初等数论 Overview

悔教

目录

1 唯一因子分解 **2**
1.1 整除、素数与唯一分解 . . . 2
1.2 最大公因子与 Bezout 等式 . . . 3
1.3 素数分布的初步估计 . . . 3

2 Gauss 整数环与二平方和问题 **4**
2.1 环中单位、不可约元、素元 . . . 4
2.2 有理素数在 $\mathbb{Z}[i]$ 中的分解 . . . 4
2.3 二平方和定理 . . . 4

3 同余理论 **5**
3.1 模 m 同余与剩余类环 . . . 5
3.2 模约化、多项式应用 . . . 5
3.3 一次同余、中国剩余定理、Euler 定理 . . . 6

4 分圆多项式 **6**

5 高次同余方程与原根 **7**
5.1 奇素数幂模数 . . . 7
5.2 2 的幂模数 . . . 8

6 二次互反律：Theorema Aureum **8**
6.1 Legendre 符号与基本性质 . . . 8
6.2 Gauss 引理与补充定律 . . . 9
6.3 二次互反律 . . . 9
6.4 Gauss 和版本 . . . 9

7 Riemann zeta 函数（只需了解主要结论） **10**

8 Dirichlet L 函数（只需了解主要结论） **11**

9 解码算术信息：Fourier 分析（只需了解主要结论） 11

10 Fermat 方程的模 p 解（只需了解主要结论） 12

10.1 一元方程 $x^n = a$ 12

10.2 Jacobi 和与 Fermat 方程 12

11 Fermat 方程的有理数解 13

11.1 $n = 2$：Pythagoras 方程 13

11.2 $n = 4$：Fermat 无穷递降 13

11.3 $n = 3$：三次分圆整数环与无穷递降 14

考前速查表 15

复习范围说明。 本提纲按讲义章节整理。第 1–6 节与第 11 节为重点：列出核心定义、结论、定理与常用判别，并尽量保留证明思路关键词。第 7–10 节不要求掌握证明，因此只记录主要结论、定理和它们的用途。

1 唯一因子分解

1.1 整除、素数与唯一分解

定义 1.1 (整除). 设 $a, b \in \mathbb{Z}$ 且 $a \neq 0$。若存在 $c \in \mathbb{Z}$ 使得 $b = ac$，则称 a 整除 b，记作 $a \mid b$。

定义 1.2 (素数). 设 $p \in \mathbb{Z}$ 且 $p \neq 0$。若仅有 $\pm 1, \pm p$ 整除 p，则称 p 是素数。通常正素数记为 $2, 3, 5, 7, \ldots$。

命题 1.3 (整除的基本性质). 对整数 a, b, c:

1. $a \neq 0 \Rightarrow a \mid a$;
2. $a \mid b$ 且 $b \mid a \Rightarrow a = \pm b$;
3. $a \mid b$ 且 $b \mid c \Rightarrow a \mid c$;
4. $a \mid b$ 且 $a \mid c \Rightarrow a \mid bx + cy$，其中 $x, y \in \mathbb{Z}$。

定理 1.4 (算术基本定理/唯一分解定理). 任何非零整数 n 可唯一写成

$$n = \operatorname{sgn}(n) \prod_{p} p^{\alpha(n,p)},$$

其中 p 遍历正素数，$\alpha(n,p) \in \mathbb{Z}_{\geq 0}$，且除有限多个 p 外 $\alpha(n,p) = 0$。

1.2 最大公因子与 Bezout 等式

定义 1.5 (p-进阶). 设 p 是正素数，定义

$$\mathrm{ord}_p(n) = \max\{a \in \mathbb{N} : p^a \mid n\}, \qquad \mathrm{ord}_p(0) = \infty.$$

重要性质：

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b).$$

定义 1.6 (最大公因子). 设 $a, b \in \mathbb{Z}$ 且不都为 0。若 $d \mid a, d \mid b$，且任意公共因子 d' 都满足 $d' \mid d$，则称 d 是 a, b 的最大公因子，记作 $\gcd(a, b) = d$，只差一个单位 ± 1。

引理 1.7 (带余除法). 设 $a, b \in \mathbb{Z}$ 且 $b > 0$，则存在 $q, r \in \mathbb{Z}$ 使

$$a = qb + r, \qquad 0 \le r < b.$$

定理 1.8 (Bezout 形式). 设 $a, b \in \mathbb{Z}$。存在 $d \in \mathbb{Z}$ 使

$$(a, b) = \{ax + by : x, y \in \mathbb{Z}\} = (d),$$

且 d 是 a, b 的最大公因子。特别地，若 $\gcd(a, b) = 1$，则存在 $u, v \in \mathbb{Z}$ 使 $au + bv = 1$。

命题 1.9 (最大公因子常用性质). *1.* $\gcd(ma, mb) = m \gcd(a, b)$（差符号不计）。

2. 若 $\gcd(a, b) = d$，则 $\gcd(a/d, b/d) = 1$。

3. 若 $\gcd(a, b) = 1$，则 $\gcd(a, bc) = \gcd(a, c)$。

1.3 素数分布的初步估计

定理 1.10 (素数无穷). $\mathbb{Z}$ 中有无穷多个正素数。经典证明：若只有 $p_1, \ldots, p_n$，则 $p_1 \cdots p_n + 1$ 有新的素因子。

定义 1.11. 令

$$\pi(x) = |\{p \le x : p \text{ 为素数}\}|, \qquad \vartheta(x) = \sum_{p \le x} \log p.$$

定理 1.12 (Chebyshev 型估计). 存在常数 $c_1, c_2 > 0$，使得当 x 充分大时

$$c_2 \frac{x}{\log x} < \pi(x) < c_1 \frac{x}{\log x}.$$

讲义还给出素数定理作为拓展：

$$\pi(x) \sim \frac{x}{\log x}, \qquad \vartheta(x) \sim x.$$

2 Gauss 整数环与二平方和问题

2.1 环中单位、不可约元、素元

定义 2.1. 设 $R \subset \mathbb{C}$ 是子环。

1. $u \in R$ 若存在 $v \in R$ 使 $uv = 1$，则称 u 为单位，单位群记作 $R^\times$。
2. 非单位 $a \in R$ 若 $a = bc$ 时 b, c 中必有一个是单位，则称 a 为不可约元。
3. $p \in R$ 若 $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$，则称 p 为素元。

素元必不可约；在 UFD 中不可约元也是素元。

定义 2.2 (Gauss 整数)**.**

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}, \qquad \mathrm{Nm}(a + bi) = a^2 + b^2.$$

范数允许在 $\mathbb{Z}[i]$ 中做带余除法，因此 $\mathbb{Z}[i]$ 是 UFD。

引理 2.3. $\mathbb{Z}[i]$ 中全部单位为

$$\{\pm 1, \pm i\}.$$

2.2 有理素数在 $\mathbb{Z}[i]$ 中的分解

定理 2.4. 设 $p \in \mathbb{Z}$ 为正素数。

1. p 在 $\mathbb{Z}[i]$ 中或者仍为素元，或者存在素元 $\pi \in \mathbb{Z}[i]$ 使 $p = \pi\overline{\pi}$。
2. p 在 $\mathbb{Z}[i]$ 中是素元当且仅当 $p \equiv 3 \pmod 4$。
3. $p = 2$ 时有 $2 = (1 + i)(1 - i)$；若 $p \equiv 1 \pmod 4$，则存在 $a, b \in \mathbb{Z}$ 使 $p = a^2 + b^2$。

2.3 二平方和定理

定理 2.5 (二平方和定理)**.** 设 $n \geq 2$，素因子分解写成

$$n = 2^\alpha p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s},$$

其中 $p_i \equiv 1 \pmod 4$，$q_j \equiv 3 \pmod 4$。则

$$n = a^2 + b^2$$

有整数解当且仅当所有 γ_j 都是偶数。此时有

$$4(\beta_1 + 1)(\beta_2 + 1) \cdots (\beta_r + 1)$$

组整数解（计入符号与顺序）。

3 同余理论

3.1 模 m 同余与剩余类环

定义 3.1 (同余). 设 $m \in \mathbb{Z}_{>0}$，$a, b \in \mathbb{Z}$。若 $m \mid (a-b)$，则称

$$a \equiv b \pmod{m}.$$

所有模 m 的等价类记作 $\mathbb{Z}/m\mathbb{Z}$，代表元可取 $0, 1, \ldots, m-1$。

命题 3.2 (同余运算性质). 若 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，则

$$a \pm c \equiv b \pm d \pmod{m}, \qquad ac \equiv bd \pmod{m}.$$

若 $\ell \mid m$，则 $a \equiv b \pmod{\ell}$。若同时 $a \equiv b \pmod{n}$，则 $a \equiv b \pmod{\operatorname{lcm}(m,n)}$。

推论 3.3. $\mathbb{Z}/m\mathbb{Z}$ 上可良定义加法与乘法：

$$[a] + [b] = [a+b], \qquad [a][b] = [ab].$$

当 $m = p$ 为素数时，$\mathbb{Z}/p\mathbb{Z}$ 是域，常记作 $\mathbb{F}_p$。

3.2 模约化、多项式应用

命题 3.4 (模约化同态). 映射

$$\pi_m : \mathbb{Z}[x_1, \ldots, x_n] \to (\mathbb{Z}/m\mathbb{Z})[x_1, \ldots, x_n]$$

满足

$$\pi_m(f+g) = \pi_m(f) + \pi_m(g), \qquad \pi_m(fg) = \pi_m(f)\pi_m(g).$$

若 $d \mid m$，还有自然约化 $\pi_{d|m}$。

推论 3.5 (模障碍). 若存在 $m > 0$ 使 $\pi_m(f) = 0$ 在 $(\mathbb{Z}/m\mathbb{Z})^n$ 中无解，则 $f = 0$ 在 $\mathbb{Z}^n$ 中无解。

推论 3.6 (Gauss 引理). 两个本原整系数多项式的乘积仍是本原多项式。由此可推出 $\mathbb{Z}[x_1, \ldots, x_n]$ 是 *UFD*。

引理 3.7 (Eisenstein 判别法). 设 $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$。若存在素数 p 使

$$p \nmid a_n, quadp \mid a_i \ (0 \le i \le n-1), \quad p^2 \nmid a_0,$$

则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

3.3 一次同余、中国剩余定理、Euler 定理

定理 3.8 (一次同余方程)**.** 同余方程

$$ax \equiv b \pmod{m}$$

有解当且仅当 $d = \gcd(a, m)$ 满足 $d \mid b$。若 x_0 是一个解，则模 m 下全部解为

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots,\ x_0 + (d-1)\frac{m}{d}.$$

推论 3.9 (可逆元判别)**.** $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ 可逆当且仅当 $\gcd(a, m) = 1$。单位群记作 $U(\mathbb{Z}/m\mathbb{Z})$。

定理 3.10 (中国剩余定理)**.** 若 $\gcd(m, n) = 1$，则

$$\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad [a]_{mn} \mapsto ([a]_m, [a]_n)$$

是环同构。于是

$$U(\mathbb{Z}/mn\mathbb{Z}) \cong U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z}).$$

定义 3.11 (Euler 函数)**.**

$$\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|.$$

若 $(m, n) = 1$，则 $\varphi(mn) = \varphi(m)\varphi(n)$；且 $\varphi(p^a) = p^a - p^{a-1}$。

定理 3.12 (Euler 定理)**.** 若 $\gcd(a, m) = 1$，则

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

特别地，若 p 为素数，则 *Fermat* 小定理给出

$$a^p \equiv a \pmod{p}.$$

定义 3.13 (阶与原根)**.** 若 $\gcd(a, m) = 1$，称最小正整数 n 使 $a^n \equiv 1 \pmod{m}$ 为 a 模 m 的阶。若该阶为 $\varphi(m)$，则 a 称为模 m 的原根。

4 分圆多项式

定义 4.1 (本原单位根与分圆多项式)**.** 设 $\zeta = e^{2\pi i/n}$。若 ξ 是 n 次单位根，且 $\xi^i \neq 1$ 对 $1 \leq i \leq n-1$ 均成立，则称 ξ 为 n 次本原单位根。定义

$$\Phi_n(x) = \prod_{\xi} (x - \xi),$$

其中 ξ 遍历所有 n 次本原单位根。其次数为 $\varphi(n)$。

引理 4.2.

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x), \qquad n = \sum_{d \mid n} \varphi(d).$$

命题 4.3. 对任意 $n \geq 1$，$\Phi_n(x)$ 是首一整数系数多项式，因而是本原多项式。

引理 4.4 (无平方因子)**.** 若 p 为素数且 $p \nmid n$，则 $x^n - 1 \in \mathbb{F}_p[x]$ 无平方因子。

定理 4.5 (分圆多项式不可约)**.** $\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

引理 4.6 (分圆多项式与阶)**.** 若 $\Phi_n(a) \equiv 0 \pmod{p}$，则 a 模 p 的阶为 n，或者 $p \mid n$。

推论 4.7 (模素数原根存在)**.** 对任意正素数 p，存在 $a \in \mathbb{Z}$ 使 a 模 p 的阶恰为 $p-1$。

推论 4.8. 若 $p \equiv 1 \pmod 4$，则存在 $x \in \mathbb{Z}$ 使

$$x^2 + 1 \equiv 0 \pmod{p}.$$

这补全了 $p \equiv 1 \pmod 4$ 的素数可写成两平方和的关键一步。

定理 4.9 (Dirichlet 定理的特例)**.** 对任意正整数 m，存在无穷多个素数满足

$$p \equiv 1 \pmod{m}.$$

5 高次同余方程与原根

定义 5.1 (n 次剩余)**.** 若 $\gcd(a, m) = 1$ 且同余方程

$$x^n \equiv a \pmod{m}$$

有解，则称 a 是模 m 的 n 次剩余。

5.1 奇素数幂模数

定理 5.2. 若 p 是奇素数，$\ell \geq 1$，则模 p^ℓ 存在原根。

推论 5.3. 设 p 为奇素数，$e \geq 1$，$\gcd(a, p) = 1$。同余方程

$$x^n \equiv a \pmod{p^e}$$

有解当且仅当

$$a^{\varphi(p^e)/d} \equiv 1 \pmod{p^e}, \qquad d = \gcd(n, \varphi(p^e)).$$

可解时恰有 d 个解。

5.2 2 的幂模数

定理 5.4. 模 2^ℓ 存在原根当且仅当 $\ell = 1, 2$。当 $\ell \geq 3$ 时，

$$\{(-1)^a 5^b : a = 0, 1,\ 0 \leq b < 2^{\ell-2}\}$$

是模 2^ℓ 的一组既约剩余系。

推论 5.5. 设 a 为奇数，$\ell \geq 3$。方程 $x^n \equiv a \pmod{2^\ell}$：

1. 若 n 为奇数，则有唯一解；
2. 若 n 为偶数，则有解当且仅当

$$a \equiv 1 \pmod 4, \qquad a^{2^{\ell-2}/d} \equiv 1 \pmod{2^\ell}, \quad d = \gcd(n, 2^{\ell-2}),$$

此时共有 $2d$ 个解。

定理 5.6 (原根存在的完全分类)**.** 正整数 m 有原根当且仅当

$$m = 2, \quad 4, \quad p^\ell, \quad 2p^\ell,$$

其中 p 为奇素数，$\ell \geq 1$。

6 二次互反律：Theorema Aureum

6.1 Legendre 符号与基本性质

定义 6.1 (Legendre 符号)**.** 设 p 是奇素数。定义

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & x^2 \equiv a \pmod p \text{ 有解且} p \nmid a, \\ -1, & x^2 \equiv a \pmod p \text{ 无解}, \\ 0, & p \mid a. \end{cases}$$

命题 6.2 (Legendre 符号性质)**.** 1. 若 $a \equiv b \pmod p$，则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$。

2. *Euler* 判别法：

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

3. 乘性：

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

命题 6.3. 模 p 的二次剩余与二次非剩余各有 $(p-1)/2$ 个，且

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

因此 -1 是模 p 平方剩余当且仅当 $p \equiv 1 \pmod 4$。

6.2 Gauss 引理与补充定律

引理 6.4 (Gauss 引理)**.** 设 p 为奇素数，$p \nmid a$。令 μ 为

$$a, 2a, \ldots, \frac{p-1}{2}a$$

模 p 后余数大于 $p/2$ 的项数。则

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

推论 6.5 (2 的补充定律)**.**

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

等价地，2 是模 p 的二次剩余当且仅当 $p \equiv \pm 1 \pmod 8$。

6.3 二次互反律

定理 6.6 (二次互反律)**.** 设 p, q 是奇素数，则

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

等价地，除非 $p \equiv q \equiv 3 \pmod 4$，否则可直接交换上下；若二者都为 $3 \pmod 4$，交换时多一个负号。

计算 Legendre 符号的流程。 将分子分解为 $-1, 2$ 和奇素数的乘积；用乘性、-1 补充定律、2 补充定律和二次互反律逐步化简到小模数。

定理 6.7 (平方剩余的同余类刻画，原型)**.** 给定非平方整数 a，存在 $M > 0$ 及若干模 M 的剩余类 r_i，使充分大的素数 p 满足

$$a \text{ 是模} p \text{ 的平方剩余} \iff p \equiv r_i \pmod M \text{ 对某个} i.$$

例：

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3,$$

并且

$$\left(\frac{6}{p}\right) = 1 \iff p \equiv 1, 5, 19, 23 \pmod{24}.$$

定理 6.8. 若 a 是非平方整数，则存在无穷多个素数 p 使 a 模 p 不是二次剩余。

6.4 Gauss 和版本

定义 6.9 (Gauss 和)**.** 令 $\zeta_p = e^{2\pi i/p}$，定义

$$g_a = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta_p^{ak}, \qquad g = g_1.$$

命题 6.10.

$$g_a = \left(\frac{a}{p}\right) g, \qquad g^2 = p^*, \qquad p^* = (-1)^{(p-1)/2} p.$$

这些性质可用于给出二次互反律的 *Gauss* 和证明。

7 Riemann zeta 函数（只需了解主要结论）

定义 7.1. 当 $\mathrm{Re}(s) > 1$ 时，Riemann zeta 函数定义为

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

命题 7.2 (Euler 乘积)**.** 当 $\mathrm{Re}(s) > 1$ 时，

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

这将 $\zeta(s)$ 与素数分布联系起来，也反映算术基本定理。

定义 7.3 (Gamma 函数与完备 zeta 函数)**.**

$$\Gamma(s) = \int_0^{\infty} e^{-y} y^s \frac{dy}{y}, \qquad Z(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

定理 7.4 (解析延拓与函数方程)**.** $Z(s)$ 可解析延拓到 $\mathbb{C} \setminus \{0, 1\}$，在 $0, 1$ 处有单极点，且满足

$$Z(s) = Z(1 - s).$$

因此 $\zeta(s)$ 可亚纯延拓到 $\mathbb{C}$，仅在 $s = 1$ 有单极点，留数为 1。

定理 7.5 (Riemann 猜想)**.** $\zeta(s)$ 的所有非平凡零点都位于直线

$$\mathrm{Re}(s) = \frac{1}{2}.$$

讲义中只作为背景介绍。

定义 7.6 (Dirichlet 密度)**.** 设 S 是素数集合的子集。若极限

$$\lim_{s \to 1^+} \frac{\sum_{p \in S} p^{-s}}{\log \frac{1}{s-1}}$$

存在，则称其为 S 的 Dirichlet 密度，记作 $d(S)$。

定理 7.7 (Dirichlet 定理)**.** 若 $\gcd(a, m) = 1$，则

$$P(a, m) = \{p \in \mathrm{Prim} : p \equiv a \pmod{m}\}$$

的 *Dirichlet* 密度存在，且

$$d(P(a, m)) = \frac{1}{\varphi(m)}.$$

8 Dirichlet L 函数（只需了解主要结论）

定义 8.1 (Dirichlet 特征). 模 m 的 Dirichlet 特征是群同态

$$\chi : U(\mathbb{Z}/m\mathbb{Z}) \to S^1.$$

它可延拓为 $\mathbb{Z}$ 上函数：若 $(n,m) > 1$，令 $\chi(n) = 0$；否则令 $\chi(n) = \chi([n])$。平凡特征记作 χ_0。

定义 8.2 (Dirichlet L 函数). 当 $\mathrm{Re}(s) > 1$ 时，

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

命题 8.3 (Euler 乘积). 当 $\mathrm{Re}(s) > 1$ 时，

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

定理 8.4 (完备 L 函数与函数方程). 对本原特征 χ，引入适当的 *Gamma* 因子和 *Gauss* 和后，完备函数 $\Lambda(\chi, s)$ 可延拓，并满足将 s 与 $1-s$ 联系起来的函数方程。其形式与 *Riemann zeta* 函数的函数方程平行。

定理 8.5 (关键非消失). 若 $\chi \neq \chi_0$，则

$$L(\chi, 1) \neq 0.$$

这是证明 *Dirichlet* 等差数列素数定理的核心输入。

9 解码算术信息：Fourier 分析（只需了解主要结论）

定义 9.1 (有限 Abel 群上的特征与 Fourier 变换). 设 A 是有限 Abel 群，$\widehat{A} = \mathrm{Hom}(A, S^1)$。对 $f \in \mathbb{C}[A]$，定义

$$\widehat{f}(\chi) = \frac{1}{\sqrt{|A|}} \sum_{a \in A} f(a)\chi(a).$$

定理 9.2 (Fourier 反演). 对任意 $f \in \mathbb{C}[A]$，有

$$\widehat{\widehat{f}} = f$$

(按讲义约定识别 A 与双对偶)。

定理 9.3 (Plancherel/Parseval). *Fourier* 变换保持 L^2 内积与范数，是有限群函数空间之间的酉变换。

命题 9.4 (卷积与 Fourier 变换). 卷积在 *Fourier* 变换下变为逐点乘法。这是用特征和解码计数信息的基本工具。

用途。 有限群 Fourier 分析用于证明 Dirichlet 定理：通过特征正交关系，把 “$p \equiv a \pmod m$” 这一条件编码为所有 Dirichlet 特征的和，再结合 $L(\chi,1)\neq 0$ 得到密度 $1/\varphi(m)$。

10 Fermat 方程的模 p 解（只需了解主要结论）

10.1 一元方程 $x^n = a$

命题 10.1. 设 $p \equiv 1 \pmod n$。令

$$N(x^n = a) = |\{x \in \mathbb{F}_p : x^n = a\}|.$$

则

$$N(x^n = a) = \sum_{\chi^n = \chi_0} \chi(a),$$

其中求和遍历 $\mathbb{F}_p^\times$ 上所有 n 次特征。

10.2 Jacobi 和与 Fermat 方程

定义 10.2 (Jacobi 和)**.** 设 χ, λ 是 $\mathbb{F}_p^\times$ 的特征，按讲义约定延拓到 $\mathbb{F}_p$。定义

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

命题 10.3 (Jacobi 和性质)**.** 若 χ, λ 非平凡，则

1. $J(\chi_0,\chi_0) = p$，$J(\chi_0,\chi) = 0$；
2. $J(\chi,\chi^{-1}) = -\chi(-1)$；
3. 若 $\chi\lambda \neq \chi_0$，则
$$J(\chi,\lambda) = \frac{\tau(\chi)\tau(\lambda)}{\tau(\chi\lambda)},$$
其中 $\tau(\chi)$ 是相应 *Gauss* 和。

推论 10.4. 若 $\chi, \lambda, \chi\lambda$ 均非平凡，则

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

命题 10.5. 设 $p \equiv 1 \pmod n$，$n > 2$，χ 是阶为 n 的非平凡特征，则

$$\tau(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

几何意义。 对 Fermat 曲线 $C_n : -x_0^n + x_1^n + x_2^n = 0$，点数 $|C_n(\mathbb{F}_{p^f})|$ 可由 Jacobi 和组织；相应的 zeta 函数

$$Z(C_n,u) = \exp\left(\sum_{f=1}^{\infty} |C_n(\mathbb{F}_{p^f})| \frac{u^f}{f}\right)$$

是有理函数，其分子根在换元 $u = p^{-s}$ 后位于 $\mathrm{Re}(s) = 1/2$，与 Riemann 猜想的形式呼应。

11 Fermat 方程的有理数解

11.1 $n = 2$：Pythagoras 方程

研究

$$x^2 + y^2 = 1$$

的有理解。

定理 11.1 (几何参数化). 所有有理解可由斜率 $k \in \mathbb{Q}$ 参数化：

$$x = \frac{1-k^2}{1+k^2}, \qquad y = \frac{2k}{1+k^2}.$$

几何解释：过有理点 $(-1, 0)$ 作斜率为 k 的直线 $y = kx + k$，其与单位圆的另一个交点给出上述公式。

定理 11.2 (勾股数组). 求 $x^2 + y^2 = 1$ 的有理解等价于求互素整数解

$$x_0^2 + y_0^2 = z_0^2.$$

在 $\mathbb{Z}[i]$ 中分解

$$(x_0 + iy_0)(x_0 - iy_0) = z_0^2.$$

若 x_0, y_0 互素，则两个因子在 $\mathbb{Z}[i]$ 中互素，故 $x_0 + iy_0$ 在相差单位意义下为平方。于是存在 $a, b \in \mathbb{Z}$，使

$$(x_0, y_0, z_0) = (\pm(a^2 - b^2), \pm 2ab, a^2 + b^2)$$

或交换前两项。

11.2 $n = 4$：Fermat 无穷递降

定理 11.3 (Fermat, $n = 4$). 方程

$$x^4 + y^4 = z^2$$

无非零整数解。因此

$$x^4 + y^4 = z^4$$

亦无非零整数解。

证明思路关键词。 假设存在 z_0 最小的正整数解，且 x_0, y_0 互素。利用奇偶性令 x_0 奇、y_0 偶，得到

$$(z_0 - x_0^2)(z_0 + x_0^2) = y_0^4, \qquad \gcd(z_0 - x_0^2, z_0 + x_0^2) = 2.$$

分析两个因子的形状，排除一种模 4 矛盾情形；剩余情形继续分解

$$4a^4 = (b^2 - x_0)(b^2 + x_0),$$

构造出更小的正整数解

$$c^4 + d^4 = b^2,$$

与 z_0 最小性矛盾。这就是无穷递降法。

11.3 $n = 3$：三次分圆整数环与无穷递降

令

$$\omega = \frac{-1+\sqrt{-3}}{2}, \qquad \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}.$$

此环是三次分圆整数环，范数为

$$\mathrm{Nm}(a + b\omega) = a^2 - ab + b^2.$$

命题 11.4 (基本事实). *1.* $\mathbb{Z}[\omega]$ 的单位为 $\pm 1, \pm\omega, \pm\omega^2$。

2. 令 $\lambda = 1 - \omega$，则 λ 是素元，且 $(\lambda^2) = (3)$。

3. 对任意 $\alpha \in \mathbb{Z}[\omega]$，定义

$$\mathrm{ord}_\lambda(\alpha) = \max\{e \in \mathbb{N} : \lambda^e \mid \alpha\}.$$

4. 任意 $\alpha \in \mathbb{Z}[\omega]$ 都与 $-1, 0, 1$ 之一模 λ 同余。

定理 11.5 (Fermat, $n = 3$). 对任意单位 $u \in \mathbb{Z}[\omega]$，方程

$$x^3 + y^3 = uz^3$$

在 $\mathbb{Z}[\omega]$ 中无非零解。因此 *Fermat* 方程

$$x^3 + y^3 = z^3$$

无非零整数解。

引理 11.6. 若 $\lambda \nmid \alpha$，则

$$\alpha^3 \equiv \pm 1 \pmod{\lambda^4}.$$

因此方程 $x^3 + y^3 = uz^3$ 不存在满足 $\lambda \nmid xyz$ 的解。

引理 11.7. 给定单位 u，若 $x^3 + y^3 = uz^3$ 有解且 $\lambda \nmid xy$，则

$$\lambda^2 \mid z.$$

引理 11.8 (递降步). 若 x_0, y_0 互素，$\lambda \nmid x_0 y_0$，且

$$x_0^3 + y_0^3 = uz_0^3,$$

则可构造单位 u_1 与新解

$$x_1^3 + y_1^3 = u_1 z_1^3$$

满足

$$\lambda \nmid x_1 y_1, \qquad \mathrm{ord}_\lambda(z_1) = \mathrm{ord}_\lambda(z_0) - 1.$$

证明思路关键词。 在 $\mathbb{Z}[\omega]$ 中分解

$$(x+y)(x+\omega y)(x+\omega^2 y) = uz^3.$$

用 λ 控制三个因子的公共部分；当 $\lambda \nmid xy$ 时，三个因子两两最大公因子恰为 λ。由 UFD 可将它们写成单位、λ 的幂和立方的乘积，再线性组合，得到一个 $\mathrm{ord}_\lambda(z)$ 严格下降的新解。无限重复会产生严格递减的非负整数列，矛盾。

备注 11.9. $n=3$ 的证明展示了 Fermat 方法在更大整数环中的推广；讲义最后指出，一部分论证可推广到 regular prime 的情形，与分圆域类数相关。

考前速查表

主题	必记结论	常用工具
唯一分解	$n = \pm\prod p^{\alpha_p}$	gcd, Bezout, ord_p
二平方和	$q \equiv 3 \pmod 4$ 指数全偶	$\mathbb{Z}[i]$ UFD
同余方程	$ax \equiv b$ 可解 $\Leftrightarrow (a,m) \mid b$	Bezout
CRT	$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	$(m,n)=1$
Euler	$a^{\varphi(m)} \equiv 1$	单位群
分圆多项式	$x^n - 1 = \prod_{d\mid n} \Phi_d$	单位根分类
原根分类	$2, 4, p^\ell, 2p^\ell$	单位群结构
二次互反律	$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$	Gauss 引理
Fermat $n=4$	$x^4+y^4=z^2$ 无非零整数解	无穷递降
Fermat $n=3$	$x^3+y^3=z^3$ 无非零整数解	$\mathbb{Z}[\omega]$, $\lambda = 1-\omega$