> 1. 写一个模指数运算函数Mod_Exp，输入a、b和m，输出a^b mod m，即a的b次方模m。

快速幂(迭代版)

```
//迭代版
int Mod_Exp(int a, int b,int m)
{
    int sum = 1;
    while (b > 0)
    {
        if (b & 1) sum = (sum * a) % m;
        b >>= 1;
        a = (a * a) % m; //计算a^{2^i}
    }
    return sum % m;
}
```

> 2. 写一个求乘法逆元的函数Mul_Inverse，输入a和m，求a模m的乘法逆元。提示，要求只输出正整数。

思路： 用$egcd$求乘法逆元

```
struct Bezout
{
    int r;
    int s; //r、s为Bezout系数
    int d; //d为gcd(a,b)
};
//求Bezout系数
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;
}
//求乘法逆元
int Mul_Inverse(int a, int m)
{
    Bezout res;
    res = egcd(a, m);
    return res.r;
}
```

> 3. 设$p = 23$和$a = 3$，使用费尔马小定理计算$a^{2019}\ mod\ p$

解:

根据Fermat小定理:

$$3^{2019} \equiv 3^{91*22+17} \equiv 3^{17} \pmod{23}$$

由**快速幂**知:

$$3^2 = 9 \pmod{23}$$

$$3^4 \equiv 9*9 \equiv 12 \pmod{23}$$

$$3^8 \equiv 12*12 \equiv 6 \pmod{23}$$

$$3^{16} \equiv 6*6 \equiv 13 \pmod{23}$$

故$3^{17} \equiv 39 \equiv 16 \pmod{23}$。结果为16。

> 4．请证明13整除$2^{70}+3^{70}$。

证明：

即证：$2^{70}+3^{70} \equiv 0 \pmod{13}$

根据Fermat小定理:$2^{70} \equiv 2^{5*12+10} \equiv 2^{10} \pmod{13}$，又$2^5 \equiv 6 \pmod{13}$

故$2^{10} \equiv 6*6 \equiv 10 \pmod{13}$。

根据Fermat小定理:$3^{70} \equiv 3^{5*12+10} \equiv 3^{10} \pmod{13}$，又$3^5 \equiv 9 \pmod{13}$

故$3^{10} \equiv 9*9 \equiv 3 \pmod{13}$。

所以有：$2^{70}+3^{70} \equiv 13 \equiv 0 \pmod{13}$

证毕。

> 5．使用欧拉定理计算$2^{100000}\ mod\ 55$

解：

因为2与55互素，根据欧拉定理：$2^{\phi(55)} \equiv 1 \pmod{55}$

而$\phi(55)=\phi(5)*\phi(11)=4*10=40$

故有：$2^{100000} \equiv 2^{2500*40} \equiv 2^{40} \equiv 1 \pmod{55}$

> 8．手动计算7^{1000}的最后两个数位等于什么？

解：

该问等价于求：$7^{1000}\ mod\ 100$

由于7和1000互素，根据欧拉定理：$7^{\phi(100)} \equiv 1 \pmod{100}$

而$\phi(100)=\phi(5^2)*\phi(2^2)=(5^2-5)*(2^2-2)=40$

故$7^{1000} \equiv 7^{25*40} \equiv 7^{40} \equiv 1 \pmod{100}$

故7^{1000}的最后两个数位为01