一、(共10分)

1. (10分) 设$a=963$, $b=657$, 计算(a,b)并找到整数s,t使得 $sa+tb=(a,b)$;

利用欧几里得辗转相除法,$(963,657)$求解过程:

$(1): 963 = 1*657+306$

$(2): 657 = 2*306+45$

$(3): 306 = 6*45+36$

$(4): 45 = 1*36+9$

$(5): 36 = 4*9+0$

因此$(963,657)=9$

sn, tn的$n=3$

$sn963+tn657=(963,657), n=3$的求解过程:

$s[-2]=1, t[-2]=0$

$s[-1]=0, t[-1]=1$

$s[0]=(-1)*0+1=1, t[0]=(-1)*1+0=-1$

$s[1]=(-2)*1+0=-2, t[1]=(-2)*-1+1=3$

$s[2]=(-6)*-2+1=13, t[2]=(-6)*3+-1=-19$

$s[3]=(-1)*13+-2=-15, t[3]=(-1)*-19+3=22$

所以$(-15)*963+22*(657)=9, s=-15, t=22$

二、(共20分)

1. (10分) 有一个人每工作八天后休息两天。有一次他在星期三、星期四休息,问最少要几周后他可以在星期四休息?

本次是星期三、四休息,设过x周后能够在星期四休息,一周7天,经过了$7x$天回到星期四,且此时休息

每个10天里,第$9,10$天休息,所以回到星期四时,应该是这个10天里的第9或者10天

同余方程为

$$7x \equiv 9 \pmod{10}$$

$$7x \equiv 10 \pmod{10}$$

解得$x \equiv 7、10 \pmod{10}$

因此至少是第7周后可以在星期四休息

2. (10分) 设$(a,n)=1, a\not\equiv 0 \pmod n$,证明:同余方程$ax\equiv b \pmod n$的解为$x\equiv a^{\varphi(n)-1}b \pmod n$. 并求解同余方程$21x\equiv 7 \pmod{100}$.

$(a,n)=1|b$,因此原式有解,而根据欧拉定理,$(a,n)=1$,所以$a^{\varphi(n)} \equiv 1 \pmod n$

因此$a\cdot a^{\varphi(n)-1} \equiv 1 \pmod n$

进而将$x\equiv a^{\varphi(n)-1}b$代入$ax\equiv b \pmod n$中,有

$a\cdot a^{\varphi(n)-1}b \equiv b \pmod n$,满足原同于方程,因此$x$是其解

根据以上结论,$21x\equiv 7 \pmod{100}$的解是:

$x\equiv 21^{\varphi(100)-1}\cdot 7 \pmod{100}, \varphi(100)=40$,因此原方程解是

$x\equiv 21^{39}\cdot 7 \pmod{100}$

利用模重复平方法,$39=1+2+2^2+2^5$

解得$x\equiv 81\cdot 7\equiv 67 \pmod{100}$

三、(共20分)

1. (10分) 求解同余式方程组： $\begin{cases} 7x \equiv 5 \pmod{18} \\ 13x \equiv 2 \pmod{15} \end{cases}$.

$7x \equiv 5 \pmod{18}$解得

$x \equiv 11 \pmod{18}$

$13x \equiv 2 \pmod{15}$解得

$x \equiv 14 \pmod{15}$

联立解得到方程组：

$$\begin{cases} x \equiv 11 \pmod{18} \\ x \equiv 14 \pmod{15} \end{cases}$$

但是$(18,15)$不互素，将方程组进一步分解为

$$\begin{cases} x \equiv 11 \equiv 1 \pmod{2} \\ x \equiv 11 \equiv 2 \pmod{9} \\ x \equiv 14 \equiv 2 \pmod{3} \\ x \equiv 14 \equiv 4 \pmod{5} \end{cases}$$

注意到$x \equiv 2 \pmod{9} \Rightarrow x \equiv 2 \pmod{3}$，因此原方程组可以写为

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{9} \quad \text{其中}2,9,5\text{两两互素} \\ x \equiv 4 \pmod{5} \end{cases}$$

进而利用中国剩余定理，$M_1 = 45, M_2 = 10, M_3 = 18, m = 90$

$M_1' = 1, M_2' = 1, M_3' = 2$

因此原方程组解为$x \equiv 1 \cdot 45 \cdot 1 + 2 \cdot 10 \cdot 1 + 4 \cdot 18 \cdot 2 \pmod{90}$

$x \equiv 29 \pmod{90}$

2. (10分) 求解同余式$x^2 + x + 7 \equiv 0 \pmod{27}$.

$f(x) = x^2 + x + 7$，注意到$27 = 3^3$，欲求解$f(x) \equiv 0 \pmod{27}$，进行同余式提升

$f(x) \equiv 0 \pmod{3}$，解得$x \equiv 1 \pmod{3}$

进而将$x = 1 + 3t_1 \pmod{9}$代入$f(x) \equiv 0 \pmod{9}$

$f(1+3t_1) \equiv f(1) + f'(1)3t_1 \equiv 9 + 3 * 3t_1 \equiv 0 \pmod{9}$

解得$t_1 \equiv 0、1、2 \pmod{3}, x = 1,4,7 \pmod{9}$

进而将$x = (1+3t_1) + 9t_2 = (1,4,7) + 9t_2 \pmod{27}$代入$f(x) \equiv 0 \pmod{27}$

(1) $x = 1 + 9t_2$时

$f(x) \equiv f(1) + f'(1)9t_2 = 9 + 27t_2 \equiv 9 \neq 0 \pmod{27}$，没有解

(2) $x = 4 + 9t_2$时

$f(x) \equiv f(4) + f'(4)9t_2 = 27 + 81t_2 \equiv 0 \pmod{27}$，解为$t_2 = 0,1,2 \pmod{3}$

此时原方程解是$x \equiv 4,13,22 \pmod{27}$

(3) $x = 7 + 9t_2$时

$f(x) \equiv f(7) + f'(7)9t_2 = 63 + 15 \cdot 9t_2 = 63 + 135t_2 \equiv 18 \neq 0 \pmod{27}$，没有解

综上所述，原同余方程解是$x \equiv 4,13,22 \pmod{27}$

四、(共15分)

1. (5分) 判断同余式 $x^2 \equiv -1 \pmod{365}$ 是否有解，有解时，求出其解数.

注意到$365=5\times 73$,且$5,73$均是素数,因此原方程可转换为方程组：

$$\begin{cases} x^2 \equiv -1 \pmod{5} & (1) \\ x^2 \equiv -1 \pmod{73} & (2) \end{cases}$$

$(\frac{-1}{5})=(-1)^{\frac{5-1}{2}}=1$,因此$(1)$有两个解

$(\frac{-1}{73})=(-1)^{\frac{72}{2}}=1$,因此$(2)$有两个解

综上,原方程有解,解的个数是$2\times 2=4$个

2. (10分) 证明:设 $m>1$是整数，a 是与 m 互素的整数.则 $a^d \equiv a^k \pmod{m} \Leftrightarrow d \equiv k \pmod{ord_m(a)}$.

$ord_m(a)$是a对模m的指数,有$a^{ord_m(a)} \equiv 1 \pmod{m}$;且$\forall d \in Z, a^d \equiv 1 \pmod{m}$均有$ord_m(a)|d$

根据欧几里得除法,d,k可以写成$d=q_1\cdot ord_m(a)+r_1, k=q_2\cdot ord_m(a)+r_2$,

而根据指数性质$a^{ord_m(a)} \equiv 1 \pmod{m}$,有$a^d \equiv a^{q_1\cdot ord_m(a)+r_1} \equiv (a^{ord_m(a)})^{q_1}\cdot a^{r_1} \equiv a^{r_1}$

同理,$a^k \equiv (a^{ord_m(a)})^{q_2}\cdot a^{r_2} \equiv a^{r_2}$

充分性.

由题干,$a^d \equiv a^k \pmod{m}$.

$\therefore a^{r_1} \equiv a^{r_2} \pmod{m}$,而$0 \le r \le ord_m(a) \le \varphi(m) < m$

而根据$5.2.1$,$a^1, a^2, ...a^{ord_m(a)}=1$是两年不同余的,所以$r_1=r_2$,

而$r_1=d \pmod{ord_m(a)}, r_2=k \pmod{ord_m(a)}$,因此$d \equiv k \pmod{ord_m(a)}$

必要性.

由题干,$d \equiv k \pmod{ord_m(a)}$,所以$r_1=r_2$

$\because a^d \equiv a^{r_1}, a^k \equiv a^{r_2}, r_1=r_2$

$\therefore a^d \equiv a^k \pmod{m}$.

综上,互为充要条件.

五、(共20分)

1. (5分) 求整数5模17的指数$ord_{17}(5)$;

17是素数,$\varphi(17)=17-1=16$,16的因数是$1,2,4,8,16$;只要对因数次方求模即可

$5^1 \equiv 5 \pmod{17}$

$5^2 \equiv 8 \pmod{17}$

$5^4 \equiv 13 \pmod{17}$

$5^8 \equiv 16 \pmod{17}$

$5^{16} \equiv 1 \pmod{17}$

综上,$ord_{17}(5)=16$,5正好是模17的原根

2. (15分) 求模47的所有原根，并且建立它的关于最小正原根的指标表，由此求解如下高次剩余$x^5 \equiv 29 \pmod{47}$.

5是模47的最小正原根,依次求解$ind_5 b; b=1,2,3...46$;

$ind_5 1=46, ind_5 2=18, ...ind_5 29=35...ind_5 46=23$

将高次剩余指标化,原式化为：

$5ind_5(x) \equiv ind_5(29) \pmod{\varphi(47)=46}$

$5ind_5(x) \equiv 35 \pmod{46}$

解得$ind_5(x) \equiv 7 \pmod{46}$

所以$x \equiv 5^{ind_5(x)} \equiv 5^7 \equiv 11 \pmod{47}$

六、(共15分)

1. (5分) 找到循环群$\mathbf{Z}_7^*$的一个生成元，并用它生成群中的所有元素.

$Z_7* = \{1,2,3,4,5,6\}$, 由于Z_7*是循环群, 其群运算可以是$\otimes$
由于运算模7, 且$0 \notin Z_7$, 因此运算封闭, 单位元$e = 1$
对于$a \in Z_7, ax \equiv 1 \pmod 7$, 由于$7$是素数, 因此$(a,7) = 1$, 所以元素有逆元.
注意到$3 \in Z_7, \{3^1, 3^2 \ldots 3^6\} = \{1,2,3,4,5,6\} = Z_7*$, 所以$3$是一个生成元
$\varphi(6) = 2$, 所以其实Z_7*有两个生成元, 形如$g^j, (j,6) = \frac{6}{6} = 1$, g是一个生成元(这里可$g = 3$)
所以$j = 1, 5$; 所以生成元是$3^1 = 3, 3^5 = 5$
$3^1 mod7 = 3$
$3^2 mod7 = 2$
$3^3 mod7 = 6$
$3^4 mod7 = 4$
$3^5 mod7 = 5$
$3^6 mod7 = 1$

2. (10 分) 设$f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$，

$g(x) = x^8 + x^4 + x^3 + x + 1 \in F_2[x]$， 求$q(x)$和$r(x)$， 使得

$f(x) = g(x)q(x) + r(x), \deg r(x) < \deg g(x)$.

$$f(x) = (x^5 + x^3)g(x) + (x^7 + x^6 + x + 1)$$
$$q(x) = x^5 + x^3, r(x) = x^7 + x^6 + x + 1$$