第十章

> 1. 运用 CRT 求解：
>
> $$x\equiv 8\pmod{11}$$
>
> $$x\equiv 3\pmod{19}$$

解：易得

$$a=8,b=3,p=11,q=19,p*q=209$$

由egcd可得

$$p^{-1}=7,q^{-1}=7$$

由CRT易得，$$x\equiv 8197+3711\pmod{209}$$

故x=41

> 2. 运用 CRT 求解：
>
> $$x\equiv 1\pmod{5}$$
>
> $$x\equiv 2\pmod{7}$$
>
> $$x\equiv 3\pmod{9}$$
>
> $$x\equiv 4\pmod{11}$$

解：易得

$$a_1=1,a_2=2,a_3=3,a_4=4$$

$$p_1=5,p_2=7,p_3=9,p_4=11$$

$$P=p_1p_2p_3*p_4=3465$$

$$\text{则对于每一个}a_i\text{都有}b_i=\frac{P}{p_i}$$

则：

$$b_1=693,b_2=495,b_3=385,b_4=315$$

由egcd可得

$$b_1^{-1}=2,b_2^{-1}=3,b_3^{-1}=4,b_4^{-1}=8$$

带入运算，易得

$$x=\sum_{i=1}^{4}a_ib_ib_i^{-1}\pmod{P}=1731$$

> 3. 手动计算
>
> $$2000^{2019} \pmod{221}$$
>
> 不允许使用电脑或者其他电子设备。[提示：这是一道看上去与中国剩余定理无关的计算题。]

解：由提示猜测，221为合数，容易验证221=13*17

不妨设

$$p=13,q=17$$

有$$Z^_{221}\cong Z^{13}Z^{17}$$

$$\begin{align*} (4050)^{2019}\pmod{1317}&= ((1,6)(11,16))^{2019} \ &= (111\pmod{13},616\pmod{17})^{2019} \ &=(11,11)^{2019}\ &=((-2)^{2019}\pmod{13},(-6)^{2019}\pmod{17})\ &=((-2)^{3}\pmod{13},(-6)^{3}\pmod{17})\ &=(5,5) \end{align}$$

由egcd易得

$$p^{-1}=4,q^{-1}=14$$

不妨设

$$x\equiv 5 \pmod{13}$$

$$x\equiv 5 \pmod{17}$$

易得x=5时成立，则有原式：

$$2000^{2019} \pmod{221}=5$$

成立

> 7. 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）。

```python
def CRT(a,b,p,q):
    n=p*q
    if p!=q:#虽然这个条件其实是显然的
        p1,q1=egcd(p,q)
    x=(a*q*q1+b*p*p1)%n
    return x

def egcd(p,q):
    r1,s1,r2,s2=1,0,0,1
    while p!=1 and q!=1:
        if p>q:
            p=p-q
            r1=r1-r2
            s1=s1-s2
        elif p<q:
            q=q-p
            r2=r2-r1
            s2=s2-s1
```

```
    if p==1:
        return r1,s1
    elif q==1:
        return r2,s2
```