Elementary Number Theory: Homework3

刘泓尊　2018011446　计 84

liu-hz18@mails.tsinghua.edu.cn

2020 年 5 月 2 日

Exercises 4.1

5. 若 a 是奇数，则 $a^2 \equiv 1 \mod 8$

证明. 设 $a = 2k+1, k \in \mathbb{Z}$, 则 $a^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. 当 k 为偶数时，$k = 2l, 4k(k+1) = 8l(2l+1)$；当 k 为奇数时，$k = (2l+1), 4k(k+1) = 8(2l+1)(l+1)$. 所以 $8 \mid 4k(k+1), k \in \mathbb{Z}$. 进而 $8 \mid a^2 - 1$.
即 $a^2 \equiv 1 \mod 8$. □

10. 若 $m > 0, a \equiv b \mod m$，则 $a \mod m = b \mod m$

证明. 因为 $a \equiv b \mod m$，则 $a = b + km, k \in \mathbb{Z}$. 进而 $a \mod m = (b+km) \mod m = (b \mod m) + (km \mod m) = b \mod m$.
所以 $a \mod m = b \mod m$ □

11. 若 $a \mod m = b \mod m$, 则 $a \equiv b \mod m$

证明. 因为 $a \mod m = b \mod m$, 所以 $(a-b) \mod m = 0$, 所以 $a - b = km, k \in \mathbb{Z}$, 即 $a = b + km$
所以 $a \equiv b \mod m$. □

15. 若 $a_j \equiv b_j \mod m, (j = 1, 2, \cdots, n)$, 则 (1) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \mod m$, (2) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \mod m$

证明. 用数学归纳法给出证明.
• $n = 1$ 是平凡的，$a_1 \equiv b_1 \mod m$, 进而 $\sum_{j=1}^{1} a_j \equiv \sum_{j=1}^{1} b_j \mod m$; $\prod_{j=1}^{1} a_j \equiv \prod_{j=1}^{1} b_j \mod m$.
• $n = 2$ 时，$a_1 \equiv b_1 \mod m, a_2 \equiv b_2 \mod m$, 所以 $m \mid (a_1 - b_1), m \mid (a_2 - b_2)$.
因为 $(a_1+a_2)-(b_1+b_2) = (a_1-b_1)+(a_2-b_2)$,所以 $m \mid (a_1+a_2)-(b_1+b_2)$, 即 $(a_1+a_2) \equiv (b_1+b_2) \mod m$.
因为 $(a_1a_2) - (b_1b_2) = (a_1a_2) + (a_1b_2) - (a_1b_2) - (b_1b_2) = a_1(a_2+b_2) - b_2(a_1+b_1)$, 所以 $m \mid a_1a_1 - b_1b_2$, 即 $a_1a_2 \equiv b_1b_2 \mod m$
• 假设上述两个命题对 n 成立，则对于 $n+1$ 有:

$\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \mod m$, $a_{n+1} \equiv b_{n+1} \mod m$. 由归纳基础，$\sum_{j=1}^{n+1} a_j \equiv \sum_{j=1}^{n+1} b_j \mod m$.
同理，$\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \mod m$，$a_{n+1} \equiv b_{n+1} \mod m$. 由归纳基础，$\prod_{j=1}^{n+1} a_j \equiv \prod_{j=1}^{n+1} b_j \mod m$. □

37. $m_1, m_2, \cdots m_k$ **两两互素，** $M = m_1 m_2 \cdots m_k$ **且** $M_j = M/m_j, j = 1, 2, \cdots, k$**. 证明当** $a_1, a_2, \cdots, a_k$ **分别取遍** $m_1, m_2, \cdots, m_k$ **的完全剩余系时，** $M_1 a_1 + M_2 a_2 + \cdots + M_k a_k$ **取遍** M **的完全剩余系**

证明. a_i 有 m_i 中取法，则 $\sum_{i=1}^{k} M_i a_i$ 有 $\prod_{i=1}^{k} m_i$ 种取法。即 M 种;
只需证: M 种取法中任意两种模 M 不同余.
假设有 $\sum_{i=1}^{k} M_i a_{i_1} \equiv \sum_{i=1}^{k} M_i a_{i_2} \mod M, a_{i_1} \neq a_{i_2}, \forall i = 1, 2, \cdots, k$
那么, $M \mid \sum_{i=1}^{k} M_i (a_{i_1} - a_{i_2})$, 进而 $m_1 \mid \sum_{i=1}^{k} M_i (a_{i_1} - a_{i_2})$.
因为 m_i 两两互素，所以 $m_i \nmid M_i, m_i \mid M_j (j \neq i)$, 进而 $m_i \mid M_i (a_{i_1} - a_{i_2})$, 进而 $m_i \mid (a_{i_1} - a_{i_2})$, 所以 $a_{i_1} \equiv a_{i_2} \mod m_i$. 矛盾!
所以 $M_1 a_1 + M_2 a_2 + \cdots + M_k a_k$ 取遍 M 的完全剩余系。 □

Exercise 4.2

15. 同余方程 $x^2 \equiv 1 \mod p^k$**,** p **为奇素数，恰有两个不同余的解** $x \equiv \pm 1 \mod p^k$**.**

证明. $x^2 - 1 = (x+1)(x-1) \equiv 0 \mod p^k$, 所以 $p^k \mid (x+1)(x-1)$. 因为 $(x+1) - (x-1) = 2$, 所以 $(x+1, x-1) \leq 2$.
因为 p 是奇素数，则或者有 $p \mid (x+1)$, 或者有 $p \mid (x-1)$；即或者有 $p^k \mid (x+1)$, 或者有 $p^k \mid (x-1)$. 所以 $x \equiv \pm 1 \mod p^k$. □

16. 同余方程 $x^2 \equiv 1 \mod 2^k$ **在** $k > 2$ **时恰有 4 个不同余的解，它们是** $x = \pm 1$ **或** $x = \pm(1 + 2^{k-1}) \mod 2^k$**; 在** $k = 1$ **时仅有一个解;** $k = 2$ **是有两个不同余的解**

证明. $k > 2$ 时，$x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \mod 2^k$, 所以 $2^k \mid (x+1)(x-1)$. 注意到 $(x+1) - (x-1) = 2$, 即两者的线性组合中有 2，所以 $(x+1, x-1) \leq 2$, 所以或者有 $2^{k-1} \mid x+1, 2 \mid x-1$, 或者有 $2^{k-1} \mid x-1, 2 \mid x+1$。
所以或者有 $x = t2^{k-1} + 1$ 或者有 $x = t2^{k-1} - 1, t \in \mathbb{Z}$
所以 x 模 2^k 的解只有 4 个，即 $x = \pm 1$ 或 $x = \pm(1 + 2^{k-1}) \mod 2^k$.
$k = 1$ 时，只有一个解 $x \equiv 1 \mod 2$.
$k = 2$ 时，有两个解 $x \equiv \pm 1 \mod 2^2$. □

Exercises 4.3

19. 考虑模不一定互素的同余方程组

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\cdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

上述方程组有解当且仅当对所有整数对 (i,j) 有 $(m_i,m_j) \mid (a_i-a_j), 1 \le i < j \le r$，且该解模 $[m_1,m_2,\cdots,m_r]$ 唯一.

先证明 $r=2$ 的情况，即同余方程组

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned}$$

有解当且仅当 $(m_1,m_2) \mid (a_1-a_2)$，且若有解则该解模 $[m_1,m_2]$ 唯一.

证明. 设第一个同余方程的解为 $x = a_1 + km_1 (k \in \mathbb{Z})$, 带入第二个同余方程得到: $a_1 + km_1 \equiv a_2 \mod m_2$, 转换为关于 k 的方程 $km_1 \equiv (a_2 - a_1) \mod m_2$，等价于 $a_2 - a_1 = k_1m_1 + k_2m_2, k_1, k_2 \in \mathbb{Z}$. 上述方程有解当且仅当 $(m_1,m_2) \mid (a_2-a_1)$。设特解为 $k = k_0$, 则通解为 $k = k_0 + m_2t/(m_1,m_2), t \in \mathbb{Z}$. 所以 $x = a_1 + km_1 = a_1 + \left(k_0 + \frac{m_2t}{(m_1,m_2)}\right) = a_1 + k_0m_1 + \frac{m_1m_2}{(m_1,m_2)}t = a_1 + k_0m_1 + [m_1,m_2]t$.
设 $x_0 = a_1 + k_0m_1$, 进而上述同余方程组有解 $x = x_0 + [m_1,m_2]t, t \in \mathbb{Z}$. 所以上述方程组有解，且模 $[m_1,m_2]$ 唯一. □

下面证明原命题:

证明. $r=2$ 时已证。假设原命题对 r 成立。对于 $r+1$ 的情形，有前 r 个方程满足 $(m_i,m_j) \mid (a_i-a_j), 1 \le i < j \le r$ 时有模 $M = [m_1,m_2,\cdots,m_r]$ 的唯一解 A，且 $x \equiv a_{r+1} \mod m_{r+1}$.
则上述条件转化为同余方程组

$$\begin{aligned} x &\equiv A \mod M \\ x &\equiv a_{r+1} \mod m_{r+1} \end{aligned}$$

上述方程有解当且仅当 $(M,m_{r+1}) \mid (A-a_{r+1})$.
下证上述条件等价于 $(m_i,m_{r+1}) \mid (a_i-a_{r+1}), i \in [1,r]$:
因为 $m_i \mid [m_1,m_2,\cdots,m_r], i \in [1,r]$, 进而 $(M,m_{r+1}) = (m_i,m_{r+1}), i \in [1,r]$. 所以 $(M,m_{r+1}) \mid (A-a_{r+1})$ 等价于 $(m_i,m_{r+1}) \mid (A-a_{r+1})$. 进而 $(A-a_{r+1}) = k(m_i,m_{r+1})$. 两侧同时模 m_i 得到 $(a_i-a_{r+1}) \equiv km_{r+1} \mod m_i$，等价于 $(m_i,m_{r+1}) \mid (a_i-a_{r+1}), i \in [1,r]$
采用上述引理的方法,上述方程有解 $x = x_0 + [[m_1,m_2,\cdots,m_r],m_{r+1}]t = x_0 + [m_1,m_2,\cdots,m_{r+1}]$.
该解模 $[m_1,m_2,\cdots,m_{r+1}]$ 唯一。 □

Exercise 6.3

10. 设 a, n 是互素的正整数，若 n 是以 a 为基的伪素数，则 n 也是以 $\overline{a}$ 为基的伪素数，其中 $\overline{a}$ 是 a 模 n 的逆.

证明. $a^n \equiv a \mod n$, $1 \equiv \overline{a^n} a^n \equiv \overline{a}^n a^n \equiv \overline{a}^n a \mod n$. 所以 $\overline{a} \equiv \overline{a}^n \mod n$. 即 $\overline{a}$ 是 a 模 n 的逆. □

Exercise 7.1

21. 若 $(m, n) = p$, 其中 m, n 为正整数, p 为素数，则 $\phi(mn) = p\phi(m)\phi(n)/(p-1)$

证明. 因为 $(m, n) = p$，所以 $p \mid n, p \mid m$. 不妨设 $n = kp$, 其中 $(n, k) = (m, k) = 1$. 所以 $\phi(n) = \phi(kp) = \phi(k)\phi(p) = \phi(k)(p-1)$. 根据例 7.7 有 $\phi(mp) = p\phi(m)$。所以 $\phi(mn) = \phi(mkp) = \phi(mp)\phi(k) = p\phi(m)\phi(n)/(p-1)$. □

22. 若 m, k 为正整数，则 $\phi(m^k) = m^{k-1}\phi(m)$.

证明. 设 m 的素数幂分解为 $m = \prod_{i=1}^{r} p_i^{a_i}$. 所以 $\phi(m) = \prod_{i=1}^{r} \phi(p_i^{a_i})$. 进而 $m^k = \prod_{i=1}^{r} p_i^{ka_i}$, $\phi(m^k) = \prod_{i=1}^{r} \phi(p_i^{ka_i})$. 因为 $\phi(p_i^{ka_i}) = p_i^{ka_i - 1}(p_i - 1) = p_i^{(k-1)a_i} p^{a_i - 1}(p_i - 1) = p^{(k-1)a_i}\phi(p_i^{a_i})$. 所以 $\phi(m^k) = \prod_{i=1}^{r} \phi(p_i^{ka_i}) = \prod_{i=1}^{r} p^{(k-1)a_i} \prod_{i=1}^{r} \phi(p_i^{a_i}) = m^{k-1}\phi(m)$ □

23.a, b 为正整数，则 $\phi(ab) = (a, b)\phi(a)\phi(b)/\phi((a, b))$, 进而推出 $(a, b) > 1$ 时，有 $\phi(ab) > \phi(a)\phi(b)$

证明. 对 a, b 进行素分解，设 $a = r_1^{a_1} r_2^{a_2} \cdots r_s^{a_s} p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, $b = r_1^{a_1} r_2^{a_2} \cdots r_s^{a_s} q_1^{n_1} q_2^{n_2} \cdots q_l^{n_l}$. 所以

$$\phi(ab) = ab\left((1-\frac{1}{r_1})(1-\frac{1}{r_2})\cdots(1-\frac{1}{r_s})\right)\left((1-\frac{1}{p_1})\cdots(1-\frac{1}{p_t})\right)\left((1-\frac{1}{q_1})\cdots(1-\frac{1}{q_l})\right)$$

$$\phi(a) = a\left((1-\frac{1}{r_1})(1-\frac{1}{r_2})\cdots(1-\frac{1}{r_s})\right)\left((1-\frac{1}{p_1})\cdots(1-\frac{1}{p_t})\right)$$

$$\phi(b) = b\left((1-\frac{1}{r_1})(1-\frac{1}{r_2})\cdots(1-\frac{1}{r_s})\right)\left((1-\frac{1}{q_1})\cdots(1-\frac{1}{q_l})\right)$$

$$\phi((a, b)) = (a, b)(1-\frac{1}{r_1})(1-\frac{1}{r_2})\cdots(1-\frac{1}{r_s})$$

所以

$$\phi(ab) = \frac{(\phi(a)\phi(b))}{\frac{(a,b)}{\phi((a,b))}} = \frac{(a, b)\phi(a)\phi(b)}{\phi((a, b))}$$

□