数论基础~~(从入门到弃疗)~~

By 可爱的Mys_C_K小学妹
&   kevinshuai小姐姐
&   ckw学姐
感谢青岛二中迟凯文友情赞助

概览

数论基础知识：取模与同余理论，(扩展)欧拉定理，卢卡斯定理，CRT。

常见数论算法：快速幂，(ex)gcd, bsgs，线性筛

莫比乌斯反演入门

杜教筛

其他还有min25筛，洲阁筛，贝尔级数，乱七八糟的数论技巧之类的。

数论基础知识

$a\%b$：a除以b余数

$a \equiv b \pmod{m}$

取模，大家应该都知道，%

同余，如果a和b对m取模得到的结果相同，那么说a和b在模m意义下相等，或者说二者同余，记作a≡b (mod m)（其实中间应该是三条杠，但是打不出来），并且就划分为同一类。

$x \equiv 0, 1, \dots, m-1 \pmod{m}$

显然模m意义下一共有m类数字，以0,1,...,m-1为代表元素。

注意负数也是可以取模的，例如(-1) mod 3 = 2。

如果a=km+r(0<=r<m)，那么a=r(mod m)，这称作"带余除法"。

特殊的，如果r=0，那么m是a的因数，a是m的倍数，称为m整除a，记作m|a

$r=0.$

$a=km$

$a=km+r$ $0\le r<m).$ $m>0$

$3+1$

$a\equiv b \pmod{m}$

$m \mid a$

$13 = 4 \times 3$

$a \equiv r \pmod m$　$a = b + km$

~~因数~~

刚才说了，如果$a|b$，也就是a整除b，那么b是a的倍数，a是b的因数。

显然如果$a|b,a|c$，那么$a|(b±c)$, $a|(bx+cy)$，即a整除b和c的线性组合

最大公因数$gcd(a,b)$，或者简写成(a,b)，定义为，最大的d，满足$d|a$且$d|b$。

显然$d|(a,b)$等价于，$d|a$且$d|b$

另一个很显然的是，$\boxed{(a,b)=(a+b,b)=(a-b,b)=(a \bmod b,b)}$

$$\frac{a|b,\ b|c}{a|c}$$

特别的，如果$(a,b)=1$，那么称作a和b互质

$(a,b) = d'$

最小公倍数$[a,b]$同理。

$a|b,\ a|c$

二者关系：$[a,b]=ab/(a,b)$，注意只对两个数字恒有效

$a|(b±c)$

$\Downarrow$

$gcd(a,b) := \max_{d} (d|a,\ d|b)$

$d|d'$

$d|a$

$3|6$

$3|9$

$3|15$

$a|(bx+cy)$

$d'|a$　$d'|b$　$d|a$　$d|b$

$\boxed{d \mid a,\ d \mid b}$

$d \le d'$. $(a,b)=(a+b,b)$

$a \mid b \to a \mid bx$

$a \mid cy$

$a \mid (bx+cy)$

数论基础知识

如果两个数字同余，那么在模意义下做加减乘运算，这两个数字有相同的效果(注意次方运算不等价)。

我们可以正常的在模意义下做加减乘运算，但是除法有些时候是有问题的，例如5=2(mod 3)，这个时候就不能两边除以2。

记d=(a,b,m)，且a=b(mod m),那么a/d=b/d(mod m/d)，注意模数也是要除以d的，例如2≡6(mod 4)，那么1=3(mod 2)，但是1!=3(mod 4)。

$1 \equiv 3 \pmod 4$ x

由此可以看出，当(a,m)>1时，除以(a,m)的因数会导致条件的性质被减弱。

$a \equiv b \pmod m$

$a \pm c \equiv b \pm c \pmod m$

$ac \equiv bc \pmod m$

欧拉定理

$$a \equiv b \pmod m \Rightarrow a-b=km$$

$$\Rightarrow ac-bc=(a-b)c=\underline{(kc)m}$$

$$\Rightarrow ac \equiv bc \pmod m$$

我们先来看第一个数论定理，叫做欧拉定理，表述如下：

对于n是质数的情况，就是一个叫做费马小定理的东西

我们只证明一个费马小定理。

$\phi(n)$：$1 \sim n$ 中有多少数 x 和 n 互质

p是质 $\phi(p)=p-1$

欧拉定理：如果(a,n)=1，即a和n互质，那么：

$$\boxed{a^{\phi(n)} \equiv 1 \ (mod\ n)}$$

其中$\phi(n)$表示1~n中，和n互质的数的个数。显然当n是质数的时候，phi(n)=n-1

性质：

$\phi(n) = \sum_{i=1}^{n}[(i,n)==1] = n\prod(1-\frac{1}{p_i})$，其中p_i是n的质因子。

$\sum_{d|n}\phi(d) = n$

$p\nmid a$ $a^{p-1} \equiv 1 \pmod p$

费马小定理

逆元

我们刚刚知道如果a和n互质则a^phi(n)=1(mod n)，那么a^(phi(n)-1)*a=1(mod n)。

而我们知道a^(-1)*a^(1)=a^0=1，因此理应a^(phi(n)-1)和a^(-1)在模n意义下相等（虽然并不是个严格的定义），而我们知道a^(-1)=1/a，所以当你做模意义下除法的时候，例如a/b=?(mod n),如果(b,n)=1那么a/b=a*b^(phi(n)-1)(mod n)。

特殊的，当n是质数p的时候，对于任意不是p倍数的a，都有/a=*a^(p-2)。

称a^(-1)为a在模n意义下的逆元，也写作inv(a)。

例如，计算40/2 mod 7，我们知道结果是=6，但是如果你先把40取模了的话就需要计算5/2 mod 7，这个就是5*2^5=6(mod 7)。可见这个东西确实是对的。

最后提醒一句，应用欧拉定理必须要满足(a,n)=1

线性求逆元（模质数意义下）

做法其实很简单，先处理阶乘fac[i]=fac[i-1]*i，然后facinv[n]=inv(fac[n])，然后facinv[i]=(i+1)*facinv[i+1]，最后inv[i]=facinv[i]*fac[i-1]即可。

inv(x)=fast_pow(x,p-2)

扩展欧拉定理

并不知道为啥是对的，反正知道结论就行了

扩展欧拉定理

$(\bmod n)$

$$a^b = a^{b\%\phi(n)}, (a,b) = 1$$
$$a^b = a^b, (a,b) > 1, b < \phi(n)$$
$$a^{b} = a^{b\%\phi(n)+\phi(n)}, (a,b) > 1, \phi(n) \le b$$

因能力、就把它
记着就行

卢卡斯定理

也不知道为什么是对的，反正知道结论就对了

$$C_n^m \equiv C_{n\%p}^{m\%p} C_{\lfloor n/p \rfloor}^{\lfloor m/p \rfloor} \pmod p$$

p质数

$$C_n^m \equiv 0 \pmod p$$

若 $n>m$

卢卡斯定理

$$if\ p\ is\ a\ prime, then \binom{n}{m}\%p = \binom{n/p}{m/p}\binom{n\%p}{m\%p}$$

特殊的如果在%p意义下n>m那么组合数的值是0。

其实就是把n和m写成p进制的数字，然后每一位求组合数然后乘起来。

（本质：n, m 写成 p 进制下数

$n_k \cdots n_0$

$m_k \cdots m_0$

用处是当n和m特别大，p是质数并且比较小的时候可以这么搞。

$p \sim 1e5$

$\boxed{n, m \sim 1e18}$

$$\boxed{C_n^m = C_{n_0}^{m_0} C_{n_1}^{m_1} \cdots C_{n_k}^{m_k}}$$

数位dp

CRT

- 传说中可以扔到垃圾桶里面的定理，其实可以自己构造出来。只有结论是有意义的。
    - 实际操作可以用exgcd代替。

常见数论算法

~~快速幂~~

~~不会吧不会吧这年头了还有人不会快速幂~~

GCD/EXGCD

gcd，求两个数的gcd

(a,b)=(a-b,b)=(a-2b,b)=...=(a%b,b)，递归即可。

gcd(a,b)= (a==0 ? b : gcd(b%a,a))

exgcd：求解一个二元一次不定方程

求满足ax+by=(a,b)的一组(x,y)，并且使得|x|+|y|最小。

扩展欧几里得：考虑一组方程ax+by=(a,b)，不妨令a<=b，那么：

$$ax + (b - a + a)y = (a, b), a(x + y) + (b - a)y = (a, b),$$
$$a(x + y) + (b - 2a + a)y = (a, b), a(x + 2y) + (b - 2a)y = (a, b)$$
$$\cdots$$
$$a(x + \left\lfloor \frac{a}{b} \right\rfloor y) + (b\%a)y = (a, b)$$
$$(b\%a)y + a(x + \left\lfloor \frac{a}{b} \right\rfloor y) = (a, b)$$
$$(b\%a)x' + ay' = (a, b)$$

这样递归求出(x',y')，然后在通过(x',y')求出(x,y)即可，边界是当a=0时x=0,y=1

显然x的系数每次会减半，因此复杂度是O(lg)的。

关于二元一次不定方程

求ax+by=c的所有整数解，或者判断无解。

首先根据裴蜀定理，这个方程有整数解当且仅当(a,b)|c，必要性显然，充分性其实就是exgcd的归纳过程。

那么我们求出一组ax+by=(a,b)的解(x,y)，然后x’=(c/(a,b))x, y’同理，那么ax’+by’=c，也就是ax+by=c的通解就是ax+by=(a,b)的通解乘以c/(a,b)。

而假设得到的一组特解是(x0,y0)，那么通解是(令d=(a,b)):

x=x0+k (b/d), y=y0-k (a/d), k是任意整数。

大家可以发现把这个东西代入确实是对的。

m

m' m' m'

扩展欧几里得的小应用

同余方程。解方程：ax=b(mod c)

先把a=0或者b=0的情况判出来。

然后，ax=b(mod c)等价于，ax-b=yc，即ax+cy=b（这里把y的符号反过来了）。这样做exgcd即可，可知有解的充要条件是(a,c)|b。注意你exgcd得到的解x是在mod c/(a,c)意义下的，也就是在mod c意义下有(a,c)组解。

代替CRT：已知x=a(mod n)，x=b(mod m)，求x mod [n,m]

这等价于：x=a+pn=b+qm，因此pn+qm=b-a，这里仍然把q的符号反过来了。可知有解的充要条件是(n,m)|(b-a)，并且求解出来的p是在mod m/(n, m)意义下的，那么x=a+pn就是在mod nm/(n,m)=[n,m]意义下的。

~~还可以用来做NOI2018 Day2 T1~~

$\frac{c}{\frac{c}{(a,c)}}$

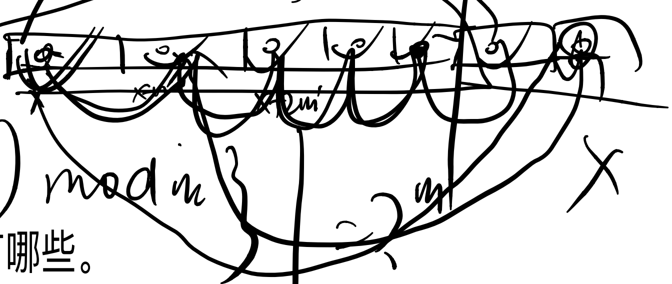
m'

2a(m-1)

BSGS

北上广深算法，拔山盖世算法

$(x+km') \bmod m$



求满足a^x=b(mod p)，p是质数，的x有哪些。

显然这些x在%(p-1)意义下循环。所以就是求在0~p-1中有多少。

其实就是在做分块，这里的bsgs要求模数是质数。

$0 \le k \le (a,m) - 1$

对于不是质数的情况有个exbsgs，请自行百度。

$x + (a,m)\frac{m}{(a,m)} \equiv x$

BSGS算法流程

考虑令s=sqrt(p)，然后对于每一个x=ks+r, $0<=r<s$

当k=0的时候只有s个x，即x=r；直接枚举，并且开个map记录mp[v]=满足a^r=v的r有多少。

当k>0时，意味着a^(ks+r)=(a^s)^k*a^r=b，即:

a^r=b*((a^s)^k)^(-1)，算出右边，然后看左边是否有r即可。

使用哈希表或者unordered_map（需要开c++11）可以做到O(sqrt(p))。

1、两只青蛙在地球赤道上，赤道等分成L个点标号0~(L-1)，两只青蛙一个在A，每次跳a步，一个在B，每次跳b步，问最少多少步后相遇，或者永不相遇。

$\underline{\min}$

BZOJ 1477

模板题

假设跳了x步，那么：

$A+ax=B+bx \pmod{L}$，即$(a-b)x=B-A \pmod{L}$，同余方程即可……

10 min

在 mod p 意义下　　循环节

在 mod (p-1) 意义下　　n

(2). 求有多少n满足1<=n<=x并且n*a^n=b (mod p).
p是一个质数，p<=1e6+3,x<=1e12,1<=a,b<p.

费马：$a^{p-1} \equiv 1 \pmod{p}$

$$a^n \equiv a^{n-2(p-1)} \equiv \cdots \equiv \boxed{a^{n\%(p-1)}} \pmod{p}$$

$n = k(p-1)+r,\quad 0 \le r < p-1$

$a^n \equiv a^{n\%(p-1)} \pmod{p}$

$$n \cdot a^n \equiv (\underbrace{\cancel{r-k}}_{r-k}) \cdot a^r \equiv b \pmod{p}$$

CF 919 E

$n\cdot a^n \equiv (r-k)a^r \equiv b \pmod p$

bsgs? 为啥p这么小? 如果没有前面的n怎么做? 没有指数上的n怎么办?

注意到前面的n是mod p意义下循环的，指数上的是模p-1循环的。

- 我们表示其中一个，例如假定n=k(p-1)+r，0<=r<p-1，那么a^n=a^r，n*a^n=(r-k)a^r=b，到这里做法就很显然了：枚举r，计算a^r，除过去，就可以解出k在模p意义下的值，然后算一下上下界即可。

枚举 $r \Rightarrow a^r \to t$ (a^{-1})

$t^{-1} = (a^r)^{-1} = (a^{-1})^r$ mod p

a^n 有 p-1 个

$(r-k)t \equiv b$

$a, a^2, \ldots, a^{p-1}$

a^p a^{p+1}

$r-k \equiv b\cdot t^{-1}$

$k \equiv r - b\cdot t^{-1} \equiv k_0 \pmod p$

mod p = k_0

莫比乌斯反演

好请让我们速成莫比乌斯反演。

~~说起来我们学校机房至少一小半人的莫反都是我讲的~~

首先介绍一些概念。

数论函数，就是正整数映射到整数的函数。

积性函数，如果一个数论函数f满足对于任意(x,y)=1，有f(xy)=f(x)f(y)，那么称f是积性函数。

显只要知道了所有的f(p^c)就可以知道所有的f(n)

完全积性函数，如果一个数论函数满足对于任意x和y，都有f(xy)=f(x)f(y)，那么称f是完全积性函数

$k = k_0 + c$ $c \geq 0$

$n = k(p-1) + r \leq x$

$k_0 + cp \leq \left\lfloor \frac{x-r}{p-1} \right\rfloor$

$r: \quad 0 \leq c \leq \frac{\left\lfloor \frac{x-r}{p-1} \right\rfloor - k_0}{p}$

$O(p \lg)$

常见积性函数举例

phi(n): 1~n中和n互质的数字个数，是积性函数

mu(n)：一会详细说

d(n): n的因数个数/因数和，二者都是积性函数

id(n)=n：就是其本身

e(n)=[n==1]，单位元，相当于判断一个数是不是1

1(n)=1：函数值恒等于1的函数

显然后面三个都是完全积性，有时候为了方便会把(n)省略。

线性筛

可以在O(n)时间内筛出1~n的所有质数。

如果F(n)是个积性函数，根据定义我们只要能够低于O(lgn)的知道每个F(p^c)的值，我们就能在O(n)时间内求出F(1)~F(n)。

具体做法是这样的，每次枚举一个数字i，枚举所有已经筛出来的1~i中的质数k，那么x=ik不是质数，并且k是x的最小质因子。如果i%k==0，就break掉k的循环。可以证明每个数字都只会被其最小的质因子筛去，同时利用这个性质可以顺便筛出一些积性函数。

这样你可以维护每个数字的最小质因子lp[n]，最小质因子对应的那个若干次方lpc[n]，这样对于积性函数每次只要计算满足lpc[n]=n的那些F[n]，然后用积性函数的性质就可以维护1~n的F。

狄利克雷卷积

如果两个函数都是积性函数，那么他们的狄利克雷卷积也是积性函数。

狄利克雷卷积

设f和g是两个数论函数，并且对于任意n>=1，存在:

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

那么称h是f和g的狄利克雷卷积。

例如，上上面关于$\phi(n)$的结论可以说是id是phi和1的卷积

莫比乌斯函数MU(N)

莫比乌斯函数

如果$n=\prod_{i=1}^{k} p_i^{a_i}$，那么$\mu(n)=$

1）1，如果n=1

2）0，如果存在质数p，满足$p^2|n$

3）$(-1)^k$，else

一个最重要的性质：$\sum_{d|n}\mu(d)=[n==1]=e(n)$

也就是“如何判断一个数字是不是1呢？只要把mu和1做狄利克雷卷积就好了”。

莫比乌斯反演

这部分推导比较多，就丢到.md文件里啦

Eg1.求$\sum_{i=1}^{n}(i,n)$，n,q<=50000

$$\sum_{i=1}^{n}(i,n)=\sum_{d|n}d\sum_{i=1}^{n}[(i,n)==d]=\sum_{d|n}\sum_{i=1}^{n}[(\frac{i}{d},\frac{n}{d})=1]$$

$$=\sum_{d|n}d\sum_{i=1}^{\frac{n}{d}}(i,\frac{n}{d})=\sum_{d|n}d\phi(\frac{n}{d})$$

这样我们在O(n)时间内预处理ϕ就可以O(sqrt(n))回答每一组询问了。

事实上我们是有$\mu*1=\phi$的：

$$\phi(n)=\sum_{i=1}^{n}[(i,n)==1]=\sum_{i=1}^{n}\sum_{d|(i,n)}\mu(d)=\sum_{d|n}\mu(d)\sum_{d|i,i\leq n}1=\sum_{d|n}\mu(d)\frac{n}{d}$$

Eg2.求：$\sum_{i=1}^{n}\sum_{j=1}^{m}f(gcd(i,j)),(n\le m)$，f(x)是一个长度为n的可以在线性时间内计算出来的函数（并不要求积性），n,q<=50000

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

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

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

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

$$=\sum_{d=1}^{n}f(d)\sum_{e=1}^{\lfloor\frac{n}{d}\rfloor}\mu(e)\left\lfloor\frac{n}{de}\right\rfloor\left\lfloor\frac{m}{de}\right\rfloor$$

这里用到了一个小小的结论：$\left\lfloor\frac{\lfloor\frac{a}{b}\rfloor}{c}\right\rfloor=\lfloor\frac{a}{bc}\rfloor$

现在还是有两个东西需要枚举，好像还是没法做。

因此我们枚举d和e的乘积T，然后考虑那么(n/T)*(m/T)的系数

$$
\begin{aligned}
&= \sum_{T=de=1}^{n} \left\lfloor \frac{n}{T} \right\rfloor \left\lfloor \frac{m}{T} \right\rfloor \sum_{d|T} f(d)\mu\left(\frac{T}{d}\right) \\
&= \sum_{T=de=1}^{n} \left\lfloor \frac{n}{T} \right\rfloor \left\lfloor \frac{m}{T} \right\rfloor g(T)
\end{aligned}
$$

就是说后面那一坨只和T有关。

显然g(T)可以在至多O(nlgn)的时间内用下面这段代码预处理求出：

```
for(int i=1;i<=n;i++) for(int j=1;i*j<=n;j++) g[i*j]+=f[i]*mu[j];
```

我们用O(A)+O(B)表示一个东西可以在O(A)的预处理情况下每次O(B)的处理一个询问。

那么现在我们已经可以做到O(nlgn)+O(n)了。

但是注意到这么一件事情：$\left\lfloor \frac{n}{T} \right\rfloor$只有$O(\sqrt{n})$种取值，因此我们只要枚举这个数值和其对应的区间，对g预处理前缀和即可做到O(nlgn)+O(sqrt(n))

有些时候g函数有特殊性质，可以在O(n)时间内求出。例如DZY Loves Maths

数论分块

额外说一句，枚举所有[n/T]，[m/T]相同的区间[s,t]可以用下面的代码：

```
for(int s=1,t;s<=min(n,m);s=t+1) t=min(n/(n/s),m/(m/s)),ans+=calc(n,s,t);//n/s=n/t,m/s=m/t
```

莫反就讲完了，题目选讲里面还有一些大家可以自行阅读

大家可以尝试推导：$\sum_{i=1}^{n}\sum_{j=1}^{m}lcm(i,j)$。同样的，n和q都是5e4。

莫反的题有些时候在推导上需要一些结论辅助，常见的例如，如果记d(n)表示n的因数个数，那么：

$d(nm)=\sum_{i|n}\sum_{j|m}[(i,j)==1]$（顺便以后就用$i\perp j$表示$[(i,j)==1]$了）

当然还有其他很多结论，这就靠大家以后自己积累了。

杜教筛

同上

本质上是已知A卷积B=C，已知B和C的前缀和都很好求，求A的前缀和。

（另，若A和B的前缀和很好求，那么显然C的前缀和可以O(sqrt(n))求出）

推荐一个讲杜教筛很好的网站，后面附有成堆的练习题，大家自行参考：

https://blog.csdn.net/skywalkert/article/details/50500009

杜教筛

求$S(n)=\sum_{i=1}^{n}\phi(i), n\le 10^9$

考虑下式:

$$\sum_{i=1}^{n}\sum_{d|i}\phi(d)=\sum_{i=1}^{n}i=\frac{n(n+1)}{2}$$

同时我们还有:

$$\begin{aligned}\sum_{i=1}^{n}\sum_{d|i}\phi(d)&=\sum_{i=1}^{n}\left(\phi(i)+\sum_{d|i,d\neq i}\phi(d)\right)\\&=\sum_{i=1}^{n}\phi(i)+\sum_{i=1}^{n}\sum_{d|i,d\neq i}\phi(d)\\&=S(n)+\sum_{k=\frac{i}{d}=2}^{n}\sum_{dk\le n}\phi(d)\\&=S(n)+\sum_{k=2}^{n}S\left(\left\lfloor\frac{n}{k}\right\rfloor\right)\end{aligned}$$

也就是说：

$$\frac{n(n+1)}{2}=S(n)+\sum_{k=2}^{n}S\left(\left\lfloor\frac{n}{k}\right\rfloor\right)$$

$$S(n)=\frac{n(n+1)}{2}-\sum_{k=2}^{n}S\left(\left\lfloor\frac{n}{k}\right\rfloor\right)$$

然后我们对后面那一坨进行之前提到过的数论分块，然后记忆化搜索，可以证明复杂度是$O(n^{\frac{3}{4}})$的。

同时如果预处理前$O(n^{\frac{2}{3}})$的S(n)，就可以做到$O(n^{\frac{2}{3}})$。

至于为啥是对的我也讲的不是很清楚。

如何求μ的前缀和请自行推导（其实就是把那个n(n+1)/2换成1）

最后一个例子（终于写完了啊啊啊啊啊）

求：$\sum_{i=1}^{n} i\phi(i)$

$$\sum_{i=1}^{n}\sum_{d|i} i\phi(d) = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{d|i} i\phi(d) &= \sum_{i=1}^{n}\left(i\phi(i) + \sum_{d|i,d\neq i} i\phi(d)\right) \\
&= \sum_{i=1}^{n} i\phi(i) + \sum_{i=1}^{n} i \sum_{d|i,d\neq i}\phi(d) \\
&= S(n) + \sum_{k=\frac{i}{d}=2}^{n}\sum_{dk\le n}\phi(d)dk \\
&= S(n) + \sum_{k=\frac{i}{d}=2}^{n} k \sum_{dk\le n}\phi(d)d \\
&= S(n) + \sum_{k=2}^{n} kS\left(\left\lfloor\frac{n}{k}\right\rfloor\right)
\end{aligned}$$

然后就没了。

推荐学习

时间原因，有些东西讲不了，但是如果要准备省选还是很重要的内容，所以在这里列出来以供参考。

列表大致按照重要程度排序，不保证按照难度排序。一些不重要的东西未保留。

高斯消元，矩阵乘法（优化dp等），拉格朗日插值

~~FFT/NTT~~/FWT

二项式反演，Min-Max容斥（其实都是广义容斥），单位根反演

~~生成函数~~，多项式理论那一套（其实学了基本没用）

Miller-Rabbin判素数和pollard-rho分解质因数（感觉用到概率不大）

~~卡特兰数~~，斯特林数，斯特林数反演（参见HDU的JZPTREE）。

杨氏表和钩子定理（不是很重要，知道即可）

min25筛（不知道现在黑科技有没有更优秀的筛法），贝尔级数~~（可用于指导构造杜教筛中的函数）~~

练习题

数论基础题我也没做过几道……

莫比乌斯反演题给大家推荐个blog，大家可以倒着做……

https://blog.csdn.net/popoqqq/article/category/2542267

杜教筛之前那个blog有附练习题