数学

成都七中易健驰

Nekopara!

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：$\varphi[n] = n * \prod(1 - \frac{1}{\mathrm{p}})$，$p$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$a^{\varphi(n)} \equiv 1 \ (mod\ n)$

~~没有证明~~

莫比乌斯函数

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

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$\mu\left[i * p[j]\right] = 0$，显然$p[j]$就是它的平方因子，否则$\mu\left[i * p[j]\right] = -\mu[i]$

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：$n = p_1^{d1} p_2^{d2} \cdots p_k^{dk}$，其中$p_i$为素数
- 则n的正约数的个数就是：$fac[n] = (1 + d_1) * (1 + d_2) * \cdots * (1 + dk)$
  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$i\%p[j]! = 0$，$\gcd(i, p[j]) = 1$，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

$$n = p_1^{a1} * p_2^{a2} * p_3^{a3} * \cdots * p_r^{ar}$$

那么它的约数和是

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

维护$low(n)$表示n的最小质因子的指数次幂，即p_1^{a1}，$sum(n)$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~~

http://blog.miskcoo.com/2014/09/linear-find-all-invert

Bzoj 1409

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

$0<p,n<2^{31}$　$0<q<p$　$0<m<=5000$

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<=10000000 mod=1000000010 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 $\mathrm{n}! * \frac{p-1}{p}$ (p是$m!$的质因数)

预处理10000000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<=1000000

Bzoj 2721解答

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

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

设$t=y-z$，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<=1000000 mod=1000000007

Bzoj 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，求买下所有猫至少要多少硬币

1<=n<=50 1<=B_i<=100000

Bzoj 3233解答

设$\mathrm{d}p[i]$表示当前最大面值为i零头所需的硬币数量的最小值

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

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

直接做复杂度爆炸，而且也没用到线性筛

Bzoj 3233解答

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

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$0 < i <= n$，求最小的$j(0 < j <= n)$且$i! = j$满足$d(i,j)$最小

2<=n<=100000 A_i<=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$i! = j$，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。

https://baike.baidu.com/item/%E7%A7%AF%E6%80%A7%E5%87%BD%E6%95%B0/8354949?fr=aladdin

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

http://www.cnblogs.com/372465774y/archive/2012/10/16/2726282.html

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

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

那我们需要知道$\varphi\left(p_i^{ki}\right)$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$\varphi\left(p_i^{ki}\right) = p_i^{ki} - p_i^{ki-1} = p_i^{ki}(1 - \frac{1}{p_i})$

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

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$\left(1-\frac{1}{p}\right)*\cdots$，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$n=p_1^{k1}*p_2^{k2}*\cdots*p_r^{kr}$

假如我们现在手贱在n后面乘一个p_r

则$n*p_r=p_1^{k1}*p_2^{k2}*\cdots*p_r^{kr+1}$

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

设$F(n)=\sum_{d|n}\varphi(d)$

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

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

我们知道$\varphi(p_r^t)=p_r^t-p_r^{t-1}$

化简得$F(n)=f(\mathrm{n})*p_r^{kr}$

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

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

得到$F(n*p_r)=f(\mathrm{n})*p_r^{kr+1}$

欧拉函数性质7的证明

已知$F(n*p_r)=f(\mathrm{n})*p_r^{kr+1}$

又有$F(n)=f(\mathrm{n})*p_r^{kr}$

所以$F(n*p_r)=F(\mathrm{n})*p_r$

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<=1000000000000000

Bzoj 4802简化版解答

根号枚举质因数+线性筛

Bzoj 4802

求$\varphi(n)$

n<=1000000000000000000

Bzoj 4802解答

用Miller-rabin和Pollard-rho来解

Bzoj 2818

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

n<=10000000

Bzoj 2818解答

枚举每个质数，那么问题变为$1 \le i,j \le \frac{n}{p}$，$\gcd(i,j) = 1$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$n\%k+m\%k \ge k$的k的集合

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

n,m<=1000000000000000 mod=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$\lfloor\frac{n+m}{\mathrm{k}}\rfloor-\lfloor\frac{n}{k}\rfloor-\lfloor\frac{m}{k}\rfloor=0$

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$=\frac{(\mathrm{n+m})(\mathrm{n+m-1})}{2}-\frac{\mathrm{n(n-1)}}{2}-\frac{\mathrm{m(m-1)}}{2}=n*m$

最终答案为$\varphi(n)+\varphi(m)+n*m$

~~打表也可以发现这个规律~~

Bzoj 3643&4803

已知n，求满足$\varphi(i) = n$的前k项

3643: n<2147483648 k=1
4803: n<=1000000000000000 k<=1000

Bzoj 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：$a \equiv b \ (mod \ m)$

https://baike.baidu.com/item/%E5%90%8C%E4%BD%99%E5%AE%9A%E7%90%86/1212360?fr=aladdin

同余

性质

1.反身性：$a \equiv a \ (mod\ m)$

2.对称性：若$a \equiv b(mod\ m)$，则$b \equiv a \ (mod\ m)$

3.传递性：若$a \equiv b(mod\ m)$，$b \equiv c(mod\ m)$，则$a \equiv c(mod\ m)$

4.相加减：若$a \equiv b(mod\ m)$，$c \equiv d(mod\ m)$，则$a \pm c \equiv b \pm d(mod\ m)$

5.相乘：若$a \equiv b(mod\ m)$，$c \equiv d(mod\ m)$，则$a * c \equiv b * d(mod\ m)$

6.相除：若$a * c \equiv b * c(mod\ m)$，则$a \equiv b(mod \frac{m}{\gcd(c,m)})$

7.幂：若$a \equiv b(mod\ m)$，则$a^c \equiv b^c(mod\ m)$

8.组合性：若$a \equiv b(mod\ m_i)\ i \in [1,n]$，则$a \equiv b(mod\ lcm(m_1, m_2, \ldots, m_n))$

https://baike.baidu.com/item/%E5%90%8C%E4%BD%99%E5%AE%9A%E7%90%86/1212360?fr=aladdin

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

~~没有证明~~

扩展欧拉定理

若a,n不互质，

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

~~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$g^1,g^2,g^3,\ldots,g^{m-1}$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$p_1^{a1}*p_2^{a2}*\cdots*p_n^{an}$，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

原根

将 $\varphi(m)$ 进行质因数分解为 $p_1^{a1} * p_2^{a2} * \cdots * p_n^{an}$，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$a^{n-1} \equiv 1\ (mod\ n)$

~~不就是低配版的欧拉定理吗~~

中国剩余定理

如果我们有同余方程组

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$\cdots$$
$$x \equiv a_n (mod\ m_n)$$

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$x^2 \equiv d(mod\ p)$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$x^2 \equiv a(mod\ p)$且$p \nmid a$

二次剩余勒让德符号/欧拉判别准则

定义

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

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$\frac{p-1}{2\mathrm{p}}$

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， $C(k,p) \equiv 0 (mod\, p)$

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

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

二次剩余解决

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~~

http://blog.miskcoo.com/2014/08/quadratic-residue

大步小步算法

用于解$a^x \equiv n(mod\ p)$

设$m = \lceil \sqrt{p} \rceil$，$x = i * m + j$

$$a^j \equiv n * a^{-m*i}(mod\ p)$$

枚举$0 \le j < p$，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$g^r \equiv a(mod\, p)$ 成立，则称r是以g为底的a对模m的一个指标

记作$r = ind(a)$

Bzoj 3884

求$2^{2^{2^{\cdots^{\infty}}}} \% p$

p<=10000000 T<=1000

Bzoj 3884解答

假如我们有一个函数$f(p)=2^{2^{2^{\cdots^{\infty}}}}\%p$

根据扩展欧拉定理

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

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

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$l \le i \le r$，$a_i = c^{a_i}$ (c, p在开局给定)

2 l r 区间求和

在模p意义下操作

1<=n,m<=50000 0<=c,a_i<p<=1000000000

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

Bzoj 2480&3239

求最小的x使$a^x \equiv n(mod\ p)$

2480: a,n,p<=1000000000 T<=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<=2000000000

Bzoj 1406解答

变化一下$x^2-1=kp$

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

设$x+1=k_1p_1$，$x-1=k_2p_2$，$k_1k_2=k$，$p_1p_2=p$

枚举p的所有约数即可

Bzoj 2219

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

Bzoj 2219解答

设$p = 2k + 1 = p_1^{a1} p_2^{a2} \dots p_n^{an}$
最终答案是$x^a \equiv b(mod\ p_i^{ai})$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$x^a \equiv 0(mod\ p^c)$，这个答案随便算

2. $\gcd(b, p^c\ ) = 1$
$x^a \equiv b(mod\ p^c)$ -> $a * ind(x) \equiv ind(b)(mod\ \varphi(p^c))$
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$ax \equiv b(mod\ p)$

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

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

如果$cnt\%a \neq 0$则无解，否则转化一下方程

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

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

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

性质

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

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$n = p_1^{k1} * p_2^{k2} * \cdots * p_m^{km}$， $d = p_1^{x1} * p_2^{x2} * \cdots * p_m^{xm}$

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

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

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

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

什么?你要看证明?

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

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

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

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

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

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

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

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

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

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

Bzoj 2440

求出第k大的无平方因子的数(不考虑1)

$k<1000000000$ $T<50$

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

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

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

暴力枚举子集?

Bzoj 2440解答

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

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

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

Bzoj 1101&2045

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

1101: 0<d<=a,b<=50000 T<=50000
2045: 0<d<=a,b<=1000000 T=1

Bzoj 1101&2045解答

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

众所周知，$\sum_{\mathrm{d}|n} \mu(d) = [n=1]$

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

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

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

Bzoj 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<=n,m<=100000 |a|<=1000000000
1<=T<=20000 mod=2147483648

Bzoj 3529解答

先不考虑a的限制，那么我们就是要计算

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

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)

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

由上一道题的结论

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

Bzoj 3529解答

设$q = dt$

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

$g(x) = \sum_{d|q} f(d)\mu\left(\frac{q}{d}\right)$~~(一个狄利克雷卷积)~~可以预处理前缀和

$\sum_{q=1}^{\min(n,m)} \left\lfloor\frac{n}{q}\right\rfloor\left\lfloor\frac{m}{q}\right\rfloor$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<=10000000 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

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

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<=10000000 T<=10000 mod=100000009

Bzoj 2693解答

从上一道题的结论继续

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

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

设

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

则

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

Bzoj 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

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

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

Bzoj 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<=4000000 T<=10000 mod=1073741824

4659: n,m<=4000000 T<=2000 mod=1073741824

Bzoj 2694&4659解答

设$n \le m$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} lcm(i,j) * |\mu(gcd(i,j))|$$

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

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

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

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

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

设$t = dp$

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

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

Bzoj 2694&4659解答

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

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

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

Bzoj 4176

求$\sum_{i=1}^{n}\sum_{j=1}^{n}d(ij)$

$(d(x)$为x的约数个数)

n<=1000000000 mod=1000000007

Bzoj 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): $(p,1),(p^2,1),\ldots,(p^x,1)$, $(1,p),(1,p^2),\ldots,(1,p^y)$, $(1,1)$,
共$x+y+1$对，因此命题得证

Bzoj 4176解答

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

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

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

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

Bzoj 4176解答

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

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

Bzoj 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<=50000 T<=10000

Bzoj 3994解答

由上一道题的结论

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

范围这么小……

预处理一下前缀和不就完了

Bzoj 4174

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

n,m<=500000 0<x<=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

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

不难发现前面那一项的值只能为0或1

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

仔细看一看

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

Bzoj 4174解答

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

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$a=\left\lfloor\frac{n}{kd}\right\rfloor$，$b\left\lfloor\frac{m}{kd}\right\rfloor$，$c=kd$

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

~~(甚至不需要分块)~~

Uoj 62

给你整数n, c, d，现在有整数$x_1, \ldots, x_n$和$b_1, \ldots, bn$满足$0 \le x_1, \ldots, xn, b_1, \ldots, bn < p$，且对于$1 \le i \le n$满足

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

T组数据每次给定$b_1, \ldots, bn$，求$x_1, \ldots, xn$

sub1: n<=100 T<=1000
sub2: n<=1000 T<=10
sub3: n<=100000 T<=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$fr(x) = \sum_{d|x} \mu(x)\, f(\frac{x}{d})$

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

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

由于反演带来了很多除法，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


有额外内容款

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

$$f^{-1}(n) = \frac{1}{f(1)} \ (\mathrm{n} = 1)$$

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

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

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

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$g(x)$

Bzoj 3944&4805

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

3944: n<=2147483647 T<=10
4805: n<=2000000000 T=1 只求$\sum_{i=1}^{n}\varphi(i)$

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

Bzoj 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<=1000000000

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

Bzoj 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
Vanilla ©2018