18340087 信息安全数学基础--第三次作业

(1)

①

由扩展欧几里得算法：

$$-2 \times 3 + 7 = 1$$

所以，

$$-2 \times 3x \equiv -2 \times 2 \pmod 7$$

$$x \equiv 3 \pmod 7$$

②

$$(6, 9) = 3$$

因为

$$3 \mid 3$$

所以该方程有解。

由扩展欧几里得算法：

$$-1 \times 2 + 3 = 1$$

所以，

$$x \equiv 2 + 3k \pmod 9,\ k \in Z$$

③

由扩展欧几里得算法：

$$5 \times 17 + -4 \times 21 = 1$$

所以，

$$x \equiv 7 \pmod{21}$$

④

$$(15, 25) = 5$$

因为

$$(5 \mid 9) = false$$

所以原方程无解。

(3)

计算可得:

$$M_1 = 462$$

$$M_2 = 385$$

$$M_3 = 330$$

$$M_4 = 210$$

$$M_1^{'} = 3$$

$$M_2^{'} = 1$$

$$M_3^{'} = 1$$

$$M_4^{'} = 1$$

所以，结果为:

$$x \equiv 1386b_1 + 365b_2 + 330b_3 + 210b_4 \pmod{2310}$$

(5)

显然地，当$x = \pm 1$时，有

$$x^2 \equiv 1 \pmod{p^k}$$

如果$p = 2, \ k = 1$，有

$$(\pm 2)^2 \equiv 0 \pmod{2}$$

所以也成立。

假设有

$$x^2 \equiv 1 \pmod{p^k}$$

$$x \equiv t \pmod{p^k}, \ t \neq \pm 1$$

当$p = 2, \ k = 1$不同时成立时:

$$x^2 \equiv 1 \pmod{p^k}$$

$$p^k \mid (x+1)(x-1)$$

由唯一分解定理，可知有且仅有一个a，使得:

$$x + 1 = a * p^{\alpha}, \ p \mid a = false$$

如果$\alpha = 0$，那么，

$$p^k|(x-1)$$

$$x \equiv 1 \pmod{p^k}$$

这与假设矛盾，不成立。

如果$\alpha \geq k$，那么，

$$x = ap^{\alpha} - 1$$

$$x \equiv -1 \pmod{p^k}$$

也与假设矛盾。所以有

$$1 \leq \alpha \leq k - 1$$

这样一来，必定有

$$p \mid (x - 1)$$

但是，

$$x - 1 = ap^{\alpha} - 2$$

由于

$$p \not| 2$$

$$p \mid ap^{\alpha}$$

所以

$$p \not| ap^{\alpha} - 2$$

$$p \not| (x - 1)$$

矛盾。所以这样的x不存在。

综上，x的解为

$$x \equiv \pm 1 \pmod{p^k}$$

(7)

①

$$\phi(14) = 6$$

所以有

$$5^6 x \equiv 3 \times 5^5 \pmod{14}$$

$$x \equiv 9 \pmod{14}$$

②

$$\phi(15) = 8$$

所以有

$$4^8 x \equiv 7 \times 4^7 \pmod{15}$$

$$x \equiv 13 \pmod{15}$$

③

$$\phi(16) = 8$$

所以有

$$3^8 x \equiv 5 \times 3^7 \pmod{16}$$

$$x \equiv 7 \pmod{16}$$

8

这个问题相当于解同余方程

$$\begin{pmatrix} x \bmod 2 = 1 \\ x \bmod 3 = 1 \\ x \bmod 5 = 1 \\ x \bmod 7 = 1 \\ x \bmod 11 = 0 \end{pmatrix}$$

由前四个方程，可以得到：

$$x \equiv 1 \pmod{210}$$

将这个方程和第5个方程组合：

$$11k \equiv 1 \pmod{210}$$

得到

$$k \equiv 191 \pmod{210}$$

所以

$$x = 2101 \pmod{2310}$$

(12)

计算可得：

$$M_1 = 110$$

$$M_2 = 99$$

$$M_3 = 90$$

$$M_1^{'} = 5$$

$$M_2^{'} = 9$$

$$M_3^{'} = 6$$

所以，结果为：

$$x \equiv 550b_1 + 891b_2 + 540b_3 \pmod{990}$$

(15)

计算可得：

$$M_1 = 10100$$

$$M_2 = 9999$$

$$M_3 = 9900$$

$$M_1^{'} = 50$$

$$M_2^{'} = 99$$

$$M_3^{'} = 51$$

所以，结果为：

$$x \equiv 505000b_1 + 989901b_2 + 504900b_3 \pmod{999900}$$

(16)

①

$$\begin{cases} -2x - 4y \equiv -2 \pmod{7} \\ 2x + y \equiv 1 \pmod{7} \end{cases}$$

$$-3y \equiv -1 \pmod{7}$$

$$4y \equiv 6 \pmod{7}$$

$$y \equiv 5 \pmod{7}$$

$$2x \equiv 3 \pmod{7}$$

$$x \equiv 5 \pmod{7}$$

所以

$$\begin{cases} x \equiv 5 \pmod{7} \\ y \equiv 5 \pmod{7} \end{cases}$$

②

$$\begin{cases} -3x - 9y \equiv -3 \pmod{7} \\ 3x + 4y \equiv 2 \pmod{7} \end{cases}$$

$$-5y \equiv -1 \pmod{7}$$

$$2y \equiv 6 \pmod{7}$$

$$y \equiv 3 \pmod{7}$$

$$x \equiv -8 \pmod 7$$

$$x \equiv 6 \pmod 7$$

所以

$$\begin{cases} x \equiv 6 \pmod 7 \\ y \equiv 3 \pmod 7 \end{cases}$$

(19)

(i)

原式等价于

$$\begin{cases} 23x \equiv 1 \pmod 4 \\ 23x \equiv 1 \pmod 5 \\ 23x \equiv 1 \pmod 7 \end{cases}$$

解上述线性方程，得：

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

所以

$$x \equiv 67 \pmod{140}$$

(ii)

$$\begin{cases} 17x \equiv 1 \pmod 4 \\ 17x \equiv 4 \pmod 5 \\ 17x \equiv 5 \pmod 7 \\ 17x \equiv 9 \pmod{11} \end{cases}$$

解上述线性方程，得：

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$$

所以

$$x \equiv 557 \pmod{1540}$$

(20)

这个问题实际上是证明存在一个x使得

$$\begin{cases} a_1 \mid x \\ a_2 \mid x+1 \\ a_3 \mid x+2 \\ \vdots \\ a_k \mid x+k-1 \end{cases}$$

这也就是说

$$\begin{cases} x \equiv 0 \pmod{a_1} \\ x \equiv -1 \pmod{a_2} \\ \vdots \\ x \equiv 1-k \pmod{a_k} \end{cases}$$

由中国剩余定理，这个方程组是有解的，证毕。

(23)

$\left(3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\right) \bmod \left(x^7-x\right) = x^6+2x^5+2x^3+15x^2+5x$

测速$x \equiv 0 \pmod 7$到$x \equiv 6 \pmod 7$的情况，

得到

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 6 \pmod 7 \end{cases}$$

(24)

首先求

$$x^4+7x+4 \equiv 0 \pmod 3$$

的解。

可以得到

$$x \equiv 1 \pmod 3$$

这时

$$-f(1)/3 = -4$$

$$f^{'}(1) = 11$$

所以

$$k \equiv 1 \pmod 3$$

$$x \equiv 4 \pmod 9$$

这时

$$-f(4)/9=-32$$

$$f^{'}(4)=263$$

所以

$$k\equiv 2 \pmod 3$$

$$x\equiv 22 \pmod{27}$$

这时

$$-f(22)/27=-8682$$

$$f^{'}(22)=42599$$

所以

$$k\equiv 0 \pmod 3$$

$$x\equiv 22 \pmod{81}$$

这时

$$-f(22)/81=-2894$$

$$f^{'}(22)=42599$$

所以

$$k\equiv 2 \pmod 3$$

$$x\equiv 184 \pmod{243}$$