作业6

> 1、手动计算$2000^{2019} \pmod{221}$，不允许使用电脑或者其他电子设备。
>
> 2、实现一个利用CRT求解同余方程的程序（Python或者C语言都可以）。
>
> 3、完成中国剩余定理群论版的证明，即证明$\mathbb{Z}_n^*$与$\mathbb{Z}_p^* \times \mathbb{Z}_q^*$同构。
>
> 4、定义映射$\psi: Z_p^* \rightarrow \{\pm 1\}$为$\psi(a)=\left(\frac{a}{p}\right)$，$\forall a \in Z_p^*$。请证明这是一个满同态。
>
> 5、使用抽象代数的语言重新证明欧拉准则。

1.计算$2000^{2019}(mod \quad 221)$

$2000^{2019}(mod \quad 221)$ =122

过程：2000与221互素，且2000 mod 221 =11,故使用费尔马小定理可知，$2000^{2019}=11^{2019}$,且$11^{220} \equiv 1 mod 221$，有

$11^{2019}=11^{220*9+39}=11^{32+1+2+4}=35*11*121*55=122(mod \quad 221)$

2.实现一个CRT求解同余方程的程序(python)

```
#CRT求同余方程的程序
#可以通过设定m来实现更多同余解，其中m=a.size+b.size
m=4
a=[]
b=[]
def egcd(a,b):
    if b==0:
        return 1,0
    else:
        x,y=egcd(b,a%b)
        return y,x-a//b*y
#案例1 a=2 b=3 p=5 q=7  ->x=17 mod 35
def inv(a,b):
    q1,q2=egcd(a,b)
    #print(q2)
    return q1
def crt():
    n=1
    for i in a:
        n*=i
    j=0
    sum=0
    #print(n)
    while(j<m/2):
        w=n/a[j]
        p1=(inv(a[j],w)+w)%w
        #print(p1)
        sum=(sum+w*b[j]*p1)%n
```

```python
        j=j+1
    return (sum+n)%n

def main():
    i=0
    arr=eval(input("输入: "))
    #input多个数用逗号隔开如8,3,11,19
    #输入为一串数字，例如分别为a1,b1,a2,b2
    #x= b1 mod a1
    #x= b2 mod a2
    #以此类推
    #例：输入 5,2,7,3 ，则能算出 最终 x= 17 mod  35
    while(i<m):
        if(i%2==0):
            a.append(arr[i])
        else:
            b.append(arr[i])
        i=i+1
    print(crt())

if __name__ == '__main__':
    main()
```

3.完成CRT群论的证明，即证明Z_n^*与$Z_p^* \times Z_q^*$同构

从以下三个方面进行证明:

(1)证明群Z_n^*与$Z_p^* \times Z_q^*$同态。

定义映射$f: Z_n^* \rightarrow Z_p^* \times Z_q^*$，$f(x)=([x \quad mod \quad p],[x \quad mod \quad q])$. 存在这样一个映射f使得$Z_n^*$与$Z_p^* \times Z_q^*$ 群同态

(2)证明映射f是双射

证明f是双射，即证明f是满射且单射。满射是显然的，根据中国剩余定理，任意序对中的两个同余式有模n唯一解。

欲证明f是单射的，那么根据单射的定义，我们任取正整数a和b∈Z_n^*，且a、b均小于n，设f(a)=f(b)，若是单射，则必有a=b。

根据中国剩余定理，我们知道

$$f(a)=([a \quad mod \quad p],[a \quad mod \quad q])$$
$$f(b)=([b \quad mod \quad p],[b \quad mod \quad q])$$

任意序对的两个同余式模n有唯一解，只可能有一个a满足f(a)，而因为f(a)=f(b)，所以b只能等于a，即a=b成立，f为单射。

因为f即单射又满射，故f为双射。

(3)证明群操作保持

不妨任取a,b∈Z_n^*，有

$$f(a \cdot b)=([a \cdot b \quad mod \quad p],[a \cdot b \quad mod \quad q])$$
$$f(a)=([a \quad mod \quad p],[a \quad mod \quad q])$$
$$f(b)=([b \quad mod \quad p],[b \quad mod \quad q])$$
$$f(a \cdot b)=([a \cdot b \quad mod \quad p],[a \cdot b \quad mod \quad q])$$
$$=([a \quad mod \quad p],[a \quad mod \quad q]) \cdot ([b \quad mod \quad p],[b \quad mod \quad q])=f(a) \cdot f(b)$$

所以，映射f成立，群操作得以保持

综合以上三点可知：Z_n^*与$Z_p^* \times Z_q^*$同构

4.定义映射$\psi : Z_p^* \to \{\pm 1\}$ 为$\psi(a) = (\frac{a}{p})$，$\forall a \in Z_p^*$，请证明这是一个满同态。

证明：$\forall a \in Z_p^*$,$\psi(a) = (\frac{a}{p})$ $Z_p^* \to \{\pm 1\}$是满同态

要证明满同态，则必须证明该映射ψ 是满射，则应该从定义出发，存在$a \in Z_p^*$ ，使得对于任意$b \in \pm 1$，都有$\psi(a) = (\frac{a}{p}) = \pm 1 = b$

$(\frac{a}{p})$是勒让德符号，有

$$(\frac{a}{p}) \begin{cases} 1 & a\text{是} mod \quad p\text{的二次剩余} \\ -1 & a\text{是} mod \quad p\text{的非二次剩余} \end{cases}$$

首先存在映射$\psi(a) = (\frac{a}{p})$ 使得对于任意a∈Z_p^* 成立，即$Z_p^* \to \{\pm 1\}$是同态

然后证明ψ是满射。

根据定理，因为p是奇素数，每一个群Z_p^*都恰好有(p-1)/2个QR（二次剩余），(p-1)/2个QNR（非二次剩余），所以必定有

当 $a \in Z_p^*$时，

1) 当a 是 Z_p^* 的QR时，$\psi(a) = (\frac{a}{p}) = 1$

2) 当a 是 Z_p^* 的QNR时，$\psi(a) = (\frac{a}{p}) = -1$

即一定存在$a \in Z_p^*$，对于任意$b \in \pm 1$，都有$\psi(a) = (\frac{a}{p}) = \pm 1 = b$ ，即映射ψ 是满射，群同态为满同态！

5.使用抽象代数的语言重新证明欧拉准则

欧拉准则：设 p 是奇素数，$a \in Z$，且 $gcd(a, p) = 1$。那么，$(\frac{a}{p}) \equiv a^{(p-1)/2} (mod \quad p)$

证明如下：

先构造映射$\eta : Z_p^* \to a^{(p-1)/2}$ ，结合第四题的满同态映射$\psi : Z_p^* \to \{\pm 1\}$，要证明欧拉准则成立，则只需证明

映射η和映射ψ 的核相等，即$ker(\eta) == ker(\psi)$。

（1）首先，构造 映射$\eta : Z_p^* \to a^{(p-1)/2}$ ，所以η是同态映射。

（2）其次，证明映射η是双射。由第四题的满同态映射$\psi : Z_p^* \to \{\pm 1\}$，可知是η显然是满射，现在要证明单射。

我们知道，$\eta(a) = a^{(p-1)/2}$，$\psi(a) = (\frac{a}{p})$

1) 任取$a \in Z_p^*$，若 $(\frac{a}{p}) = 1$ ，则存在$b \in Z_p^*$，使得 $b^2 \equiv a \quad mod p$，且根据费尔马小定理，有

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \quad mod \quad p$$

2)同理， 任取$a \in Z_p^*$，若 $a^{(p-1)/2} = 1$ ，根据二次剩余的定义及定理，这样的a有 (p-1)/2个，

而对于勒让德符号$(\frac{a}{p}) = 1$的情况，只有a为模p的二次剩余才能成立，所以 此时

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

联立1)和2)，对于所有的模p二次剩余a，有ker(η) = ker (ψ)，即η是单射。

（3）任取$a, b \in Z_p^*$，根据构造的映射，有

$$\eta(a \cdot b) = (a \cdot b)^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2} = \eta(a) \cdot \eta(b)$$

所以有群操作保持。

由以上三点以及第一同构定理可知，$\eta : Z_p^* \to a^{(p-1)/2}$ 是 同构映射，即欧拉准则（$(\frac{a}{p}) \equiv a^{(p-1)/2}(mod \quad p)$）成立。