Elementary Number Theory: Homework3

刘泓尊　2018011446　计 84

2020 年 4 月 15 日

1. 良序公理 (The Well-Ordering Property): 每个**非空**的**正整数**集合都有**最小元**。
   正整数集合是良序的，所有整数的集合不是良序的，因为其可能没有最小元。

2. 证明 $\sqrt{2}$ 是无理数:
   假设 $\sqrt{2}$ 是有理数，则存在正整数 a 和 b 使得 $\sqrt{2} = a/b$. 所以 $S = \{k\sqrt{2} \mid k, k\sqrt{2} \in \mathbb{Z}^+\}$ 是非空的正整数集合 (因为至少有 $a = b\sqrt{2} \in S$.)
   由良序公理，S 有最小元，记为 $s = t\sqrt{2}$. 进而 $s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s-t)\sqrt{2}$
   因为 $s\sqrt{2} = 2t$ 和 $t\sqrt{2}$ 都是整数，所以 $(s-t)\sqrt{2}$ 是整数，又 $s\sqrt{2} - s > 0$, 所以 $(s-t)\sqrt{2} \in S$, 而 $s(\sqrt{2}-1) < s$，与 s 是最小元矛盾！
   所以 $\sqrt{2}$ 是无理数。

3. 证明: $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}, s.t. \quad a = bq + r, (0 \le r \le b-1)$
   构造集合 $S = \{a - bk \mid a, k \in \mathbb{Z}, b \in \mathbb{Z}^+, a - bk \ge 0\}$, 显然 S 非空，(取 $k = \lfloor \frac{a}{b} \rfloor$ 即可)
   存在性: 由良序公理，S 中有最小元，设为 $r = a - bq \ge 0$。
   假设 $r \ge b$, 则 $0 \le r - b = a - bq - b = a - (q+1)b < r$，而 $r - b \in S$, 所以与 r 是最小元矛盾! 所以 $0 \le r \le b - 1$.
   唯一性: 假设 $\exists q_1, r_1, q_2, r_2$ 使得 $a = bq_1 + r_1, a = bq_2 + r_2$, 且 $0 \le r_1, r_2 \le b - 1$. 有 $a - a = b(q_1 - q_2) + (r_1 - r_2) = 0$, 即 $(r_2 - r_1) = b(q_1 - q_2)$, 必有 $b \mid (r_2 - r_1)$, 而 $-b < r_2 - r_1 < b$, 矛盾！
   所以 q, r 唯一。所以 $\exists! q, r \in \mathbb{Z}, s.t. \quad a = bq + r, (0 \le r \le b-1)$.

4. 证明数学归纳法
   往证: 若集合 A 满足: $1 \in A, n \in A$, 那么有 $n+1 \in A$，则 A 一定是所有正整数的集合。
   设 A 是包含 1 的集合，并且如果它包含整数 n, 则一定包含整数 $n+1$. 假定 A 不是所有正整数的集合，则存在正整数 $x \notin A$.
   设 S 为不包含在 A 中的正整数集合。由良序性质，S 存在最小元 k, 由于 1 不在 S 中，所以 $k \ge 2$.
   因为 $k - 1 < k$，所以 $k - 1 \in A$, 根据假设，$k \in A$, 即 $k \notin S$. 矛盾！
   所以 A 是所有正整数的集合。

5. 证明: 每个大于 1 的整数都有素因子.
   反证法: 假设存在整数 > 1 且没有素因子，这些数组成非空集合 S.
   由良序公理, S 有最小元，设为 m, 因为 $m \mid m$ 且 m 没有素因子, 所以 m 不是素数 (如果 m 是素数，那么 m 就有了“素”因子 m, 不满足定义。所以 m 可以表示为 $m = ab, 0 < a < m, 0 < b < m$. 由 $a < n$ 可知 a 有素数因子，而 a 的素因子也是 m 的素因子，从而 n 有素因子。矛盾！结论成立。

6. 每个大于 1 的正整数都可以**唯一地**表示成非负素数的乘积，在乘积中的素因子按照非降序排列
   反证法，假设存在大于 1 的正整数无法表示成非负素数的乘积，它们组成非空集合 S
   由良序公理, S 中有最小元 n, 若 n 为素数，则 $n = n$ 是素数乘积，所以 n 是合数.
   设 $n = ab, a, b \in \mathbb{Z}^+, 1 < a \leq b < n$. 那么 $a, b \notin S$. 所以 a, b 可以写成非负素数乘积。进而 n 也可以写成非负素数乘积。矛盾!
   所以每个大于 1 的正整数都可以表示成非负素数的乘积
   下证此表示法唯一:
   假设存在两种表示: $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$, 且素因子非降序排列。
   约去等式两侧相同的素因子得到: $n = p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$, $u, v \geq 1$.
   那么有 p_{i_1} 整除左侧，不能整除右侧，矛盾！(由题 11 保证)
   所以表示是唯一的。

7. 证明: 若 n 是合数，则 n 一定有一个不超过 $\sqrt{n}$ 的素因子。
   设 $n = ab$, 不妨设 $0 < a \leq b < n$, 那么 $a^2 \leq ab = n$, 得到 $a \leq \sqrt{n}$. 否则若 $b \geq a > \sqrt{n}$, $ab > \sqrt{n} \cdot \sqrt{n} = n$.
   因为每个大于 1 的正整数都有素因子，所以 a 至少有一个素因子 $p \leq a$, 进而 p 也是 n 的因子，$p \leq \sqrt{n}$.

8. 证明: 两个不全为 0 的整数 a, b 的最大公因子是 a, b 线性组合中最小的正整数。
   设集合 $S = \{ma + nb \mid m, n \in \mathbb{Z}, ma + nb > 0\}$, 因为 $(a, -a, b, -b$ 中至少有一个属于 S, 所以 S 非空)。由良序公理，$d = ma + nb, m, n \in \mathbb{Z}$. 不妨设 $a \neq 0$, 往证 $d \mid a$
   设 $a = dq + r, 0 \leq r < d$, $r = a - dq = a - (ma + nb)q = (1 - qm)a - qnb$. 若 $r > 0$, 则 r 是 a, b 的线性组合，且 $r < d$, 矛盾！所以 $r = 0$.
   所以 $a = dq, d \mid a$. 同理 $d \mid b$, d 是 a, b 的公因子, 且是 a, b 线性组合中最小的正整数
   $\forall e \in \mathbb{Z}^+, e \mid a, e \mid b$, 有 $e \mid ma + nb = d$, 所以 $e \leq d$. 所以 d 是最大公因子。

9. $a, b \in \mathbb{Z}^+$, a, b 线性组合的集合与 (a, b) 倍数构成的集合等价
   设 $d = (a, b)$, 我们证明每个 a, b 的线性组合是 d 的倍数。
   注意到 $d \mid a, d \mid b$, 所以 $d \mid ma + nb$, 所以每个 a, b 的线性组合是 d 的倍数。
   现在证明每个 d 的倍数是 a, b 的线性组合:
   存在整数 r, s 使得 $(a, b) = ra + sb$, 进而 $kd = k(a, b) = (kr)a + (ks)b$. 所以每个 d 的倍数是 a, b 的线性组合。
   综上所述，$a, b \in \mathbb{Z}^+$, a, b 线性组合的集合与 (a, b) 倍数构成的集合等价。

10. 两个不全为 0 的整数 a, b, $d = (a, b)$ 当且仅当: (1).$d \mid a, d \mid b$ (2). 若 c 是整数且 $c \mid a, c \mid b$, 则 $c \mid d$.
    必要性: 已知 $d = (a, b)$, 则 $d \mid a, d \mid b$. 存在 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$, 若 $c \mid a, c \mid b$, 则 $c \mid ma + nb = d$.
    充分性: 对于 a, b 的任一公因子 c 有 $c \mid d$, 那么 $c \leq d$. 而 d 是 a, b 的公因子，即 d 是最大公因子，$d = (a, b)$

11. $a_1, a_2, \cdots, a_n \in \mathbb{Z}^+$, p 是素数，若 $p \mid a_1 a_2 \cdots a_n$，则存在 $a_i, i \in [1, n]$, 使得 $p \mid a_i$.
    使用数学归纳法: $n = 1$ 的情况是平凡的，假设对 n 成立。考虑 $n+1$ 个整数 $a_1 a_2 \cdots a_{n+1}$，它能被 p 整除。或者有 $(a_1 a_2 \cdots a_n, p) = 1$ 或者有 $(a_1 a_2 \cdots a_n, p) = p$. 如果 $(a_1 a_2 \cdots a_n, p) =$

1，则 $p \mid a_{n+1}$. 另一方面，如果 $(a_1a_2\cdots a_n, p) = p$，即 $p \mid a_1a_2\cdots a_n$, 由归纳假设 $p \mid a_i, i \in [1, n]$. 所以对 $n+1$ 命题成立。

12. 设 $a, b \in \mathbb{Z}, d = (a, b)$ ，方程 $ax + by = c$ 有整数解的充要条件是 $d \mid c$. 若 $x = x_0, y = y_0$ 是一组特解，则通解是 $x = x_0 + (b/d)n, y = y_0 - (a/d)n, n \in \mathbb{Z}$.
必要性: 假设方程有整数解 (x, y), 因为 $d \mid a, d \mid b$，则 $d \mid ax + by = c$.
充分性: 假设 $d \mid c = ax + by$. 因为存在 a, b 的线性组合 $as + bt = d$ 且 $d \mid c$, 所以有整数 e 使得 $de = c$, 即 $c = (as + bt)e = a(se) + b(te)$, 所以有整数解 $x_0 = se, y_0 = te$.
下面证明 $d \mid c$ 时有无穷多解:
往证: $x = x_0 + (b/d)n, y = y_0 - (a/d)n, \forall n \in \mathbb{Z}$ 是方程的解
因为 $ax + by = ax_0 + by_0 + a(b/d)n - b(a/d)n = ax_0 + by_0 = c$ 所以有无穷多解。
下面证明只能为上述形式的解:
假设 x, y 满足 $ax + by = c$, 因为 $ax_0 + by_0 = c$，有 $(ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0) = 0$，因此 $a(x - x_0) = b(y_0 - y)$, 进而 $(a/d)(x - x_0) = (b/d)(y - y_0)$. 因为 $(a/d, b/d) = 1$, 所以 $(a/d) \mid (y_0 - y)$, 所以存在整数 n 使得 $(a/d)n = (y_0 - y)$，即 $y = y_0 - (a/d)n$. 带入原方程得到 $x = x_0 + (b/d)n$

13. $a, b, c \in \mathbb{Z}$, 则 $(a + bc, b) = (a, b)$
一方面，设 $d = (a + bc, b)$，所以 $d \mid a + bc - bc = a, d \mid b$, 所以 $d \mid (a, b)$.
另一方面，存在 m, n 使得 $d = m(a + bc) + nb = ma + (cm + n)b$, 所以 d 是 a, b 的线性组合，设 $e = (a, b)$ 有 $e \mid a, e \mid b$ 所以 $e = (a, b) \mid d$
所以 $d = (a, b)$, 即 $(a + bc, b) = (a, b)$

14. $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+, a \equiv b \mod m$ 当且仅当存在整数 k 使得 $a = b + km$
必要性：因为 $a \equiv b \mod m$, 所以 $m \mid (a - b)$, 即 $\exists k \in \mathbb{Z}, a - b = km, a = b + km$.
充分性：$a - b = km$, 所以 $m \mid (a - b)$，所以 $a \equiv b \mod m$.

15. $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+, d = (c, m), ac \equiv bc \mod m$, 则 $a \equiv b \mod (m/d)$
因为 $ac \equiv bc \mod m$, 所以 $m \mid (ac - bc) = c(a - b)$，所以 $\exists k \in \mathbb{Z}, c(a - b) = km$
进而 $(c/d)(a - b) = k(m/d)$, 因为 $(c/d, m/d) = 1$, 所以 $(m/d) \mid (a - b)$, 即 $a \equiv b \mod (m/d)$

16. $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+, a \equiv b \mod m, c \equiv d \mod m$ 则: $a + c \equiv b + d \mod m, a - c \equiv b - d \mod m, ac \equiv bd \mod m$
(1). $(a+c)-(b+d) = (a-b)+(c-d)$, 因为 $m \mid a-b, m \mid c-d$ 所以 $m \mid (a+c)-(b+d)$, 即 $a + c \equiv b + d \mod m$
(2). $(a-c)-(b-d) = (a-b)-(c-d)$, 因为 $m \mid a-b, m \mid c-d$ 所以 $m \mid (a-c)-(b-d)$, 即 $a - c \equiv b - d \mod m$
(3). $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$, 因为 $m \mid a - b, m \mid c - d$ 所以 $m \mid (a - b)c + b(c - d) = ac - bd$, 即 $ac \equiv bd \mod m$

17. 若 $a_j \equiv b_j \mod m, j = 1, 2, \cdots, n$, m 是正整数，$a_j, b_j \in \mathbb{Z}$, 则 (1). $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} \mod m$, (2). $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} \mod m$
同上一题，数学归纳法可证.

18. 若 $a \equiv b \mod m, c \equiv d \mod n, a, b, c, d \in \mathbb{Z}, m, n \in \mathbb{Z}^+$ 下列结论是否成立?
(1). $a \pm c \equiv b \pm d \mod (m, n), ac \equiv bd \mod (m, n)$
(2). $a \pm c \equiv b \pm d \mod [m, n], ac \equiv bd \mod [m, n]$
(1). $m \mid a - b, n \mid c - d$. 设 $d = (m, n)$ 则 $d \mid m, d \mid n$, 进而 $d \mid a - b, d \mid c - d$, 又 $a \pm c \equiv b \pm d = (a - b) \pm (c - d)$, 所以 $d \mid (a - b) \pm (c - d) = a \pm c \equiv b \pm d$, 即 $a \pm c \equiv b \pm d \mod (m, n)$.
$ac - bd = (a - b)c + (c - d)b$, 同理可得 $d \mid ac - bd$, 即 $ac \equiv bd \mod (m, n)$
(2). 不成立。取 $a = 5, b = 3, m = 2, c = 7, d = 4, n = 3$。则 $[m, n] = 6$, 进而 $(a + c) - (b + d) = 5, ac - bd = 23, (a - c) - (b - d) = -1$, 它们都不能被 $[m, n] = 6$ 整除。

19. $r_1, r_2, \cdots r_m$ 是模 m 的完全剩余系，且正整数 a 使得 $(a, m) = 1$, 则对任意整数 b, $ar_1 + b, ar_1 + b, \cdots ar_m + b$ 是模 m 的完全剩余系
原命题等价于: $ar_i + b$ 任意两数模 m 不同余。
假设存在 $(ar_i + b) \equiv (ar_j + b) \mod m, i \nmid j$，则 $m \mid (ar_i + b) - (ar_j + b) = a(r_i - r_j)$.
因为 $(a, m) = 1$，所以 $m \mid (r_i - r_j)$, 即 $r_i \equiv r_j \mod m$. 矛盾!
所以，对任意整数 b, $ar_1 + b, ar_1 + b, \cdots ar_m + b$ 是模 m 的完全剩余系。

20. $m_1, m_2, \cdots m_k$ 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
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。

21. $a \equiv b \mod m_i, i = 1, 2, \cdots, k, a, b \in \mathbb{Z}, m_i \in \mathbb{Z}^+$，那么 $a \equiv b \mod [m_1, m_2, \cdots m_k]$.

引理: $[a, b] \mid c$ 当且仅当 $a \mid c$ 且 $b \mid c$
必要性: 因为 $[a, b] \mid c$, $a \mid [a, b]$, 所以 $a \mid c$。同理 $b \mid c$
充分性: 对 a, b, c 做最小素分解, $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, c = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$. 若 $a \mid c$ 且 $b \mid c$，则 $r_i \leq c_i, s_i \leq c_i$，进而 $\max(r_i, s_i) \leq c_i$，
所以 $[a, b] = p_1^{\max(s_1, r_1)} p_2^{\max(s_2, r_2)} \cdots p_k^{\max(s_k, r_k)} \mid c$，即 $[a, b] \mid c$

因为 $a \equiv b \mod m_i, i = 1, 2, \cdots, k$, 所以 $m_i \mid (a - b), i = 1, 2, \cdots, k$
由上述引理，得到 $[m_1, m_2, \cdots m_k] \mid (a - b)$
所以 $a \equiv b \mod [m_1, m_2, \cdots m_k]$.

22. $a, b, m \in \mathbb{Z}, m \in \mathbb{Z}^+, (a, m) = d$。若 $d \nmid b$，则 $ax \equiv b \mod m$ 无解；若 $d \mid b$, 则 $ax \equiv b \mod m$ 恰有 d 个模 m 不同余的解
线性同余方程 $ax \equiv b \mod m$ 等价于二元线性丢番图方程 $ax - my = b$, x 是原方程的解当且仅当 $\exists y \in \mathbb{Z}$ 使得 $ax - my = b$.

由 12 题可知:$d \nmid b$ 时，$ax - my = b$ 无整数解。

$d \mid b$ 时，有无穷多解，通解为 $x = x_0 + (m/d)n, y = y_0 + (a/d)n$, 即原方程有无穷多解 x 满足 $x = x_0 + (m/d)n$ 的形式。

下证模 m 互不同余的解有 d 个:

考虑 $x_1 = x_0 + (m/d)n_1, x_2 = x_0 + (m/d)n_2$ 使得 $x_1 \equiv x_2 \mod m$ 即 $x_0 + (m/d)n_1 \equiv x_0 + (m/d)n_2 \mod m$. 进而 $(m/d)n_1 \equiv (m/d)n_2 \mod m$, 又 $(m, m/d) = m/d$ 所以由 15 题得: $n_1 \equiv n_2 \mod m/(m/d) = d$.

进而原方程的解由 $x_0+(m/d)n$ 给出,其中 n 取遍 d 的一个完全剩余系,如 $n = 0, 1, \cdots d-1$.

所以原方程有 d 个模 m 不同余的解。

23. 证明同余方程 $x^2 \equiv 1 \mod 2^k$ 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

$k > 2$ 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 $x \equiv \pm 1 \mod 2^2$

类似地可以证明，$x^2 \equiv 1 \mod p^k$, p 为奇数时，可以得到 2 个解 $x \equiv \pm 1 \mod p^k$

24. 中国剩余定理 (Chinese Remainder Theorem):

设 $m_1, m_2, \cdots, m_r$ 是两两互素的正整数，同余方程组:

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

有模 $M = m_1 m_2 \cdots m_r$ 的唯一解

存在性: 构造同余方程组的一个联立解，令 $M_i = M/m_i$, 因为 $m_1, m_2, \cdots, m_r$ 是两两互素的正整数, 所以 $(M_i, m_i) = 1$.

设 $M_k y_k \equiv 1 \mod m_k$, 即 M_k 模 m_k 的逆是 y_k.

构造和

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

往证 x 为上述 r 个同余方程的联立解：

因为 $j \neq k$ 时，$m_j \mid M_k$, 所以 $x \equiv a_k M_k y_k \mod m_k$. 又 $a_k M_k y_k \equiv a_k \mod m$, 所以 $x \equiv a_k \mod m_k$.

唯一性: 即任意两个解模 M 同余:

假设 x_1, x_2 均为方程组的联立解。则由 $x_1 \equiv x_2 \mod m_k, \forall k$. 由 21 题, $x_1 \equiv x_2 \mod M = [m_1, m_2, \cdots, m_r] = m_1 m_2 \cdots m_r$. 因此，任意两个解模 M 同余。

25. 求同余方程 $2x^3 + 7x - 4 \equiv 0 \mod 100$.

因为 $100 = 2^2 5^2$, 所以同余方程变换为:

$$2x^3 + 7x - 4 \equiv 0 \mod 4$$

$$2x^3 + 7x - 4 \equiv 0 \mod 25$$

因为 $2x^3 + 7x - 4 \equiv 0 \mod 4$，所以 x 一定为偶数。对 $x = 0, 1, 2, 3$ 一一验证得到 $x \equiv 0 \mod 4$ 是解。

为了求解 $2x^3 + 7x - 4 \equiv 0 \mod 25$ 的解，我们观察 $2x^3 + 7x - 4 \equiv 0 \mod 5$ 的解为 $x \equiv 1 \mod 5$(显然，前者的解也是后者的解，后者的解不一定是前者的解, 我们将对后者的解加以约束，来求得前者的解). 所以 $x = 1 + 5t$, 带入原方程:$2(1 + 5t)^3 + 7(1 + 5t) - 4 \equiv 0 \mod 25$，化简得到 $65t + 5 \equiv 15t + 5 \equiv 0 \mod 5$, 消去因子 $(5, 5) = 5$ 得到 $3t + 1 \equiv 0 \mod 5$, 所以解为 $t \equiv 3 \mod 5$.

这说明模 25 的解是 $x \equiv 1 + 5t \equiv 1 + 5 * 3 \equiv 16 \mod 25$, 进而我们得到线性同余方程:

$$x \equiv 0 \mod 4$$

$$x \equiv 16 \mod 25$$

使用中国剩余定理得到解为:$x \equiv 16 \mod 100$