数论大杂烩

BY GY

自我介绍

- 附中16级学渣，已毕业
- 高校录取结果没出
- 所以暂时处于没学上的状态
- 虽然想和其他dalao一样吹自己CF多少分
- 但是没有打过
- 没了

欧几里德算法

欧几里德算法（gcd）

- Greatest Common Divisor(GCD)
- 最大公因数

暴力

```
for(int i=1;i<=min(a,b);i++){
    if(!(a%i)&&!(b%i)) ans=i;
}
```

欧几里德算法

```
int gcd(int a,int b){
    return b==0?a:gcd(b,a%b);
}
```

扩展欧几里德算法

扩展欧几里德算法

- 解不定方程ax+by=c（其中x，y均为整数）
- 例如6x+15y=9
- 一个方程两个未知数
- 一定有多组解
- 先只要求一组解
- 注意扩欧求解的是ax+by=gcd(a,b)
- 结果要按c与gcd(a,b)的倍数关系等比例扩大

扩展欧几里德算法

```
void exgcd(int a,int b,int& d,int& x,int& y){
    if(!b){d=a;x=1;y=0;}
    else{exgcd(b,a%b,d,y,x);y-=(a/b)*x;}
}
```

```
printf("%d %d",x*(c/d),y*(c/d));
```

扩展欧几里德算法

- 可以证明，若ax+by=c的一组整数解为(x,y)
- 则它的任意整数解可以写成(x+kb’,y-ka’)
- 其中a’=a/gcd(a,b) b’=b/gcd(a,b) k为任意正整数

扩展欧几里德算法

- 若要求x为最小正整数时的那一组解
- 只需先找出最小的正x再反推出y即可
- 课后练习
- 洛谷p1082

题目描述

求关于x的同余方程 $ax \equiv 1 \pmod{b}$ 的最小正整数解。

输入输出格式

输入格式：

一行，包含两个正整数 a, b，用一个空格隔开。

输出格式：

一个正整数 x_0，即最小正整数解。输入数据保证一定有解。

乘法逆元

乘法逆元

逆元定义

> 若$a*x\equiv 1\pmod{b}$，且a与b互质，那么我们就能定义：x 为 a 的逆元，记为a^{-1}，所以我们也可以称 x 为 a 在 $\bmod b$ 意义下的倒数，
>
> 所以对于 $\frac{a}{b}\pmod{p}$，我们就可以求出 b 在 $\bmod p$ 下的逆元，然后乘上 a，再 $\bmod p$，就是这个分数的值了。

乘法逆元

- 例题：洛谷p3811

题目描述

给定n,p求1~n中所有整数在模p意义下的乘法逆元。

乘法逆元

- 利用扩展欧几里得求乘法逆元
- 从定义入手
- 解同余方程$a * x \equiv 1 \pmod{b}$
- 转化成不定方程ax+by=1
- 然后就是普通的扩欧了

乘法逆元

- 利用费马小定理

若p为素数，a为正整数，且a、p互质。则有$a^{p-1} \equiv 1(\mathrm{mod} p)$。

- 快速幂即可

$$a * x \equiv 1 \pmod p$$

$$a * x \equiv a^{p-1} \pmod p$$

$$x \equiv a^{p-2} \pmod p$$

乘法逆元

- 线性求乘法逆元
- 很尴尬
- 其实我也不大懂
- 体感不常用
  - (反正我没用到过
- 但是过例题只能用
- 这种方法
  - (能背过就背背不过就算

首先我们有一个,$1^{-1} \equiv 1 \pmod p$

然后设 $p = k * i + r, (1 < r < i < p)$ 也就是 k 是 p/i 的商，r 是余数。

再将这个式子放到 $\pmod p$意义下就会得到:

$$k * i + r \equiv 0 \pmod p$$

然后乘上i^{-1},r^{-1}就可以得到:

$$k * r^{-1} + i^{-1} \equiv 0 \pmod p$$

$$i^{-1} \equiv -k * r^{-1} \pmod p$$

$$i^{-1} \equiv -\lfloor \frac{p}{i} \rfloor * (p \bmod i)^{-1} \pmod p$$

于是，我们就可以从前面推出当前的逆元了。

代码也很短:

```
inv[1] = 1;
for(int i = 2; i < p; ++ i)
    inv[i] = (p - p / i) * inv[p % i] % p;
```

埃氏筛法

埃氏筛法

- 线性筛素数
- 需要使用大量素数时打素数表用
- 例题：洛谷p3383

题目描述

如题，给定一个范围N，你需要处理M个某数字是否为质数的询问（每个数字均在范围1-N内）

输入输出格式

输入格式：

第一行包含两个正整数N、M，分别表示查询的范围和查询的个数。

接下来M行每行包含一个不小于1且不大于N的整数，即询问该数是否为质数。

输出格式：

输出包含M行，每行为Yes或No，即依次为每一个询问的结果。

埃氏筛法

- 思想非常简单
- 对于每个非负整数p，删除2p,3p,4p……
- 处理完所有数后，没有被删除的就是素数

```
memset(vis,0,sizeof(vis));//0为素数 1为合数
for(int i=1;i<=n;i++)
    for(int j=i*2;j<=n;j+=i)
        vis[j]=1;
```

埃氏筛法

- 效率很高，可以证明复杂度为O(nlogn)
- 但我们依然可以继续改进
- 1.只需要删除素数的整数倍即可
- 2.第二重可以直接从i*i开始

```
p[1]=1;
for(int i=2;i<=n;i++) if(!p[i]&&(ll)i*i<=n)
    for(int j=i*i;j<=n;j+=i) p[j]=1;
```

唯一分解定理

唯一分解定理

- 本来打算在乘法逆元之后讲
- 但是埃筛是前置技能必须先点出来
- 乘法逆元目前最大的用处就是分数的模运算
- 其实分数的模运算也可以用唯一分解定理解决
- 算术基本定理可表述为：任何一个大于1的自然数 N,如果N不为质数，那么N可以唯一分解成有限个质数的乘积 N=P1^a1*P2^a2*P3^a3*......*Pn^an，这里 P1<P2<P3......<Pn均为质数，其中指数ai是正整数。
- 可以利用唯一分解定理将分数取模转化为乘法取模
- 还可证明gcd(a,b)*lcm(a,b)=a*b
- 由此可以求出最小公倍数

课后练习

- 洛谷p1082
- 分发下去的例题和例题2