信安数基第3次作业-冯尔亨-2022302181

1. $17x \equiv 14 \pmod{21}$

∵ $(17, 21) = 1$，先计算 $17x \equiv 1 \pmod{21}$，利用辗转相除法得除法，

$21 = 17 \times 1 + 4$

$17 = 4 \times 4 + 1$

$1 = 17 - 4 \times 4 = 17 - 4 \times (21 - 17) = 5 \times 17 - 4 \times 21$

解得一个特解 $x_0 \equiv 5 \pmod{21}$

则原方程有一个特解 $x_0' \equiv 14 x_0 \pmod{21}$ $\equiv 14 \times 5 \pmod{21} \equiv 7 \pmod{21}$

则原方程的所有解为 $x \equiv 7 + t \cdot \frac{21}{(17,21)} \pmod{21}$，当 $t = 0$ 时，解为 $x = 7$

2. 证明：同余方程组 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ 有解当且仅当 $(m_1, m_2) \mid (a_1 - a_2)$

并证明若有解，该解模 $[m_1, m_2]$ 是唯一的.

证明：(1) 设 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ 有解，故 $\begin{cases} x = a_1 + sm_1 & ① \\ x = a_2 + tm_2 & ② \end{cases}$

①-②有 $a_1 - a_2 + sm_1 - tm_2 = 0$ 故有 $sm_1 - tm_2 = a_2 - a_1$ ③

由贝祖公式的判定条件，若上述方程有解，则有 $(m_1, m_2) \mid (a_1 - a_2)$

(2) 由③ $\frac{sm_1}{(m_1, m_2)} - \frac{tm_2}{(m_1, m_2)} = \frac{a_2 - a_1}{(m_1, m_2)}$ ④ 可化简为

则 $\left(\frac{m_1}{(m_1, m_2)}, \frac{m_2}{(m_1, m_2)}\right)$ 互素 $s' \frac{m_1}{(m_1, m_2)} - t' \frac{m_2}{(m_1, m_2)} = 1$ ⑤

解上述二元一次不定方程可得到一组特解 $\begin{cases} s = s_0 \\ t = t_0 \end{cases}$

从而该方程有一切通解 $\begin{cases} s = s_0 + k \frac{m_2}{(m_1, m_2)} \\ t = t_0 + k \frac{m_1}{(m_1, m_2)} \end{cases}$ 将通解代入①②得

则该解模 $[m_1, m_2]$ 是唯一的

1705546

19. ii) $23x \equiv 1 \pmod{140}$;

原式可转化为同余方程组 $\begin{cases} 23x \equiv 1 \pmod 4 \\ 23x \equiv 1 \pmod 5 \\ 23x \equiv 1 \pmod 7 \end{cases}$ 采用中国剩余定理

$m = 4\times5\times7 = 140$

$m_1 = 5\times7 = 35$, $m_2 = 4\times7 = 28$, $m_3 = 4\times5 = 20$.

又 $M_i' \cdot M_i \equiv 1 \pmod{m_i}$ 解得 $\begin{cases} M_1' \equiv 3 \pmod 4 \\ M_2' \equiv 2 \pmod 5 \\ M_3' \equiv 6 \pmod 7 \end{cases}$

$\therefore \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$

则 $x \equiv 3\times35\times3 + 2\times28\times2 + 4\times20\times6 = 67 \pmod{140}$

iii) $17x \equiv 229 \pmod{1540}$

原式可转化为同余式组 $\begin{cases} 17x \equiv 4 \pmod 5 \\ 17x \equiv 1 \pmod 4 \\ 17x \equiv 5 \pmod 7 \\ 17x \equiv 9 \pmod{11} \end{cases}$

$M = 4\times7\times11 = 308$

$M_2 = 5\times7\times11 = 385$

$M_3 = 5\times4\times11 = 220$

$M_4 = 5\times4\times7 = 140$

$M_1' \equiv 2 \pmod 5$

$M_2' \equiv 1 \pmod 4$

$M_3' \equiv 5 \pmod 7$

$M_4' \equiv 7 \pmod{11}$

$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$ 由中国剩余定理

$x \equiv 2\times308\times2 + 1\times385\times1 + 4\times220\times5 + 7\times140\times7$

$\equiv 557 \pmod{1540}$

23. $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod 7$

原式可化为 $r(x) = x^6 + 2x^5 + 2x^3 + 15x^2 + 5x \equiv 0 \pmod 7$

$x^7 - x$ 除 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x$

商 $3x^7 + 4x^6 + 2x^4 + x^2 + 3x + 4$

$3x^{14} - 3x^8$

$4x^{13} + 2x^{11} + x^9 + x^8 + x^6$

$4x^{13} - 4x^7$

$2x^{11} + x^9 + 3x^8 + 4x^7 + x^6$

$2x^{11} - 2x^5$

$x^9 + 3x^8 + 4x^7 + x^6 + 2x^5$

$x^9 - x^3$

$3x^8 + 4x^7 + x^6 + 2x^5 + 2x^3$

$3x^8 - 3x^2$

$4x^7 + x^6 + 2x^5 + 2x^3 + 15x^2 + x$

$r(0) = 0 \pmod 7$

$r(1) = 4 \pmod 7$

$r(2) = 4 \pmod 7$

$r(3) = 5 \pmod 7$

$r(4) = 1 \pmod 7$

$r(5) = 6 \pmod 7$

$r(6) = 0 \pmod 7$

故同余式的解为 $x \equiv 0, 6 \pmod 7$

24. $f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{243}$

$f'(x) = 4x^3 + 7 \pmod{243}$

直接验算 $f(x) \equiv 0 \pmod 3$ 有一解 $x_1 \equiv 1 \pmod 3$

以 $x = 1 + 3t_1$ 代入 $f(x) \equiv 0 \pmod 9$ 得

$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9$

$\because f(1) \equiv 3 \pmod 9,\ f'(1) \equiv 2 \pmod 9$

故此同余式可写成 $3 + 3t_1 \cdot 2 \equiv 0 \pmod 9$

即 $2t_1 \equiv -1 \pmod 3$ $t_1 \equiv 1 \pmod 3$

故 $f(x) \equiv 0 \pmod 9$ 解为 $x_2 \equiv 1 + 3t_1 = 4 \pmod 9$

再以 $x = 4 + 9t_2$ 代入 $f(x) \equiv 0 \pmod{27}$ 得

$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}$

$f(4) \equiv 18 \pmod{27}$ $f'(4) \equiv 20 \pmod{27}$

故此同余式可写成 $18 + 9t_2 \cdot 20 \equiv 0 \pmod{27}$

即 $20t_2 \equiv -2 \pmod 3$

$t_2 \equiv 2 \pmod 3$

同余式 $f(x) \equiv 0 \pmod{27}$ 解为 $x_3 = 4 + 9t_2 \equiv 22 \pmod{27}$

再以 $x = 22 + 27t_3$ 代入 $f(x) \equiv 0 \pmod{81}$ 得

$f(22) + 27t_3 f'(22) \equiv 0 \pmod{81}$

$f(22) \equiv 0 \pmod{81},\ f'(22) \equiv 74 \pmod{81}$

即 $27 \times t_3 \times 74 \equiv 0 \pmod{81}$

$74t_3 \equiv 0 \pmod 3$

$t_3 \equiv 0 \pmod 3$ $x_4 \equiv 22 \pmod{81}$

再以 $x = 22 + 81t_4$ 代入 $f(x) \equiv 0 \pmod{243}$

$f(22) = 162 \pmod{243}$ $f'(22) \equiv 74 \pmod{243}$

~~即 $4t_4^3 + 3t_4 + 7 \equiv 0 \pmod{243}$~~ $162 + 81t_4 \times 74 \equiv 0 \pmod{243}$

~~即 $2 + t_4 \equiv 4 \pmod{243}$~~ 即 $2 + 74t_4 \equiv 0 \pmod 3$

~~解得 $t_4 \equiv 58 \pmod{243}$~~ $t_4 \equiv 2 \pmod 3$

$t_4 \equiv$ 代入得 $x = 22 + 81 \times 2 \equiv 184 \pmod{243}$