)$ is holomorphic on $\Re(s) > 0$.*

Proof: It suffices to show the L-series locally converges uniformly on $\Re(s) > 0$. Then, by the *Weierstrass principle*, the L-series defines a holomorphic function on $\Re(s) > 0$.

For each $s > 0$, since $\{n^{-s}\}$ is monotonically decreasing and the part sum of $\chi(n)$ is bounded, the L-series converges. By Theorem A.8, the L-series locally converges uniformly on $\Re(s) > 0$. □

An short but acrobatic proof

We have seen that to prove , it suffices to show $L(1, \chi) \neq 0$ for any real non-principal character χ. If there is such a real character χ such that $L(1, \chi) = 0$, then the product

$$L(s, \chi)L(s, \mathbf{1})$$

is holomorphic on $\Re(s) > 0$.

Consider the function

$$\psi(s) := \frac{L(s, \chi)L(s, \mathbf{1})}{L(2s, \mathbf{1})}.$$

Then it is holomorphic on $\Re(s) > \frac{1}{2}$ and $\psi(s) \to 0$ when $s \to \frac{1}{2}$.

For each prime p with $p \nmid m$, we have $\chi(p) = 1$ or -1. For $\chi(p) = -1$, we have

$$\frac{(1 - \chi(p)p^{-s})^{-1}(1 - \mathbf{1}(p)p^{-s})^{-1}}{(1 - \mathbf{1}(p)p^{-2s})^{-1}} = \frac{(1 + p^{-s})^{-1}(1 - p^{-s})^{-1}}{(1 - p^{-2s})^{-1}} = 1.$$

Therefore, for $\Re(s) > 1$, we have

$$\psi(s) = \prod_{\chi(p)=1}\frac{1 + p^{-s}}{1 - p^{-s}}.$$

Then, we can write $\psi(s)$ as a Dirichlet series

$$\psi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

with $a_n \geqslant 0$ and $a_1 = 1$. From what we have known so far, the series converges for $\Re(s) > 1$.

By Lemma A.9, this series defines the holomorphic function $\psi(s)$ on $\Re(s) > \frac{1}{2}$. Therefore it has an expansion in powers series centered at $s = 2$ with a radius of convergence at least $\frac{3}{2}$. Note that

$$b_k := (-1)^k \psi^{(k)}(2) = \sum_{n=1}^{\infty} a_n (\log n)^k n^{-2} \geqslant 0.$$

Then

$$\psi(s) = \sum_{k=0}^{\infty} \frac{b_k}{k!} (2-s)^k$$

for $|s-2| < \frac{3}{2}$. In particular, when $\frac{1}{2} < s < 2$, we have

$$\psi(s) \geqslant \psi(2) = 1,$$

which contradicts the fact that $\psi(s) \to 0$ when $s \to \frac{1}{2}$.

A proof in Serre's book

We now introduce a proof from Serre's book []. This may be the most natural proof in this section.

Consider the product

$$\zeta_m(s) = \prod_{\chi \in \widehat{\mathbb{G}(m)}} L(s, \chi).$$

Assume there is a character χ such that $L(1, \chi) = 0$. Then, ζ_m defines a holomorphic function on $\Re(s) > 0$.

However, we will show

3.3 Proposition *$\zeta_m(s)$ diverges at $s = \frac{1}{\phi(m)}$.*

To do this, we need the following lemma.

3.4 Lemma *For p a prime with $p \nmid m$, denote the order of $\overline{p}$ in $\mathbb{G}(m)$ by $f(p)$ and let*

$$g(p) = \frac{\phi(m)}{f(p)}.$$

Then

$$\prod_{\chi} (1 - \chi(p)t) = (1 - t^{f(p)})^{g(p)}.$$

Proof: Since each $\chi(p)$ is a $f(p)$-th root of unity, it remains to show that the number of χ such that $\chi(p)$ gives the same $f(p)$-th root of unity is $g(p)$.

Indeed, consider the character $|p\rangle$ on $\widehat{\mathbb{G}(m)}$:

$$\chi \longmapsto \chi(p).$$

Now, for any $f(p)$-th root of unity ξ, the set $\{\chi|\chi(p) = \xi\}$ is precisely $|p\rangle^{-1}(\xi)$, which is isomorphic to $\ker|p\rangle$ and thus is of cardinal $g(p)$. □

Using this lemma and the Euler product formula, we see

$$\zeta_m(s) = \prod_{\chi}\prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1} = \prod_{p\nmid m}(1-p^{-f(p)s})^{-g(p)}$$

for $\Re(s) > 1$. In this domain, the above Euler product can be written into a Dirichlet series with real and non-negative coefficients. Hence, by Lemma A.9, the above formula holds for $\Re(s) > 0$.

Now we can finish the proof by showing Proposition 3.3.

Proof (Proposition 3.3): For $s > 0$, we have

$$\zeta_m(s) \geqslant \prod_{p\nmid m}(1-p^{-\phi(m)s})^{-1} = \sum_{(n,m)=1}\frac{1}{n^{\phi(m)s}} \geqslant \sum_{p\nmid m}\frac{1}{p^{\phi(m)s}}.$$

However, $\sum\limits_{p\nmid m}\dfrac{1}{p^{\phi(m)s}}$ diverges at $s = \frac{1}{\phi(m)}$, thus so dose $\zeta_m(s)$. □

Landau's 1905 proof

For any real non-principal character χ, we define

$$r(n) = \sum_{d|n}\chi(d).$$

Consider the Dirichlet series

$$Z(s,\chi) := \zeta(s)L(s,\chi) = \sum_{n} r(n)n^{-s}.$$

If $L(1,\chi) = 0$, then $Z(s,\chi)$ defines a holomorphic function on $\Re(s) > 0$. Now, it remains to show $Z(s,\chi)$ diverges at some point $s_0 > 0$.

But before going forward, we prove some properties of $r(n)$ first.

3.5 Lemma *r is **multiplicative**, which means $r(nn') = r(n)r(n')$ whenever $(n,n') = 1$.*

Proof: Since $(n, n') = 1$, we have

$$r(nn') = \sum_{d|nn'} \chi(d) = \sum_{d|n} \chi(d) \sum_{d'|n'} \chi(d') = r(n)r(n').$$

Here the middle equality holds since χ is a homomorphism of multiplicative groups. □

Thus, to determine the values of all $r(n)$, it suffices to determine the values of all $r(p^k)$ with p^k a prime power. Indeed, we have

$$r(p^k) = \begin{cases} 1 & p \mid m, \\ k+1 & \chi(p) = 1, \\ 1 & \chi(p) = -1 \text{ and } 2 \mid k, \\ 0 & \chi(p) = -1 \text{ and } 2 \nmid k. \end{cases}$$

Therefore, $r(n) \geqslant 0$ and $r(n^2) \geqslant 1$.

By the above fact of $r(n)$, for $s > 0$, we have

$$Z(s, \chi) \geqslant \sum_n r(n^2) n^{-2s} \geqslant \sum_n n^{-2s}.$$

Since $\sum_n n^{-2s}$ diverges at $s = \frac{1}{2}$, so does $Z(s, \chi)$.

§ 4 Mertens' proofs

Let χ be a real non-principal character, we need to show $L(1, \chi) \neq 0$.

To do this, Mertens estimated a finite sum $T(x)$ in each proof, showing an inequality which is absurd if $L(1, \chi) = 0$. The first estimation is based on Dirichlet's hyperbola method and the second is based on convolutions. Both of the proofs use Stieltjes integrals.

Dirichlet's hyperbola method

The following problem exemplify how Dirichlet's hyperbola method works.

Problem (Mean value problem) *Let $\tau(n)$ denote the number of natural numbers which divides n. Estimate the finite sum*

$$\sum_{n \leqslant x} \tau(n).$$

First, we have an easy but coarse estimation. Indeed,

$$\sum_{n \leqslant x} \tau(n) = \sum_{n \leqslant x} \left[\frac{x}{n}\right] \leqslant \sum_{n \leqslant x} \frac{x}{n} = x \log x + \gamma x + O(1).$$

Similarly,

$$\sum_{n\leqslant x}\tau(n)\geqslant x\log x+\gamma x-x+O(1).$$

Therefore

$$\sum_{n\leqslant x}\tau(n)=x\log x+O(x).$$

To improve the above estimation, consider that $\sum\limits_{n\leqslant x}\left[\frac{x}{n}\right]$ is the number of positive integer points under the hyperbola $nn'=x$. Therefore

$$\begin{aligned}\sum_{n\leqslant x}\tau(n)&=\sum_{nn'\leqslant x}1\\&=\sum_{n\leqslant\sqrt{x}}\sum_{n'\leqslant\frac{x}{n}}1+\sum_{n'\leqslant\sqrt{x}}\sum_{n\leqslant\frac{x}{n'}}1-\sum_{n,n'\leqslant\sqrt{x}}1\\&=2\sum_{n\leqslant\sqrt{x}}\left[\frac{x}{n}\right]-\left[\sqrt{x}\right]^2\\&\leqslant 2\sum_{n\leqslant\sqrt{x}}\frac{x}{n}-x\\&=2x\left(\log\sqrt{x}+\gamma+O(\frac{1}{\sqrt{x}})\right)-x\\&=x\log x+(2\gamma-1)x+O(\sqrt{x}).\end{aligned}$$

Similarly,

$$\sum_{n\leqslant x}\tau(n)\geqslant x\log x+(2\gamma-1)x-2\sqrt{x}+O(\sqrt{x}).$$

Therefore

$$\sum_{n\leqslant x}\tau(n)=x\log x+(2\gamma-1)x+O(\sqrt{x}).$$

Mertens' 1895 proof

The finite sum $T(x)$ to be estimate in this proof is

$$T(x)=\sum_{n\leqslant x}\frac{r(n)}{n^{1/2}}.$$

We will show that

$$T(x)=2\sqrt{x}L(1,\chi)+O(1). \tag{8}$$

Thus $T(x)=O(1)$ if $L(1,\chi)=0$.

However, since $r(n) \geqslant 0$ and $r(n^2) \geqslant 1$,

$$T(x) \geqslant \sum_{n \leqslant \sqrt{x}} \frac{r(n^2)}{n} \geqslant \sum_{n \leqslant \sqrt{x}} \frac{1}{n} = \frac{1}{2} \log x + \gamma + O(x^{-1/2}),$$

which contradicts with $T(x) = O(1)$.

To show (8), we need a lemma.

4.1 Lemma *Let χ be a non-principal character. Then for any $s > 0$ and function $N(x) > x$ (which can be taken to be $N(x) = \infty$), we have*

$$\sum_{x \leqslant n \leqslant N(x)} \frac{\chi(n)}{n^s} = O(x^{-s}).$$

In particular, we have

$$\sum_{n \leqslant x} \frac{\chi(n)}{n^s} = L(s, \chi) + O(x^{-s}).$$

Proof: We may assume $N = N(x)$ is an integer. Since

$$|X_{x,y}| := \left| \sum_{x \leqslant n \leqslant y} \chi(n) \right| \leqslant \phi(m),$$

by Abel's summand method, we have

$$\begin{aligned} \left| \sum_{x < n \leqslant N} \frac{\chi(n)}{n^s} \right| &= \left| \sum_{x < n \leqslant N-1} X_{x,n} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{X_{x,N}}{N^s} \right| \\ &\leqslant \sum_{x < n \leqslant N-1} \phi(m) \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| + \frac{\phi(m)}{N^s} \\ &= \frac{\phi(m)}{([x]+1)^s} < \frac{\phi(m)}{x^s}. \end{aligned}$$

□

Now, we have

$$\begin{aligned} T(x) &= \sum_{n \leqslant x} \sum_{d|n} \frac{\chi(d)}{n^{1/2}} = \sum_{nn' \leqslant x} \frac{\chi(n)}{(nn')^{1/2}} \\ &= \sum_{n \leqslant \sqrt{x}} \frac{\chi(n)}{n^{1/2}} \sum_{n' \leqslant \frac{x}{n}} \frac{1}{n'^{1/2}} + \sum_{n' \leqslant \sqrt{x}} \frac{1}{n'^{1/2}} \sum_{\sqrt{x} \leqslant n \leqslant \frac{x}{n'}} \frac{\chi(n)}{n^{1/2}}. \end{aligned}$$

By Lemma 4.1,

$$\begin{aligned} \sum_{n' \leqslant \sqrt{x}} \frac{1}{n'^{1/2}} \sum_{\sqrt{x} \leqslant n \leqslant \frac{x}{n'}} \frac{\chi(n)}{n^{1/2}} &= \sum_{n' \leqslant \sqrt{x}} \frac{1}{n'^{1/2}} O(x^{-1/4}) \\ &= (2x^{1/4} + O(1)) O(x^{-1/4}) = O(1). \end{aligned}$$

Therefore

$$T(x) = \sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{n^{1/2}} \left(2\frac{\sqrt{x}}{n^{1/2}} - 3 + n^{1/2}O(x^{-1/2})\right) + O(1)$$
$$= 2\sqrt{x} \sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{n} - 3 \sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{n^{1/2}} + \sum_{n\leqslant\sqrt{x}} \chi(n)O(x^{-1/2}) + O(1).$$

Using Lemma 4.1 again, we see

$$T(x) = 2\sqrt{x}L(1,\chi) + O(1) - 3L(\frac{1}{2},\chi) + O(x^{-1/4}) + O(x^{-1/2}) + O(1)$$
$$= 2\sqrt{x}L(1,\chi) + O(1),$$

which shows (8).

Mertens' 1899 proof

The finite sum $T(x)$ to be estimate in this proof is

$$T(x) = \sum_{n\leqslant x} r(n)(1 - \frac{n}{x}).$$

We will show that

$$\sum_{n\leqslant x} r(n)(1 - \frac{n}{x}) = \sum_{d\leqslant x} \chi(d) f(\frac{x}{d}), \tag{9}$$

where the function $f(x)$ is defined to be the finite sum

$$f(x) = \sum_{n\leqslant x} (1 - \frac{n}{x}).$$

The function $f(x)$ has good properties such as

4.2 Lemma *The function $f(x)$ is non-negative, continuous and monotonically increasing.*

By estimating $f(x)$, we will show that

$$f(x) = \frac{1}{2}x + O(1). \tag{10}$$

With these facts, we can estimate $T(x)$ as follows.
For $0 \leqslant y < x$, write

$$S = \sum_{d\leqslant y} \chi(d) f(\frac{x}{d}).$$

Then, by (10) and Lemma 4.1

$$\begin{aligned} S &= \sum_{d\leqslant y}\chi(d)(\frac{x}{2d}+O(1)) \\ &= \frac{x}{2}\sum_{d\leqslant y}\frac{\chi(d)}{d}+(\sum_{d\leqslant y}\chi(d))O(1) \\ &= \frac{x}{2}L(1,\chi)+\frac{x}{2}O(y^{-1}). \end{aligned}$$

As for $T(x)-S$, by the Abel's summand method, we have

$$\begin{aligned} \left|\sum_{y<d\leqslant x}\chi(d)f(\frac{x}{d})\right| &\leqslant \phi(m)(\sum_{y<d\leqslant x-1}\left|f(\frac{x}{d})-f(\frac{x}{d+1})\right|+f(\frac{x}{[x]})) \\ &\leqslant \phi(m)f(\frac{x}{y})=\frac{\phi(m)x}{2y}+O(1) \end{aligned}$$

Therefore for any function $y(x)$ such that $0\leqslant y(x)<x$, we have

$$T(x)=\frac{x}{2}L(1,\chi)+O(xy^{-1}). \tag{11}$$

On the other hand, since $r(n)\geqslant 0$ and $r(n^2)\geqslant 0$,

$$\begin{aligned} \sum_{n\leqslant x}r(n)(1-\frac{n}{x}) &\geqslant \sum_{n\leqslant\sqrt{x}}r(n^2)(1-\frac{n^2}{x}) \geqslant \sum_{n\leqslant\sqrt{x}}(1-\frac{n^2}{x}) \\ &= [\sqrt{x}]-\frac{[\sqrt{x}]([\sqrt{x}]+1)(2[\sqrt{x}]+1)}{6x}. \\ &\geqslant \frac{2}{3}\sqrt{x}+O(1), \end{aligned}$$

which contradicts with (11).

Properties of $f(x)$

We first prove the following lemma, which implies Lemma 4.2 and (10).

4.3 Lemma *The function $f(x)$ is non-negative and continuous. For x not an integer, we have*

$$f'(x)=\frac{[x]([x]+1)}{2x^2}.$$

In particular, $f(x)$ is monotonically increasing. Moreover, we have

$$f(x)=\frac{x}{2}-\frac{1}{x}\int_0^x\{t\}\mathrm{d}t.$$

Proof: First, we have

$$f(x) = [x] + 1 - \frac{[x]([x]+1)}{2x},$$

which is obviously continuous in stretches. For n an integer, we have

$$\begin{aligned}\lim_{x\to n^-} &= n - 1 + 1 - \frac{(n-1)(n-1+1)}{2n} = \frac{n+1}{2},\\ \lim_{x\to n^+} &= n + 1 - \frac{2(n+1)}{2n} = \frac{n+1}{2}.\end{aligned}$$

Therefore $f(x)$ is continuous.

For x not an integer, then both $[x]$ and $[x]([x]+1)$ are constant in a sufficiently small neighborhood of x. Hence

$$f'(x) = \frac{[x]([x]+1)}{2x^2}.$$

Note that the right side of above is always nonnegative and that $f(x) \geqslant 0$, then $f(x)$ is monotonically increasing.

The function $g(x) = 1 - \frac{t}{x}$ is continuous and monotonically decreasing to 0, thus we have

$$\begin{aligned}f(x) &= \int_0^x (1-\frac{t}{x})\mathrm{d}[t]\\ &= \int_0^x (1-\frac{t}{x})\mathrm{d}t - \int_0^x (1-\frac{t}{x})\mathrm{d}\{t\}\\ &= (t - \frac{t^2}{2x})\Big|_0^x - (1-\frac{t}{x})\{t\}\Big|_0^x + \frac{1}{x}\int_0^x \{t\}\mathrm{d}t\\ &= x - \frac{x}{2} - \frac{1}{x}\int_0^x \{t\}\mathrm{d}t = \frac{x}{2} - \frac{1}{x}\int_0^x \{t\}\mathrm{d}t.\end{aligned}$$ □

Now, it remains to prove (9).

We have

$$\begin{aligned}\sum_{n\leqslant x} r(n)(1-\frac{n}{x}) &= \sum_{n\leqslant x}(1-\frac{n}{x})\sum_{d|n}\chi(d)\\ &= \sum_{n\leqslant x}\sum_{d|n}\chi(d) - \frac{1}{x}\sum_{n\leqslant x} n\sum_{d|n}\chi(d)\\ &= \sum_{d\leqslant x}\chi(d)\sum_{n\leqslant \frac{x}{d}} 1 - \frac{1}{x}\sum_{d\leqslant x} d\chi(d)\sum_{n\leqslant \frac{x}{d}} n\\ &= \sum_{d\leqslant x}\chi(d)(\sum_{n\leqslant \frac{x}{d}} 1 - \sum_{n\leqslant \frac{x}{d}}\frac{n}{\frac{x}{d}})\\ &= \sum_{d\leqslant x}\chi(d) f(\frac{x}{d}).\end{aligned}$$

§ 5 Class number formula I: the characters

In this section, we will give explicit formula for Dirichlet characters and determine all real primitive characters. To do this, we first factorize $\mathbb{G}(m)$ into a product of cyclic groups. Then, such factorization also works for its dual group and hence gives all characters of m. After that, we consider the relation between their order and period, which further gives all real primitive characters.

Dirichlet characters

Note that taking unit group is right adjoint to the group ring construction. In particular, the unit group of a product of some rings is isomorphic to the product of their unit groups. Thus, by the Chinese Reminder Theorem, we have

$$\mathbb{G}(m) \cong \prod_i \mathbb{G}(p_i^{r_i})$$

and hence

$$\widehat{\mathbb{G}(m)} \cong \bigoplus_i \widehat{\mathbb{G}(p_i^{r_i})}$$

Therefore, to determine characters of m in general, it suffices to determine in the case m is a prime power.

Before going forward, we point out that the elements of the dual group of any cyclic group $\mathbb{Z}/n$ are of the form

$$\chi(\overline{g}) = \omega^g,$$

where ω is a n-th root of unity and g is any representative of $\overline{g}$ in $\mathbb{Z}$. So, to determine characters of q for q a prime power, it suffices to determine how $\mathbb{G}(q)$ factorizes into cyclic groups.

Let $q = p^r$ with p an odd prime. By Lemma 5.1, $\mathbb{G}(q) \cong \mathbb{Z}/\phi(q)$. For any integer n with $(n, q) = 1$, let $v(n)$ the image of $\overline{n}$ under this isomorphism. Then each character of q is given by a composition of v with an elements of $\widehat{\mathbb{Z}/\phi(q)}$. In particular, let ω be a $\phi(q)$-th root of unity, then the corresponding character is given by

$$\chi(n) := \omega^{v(n)}.$$

By Lemma 5.1, the story is similar for $q = 2$ or 4, while when $q = 2^r$ with $r \geqslant 3$, there is no primitive root $\bmod q$.

By Lemma 5.4, $\mathbb{G}(2^r) \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{r-2}$. We use sgn (resp. v) to denote the composition $\mathbb{G}(2^r) \to \mathbb{Z}/2$ (resp. $\mathbb{G}(2^r) \to \mathbb{Z}/2^{r-2}$). Then each character of 2^r is given by two compositions $\delta \circ \mathrm{sgn}, \rho \circ v$ with $\delta \in \widehat{\mathbb{Z}/2}$ and $\rho \in \widehat{\mathbb{Z}/2^{r-2}}$. In particular, let ω be a 2^{r-2}-th root of unity, then the corresponding characters are given by

$$\chi(n) = \omega^{v(n)}, \quad \chi'(n) = (-1)^{\mathrm{sgn}(n)}\omega^{v(n)}.$$

Primitive roots

By a ***primitive root*** $\bmod m$, we mean an integer g such that $\overline{g}$ is a generator of the multiplicative group $\mathbb{G}(m)$. If such a primitive root exists, then $\mathbb{G}(m) \cong \mathbb{Z}/\phi(m)$ via equation $g^{v(n)} \equiv n \pmod{q}$.

5.1 Lemma *There exists a primitive root* $\bmod m$ *if and only if* m *is taken to be any one of the following forms.*

- $m = 2$*;*
- $m = 4$*;*
- m *is an odd prime power;*
- m *is a product of an odd prime power with* 2*.*

Proof: Factorize m into primes:

$$m = p_1^{r_1} \cdots p_k^{r_k}.$$

Then, for any integer g with $(m, g) = 1$, we have

$$g^{\phi(p_i^{r_i})} \equiv 1 \pmod{p_i^{r_i}}, \quad i = 1, \cdots, k.$$

Let n be the *least common multiple* of $\phi(p_1^{r_1}), \cdots, \phi(p_k^{r_k})$. Then

$$g^n \equiv 1 \pmod{p_i^{r_i}}, \quad i = 1, \cdots, k.$$

Hence

$$g^n \equiv 1 \pmod{m}.$$

Note that $n = \phi(m)$ if and only if $\phi(p_1^{r_1}), \cdots, \phi(p_k^{r_k})$ are relatively prime to each other. Since

$$\phi(p_i^{r_i}) = p_i^{r_i - 1}(p_i - 1),$$

it must be even whenever $p_i^{r_i} > 2$. Therefore $n = \phi(m)$ only if m is either a prime power or a product of an odd prime power with 2.

Let p be an odd prime. Then $\mathbb{F}_p^{\times} \cong \mathbb{Z}/(p-1)$ and hence there exists a primitive root $\bmod p$, saying g. Then either g or $g + p$ satisfies the condition of Lemma 5.2 and hence serves as a primitive root $\bmod p^r$ for all $r > 1$. Moreover, either g or $g + p^r$ is an odd primitive root $\bmod p^r$ and hence serves as a primitive root $\bmod 2p^r$ by the Chinese Reminder Theorem.

It is easy to see that 1 is a primitive root $\bmod 2$ and that -1 is a primitive root $\bmod 4$. However, if $m = 2^r$ with $r \geqslant 3$, then there are no primitive roots since Lemma 5.3. □

5.2 Lemma *Let* p *be an odd prime and* g *a primitive root* $\bmod p$ *such that* $g^{p-1} \not\equiv 1 \pmod{p^2}$*. Then* $g^{\phi(p^{r-1})} \not\equiv 1 \pmod{p^r}$ *for* $r \geqslant 2$*. In particular,* g *is a primitive root* $\bmod p^r$*.*

Proof: Let g be an integer such that $v_p(g^{p-1}-1)=1$. We need to show $v_p(g^{\phi(p^r)}-1)=r$ for $r \geqslant 1$.

Write $g^{p-1}-1=ph$ with $v_p(h)=0$. We have

$$g^{\phi(p^r)}-1=(ph+1)^{p^{r-1}}-1=\sum_{i=0}^{p^{r-1}-1}\binom{p^{r-1}}{i}(ph)^{p^{r-1}-i}.$$

Let $a_i=\binom{p^{r-1}}{i}(ph)^{p^{r-1}-i}$, then

$$v_p(a_i)=p^{r-1}+r-1-v_p(i)-i.$$

For $i \leqslant p^{r-2}$, it is easy to see that $v_p(a_i) \geqslant r+1$.

For $p^{r-2}<i<p^{r-1}$, we have

$$i+v_p(i) \leqslant p^{r-1}-p^{v_p(i)}+v_p(i).$$

Since $p^j-j \geqslant 2$ for $j \geqslant 1$, we see that $v_p(a_i) \geqslant r+1$ if $v_p(i) \geqslant 1$. If $v_p(i)=0$ but $i \leqslant p^{r-1}-2$, then $i+v_p(i) \leqslant p^{r-1}-2$ and hence $v_p(a_i) \geqslant r+1$.

However, for $i=p^{r-1}-1$, we have

$$v_p(a_{p^{r-1}-1})=p^{r-1}+r-1-0-(p^{r-1}-1)=r.$$

Therefore $v_p(g^{\phi(p^r)}-1)=r$. □

5.3 Lemma *For any odd integer g, we have $g^{2^{r-2}} \equiv 1 \pmod{2^r}$ if $r>2$.*

Proof: It suffices to show $v_2(g^{2^{r-2}}-1) \geqslant r$. Writing $g=2h+1$, we have

$$v_2(g^{2^{r-2}}-1)=v_2\left(\sum_{i=0}^{2^{r-2}-1}\binom{2^{r-2}}{i}(2h)^{2^{r-2}-i}\right).$$

Let $a_i=\binom{2^{r-2}}{i}(2h)^{2^{r-2}-i}$. Then

$$v_2(a_i)=r-2-v_2(i)+(2^{r-2}-i)(1+v_2(h)) \geqslant 2^{r-2}+r-2-v_2(i)-i.$$

If $v_2(h) \geqslant 1$, then the above is obviously greater than r. So, we may assume $v_2(h)=0$ and hence

$$v_2(a_i)=2^{r-2}+r-2-v_2(i)-i.$$

For $i \leqslant 2^{r-3}$, it is easy to see that $v_2(a_i) \geqslant r$.

For $2^{r-3}<i<2^{r-2}$, we have

$$i+v_2(i) \leqslant 2^{r-2}-2^{v_2(i)}+v_2(i).$$

Since $2^j-j \geqslant 2$ for $j \geqslant 2$, we see that $v_2(a_i) \geqslant r$ if $v_2(i) \geqslant 2$. If $v_2(i) \leqslant 1$ but $i<2^{r-2}-2$, then $i+v_2(i) \leqslant 2^{r-2}-2$ and hence $v_2(a_i) \geqslant r$.

Therefore, we have

$$v_2(g^{2^{r-2}}-1) \geqslant \min\{r, v_2(a_{2^{r-2}-2}+a_{2^{r-2}-1})\},$$

and it reminds to show $v_2(a_{2^{r-2}-2}+a_{2^{r-2}-1}) \geqslant r$.

One can see that

$$\begin{aligned} v_2(a_{2^{r-2}-2}) &= 2^{r-2}+r-2-1-(2^{r-2}-2) = r-1, \\ v_2(a_{2^{r-2}-1}) &= 2^{r-2}+r-2-0-(2^{r-2}-1) = r-1. \end{aligned}$$

Hence $v_2(a_{2^{r-2}-2}+a_{2^{r-2}-1}) > r-1$. □

This lemma show that $\mathbb{G}(2^r)$ is not cyclic if $r > 2$. However, we have

5.4 Lemma *For $q = 2^r$ with $r > 2$, any element of $\mathbb{G}(q)$ has the form $\overline{\pm 5^v}$, where $v = 0, 1, \cdots, 2^{r-2}-1$.*

Proof: Since $\overline{5} \in \mathbb{G}(q)$, we see all those $\overline{\pm 5^v}$ lie in $\mathbb{G}(q)$. It reminds to show they are distinct. To do this, it suffices to show there is no $0 \leqslant v \leqslant 2^{r-2}-1$ such that $5^v \equiv 1 \pmod{2^r}$ or $5^v \equiv -1 \pmod{2^r}$.

By computing the 2-adic valuation of $(1+4)^{2^{r-2}}-1$, we see that the order of 5 is at most 2^{r-2}.

By computing the 2-adic valuation of $(1+4)^{2^{r-3}} - 2^{r-3}\cdot 4 - 1$, we see that $5^{2^{r-3}} \not\equiv 1 \pmod{2^r}$. Since the order of 5 must divide $\phi(2^r) = 2^{r-1}$, the order of 5 is 2^{r-2}. In particular, we see that $5^v \not\equiv 1 \pmod{2^r}$.

By computing the 2-adic valuation of $(1+4)^{2^{r-3}} - 2^{r-3}\cdot 4 + 1$, we see that $5^{2^{r-3}} \not\equiv -1 \pmod{2^r}$. Since the order of -1 is 2, we see that $5^v \not\equiv -1 \pmod{2^r}$ as desired. □

Primitive characters

Note that any character χ of $\mathbb{G}(m)$ is a periodic function on $\mathbb{Z}$ having a period m. If m is furthermore the *least positive period* of χ, then we say it is a ***primitive character***.

If χ is imprimitive, then the least positive period m' of χ divides m. We claim that χ can be induced from a primitive character χ' of m'.

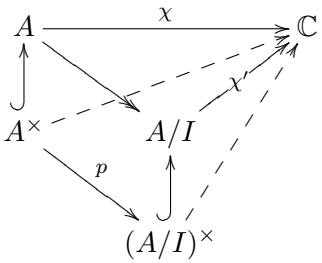
In fact, we will prove this in a much more general context. Let A be a commutative ring and I an ideal of it. By a ***character*** χ of I, we mean a class function module I on A which defines an irreducible representation of $(A/I)^\times$ and takies 0 as value of other classes.

5.5 Lemma *If a character χ of I on A is a class function module J, then it is also a character of J.*

Proof: By replacing A/I by A, J/I by I, we see that it suffices to prove in the case I is trivial.

Now, let χ be a class function module I on A which defines an irreducible representation of $A^\times$ and takes 0 as values of other elements. We need to show that χ is a character of I.

Since χ is a class function module I, the following diagram commutes.



Here, χ' is the function induced by χ and p is the restriction of the projection $A \to A/I$ to $A^\times$, which is automatically a group homomorphism. Thus, it reminds to show p is surjective. Then the restriction of χ' to $(A/I)^\times$ defines an irreducible representation of $(A/I)^\times$.

Let $X = \operatorname{Spec} A$ be the prime spectrum of A and $V(I)$ its closed subset consists of primes which contains I. Then an element $y \in A/I$ is a function on $V(I)$ and its preimage in A is a function on X such that its restriction to $V(I)$ agrees with y. in particular, those elements in $(A/I)^\times$ has preimages which are functions on X taking non-zero values in $V(I)$. If we know that $V(I)$ is already X, then we see that those functions are in $A^\times$ and hence p is surjective.

Assume $V(I) \neq X$. Then there exists some $g \in I$ such that $V(g) \neq X$. Let f be a function taking non-zero values in $V(g)$ and 0 outside of $V(g)$. Then $f \notin A^\times$ and $\chi(f) = 0$. On the other hand, $f + g$ taking non-zero values everywhere, hence $f + g \in A^\times$. Then $\chi(f + g) \neq 0$, which contradicts to χ is a class function module I. □

Let χ be an imprimitive character of m with m' its least positive period. Then χ is induced from a primitive character χ' of m'. Moreover, we have

$$L(1, \chi) = \prod_{p \nmid m} (1 - \chi(p)p^{-1})^{-1} = \prod_{p \nmid m'} (1 - \chi'(p)p^{-1})^{-1} = L(1, \chi').$$

Thus to show $L(1, \chi) \neq 0$ in general, we only need to consider real primitive characters.

Note that there is a natural monomorphism between left exact functors

$$\operatorname{Hom}(-, \mathbb{Z}/2) \rightarrowtail \operatorname{Hom}(-, S^1)$$

identifying elements of $\operatorname{Hom}(G, \mathbb{Z}/2)$ with characters of G taking real values. Therefore, real characters of m must be the products of real characters of q with q runs over primary factors of m. Thus, to determine all real primitive

characters of m in general, it suffices to determine real primitive characters of $q = p^r$ a prime power.

For $q = p^r$ an odd prime power with $r > 1$, let χ be a real character of p^r. We claim that χ is imprimitive. First, we have seen

$$\chi(n) = e_{\phi(p^r)}(kv(n))$$

for some $0 < k < \phi(p^r)$. Notice that $e^{2\pi ix}$ is real if and only if x is an *super integer*, meaning either an integer or the sum of an integer with $\frac{1}{2}$. Hence $2k\phi(p^r)^{-1}$ is an integer. Since $\phi(p^r) = p^{r-1}(p-1)$, we have $p \mid k$. However, if this is the case, χ must have a period p^{r-1}. Indeed, since

$$(n + p^{r-1})^p \equiv n^p \pmod{p^r},$$

we have

$$mv(n + p^{r-1}) \equiv mv(n) \pmod{\phi(p^r)},$$

which shows $\chi(n + p^{r-1}) = \chi(n)$.

For $q = p$ an odd prime, we have seen before that the only non-principal real character of p is the Legendre symbol $\left(\frac{-}{p}\right)$, which is obviously primitive.

Likewise, the only non-principal real character of 4 is

$$\chi_4(n) = \begin{cases} 1 & n \equiv 1 \pmod 4, \\ -1 & n \equiv 3 \pmod 4. \end{cases}$$

which is also primitive.

For $q = 8$, there are three non-principal real characters: the imprimitive character induced from χ_4, the primitive character

$$\chi_8(n) = \begin{cases} 1 & \pm 1 \pmod 8, \\ -1 & \pm 3 \pmod 8, \end{cases}$$

and their product $\chi_4\chi_8$, which is also primitive.

For $q = 2^r$ with $r > 3$, any real character χ of q must be imprimitive. Indeed, χ is of the form

$$\chi(n) = (-1)^{t\,\mathrm{sgn}(n)} e_{2^{r-2}}(kv(n)).$$

Note that this implies that $k2^{3-r}$ is an integer and hence k is even. Then $e_{2^{r-2}}(kv(n))$ has period 2^{r-1}. Indeed, we have

$$kv(n + 2^{r-1}) \equiv kv(n) \pmod{2^{r-2}}$$

since

$$\begin{aligned} 5^{kv(n+2^{r-1})} &\equiv (-1)^{k\,\mathrm{sgn}(n+2^{r-1})} 5^{kv(n+2^{r-1})} \\ &\equiv (n + 2^{r-1})^k \\ &\equiv n^k \\ &\equiv (-1)^{k\,\mathrm{sgn}(n)} 5^{kv(n)} \\ &\equiv 5^{kv(n)} \pmod{2^r} \end{aligned}$$

in this case. On the other hand, $(-1)^{\mathrm{sgn}(n)}$ has period 4 since

$$\begin{aligned}(-1)^{\mathrm{sgn}(n+4)} &\equiv (-1)^{\mathrm{sgn}(n+4)}5^{v(n+4)}\\ &\equiv (n+4)^k\\ &\equiv n^k\\ &\equiv (-1)^{k\,\mathrm{sgn}(n)}5^{kv(n)}\\ &\equiv (-1)^{k\,\mathrm{sgn}(n)} \pmod 4\end{aligned}$$

in this case. Therefore, χ also has period 2^{r-1} and hence is imprimitive.

We organize the above classification as follows.

5.6 Proposition *Let $q = p^r$ a prime power. Then, χ is a primitive character of q if and only if the subgroup of $\widehat{\mathbb{G}(q)}$ generated by it contains a maximal p-cyclic subgroup. In particular, the real primitives of q are*

- $\left(\frac{\cdot}{p}\right)$ *if $q = p$ an odd prime,*
- χ_4 *if $q = 4$,*
- χ_8 *and $\chi_4\chi_8$ if $q = 8$.*

Proof: We give an abstract proof as follows.

Let $\mathbb{Z}_p$ denote the ring of p-adic integers. Since

$$\mathbb{Z}_p = \varprojlim_r \mathbb{Z}/p^r$$

and taking unit group is left exact, we have

$$\mathbb{G}(p^\infty) := \mathbb{Z}_p^\times = \varprojlim_r \mathbb{G}(p^r)$$

and hence

$$\widehat{\mathbb{G}(p^\infty)} = \varinjlim_r \widehat{\mathbb{G}(p^r)}.$$

By Lemma 5.5, we can the translation map in the above direct limit is injective and identify characters of p^r with imprimitive characters of p^{r+1}. Hence the group $\widehat{\mathbb{G}(p^\infty)}$ is obtained from a regular filtration

$$0 < \widehat{\mathbb{G}(p)} < \cdots < \widehat{\mathbb{G}(p^r)} < \widehat{\mathbb{G}(p^{r+1})} < \cdots < \widehat{\mathbb{G}(p^\infty)}.$$

and its decomposition into homogeneous terms is

$$\widehat{\mathbb{G}(p^\infty)} \cong \bigoplus_r \widehat{\mathbb{G}(p^r)}/\widehat{\mathbb{G}(p^{r+1})}.$$

By a *character of p^∞*, we mean an element in $\widehat{\mathbb{G}(p^\infty)}$. Then the filtration and the decomposition shows that the

- χ lies in $\widehat{\mathbb{G}p^r}$ if and only if it has period p^r,
- and in particular, χ lies in $\widehat{\mathbb{G}(p^r)}/\widehat{\mathbb{G}(p^{r+1})}$ if and only if it is a primitive character.

In the case p is an odd prime, every $\widehat{\mathbb{G}(p^r)}$ is cyclic of order $\phi(p^r)$, hence

$$\widehat{\mathbb{G}(p^r)} = \left\{ \chi \in \widehat{\mathbb{G}(p^\infty)} \middle| \chi^{\phi(p^r)} = \mathbf{1} \right\}.$$

In particular, a character of p^r is primitive if and only if its order has factor p^{r-1} if and only if it generates at least the whole Sylow p-subgroup of $\widehat{\mathbb{G}(p^r)}$.

As for $p = 2$, we have

$$\mathbb{G}(2^r) \cong \begin{cases} 0 & r = 1, \\ \mathbb{Z}/2 & r = 2, \\ \mathbb{Z}/2 \times \mathbb{Z}/\phi(2^{r-1}) & r > 2. \end{cases}$$

Hence for $r > 2$,

$$\widehat{\mathbb{G}(2^r)} = \mathbb{Z}/2 \times \left\{ \chi \in \widehat{\mathbb{G}(2^\infty)} \middle| \chi^{\phi(2^{r-1})} = \mathbf{1} \right\}.$$

In particular, a character of 2^r is primitive if and only if its order has factor 2^{r-2} if and only if it generates at least the whole maximal cyclic 2-subgroup of $\widehat{\mathbb{G}(2^r)}$. □

§ 6 Class number formula II: the quadratic discriminants

In this section, we write the real primitive characters into a uniform form, which reveal the hidden connection between them and quadratic fields. To do this, we introduce the *Kronecker symbol* via observations based on the law of quadratic reciprocity. After that, we obtain the condition when there is a real primitive character of m, which happens to be the same for m to be a quadratic discriminant.

Kronecker symbol

We have seen the real primitives of q are

- $\left(\frac{-}{p}\right)$ if $q = p$ an odd prime,
- χ_4 if $q = 4$,
- χ_8 and $\chi_4\chi_8$ if $q = 8$.

We now write them into a uniform form.

Recall that *the law of quadratic reciprocity* says

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

for p, q two odd primes and the *supplementary laws* says

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

for all odd prime p.

Let $q^* = (-1)^{\frac{q-1}{2}} q$, the law of quadratic reciprocity is equivalent to say

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

Inviting the ***Jacobi symbol***, which is

$$\left(\frac{a}{n}\right) := \left(\frac{a}{q_1}\right)^{r_1} \cdots \left(\frac{a}{q_k}\right)^{r_k}$$

for a any integer and $n = q_1^{r_1} \cdots q_k^{r_k}$ any positive odd integer, we see that Jacobi symbol is also multiplicative for a. For any odd integer n, we define $n^* := (-1)^{\frac{n-1}{2}} n$. Note that, for any odd integers a, b, we have

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

Therefore

$$(n_1 n_2)^* = n_1^* n_2^*,$$

and in particular,

$$n^* = \prod_i (p_i^*)^{r_i}$$

for any $n = \prod_i p_i^{r_i}$ a positive odd integer. Let $a = \prod_j q_j^{s_j}$ another positive odd integer, we have

$$\left(\frac{n^*}{a}\right) = \prod_{i,j} \left(\frac{p_i^*}{q_j}\right)^{r_i+s_j} = \prod_{i,j} \left(\frac{q_j}{p_i}\right)^{r_i+s_j} = \left(\frac{a}{n}\right).$$

As for the *supplementary laws*, we already have

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

for any positive odd integer n. Since for any odd integers a, b,

$$\frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2,$$

we have

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Now the symbol $\left(\frac{a}{n}\right)$ has already been defined for all integer a and all positive odd integer n. To extend the definition to all integer $(a,n) = 1$ and keep it being multiplicative, it suffices to define $\left(\frac{}{2}\right)$ and $\left(\frac{}{-1}\right)$.

Let n be any positive odd integer. Then, we can define

$$\left(\frac{n^*}{2}\right) := \left(\frac{2}{n}\right), \quad \text{and} \quad \left(\frac{n^*}{-1}\right) := \left(\frac{-1}{n}\right).$$

To determine the rest values, it suffices to determine

$$\left(\frac{2}{2}\right), \left(\frac{-1}{2}\right), \left(\frac{2}{-1}\right), \left(\frac{-1}{-1}\right).$$

As we hope $\left(\frac{a}{n}\right)$ keep 0 whenever $(a,n) \neq 1$, we put

$$\left(\frac{2}{2}\right) = 0.$$

As we hope to keep the supplementary law at least for odd integers, we put

$$\left(\frac{-1}{-1}\right) = (-1)^{\frac{-1-1}{2}} = -1$$

and

$$\left(\frac{2}{-1}\right) = (-1)^{\frac{(-1)^2-1}{8}} = 1.$$

Note that the law of quadratic reciprocity will not hold for a, n both negative since

$$\left(\frac{-1}{-1}\right)\left(\frac{-1}{-1}\right) = 1 \neq (-1)^{\frac{-1-1}{2}\frac{-1-1}{2}}.$$

More seriously, $(-1)^{\frac{a-1}{2}}$ with a even will not be real and hence the formula is nonsense. Therefore, the law of quadratic reciprocity need to modified in this general case.

For n any integer, we use n' to denote its odd part which means n' is odd and n/n' is a power of 2. We define $n^* = (-1)^{\frac{n'-1}{2}} n$. Then, the *law of quadratic reciprocity* can be modified into

$$\left(\frac{a}{|n|}\right) = \left(\frac{n^*}{a}\right),$$

which covers the law of quadratic reciprocity for Jacobi symbol and holds for all values we have defined. Since $2^* = 2$ the remind one $\left(\frac{-1}{2}\right)$ have to be defined as

$$\left(\frac{-1}{2}\right) = \left(\frac{2}{-1}\right) = 1.$$

In this way, we have already defined the symbol $\left(\frac{a}{n}\right)$ for all relatively prime integers a, n. This symbol is called the ***Kronecker symbol***.

For any odd integer n, we have

$$\chi_4(n) = \left(\frac{-1}{n}\right) = \left(\frac{-4}{n}\right),$$
$$\chi_8(n) = \left(\frac{2}{n}\right) = \left(\frac{8}{n}\right),$$
$$\chi_4(n)\chi_8(n) = \left(\frac{-8}{n}\right),$$

For any integer n with $p \nmid n$ for the odd prime p, we have

$$\left(\frac{n}{p}\right) = \left(\frac{p^*}{n}\right).$$

6.1 Proposition *There is a real primitive character of d and it is of the form $\left(\frac{d}{-}\right)$ if and only if d is a product of relatively prime factors each of them is one of the follows.*

- $-4, 8$ *or* -8*;*
- $(-1)^{\frac{p-1}{2}}p$ *with p an odd prime.*

Quadratic forms

How does those d looks like?

6.2 Proposition *There exists a real primitive character of d if and only if d belongs to one of the following sets.*

- $N_1 := \{n | n \equiv 1 \pmod 4$ *is square free*$\}$.
- $N_2 = \{4n | n \equiv 2, 3 \pmod 4$ *is square free*$\}$.

Proof: First, since for any integer n with $n \equiv 1 \pmod 4$, $n^* = n$, we see that the following sets are equal.

$$1 + 4\mathbb{Z} = \left\{ \prod_p (-1)^{\frac{p-1}{2}} p \middle| (-1)^{\frac{p-1}{2}} p \equiv 1 \pmod 4 \right\}.$$

Therefore the set of d such that there exists a real primitive character of d is precisely

$$N_1 \sqcup (-4N_1 \cup 8N_1 \cup -8N_1).$$

One can see that $-4N_1 \cup 8N_1 \cup -8N_1 = N_2$. □

Recall that (see, for instance Neukirch §I.2, Ex 4)

6.3 Lemma *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Assume D is square free. Then the integral basis of $\mathcal{O}_K$ is*

$$\begin{cases} 1, \sqrt{D} & D \equiv 2, 3 \pmod 4, \\ 1, \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4. \end{cases}$$

In particular, the discriminant of K is

$$d(K) = \begin{cases} 4D & D \equiv 2, 3 \pmod 4, \\ D & D \equiv 1 \pmod 4. \end{cases}$$

We see that there exists real primitive character of d if and only if d is a discriminant of a quadratic field.

A ***quadratic form*** f is a polynomial in $\mathbb{Z}[x, y]$ of the form

$$f = ax^2 + bxy + cy^2.$$

Its ***discriminant*** is

$$d(f) = b^2 - 4ac.$$

Note that either $4 \mid d(f)$ or $d(f) \equiv 1 \pmod 4$.

The discriminant $d(f)$ of a quadratic form

$$ax^2 + bxy + cy^2$$

is also a discriminant of the quadratic polynomial

$$ax^2 + bx + c.$$

Let θ be a root of it. Then $a\theta$ is an integer in the quadratic field $K = \mathbb{Q}(\theta)$ and hence $\mathfrak{a} = \mathbb{Z} + a\theta\mathbb{Z}$ is an order in K whose discriminant is again $d(f)$. By the general proposition, we have

$$d(f) = (\mathcal{O}_K : \mathfrak{a})^2 d_K$$

where d_K denotes the discriminant of K.

6.4 Lemma *Let f be an n-th irreducible polynomial with leading coefficient a and a root θ. Then f is primitive if and only if $1, a\theta, \cdots, (a\theta)^{n-1}$ form an integral basis of $K = \mathbb{Q}(\theta)$.*

By a ***fundamental discriminant***, we mean an integer d such that any quadratic form f with $d(f) = d$ has the property $(a, b, c) = 1$.

6.5 Proposition *d is a discriminant of a quadratic form if and only if it is a product of a discriminant of a quadratic field with a square. In particular, d is a fundamental discriminant if and only if $d \in N_1$ or N_2.*

Proof: Let $f = ax^2 + bxy + cy^2$ be a quadratic form whose discriminant d belongs to $N_1 \cup N_2$ but $(a, b, c) \neq 1$. Then $(a, b, c) = 2$ and $d \in N_2$. However, in this case, $\frac{f}{2}$ is also a quadratic form whose discriminant is $\frac{1}{4}d$. Thus $d \in 4N_1$ which contradicts to $d \in N_2$.

Conversely, □

The group $\mathrm{SL}(2, \mathbb{Z})$ actions on the space $\mathcal{Q}(d)$ of quadratic forms with a given discriminant d. Let $h(d)$ be the cardinal of $\mathcal{Q}(d)/SL(2, \mathbb{Z})$, called the ***class number*** of d.

6.6 Lemma *$h(d)$ is finite.*

6.7 Lemma *Let $f(x, y) = ax^2+bxy+cy^2$ be a quadratic form with discriminant d. If $d < 0$, $f(x, y)$ is definite. If $d > 0$, $f(x, y)$ is indefinite.*

Proof: $f(1, 0) = a$ while $f(b, -2a) = -da$.

$4af(x, y) = (2ax + by)^2 - dy^2$. Thus $af \geqslant 0$. □

6.8 Lemma *Each class contains a form such that $|b| \leqslant |a| \leqslant |c|$.*

Proof: Let f be a quadratic form in a certain class. Let a be a number such that $|a|$ is minimal in the condition a can be represented by f.

$a = f(s, t)$. exists u, v such that $us - vt = 1$, thus $\begin{pmatrix} s & u \\ t & v \end{pmatrix}$ trans f to a quadratic form (a, b', c') with leading coefficient a. exists h such that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ trans (a, b', c') to (a, b, c) such that $|b| \leqslant |a|$. c is represented by f, thus $|a| \leqslant |c|$. □

Proof: If $d > 0$, we see since $|b| \leqslant |a| \leqslant |c|$,

$$|ac| \geqslant b^2 = d + 4ac > 4ac$$

$$4a^2 \leqslant 4|ac| = -4ac = d - b^2 \leqslant d.$$

$$|b| \leqslant |a| \leqslant \frac{\sqrt{d}}{2}.$$

Hence a, b and thus c are bounded and hence is finite.

If $d < 0$, let $a > 0$, then $c > 0$.

$|b| \leqslant a \leqslant c$.

$$4a^2 \leqslant 4ac = b^2 - d \leqslant |d| + a^2$$

Thus $3a^2 \leqslant |d|$. □

Let $R(n)_f$ be the number of how many ways can we represented by f. Let $R(n) = \sum_f R(n_f)$ where f runs over a set of representatives.

$$R(n) = w \sum_{\nu | n} \left(\frac{d}{\nu}\right)$$

§ A Some lemmas from analysis

Elementary techniques

A.1 Lemma (Abel Summation) *If* $A_{k,l} = \sum_{n=k}^{l} a_n$, *then*

$$\sum_{n=k}^{l} a_n b_n = \sum_{n=k}^{l-1} A_{k,n}(b_n - b_{n+1}) + A_{k,l} b_l.$$

A.2 Lemma *If both* $f(n)$ *and* $g(n)$ *are completely multiplicative functions, then*

$$\sum_{n\leqslant x} f(n) \sum_{d|n} g(d) = \sum_{d\leqslant x} f(d)g(d) \sum_{n\leqslant \frac{x}{d}} f(n).$$

Measures and integrals

A.3 (Measurable sets and measures) content

A.4 Lemma *For* $f(x)$ *a monotonic continuous function with positive value and is decreasing to* 0, *we have*

$$\sum_{n\leqslant x} f(n) = \int_1^x f(t)\mathrm{d}t - f(1) + O(f(x)).$$

Proof: We have

$$\sum_{n\leqslant x} f(n) = \int_1^x f(t)\mathrm{d}[t] = \int_1^x f(t)\mathrm{d}t - \int_1^x f(t)\mathrm{d}\{t\}.$$

Since

$$\int_1^x f(t)\mathrm{d}\{t\} = f(x)\{x\} - \int_1^x \{t\}\mathrm{d}f(t)$$

and

$$\int_1^x \{t\}\mathrm{d}f(t) \geqslant \int_1^x \mathrm{d}f(t) = f(x) - f(1),$$

we have

$$\int_1^x f(t)\mathrm{d}\{t\} \leqslant f(1) - (1 - \{x\})f(x).$$

On the other hand, we have

$$\begin{aligned}\int_1^x f(t)\mathrm{d}\{t\} &= \int_1^\infty f(t)\mathrm{d}\{t\} - \int_x^\infty f(t)\mathrm{d}\{t\} \\ &\geqslant -f(1) + (1 - \{x\})f(x).\end{aligned}$$

Therefore

$$\int_1^x f(t)\mathrm{d}\{t\} = f(1) + O(f(x)),$$

and hence

$$\sum_{n\leqslant x} f(n) = \int_1^x f(t)\mathrm{d}t - f(1) + O(f(x)).$$

□

Complex analysis

A.5 Proposition *$D(s)$ converges at s_0, then it converges uniformly in $\Re(s) > \Re(s_0)$.*

A.6 Lemma *If a sequence of holomorphic functions converges uniformly to a function. Then this function is also holomorphic.*

A.7 Lemma (Holomorphic implies analytic) *If f holomorphic in a domain Ω. Let D be a disc in Ω with center z_0. Then we can expanse f as*

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

where $a_n = \frac{f^{(n)}(z_0)}{n!}$.

Proof: Let

$$f(z) = \frac{1}{2\pi i} \int_C \frac{f(\xi)}{\xi - z} \mathrm{d}\xi.$$

where $C = \partial D$.

Write

$$\frac{1}{\xi - z} = \frac{1}{\xi - z_0} \cdot \frac{1}{1 - \frac{z - z_0}{\xi - z_0}}.$$

There exists $0 \leqslant r \leqslant 1$ such that $\left|\frac{z - z_0}{\xi - z_0}\right| < r$.

$$\begin{aligned} f(z) &= \frac{1}{2\pi i} \int_C \frac{f(\xi)}{\xi - z_0} \sum_{n=0}^{\infty} (\frac{z - z_0}{\xi - z_0})^n \mathrm{d}\xi \\ &= \sum_{n=0}^{\infty} (\frac{1}{2\pi i} \int_C \frac{f(\xi)}{(\xi - z_0)^{n+1}} \mathrm{d}\xi)(z - z_0)^n \end{aligned}$$

Let M be the maximal of $|f(\xi)|$ and $|\xi - \zeta_0| = t < 1$, then

$$\left|\frac{1}{2\pi i} \int_C \frac{f(\xi)}{(\xi - z_0)^{n+1}} \mathrm{d}\xi\right| < \frac{M}{t^n}.$$

□

Dirichlet series

A ***(general) Dirichlet series*** is a series of the form

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n z},$$

where a_n, z are complex numbers and $\{\lambda_n\}$ is a strictly increasing sequence of positive numbers that tends to infinity.

A.8 Theorem (Fundamental Theorem) *If a Dirichlet series $\sum_n a_n e^{-\lambda_n z}$ converges at $z = z_0$, then it converges uniformly in every domain of the form $\{z | \Re(z - z_0) \geqslant 0, |\arg(z - z_0)| \leqslant \alpha\}$ with $\alpha < \frac{\pi}{2}$.*

Proof: We may assume $z_0 = 0$. We now want to show that for any $\epsilon > 0$, there exists an integer N such that for any $k, l > N$ and any z lies in the domain $\Re(z) \geqslant 0, |\arg(z)| \leqslant \alpha$,

$$\left| \sum_{n=k}^{l} a_n e^{-\lambda_n z} \right| < \epsilon.$$

Since $\sum_n a_n = f(0)$ converges, for any $\epsilon' > 0$, there exists an integer N such that for any $k, l > N$,

$$\left| \sum_{n=k}^{l} a_n \right| < \epsilon'.$$

Let $A_{k,l} = \sum_{n=k}^{l} a_n$, then

$$\begin{aligned}
\left| \sum_{n=k}^{l} a_n e^{-\lambda_n z} \right| &= \left| \sum_{n=k}^{l-1} A_{k,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{k,l} e^{-\lambda_l z} \right| \\
&\leqslant \sum_{n=k}^{l-1} \epsilon' \left| e^{-\lambda_n z} - e^{-\lambda_{n+1} z} \right| + \epsilon' \\
&= \sum_{n=k}^{l-1} \epsilon' \left| z \int_{\lambda_n}^{\lambda_{n+1}} e^{-tz} \mathrm{d}t \right| + \epsilon' \\
&\leqslant \sum_{n=k}^{l-1} \epsilon |' z| \int_{\lambda_n}^{\lambda_{n+1}} \left| e^{-tz} \right| \mathrm{d}t + \epsilon' \\
&= \sum_{n=k}^{l-1} \frac{\epsilon' |z|}{|\Re(z)|} (e^{-\lambda_n \Re(z)} - e^{-\lambda_{n+1} \Re(s)}) + \epsilon' \\
&= \frac{\epsilon' |z|}{|\Re(z)|} (e^{-\lambda_k \Re(z)} - e^{-\lambda_l \Re(z)}) + \epsilon' \\
&\leqslant (2 \frac{|z|}{|\Re(z)|} + 1) \epsilon' \leqslant (2 \cos \alpha + 1) \epsilon'.
\end{aligned}$$

□

By the fundamental theorem, any Dirichlet series $f(z) = \sum_n a_n e^{-\lambda_n z}$ admits an ***abscissa of convergence*** σ_c, which is either a real number or the formal bounds $\infty, -\infty$ such that f converges for all z with $\Re(z) > \sigma_c$ and for no z with $\Re(z) < \sigma_c$.

Since a Dirichlet series $f(z) = \sum_n a_n e^{-\lambda_n z}$ locally uniformly converges in $\Re(z) > \sigma_c$ and each part sum is holomorphic, by the *Weierstrass principle*, $f(z)$ defines a holomorphic function $f(z)$ on $\Re(z) > \sigma_c$ and the *differentiated series*

$$-\sum_{n=1}^{\infty} a_n \lambda_n e^{-\lambda_n z}$$

is locally uniformly convergent to $f'(z)$ in $\Re(z) > \sigma_c$.

A.9 Lemma (Landau) *Let $f(z) = \sum_n a_n e^{-\lambda_n z}$ be a Dirichlet series such that $a_n \geqslant 0$. Suppose f converges when $\Re(z) > r$ and the function f can be extended analytically to a function holomorphic in a neighborhood of the point $z = r$. Then there exists a number $\epsilon > 0$ such that f converges for $\Re(z) > r - \epsilon$. In particular, σ_c is a singularity of the function $f(z)$.*

Proof: We may assume $r = 0$. f is holomorphic in a disc

$$D(1, \epsilon) := \{z \,|\, |z - 1| \leqslant 1 + \epsilon\},$$

with $\epsilon > 0$. Since $f^{(k)}(1) = \sum_n a_n (-\lambda_n)^k e^{-\lambda_n}$, we can expand f in $D(1, \epsilon)$ as the power series

$$f(z) = \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!} (z - 1)^k$$

We have

$$f(-\epsilon) = \sum_{k=0}^{\infty} \frac{1}{k!} (1 + \epsilon)^k (-1)^k f^{(k)}(1).$$

Therefore

$$\begin{aligned} f(-\epsilon) &= \sum_{k=0}^{\infty} \sum_n \frac{1}{k!} (1 + \epsilon)^k (-1)^k a_n \lambda_n^k e^{-\lambda_n} \\ &= \sum_n a_n e^{-\lambda_n} \sum_{k=0}^{\infty} \frac{1}{k!} ((1 + \epsilon)\lambda_n)^k \\ &= \sum_n a_n e^{-\lambda_n (-\epsilon)}. \end{aligned}$$

Then, by the lemma, f converges in $\Re(z) > -\epsilon$. □

§ B Other applications of the methods

Gauss' criterion for Euclidean constructions

A ***Fermat prime*** is a prime of the form $q = 2^k + 1$ (note that in this case, k must be a power of 2).

B.1 Theorem *The regular n-gon can be inscribed in a given circle by a Euclidean construction (i.e. using ruler and compasses only), if and only if n is a product of a power of 2 with distinct Fermat primes.*

Note that the above theorem can be interpreted by the following lemma.

B.2 Lemma *The followings are equivalent.*

1. *The regular n-gon can be inscribed in a given circle by a Euclidean construction.*
2. *$z = \cos\frac{2\pi}{n}$ can be obtained from a tower of real square roots.*
3. *The maximal real subfield of n-th cyclotomic field $\mathbb{Q}(\xi_n)$ can be generated by a tower of quadratic extensions.*

If this is the case, we say n is a constructible degree.

Assume $n > 2$. Note that the degree of the maximal real subfield of $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$ is $\frac{1}{2}\phi(n)$. Thus to show the necessity of the condition is equivalent to show

B.3 Lemma *$\phi(n)$ is a power of 2 if and only if n is a product of a power of 2 with distinct Fermat primes.*

Proof: This follows from the *Euler's product formula*

$$\phi(n) = n\prod_{p|n}(1 - \frac{1}{p}).$$

□

Next, we show that the condition is sufficient. First, note that whenever two numbers n_1, n_2 with $(n_1, n_2) = 1$ are constructible degrees, then so is $n_1 n_2$. As the construction of 2^k-gons are easy, it reminds to show Fermat primes are constructible degrees.

From now on, let $q = 2^k + 1$ with $k > 1$ since the 3-gon, i.e. regular triangle, is easy to construct.

Let $\xi = e^{\frac{2\pi \mathrm{i}}{q}}$. For $1 \leqslant i \leqslant k$, let $s_i = 2^i$ and let

$$\eta_j^{(i)} = \sum_{v(n)\equiv j \pmod{s_i}} \xi^n, \quad j = 1, 2, \cdots, s_i,$$

be the *Gauss periods* for s_i. Let $Q_i := \mathbb{Q}(\{\eta_j^{(i)}\}_{j\in[s_i]})$.

B.4 Lemma *When $1 \leqslant i \leqslant k-1$, $Q_i \subset \mathbb{R}$.*

Proof: Since $2v(-1) \equiv v(1) \pmod{q-1}$, we see that $v(-1) \equiv 0 \pmod{s_i}$ for all $1 \leqslant i \leqslant k-1$. For those i, $v(-n) = v(n)$, thus $\bar{\eta}_j^{(i)} = \eta_j^{(i)}$ which implies they lie in $\mathbb{R}$. □

B.5 Lemma *For $1 \leqslant i \leqslant k-1$ and $j \in [s_i]$, we have $[Q_i(\eta_j^{(i+1)}, \eta_{j+s_i}^{(i+1)}) : Q_i] = 2$.*

Proof: Let $F(x)$ be the $\mathbb{Z}[t]$-polynomial

$$F(x) = \left(t - \sum_{v(n) \equiv j \pmod{s_{i+1}}} x^n\right)\left(t - \sum_{v(n) \equiv j+s_i \pmod{s_{i+1}}} x^n\right).$$

Then for any n with $v(n) \equiv 0 \pmod{s_i}$, either $v(n) \equiv 0 \pmod{s_{i+1}}$ or $v(n) \equiv s_i \pmod{s_{i+1}}$. In the former case, $v(nn') \equiv v(n') \pmod{s_{i+1}}$ and thus $F(\xi^n) = F(\xi)$. In the later case, $v(nn') \equiv v(n') + s_i \pmod{s_{i+1}}$ and thus $F(\xi^n) = F(\xi)$ again. By Lemma 2.4, there exist $b_1(t), \cdots, b_{s_i}(t) \in \mathbb{Z}[t]$ such that

$$(t - \eta_j^{(i+1)})(t - \eta_{j+s_i}^{(i+1)}) = F(\xi) = b_1(t)\eta_1 + \cdots + b_{s_i}(t)\eta_{s_i}.$$

From the above, we see $\eta_j^{(i+1)}, \eta_{j+s_i}^{(i+1)}$ are roots of a quadratic polynomial over Q_i as desired. □

Using the above lemma, we see $Q_k = \mathbb{Q}(\xi_q)$, Q_{k-1} is its maximal real subfield and

$$\mathbb{Q} \subset Q_1 \subset Q_2 \subset \cdots \subset Q_{k-1}$$

is a tower of real quadratic extensions.

References

Algebra

[Lang 2002] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Atiyah 1969] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.