

数学

成都七中易健驰

VANILLA WARNING

I find that someone have finished most of the problems in this courseware, so he/she can easily cut the problem as he/she knows the solution. To prevent he/she watering too many points and to give other students more time to think, everyone should follow the coming requirements:

- Don't make noise, if you find that this lesson is too boring to study, just do what you want to do, remember, don't make noise.
- When there comes a new problem and you can cut it, don't be too excited or say "Too waterful, just skip it!". Don't talk about the solution without my permission.
- To make sure that everyone can study well, after showing the solution of a problem, I may random or force point someone to retell it again, even though he/she is doing something else. If he/she can't retell it well, he/she will lose some points.
- In order to make everyone has chance to get points, each student has a limit to get points. When you have answered enough, you can continue to answer the questions without getting points. (5 times -10 points)
- If you break these requirements, you will lose some points.
- Vanilla reserves the right of final explanation.

数学



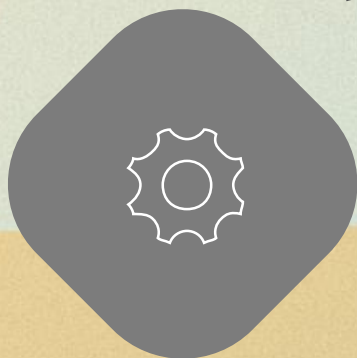
线性筛



欧拉函数



同余



素数



莫比乌斯反演



额外内容

怎么尽是些无聊的内容





简单筛

```
#include<bits/stdc++.h>
#define maxx 1000007
using namespace std;
int check[maxx],prime[maxx],pos=0,flag;
int main(){
    for(int i=2;i<maxx;i++){
        flag=1;
        for(int j=2;j<sqrt(i);j++){
            if(i%j==0){
                flag=0;
            }
        }
        if(flag==1){
            prime[pos++]=i;
        }
    }
    return 0;
}
```




优化筛

```
#include<bits/stdc++.h>
#define maxx 1000007
using namespace std;
int check[maxx],prime[maxx],pos=0,flag;
int main(){
    for(int i=2;i<maxx;i++){
        if(!check[i]){
            prime[pos++]=i;
        }
        for(int j=2*i;j<maxx;j+=i){
            check[j]=1;
        }
    }
    return 0;
}
```



线性筛

- 用来筛素数、欧拉函数、莫比乌斯函数、约数个数、约数和……

素数：只能被自己和1整除的数

欧拉函数：小于 n 的正整数中与 n 互质的数的数目

莫比乌斯函数：

1) $\mu(1) = 1$

2) 当 n 存在平方因子时, $\mu(n) = 0$

3) 当 n 是素数或奇数个不同素数之积时, $\mu(n) = -1$

4) 当 n 是偶数个不同素数之积时, $\mu(n) = 1$



线性筛素数

基本思想：

- 当前数字是 $n = p_1^a * p_2^b * p_3^c$ ($p_1 < p_2 < p_3$ 且均为素数)，一次循环筛除小于等于 p_1 的素数乘以 n 得到的数
- 比如 p_1 之前有 p_i, p_j 和 p_k 三个素数，则此次循环筛掉 $p_i * n, p_j * n, p_k * n$ 和 $p_1 * n$ ，`prime`里的素数都是升序排列的，时的`prime[j]`就是这里的 p_1 ，`break`
- 优点：没有重复筛同一个数
- 原因：按照一个数的最小素因子筛选，比如6只按2筛去



线性筛欧拉函数

基本思想：

- 当 i 为素数时，显然 $\varphi[i] = i - 1$
- 当 $i \% p[j] \neq 0$ 时， $\gcd(i, p[j]) = 1$ ，由积性函数的性质可得 $\varphi[i * p[j]] = \varphi[i] * \varphi[p[j]] = \varphi[i] * (p[j] - 1)$ (p 数组表示素数)
- 当 $i \% p[j] == 0$ 时，根据欧拉函数的求法： $\varphi[n] = n * \prod (1 - \frac{1}{p})$ ， p 为 n 的质因子，故若 $i \% p[j] == 0$ ， $i * p[j]$ 的质因子数不变

所以：

$$\varphi[i * p[j]] = i * p[j] * \prod (1 - 1/p) = p[j] * i * \prod (1 - 1/p) = p[j] * \varphi[i]$$



欧拉定理

若 a, n 互质,

则 $a^{\varphi(n)} \equiv 1 \pmod{n}$

没有证明



莫比乌斯函数

$$\begin{cases} \mu(n) = 1 & (n = 1) \\ \mu(n) = (-1)^k & (n = p_1 * p_2 * \dots * p_k) \\ \mu(n) = 0 & (others) \end{cases}$$

用处：

学习莫比乌斯反演你就知道了



线性筛莫比乌斯函数

基本思想

$$\mu[1] = 1$$

若 i 为素数则 $\mu[i] = -1$ ，若 $i \% p[j] == 0$ 则 $\mu[i * p[j]] = 0$ ，显然 $p[j]$ 就是它的平方因子，否则 $\mu[i * p[j]] = -\mu[i]$

所以它是一个积性函数



线性筛约数个数

基本思想：

- 根据约数个数定理：对于一个大于1正整数 n 可以分解质因数： $n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ ，其中 p_i 为素数
- 则 n 的正约数的个数就是： $fac[n] = (1 + d_1) * (1 + d_2) * \cdots * (1 + d_k)$
我们需要一个辅助数组 $d[i]$ ，表示 i 的最小质因子的次幂，(最小的原因是素数筛里每次都是用最小的质因子来筛合数的)，还是三种情况：

1) 当 i 为素数时， $fac[i] = 2$ ， $d[i] = 1$

2) 当 $i \% p[j] \neq 0$ ， $\gcd(i, p[j]) = 1$ ，由积性函数的性质可得

$$fac[i * p[j]] = fac[i] * fac[p[j]] = fac[i] * 2$$
$$d[i * p[j]] = 1$$

3) 当 $i \% p[j] == 0$ 时，出现平方因子，最小质因子的次幂加1，因此有

$$fac[i * p[j]] = \frac{fac[i]}{d[i] + 1} * (d[i] + 2)$$
$$d[i * p[j]] = d[i] + 1$$



线性筛代码

```
#include<bits/stdc++.h>
#define maxx 1000007
using namespace std;
int pnum,p[maxx],noprime[maxx],d[maxx],phi[maxx],mob[maxx],fac[maxx];
int main(){
    phi[1]=1;
    mob[1]=1;
    fac[1]=1;
    for(int i=2;i<maxx;i++){
        if(!noprime[i]){
            phi[i]=i-1;
            mob[i]=-1;
            p[pnum++]=i;
            fac[i]=2;
            d[i]=1;
        }
        for(int j=0;j<pnum&& i*p[j]<maxx;j++){
            noprime[i*p[j]]=1;
            if(i%p[j]==0){
                phi[i*p[j]]=phi[i]*p[j];
                mob[i*p[j]]=0;
                fac[i*p[j]]=fac[i]/(d[i]+1)*(d[i]+2);
                d[i*p[j]]=d[i]+1;
                break;
            }
            phi[i*p[j]]=phi[i]*(p[j]-1);
            mob[i*p[j]]=-mob[i];
            fac[i*p[j]]=fac[i]*2;
            d[i*p[j]]=1;
        }
    }
    return 0;
}
```




线性筛约数和

$$n = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * \dots * p_r^{a_r}$$

那么它的约数和是

$$\prod_{i=1}^r \sum_{j=0}^{a_i} p_i^j$$

维护 $low(n)$ 表示 n 的最小质因子的指数次幂，即 $p_1^{a_1}$ ， $sum(n)$ 表示 n 的最小质因子对答案的贡献，即 $\sum_{j=0}^{a_1} p_1^j$

然后像筛约数个数一样那样筛就好了



线性筛逆元

$$inv[i] = -\left(\frac{p}{i}\right) * inv[p \% i]$$

p 是模数

没有证明



Bzoj 1409

求 m 组 $p^{F[n]} \% q$ 其中 F 是斐波那契数列, p 是质数, $q < p$

$0 < p, n < 2^{31}$ $0 < q < p$ $0 < m \leq 5000$



Bzoj 1409解答

由于 p, q 互质, 使用线性筛 (求欧拉函数)和矩阵快速幂(求斐波拉契数列)以及快_(màn)速幂(求答案)



Bzoj 2186

求 $\varphi(m!) * \frac{n!}{m!} \% mod$

$0 < n, m \leq 10000000$ mod=10000000010 $T < 10000$



Bzoj 2186解答

明显 $\varphi(m!) = m! * \frac{p-1}{p}$ (p 是 $m!$ 的质因数)

题目转为求 $n! * \frac{p-1}{p}$ (p 是 $m!$ 的质因数)

预处理100000000的素数和逆元以及 $n!$



Bzoj 2721

求不定方程 $\frac{1}{x} + \frac{1}{y} = \frac{1}{n!}$, 有多少组 (x, y) 的解

$n \leq 1000000$



Bzoj 2721 解答

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n!}, \text{ 设 } z = n!$$

$$\text{则 } \frac{1}{x} + \frac{1}{y} = \frac{1}{z}, \quad x = \frac{y * z}{y - z}$$

$$\text{设 } t = y - z, \text{ 那么 } x = z + \frac{z^2}{t}$$

筛出 $n!^2$ 的约数个数即可，这就是答案



Bzoj 3288

$n * n$ 大小的矩阵, 第 i 行第 j 列的数是 $\gcd(i, j)$, 求其行列式

$0 < n \leq 1000000 \text{ mod} = 1000000007$



Bz oj 3288 解答

高斯消元后发现对角线上的数是 $\varphi(i)$

线性筛出 φ 后全部相乘

没有证明



Bzoj 3233

你来构造一堆硬币面值 A ，数量自定义，硬点 $A_1 = 1$ ，然后对于任意 $b > a$ ，要求 A_b 是 A_a 的倍数

现在要购买 n 只猫，每只猫有一个价格 B_i 而且要求单独付钱，求买下所有猫至少需要多少硬币

$1 \leq n \leq 50$ $1 \leq B_i \leq 100000$



Bzoj 3233解答

设 $dp[i]$ 表示当前最大面值为 i 零头所需的硬币数量的最小值

$$dp[i] = \min \left(dp[j] + \sum_{k=1}^n \left\lfloor \frac{B_k \% i}{j} \right\rfloor \right) (j|i)$$

$$ans = \min(dp[i] + \sum_{k=1}^n \left\lfloor \frac{B_k}{i} \right\rfloor)$$

直接做复杂度爆炸，而且也没用到线性筛



Bzoj 3233解答

$$dp[i] = \min \left(dp[j] + \sum_{k=1}^n \left\lfloor \frac{B_k \% i}{j} \right\rfloor \right) (j|i)$$

优化一下，每次要保证 $\frac{i}{j}$ 是个质数，否则不是最优解

为什么呢？

如果不是素数，那我可以取一个更小的面值(反正面值数量没有限制)，从而得到更小的答案



Bzoj 2790

定义 $f(a)$: 任意选一个质数 p , 将 a 变为 $a * p$ 或 a/p (仅 $p|a$ 时)
 $d(x, y)$ 表示 x 至少经过多少次 $f(x)$ 变成 y

现在给出一个序列 A_1 到 A_n , 对于每一个 $0 < i \leq n$, 求最小的 j ($0 < j \leq n$) 且 $i \neq j$ 满足 $d(i, j)$ 最小

$2 \leq n \leq 100000$ $A_i \leq 1000000$



Bzoj 2790解答

设 $g[x]$ 表示 x 是几个质因数的乘积(包含重复的)

那么答案就是 $g[i] + g[j] - 2 * g[\gcd(i, j)]$

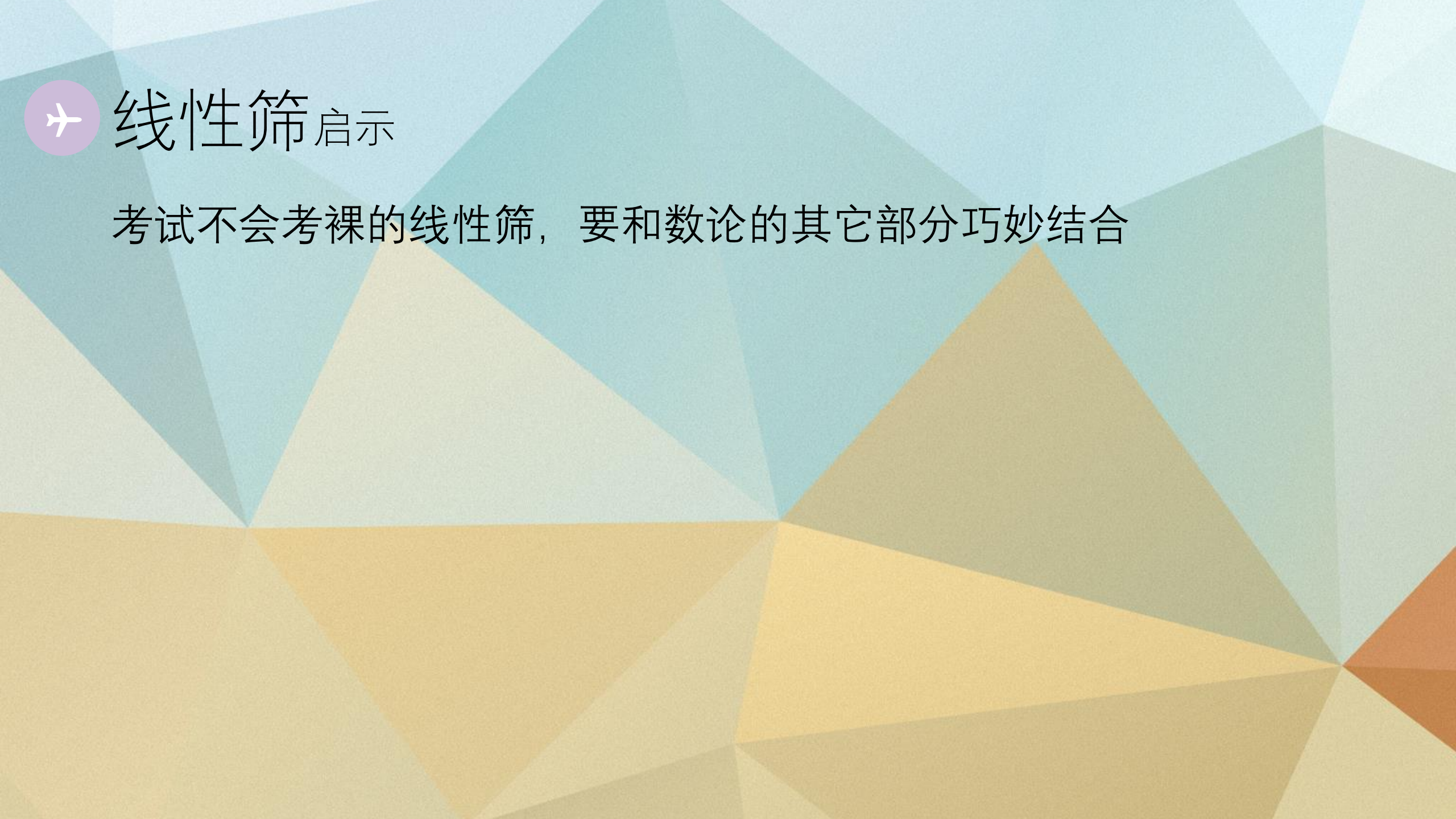
明显 $g[x]$ 可以线性筛

那么我们应该最小化 $g[j] - 2 * g[\gcd(i, j)]$

枚举 A_i 的所有因数 x , $f[x]$ 表示是 x 的倍数的 A_j 使得 $g[A_j]$ 最小的数

因为要求 $i \neq j$, 所以得维护最小值和次小值

最后对于每个 A_i 暴力枚举每个因数更新最小值即可



✈ 线性筛_{启示}

考试不会考裸的线性筛，要和数论的其它部分巧妙结合



欧拉函数

基本定义

- 小于 n 的正整数中与 n 互质的数的数目

性质

- 1) 对于一个素数 p , $\varphi(p) = p - 1$
- 2) 对于两个互质的数, $\varphi(pq) = \varphi(p) * \varphi(q)$
- 3) 是积性函数但不是完全积性函数
- 4) 单个计算方法
- 5) 除了 $\varphi(2) = 1$, 其余 $\varphi(x)$ 均为偶数
- 6) 所有比 n 小的与 n 互质的数之和为 $n * \frac{\varphi(n)}{2}$
- 7) 若正整数 n , 则 $\sum_{d|n} \varphi(d) = n$



欧拉函数性质1的证明

对于一个素数 p , $\varphi(p) = p - 1$

比一个素数小的数都与它互质

≡ 积性函数和完全积性函数

积性函数

对于任意互质的整数 a 和 b 有性质 $f(ab) = f(a)f(b)$ 的数论函数。

完全积性函数

对于任意整数 a 和 b 有性质 $f(ab) = f(a)f(b)$ 的数论函数。



欧拉函数性质2&3的证明

对于两个互质的数, $\varphi(pq) = \varphi(p) * \varphi(q)$
是积性函数但不是完全积性函数

xtc: "这不是常识吗?"

百度百科的证明是错的

由于篇幅所限, 若欲阅读详细证明, 请单击左下角链接



欧拉函数性质4的证明

单个计算方法 $\varphi(n) = n * \prod_{p|n} \left(1 - \frac{1}{p}\right)$ p 是质因子

设 $n = p_1^{k1} * p_2^{k2} * \dots * p_r^{kr}$

由性质2, $\varphi(n) = \varphi(p_1^{k1}) * \varphi(p_2^{k2}) * \dots * \varphi(p_r^{kr})$

那我们需要知道 $\varphi(p_i^{ki})$ 如何计算

比 p_i^{ki} 小的正整数必须不含质因数 p_i 才行, 而含有 p_i 的数有 p_i^{ki-1} 个

所以 $\varphi(p_i^{ki}) = p_i^{ki} - p_i^{ki-1} = p_i^{ki} \left(1 - \frac{1}{p_i}\right)$

那么 $\varphi(n) = p_1^{k1} \left(1 - \frac{1}{p_1}\right) * p_2^{k2} \left(1 - \frac{1}{p_2}\right) * \dots * p_r^{kr} \left(1 - \frac{1}{p_r}\right)$

也就是 $\varphi(n) = n * \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|n} (p - 1)$



欧拉函数性质5的证明

除了 $\varphi(2) = 1$ ，其余 $\varphi(x)$ 均为偶数

若 x 是奇数

那么 $\varphi(x)$ 一定会有一项 $\left(1 - \frac{1}{p}\right) * \dots$ ，其中 p 是一个奇质因子

所以是偶数

若 x 是大于2的偶数

若只有一个质因数2，去掉一个质因数2过后和 x 为奇数的情况一样

若有很多质因数2，去掉一个质因数2还是偶数



欧拉函数性质6的证明

所有比 n 小的与 n 互质的数之和为 $n * \frac{\varphi(n)}{2}$

若存在小于 n 的 x 使 $\gcd(x, n) = 1$ ，那么一定有 $\gcd(x, n - x) = 1$

那么就可以得知与 n 互质的数都是成对存在的，并且和为 n



欧拉函数性质7的证明

若正整数 n ，则 $\sum_{d|n} \varphi(d) = n$

设 $n = p_1^{k_1} * p_2^{k_2} * \dots * p_r^{k_r}$

假如我们现在手贱在 n 后面乘一个 p_r

则 $n * p_r = p_1^{k_1} * p_2^{k_2} * \dots * p_r^{k_r+1}$

设 $f(n) = \sum_{d|n} \sum_{t|d, t|p_r} \mu(t) \varphi(d)$

1) 若 $\gcd(d, p_r) = 1$ ，有 $t = 1$ ，整个后面为 $\varphi(d)$

2) 若 $\gcd(d, p_r) = p_r$ ，有 $t_1 = 1, t_2 = p_r$ ，整个后面为0

p_r 是质数所以 $\mu(p_r) = -1$



欧拉函数性质7的证明

$f(n)$ 完全排除了来自 p_r 的干扰

$$\text{设 } F(n) = \sum_{d|n} \varphi(d)$$

$$\text{那么 } F(n) = f(n) * (\varphi(1) + \varphi(p_r) + \varphi(p_r^2) + \cdots + \varphi(p_r^{kr}))$$

$$\text{所以 } F(n * p_r) = f(n) * (\varphi(1) + \varphi(p_r) + \varphi(p_r^2) + \cdots + \varphi(p_r^{kr}) + \varphi(p_r^{kr+1}))$$

$$\text{我们知道 } \varphi(p_r^t) = p_r^t - p_r^{t-1}$$

$$\text{化简得 } F(n) = f(n) * p_r^{kr}$$

$$\text{同理 } F(n * p_r) = f(n * p_r) * p_r^{kr+1}$$

由于 $f(n)$ 完全排除了来自 p_r 的干扰，所以 $f(n * p_r) = f(n)$

$$\text{得到 } F(n * p_r) = f(n) * p_r^{kr+1}$$



欧拉函数性质7的证明

已知 $F(n * p_r) = f(n) * p_r^{kr+1}$

又有 $F(n) = f(n) * p_r^{kr}$

所以 $F(n * p_r) = F(n) * p_r$

明显 $F(1) = 1$

终于 $F(n) = n$

也就是 $\sum_{d|n} \varphi(d) = n$



欧拉函数性质7的拓展

随手推导一下

$$\sum_{i=1}^n i = \sum_{i=1}^n \sum_{d|i} \varphi(d) = \sum_{d=1}^n \varphi(d) \left\lfloor \frac{n}{d} \right\rfloor$$

再反演一下

$$\varphi(n) = \sum_{d|n} \mu(d) * \frac{n}{d}$$

不知道有什么用



Bzoj 4802简化版

求 $\varphi(n)$

$n \leq 1000000000000000$



Bzoj 4802简化版解答

根号枚举质因数+线性筛



Bzoj 4802

求 $\varphi(n)$

$n \leq 1000000000000000000$



Bzoj 4802解答

用Miller-rabin和Pollard-rho来解



Bzoj 2818

求 $1 \leq i, j \leq n$, 且 $\gcd(i, j)$ 是素数的有序对数

$n \leq 10000000$



Bzoj 2818解答

枚举每个质数，那么问题变为 $1 \leq i, j \leq \frac{n}{p}$, $\gcd(i, j) = 1$ 的数量

假设 $i < j$ ，那么对于每个 j ，答案为 $\varphi(j)$

要求有序对，那么乘2就好了，再减去多余的一对(1,1)

预处理 φ 的前缀和 sum

$$ans = \sum_p (sum[\frac{n}{p}] * 2 - 1)$$



Bzoj 4173

设 $S(n, m)$ 表示所有 $n \% k + m \% k \geq k$ 的 k 的集合

求 $\varphi(n) + \varphi(m) + \sum_{k \in S(n, m)} \varphi(k)$

$n, m \leq 1000000000000000000 \bmod = 998244353$



Bzoj 4173 解答

稍微转化一下，题目限制变为 $\left\lfloor \frac{n+m}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{m}{k} \right\rfloor = 1$

$\sum_{k \in S(n,m)} \varphi(k)$ 变成 $\sum_{\left\lfloor \frac{n+m}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{m}{k} \right\rfloor = 1} \varphi(k)$

那就是 $\sum_{k=1}^{n+m} \left(\left\lfloor \frac{n+m}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{m}{k} \right\rfloor \right) \varphi(k)$

因为其它情况下 $\left\lfloor \frac{n+m}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{m}{k} \right\rfloor = 0$

注意到后两项的上限

所以有 $\sum_{k=1}^{n+m} \varphi(k) * \left\lfloor \frac{n+m}{k} \right\rfloor - \sum_{k=1}^n \varphi(k) * \left\lfloor \frac{n}{k} \right\rfloor - \sum_{k=1}^m \varphi(k) * \left\lfloor \frac{m}{k} \right\rfloor$



Bzoj 4173 解答

那么 $\sum_{k=1}^n \varphi(k) * \left\lfloor \frac{n}{k} \right\rfloor$ 是什么呢?

由于性质7: $\sum_{d|n} \varphi(d) = n$

那么 $\sum_{k=1}^n \varphi(k) * \left\lfloor \frac{n}{k} \right\rfloor = \sum_{i=1}^n \sum_{k|i}^i \varphi(k) = \sum_{i=1}^n i = \frac{n(n-1)}{2}$

所以原式 = $\frac{(n+m)(n+m-1)}{2} - \frac{n(n-1)}{2} - \frac{m(m-1)}{2} = n * m$

最终答案为 $\varphi(n) + \varphi(m) + n * m$

打表也可以发现这个规律



Bz oj 3643&4803

已知 n , 求满足 $\varphi(i) = n$ 的前 k 项

3643: $n < 2147483648$ $k = 1$

4803: $n \leq 1000000000000000000$ $k \leq 1000$



Bz oj 3643&4803解答

我们知道 $\varphi(n) = n * \prod_{p|n} \left(1 - \frac{1}{p}\right)$

所以 $n = \varphi(n) * \prod_{p|n} \left(\frac{p}{p-1}\right)$

则 p_k 是 n 的约数

线性筛出 \sqrt{n} 以内的质数，然后dfs尝试去获得 n ，当 $x \geq \sqrt{n}$ ，使用miller-rabin判断质数，一旦是质数，就退出
注意特判2

答案数量大概在500000以内



同余

基本定义

- 两个整数 a 、 b ，若它们除以整数 m 所得的余数相等，则称 a 与 b 对于模 m 同余或 a 同余于 b 模 m 。
- 记作： $a \equiv b \pmod{m}$



同余

性质

- 1.反身性： $a \equiv a \pmod{m}$
- 2.对称性：若 $a \equiv b \pmod{m}$ ，则 $b \equiv a \pmod{m}$
- 3.传递性：若 $a \equiv b \pmod{m}$ ， $b \equiv c \pmod{m}$ ，则 $a \equiv c \pmod{m}$
- 4.相加减：若 $a \equiv b \pmod{m}$ ， $c \equiv d \pmod{m}$ ，则 $a \pm c \equiv b \pm d \pmod{m}$
- 5.相乘：若 $a \equiv b \pmod{m}$ ， $c \equiv d \pmod{m}$ ，则 $a * c \equiv b * d \pmod{m}$
- 6.相除：若 $a * c \equiv b * c \pmod{m}$ ，则 $a \equiv b \pmod{\frac{m}{\gcd(c,m)}}$
- 7.幂：若 $a \equiv b \pmod{m}$ ，则 $a^c \equiv b^c \pmod{m}$
- 8.组合性：若 $a \equiv b \pmod{m_i} \ i \in [1, n]$ ，则 $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_n)}$



同余

掌握如下定理或知识

- 欧拉定理
- 原根
- 费马小定理
- 中国剩余定理
- 二次剩余
- 大步小步算法



欧拉定理

若 a, n 互质,

则 $a^{\varphi(n)} \equiv 1 \pmod{n}$, 就是 $a^b \equiv a^{b \% \varphi(n)} \pmod{n}$

没有证明



扩展欧拉定理

若 a, n 不互质,

则 $a^b \equiv a^{b \% \varphi(n) + \varphi(n)} \pmod{n}$

没有证明



原根

$2, 4, pa, 2pa$ (p 是奇数) 这些数有原根, 且个数为 $\varphi(\varphi(m))$

若 g 是 m 的一个原根, 则 $g^1, g^2, g^3, \dots, g^{m-1}$ 可以刚好表示完 1 到 $m-1$ 的所有自然数

这样一来, 乘法可以变作加法与快速幂的结合

怎么求原根呢?

将 $\varphi(m)$ 进行质因数分解为 $p_1^{a_1} * p_2^{a_2} * \dots * p_n^{a_n}$, 若恒有 $g^{\frac{\varphi(m)}{p_i}} \neq 1 \pmod{m}$, 则 g 是 m 的一个原根

g 从 $\varphi(m)$ 向下枚举即可



原根

将 $\varphi(m)$ 进行质因数分解为 $p_1^{a_1} * p_2^{a_2} * \dots * p_n^{a_n}$, 若恒有 $g^{\frac{\varphi(m)}{p_i}} \neq 1(mod\ m)$, 则 g 是 m 的一个原根

g 从 $\varphi(m)$ 向下枚举即可

这是什么原理?

我们都知道若 a, n 互质, 则 $a^{\varphi(n)} \equiv 1(mod\ n)$ (欧拉定理)

所以我们只要保证 $a^n \equiv 1(mod\ m)$ 只在 $n = \varphi(m)$ 时成立即可



费马小定理

若 a, n 互质, n 是个质数

则 $a^{n-1} \equiv 1 \pmod{n}$

不就是低配版的欧拉定理吗



中国剩余定理

如果有同余方程组

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

设 $M = \prod_{i=1}^n m_i$, $M_i = M/m_i$, t_i 为 M_i 在模 m_i 下的逆元

那么在模 M 的意义下

$$x = \sum_{i=1}^n a_i t_i M_i$$



二次剩余

当存在某个 $x^2 \equiv d \pmod{p}$ 式子成立时，称“ d 是模 p 的二次剩余”

当对任意 x 不成立时，称“ d 是模 p 的二次非剩余”

说白了就是模意义下能否开根号

我们今天只讨论 p 是奇质数的情况

即求解 $x^2 \equiv a \pmod{p}$ 且 $p \nmid a$

≡ 二次剩余 勒让德符号/欧拉判别准则

定义

若 $p \mid d$, 则 $\left(\frac{d}{p}\right) = 0$

若 d 是模 p 的二次剩余, 则 $\left(\frac{d}{p}\right) = 1$

若 d 是模 p 的二次非剩余, 则 $\left(\frac{d}{p}\right) = -1$

≡ 二次剩余 勒让德符号/欧拉判别准则

其中 $\left(\frac{d}{p}\right) = d^{\frac{p-1}{2}}$

设 $x^2 \equiv d \pmod{p}$, 那么 $\left(\frac{d}{p}\right) = x^{p-1} \equiv \pm 1 \pmod{p}$

若 d 是二次剩余, 由费马小定理, 那么 x 存在

若 d 是二次非剩余, 由费马小定理, 那么 x 不存在



二次剩余解决

设 a 满足 $w = a^2 - n$, w 对于 p 不是二次剩余, 这个 a 直接随机就好了
由于 x 的数量是 $\frac{p-1}{2}$, 所以期望下随出来一个合法 w 的概率是 $\frac{p-1}{2p}$

期望下大概就随机两次吧

我们最后的答案是 $x = (a + \sqrt{w})^{\frac{p+1}{2}}$



二次剩余解决

以下所有运算皆在模意义下

你问我为什么 $x = (a + \sqrt{w})^{\frac{p+1}{2}}$?

那是因为 $x^2 = (a + \sqrt{w})^{p+1} = (a + \sqrt{w})^p * (a + \sqrt{w})$

由二项式定理 $(a + \sqrt{w})^p = \sum_{k=0}^p C(k, p) * a^k * (\sqrt{w})^{p-k}$

因为我们在模意义下计算，所以 $0 < k < p$ 时， $C(k, p) \equiv 0 \pmod{p}$

所以 $(a + \sqrt{w})^p = a^p + \sqrt{w}^p$

由费马小定理 $a^{p-1} = 1$

由欧拉判别准则 $\sqrt{w}^{p-1} = -1$

那么 $(a + \sqrt{w})^p = a - \sqrt{w}$

$x^2 = (a - \sqrt{w}) * (a + \sqrt{w}) = a^2 - w = n$



二次剩余解决

$$\text{所以 } x = (a + \sqrt{w})^{\frac{p+1}{2}}$$

其实还可以发现，若 n 是质数，有 $(a + b)^n \equiv a^n + b^n \pmod{n}$

当 p 不是质数的时候呢?点击左下角链接



大步小步算法

用于解 $a^x \equiv n \pmod{p}$

设 $m = \lfloor \sqrt{p} \rfloor$, $x = i * m + j$

$$a^j \equiv n * a^{-m*i} \pmod{p}$$

枚举 $0 \leq j < p$, 将 (a^j, j) 加入 hash 表

然后枚举右边的 i , 设 x 是 a^{m*i} 在模 p 意义下的逆元

那么右边就变成 $n * x$, 然后在左边的 hash 表里面找有没有对应的就好了



指标

设 g 是 p 的原根, 若 $g^r \equiv a \pmod{p}$ 成立, 则称 r 是以 g 为底的 a 对模 m 的一个指标

记作 $r = \text{ind}(a)$



Bzoj 3884

求 $2^{2^{2^{\dots^{\infty}}}} \% p$

$p \leq 100000000$ $T \leq 1000$



Bz oj 3884 解答

假如我们有一个函数 $f(p) = 2^{2^{2^{\dots^{\infty}}}} \% p$
根据扩展欧拉定理

$$f(p) = 2^{(2^{2^{\dots^{\infty}}}) \% \varphi(p) + \varphi(p)} \% p$$

$$f(p) = 2^{f(\varphi(p)) + \varphi(p)} \% p$$

递归做下去，明显 $\varphi(p)$ 会很快降为 1，然后回溯即可



Bzoj 4869

维护一个序列，支持如下操作

1 $l\ r$ 对于所有 $l \leq i \leq r$, $a_i = c^{a_i}$ (c, p 在开局给定)

2 $l\ r$ 区间求和

在模 p 意义下操作

$1 \leq n, m \leq 50000$ $0 \leq c, a_i < p \leq 10000000000$



Bzoj 4869解答

和上一题原理一样，明显任意一个位置上的数迭代几次后就会变成定值，事实上这个值是 $\log n$ (没有证明)

线段树维护，记录每个位置被修改了几次，若一个结点下的整个区间都修改到顶了，就不用再修改了

据说可以预处理 c 的次方来避免快速幂的复杂度



Bzoi 2480&3239

求最小的 x 使 $a^x \equiv n \pmod p$

2480: $a, n, p \leq 10000000000$ $T \leq 100$

3239: $a, n, p < 2147483648$ $T = 7$



Bzoj 2480&3239解答

扩展大步小步算法



Bzoj 1406

求 $x^2 \equiv 1(mod\ p)$ 的所有 $x(< p)$

$p \leq 2000000000$



Bzoj 1406解答

变化一下 $x^2 - 1 = kp$

$$(x + 1)(x - 1) = kp$$

设 $x + 1 = k_1 p_1$, $x - 1 = k_2 p_2$, $k_1 k_2 = k$, $p_1 p_2 = p$

枚举 p 的所有约数即可



Bzoj 2219

求满足 $x^a \equiv b \pmod{2k+1}$ 的 $x (\leq 2k)$ 的数量



Bzoi 2219解答

设 $p = 2k + 1 = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$

最终答案是 $x^a \equiv b \pmod{p_i^{a_i}}$ 的答案数量的乘积
于是分情况讨论

1. $\gcd(b, p^c) = p^c$

那么就有 $x^a \equiv 0 \pmod{p^c}$, 这个答案随便算

2. $\gcd(b, p^c) = 1$

$x^a \equiv b \pmod{p^c} \rightarrow a * \text{ind}(x) \equiv \text{ind}(b) \pmod{\varphi(p^c)}$

大步小步算出 ind 后, 这是一个很简单的同余方程



Bzoj 2219解答

这个很简单的同余方程长成这样 $ax \equiv b(\text{mod } p)$

如果 $b \% \gcd(a, p) \neq 0$ 则无解，否则解的个数为 $\gcd(a, p)$

3. $\gcd(b, p^c) > 1$

设 $b = p^{cnt} * b_2$ ，则

$$x^a \equiv p^{cnt} * b_2(\text{mod } p^c)$$

如果 $cnt \% a \neq 0$ 则无解，否则转化一下方程

$$\left(\frac{x}{p^{\frac{cnt}{a}}} \right)^a \equiv b_2(\text{mod } p^{c-cnt})$$

此时 $\gcd(p^{c-cnt}, b_2) = 1$ ，转为上一种情况，注意 x 的取值范围会改变，还要乘上 $p^{cnt - \frac{cnt}{a}}$



素数

真的没什么好讲的



素数

哥德巴赫猜想

任一大于2的偶数都可写成两个质数之和
在OI的数据范围里成立



素数

Miller Rabin 算法

费马小定理和二次探测都用上
自己去切掉Bzoj 3667

莫比乌斯反演吗？
听上去还不错





莫比乌斯函数

$$\begin{cases} \mu(n) = 1 & (n = 1) \\ \mu(n) = (-1)^k & (n = p_1 * p_2 * \cdots * p_k) \\ \mu(n) = 0 & (others) \end{cases}$$

性质

1) 积性函数

$$2) \sum_{d|n} \mu(d) = [n = 1]$$



莫比乌斯函数性质1的证明

积性函数

参阅线性筛部分

莫比乌斯函数性质2的证明

$$\sum_{d|n} \mu(d) = [n = 1]$$

当 $n = 1$ 时, $\mu(1) = 1$

当 $n > 1$ 时, 设 $n = p_1^{k_1} * p_2^{k_2} * \dots * p_m^{k_m}$, $d = p_1^{x_1} * p_2^{x_2} * \dots * p_m^{x_m}$

根据 μ 的定义, 只用考虑 $x_i = 0$ or 1

若 $\mu(d) \neq 0$, 那么每个质因数在 d 中不能出现超过一次, 假设 d 中存在 r 个 x_i 为 1 , 则

$$\sum_{d|n} \mu(d) = C(0, m) - C(1, m) + C(2, m) - \dots + (-1)^m * C(m, m) = \sum_{r=0}^m \binom{m}{r} (-1)^r$$

由二项式定理

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

令 $x = 1, y = -1$, 得证



莫比乌斯反演公式

现在直接套用

$$F(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

什么?你要看证明?

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

$$f(n) = \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} f(k)$$

$$f(n) = \sum_{k|n} f(k) \sum_{d|\frac{n}{k}} \mu(d)$$

我们知道只有当 $\frac{n}{k} = 1$ 即 $k = n$ 的时候后半部分才等于1, 其他情况都为0, 所以就等于 $f(n)$



莫比乌斯反演另一种公式

$$F(n) = \sum_{n|d} f(d) \Rightarrow f(n) = \sum_{n|d} \mu\left(\frac{d}{n}\right) F(d)$$

≡ 莫比乌斯函数性质3和证明

对于任意正整数 n 有 $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$

只需要令 $F(n) = n, f(n) = \varphi(n)$ ，代入莫比乌斯反演的公式

$$F(n) = \sum_{d|n} f(d) \quad (\text{欧拉函数性质7})$$

$$f(n) = \sum_{d|n} \mu(d) * F\left(\frac{n}{d}\right)$$

$$\varphi(n) = \sum_{d|n} \mu(d) * \frac{n}{d}$$

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$$



Bzoj 2440

求出第 k 大的无平方因子的数(不考虑1)

$k < 10000000000$ $T < 50$



Bzoj 2440解答

二分答案，查询 $[1, n]$ 中有多少满足
设质数集 p
随便容斥一下，那么答案就是

$$n - (S(p_1) + S(p_2) + \cdots + S(p_k)) + (S(p_1p_2) + S(p_1p_3) + \cdots + S(p_{k-1}p_k)) + \cdots + (-1)^k S(\prod_{i=1}^k p_i)$$

其中 $S(i)$ 表示 $\left\lfloor \frac{n}{i} \right\rfloor$

暴力枚举子集？



Bzoj 2440解答

$$n - (S(p_1) + S(p_2) + \cdots + S(p_k)) + (S(p_1p_2) + S(p_1p_3) + \cdots + S(p_{k-1}p_k)) + \cdots + (-1)^k S(\prod_{i=1}^k p_i)$$

不难发现 μ 的系数和这个容斥很像啊

若 d 是由奇数个不同质数组成, $\mu(d) = -1$

若 d 是由偶数数个不同质数组成, $\mu(d) = 1$

若 d 含有平方因子, $\mu(d) = 0$, 正巧我们也不想要它们

所以答案是

$$\sum_{d=1}^{\lfloor \sqrt{n} \rfloor} \mu(d) * \left\lfloor \frac{n}{d * d} \right\rfloor$$



Bzoi 1101&2045

给定 a, b, d , 求有多少对 (x, y) , 满足 $x \leq a, y \leq b$ 且 $\gcd(x, y) = d$,
多组询问

1101: $0 < d \leq a, b \leq 50000$ $T \leq 50000$

2045: $0 < d \leq a, b \leq 1000000$ $T = 1$



Bzoj 1101&2045解答

把题面改为 $x \leq \frac{a}{d}, y \leq \frac{b}{d}$ 且 $\gcd(x, y) = 1$, 改变 a, b 的意义

众所周知, $\sum_{d|n} \mu(d) = [n = 1]$

$$\sum_{x=1}^a \sum_{y=1}^b [(x, y) = 1] = \sum_{x=1}^a \sum_{y=1}^b \sum_{d|(x, y)} \mu(d)$$

$$= \sum_{d=1}^{\min(a, b)} \mu(d) \sum_{x=1 \& d|x}^a \sum_{y=1 \& d|y}^b 1 = \sum_{d=1}^{\min(a, b)} \mu(d) * \left\lfloor \frac{a}{d} \right\rfloor * \left\lfloor \frac{b}{d} \right\rfloor$$

还是过不了, 但是不难发现 $\left\lfloor \frac{a}{d} \right\rfloor, \left\lfloor \frac{b}{d} \right\rfloor$ 的取值有限, 所以分块一下就好了



Bzoj 1101&2045解答

改一下代码可以过Bzoj 2301



Bzoi 1101&2045发现

以后把这个当一个结论来用

$$\sum_{x=1}^a \sum_{y=1}^b [(x, y) = 1] = \sum_{d=1}^{\min(a, b)} \mu(d) * \left\lfloor \frac{a}{d} \right\rfloor * \left\lfloor \frac{b}{d} \right\rfloor$$



Bzoj 3529

一张 $n * m$ 的数表，第 i 行第 j 列是所有 i 和 j 的公约数之和，计算数表内不大于 a 的所有数之和，多次询问

$1 \leq n, m \leq 100000$ $|a| \leq 10000000000$

$1 \leq T \leq 20000$ $\text{mod} = 2147483648$



Bzoj 3529 解答

先不考虑 a 的限制，那么我们就就是要计算

$$\sum_{i=1}^n \sum_{j=1}^m \sum_{d|i, d|j} d = \sum_{i=1}^n \sum_{j=1}^m \sum_{d=1}^{\min(n,m)} f(d) * [\gcd(i, j) = d]$$

其中 $f(d)$ 表示 d 的约数和，我们知道可以线性筛出来(参见线性筛部分)

$$= \sum_{d=1}^{\min(n,m)} f(d) \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} \sum_{j=1}^{\lfloor \frac{m}{d} \rfloor} [\gcd(i, j) = 1]$$

由上一道题的结论

$$= \sum_{d=1}^{\min(n,m)} f(d) \sum_{t=1}^{\min(\lfloor \frac{n}{d} \rfloor, \lfloor \frac{m}{d} \rfloor)} \mu(t) \left\lfloor \frac{n}{dt} \right\rfloor \left\lfloor \frac{m}{dt} \right\rfloor$$



Bzoj 3529 解答

设 $q = dt$

$$\sum_{d=1}^{\min(n,m)} f(d) \sum_{t=1}^{\min(\lfloor \frac{n}{d} \rfloor, \lfloor \frac{m}{d} \rfloor)} \mu(t) \lfloor \frac{n}{dt} \rfloor \lfloor \frac{m}{dt} \rfloor = \sum_{q=1}^{\min(n,m)} \lfloor \frac{n}{q} \rfloor \lfloor \frac{m}{q} \rfloor \sum_{d|q} f(d) \mu\left(\frac{q}{d}\right)$$

$g(x) = \sum_{d|q} f(d) \mu\left(\frac{q}{d}\right)$ (一个狄利克雷卷积) 可以预处理前缀和
 $\sum_{q=1}^{\min(n,m)} \lfloor \frac{n}{q} \rfloor \lfloor \frac{m}{q} \rfloor$ 可分块

但是现在有 a 的限制



Bzoj 3529解答

xtc:

将询问按 a 的大小离线， $f(x)$ 也从小到大排序

我们就动态维护一个树状数组 c ，每一位 $c[x]$ 存的是卷积 $g(x)$ 中 $f(d)$ 不超过 a 的数之和，每次询问之前准备好即可



Bzoj 2154

求 $\sum_{i=1}^n \sum_{j=1}^m lcm(i, j)$

$n, m \leq 10000000 \text{ mod} = 20101009$



Bzoj 2154 解答

$$\sum_{i=1}^n \sum_{j=1}^m lcm(i, j) = \sum_{i=1}^n \sum_{j=1}^m \frac{ij}{gcd(i, j)}$$

$$= \sum_{p=1}^{\min(n, m)} \sum_{i=1}^n \sum_{j=1}^m \frac{ij}{p} [gcd(i, j) = p]$$

$$= \sum_{p=1}^{\min(n, m)} \sum_{i=1}^{\lfloor \frac{n}{p} \rfloor} \sum_{j=1}^{\lfloor \frac{m}{p} \rfloor} pij [gcd(i, j) = 1]$$

$$= \sum_{p=1}^{\min(n, m)} p \sum_{i=1}^{\lfloor \frac{n}{p} \rfloor} \sum_{j=1}^{\lfloor \frac{m}{p} \rfloor} ij \sum_{d|gcd(i, j)} \mu(d)$$

$$= \sum_{p=1}^{\min(n, m)} p \sum_{i=1}^{\lfloor \frac{n}{p} \rfloor} \sum_{j=1}^{\lfloor \frac{m}{p} \rfloor} ij \sum_{d|i, d|j} \mu(d)$$

$$= \sum_{p=1}^{\min(n, m)} p \sum_{d=1}^{\min(\lfloor \frac{n}{p} \rfloor, \lfloor \frac{m}{p} \rfloor)} \mu(d) \sum_{i=1}^{\lfloor \frac{n}{pd} \rfloor} id \sum_{j=1}^{\lfloor \frac{m}{pd} \rfloor} jd$$

$$= \sum_{p=1}^{\min(n, m)} p \sum_{d=1}^{\min(\lfloor \frac{n}{p} \rfloor, \lfloor \frac{m}{p} \rfloor)} d^2 \mu(d) \sum_{i=1}^{\lfloor \frac{n}{pd} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{pd} \rfloor} j$$



Bzoj 2154 解答

$$\sum_{i=1}^n \sum_{j=1}^m \text{lcm}(i, j) = \sum_{p=1}^{\min(n, m)} p \sum_{d=1}^{\min(\lfloor \frac{n}{p} \rfloor, \lfloor \frac{m}{p} \rfloor)} d^2 \mu(d) \sum_{i=1}^{\lfloor \frac{n}{pd} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{pd} \rfloor} j$$

预处理 μ 和 $\mu(i) * i^2$ 及其前缀和
分块套分块即可



Bzoj 2693

求 $\sum_{i=1}^n \sum_{j=1}^m lcm(i, j)$, 多组询问

$n, m \leq 10000000$ $T \leq 10000$ $\text{mod} = 1000000009$



Bzoj 2693解答

从上一道题的结论继续

$$\begin{aligned}\sum_{i=1}^n \sum_{j=1}^m \text{lcm}(i, j) &= \sum_{p=1}^{\min(n, m)} p \sum_{d=1}^{\min(\lfloor \frac{n}{p} \rfloor, \lfloor \frac{m}{p} \rfloor)} d^2 \mu(d) \sum_{i=1}^{\lfloor \frac{n}{pd} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{pd} \rfloor} j \\ &= \sum_{k=1}^{\min(n, m)} \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor} i \sum_{j=i}^{\lfloor \frac{m}{k} \rfloor} j \sum_{d|k} d^2 \mu(d) * \frac{k}{d}\end{aligned}$$

设

$$f(k) = \sum_{d|k} d^2 \mu(d) * \frac{k}{d} = k \sum_{d|k} \mu(d) * d$$

则

$$= \sum_{k=1}^{\min(n, m)} \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor} i \sum_{j=i}^{\lfloor \frac{m}{k} \rfloor} j * f(k)$$



Bz oj 2693 解答

现在要快速预处理出

$$f(k) = \sum_{d|k} d^2 \mu(d) * \frac{k}{d} = k \sum_{d|k} \mu(d) * d$$

$f(x)$ 可以表示为两个积性函数的狄利克雷卷积，也是积性函数
不难发现当 w 是质数时

$$f(w) = w - w^2$$

当 n 是几个一次质数组合时

$$f(n) = f(p_1) * f(p_2) * \cdots * f(p_n)$$

当 a 有系数次数增加时 ($b|a$)

$$f(a * b) = f(a) * b$$

然后就可以线性筛了，前面部分照常分块



Bz oj 2694&4659

求 $\sum_{i=1}^n \sum_{j=1}^m lcm(i, j) * |\mu(gcd(i, j))|$, 多组询问
(即最大公倍数不包含平方因子)

2694: $n, m \leq 4000000$ $T \leq 10000$ $mod = 1073741824$

4659: $n, m \leq 4000000$ $T \leq 2000$ $mod = 1073741824$



Bzoj 2694&4659解答

设 $n \leq m$

$$\begin{aligned}
 & \sum_{i=1}^n \sum_{j=1}^m \text{lcm}(i, j) * |\mu(\text{gcd}(i, j))| \\
 &= \sum_{d=1}^n |\mu(d)| \sum_{i=1}^n \sum_{j=1}^m [\text{gcd}(i, j) = d] \frac{ij}{d} \\
 &= \sum_{d=1}^n |\mu(d)| \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} \sum_{j=1}^{\lfloor \frac{m}{d} \rfloor} [\text{gcd}(i, j) = 1] ijd \\
 &= \sum_{d=1}^n d |\mu(d)| \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{d} \rfloor} j \sum_{p|\text{gcd}(i, j)} \mu(p)
 \end{aligned}$$

$$\begin{aligned}
 &= \sum_{d=1}^n d |\mu(d)| \sum_{p=1}^{\lfloor \frac{n}{d} \rfloor} \mu(p) \sum_{i=1}^{\lfloor \frac{n}{dp} \rfloor} ip \sum_{j=1}^{\lfloor \frac{m}{dp} \rfloor} jp \\
 &= \sum_{d=1}^n d |\mu(d)| \sum_{p=1}^{\lfloor \frac{n}{d} \rfloor} p^2 \mu(p) \sum_{i=1}^{\lfloor \frac{n}{dp} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{dp} \rfloor} j
 \end{aligned}$$

设 $t = dp$

$$\begin{aligned}
 &= \sum_{t=1}^n \sum_{i=1}^{\lfloor \frac{n}{t} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{t} \rfloor} j \sum_{p|t} p^2 \mu(p) \frac{t}{p} \left| \mu\left(\frac{t}{p}\right) \right| \\
 &= \sum_{t=1}^n t \sum_{i=1}^{\lfloor \frac{n}{t} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{t} \rfloor} j \sum_{p|t} p \mu(p) \left| \mu\left(\frac{t}{p}\right) \right|
 \end{aligned}$$



Bz oj 2694&4659解答

$$\sum_{i=1}^n \sum_{j=1}^m lcm(i, j) * |\mu(gcd(i, j))| = \sum_{t=1}^n t \sum_{i=1}^{\lfloor \frac{n}{t} \rfloor} i \sum_{j=1}^{\lfloor \frac{m}{t} \rfloor} j \sum_{p|t} p \mu(p) \left| \mu\left(\frac{t}{p}\right) \right|$$

设 $f(t) = \sum_{p|t} p \mu(p) \left| \mu\left(\frac{t}{p}\right) \right|$

不难发现当 w 是质数时

$$f(w) = 1 - w$$

设 p_i 是 w 的最小质因子

当 w 不含有 p_i^1

$$f(w * p_i) = f(w) * f(p_i)$$

当 w 含有 p_i^1

$$f(w * p_i) = -f\left(\frac{w}{p_i}\right) * p_i$$

当 w 含有 p_i^2

$$f(w * p_i) = 0$$

然后就可以线性筛了，前面部分照常分块



Bz oj 4176

求 $\sum_{i=1}^n \sum_{j=1}^n d(ij)$

($d(x)$ 为 x 的约数个数)

$n \leq 10000000000 \text{ mod} = 1000000007$



Bzoi 4176解答

首先是一个结论

$$d(nm) = \sum_{i|n} \sum_{j|m} [\gcd(i, j) = 1]$$

只考虑质数 p , 设 $n = a * p^x$, $m = b * p^y$, 那么等式左端 p 的贡献显然为 $x + y + 1$
等式右边 p 的贡献为数对 (i, j) : $(p, 1), (p^2, 1), \dots, (p^x, 1), (1, p), (1, p^2), \dots, (1, p^y), (1, 1)$,
共 $x + y + 1$ 对, 因此命题得证



Bzoj 4176 解答

$$\sum_{i=1}^n \sum_{j=1}^n d(ij) = \sum_{i=1}^n \sum_{j=1}^n \sum_{x|i} \sum_{y|j} [\gcd(i, j) = 1]$$

$$= \sum_{i=1}^n \sum_{j=1}^n \sum_{x|i} \sum_{y|j} \sum_{d|\gcd(x,y)} \mu(d)$$

$$= \sum_{d=1}^n \sum_{a=1}^{\lfloor \frac{n}{d} \rfloor} \sum_{b=1}^{\lfloor \frac{m}{d} \rfloor} \sum_{p=1}^{\lfloor \frac{n}{ad} \rfloor} \sum_{q=1}^{\lfloor \frac{m}{bd} \rfloor} \mu(d)$$

$$= \sum_{d=1}^n \mu(d) \left(\sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} \left\lfloor \frac{n}{id} \right\rfloor \right)^2$$



Bzoj 4176解答

$$\sum_{i=1}^n \sum_{j=1}^n d(ij) = \sum_{d=1}^n \mu(d) \left(\sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} \left\lfloor \frac{n}{id} \right\rfloor \right)^2$$

分块一下不就好了

……唔，n太大了，没法维护前缀和怎么办啊

那就杜教筛(额外内容)吧



Bz oj 3994

求 $\sum_{i=1}^n \sum_{j=1}^m d(ij)$ ，多组询问
($d(x)$ 为 x 的约数个数)

$n, m \leq 50000$ $T \leq 10000$



Bzoj 3994解答

由上一道题的结论

$$\sum_{i=1}^n \sum_{j=1}^m d(ij) = \sum_{d=1}^n \mu(d) \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} \lfloor \frac{n}{id} \rfloor \sum_{j=1}^{\lfloor \frac{m}{d} \rfloor} \lfloor \frac{m}{jd} \rfloor$$

范围这么小……

预处理一下前缀和不就完了



Bzoj 4174

$$\text{求} \sum_{i=1}^n \sum_{j=1}^m \sum_{k=0}^{k < j} \left\lfloor \frac{ik+x}{j} \right\rfloor$$

$n, m \leq 500000$ $0 < x \leq 100000$ x 是实数并精确到小数点后八位



Bzoj 4174 解答

明显 x 可以直接当作整数，小数点后的东西没用，后文的 x 是整数

假设我们已经确定了 i 和 j ，要求 $\sum_{k=0}^{j-1} \left\lfloor \frac{ik+x}{j} \right\rfloor$

$$\sum_{k=0}^{j-1} \left\lfloor \frac{ik+x}{j} \right\rfloor = \sum_{k=0}^{j-1} \left\lfloor \frac{ik \% j + x}{j} \right\rfloor + \sum_{k=0}^{j-1} \frac{ik - ik \% j}{j}$$

令 $d = \gcd(i, j)$ ， $\sum_{k=0}^{j-1} \left\lfloor \frac{ik \% j + x}{j} \right\rfloor$ 有一个长度为 $\frac{j}{d}$ 的循环节

$$= d \sum_{k=0}^{\left\lfloor \frac{j}{d} \right\rfloor - 1} \left\lfloor \frac{dk \% j + x}{j} \right\rfloor$$

现在把里面的 x 也拆出来

$$= d \left(\sum_{k=0}^{\left\lfloor \frac{j}{d} \right\rfloor - 1} \frac{kd \% j + x \% j}{j} + \frac{x - x \% j}{j} \right)$$



Bzoj 4174解答

观察一下

$$d \left(\sum_{k=0}^{\lfloor \frac{j}{d} \rfloor - 1} \frac{kd \% j + x \% j}{j} + \frac{x - x \% j}{j} \right)$$

不难发现前面那一项的值只能为0或1

$$= d \left(\sum_{k=0}^{\lfloor \frac{j}{d} \rfloor - 1} [kd \% j + x \% j \geq j] + \frac{x - x \% j}{j} \right)$$

仔细看一看

$$\sum_{k=0}^{\lfloor \frac{j}{d} \rfloor - 1} [kd \% j + x \% j \geq j] = \left\lfloor \frac{x \% m}{d} \right\rfloor$$



Bzoj 4174 解答

$$d \left(\sum_{k=0}^{\lfloor \frac{j}{d} \rfloor - 1} [kd \% j + x \% j \geq j] + \frac{x - x \% j}{j} \right) = d \left(\left\lfloor \frac{x \% m}{d} \right\rfloor + \frac{x - x \% j}{j} \right) = d \left\lfloor \frac{x}{d} \right\rfloor$$

最初的式子

$$\sum_{k=0}^{j-1} \left\lfloor \frac{ik + x}{j} \right\rfloor = d \left\lfloor \frac{x}{d} \right\rfloor + \sum_{k=0}^{j-1} \frac{ik - ik \% j}{j}$$

再来看 $\sum_{k=0}^{j-1} \frac{ik - ik \% j}{j}$, 和前面同理

$$\sum_{k=0}^{j-1} \frac{ik - ik \% j}{j} = \sum_{k=0}^{j-1} \frac{ik}{j} - \sum_{k=0}^{j-1} \frac{ik \% j}{j} = \frac{i(j-1)}{2} - \frac{d}{j} \sum_{k=0}^{\frac{j}{d}-1} kd = \frac{i(j-1) - (j-d)}{2}$$

所以最后的式子是

$$d \left\lfloor \frac{x}{d} \right\rfloor + \frac{i(j-1) - (j-d)}{2}$$



Bzoj 4174 解答

我们要计算

$$\sum_{i=1}^n \sum_{j=1}^m d \left\lfloor \frac{x}{d} \right\rfloor + \frac{i(j-1) - (j-d)}{2}$$

于是容斥(反演)一下, 设 $a = \left\lfloor \frac{n}{kd} \right\rfloor$, $b = \left\lfloor \frac{m}{kd} \right\rfloor$, $c = kd$

$$= \sum_{d=1}^{\min(n,m)} \sum_{k=1}^{\min(\frac{n}{d}, \frac{m}{d})} \mu(k) \left(abd \left\lfloor \frac{x}{d} \right\rfloor + \frac{ab(a+1)(b+1)c^2}{4} - \frac{a(a+1)bc}{2} - \frac{b(b+1)ac}{2} \right)$$

(甚至不需要分块)



Uoj 62

给你整数 n, c, d , 现在有整数 x_1, \dots, x_n 和 b_1, \dots, b_n 满足
 $0 \leq x_1, \dots, x_n, b_1, \dots, b_n < p$, 且对于 $1 \leq i \leq n$ 满足

$$\sum_{j=1}^n \gcd(i, j)^c \operatorname{lcm}(i, j)^d x_j \equiv b_i \pmod{p}$$

T 组数据每次给定 b_1, \dots, b_n , 求 x_1, \dots, x_n

sub1: $n \leq 100$ $T \leq 1000$

sub2: $n \leq 1000$ $T \leq 10$

sub3: $n \leq 100000$ $T \leq 3$



Uoj 62解答

整道题在模意义下做，将

$$\sum_{j=1}^n \gcd(i, j)^{c-d} i^d j^d x_j = b_i$$

转换为

$$\sum_{j=1}^n f(\gcd(i, j)) g(i) h(j) x_j = b_i$$

设 $f(x) = \sum_{d|x} fr(d)$ ，那么 $fr(x) = \sum_{d|x} \mu(x/d) f(d)$

$$\sum_d \sum_{j=1}^n [d|i][d|j] fr(d) g(i) h(j) x_j = b_i$$

移项

$$\sum_{d|i} fr(d) \sum_{j=1}^n [d|j] h(j) x_j = b_i / g(i)$$



Uoj 62解答

$$\sum_{d|i} fr(d) \sum_{j=1}^n [d|j] h(j) x_j = b_i / g(i)$$

注意到 $\sum_{j=1}^n [d|j] h(j) x_j$ 只与 d 有关系

设 $z_d = \sum_{j=1}^n [d|j] h(j) x_j$

$$\sum_{d|i} fr(d) z_d = b_i / g(i)$$

看上去又可以反演呢

设 $fz(d) = fr(d) z_d$

$$fz(i) = \sum_{d|i} \mu(d) * b_{\frac{i}{d}} / g(\frac{i}{d})$$

而

$$z_d = \frac{fz(d)}{fr(d)} = \sum_{j=1}^n [d|j] h(j) x_j$$



Uoj 62解答

$$\sum_{j=1}^n [d|j] h(j) x_j = z_d$$

使用另一个反演公式

$$h(d) x_d = \sum_{j=1}^n [d|j] \mu\left(\frac{j}{d}\right) z_j$$

好我们得到了 $h(d)x_d$ ，那么这道题就算做完了

由于反演带来了许多除法，所以可能有多解或无解，特判一下就好了



我倒想离开这无聊的课堂

我倒想学习额外内容

是时候做出选择了

有额外内容欸





狄利克雷卷积

两个函数 $f(x), g(x)$ ，他们的狄利克雷卷积是 $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$

两个积性函数的狄利克雷卷积仍为积性函数

其运算满足交换律和结合律

逆元

$$f^{-1}(n) = \frac{1}{f(1)} \quad (n = 1)$$
$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n \text{ \& } d \neq n} f(\frac{n}{d}) f^{-1}(d) \quad (otherwise)$$

≡ 杜教筛

有些题要求算一个积性函数的前缀和，但是数据达到了1000000000，常规的线性筛就不管用了，这时候我们就可以使用杜教筛

先构造一个积性函数 $g(x)$ ，并与 $f(x)$ 做卷积

$$(g * f)(i) = \sum_{d|i} g(d)f\left(\frac{i}{d}\right)$$

如果 $g(x)$ 和 $(g * f)(x)$ 的前缀和都可以在较好的时间复杂度内求出来，那么我们可以套用杜教筛的公式

$$g(1)s(n) = \sum_{i=1}^n (f * g)(i) - \sum_{i=2}^n g(i)s\left(\left\lfloor \frac{n}{i} \right\rfloor\right)$$

然后记忆化递归计算即可

所以使用杜教筛的关键是构造 $g(x)$



Bz oj 3944&4805

求 $\sum_{i=1}^n \mu(i)$ 和 $\sum_{i=1}^n \varphi(i)$

3944: $n \leq 2147483647$ $T \leq 10$

4805: $n \leq 2000000000$ $T=1$ 只求 $\sum_{i=1}^n \varphi(i)$

$$g(1)s(n) = \sum_{i=1}^n (f * g)(i) - \sum_{i=2}^n g(i)s\left(\left\lfloor \frac{n}{i} \right\rfloor\right)$$



Bz oj 3944&4805 解答

对于 μ , 取 $g(x) = 1$, $(g * f)(x) = [x = 1]$, $(g * f)$ 前缀和为1

对于 φ , 取 $g(x) = 1$, $(g * f)$ 前缀和为 $\frac{n(n+1)}{2}$

套用杜教筛公式即可



Bzoj 4916

求 $\sum_{i=1}^n \mu(i^2)$ 和 $\sum_{i=1}^n \varphi(i^2)$

$n \leq 10000000000$

$$g(1)s(n) = \sum_{i=1}^n (f * g)(i) - \sum_{i=2}^n g(i)s\left(\left\lfloor \frac{n}{i} \right\rfloor\right)$$



Bz oj 4916

第一问明显答案为1(斜眼笑)

大家都知道 $\varphi(i^2) = i * \varphi(i)$

取 $g(x) = x$, $(g * f)(x) = x^2$, $(g * f)$ 的前缀和为 $\frac{n(n+1)(2n+1)}{6}$

套用杜教筛公式即可



洲阁筛

咕咕咕

END

