```
#include "mat.h"
#include <iostream>

using namespace std;

mat::mat()
{}
ZZ mat::resto_chino(ZZ a1,ZZ p1, ZZ a2, ZZ p2){
    a1=mod(a1,p1);
    a2=mod(a2,p2);
    ZZ P = p1*p2;
    ZZ q1 = inv_mult(mod(p2,P),p1);
    ZZ q2 = inv_mult(mod(p1,P),p2);
    return mod(mod(a1*p2*q1,P)+mod(a2*p1*q2,P),P);
}
ZZ mat::inv_mult(ZZ a,ZZ n){

    ZZ save=n;
    ZZ aux,r,q;
    ZZ inv1=conv<ZZ>("0");
    ZZ inv2=conv<ZZ>("1");

    do{
        q=n/a;
        r = n-a*q;
        n=a; a=r;
        aux = inv1-q*inv2;
        inv1=inv2;
        inv2=aux;
    }while(r!=0);

    if(inv1>0)
        return inv1;
    return save+inv1;
}
ZZ mat::mcd(ZZ m, ZZ n){
    ZZ r;
    do{
        r=mod(m,n);
        m=n;n=r;
    }while(r!=0);

    return m;
}
ZZ mat::pow(ZZ base,ZZ potencia,ZZ n){
    ZZ aux = base;
    ZZ total = conv<ZZ>("1");
    while(potencia>0){
        if(potencia%2){
            total*=aux;
            total=mod(total,n);
        }
        aux*=aux;
        aux=mod(aux,n);
        cout << aux << endl;
        potencia/=2;
    }
    cout << endl;
```

```
    return total;
}
ZZ mat::mod(ZZ a,ZZ b){
    ZZ r = a-b*(a/b);
    if(r<0)return r+b;
    return r;
}
```