第三章课后习题

P_{121}-123. 习题 (1), (3), (17)

P_{123}. 习题 (16), (18), (23), (24)

(1) ① $3x\equiv 2 \pmod 7$

直接检验，得 $x\equiv 3 \pmod 7$　　✗ 不能这么草率重写.

② $6x\equiv 3 \pmod 9$ 等价于 $2x\equiv 1 \pmod 3$

直接检验，得 $x\equiv 2 \pmod 3$

① ∵ $(3,7)=1|2$

∴ 有解.

令 $a=3$, $b=2$, $m=7$

$\frac{a}{(a,m)}=3$　$\frac{b}{(a,m)}=2$, $\frac{m}{(a,m)}=7$

求 x_0, 有 $\frac{a}{(a,m)}x_0\equiv 1 \left(\bmod \frac{m}{(a,m)}\right)$

即 $3x_0\equiv 1 \pmod 7$, 得 $x_0=5 \pmod 7$

∴ 特解 $x_1\equiv x_0\cdot\frac{b}{(a,m)}\equiv 5\cdot 2\equiv 3 \pmod 7$

∴ $ax\equiv b \pmod m$ 的解为 $x\equiv 3+7t \pmod 7$

② $6x\equiv 3 \pmod 9$

∵ $(6,9)=3|3$

∴ 有解

令 $a=6$, $b=3$, $m=9$

$\frac{a}{(a,m)}=2$, $\frac{b}{(a,m)}=1$, $\frac{m}{(a,m)}=3$

求 x_0, 有 $\frac{a}{(a,m)}x_0\equiv 1 \left(\bmod \frac{m}{(a,m)}\right)$

即 $2x_0\equiv 1 \pmod 3$, $x_0\equiv 2 \pmod 3$

∴ 特解 $x_1\equiv x_0\cdot\frac{b}{(a,m)}\equiv 2 \pmod 3$

∴ $ax\equiv b \pmod m$ 的解为 $(2+3t) \pmod 9$

③ $17x \equiv 14 \pmod{21}$

$\because (17, 21) = 1 \mid 14$

$\therefore$ 有解

求 x_0 满足 $17x_0 \equiv 1 \pmod{21}$

得 $x_0 \equiv 5 \pmod{21}$

$\therefore$ 特解 $x_1 \equiv 5 \cdot \frac{b}{(a,m)} \equiv 5 \times 14 = 7 \pmod{21}$

$\therefore 17x \equiv 14 \pmod{21}$ 解为 $7 \pmod{21}$

④ $15x \equiv 9 \pmod{25}$

$\because (15, 25) = 5 \nmid 9$

$\therefore$ 无解

(3) $m_1 = 5,\ m_2 = 6,\ m_3 = 7,\ m_4 = 11$ 互素

$M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2310$

$$\begin{cases} M_1 = \frac{M}{m_1} = 462 \\ M_2 = \frac{M}{m_2} = 385 \\ M_3 = \frac{M}{m_3} = 330 \\ M_4 = \frac{M}{m_4} = 210 \end{cases}$$

求解 $\begin{cases} M_1 M_1' \equiv 1 \pmod{5} \\ M_2 M_2' \equiv 1 \pmod{6} \\ M_3 M_3' \equiv 1 \pmod{7} \\ M_4 M_4' \equiv 1 \pmod{11} \end{cases}$ 得 $\begin{cases} M_1' \equiv 3 \pmod{5} \\ M_2' \equiv 1 \pmod{6} \\ M_3' \equiv 1 \pmod{7} \\ M_4' \equiv 1 \pmod{11} \end{cases}$

$462 M_1' \equiv 1 \pmod{5}$

$2M_1' \equiv 1 \pmod{5}$ $\qquad 2)M_1' \equiv 1 \pmod{6}$

385 $\qquad$ 6 $\qquad$ M_1'

$\therefore$ 解 $x \equiv 462 \times 3 b_1 + 385 \times 1 b_2 + 330 \times 1 b_3 + 210 \times 1 b_4$

(7) 注意跟(1)的不同

① $5x \equiv 3 \pmod{14}$

$\because (5, 14) = 1 \mid 3$ $\therefore$ 有解

$\varphi(14) = \varphi(2) \cdot \varphi(7) = 1 \times 6 = 6$

$\therefore$ 由欧~~拉~~定理得 $5^{\varphi(14)} = 5^6 \equiv 1 \pmod{14}$

$\therefore x_0 \equiv 5^5 \times 3 \equiv 9 \pmod{14}$

② $(4, 15) = 1 \mid 17$

$\therefore$ 有唯一解

$\therefore \varphi(15) = \varphi(3)\varphi(5) = 2 \times 4 = 8$

$\therefore 4^8 \equiv 1 \pmod{15}$

$\therefore\ x \equiv 4^7 \times 7 \equiv 7/4 \equiv 28/16 \equiv 13/1 \equiv 13 \pmod{15}$ 注意这化简

③ 略.

(16) ① $\begin{cases} x+2y \equiv 1 \pmod 7 & a. \\ 2x+y \equiv 1 \pmod 7 & b. \end{cases}$

$2b:\ 4x+2y \equiv 2 \pmod 7$

$2b-a:\ 3x \equiv 1 \pmod 7$

解得 $x \equiv 5 \pmod 7$

代入 b: $y+3 \equiv 1 \pmod 7$

解得 $y \equiv 5 \pmod 7$

② $\begin{cases} x+3y \equiv 1 \pmod 7 & a. \\ 3x+4y \equiv 2 \pmod 7 & b. \end{cases}$

$3a:\ 3x+9y \equiv 3 \pmod 7$

$3a-b:\ 5y \equiv 1 \pmod 7$

解得 $y \equiv 3 \pmod 7$

代入 a. $x+2 \equiv 1 \pmod 7$

解得 $x \equiv 6 \pmod 7$

(17) $312^{13} \pmod{667}$

$13 = 2^3 + 2^2 + 2^0$

$\therefore n_0 = 1,\ a_0 \equiv 312,\ b_1 \equiv 312^2 \equiv \_\_ \bmod 667$

$n_1 = 0,\ a_1 = a_0 = 312$ ... 手算还是太大了

故发现 $667 = 23 \times 29$

等价于 $\begin{cases} 312^{13} \equiv b_1 \pmod{23} \\ 312^{13} \equiv b_2 \pmod{29} \end{cases}$

求解得 $\begin{cases} b_1=8 \\ b_2=4 \end{cases}$

$\therefore$ 求 $\begin{cases} x\equiv 8 \pmod{23} \\ x\equiv 4 \pmod{29} \end{cases}$ 得 $x\equiv 468 \pmod{667}$

(18) $1309 = 7\times 11\times 17$

$\therefore \varphi(1309)=\varphi(7)\varphi(11)\varphi(17)=6\times 10\times 16=960$

$\therefore 2^{\varphi(1309)}\equiv 2^{960}\equiv 1 \pmod{1309}$

$\therefore 2^{1000000}\equiv x$ 也不好算

等价 $\begin{cases} 2^{1000000}\equiv b_1 \pmod 7 \\ 2^{1000000}\equiv b_2 \pmod{11} \\ 2^{1000000}\equiv b_3 \pmod{17} \end{cases}$ 又 $\because \begin{cases} 2^6\equiv 1 \pmod 7 \\ 2^{10}\equiv 1 \pmod{11} \\ 2^{16}\equiv 1 \pmod{17} \end{cases}$

得 $x\equiv 562 \pmod{1309}$

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

由费马小定理得，$x^7-x\equiv 0 \pmod 7$

$r_0(x)=f(x)-3x^7(x^7-x)=14x^{13}+2x^{11}+x^9+3x^8+x^6+x^3+12x^2+x$

$r_1(x)=r_0(x)-14x^6(x^7-x)\ \cdots\cdots$

最终得 $r(x)=x(x^5+2x^4+2x^2+15x+5)\equiv 0 \pmod 7$

直接检验 $0,\pm 1,\pm 2,\pm 3$ 得解为 $x\equiv 0,6 \pmod 7$

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

$243=3^5$

求解 $f(x)=x^4+7x+4\equiv 0 \pmod 3$

得特解为 $x\equiv 1 \pmod 3$

$f'(x_1)\equiv 4\times 1^3+7\equiv -1 \pmod 3$

$f'(x_1)^{-1}\equiv -1 \pmod 3$

由$\begin{cases} f(x_1)=1^4+7+4=12 \\ f(x_2)=4^4+7\times4+4=288 \\ f(x_3)=22^4+7\times22+4=234414 \\ f(x_4)=234414 \end{cases}$

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

的解为 $x_5\equiv 184 \pmod{243}$