Notes of Elementary Number Theory

Yuang Lu

2025 Fall

Chapter 1

2025/9/11

Office Hour: Friday 4:00 p.m. – 5:00 p.m. Homework hand in before class.

1.1 Unique Factorization in Rings

Theorem 1.1. Any integer n can be written of the form

$$n = (-1)^{\varepsilon(n)} p_1^{r_1} \cdots p_m^{r_m}, \quad \varepsilon(n) = \begin{cases} -1, & n < 0, \\ 0, & n > 0, \end{cases}$$

where p_i are prime numbers.

Proof. Existence. WLOG, $n > 0$. $n = 1$ is trivial. Suppose that the factorization works for any $m \leq n-1$. If n is prime number, OK. If n is not a prime, then $\exists \text{prime} p < n$ s.t. $p \mid n$. $n = pn_1, n_1 < n$. By induction, $n_1 = p_1^{r_1} \cdots p_m^{r_m}$, and $n = pp_1^{r_1} \cdots p_m^{r_m}$.

Uniqueness. If $n = p_1^{r_1} \cdots p_m^{r_m} = q_1^{t_1} \cdots q_s^{t_s}$. $\exists 1 \leq i \leq s$, s.t. $p_1 = q_i$. By induction, the factorization of $\frac{M}{p_1}$ is same to $\frac{M'}{p_1}$. □

The goal of the course is to generalize this property to general rings.

Definition 1.1. Let R be an *integeral domain* if $ab = 0 \implies a = 0$ or $b = 0$.

We call $p \in R$ *irreducible* if $ab = p \implies a$ is a unit or b is a unit.

We call p a *prime* if $p \neq 0$ and $p \neq$ unit and $p \mid ab \implies p \mid a$ or $p \mid b$.

We ask when primes are always irreducibles and when irreducibles are always primes.

Proposition 1.2. prime $\implies$ irreducible.

Proof. For a prime p, assume $p = ab$, so $p \mid ab$ and hence $p \mid a$ or $p \mid b$. Suppose $p \mid a$, then $\exists c \in R$ s.t. $pc = a$. We have $pcb = p$, and $p(cb - 1) = 0$. Since p is prime, $p \neq 0$. Since R is an integral domain, $cb = 1$ and thus b is a unit. □

The converse is not true for general integral doamin.

Definition 1.2. If any $a \in R$ can be uniquely factored into the form

$$a = p_1^{r_1} \cdots p_m^{r_m},$$

with p_i being prime, then we call R *uniquely factorization domain.*

A natural consequence is that irreducibles are always primes.

Proposition 1.3. irreducible $\implies$ prime.

Proof. If p is irreducible, $\exists$ a factorization $p = up_1^{r_1} \cdots p_m^{r_m} = p_1 b = p_1 \cdot \text{unit}$. So p is a prime. □

Definition 1.3. If any ideal I of R is principal, i.e., $I = (a)$ for some $a \in R$, then R is a *principal ideal domain*.

An easy fact is that $\mathbb{Z}$ is a PID. We would like to prove that for PIDs, irreducibles are primes and further prove that PID $\subseteq$ UFD.

Assume R is a PID. $d \in R$ is called "the greatest common divisor" of a and b if it satisfies:

- $d \mid a$ and $d \mid b$.
- for any $d' \mid a$ and $d' \mid b$, we have $d' \mid d$.

Lemma 1.4. If d, d' are both g.c.d. of a and b, then $d = ud'$[1], for some unit u.

Proof. Since $d \mid d' \mid d$, then $\exists a, b \in R$ s.t. $ad = d'$ and $bd' = d$, so $abd = d$. It implies that $ab = 1$ and hence $d' = ad$ where a is unit. □

Proposition 1.5. Any $a, b \in R$ have a g.c.d. d and $(d) = (a, b)$ as ideals. (Under the assumption that R is a PID, and so are the results below.)

Proof. Since R is PID, we have $(a, b) = (d)$ for some d, and hence $d \mid a$, $d \mid b$. For any $d' \mid a$ and $d' \mid b$, and since there exist s, t such that $d = sa + tb$, we have $d' \mid d$. By definition, d is g.c.d. of a and b. □

Corollary 1.6. If a, b are coprime (i.e. their g.c.d. is 1) in R, then $(a, b) = R$.

Proposition 1.7. If R is PID, irreducible $\implies$ prime.

Proof. For any irreducible $p \in R$, suppose that $p \mid ab$ and $p \nmid a$, then let $d = \gcd(p, a)$. $d \mid p \implies \exists c \in R$ s.t. $p = cd$. If d is not a unit, $d = p \implies p \mid a$. A contradiction. Hence d is a unit and a, p are coprime. There exists $s, t \in R$ s.t. $as + tp = 1$. $abs + tpb = b$ and since $p \mid ab$ and $p \mid p$, we have $p \mid b$. p is prime. □

Lemma 1.8. For any $m \in R$, there exists irreducible element $b \in R$ s.t. $b \mid m$.

Proof. Suppose m irreducible. Trivial.

Suppose m reducible. $\exists$ non-units $a_1, b_1 \in R$ s.t. $a_1 b_1 = m$. Apparently, if this lemma fails, then we obtain infinitely many reducibles $\{a_i\}$ s.t. $(a_i) \subsetneq (a_{i-1})$ since

$$a_i = a_{i+1} b_{i+1} \tag{1.1}$$

. Consider

$$\bigcup_{i=1}^{\infty} (a_i),$$

which is an ideal of R. R is a PID, so there exists $b \in R$ s.t.

$$(b) = \bigcup_{i=1}^{\infty} (a_i).$$

But $\exists n$ s.t. $b = (a_n)$ and $(a_{n+m}) = (a_n)$ for any $m \geq 1$, a contradiction to (1.1). □

[1] Call such d and d' *associate*.

Theorem 1.9. PID $\subseteq$ UFD.

Proof. For any $a \in R$, $\exists$ irreducible b_1, which is also prime, s.t. $a = b_1 a_1$. And we have $a_1 = b_2 a_2 \implies a = b_1 b_2 a_2$. If has to stop at some n by the argument of the previous lemma. We thus reach the conclusion that $a = b_1 b_2 \cdots b_n$ with b_i being prime. □

Definition 1.4. We call R a *Noetherian domain* if any chain of ideals is stable, i.e., for

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

$\exists n$ s.t. $I_n = I_m$ for any $m \geq n$.

Proposition 1.10. The above definition is equivalent to any ideal being finitely generated.

Proof. " $\implies$ ". Suppose $\exists I$ is not f.g., any $a_1 \in I$, $\exists a_2$ s.t. $a_2 \notin (a_1)$. $I \neq (a_1, a_2) \triangleq I_2 \implies \exists a_3 \in I$ s.t. $a_3 \notin (a_1, a_2)$. $I_3 \triangleq (a_1, a_2, a_3)$. The process goes on and we obtain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. A contradicition to the original defintion.

" $\impliedby$ ". For any $I_1 \subseteq I_2 \subseteq \cdots$. We know $I_0 \triangleq \bigcup_{i=1}^{\infty} I_i$ is an ideal of R, so $\exists \alpha_1, \ldots, \alpha_m \in I_0$ s.t. $I_0 = (\alpha_1, \ldots, \alpha_m)$. Then $\exists n$ s.t. $\alpha_i \in I_n$ for any $i \in \{1, \ldots, m\}$. It follows that $I_n = I_0 = I_m$ for any $m \geq n$, and $I_n \subseteq I_m \subseteq I_0 = I_n$. □

Question: What is the relation between Noetherian domains and UFDs?

Take $K[x, y, z]/(x^2 - yz)$.

Proposition 1.11. If R is Noetherian, then $R[x]$ is Noetherian.

Proof. For I an ideal in R, take $I_0 = \{f_a : f \in I\}$, where f_a is the leading coefficient of f. Then $\exists f_1, \ldots, f_s$ s.t. $(f_{1a}, \ldots, f_{sa}) = I_0$. We can only consider $f \in I$ s.t. $\deg(f) \leq \max\{f_1, \ldots, f_s\} - 1 \triangleq m$. Consider $I_1 = \{f_a : \deg(f) = m\}$, which is f.g. And further consider f with smaller degrees. □

Then $K[x, y, z]/(x^2 - yz)$ is Noetherian, but $x \mid x^2 = yz$ yet $x \nmid y, x \nmid z$, so this ring is not UFD. For the converse, consider $R = \mathbb{C}[x_1, x_2, \ldots]$ which is not Noetherian, but a UFD.

Definition 1.5. We call R a *Euclidean domain* if there is a function

$$\lambda : R \setminus \{0\} \to \{0, 1, \ldots\}$$

s.t. for any $a, b \in R$, $b \neq 0$, there exists $c, d \in R$, s.t. $a = bc + d$ for $d = 0$ or $\lambda(d) < \lambda(b)$.

Example. $\mathbb{Z}$ is Eucildean domain, since we can have $\lambda(n) = |n|$.

Proposition 1.12. Eucildean domain $\implies$ PID.

Proof. Suppose R is a ED. For any ideal I of R let n be $\min\{\lambda(a) \mid a \in I \setminus \{0\}\}$. Let $a \in I$ s.t. $\lambda(a) = n$. Then $(a) = I$, else we have $b \in I \setminus (a)$, $b = sa + r$ with $\lambda(r) < \lambda(a)$, which is impossible. □

Example (Non-example)**.** $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is PID but not ED.

Example. Some examples of ED.

- $k[x]$, k is a field, $\lambda(f) \triangleq \deg(f)$.
- $k[[x]]$, $\lambda(f) = \{n : a_m \neq 0\}$.

- $k\langle x\rangle \triangleq \{f \in k[[x]] : \lim_{i\to\infty} a_i = 0\}$, where k satisfies strong triangluar inequality[2], with $\lambda(f) = \{i : a_i \neq 0\}$.

Proposition 1.13. $\mathbb{Z}[i]$ is ED with $\lambda(a+bi) = a^2 + b^2$.

Proof. For $c+di, a+bi \neq 0$, WTS $\exists s, r$ s.t. $s(a+bi) + r = c + di$, $\lambda(s) < \lambda(a+bi)$. Let $\frac{c+di}{a+bi} = \alpha + \beta i \in \mathbb{R} + \mathbb{R}i$. $\exists m, n \in \mathbb{Z}$ s.t. $|m - \alpha| < \frac{1}{2}$, $|n - \beta| < \frac{1}{2}$. Consider $c + di = (a+bi)(m+ni) + A + Bi$. Then

$$\alpha + \beta i - (m + ni) = \frac{A + Bi}{a + bi},$$

so

$$\lambda(A + Bi) = \lambda(a+bi)\lambda((\alpha - m) + (\beta - n)i) < \lambda(a+bi). \qquad \square$$

Remark. $\mathbb{Z}[\omega]$ is a Euclidean domain with $\lambda(a + b\omega) = a^2 + b^2 + ab$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. The proof is the same as above.

Proposition 1.14 (Application of Unique Factorization)**.** In $\mathbb{Z}$, there are infinitely many prime numbers.

Proof. Suppose $p_1, \ldots, p_m$ are all the primes of $\mathbb{Z}$. Consider $p_1 \cdots p_m + 1$. Since $\mathbb{Z}$ is UFD,

$$p_1 \cdots p_m + 1 = p_1^{r_1} \cdots p_m^{r_m}.$$

We must have $r_i = 0$, $p_1 \cdots p_m + 1 = 1$. A contradicition. $\square$

1.2 Möbius Function

Definition 1.6. The Möbius function μ is defined as

$$\mu(n) \triangleq \begin{cases} 1, & n = 1, \\ 0, & n \text{ is not square free}, \\ (-1)^m, & n = p_1 \cdots p_m \text{ for } p_i \neq p_j \text{ with } i \neq j. \end{cases}$$

Proposition 1.15. If $n > 1$,

$$\sum_{d|n} \mu(d) = 0.$$

Proof. Let $n = \prod_{i-1}^{m} p_i^{r_i}$. Then

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|n, p_1 || d} \mu(d) + \sum_{d|n, p_1^2 | d} \mu(d) + \sum_{d|n, p_1 \nmid d} \mu(d) \\ &= \sum_{d|\frac{n}{p_1^{r_1}}} \mu(d)(-1) + \sum_{d|\frac{n}{p_1^{r_1}}} \mu(d) = 0. \end{aligned} \qquad \square$$

[2] In a field k with norm, the strong triangluar inequality is the following.

$$|a + b| \leq \max\{|a|, |b|\}.$$

Some examples include p-adic integers $\mathbb{Z}_p$, with $\left|\sum_{i=0}^{\infty} a_i p^i\right| = p^{-\min\{i : a_i \neq 0\}}$

Chapter 2

2025/9/18

Theorem 2.1 (Möbius Inversion Theorem)**.** If $F(n) = \sum_{d|n} f(d)$, then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Remark. Notation: For $f, g : \mathbb{Z}_{\geq 0} \to \mathbb{R}$,

$$f \circ g(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Then the theorem is equivalent to $\mu \circ F = \mu \circ f \circ \varphi$.

Proof. We have

$$\mu \circ f \circ \varphi = f \circ (\mu \circ \varphi) = f \circ \delta_{1n} = f \qquad \square$$

Definition 2.1. The following function is called *Euler function*.

$$\phi(n) = \#\left\{1 \leq a \leq n \mid (a, n) = 1\right\}.$$

Lemma 2.2. $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.

Proof. The following map is an isomorphism.

$$\begin{aligned} U(mn) &\to U(m) \times U(n) \\ \overline{a} &\mapsto (a \mod m, a \mod n). \end{aligned} \qquad \square$$

Theorem 2.3. $\phi \circ \varphi(n) = n$.

Proof. If $n = 1$, trivial. Suppose that for $n \geq 1$, this result holds for any $m \leq n - 1$. Write $n = p_1^{r_1} \cdots p_n^{r_n}$.

If $n = p$,

$$\sum_{d|p} \phi(d) = \phi(p) + \phi(1) = p - 1 + 1 = p.$$

Else, $n = p_1 m$, $m \geq 2$.

$$\sum_{d|n} \phi(d) = \sum_{d|n, p_1^{r_1} | d} \phi(d) + \sum_{d|n, p_1^{r_1} \nmid d} \phi(d) = \sum_{d|\, n/p_1^{r_1}} \phi(d) + \sum_{d|\, n/p_1} \phi(d) = \phi\left(p_1^{r_1}\right) \frac{n}{p_1^{r_1}} + \frac{n}{p_1} = n. \qquad \square$$

2.1 Congruence

Notation: $m \in \mathbb{Z}_{\geq 1}$. $a, b \in \mathbb{Z}$. For $a, b \in \mathbb{Z}$, if $m \mid a - b$, then we put $a \equiv b \pmod{m}$.

Proposition 2.4. 1. $a \equiv a \pmod{m}$.

2. $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

3. $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Thus $\equiv$ is an equivalent relation.

Definition 2.2. Fix $m \in \mathbb{Z}_{\geq 1}$. Put $\overline{a} := \{a + km \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$. Call $\overline{a}$ a *congruence class modulo m*.

Proposition 2.5. 1. $\overline{a} = \overline{b}$ iff $a \equiv b \pmod{m}$.

2. $\overline{a} = \overline{b}$ iff $a \not\equiv \pmod{m}$ iff $\overline{a} \cap \overline{b} = \varnothing$.

3. There are precisely m congruence classes modulo m, namely $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Definition 2.3. Map

$$\begin{aligned} \bar{\cdot}_m : \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ a &\mapsto a + m\mathbb{Z} \end{aligned}$$

is a ring homomorphism.

We often write $\bar{\cdot} := \bar{\cdot}_m$.

For any $f(\underline{x}) = \sum_{I \in \mathbb{Z}^n_{\geq 0}} a_I \underline{x}^I$, we put $\overline{f} = \sum_{I \in \mathbb{Z}^n_{\geq 0}} \overline{a}_I \underline{x}^I \in \mathbb{Z}/m\mathbb{Z}[\underline{x}]$. The number of solutions of $f(x) = 0$ modulo m is the number of

$$(\overline{b}_1, \ldots, \overline{b}_n) \in (\mathbb{Z}/m\mathbb{Z})^n$$

s.t. $\overline{f}(b_1, \ldots, b_n) = 0$.

Definition 2.4. $ax \equiv b \pmod{m}$ has solution iff $\gcd(a, m) \mid b$. If it has solution, the number of solutions is equal to $\gcd(a, m)$.

Proof. Let $d := \gcd(a, m)$. " $\Longleftarrow$ ". $ax \equiv b \pmod{m} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. Since $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, $\exists s, t \in \mathbb{Z}$ s.t. $s\frac{a}{d} + t\frac{m}{d} = 1$ and hence

$$\frac{a}{d} s \frac{b}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

" $\Longrightarrow$ ". Suppose for some x, $ax \equiv b \pmod{m}$, $\exists k \in \mathbb{Z}$, $ax - b = km$. $d \mid ax - km = b$.

For the second part, since $\exists s, t \in \mathbb{Z}$ s.t. $s\frac{a}{d} \equiv 1 \pmod{\frac{m}{d}}$, $x \equiv \frac{b}{d} s \pmod{\frac{m}{d}}$. Hence $\left\{x + \frac{m}{d} i : i = 0, 1, \ldots, d-1\right\}$ is the set of solution of $ax \equiv b \pmod{m}$. □

Corollary 2.6. If $\gcd(a, m) = 1$, then $ax \equiv b \pmod{m}$ has unique solution.

Corollary 2.7. $ax \equiv b \pmod{p}$, where $a \not\equiv 0 \pmod{p}$ has unique solution.

Proposition 2.8. An element $\overline{a}$ in $\mathbb{Z}/m\mathbb{Z}$ is a unit iff $\gcd(a, m) = 1$.

Proof. $\overline{a}$ is a unit iff $ax \equiv 1 \pmod{m}$ has solution iff $\gcd(a, m) \mid 1$ iff $\gcd(a, m) = 1$. □

As a result, there are exactly $\phi(m)$ units in $\mathbb{Z}/m\mathbb{Z}$.

Proposition 2.9. $\mathbb{Z}/m\mathbb{Z}$ is a field iff $m = p$.

Proof. If $m = p$, by the above corollary.

Otherwise $m = m_1 m_2$, with $m_1, m_2 \geq 2$, known $\overline{m_1 m_2} = 0$ but $\overline{m_1} \neq 0 \overline{m_2} \neq 0$. It follows that $\overline{m_1}$, $\overline{m_2}$ are zero divisors. $\mathbb{Z}/m\mathbb{Z}$ is not an ID hence not a field. □

Corollary 2.10 (Euler's Theorem)**.** If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Define $U(\mathbb{Z}/m\mathbb{Z}) := \left\{\overline{a} \in \mathbb{Z}/m\mathbb{Z} \mid \exists \overline{b}, \overline{a}\overline{b} = \overline{1}\right\}$ is a group under $\times$.

Proof. $\overline{a}^{\#U(\mathbb{Z}/m\mathbb{Z})} = \overline{1}$. □

Theorem 2.11 (Fermat's little theorem)**.** $\gcd(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}$.

Proposition 2.12 (Wilson's theorem)**.**

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. For any $a \not\equiv 1, p-1, a \in \{1, \ldots, p-1\}$, $\exists b \neq a$ s.t. $ab \equiv 1 \pmod{p}$. Make a pairing $(a, \sigma(a)), \ldots$ in the above way with $\frac{p-3}{2}$ pairs. Then

$$(p-1)! \equiv 1 \cdot (p-1) \sum_{i=1}^{\frac{p-3}{2}} a_i \sigma(a_i) \equiv -1 \pmod{p}.$$ □

Generalization. Suppose R is a PID. For any $a, b, m \in R$, $ax \equiv b \pmod{m}$ has solution iff $b \in (a, m)$, i.e. $\gcd(a, m) \mid b$. The number of solutions can be infinite, as in $R = \mathbb{C}[t]$,

$$(t-a)x \equiv 0 \pmod{(t-a)(t-b)}$$

has all $z(t-b)$ as its solutions.

Proposition 2.13. $R/(m)$ is field iff m is prime.

Proof. m is a prime, then for any $a \notin (m)$, WTS $\exists b \in R$, s.t. $ab \equiv 1 \pmod{m}$. Since $(a, m) = R$, there exists $b, t \in R$ s.t. $ab + mt = 1$.

If m is not a prime, then it is not irreducible, and hence $m = m_1 m_2$ where m_1, m_2 are not units. Then m_1, m_2 are both zero-divisors in $R/(m)$, contradicting with $R/(m)$ being a field. □

Corollary 2.14. If $f \in k[x]$ is irreducible, then $k[x]/(f(x))$, often called *residue field*.

Lemma 2.15. R is PID. If $a_1, \ldots, a_n$ are all coprime to m, so is $a_1 \cdots a_n$.

Proof. Since $U(R/(m))$ is a group. $\overline{a} = a + (m) \in U(R/(m))$ iff $(a, m) = R$. Hence if $a_1, \ldots, a_m$ are all coprime to m, then $a_1 \cdots a_m \in U(R/(m))$. □

Lemma 2.16. Suppose that $a_1, \ldots, a_n$ all divide m, and $\gcd(a_i, a_j) = 1$ for all $i \neq j$, then $a_1 \cdots a_m$ divides m.

Proof. By induction, it is enough to consdier $n = 2$ case. Suppose $\gcd(a, b) = 1$ and $a \mid m$, $b \mid m$. There exists c s.t. $ac = m$. WTS $b \mid c$. $\exists s, t$ s.t. $as + bt = 1$, and hence $acs + bct = c$. b divides LHS so divides $RHS = c$ as well. □

Theorem 2.17 (General Chinese Remainder Theorem)**.** Suppose $m_1, \dots, m_n$ are pairwise coprime. $m_1 \cdots m_n = m$. Then

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_n \pmod{m_n} \end{cases} \tag{2.1}$$

has unique solution $x \mod m$.

Proof. By Lemma 2.15, m_j and $\frac{m}{m_j}$ are coprime. $\exists u_j, v_j \in R$ s.t. $u_j m_j + v_j \frac{m}{m_j} = 1$. Then

$$v_j \frac{m}{m_j} \equiv \begin{cases} 1, & \mod m_j, \\ 0, & \mod m_i \text{ where } i \neq j. \end{cases}$$

Take

$$x = \sum_{j=1}^{n} b_j v_j \frac{m}{m_j}$$

as a solution of (2.1).

Suppose x, y are both solution of (2.1). Then $x - y \equiv 0 \pmod{m_j}, j \in \{1, \dots, n\}$. By Lemma 2.16 we have $m \mid x - y$ or $x \equiv y \pmod{m}$. □

Proposition 2.18. If $m = m_1 \cdots m_n$, $m_1, \dots, m_n$ are pairwise coprime, then

$$\begin{aligned} \varphi : R/(m) &\to R/(m_1) \times \cdots \times R/(m_n) \\ a + (m) &\mapsto (a + (m_1), \dots, a + (m_n)) \end{aligned}$$

is a ring isomorphism.

Proof. By CRT, φ is surjective. By Lemma 2.16, φ is injective. □

Corollary 2.19.

$$U(R/(m)) \cong U(R/(m_1)) \times \cdots \times U(R/(m_n)).$$

Corollary 2.20. $R = \mathbb{Z}$, $m = p_1^{r_1} \cdots p_n^{r_n}$, then

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\cong \mathbb{Z}/\left(p_1^{r_1}\right)\mathbb{Z} \times \cdots \times \mathbb{Z}/\left(p_n^{r_n}\right)\mathbb{Z} \\ U(\mathbb{Z}/m\mathbb{Z}) &\cong U(\mathbb{Z}/\left(p_1^{r_1}\right)\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/\left(p_n^{r_n}\right)\mathbb{Z}) \end{aligned}$$

To study the structure of $U(\mathbb{Z}/n\mathbb{Z})$, we only need to study each $U(\mathbb{Z}/(p_i^{r_i})\mathbb{Z})$. Our goal is to prove that $U(\mathbb{Z}/p^r\mathbb{Z})$ is cyclic.

Proposition 2.21 (Step One)**.** $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic.

Lemma 2.22. Let $f \in k[x]$, k is a field. Then f has at most $\deg f$ roots in k.

Proof. By induction. $n = 1$, OK.

Suppose that it holds for any $m \leq n$. Consider $\deg f = n + 1$. If f has no root in k, trivial. Otherwise, $\alpha \in k$ is a root of k. $f(x) = (x - \alpha)g(x)$ with $\deg g = n$. By induction, the number of roots of g in $k \leq n$. □

Proposition 2.23.

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}. \tag{2.2}$$

Proof. (2.2) $\iff$ $x^{p-1}-1 = (x-1)\cdots(x-p+1)$ in $\mathbb{F}_p[x]$. Given that $\forall p \nmid i\ i^{p-1}-1 \equiv 0 \pmod p$, i.e. $1,\ldots,p-1$ are distinct roots of $x^{p-1}-1$. By Lemma 2.22, $x^{p-1}-1 = (x-1)\cdots(x-p+1)$. □

Another proof of Wilson's theorem. Take $x = 0$, then

$$-1 \equiv (-1)(-2)\cdots(-p+1) \equiv (p-1)(p-2)\cdots(p-p+1) \equiv (p-1)! \pmod p. \qquad \square$$

Proposition 2.24. If $d \mid p-1$, then $x^d \equiv 1 \pmod p$ has exactly d distinct roots in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Since

$$x^{p-1} - 1 = \left(x^d - 1\right)\left(x^{d\left(\frac{p-1}{d}-1\right)} + \cdots + 1\right),$$

with the LHS has $p-1$ distinct roots, $x^d - 1$ at most d, and the other component at most $p-1-d$, $x^d - 1$ must have exactly d roots. □

Proof of Proposition 2.21. Let $\psi(n) = \{i \in U(\mathbb{Z}/p\mathbb{Z}) \mid i \text{ has order } n \text{ in } U(\mathbb{Z}/p\mathbb{Z})\}$. Then

$$n = \#\{\overline{x} \in U(\mathbb{Z}/p\mathbb{Z}) \mid x^n \equiv 1 \pmod m\} = \sum_{d\mid n} \psi(d) = \sum_{d\mid n} \phi(d).$$

By Möbius inversion,

$$\psi(n) = \sum_{d\mid n} \mu(d)\frac{n}{d} = \phi(n).$$

Since $\psi(p-1) = \phi(p-1) \geq 1$, there exists $i \in U(\mathbb{Z}/p\mathbb{Z})$ s.t. $\bar{i}$ has order $p-1$. □

Proposition 2.25 (Step Two)**.** $U(\mathbb{Z}/p^r\mathbb{Z})$ is cyclic for any $r \geq 1$.

Proof. $r = 1$, OK.

Suppose it holds for $r = n \geq 1$. Consider $r = n+1$. By inductive assumption, $\exists a \in \{1,\ldots,p^n-1\}$ s.t. $a^{p^{n-1}(p-1)} \equiv 1 \mod p^n$ but not for smaller powers.

Consider $a + kp$, hope to determine some k s.t. $a + kp$ is a primitive root of p^{n+1}. This is equivalent to finding a k s.t.

$$\begin{cases} a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}} \\ a^{p^n s} \equiv 1 \pmod{p^{n+1}}, \quad s \mid p-1 \text{ but } s \neq p-1. \end{cases}$$

Since

$$\begin{aligned}(a+kp)^{p^n s} &= \left(a^{p^n} + a^{p^n-1}kp\cdot p^n + \cdots\right)^s \\ &\equiv a^{p^n s} \equiv a^{p^{n-1}s} \not\equiv 1 \pmod{()p^{n+1}}.\end{aligned}$$

And

$$\begin{aligned}(a+kp)^{(p-1)p^{n-1}} &\equiv a^{(p-1)p^{n-1}} + kp(p-1)p^{n-1}a^{(p-1)p^{n-1}-1} \\ &\equiv 1 + bp^n + a^{-1}kp(p-1)p^{n-1} \mod p^{n+1},\end{aligned}$$

where $1 + bp^n \equiv a^{(p-1)n^{p-1}}$. Take $k(p-1) \not\equiv ab$ and we are done. □

Goal: Solve $x^n \equiv a \pmod m$.

Definition 2.5. If $x^n \equiv a$ has solution, we call a an *n-th power residue*.

Chapter 3

2025/9/25

Since for finite Abelian group G, we have

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_l\mathbb{Z}.$$

Lemma 3.1. If $G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_l\mathbb{Z}$, the equation $nx = b$ is solvable in G, where $n \in \mathbb{Z}$ $b \in G$, iff $\gcd(n, m_i) \mid b_i$ iff $\frac{m_i}{d_i} b_i \equiv 0 \pmod{m_i}$, where $d_i = \gcd(m_i, n)$.

Goal: Find out when $x^n \equiv a \pmod{m}$ is solvable.

Lemma 3.2.

$$(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z},$$

Proof. by proving that $(\mathbb{Z}/2^e\mathbb{Z})^\times = \left\{(-1)^i 5^j \mid i = 0, 1, j = 0, \ldots, 2^{e-2}\right\}$. For j_1, j_2 s.t. $5^{j_1} \equiv 5^{j_2} \pmod{2^e}$, then $5^{j_1 - j_2} \equiv 1 \pmod{2^e}$. If

$$(1+4)^k = 1 + 4k + 4^2 \binom{k}{2} \equiv 1 \pmod{2^e},$$

we have $k = 2^{e-2}$. □

Proposition 3.3. Suppose that a is odd. The equation

$$x^n \equiv a \pmod{2^e}, \quad e \geq 3$$

has solution iff

1. n is odd, or
2. n is even, $a \equiv 1 \pmod 4$, and
$$a^{\frac{e-2}{d}} \equiv 1 \pmod{2^e},$$
where $d = \gcd(e-2, n)$.

Proof. Let $k = 2^{e-2}$, 5 has order k in $\left(\mathbb{Z}/2^{e-2}\mathbb{Z}^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}\right)$. Let $a = (-1)^{i_a} 5^{j_a}$. Then

$$i_a \cdot \frac{2}{\gcd(2, n)} \equiv 0 \pmod 2$$
$$j_a \cdot \frac{2^{e-2}}{\gcd(2^{e-2}, n)} \equiv \pmod{2^{e-2}}.$$

If n is odd, the condition is trivial.

If n is even, $i_a = 2 \iff a \equiv 1 \pmod 4$, and

$$\left(5^{j_a}\right)^{2^{e-2}/\gcd(2^{e-2},n)} \equiv 1 \pmod{2^e} \iff a^{2^{e-2}/\gcd(2^{e-2},n)} \equiv 1 \pmod{2^e}. \qquad \square$$

Corollary 3.4. For $n = 2^l n_0$, $\gcd(n_0, 2) = 1$, if $x^n \equiv a \pmod{2^{2l+1}}$ is solvable, so does $x^n \equiv a \pmod 2^e$ for all $e \geq 2l + 1$.

They have the same number of roots 2^l.

Proof. From $x^n \equiv a \pmod{2^{2l+1}}$ being solvable, we have

$$\begin{gathered} a \equiv 1 \pmod 4 \\ a^{2^{2l-1}/\gcd(2^{2l-1},n)} \equiv 1 \pmod{2^{2l+1}} \quad \Longrightarrow \quad a^{l-1} \equiv 1 \pmod{2^{2l+1}}. \end{gathered}$$

For any $e \geq 2l + 1$, consider

$$a^{2^{e-2}/\gcd(2^{e-2},n)} \equiv a^{2^{e-2}/2^l} = \left(a^{2l+1-2/2^l}\right)^{2^{e-(2l+1)}} = \left(1 + k2^{2l+1}\right)^{2^{e-(2l+1)}} \equiv 1 \pmod{2^e}.$$

For e, the congruence equation has $\gcd(n, 2^{e-2}) = 2^l$ solutions. $\square$

Known $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is a cyclic group of order $p^{r-1}(p-1) = \phi(p^r)$.

Proposition 3.5. $x^n \equiv a \pmod{p^r}$ has solution iff $x^n \equiv a \pmod p$ has solution, where $\gcd(n, p) = 1$.

Proof. $x^n \equiv a \pmod{p^r}$ has solution iff

$$a^{\phi(p^r)/\gcd(n,\phi(p^r))} \equiv 1 \pmod{p^r} \iff a^{p^{r-1}(p-1)/\gcd(n,p-1)} \equiv 1 \pmod{p^r}.$$

Suppose that it works for $r = 1$.

$$a^{p-1/\gcd(p-1,n)} = 1 + pk.$$

Then

$$(1 + pk)^{p^{r-1}} \equiv 1 \pmod{p^r}. \qquad \square$$

Remark. The number of solutions is $\gcd(n, p - 1)$.

For general $x^n \equiv a \pmod m$, write $m = 2^e p_1^{r_1} \cdots p_l^{r_l}$. And the condition and the number of solutions follows.

3.1 Quadratic residue

For p a prime, for any $a \in \mathbb{Z}$, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod p \\ -1, & \text{if } x^2 \not\equiv \pmod p \\ 0, & \text{if } p \mid a. \end{cases}$$

Proposition 3.6. 1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

2. $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3. If $a \equiv b \pmod{p}$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. Since $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, $x^2 \equiv a \pmod{p}$ has solution iff $a^{p-1/\gcd(p-1,2)} \equiv 1 \pmod{p}$ iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. □

Theorem 3.7 (Law of quadratic Reciprocity)**.** 1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod{p}$.

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

3. For $p \neq q$ primes ≥ 3,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. 1. Trivial.

2. Consider $1, 2, \ldots, \frac{p-1}{2}$. Since $i \equiv p - i = 2 \cdot \frac{p-i}{2} \pmod{p}$ for i odd. We have
$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= (-1)(-1)\cdot 2(-1)^2 \cdot (-3)(-1)^3 \cdots \left(\pm\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}} \\ &= 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!(-1)^{\sum_{i=1}^{\frac{p-1}{2}} k}.\end{aligned}$$
Hence
$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{\left(1+\frac{p-1}{2}\right)\frac{p-1}{2}}{2}} = (-1)^{\frac{p^2-1}{8}}.$$

3. Consider the map
$$\begin{aligned}\phi : (\mathbb{Z}/pq\mathbb{Z})^\times &\to (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \\ a &\mapsto (a \mod p, a \mod q).\end{aligned}$$
By CRT, ϕ is an isomorphism. Further, consider
$$\begin{aligned}S_1 &= \left\{1, \ldots, \frac{p-1}{2}\right\} \times \{1, \ldots, q-1\} \\ S_2 &= \{1, \ldots, p-1\} \times \left\{1, \ldots, \frac{q-1}{2}\right\} \\ S_3 &= \left\{1, \ldots, \frac{pq-1}{2}\right\} \setminus \{k \mid q \mid k \text{ or } p \mid k\}.\end{aligned}$$
Since S_1, S_2 contains exactly half of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$, S_3 half of $(\mathbb{Z}/pq\mathbb{Z})^\times$, we have
$$\prod_{x \in S_1} \phi(x) \overset{\text{up to sign}}{=} \prod_{x \in S_3} x.$$

Consider $\phi^{-1}\left(\prod_{x\in S_3} x\right)$. Since

$$\begin{aligned} S_3 = \{&1, 2, \ldots, p-1 \\ &1+p, 2+p, \ldots, p-1+p \\ &\vdots \\ &1+\left(\frac{q-1}{2}-1\right)p, \ldots, (p-1)+\left(\frac{q-1}{2}-1\right)p \\ &1+\frac{q-1}{2}p, \ldots, \frac{p-1}{2}+\frac{q-1}{2}p\Big\} \setminus \{q, 2q, \ldots, \frac{p-1}{2}q\} \end{aligned}$$

So

$$\prod_{x\in S_3} = ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \Big/ q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = (p-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p.$$

Note that

$$S_1 = \left(\left(\frac{p-1}{2}\right)!\right)^{q-1} = S_3\left(\frac{q}{p}\right) \pmod p,$$

and similarly $S_2 = S_3\left(\frac{p}{q}\right)$. We only need to find out the relation between S_1 and S_2. But observe

$$\begin{aligned} S_1 &= \left(\left(\frac{p-1}{2}\right)!\right)^{q-1} \\ S_2 &= ((p-1)!)^{\frac{q-1}{2}}, \end{aligned}$$

so $S_1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} S_2$. And we are done. □

Definition 3.1. The *Jacobi symbol* is defined for $m = \prod_{i=1}^{l} p_i$, where p_i could be equal to p_j, let

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_l}\right).$$

Proposition 3.8. For n, m both odd, we have

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

where $\gcd(m, n) = 1$.

Proof. Suppose $m = \prod_{i=1}^{l} p_i, n = \prod_{j=1}^{s} q_j$, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)\prod_{i,j}\left(\frac{q_j}{p_i}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

WTS,

$$\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2} = \frac{m-1}{2}\frac{n-1}{2} \pmod 2.$$

This is easy since we have $\frac{rs-1}{2} \equiv \frac{r-1}{2}\frac{s-1}{2} \pmod 2$ for odd r, s. □

Proposition 3.9. Reproof of

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

Proof.

$$\begin{aligned}\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{p-2}\right)(-1)^{\frac{p-1}{2}\frac{p-3}{2}} \\ = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{p-3}{2}}\left(\frac{2}{p-2}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{2}{p-2}\right) = (-1)^{\frac{p-1}{2}+\frac{p-3}{2}}\left(\frac{2}{p-4}\right) = \cdots \\ = (-1)^{\sum_{k=2}^{\frac{p-1}{2}} k}\left(\frac{2}{p-3}\right) = (-1)^{\frac{p^2-1}{8}}.\end{aligned}$$

□

Remark. In the previous proof, we ommitted the proof of

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

which is easy.

3.2 Quadratic Gauss sum

Let $\zeta := e^{\frac{2\pi i}{p}}$.

Lemma 3.10. For $a \in \{0, \ldots, p-1\}$, let

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} 0, & \text{if } a \neq 0 \\ p, & \text{if } a = 0. \end{cases}$$

Proof. If $a = 0$, $\zeta^{at} = 1$. We are done.

If $a \neq 0$,

$$\left(\sum_{t=0}^{p-1} \zeta^{at}\right)\zeta^a = \sum_{t=0}^{p-1} \zeta^{at} \quad \Longrightarrow \quad \sum_{t=0}^{p-1} \zeta^{at}(\zeta^a - 1) = 0.$$

Since $\zeta^{at} \neq 0$, we are done. □

Lemma 3.11.

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0.$$

Proof. There are exactly $\frac{p-1}{2}$ $a \in \{1, \ldots, p-1\}$ satisfying $x^2 \equiv a \pmod{p}$. □

Definition 3.2. Let

$$g_a := \sum_{t=0}^{p-1} \zeta^{at}\left(\frac{t}{p}\right)$$

be the *quadratic Gauss sum*.

Proposition 3.12. $g_a = \left(\frac{a}{p}\right) g_1$, for $\gcd(a,p) = 1$.

Proof.

$$g_a = \sum_{t=0}^{p-1} \zeta^{at} \left(\frac{at}{p}\right)\left(\frac{a}{p}\right) = g_1 \left(\frac{a}{p}\right). \qquad \square$$

Proposition 3.13.

$$g_1^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. Consider $\sum_{a=0}^{p-1} g_a g_{-a}$,

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1}\sum_{x=0}^{p-1} \zeta^{ax}\left(\frac{x}{p}\right)\sum_{y=0}^{p-1}\zeta^{-ay}\left(\frac{y}{p}\right) = \sum_{x,y}\left(\frac{xy}{p}\right)\sum_{a=0}^{p-1}\zeta^{a(x-y)} = \sum_{x=0}^{p-1}\left(\frac{x^2}{p}\right)p = p(p-1)$$

With $g_0 = 0$,

$$p(p-1) = \sum_{a=1}^{g_a g_{-a}} = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g_1^2 = (p-1)\left(\frac{-1}{p}\right) g_1^2. \qquad \square$$

Proposition 3.14. Reproof of quadratic reciprocity law.

Proof. Consider g_1^{q-1}. Let $g_1^2 = p(-1)^{\frac{p-1}{2}} := p^*$. So

$$g_1^{q-1} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

On the other hand,

$$g_1^q = \left(\sum_{t=0}^{p-1} \zeta^t \left(\frac{t}{p}\right)\right)^q \in g_q + q\mathbb{Z}[\zeta] = \left(\frac{q}{p}\right) g_1 + q\mathbb{Z}[\zeta].$$

Cancal out one g_1 on both sides,

$$\left(\frac{p^*}{q}\right) = g_1^{q-1} = \left(\frac{q}{p}\right) + \frac{q}{g_1} A, \quad A \in \mathbb{Z}[\zeta].$$

So

$$\left(\frac{p^*}{q}\right) - \left(\frac{q}{p}\right) \in q\mathbb{Z}\left[\zeta, \frac{1}{p}\right] \cap \mathbb{Z} = q\mathbb{Z} \quad \Longrightarrow \quad \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Therefore,

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

Chapter 4

2025/10/9

Recall $g_1 = (-1)^{\frac{p-1}{2}} p$, so

$$g_1 = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \pmod 4 \\ \pm i\sqrt{p}, & p \equiv 3 \pmod 4. \end{cases}$$

Goal. Prove that

$$g_1 = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod 4 \\ i\sqrt{p}, & p \equiv 3 \pmod 4. \end{cases}$$

Consider

$$\begin{aligned} \prod_{i=1}^{\frac{p-1}{2}} \left(\zeta^{2i-1} - \zeta^{-(2i-1)}\right)^2 &= \prod_{i=1}^{\frac{p-1}{2}} \left(\zeta^{2i-1} - \zeta^{-(2i-1)}\right) (-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} \left(\zeta^{-(2i-1)} - \zeta^{2i-1}\right) \\ &= \prod_{i=1}^{\frac{p-1}{2}} \left(1 - \zeta^{-2(2i-1)}\right) \prod_{i=1}^{\frac{p-1}{2}} \left(1 - \zeta^{2(2i-1)}\right) (-1)^{\frac{p-1}{2}}. \end{aligned}$$

Let $S = \left\{2i-1 \mid i = 1, \ldots, \frac{p-1}{2}\right\} \cup \left\{-(2i-1) \mid i = 1, \ldots, \frac{p-1}{2}\right\} = \{p-2, \ldots, 1, -1, \ldots, -p+2\}$, which is a complete set modulo p, and so is $2S$. Hence the original expression is equal to

$$\prod_{i=1}^{p-1} \left(1 - \zeta^i\right) (-1)^{\frac{p-1}{2}} = p(-1)^{\frac{p-1}{2}} = g_1^2.$$

where the last equation is because of the following lemma.

Lemma 4.1.

$$\frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}.$$

Next we prove

$$\prod_{j=1}^{\frac{p-1}{2}} \left(\zeta^{2j-1} - \zeta^{-2j+1}\right) = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod 4 \\ i\sqrt{p}, & p \equiv 3 \pmod 4. \end{cases}$$

This is because

$$LHS = \prod_{j=1}^{\frac{p-1}{2}} 2i \sin \frac{2\pi(2j-1)}{p}.$$

Since the absolute value has been determined already, we only need to consider the signature. We have $0 < \frac{2\pi(2j-1)}{p} < 2\pi$, where $0 < \frac{2\pi(2j-1)}{p} < \pi$ iff $j < \frac{p+2}{4}$. If $p \equiv 1 \pmod 4$, then $\frac{p-1}{2}$ is even, the signature is $i^{\frac{p-1}{2}}(-1)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{2}} = 1$. If $p \equiv 3 \pmod 4$, then the signature is $i^{\frac{p-1}{2}}(-1)^{\frac{p-3}{2}} = i(-1)^{\frac{p-3}{2}} = i$.

Then it is time to prove

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\zeta^{2i-1} - \zeta^{-(2i-1)}\right) = g_1.$$

Take $\epsilon_p \in \{\pm 1\}$ s.t.

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\zeta^{2i-1} - \zeta^{-(2i-1)}\right) - \epsilon_p g_1 = 0.$$

Let $f(x) := \prod_{i=1}^{\frac{p-1}{2}} \left(x^{2i-1} - x^{p-(2i-1)}\right) - \epsilon_p \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) x^i$ is a polynomial. $f(\zeta) = 0$. Study the minimal irreducible polynomial of ζ over $\mathbb{Z}$. $\zeta^p = 1$ and $1 + \zeta + \cdots + \zeta^{p-1} = \frac{\zeta^p - 1}{\zeta - 1} = 0$.

Lemma 4.2.

$$F(x) := 1 + x + \cdots + x^{p-1}$$

is irreducible over $\mathbb{Q}$.

Proof.

$$F(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} x^{i-1}.$$

The coefficients of $F(x+1)$ form an Eisenstein series, so $F(x+1)$ is irreducible and so is $F(x)$. □

We have $(1 + \cdots + x^{p-1}) \mid f(x)$. On the other hand, $f(1) = 0$. Hence $(1 - x^p) = (x-1)(1 + \cdots + x^{p-1}) \mid f(x)$ and we can write

$$f(x) = (1 - x^p)g(x), \tag{4.1}$$

where $g(x) \in \mathbb{Q}[x]$.

Take $x = e^z$. Compare $z^{\frac{p-1}{2}}$ of the Taylor expansions of two functions in (4.1).

$$e^{z(2i-1)} - e^{z(-2i+1)} = z(2i-1) - z(-2i+1) + \mathcal{O}(z^2) = z(4i-2) + \mathcal{O}(z^2).$$

Hence the coefficient of $z^{\frac{p-1}{2}}$ on the left hand side is

$$\prod_{i=1}^{\frac{p-1}{2}} (4i-2) - \epsilon_p \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) i^{\frac{p-1}{2}} \frac{1}{(\frac{p-1}{2})!}.$$

While on the right hand side,

$$(1 - e^{zp})g(e^z) \equiv 0 \pmod p.$$

This gives the congruence

$$\left(\frac{p-1}{2}\right)! \prod_{i=1}^{\frac{p-1}{2}} (4i-2) \equiv \epsilon_p \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) i^{\frac{p-1}{2}} \equiv \epsilon_p (p-1) \equiv -\epsilon_p \pmod p,$$

while

$$\Big(\frac{p-1}{2}\Big)!\prod_{i=1}^{\frac{p-1}{2}}(4i-2)=2\times\cdots\times(p-1)\times 1\times\cdots\times(p-2)=(p-1)!\equiv -1 \pmod p.$$

Together we obtain $\epsilon_p = 1$. Goal achieved.

4.1 Gauss and Jacobi sum

Fact. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a finite field. Call $\chi : (\mathbb{F}_p^\times, \times) \to \mathbb{C}^\times$ a multiplicative character if it is a group homomorphism. Call $\chi : (\mathbb{F}_p, +) \to \mathbb{C}^\times$ a additive character if it is a group homomorphism.

Hence, $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a multliplicative character. $a \mapsto \zeta^a$ is a additive character. So we can see the Gauss sum

$$g_a = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^{ai}$$

as the sum of a mult-character multiplying an add-character.

For a general multiplicative character χ of $\mathbb{F}_p$, we put

$$g_a(\chi) := \sum_{i=0}^{p-1}\chi(i)\zeta^{ai}.$$

where

$$\chi(0) = \begin{cases} 0, & \chi \neq \epsilon \\ 1, & \chi = \epsilon, \end{cases}$$

where $\epsilon(a) \equiv 1$ is the trivial character.

Proposition 4.3. 1.

$$g_a(\chi) = g_1(\chi)\overline{\chi(a)},$$

if $\chi \neq \epsilon$.

2. $g_a(\epsilon) = 0$, for $a \neq 0$.
3. $a = 0, \chi \neq \epsilon$, then $g_0(\chi) = 0$.
4. $a = 0, \chi = \epsilon$, then $g_0(\epsilon) = p$.

Proof. 1.

$$g_a(\chi) = \sum_{i=0}^{p-1}\chi(i)\zeta^{ai} = \overline{\chi(a)}\sum_{i=1}^{p-1}\chi(ia)\zeta^{ai} = \overline{\chi(a)}g_1(\chi).$$

2.

$$g_0(\epsilon) = \sum_{i=0}^{p-1}\zeta^{ai} = \frac{1-\zeta^{ap}}{1-\zeta^p} = 0.$$

3. Since χ non-trivial, there exists $b \in \mathbb{F}_p^\times$ s.t. $\xi(b) \neq 1$.

$$g_0(\chi) = \sum_{i=0}^{p-1}\chi(i) = \sum_{i=0}^{p-1}\chi(ib) = 0.$$

4. Trivial. □

Proposition 4.4.

$$|g_a(\chi)| = \sqrt{p}, \quad \xi \neq \epsilon.$$

Proof. Consider

$$\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)} = \sum_{a=0}^{p-1}\sum_{x=1}^{p-1}\chi(x)\zeta^{ax}\sum_{y=1}^{p-1}\overline{\chi(y)}\zeta^{-ay} = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\chi\left(\frac{x}{y}\right)\sum_{a=0}^{p-1}\zeta^{a(x-y)} = \sum_{x=1}^{p-1} p = (p-1)p.$$

Suppose $\chi \neq \epsilon$,

$$\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)} = g_1(\chi)\overline{g_1(\chi)}\sum_{a=1}^{p-1}\overline{\chi(a)}\chi(a) = (p-1)|g_1(\chi)|^2.$$

Hence $|g_a(\chi)| = |g_1(\chi)| = \sqrt{p}$. □

Another Proof.

$$g_1(\chi)\overline{g_1(\chi)} = \sum_{x=1}^{p-1}\chi(x)\zeta^x\sum_{y=1}^{p-1}\overline{\chi(y)}\zeta^{-y} = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\chi\left(\frac{x}{y}\right)\zeta^{x-y} = \sum_{k=0}^{p-1}\zeta^k\sum_{y=1}^{p-1}\chi\left(\frac{y+k}{y}\right).$$

For $k \neq 0$, $\eta_k : \mathbb{F}_p^\times \to \mathbb{F}_p, y \mapsto \frac{y+k}{y}$ is injective, and $\mathrm{Im}(\eta_k) = \mathbb{F}_p \setminus \{1\}$. So the original expression is equal to

$$\sum_{k=1}^{p-1}\zeta^k(-1) + \zeta^0(p-1) = 1 + p - 1 = p.$$ □

For two multilicative character χ and λ of $\mathbb{F}_p$, we define

$$J(\chi,\lambda) := \sum_{a+b=1}\chi(a)\lambda(b),$$

called the *Jacobi sum*.

Goal. Compute the number of solutions of $x^n + y^n = 1$ in $\mathbb{F}_p$, denoted by $N(x^n + y^n = 1)$.

Proposition 4.5. For $\chi, \lambda \neq \epsilon$, and $\chi\lambda \neq \epsilon$,

1. $J(\epsilon,\epsilon) = p$.
2. $J(\epsilon,\chi) = J(\chi,\epsilon) = 0$.
3. $J(\chi,\chi^{-1}) = -\chi(-1)$.
4. $J(\chi,\lambda) = \frac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}$.

Proof. The first two is trivial.

$$J(\chi,\chi^{-1}) = \sum_{a\neq 0}\chi\left(\frac{1-a}{a}\right) = \sum_{i=0}^{p-1}\chi(i) - \chi(-1) = \chi(-1).$$

$$J(\chi,\lambda)g_1(\chi\lambda) = \sum_{a+b=1}\chi(a)\lambda(b)\sum_{c=0}^{p-1}\chi\lambda(c)\zeta^c = \sum_{a+b=1}\sum_{c=0}^{p-1}\chi(ac)\lambda(bc)\zeta^{ac+bc}.$$

Take $d = ac, f = bc$, then the original expression becomes

$$\sum_{d,f} \chi(d)\zeta^d \lambda(f)\zeta^f = g_1(\chi)g_1(\lambda). \qquad \square$$

Recall that

$$N(x^n = a) = \begin{cases} 1, & a = 0 \\ d, & a^{\frac{p-1}{d}} \equiv 1 \pmod{p} \\ 0, & \text{otherwise,} \end{cases}$$

where $d = \gcd(n, p-1)$. Hence

$$N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)N(x^n = b).$$

Definition 4.1. For a character χ, we call d its *order* if $\chi^d(a) = 1$ for all $a \in \mathbb{F}_p^\times$ and any $d' \mid d, d' \neq d$, there exists $a \in \mathbb{F}_p^\times$, $\chi^d(a) \neq 1$.

Proposition 4.6. Let χ be any character of order $d = \gcd(n, p-1)$, then

$$N(x^n = a) = \sum_{i=0}^{d-1} \chi^i(a).$$

Proof. $a = 0$. Trivial.

$a \neq 0$ and $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, take g a primitive root modulo p, $a = g^{ds}$. Hence

$$\sum_{i=0}^{d-1} \chi^i(a) = \sum_{i=0}^{d-1} (\chi(g))^{dsi} = d.$$

$a \neq 0$ and $a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$, take g a p.r. and $a = g^{d_1 s}$, where $\gcd\left(s, \frac{d}{d_1}\right) = 1$. There exists u, v s.t. $us + \frac{d}{d_1}v = 1$. So $\chi(g^{d_1 s}) \neq 1$, because otherwise we have $\chi(g^{d_1 us}) = \chi(g^{d_1 us + dv}) = \chi(g^{d_1}) = 1$, which is impossible. It follows that the original expression is equal to

$$\sum_{i=0}^{d-1} \chi^i(g^{d_1 s}) = \sum_{i=0}^{d-1} \chi(g^{si})^{d_1} = 0. \qquad \square$$

We now have

$$\begin{aligned} N(x^n + y^n = 1) &= \sum_{a+b=1} N(x^n = a)N(x^n = b) = \sum_{a+b=1} \sum_{i=0}^{d-1} \chi^i(a) \sum_{j=0}^{d-1} \chi^j(b) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} J(\chi^i, \chi^j) \\ &= J(\epsilon, \epsilon) + \sum_{i=0}^{d-1} J(\epsilon, \chi^i) + \sum_{i=1}^{d-1} J(\chi^i, \epsilon) + \sum_{i=1}^{d-1} J(\chi^i, \chi^{-i}) + \sum_{i,j \neq 0, i+j \neq 0} J(\chi^i, \chi^j) \\ &= p + (-\chi(-1))(p-1) + \sum_{i,j \neq 0, i+j \neq 0} \frac{g_1(\chi^i)g_1(\chi^j)}{g_1(\chi^{i+j})}. \end{aligned}$$

As a result,

$$|N(x^n + y^n = 1) - p + \chi(-1)(p-1)| \leq (d^2 - 3d + 2)\sqrt{p}.$$

Applications. When $n = 2$, take $\chi = \left(\frac{\cdot}{p}\right)$. Then

$$N(x^2 + y^2 = 1) = p - (-1)^{\frac{p-1}{2}}.$$

When $n = 3$, take χ that has order 3. Then

$$N(x^3 + y^3 = 1) = p - 2\chi(-1) + J(\chi, \chi) + \overline{J(\chi, \chi)}$$

Because $\chi^3(-1) = \chi^2(-1) = 1$,

$$|N(x^n + y^n = 1) - p + 2| \leq 2\sqrt{p}.$$

Proposition 4.7. If $p \equiv 1 \pmod 4$, then there exists a unique integer A and B s.t. $A^2 + B^2 = p$, up to sign.

Proof. Existence. Since $p \equiv 1 \pmod 4$, we can construct a character χ of order 4 by assigning the value of a primitive root g to i, $\chi(g) = i$.

Consider $J(\chi, \chi) = \sum_{a+b=1} \chi(a)\chi(b) \in \mathbb{Z}[i]$, we have

$$|J(\chi, \chi)| = \frac{\sqrt{p}\sqrt{p}}{\sqrt{p}} = \sqrt{p}.$$

Let $J(\chi, \chi) = A + Bi$, then $A^2 + B^2 = p$.

Uniqueness. Suppose that $A^2 + B^2 = C^2 + D^2 = p$. We know $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ and $\mathbb{Z}[i]$ is a Euclidean domain and thus a UFD. It suffices to prove that $A + Bi$ is irreducible. Suppose that $A + Bi = (a + bi)(c + di)$ and $a + bi, c + di \notin \mathbb{Z}[i]$. But $p = A^2 + B^2 = (a^2 + b^2)(c^2 + d^2)$. A contradiction. □

Proposition 4.8. If $p \equiv 1 \pmod 3$, then there are integers A and B s.t. $p = A^2 - AB + B^2$.

Proof. Take $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times, g \mapsto \omega$. Similarly, $|J(\chi, \chi)| = \sqrt{p}$. Let $J(\chi, \chi) = a + b\omega$ and we have $a^2 - ab + b^2 = p$. □

Chapter 5

2025/10/16

Proposition 5.1. Suppose $p \equiv 1 \pmod 3$. There exists a unique A, B (up to sign) s.t. $A^2 + 27B^2 = 4p$.

Recall that we have proven there exists a, b s.t. $a^2 - ab + b^2 = p$, so it suffices to prove that $4a^2 - 4ab + 4b^2$ can be written as the desired form. Notice that $4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$, but b might not be divisible by 3.

Lemma 5.2. For $a^2 - ab + b^2 = p$, $p \equiv 1 \pmod 3$, one of a, b and $a - b$ is divisible by 3.

Proof. If $a \not\equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$, then $a^2 \equiv b^2 \equiv 1 \pmod 3$, so

$$a^2 - ab + b^2 \equiv 2 - ab \equiv p \equiv 1 \pmod 3 \implies ab \equiv \pmod 3 \implies a \equiv b \pmod 3. \ \square$$

Proof of Proposistion 5.1. Since $a^2 - ab + b^2 = (a - b)^2 - (a - b)(-b) + (-b)^2$, we can conlude that there exists a, b s.t. $3 \mid a$ and $a^2 - ab + b^2 = p$. This completes the proof of existence of $A^2 + 27B^2 = p$.

Now for uniqueness. Consider

$$\frac{A^2 + 27B^2}{4} = \frac{A + 3\sqrt{3}iB}{2} \frac{A - 3\sqrt{3}iB}{2},$$

where each component on the right hand side lies in $\mathbb{Q}[\omega]$, with norm equal to p. Given that $A \equiv B \pmod 2$, we have

$$\frac{A + 3\sqrt{3}iB}{2} = \frac{A + 3B}{2} + 3\omega B \in \mathbb{Z}[\omega].$$

Since $\mathbb{Z}[\omega]$ is a Euclidean domain, $\frac{A+3\sqrt{3}iB}{2}$ is irreducible. Suppose $A_1^2 + 27B_1^2 = A_2^2 + 27B_2^2 = p$. Then WLOG,

$$\frac{A_1 + 3\sqrt{3}iB_1}{2} \mid \frac{A_2 + 2\sqrt{3}iB_2}{2},$$

or

$$\frac{A_1 + 3\sqrt{3}iB_1}{2} u = \frac{A_2 + 2\sqrt{3}iB_2}{2},$$

where u is a unit. However, we know $U(\mathbb{Z}[\omega])$ contains elements whose norms are equal to 1, so $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm(1 + \omega)\}$.

If $u = \omega$, we could obtain $A_1 = 3B_2$, and $3 \mid A_1$, so $3 \mid p$, a contradiction. Similarly, we can tell that $-\omega, \pm(1 + \omega)$ is also not possible.

Hence $u = \pm 1$, giving the uniqueness. $\square$

Proposition 5.3. If χ is a character of order 3, and $J(\chi,\chi) = a + b\omega$, then $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$.

Proof. Since $\chi \neq \overline{\chi}$,

$$J(\chi,\chi) = \frac{g_1(\chi)g_1(\chi)}{g_1(\chi^2)}.$$

Calculate

$$\overline{g_1(\chi^2)} = \overline{\sum_{x=0}^{p-1} \chi^2(x)\zeta_p^x} = \sum_{x=0}^{p_{01}} \chi(x)\zeta_p^{-x} = \chi(-1)g_1(\chi) = g_1(\chi),$$

where the last equation is given by the fact that χ has order 3.

Recall $|g_1(\chi)| = \sqrt{p}$, so

$$g_1^3(\chi) = J(\chi,\chi)|g_1(\chi)|^2 = J(\chi,\chi)p \equiv J(\chi,\chi) \pmod 3.$$

On the other hand,

$$g_1^3(\chi) = \left(\sum_{i=0}^{p-1} \chi(i)\zeta_p^i\right)^3 \equiv \sum_{i=0}^{p-1} (\chi(i))^3 \left(\zeta_p^i\right)^3 = \sum_{i=1}^{p-1} \zeta_p^{3i} = -1 \mod 3\mathbb{Z}[\zeta_p,\omega].$$

So

$$\mathbb{Z}[\omega] \ni J(\chi,\chi) \equiv -1 \mod 3\mathbb{Z}[\zeta_p,\omega],$$

and since $\mathbb{Z}[\omega] \cap_3 \mathbb{Z}[\omega,\zeta_p] = 3\mathbb{Z}[\omega]$, we have $J(\chi,\chi) \equiv -1 \mod 3\mathbb{Z}[\omega]$. It follows that

$$a + b\omega \equiv -1 \mod 3\mathbb{Z}[\omega] \quad \Longrightarrow \quad a \equiv -1 \pmod 3 \quad b \equiv 0 \pmod 3. \qquad \square$$

Corollary 5.4. $N(x^2 + y^2 = 1) = p - 2 + A$, where A is the unique positive solution of $A^2 + 27B^2 = 4p$.

Proof. Calculate

$$\begin{aligned} N(x^2+y^2=1) &= \sum_{i=0}^{2}\sum_{j=0}^{2} J(\chi^i,\chi^j) \\ &= J(\epsilon,\epsilon) + 2J(\chi,\epsilon) + 2J(\chi^2,\epsilon) + 2J(\chi,\chi^2) + J(\chi,\chi) + J(\chi^2,\chi^2) \\ &= p - 2 + J(\chi,\chi) + J(\chi^2,\chi^2) = p - 2 + 2\,\mathrm{Re}(J(\chi,\chi)) \\ &= p - 2 + (2a - b). \end{aligned}$$

Since $|2J(\chi,\chi)|^2 = 4p^2 = (2a-b)^2 + 3b^2 = (2a-b)^2 + 27b'^2$, where the last equation is because $b \equiv 0 \pmod 3$, from the uniqueness of $A^2 + 27B^2 = 4p$, $2a - b = A$ up to sign. $\square$

5.1 Finite Fields

Known. For prime p, $\mathbb{F}_p^\times$ is cyclic. We claim that any finite field is of the form $\mathbb{F}_{p^r}$, which is a field extension of $\mathbb{F}_p$ for some p, especially of order p^r.

Theorem 5.5. $\mathbb{F}_q^\times$ is cyclic.

Proof. For $\alpha \in \mathbb{F}_q^\times$, let d be the smallest positive integer s.t. $\alpha^d = 1$, and call d the order of α. $\alpha^{p-1} = 1$. Let $\psi(d) := \#\{\alpha \in \mathbb{F}_q \mid \alpha \text{ has order } d\}$. Then $p^r - 1 = \sum_{d|p^r-1} \psi(d)$ and

$$\sum_{d'|d} \psi(d') = \#\{\alpha \mid \alpha^d - 1 = 0\} = 0.$$

By Möbius inversion,

$$\psi(d) = \sum_{d'|d} d' \mu\left(\frac{d}{d'}\right) = \phi(d).$$

Hence $\psi(p^r - 1) = 0$, there exists a primitive root of $\mathbb{F}_q^\times$, and it is cyclic. □

We are interested in considering the finite extensions of $\mathbb{F}_p$, or $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. To prove that each finite field is isomorphic to some $\mathbb{F}_{p^r}$, and we are going to achieve this goal by the following three steps.

1. $\mathbb{F}_{p^r} = \{x \in \overline{\mathbb{F}}_p \mid x^{p^r} - x = 0\}$ is a field.
2. Any finite field F, there exists p s.t. $pF = 0$.
3. F is some algebraic extension of $\mathbb{F}_p$, i.e. $F = \mathbb{F}_p[\alpha_1, \ldots, \alpha_i]$, so we can embed F into $\overline{\mathbb{F}}_p$ with map $\phi : F \hookrightarrow \overline{\mathbb{F}}_p$. As $\phi(F) \subseteq \mathbb{F}_{p^r}$ and they have the same size as sets, $\phi(F) = \mathbb{F}_{p^r}$. Hence $|F| = p^r$ and all such F is isomorphic.

Proposition 5.6. General finite field F contains $\mathbb{F}_p$ for some p.

Proof. $1 \in F$. Take m be the minimal positive integer s.t. $m \cdot 1 = 0$. Prove $m = p$ for some p. Suppose otherwise, $m = m_1 m_2$. This leads to $m_1 \cdot 1 = 0$ or $m_2 \cdot 1 = 0$, contradictory to the minimality of m. Hence we have $\mathbb{F}_p = \{0, 1, \ldots, p-1\} \subseteq F$. □

Remark. p in the previous proof is called the *character* of $\mathbb{F}$.

Proposition 5.7. The previously defined $\mathbb{F}_{p^r}$ is a field.

Proof. For $\alpha, \beta \in \mathbb{F}_{p^r}$,

$$\begin{aligned}(\alpha+\beta)^{p^r} - (\alpha+\beta) = \alpha^{p^r} + \beta^{p^r} - \alpha - \beta = 0\\ (\alpha\beta)^{p^r} - \alpha\beta = \alpha\beta - \alpha\beta = 0\\ \left(\frac{1}{\alpha}\right)^{p^r} - \frac{1}{\alpha} = \frac{1}{\alpha} - \frac{1}{\alpha} = 0.\end{aligned}$$

□

Proposition 5.8. Any $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$ iff $r \mid s$.

Proof. " $\Longleftarrow$ ".

$$\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s} \iff (\forall \alpha \in \overline{\mathbb{F}}_p \text{ s.t. } \alpha^{p^r} - \alpha = 0 \implies \alpha^{p^s} - \alpha = 0)$$

" $\Longrightarrow$ ". $x^{p^r} - x \mid x^{p^s} - x \iff x^{p^r-1} - 1 \mid x^{p^s-1} - 1 \iff p^r - 1 \mid p^s - 1 \iff r \mid s$. □

Corollary 5.9. For any p^r, there exists a finite field F s.t. $|F| = p^r$.

Proof. Take $F = \left\{x \in \overline{\mathbb{F}}_p \mid x^{p^r} - x = 0\right\}$. Since $(x^{p^r} - x)' = -1 \neq 0$, the polynomal has no multiple roots and hence $|F| = p^r$. □

Proposition 5.10. Any irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree d divides $x^{p^d} - x$.

Proof. Take α be a root of f in $\overline{\mathbb{F}}_p$. We know $\mathbb{F}_p[\alpha]| = p^d$, so $\mathbb{F}_p \cong \mathbb{F}_{p^d}$, and $\alpha^{p^d} - \alpha = 0$. On the other hand, f is irreducible, so it is the minimal polynomial of α. $f \mid x^{p^d} - x$. □

Corollary 5.11. Any irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree d divides $x^{p^n} - x$ iff $d \mid n$.

Proof. We first prove a lemma.

Lemma 5.12. Any irreducible f of order $d' > d$, $f \nmid x^{p^d} - x = 0$

Proof. Suppose $f \mid x^{p^d} - x$. Take α a root of f. Then $\alpha^{p^d} - \alpha = 0$, so $\alpha \in \mathbb{F}_{p^d}$. But $|\mathbb{F}_{p^d}| = p^{d'} > p^d = |\mathbb{F}_{p^d}|$, a contradicition to $\alpha \in \mathbb{F}_{p^d}$. □

By virtue of the lemma, we are able to prove that any irreducible f of order d', $f \mid x^{p^d} - x$ iff $d' \mid d$. □

Theorem 5.13. Let $F_d(x)$ be the product of all distinct irreducible polynomials of degree d in $\mathbb{F}_p[x]$. Then $\forall n \geq 1$ we have

$$\prod_{d|n} F_d(x) = x^{p^n} - x.$$

Proof. Since $\mathbb{F}_p[x]$ is a Euclidean domain, we can write

$$x^{p^n} - x = \prod_{f \text{ irreducible}} f^{e_f} = \prod_{f \text{ irreducible}, \deg f | n} f.$$

So $f \mid F_d(x)$ for some d and it suffices to prove that $e_f = 1$. Suppose not. Let f_0 be one of f s.t. $e_{f_0} \geq 2$.

$$-1 = \left(x^{p^n} - x\right)' = \left(\prod_f f^{e_f}\right)' = \left(e_{f_0} f_0^{e_f - 1}\right)\left(\prod_{f \neq f_0} f^{e_f}\right) + \left(\prod_{f \neq f_0} f^{e_f}\right)'.$$

Plugging in α a root of f_0 provides a contradiction. □

Let T_d be the number of irreducible polynomial of degree d in $\mathbb{F}$. From $\deg(F_d) = T_d d$, we have $\sum_{d|n} T_d d = p^n$. By Möbius inversion,

$$T_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

We turn to examine the equations in finite fields.

Theorem 5.14 (Chevally's theorem)**.** If $F = \mathbb{F}_q$, $q = p^r$, let $f(x) \in \mathbb{F}[x] := F[x_1, \ldots, x_n]$. Suppose

1. $F(0) = 0$.
2. $n > \deg f := \max_{i \in I}\{i_1 + \cdots + i_n\} = d$, where $f = \sum_{\underline{i} \in I} c_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n}$

Then f has at least q roots in $\mathbb{A}^n(F) = \{(x_1, \ldots, x_n) \in F^n\}$.

Proof. Take $N_f := \sum_{\underline{a}\in\mathbb{A}^n(F)}(1-f(\underline{a})^{q-1})$ is the number of roots of f. Then it is enough to show $q \mid N_f$.

$\deg f = d$, $\deg f^{q-1} = d(q-1)$. $f^{q-1} = \sum_{\underline{j}\in I} c_{\underline{j}} x_1^{j_1}\cdots x_n^{j_n}$. For any $\underline{j} \in I$, at least one of $i \in \{1,\dots,n\}$ satisfies $j_i < q-1$. Fix other items and let x_i runs through F.

Lemma 5.15.

$$\sum_{x\in F} x^i = \begin{cases} |F|-1, & q-1 \mid i, i\neq 0, \\ |F|, & i = 0, \\ 0, & q-1 \nmid i. \end{cases}$$

So $q \mid \sum_{\underline{a}\in F^n} c_{\underline{i}} x_1^{j_1}\cdots x_n^{j_n}$ and hence

$$q \mid \sum_{\underline{a}\in F^n} f(\underline{a})^{q-1} \quad\Longrightarrow\quad q \mid N_f \quad\Longrightarrow\quad N_f \geq q. \qquad \square$$

More generally, we have the following theorem.

Theorem 5.16 (Ax, Katz)**.** Let $f_1,\dots,f_r \in F[x_1,\dots,x_n]$ be polynomials of degree $d_i \geq 1$. Suppose $\sum_{i=1}^r d_i < n$, then let $M_f = \left\lceil \frac{n-\sum_{i=1}^r d_i}{\max_{1\leq i\leq r} d_i} \right\rceil$. Then $N_f := \{\underline{x} \in \mathbb{A}_{F^n} \mid f_i(\underline{x}) = 0\}$ satisfies $q^{M_f} \mid N_f$.

5.2 Hasse-Weil Zeta Function

Definition 5.1. Define a *variety* X over $\mathbb{F}_q$ by $X := \left\{(x_1,\dots,x_n) \in \overline{\mathbb{F}}_p \mid f_i(\underline{x}) = 0, 1 \leq i \leq r\right\}$. And $X(\mathbb{F}_{q^m}) := \{(x_1,\dots,x_n) \in \mathbb{F}_{q^m} \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}$

Definition 5.2. If $N_m(X) := \#X(\mathbb{F}_{p^m})$, then the *Hasse-Weil zeta function* is defined to be

$$Z(X,t) := \exp \sum_{m\geq 1} \frac{N_m(X)}{m} t^m \in \mathbb{Q}[[t]].$$

Example. $X = \mathbb{A}^n_{F_p}$, $|X(\mathbb{F}_{p^m})| = |N_m(X)| = p^{mn}$.

$$Z(\mathbb{A}^n_{\mathbb{F}_p}) = \exp\left(\sum_{m\geq 1} \frac{p^{mn}}{m} t^m\right) = e^{-\ln(1-p^n t)} = \frac{1}{1-p^n t}.$$

Definition 5.3. Define $\mathbb{P}^n_{\mathbb{F}_p} := \left(\mathbb{A}^{n+1}_{\mathbb{F}_p} \setminus \{0\}\right) / \sim$, where $\sim$ is defined by

$$(a_1,\dots,a_{n+1}) \sim (b_1,\dots,b_{n+1}) \iff \exists 0 \neq c \in \mathbb{F}_p \text{ s.t. } a_i c = b_i.$$

Example. Calculate

$$N_m(\mathbb{P}^n_{\mathbb{F}_p}) = \frac{p^{(n+1)m}-1}{p^m-1}.$$

And

$$Z(\mathbb{P}^n_{\mathbb{F}_p}) = \exp\left(\sum_{m=1}^{\infty} \frac{p^{(n+1)m}-1}{m(p^m-1)} t^m\right) = \frac{1}{1-t}\cdots\frac{1}{1-p^n t}.$$

L'algèbre n'est qu'une géométrie écrite; la géometrie n'est qu'une algèbre figurée.

Chapter 6

2025/10/23

6.1 Hasse-Weil zeta function

Last time we defined the function locally over $\mathbb{F}_p$, where

$$Z(X,T) := \exp\left(\sum_{m=1}^{\infty} \frac{N_m(x)}{m} T^m\right).$$

Theorem 6.1 (Weil conjecture)**.** Let X be a smooth projective variety over $\mathbb{F}_p$.

1. (*Rationality*). $Z(X,s) = \frac{P(T)}{Q(T)} \in \mathbb{Q}(T)$.
2. (*Functional equation*). $Z\left(X, \frac{1}{p^n T}\right) = \pm p^{\dim XE/2} T^E Z(X,T)$, where E is the Euler characteristic number of X.
3. $Z(X,T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}$, where $P_i \in \mathbb{Z}[T]$. If we write $P_i(T) = \prod_j (1-\alpha_{ij}T)$ with $a_{ij} \in \mathbb{C}$, then $|a_{ij}| = p^{\frac{i}{2}}$.

Remark (Special case). If $f \in \mathbb{F}_p[\underline{x}]$ is a homogenous polynomial of degree d, take the hypersurface defined by f.

$$H_f := \left\{\underline{x} \in \overline{F}_p \mid f(\underline{x}) = 0\right\}.$$

Then $\dim H_f = n-1$, and

$$Z(H_f,T) = \frac{PT^{(-1)^n}}{(1-T)\cdots(1-p^{n-1}T)}.$$

where roots has norm $p^{\frac{n-1}{2}}$ pure of weight $n-1$. $\deg P(T) = d^{-1}((d-1)^{n+1} + (-1)^{n+1}(d-1))$.

Definition 6.1 (Global version)**.** Let K be a number field.

$$Z(V,S) := \prod_{\mathfrak{p} \text{ prime ideal in } O_k} Z(V_{\mathfrak{p}}, |N(\mathfrak{p})|^s),$$

where $N(\mathfrak{p})$ the norm of $\mathfrak{p}$ as prime ideal and

$$V_{\mathfrak{p}} = \left\{\underline{x} \in \overline{\mathbb{F}}_p \mid f_1 \mod p, \ldots, f_m \mod p\right\}^{1}.$$

[1] only when $V_{\mathfrak{p}}$ has good reduction

Example (Riemann zeta function)**.**

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = Z(\mathrm{spec}(\mathbb{Z}), p^{-s}) = \sum_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

In the following we will mostly be concerned with the Riemann zeta function and its generalization, the L function.

Lemma 6.2.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s})^{-1}\right) = \prod_{p} \left(\sum_{k=0}^{\infty} \frac{1}{p^{sk}}\right).$$

Proof. Fix s. For N, consider primes $p < N$.

$$\sum_{n=1}^{N} \frac{1}{n^s} < \prod_{p<N} \left(\sum_{k=0}^{\infty} \frac{1}{p^{ks}}\right) < \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

By squeeze lemma, we complete the proof. □

We denote the Riemann zeta function by

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

and $\left(1 - \frac{1}{p^s}\right)^{-1}$ the Euler factor of $\zeta(s)$.

We would like to find the meromorphic extension of $f(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ to $\mathbb{C}$. Known $f(s)$ is defined for $\mathrm{Re}(s) > 1$, and

$$\left(1 - \frac{2}{2^s}\right) f(s) = \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{1}{n^s}$$

is defined for $\mathrm{Re}(s) > 0$ (Dirichlet criterion). Define

$$f(s) := \frac{\sum \frac{(-1)^n}{n^s}}{1 - \frac{2}{2^s}}.$$

WTS $f(s)$ has a unique pole at $s = 1$, which is simple. Zeros of $1 - \frac{2}{2^s} = 0$ are $s = 1 - \frac{2\pi ni}{2 \ln 2}$, $n \in \mathbb{Z}$. But the nominator may be zero, so we consider another extension. Since if F_1 and F_2 are the meromorphic extension of f over $\mathrm{Re}(s) > 0$, then $F_1 = F_2$, we consider

$$f_2 = \left(1 - \frac{3}{3^s}\right) \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} - \frac{2}{3^s} + \cdots$$

which converges over $\mathrm{Re}(s) > 0$. Define $F_2 = \frac{f_2}{1 - \frac{3}{3^s}}$. The possible pole points $s = 1 - \frac{2\pi ni}{\ln 3}$ for $n \in \mathbb{Z}$. Note

$$\left\{1 - \frac{2\pi ni}{\ln 3} \mid n \in \mathbb{Z}\right\} \cap \left\{1 - \frac{2\pi ni}{\ln 2} \mid n \in \mathbb{Z}\right\} = 1$$

as $\frac{\ln 2}{\ln 3}$ irrational. Hence

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

can be extended to $\mathrm{Re}(s) > 0$. In the strip $0 < \mathrm{Re}(s) < 1$, we have

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s).$$

By means of this functional equation, we can in fact extend $\zeta(s)$ to the whole plane $\mathbb{C}$.

Known $\zeta(s) = \frac{a}{s-1} + \eta(s)$ around $s = 1$, where $\eta(s)$ is analytic. We would like to determine a.

Lemma 6.3.

$$\lim_{\mathbb{R} \ni s \to 1^+} \zeta(s)(s-1) = 1$$

Proof.

$$\frac{1}{n^s} < \int_{n-1}^{n} t^{-s} \mathrm{d}t < \frac{1}{(n-1)^s}.$$

Hence after summation

$$\sum_{n=2}^{\infty} \frac{1}{n^s} < \int_2^{\infty} \frac{1}{t^s} \mathrm{d}t < \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where

$$\int_2^{\infty} \frac{1}{t^s} \mathrm{d}t = -\frac{1}{s-1} \frac{1}{t^{s-1}} \Big|_2^{\infty} = \frac{1}{s-1} \frac{1}{2^{s-1}}.$$

Hence we have $(s-1)\zeta(s) - (s-1) = (s-1)\sum_{n=2}^{\infty} \frac{1}{n^s} < \frac{1}{2^{s-1}}$ and $(s-1)\zeta(s) > \frac{1}{2^{s-1}}$. By squeeze lemma, we have

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1. \qquad \square$$

6.2 Dirichlet density theorem

Definition 6.2. A set of positive prime $\mathcal{P}$ is said to have *Dirichlet density* if

$$d(\mathcal{P}) := \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}{\ln\left(\frac{1}{s-1}\right)}$$

exists.

Proposition 6.4. 1. If $\mathcal{P}$ is finite, then $d(\mathcal{P}) = 0$.

2. If $\mathcal{P} = \{\text{primes}\} \setminus \{\text{finite ptimes}\}$, then $d(\mathcal{P}) = 1$.

Proof. 1. The nominator is finite but the divisor tends to infinity.

2. WLOG, let $\mathcal{P} = \{\text{primes}\}$. By a previous lemma,

$$\lim_{s \to 1^+} \frac{\zeta(s)}{\ln\left(\frac{1}{s-1}\right)} = 1.$$

So we only need to consider

$$\sum_p \frac{1}{p^s} - \ln \zeta(s) = \sum_p \frac{1}{p^s} - \sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} = \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^{ks}}.$$

Moreover

$$\sum_{k=2}^{\infty}\sum_{p}\frac{1}{kp^{ks}} \le \sum_{k=2}^{\infty}\sum_{n=2}^{\infty}\frac{1}{kn^{ks}} \le \sum_{k=2}^{\infty}\frac{1}{k}\left(\frac{2}{2^{ks}}+\frac{4}{4^{ks}}+\cdots\right) = \sum_{k=2}^{\infty}\frac{1}{k}\left(\sum_{l=1}^{\infty}\frac{1}{2^{l(ks-1)}}\right)$$
$$= \sum_{k=2}^{\infty}\frac{1}{k}\frac{1}{2^{ks-1}}$$

is bounded.

Hence $d(\mathcal{P}) = 1$. □

Proposition 6.5. There exists $\mathcal{P}$ s.t. $d(\mathcal{P})$ is not defined.

Proof. We know when $s \to 1^+$,

$$\frac{\sum_p \frac{1}{p^s}}{\ln\left(\frac{1}{s-1}\right)} \to 1.$$

So there exists $s > 1$ s.t.

$$\frac{\sum_p \frac{1}{p^{s_1}}}{\ln\left(\frac{1}{s_1-1}\right)} > \frac{3}{4}.$$

Further there exists $N_1 > 0$ s.t.

$$\frac{\sum_{p<N_1} \frac{1}{p^{s_1}}}{\ln\left(\frac{1}{s_1-1}\right)} > \frac{3}{4}.$$

And for $\epsilon = \frac{1}{8}$, there exists $N_2 > N_1$ s.t.

$$\frac{\sum_{p>N_2} \frac{1}{p^{s_1}}}{\ln\left(\frac{1}{s_1-1}\right)} < \epsilon = \frac{1}{8}$$

We know by the previous proposition,

$$\lim_{s\to 1^+}\frac{\sum_{p<N_1} \frac{1}{p^s}}{\ln\left(\frac{1}{s-1}\right)} = 0.$$

Take $1 < s_2 < s_1$ s.t.

$$\frac{\sum_{p<N_1} \frac{1}{p^{s_2}}}{\ln\left(\frac{1}{s_2-1}\right)} < \frac{1}{8}$$

And $N_3 > N_2$ s.t.

$$\frac{\sum_{N_2\le p\le N_3} \frac{1}{p^{s_2}}}{\ln\left(\frac{1}{s_2-1}\right)} < \frac{1}{4}$$

Continue this process, to get a series of $N_1, N_2, N_3, \ldots$ and $s_1, s_2, s_3, \ldots$ such that when $s = s_k$, the predominant component in the original summation

$$\frac{\sum_p \frac{1}{p^s}}{\ln\left(\frac{1}{s-1}\right)}$$

is those satisfying $p \in [N_{2i-1}, N_{2i}]$. Take $\mathcal{P} = \{p \mid p \in [N_{2k-1}, N_{2k}], k \in \mathbb{Z}$, and then according to the process, the sum will be around $\frac{3}{4}$ when $s = s_{2k-1}$ and around $\frac{1}{4}$ when $s = s_{2k}$. Hence it converges not. □

Definition 6.3. If we have $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$, define the *Dirichlet character*

$$\begin{aligned}\chi : \mathbb{Z} &\to \mathbb{C}^\times \\ n &\mapsto \begin{cases}\chi(\overline{n}), & \gcd(m,n) = 1 \\ 0, & \gcd(m,n) \neq 1.\end{cases}\end{aligned}$$

Proposition 6.6. 1. $\chi(n + mk) = \chi(n)$, $\forall n, k \in \mathbb{Z}$.

2. $\chi(nk) = \chi(n)\chi(k)$.

3. $\chi(n) \neq 0$, $\forall \gcd(n, m) = 1$.

For A an abelian group, let $\widehat{A} := \{\chi : A \to \mathbb{C}^\times \mid \text{group homomorphism}\}$.

Lemma 6.7. $\widehat{A}$ is a group.

Lemma 6.8. Finite abelian group is isomorphic to

$$\bigoplus_{i=1}^{l} (\mathbb{Z}/r_i\mathbb{Z}).$$

In particular, when $r_1 \mid r_2 \mid \cdots \mid r_l$.

Lemma 6.9. $A \cong \widehat{A}$ for finite abelian group.

Proof. Let $A = \left\{g_1^{i_1} \cdots g_n^{i_n} \mid 1 \leq i_j \leq r_j\right\}$, then

$$\widehat{A} = \left\{\chi : g_i \to \zeta_{r_j}^{s_i}\right\} \cong \bigoplus_{i=1}^{l} (\mathbb{Z}/r_i\mathbb{Z}). \qquad \square$$

Lemma 6.10. A a finite abelian group, $\chi, \psi \in \widehat{A}$ and $n = \#A$. Then

1. $\sum_{a \in A} \chi(a)\overline{\psi(b)} = n\delta(\chi, \delta)$.

2. $\sum_{\chi \in \widehat{A}} \chi(a)\overline{\chi(b)} = n\delta(a, b)$.

Corollary 6.11. For χ, ψ Dirichlet characters modulo m, and $a, b \in \mathbb{Z}$,

1. $\sum_{a=0}^{m-1} \chi(a)\overline{\chi(a)} = \phi(m)\delta(\chi, \psi)$.

2. $\sum_{\chi \text{ Dirichlet character}} \chi(a)\overline{\chi(b)} = \delta(a, b)\phi(m)$, where

$$\delta(a, b) = \begin{cases}1, & a \equiv b \pmod{m} \\ 0, & \text{otherwise.}\end{cases}$$

Definition 6.4. For χ a Dirichlet characteristic modulo m, define the *Dirichlet L-function*

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1}.$$

Remark. If χ_0 is trivial characteristic, then

$$\zeta(s) = L(\chi_0, s) \prod_{p|m} \left(1 - \frac{1}{p^s}.\right)^{-1}$$

Corollary 6.12. If $m = 1$, then

$$L(\chi_0, s) = \zeta(s)$$

for $\mathrm{Re}(s) > 1$.

Our goal is the following theorem.

Theorem 6.13 (Dirichlet prime density theorem)**.**

$$d(\mathcal{P}_a) = \frac{1}{\phi(m)},$$

where $\mathcal{P}_a = \{p \equiv a \pmod m \mid p \text{ is a prime}\}$.

Definition 6.5.

$$G(\chi, s) := \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k) p^{-sk}}{k} = \ln(L(\chi, s)).$$

It is defined over $\mathrm{Re}(s) > 1$.

Proposition 6.14.

$$\lim_{s \to 1^+} \frac{G(\chi_0, s)}{\ln\left(\frac{1}{s-1}\right)} = 1,$$

and $G(\chi, s)$ is bounded for $\chi \neq \chi_0$.

This proposition leads to the Dirichlet prime density theorem, as

$$\begin{aligned}\lim_{s \to 1^+} \frac{\sum_\chi \overline{\chi(a)} G(\chi, s)}{\ln\left(\frac{1}{s-1}\right)} &= \lim_{s \to 1^+} \frac{\sum \overline{\chi(a)} \sum_p \sum_{k=1} \frac{\chi(p^k) p^{-sk}}{k}}{\ln\left(\frac{1}{s-1}\right)} = \lim_{s \to 1^+} \frac{\sum \overline{\chi(a)} \sum_p \chi(p) p^{-s}}{\ln\left(\frac{1}{s-1}\right)} \\ &= \lim_{s \to 1^+} \sum_p \sum_\chi \frac{\chi\left(\frac{p}{a}\right) p^{-s}}{\ln\left(\frac{1}{s-1}\right)} = \lim_{s \to 1^+} \sum_{p, p \equiv a \pmod m} \frac{\phi(m) p^{-s}}{\ln\left(\frac{1}{1-s}\right)} = 1.\end{aligned}$$

Proof of Proposition 6.14. Since $L(\chi_0, s) = \zeta(s) / \prod_{p|m} \left(1 - \frac{1}{p^s}\right)^{-1}$, and

$$\lim_{s \to 1^+} \frac{\ln \zeta(s)}{\ln\left(\frac{1}{s-1}\right)} = 1$$

we indeed have

$$\lim_{s \to 1^+} \frac{\ln L(\chi_0, s)}{\ln \frac{1}{s-1}} = 1.$$

Lemma 6.15. For $\chi \neq \chi_0$, $L\chi, s)$ has an extension to an analytic function on $\mathrm{Re}(s) > 0$.

Take $F(s) := \exp\left(\sum_\chi G(\chi, s)\right) = \prod_\chi L(\chi, s)$. Then for real $s > 1$, we have $F(s) \geq 1$. as

$$F(s) = \exp\left(\sum_\chi \sum_{p,k\geq 1} \frac{\chi(p^k)p^{-sk}}{k}\right) = \exp\left(\sum_{p,k,p^k\equiv 1 \pmod m} \frac{\phi(m)p^{-sk}}{k}\right) \geq 1,$$

where the last equality is from

$$\sum_\chi \chi(a) = \begin{cases}\phi(m), & a \equiv 1 \pmod m \\ 0, & a \not\equiv 1 \pmod m.\end{cases}$$ □

Proposition 6.16 (Complex χ)**.** If χ is complex, i.e., $\{\chi(a) \mid a \in \mathbb{Z}\} \not\subseteq \mathbb{R}$ If χ is a complex characterisitc modulo m, then $L(\chi, 1) \neq 0$.