2022.07.16 数论讲义

同余方程和不定方程及相关问题

目录

1 用到的基础知识

定理 1. (带余除法) 设 a, b 是两个整数且 $b \neq 0$. 则存在唯一的一对整数 q 和 r, 使得

$$a = bq + r, \quad 0 \leq r < |b|.$$

定理 2. (Bezout 定理，也称贝祖定理或裴蜀定理) 假设 a 和 b 都是正整数, d 是 a 和 b 的最大公因数，则存在整数 m 和 n, 使得 $ma + nb = d$.

定理 3. 设 $a, b \in \mathbb{N}^*$, $n \in \mathbb{Z}$. 则方程 $ax + by = n$ 有整数解 (x, y) 当且仅当 $(a, b)|n$. 而且此时方程的所有解为

$$(x, y) = \left(x_0 + t \cdot \frac{b}{d}, y_0 - t \cdot \frac{a}{d}\right),$$

其中 $d = (a, b)$, (x_0, y_0) 是方程的一个特解.

定理 4. (算术基本定理) 设 n 是大于 1 的正整数，则 n 可唯一的表示为一些互不相同的素数方幂的乘积, 即

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

其中 $p_1, p_2, \ldots, p_r$ 是互不相同的素数且 $p_1 < p_2 < \cdots < p_r$, $e_i \geq 1$, $1 \leq i \leq r$. 这儿的唯一性是指：如果还存在不同的素数 $q_1, q_2, \ldots, q_k$ 且 $q_1 < q_2 < \cdots < q_k$ 以及 $f_j \geq 1, 1 \leq j \leq k$ 使得

$$n = q_1^{f_1} q_2^{f_2} \cdots q_k^{f_k}.$$

则 $r = k$, 且 $p_i = q_i, e_i = f_i, i = 1, \ldots, r$.

定理 5. 设 $a, b, m, n \in N^*$ 且 $ab \neq 1, (a, b) = 1$. 不妨设 $a \geq b, n \geq m$. 则下列结论成立.

(1) $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

(2) $(a^m - b^m) | (a^n - b^n) \Leftrightarrow m | n$.

(3) $(a^m + b^m) | (a^n + b^n) \Leftrightarrow m | n$, 且 $\frac{n}{m}$ 是奇数.

1.1 同余

定义 1. 设 $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}^*$. 当 $m | (a - b)$ 时, 我们说 a, b 模 m 同余, 记作 $a \equiv b \pmod{m}$. 当 m 不能整除 $a - b$ 时，我们说 a, b 模 m 不同余，记作 $a \not\equiv b \pmod{m}$.

引理 1. 同余的等价性: 设 $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}^*$, 则

(1) **自身性:** $a \equiv a \pmod{m}$;

(2) **对称性:** 如果 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$;

(3) **传递性:** 如果 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$.

引理 2. 设 $a, b, c, d \in \mathbb{Z}, m, n \in \mathbb{N}^*$, 且 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 则

$$a + c \equiv b + d \pmod{m}$$

$$a - c \equiv b - d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

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

引理 3. 设 $a, b, c \in \mathbb{Z}, m \in \mathbb{N}^*$ 且 $c \not\equiv 0 \pmod{m}$, 如果 $ac \equiv bc \pmod{m}$, 则 $a \equiv b \pmod{\frac{m}{(m,c)}}$. 特别地, 如果 $(m, c) = 1$, 则 $a \equiv b \pmod{m}$.

引理 4. 设 $a, b, c \in \mathbb{Z}, m \in \mathbb{N}^*$ 且 $c \neq 0$. 如果 $ac \equiv bc \pmod{mc}$, 则 $a \equiv b \pmod{m}$.

引理 5. 设 $a, b \in \mathbb{Z}, m, n \in \mathbb{N}^*$ 且 $n | m$. 如果 $a \equiv b \pmod{m}$, 则 $a \equiv b \pmod{n}$.

引理 6. 设 $a,b\in\mathbb{Z},m_i\in\mathbb{N}^*,i=1,2,\ldots,n.$ 如果 $a\equiv b\pmod{m_i},i=1,2,\ldots,n,$ 则

$$a\equiv b\pmod{[m_1,m_2,\cdots,m_n]}.$$

定义 2. 设 $a,b\in\mathbb{Z},\ m\in\mathbb{N}^*,$ 当 $a\not\equiv 0\pmod{m}$ 时, 我们把

$$ax+b\equiv 0\pmod{m} \tag{1}$$

叫做模 m 的一次同余式.

定理 6. 设 $a\not\equiv 0\pmod{m},$ 则一次同余式

$$ax+b\equiv 0\pmod{m} \tag{2}$$

有整数解的充分必要条件是 $(m,a)|b.$

1.2 同余方程组及孙子定理(中国剩余定理)

定理 7. 孙子定理(中国剩余定理) 设 $k\geq 2,\ m_1,\cdots,m_k$ 是 k 个两两互素的正整数, 则对任意 $b_1,b_2,\ldots,b_k\in\mathbb{Z},$ 同余式组

$$\begin{cases} x\equiv b_1 \pmod{m_1}\\ x\equiv b_2 \pmod{m_2}\\ \cdots \qquad \cdots\\ x\equiv b_k \pmod{m_k}\end{cases} \tag{3}$$

有解且具有唯一的解:

$$x\equiv b_1M_1'M_1+b_2M_2'M_2+\cdots+b_kM_k'M_k\pmod{M}. \tag{4}$$

其中 $M=m_1m_2\cdots m_k=m_iM_i,\ M_i'M_i\equiv 1\pmod{m_i},\ 1\leq i\leq k.$

定理 8. 若 $m_1,m_2,\ldots,m_k$ 是 k 个两两互素的正整数, 令 $m=m_1m_2\cdots m_k.$ 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ \ a_i\in\mathbb{Z},i=0,1,\ldots,n,\ a_n\not\equiv 0\pmod{m}.$$

则同余式

$$f(x)\equiv 0\pmod{m} \tag{5}$$

有解的充分必要条件是同余式

$$f(x)\equiv 0\pmod{m_i}\ (i=1,2,\ldots,k)$$

都有解. 并且, 若用 T_i 表示 $f(x)\equiv 0\pmod{m_i}$ 的模 m_i 互不相同的解数, T 表示 (5) 式模 m 互不相同的解数, 则 $T=T_1T_2\cdots T_k.$

1.3 完全剩余系与缩系

定义 3. 设 m 是给定的正整数, $r \in \{0,1,2,\ldots,m-1\}$, 令 $C_r = \{qm+r \mid q \in \mathbb{Z}\}$, 则 $C_0, C_1, \ldots, C_{m-1}$ 叫做模 m 的剩余类.

定理 9. 设 $m > 0, C_0, C_1, \ldots, C_{m-1}$ 是模 m 的剩余类, 则有

(1) 每一个整数恰好包含在某一个类 C_j 里, 这里 $0 \le j \le m-1$.

(2) 两个整数 x, y 属于同一个类的充分必要条件是 $x \equiv y \pmod{m}$.

定义 4. 在模 m 的剩余类 $C_0, C_1, \ldots, C_{m-1}$ 中各取一数 $a_j \in C_j, j = 0,1,\ldots,m-1$, 此 m 个数 $a_0, a_1, \ldots, a_{m-1}$ 称为模 m 的一组完全剩余系.

定理 10. (1) m 个整数构成模 m 的一组完全剩余系的充分必要条件是两两模 m 不同余;

(2) 设 $(k,m) = 1$, $a_1, \ldots, a_m \in \mathbb{Z}$, 则 $a_1, \ldots, a_m$ 是模 m 的一组完全剩余系的充分必要条件是 $ka_1, \ldots, ka_m$ 是模 m 的一组完全剩余系;

(3) 设 $m_1 > 0, m_2 > 0, (m_1, m_2) = 1$, 而 x_1, x_2 分别通过模 m_1, m_2 的完全剩余系, 则 $m_2x_1 + m_1x_2$ 通过模 m_1m_2 的完全剩余系.

定义 5. (1) 设 $m \in \mathbb{N}^*$. 令 $\varphi(m) = \sharp\{k \mid 1 \le k \le m, (k,m) = 1\}$, 即 $\varphi(m)$ 表示不大于 m 且和 m 互素的正整数的个数. 函数 $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*, m \mapsto \varphi(m)$, 称为欧拉(Euler) 函数.

(2) 设 $a_1, \ldots, a_{\varphi(m)} \in \mathbb{Z}$ 满足 $(a_i, m) = 1, a_i \not\equiv a_j \pmod{m}, \forall\, i \ne j \in \{1,2,\ldots,\varphi(m)\}$, 则称 $a_1, \ldots, a_{\varphi(m)}$ 是模 m 的一组缩系.

定理 11. (1) 设 $a_1, a_2, \ldots, a_m$ 是模 m 的一组完全剩余系, 则

$$\{a_i \mid (a_i, m) = 1,\ i = 1,2,\ldots,m\}$$

是模 m 的一组缩系.

(2) 设 $a_1, \ldots, a_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, $k \in \mathbb{Z}$ 且 $(k,m) = 1$, 则下列等价:

(i) $a_1, \ldots, a_{\varphi(m)}$ 是模 m 的一组缩系, 即 $a_1, \ldots, a_{\varphi(m)}$ 模 m 两两不同余;

(ii) $ka_1, \ldots, ka_{\varphi(m)}$ 是模 m 的一组缩系.

定理 12. 设 m_1, m_2 是两个正整数且 $(m_1, m_2) = 1$. 如果 x_1, x_2 分别通过模 m_1, m_2 的缩系, 则 $m_2x_1 + m_1x_2$ 通过模 m_1m_2 的缩系.

推论 1. 若 $(m_1, m_2) = 1$, 则 $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$.

定理 13. 设 $n \geq 1$, 则有 $\sum\limits_{d|n} \varphi(d) = n$.

定理 14. 设 n 的标准分解为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = n \prod_{p|n} (1 - \frac{1}{p}).$$

其中乘积 $\prod\limits_{p|n}$ 表示 p 跑遍 n 的所有素因子.

1.4 欧拉定理、费马小定理

定理 15. (欧拉定理) 设 m 是大于 1 的整数，a 是一个整数且满足 $(a, m) = 1$, 则

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

定理 16. (费马小定理) 设 p 是一个素数，$a \in \mathbb{Z}$.

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

(2) 如果 $(a, p) = 1$, 则 $a^{p-1} \equiv 1 \pmod{p}$.

1.5 原根

定义 6. 设 $m \in \mathbb{N}^*, a \in \mathbb{Z}$ 且 $(a, m) = 1$. 使得 $a^l \equiv 1 \pmod{m}$ 成立的最小的正整数 l 称为 a 模 m 的阶. 记为 $l = \mathrm{ord}_m(a)$.

定理 17. 设 l 为 a 模 m 的阶, $s \in \mathbb{Z}$. 则 $a^s \equiv 1 \pmod{m} \Leftrightarrow l | s$.

定义 7. 设 m 是大于 1 的整数. 如果存在与 m 互素的整数 g 使得 g 模 m 的阶为 $\varphi(m)$, 则称 g 是模 m 的一个原根.

定理 18. 设 m 是大于 1 的整数, 则整数 g 是模 m 的原根 $\Leftrightarrow g, g^2, \ldots, g^{\varphi(m)}$ 是模 m 的一组缩系.

定理 19. 设 m 是大于 1 的整数, 则存在模 m 的原根 $\Leftrightarrow m = 2, 4, p^\alpha, 2p^\alpha$, 其中 $\alpha \geq 1$, p 是奇素数.

推论 2. 设 p 是一个素数，则

(1) 一定存在模 p 的原根，即存在 $1 \leq g \leq p$, 使得 g 模 p 的阶是 $p - 1$, 从而 $g, g^2, \ldots, g^{p-1}$ 是模 p 的一个缩系.

(2) 恰好有 $\varphi(p - 1)$ 个模 p 两两互不同余的原根.

1.6 积性函数

定义 8. 设 f 是定义在正整数集上的函数.

(1) 如果对任意正整数 m,n 且 $(m,n)=1$, 总有 $f(mn)=f(m)f(n)$, 则称函数 f 是积性函数.

(2) 如果对任意正整数 m,n, 总有 $f(mn)=f(m)f(n)$, 则称函数 f 是完全积性函数.

定理 20. 欧拉函数具有如下性质.

(1) $\varphi(n)$ 是积性函数，即, 如果 $(m,n)=1$ 则 $\varphi(mn)=\varphi(m)\varphi(n)$.

(2) 设 $(m,n)=d$, 则 $\varphi(mn)=\varphi(m)\varphi(n)\frac{d}{\varphi(d)}$.

(3) 如果 $m|n$, 则 $\varphi(m)|\varphi(n)$.

(4) 对任意正整数 m, 有 $\sum\limits_{d|m}\varphi(d)=m$.

1.7 提升幂引理

提升幂(LTE)引理： 设 n 是正整数, 如果 p 是奇素数, $x,y\in\mathbb{Z}$, $p|x-y,(p,x)=1$, 那么

$$v_p(x^n-y^n)=v_p(x-y)+v_p(n).$$

推论 3. 设 n 是正奇数, 如果 p 是奇素数, $x,y\in\mathbb{Z}$, $p|x+y,(p,x)=1$, 那么

$$v_p(x^n+y^n)=v_p(x+y)+v_p(n).$$

2 例题选讲

1. 证明: 不定方程 $x^2 - y! = 2022$ 没有正整数解.

2. 设 $a, b \in \mathbb{N}$ 且 $(a, b) = 1,\ a > 1, b > 1$. 令 $S_{a,b} = \{ax + by \mid x, y \in \mathbb{N}\}$.

(1) 不定方程 $ax + by = n$ 有非负整数解当且仅当 $n \in S_{a,b}$.

(2) 不在 $S_{a,b}$ 中的最大整数为 $(a-1)(b-1) - 1 = ab - a - b$. 因此, 对任意正整数 $n \geqslant (a-1)(b-1)$, 不定方程 $ax + by = n$ 有非负整数解.

(3) 共有 $\frac{1}{2}(a-1)(b-1)$ 个正整数不在集合 $S_{a,b}$ 中, 即共有 $\frac{1}{2}(a-1)(b-1)$ 个正整数 n 使得不定方程 $ax + by = n$ 没有非负整数解.

(4) 对任意整数 $t : 0 \leq t \leq ab - a - b$, 则 $t \in S_{a,b}$ 当且仅当 $ab - a - b - t \notin S_{a,b}$, 即不定方程 $ax + by = t$ 和 $ax + by = ab - a - b - t$ 中有且仅有一个方程有非负整数解.

3. 设 $p \geq 5$ 是素数. 并设

$$\sum_{i=1}^{p-1} \frac{1}{i^2} = \frac{b}{a}, \quad \sum_{i=1}^{p-1} \frac{1}{i} = \frac{t}{s},\ a, b, s, t \in \mathbb{N}^*,\ \ (a, b) = 1,\ (s, t) = 1.$$

证明: $p|b,\ p^2|t$.

4. (1) 设 k 是一个正整数且对正整数 m 的任一素因子 p, 都有 $p - 1 \nmid k$. 证明:

$$\sum_{1 \leq i \leq m, (i,m)=1} \frac{1}{i^k} \equiv 0 \pmod{m}.$$

(2) 设 p 是素数, 如果存在正奇数 k 满足 $p - 1 \nmid k + 1$, 证明: $\sum\limits_{i=1}^{p-1} \frac{1}{i^k} \equiv 0 \pmod{p^2}$.

5. 设 $m = 2^e p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \geqslant 2$, 其中 $e, k \in \mathbb{N}, p_1, p_2, \ldots, p_k$ 是互异的奇素数, $e_1, e_2, \ldots, e_k \in \mathbb{N}^*$, 则同余方程 $x^2 \equiv 1 \pmod{m}$ 模 m 互不相同的解数为

$$\begin{cases} 2^k & e = 0, 1, \\ 2^{k+1}, & e = 2, \\ 2^{k+2}, & e \geq 3. \end{cases}$$

特别地, 同余方程 $x^2 \equiv 1 \pmod{m}$ 仅有两个模 m 不同的解当且仅当 $m = 4, p^\alpha, 2p^\alpha$, 其中 p 是奇素数, $\alpha \in \mathbb{N}^*$.

6. 设整数 $m \geq 2$. 令 $S = \{1 \leq k \leq m \mid (k, m) = 1\}$, $P = \prod_{k \in S} k$. 证明: $P \equiv \pm 1 \pmod{m}$ 且 $P \equiv -1 \pmod{m}$ 当且仅当存在模 m 的原根, 即 $m = 2, 4, p^\alpha, 2p^\alpha$, 其中 p 是奇素数, $\alpha \in \mathbb{N}^*$.

7. 求同余方程 $x^x \equiv 1 \pmod{101}$ 在介于 101 与 101^2 之间的整数解的个数.

8. 设整数 $n \geqslant 2$. 证明: 不定方程 $(x+1)^n - x^n = ny$ 在正整数集合中无解.

9. 设整数 $n \geq 2$. 证明: $n \nmid 2^n - 1$.

10. (1) 设 p 和 q 是两个素数, $a \in \mathbb{Z}$. 如果 $p \left| \dfrac{a^q - 1}{a - 1} \right.$, 则 $p \equiv 1 \pmod{q}$ *or* $p = q$.

(2) 证明: 不定方程 $\frac{x^7 - 1}{x - 1} = y^5 - 1$ 没有整数解.

11. 求不定方程 $1 + 2^x + 2^{2x+1} = y^2$ 的所有整数解.

12. 证明: 不定方程 $3 \cdot 2^x + 1 = y^2$ 仅有正整数解 $(x, y) = (3, 5), (4, 7)$.

13. 求所有满足方程 $8^x + 15^y = 17^z$ 的正整数解.

14. 设 m 是正的偶数, k 是自然数, 证明: $2^m + m^2 = k^2$ 有唯一的解 $m = 6, k = 10$.

15. 求解不定方程 $7^x = 3^y + 4$ 和 $2^x + 3 = 11^y$.

16. 证明: 不定方程 $y^2 = x^3 + 45$ 没有整数解.