一 GCD：辗转相除法

没难度，主要是理解，后面你们可能会遇到稍难的题目，就是考察原理：

设 gcd(a+mb,b) = k

b = n2 * k

a+mb = n1*k

a = (n1-m*n2)*k

接下来只需证明 n2 和(n1-m*n2)没有公因子

假设有公因子 r

n2 = num2 * r

(n1-m*n2) = num1 * r

n1 - m*num2*r = num1*r

n1 = (num1+m*num2)*r

n1 和 n2 有公因子,与上面 gcd(a+mb,b) = k 矛盾,所以 n2 和(n1-m*n2)没有公因子.

综上:gcd(a+mb,b)=gcd(a,b)

```
int gcd(int a,int b)
{
    return b?gcd(b,a%b):a;
}
```

二 素数筛法：

做这类题目提前预估复杂度，看清数据范围；

普通求解素数时间复杂度：sqrt(n)

```
for(int i = 2; i <= sqrt(n); i++) {
    if(n % i == 0) return false;
}
return true; //是素数
```

最简单的素筛证明就是，拿笔走一遍，很快你就发现就是利用小的数筛大的数；

```
//打表预处理，降低时间复杂度
//Max 最大 = 1e7 左右
memset(a, 0, sizeof(a));
a[0] = a[1] = 1; //真值非素数
for(int i=2; i * i <= max; i++) {
    if(!a[i]){
        for(int j = i + i; j <= max; j += i) //是 i 的倍数便不是素数
            a[j]=1;
    }
}
```

其他方法也可自学；

三 快速幂：

网上有很多证明过程，关键就是二分的思想：

If(b % 2 == 0) a^b = [a^(b / 2)]^2 ;

If(b % 2 == 1) a^b = a * [a^(b / 2)]^2 ; //由于 b 是奇数，5 / 2 = 2 ;

理解了这个，套进模板手动画画就应该理解了

//mod 是取模值，这里是同余定理的应用

```
LL q_mod(LL a, LL b, LL mod) {
    LL ans = 1;
    while(b) {
        if(b&1) ans = ans * a % mod; //表示指数是奇数
        a = ((a % mod) * (a % mod)) % mod; //有可能 a * a 爆掉 long long
        b >>= 1; //b /= 2;
    }
    return ans;
}
```

四 同余定理：

(a * c)%b = ((a % b) * (c % b))%b;

(a + c)%b = ((a % b) + (c % b))%b;

(a - c)%b = ((a % b) - (c % b) + b)%b; //思考为什么 +b

除法不适用；

以上是模板及原理，不足的地方你们可以学习其他的，切记理解学习；