数论函数初步

Quack

2022 年 7 月 17 日

目录

数论函数

定义 (数论函数)

在全体正整数（或者整数）上定义的函数称作数论函数。

定义 (积性)

积性：若 $\gcd(a, b) = 1$，则 $f(ab) = f(a)f(b)$。

数论函数

例 (积性数论函数)

$1(x) = 1, Id(x) = x, I(x) = [x = 1]$;

欧拉函数 $\varphi(x)$。

数论函数

定义 (狄利克雷卷积)

数论函数 $f(n)$ 和 $g(n)$ 的狄利克雷卷积 $h(n)$ 定义为：

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

记作 $h = f * g$。

定理

两个积性函数的狄利克雷卷积也是积性函数。

数论函数

证明.

$$h(xy)=\sum_{d|xy}f(d)g(\frac{xy}{d})=\sum_{d_1|x}\sum_{d_2|y}f(d_1d_2)g(\frac{xy}{d_1d_2})$$

$$=\sum_{d_1|x}f(d_1)g(\frac{x}{d_1})\sum_{d_2|y}f(d_2)g(\frac{y}{d_2})=h(x)h(y)$$

□

数论函数

定理

两个积性函数的对应位置相乘也是积性函数。

很显然，证明略。

数论函数

所以我们可以定义更多的数论函数，以及用卷积描述它们之间的关系：

例 (数论函数)

$d(x)=\sum_{d|n}1$，即 $d=1*1$；
$n=\sum_{d|n}\varphi(d)$，即 $Id=\varphi*1$。

数论函数

下面研究卷积的性质。

定理 (卷积运算律)

交换律：设有两个积性函数 f, g，则 $f * g = g * f$。
结合律：设有两个积性函数 f, g, h，则 $(f * g) * h = f * (g * h)$。

交换律的证明很显然。
结合律的证明可以把式子改写成矩阵形式，然后用矩阵的结合律来证明。应该大力推式子也可以。

数论函数

定理 (单位元)

I 是单位元：对任意的数论函数 f，$f * I = I * f = f$。

证明.

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

□

数论函数

定义 (狄利克雷逆)

若 $f * g = I$，则数论函数 f, g 互为彼此的狄利克雷逆。

莫比乌斯反演

定义 (莫比乌斯函数)

定义莫比乌斯函数 $\mu(n)$。
当 $n = 1$ 时，$\mu(n) = 1$。
当 n 是 square-free number 时，设 n 的质因数分解有 k 项，则 $\mu(n) = (-1)^k$。
否则，$\mu(n) = 0$。

不难验证 μ 也是积性函数。

莫比乌斯反演

定理

$I=\mu*1$，即 μ 和 1 互为彼此的逆。

证明.

设 n 的不同质因子有 k 个，分别为 $p_1,\cdots,p_k$，那么有

$$\sum_{d|n}\mu(d)=\sum_{i=1}^{k}\sum_{\text{k 个选 i 个, 积为 c}}\mu(c)$$
$$=\sum_{i=1}^{k}\sum_{\text{k 个选 i 个}}(-1)^i=\sum_{i=1}^{k}\binom{k}{i}(-1)^i=(1-1)^k$$
$$=[k=0]=I(n)$$

□

莫比乌斯反演

定义 (莫比乌斯变换)

设数论函数 f，称 $F = f * 1$ 为莫比乌斯变换。

定义 (莫比乌斯反演)

设数论函数 F，称 $f = F * \mu$ 为莫比乌斯反演。

例

$d = 1 * 1$，即 $d * \mu = 1$；

$Id = \varphi * 1$，即 $Id * \mu = \varphi$。

厄拉多塞筛法

例 (厄拉多塞筛法)

$O(n\log\log n)$ 判断 $2\sim n$ 的所有数是否是质数。

有一张写了 $2\sim n$ 这些数的表，2 是质数，我们把表中其他所有 2 的倍数划去。然后 3 没有被划去，说明 3 是质数，把表中其他所有 3 的倍数划去。以此类推。
时间复杂度 $O(n+\frac{n}{2}+\frac{n}{3}+\frac{n}{5}+\frac{n}{7}+\cdots)=O(n\log\log n)$。

线性筛

例 (线性筛)

$O(n)$ 判断 $2 \sim n$ 的所有数是否是质数。

厄拉多塞筛法在筛 $30 = 2 \times 3 \times 5$ 这样的数时，会被 $2, 3, 5$ 重复筛。
线性筛的思路是，保证每个数只被它的最小的质因子筛去。

线性筛

例 (线性筛)

$O(n)$ 判断 $2 \sim n$ 的所有数是否是质数。

厄拉多塞筛法在筛 $30 = 2 \times 3 \times 5$ 这样的数时，会被 $2, 3, 5$ 重复筛。
线性筛的思路是，保证每个数只被它的最小的质因子筛去。

线性筛

我们先给出代码：

线性筛

```
for(int i = 2; i <= n; i++){
    if(isp[i] == 0) pr[++cnt] = i;
    for(int j = 1; j <= cnt && pr[j] * i <= n; j++){
        isp[i * pr[j]] = 1;
        if(i % pr[j] == 0) break;
    }
}
```

保证每个数只被它的最小的质因子筛去，代码中体现在 i % pr[j] == 0。
pr 数组中的质数是递增的，当 $pr[j]|i$ 时，$pr[j]|pj[j+1]i$，那么 $pj[j+1]i$ 这个合数应该被 $pr[j]$ 这个更小的质数筛掉。
另外，当 $pr[j]|i$ 时，$pr[j]$ 是 i 的最小质因子。否则 $pr[j]$ 是 $pr[j]i$ 的最小质因子。

线性筛

例 (线性筛)

$O(n)$ 求出某些积性函数在 $1 \sim n$ 处的所有取值。

我们沿用线性筛的过程，考虑这个问题。
首先，线性筛筛出质数的时候，我们需要求这个积性函数在质数处的取值。
其次，在 for 循环中，设 $k = pr[j]$，当 $k|i$ 时，由上面的讨论，k 是 i 的最小质因子，设 k 在 i 中的幂次为 a，那么 $f(ki) = \frac{f(k^{a+1})}{f(k^a)} f(i)$。
否则，因为 k 是质数，那么 $\gcd(k, i) = 1$，那么 $f(ki) = f(k)f(i)$。

线性筛

例 (线性筛欧拉函数)

$O(n)$ 求出欧拉函数在 $1 \sim n$ 处的所有取值。

由于 $\frac{\varphi(k^{a+1})}{\varphi(k^a)} = k$，为一个定值，所以线性筛欧拉函数很容易。

线性筛欧拉函数

```
for(int i = 2; i <= n; i++){
    if(isp[i] == 0) {pr[++cnt] = i; phi[i] = i - 1;}
    for(int j = 1; j <= cnt && pr[j] * i <= n; j++){
        isp[i * pr[j]] = 1;
        if(i % pr[j] == 0) {
            phi[i * pr[j]] = phi[i] * pr[j];
            break;
        }
        phi[i * pr[j]] = phi[i] * (pr[j] - 1);
    }
}
```

线性筛

例 (线性筛莫比乌斯函数)

$O(n)$ 求出莫比乌斯函数在 $1 \sim n$ 处的所有取值。

由于 $\frac{\mu(k^{a+1})}{\mu(k^a)} = 0$，为一个定值，所以也很容易。

线性筛莫比乌斯函数

```
for(int i = 2; i <= n; i++){
    if(isp[i] == 0) {pr[++cnt] = i; mu[i] = -1;}
    for(int j = 1; j <= cnt && pr[j] * i <= n; j++){
        isp[i * pr[j]] = 1;
        if(i % pr[j] == 0) {
            mu[i * pr[j]] = 0;
            break;
        }
        mu[i * pr[j]] = mu[i] * -1;
    }
}
```

线性筛

例 (线性筛约数个数)

$O(n)$ 求出约数个数函数 τ 在 $1 \sim n$ 处的所有取值。

由于 $\frac{\tau(k^{a+1})}{\tau(k^a)} = \frac{a+2}{a+1}$，不为一个定值，所以在筛的过程中还要维护 i 的最小质因子的次数。

线性筛

线性筛约数个数

```
for(int i = 2; i <= n; i++){
    if(isp[i] == 0) {pr[++cnt] = i; tau[i] = 2; g[i] = 2;}
    for(int j = 1; j <= cnt && pr[j] * i <= n; j++){
        isp[i * pr[j]] = 1;
        if(i % pr[j] == 0) {
            tau[i * pr[j]] = (g[i] + 1) * tau[i] / g[i];
            g[i * pr[j]] = g[i] + 1;
            break;
        }
        tau[i * pr[j]] = tau[i] * 2;
        g[i * pr[j]] = 2;
    }
}
```

整数分块

定理 (整数分块)

对任意的 i，$\lfloor \frac{n}{i} \rfloor$ 只有 $O(\sqrt{n})$ 种取值。

证明.

当 $1 \leq i \leq \sqrt{n}$ 时，$\frac{n}{i}$ 有 $O(\sqrt{n})$ 种取值。
当 $i > \sqrt{n}$ 时，$\frac{n}{i} \leq \sqrt{n}$，也只有 $O(\sqrt{n})$ 种取值。
综上，只有 $O(\sqrt{n})$ 种取值。 $\square$

整数分块

例 (计算下取整分式的和式)

计算 $\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor$。

由于 $\lfloor \frac{n}{i} \rfloor$ 只有 $O(\sqrt{n})$ 种取值，并且，使得 $\lfloor \frac{n}{i} \rfloor$ 取相同取值的 i 也是一段一段的，所以我们只需要一段一段地计算即可。

整数分块

```
ll res = 0;
for(int l = 1, r; l <= n; l = r + 1) {
   r = n / (n / l);
   res += (r - l + 1) * (n / l);
}
```

莫比乌斯反演

例（accoders3465）

给出 n, m，求 $2\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j) - nm$。
数据范围：$n, m \le 10^5$。

莫比乌斯反演

例 (accoders3465)

给出 n, m，求 $2\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j) - nm$。
数据范围：$n, m \le 10^5$。

我们之前学欧拉函数的时候，能求 $\sum_{i=1}^{n}\sum_{j=1}^{n}\gcd(i,j)$，但是当 $n \ne m$ 时，就不能再用欧拉函数求了。
还是之前的套路，
$\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j) = \sum_{k=1}^{\min(n,m)} k \sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j) = k]$。
设 $a = \lfloor\frac{n}{k}\rfloor, b = \lfloor\frac{m}{k}\rfloor$，继续推：
$\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j) = \sum_{k=1}^{\min(n,m)} k \sum_{i=1}^{a}\sum_{j=1}^{b}[\gcd(i,j) = 1]$。

莫比乌斯反演

$$\sum_{k=1}^{\min(n,m)} k\sum_{i=1}^{a}\sum_{j=1}^{b}[\gcd(i,j)=1]=\sum_{k=1}^{\min(n,m)} k\sum_{i=1}^{a}\sum_{j=1}^{b} I(\gcd(i,j))$$

$$=\sum_{k=1}^{\min(n,m)} k\sum_{i=1}^{a}\sum_{j=1}^{b}\sum_{d\mid\gcd(i,j)}\mu(d)=\sum_{k=1}^{\min(n,m)} k\sum_{d=1}^{\min(a,b)}\sum_{i=1}^{\lfloor\frac{a}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{b}{d}\rfloor}\mu(d)$$

$$=\sum_{k=1}^{\min(n,m)} k\sum_{d=1}^{\min(a,b)}\mu(d)\lfloor\frac{a}{d}\rfloor\lfloor\frac{b}{d}\rfloor$$

到这里用整数分块已经可以做到 $O(n\sqrt{n})$ 的复杂度，足以通过此题。

莫比乌斯反演

整数分块

```
for(int k=1;k<=min(n,m);k++){
    int a=n/k,b=m/k;
    ll sum=0;
    for(int l=1,r;l<=min(a,b);l=r+1){
        r=min(a/(a/l),b/(b/l));
        sum+=1ll*(smu[r]-smu[l-1])*(a/l)*(b/l);
    }
    ans+=sum*k;
}
```

莫比乌斯反演

由答案的对称性，不妨设 $n \le m$，然后我们继续推：

$$\sum_{k=1}^{n} k \sum_{d=1}^{a} \mu(d) \lfloor \frac{a}{d} \rfloor \lfloor \frac{b}{d} \rfloor = \sum_{k=1}^{n} k \sum_{d=1}^{\lfloor \frac{n}{k} \rfloor} \mu(d) \lfloor \frac{n}{kd} \rfloor \lfloor \frac{m}{kd} \rfloor$$

$$\overset{T=kd}{=\!=} \sum_{T=1}^{n} \lfloor \frac{n}{T} \rfloor \lfloor \frac{m}{T} \rfloor \sum_{k|T} k\mu(\frac{T}{k})$$

由于 $Id * \mu = \varphi$，所以 $\sum_{k|T} k\mu(\frac{T}{k}) = \varphi(T)$，那么最终答案就是 $\sum_{T=1}^{n} \lfloor \frac{n}{T} \rfloor \lfloor \frac{m}{T} \rfloor \varphi(T)$。这个式子在线性筛出 φ 及其前缀和的情况下可以用整数分块做到 $O(\sqrt{n})$ 一次回答（用于应对多组询问的情况）。这样我们就得到了一种 $O(n) - O(\sqrt{n})$ 的算法。

莫比乌斯反演

例 (accoders6724)

给出 n, m，求 $\sum_{i=1}^{n} \sum_{j=1}^{m} [\gcd(i, j) \in P]$。

数据范围：多组数据，$1 \le T \le 10^4$，$n, m \le 10^7$。

莫比乌斯反演

例 (accoders6724)

给出 n, m，求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j) \in P]$。
数据范围：多组数据，$1 \le T \le 10^4$，$n, m \le 10^7$。

类似的推法，最后得到：

$$\sum_{T=1}^{n}\lfloor\frac{n}{T}\rfloor\lfloor\frac{m}{T}\rfloor\sum_{k|T,k\in P}\mu(\frac{T}{k})$$

设 $g(T) = \sum_{k|T,k\in P}\mu(\frac{T}{k})$，看上去不是很好线性筛，不过可以厄拉多塞筛法在 $O(n\log\log n)$ 内算出其前缀和，然后用整数分块回答询问。

Thanks!