第二章作业

(1)

第一问

$$\{9,\ 1,\ 10,\ 3,\ 13,\ 5,\ 15,\ 7,\ 17\}$$

第二问

$$\{0,\ 10,\ 2,\ 12,\ 4,\ 14,\ 6,\ 16,\ 8\}$$

第三问

不可能，因为模10的一个剩余类

$$1+k\cdot 10,\ k\in Z$$

其中大于0的所有元素为奇数。

同理，

$$2+k\cdot 10,\ k\in Z$$

大于0的所有元素为偶数。

故实现不了“全为奇数”或“全为偶数”

(2)

注意到：

$$(m-1)^2=m^2-2m+1$$

$$(m-1)^2-1=m^2-2m$$

$$\frac{m^2-2m}{m}=m-2$$

所以，当$m>2$时，

$$m\mid (m-1)^2-1$$

这也就是说：

$$(m-1)^2\equiv 1^2 \pmod m$$

所以，这个集合一定不是模m的完全剩余系

(5)

(i)

剩余类$1 \pmod 5$可以写作:

$$1+k\cdot 5, k\in Z$$

显然，k可以写为:

$$k=\begin{cases}3p\\3p+1\\3p+2\end{cases}$$

其中$p\in Z$

这样一来，原剩余类可以写作:

$$\begin{cases}15p+1\\15p+6\\15p+11\end{cases}$$

所以，原剩余类可以写作:

$$\{1 \pmod{15}\}\cup\{6 \pmod{15}\}\cup\{11 \pmod{15}\}$$

(ii)

同理，

$$[6]\cup[18]\cup[30]\cup[42]\cup[54]\cup[66]\cup[80]\cup[92]\cup[104]\cup[116]$$

(iii)

同理，

$$[6]\cup[16]\cup[26]\cup[36]\cup[46]\cup[56]\cup[66]\cup[76]$$

(6)

这个题有些指代不明，有两种理解方式:

- 以"2003年5月9日"为起点，之后的"第$2^{20080509}$天"
- 以公元0年0月0日为起点，之后的"第$2^{20080509}$天"

我们知道，

$$2^3 \bmod 7=1$$

而

$$3\mid 20080509$$

这样一来，

$$2^{20080509} \bmod 7=((2^3)\cdot(2^3)\cdot(2^3)\ldots 2^3) \bmod 7=1 \bmod 7$$

所以，

- 按照第一种理解，为星期六
- 按照第二种理解，为星期二

(7)

(i)

使用数学归纳法，

- 归纳基：当$n=1$时，有$a_1 \equiv b_1 \pmod m$
- 归纳步：
    - 当$n=k-1$时，假设$a_i+...+a_{k-1} \equiv b_1+...+b_{k-1} \pmod m$
    - 显然，$a_i+...+a_{k-1}$也是一个整数，记为A，同样地，$b_1+...+b_{k-1}$记为B
    - 由同余的性质，有

    $$A+a_k \equiv B+b_k \pmod m$$

    即

    $$a_i+...+a_k \equiv b_1+...+b_k \pmod m$$

(ii)

使用数学归纳法，

- 归纳基：当$n=1$时，有$a_1 \equiv b_1 \pmod m$
- 归纳步：
    - 当$n=k-1$时，假设$a_i...a_{k-1} \equiv b_1...b_{k-1} \pmod m$
    - 显然，$a_i...a_{k-1}$也是一个整数，记为A，同样地，$b_1...b_{k-1}$记为B
    - 由同余的性质，有

    $$Aa_k \equiv Bb_k \pmod m$$

    即

    $$a_i...a_k \equiv b_1...b_k \pmod m$$

(13)

加法表

$$C_0+C_0=C_0$$

$$C_0+C_1=C_1$$

$$C_0+C_2=C_2$$

$$C_0 + C_3 = C_3$$

$$C_0 + C_4 = C_4$$

$$C_0 + C_5 = C_5$$

$$C_0 + C_6 = C_6$$

$$C_0 + C_7 = C_7$$

$$C_0 + C_8 = C_8$$

$$C_0 + C_9 = C_9$$

$$C_0 + C_{10} = C_{10}$$

$$C_1 + C_1 = C_2$$

$$C_1 + C_2 = C_3$$

$$C_1 + C_3 = C_4$$

$$C_1 + C_4 = C_5$$

$$C_1 + C_5 = C_6$$

$$C_1 + C_6 = C_7$$

$$C_1 + C_7 = C_8$$

$$C_1 + C_8 = C_9$$

$$C_1 + C_9 = C_{10}$$

$$C_1 + C_{10} = C_0$$

$$C_2 + C_2 = C_4$$

$$C_2 + C_3 = C_5$$

$$C_2 + C_4 = C_6$$

$$C_2 + C_5 = C_7$$

$$C_2 + C_6 = C_8$$

$$C_2 + C_7 = C_9$$

$$C_2 + C_8 = C_{10}$$

$$C_2 + C_9 = C_0$$

$$C_2 + C_{10} = C_1$$

$$C_3 + C_3 = C_6$$

$$C_3 + C_4 = C_7$$

$$C_3 + C_5 = C_8$$

$$C_3 + C_6 = C_9$$

$$C_3 + C_7 = C_{10}$$

$$C_3 + C_8 = C_0$$

$$C_3 + C_9 = C_1$$

$$C_3 + C_{10} = C_2$$

$$C_4 + C_4 = C_8$$

$$C_4 + C_5 = C_9$$

$$C_4 + C_6 = C_{10}$$

$$C_4 + C_7 = C_0$$

$$C_4 + C_8 = C_1$$

$$C_4 + C_9 = C_2$$

$$C_4 + C_{10} = C_3$$

$$C_5 + C_5 = C_{10}$$

$$C_5 + C_6 = C_0$$

$$C_5 + C_7 = C_1$$

$$C_5 + C_8 = C_2$$

$$C_5 + C_9 = C_3$$

$$C_5 + C_{10} = C_4$$

$$C_6 + C_6 = C_1$$

$$C_6 + C_7 = C_2$$

$$C_6 + C_8 = C_3$$

$$C_6 + C_9 = C_4$$

$$C_6 + C_{10} = C_5$$

$$C_7 + C_7 = C_3$$

$$C_7 + C_8 = C_4$$

$$C_7 + C_9 = C_5$$

$$C_7 + C_{10} = C_6$$

$$C_8 + C_8 = C_5$$

$$C_8 + C_9 = C_6$$

$$C_8 + C_{10} = C_7$$

$$C_9 + C_9 = C_7$$

$$C_9 + C_{10} = C_8$$

$$C_{10} + C_{10} = C_9$$

乘法表

$$C_0 * C_0 = C_0$$

$$C_0 * C_1 = C_0$$

$$C_0 * C_2 = C_0$$

$$C_0 * C_3 = C_0$$

$$C_0 * C_4 = C_0$$

$$C_0 * C_5 = C_0$$

$$C_0 * C_6 = C_0$$

$$C_0 * C_7 = C_0$$

$$C_0 * C_8 = C_0$$

$$C_0 * C_9 = C_0$$

$$C_0 * C_{10} = C_0$$

$$C_1 * C_1 = C_1$$

$$C_1 * C_2 = C_2$$

$$C_1 * C_3 = C_3$$

$$C_1 * C_4 = C_4$$

$$C_1 * C_5 = C_5$$

$$C_1 * C_6 = C_6$$

$$C_1 * C_7 = C_7$$

$$C_1 * C_8 = C_8$$

$$C_1 * C_9 = C_9$$

$$C_1 * C_{10} = C_{10}$$

$$C_2 * C_2 = C_4$$

$$C_2 * C_3 = C_6$$

$$C_2 * C_4 = C_8$$

$$C_2 * C_5 = C_{10}$$

$$C_2 * C_6 = C_1$$

$$C_2 * C_7 = C_3$$

$$C_2 * C_8 = C_5$$

$$C_2 * C_9 = C_7$$

$$C_2 * C_{10} = C_9$$

$$C_3 * C_3 = C_9$$

$$C_3 * C_4 = C_1$$

$$C_3 * C_5 = C_4$$

$$C_3 * C_6 = C_7$$

$$C_3 * C_7 = C_{10}$$

$$C_3 * C_8 = C_2$$

$$C_3 * C_9 = C_5$$

$$C_3 * C_{10} = C_8$$

$$C_4 * C_4 = C_5$$

$$C_4 * C_5 = C_9$$

$$C_4 * C_6 = C_2$$

$$C_4 * C_7 = C_6$$

$$C_4 * C_8 = C_{10}$$

$$C_4 * C_9 = C_3$$

$$C_4 * C_{10} = C_7$$

$$C_5 * C_5 = C_3$$

$$C_5 * C_6 = C_8$$

$$C_5 * C_7 = C_2$$

$$C_5 * C_8 = C_7$$

$$C_5 * C_9 = C_1$$

$$C_5 * C_{10} = C_6$$

$$C_6 * C_6 = C_3$$

$$C_6 * C_7 = C_9$$

$$C_6 * C_8 = C_4$$

$$C_6 * C_9 = C_{10}$$

$$C_6 * C_{10} = C_5$$

$$C_7 * C_7 = C_5$$

$$C_7 * C_8 = C_1$$

$$C_7 * C_9 = C_8$$

$$C_7 * C_{10} = C_4$$

$$C_8 * C_8 = C_9$$

$$C_8 * C_9 = C_6$$

$$C_8 * C_{10} = C_3$$

$$C_9 * C_9 = C_4$$

$$C_9 * C_{10} = C_2$$

$$C_{10} * C_{10} = C_1$$

(22)

原式等价于

$$(8-7)\cdot(9-7)\cdot\ldots\cdot(13-7) \pmod 7$$

即

$$6! \pmod 7$$

因为

$$(7-1)! = -1 \pmod 7$$

所以原式等于

$$-1 \pmod 7$$

(24)

由费马小定理

$$3^6 \equiv 1 \pmod 7$$

而

$$1000000 \bmod 6 = 4$$

所以，原式等价于

$$3^4 \pmod 7 = 81 \pmod 7 = 4 \pmod 7$$

(26)

由Wilson定理：

$$(p-1)! = -1 \pmod p$$

而，

$$\begin{aligned} p-1 &\equiv -1 \pmod p \\ p-2 &\equiv -2 \pmod p \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod p \end{aligned}$$

把$(p-1)!$中的每一个大于等于$\frac{p+1}{2}$的数都换成上式右侧的数：

$$1 \cdot 2 \cdots \frac{(p-1)}{2} \cdot (-1) \cdots \cdot (-\frac{(p-1)}{2}) \equiv -1 \pmod p$$

即：

$$(\frac{p-1}{2}!)^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$$

也即是：

$$(\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

因为

$$p \equiv 3 \pmod 4$$

所以

$$(-1)^{\frac{p+1}{2}} = 1$$

原式可以写成：

$$(\frac{p-1}{2}!)^2 \equiv 1 \pmod p$$

而我们知道

$$3! \equiv -1 \pmod 7$$

$$11! \equiv 1 \pmod{23}$$

所以，当$p \equiv 3 \pmod 4$时，有

$$\frac{p-1}{2}! \equiv \pm 1 \pmod p$$

(28)

继续利用(26)中的关系：

$$
\begin{aligned}
p-1 &\equiv -1 \pmod p \\
p-2 &\equiv -2 \pmod p \\
&\vdots \\
p-k+1 &\equiv -(k-1) \pmod p
\end{aligned}
$$

把$(p-1)!$中大于$p-k$的项换成右边的式子，$(p-1)!$可以写成：

$$1 \cdot 2 \cdot 3 \cdots (p-k) \cdots (-(k-1)) \cdots (-1)$$

即

$$(p-k)!(k-1)!(-1)^{k-1}$$

所以

$$(p-k)!(k-1)!(-1)^{k-1} \equiv -1 \pmod p$$

所以

$$(p-k)!(k-1)! \equiv -1^{k} \pmod p$$

(33)

$$a^7-a=(a-1)a(a+1)\left(a^2-a+1\right)\left(a^2+a+1\right)$$

首先，由$(a,3)=1$，有

$$a^2 \equiv 1 \pmod 3$$

这也就是说

$$3 \mid (a-1)(a+1)$$

这说明

$$3 \mid a-1$$

或

$$3 \mid a+1$$

成立。而这也说明

$$3 \mid a+2$$

或

$$3 \mid a-2$$

成立。所以，

$$3 \mid (a^2-1)+(a+2)$$

或

$$3 \mid (a^2-1)-(a-2)$$

成立。所以

$$9 \mid (a-1)(a^2+a+1)$$

或

$$9 \mid (a+1)(a^2-a+1)$$

成立，故

$$9 \mid (a-1)a(a+1)\left(a^2-a+1\right)\left(a^2+a+1\right)=a^7-a$$

成立。

由费马小定理

$$a^7 \equiv a \pmod 7$$
$$7 \mid a^7-a$$

综上

$$63 \mid a^7-a$$
$$a^7 \equiv a \pmod{63}$$

(34)

因为a与32760互素，而

$$32760=2^3\cdot 3^2\cdot 5\cdot 7\cdot 13$$

所以，a与

$$\{2^3,3^2,5,7,13\}$$

都互素。

所以：

$$a^4 \equiv 1 \pmod 8$$
$$a^6 \equiv 1 \pmod 9$$
$$a^4 \equiv 1 \pmod 5$$
$$a^6 \equiv 1 \pmod 7$$
$$a^{12} \equiv 1 \pmod{13}$$

而且，显然地

$$(a^3,8)=1$$
$$(a^2,9)=1$$

$$(a^3, 5) = 1$$

$$(a^2, 7) = 1$$

所以

$$a^{12} = (a^4)^3 \equiv 1 \pmod 8$$

$$a^{12} = (a^6)^2 \equiv 1 \pmod 9$$

$$a^{12} = (a^4)^3 \equiv 1 \pmod 5$$

$$a^{12} = (a^6)^2 \equiv 1 \pmod 7$$

$$a^{12} \equiv 1 \pmod{13}$$

所以

$$a^{12} \equiv 1 \pmod{8 \cdot 9 \cdot 5 \cdot 7 \cdot 13}$$

$$a^{12} \equiv 1 \pmod{32760}$$