初等数论

h10

2018 年 1 月 9 日

简介

初等数论是研究数的规律，特别是整数性质的数学分支。它是数论的一个最古老的分支。它以算术方法为主要研究方法，主要内容有整数的整除理论、同余理论、连分数理论和某些特殊不定方程。换言之，初等数论就是用初等、朴素的方法去研究数论。

带余除法与整除

带余除法就是带有余数的除法，被除数=除数*商+余数。

带余除法定理：设 $a, b \in Z; a \geq b; b \neq 0$，则存在唯一的整数对 (q, r) 可以使得 $a = bq + r$，其中 $0 \leq r < |b|$

整除则代表着带余除法中 $r = 0$ 的特殊情况，若 $a = bq + 0$ 则称 “b 整除 a” 或 “a 能被 b 整除”，记为 $b|a$

取整

下取整在数学中一般记作 $\lfloor x \rfloor$，在计算机科学中一般记作floor(x)，表示不超过x的整数中最大的一个

上取整在数学中一般记作 $\lceil x \rceil$，在计算机科学中一般记作ceil(x)，表示不小于x的整数中最小的一个

显然带余除法中的 q 就是 $\lfloor \frac{a}{b} \rfloor$

$$\lceil \frac{a}{b} \rceil = \lfloor \frac{a+b-1}{b} \rfloor$$
$$\lfloor \frac{a}{b} \rfloor = \lceil \frac{a-b+1}{b} \rceil$$

取整

$$a > \left\lfloor \frac{c}{b} \right\rfloor \Leftrightarrow ab > c$$

$$a < \left\lceil \frac{c}{b} \right\rceil \Leftrightarrow ab < c$$

$$a \leq \left\lfloor \frac{c}{b} \right\rfloor \Leftrightarrow ab \leq c$$

$$a < \left\lfloor \frac{c}{b} \right\rfloor \Leftrightarrow ab < c - b + 1$$

$$a \geq \left\lceil \frac{c}{b} \right\rceil \Leftrightarrow ab \geq c$$

$$a > \left\lceil \frac{c}{b} \right\rceil \Leftrightarrow ab > c + b - 1$$

最大公约数与最小公倍数

顾名思义，最大公因数是指两个或多个整数共有约数中最大的一个，最小公倍数是指两个或多个整数共有倍数中最小的一个

a 与 b 的最大公因数记为 $gcd(a, b)$

a 与 b 的最小公倍数记为 $lcm(a, b)$

$$lcm(a, b) = \frac{ab}{gcd(a,b)}$$

$$lcm(a, b, c) = \frac{abc}{gcd(a,b,c)^2}$$

$$ab = gcd(a, b) lcm(a, b)$$

$$\frac{a}{gcd(a,b)} \frac{b}{gcd(a,b)} = \frac{lcm(a,b)}{gcd(a,b)}$$

欧几里得算法

欧几里德算法又称辗转相除法，用于计算两个正整数 a, b 的最大公约数

即利用 $gcd(a, b) = gcd(b, a \ mod \ b)$ 的性质递归求解 $gcd(a, b)$

当递归至 $b = 0$ 时 a 就是答案

拓展欧几里得算法

给定 a, b, c，求关于 x, y 的方程 $ax + by = c$ 的任意一组解

只有 $gcd(a, b)|c$ 时有解

假设我们已经求出了 $b * x0 + (a \ mod \ b) * y0 = c$ 对于 $x0, y0$ 的解

则 $b * x0 + (a - \lfloor \frac{a}{b} \rfloor b) * y0 = c$

$a * y0 + b * (x0 - \lfloor \frac{a}{b} \rfloor y0) = c$

所以 $x = y0, y = x0 - \lfloor \frac{a}{b} \rfloor y0$

当递归至 $b = 0$ 时显然 $x = \frac{c}{a}, y = 0$

类欧几里得算法

给定 n, a, b, c，求

$$f(n, a, b, c) = \sum_{i=0}^{n} \lfloor \frac{ai + b}{c} \rfloor$$

$n <= 10^{18}$

除了上式外还有很多可以用类欧几里得算法计算的公式，由于篇幅原因在此不讲了，传送门http://blog.csdn.net/werkeytom_ftd/article/details/53812718

类欧几里得算法

如果 $a >= c$，就先取下模

$$f(n,a,b,c)=\sum_{i=0}^{n}\lfloor\frac{ai+b}{c}\rfloor$$
$$=\sum_{i=0}^{n}\sum_{j=0}^{\lfloor\frac{ai+b}{c}\rfloor-1}1$$
$$=\sum_{j=0}^{\lfloor\frac{an+b}{c}\rfloor-1}\sum_{i=0}^{n}[j<\lfloor\frac{ai+b}{c}\rfloor]$$

类欧几里得算法

$$
\begin{aligned}
&= \sum_{j=0}^{\lfloor \frac{an+b}{c} \rfloor - 1} \sum_{i=0}^{n} [cj < (ai+b) - c + 1] \\
&= \sum_{j=0}^{\lfloor \frac{an+b}{c} \rfloor - 1} \sum_{i=0}^{n} [\lfloor \frac{cj+c-b-1}{a} \rfloor < i] \\
&= \sum_{j=0}^{\lfloor \frac{an+b}{c} \rfloor - 1} (n - \lfloor \frac{cj+c-b-1}{a} \rfloor) \\
&= n * \lfloor \frac{an+b}{c} \rfloor - f(\lfloor \frac{an+b}{c} \rfloor - 1, c, c-b-1, a)
\end{aligned}
$$

质数

质数的定义：一个大于1的自然数，除了1和它自身外，不能被其他自然数整除的数叫做质数；否则称为合数

质数的性质：

1.质数的个数是无穷的

2.若 a 为大于 1 的整数，在区间 $(a, 2a]$ 中必存在至少一个质数

3.若 n 为正整数，在 n^2 到 $(n+1)^2$ 之间至少有一个质数

4.若 n 为大于 1 的整数，在 n 到 $n!$ 之间至少有一个质数

5.质数的个数公式 $\pi(n)$ 约等于 $\frac{n}{log(n)}$

判断质数

1.定义法 $O(n)$

2.试除法 $O(\sqrt{n})$

3.预处理版试除法：预处理 $O(\sqrt{n})$，查询 $O(\frac{\sqrt{n}}{log(n)})$

4.概率优化：大于等于5的质数模6一定等于1或5

5.Miller-Rabin：$O(log^2(n))$，基于费马小定理的非确定性算法，等讲完费马小定理再讲

大数质因数分解 Pollard-rho

Pollard-rho算法的流程是先判断当前数 n 是否是素数，是则直接返回，否则试图找到当前数的一个因子 p，然后递归 p 与 $\frac{n}{p}$

定义函数 $f(x)$ 为 $[0,n)$ 向 $[0,n)$ 的一个随机映射

设 $x1$ 为一个 $[0,n)$ 内的随机数，令 $x2=f(x1)$

不停执行以下操作：

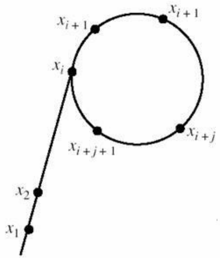
1.令 $p=gcd(|x1-x2|,n)$ 若 $p\neq 1$ 那么 p 就是 n 的一个因子并退出

2.令 $x1=f(x1),x2=f(f(x2))$

3.若 $x1=x2$ 那么说明陷入了循环，换一个新的随机函数 f 与一个新的 $x1$，并令 $x2=f(x1)$

大数质因数分解 Pollard-rho

为什么 $x1 = x2$ 就陷入了循环呢，因为如果将 $x, f(x), f(f(x)), \ldots$ 这整个轨迹画出来，那么一定会形成一个 ρ 型的环，如果 $x1, x2$ 相差的步数正好是环的大小，那么它们就会在次重叠，此时也正好会进入循环



快于线性筛的求质数个数方案

定义 $\pi(n)$ 表示区间 $[1, n]$ 内的质数个数，有没有比 $O(n)$ 的线性筛更快的做法？

设 $f(n, m)$ 表示区间 $[1, n]$ 内不包含因子 $p_1, p_2, ..., p_m$ 的数字的个数，则有

$$f(n, m) = f(n, m-1) - f(\lfloor \frac{n}{p_m} \rfloor, m-1)$$

可以看出计算 $f(n, m)$ 的复杂度为 $O(m * n^{\frac{1}{2}})$

快于线性筛的求质数个数方案

令 $k=n^{\frac{1}{3}}$，再设 $P_r(n,m)$ 表示区间 $[1,n]$ 内最小质因子大于 p_m 且有 r 个质因子的数的个数，那么有

$$\pi(n)=\pi(k)+f(n,\pi(k))-1-P_2(n,\pi(k))$$

$P_2(n,m)$ 的计算方案如下

$$P_2(n,m)=\sum_{p_m<d\le n^{\frac{1}{2}},d\ \ is\ \ prime}\pi(\lfloor\frac{n}{d}\rfloor)-\pi(d-1)$$

可以看出计算 $P_2(n,\pi(k))$ 的复杂度为 $O(\frac{n}{k})$

于是总复杂度为 $O(\pi(k)*n^{\frac{1}{2}}+\frac{n}{k})=O(\frac{n^{\frac{5}{6}}}{log(n)})$

快于线性筛的求质数个数方案

还能更快

令 $k = n^{\frac{1}{4}}$，则有

$$\pi(n) = \pi(k) + f(n, \pi(k)) - 1 - P_2(n, \pi(k)) - P_3(n, \pi(k))$$

$P_3(n, m)$ 的计算方案如下

$$P_3(n, m) = \sum_{p_m < d \le n^{\frac{1}{3}}, d \ \ is \ \ prime} P_2(\lfloor \frac{n}{d} \rfloor, \pi(d-1))$$

快于线性筛的求质数个数方案

虽然我们需要多次计算 $P_2(n,m)$，但是如果我们先 $O(\frac{n}{k})$ 预处理出所有的 $\forall_{p_{\pi(k)}<d\le n^{\frac{1}{2}},d\ \ is\ \ prime}\pi(\lfloor\frac{n}{d}\rfloor)$，那么单次计算 $P_2(n,m)$ 的复杂度为 $O(n^{\frac{1}{2}})$

由于 $O(\sum_{d\le n^{\frac{1}{3}},d\ \ is\ \ prime}\sqrt{(\frac{n}{k})})=O(n^{\frac{2}{3}})$，所以总复杂度为 $O(n^{\frac{3}{4}})$

还可以更快，the Meissel, Lehmer, Lagarias, Miller, Odlyzko method，感兴趣的同学可以课后了解一下

模运算

$$a \bmod b = a - \lfloor \frac{a}{b} \rfloor b$$

同余的定义

$$a \equiv b \pmod{p} \Leftrightarrow a \ mod \ p = b \ mod \ p$$

线性同余方程

求解关于 x 的方程 $ax \equiv b \pmod{p}$

转换为 $ax + kp = b$, 用拓展欧几里得算法即可

中国剩余定理

求解关于 x 的方程 $\forall i \in [0, k], x \equiv x_i \pmod{m_i}$

$$M = \Pi_{i=1}^{k} m_i$$

$$M_i = \frac{M}{m_i}$$

$$M_i \times M_i^{-1} \equiv 1 \pmod{m_i}$$

$$x \equiv \sum_{i=1}^{k} x_i \times M_i \times M_i^{-1} \pmod{M}$$

组合数取模（Lucas定理）

$$\binom{n}{m} \equiv \binom{\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{m}{p} \rfloor} \binom{n \bmod p}{m \bmod p} \pmod{p}$$

费马小定理

假如 p 是质数，且 $gcd(a,p)=1$，那么 $a^{p-1}\equiv 1 \pmod p$

注意费马小定理的反定理是错的，但是错误概率不大

Miller-Rabbin算法：如果 $a^{p-1}\equiv 1 \pmod p$（a 为任意小于 p 的正整数）则可近似认为 p 为素数

多次用不同的 a 来尝试 p 是否为素数，可以将错误率降低到可接受范围

Miller-Rabbin二次探测

为了提高检测效率，我们要经行二次探测优化，其原理是根据一个定理：如果 p 是一个素数，那么对于 $x(0 < x < p)$ ，若 $x^2 \equiv 1 \pmod p$，则 $x = 1$ 或 $x = p - 1$

进行如下操作

1.若 $a^{p-1} \not\equiv 1 \pmod p$，那么 p 不是质数，退出

2.令 $t = p - 1$

3.若 t 是奇数，那么 p 可能是质数，退出

4.若 $a^{\frac{t}{2}} \equiv -1 \pmod p$，那么 p 可能是质数，退出

5.若 $a^{\frac{t}{2}} \not\equiv 1 \pmod p$，那么 p 不是质数，退出

6.令 $t = \frac{t}{2}$，回到 3 操作

欧拉定理

对于正整数 n，令 $\varphi(n)$ 表示比 n 小的与 n 互质的数的个数，有

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

其中 $\varphi(n)$ 称为欧拉函数。

扩展欧拉定理

$$a^b \equiv \begin{cases} a^{b \ mod \ \varphi(p)} & gcd(a,p)=1 \\ a^b & gcd(a,p)\neq 1, b<\varphi(p) \\ a^{b \ mod \ \varphi(p)+\varphi(p)} & gcd(a,p)\neq 1, b\geq\varphi(p) \end{cases} \pmod p$$

例题

求

$$2^{(2^{(2^{\cdots})})} \mod p$$

1000组数据，$p \leq 10^7$

例题

令 $p = 2^k q$，其中 q 为奇数

则答案可以写成 $2^{(2^{(2^{\cdots})}-k)} \mod q$，此时可以用欧拉定理，求出 $2^{(2^{(2^{\cdots})})} \mod \varphi(q)$，在一直递归下去，直到 $\varphi(q) = 1$ 时返回 0

乘法逆元

对于整数 a, p，如果存在 x 满足 $ax \equiv 1 \pmod{p}$，那么 x 是 a 在模 p 下的乘法逆元

乘法逆元可以用扩展欧几里得求，解方程 $ax + bp = 1$ 即可

如果 $gcd(a, p) = 1$ 也可以用欧拉定理，$a * a^{\varphi(p)-1} \equiv 1 \pmod{p}$

RSA公钥系统

见
https://www.zhihu.com/question/48927324?sort=created

二次同余式

二次同余式是关于未知数的二次多项式的同余方程，形如

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

形如 $x^2 \equiv a \pmod{p}$ 的二次同余式则称为最简二次同余式

二次剩余

剩余类：所有与整数 a 模 p 同余的整数构成的集合叫做模 p 的一个剩余类,记作 $[a]$

二次剩余：假设 p 是素数，a 是整数，如果存在一个整数 x 使得 $x^2 \equiv a \pmod{p}$，那么就称 a 在 p 的剩余类中是二次剩余的

二次非剩余：（类似二次剩余）

a 是模 p 的二次剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

a 是模 p 的二次非剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

二次互反律

设 a, p 是两个非零整数，我们定义 $\left(\frac{a}{p}\right)$：若 a 是模 p 的二次剩余，则记 $\left(\frac{a}{p}\right) = 1$ 否则记 $\left(\frac{a}{p}\right) = -1$

二次互反律：设 p 和 q 为不同的奇素数，则

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

指数

对于两个互质的整数 a, p，定义 a 对模 p 的阶为最小的满足 $a^d \equiv 1 \pmod{p}$ 的正整数 d，记作 $\delta_p(a)$

显然 $\delta_p(a) | \varphi(p)$

定理：$\delta_p(a^k) = \frac{\delta_p(a)}{gcd(\delta_p(a), k)}$

推论：$gcd(\delta_p(a), k) = 1$ 时，$\delta_p(a^k) = \delta_p(a)$

求阶：因为 $\delta_p(a) | \varphi(p)$，暴力枚举 $\varphi(p)$ 的约数即可

原根及其存在条件

满足 $\delta_p(a)=\varphi(p)$ 的 a 称为 p 的原根

原根存在的条件：$2,4,p^k,2p^k$ 其中 p 表示奇质数，k 为任意自然数

原根的性质：

1.原根一旦有就有 $\varphi(\varphi(p))$ 个

2.设 p 是奇质数，g 是 p 的原根，则 g 或者 $g+p$ 是 p^2 的一个原根

3.设 p 是奇质数，k 是任意自然数，g 是 p^k 的一个原根，则 g 与 $g+p^k$ 中的奇数是 $2p^k$ 的一个原根

求原根：暴力枚举略

BSGS

求解关于 x 的方程 $a^x \equiv b \pmod{p}$，其中 a, b 与 p 互质

暴力自然是 $O(\varphi(p))$ 的

考虑使用BSGS，设一个参数 l，将 $a0, a1, a2, ..., a^{l-1}$ 存入hash表，然后枚举 $k \le \frac{\varphi(p)-1}{l}$，每次查询hash表中是否有 j 满足 $a^{kl+j} \equiv b \pmod{p}$，即 ba^{-kl} mod p

乘法逆元可以用拓展欧几里得算法求，当 p 为质数时则更简单

l 取 $\sqrt{\varphi(p)}$ 复杂度最优：预处理和单次查询都是 $O(\sqrt{\varphi(p)})$的，当然也可以根据具体情况调整 l 的大小

ExBSGS

如果 a, b 不与 p 互质呢？

原理很简单，我们需要把 a, p 变成互质的，每次取 $d = gcd(a, p)$，

如果 $d \not| b$，显然无解，否则把方程左右两边以及模数各除掉一个 d

那么方程 $a^x \equiv b \pmod p$ 就会变成 $\frac{a}{d} * a^{x-1} \equiv \frac{b}{d} \pmod{\frac{p}{d}}$

递归下去直到 $d = 1$，此时方程大概长这样：$a0 * a^{x-k} \equiv b0 \pmod{\frac{p}{0}}$，其中 $gcd(a, p0) = 1$，可以直接BSGS

如果 $x < k$ 怎么办？暴力枚举 x 很小的情况即可

例题：bzoj2219

给定自然数 A, B, K 求在 $[0, 2K]$ 之间满足 $x^A \equiv B \pmod{2K+1}$ 的 x 的个数

$A, B, 2K+1 \leq 10^9$

例题：bzoj2219

先把 $2K+1$ 分解成 $p_1^{a_1}p_2^{a_2}...p_k^{a_k}$

对所有单个方程 $x^A \equiv B \pmod{p_i^{a_i}}, x \in [0, p_i^{a_i}]$ 求解合法的 x 的个数，最终的答案是所有单个方程答案的乘积

求解单个方程见 http://blog.csdn.net/regina8023/article/details/44863519

积性函数

数论函数：定义域为正整数的函数

积性函数：$\forall gcd(a,b)=1$，满足 $f(ab)=f(a)f(b)$ 的函数

完全积性函数：对于任意 a,b，满足 $f(ab)=f(a)f(b)$ 的函数

积性函数的性质：如果 $f(x),g(x)$ 是积性函数，那么以下函数皆为积性函数

$1.h(x)=f(x^p)$

$2.h(x)=f^p(x)$

$3.h(x)=f(x)g(x)$

$4.h(x)=\sum_{d|x}f(i)g(\frac{x}{i})$

常见的积性函数

$$e(n) = [n = 1]$$
$$id(n) = n$$
$$1(n) = 1$$
$$\sigma_k(n) = \sum_{d|n} d^k$$
$$\varphi(n) = \sum_{i=1}^{n} [gcd(i, n) = 1]$$
$$\mu(n) = \begin{cases} 0 & \exists d > 1, d^2|n \\ (-1)^k & n = \prod_{i=1}^{k} p_i \end{cases}$$

常见积性函数的一些性质

$$\varphi(ab) = \varphi(a)\varphi(b)\frac{gcd(a,b)}{\varphi(gcd(a,b))} = \varphi(lcm(a,b))\varphi(gcd(a,b))$$

$$\sigma_0(ab) = \sum_{i|a}\sum_{j|b}[gcd(i,j) = 1]$$

狄利克雷卷积

定义两个数论函数 f, g 的狄利克雷卷积为

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

狄利克雷卷积的性质

交换律：$f * g = g * f$

结合律：$(f * g) * h = f * (g * f)$

分配律：$f * (g + h) = f * g + f * h$

单位元：$f * e = e * f = f$

常见的狄利克雷卷积

$$d(n) = \sum_{d|n} 1 \qquad \Leftrightarrow d = 1 * 1$$

$$\sigma(n) = \sum_{d|n} d \qquad \Leftrightarrow \sigma = d * 1$$

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \qquad \Leftrightarrow \varphi = \mu * Id$$

$$e(n) = \sum_{d|n} mu(d) \qquad \Leftrightarrow e = \mu * 1$$

容斥与反演

容斥原理

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k|$$

二项式反演

$$b_k = \sum_{i=0}^{k} (-1)^i \binom{k}{i} a_i \Leftrightarrow a_k = \sum_{i=0}^{k} (-1)^i \binom{k}{i} b_i$$

莫比乌斯反演

莫比乌斯反演

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

莫比乌斯反演的扩展形式

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

$$g(n)=\sum_{d\geq 1}f(\frac{n}{d})\Leftrightarrow f(n)=\sum_{d\geq 1}\mu(d)g(\frac{n}{d})$$

φ, μ前缀和

$$\phi(n)=\sum_{i=1}^{n}\varphi(i)=\sum_{i=1}^{n}(i-\sum_{d|i,d\neq i}\varphi(d))=\frac{n(n+1)}{2}-\sum_{i=2}^{n}\Phi(\lfloor\frac{n}{i}\rfloor)$$

$$M(n)=\sum_{i=1}^{n}\mu(i)=\sum_{i=1}^{n}([i==1]-\sum_{d|i,d\neq i}\mu(d))=1-\sum_{i=2}^{n}M(\lfloor\frac{n}{i}\rfloor)$$

预处理前 $n^{2/3}$ 项，更大的范围递归，$O(n^{2/3})$

可见杜教筛局限性较大，洲阁筛则可以在 $O(\frac{n^{\frac{3}{4}}}{\log(n)})$ 复杂度内求出大多数积性函数的前缀和

例题

求

$$F(i)=\sum_{i=1}^{n}\sum_{j=1}^{n}lcm(i,j)$$

$$n\le 10^{10}$$

例题

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

$$=\sum_{d=1}^{n}d\sum_{g=1}^{\lfloor\frac{n}{d}\rfloor}\mu(g)*g^2*S(\lfloor\frac{n}{dg}\rfloor)$$

$$=\sum_{g=1}^{n}\mu(g)*g^2\sum_{d=1}^{\lfloor\frac{n}{g}\rfloor}d*S(\lfloor\frac{n}{dg}\rfloor)$$

其中 $S(n)=(1+2+3+...+n)^2$

例题

很明显整除分块

其中 $\sum_{d=1}^{\lfloor\frac{n}{g}\rfloor} d * S(\lfloor\frac{n}{dg}\rfloor)$ 可以通过预处理前 $n^{\frac{2}{3}}$ 来做到 $O(n^{\frac{2}{3}})$

令 $t(n) = \mu(n) * n^2$，现在我们要做到快速求 t 的前缀和 T

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

$$\sum_{i=1}^{n}\sum_{d|i} t(i)(\frac{i}{d})^2 = \sum_{d=1}^{n} d^2 \sum_{i=1}^{\lfloor\frac{n}{d}\rfloor} t(d) = \sum_{d=1}^{n} d^2 T(\lfloor\frac{n}{d}\rfloor)$$

杜教筛即可