第 7次课后作业

1. $\left(\dfrac{127}{715}\right) = \left(\dfrac{127}{5}\right) \times \left(\dfrac{127}{143}\right) = (-1)^{\frac{4}{2}\cdot\frac{126}{2}} \left(\dfrac{2}{5}\right) \times (-1)^{\frac{126}{2}\cdot\frac{142}{2}} \left(\dfrac{16}{127}\right)$

$715 = 5 \times 143$ $\qquad\qquad = (-1) \times (-1) = 1$

2. $p = 401$, $p-1 = 400 = 2^4 \times 100 = 2^4 \times 25$ $\quad t = 4, s = 25,$

$\left(\dfrac{2}{401}\right) = (-1)^{\frac{401^2-1}{8}} = 1$. $\qquad \left(\dfrac{3}{401}\right) = (-1)^{\frac{2}{2}\cdot\frac{400}{2}} \cdot \left(\dfrac{2}{3}\right) = -1$ 即 $n = 3$

求 a^{-1}: $401 = 41 \times 9 + 32$ $\qquad 1 = 5-4$ $\qquad\qquad = 2 \times 32 - 7 \times 9$

$41 = 32 \times 1 + 9$ $\qquad = 5 - (9-5)$ $\qquad\qquad = 2 \times 32 - 7 \times (41-32)$

$32 = 9 \times 3 + 5$ $\qquad = 2 \times 5 - 9 = -9 + 2 \times 5$ $\quad = 9 \times 32 - 7 \times 41$

$9 = 5 \times 1 + 4$ $\qquad \overline{= 2 \cdot 5 - 9 + 1}$ $\qquad\quad = -7 \times 41 + 9 \times (401 - 9 \times 41)$

$5 = 4 + 1$ $\qquad\quad = -9 + 2 \times (32 - 3 \times 9)$ $\quad = -88 \times 41 + 9 \times 401$

$a^{-1} = -88 = 313$

$b = 3^{25} \bmod 401 = 268$

$k = $ $\quad X_3 = 41^{13} \bmod 401 = 338$.

$k = 1$, $X_2 = 338 \times 268^{j_0 \times 2^0}$

求 j_0: $(313 \times 338^2)^4 \equiv 1 \pmod{p}$ $\qquad j_0 = 0$. $\qquad X_2 = 338$

$k = 2$ j_1: $(313 \times 338^2)^{2^1} \equiv 1 \pmod{p}$ $\qquad j_1 = 0$. $\quad X_1 = 338$

$k = 3$ j_2: $(313 \times 338^2)^1 \equiv -1 \pmod{p}$ $\quad j_2 = 1$. $\quad X_0 = 338 \times 268^4 \bmod p = 344$

$401 - 344 = 57$.

即 $x \equiv 57 \pmod{401}$ 和 $x \equiv 344 \pmod{401}$ 是 $x^2 \equiv 41 \pmod{401}$ 的两个解

3. $5x^2 + 3x - 4 \equiv 0 \bmod 10$ 令 $y = 5x^2 + 3x - 4$.

$x = 0$ $\quad y = -4$ 不成立 $\qquad\qquad x = 7$, $y \equiv 2 \pmod{10}$ 不成立

$x = 1$ $\quad y = 4$ 不成立 $\qquad\qquad x = 8$, $y \equiv 0 \pmod{10}$ 不成立

$x = 2$ $\quad y \equiv 2 \pmod{10}$ 不成立 $\quad x = 9$, $y \equiv 8 \pmod{10}$ 不成立

$x = 3$ $\quad y \equiv 0 \pmod{10}$ 成立

$x = 4$ $\quad y \equiv 8 \pmod{10}$ 不成立

$x = 5$, $y \equiv 6 \pmod{10}$ 不成立 $\qquad\qquad$ 即 $x \equiv 8 \pmod{10}$

$x = 6$, $y \equiv 4 \pmod{10}$ 不成立 $\qquad\qquad\qquad x \equiv 3 \pmod{10}$

4. $49x^5 + 25x^3 - 6x^2 + 3x - 10 \equiv 0 \bmod 23$

$49 \equiv 3 \ (\bmod\ 23)$ $23 = 3 \times 7 + 2$ $1 = 3 - 2$
$\qquad\qquad\qquad\qquad 3 = 2 + 1 \qquad\quad = 3 - (23 - 3 \times 7)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad = 8 \times 3 - 23$

$3x^5 + 2x^3 - 6x^2 + 3x - 10 \equiv 0 \ (\bmod\ 23)$

$\times 8:$ $24x^5 + 16x^3 - 48x^2 + 24x - 80 \equiv 0 \ (\bmod\ 23)$

$\underline{x^5 + 16x^3 - 2x^2 + x - 11 \equiv 0 \ (\bmod\ 23)}$

5. $\frac{1}{x^7} \ (x^7 - x) \equiv 0 \ (\bmod\ 7)$

$$
\begin{array}{r}
2x^{11} + 5x^9 - 20x^6 + 2x^5 - 3x^4 + 30x^3 + 4x - 20 \\
\hline
\end{array}
$$

$x^7 - x \overline{\big)\, 2x^{18} + 5x^{16} - 20x^{13} - 3x^{11} + 15x^{10} + 4x^8 + 16x^6 - x^3 + 5x + 8}$

$\underline{2x^{18} - 2x^{12}}$

$\quad 5x^{16} - 20x^{13} + 2x^{12} - 3x^{11} + 15x^{10} + 4x^8 + 16x^6 - x^3 + 5x + 8$

$\quad \underline{5x^{16} - 5x^{10}}$

$\quad -20x^{13} + 2x^{12} - 3x^{11} + 30x^{10} + 4x^8 + 16x^6 - x^3 + 5x + 8$

$\quad \underline{-20x^{13} + 20x^7}$

$\qquad 2x^{12} - 3x^{11} + 30x^{10} + 4x^8 - 20x^7 + 16x^6 - x^3 + 5x + 8$

$\qquad \underline{2x^{12} - 2x^6}$

$\qquad -3x^{11} + 30x^{10} + 4x^8 - 20x^7 + 18 x^6 \mp x^3 + 5x + 8$

$\qquad \underline{-3x^{11} + 3x^5}$

$\qquad\quad 30x^{10} + 4x^8 - 20x^7 + 18 x^6 - 3x^5 \mp x^3 + 5x + 8$

$\qquad\quad \underline{30x^{10} - 30x^4}$

$\qquad\qquad 4x^8 - 20x^7 + 18x^6 - 3x^5 + 30x^4 \mp x^3 + 5x + 8$

$\qquad\qquad \underline{4x^8 - 4x^2}$

$\qquad\qquad -20x^7 + 18x^6 - 3x^5 + 30x^4 - x^3 + 4x^2 + 5x + 8$

$\qquad\qquad \underline{-20x^7 + 20x}$

$\qquad\qquad\qquad 18x^6 - 3x^5 + 30x^4 - x^3 + 4x^2 - 15x + 8$

即 有 $18x^6 - 3x^5 + 30x^4 - x^3 + 4x^2 - 15x + 8 \equiv 0 \ (\bmod\ 7)$