第一次作业

> 1. **用 C 语言编程实现一种迭代版本的简单乘法。**

```c
int Multiply(int a, int b)
{
    int res = 0;
    int x = 1; //2的0次方
    while (b > 0)
    {
        if (b & 1) res += a * x;
        b = b >> 1;//b右移一个bit
        x = x << 1; //计算2的i次方
    }
    return res;
}
```

> 2. **证明除法算法：对任意给定的整数a和b，其中$b>0$，存在唯一的整数对q（商）和r（余数）使得，**
>
> $$a=qb+r$$
>
> **且** $0\le r<b$。

证明：

先证明存在性：构造集合$S=\{a-bk:k\in Z \text{ 且 } a-bk\ge 0\}$，显然，集合$S$非空，由良序原则，存在一个最小元$r\in S$ 且 $r=a-qb$，因此，$a=qb+r,r\ge 0$。我们采用**反证法**，假设最小元$r>b$，则$\exists t\in Z\ s.t.\ r=tb+r^*$，则有

$$a=qb+r=qb+tb+r^*=(q+t)b+r^*$$

令 $q+t=q^*\in Z$ 则有

$$a=q^*b+r^*$$

此时存在$r^*<r$,则此时的最小元为r^*,与假设矛盾。故$0\le r<b$。

后证明唯一性：

我们才用**反证法**，假设存在两对$(q_1,r_1)(q_2,r_2)$满足$a=qb+r$，其中$q_1\neq q_2$，$r_1\neq r_2$，$0\leq r_1<b$，$0\leq r_2<b$，则有：

$$q_1b+r_1=q_2b+r_2$$

处理得：$(q_1-q_2)b=(r_2-r_1)$。又$0\leq r_1<b$，$0\leq r_2<b$，有$-b<r_2-r_1<b$，故$-1<q_1-q_2<1$，$q_1-q_2=0\Leftrightarrow q_1=q_2$

与假设不符，故**只存在一对**$(q,r)\ s.t.\ 0\leq r<b$且$a=qb+r$，证毕。

> 3. **用C语言编程实现一种迭代版本的gcd算法和一种egcd算法。利用gcd算法，写程序完成以下函数的功能。输入：一个正整数n；输出：大于等于1，小于n，且与n互素的正整数的个数。**

- 迭代版gcd

```c
int gcd(int a, int b)
{
    while (b)
    {
        int temp = b;
        b = a % b;
        a = temp;
    }
    return a;
}
```

- 迭代版$egcd$

```c
struct Bezout
{
    int r;
    int s; //r、s为Bezout系数
    int d; //d为gcd(a,b)
};
Bezout egcd(int a, int b)
{
    Bezout res;
    int r0 = 1, r1 = 0, s0 = 0, s1 = 01, q; //初始化
    while (b)
    {
        q = a / b;
```

```
        //以下计算gcd(a,b)
        int temp = a % b;
        a = b;
        b = temp;
        //以下计算Bezout系数
        int tr = r0;
        int ts = s0;
        r0 = r1;
        r1 = tr - q * r1;
        s0 = s1;
        s1 = ts - q * s1;
    }
    res.r = r0;
    res.s = s0;
    res.d = a;
    return res;
}
```

- 欧拉函数

```
int Euler(int n)
{
    int count = 0;
    for (int i = 1; i < n; i++)
    {
        if (gcd(i, n) == 1) count++;
    }
    return count;
}
```

> 6. 假设$g^a \equiv 1\ (mod\ m)$且 $g^b \equiv 1(mod\ m)$,请证明:
> $g^{gcd(a,b)} \equiv 1(mod\ m)$.

证明:

由$Bézout$定理可得：$gcd(a,b) = ar + bs$，且a与b的最大公因子是唯一的。

即证：$g^{ar+bs} \equiv 1 \pmod m$

$g^a \equiv 1 \pmod m \Rightarrow (g^a)^r \equiv 1 \pmod m$

$g^b \equiv 1 \pmod m \Rightarrow (g^b)^s \equiv 1 \pmod m$

故有$g^gcd(a,b) \equiv g^{ar+bs} \equiv (g^a)^r(g^b)^s \equiv 1 \pmod m$，证毕。

> 8．证明：如果$gcd(a,b)=d$,则$gcd(a/d,b/d)=1$

证明：

根据$B\acute{e}zout$定理，$\exists r,s \in Z$使得$ar+bs=gcd(a,b)=d$

左右同除以d，有$\frac{ar}{d}+\frac{bs}{d}=1$

故$\exists r^*,s^*$使得$r^*\frac{a}{d}+s^*\frac{b}{d}=1$

故$gcd(a/d,b/d)=1$，证毕。