初等数论速通指南

~~从入坑到入土~~

Edit with LaTeX, Version β1.1. (下载链接)

前 言

这是笔者在学习 **数论基础** (MATH511807) 课程时的笔记. 此笔记聚焦于课程讲义 ([数论基础] 陆亚明, 易媛编) 中的定义、定理与例子, 同时提供了一部分重要习题的思路与解答. 此外, 在笔记的最后附一组参考题, 以供读者练习和检验学习成果.

本笔记可供学习数论基础课程的数学试验班和数学类同学在学习及复习时作以参考, 但笔者建议读者**合理使用这份笔记**——若您对于目录中提及的知识有足够的熟练度, 那大可抛开这份笔记, 复习时完成知识梳理后直接做题, 不必浪费宝贵的个人时间; 但当您对于课程所讲内容感到迷惑时, 希望这份笔记能有助于您对这门课程的学习与理解.

由于笔者水平有限且文件编写过程略显匆忙, 笔记中的缺陷与错误在所难免, 恳请读者发现时及时联系笔者 (HyX379@outlook.com) 批评指正, 不胜感激.

黄彦熙

2023 年 10 月 20 日

目 录

第一章　整除

由于整数集 $\mathbb{Z}$ 对于加法、减法和乘法三种运算封闭而对除法不封闭, 因此整除性是初等数论研究和讨论的首要问题.

§1.1　整除的基本概念

定义 1.1.1. 设 $a, b \in \mathbb{Z}$ 且 $b \neq 0$, 称 b **整除** a, 如果存在 $q \in \mathbb{Z}$, 使得 $a = bq$, 记作 $b \mid a$, 此时称 a 为 b 的**倍数**, b 为 a 的**除数** (也称**因数**); 反之则称 b **不整除** a, 记作 $b \nmid a$.

命题 1.1.1 (整除的基本性质)**.** 设 $a, b, c \in \mathbb{Z}$, 则有

(1) $b \mid a \;\Leftrightarrow\; -b \mid a \;\Leftrightarrow\; b \mid -a \;\Leftrightarrow\; |b| \mid |a|$;

(2) $b \mid a \wedge c \mid b \;\Rightarrow\; c \mid a$;

(3) 若 $b \mid a_k$ $(k = 1, \cdots, n)$, 则对任意的 $m_k \in \mathbb{Z}$, 都有 $b \mid \sum_{k=1}^{n} a_k m_k$;

(4) 设 $m \in \mathbb{Z}$ 且 $m \neq 0$, 则 $b \mid a \;\Leftrightarrow\; mb \mid ma$;

(5) $b \mid a \wedge a \mid b \;\Leftrightarrow\; a = \pm b$ (即 $|a| = |b|$);

(6) 若 $a \neq 0$ 且 $b \mid a$, 则 $|b| \leqslant |a|$.

证明. 充分利用定义.

(1) $b \mid a$ 则存在 $q \in \mathbb{Z}$ 使得 $a = bq$, 则 $-a = -bq$ 且 $|a| = |b|\,|q|$, 即 $b \mid -a$, $-b \mid a$ 且 $|b| \mid |a|$, 其它证明类似;

(2) 易知存在 $p, q \in \mathbb{Z}$, 使得 $a = qb$ 且 $b = pc$, 则 $a = (pq)c$, 即 $c \mid a$;

(3) 易知存在 $q_k \in \mathbb{Z}$ 使得 $a_k = bq_k$, $\sum_{k=1}^{n} a_k m_k = b(\sum_{k=1}^{n} q_k m_k)$, 即 $b \mid \sum_{k=1}^{n} a_k m_k$;

(4) $\Rightarrow$ 显然, $\Leftarrow$ 成立是因为 $ma = mbq$ 且 $m \neq 0$, 即可推出 $a = bq$, 即 $b \mid a$;

(5) 因 $b \mid a$ 则存在 $q \in \mathbb{Z}$ 使得 $a = bq$; 同理, 存在 $p \in \mathbb{Z}$ 使得 $b = ap$, 于是有 $a = a(pq)$, 又 $a \neq 0$, 则 $pq = 1$, 即 $p = q = \pm 1$, 故 $|a| = |b|$;

(6) 存在 $q \in \mathbb{Z}$ 使 $a = bq$, 即 $|a| = |b|\,|q|$. 又 $a \neq 0$, 则 $|q| \geqslant 1$, 即 $|a| = |q|\,|b| \geqslant |b|$.

这样, 我们便完成了所有的证明. □

例 1.1.1. 设 $f \in \mathbb{Z}[x]$ 且 $d \mid a-b$, 则 $d \mid f(a)-f(b)$.

证明. $a=b$ 时显然成立; $a \neq b$ 时, 设 $f=\sum\limits_{k=1}^{n} a_k x^k$, 则 $f(a)-f(b)=\sum\limits_{k=1}^{n} a_k(a^k-b^k)$, 又 $a^k-b^k=(a-b)(a^{k-1}+\cdots+b^{k-1})$ $(\forall k \in \mathbb{Z}_{\geqslant 0})$, 即 $a-b \mid a^k-b^k$, 故 $d \mid f(a)-f(b)$. □

例 1.1.2. 设 $a, q \in \mathbb{Z}$ 且 $q>0$, 证明:

$$\sum_{k=1}^{q} e\left(\frac{ak}{q}\right)=\begin{cases} q, & \text{若 } q \mid a, \\ 0, & \text{若 } q \nmid a. \end{cases}$$

其中 $e(x):=e^{2\pi \mathrm{i} x}$, i 是虚数单位.

证明. 将上式左边记作 S_q. 当 $q \mid a$ 时, 对任意的 $k \in \mathbb{Z}$ 都有 $e\left(\frac{ak}{q}\right)=1$, 从而有 $S_q=q$; 当 $q \nmid a$ 时, 注意到 $e\left(\frac{a}{q}\right) \neq 1$, 于是有 $S_q=e\left(\frac{a}{q}\right) \cdot \dfrac{1-e\left(\frac{aq}{q}\right)}{1-e\left(\frac{a}{q}\right)}=0$. □

注记 1.1.1. 这一例子中的函数给出了一种转化求和中整除条件的方法, 即

$$\boxed{\sum_{\substack{n \leqslant x \\ q \mid f(n)}} 1=\sum_{n \leqslant x} \frac{1}{q} \sum_{k=1}^{q} e\left(\frac{f(n)k}{q}\right).}$$

命题 1.1.2. 设 $d_1, \cdots, d_n$ 是 $a \in \mathbb{Z}_{>0}$ 的全体正除数, 则 $\frac{a}{d_1}, \cdots, \frac{a}{d_n}$ 也是 a 的全体正除数.

证明. 由 $d_k \mid a$ 知 $\frac{a}{d_k} \in \mathbb{Z}_{>0}$ 从而 $\frac{a}{d_k} \mid a$, 则

$$\left\{\frac{a}{d_1}, \cdots, \frac{a}{d_n}\right\} \subseteq \{d_1, \cdots, d_n\}.$$

另一方面, $\frac{a}{d_k} \neq \frac{a}{d_l}$ $(\forall\, k \neq l)$, 故

$$\left|\left\{\frac{a}{d_1}, \cdots, \frac{a}{d_n}\right\}\right|=n=|\{d_1, \cdots, d_n\}|,$$

即 $\left\{\frac{a}{d_1}, \cdots, \frac{a}{d_n}\right\}=\{d_1, \cdots, d_n\}$. □

注记 1.1.2. 这一命题表明, 一个整数的除数是**成对出现**的, 从而 $\sum\limits_{d \mid n} f(d)=\sum\limits_{d \mid n} f\left(\frac{n}{d}\right)$.

定理 1.1.1. 设 $a, b \in \mathbb{Z}$ 且 $b>0$, 则存在唯一的 $q, r \in \mathbb{Z}$, 使得 $a=bq+r$ 且 $0 \leqslant r<b$.

证明. 存在性. 考虑集合 $\{nb : n \in \mathbb{Z}\}$, 可知必然存在 $q \in \mathbb{Z}$ [†], 使得 $qb \leqslant a < (q+1)b$. 现令 $r := a - bq$, 则有 $a = bq + r$ 且 $0 \leqslant r < b$.

唯一性. 假设存在整数 q_1, r_1 与 q_2, r_2 均满足 $a = bq_k + r_k$ 且 $0 \leqslant r_k < b$ $(k = 1, 2)$, 则 $b(q_1 - q_2) = r_1 - r_2$, 这表明 $r_1 - r_2$ 是 b 的倍数, 但 $0 \leqslant |r_1 - r_2| < b$, 所以 $r_1 - r_2 = 0$, 即 $r_1 = r_2$ 且 $q_1 = q_2$, 也就是说, 满足条件的 q, r 是唯一的. □

注记 1.1.3. 这便是知名的**带余除法**. 这一定理中的 q 称为 a 除以 b 所得的 **(不完全) 商**, r 称为 a 除以 b 所得的 **(最小非负) 余数**.

类似地, 可以证明存在唯一的整数 q' 与 r', 使得 $a = bq' + r'$ 且 $1 \leqslant r' \leqslant b$, 这样的 r' 被称为 a 除以 b 所得的**最小正余数**; 同样地, 可以证明存在整数 q'' 与 r'', 使得 $a = bq'' + r''$ 且 $-\dfrac{b}{2} \leqslant r'' \leqslant \dfrac{b}{2}$, 这样的 r' 被称为 a 除以 b 所得的**绝对最小余数**.

需要指出, 绝对最小余数并不总是唯一的, 例如 $6 = 4 \times 1 + 2 = 4 + (-2)$. 也就是说, 绝对最小余数在 $a \neq \left(k + \dfrac{1}{2}\right) b$ $(k \in \mathbb{Z})$ 时总是唯一的.

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 1.1.3. 证明: 对任意的奇数 n, 都有 $8 \mid n^2 - 1$.

证明. 设奇数 $n := 2k+1$ $(k \in \mathbb{N})$, 则 $n^2 - 1 = (n-1)(n+1) = 4k(k+1)$, 又 $2 \mid k(k+1)$, 故 $8 \mid 4k(k+1)$, 即 $8 \mid n^2 - 1$. □

例 1.1.4. 证明: $\forall\, n \in \mathbb{Z}$, $6 \mid n(n+1)(2n+1)$.

证明. 注意到 $2 \mid n(n+1)$, 故只需证 $3 \mid n(n+1)(2n+1)$, 分为 $3 \mid n$, $3 \mid n+1$ 与 $3 \mid n+2$ 三种情形讨论即证. □

例 1.1.5. 设 $k \in \mathbb{Z}_{>0}$, 证明: $n^2 \mid (n+1)^k - 1$ 成立的充要条件是 $n \mid k$.

证明. 由于 $(n+1)^k - 1 = n^k + kn^{k-1} + \cdots + kn$, 所以 $n^2 \mid (n+1)^k - 1$ 当且仅当 $n^2 \mid kn$, 而 $n \neq 0$, 故 $n^2 \mid (n+1)^k - 1$ 当且仅当 $n \mid k$. □

例 1.1.6. 证明: $\forall\, a, b \in \mathbb{Z}$, $8 \nmid a^2 - b^2 - 2$.

证明. 注意到任一完全平方数 n^2 除以 8 的余数只可能为 0, 1 或 4, 故不存在两个完全平方数相减后除以 8 的余数为 2. □

例 1.1.7. 证明: 若 $3 \nmid xy$, 则 $x^2 + y^2$ 不是完全平方数.

[†]事实上, q 的存在性并不是显然的, 需要通过 $\mathbb{Z}$ 中的 Archimedean 性质与良序原理才能得到.

证明. 注意到任一完全平方数 n^2 除以 3 的余数只可能为 0 或 1 且 $3 \nmid xy$, 故式 x^2+y^2 除以 3 的余数为 2, 它显然不是完全平方数. □

例 1.1.8. 证明: $\forall n \in \mathbb{Z}_{>0}$, $6^n n! \mid (3n)!$.

证明. 归纳. 显然 $n = 1, 2$ 时分别有 $6 \mid 6$ 和 $72 \mid 720$, 显然成立. 假设 $n = k$ 时成立, 则当 $n = k+1$ 时只需证明 $6(k+1) \mid (3k+3)(3k+2)(3k+1)$, 即 $2 \mid (3k+1)(3k+2)$, 这是显然成立的. 因此 $\forall n \in \mathbb{Z}_{>0}$, $6^n n! \mid (3n)!$. (也可以直接证明.) □

例 1.1.9. 设 $f := \sum_{k=1}^{n} a_k x^k \in \mathbb{Z}[x]$ 且 $f(0)$ 与 $f(1)$ 均为奇数, 证明: f 没有整数根.

证明. 反证法. 假设 f 存在整数根 $q = 2k+l$ ($q \in \mathbb{Z}, l = 0, 1$), 则 $f(q) = \sum_{k=1}^{n} a_n (2k+l)^k = 2h + f(l)$, 而 $f(0)$ 与 $f(1)$ 均为奇数, 矛盾! 因此, f 没有整数根. □

注记 1.1.4. 这一命题的后一条件还可以推广为 $f(0), \cdots, f(m-1)$ 均不被 m 整除, 原命题仍然成立. 这一例题即为 $m = 2$ 的情形.

例 1.1.10. 证明: 每个整数都可以用十进制唯一表示.

证明. 存在性 是显然的, 这源于十进制数本身的表示; 唯一性 利用反证法即可证明. □

§1.2 最大公因数

定义 1.2.1. 设 $a_1, \cdots, a_n$ 为 n 个整数, 称 $d \in \mathbb{Z}$ 为 $a_1, \cdots, a_n$ 的**公因数**, 如果 $d \mid a_k$ ($k = 1, \cdots, n$). 当 $a_1, \cdots, a_n$ 不全为 0 时, 这些数的公因数中最大者称为 $a_1, \cdots, a_n$ 的**最大公因数**, 记作 $(a_1, \cdots, a_n)$. 称 $a_1, \cdots, a_n$ **互质**, 如果 $(a_1, \cdots, a_n) = 1$. 称 $a_1, \cdots, a_n$ **两两互质**, 如果 $(a_j, a_k) = 1$ ($\forall 1 \leqslant j, k \leqslant n$ 且 $j \neq k$).

命题 1.2.1. (1) $(a_1, \cdots, a_n) = (|a_1|, \cdots, |a_n|)$; (2) $\forall b \neq 0$, $(0, b) = |b|$; (3) 设 $b > 0$, 那么 $(a, b) = b$ 当且仅当 $b \mid a$; (4) 设 a, b, c 不全为 0 且 $a = bq + c$ ($q \in \mathbb{Z}$), 则 $(a, b) = (b, c)$.

证明. (2), (3) 据定义可直接证明; (1), (4) 只需说明对应公因数的集合相同即可. □

例 1.2.1 (Fermat 数)**.** 记 $F_n := 2^{2^n} + 1$ ($n \in \mathbb{Z}_{\geqslant 0}$), 证明: 当 $m \neq n$ 时有 $(F_m, F_n) = 1$.

证明. 不妨设 $m > n$. 由于 $2^{2^n} + 1 \mid 2^{2^m} - 1$, 所以 $(F_m, F_n) = (2^{2^m} + 1 - (2^{2^m} - 1), 2^{2^n} + 1) = (2, 2^{2^n} + 1) = 1$. □

注记 1.2.1. 可以证明, 如果形如 2^k+1 的数为质数, 则 k 必然是 2 的幂, 因此 P.de Fermat 猜测形如 $2^{2^n}+1$ 的数均为质数. 尽管这一猜想被 Euler 推翻了, 但人们依然将这类数用 Fermat 的名字命名.

定理 1.2.1 (辗转相除法)**.** 设 $a,b\in\mathbb{Z}_{>0}$, 又设由带余除法可得下面一系列等式:

$$\begin{aligned}
a&=bq_1+r_1, && 0<r_1<b,\\
b&=r_1q_2+r_2, && 0<r_2<r_1,\\
&\cdots && \cdots\\
r_{n-2}&=r_{n-1}q_n+r_n, && 0<r_n<r_{n-1},\\
r_{n-1}&=r_nq_{n+1}.
\end{aligned}$$

那么 (1) $r_n=(a,b)$; (2) 存在 $x,y\in\mathbb{Z}$ 使得 $r_n=ax+by$.

证明. 据**命题 1.2.1 (4)** 可知 $r_n=(r_{n-1},r_n)=(r_{n-1},r_{n-2}-r_{n-1}q_n)=(r_{n-1},r_{n-2})$, 以此类推可得 $r_n=(r_{n-1},r_{n-2})=\cdots=(b,r_1)=(a,b)$. 再将已知的等式一一回代, 可得

$$\begin{aligned}
r_n&=r_{n-2}-r_{n-1}q_n=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-1})q_n=-q_nr_{n-3}+(1+q_{n-1}q_n)r_{n-2}\\
&=-q_nr_{n-3}+(1+q_{n-1}q_n)(r_{n-4}-r_{n-3}q_{n-2})\\
&=(1+q_{n-1}q_n)r_{n-4}-(q_n+(1+q_{n-1}q_n)q_{n-2})r_{n-3}=\cdots
\end{aligned}$$

故存在 $x,y\in\mathbb{Z}$ 使得 $r_n=ax+by$. □

注记 1.2.2. 在我国, 上述方法源于《九章算术》中的更相减损术; 国外称为 Euclid 算法.

推论 1.2.1. 设 $a,b\in\mathbb{Z}$, 则 $(a,b)=1$ 当且仅当 $\exists\,x,y\in\mathbb{Z}$ 使得 $ax+by=1$.

证明. 必要性 可由**定理 1.2.1** 给出, 下证充分性. 若存在 $x,y\in\mathbb{Z}$ 使得 $ax+by=1$, 则 a,b 的任一公因数 d 均满足 $d\mid 1$, 从而有 $(a,b)=1$. □

例 1.2.2. 求 $(-1859,1573)$, 并求一组 $x,y\in\mathbb{Z}$ 使得 $(-1859)x+1573y=(-1859,1573)$.

解. 利用辗转相除法可得 $1859=1573+286$, $1573=286\times5+143$, $286=143\times2$, 所以 $(-1859,1573)=143$. 此外,

$$143=1573-5\times286=1573-5\times(1859-1573)=5\times(-1859)+6\times1573,$$

故 $x=5$, $y=6$ 即为一组满足条件的 x,y. □

例 1.2.3. 设 $m,n\in\mathbb{Z}_{\geqslant1}$, 证明 $(2^m-1,2^n-1)=2^{(m,n)}-1$.

证明. 由辗转相除法知

$$\begin{aligned} m &= nq_1 + r_1, & 0 < r_1 < n, \\ n &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\ &\cdots & \cdots \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1}, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

其中 $r_k = (m, n)$. 则 $(2^m - 1, 2^n - 1) = (2^{r_1}(2^{nq_1} - 1) + 2^{r_1} - 1, 2^n - 1) = (2^n - 1, 2^{r_1} - 1)$, 以此类推便有 $(2^m - 1, 2^n - 1) = (2^n - 1, 2^{r_1} - 1) = \cdots = (2^{r_{k-1}} - 1, 2^{r_k} - 1) = 2^{r_k} - 1$, 所以 $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$. □

命题 1.2.2. 设 a, b 不全为 0, 则 d 是 a, b 的公因数当且仅当 $d \mid (a, b)$.

证明. 充分性. 由定理 1.2.1 知 $\exists x, y \in \mathbb{Z}$ 使得 $(a, b) = ax + by$, 故 $d \mid (a, b)$.

必要性. 因 (a, b) 为 a, b 的公因数, 故据命题 1.1.1 (2) 可得 $d \mid a$ 且 $d \mid b$. □

命题 1.2.3. 设 $a, b, c \in \mathbb{Z}$ 且 $(a, c) = 1$, 则 (1) $(ab, c) = (b, c)$; (2) $c \mid ab$ 则 $c \mid b$; (3) $a \mid b$ 且 $c \mid b$ 则 $ac \mid b$.

证明. 据**定理 1.2.1** 可知存在 $x, y \in \mathbb{Z}$ 使得 $ax + cy = 1$.

(1) 首先, b 与 c 的公因数必为 ab 与 c 的公因数; 其次, 由 $(ab)x + c(by) = b$ 知, ab 与 c 的公因数均为 b 与 c 的公因数. 故 $(ab, c) = (b, c)$.

(2) 是 (1) 的直接结论.

(3) 不妨设 $b = am = cn$ $(m, n \in \mathbb{Z})$, 则 $b = (ax + cy)b = ac(nx + my)$, 从而 $ac \mid b$. □

推论 1.2.2. 设 $a_1, \cdots, a_n$ 与 $b_1, \cdots, b_m$ 是两组整数, 若对于任意的 i, j 都有 $(a_i, b_j) = 1$, 则 $(a_1 \cdots a_n, b_1 \cdots b_m) = 1$.

证明. 对给定的 a_i, 有 $(a_i, b_j) = 1$ $(\forall\, j)$, 据**命题 1.2.3 (1)** 得 $(a_i, b_1 \cdots b_m) = 1$, 再由 i 的任意性及**命题 1.2.3 (1)** 知 $(a_1 \cdots a_n, b_1 \cdots b_m) = 1$. □

下面我们介绍另一种刻画最大公因数的方式.

定理 1.2.2 (Bézout)**.** 设 a, b 不全为 0, 则 $(a, b) = \min\{ax + by > 0 : x, y \in \mathbb{Z}\}$.

证明. 记 $S := \{ax + by > 0 : x, y \in \mathbb{Z}\}$, 则 $S \neq \varnothing$ 且 $S \subset \mathbb{Z}_{\geqslant 0}$, 故由良序定理可知 S 有最小元, 记作 d. 下证 $d = (a, b)$.

记 $d := ax_0 + by_0$, 据带余除法知存在 $q, r \in \mathbb{Z}$ 使得 $a = qd + r$ $(0 \leqslant r < d)$. 若 $r \neq 0$, 则由 $r = a - qd = a(1 - qx_0) - bqy_0$ 知 $r \in S$, 这与 d 的最小性矛盾. 因此 $r = 0$, 从而 $d \mid a$, 类似地有 $d \mid b$, 故 d 是 a, b 的公因数. 此外, 由 $d = ax_0 + by_0$ 可知 a, b 的公因数均整除 d, 从而 $d = (a, b)$. □

命题 1.2.4. 设 a, b 不全为 0, 则 (1) $\forall\, k > 0$, $k(a, b) = (ka, kb)$; (2) 设 d 是 a, b 的公因数, 则 $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \dfrac{(a, b)}{|d|}$. 特别地, $\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = 1$.

证明. 据 Bézout 定理知

$$(ka, kb) = \min\{kax + kby > 0 : x, y \in \mathbb{Z}\} = k \cdot \min\{ax + by > 0 : x, y \in \mathbb{Z}\} = k(a, b),$$

这就证明了 (1), (2) 可由 (1) 直接得到. □

最后, 我们来考虑求多个数的最大公因数的问题. 根据 Bézout 定理可得:

定理 1.2.3. 设 $a_1, \cdots, a_n \in \mathbb{Z}$ 不全为 0, 则

$$(a_1, \cdots, a_n) = \min\{a_1x_1 + \cdots + a_nx_n > 0 : x_i \in \mathbb{Z}\,(i = 1, \cdots, n)\}.$$

由此可得如下推论.

推论 1.2.3. 设 $a_1, \cdots, a_n$ 为整数.

(1) 若 $a_1, \cdots, a_n$ 不全为 0, 则 d 为 $a_1, \cdots, a_n$ 的公因数当且仅当 $d \mid (a_1, \cdots, a_n)$;

(2) $(a_1, \cdots, a_{n+1}) = ((a_1, \cdots, a_n), a_{n+1})$.

证明. (1) 是**定理 1.2.3** 的直接推论, 下证 (2).

一方面, 如果 d 是 $a_1, \cdots, a_{n+1}$ 的公因数, 则必有 $d \mid (a_1, \cdots, a_n)$ 且 $d \mid a_{n+1}$, 即 d 是 $(a_1, \cdots, a_n)$ 与 a_{n+1} 的公因数; 另一方面, 若 d 是 $(a_1, \cdots, a_n)$ 和 a_{n+1} 的公因数, 则由 (1) 知 d 是 $a_1, \cdots, a_{n+1}$ 的公因数, 因此 $(a_1, \cdots, a_n)$ 和 a_{n+1} 的公因数集合与 $a_1, \cdots, a_{n+1}$ 的公因数集合相等, 从而 $(a_1, \cdots, a_{n+1}) = ((a_1, \cdots, a_n), a_{n+1})$. □

注记 1.2.3. 推论 1.2.3 (2) 说明, 我们可将求多个整数的最大公因数问题**转化**为求两个整数的最大公因数.

例 1.2.4. 计算 $(234, 312, 585)$.

解. 注意到 $(234, 312) = 78$ 且 $(78, 585) = 39$, 故 $(234, 312, 585) = 39$. □

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 1.2.5. 求 $(105, 182)$, 并求一组 $x, y \in \mathbb{Z}$ 使得 $105x + 182y = (105, 182)$.

解. 注意到 $(105, 182) = (105, 77) = (28, 77) = 7 \times (4, 11) = 7$ 且 $7 = 7 \times 105 + (-4) \times 182$, 所以 $x = 7, y = -4$ 为一组满足条件的 x, y. □

例 1.2.6. 证明: $\forall\, n \in \mathbb{Z}_{>0}$, $\dfrac{21n+4}{14n+3}$ 为既约分数.

证明. 由于 $3(14n+3) - 2(21n+4) = 1$, 据 Bézout 定理知 $(21n+4, 14n+3) = 1$, 所以 $\dfrac{21n+4}{14n+3}$ 为既约分数. □

例 1.2.7. 设 $2 \nmid n$, 证明 $24 \mid n(n^2-1)$.

证明. 由 $3 \mid (n-1)n(n+1)$ 及**例 1.1.3** 的结论可得 $24 \mid n(n^2-1)$. □

例 1.2.8. 设 $a, b \in \mathbb{Z}_{>0}$, 证明 $17 \mid 2a + 3b$ 当且仅当 $17 \mid 9a + 5b$.

证明. 注意到 $(9a + 5b) + 4(2a + 3b) = 17(a + b)$, 故 $17 \mid 2a + 3b \Leftrightarrow 17 \mid 9a + 5b$. □

例 1.2.9. 设 $(a, b) = 1$, 证明 $(a + b, a^2 + ab + b^2) = 1$.

证明. 因 $(a, b) = 1$, 故 $(a+b, ab) = 1$. 又 $(a+b)^2 - (a^2+ab+b^2) = ab$, 故 $(a+b, a^2+ab+b^2) = (a + b, ab) = 1$. □

例 1.2.10. 设 $a, b, m, n \in \mathbb{Z}_{>0}$, $a \geqslant b$ 且 $(a, b) = 1$, 证明 $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

证明. 因为 $a^{(m,n)} - b^{(m,n)} \mid a^m - b^m$ 且 $a^{(m,n)} - b^{(m,n)} \mid a^n - b^n$, 故只需证明

$$(a^m - b^m, a^n - b^n) \mid a^{(m,n)} - b^{(m,n)}.$$

记 $c := (a^m - b^m, a^n - b^n)$, 则 $(b, c) = 1$ (否则会与 $(a, b) = 1$ 矛盾). 设 $d := (m, n)$, 据 Bézout 定理知, 存在 $u, v \in \mathbb{Z}_{\geqslant 0}$ 使得 $um - vn = (m, n) = d$ 由 $c \mid a^n - b^n$ 有 $c \mid a^{vn} - b^{vn}$, 进而得到 $c \mid a^d \cdot (a^{vn} - b^{vn}) = a^{um} - a^d \cdot b^{vn}$. 而由 $c \mid a^m - b^m$ 有 $c \mid a^{um} - b^{um}$, 相减得 $c \mid (a^d - b^d)b^{vn}$. 但 $(b, c) = 1$, 于是 $c \mid a^d - b^d$, 即 $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$. □

例 1.2.11. 设正整数数列 $\{a_n\}$ 严格递增, 证明: 存在项 a_s, a_t, 使得存在无穷多个 a_n 可表示为 $a_n = a_s x + a_t y$ $(x, y \in \mathbb{Z})$ 的形式.

证明. 对于 a_1 的每个正因子 d, 记 $S_d := \{a_n : (a_1, a_n) = d\}$. 因 a_1 只有有限多个正因子, 故必存在 $d_0 \mid a_1$ 使得 S_{d_0} 是无限集. 现取 $a_t \in S_{d_0}$, 由辗转相除法知存在 $x, y \in \mathbb{Z}$ 使得 $a_1 x + a_t y = d_0$. 因此, 对于 S_{d_0} 中的任一元素 a_n 都有 $a_n = d_0 \cdot \dfrac{a_n}{d} = a_1 \cdot \dfrac{x a_n}{d_0} + a_t \cdot \dfrac{y a_n}{d_0}$, 其中 $\dfrac{x a_n}{d_0}, \dfrac{y a_n}{d_0} \in \mathbb{Z}$. □

例 1.2.12. 设 $a > b > 0$, 证明在辗转相除法中有 $r_{k+2} \leqslant \dfrac{1}{2} r_k$ $(\forall\, k \geqslant 1)$, 进而可推出辗转相除法在运算步数不超过 $2\log_2 b + 1$ 后就会中止.

证明. 一方面, 如果 $r_{k+1} \leqslant \dfrac{1}{2} r_k$, 则有 $r_{k+2} < r_{k+1} \leqslant \dfrac{1}{2} r_k$; 另一方面, 如果 $r_{k+1} > \dfrac{1}{2} r_k$, 则由 $r_k = r_{k+1} q_{k+2} + r_{k+2}$ 知必有 $q_{k+2} = 1$, 从而 $r_{k+2} = r_k - r_{k+1} \leqslant \dfrac{1}{2} r_k$. 此外, 利用归纳可得 $r_{2k+1} \leqslant \dfrac{r_1}{2^k} < \dfrac{b}{2^k}$, 故当 $b < 2^k$ 时 r_{2k+1} 只能为 0, 即辗转相除法在运算不超过 $2\log_2 b + 1$ 次后就会中止. □

§1.3 最小公倍数

定义 1.3.1. 设 n 个整数 $a_1, \cdots, a_n$ 均不为 0, 称 $m \in \mathbb{Z}$ 是 $a_1, \cdots, a_n$ 的**公倍数**, 如果 $a_k \mid m$ $(m = 1, \cdots, n)$. 称这些正的公倍数中的最小者为 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

命题 1.3.1. 设整数 $a_1, \cdots, a_n$ 均不为 0, 则 $[a_1, \cdots, a_n] = [|a_1|, \cdots, |a_n|]$.

证明. 显然 $a_1, \cdots, a_n$ 的正公倍数的集合与 $|a_1|, \cdots, |a_n|$ 的正公倍数的集合相同. □

命题 1.3.2. m 为 $a_1, \cdots, a_n$ 的公倍数当且仅当 $[a_1, \cdots, a_n] \mid m$.

证明. 充分性显然, 下证必要性. 记 $m_0 := [a_1, \cdots, a_n]$, 据带余除法知存在 $q, r \in \mathbb{Z}$ 使得 $m = q m_0 + r$ (其中 $0 \leqslant r < m_0$). 因为对任意的 k 有 $a_k \mid m$ 及 $a_k \mid m_0$, 故 $a_k \mid r$, 即 r 是 $a_1, \cdots, a_n$ 的公倍数, 而由 m_0 的定义可知 $r = 0$, 因此 $m_0 \mid m$. □

推论 1.3.1. 设 $a_1, \cdots, a_n, a_{n+1}$ 均不为 0, 则 $[a_1, \cdots, a_{n+1}] = [[a_1, \cdots, a_n], a_{n+1}]$.

证明. 只需说明 $a_1, \cdots, a_{n+1}$ 的公倍数集合与 $[a_1, \cdots, a_n], a_{n+1}$ 的公倍数集合相等即可. 具体的证明过程可参考**推论 1.2.3 (2)** 的证明. □

下面给出一个重要的定理, 它提供了一种常用的计算最小公倍数的方法.

定理 1.3.1. 设 $a, b \in \mathbb{Z}_{>0}$, 则 $(a, b)[a, b] = ab$.

证明. 设 $d := (a, b)$, $a := da_0$, $b := db_0$ (其中 $(a_0, b_0) = 1$), 则 $ab/(a, b) = da_0 b_0$ 是 a 和 b 的一个公倍数. 同时, 据辗转相除法知存在 $x, y \in \mathbb{Z}$ 使得 $d = ax + by$, 因此对 a, b 的任一正公倍数 m 都有

$$\frac{m}{da_0 b_0} = \frac{md}{ab} = \frac{m}{ab}(ax + by) = \frac{m}{b} x + \frac{m}{a} y \in \mathbb{Z},$$

于是 $m \geqslant da_0 b_0$, 这说明 $[a, b] = da_0 b_0$, 因此 $(a, b)[a, b] = ab$. □

命题 1.3.3. $\forall a, b \in \mathbb{Z}$, $k \in \mathbb{Z}_{>0}$, 都有 $[ka, kb] = k\,[a, b]$.

证明. 据**定理 1.3.1** 及**命题 1.2.4 (1)** 可得 $[ka, kb] = \dfrac{k^2ab}{(ka, kb)} = \dfrac{k^2ab}{k(a, b)} = k\,[a, b]$. □

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 1.3.1. 设正整数 $a < b < c$ 满足 $(a, b, c) = 10$ 且 $[a, b, c] = 100$, 求 a, b, c.

解. 设 $a := 10a_0$, $b := 10b_0$, $c := 10c_0$ 且 $(a_0, b_0, c_0) = 1$, 则 $[a, b, c] = 10\,[a_0, b_0, c_0] = 100$, 即 $a_0b_0c_0 = 10$. 又因为 $a < b < c$, 即 $a_0 < b_0 < c_0$, 所以 $a_0 = 1$, $b_0 = 2$, $c_0 = 5$. 因此, $a = 10$, $b = 20$, $c = 50$. □

例 1.3.2. 试求满足 $[a, b] = 150$ 及 $a - 2b = 13$ 的全部正整数 a, b.

解. 设 $(a, b) := d$, $a := da_0$, $b := db_0$ 且 $(a_0, b_0) = 1$, 则有 $[a, b] = da_0b_0 = 150$ 且 $d(a_0 - 2b_0) = 13$, 即 $d \mid 13$ 且 $d \mid 150$, 故 $d = 1$, 即 $ab = 150$ 且 $a - 2b = 13$.

解方程 $\dfrac{150}{b} - 2b = 13$, 可得 $b = 6$ (舍负根), 从而 $a = 25$. □

例 1.3.3. 设 $a, b, c \in \mathbb{Z}_{>0}$, 证明: $(a, b, c)\,[a, b, c] = abc$ 当且仅当 $(a, b) = (b, c) = (c, a) = 1$.

证明. 充分性是显然的, 下证必要性. 因为

$$[a, b, c] = [[a, b], c] = \left[\frac{ab}{(a, b)}, c\right] = \frac{abc}{(a, b)(ab/(a, b), c)} = \frac{abc}{(ab, c(a, b))} = \frac{abc}{(ab, bc, ca)},$$

所以 $(a, b, c) = (ab, bc, ca)$. 设 $d := (a, b, c)$, 则 $(ab, bc, ca) = d^2$, 即 $d^2 - d = 0$. 又 $d \neq 0$, 故 $d = 1$, 即 $(a, b, c) = 1 = (ab, bc, ca) = (b(a, c), ca)$, 从而 $(a, b) = (b, c) = (c, a) = 1$. □

例 1.3.4. 设 $a, b \in \mathbb{Z}$ 且 $a, b \neq 0$, 证明 $(a, b) = (a + b, [a, b])$.

证明. 设 $(a, b) := d$, $a := da_0$, $b := db_0$ 且 $(a_0, b_0) = 1$, 则

$$(a + b, [a, b]) = (d(a_0 + b_0), da_0b_0) = d = (a, b).$$

这是因为 $(a_0, b_0) = 1 \Rightarrow (a_0 + b_0, a_0b_0) = 1$. □

§1.4 算术基本定理

定义 1.4.1. 对于一个大于 1 的整数, 称它为**素数** (或**质数**), 如果它的正因数只有 1 和它本身, 否则称之为**合数**. 一般地, 我们用记号 $\pi(x)$ 表示不超过 x 的素数个数.

命题 1.4.1. 设 $a \in \mathbb{Z}_{>1}$, 则 a 除 1 以外的最小正因数 q 是素数且 a 为合数时有 $q \leqslant \sqrt{a}$.

证明. 首先, 若 q 不是素数, 则必存在 q 的因子 r 满足 $1 < r < q$, 于是 $r \mid a$, 这与 q 的最小性矛盾. 其次, 若 a 是合数, 则 $\dfrac{a}{q}$ 也是 a 的大于 1 的因子, 故由 q 的最小性知 $q \leqslant \dfrac{a}{q}$, 即 $q \leqslant \sqrt{a}$. □

这一命题提供了一个检测素数的方法, 称为 **Eratothenes 筛法**.

定理 1.4.1. 存在无穷多个素数, 即 $\lim\limits_{x\to+\infty} \pi(x) = +\infty$.

证明. 由于 $\forall n \in \mathbb{Z}_{>0}$, $n! + 1$ 的素因子必大于 n, 故存在无穷多个素数. □

命题 1.4.2. 设 p 是素数, 则 $\forall a \in \mathbb{Z}$, 要么 $p \mid a$, 要么 $(p, a) = 1$.

证明. 因为 $(p, a) \mid p$ 且 p 为素数, 所以 $(p, a) = p$ 或 $(p, a) = 1$, 而前者也即 $p \mid a$. □

命题 1.4.3. 设 $p \mid a_1 \cdots a_n$, 则至少存在某个 $k \in [1, n] \cap \mathbb{Z}$, 使得 $p \mid a_k$.

证明. *反证法*. 若不然, 则由**命题 1.4.2** 知 $(p, a_k) = 1$ $(k = 1, \cdots, n)$, 进而由**推论 1.2.2** 知 $(p, a_1 \cdots a_n) = 1$, 这与假设矛盾. □

定理 1.4.2 (算术基本定理). 设 $a \in \mathbb{Z}_{>1}$, 则必有 $a = p_1 \cdots p_n$, 其中 p_k $(1 \leqslant k \leqslant n)$ 均为素数, 且在不计乘积次序的情况下上述表达式是唯一的.

证明. *存在性.* 利用第二数学归纳法. 当 $a = 2$ 时命题显然成立. 现设对 $a > 2$ 而言, 所有满足 $2 \leqslant k < a$ 的整数 k 均可表示为素数的乘积, 下证 a 也可以表示为素数的乘积. 事实上, 若 a 为素数, 则命题显然成立; 若 a 为合数, 则 $a = a_1 a_2$ (其中 $a_1, a_2 \in [2, a)$), 由归纳假设知 a_1, a_2 均可以表示为素数的乘积, 从而 a 也可以表示为素数的乘积.

唯一性. 不妨设 $p_1 \leqslant p_2 \leqslant \cdots \leqslant q_n$, 如果还有 $a = q_1 \cdots q_m$ (其中 $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m$ 且 q_k 均为素数), 下证 $m = n$ 且 $q_k = p_k$. 不失一般性, 设 $m \geqslant n$, 由于 $p_1 \mid q_1 \cdots q_m$, 故存在 q_j 使得 $p_1 \mid q_j$, 从而 $p_1 = q_j$. 类似地, 由 $q_1 \mid p_1 \cdots p_n$ 知存在 p_k 使得 $q_1 = p_k$. 于是, $p_k = q_1 \leqslant q_j = p_1 \leqslant p_k$, 这表明 $p_1 = q_1$, 从而 $p_2 \cdots p_n = q_2 \cdots q_m$, 类似可得 $p_2 = q_2, \cdots, p_n = q_n$ 以及必有 $m = n$. □

若在 a 的素数乘积表达式中把相同的素数合并为幂的形式, 即可得到以下结论.

命题 1.4.4. 任意大于 1 的整数 a 均可以被唯一地表示为 $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ 的形式 (其中 $p_1 < p_2 < \cdots < p_n$ 为素数且 $\alpha_k > 0$, $1 \leqslant k \leqslant n$), 这称为 a 的**标准分解式**.

注记 1.4.1. 有时为方便计, 我们会在这一表达式中添加若干素数的 0 次幂.

命题 1.4.5. 设 $a \in \mathbb{Z}_{>1}$ 且具有标准分解式 $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, 则 d 为 a 的正因数当且仅当

$$d = p_1^{\beta_1} \cdots p_n^{\beta_n} \qquad \text{且} \quad 0 \leqslant \beta_k \leqslant \alpha_k \ (1 \leqslant k \leqslant n).$$

证明. 充分性是显然的, 下证必要性. 由于 d 为 a 的正因数, 所以 d 的素因子必是 a 的素因子, 从而可以写成 $d = p_1^{\beta_1} \cdots p_n^{\beta_n}$ 且 $0 \leqslant \beta_k \leqslant \alpha_k \, (1 \leqslant k \leqslant n)$ 的形式. 此外, 对任意的 k, 由 $d \mid a$ 知 $p_k^{\beta_k} \mid a$, 并且由素数 p_k 两两不同可知 $\left(p_k^{\beta_k}, \dfrac{a}{p_k^{\alpha_k}}\right) = 1$, 于是据命题 1.2.3 (2) 可得 $p_k^{\beta_k} \mid p_k^{\alpha_k}$, 从而 $\beta_k \leqslant \alpha_k$. □

命题 1.4.6. 设 $a, b \in \mathbb{Z}_{>0}$ 且分别有分解式

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad b = p_1^{\beta_1} \cdots p_n^{\beta_n} \ (\alpha_k, \beta_k \geqslant 0),$$

那么

$$(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n}, \qquad [a, b] = p_1^{\delta_1} \cdots p_n^{\delta_n},$$

其中 $\gamma_k := \min(\alpha_k, \beta_k)$, $\delta_k := \max(\alpha_k, \beta_k)$. 这一命题也是算术基本定理的一个推论. □

定义 1.4.2. 设 $a \in \mathbb{Z}_{>0}$, 称 a 是一个**无平方因子数**, 如果 a 不能被素数的平方整除.

容易知道 a 是无平方因子数当且仅当 $a = 1$ 或 $a \geqslant 2$ 且 a 的标准分解式中所有 α_k 均为 1.

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 1.4.1. 证明: $\forall\, n \in \mathbb{N}^*$, 存在连续的 n 个整数, 它们全是合数.

证明. 考虑连续的 n 个整数 $(n+1)! + 2, \cdots, (n+1)! + (n+1)$, 显然它们都是合数. □

例 1.4.2. 证明: 若 $2^n + 1$ 为素数, 则 n 必为 2 的幂.

证明. 反设 $n = pk$, 其中 p 为奇数, 则

$$2^n + 1 = 2^{pk} + 1 = (2^k + 1)(2^{k(p-1)} - 2^{k(p-2)} + \cdots - 2^k + 1),$$

而 $2^k + 1 > 2 + 1 = 3$ 且 $2^{k(p-1)} - 2^{k(p-2)} + \cdots - 2^k + 1 > 1$, 这表明 $2^n + 1$ 为合数, 矛盾! 故 n 必为 2 的幂. □

例 1.4.3 (Goldbach)**.** 设 $n \geqslant 1$, $f(x) := \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ 且 $a_n > 0$, 证明存在无穷多个 $m \in \mathbb{Z}$ 使得 $f(m)$ 是合数.

证明. 若 $|a_n| \neq 1$, 结论显然成立, 这是因为如果 m 是 a_0 的任何倍数, 则必有 $a_0 \mid f(m)$. 其实, 这无限多个 $f(m)$ 是 a_0 的倍数且 $|f(m)| \neq a_0$, 因为 $f(m)$ 只能有限多次取到 $\pm a_0$. 若 $|a_n| = 1$, 注意到 $n \geqslant 1$, 则必存在 $k \in \mathbb{Z}$ 使得 $|f(k)| \neq 1$. 设 p 为 $f(k)$ 的任意素因数, 则 $p \mid f(k+rp) - f(k)$ $(r \in \mathbb{Z})$. 而满足 $f(k+rp) = \pm p$ 的 $r \in \mathbb{Z}$ 一定只有有限多个, 故存在无限多个 r 使得 $p \mid f(k+rp)$. 这样, 我们便证明了这一结论. □

例 1.4.4. 证明 $(a,b,c)(ab,bc,ca) = (a,b)(b,c)(c,a)$.

证明. 将 a,b,c 表示为标准分解式即可验证. □

例 1.4.5. 设 $(a,b) = (c,d) = 1$, 证明 $(ac,bd) = (a,d)(b,c)$.

证明. 将 a,b,c,d 表示为标准分解式即可验证. □

例 1.4.6. 设 $n,k \in \mathbb{Z}_{>0}$ 且 $k \geqslant 2$. 证明 n 可以被唯一地表示为 $n = ab^k$ 的形式, 其中 $a,b \in \mathbb{Z}_{>0}$ 且 a 不被任一素数的 k 次幂整除. 特别地, n 可唯一地表示成 $n = ab^2$ 的形式, 其中 $a,b \in \mathbb{Z}_{>0}$ 且 a 为无平方因子数.

证明. 存在性. 不妨设 $n \geqslant 2$, 且其标准分解式为 $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. 由带余除法知存在 $q_j, r_j \in \mathbb{Z}$ $(1 \leqslant j \leqslant m)$ 使得 $\alpha_j = q_j k + r_j$ 且 $0 \leqslant r_j < k$. 于是, 我们若记 $a = p_1^{r_1} \cdots p_m^{r_m}$, $b = p_1^{q_1} \cdots p_m^{q_m}$, 则 $n = ab^k$ 且 a 不被任意素数的 k 次幂整除.

唯一性. 若还存在正整数 a', b' 使得 $n = a'b'^k$ 且 a' 不被任意素数的 k 次幂整除, 则 $ab^k = a'b'^k$. 首先来证明 $b \mid b'$. 事实上, 若 $b \nmid b'$, 则必存在素数 p 以及 $\beta \in \mathbb{Z}_{>0}$ 使得 $p^\beta \mid b$ 且 $p^\beta \nmid b'$, 于是必存在非负整数 $\gamma < \beta$ 使得 $v_p(b') = \gamma$. 在等式 $ab^k = a'b'^k$ 两侧同时约去 $\beta^{k\gamma}$ 并模 p^k 即可推出矛盾, 因此 $b \mid b'$, 同理有 $b' \mid b$, 所以 $b = b'$, 进而有 $a = a'$. □

例 1.4.7. 设 $n \in \mathbb{Z}_{\geqslant 2}$, 利用例 1.4.6 的结论证明 $\pi(n) \geqslant \dfrac{1}{2}\log_2 n$.

证明. 由于区间 $[1,n]$ 中的每个整数 m 均为唯一地表示为 $m = ab^2$ 的形式, 其中 $b \leqslant \sqrt{n}$ 且 a 为无平方因子数. 因为不超过 n 的素数一共有 $\pi(n)$ 个, 所以恰好为 k 个不超过 n 的素数乘积的数共有 $\dbinom{\pi(n)}{k}$ 个, 进而对 $k = 0, \cdots, \pi(n)$ 求和可知 a 的可能取值的个数不超过 $2^{\pi(n)}$, 于是 $n \leqslant 2^{\pi(n)} \cdot \sqrt{n}$, 从而 $\pi(n) \geqslant \dfrac{1}{2}\log_2 n$. □

例 1.4.8. 设 d 是一个无平方因子数且 $d \mid mn$, 证明 $d = \dfrac{(d,m)(d,n)}{(d,m,n)}$.

证明. 只需对 $d = p$ 为素数, $m = p^\alpha$, $n = p^\beta$ 且 $\alpha + \beta \geqslant 1$ 的情形来证明结论即可, 即证 $p = p^{\min(1,\alpha)+\min(1,\beta)-\min(1,\alpha,\beta)}$. 若 $\alpha = 0$, 则 $\beta \geqslant 1$ 则该式显然成立; 若 $\alpha \geqslant 1$, 则 $\min(1,\alpha,\beta) = \min(1,\beta)$, 从而该式成立. 综上, 我们便证明了这一结论. □

例 1.4.9 (Richert)**.** 设 $x \geqslant 2$, $r \in \mathbb{Z}_{\geqslant 2}$, $1 < u < r < v$. 又设无平方因子数 $n \leqslant x$ 且 n 的素因子均不小于 $x^{1/v}$. 记

$$\rho(n) := 1 - \frac{1}{r-u} \sum_{\substack{x^{1/v} < p \leqslant x^{1/u} \\ p \mid n}} \left(1 - \frac{u \log p}{\log x}\right),$$

证明: 如果 $\rho(n) > 0$, 则 n 至多有 $r-1$ 个素因子.

证明. 记 $\Omega(n)$ 表示 n 的素因子个数, 则

$$\begin{aligned} 0 < \rho(n)(r-u) &= r - u - \sum_{\substack{x^{1/v} < p \leqslant x^{1/u} \\ p \mid n}} \left(1 - \frac{u \log p}{\log x}\right) \\ &\leqslant r - u - \sum_{p \mid n} \left(1 - \frac{u \log p}{\log x}\right) = r - u - \Omega(n) + u \frac{\log n}{\log x} \leqslant r - \Omega(n), \end{aligned}$$

因此, $\Omega(n) < r$, 即 n 至多有 $r-1$ 个素因子. □

例 1.4.10 (陈景润)**.** 设 $x \geqslant 2$, 又设无平方因子数 $n \leqslant x$ 且 n 的素因子均不小于 $x^{1/10}$. 记

$$\rho(n) := 1 - \frac{1}{2} \sum_{\substack{x^{1/10} \leqslant p < x^{1/3} \\ p \mid n}} 1 - \frac{1}{2} \sum_{\substack{p_1 p_2 p_3 = n \\ x^{1/10} \leqslant p_1 < x^{1/3} \leqslant p_2 < (x/p_1)^{1/2}}} 1,$$

这里的求和变量均为素数, 证明: 如果 $\rho(n) > 0$, 则 n 至多有 2 个素因子.

证明. 为记号方便, 我们记

$$\rho_1(n) := \sum_{\substack{x^{1/10} \leqslant p < x^{1/3} \\ p \mid n}} 1, \qquad \rho_2(n) := \sum_{\substack{p_1 p_2 p_3 = n \\ x^{1/10} \leqslant p_1 < x^{1/3} \leqslant p_2 < (x/p_1)^{1/2}}} 1,$$

则

$$\rho(n) = 1 - \frac{1}{2}\rho_1(n) - \frac{1}{2}\rho_2(n).$$

反设 n 至少有 3 个素因子, 则 n 必有在 $\left[x^{1/10}, x^{1/3}\right)$ 中的素因子, 从而 $\rho_1(n) \geqslant 1$, 再由 $\rho(n) > 0$ 知 $\rho_1(n) = 1$, 这意味着 n 有一个位于 $\left[x^{1/10}, x^{1/3}\right)$ 中的素因子且其余素因子均不小于 $x^{1/3}$, 故 n 恰有 3 个素因子. 记 $n := p_1 p_2 p_3$, 其中 $p_1 < p_2 < p_3$, 则

$$x^{1/10} \leqslant p_1 < x^{1/3} \leqslant p_2 < p_3, \qquad p_2^2 < \frac{n}{p_1} \leqslant \frac{x}{p_1},$$

故 $\rho_2(n) \geqslant 1$, 但这会导致 $\rho(n) \leqslant 0$, 从而与假设矛盾.

这样, 我们便证明了这一结论. □

类似地, 我们还可以证明如下结论.

例 1.4.11. 设 $\mathscr{A} \subset \mathbb{N}^*$ 是无限集, $\rho(n)$ 如上题所定义. 若对充分大的 x 均有

$$\sum_{\substack{x/2<n\leqslant x\\ p|n\Rightarrow p\geqslant x^{1/10}}} \mu^2(n)\rho(n) > 0$$

(其中 $\mu(n)$ 为 Möbius 函数), 则集合 $\mathscr{A}$ 中存在无穷多个元素, 其至多有 2 个素因子.

§1.5 取整函数

定义 1.5.1. 设 $x \in \mathbb{R}$, 用 $\lfloor x \rfloor$ 表示不超过 x 的最大整数, 并称之为 x 的**整数部分**; 称 $\{x\} := x - \lfloor x \rfloor$ 为 x 的**小数部分**. 函数 $\lfloor x \rfloor$ 也被称作 **(向下) 取整函数**. ‡

我们指出, 一部分书籍和文献中也会用 $[x]$ 表示这一函数. 下面给出一些取整函数的基本性质.

命题 1.5.1. 设 $x, y \in \mathbb{R}$, 则

(1) $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1, \quad 0 \leqslant \{x\} < 1;$

(2) $\forall\, m \in \mathbb{Z}$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m;$

(3) $x \leqslant y \;\Rightarrow\; \lfloor x \rfloor \leqslant \lfloor y \rfloor;$

(4) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor \leqslant \lfloor x \rfloor + \lfloor y \rfloor + 1;$

(5) $\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor, & x \in \mathbb{Z}, \\ -\lfloor x \rfloor - 1, & x \notin \mathbb{Z}; \end{cases} \qquad \{-x\} = \begin{cases} -\{x\} = 0, & x \in \mathbb{Z}, \\ 1 - \{x\}, & x \notin \mathbb{Z}; \end{cases}$

(6) $\forall\, m \in \mathbb{Z}_{>0}$, $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \dfrac{x}{m} \right\rfloor;$

(7) (**带余除法**) $\forall\, a, b \in \mathbb{Z}$, $b > 0$, 有 $a = b \left\lfloor \dfrac{a}{b} \right\rfloor + b \left\{ \dfrac{a}{b} \right\};$

(8) 设 $a \in \mathbb{Z}_{>0}$, $x > 1$, 则区间 $[1, x]$ 中被 a 整除的正整数个数为 $\left\lfloor \dfrac{x}{a} \right\rfloor$.

这些结论的证明利用定义即可完成, 这里不再赘述. □

定义 1.5.2. 设 $a, b \in \mathbb{Z}$, $a > 1$ 且 $b \neq 0$. 若 $a^k \mid b$ 且 $a^{k+1} \nmid b$, 则称 a^k **恰好整除** b, 记作 $a^k \parallel b$. 若素数 p 满足 $p^k \parallel b$, 则称 k 为 b 的 p **进指数赋值**, 记作 $v_p(b)$.

特别地, 为方便起见, 我们约定 $v_p(0) = \infty$.

由算术基本定理知, 对任意的 $a \in \mathbb{Z}_{>0}$ 都有 $a = \prod\limits_p p^{v_p(a)}$, 其中 p 通过全体素数.

‡对应地, 对 $x \in \mathbb{R}$ 也有**向上取整函数** $\lceil x \rceil$.

命题 1.5.2. 设 p 为素数, $a,b\in\mathbb{Z}$, 则

(1) $v_p(ab)=v_p(a)+v_p(b)$; (2) $v_p(a+b)\geqslant\min(v_p(a),v_p(b))$.

证明. 不妨设 a,b 与 $a+b$ 均不为 0, 并记 $a=p^ka_0$, $b=p^\ell b_0$ (其中 $p\nmid a_0b_0$). 因此 $v_p(a)=k$ 且 $v_p(b)=\ell$.

(1) 由 $ab=p^{k+\ell}a_0b_0$ 知 $v_p(ab)=v_p(a)+v_p(b)$;

(2) 不妨设 $k\leqslant\ell$, 由 $a+b=p^k(a_0+p^{\ell-k}b_0)$ 知 $v_p(a+b)\geqslant k=\min(v_p(a),v_p(b))$. □

定理 1.5.1. 设 $n\in\mathbb{Z}_{>0}$, p 为素数, 则 $v_p(n!)=\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor$.

证明. 由**命题 1.5.2 (1)** 可得 $v_p(n!)=\displaystyle\sum_{m\leqslant n}v_p(m)=\sum_{m\leqslant n}\sum_{1\leqslant k\leqslant v_p(m)}1=\sum_{k\geqslant1}\sum_{\substack{m\leqslant n\\ v_p(m)\geqslant k}}1$, 而此式右侧的内层和表示不超过 n 且被 p^k 整除的正整数个数, 而由**命题 1.5.1 (8)** 可知这等于 $\left\lfloor\dfrac{n}{p^k}\right\rfloor$, 这便证明了结论. □

结合前面便可得到 $n!$ 的标准分解式:

$$n!=\prod_{p\leqslant n}p^{\sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor}\ (\text{其中 } p \text{ 为素数}).$$

推论 1.5.1. 若 $p_1<p_2$, 则 $v_{p_1}(n!)\geqslant v_{p_2}(n!)$.

例 1.5.1. 计算 30! 的十进制表示末尾 0 的个数.

解. 因 2 与 5 相乘在末尾产生 1 个 0 且 $v_2(30!)\geqslant v_5(30!)=7$, 故 30! 末尾有 7 个 0. □

例 1.5.2. 设 $a_j\geqslant0$ $(1\leqslant j\leqslant k)$ 且 $n:=a_1+\cdots+a_k$, 证明 $\dfrac{n!}{a_1!\cdots a_k!}\in\mathbb{Z}$.

证明. 不妨设 $a_j>0$ $(\forall\, j)$, 只需证明对任意的素数 p 都有

$$v_p(n!)\geqslant v_p(a_1!)+\cdots+v_p(a_k!).$$

而这可以由**定理 1.5.1** 及 $\left\lfloor\dfrac{n}{p_j}\right\rfloor\geqslant\left\lfloor\dfrac{a_1}{p^j}\right\rfloor+\cdots+\left\lfloor\dfrac{a_k}{p^j}\right\rfloor$ (参见**命题 1.5.1 (4)**) 得到. □

例 1.5.3. 设 $m,n\in\mathbb{Z}_{>0}$, 证明 $n!(m!)^n\mid(mn)!$.

证明. 据**定理 1.5.1**, 只需证明对任意的素数 p 都有 $\displaystyle\sum_j\left\lfloor\frac{mn}{p^j}\right\rfloor\geqslant n\sum_j\left\lfloor\frac{m}{p^j}\right\rfloor+\sum_j\left\lfloor\frac{n}{p^j}\right\rfloor$.

设 $m=p^\ell c$ 且 $p\nmid c$. 当 $j\leqslant\ell$ 时, 由于 $p^j\mid m$, 故 $\left\lfloor\dfrac{mn}{p^j}\right\rfloor=n\left\lfloor\dfrac{m}{p^j}\right\rfloor$, 从而

$$\sum_{j\leqslant\ell}\left\lfloor\frac{mn}{p^j}\right\rfloor=n\sum_{j\leqslant\ell}\left\lfloor\frac{m}{p^j}\right\rfloor.$$

当 $j>\ell$ 时, 记 $m=qp^j+r$ (其中 $0<r\leqslant p^j-1$), 则

$$\left\lfloor\frac{mn}{p^j}\right\rfloor=\left\lfloor\frac{(qp^j+r)}{q^j}\right\rfloor=nq+\left\lfloor\frac{nr}{q^j}\right\rfloor=n\left\lfloor\frac{m}{p^j}\right\rfloor+\left\lfloor\frac{nr}{q^j}\right\rfloor,$$

其中 $\dfrac{r}{p^j}=\left\{\dfrac{m}{p^j}\right\}=\left\{\dfrac{c}{p^{j-\ell}}\right\}\geqslant\dfrac{1}{p^{j-\ell}}$, 从而对任何 $j>\ell$ 都有 $\left\lfloor\dfrac{mn}{p^j}\right\rfloor\geqslant n\left\lfloor\dfrac{m}{p^j}\right\rfloor+\left\lfloor\dfrac{n}{p^{j-\ell}}\right\rfloor$. 于是,

$$\sum_{j>\ell}\left\lfloor\frac{mn}{p^j}\right\rfloor\geqslant n\sum_{j>\ell}\left\lfloor\frac{m}{p^j}\right\rfloor+\sum_{j>\ell}\left\lfloor\frac{n}{p^{j-\ell}}\right\rfloor=n\sum_{j>\ell}\left\lfloor\frac{m}{p^j}\right\rfloor+\sum_{j\geqslant1}\left\lfloor\frac{n}{p^j}\right\rfloor.$$

这样, 我们便证明了这一结论. □

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 1.5.4. 设 $n\in\mathbb{Z}^*$, $a\in\mathbb{R}$, 证明 $\displaystyle\sum_{k=0}^{n-1}\left\lfloor a+\frac{k}{n}\right\rfloor=\lfloor na\rfloor$.

证明. 不难知道存在 $m\in[0,n-1]\cap\mathbb{Z}$, 使得 $m\leqslant n\{a\}<m+1$, 即 $\dfrac{m}{n}\leqslant\{a\}<\dfrac{m+1}{n}$, 这是由于 $0\leqslant\{a\}<1$, 从而,

$$\begin{aligned}\sum_{k=0}^{n-1}\left\lfloor a+\frac{k}{n}\right\rfloor=\lfloor na\rfloor&=\sum_{k=0}^{n-m-1}\left\lfloor a+\frac{k}{n}\right\rfloor+\sum_{k=n-m}^{n-1}\left\lfloor a+\frac{k}{n}\right\rfloor\\&=(n-m)\lfloor a\rfloor+m(\lfloor a\rfloor+1)=n\lfloor a\rfloor+m,\end{aligned}$$

而 $\lfloor na\rfloor=n\lfloor a\rfloor+n\{a\}=n\lfloor a\rfloor+m$, 所以 $\displaystyle\sum_{k=0}^{n-1}\left\lfloor a+\frac{k}{n}\right\rfloor=\lfloor na\rfloor$. □

例 1.5.5. 设 p 是一个素数, 在 $\mathbb{Q}$ 上定义函数 v_p 为

$$v_p\left(\frac{a}{b}\right)=v_p(a)-v_p(b),\qquad\forall\,a,b\in\mathbb{Z},\ \ b\neq0.$$

(1) 试说明上述定义的合理性;

(2) 证明: $\forall\,x,y\in\mathbb{Q}$ 都有 $v_p(x+y)\geqslant\min(v_p(x),v_p(y))$.

证明. (1) 验证 v_p 对每个 $x\in\mathbb{Q}$ 有定义且右唯一. (2) 类似**命题 1.5.2 (2)** 证明即可. □

例 1.5.6. 设 $n=p^rm$, 其中 p 为素数, $r>1$ 且 $p\nmid m$. 证明 $p\nmid\dbinom{n}{p^r}$.

证明. 这是因为

$$\begin{aligned}v_p\left(\binom{n}{p^r}\right)&=v_p(n!)-v_p(p^r!)-v_p((n-p^r)!)\\&=\sum_{j=1}^{\infty}\left\lfloor\frac{p^rm}{p^j}\right\rfloor-\sum_{j=1}^{\infty}\left\lfloor\frac{p^r}{p^j}\right\rfloor-\sum_{j=1}^{\infty}\left\lfloor\frac{p^r(m-1)}{p^j}\right\rfloor\\&=\sum_{j>r}\left\lfloor\frac{m}{p^{j-r}}\right\rfloor-\sum_{j>r}\left\lfloor\frac{m-1}{p^{j-r}}\right\rfloor=0,\end{aligned}$$

其中最后一步用到了 $p\nmid m$. 这样, 我们便证明了这一结论. □

例 1.5.7. 设 $n \in \mathbb{Z}_{>0}$, 证明: 在 $(\sqrt{5}+\sqrt{6})^{2n}$ 的十进制表示中小数点后前 n 位数字相同.

证明. 考察数列 $a_n := (\sqrt{6}+\sqrt{5})^{2n} + (\sqrt{6}-\sqrt{5})^{2n} = (11+2\sqrt{30})^n + (11-2\sqrt{30})^n$, 则有 $a_n = 22a_{n-1} - a_{n-2}$ $(\forall\, n \in \mathbb{Z}_{\geqslant 3})$ 且 $a_1 = 22$, $a_2 = 482$, 于是归纳可得 $\forall\, n \in \mathbb{Z}_{>0}$, $a_n \in \mathbb{Z}_{>0}$. 同时, 注意到

$$(\sqrt{6}-\sqrt{5})^{2n} = \frac{1}{(\sqrt{6}+\sqrt{5})^{2n}} = \frac{1}{(11+2\sqrt{30})^n} < \frac{1}{10^n},$$

故 $(\sqrt{6}-\sqrt{5})^{2n}$ 小数点后前 n 位均为 0, 从而 $(\sqrt{5}+\sqrt{6})^{2n}$ 小数点后前 n 位数均为 9. □

类似地, 利用这种方法, 我们还可以证明下述结论.

例 1.5.8 (第六届美国 Putnam 数学竞赛)**.** 设 $n \in \mathbb{Z}_{>0}$, 证明 $2^{n+1} \parallel \lfloor (1+\sqrt{3})^{2n+1} \rfloor$. □

第二章　不定方程

不定方程是指未知数个数大于 1 且未知数只取整数值的方程, 也称为 Diophantus (丢番图) 方程. 我们主要讨论两类简单的不定方程.

§2.1　一次不定方程

首先讨论较基础的二元一次不定方程.

命题 2.1.1. 设 $a,b,c\in\mathbb{Z}$ 且 a,b 不全为 0, 则方程

$$ax+by=c \tag{2.1}$$

有解的充要条件是 $(a,b)\mid c$. 当其有解时, 其全部解为

$$\begin{cases} x=x_0+\dfrac{b}{(a,b)}k, \\ y=y_0-\dfrac{a}{(a,b)}k, \end{cases}\quad (k\in\mathbb{Z}), \tag{2.2}$$

其中 x_0,y_0 是一组特解.

证明. 记 $d:=(a,b)$. 若 (2.1) 有解, 则由 $d\mid a$ 且 $d\mid b$ 知 $d\mid c$. 同时, 据辗转相除法可知存在 $m,n\in\mathbb{Z}$ 使得 $d=am+bn$, 若 $d\mid c$ 则 $c=\dfrac{c}{d}\cdot d=\dfrac{c}{d}(am+bn)$, 从而 (2.1) 有解.

设 x_0,y_0 是一组特解, 则 $ax_0+by_0=c$. 一方面, 不难验证 (2.2) 是 (2.1) 的解; 另一方面, 对 (2.1) 的任意一组解 x,y 而言, 由 $ax+by=ax_0+by_0=c$ 知 $a(x-x_0)=b(y_0-y)$, 即 $\dfrac{a}{d}(x-x_0)=\dfrac{b}{d}(y_0-y)$. 注意到 $\left(\dfrac{a}{d},\dfrac{b}{d}\right)=1$, 故必有 $\dfrac{a}{d}\mid y_0-y$ 且 $\dfrac{b}{d}\mid x-x_0$, 因此原方程的任意一组解 x,y 必然具有形式 (2.2). 即 (2.2) 是 (2.1) 的全部解. □

例 2.1.1. 求 $7x+4y=65$ 的全部解.

解. 注意到 $7\cdot(-1)+4\cdot 2=(7,4)=1$, 故 $x_0=-65$, $y_0=130$ 是一组特解, 从而原方程的全部解为 $\begin{cases} x=-65+4k, \\ y=130-7k, \end{cases}\ (k\in\mathbb{Z})$. □

注记 2.1.1. 其实也可以用瞪眼法得到 $7\cdot 7+4\cdot 4=65$, 从而得到原不定方程的全部解.

对于含有更多未知量的一次不定方程, 我们可以利用定理 1.2.3 得到下述结论.

推论 2.1.1. 设 $a_1, \cdots, a_n$ 及 N 均为整数, a_k $(1 \leqslant k \leqslant n)$ 不全为 0, 则方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$$

有解的充要条件是 $(a_1, \cdots, a_n) \mid N$.

例 2.1.2. 设 a, b 是两个互素的正整数, N 是一个充分大的正整数. 证明: 不定方程 $ax + by = N$ 的正整数解的个数等于 $(ab)^{-1}N + O(1)$, 其中 O 常数仅与 a, b 有关.

证明. 由 (2.2) 及 $(a, b) = 1$ 可得 $\begin{cases} x = x_0 + bk, \\ y = y_0 - ak, \end{cases}$ (其中 $k \in \mathbb{Z}$, (x_0, y_0) 为原方程的一组特解), 则 $x, y \in \mathbb{Z}_{>0}$ 时有 $-\dfrac{y_0}{a} < k < \dfrac{x_0}{b}$, 故原方程组正整数解的个数为

$$\left\lfloor \frac{x_0}{b} - \left(-\frac{y_0}{a}\right) \right\rfloor + O(1) = \left\lfloor \frac{ax_0 + by_0}{ab} \right\rfloor + O(1) = \left\lfloor \frac{N}{ab} \right\rfloor + O(1),$$

其中常数 $O(1)$ 取决于 a, b, x_0, y_0, 可能的取值为 $0, \pm 1$. □

例 2.1.3. 设 a, b, c, N 是四个给定的整数且 $(a, b, c) = 1$, 证明: 不定方程 $ax + by + cz = N$ 的全部解为

$$\begin{cases} x = x_0 + cqk + \dfrac{b}{d}\ell, \\ y = y_0 + crk - \dfrac{a}{d}\ell, \\ z = z_0 - dk, \end{cases} \quad (k, \ell \in \mathbb{Z})$$

其中 x_0, y_0, z_0 是方程的一组特解, $d := (a, b)$ 且 q, r 是满足 $aq + br = d$ 的一组整数. □

§2.2 勾股方程

本节的目的是给出不定方程

$$x^2 + y^2 = z^2 \tag{2.3}$$

的全部解. 在证明主要结论前, 我们先介绍一个引理.

引理 2.2.1. 不定方程

$$uv = w^2, \qquad u, v, w \in \mathbb{Z}_{>0},\ (u, v) = 1 \tag{2.4}$$

的全部解为

$$u = a^2,\ \ v = b^2,\ \ w = ab, \tag{2.5}$$

其中 $a, b \in \mathbb{Z}_{>0}$ 且 $(a, b) = 1$.

证明. (2.5) 显然是 (2.4) 的解, 下证 (2.4) 的解均形如 (2.5). 不妨设 $u>1$, $v>1$, 且 u,v 的标准分解式分别为 $u=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $v=q_1^{\beta_1}\cdots q_\ell^{\beta_\ell}$. 由 $(u,v)=1$ 知 $p_i\neq q_j$ $(\forall\, i,j)$, 于是 $w^2=uv=p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_\ell^{\beta_\ell}$ 为 w^2 的标准分解式, 故任何 α_i,β_j 均为偶数, 从而 u,v 均为完全平方数. □

下面来讨论 (2.3) 的解. 首先对问题作一些简化处理. 如果记 $d:=(x,y)$, 则 $d^2\mid z^2$, 从而 $d\mid z$, 此时可在方程 (2.3) 两侧同时除以 d^2 化简, 因此我们不妨设 $(x,y)=1$. 此外, 又因为 x 与 y 必然为一个奇数和一个偶数, 故不妨设 $2\mid x$.

定理 2.2.1. 不定方程 (2.3) 的适合条件 $x,y,z\in\mathbb{Z}_{>0}$, $(x,y)=1$ 且 $2\mid x$ 的全部解为

$$x=2ab,\ \ y=a^2-b^2,\ \ z=a^2+b^2, \tag{2.6}$$

其中 $a>b>0$, $(a,b)=1$ 且 a,b 一奇一偶.

证明. 首先证明 (2.7) 是满足条件的 (2.3) 的解, 只需验证 $(x,y)=1$. 实际上, 若记 $d:=(x,y)$, 则由 $x^2+y^2=z^2$ 知 $d^2\mid z^2$ 从而 $d\mid z$. 于是由 $d\mid y\pm z$ 可得 $d\mid 2a^2$ 且 $d\mid 2b^2$. 注意到 $(a,b)=1$ 且 a,b 一奇一偶, 故必有 $d=1$.

其次证明满足条件及 (2.6) 的解均可以写成 (2.7) 的形式. 设 x,y,z 是这样的一组解, 则由 $2\mid x$ 与 $(x,y)=1$ 知 $2\nmid yz$ 且 $(y,z)=1$, 于是

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2},\qquad \left(\frac{z+y}{2},\frac{z-y}{2}\right)=1,$$

这是因为若正整数 $d\mid\left(\dfrac{z+y}{2},\dfrac{z-y}{2}\right)$ 则必有 $d\mid y$ 且 $d\mid z$, 即 $d\mid(y,z)$, 从而 $d=1$.

据**引理 2.2.1** 可知, 存在 $a,b\in\mathbb{Z}$ 使得

$$\frac{z+y}{2}=a^2,\qquad \frac{z-y}{2}=b^2,\qquad \frac{x}{2}=ab,$$

其中 $a>0$, $b>0$ 且 $(a,b)=1$, 由此便得 $x=2ab$, $y=a^2-b^2$, $z=a^2+b^2$. 此外, 由 $2\nmid y$ 知 a,b 一奇一偶. 这样, 我们便证明了这一结论. □

下面来介绍上述定理的一个应用.

命题 2.2.1. 方程 $x^4+y^4=z^2$ 没有正整数解.

证明 (Fermat). 反设 $x^4+y^4=z^2$ 有整数解, 现选取该方程的一组解 x_0,y_0,z_0 并假设 z_0 是所有正整数解的 z 值中最小的一个, 那么必有 $(x_0,y_0)=1$, 否则便有 $(x_0,y_0)>1$, $(x_0,y_0)^2\mid z_0$ 以及

$$\left(\frac{x_0}{(x_0,y_0)}\right)^4+\left(\frac{y_0}{(x_0,y_0)}\right)^4=\left(\frac{z_0}{(x_0,y_0)^2}\right)^2,$$

这与 z_0 的最小性矛盾.

由**定理 2.2.1** 知 x_0^2, y_0^2 一奇一偶, 不妨设 x_0^2 是偶数, 于是

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

其中 $a > b > 0$, $(a, b) = 1$ 且 a, b 一奇一偶. 注意到 y_0 是奇数, 故 y_0^2 除以 4 余 1, 因此必有 $2 \nmid a$ 且 $2 \mid b$. □

注记 2.2.1. 上述证明用到的这一方法也称为**无穷递降法**.

推论 2.2.1 (Fermat)**.** 方程 $x^4 + y^4 = z^4$ 没有满足 $xyz \neq 0$ 的解.

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 2.2.1. 设 $n \in \mathbb{Z}_{>0}$, 证明 n 可表为两个整数平方和的充要条件是 $2n$ 可表为两个整数平方和.

证明. 必要性. 若 $n = x^2 + y^2$ $(x, y \in \mathbb{Z})$, 则 $2n = 2(x^2 + y^2) = (x + y)^2 + (x - y)^2$, 即该结论显然成立.

充分性. 若 $2n = u^2 + v^2$ $(u, v \in \mathbb{Z})$, 则 $n = \dfrac{u^2 + v^2}{2} = \left(\dfrac{u + v}{2}\right)^2 + \left(\dfrac{u - v}{2}\right)^2$. 注意到 $2 \mid u^2 + v^2$, 则 u, v 同为奇数或偶数, 从而 $\dfrac{u + v}{2}, \dfrac{u - v}{2} \in \mathbb{Z}$.

这样, 我们便证明了这一结论. □

例 2.2.2. 求不定方程 $y^2 = x^3 - x$ 的全部整数解.

证明. 注意到 $y^2 = x(x^2 - 1) \geqslant 0$, 即 $-1 \leqslant x \leqslant 0$ 或 $x \geqslant 1$, 所以只需考虑 $x = -1, 0$ 以及 $x \geqslant 1$ 时原不定方程的解. 显然 $(x, y) = (0, 0), (\pm 1, 0)$ 是原方程的 3 组解, 下面考虑 $x > 1$ 的情形. 注意到 (x_0, y_0) 是原方程的一组解当且仅当 $(x_0, -y_0)$ 是原方程的一组解, 不妨设 $y > 0$. 由于 $(x - 1, x) = (x, x + 1) = 1$, 则 $(x, x^2 - 1) = 1$, 据**引理 2.2.1** 知, 存在 $u, v \in \mathbb{Z}_{>0}$, $(u, v) = 1$ 使得 $x = u^2$, $x^2 - 1 = v^2$, $y = uv$, 即 $x^2 = u^4 = v^2 - 1$, 从而 $(u^2 + v)(u^2 - v) = 1$, 则必有 $u^2 + v = u^2 - v = 1$, 这表明 $u = 1$ 且 $v = 0$, 即 $y = 0$, 这与 $y > 0$ 矛盾.

所以, 原方程的所有整数解为 $(x, y) = (0, 0)$ 或 $(\pm 1, 0)$. □

第三章　同余

§3.1　同余的基本概念

定义 3.1.1. 设 $m \in \mathbb{Z}_{>0}$, 称 a 与 b **关于模** m **同余**, 如果 $m \mid a-b$. 记作 $a \equiv b \pmod{m}$. 否则称 a 与 b 关于模 m 不同余, 记作 $a \not\equiv b \pmod{m}$.

不难验证关于模 m 同余是一个等价关系. 下面是同余的一些基本性质.

命题 3.1.1. 设 $m \in \mathbb{Z}_{>0}$,

(1) $a \equiv b \pmod{m}$ 当且仅当 a, b 除以 m 所得的最小非负余数相等.

(2) 若 $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m}$, 则 $a+c \equiv b+d \pmod{m}$ 且 $ac \equiv bd \pmod{m}$.

(3) $qa \equiv qb \pmod{m}$ 当且仅当 $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{(q,m)}\right)$.

(4) 若 $a \equiv b \pmod{m}$, 则 $(a,m) = (b,m)$.

(5) 若 $(a,m) = 1$, 则存在 a' 使得 $aa' \equiv 1 \pmod{m}$, 并且这样的 a' 在模 m 下是唯一的. 我们称 a' 为 a **在模** m **下的逆**, 通常将 a 的逆记作 $\bar{a}$ 或 a^{-1}.

(6) 同余式组 $a \equiv b \pmod{m_k}$ $(k = 1, \cdots, n)$ 成立当且仅当 $a \equiv b \pmod{[a_1, \cdots, a_n]}$.

证明. (1) 可由带余除法直接推出. (4) 为**命题 1.2.4 (4)** 的推论. (6) 即**命题 1.3.2**.

(2) 设 $a := b + km$, $c := d + \ell m$ (其中 $k, \ell \in \mathbb{Z}$), 则有 $a + c = (b+d) + (k+\ell)m$, $ac = bd + (b\ell + dk + k\ell m)m$, 所以 $a + c \equiv b + d \,(\mathrm{mod}\, m)$ 且 $ac \equiv bd \,(\mathrm{mod}\, m)$.

(3) $qa \equiv qb \,(\mathrm{mod}\, m)$ 当且仅当 $m \mid q(a-b)$, 即 $\dfrac{m}{(q,m)} \,\Big|\, \dfrac{q}{(q,m)}(a-b)$, 这式成立当且仅当 $\dfrac{m}{(q,m)} \,\Big|\, a-b$, 即 $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{(q,m)}\right)$.

(5) 由辗转相除法知存在 $x, y \in \mathbb{Z}$ 使得 $ax + my = 1$, 于是 $ax \equiv 1 \,(\mathrm{mod}\, m)$. 再由 (3) 知这样的 x 在模 m 下是唯一的. □

例 3.1.1. 求 3^{406} 的个位数字.

解. 我们有 $3^{406} \equiv (-1)^{203} \equiv -1 \equiv 9 (\mathrm{mod}\, 10)$, 故 3^{406} 的个位数字为 9. □

例 3.1.2. 证明不定方程 $x^2 - 5y^2 = 203$ 无解.

证明. 由于 $203 = 7 \cdot 29$, 如果 (x_0, y_0) 是原方程的一组解, 则 $(x_0, 203) = (y_0, 203) = 1$ 且 $x_0^2 \equiv 5y_0^2 \pmod 7$, 即 $(x_0\bar{y_0})^2 \equiv 5 \pmod 7$, 这与 n^2 模 7 仅可能与 0, 1, 2, 4 同余矛盾. 故原方程无解. □

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 3.1.3. 求所有的 $n \in \mathbb{Z}_{>0}$, 使得 $7^n + 1$ 是 10 的倍数.

解. 注意到 $7^2 \equiv 49 \equiv 9 \equiv -1 \pmod{10}$, 即 $7^4 \equiv (-1)^2 \equiv 1 \pmod{10}$, 故 $\forall k \in \mathbb{N}^*$ 都有 $7^{4k+2} \equiv 1 \pmod{10}$, 即此时 $10 \mid 7^{4k+2} + 1$. 故所求的正整数为 $n = 4k + 2$ $(k \in \mathbb{N})$. □

例 3.1.4. 证明不定方程 $x^2 - 3y^2 = 187$ 无解.

证明. 注意到 $187 = 11 \cdot 17$, 若 (x_0, y_0) 是原方程的一组解, 则 $(x_0, 187) = (y_0, 187) = 1$ 且 $x_0^2 \equiv 3y_0^2 \pmod{17}$, 即 $(x_0\bar{y_0})^2 \equiv 3 \pmod{17}$. 而任意完全平方数 n^2 模 17 的余数仅可能为 0, 1, 2, 4, 5, 8, 9, 15, 16, 矛盾. 因此原方程无解. □

§3.2 剩余类与剩余系

定义 3.2.1. 给定模 m, 对任意的整数 r, 称与 r 关于模 m 同余的全体整数构成的集合为模 m 的一个**剩余类** (也称**同余类**), 记作 $r \bmod m := \{r + km : k \in \mathbb{Z}\}$.

利用带余除法可以验证以下结论.

命题 3.2.1. 设 $m \in \mathbb{Z}_{>0}$,

(1) $r \bmod m = s \bmod m$ 当且仅当 $r \equiv s \pmod m$;

(2) $\forall r, s \in \mathbb{Z}$, 要么 $r \bmod m = s \bmod m$, 要么 $r \bmod m \cap s \bmod m = \varnothing$;

(3) 有且仅有 m 个不同的模 m 的同余类, 它们是 $0 \bmod m, 1 \bmod m, \cdots, (m-1) \bmod m$, 即 $\mathbb{Z} = \bigcup_{k=0}^{m-1} k \bmod m$. 我们将全体关于模 m 的同余类构成的集合记为 $\mathbb{Z}/m\mathbb{Z}$ 或 $\mathbb{Z}_m$.

注记 3.2.1. 其实, 这里的记号 $\mathbb{Z}/m\mathbb{Z} := \{r + km : r, k \in \mathbb{Z}\}$ 采用的是商群的记号. 当然, 利用代数学的知识也可验证, 集合 $\mathbb{Z}_m$ 可以赋予模 m 上的加法运算, 因此 $(\mathbb{Z}/m\mathbb{Z}, +)$ 是一个 Abel 群, 称为*整数模 m 加法群*.

定义 3.2.2. 称 $\{a_1, \cdots, a_m\}$ 为模 m 的一个**完全剩余系**, 如果整数 $a_1, \cdots, a_m$ 两两模 m 不同余.

通过这一定义我们可以看出, $\{a_1,\cdots,a_m\}$ 是模 m 的一个完全剩余系当且仅当每个 a_k 都来源于不同的剩余类.

下面讨论与 m 互素的全体整数在模 m 的剩余类中的分布情况. 由**命题 3.1.1 (4)** 知, 若 $(r,m)=1$, 则 $r \bmod m$ 中的每个元素都与 m 互素, 这保证了下述定义的合理性.

定义 3.2.3. 称 $r \bmod m$ 为模 m 的**既约剩余类**, 如果 $(r,m)=1$.

命题 3.2.2. 模 m 的全部既约剩余类是 $r \bmod m$, 其中 $1 \leqslant r \leqslant m$ 且 $(r,m)=1$. 我们把模 m 的全部既约剩余类的个数记为 $\varphi(m)$, 并称 $\varphi:\mathbb{Z}_{>0}\to\mathbb{Z}_{>0}$ 为 **Euler 函数**.

按照定义, $\varphi(m)$ 也即是 $\{1,2,\cdots,m\}$ 中与 m 互素的元素个数.

定义 3.2.4. 从模 m 的每个既约剩余类中各取一个元素所形成的集合称为模 m 的一个**简化剩余系**, 这表明模 m 的每个简化剩余系中都恰有 $\varphi(m)$ 个元素.

例如, $\{1,5\}$ 是模 6 的一个简化剩余系; 若 p 是素数, 则 $\{1,2,\cdots,p-1\}$ 是模 p 的一个简化剩余系.

定理 3.2.1. 设 $n\in\mathbb{Z}_{>0}$, 则 $\displaystyle\sum_{d\mid n}\varphi(d)=n$. 这里 $\displaystyle\sum_{d\mid n}$ 表示对 n 的全体正因数求和.

证明. 将 $[1,n]$ 中的整数按照它与 n 的最大公因数分类, 可得

$$n=\sum_{k\leqslant n}1=\sum_{d\mid n}\sum_{\substack{k\leqslant n\\(k,n)=d}}1=\sum_{d\mid n}\sum_{\substack{k\leqslant n/d\\(k,n/d)=1}}1=\sum_{d\mid n}\varphi\left(\frac{n}{d}\right)=\sum_{d\mid n}\varphi(d).$$

其中最后一步利用了**命题 1.1.2**. □

命题 3.2.3. 设 $(a,m)=1$, $b\in\mathbb{Z}$.

(1) $\{x_1,\cdots,x_m\}$ 是模 m 的完全剩余系当且仅当 $\{ax_1+b,\cdots,ax_m+b\}$ 是模 m 的完全剩余系;

(2) $\left\{x_1,\cdots,x_{\varphi(m)}\right\}$ 是模 m 的简化剩余系当且仅当 $\left\{ax_1,\cdots,ax_{\varphi(m)}\right\}$ 是模 m 的简化剩余系.

证明. (1) 这是因为 $x_i\not\equiv x_j\,(\bmod m)$ 当且仅当 $ax_i+b\not\equiv ax_j+b\,(\bmod m)$.
(2) 这是因为 $x_i\not\equiv x_j\,(\bmod m)$ 当且仅当 $ax_i\not\equiv ax_j\,(\bmod m)$ 以及 $(x_k,m)=1$ 当且仅当 $(ax_k,m)=1$. □

例 3.2.1. 设 $m\in\mathbb{Z}_{>1}$, $(a,m)=1$, $b\in\mathbb{Z}$. 求 $\displaystyle\sum_{n\leqslant m}\left\{\frac{an+b}{m}\right\}$.

解. 注意到 $\left\{\dfrac{x}{m}\right\}$ 周期为 m 且 $an+b$ (其中 $n \leqslant m$, $(a,m)=1$) 通过模 m 的一个完全剩余系, 故

$$\sum_{n\leqslant m}\left\{\frac{an+b}{m}\right\}=\sum_{n\leqslant m}\left\{\frac{n}{m}\right\}=\sum_{n\leqslant m-1}\frac{n}{m}=\frac{m-1}{2}.$$

最后一步的计算是通过配对得到的. □

命题 3.2.4. 设 $\{x_1,\cdots,x_m\}$, $\{y_1,\cdots,y_n\}$ 分别为模 m,n 的一个完全剩余系. 我们记 $z_{ij}:=x_i+my_j$, 则 $\{z_{ij}:1\leqslant i\leqslant m,1\leqslant j\leqslant n\}$ 是模 mn 的一个完全剩余系.

证明. 这样的 z_{ij} 共有 mn 个, 故只需证明它们两两不同余即可.

若存在 i_1,i_2,j_1,j_2 使得 $z_{i_1j_1}\equiv z_{i_2j_2}\,(\mathrm{mod}\,mn)$, 即 $x_{i_1}+my_{j_1}\equiv x_{i_2}+my_{j_2}\,(\mathrm{mod}\,mn)$, 则将这一关系式约化到模 m 上可得 $x_{i_1}\equiv x_{i_2}\,(\mathrm{mod}\,m)$, 因此 $i_1=i_2$. 将这代入上式可得 $my_{j_1}\equiv my_{j_2}\,(\mathrm{mod}\,mn)$, 再由**命题 1.2.1 (3)** 可得 $y_{j_1}\equiv y_{j_2}\,(\mathrm{mod}\,n)$, 从而 $j_1=j_2$. □

命题 3.2.5. 设 $M:=mn$ 且 $(m,n)=1$. 若记 $z_{ij}:=nx_i+my_j$ $(1\leqslant i\leqslant s,\,1\leqslant j\leqslant t)$, 则这样的 z_{ij} 构成模 M 的一个完全/简化剩余系的充要条件是 $\{x_1,\cdots,x_t\}$ 和 $\{y_1,\cdots,y_t\}$ 分别为模 m,n 的一个完全/简化剩余系.

证明. 我们先对完全剩余系进行证明.

充分性. 此时 $s=m$, $t=n$. 由于这样的 z_{ij} 共有 M 个, 故只需证明它们关于模 M 两两不同余. 若存在指标 i_1,i_2,j_1,j_2 使得 $z_{i_1j_1}\equiv z_{i_2j_2}\,(\mathrm{mod}\,M)$, 则将该同余式分别约化到模 m,n 上可得 $nx_{i_1}\equiv nx_{i_2}\,(\mathrm{mod}\,m)$, $my_{j_1}\equiv my_{j_2}\,(\mathrm{mod}\,n)$, 而注意到 $(m,n)=1$, 故 $x_{i_1}\equiv x_{i_2}\,(\mathrm{mod}\,m)$ 且 $y_{j_1}\equiv y_{j_2}\,(\mathrm{mod}\,n)$, 从而 $i_1=i_2$ 且 $j_1=j_2$.

必要性. 设全体 z_{ij} (其中 $1\leqslant i\leqslant s$, $1\leqslant j\leqslant t$) 构成模 M 的一个完全剩余系, 则 $st=M=mn$. 取定 y_1, 由 $z_{i1}=nx_i+my_1$ 关于模 m 两两不同余且 $(m,n)=1$ 可知 x_i 关于模 m 两两不同余, 从而 $s\leqslant m$, 同理可得 $t\leqslant n$. 但注意到 $st=mn$, 所以必有 $s=m$ 且 $t=n$.

为证明简化剩余系的情形, 只需证明 $(z_{ij},M)=1\Leftrightarrow(x_i,m)=(y_i,n)=1$. 实际上, $(z_{ij},M)=1$ 当且仅当 $(z_{ij},m)=(z_{ij},n)=1$, 而由 $(m,n)=1$ 可知 $(z_{ij},m)=(nx_i,m)=(x_i,m)$, 同理可得 $(z_{ij},n)=(y_j,n)$, 从而命题得证. □

推论 3.2.1. 若 $m,n\in\mathbb{Z}_{>0}$ 且 $(m,n)=1$, 则 $\varphi(mn)=\varphi(m)\varphi(n)$.

这表明 Euler 函数 φ 是积性函数, 这是一个美好的性质 (见 §7.1).

命题 3.2.6. 设 $n\in\mathbb{Z}_{>0}$, 则 $\varphi(n)=n\prod\limits_{p\mid n}\left(1-\dfrac{1}{p}\right)$, 其中 $\prod\limits_{p\mid n}$ 表示 p 通过 n 的全部素因子.

证明. $n=1$ 时命题显然成立, 下设 $n\geqslant 2$ 且 n 的标准分解式为 $n:=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. 据推论 3.2.1 可得 $\varphi(n)=\varphi(p_1^{\alpha_1})\cdots\varphi(p_r^{\alpha_r})$. 而

$$\varphi(p^\alpha)=\sum_{\substack{k=1\\(k,p)=1}}^{p^\alpha}1=\sum_{k=1}^{p^\alpha}1-\sum_{\substack{k=1\\p|k}}^{p^\alpha}1=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right).$$

这样, 我们便证明了这一结论. □

例 3.2.2. 设 $(n,q)=1$, 计算 Ramanujan 和 $c_q(n):=\sum\limits_{\substack{k\leqslant q\\(k,q)=1}}e\left(\dfrac{kn}{q}\right)$.

解. 注意到函数 $e\left(\dfrac{x}{q}\right)$ 的周期为 q, 故由**命题 3.2.3 (2)** 知 $c_q(n)=c_q(1)$.

若 $(q_1,q_2)=1$, 则当 a,b 分别通过模 q_1,q_2 的简化剩余系时, aq_2+bq_1 通过模 q_1q_2 的简化剩余系, 故

$$\begin{aligned}c_{q_1q_2}(1)&=\sum_{\substack{k\leqslant q_1q_2\\(k,q_1q_2)=1}}e\left(\frac{k}{q_1q_2}\right)=\sum_{\substack{a\leqslant q_1\\(a,q_1)=1}}\sum_{\substack{b\leqslant q_2\\(b,q_2)=1}}e\left(\frac{aq_2+bq_1}{q_1q_2}\right)\\&=\sum_{\substack{a\leqslant q_1\\(a,q_1)=1}}e\left(\frac{a}{q_1}\right)\sum_{\substack{b\leqslant q_2\\(b,q_2)=1}}e\left(\frac{b}{q_2}\right)=c_{q_1}(1)\,c_{q_2}(1).\end{aligned}$$

因此, 如果 q 具有标准分解式 $q:=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, 则 $c_q(1)=c_{p_1^{\alpha_1}}(1)\cdots c_{p_r^{\alpha_r}}(1)$. 注意到

$$c_{p^\alpha}(1)=\sum_{\substack{k\leqslant p^\alpha\\(k,p)=1}}e\left(\frac{k}{p^\alpha}\right)=\sum_{k\leqslant p^\alpha}e\left(\frac{k}{p^\alpha}\right)-\sum_{k\leqslant p^{\alpha-1}}e\left(\frac{k}{p^{\alpha-1}}\right)=\begin{cases}-1, & \alpha=1,\\ 0, & \alpha>1.\end{cases}$$

所以

$$c_q(n)=\begin{cases}1, & q=1,\\ (-1)^r, & q=p_1\cdots p_r,\text{其中 }p_1,\cdots,p_r\text{ 是两两不同的素数},\\ 0, & \text{其它}.\end{cases}$$

上式右边即为知名的 Möbius 函数 $\mu(q)$. □

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 3.2.3. 设 $n=k\ell$ 且 ℓ 的素因子均整除 k, 则 $\varphi(n)=\ell\varphi(k)$.

证明. *Key*: *k 与 ℓ 只有 k 能完整包含 n 的所有素因子*. 用唯一分解式计算验证即可. □

例 3.2.4. 设 $p>3$ 且 p 与 $p+2$ 均为素数, 证明 $\varphi(p+1)\leqslant\dfrac{p+1}{3}$.

证明. 因 $p>3$ 且 $p,p+2$ 均为素数, 故 $p\geqslant 5$ 且 $2\mid p+1$. 而连续的 3 个正整数中必有一个是 3 的倍数, 故 $3\mid p+1$. 于是, $\varphi(p+1)\leqslant (p+1)\left(1-\dfrac{1}{2}\right)\left(1-\dfrac{1}{3}\right)=\dfrac{p+1}{3}$. □

例 3.2.5. 设 p 为素数, $1\leqslant t\leqslant s$. 证明: 所有的 $u+p^{s-t}v$ (其中 $u=0,1,\cdots,p^{s-t}-1$, $v=0,1,\cdots,p^t-1$) 为模 p^s 的一个完全剩余系.

证明. 不难知道 $u+p^{s-t}v$ 在取遍所有给定值后共得到 p^s 个整数, 只需验证这 p^s 个整数对模 p^s 两两不同余. (反证法即可, 这里略去过程) □

例 3.2.6. 设 $m\geqslant 2$ 且 $(a,m)=1$. 求 $\displaystyle\sum_{\substack{k\leqslant m\\(k,m)=1}}\left\{\frac{ak}{m}\right\}$.

解. 只需注意到

$$\sum_{\substack{k\leqslant m\\(k,m)=1}}\left\{\frac{ak}{m}\right\}=\sum_{\substack{k\leqslant m\\(k,m)=1}}\left\{\frac{k}{m}\right\}=\sum_{\substack{k\leqslant m\\(k,m)=1}}\frac{k}{m}=\sum_{\substack{k\leqslant m\\(k,m)=1}}\frac{m-k}{m}=\varphi(m)-\sum_{\substack{k\leqslant m\\(k,m)=1}}\frac{k}{m},$$

因此 $\displaystyle\sum_{\substack{k\leqslant m\\(k,m)=1}}\left\{\frac{ak}{m}\right\}=\sum_{\substack{k\leqslant m\\(k,m)=1}}\frac{k}{m}=\frac{\varphi(m)}{2}$. □

例 3.2.7. 设 $f\in\mathbb{Z}[x]$, 对任意的 $n\in\mathbb{N}^*$, 记 $\varphi_f(n):=\displaystyle\sum_{\substack{k\leqslant n\\(f(k),n)=1}}1$. 证明: 当 $(m,n)=1$ 时, $\varphi_f(mn)=\varphi_f(m)\varphi_f(n)$ (即 φ_f 是积性函数).

证明. $(m,n)=1$ 时, 由**命题 3.2.5** 知

$$\begin{aligned}\varphi_f(mn)&=\sum_{\substack{j\leqslant mn\\(f(j),mn)=1}}1=\sum_{\substack{j\leqslant mn\\(f(j),m)=(f(j),n)=1}}1=\sum_{\substack{k\leqslant m\ \ell\leqslant n\\(f(kn+\ell m),m)=(f(kn+\ell m),n)=1}}\sum1\\&=\sum_{\substack{k\leqslant m\ \ell\leqslant n\\(f(kn),m)=(f(\ell m),n)=1}}\sum1=\sum_{\substack{k\leqslant m\\(f(k),m)=1}}\sum_{\substack{\ell\leqslant n\\(f(\ell),n)=1}}1=\varphi_f(m)\varphi_f(n).\end{aligned}$$

这样, 我们便证明了这一结论. □

§3.3 Euler 定理

定理 3.3.1 (Euler)**.** 设 $m\in\mathbb{Z}_{>0}$ 且 $(a,m)=1$, 则 $a^{\varphi(m)}\equiv 1\,(\mathrm{mod}\,m)$.

证明. 设 $\{x_1,\cdots,x_{\varphi(m)}\}$ 是模 m 的一个简化剩余系, 由 $(a,m)=1$ 知 $\{ax_1,\cdots,ax_{\varphi(m)}\}$ 也是模 m 的一个简化剩余系, 即

$$x_1\cdots x_{\varphi(m)}\equiv(ax_1)\cdots(ax_{\varphi(m)})\,(\mathrm{mod}\,m),$$

因此 $a^{\varphi(m)}\equiv 1\,(\mathrm{mod}\,m)$. □

特别地, 当 m 为素数时, 我们可以得到下面的结论 (常称为 Fermat 小定理).

定理 3.3.2 (Fermat)**.** 若 p 为素数, 则 $\forall\, a \in \mathbb{Z}$ 都有 $a^p \equiv a \,(\mathrm{mod}\, p)$.

证明. 若 $p \mid a$, 则命题显然成立; 若 $p \nmid a$, 则由**定理 3.3.1** 即证. □

推论 3.3.1. 当 $m \geqslant 3$ 时 $\varphi(m)$ 必为偶数 (在**定理 3.3.1** 中取 $a = -1$ 即得).

注记 3.3.1. 一个自然的想法是去讨论 Euler 定理的逆命题是否成立, 这一问题的答案是否定的. R.D.Carmichael 不仅指出了 561 是满足上述条件的的一个合数, 还对这一问题进行了系统的研究, 因此人们把满足条件的合数 n 称为 Carmichael 数.

例 3.3.1. 求 $2017^{2017^{100}}$ 在十进制表示下的末两位数字.

解. 因 $\varphi(100) = 40$ 且 $(2017, 100) = 1$, 故 $2017^{40k} \equiv 1 \,(\mathrm{mod}\, 10)$, $\forall\, k \in \mathbb{Z}_{>0}$. 注意到

$$2017^{100} \equiv 17^{100} \equiv 289^{59} \equiv 9^{50} \equiv 81^{25} \equiv 1 \,(\mathrm{mod}\, 40),$$

故 $2017^{2017^{100}} \equiv 2017 \equiv 17 \,(\mathrm{mod}\, 100)$, 即 $2017^{2017^{100}}$ 在十进制表示下的末两位为 17. □

例 3.3.2. 有理数 $\dfrac{a}{b}$ (其中 $0 < a < b$ 且 $(a, b) = 1$) 在十进制下可表为纯循环小数的充要条件是 $(b, 10) = 1$.

证明. 必要性. 若 $\dfrac{a}{b} = 0.\dot{a_1}a_2 \cdots \dot{a_t}$, 则有 $10^t \cdot \dfrac{a}{b} = 10^{t-1}a_1 + \cdots + a_t + \dfrac{a}{b}$, 故 $b \mid 10^t - 1$, 从而 $(b, 10) = 1$.

充分性. 若 $(b, 10) = 1$, 则存在 $t \in \mathbb{Z}_{>0}$ 使得 $10^t \equiv 1 \,(\mathrm{mod}\, b)$. 不妨设 t 是满足这一条件的最小正整数, 从而存在 $q \in \mathbb{Z}$ 使得 $10^t a = qb + a$ 且

$$0 < q < 10^t \cdot \frac{a}{b} \leqslant 10^t \cdot \frac{b-1}{b} < 10^t - 1.$$

因此可设 $q := 10^{t-1}q_1 + \cdots + 10q_{t-1} + q_t$, 于是由 $10^t \cdot \dfrac{a}{b} = q + \dfrac{a}{b}$ 可得

$$\frac{a}{b} = 0.q_1 \cdots q_t + \frac{1}{10^t} \cdot \frac{a}{b},$$

反复利用此式即得 $\dfrac{a}{b} = 0.\dot{q_1} \cdots \dot{q_t}$. □

注记 3.3.2. 由这一例子的证明过程可以看出, 当既约真分数 $\dfrac{a}{b}$ 可以表示为纯循环小数时, 其循环节的长度是使得 $10^t \equiv 1 \,(\mathrm{mod}\, b)$ 成立的最小正整数 t.

类似地, 我们还有下述结论.

推论 3.3.2. 设整数 $0 < a < b$, $(a,b) = 1$ 且 $b := 2^\alpha 5^\beta b_0$ (其中 α, β 不全为 0 且 $b_0 > 1$), 则 $\dfrac{a}{b}$ 在十进制下可表为混循环小数, 其中不循环的位数为 $r := \max(\alpha, \beta)$.

只需注意到 $(b_1, 10) = 1$, 即 $\dfrac{a}{b_0}$ 是纯循环小数; 而 $\dfrac{a}{b} = \dfrac{1}{2^\alpha 5^\beta} \cdot \dfrac{a}{b_0} = \dfrac{2^{r-\alpha}5^{r-\beta}}{10^r} \cdot \dfrac{a}{b_0}$ 中 $\dfrac{2^{r-\alpha}5^{r-\beta}}{10^r}$ 是有限小数且位数为 r, 故 $\dfrac{a}{b}$ 可表为混循环小数且非循环节长度为 r.

考虑一些例子, 这些例题来源于讲义上的课后习题.

例 3.3.3. 求 $100^{100^{100}}$ 除以 27 的最小非负余数.

解. 因 $\varphi(27) = 18$ 且 $(100, 27) = 1$, 故 $100^{18k} \equiv 1 \pmod{27}$, $\forall\, k \in \mathbb{Z}_{>0}$. 注意到

$$100^{100} \equiv (-8)^{100} \equiv 8^{100} \equiv (8^2)^{50} \equiv 2^6 \equiv 10 \pmod{18},$$

故 $100^{100^{100}} \equiv 100^{10} \equiv (-8)^{10} \equiv (10)^5 \equiv (-8)^2 \cdot 10 \equiv -8 \equiv 19 \pmod{27}$, 即 $100^{100^{100}}$ 除以 27 的最小非负余数为 19. □

例 3.3.4. 设 $m, n \in \mathbb{Z}_{>0}$ 且 $(m, n) = 1$, 证明 $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.

证明. 由 Euler 定理, 可得 $m^{\varphi(n)} \equiv 1 \pmod{n}$ 且 $n^{\varphi(m)} \equiv 1 \pmod{m}$, 即 $n \mid m^{\varphi(n)} - 1$ 且 $m \mid n^{\varphi(m)} - 1$. 所以

$$mn \mid (m^{\varphi(n)} - 1)(n^{\varphi(m)} - 1) = m^{\varphi(n)}n^{\varphi(m)} - (m^{\varphi(n)} + n^{\varphi(m)}) + 1,$$

此即 $mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$, 故 $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$. □

例 3.3.5. 设 $n \in \mathbb{Z}_{>0}$, 证明: $\left(\prod\limits_{\substack{m \leqslant n \\ (m,n)=1}} m \right)^2 \equiv 1 \pmod{n}$.

证明. 为方便起见, 我们记

$$A := \prod_{\substack{m \leqslant n \\ (m,n)=1}} m,$$

则 $\left\{ \dfrac{A}{m} : 1 \leqslant m \leqslant n, (m,n) = 1 \right\}$ 是模 n 的一个简化剩余系, 于是

$$A \equiv \prod_{\substack{m \leqslant n \\ (m,n)=1}} \frac{A}{m} \equiv A^{\varphi(n)-1} \pmod{n},$$

进而我们得到 $A^2 \equiv A^{\varphi(n)} \equiv 1 \pmod{n}$. □

第四章　同余方程

§4.1　基本概念及一次同余方程

定义 4.1.1. 设 $f := \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ 且 $m \in \mathbb{Z}_{>0}$. 我们称 $f(x) \equiv 0 \pmod{m}$ 为关于模 m 的**同余方程**. 如果 $x_0 \in \mathbb{Z}$ 满足 $f(x_0) \equiv 0 \pmod{m}$, 则称 $x \equiv x_0 \pmod{m}$ 为该同余方程的一个**解**.

我们指出, **例 1.1.1** 中的结论保证了上述定义的合理性.

例 4.1.1. $x^4+4x^2+1 \equiv 0 \pmod{5}$ 无解, $x^2-1 \equiv 0 \pmod{8}$ 全部解为 $x \equiv \pm 1, \pm 3 \pmod{8}$.

首先, 我们来考虑较为基础的一次同余方程.

命题 4.1.1. 记 $d := (a, m)$, 则同余方程

$$ax \equiv b \pmod{m} \tag{4.1}$$

有解的充要条件是 $d \mid b$. 当 (4.1) 有解时, 其全部解为

$$x \equiv x_0 + \frac{m}{d}k \pmod{m}, \qquad k = 0, 1, \cdots, d-1, \tag{4.2}$$

其中 $x_0 \pmod{m}$ 是 (4.1) 的一个特解. 因此, 若 (4.1) 有解, 则它共有 d 个解.

证明. $x \pmod{m}$ 是 (4.1) 的一个解当且仅当存在 $y \in \mathbb{Z}$ 使得 $ax + my = b$, 据命题 2.1.1 可知后者有解当且仅当 $d \mid b$. 此外, 若 $d \mid b$ 且 x_0, y_0 是 $ax + my = b$ 的一组特解, 则该不定方程的全部解为

$$\begin{cases} x = x_0 + \dfrac{m}{d}k, \\ y = y_0 - \dfrac{a}{d}k, \end{cases} \quad k \in \mathbb{Z}.$$

因此, (4.1) 的全部解可由 (4.2) 给出. □

注记 4.1.1. 这里, 我们相当于将二元一次不定方程**约化**到模 m 中来解决一次同余方程.

推论 4.1.1. 若 $(a,m)=1$, 则同余方程 $ax\equiv b\,(\mathrm{mod}\,m)$ 有唯一解.

例 4.1.2. 求解同余方程 $10x\equiv 6\,(\mathrm{mod}\,12)$.

解. 原方程即 $5x\equiv -x\equiv 3\,(\mathrm{mod}\,6)$, 故其解为 $x\equiv 3\,(\mathrm{mod}\,6)$, 即 $x\equiv 3,9\,(\mathrm{mod}\,12)$. □

对于一般的同余方程, 由**命题 3.1.1 (6)** 可得下述结论.

命题 4.1.2. 设 $m_1,\cdots,m_k$ 是 k 个两两互素的正整数, 记 $m:=\prod_{j=1}^{k}m_j$. 则同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,m)$ 与同余方程组 $f(x)\equiv 0\,(\mathrm{mod}\,m_j)$ $(j=1,\cdots,k)$ **等价**. □

例 4.1.3. 求解同余方程 $x^5\equiv 4\,(\mathrm{mod}\,15)$.

解. 据**命题 4.1.2**, 这等价于

$$\begin{cases} x^5\equiv 4\equiv 1\,(\mathrm{mod}\,3),\\ x^5\equiv 4\equiv -1\,(\mathrm{mod}\,5). \end{cases}$$

其中, 第一个方程的解为 $x\equiv 1\,(\mathrm{mod}\,3)$, 第二个方程的解为 $x\equiv -1\equiv 4\,(\mathrm{mod}\,5)$. 因此, 原方程的解为 $x\equiv 4\,(\mathrm{mod}\,5)$. □

这一例子提示了我们一个解同余方程的方法. 设 m 的标准分解式为 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, 由命题 4.1.2 知同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,m)$ 等同于同余方程组 $f(x)\equiv 0\,(\mathrm{mod}\,p_k^{\alpha_k})$ (其中 $k=1,\cdots,r$). 如果其中的某个方程无解, 则原方程无解; 上述方程都有解时, 我们可将它们先解出, 进而再得到原方程的解. 这便将问题归结为一次同余方程组的求解.

例 4.1.4. 设 $f(x_1,\cdots,x_n)\in\mathbb{Z}[x_1,\cdots,x_n]$, 证明同余方程 $f(x_1,\cdots,x_n)\equiv 0\,(\mathrm{mod}\,m)$ 的解数为

$$\frac{1}{m}\sum_{a\leqslant m}\sum_{x_1\leqslant m}\cdots\sum_{x_n\leqslant m}e\left(\frac{af(x_1,\cdots,x_n)}{m}\right).$$

证明. 只需注意到对每组取定的 $(x_1,\cdots,x_n)$ 都有

$$\sum_{a=1}^{m}\frac{1}{m}e\left(\frac{af(x_1,\cdots,x_n)}{m}\right)=\begin{cases}1, & m\mid f(x_1,\cdots,x_n),\\ 0, & m\nmid f(x_1,\cdots,x_n)\end{cases}$$

并且 $1\leqslant x_1,\cdots,x_n\leqslant m$ 时可取遍模 m 下 $f(x_1,\cdots,x_n)$ 的所有可能值, 故同余方程 $f(x_1,\cdots,x_n)\equiv 0\,(\mathrm{mod}\,m)$ 的解数为

$$\frac{1}{m}\sum_{a\leqslant m}\sum_{x_1\leqslant m}\cdots\sum_{x_n\leqslant m}e\left(\frac{af(x_1,\cdots,x_n)}{m}\right).$$

□

注记 4.1.2. 特别地, 如果取 $f(x_1,\cdots,x_n):=\sum_{k=1}^{n}a_kx_k-b$ 并记 $d:=(a_1,\cdots,a_n,m)$, 则方程 $f(x_1,\cdots,x_n)\equiv 0\,(\mathrm{mod}\,m)$ 有解的充要条件是 $d\mid b$, 并且此时它的解数为 dm^{n-1}.

§4.2 中国剩余定理

本节我们着重讨论一次同余方程组的求解.

定理 4.2.1 (中国剩余定理)**.** 设 m_j $(j=1,\cdots,k)$ 是两两互素的正整数并记 $m:=\prod_{j=1}^{k} m_j$, 则同余方程组 $x\equiv a_j \pmod{m_j}$ $(j=1,\cdots,k)$ 对模 m 有唯一解.

证明. *存在性*. 记 $M_j:=\dfrac{m}{m_j}$, 则 $(M_j,m_j)=1$, 故存在 $\overline{M_j}\in\mathbb{Z}$ 使得 $\overline{M_j}M_j\equiv 1\pmod{m_j}$. 因为对任意的 ℓ 有

$$\sum_{j=1}^{k} a_j\overline{M_j}M_j\equiv a_\ell\overline{M_\ell}M_\ell\equiv a_\ell \pmod{m_\ell},$$

所以 $x\equiv\sum_{j=1}^{k} a_j\overline{M_j}M_j \pmod{m}$ 是原同余方程组的一个解.

唯一性. 设 $x_1 \pmod{m}$, $x_2 \pmod{m}$ 均为原方程组的解, 则 $x_1\equiv x_2 \pmod{m_j}$ (其中 $1\leqslant j\leqslant k$), 于是由命题 1.3.2 知 $x_1\equiv x_2 \pmod{m}$. □

例 4.2.1 (*孙子算经*)**.** 今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何? *这便是知名的“物不知其数”问题.*

解. 这实际上是在求解同余方程组

$$\begin{cases} x\equiv 2 \pmod{2},\\ x\equiv 3 \pmod{5},\\ x\equiv 2 \pmod{7}. \end{cases}$$

取 $m_1=3$, $m_2=5$, $m_3=7$, 按照定理 4.2.1 的证明过程依次计算对应的数值, 可得 $M_1=35$, $M_2=21$, $M_3=15$, $\overline{M_1}=2$, $\overline{M_2}=1$, $\overline{M_3}=1$, 因此我们得到, 原同余方程组的解为 $x\equiv 2\cdot 35\cdot 2+3\cdot 21\cdot 1+2\cdot 15\cdot 1\equiv 23 \pmod{105}$. □

注记 4.2.1. *三人同行七十稀, 五树梅花廿一枝, 七子团圆正月半, 除百零五便得知.*

需要注意的是, **定理 4.2.1** 要求同余式中的模两两互素, 但在实际应用中这一条件往往难以满足. 下述定理彻底解决了这一问题.

定理 4.2.2. 设 m_j 为正整数 $(j=1,\cdots,k)$ 并记 $m:=[m_1,\cdots,m_k]$. 则同余方程组 $x\equiv a_j \pmod{m_j}$ $(j=1,\cdots,k)$ 有解当且仅当 $(m_i,m_j)\mid a_i-a_j$ $(\forall\, i\neq j)$. 当这一方程组有解时, 它对模 m 有唯一解.

证明. 这一方程组解的唯一性可类似于**定理 4.2.1** 的证明来处理, 我们主要证明原方程组解的存在性.

必要性. 若 x_0 是原方程组的一个解, 则 $m_j \mid x_0 - a_j$ $(\forall\, j)$, 于是对任意的 $i \neq j$ 都有 $(m_i, m_j) \mid x_0 - a_i$ 且 $(m_i, m_j) \mid x_0 - a_j$, 因此 $(m_i, m_j) \mid a_i - a_j$.

充分性. 设 m 的全部素因子为 $p_1, \cdots, p_r$, 并记 $m_i := p_1^{\alpha_{i1}} \cdots p_r^{\alpha_{ir}}$ (其中 $1 \leqslant i \leqslant k$, $\alpha_{ij} \geqslant 0$). 又记 $\beta_j := \max\{\alpha_{ij} : i = 1, \cdots, k\}$, 于是由**命题 4.1.2** 知原同余方程组等价于 $x \equiv a_i \,(\mathrm{mod}\, p_j^{\alpha_{ij}})$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant r)$. 因 $(m_i, m_j) \mid a_i - a_j$ $(\forall\, i \neq j)$, 故当 $\alpha_{ij} < \beta_j$ 时同余式 $x \equiv a_i (\mathrm{mod}\, p_j^{\alpha_{ij}})$ 是多余的. 从而上述方程组等价于 $x \equiv a_{i(j)} \,(\mathrm{mod}\, p_j^{\beta_j})$ $(1 \leqslant j \leqslant r)$, 这里 $i(j)$ 表示使得 $\alpha_{ij} = \beta_j$ 成立的 i (若存在多个满足条件的 i 则任取一个即可). 根据中国剩余定理可知, 原同余方程组对模 $p_1^{\beta_1} \cdots p_r^{\beta_r} =: m$ 有唯一解.

这样, 我们便证明了这一结论. □

推论 4.2.1. 以 $\rho(f, m)$ 表示同余方程 $f(x) \equiv 0 \,(\mathrm{mod}\, m)$ 的解数, 则对任意的 $(m, n) = 1$ $(m, n \in \mathbb{Z})$ 都有 $\rho(f, mn) = \rho(f, m)\rho(f, n)$. 即 $\rho(f, m)$ 对于第二个元素具有可乘性.

例 4.2.2. 求解同余方程组

$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 6), \\ x \equiv 3 \,(\mathrm{mod}\, 20), \\ x \equiv 13 \,(\mathrm{mod}\, 15). \end{cases}$$

解. 由**定理 4.2.2** 可验证上述同余方程组有解且它等价于

$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 3), \\ x \equiv 3 \,(\mathrm{mod}\, 4), \\ x \equiv -2 \,(\mathrm{mod}\, 5). \end{cases}$$

类似于**例 4.2.1** 可求得原同余方程组的解为 $x \equiv 43 \,(\mathrm{mod}\, 60)$. □

例 4.2.3. 设 $(m, n) = 1$, $\ell \,(\mathrm{mod}\, mn)$ 是同余方程组

$$\begin{cases} x \equiv a \,(\mathrm{mod}\, m), \\ x \equiv b \,(\mathrm{mod}\, n), \end{cases}$$

的解, 又设 $\bar{n}$ 和 $\bar{m}$ 分别满足 $n\bar{n} \equiv 1 \,(\mathrm{mod}\, m)$ 和 $m\bar{m} \equiv 1 \,(\mathrm{mod}\, n)$. 证明:

$$\frac{\ell}{mn} - \frac{a\bar{n}}{m} - \frac{b\bar{m}}{n} \in \mathbb{Z}.$$

证明. 只需证明 $mn \mid \ell - a\bar{n}n - b\bar{m}m$. 因 $l \equiv a \pmod{m}$ 且 $n\bar{n} \equiv 1 \pmod{m}$, 故 $m \mid \ell - a\bar{n}n - b\bar{m}m$, 同理可证 $n \mid \ell - a\bar{n}n - b\bar{m}m$. 又 $(m,n) = 1$, 所以 $mn \mid \ell - a\bar{n}n - b\bar{m}m$. □

类似地, 我们还可以证明下述结论.

例 4.2.4. 设 $(m,n) = 1$, $d \mid a - b$, $\ell \pmod{dmn}$ 是同余方程组

$$\begin{cases} x \equiv a \pmod{dm}, \\ x \equiv b \pmod{dn}, \end{cases}$$

的解, 又设 $\bar{n}$ 满足 $n\bar{n} \equiv 1 \pmod{m}$. 证明:

$$\frac{\ell}{dmn} - \frac{a-b}{d} \cdot \bar{n}m - \frac{b}{dmn} \in \mathbb{Z}.$$

例 4.2.5. 设 $q \in \mathbb{Z}_{>0}$. 对任意的 $m, n \in \mathbb{Z}$, 定义 Kloosterman 和为

$$S(m,n;q) := \sum_{\substack{1 \leqslant a \leqslant q \\ (a,q)=1}} e\left(\frac{am + \bar{a}n}{q}\right),$$

其中 $\bar{a}$ 为 a 在模 q 下的逆. 证明:

(1) $S(m,n;q) = S(n,m;q)$;

(2) 若 $(k,q) = 1$, 则有 $S(km,n;q) = S(m,kn;q)$;

(3) 若 $(q,r) = 1$, 则有 $S(m,n;qr) = S(\bar{r}m, \bar{r}n; q)S(\bar{q}m, \bar{q}n; r)$, 其中 $\bar{q}$ 和 $\bar{r}$ 分别满足 $q\bar{q} \equiv 1 \pmod{r}$ 和 $r\bar{r} \equiv 1 \pmod{q}$.

证明. (1) 可由结论 $\{x_1, \cdots, x_{\varphi(m)}\}$ 是模 m 的一个简化剩余系, 则 $\{\overline{x_1}, \cdots, \overline{x_{\varphi(m)}}\}$ 也是模 m 的一个简化剩余系得到, (2) 可由命题 3.2.3 (2) 得到, 下证 (3). 由命题 3.2.5 知,

$$S(m,n;qr) = \sum_{\substack{a=1 \\ (a,qr=1)}}^{qr} e\left(\frac{am + \bar{a}n}{qr}\right) = \sum_{\substack{j \leqslant q, k \leqslant r \\ (j,q)=(k,r)=1}} \sum e\left(\frac{(jr+kq)m + \ell n}{qr}\right),$$

其中 ℓ 满足 $\ell(jr + kq) \equiv 1 \pmod{qr}$, 这当且仅当 $\ell \equiv \overline{jr} \pmod{q}$ 且 $\ell \equiv \overline{kq} \pmod{r}$, 其中 $\overline{jr}$ 和 $\overline{kq}$ 分别满足 $jr \cdot \overline{jr} \equiv 1 \pmod{q}$ 与 $kq \cdot \overline{kq} \equiv 1 \pmod{r}$. 于是

$$\begin{aligned} S(m,n;qr) &= \sum_{\substack{j \leqslant q, k \leqslant r \\ (j,q)=(k,r)=1}} \sum e\left(\frac{(jr+kq)m}{qr} + \frac{\overline{jr} \cdot \bar{r}}{q}n + \frac{\overline{kq} \cdot \bar{q}}{r}n\right) \\ &= \sum_{\substack{j \leqslant q \\ (j,q)=1}} e\left(\frac{jm + \overline{jr^2}n}{q}\right) \sum_{\substack{k \leqslant r \\ (k,r)=1}} e\left(\frac{km + \overline{kq^2}n}{r}\right) \\ &= S(m, \overline{r^2}n; q)S(m, \overline{q^2}n; r) = S(\bar{r}m, \bar{r}n; q)S(\bar{q}m, \bar{q}n; r), \end{aligned}$$

上式中最后一步用到了 (2) 的结论. □

§4.3 以素数幂为模的同余方程

如前所述, 我们可将同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,m)$ 的求解转化为对 $f(x)\equiv 0\,(\mathrm{mod}\,p^\alpha)$ 的求解. 此外, 由推论 4.2.1 知, 这一方程解的个数可以分解为对应方程组解个数的乘积. 本节的目的就是讨论这样的同余方程的解数及求解的问题.

首先讨论 $\alpha=1$ 的情形.

定理 4.3.1 (Lagrange)**.** 设 $f:=\sum\limits_{k=1}^{n}a_kx^k\in\mathbb{Z}[x]$ 且素数 $p\nmid a_n$, 则 $\rho(f,p)\leqslant\min(n,p)$.

证明. 注意到 $\rho(f,p)\leqslant p$ 恒成立, 故只需说明 $\rho(f,p)\leqslant n$. 我们归纳地证明这一结论.

当 $n=1$ 时命题显然成立. 现设对于任何满足条件的 $f\in\mathbb{Z}[x]$ 且 $\deg f=n-1$ 均有 $\rho(f,p)\leqslant n-1$, 则对于某个 n 次多项式 f 而言, 一方面, 若 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 无解, 则 $\rho(f,p)=0\leqslant n$; 另一方面, 若 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 有解 x_0, 则 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 等价于 $f(x)-f(x_0)\equiv 0\,(\mathrm{mod}\,m)$. 注意到 $f(x)-f(x_0)=\sum\limits_{k=1}^{n}a_k(x^k-x_0^k)=(x-x_0)g(x)$, 其中 $g(x)=a_nx^{n-1}+\cdots\in\mathbb{Z}[x]$ 且首项系数与 p 互素, 故 $f(x)\equiv 0\,(\mathrm{mod}\,m)$ 等价于 $x\equiv x_0\,(\mathrm{mod}\,m)$ 或 $g(x)\equiv 0\,(\mathrm{mod}\,m)$, 进而由归纳假设可得 $\rho(f,p)\leqslant 1+\rho(g,p)\leqslant n$.

这样, 我们便证明了这一结论. □

注记 4.3.1. 对本定理而言, 模为素数这一条件是不可缺的 (见**例 4.1.1**).

定理 4.3.2 (Wilson)**.** 设 $n\in\mathbb{Z}_{>1}$, 则 n 是素数的充要条件为 $(n-1)!\equiv -1\,(\mathrm{mod}\,n)$.

证明. *充分性*. 若 $(n-1)!\equiv -1\,(\mathrm{mod}\,n)$, 则对于 n 的任一满足 $m<n$ 的因子 m 而言, 均有 $-1\equiv(n-1)!\equiv 0\,(\mathrm{mod}\,m)$, 从而 $m=1$, 这表明 n 是素数.

必要性. 现设 $n=p$ 是一个素数. 当 $p=2$ 时命题显然成立, 下设 $p\geqslant 3$. 记

$$f(x):=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1,$$

由 Fermat 小定理知 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 共有 $p-1$ 个解, 即 $x\equiv k\,(\mathrm{mod}\,p)$ $(k=1,\cdots,p-1)$. 注意到 $\deg f<p-1$, 故由**定理 4.3.1** 知 f 的每个系数均被 p 整除. 特别地, p 整除 f 的常数项, 即 $(p-1)!\equiv -1\,(\mathrm{mod}\,p)$. □

推论 4.3.1. 对任意整数 $1\leqslant k\leqslant p-1$ (p 为素数) 都有 $(k-1)!(p-k)!\equiv(-1)^k\,(\mathrm{mod}\,p)$.

证明. 当 $k=1$ 时这即为 Wilson 定理, 下面设 $k\geqslant 2$. 注意到 $j\equiv -(p-j)\,(\mathrm{mod}\,p)$, 故 $(k-1)!(p-k)!\equiv(p-k)!(-1)^{k-1}\prod\limits_{j=1}^{k-1}(p-1)!\equiv(-1)^k\,(\mathrm{mod}\,p)$. □

推论 4.3.2. 设素数 $p>3$, 正整数 $k<p-1$, 证明 $\displaystyle\sum_{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant p-1}\prod_{j=1}^{k}i_j\equiv 0\,(\mathrm{mod}\,p)$.

证明. 在 Wilson 定理的证明中我们证明了多项式 $(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1$ 的系数均为 p 的倍数, 而式

$$\sum_{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant p-1}\prod_{j=1}^{k}i_j$$

恰是此多项式的 x^{p-k-1} 项系数的绝对值, 因此 $\displaystyle\sum_{1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant p-1}\prod_{j=1}^{k}i_j\equiv 0\,(\mathrm{mod}\,p)$. □

命题 4.3.1. 设 p 是奇素数, 则同余方程 $x^2+1\equiv 0\,(\mathrm{mod}\,p)$ 有解当且仅当 $p\equiv 1\,(\mathrm{mod}\,4)$.

证明. 充分性. 若 $p\equiv 1\,(\mathrm{mod}\,4)$, 则由 Wilson 定理及 $p-k\equiv -k\,(\mathrm{mod}\,p)$ 得

$$(-1)\equiv(p-1)!\equiv(-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2\,(\mathrm{mod}\,p),$$

从而 $\left(\dfrac{p-1}{2}\right)!$ 是同余方程 $x^2+1\equiv 0\,(\mathrm{mod}\,p)$ 的一个解.

必要性. 假设方程 $x^2+1\equiv 0\,(\mathrm{mod}\,p)$ 有解 x_0, 则 $p\nmid x_0$, 于是由 Fermat 小定理得

$$1\equiv x_0^{p-1}\equiv(x_0^2)^{(p-1)/2}\equiv(-1)^{(p-1)/2}\,(\mathrm{mod}\,p),$$

由于 p 是奇素数, 故必有 $2\left|\dfrac{p-1}{2}\right.$, 即 $p\equiv 1\,(\mathrm{mod}\,4)$. □

推论 4.3.3. 设 p 为素数, 记 $\rho(p)$ 表示同余方程 $x^2+1\equiv 0\,(\mathrm{mod}\,p)$ 的解数, 则

$$\rho(p)=\begin{cases}1, & p=2\\ 2, & p\equiv 1\,(\mathrm{mod}\,4),\\ 0, & p\equiv 3\,(\mathrm{mod}\,4).\end{cases}$$

命题 4.3.2. 存在无穷多个形如 $4n+1$ 的素数.

证明. 反设仅有有限多个形如 $4n+1$ 的素数, 记为 $p_1,\cdots,p_r$. 现令 $N:=(2p_1\cdots p_r)^2+1$, 由**命题 4.3.1** 知 N 的素因子均应形如 $4n+1$, 但 N 的素因子不可能为 $p_1,\cdots,p_r$, 从而得出矛盾. □

设 $q\neq 0$, 我们称集合 $\{a+qn:n\in\mathbb{Z}\}$ 为**算术级数**. 作为结论 $\lim\limits_{x\to+\infty}\pi(x)=+\infty$ 的推广, 人们希望了解 $(a,q)=1$ 时上述算术级数是否也都包含无穷多个素数. Euler 先在 $a=1$ 时证明了该算术级数中有无穷多个素数, 而 Dirichlet 于 1837 年证明了一般情形.

下面讨论 $\alpha>1$ 的情形. 注意到 $f(x_0)\equiv 0\,(\mathrm{mod}\,p^\alpha)$ 时必有 $f(x_0)\equiv 0\,(\mathrm{mod}\,p^{\alpha-1})$, 故我们可以从 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 的解出发通过逐步提高 p 的次幂来求解. 这一做法称为 Hensel 引理, 其本质上可以视为求解方程根的 Newton 法的同余版本.

命题 4.3.3 (Hensel 引理)**.** 设 $\alpha \geqslant 1$, p 为素数, $f \in \mathbb{Z}[x]$ 且 x_0 是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的一个解. 以 ρ 表示 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的满足 $x \equiv x_0 \pmod{p^\alpha}$ 的解的个数.

(1) 若 $f'(x_0) \not\equiv 0 \pmod{p}$, 则 $\rho = 1$ 且这一解由下式给出:

$$x \equiv x_0 + \ell p^\alpha \pmod{p^{\alpha+1}}, \qquad \text{其中} \quad f'(x_0)\ell \equiv -\frac{f(x_0)}{p} \pmod{p};$$

(2) 若 $f'(x_0) \equiv 0 \pmod{p}$ 且 $f(x_0) \not\equiv 0 \pmod{p^{\alpha+1}}$, 则 $\rho = 0$;

(3) 若 $f'(x_0) \equiv 0 \pmod{p}$ 且 $f(x_0) \equiv 0 \pmod{p^{\alpha+1}}$, 则 $\rho = p$ 且这 p 个解由下式给出

$$x \equiv x_0 + \ell p^\alpha, \qquad \ell = 0, 1, \cdots, p-1.$$

证明. 不妨设 $f := \sum_{k=1}^{n} a_k x^k$, $\deg f = n$. 由 Taylor 公式, 有

$$f(x_0 + \ell p^\alpha) = f(x_0) + f'(x_0)\ell p^\alpha + \frac{f''(x_0)}{2!}\ell^2 p^{2\alpha} + \cdots + \frac{f^{(n)}(x_0)}{n!}\ell^n p^{n\alpha},$$

因此 $x_0 + \ell p^\alpha$ 满足方程 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 当且仅当

$$f(x_0) + f'(x_0)\ell p^\alpha \equiv 0 \pmod{p^{\alpha+1}}.$$

注意到 $p^\alpha \mid f(x_0)$, 故上式的同余方程等价于

$$f'(x_0)\ell \equiv -\frac{f(x_0)}{p} \pmod{p},$$

(1) 若 $f'(x_0) \not\equiv 0 \pmod{p}$, 则显然 $\rho = 1$, 且这一解由下式给出:

$$x \equiv x_0 + \ell p^\alpha \pmod{p^{\alpha+1}}, \qquad \text{其中} \quad f'(x_0)\ell \equiv -\frac{f(x_0)}{p} \pmod{p};$$

(2) 若 $f'(x_0) \equiv 0 \pmod{p}$ 且 $f(x_0) \not\equiv 0 \pmod{p^{\alpha+1}}$, 则 $\rho = 0$;

(3) 若 $f'(x_0) \equiv 0 \pmod{p}$ 且 $f(x_0) \equiv 0 \pmod{p^{\alpha+1}}$, 则 $\rho = p$ 且这 p 个解由下式给出

$$x \equiv x_0 + \ell p^\alpha, \qquad \ell = 0, 1, \cdots, p-1.$$

这样, 我们便证明了这一结论. □

例 4.3.1. 解同余方程 $x^4 + 7x + 4 \equiv 0 \pmod{27}$.

解. 记 $f(x) := x^4 + 7x + 4$, 则同余方程 $f(x) \equiv 0 \pmod{3}$ 有唯一解 $x \equiv 1 \pmod{3}$ 且 $f'(1) = 11 \not\equiv 0 \pmod{3}$, 于是由 Hensel 引理知方程 $f(x) \equiv 0 \pmod{9}$ 有唯一解 $1 + 3\ell \pmod{9}$, 其中 $11\ell \equiv -4 \pmod{3}$, 于是取 $\ell = 1$, 即 $f(x) \equiv 0 \pmod{9}$ 有唯一解 $x \equiv 4 \pmod{9}$. 注意到 $f'(4) = 263 \not\equiv 0 \pmod{3}$, 故再次利用 Hensel 引理知 $f(x) \equiv 0 \pmod{27}$ 有唯一解 $4 + 9k \pmod{27}$, 其中 $263k \equiv -32 \pmod{3}$, 于是可取 $k = 2$, 因此原同余方程有唯一解 $x \equiv 22 \pmod{27}$. □

推论 4.3.4. 设 $f \in \mathbb{Z}[x]$, p 为素数. 若 $f(x) \equiv 0 \pmod{p}$ 与 $f'(x) \equiv 0 \pmod{p}$ 无公共解, 则对任意的 $\alpha \geqslant 1$ 有 $\rho(f, p^\alpha) = \rho(f, p)$.

证明. 只需对任意的 $\alpha \geqslant 1$ 证明 $\rho(f, p^{\alpha+1}) = \rho(f, p^\alpha)$ 即可. 一方面, $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的解必是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解; 另一方面, $f(x) \equiv 0 \pmod{p^\alpha}$ 的任意解 $x_0 \pmod{p^\alpha}$ 均满足 $f(x_0) \equiv 0 \pmod{p}$, 进而由条件知 $p \nmid f'(x_0)$, 因此由 Hensel 引理知从 x_0 出发可以得到 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的一个解. 因此, $\rho(f, p^{\alpha+1}) = \rho(f, p^\alpha)$. □

§4.4　表素数为两整数的平方和

作为**命题 4.3.1** 的一个应用, 我们来研究哪些整数可以表示为两个整数的平方和的形式. 首先从素数开始讨论. 又注意到 $2 = 1^2 + 1^2$, 所以我们只需考虑不小于 3 的素数.

定理 4.4.1. 设 p 是奇素数, 则 p 可表为两整数平方和的充要条件是 $p \equiv 1 \pmod{4}$.

证明. 必要性. 若存在 $x, y \in \mathbb{Z}$ 使得 $x^2 + y^2 = p$, 则 $p \nmid xy$ 且 $x^2 \equiv -y^2 \pmod{p}$, 进而有 $(x\bar{y})^2 \equiv -1 \pmod{p}$, 于是由命题 4.3.1 知 $p \equiv 1 \pmod{4}$.

充分性. 下证每个满足 $p \equiv 1 \pmod{4}$ 的素数 p 均为两个整数的平方和. 由条件知存在 $\ell \in \mathbb{Z}$ 使得 $\ell^2 \equiv -1 \pmod{p}$, 现考虑满足 $0 \leqslant x, y \leqslant \sqrt{p}$ 的有序对 (x, y), 这样的有序对的个数为 $(\lfloor\sqrt{p}\rfloor + 1)^2 > p$, 由抽屉原理知必存在有序对 (x_1, y_1) 与 (x_2, y_2) 使得

$$x_1 - \ell y_1 \equiv x_2 - \ell y_2 \pmod{p}.$$

若记 $x := |x_1 - x_2|$, $y := |y_1 - y_2|$, 则有 $x, y \in \left[0, \sqrt{p}\right]$ 且 $x \equiv \pm \ell y \pmod{p}$. 于是

$$0 < x^2 + y^2 < 2p, \qquad x^2 + y^2 = x^2 - (\ell y)^2 \equiv 0 \pmod{p},$$

因此必有 $x^2 + y^2 = p$. □

当 $p \equiv 1 \pmod{4}$ 时, 上述存在性的证明中并没有给出 p 表为两整数平方和的具体表达式. 事实上我们可以说明, 这种表示方式在不考虑 x 与 y 的顺序和符号的前提下是唯一的 (见**例 4.4.1**).

定理 4.4.2. 设 $n \in \mathbb{Z}_{>0}$ 且 $n = n_1^2 n_2$, 其中 n_2 为无平方因子数, 则 n 可表为两整数平方和的充要条件是 n_2 的任意奇素因子 $q \equiv 1 \pmod{4}$.

证明. 必要性. 设 p 是奇素数且 $p \mid n_2$, 由于 n 可表为两整数的平方和, 故存在 $x, y \in \mathbb{Z}$ 使得 $x^2 + y^2 = n$. 若记 $d := (x, y)$, 则 $d^2 \mid n$, 而又由 n_2 是无平方因子数可得 $d \mid n_1$.

现记 $x = dx_0$, $y = dy_0$, $n_1 = dm$, 则 $(x_0, y_0) = 1$ 且 $x_0^2 + y_0^2 = m^2 n_2$. 因此 $p \nmid x_0 y_0$ 且 $x_0^2 \equiv -y_0^2 \pmod{p}$, 即 -1 是模 p 的二次剩余, 进而有 $p \equiv 1 \pmod{4}$.

充分性. 现设 n_2 的任意奇素因子 $q \equiv 1 \pmod{4}$, 不难验证

$$(u^2 + v^2)(s^2 + t^2) = (us + vt)^2 + (ut - vs)^2,$$

这意味着可表为两整数平方和的整数的乘积也可写成两整数的平方和, 结合 $2 = 1^2 + 1^2$ 及**定理 4.4.1** 知 n_2 可表为两整数的平方和, 从而 n 可表为两整数的平方和. □

例 4.4.1. 设素数 $p \equiv 1 \pmod{4}$, 证明方程 $x^2 + y^2 = p$ $(0 \leqslant x \leqslant y)$ 有唯一解.

证明. 只需证唯一性. 设 $0 < x_1 < y_1 < \sqrt{p}$, $0 < x_2 < y_2 < \sqrt{p}$ 满足

$$x_1^2 + y_1^2 = x_2^2 + y_2^2 = p,$$

则 $p \nmid x_1 y_1 x_2 y_2$ 且 $(x_1 \bar{y_1})^2 \equiv (x_2 \bar{y_2})^2 \equiv 1 \pmod{p}$, 于是

$$x_1 \bar{y_1} \equiv \pm x_2 \bar{y_2} \pmod{p}.$$

首先证明上式中的负号不可能成立. 反设 $x_1 \bar{y_1} + x_2 \bar{y_2} \equiv 0 \pmod{p}$, 则由

$$0 < x_1 y_2 + y_1 x_2 < 2p$$

知必有 $x_1 y_2 + y_1 x_2 = p$, 于是 $(x_1 x_2 - y_1 y_2)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) - (x_1 y_2 + y_1 x_2)^2 = 0$, 这与条件矛盾. 因此有 $x_1 y_2 \equiv y_1 x_2 \pmod{p}$, 又由 $x_1 y_2, y_1 x_2 \in (0, p)$ 知 $x_1 y_2 = x_2 y_1$, 注意到 $(x_1, y_1) = (x_2, y_2) = 1$, 因此 $x_1 = x_2$, $y_1 = y_2$, 即原方程有唯一解. □

第五章　原根与指标

在 §3.2 中, 我们介绍了完全剩余系与简化剩余系, 前者的结构较为简单, 我们可以用简洁且规律的方式将其表示出来; 但后者结构较为复杂. 对于一般的 $m \in \mathbb{Z}$, 我们希望给出简化剩余系的一个较简便的表示方法, 以便更好地了解其结构并进行应用. 本章的目的便是来完成这一工作.

§5.1　基本概念

由 Euler 定理, 若 $(a,m)=1$ 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$. 这保证了下述定义的合理性.

定义 5.1.1. 设 $m \in \mathbb{Z}_{>1}$ 且 $(a,m)=1$. 我们称使得同余式 $a^{\gamma} \equiv 1 \pmod{m}$ 成立的最小正整数 γ 为 a 对模 m 的**阶** (或**指数**), 记作 $\delta_m(a)$. 特别地, 如果 $\delta_m(a)=\varphi(m)$, 则称 a 是模 m 的一个**原根**.

下面我们给出阶和原根的一些基本性质.

命题 5.1.1. 设 $(a,m)=1$.

(1) 若 $a \equiv b \pmod{m}$, 则 $\delta_m(a)=\delta_m(b)$;

(2) 若 $a^k \equiv a^{\ell} \pmod{m}$, 则 $k \equiv \ell \pmod{m}$. 特别地, $\delta_m(a) \mid \varphi(m)$;

(3) a^j $(j=0,1,\cdots,\delta_m(a)-1)$ 模 m 两两不同余. 特别地, a 是模 m 的原根当且仅当 $\left\{a^0,a^1,\cdots,a^{\varphi(m)-1}\right\}$ 为模 m 的一个简化剩余系;

(4) a 是模 m 的原根当且仅当对任意的素数 $p \mid \varphi(m)$ 都有 $a^{\varphi(m)/p} \not\equiv 1 \pmod{m}$;

(5) 对任意的 $k \in \mathbb{Z}_{\geqslant 0}$ 都有 $\delta_m(a^k)=\dfrac{\delta_m(a)}{(\delta_m(a),k)}$.

证明. (1) 由条件知 $a^{\gamma} \equiv 1 \pmod{m}$ 当且仅当 $b^{\gamma} \equiv 1 \pmod{m}$, 故 $\delta_m(a)=\delta_m(b)$.

(2) 由带余除法知存在 $q,r \in \mathbb{Z}$ 使得 $k-\ell=q\delta_m(a)+r$ (其中 $0 \leqslant r < \delta_m(a)$). 因为 $a^k \equiv a^{\ell} \pmod{m}$, 所以 $a^r \equiv a^{q\delta_m(a)+r} \equiv a^{k-\ell} \equiv 1 \pmod{m}$, 由 $\delta_m(a)$ 的最小性知 $r=0$, 即 $\delta_m(a) \mid k-\ell$. 特别地, 由 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 知 $\delta_m(a) \mid \varphi(m)$.

(3) 可由 (2) 直接推出.

(4) 一方面, 若 a 是模 m 的原根, 则 $\delta_m(a)=\varphi(m)$, 于是由 $\delta_m(a)$ 的最小性知任意的素数 $p\mid\varphi(m)$ 均有 $a^{\varphi(m)/p}\not\equiv 1\,(\mathrm{mod}\,m)$; 另一方面, 若 a 不是模 m 的原根, 则 $\delta_m(a)<\varphi(m)$, 注意到由 (2) 知 $\delta_m(a)\mid\varphi(m)$, 所以存在素数 p 使得 $p\left|\dfrac{\varphi(m)}{\delta_m(a)}\right.$, 这一素数 p 满足 $a^{\varphi(m)/p}\equiv 1\,(\mathrm{mod}\,m)$.

(5) 记 $\delta:=\delta_m(a)$, $\delta':=\delta_m(a^k)$. 由定义知 $(a^k)^{\delta'}\equiv 1\,(\mathrm{mod}\,m)$, 于是由 (2) 知 $\delta\mid k\delta'$, 从而 $\dfrac{\delta}{(\delta,k)}\left|\delta'\right.$. 此外, 由

$$a^{k\delta/(\delta,k)}\equiv(a^{\delta})^{k/(\delta,k)}\equiv 1\,(\mathrm{mod}\,m)$$

知 $\delta'\left|\dfrac{\delta}{(\delta,k)}\right.$, 从而 $\delta'=\dfrac{\delta}{(\delta,k)}$. □

例 5.1.1. 由 $3^8\not\equiv 1\,(\mathrm{mod}\,17)$ 知 3 是模 17 的原根; 由 $2^2,2^5\not\equiv 1\,(\mathrm{mod}\,11)$ 知 2 是模 11 的原根. □

例 5.1.2. 在前面我们引入了 Fermat 数 $F_n=2^{2^n}$ $(n\geqslant 0)$, Fermat 验证了当 $0\leqslant n\leqslant 4$ 时 F_n 均为素数并猜测所有的 F_n 均为素数, 但是 Euler 于 1732 年发现了 $641\mid F_5$, 这便推翻了 Fermat 的猜想 (而实际上更糟糕的是, 到目前为止人们已经验证了自 F_0 到 F_{310} 的所有 Fermat 数, 除 $0\leqslant n\leqslant 4$ 以外尚未发现其它的 Fermat 数 F_n 是素数. 因此目前人们猜想, 自 F_5 以后的所有 Fermat 数均为合数). 下面我们来看看 Euler 是如何找出这一整除关系式的.

设 p 是 F_5 的一个素因子. 因为 $2^{2^5}\equiv -1\,(\mathrm{mod}\,p)$, 所以 $2^{2^6}\equiv 1\,(\mathrm{mod}\,p)$, 这表明 $\delta_p(2)=2^6=64$, 而 $\delta_p(2)\mid\varphi(p)=p-1$, 所以 p 是形如 $64k+1$ 的素数 (事实上, 还可以进一步证明 p 是形如 $128k+1$ 的素数), 前几个这样的素数依次为 193, 257, 449, 577, 641, 逐一验证后发现 $641\mid F_5$.

例 5.1.3. 设 p 是素数, 证明 Mersenne 数 2^p-1 的素因子均大于 p, 从而得到存在无穷多个素数.

证明. 若奇素数 $q\mid 2^p-1$, 则 $2^p\equiv 1\,(\mathrm{mod}\,q)$, 于是 $\delta_q(2)\mid p$ 从而 $\delta_q(2)=p$ 并且 $\delta_q(2)\mid\varphi(q)=q-1$, 即 $p\mid q-1$, 故必有 $q>p$. □

例 5.1.4. 设模 m 有原根, 证明在模 m 的一个简化剩余系中原根共有 $\varphi(\varphi(m))$ 个.

证明. 设 g 是模 m 的一个原根, 则 $\{g^j:1\leqslant j\leqslant\varphi(m)\}$ 是模 m 的一个简化剩余系, 并且由命题 5.1.1 (5) 知 g^j 是模 m 的原根当且仅当 $(j,\varphi(m))=1$, 因此模 m 的原根共有 $\varphi(\varphi(m))$ 个. □

根据**命题 5.1.1 (3)**, 我们可以给出如下定义.

定义 5.1.2. 设 g 是模 m 的原根, $(a,m)=1$. 若 $a\equiv g^{\gamma}\,(\mathrm{mod}\,m)$ $(0\leqslant\gamma\leqslant\varphi(m))$, 则称 γ 为 a 对模 m 以 g 为底的**指标**, 记作 $\mathrm{ind}_g a$ 或 $\mathrm{ind}\,a$.

指标有如下类似于对数函数的性质.

命题 5.1.2. 设 g,h 是模 m 的原根, 我们有

(1) 若 $(a_1,\cdots,a_n,m)=1$, 则 $\mathrm{ind}_g(a_1\cdots a_n)\equiv\mathrm{ind}_g a_1+\cdots+\mathrm{ind}_g a_n\,(\mathrm{mod}\,\varphi(m))$;

(2) (换底公式) 若 $(a,m)=1$, 则 $\mathrm{ind}_g a\equiv\mathrm{ind}_g h\cdot\mathrm{ind}_h a\,(\mathrm{mod}\,\varphi(m))$.

证明. 这两个结论分别可由

$$g^{\mathrm{ind}_g(a_1\cdots a_n)}\equiv a_1\cdots a_n\equiv g^{\mathrm{ind}_g a_1}\cdot\cdots\cdot g^{\mathrm{ind}_g a_n}\,(\mathrm{mod}\,m)$$

以及

$$g^{\mathrm{ind}_g a}\equiv a\equiv h^{\mathrm{ind}_h a}\equiv(g^{\mathrm{ind}_g h})^{\mathrm{ind}_h a}=g^{\mathrm{ind}_g h\cdot\mathrm{ind}_h a}\,(\mathrm{mod}\,m)$$

并结合**命题 5.1.1 (2)** 得到. □

§5.2 原根存在的条件

本节的目的是证明下述定理:

定理 5.2.1. 模 m 有原根当且仅当 m 是如下形式的数之一

$$1,\ \ 2,\ \ 4,\ \ p^{\alpha},\ \ 2p^{\alpha},\tag{*}$$

其中 p 为奇素数, $\alpha\geqslant 1$.

证明的大致思路和步骤如下:

(1) 模 p 存在原根 $\Rightarrow$ 模 p^{α} 存在原根 $\Rightarrow$ 模 $2p^{\alpha}$ 存在原根.

(2) 当 m 不是 (*) 式中的数值时, m 没有原根.

我们首先通过以下几个命题来证明其充分性.

命题 5.2.1. 设 p 为素数且 $d\mid p-1$, 则在模 p 的一个简化剩余系中阶为 d 的元素共有 $\varphi(d)$ 个.

证明. 记 $S_d:=\{1\leqslant a\leqslant p-1:\delta_p(a)=d\}$, $f(d):=|S_d|$, 则 $\sum\limits_{d|p-1}f(d)=p-1$. 于是有

$$\sum_{d|p-1}(\varphi(d)-f(d))=0.$$

因此只需证明对任意的 $d \mid p-1$ 都有 $f(d) \leqslant \varphi(d)$ 即可. 不妨设 $f(d) \geqslant 1$, 则存在 $a \in S_d$, 由 S_d 的定义知 a^j $(j = 1, \cdots, d)$ 对于模 p 两两不同余且它们都是 $x^d \equiv 1 \pmod p$ 的根. 注意到由 Lagrange 定理知这一同余方程至多有 d 个根, 所以这些 a^j 是这一方程的全部解. 则对任意的 $y \in S_d$, 必存在 $1 \leqslant j_0 \leqslant d$ 使得 $y \equiv a^{j_0} \pmod p$. 又因为 y 的阶也是 d, 故由**命题 5.1.1 (5)** 知 $(j_0, d) = 1$, 这就证明了 $f(d) \leqslant \varphi(d)$. □

在**命题 5.2.1** 中取 $d = p - 1$ 便可得到下述推论.

推论 5.2.1. 若 p 为素数, 则模 p 的原根共有 $\varphi(p-1)$ 个.

下面我们要对奇素数 p 证明模 p^α 的原根的存在性. 在此之前, 首先注意到 g 是模 p^α 的原根可以推出 g 必为模 $p^{\alpha-1}$ 的原根. 事实上, 若以 d 表示 g 对模 $p^{\alpha-1}$ 的阶, 则 $d \mid \varphi(p^{\alpha-1})$ 且 $g^d \equiv 1 \pmod{p^{\alpha-1}}$. 若记 $g^d := 1 + kp^{\alpha-1}$, 则由二项式定理知

$$\begin{aligned} g^{dp} &= (1 + kp^{\alpha-1}) \\ &= 1 + \binom{p}{1} kp^{\alpha-1} + \binom{p}{2} (kp^{\alpha-1})^2 + \cdots + \binom{p}{p} (kp^{\alpha-1})^p \equiv 1 \pmod{p^\alpha}, \end{aligned}$$

于是由 g 是模 p^α 的原根可推出 $\varphi(p^\alpha) \mid dp$, 此即 $\varphi(p^{\alpha-1}) \mid d$, 结合 $d \mid \varphi(p^{\alpha-1})$ 便得 $d = \varphi(p^{\alpha-1})$. 因此, 我们可以从模 p 的原根中寻找模 p^α 的原根.

命题 5.2.2. 设 p 为奇素数且 $\alpha \geqslant 1$, 则模 p^α 的原根存在.

证明. 设 g 是模 p 的一个原根. 我们首先证明 g 和 $g + p$ 中至少有一个是模 p^2 的原根. 记 g 对模 p^2 的阶为 d, 则 $d \mid \varphi(p^2) = p(p-1)$. 又由于 $g^d \equiv 1 \pmod{p^2}$, 从而 $g^d \equiv 1 \pmod p$, 故有 $\varphi(p) \mid d$. 因此 $d = p(p-1)$ 或 $d = p - 1$. 若前者成立, 则 g 是模 p^2 的原根. 现假设 $d = p - 1$, 我们来证明 $g + p$ 是 p^2 的原根. 由于 $g + p$ 也是模 p 的原根, 故类似可证 $g + p$ 对模 p^2 的阶为 $p(p-1)$ 或 $p - 1$, 由于 $g^{p-1} \equiv 1 \pmod{p^2}$, 故由二项式定理知

$$(g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2} p + \binom{p-1}{2} g^{p-3} p^2 + \cdots \equiv 1 - pg^{p-2} \pmod{p^2}.$$

因此 $g + p$ 对模 p^2 的阶为 $p(p-1)$, 从而它是模 p^2 的原根.

接下来我们用数学归纳法证明: 若 h 是模 p^2 的原根, 则它必是模 p^α $(\forall\, \alpha \geqslant 2)$ 的原根. 假设对某个 $\alpha \geqslant 2$ 而言, h 是模 p^α 的原根, 并以 d 表示 h 对模 $p^{\alpha+1}$ 的阶, 则 $\varphi(p^\alpha) \mid d$ 且 $d \mid \varphi(p^{\alpha+1})$, 从而 $d = p^{\alpha-1}(p-1)$ 或 $d = p^\alpha(p-1)$. 为了证明 h 是模 $p^{\alpha+1}$ 的原根, 只需证明 $d \neq p^{\alpha-1}(p-1)$, 这等价于

$$h^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}, \tag{\#}$$

由 Euler 定理可知 $h^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^{\alpha-1}}$, 故存在 $k \in \mathbb{Z}$ 使得 $h^{p^{\alpha-2}(p-1)} = 1 + kp^{\alpha-1}$. 注意到 h 是模 p^α 的原根, 所以 $h^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$, 这表明 $(k,p) = 1$. 此外,

$$h^{p^{\alpha-1}(p-1)} = (1+kp^{\alpha-1})^p = 1 + kp^\alpha + \binom{p}{2}(kp^{\alpha-1})^2 + \cdots \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}},$$

后一步得自 $2\alpha - 1 \geqslant \alpha + 1$ ($\alpha \geqslant 2$), 再由 $(k,p) = 1$ 即得 (#). □

命题 5.2.3. 设 p 为奇素数且 $\alpha \geqslant 1$, 则模 $2p^\alpha$ 的原根存在.

证明. 设 g 是模 p^α 的原根, 则 $g + p^\alpha$ 也是模 p^α 的原根且 g 与 $g + p^\alpha$ 中必有一个是奇数, 我们记为 h. 下证 h 是模 $2p^\alpha$ 的原根. 首先, $(h, 2p^\alpha) = 1$. 其次, 若以 d 表示 h 对模 $2p^\alpha$ 的阶, 则 $d \mid \varphi(2p^\alpha)$. 此外, 由 h 是模 p^α 的原根知 $\varphi(p^\alpha) \mid d$, 而注意到 $\varphi(2p^\alpha) = \varphi(p^\alpha)$, 故 $d = \varphi(2p^\alpha)$, 从而命题得证. □

由于当 $m = 1, 2, 4$ 时模 m 的原根显然存在, 故结合**推论 5.2.1** 和**命题 5.2.2**, **5.2.3**, 我们证明了**定理 5.2.1** 的充分性. 下面来证明这一定理的必要性. 为此, 我们先证明下述引理.

引理 5.2.1. 设 $m = rs$, 其中 $r, s > 2$ 且 $(r,s) = 1$, 则模 m 没有原根.

证明. 由 $(r,s) = 1$ 知 $\varphi(m) = \varphi(r)\varphi(s)$. 由于 r, $s > 2$, 故由**推论 3.3.1** 知 $\varphi(r)$, $\varphi(s)$ 均为偶数, 从而 $4 \mid \varphi(m)$. 现记 $d := \varphi(m)/2$, 则 $\varphi(r)$ 与 $\varphi(s)$ 均为 d 的因子, 故对任意的 $(a,m) = 1$ 都有 $a^d \equiv 1 \pmod{r}$ 且 $a^d \equiv 1 \pmod{s}$, 从而 $a^d \equiv 1 \pmod{m}$, 这表明 a 不是模 m 的原根. □

定理 5.2.1 必要性的证明. 若 $m \neq 1, 2, 4, p^\alpha, 2p^\alpha$, 则只可能有如下 3 种情形:

(i) $m = 2^\alpha$, 其中 $\alpha \geqslant 3$;

(ii) $m = 2^\alpha p^\beta$, 其中 p 是奇素数且 $\alpha \geqslant 2$, $\beta \geqslant 1$;

(iii) m 至少有 2 个奇素因子.

其中, 对于后两种情形, 我们可利用**引理 5.2.1** 推知模 m 没有原根, 下面考虑情形 (i). 我们来对任意的奇数 a 证明 $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$, 由此便得模 2^α 没有原根. 下面利用数学归纳法证明这一结论. 当 $\alpha = 3$ 时结论显然成立, 现设 $a^{2^{\alpha-2}} = 1 + 2^\alpha k$ ($k \in \mathbb{Z}$), 于是

$$a^{2^{\alpha-1}} = (1 + 2^\alpha k)^2 = 1 + 2^{\alpha+1}k + 2^{2\alpha}k^2 \equiv 1 \pmod{2^{\alpha+1}},$$

这样, 我们便证明了这一结论. □

§5.3　指标组

由**命题 5.1.1 (2)** 知, 若模 m 的原根存在, 则其简化剩余系可用原根的幂表示出来, 这无疑是非常方便的. 因此, 当原根不存在时, 我们也希望能对其简化剩余系作出类似的表示. 为此, 我们引入指标组的概念.

引理 5.3.1. $\forall n \geqslant \mathbb{Z}_{\geqslant 0}$, 都有 $2^{n+2} \parallel 5^{2^n} - 1$.

证明. 我们利用数学归纳法来证明这一结论. $n = 0$ 时命题显然成立, 现设命题对 n 成立, 即 $2^{n+2} \parallel 5^{2^n} - 1$, 结合 $2 \parallel 5^{2^n} + 1$ (这可由 $5^{2^n} \equiv 1 \pmod 4$ 推知) 得 $2^{n+3} \parallel 5^{2^{n+1}} - 1$. 这样, 我们便证明了这一结论. □

命题 5.3.1. 若 $\alpha \geqslant 3$, 则

$$\left\{\pm 5^j : 0 \leqslant j < 2^{\alpha-2}\right\}$$

是模 2^α 的一个简化剩余系.

证明. 用 d 表示 5 对于模 2^α 的阶, 则 $d \mid \varphi(2^\alpha) = 2^{\alpha-1}$, 故存在 $k \in \mathbb{Z}$ 使得 $d = 2^k$, 由上节讨论知 $k \leqslant \alpha - 2$; 另一方面, 由引理 5.3.1 知 $k \geqslant \alpha - 2$, 故必有 $k = \alpha - 2$. 这表明 5^j $(0 \leqslant j < 2^{\alpha-2})$ 关于模 2^α 两两不同余, 注意到 $5^j \equiv 1 \pmod 4$, 因此有

$$\left\{5^j : 0 \leqslant j < 2^{\alpha-2}\right\} = \left\{1 \leqslant n \leqslant 2^\alpha : n \equiv 1 \pmod 4\right\},$$

由此即得

$$\left\{-5^j : 0 \leqslant j < 2^{\alpha-2}\right\} = \left\{1 \leqslant n \leqslant 2^\alpha : n \equiv -1 \pmod 4\right\}.$$

这样, 我们便证明了这一结论. □

推论 5.3.1. 令

$$c_{-1} := \begin{cases} 1, & \alpha = 0, 1, \\ 2, & \alpha \geqslant 2, \end{cases} \quad \text{以及} \quad c_0 := \begin{cases} 1, & \alpha = 1, \\ 2^{\alpha-2}, & \alpha \geqslant 2. \end{cases}$$

则对模 2^α 的简化剩余系中的任一元素 a, 均存在唯一的一对整数 γ_{-1}, γ_0, 使得 $0 \leqslant \gamma_{-1} < c_{-1}$, $0 \leqslant \gamma_0 < c_0$ 以及

$$a \equiv (-1)^{\gamma_{-1}} 5^{\gamma_0} \pmod{2^\alpha}.$$

我们称 γ_{-1}, γ_0 是 a 对于模 2^α 的**指标组**.

下面我们来考虑一般合数模的情形.

定理 5.3.1. 设 $m=2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, 其中 $p_1,\cdots,p_r$ 为互不相同的奇素数. 又设 g_j 是模 $p_j^{\alpha_j}$ $(1\leqslant j\leqslant r)$ 的原根, c_{-1} 和 c_0 如上所定义, 则

$$\left\{(-1)^{\gamma_{-1}}5^{\gamma_0}M_0\overline{M_0}+\sum_{j=1}^{r}g_j^{\gamma_j}M_j\overline{M_j}:\begin{array}{l}0\leqslant\gamma_{-1}<c_{-1},\ \ 0\leqslant\gamma_0<c_0\\ 0\leqslant\gamma_j<\varphi(p_j^{\alpha_j})\ \ (1\leqslant j\leqslant r)\end{array}\right\}\tag{5.1}$$

是模 m 的一个简化剩余系, 其中 $M_0=\dfrac{m}{2^{\alpha}}$, $M_j=\dfrac{m}{p_j^{\alpha_j}}$ 且

$$M_0\overline{M_0}\equiv 1\,(\mathrm{mod}\,2^{\alpha}),\quad M_j\overline{M_j}\equiv 1\,(\mathrm{mod}\,p_j^{\alpha_j})\ \ (1\leqslant j\leqslant r).$$

证明. 假设存在两组数 $\gamma_{-1},\gamma_0,\cdots,\gamma_r$ 和 $\gamma'_{-1},\gamma'_0,\cdots,\gamma'_r$, 使得

$$(-1)^{\gamma_{-1}}5^{\gamma_0}M_0\overline{M_0}+\sum_{j=1}^{r}g_j^{\gamma_j}M_j\overline{M_j}\equiv(-1)^{\gamma'_{-1}}5^{\gamma'_0}M_0\overline{M_0}+\sum_{j=1}^{r}g_j^{\gamma'_j}M_j\overline{M_j}\,(\mathrm{mod}\,m),$$

则有

$$\begin{cases}(-1)^{\gamma_{-1}}5^{\gamma_0}\equiv(-1)^{\gamma'_{-1}}5^{\gamma'_0}\,(\mathrm{mod}\,2^{\alpha}),\\ g_1^{\gamma_1}\equiv g_1^{\gamma'_1}\,(\mathrm{mod}\,p_1^{\alpha_1}),\\ \cdots\cdots\cdots\cdots,\\ g_r^{\gamma_r}\equiv g_r^{\gamma'_r}\,(\mathrm{mod}\,p_r^{\alpha_r}).\end{cases}$$

于是由**推论 5.3.1** 及原根的定义知 $\gamma_j=\gamma'_j$ $(-1\leqslant j\leqslant r)$, 这表明式 (5.1) 集合中的元素关于模 m 两两不同余. 另一方面, 容易验证该集合中的元素均与 2^{α} 以及 $p_j^{\alpha_j}$ $(1\leqslant j\leqslant r)$ 互素, 从而与 m 互素, 且元素个数为 $c_{-1}c_0\varphi(p_1^{\alpha_1})\cdots\varphi(p_r^{\alpha_r})=\varphi(m)$. 因此 (5.1) 是模 m 的一个简化剩余系. □

定义 5.3.1. 在**定理 5.3.1** 的条件下, 若与 m 互素的整数 a 满足

$$a\equiv(-1)^{\gamma_{-1}}5^{\gamma_0}M_0\overline{M_0}+\sum_{j=1}^{r}g_j^{\gamma_j}M_j\overline{M_j}\,(\mathrm{mod}\,m),$$

其中 $0\leqslant\gamma_{-1}<c_{-1}$, $0\leqslant\gamma_0<c_0$, $0\leqslant\gamma_j<\varphi(p_j^{\alpha_j})$ $(1\leqslant j\leqslant r)$, 则称数组 $\gamma_{-1},\gamma_0,\cdots,\gamma_r$ 是 a 关于模 m 的**指标组**.

例 5.3.1. 沿用**定理 5.3.1** 中的记号, 并对 $-1\leqslant k\leqslant r$ 记

$$h_k:=(-1)^{\delta_{k,-1}}5^{\delta_{k,0}}M_0\overline{M_0}+\sum_{j=1}^{r}g_j^{\delta_{k,j}}M_j\overline{M_j},$$

其中 Kronecker δ 符号 $\delta_{k,\ell}$ 按下述方式定义:

$$\delta_{k,\ell}:=\begin{cases}1, & k=\ell,\\ 0, & k\neq\ell.\end{cases}$$

证明

$$\left\{ h_{-1}^{\gamma_{-1}} h_0^{\gamma_0} \cdots h_r^{\gamma_r} : \begin{array}{l} 0 \leqslant \gamma_{-1} < c_{-1},\ \ 0 \leqslant \gamma_0 < c_0 \\ 0 \leqslant \gamma_j < \varphi(p_j^{\alpha_j})\ \ (1 \leqslant j \leqslant r) \end{array} \right\} \tag{5.2}$$

是模 m 的一个简化剩余系.

证明. 首先, 若存在两组数 $\gamma_{-1}, \gamma_0, \cdots, \gamma_r$ 和 $\gamma'_{-1}, \gamma'_0, \cdots, \gamma'_r$, 使得

$$h_{-1}^{\gamma_{-1}} h_0^{\gamma_0} \cdots h_r^{\gamma_r} \equiv h_{-1}^{\gamma'_{-1}} h_0^{\gamma'_0} \cdots h_r^{\gamma'_r} \pmod{m},$$

则有

$$\begin{cases} (-1)^{\gamma_{-1}} 5^{\gamma_0} \equiv (-1)^{\gamma'_{-1}} 5^{\gamma'_0} \pmod{2^\alpha}, \\ g_1^{\gamma_1} \equiv g_1^{\gamma'_1} \pmod{p_1^{\alpha_1}}, \\ \cdots\cdots\cdots\cdots, \\ g_r^{\gamma_r} \equiv g_r^{\gamma'_r} \pmod{p_r^{\alpha_r}}. \end{cases}$$

于是推知 $\gamma_j = \gamma'_j$ $(-1 \leqslant j \leqslant r)$, 这表明 (5.2) 集合中的元素关于模 m 两两不同余. 其次, 不难验证该集合中的元素均与 2^α 以及 $p_j^{\alpha_j}$ $(1 \leqslant j \leqslant r)$ 互素, 从而与 m 互素, 并且元素个数为 $c_{-1}c_0\varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \varphi(m)$. 因此 (5.2) 是模 m 的一个简化剩余系. □

§5.4 n 次剩余

作为前两节结果的一个应用, 下面我们来讨论 n 次剩余.

定义 5.4.1. 设 $m \in \mathbb{Z}_{>0}$ 且 $(a, m) = 1$. 若同余方程

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

有解, 则称 a 是模 m 的一个 n **次剩余**. 反之, 则称 a 是模 m 的一个 n **次非剩余**.

设 $m = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, 其中 $p_1, \cdots, p_r$ 为互不相同的奇素数, 则同余方程 (*) 等价于

$$\begin{cases} x^n \equiv a \pmod{2^\alpha}, \\ x^n \equiv a \pmod{p_1^{\alpha_1}}, \\ \cdots\cdots\cdots\cdots \\ x^n \equiv a \pmod{p_r^{\alpha_r}}. \end{cases}$$

因此我们只需对模为素数幂的情形讨论同余方程 (*).

命题 5.4.1. 设模 m 有原根 g, $(a,m)=1$, 则 (*) 有解的充要条件是 $(n,\varphi(m)) \mid \mathrm{ind}_g a$. 并且, 在有解的情形下, (*) 恰有 $(n,\varphi(m))$ 个解.

证明. 记 $\mathrm{ind}_g x = y$, 则同余方程 (*) 等价于 $g^{ny} \equiv g^{\mathrm{ind}_g a} \pmod m$, 由**命题 5.1.1 (2)** 知其等价于 $ny \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$, 再由**命题 4.1.1** 即得结论. □

命题 5.4.2. 设 $m = 2^\alpha$ $(\alpha \geqslant 3)$, $a \equiv (-1)^{\gamma_{-1}} 5^{\gamma_0} \pmod{2^\alpha}$, 则当 $2 \nmid n$ 时 (*) 仅有一个解; 当 $2 \mid n$ 时, (*) 有解当且仅当 $\gamma_{-1} = 0$ 且 $(n, 2^{\alpha-2}) \mid \gamma_0$, 此时 (*) 恰有 $(n, 2^{\alpha-2})$ 个解.

证明. 令 $x \equiv (-1)^u 5^v \pmod{2^\alpha}$, 则由**推论 5.3.1** 知 (*) 等价于

$$nu \equiv \gamma_{-1} \pmod 2 \qquad \text{且} \qquad nv \equiv \gamma_0 \pmod{2^{\alpha-2}},$$

从而可由**命题 4.1.1** 推知结论. □

例 5.4.1. 解同余方程 $x^4 \equiv 13 \pmod{17}$.

解. 我们已在**例 5.1.1** 中验证 3 是模 17 的一个原根, 并且有 $\mathrm{ind}_3 13 = 4$. 记 $\mathrm{ind}_3 x = y$, 则原同余方程等价于 $4y \equiv 4 \pmod{16}$, 因为这一方程有 4 个解 $y \equiv 1, 5, 9, 13 \pmod{16}$, 所以原同余方程有 4 个解 $x \equiv 3^1, 3^5, 3^9, 3^{13} \pmod{17}$, 即 $x \equiv 3, 5, 12, 14 \pmod{17}$. □

例 5.4.2. 作为二次剩余的一个应用, 我们来看看 C.F.Gauss 是如何证明 Wilson 定理的.

不妨设 $p \geqslant 5$ 是奇素数, 若 $(a,p)=1$, 则 $a \equiv \bar{a} \pmod p$ 当且仅当 $a^2 \equiv 1 \pmod p$, 由**命题 5.4.1** 知该方程只有 2 个解, 即 $a \equiv \pm 1 \pmod p$, 因此区间 $[2, p-2]$ 中的每个整数 b 都不与 $\bar{b}$ 关于模 p 同余. 而注意到 $b\bar{b} \equiv 1 \pmod p$, 所以通过将 b 与 $\bar{b}$ 两两配对可得 $2 \cdots (p-2) \equiv 1 \pmod p$, 进而有 $(p-1)! \equiv -1 \pmod p$.

利用类似的方法, Gauss 将 Wilson 定理推广至更一般的形式:

$$\prod_{\substack{m \leqslant n \\ (m,n)=1}} m \equiv \begin{cases} -1 \pmod n, & \text{模 } n \text{ 有原根}, \\ 1 \pmod n, & \text{模 } n \text{ 没有原根}. \end{cases}$$

例 5.4.3. 设 a 是奇数, 证明:

(1) $x^2 \equiv a \pmod 2$ 有且仅有 1 个解;

(2) $x^2 \equiv a \pmod 4$ 有解当且仅当 $a \equiv 1 \pmod 4$, 此时该方程有 2 个解;

(3) $\alpha \geqslant 3$ 时 $x^2 \equiv a \pmod{2^\alpha}$ 有解当且仅当 $a \equiv 1 \pmod 8$, 此时该方程有 4 个解.

证明. (1) (2) 已证, 下面主要对 (3) 证明. 必要性. 因 a 是奇数, 故 $x^2 \equiv a \pmod{2^\alpha}$ 有解可得 x 也是奇数, 从而 $a \equiv x^2 \equiv 1 \pmod 8$. 充分性. 设 γ_{-1}, γ_0 是 a 对于模 2^α 的指标组, 则由 $(-1)^{\gamma_{-1}} 5^{\gamma_0} \equiv a \equiv 1 \pmod 8$ 及 $5^n \equiv \begin{cases} 1 \pmod 8, 2 \mid n \\ 5 \pmod 8, 2 \nmid n \end{cases}$ 知必有 $\gamma_{-1} = 0$ 且 $2 \mid \gamma_0$, 进而由**命题 5.4.2** 知 $x^2 \equiv a \pmod{2^\alpha}$ 有 4 个解. □

第六章　二次剩余

在 §5.4 中, 我们给出了同余方程 $x^n \equiv a \pmod m$ 有解的充要条件, 并在有解时给出了解数的公式, 但在实际的应用中对于数值较大的模去获得原根、指标或指标组的信息是很困难的, 因此去检验这些充要条件也很困难. 本章的目的是去讨论二次同余方程, 并对模为素数的情形给出其是否有解的一个简单判定方法.

§6.1　总论

一般的**二次同余方程**即 $ax^2 + bx + c \equiv 0 \pmod m$. 当 $(2a, m) = 1$ 时, 利用配方法可将该同余方程化简为

$$a(x + \overline{2a}b)^2 + c - \overline{4a}b^2 \equiv 0 \pmod m,$$

进而得到

$$(x + \overline{2a}b)^2 \equiv \overline{a}(\overline{4a}b - c) \pmod m,$$

其中 $\bar t$ 表示 t 在模 m 下的逆. 因此在本章中, 我们主要讨论这种形如 $y^2 \equiv k \pmod m$ 的同余方程. 按照**定义 5.4.1**, 当 $y^2 \equiv k \pmod m$ 有解时我们称 k 为模 m 的**二次剩余**.

命题 6.1.1. 设 a 是模 m 的二次剩余, 并记 $\omega(m) := \sum\limits_{p|m} 1$, 则同余方程 $x^2 \equiv a \pmod m$ 的解数为

$$N = \begin{cases} 2^{\omega(n)+1}, & m \equiv 0 \pmod 8, \\ 2^{\omega(n)-1}, & m \equiv 2 \pmod 4, \\ 2^{\omega(n)}, & \text{其它情形.} \end{cases}$$

证明. 因 a 是模 m 的二次剩余, 故存在 u 使得 $u^2 \equiv a \pmod m$. 令 $x := yu$ 知原方程可化为 $y^2 \equiv 1 \pmod m$. 现记 $f(y) := y^2 - 1$, $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, 则 $N = \rho(f, p_1^{\alpha_1}) \cdots \rho(f, p_r^{\alpha_r})$. 因此只需计算 $\rho(f, p^\alpha)$. 若 $p > 2$, 则由命题 5.4.1 知 $\rho(f, p^\alpha) = 2$, 相应的两个解也即为 $\pm 1 \pmod{p^\alpha}$. 若 $p = 2$, 则分 $\alpha = 1, 2$ 和 $\alpha \geqslant 3$ 三种情况讨论, 由**例 5.4.3** 得它们分别有 1, 2, 4 个解. 综上, 我们便证明了这一结论. □

定理 6.1.1. 设 $m>2$ 且 g 是模 m 的原根, 则模 m 的二次剩余共有 $\dfrac{\varphi(m)}{2}$ 个, 它们分别同余于 $g^{2j}\left(1\leqslant j\leqslant\dfrac{\varphi(m)}{2}\right)$.

证明. 首先, 显然 $g^{2j}\ \left(1\leqslant j\leqslant\dfrac{\varphi(m)}{2}\right)$ 均为模 m 的二次剩余; 同时, 若 a 是模 m 的二次剩余, 则存在 $u\in\mathbb{Z}$, $(u,m)=1$ 使得 $a\equiv u^2\,(\mathrm{mod}\,m)$, 注意到一定存在正整数 $j\in[1,\varphi(m)]$ 使得 $u\equiv g^j\,(\mathrm{mod}\,m)$, 故 a 必同余于某个 g^{2j}. 若 $j\leqslant\dfrac{\varphi(m)}{2}$, 则命题得证; 若 $\dfrac{\varphi(m)}{2}<j\leqslant\varphi(m)$, 则由 $\varphi(m)$ 是偶数 (参见推论 3.3.1) 可知

$$a\equiv g^{2j}\equiv g^{2j-\varphi(m)}\equiv g^{2(j-\frac{\varphi(m)}{2})}\,(\mathrm{mod}\,m)$$

且 $1\leqslant j-\dfrac{\varphi(m)}{2}\leqslant\dfrac{\varphi(m)}{2}$. □

注记 6.1.1. 上述定理表明, 当整数 $m>2$ 且模 m 有原根时, 模 m 的一个简化剩余系中二次剩余与非二次剩余**各占一半**.

§6.2 Legendre 符号

定义 6.2.1. 对于奇素数 p, **Legendre 符号** $\left(\dfrac{\cdot}{p}\right)$ 是按下述方式定义的:

$$\left(\frac{a}{p}\right):=\begin{cases}0, & p\mid a,\\ 1, & a\text{ 是模 }p\text{ 的二次剩余},\\ -1, & a\text{ 是模 }p\text{ 的二次非剩余}.\end{cases}$$

注记 6.2.1. 不难看出, 同余方程 $x^2\equiv a\,(\mathrm{mod}\,p)$ 的解数为 $1+\left(\dfrac{a}{p}\right)$.

通过以上定义, 我们可将以素数为模的同余方程 $x^2\equiv a\,(\mathrm{mod}\,p)$ 的可解性问题转化为对 Legendre 符号的计算. 本节后面的部分就是要给出一些具体算法, 使得 Legendre 符号能通过这些算法较为轻易的计算出来.

引理 6.2.1. 设 p 是奇素数, g 是模 p 的一个原根, 则对任意的 $j\geqslant 0$ 有 $\left(\dfrac{g^j}{p}\right)=(-1)^j$.

证明. 注意到 $\left(\dfrac{g^j}{p}\right)$ 与 $(-1)^j$ 均只能取 ±1, 并且由 $2\mid\varphi(p)$ 及**定理 6.1.1** 知 $\left(\dfrac{g^j}{p}\right)=1$ 当且仅当 $2\mid j$, 明所欲证. □

下面给出 Legendre 符号的一些基本性质.

命题 6.2.1. 设 p 是奇素数, 则

(1) $\left(\dfrac{a}{p}\right)$ 是以 p 为周期的周期函数;

(2) 若 $(a,p)=1$, 则 $\left(\dfrac{a^2}{p}\right)=1$;

(3) (完全可乘性) $\forall a,b\in\mathbb{Z}$, 都有 $\left(\dfrac{ab}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

证明. (1) 与 (2) 是显然的, 下证 (3). 不妨假设 $(ab,p)=1$, 于是对于模 p 的一个原根 g, 存在 j,k 使得 $a\equiv g^j\,(\mathrm{mod}\,p)$ 且 $b\equiv g^k\,(\mathrm{mod}\,p)$, 从而由引理 6.2.1 知

$$\left(\frac{ab}{p}\right)=\left(\frac{g^{j+k}}{p}\right)=(-1)^{j+k}=(-1)^j(-1)^k=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

若 $(ab,p)>1$, 则必有 $p\mid a$ 或 $p\mid b$, 即等式两侧均为 0, 故命题得证. □

由上述命题及算术基本定理知, 为了计算一般的 Legendre 符号, 只需知道

$$\left(\frac{-1}{p}\right),\quad \left(\frac{2}{p}\right),\quad \left(\frac{q}{p}\right)\ (\text{其中 } p,q \text{ 均为奇素数}).$$

三者的值即可. 下面我们来依次确定它们的值.

定理 6.2.1 (Euler)**.** 设 p 是奇素数, 则对任意的整数 a 都有

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\,(\mathrm{mod}\,p). \tag{6.1}$$

证明. 当 $p\mid a$ 时 (6.1) 显然成立, 故不妨设 $(a,p)=1$, 于是对于模 p 的原根 g, 存在 j 使得 $a\equiv g^j\,(\mathrm{mod}\,p)$. 现记 $h:=g^{\frac{p-1}{2}}$, 则 $h^2\equiv 1\,(\mathrm{mod}\,p)$, 注意到 g 是模 p 的一个原根, 从而 $h\equiv -1\,(\mathrm{mod}\,p)$, 于是由引理 6.2.1 知

$$\left(\frac{a}{p}\right)=\left(\frac{g^j}{p}\right)=(-1)^j\equiv h^j\equiv (g^{\frac{p-1}{2}})^j\equiv a^{\frac{p-1}{2}}\,(\mathrm{mod}\,p).$$

这样, 我们便证明了这一结论. □

在上述定理中取 $a=-1$ 便可再次得到**命题 4.3.1** 的结论.

命题 6.2.2. 设 p 是奇素数, 则 $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. 因此, -1 是模 p 的二次剩余当且仅当 $p\equiv 1\,(\mathrm{mod}\,4)$.

定理 6.2.2 (Gauss)**.** 设 p 是奇素数且 $(a,p)=1$. 若 $a,2a,\cdots,\dfrac{p-1}{2}a$ 诸数除以 p 的最小非负余数中大于 $\dfrac{p}{2}$ 的共有 μ 个, 则

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

证明. 对诸 ak 除以 p 的最小非负余数进行分类, 记这些余数中小于 $\frac{p}{2}$ 者为 $a_1,\cdots,a_\nu$, 大于 $\frac{p}{2}$ 者为 $b_1,\cdots,b_\mu$, 则

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!=\prod_{k\leqslant\frac{p-1}{2}}ak\equiv\prod_{i=1}^{\nu}a_i\prod_{j=1}^{\mu}b_j\,(\mathrm{mod}\,p).$$

由 $(a,p)=1$ 知对任意的 $x,y\in\left[1,\frac{p-1}{2}\right]$, $x\neq y$ 可推知 $ax\neq\pm ay\,(\mathrm{mod}\,p)$, 因此

$$\{a_1,\cdots,a_\nu,p-b_1,\cdots,p-b_\mu\}=\left\{1,2,\cdots,\frac{p-1}{2}\right\},$$

于是有

$$\prod_{i=1}^{\nu}a_i\prod_{j=1}^{\mu}b_j\equiv(-1)^\mu\prod_{i=1}^{\nu}a_i\prod_{j=1}^{\mu}(p-b_j)\equiv(-1)^\mu\left(\frac{p-1}{2}\right)!\,(\mathrm{mod}\,p).$$

结合利用**定理 6.2.1** 便得

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\equiv(-1)^\mu\,(\mathrm{mod}\,p).$$

这样, 我们便证明了这一结论. □

命题 6.2.3. 设 p 是奇素数, 则 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$. 因此, 2 是模 p 的二次剩余当且仅当 $p\equiv\pm1\,(\mathrm{mod}\,8)$.

证明. 我们在**定理 6.2.2** 中取 $a=2$ 并沿用其中的记号. 分两种情形讨论:

(1) 若 $p\equiv1\,(\mathrm{mod}\,4)$, 则

$$\left\{ak:1\leqslant k\leqslant\frac{p-1}{2}\right\}=\left\{2,\cdots,\frac{p-1}{2},\frac{p+3}{2},\cdots,p-1\right\},$$

此时 $\mu=\frac{p-1}{4}$, 从而 $\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{4}}=((-1)^{\frac{p-1}{4}})^{\frac{p+1}{2}}=(-1)^{\frac{p^2-1}{8}}$.

(2) 若 $p\equiv3\,(\mathrm{mod}\,4)$, 则

$$\left\{ak:1\leqslant k\leqslant\frac{p-1}{2}\right\}=\left\{2,\cdots,\frac{p-3}{2},\frac{p+1}{2},\cdots,p-1\right\},$$

此时 $\mu=\frac{p+1}{4}$, 从而 $\left(\frac{2}{p}\right)=(-1)^{\frac{p+1}{4}}=((-1)^{\frac{p+1}{4}})^{\frac{p-1}{2}}=(-1)^{\frac{p^2-1}{8}}$.

综上, 我们便证明了这一结论. □

最后, 我们来讨论 $\left(\frac{q}{p}\right)$ 的计算, 其中 p 与 q 均为奇素数. 这里的关键步骤是下面的**二次互反律**, 它使得在 $p>q$ 时可通过计算 $\left(\frac{p}{q}\right)$ 去代替对 $\left(\frac{q}{p}\right)$ 的计算, 这意味着我们

只需对更小的模去计算 Legendre 符号, 结合周期性并反复应用二次互反律就可以不断地降低模, 从而达到计算目的.

二次互反律是由 Legendre 于 1785 年提出的, 但他给出的证明依赖于一个当时尚未解决的命题, 即首项与公差互素的等差数列中有无穷多个素数. 第一个严格的证明由 Gauss 于 1801 年给出.

定理 6.2.3 (**二次互反律**)**.** 设 p 与 q 是两个不同的奇素数, 则

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}. \tag{6.2}$$

证明. 我们在定理 6.2.2 中取 $a=q$ 并沿用该定理及其证明中的记号. 因为

$$qk=p\left\lfloor\frac{qk}{p}\right\rfloor+p\left\{\frac{qk}{p}\right\},\quad \text{其中 } 0\leqslant p\left\{\frac{qk}{p}\right\}<p,$$

因此 $p\left\{\frac{qk}{p}\right\}$ 也即为 qk 除以 p 的最小非负余数. 对上式的 k 求和可得

$$\begin{aligned}
q\sum_{k=1}^{\frac{p-1}{2}}k&=p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{i=1}^{\nu}a_i+\sum_{j=1}^{\mu}b_j\\
&=p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{i=1}^{\nu}a_i+\sum_{j=1}^{\mu}(p-b_j)+2\sum_{j=1}^{\mu}b_j-p\mu\\
&=p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{k=1}^{\frac{p-1}{2}}k+2\sum_{j=1}^{\mu}b_j-p\mu.
\end{aligned}$$

由于 q,p 均为奇素数, 故

$$\mu\equiv p\mu=p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor-(q-1)\sum_{k=1}^{\frac{p-1}{2}}k+2\sum_{j=1}^{\mu}b_j\equiv\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor\pmod 2.$$

从而由定理 6.2.2 知

$$\left(\frac{q}{p}\right)=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor},$$

同理可得

$$\left(\frac{p}{q}\right)=(-1)^{\sum\limits_{\ell=1}^{\frac{q-1}{2}}\left\lfloor\frac{p\ell}{p}\right\rfloor},$$

因此只需证明

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{\ell=1}^{\frac{q-1}{2}}\left\lfloor\frac{p\ell}{q}\right\rfloor=\frac{(p-1)(q-1)}{4}. \tag{6.3}$$

事实上, 我们有

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{\ell=1}^{\frac{q-1}{2}}\left\lfloor\frac{p\ell}{q}\right\rfloor&=\sum_{k=1}^{\frac{p-1}{2}}\sum_{\ell\leqslant qk/p}1+\sum_{\ell=1}^{\frac{q-1}{2}}\sum_{k\leqslant p\ell/q}1\\&=\sum_{k<p/2}\sum_{\ell\leqslant qk/p}1+\sum_{k<p/2}\sum_{qk/p\leqslant\ell<q/2}1,\end{aligned}$$

又注意到 k 与 ℓ 的求和范围导致 $p\ell=qk$ 不可能成立, 所以

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{qk}{p}\right\rfloor+\sum_{\ell=1}^{\frac{q-1}{2}}\left\lfloor\frac{p\ell}{q}\right\rfloor=\sum_{k<p/2}\sum_{\ell<q/2}1=\frac{p-1}{2}\cdot\frac{q-1}{2}=\frac{(p-1)(q-1)}{4},$$

这便证明了 (6.3), 至此定理得证. □

其实, 我们还可以进一步得到如下的显式结论:

$$\left(\frac{q}{p}\right)=\begin{cases}-\left(\dfrac{p}{q}\right), & p\equiv q\equiv-1 \pmod 4,\\ \left(\dfrac{p}{q}\right), & \text{其他情形.}\end{cases}$$

例 6.2.1. 判断同余方程 $x^2\equiv 286 \pmod{563}$ 是否有解.

解. 注意到 563 为素数, 且

$$\left(\frac{286}{563}\right)=\left(\frac{2}{563}\right)\left(\frac{11}{563}\right)\left(\frac{13}{563}\right)=-\left(\frac{11}{563}\right)\left(\frac{13}{563}\right),$$

其中

$$\left(\frac{11}{563}\right)=-\left(\frac{563}{11}\right)=-\left(\frac{2}{11}\right)=1,\quad\left(\frac{13}{563}\right)=\left(\frac{563}{13}\right)=\left(\frac{4}{13}\right)=1,$$

因此 $\left(\dfrac{286}{563}\right)=-1$, 从而原同余方程无解. □

例 6.2.2. 求所有的素数 $p>3$, 使得 3 是其二次剩余.

解. (1) 若 $p\equiv 1 \pmod 4$, 则 $1=\left(\dfrac{3}{p}\right)=\left(\dfrac{p}{3}\right)$, 从而 $p\equiv 1 \pmod 3$, 故 $p\equiv 1 \pmod{12}$.
(2) 若 $p\equiv -1 \pmod 4$, 则 $1=\left(\dfrac{3}{p}\right)=-\left(\dfrac{p}{3}\right)$, 即 $p\equiv -1 \pmod 3$, 故 $p\equiv -1 \pmod{12}$.

综上, 素数 p 满足条件当且仅当 $p\equiv\pm 1 \pmod{12}$. □

例 6.2.3. 设 p 是奇素数, $(a,p)=1$, 计算 $\displaystyle\sum_{n\leqslant p}\left(\frac{an+b}{p}\right)$.

解. 因 $\left(\dfrac{a}{p}\right)$ 周期为 p, 进而由**命题 3.2.3 (1)** 知

$$\sum_{n\leqslant p}\left(\frac{an+b}{p}\right)=\sum_{n<p}\left(\frac{n}{p}\right)=0,$$

其中, 最后一步得自**定理 6.1.1**. □

例 6.2.4. 设素数 $p>3$, 证明

$$\sum_{\substack{1\leqslant k\leqslant p\\ \left(\frac{k}{p}\right)=1}} k\equiv 0\,(\mathrm{mod}\,p).$$

证明. 因为 $p>3$, 故存在模 p 的二次剩余 a 使得 $a\not\equiv 1\,(\mathrm{mod}\,p)$. 注意到 k 通过模 p 的全部二次剩余当且仅当 ak 通过模 p 的全部二次剩余, 故

$$\sum_{\substack{1\leqslant k\leqslant p\\ \left(\frac{k}{p}\right)=1}} k\equiv a\sum_{\substack{1\leqslant k\leqslant p\\ \left(\frac{k}{p}\right)=1}} k\,(\mathrm{mod}\,p),$$

由此便可得到结论. □

例 6.2.5. 设 p 是形如 $4n+1$ 的素数, a 是满足 $a^2\equiv -1\,(\mathrm{mod}\,p)$ 的整数, 证明 $2a$ 是模 p 的二次剩余.

证明. 由**定理 6.2.1** 及题设知 $\left(\dfrac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{4}}\,(\mathrm{mod}\,p)$, 故 $\left(\dfrac{a}{p}\right)=(-1)^{\frac{p-1}{4}}$. 又因 $\dfrac{p+1}{2}$ 是奇数, 故 $\left(\dfrac{a}{p}\right)=(-1)^{\frac{p-1}{4}\cdot\frac{p+1}{2}}=(-1)^{\frac{p^2-1}{8}}=\left(\dfrac{2}{p}\right)$, 进而有 $\left(\dfrac{2a}{p}\right)=1$, 这表明 $2a$ 是模 p 的二次剩余. □

例 6.2.6. 设 p 是奇素数, 试求集合 $\{1,2,\cdots,p-2\}$ 中使得 n 与 $n+1$ 均是模 p 的二次剩余的元素 n 的个数, 并由此证明 $p\geqslant 7$ 时必有两个相邻的整数皆为模 p 的二次剩余.

证明. 用 N 表示这样的 n 的个数, 则

$$\begin{aligned}N&=\frac{1}{4}\sum_{n\leqslant p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right)\\&=\frac{1}{4}\sum_{n\leqslant p-2}\left(1+\left(\frac{n}{p}\right)+\left(\frac{n+1}{p}\right)+\left(\frac{n(n+1)}{p}\right)\right)\\&=\frac{1}{4}\left(p-2-\left(\frac{-1}{p}\right)-1+\sum_{n\leqslant p-2}\left(\frac{n(n+1)}{p}\right)\right).\end{aligned}$$

又注意到

$$\sum_{n\leqslant p-2}\left(\frac{n(n+1)}{p}\right)=\sum_{n\leqslant p-1}\left(\frac{n^2(\bar{n}+1)}{p}\right)=\sum_{n\leqslant p-1}\left(\frac{\bar{n}+1}{p}\right)=\sum_{n\leqslant p-1}\left(\frac{n+1}{p}\right)=-1,$$

因此 $N=\dfrac{1}{4}\left(p-\left(\dfrac{-1}{p}\right)\right)-1$. □

§6.3 Jacobi 符号

当我们对 Legendre 符号 $\left(\frac{q}{p}\right)$ 应用二次互反律时, 必须要求 q 也是奇素数, 考虑到对较大的数进行素因子分解并不是一件容易的事, 因此 §6.2 中的算法在实际应用中颇为不便. 为了解决这一问题, 我们引入 Jacobi 符号.

定义 6.3.1. 设奇数 $P>1$ 且 $P=p_1\cdots p_r$, 其中 $p_1,\cdots,p_r$ 均为素数 (不必两两不同). 对整数 a, 我们定义 **Jacobi 符号** $\left(\frac{a}{P}\right)$ 为:

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right),$$

其中 $\left(\frac{a}{p_j}\right)$ $(1\leqslant j\leqslant r)$ 是 Legendre 符号.

注记 6.3.1. 我们指出:

(i) Jacobi 符号 $\left(\frac{\cdot}{P}\right)$ 取值于 $\{0,\pm1\}$, 并且 $\left(\frac{a}{P}\right)=0$ 当且仅当 $(a,P)>1$;

(ii) 不能从 $\left(\frac{a}{P}\right)=1$ 推出同余方程 $x^2\equiv a\pmod P$ 有解, 例如 $x^2\equiv 2\pmod 9$ 无解, 而 $\left(\frac{2}{9}\right)=\left(\frac{2}{3}\right)^2=1$;

(iii) 但是, 我们可以从 $\left(\frac{a}{P}\right)=-1$ 推出同余方程 $x^2\equiv a\pmod P$ 无解.

Jacobi 符号具有如下和 Legendre 符号相似的一些性质:

命题 6.3.1. 设 P,Q 均是大于 1 的奇数.

(1) $\forall\, a,b\in\mathbb{Z}$, $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$;

(2) $\left(\frac{\cdot}{P}\right)$ 是以 P' 为周期的周期函数, 其中 $P':=\prod\limits_{p\mid P}p$ 为 P 的无平方因子核;

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

(4) $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$;

(5) 若 $(P,Q)=1$, 则 $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{\frac{(P-1)(Q-1)}{4}}$.

证明. (1) 和 (2) 可直接由 Jacobi 符号的定义得出, 下证 (3) 和 (4). 设 $P:=p_1\cdots p_r$ 为其素因子分解, 则

$$\begin{aligned}\frac{P-1}{2}&=\frac{p_1\cdots p_r-1}{2}\\&=\frac{\left(1+2\,\frac{p_1-1}{2}\right)\cdots\left(1+2\,\frac{p_r-1}{2}\right)-1}{2}\equiv\sum_{j=1}^{r}\frac{p_j-1}{2}\pmod 2.\end{aligned}\tag{6.4}$$

因此

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^{\sum\limits_{j=1}^{r}\frac{p_j-1}{2}}=(-1)^{\frac{P-1}{2}}.$$

类似地, 由

$$\begin{aligned}\frac{P^2-1}{8}&=\frac{p_1^2\cdots p_r^2-1}{8}\\&=\frac{\left(1+8\,\dfrac{p_1^2-1}{8}\right)\cdots\left(1+2\,\dfrac{p_r^2-1}{8}\right)-1}{8}\equiv\sum_{j=1}^{r}\frac{p_j^2-1}{8}\pmod 2\end{aligned}\tag{6.5}$$

可得 (4). 最后来证明 (5). 设 $Q=q_1\cdots q_s$ 为 Q 的素因子分解, 于是由二次互反律及 (6.4) 知

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)=(-1)^{\sum\limits_{i=1}^{r}\sum\limits_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}}=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}},$$

这样便完成了证明. □

设 p 是一个奇素数, $(a,p)=1$. 由**命题 6.3.1** 我们知道, 对于 $\left(\dfrac{a}{p}\right)$ 而言, 无论是将它当作 Legendre 符号还是 Jacobi 符号进行计算, 得到的值是相同的. 因此我们可以将它看作 Jacobi 符号进行计算, 并根据得到的值判断同余方程 $x^2\equiv a\pmod p$ 是否有解.

例 6.3.1. 已知 $F_4=2^{2^4}+1=65537$ 为素数, 试判断同余方程 $x^2\equiv 24883\pmod{65537}$ 是否有解.

解. 我们来计算 Jacobi 符号

$$\begin{aligned}\left(\frac{24883}{65537}\right)&=\left(\frac{65537}{24883}\right)=\left(\frac{15771}{24883}\right)=-\left(\frac{24883}{15771}\right)=-\left(\frac{9112}{15771}\right)\\&=-\left(\frac{2^3}{15771}\right)\left(\frac{1139}{15771}\right)=-\left(\frac{15771}{1139}\right)=-\left(\frac{964}{1139}\right)=-\left(\frac{4\times 241}{1139}\right)\\&=-\left(\frac{241}{1139}\right)=-\left(\frac{1139}{241}\right)=\left(\frac{-66}{241}\right)=-\left(\frac{-1}{241}\right)\left(\frac{2}{241}\right)\left(\frac{33}{241}\right)\\&=-\left(\frac{241}{33}\right)=\left(\frac{10}{33}\right)=-\left(\frac{2}{33}\right)\left(\frac{5}{33}\right)=-\left(\frac{33}{5}\right)=-\left(\frac{-2}{5}\right)=1,\end{aligned}$$

故原同余方程有解. □

注记 6.3.2. 事实上, 手算将 24883 分解为两个素数 149 与 167 之积是很困难的; 即使可利用周期性得到 $\left(\dfrac{24883}{65537}\right)=\left(\dfrac{-2\times 20327}{65537}\right)$ 也需要考虑 20327 的素因子分解, 事实上 20327 是素数, 手算判定这一结果也十分困难.

据陆老师本人亲口所述, 24883 这个数是他刻意精挑细选得到的 (笑).

第七章　数论函数简介—定义与例子

定义 7.1.1. 设 $S \subset \mathbb{Z}$, 称映射 $f : S \to \mathbb{C}$ 为**数论函数**或**算术函数**.

例 7.1.1. 在这个例子中, 我们给出一些定义在 $\mathbb{Z}_{>0}$ 上的重要数论函数.

(1) **除数函数** $\tau(n)$: $\tau(n)$ 表示 n 的正因子的个数, 即

$$\tau(n) := \sum_{d|n} 1 = \sum_{dk=n} 1.$$

更一般地, 对 $k \in \mathbb{Z}_{>0}$ 记

$$\tau_k(n) := \sum_{d_1 \cdots d_k = n} 1,$$

特别地, $\tau_2(n) = \tau(n)$.

(2) 作为除数函数的推广, 我们可对一般的 $\nu \in \mathbb{C}$ 定义函数

$$\sigma_\nu(n) := \sum_{d|n} d^\nu.$$

特别地, 我们将 $\sigma_1(n)$ 简记为 $\sigma(n)$, 称为**除数和函数**.

(3) **Euler 函数** $\varphi(n)$: $\varphi(n)$ 表示 n 的既约剩余类的个数. 在命题 3.2.6 中我们证明了

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

(4) **Möbius 函数** $\mu(n)$:

$$\mu(n) := \begin{cases} 1, & n = 1, \\ (-1)^r, & n = p_1 \cdots p_r, \text{其中 } p_1, \cdots, p_r \text{ 是两两不同的素数}, \\ 0, & \text{其它情形, 即存在素数 } p \text{ 使得 } p^2 \mid n. \end{cases}$$

(5) **von Mangoldt 函数** $\Lambda(n)$:

$$\Lambda(n) := \begin{cases} \log p, & \text{若 } n = p^k, \text{其中 } p \text{ 为素数且 } k \geqslant 1, \\ 0, & \text{其它情形.} \end{cases}$$

(6) $\omega(n)$ 和 $\Omega(n)$: $\omega(n)$ 表示 n 的不同的素因子的个数, $\Omega(n)$ 表示 n 的全部素因子的个数 (按重数计算), 即

$$\omega(n) := \sum_{p|n} 1, \qquad \Omega(n) := \sum_{p^\alpha \| n} \alpha.$$

(7) **Liouville 函数** $\lambda(n)$:

$$\lambda(n) := (-1)^{\Omega(n)}.$$

定义 7.1.2. 设 $S \subset \mathbb{Z}$ 对乘法封闭且 $1 \in S$, f 是定义在 S 上的不恒等于 0 的数论函数. 若对 S 中任意两个互素的整数 m, n 均有

$$f(mn) = f(m)f(n),$$

则称 f 是**可乘的** (也称 f 为**积性函数**). 如果上式对任意的两个整数 m, n 均成立, 则称 f 是**完全可乘的**.

例 7.1.2. 由推论 3.2.1 可知 φ 是 $\mathbb{Z}_{>0}$ 上的可乘函数. 此外, 不难验证 $\mu(n)$ 是 $\mathbb{Z}_{>0}$ 上的可乘函数, 并且由 $\omega(mn) = \omega(m) + \omega(n)$ $((m,n) = 1)$ 以及 $\Omega(mn) = \Omega(m) + \Omega(n)$ $(\forall\, m, n \in \mathbb{Z}_{>0})$ 可得 $\lambda(mn) = \lambda(m)\lambda(n)$, 即 $\lambda(n)$ 是 $\mathbb{Z}_{>0}$ 上的完全可乘函数. 此外, $\Lambda(n)$ 不是可乘函数. □

例 7.1.3. 设 d 是一个给定的整数, 则 $f(n) := (n, d)$ 是 $\mathbb{Z}$ 上的可乘函数.

证明. 当 $(m, n) = 1$ 时, 由命题 1.2.4 知

$$\begin{aligned} f(m)f(n) = (m,d)(n,d) &= (mn, md, nd, d^2) \\ &= (mn, d(m,n), d^2) = (mn, d, d^2) = (mn, d) = f(mn), \end{aligned}$$

故 f 是 $\mathbb{Z}$ 上的可乘函数. □

在一般情况下, 我们所研究的都是定义在 $\mathbb{Z}_{>0}$ 或 $\mathbb{Z}$ 上的数论函数. 因此为方便起见, 在后面的讨论中我们均将数论函数的定义域略去不提.

设 n 具有标准分解式 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. 那么当 f 可乘时,

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_r^{\alpha_r});$$

当 f 完全可乘时,

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_r)^{\alpha_r}.$$

因此, 可乘函数由它在素数幂处的取值决定, 而完全可乘函数由它在素数处的取值决定.

命题 7.1.1. 设 f 是一个可乘函数, 则 $f(1)=1$.

证明. 不妨设 $f(a)\neq 0$, 则由 $f(a)=f(a)f(1)$ 可得 $f(1)=1$. □

例 7.1.4. 设 f 是一个定义在 $\mathbb{Z}_{>0}$ 上的可乘函数. 证明: 对任意的正整数 m,n, 都有

$$f(m)f(n)=f((m,n))f([m,n]).$$

证明. 由于 f 可乘, 利用 m,n 的标准分解式及命题 1.4.6 即证. □

一组参考题

正如标题所说, 这是一组具有一定参考意义的练习题, 读者不妨拿来做做练练手.

一、 (20 分) 叙述以下定义或定理:

(1) 模 m 的简化剩余系;

(2) von Mangoldt 函数;

(3) 原根;

(4) Lagrange 定理.

二、 (10 分) 已知 $(a,b)=1$, 证明 $(a+b,a^2+ab+b^2)=1$.

三、 (10 分) 设整数 $a,n\geqslant 2$ 且 a^n-1 为素数. 证明 $a=2$ 且 n 为素数.

四、 (10 分) 判断同余方程组

$$\begin{cases} x\equiv 1 \pmod 6,\\ x\equiv 5 \pmod{28},\\ x\equiv -2 \pmod{21}, \end{cases}$$

是否有解, 若有, 则求出其解; 若没有, 说明理由.

五、 (10 分) 已知 1777 是素数, 判断同余方程 $x^2\equiv 3431 \pmod{1777}$ 是否有解, 并说明理由.

六、 (10 分) 设整数 $m\geqslant 2$, $(a,m)=1$, 求 $\displaystyle\sum_{\substack{k\leqslant m\\(k,m=1)}}\left\{\frac{ak}{m}\right\}$.

七、 (10 分) 设 $(m,n)=1$ 且 $(a,mn)=1$, 证明 $\delta_{mn}(a)=[\delta_m(a),\delta_n(a)]$, 并求 $\delta_{120}(7)$.

八、 (20 分)

(1) 设 $p>3$ 为奇素数, 证明 $\left(\dfrac{-3}{p}\right)=1$ 当且仅当 $p\equiv 1 \pmod 6$.

(2) 证明形如 $6n+1$ 的素数有无穷多个.