

例 1. a) 写出模 9 的一个完全剩余系, 它的每个数是奇数;

b) 写出模 9 的一个完全剩余系, 它的每个数是偶数.

解. a) $\{-7, -5, -3, -1, 1, 3, 5, 7, 9\}$;

b) $\{-8, -6, -4, -2, 0, 2, 4, 6, 8\}$.

例 2. 证明: 当 $m > 2$ 时, $0^2, 1^2, \dots, (m-1)^2$ 一定不是模 m 的完全剩余系.

证明. 由于 $(m-1)^2 \equiv m^2 - 2m + 1 \equiv m(m-2) + 1 \equiv 1 \pmod{m}$, 我们得出 $0, 1, \dots, m-1$ 中至多有 $m-1$ 个互相不同余的数. 所以该数列不可能是模 m 的完全剩余系. \square

例 3. 证明: 如果 $a^k \equiv b^k \pmod{m}$, $a^{k+1} \equiv b^{k+1} \pmod{m}$, 这里 a, b, k, m 是整数, $k > 0, m > 0$, 并且 $(a, m) = 1$, 那么 $a \equiv b \pmod{m}$. 如果去掉 $(a, m) = 1$ 这个条件, 结果仍成立吗?

证明. 从 $a^k \equiv b^k \pmod{m}$, $a^{k+1} \equiv b^{k+1} \pmod{m}$ 开始, 将其两边同乘 b , 得到 $a^k b \equiv b^{k+1} \equiv a^{k+1} \pmod{m}$, 经移项得 $a^k(a-b) \equiv 0 \pmod{m}$, 即 $m \mid a^k(a-b)$.

由于 $(a, m) = 1$, 必然有 $(a^k, m) = 1$ 成立. 所以 $m \mid (a-b)$, 即 $a \equiv b \pmod{m}$. \square

例 4. $1^3 + 2^3 + \dots + (n-1)^3 \equiv 0 \pmod{n}$ 对于符合什么条件的正整数 n 成立?

证明. 已知平方和公式为 $\sum_{k=1}^n k^2 = n(n+1)(2n+1)/6$, 首先求出立方和公式, 设 $S_n = \sum_{k=1}^n k^3$, $E_n = S_n - \int_0^n x^3 dx$, 我们有

$$\begin{aligned} E_n &= S_n - \int_0^n x^3 dx \\ &= \sum_{k=1}^n \left(k^3 - \int_{k-1}^k x^3 dx \right) \\ &= \sum_{k=1}^n \left(\frac{3}{2}k^2 - k + \frac{1}{4} \right) \\ &= (2n^3 + n^2)/4, \end{aligned} \quad \text{那么} \quad \begin{aligned} S_n &= E_n + n^4/4 \\ &= (n(n+1))^2/4. \end{aligned}$$

所以 $1^3 + 2^3 + \dots + (n-1)^3 = (n(n-1))^2/4$. 题目便转为求使 $(n(n-1))^2/4 \equiv 0 \pmod{n}$ 成立的 n , 即 $n \mid (n(n-1))^2/4$. 由此得存在整数 k 使得 $kn = (n(n-1))^2/4$. 经移项得 $4k = n(n-1)^2$, 即 $4 \mid n(n-1)^2$.

i) 当 $n = 4k$ 时, $n(n-1)^2 = 4k(4k-1)$, 能被 4 整除;

ii) 当 $n = 2k+1$ 时, $n(n-1)^2 = 4k^2(2k+1)$, 能被 4 整除;

iii) 当 $n = 4k+2$ 时, $n(n-1)^2 = (4k+2)(4k+1)^2 = 4(16k^3 + 16k^2 + 5k) + 2$.

故 $n(n-1)^2 \equiv 2 \pmod{4}$, 它不能被 4 整除.

所以, 当 n 不取形式为 $4k+2$ 形式的整数时, 原式成立. \square

例 5. 证明: 如果 p 是素奇数, 那么 $1^2 \cdot 3^2 \cdots (p-4)^2 \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

证明. 将平方项拆分成正负两项相乘,

$$\begin{aligned} & 1^2 \cdot 3^2 \cdots (p-4)^2 \cdot (p-2)^2 \\ & \equiv 1 \cdot (-1) \cdot 3 \cdot (-3) \cdots (p-4) \cdot (4-p) \cdot (p-2) \cdot (2-p) \cdot (-1)^{(p-1)/2} \\ & \equiv 1 \cdot (p-1) \cdot 3 \cdot (p-3) \cdots (p-4) \cdot 4 \cdot (p-2) \cdot 2 \cdot (-1)^{(p-1)/2} \\ & \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \cdot (-1)^{(p-1)/2} \\ & \equiv (-1)^{(p+1)/2} \pmod{p}. \end{aligned} \quad \square$$

定理 1. 若 x, y 是整数, p 是素数, 且 $x^2 \equiv y^2 \pmod{p}$, 那么 $x \equiv \pm y \pmod{p}$.

证明. 由 $x^2 \equiv y^2 \pmod{p}$ 知 $p \mid (x^2 - y^2) = (x-y)(x+y)$. 因为 p 是素数, 我们有 $p \mid (x-y)$ 或 $p \mid (x+y)$, 故 $x \equiv y \pmod{p}$ 或 $x \equiv -y \pmod{p}$. \square

例 6. 运用 Wilson 理论证明: 如果 p 是素数, 并且 $p \equiv 1 \pmod{4}$, 那么同余式 $x^2 \equiv -1 \pmod{p}$ 就有两不同余解 $x \equiv \pm \left(\frac{p-1}{2}\right)! \pmod{p}$.

证明. 由 $x^2 \equiv -1 \pmod{p}$ 得

$$\begin{aligned} x^2 & \equiv 1 \cdot 2 \cdots (p-2) \cdot (p-1) \\ & \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2) \cdot (p-1) \\ & \equiv \left(\frac{p-1}{2}\right)^2 \cdots 2^2 \cdot 1^2 \cdot (-1)^{(p-1)/2} \pmod{p}. \end{aligned}$$

由于 $p \equiv 1 \pmod{4}$, 存在整数 k , 使得 $n = 4k+1$ 成立, 则 $(p-1)/2 = 2k$ 是偶数, $(-1)^{(p-1)/2} = 1$. 再由定理 1 可得 $x \equiv \pm \left(\frac{p-1}{2}\right)! \pmod{p}$. \square

例 7. 证明: 如果 $c_1, c_2, \dots, c_{\phi(m)}$ 是模 m 的简化剩余系, 其中 $m \geq 3$, 那么 $c_1 + c_2 + \dots + c_{\phi(m)} \equiv 0 \pmod{m}$.

证明. c 在 m 的简化剩余系中, 那么 $n-c$ 也在 m 的简化剩余系中, 因为 $(c, n) = (n-c, n)$. 但是不可能出现 $c = n-c$ 的情况, 否则 $2c = n$, 则 $(c, n) = c$, 不符合 c 与 n 互质的要求. 所以, 可以将简化剩余系中 c_i 和 $n-c_i$ 两两配对, 使各对中两个元素的和为 n , 进而使所有元素的总和与 0 模 m 同余. \square

例 8. 设 p 是奇素数, k 是正整数. 证明: 同余式 $x^2 \equiv 1 \pmod{p^k}$ 正好有两个不同余的解 $x \equiv \pm 1 \pmod{p^k}$.

证明. 假设 $x^2 \equiv 1 \pmod{p^k}$, 那么 $x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \pmod{p^k}$, 这要求了 $p^k \mid (x-1)(x+1)$. 由于 $(x+1) - (x-1) = 2$, 并且 p 是奇素数 ($p^k \geq 3$), 所以 p^k 只能整除 $x-1$ 和 $x+1$ 中的一个. 故原同余式恰好有两个解, 即 $x \equiv \pm 1 \pmod{p^k}$. \square

例 9. 证明: $k > 2$ 时, 同余式 $x^2 \equiv 1 \pmod{2^k}$ 恰好有四个不同余的解, 它们是 $x \equiv \pm 1$ or $\pm(1 + 2^{k-1}) \pmod{2^k}$; $k = 1$ 时, 该同余式有一个解; $k = 2$ 时, 该同余式有两个不同余的解.

证明. 假设 $x^2 \equiv 1 \pmod{2^k}$, 那么 $x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \pmod{2^k}$, 这要求了 $2^k \mid (x-1)(x+1)$. 注意到 $x-1$ 和 $x+1$ 都是偶数, 并且 $(x+1) - (x-1) = 2$, 所以这两数中的一个不能被 2 以上的 2 的正幂次整除. 故 $2^{k-1} \mid x-1$ 且 $2 \mid x+1$ 或 $2^{k-1} \mid x+1$ 且 $2 \mid x-1$. 由此得出原同余式的解有形式 $x = t2^{k-1} + 1$ 和 $x = t2^{k-1} - 1$.

i) $k > 2$ 时, 取 $t = 0$ or 1 , 得到四个不同余的解 $x \equiv \pm 1$ or $\pm(1 + 2^{k-1}) \pmod{2^k}$;

ii) $k = 1$ 时, 取 $t = 0$, 只得到一个解 $x \equiv 1 \pmod{2}$;

iii) $k = 2$ 时, 取 $t = 0$, 得到两个不同余的解 $x \equiv \pm 1 \pmod{4}$. \square

例 10. 证明: 同余方程组 $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ 有解当且仅当 $(m_1, m_2) \mid a_1 - a_2$. 并证明若有解, 则该解模 $[m_1, m_2]$ 是唯一的.

证明. 若第一条同余式成立, 当且仅当存在整数 k , 使得 $x = a_1 + m_1k$ 成立. 将其代入第二条同余式, 得到 $a_1 + m_1k \equiv a_2 \pmod{m_2}$, 或者

$$m_1k \equiv a_2 - a_1 \pmod{m_2}. \quad (1)$$

如果该同余式有解, 那么原同余方程组有解, 当且仅当 $(m_1, m_2) \mid a_1 - a_2$.

现在假定 $(m_1, m_2) \mid a_1 - a_2$, 则 (1) 式恰好有 (m_1, m_2) 个解. 将 (1) 式的一个解记为 k_0 , 这些解为 $k_0 + jm_2/(m_1, m_2)$, $j = 0, 1, \dots, (m_1, m_2) - 1$. 那么根据 $x = a_1 + m_1k$, 得出原同余方程组的解为 $a_1 + m_1k_0 + jm_1m_2/(m_1, m_2) = a_1 + m_1k_0 + j[m_1, m_2]$, $j = 0, 1, \dots, (m_1, m_2) - 1$, 它们模 $[m_1, m_2]$ 同余. 所以原方程组的解模 $[m_1, m_2]$ 是唯一的. \square

例 11. 求解同余式 $59x \equiv 20 \pmod{91}$. 使用欧几里得算法和中国剩余定理.

解. a) 使用欧几里得算法.

求解原同余式, 首先求解 $59x - 91y = (59, 91)$. 使用欧几里得算法 (递推式 $s_j = s_{j-2} - q_{j-1}s_{j-1}$ 和 $t_j = t_{j-2} - q_{j-1}t_{j-1}$, 其中 q_j 代表第 j 次使用带余除法的商):

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j	
0	91	59	1	32	1	0	
1	59	32	1	27	0	1	
2	32	27	1	5	1	-1	这说明了该方程的特解
3	27	5	5	2	-1	2	为 $x_0 = -37, y_0 = -24$.
4	5	2	2	1	2	-3	
5	2	1	2	0	-11	17	
6					24	-37	

所以 $59 \cdot (-37) \equiv 59 \cdot 54 \equiv 1 \pmod{91}$, 即 59 模 91 的乘法逆元为 54. 代入原方程, $x \equiv 20 \cdot (59)^{-1} \equiv 20 \cdot 54 \equiv 79 \pmod{91}$.

b) 使用中国剩余定理.

由于 $91 = 7 \cdot 13$, 我们有同余方程组

$$\begin{array}{ll} 59x \equiv 3x \equiv 6 \pmod{7} & \text{或者} \quad x \equiv 2 \pmod{7} \\ 59x \equiv 7x \equiv 7 \pmod{13} & x \equiv 1 \pmod{13}. \end{array}$$

根据例 10, 该方程组模 91 有唯一解且该解就是原同余式的解. 根据中国剩余定理, 我们有 $M = 7 \cdot 13 = 91$, $M_1 = 91/7 = 13$, $M_2 = 91/13 = 7$. 要确定 y_1 和 y_2 , 解 $13y_1 \equiv 1 \pmod{7}$ 得出 $y_1 = 6$, 解 $7y_2 \equiv 1 \pmod{13}$ 得出 $y_2 = 2$. 所以该同余方程组的解为 $x = a_1M_1y_1 + a_2M_2y_2 = 2 \cdot 13 \cdot 6 + 1 \cdot 7 \cdot 2 \equiv 79 \pmod{91}$.