数论 2

前置公式

\begin{equation}\left(\sum_{d\mid n}f(x)\right)\left(\sum_{d\mid m}g(x)\right)=\sum_{d_1\mid n}\sum_{d_2\mid m}f(d_1)g(d_2)\tag{1}\end{equation}

\begin{equation}\sum_{m=1}^n\sum_{d\mid (n,m)}f(d)=\sum_{d\mid n}\frac{f(d)n}d\tag{2}\end{equation}

\begin{equation}\sum_{x\mid n}\left(f(x)\sum_{y\mid\frac nx}g(y)\right)=\sum_{y\mid n}\left(g(y)\sum_{x\mid\frac ny}f(x)\right)\tag{3}\end{equation}

可积函数

一般可积函数

定义

数论函数 θ 被定义为可积函数，若

$(a)\ \exists n\left(\theta(n)\ne 0\right)$

$(b)\ \forall n\forall m \left((n,m)=1\to \theta(n\ast m)= \theta(n)\ast\theta(m)\right)$

性质

假定 θ 为可积函数，则

$$ \begin{array}{l} (1)\ \theta(1)=1\\ (2)\ \theta(n)=\theta\left(p_1^{\alpha_1}\right)\theta\left(p_2^{\alpha_2}\right)\ldots\theta\left(p_k^{\alpha_k}\right)\\ (3)\theta_1,\theta_2\text{可积}\to \theta_1\theta_2\text{可积}\\ \end{array} $$

定理

若 θ 为可积函数，则

$$ \begin{array}{l} (1)\ \psi(n)=\sum_{d\mid n}\theta(d)\text{可积}\\ (2)\ \psi(n)=\prod_{i=1}^k\left(1+\theta\left(p_k\right)+\theta\left(p_k^2\right)+\ldots+\theta\left(p_k^{\alpha_k}\right) \right)\end{array} $$

证明

设 $(n,m)=1$ 则对 $d\mid nm$ 一定存在唯一 $d_1\mid n,d_2\mid m,d=d_1d2$

同时，对每对 $d_1\mid n,d_2\mid m$ 一定有 $d=d_1d_2$ $d\mid nm$

所以根据 (1) 式

\begin{equation}\psi(nm)=\sum_{d\mid nm} \theta(d)=\sum_{d_1\mid n}\sum_{d_2\mid m}\theta(d_1)\theta(d_2)=\left(\sum_{d\mid n}\theta(d)\right)\left(\sum_{d\mid m}\theta(d)\right)=\psi(n)\psi(m)\end{equation}

\begin{equation}\psi(n)=\prod_{i=1}^k\psi\left(p_k^{\alpha_k}\right)=\prod_{i=1}^k\left(1+\theta\left(p_k\right)+\theta\left(p_k^2\right)+\ldots+\theta\left(p_k^{\alpha_k}\right)\right)\tag{4}\end{equation}

莫比乌斯函数

定义

$$ \mu (n)= \begin{cases} 1 &n=1\\ (-1)^k &n=p_1p_2\ldots p_k\\ 0 &otherwise \end{cases} $$

性质

若 θ 为可积函数，根据 (4) 式

\begin{equation}\sum_{d\mid n}\mu (d)\theta (d)=\prod_{i=1}^k\left(1+\mu\left(p_k\right)\theta\left(p_k\right)+\mu\left(p_k^2\right)\theta\left(p_k^2\right)+\ldots+\mu\left(p_k^{\alpha_k}\right)\theta\left(p_k^{\alpha_k}\right)\right)=\prod_{i=1}^k\left(1-\theta\left(p_k\right)\right)\tag{5}\end{equation}

特别地

\begin{equation}\theta (n)\equiv 1,\sum_{d\mid n}\mu (d)=\begin{cases} 1 &n=1\\ 0 &otherwise\\ \end{cases}\tag{6}\end{equation}

\begin{equation}\theta (n)=\frac 1n,\sum_{d\mid n}\frac{\mu (d)}d=(1-p_1)(1-p_2)\ldots(1-p_k)\tag{7}\end{equation}

欧拉函数

定义

\begin{equation}\varphi(n)=\sum_{m=1}^n [(n,m)=1]\end{equation}

性质

根据 (2) 式、(6) 式和 (7) 式

\begin{equation}\varphi(n)=\sum_{m=1}^n [(n,m)=1]=\sum_{m=1}^n\sum_{d\mid (n,m)}\mu (d)=n\sum_{d\mid n}\frac {\mu (d)}d=n(1-p_1)(1-p_2)\ldots(1-p_k)\end{equation}

其他常见可积函数

\begin{equation}d(n)=\sum_{d\mid n}1=\prod_{i=1}^k(\alpha_k+1)\end{equation}

\begin{equation}\sigma (n)=\sum_{d\mid n}d=\prod_{i=1}^k\left(1+p_k+p_k^2+\ldots+p_k^{\alpha_k} \right)\end{equation}

完全积性函数

$f(x)$ 被定义为完全积性函数若 $\forall n\forall m(f(nm)= f(n)f(m))$

\begin{equation}e(n)=[n==1]\end{equation}

\begin{equation}I(n)=1\end{equation}

\begin{equation}id(n)=n\end{equation}

线性筛法

先给出线性筛素数的代码

```
const int MAXP=1e6;
bool vis[MAXP];
int prime[MAXP],cnt;
void Prime(){
    vis[1]=true;
    _for(i,2,MAXP){
        if(!vis[i]) prime[cnt++]=i;
        for(int j=0;j<cnt&&i*prime[j]<MAXP;j++){
            vis[i*prime[j]]=true;
            if(i%prime[j]==0) break;
        }
    }
}
```

基于线性筛素数和可积函数性质，如果能在 $O(1)$ 时间求出 $f(p^k)$就可以线性筛 f 函数，例如

```
const int MAXP=1e6;
bool vis[MAXP];
int prime[MAXP],mu[MAXP],cnt;
void Mu(){
```

```
    vis[1]=true,mu[1]=1;
    _for(i,2,MAXP){
        if(!vis[i])mu[i]=-1,prime[cnt++]=i;
        for(int j=0;j<cnt&&i*prime[j]<MAXP;j++){
            vis[i*prime[j]]=true;
            if(i%prime[j])
            mu[i*prime[j]]=-mu[i];
            else{
                mu[i*prime[j]]=0;
                break;
            }
        }
    }
}
```

```
const int MAXP=1e6;
bool vis[MAXP];
int prime[MAXP],phi[MAXP],cnt;
void Phi(){
    vis[1]=true,phi[1]=1;
    _for(i,2,MAXP){
        if(!vis[i])phi[i]=i-1,prime[cnt++]=i;
        for(int j=0;j<cnt&&prime[j]*i<MAXP;j++){
            vis[i*prime[j]]=true;
            if(i%prime[j])
            phi[i*prime[j]]=phi[i]*(prime[j]-1);
            else{
                phi[i*prime[j]]=phi[i]*prime[j];
                break;
            }
        }
    }
}
```

```
const int MAXP=2e6;
bool vis[MAXP];
int prime[MAXP],d[MAXP],mpow[MAXP],cnt;
void D(){
    vis[1]=true,d[1]=1;
    _for(i,2,MAXP){
        if(!vis[i])d[i]=2,mpow[i]=1,prime[cnt++]=i;
        for(int j=0;j<cnt&&prime[j]*i<MAXP;j++){
            vis[i*prime[j]]=true;
            if(i%prime[j])
            d[i*prime[j]]=d[i]<<1,mpow[i*prime[j]]=1;
            else{
d[i*prime[j]]=d[i]/(mpow[i]+1)*(mpow[i]+2),mpow[i*prime[j]]=mpow[i]+1;
                break;
```

```
                }
            }
        }
    }
```

简单地说，

\begin{equation}f(ip)=\begin{cases} f(i)f(p) &p\text{ 不是 }i\text{ 的最小素因子}\\ f(i)\frac{f(p^{k+1})}{f(p^k)} &p\text{是}i\text{ 的最小素因子}\\ \end{cases}\end{equation}

如有必要，额外存储每个数的最小素因子的幂次即可。

狄利克雷卷积

定义

两个数论函数 f、g 的迪利克雷卷积运算为 \begin{equation}(f\ast g)(n)=\sum_{d\mid n}f(d)\ast g(\frac nd)\end{equation}

性质

1、交换律：$f\ast g=g\ast f$

2、结合律：$f\ast (g\ast h)=(f\ast g)\ast h$

3、分配律：$(f+g)\ast h=f\ast h+g\ast h$

4、单位元：$e\ast f=f$

5、逆元：对每个 $f(1)\ne 0$ 的数论函数 f，一定存在某个数论函数 g 使得 $f\ast g=e$

6、两个可积函数的迪利克雷卷积仍为可积函数，可积函数的逆元也为可积函数。

性质 5 证明

事实上，构造\begin{equation}g(n)=\frac 1{f(1)}\left(e(n)-\sum_{d\mid n,d\ne 1}f(d)\ast g(\frac nd)\right)\end{equation}

知 $g(n)$ 可由 $g(1\sim n-1)$ 递推得到，且 \begin{equation}\sum_{d\mid n}f(d)\ast g(\frac nd)=f(1)\ast g(n)+\sum_{d\mid n,d\ne 1}f(d)\ast g(\frac nd)=e(n)\end{equation}

莫比乌斯反演定理

设 $F(x)$、$f(x)$ 为数论函数，若 \begin{equation}F(n)=\sum_{d\mid n}f(d)\end{equation}

则 \begin{equation}f(n)=\sum_{d\mid n}\mu (d)F(\frac nd)\tag{8}\end{equation}

该定理的另一种形式为若 \begin{equation}F(n)=\sum_{n\mid d}f(d)\end{equation}

则 \begin{equation}f(n)=\sum_{n\mid d}\mu (\frac dn)F(d)\tag{9}\end{equation}

事实上，该定理等价于若 $F=f\ast I$ 则 $f=F\ast\mu$ 简单地说，莫比乌斯反演定理即证明 $e=I\ast \mu$

证明

根据 (3) 式和 (6) 式

\begin{equation}\sum_{d\mid n}\mu (d)F(\frac nd)=\sum_{d\mid n}\left(\mu (d)\sum_{d_1\mid \frac nd}f(d_1)\right)=\sum_{d_1\mid n}\left(f(d_1)\sum_{d\mid \frac n{d_1}}\mu (d)\right)=f(n)\end{equation}

一些常见的狄利克雷卷积

1 $I\ast \mu=e$

2 $\mu\ast id=\varphi$

3 $I\ast id=\sigma$

4 $I\ast I=d$

5 $I\ast \varphi=id$

证明 1

莫比乌斯反演定理已证明。

证明 2

欧拉函数性质推导过程已证明。

证明 3

根据定义。

证明 4

根据定义。

证明 5

根据前面结论$I\ast \varphi=I\ast (\mu\ast id)=(I\ast \mu)\ast id=e\ast id=id$

算法练习

习题1

题意

题解