清華大學
Tsinghua University

数论入门到入坟

清华大学学生算法协会　Mys_C_K

2024.08.14

Q & A

- Q：你看起来好~~可爱~~菜你是谁啊？
- A：我是清华算协的 Mys_C_K 确实非常~~可爱~~菜。
- Q：你凭什么给我们讲课啊？你都拿过什么奖啊？
- A：2015 普及组二等，2017 提高组一等里面垫底，WC2018 没牌，APIO2017 铜牌，NOI2018 铜牌，WC2019 铜牌~~我就是炼铜术士~~。
- Q：会不会讲的太简单啊？
- A：……如果觉得简单可以狠狠~~嘲讽~~睡觉……
- Q：Zzz…
- A：阿巴阿巴

清華大學
Tsinghua University

Part I: 数论基础

概要

- 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

数论基础知识

- 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。
- 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。 $-1 \equiv 2 \pmod 3$
- 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

$(m>0)$

Def (C++) : a%b $a\%m = b\%m$. $a \equiv b \pmod m$

(同余) $a \equiv r \pmod m$ $0 \le r < m$

(带余除法) $a = km + r$. $k \in \mathbb{Z}$

若 $r = 0$. $\Leftrightarrow a = km$, $k \in \mathbb{Z}$. 记作 $m \mid a$ 整除

$-1 \equiv 2 \pmod 3$

$\Updownarrow$

$-1 \equiv (-1)\times 3 + 2$

prop $a \mid b$, $a \mid c \Rightarrow a \mid bx + cy$. $x, y \in \mathbb{Z}$.

Def $gcd(a,b) \triangleq \max\limits_{\substack{d \mid a \\ d \mid b}} d$

$a = p_1^{a_1} \cdots p_k^{a_k}$. p_i 质

$b = p_1^{b_1} \cdots p_k^{b_k}$

$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$

$c \mid a \Leftrightarrow c_1 \le a_1, \cdots c_k \le a_k$

$c = p_1^{c_1} \cdots p_k^{c_k} \le gcd(a,b)$

$d = (a,b)$

推论 $c \mid d \Leftrightarrow c \mid a, c \mid b$

$\forall i$ $\Updownarrow$ $\Leftrightarrow$ $c_i \le a_i$; $c_i \le b_i$

$c_i \le \min(a_i, b_i)$

prop $(a,b) = (a \pm b, b)$

pf $d = (a,b) \Rightarrow d \mid a, d \mid b \Rightarrow d \mid a+b, d \mid b$ 推论 $\Rightarrow d \mid (a+b, b)$

$\Rightarrow (a,b) \mid (a+b, b)$

同理 $(a+b, b) \mid (a,b)$ $\Rightarrow (a,b) = (a+b, b)$

$a,b>0$

col $(a,b) = (a-b, b) = (a-2b, b) = \cdots = (a\%b, b)$ 证明 $\Rightarrow$ 求 gcd

Def $(a,b) = 1$. a, b 互质. $a \perp b$

$a = p_1^{a_1} \cdots p_k^{a_k}$

最小公倍数 $[a,b] = p_1^{\max(a_1,b_1)} \cdots p_k^{\max(a_k,b_k)}$

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，(a,b)=(a+b,b)=(a-b,b)=(a mod b,b)
- 特别的，如果(a,b)=1，那么称作a和b互质
- 最小公倍数[a,b]同理。
- 二者关系：[a,b]=ab/(a,b)，注意只对两个数字恒有效

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)。
- 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。

— prop. $a_1 \equiv b_1 \pmod m$
$a_2 \equiv b_2 \pmod m$

加.减.乘 $\begin{cases} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m \\ a_1 a_2 \equiv b_1 b_2 \pmod m \end{cases}$

$(k_1 m + r_1)(k_2 m + r_2) = \underbrace{k_1 k_2 m^2 + k_1 r_2 m + k_2 r_1 m}_{} + r_1 r_2$

$a_1 a_2 \equiv r_1 r_2 \pmod m$

eg. 除法 X. eg. $2 \equiv 6 \pmod 4 \not\Rightarrow 1 \equiv 3 \pmod 4$

$\Rightarrow 1 \equiv 3 \pmod 2$

P.S. 时间有限. 一些数论不给证明

Thm (欧拉定理) $(a,n)=1$ 则. $a^{\varphi(n)} \equiv 1 \pmod n$

其中 $\varphi(n)$: Euler 函数 $\triangleq$ 1~n 中与 n 互质的数的个数

eg. p 质. 1~(p-1) 与 p 互质. $\varphi(p) = p-1$

$\varphi(2^n) = \begin{cases} 2^{n-1}, & n>0 \\ 1, & n=0 \end{cases}$

$(a,p)=1 \Leftrightarrow p \nmid a$

Col (费马定理) $n=p$ 为质. $a^{p-1} \equiv 1 \pmod p$.

Pf. 断言 $a, 2a, 3a, \ldots, (p-1)a$ 在 mod p 意义下两两不同. (p-1个数)

i.e. $\forall 1 \le i < j \le p-1$. $ia \not\equiv ja \pmod p$

Pf. $(j-i)a$ 不是 p 倍数 $p \mid (j-i)a$ $(j-i)a \not\equiv 0 \pmod p$
$1 \le j-i \le p-2$ $ja \not\equiv ia \pmod p$

又显然 $ia \not\equiv 0 \pmod p$ $\forall 1 \le i \le p-1$

在 $[1, (p-1)]$

$\Longrightarrow$ 是 1~(p-1) 的排列 $\Rightarrow 1a \cdot 2a \cdot 3a \cdots (p-1)a \equiv (p-1)! \pmod p$

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

$\Rightarrow (a^{p-1}-1)(p-1)! \equiv 0 \pmod p$. $p \nmid (p-1)!$

欧拉定理

$\Rightarrow a^{p-1} \equiv 1 \pmod p$ QED.

欧拉定理：如果(a,n)=1，即a和n互质，那么：

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

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。

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

“扩展欧拉定理”

$\exists (a,n) \neq 1.$

$$\begin{cases} a^b = a^{b\%\phi(n)}, (a,b) = 1 \\ a^b = a^b, (a,b) > 1, b < \phi(n) \\ a^b = a^{b\%\phi(n)+\phi(n)}, (a,b) > 1, \phi(n) \leq b \end{cases}$$

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)。

$a^{\varphi(n)} \equiv 1 \pmod n$ $(a,n)=1$

$ax \equiv 1 \pmod n$, $(a,n)=1 \Rightarrow x$ 为 a 的"逆元"

由Euler定理. $a^{\varphi(n)-1} \cdot a \equiv 1 \pmod n$

令 $x = a^{\varphi(n)-1} \Rightarrow ax \equiv 1 \pmod n$

特别：n=p 时，$a^{-1} \equiv a^{p-2} \pmod{p}$

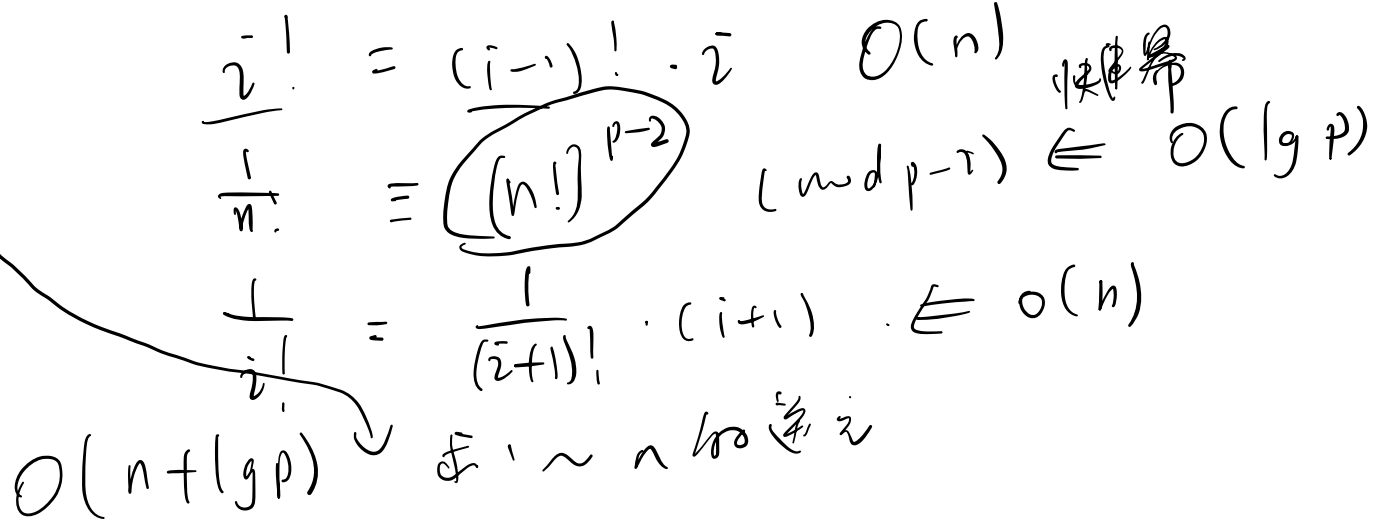
逆元

- 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！

$5 \cdot 2^{-1} \equiv 5 \cdot 2^{5} \pmod{7}$

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)



Lucas 卢卡斯定理

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m>n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。

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。

中国剩余定理 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
- 应该没人不会吧

$n \sim 10^{18}$

$a^n \pmod p$

$a^n = \left(a^{\lfloor \frac{n}{2} \rfloor}\right)^2 \cdot a^{n\%2}$

$a^{n\%2}$: a, 1

$O(\lg n)$

常见数论算法

- 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

Thm. $a \geq b$. $a\%b < \frac{1}{2}a$

pf. $a \geq 2b$. $\frac{a\%b}{a} < \frac{b}{a} \leq \frac{b}{2b} = \frac{1}{2}$

$b \leq a < 2b$. $a\%b = a-b$

$\frac{a\%b}{a} = \frac{a-b}{a} = 1-\frac{b}{a} < 1-\frac{1}{2} = \frac{1}{2}$

$\frac{b}{a} > \frac{1}{2}$

$b > \frac{a}{2}$

$(b\%(a\%b), a\%b)$

$< \frac{1}{2}a$

$O(\lg a + \lg b)$

$ax+by=c$ 令 $d=(a,b)$ 存解 $\Rightarrow d|c$

$\Leftarrow$

$d|a, d|b \Rightarrow d|ax+by=c$

"辗转相除法"

$a \geq b$

$a = \lfloor \frac{a}{b} \rfloor b + (a\%b)$

$ax+by=d$

$\left(\lfloor \frac{a}{b} \rfloor b + a\%b\right)x + by = d$

$\rightarrow b\left(\lfloor \frac{a}{b} \rfloor x + y\right) + (a\%b)x = d$

$(a,b) \rightleftarrows (b, a\%b) \rightarrow \cdots \rightarrow (d,0)$ $O(\lg a + \lg b)$

$dx + 0y = d$?

特解 $x=1$

$y=0$ 任意.

$bu + (a\%b)v = d$ 一解 $\tilde{x}, \tilde{y}$

$\begin{cases} \tilde{x} = \lfloor \frac{a}{b} \rfloor x + y \\ \tilde{y} = x \end{cases} \Leftrightarrow \begin{cases} x = \tilde{y} \\ y = \tilde{x} - \lfloor \frac{a}{b} \rfloor \tilde{y} \end{cases}$

通解 $ax+by=c$ $\overset{(a,b)\mid c}{\Rightarrow}$ 有特解 x_0, y_0.

$ax_0 + by_0 = (a,b)$ 令 $d=(a,b)$

$a(x_0+\Delta x) + b(y-\Delta y) = (a,b)$

$a\Delta x - b\Delta y = 0$

$\div d \Rightarrow$ $a'\Delta x = b'\Delta y$ $a' = \frac{a}{d}$. $b' = \frac{b}{d}$. $\Rightarrow (a',b') = 1$

$a' \mid a'\Delta x = b'\Delta y \Rightarrow \begin{cases} a' \mid \Delta y \\ b' \mid \Delta x \end{cases} \Rightarrow \Delta x = k \cdot \frac{b}{d}$. $k \in \mathbb{Z}$

$\begin{cases} x = x_0 + k\frac{b}{(a,b)} & k \in \mathbb{Z} \\ y = y_0 - k\frac{a}{(a,b)} \end{cases}$ 是通解.

$ax_0 + by_0 = (a,b) \overset{?}{\Rightarrow} a\left(x_0 \cdot \frac{c}{(a,b)}\right) + b\cdot\left(y_0 \frac{c}{(a,b)}\right) = c$

$\widetilde{x_0}$ $\widetilde{y_0}$

$\begin{cases} 13x + 5y = 1 \Rightarrow 8u+5v \Rightarrow 5p+3q \Rightarrow \\ exgcd \end{cases}$

EXGCD

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。

二元一次方程

- 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。

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

eg. $ax \equiv b \pmod n$ "同余方程"

$ax - b = -y \cdot n$ $\quad y \in \mathbb{Z}$

$\Leftrightarrow ax + ny = b$. exgcd 可求

有解 $\Leftrightarrow (a,n) \mid b$

exgcd $\Rightarrow x_0, y_0$

通解 $x = x_0 + k \cdot \frac{n}{(a,n)}$. $k \in \mathbb{Z}$

$\Leftrightarrow x \equiv x_0 \pmod{\frac{n}{(a,n)}}$

exgcd

$x \equiv ? \pmod{\frac{n}{(a,n)}}$ 模数 $\Rightarrow$ x在 mod n 意义下有 (a,n) 个解

$x \equiv 3 \pmod{10} \Rightarrow x = 3, 13, 23, 33, 43 \pmod{50}$

eg CRT

$a \equiv a_1 \pmod{n_1}$ $\quad a \equiv a_2 \pmod{n_2}$

$a - a_1 = x \cdot n_1$ $\quad a - a_2 = -y \cdot n_2$

$a = x \cdot n_1 + a_1 = -y \cdot n_2 + a_2$

$n_1 x + n_2 y = a_2 - a_1$

有解 $\Leftrightarrow (n_1, n_2) \mid a_2 - a_1$

exgcd $\Rightarrow x_0, y_0$ 合法解. $x = x_0 + k \frac{n_2}{(n_1,n_2)}$. $k \in \mathbb{Z}$

$\Downarrow$

$a = x_0 n_1 + k \frac{n_1 n_2}{(n_1,n_2)} + a_1$. $k \in \mathbb{Z}$

$\Downarrow [n_1, n_2]$

$\Updownarrow$

$a \equiv x_0 n_1 + a_1 \pmod{[n_1, n_2]}$

BSGS

- 北上广深算法，拔山盖世算法
- 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。
- 对于不是质数的情况有个exbsgs，请自行百度。

BSGS

- 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))。

Eg

- 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。

Sol

- 模板题
- 假设跳了x步，那么：
- $A+ax=B+bx(\mod L)$，即$(a-b)x=B-A(\mod L)$，同余方程即可……

Eg

- 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.

Sol

- 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。

清華大學
Tsinghua University

Part II: 莫比乌斯反演与杜教筛

概要

- 莫比乌斯反演入门
- 杜教筛

Def. $f: \mathbb{N}^+ \to \mathbb{N}^+$ (定义域 自变量 值域 因变量 是正整数)

称为数论函数 (无特别说明为正整数)

若 f 满足 $\forall x \perp y$ $f(xy) = f(x) \cdot f(y)$

称 f 为积性函数

eg. $id(x) \triangleq x$ 完全积性 $id(xy) = xy = id(x)\,id(y)$

$\mathbb{1}(x) \triangleq 1$ 完全积性

$e(x) = \begin{cases} 1, & x=1 \\ 0, & x>1 \end{cases}$ 完全积性

$\varphi(n)$ 是积性?

$\varphi(n)$ = $1 \sim n$ 中与 n 互质的数的个数. $n = p_1^{a_1} \cdots p_k^{a_k}$, p_i 质

$1 \sim n$ 中含 p_1 的倍数 $\frac{n}{p_1}$ $n \to n - \frac{n}{p_1} = n(1-\frac{1}{p_1})$

再减 $n(1-\frac{1}{p_1})$ 减去 p_2 的 $\cdots$ $n(1-\frac{1}{p_1})(1-\frac{1}{p_2})$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$n = p_1^{a_1} \cdots p_k^{a_k}$

$m = q_1^{b_1} \cdots q_t^{b_t}$ (p_i, q_j 两两不同)

$(n, m) = 1$

$\varphi(nm) = nm\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_t}\right)$

$= \varphi(n)\,\varphi(m)$

$d_0(n)$ 因数个数 $\}$ 积性

$d_1(n)$ 因数和 $\}$ 积性

Def 给定 f, g 令 $h(n) = \sum_{d \mid n} f(d) \cdot g\left(\frac{n}{d}\right)$

称 h 为 f 和 g 的 (狄利克雷) 卷积.

记作 $h = f * g$

prop 若 f, g 积性. 则 $h = f * g$ 也积性.

$\forall x \perp y$. $h(xy) = \overset{f,g\text{积性}}{=}$

eg. 因数个数

$d_0(n) = \sum_{d \mid n} \mathbb{1}(d) \cdot \mathbb{1}\left(\frac{n}{d}\right)$

$d_0 = \mathbb{1} * \mathbb{1}$

因数和 $d_1(n) = \sum_{d \mid n} id(d) \cdot \mathbb{1}\left(\frac{n}{d}\right)$ $d_1 = id * \mathbb{1}$

因数和的因数和 $d_2(n) = \sum_{d \mid n} d_1(d) \cdot \mathbb{1}\left(\frac{n}{d}\right)$ $d_2 = d_1 * \mathbb{1}$.

Thm. $\boxed{\varphi * \mathbb{1} = id} \Leftrightarrow \boxed{\sum_{d \mid n} \varphi(d) = n}$

设 $n = p_1^{a_1} \cdots p_k^{a_k}$. 只要能算 $f(p_1^{a_1}) \cdots f(p_k^{a_k}) \Rightarrow f(n)$

f 积性

$\Rightarrow f$ 积性. 只要知道 $f(p^c)$ 的值

i.e. 只需证明 $(\varphi * \mathbb{1})(p^c) = id(p^c)$

$\forall$ 质 p. $c \geq 0$

$(\varphi * \mathbb{1})(p^c) = \varphi(p^0) + \varphi(p^1) + \cdots + \varphi(p^c)$

$\varphi(p^k) = \begin{cases} 1, & k = 0 \\ -p^{k-1} + p^k, & k \geq 1 \end{cases}$

$= 1 - 1 + p - p + p^2 + \cdots - p^{c-1} + p^c = p^c = id(p^c)$

Def 对 $n = p_1^{a_1} \cdots p_k^{a_k}$ 令

$$\mu(n) = \begin{cases} 1, & n=1 \ (k=0) \\ 0, & \exists i.\ a_i \geq 2 \ (\exists p.\ p^2 \mid n) \\ (-1)^k & n = p_1 \cdots p_k \ (a_1 = \cdots = a_k = 1) \end{cases}$$

定义 μ 为积性函数. 满足

$$\mu(p^c) = \begin{cases} 1, & c=0 \\ -1, & c=1 \\ 0, & c \geq 2 \end{cases}$$

$$\mu(p_1^{a_1} \cdots p_k^{a_k}) = \mu(p_1^{a_1}) \cdots \mu(p_k^{a_k})$$

$$e(n) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases} = [n=1]$$

Mobius 反演的核心内容：$\mu * \mathbb{1} = e$

莫比乌斯

pf: $(\mu * \mathbb{1})(p^c) = \mu(p^0) + \mu(p^1) + \cdots$

$= 1$ $\quad c=0$

$= e(p^c)$

$= 0$ $\quad c \geq 1$

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & n=1 \\ 0, & n>0 \end{cases} = [n=1]$$

构造

prop. $\boxed{\mu * id = \varphi}$

pf1 代 p^c.

pf2: $\varphi(n) = \sum_{i=1}^{n} [(i,n)=1] = \sum_{i=1}^{n} \sum_{d \mid \frac{n}{d}, d \mid i} \mu(d)$ $\quad \mu * \mathbb{1} = e$

$$= \sum_{d \mid n} \mu(d) \sum_{d \mid i}^{i \leq n} 1 = \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$$

$\sum_{d \mid i}^{i \leq n} 1 = \frac{n}{d}$

$\varphi = \mu * id$

$d \mid (a,b) \Leftrightarrow d \mid a$ 且 $d \mid b$

$n \sim$ les. $f \sim$ les $\quad d \mid a, d \mid b$

$(a,b)=d \iff \left(\frac{a}{d},\frac{b}{d}\right)=1$

eg. $\sum_{i=1}^{n}(i,n)$

枚举 n 次

$$=\sum_{d\mid n} d\cdot\sum_{i=1}^{\frac{n}{d}}\left[(id,n)=d\right]$$

$$=\sum_{d\mid n} d\cdot\sum_{i=1}^{\frac{n}{d}}\left[\left(i,\frac{n}{d}\right)=1\right]$$

$i\le\left\lfloor\frac{n}{d}\right\rfloor$

$$=\sum_{d\mid n} d\sum_{i=1}^{\frac{n}{d}}1\sum_{e\mid i,\ e\mid\frac{n}{d}}\mu(e)$$

$$=\sum_{d\mid n} d\sum_{e\mid\frac{n}{d}}\mu(e)\cdot\underbrace{\sum_{e\mid i,\ i\le\frac{n}{d}}1}_{\frac{n}{de}}=\sum_{d\mid n}\frac{d}{}\sum_{e\mid\frac{n}{d}}\mu(e)\cdot\frac{n}{de}$$

$T=de$, $e=\frac{T}{d}$

$$=\sum_{T\mid n}\frac{n}{T}\underbrace{\sum_{d\mid T} d\cdot\mu\left(\frac{T}{d}\right)}_{\varphi(T)}=\sum_{T\mid n}\frac{n}{T}\varphi(T)$$

"线性筛" $\to O(n)$. $\varphi(1)\sim\varphi(n)$, $\mu(1)\sim\mu(n)$

$O(q\cdot d_0(n))$

$n\le m$

$O(n)$

$f(1)\sim f(m)$ 已知.

eg. $\sum_{i=1}^{n}\sum_{j=1}^{m} f(\gcd(i,j))$ 每组询问 n 不一样

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

$i=i'd$, $i'\le\left\lfloor\frac{n}{d}\right\rfloor$

$j=j'd$, $j'\le\left\lfloor\frac{m}{d}\right\rfloor$

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

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

$i:1\sim\left\lfloor\frac{n}{d}\right\rfloor$ 里是 e 倍数 $\left\lfloor\frac{\lfloor\frac{n}{d}\rfloor}{e}\right\rfloor=\left\lfloor\frac{n}{de}\right\rfloor$

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

令 $T=de$

$$=\sum_{T=1}^{n}\left\lfloor\frac{n}{T}\right\rfloor\left\lfloor\frac{m}{T}\right\rfloor\underbrace{\sum_{d\mid T} f(d)\cdot\mu\left(\frac{T}{d}\right)}_{(f*\mu)(T)}=\sum_{T=1}^{n}\left\lfloor\frac{n}{T}\right\rfloor\left\lfloor\frac{m}{T}\right\rfloor g(T)$$

Prop $\left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor$

$a = kb + r. \quad 0 \le r < b$

$\lfloor \frac{a}{b} \rfloor = k = pc + q. \quad 0 \le q < c$

$\left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor = p.$

$a = kb + r = (pc+q)b + r = pbc + qb + r$

$\lfloor \frac{a}{bc} \rfloor = p + \lfloor \frac{qb+r}{bc} \rfloor = p$

$qb + r \le (c-1)b + b - 1 = bc - 1 < bc$

$q \le c-1 \quad r \le b-1$

$\Rightarrow \sum_{T=1}^{n} \lfloor \frac{n}{T} \rfloor \lfloor \frac{m}{T} \rfloor g(T)$

若已知 $f(1 \sim n) \cdot g(1 \sim n) \quad h = f * g$

$O(n \lg n)$ 求 $h(1 \sim n)$

$h(n) = \sum_{d \mid n} f(d)\, g(\frac{n}{d})$ $\quad \frac{n}{d} = e$

```
h(i)=0
for( d = 1 .. n)
    for(e = 1 ... ⌊n/d⌋)  h(de) += f(d) g(e)
```

$O(n + \frac{n}{2} + \frac{n}{3} + \dots \frac{n}{n}) = O(n \lg n)$

Thm. $\lfloor \frac{n}{i} \rfloor$ 当 $i = 1 \dots n$ 只有 $O(\sqrt{n})$ 种取值

① $i \le \sqrt{n}$ $\lfloor \frac{n}{i} \rfloor$ 只有 $O(\sqrt{n})$

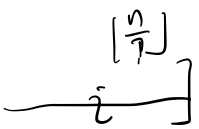
② $i > \sqrt{n}$ $\lfloor \frac{n}{i} \rfloor < \sqrt{n}$ 只有 $O(\sqrt{n})$

对 $d=\lfloor \frac{n}{i} \rfloor$，算有哪些 j 满足 $\lfloor \frac{n}{j} \rfloor = d$

$\lfloor \frac{n}{i} \rfloor = d \Leftrightarrow id \le n \le id+i-1$

$\lfloor \frac{n}{j} \rfloor = d \quad jd \le n \le jd+j-1$

$j \le \lfloor \frac{n}{d} \rfloor = \lfloor \frac{n}{\lfloor \frac{n}{i} \rfloor} \rfloor$



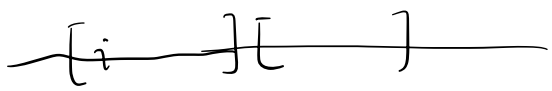
算 $1\sim n$ 中 $\lfloor \frac{n}{i} \rfloor$ 取值为多少种值对应 for i 的写法

```
for(i=1; i<=n; i=⌊n/⌊n/i⌋⌋+1)
```

$\lfloor \frac{n}{\lfloor \frac{n}{i} \rfloor} \rfloor$ // $O(\sqrt{n})$

$\forall j \in [i, \lfloor \frac{n}{\lfloor \frac{n}{i} \rfloor} \rfloor]$

$\lfloor \frac{n}{j} \rfloor = \lfloor \frac{n}{i} \rfloor$



$n \le m$

$\sum_{i=1}^{n} \lfloor \frac{n}{i} \rfloor \lfloor \frac{m}{i} \rfloor g(i)$

```
for(i=1; i<=n; i=min(⌊n/⌊n/i⌋⌋, ⌊m/⌊m/i⌋⌋)+1)   ← O(√n+√m)
// l=i, r=i.
ans += ⌊n/i⌋⌊m/i⌋ (g(l)+...+g(r))
```

$\forall i \in [l, r]$ $\lfloor \frac{n}{i} \rfloor$ $\lfloor \frac{m}{i} \rfloor$ 值一样

$O(\sqrt{n})$

数论分块

$f*\mu = g$

$O(n \lg n + q\sqrt{n})$

"线性筛"

思想：每个数：有 i 为其最小质因子时筛去

传统筛 for(i=2...n) if(i是质数) for(j=i...$\lfloor \frac{n}{i} \rfloor$) (i×j) 设为合数

$O(n \lg \lg n)$

np(i)：i 是合数

c=0

```
for( i=2...n)
{
  if( !np(i)) p[++cnt]=i;        i*pj
  for( j=1 ; j<=cnt && i*pj<=n ; j++)
  {
    np(i*pj)=1;                  → 1次
    if(i%pj==0) break;           → 保证 每个数 只在 最小的 pj 处筛掉
  }
}
```

$O(n) \longrightarrow \mu(p^c)=\begin{cases}1, & c=0\\ -1, & c=1\\ 0, & c>1\end{cases}$

$\varphi(p_1^{a_1}\cdots p_k^{a_k})=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

```
for( i=2...n)
{
  if( !np(i)) p[++cnt]=i, μ(i)=i-1, φ(i)=i-1;
  for( j=1 ; j<=cnt && i*pj<=n ; j++)
  { int x=i*pj ;  // μ(x)
    np(x)=1;
    if(i%pj==0)  // pj^2 | x
    { μ(x)=0; φ(x)=φ(i)*pj;
      break;
    }
    else { μ(x)=-μ(i) . φ(x)=φ(i)(pj-1) }
  }
}
```

μ(x)　　$f(p^c)$

预算 $p_j \mid i$ 的 $f(i\cdot p_j)$

p_j 是 x 最小质因子.

$g(x)=g(i)\cdot p^s$　　$h(x)=h(i)+1$

$p_j^?$ 和 p_j 无关

$x=g(x)$　$\frac{x}{g(x)}$

$f(x)=f(g(x))\cdot f\left(\frac{x}{g(x)}\right)$

$n=p_1^{a_1}\cdots p_k^{a_k}$, $p_1<\cdots<p_k$

$g(n)=p_1^{a_1}$

基本定义

- 好请让我们速成莫比乌斯反演
- 首先介绍一些概念。
- 数论函数，就是正整数映射到非负整数的函数。
- 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

常见积性函数

- 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

- 重要结论：两个积性函数的(狄利克雷)卷积还是积性函数

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

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

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：

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

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

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

$$= \sum_{T=de=1}^{n} \left\lfloor \frac{n}{T} \right\rfloor \left\lfloor \frac{m}{T} \right\rfloor g(T)$$

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：

```
1 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：

```
1  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
```

杜教筛

杜教筛

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

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：

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

杜教筛

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：$\sum_{i=1}^{n} i\phi(i)$

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

$$\sum_{i=1}^{n}\sum_{d|i} i\phi(d) = \sum_{i=1}^{n}\left(i\phi(i) + \sum_{d|i,d\neq i} i\phi(d)\right)$$

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

$$= S(n) + \sum_{k=\frac{i}{d}=2}^{n} \sum_{dk\leq n} \phi(d)dk$$

$$= S(n) + \sum_{k=\frac{i}{d}=2}^{n} k \sum_{dk\leq n} \phi(d)d$$

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

然后就没了。

如何构造杜教筛卷积：贝尔函数

清華大學
Tsinghua University

感谢