王鸣一 第五次作业，2023211475.

1. ①求 $(256, 337)$ $337 = 256 + 81$ 即 $(256, 337) = 1$

$256 = 81 \times 3 + 13$

$81 = 13 \times 6 + 3$

$13 = 3 \times 4 + 1$

② 求 $a^{-1} \pmod m$

$256 x_1 \equiv 1 \bmod 337$

$1 = 13 - 3 \times 4$

$= 13 - 4 \times (81 - 13 \times 6)$

$= -4 \times 81 + 25 \times 13$

$= -4 \times 81 + 25 \times (256 - 3 \times 81)$

$= -79 \times 81 + 25 \times 256$

$= 25 \times 256 - 79 \times (337 - 256)$

$= -79 \times 337 + 104 \times 256$

即 $x_1 = 104$ $x_0 \equiv 104 \pmod{337}$

$x' \equiv \overset{179}{\cancel{256}} \times 104 \cancel{+104} \pmod{337}$

$x \equiv 81 \pmod{337}$

$x \equiv 81 + 104t \pmod{337}$

$t = 0$,

即 $x \equiv 81 \pmod{337}$

2. ①求 $(28, 35) = 7$.

② ~~求~~ $4x \equiv 1 \bmod 5$.

求 $4^{-1} \pmod 5$ $4 \times 4 = 16$

即为4

③ $x_1 \equiv 3 \times 4 \pmod 5$

$\equiv 2 \pmod 5$

④ $x \equiv 2\cancel{x} + 5t \pmod{35}$ $t = 0, 1, 2 \cdots 6$.

即 $x \equiv 2 + 5t \pmod{35}$ $t = 0, 1, 2, \cdots 6$.

3. $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$ $b_1 = 1$ $b_2 = 2$, $b_3 = 4$ $k = 3 \times 4 \times 5 = 60$

$M_1 = 20$. $M_1 \cdot M_1^{-1} \equiv 1 \pmod 3$ $M_2 = 15$. $M_2 \cdot M_2^{-1} \equiv 1 \pmod 4$

$M_1^{-1} = 2$ $M_2^{-1} = 3$

$M_3 = 12$. $M_3 \cdot M_3^{-1} \equiv 1 \pmod 5$

$M_3^{-1} = 3$

$x \equiv b_1 M_1 M_1^{-1} + b_2 M_2 M_2^{-1} + b_3 M_3 M_3^{-1} = 274 \pmod{60}$

$x \equiv 34 \pmod{60}$ 即这个数最小是34.

4. $77=7\times 11$

$2^3=8$. $8\equiv 1 \pmod 7$

$2^{10}=1024$ $1024\equiv 1 \pmod{11}$

$$\begin{array}{r} 674 \\ 3\overline{)2024} \\ 18 \\ \hline 22 \\ 21 \\ \hline 14 \\ 12 \\ \hline 2 \end{array}$$

即 $2^{2024}\equiv 4 \pmod 7$

$2^{2024}\equiv 16 \pmod{11}$

$\equiv 5 \pmod{11}$

即求 $\begin{cases} x\equiv 4 \pmod 7 \\ x\equiv 5 \pmod{11} \end{cases}$

$b_1=4$ $k=77$ $M_1=11$ $M_2=7$

$b_2=5$.

$M_1\cdot M_1^{-1}\equiv 1 \pmod 7$ $M_2\cdot M_2^{-1}\equiv 1 \pmod{11}$

$M_1^{-1}=2$ $M_2^{-1}=8$.

$x\equiv 4\times 11\times 2+5\times 7\times 8 \pmod{77}$

$x\equiv 60 \pmod{77}$

即 $2^{2024} \bmod 77$ 为 60.