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

$$p \not\mid 2$$

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

所以

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

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

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

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

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

③

$$\phi(16) = 8$$

所以有

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

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

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

$$x = 2101 \pmod{210}$$