哈尔滨工业大学

初等数论

XPCHF

哈尔滨工业大学

中国剩余定理

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？

——《孙子算经》

中国剩余定理

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？

同余方程组：

$$
\begin{aligned}
x &\equiv 2 \pmod 3\\
x &\equiv 3 \pmod 5\\
x &\equiv 2 \pmod 7
\end{aligned}
$$

中国剩余定理

	mod 3	mod 5	mod 7
70	1	0	0
21	0	1	0
15	0	0	1

$$70 * 2 + 21 * 3 + 15 * 2 = 233$$

同余方程组：

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

3 * 5 * 7 = 105

方程组的解： 233 + 105n

233 % 105 = 23

中国剩余定理

$$(S):\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

(m_i互质)

$$x = \left(\sum_{i=1}^{n} a_i t_i M_i\right) mod M$$

$M = m_1 * m_2 * \ldots * m_n$

$M_i = M/m_i$

$M_i * t_i \equiv 1 \pmod{m_i}$

$x = k*M+\sum(a_i*t_i*M_i)$, $k \in Z$

扩展中国剩余定理

x ≡ a1 (mod m1)
x ≡ a2 (mod m2)

x = m1 * x1 + a1 = m2 * x2 + a2
m1 * x1 + m2 * x2 = a2 - a1
exgcd -> x1 k = m1 * x1 + a1
x ≡ k (mod lcm(m1,m2))

扩展中国剩余定理

x ≡ a1 (mod m1)
x ≡ a2 (mod m2)

x = m1 * x1 + a1 = m2 * x2 + a2
m1 * x1 + m2 * x2 = a2 - a1
exgcd -> x1 k = m1 * x1 + a1
x ≡ k (mod lcm(m1,m2))

哈尔滨工业大学

莫比乌斯反演

莫比乌斯函数：μ(d) 容斥系数

当d=1时，μ(d)=1；

当d=Πpi且pi为互异素数时μ(d)=(−1)^k。

只要当d含有任何质因子的幂次大于2，则函数值为0.

莫比乌斯函数

```
void get_mu(int n)
{
    mu[1]=1;
    for(int i=2;i<=n;i++)
    {
        if(!vis[i]){prim[++cnt]=i;mu[i]=-1;}
        for(int j=1;j<=cnt&&prim[j]*i<=n;j++)
        {
            vis[prim[j]*i]=1;
            if(i%prim[j]==0)break;
            else mu[i*prim[j]]=-mu[i];
        }
    }
}
```

莫比乌斯函数：$\mu(d)$ 容斥系数

当d=1时，$\mu(d)=1$；

当$d=\Pi p_i$且p_i为互异素数时$\mu(d)=(-1)^k$。

只要当d含有任何质因子的幂次大于2，则函数值为0.

莫比乌斯反演

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

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

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

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

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

给定N, M,求1<=x<=N, 1<=y<=M 且gcd(x, y)为质数的(x, y)有多少对?

给定N, M,求1<=x<=N, 1<=y<=M 且gcd(x, y)为质数的(x, y)有多少对？

$$f(d)=\sum_{i=1}^{N}\sum_{j=1}^{M}\left[\gcd(i,j)=d\right]$$

$$Ans=\sum_{p\in prim} f(p)$$

莫比乌斯反演

$$f(d)=\sum_{i=1}^{N}\sum_{j=1}^{M}\left[\gcd(i,j)=d\right]$$

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

莫比乌斯反演

$$f(d)=\sum_{i=1}^{N}\sum_{j=1}^{M}[\gcd(i,j)=d]$$

$$F(n)=\sum_{n\mid d}f(d)=\left\lfloor\frac{N}{n}\right\rfloor\left\lfloor\frac{M}{n}\right\rfloor$$

莫比乌斯反演

$$F(n)=\left\lfloor\frac{N}{n}\right\rfloor\left\lfloor\frac{M}{n}\right\rfloor$$

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

莫比乌斯反演

$$Ans = \sum_{p \in prim} \sum_{p \mid d} \mu\left(\frac{d}{p}\right) \left\lfloor \frac{N}{d} \right\rfloor \left\lfloor \frac{M}{d} \right\rfloor$$

$$Ans = \sum_{d=1}^{\min(N,M)} \sum_{p \mid d,\, p \in prim} \mu\left(\frac{d}{p}\right) \left\lfloor \frac{N}{d} \right\rfloor \left\lfloor \frac{M}{d} \right\rfloor$$

莫比乌斯反演

$$Ans = \sum_{d=1}^{\min(N,M)} \sum_{p|d,\, p\in prim} \mu\left(\frac{d}{p}\right)\left\lfloor\frac{N}{d}\right\rfloor\left\lfloor\frac{M}{d}\right\rfloor$$

$$Ans = \sum_{d=1}^{\min(N,M)} \left\lfloor\frac{N}{d}\right\rfloor\left\lfloor\frac{M}{d}\right\rfloor \sum_{p|d,\, p\in prim} \mu\left(\frac{d}{p}\right)$$

$$Ans=\sum_{d=1}^{\min(N,M)}\left\lfloor\frac{N}{d}\right\rfloor\left\lfloor\frac{M}{d}\right\rfloor\sum_{p|d,p\in prim}\mu\left(\frac{d}{p}\right)$$

后面的求和：线性筛维护

单次查询：O(n)

多次查询：O(n+q*sqrt(n))

哈尔滨工业大学

一些有趣的东西

法雷级数

0/1								1/1
0/1				1/2				1/1
0/1		1/3		1/2		2/3		1/1
0/1	1/4	1/3	2/5	1/2	3/5	2/3	3/4	1/1

用途：分数逼近

两个时间复杂度问题

```
for(int i=1; i<=n; i++)
    for(int j=i; j<=n; j+=i);
```

$$n + n/2 + n/3 + ... + n/n = O(n\log n)$$

```
for(i: prime);
```

O(n以内质数) $= O(n/\log n)$

指数循环节

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

Lucas定理

$$C_n^m = C_{n/p}^{m/p} C_{n\%p}^{m\%p} \pmod p$$

Berlekamp Massey算法

用途：常系数k阶递推式求值

板子随后送上…

http://oeis.org/

数列查询万能工具

哈尔滨工业大学

更多的数论？

数论对数
二次剩余
原根
BSGS(大步小步算法)
斐波那契循环节

prufer序列
基尔霍夫矩阵
矩阵树定理
Burnside引理
polya计数

多项式除法
多项式取余
多项式求逆
拉格朗日插值

FFT(快速傅里叶变换)
FWT(快速沃尔什变换)
NTT(快速数论变换)
生成函数-分治FFT算法

哈尔滨工业大学

谢谢您的观看