数论基础

nixnehc
省选B班

Miller-Rabin

二向探测定理：$x^2 \equiv 1(\mod p) \Longleftrightarrow x \equiv -1(\mod p) || x \equiv 1(\mod p)$

C++

```cpp
int primes[12]={2,3,5,7,11,13,17,19,23,29,31,37};

bool mr(int x,int p)
{
    if(x==p) return true;
    int k=x-1;
    while(k)
    {
        int t=qpow(p,k,x);
        if(t!=1 && t!=x-1) return false;
        if((k&1)==1 || t==x-1) return true;
        k=k>>1;
    }
    return true;
}

bool is_primes(int x)
{
    for(int i=0;i<12;i++)
        if(!mr(x,primes[i])) return false;
    return true;
}
```

积性函数

积性函数

满足 $f(ab)=f(a)*f(b)(gcd(a,b)=1)$

知道质数幂时的 f 即可知所有 f

$f(p_1^{c1}*p_2^{c2}*......)=f(p_1^{c1})*f(p_2^{c2})*.....$

常见的积性函数:

σ_n: n的因子数

μ_n : 莫比乌斯函数

φ_n : 欧拉函数

d_n : n的约数个数

$e_n:[n=1]$

$I_n=1$

$id_n=n$

迪利克雷卷积

$f = h * g$

$\rightarrow f(x) = \sum_{d|x} h(d) * g(x/d)$

f,g 积性， $f * g$ 积性

$f * e = f$

$id = \varphi * I$

$\mu * I = e$

$O(nloglogn)$ 求 $g = f * I$ 或 $g = f * \mu$

莫比乌斯反演

莫比乌斯反演

本质： $\mu * I = e$

$$\sum_{d|n} \mu_d = \sum_i C_{\omega_n}^i (-1)^i = (1-1)^{\omega_n} = [n == 1]$$

$f = g * I$

$f(n) = \sum_{d|n} g(d)$

$\rightarrow$

$g = f * \mu$

$g(n) = \sum_{d|n} g(d) * \mu(n/d)$

f，g 不要求为积性函数

求 $\sum_{i=1}^{n}\sum_{j=1}^{n} f(gcd(i,j))$ $n=10^7$

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

AGC 038C 给 n 个数 a_i，求 $\sum_{i=1}^{i=n}\sum_{j=1}^{j=n} lcm(a_i, a_j)$ $n = 10^6$

题意：给定 n，求 $\sum_{i=1}^{n} \gcd\left(\left\lfloor \sqrt[3]{i} \right\rfloor, i\right) \bmod 998244353$，其中 $n \le 1 \times 10^{21}$。

定义$F(n)=\sum_{i=1}^{n}\sum_{j=1}^{n}[gcd(i,j)+lcm(i,j)\geqslant n]$，其中[]是艾弗森约定，现在要求出$ans_n=\sum_{i=1}^{n}F(i)$.

求 ans_{1-n}。 $n=10^6$

基本和组

基本和组

$D(x) = \{\lfloor x/1 \rfloor, \lfloor x/2 \rfloor, \lfloor x/3 \rfloor, \lfloor x/4 \rfloor ..... \lfloor x/x \rfloor\}$ 大小为 $O(\sqrt{n})$

$\{\lfloor x/1^2 \rfloor, \lfloor x/2^2 \rfloor, \lfloor x/3^2 \rfloor, \lfloor x/4^2 \rfloor ..... \lfloor x/\sqrt{x}^2 \rfloor\}$ 大小?

$D(\lfloor x/a \rfloor) \in D(x)$

$\lfloor x/ab \rfloor = \lfloor \lfloor x/a \rfloor /b \ \rfloor$

$f = g * h$， 求已知 G, H ,求 $F(n)$ （F, G, H 分别为 f， g， h 前缀和)

$f = g * h$,已知 $G(D(n)), H(D(n))$,求 $F(D(n))$ 。

杜教筛

$h = f * g$

F，H 好求，求 G

tips：求 $\sum f(i) * i^2$

神秘trick?

求 $\sum_{i=1}^{n} \mu^2$

求 $\sum_{n=1}^{N} \sum_{d_1*d_2=n\&gcd(d_1,d_2)=1} 1$

求 $\sum_{i=1}^{n} \sum_{j=1}^{n} d(ij)$

求 $\sum_{i=1}^{n} \sum_{j=1}^{n} \sigma_1(ij)$

神秘trick?

$\mu_n^2=\sum_{i^2|n}\mu_i$

求 1-n 里无平方因子数的个数

$2^{\omega_n}=\sum_{d_1*d_2=n\&gcd(d_1,d_2)=1}1$

求 $\sum 2^{\omega_n}$

$d(ij)=\sum_{d_1|i\&d_2|j\&gcd(d_1,d_2)=1}1$

$\sigma_1(ij)=\sum_{d_1|i}\sum_{d_2|j}[gcd(d_1,d_2)=1]\frac{i}{d_1}d_2$

powerful number筛

powerful number：每个素因子次数≥2

→powerful number 可以写成 x^2y^3 形式

→powerful number 个数为 $O(\sqrt{n})$

可以构造出 $g(i)$ 使和 $f(i)$ 在质数时的取值相同，则可以求 $F(n)$，复杂度 $O(\sqrt{n})$

$$f = g * \sigma$$

发现 σ 只在 powerful number 处有值

$$F(n) = \sum_{i<n} f_i = \sum_{ij<=n} g_i * \sigma_j = \sum \sigma_i * G(\lfloor \frac{n}{i} \rfloor)$$

$$f(p^q) = p$$

$$f(p^q) = p^{q-[q \mod p]}$$

min_25筛

$f(i)$ 在质数幂处的定义为低次多项式，则可以求 $\sum_{i=1}^{n} f(i)$,大约 2s 跑 $n=10^{10}$

$F(n)=\sum_{i=1}^{n} f(i)$

$G(n)=\sum_{i=1}^{n} f(i)[i=prime]$

$F(i,n)=\sum_{i=1}^{n} f(i)[i\text{的最小质因子} \geq p_i]$

step1:求 $G(D(n))$

构造一 h_n , h_n 与 f_n 在质数处取值相同，且 h 为完全积性函数。

类似线筛地去除所有和数，求出 $G(D(n))$

step2:

$F(i,n)=G(n)-\sum_{k=1}^{i-1} f(p_i)+$
$\sum_{k\geq i \& p_k^2<=n} \sum_{p_k^{e+1}<=j} f(p_k^{e+1})+f(p_k^e)*F(k+1,\lfloor \frac{j}{p_k^e} \rfloor)$

相当于用之前处理出来的 G 把枚举每个数时的最大质因子减枝掉。

LOJ 6053

某一天，你发现了一个神奇的函数$f(x)$，它满足很多神奇的性质：

1. $f(1)=1$。
2. $f(p^c)=p\oplus c$（p 为质数，$\oplus$表示异或）。
3. $f(ab)=f(a)\cdot f(b)$（a 与 b 互质）。

你看到这个函数之后十分高兴，于是就想要求出 $\sum\limits_{i=1}^{n} f(i)$。

由于这个数比较大，你只需要输出 $\sum\limits_{i=1}^{n} f(i) \bmod (10^9+7)$。

$n=10^{10}$

luogu P5325

定义积性函数 $f(x)$，且 $f(p^k)=p^k(p^k-1)$（p 是一个质数），求

$$\sum_{i=1}^{n} f(i)$$

对 10^9+7 取模。

$$n=10^{10}$$

小结

- 杜教筛 $O(n^{\frac{2}{3}})$ 构造 $f*g=h$，g，h 前缀和好算
- min_25 $O(n^{1-\omega})$ f 在质数处取值为低次多项式
- PN 筛 $O(\sqrt{n})$ 构造出 $g(p)=f(p)$