数论入门

陆明琪

清华大学

July 29, 2023

整除

若 $a = bk$，其中 a, b, k 都是整数，则称 b 整除 a，记做 $b|a$。也称 b 是 a 的约数（因数）、a 是 b 的倍数

整除

若 $a = bk$，其中 a, b, k 都是整数，则称 b 整除 a，记做 $b|a$。
也称 b 是 a 的约数（因数）、a 是 b 的倍数
若 $a|b$ 且 $a|c$，则 $a|b + c$
若 $a|b$ 且 k 为整数，则 $a|kb$

例子

枚举所有因数

例子

枚举所有因数
大于 $\sqrt{N}$ 的因数只有最多一个
所以只需要枚举小于等于 $\sqrt{N}$ 的因数

例子：小 L 的光

给出一排 n 盏灯的初始状态，用 1 来表示这个灯是暗的，用 0 表示这个灯是亮的。

每次可以操作一个开关，当操作第 i 个开关时，所有编号为 i 的约数（包括 1 和 i ）的灯的状态都会被改变。

问最少多少次操作能使所有灯都亮着。如果没有可行方案的话，输出 -1 。

例子：小 L 的光

给出一排 n 盏灯的初始状态，用 1 来表示这个灯是暗的，用 0 表示这个灯是亮的。

每次可以操作一个开关，当操作第 i 个开关时，所有编号为 i 的约数（包括 1 和 i）的灯的状态都会被改变。

问最少多少次操作能使所有灯都亮着。如果没有可行方案的话，输出 -1。

$n \le 10^5$

例子：小 L 的光

给出一排 n 盏灯的初始状态，用 1 来表示这个灯是暗的，用 0 表示这个灯是亮的。

每次可以操作一个开关，当操作第 i 个开关时，所有编号为 i 的约数（包括 1 和 i ）的灯的状态都会被改变。

问最少多少次操作能使所有灯都亮着。如果没有可行方案的话，输出 -1 。

$n \leq 10^5$

$n \leq 10^6$

例子：小 L 的光

给出一排 n 盏灯的初始状态，用 1 来表示这个灯是暗的，用 0 表示这个灯是亮的。

每次可以操作一个开关，当操作第 i 个开关时，所有编号为 i 的约数（包括 1 和 i ）的灯的状态都会被改变。

问最少多少次操作能使所有灯都亮着。如果没有可行方案的话，输出 -1 。

$n \leq 10^5$

$n \leq 10^6$

枚举因数 $\rightarrow$ 枚举倍数

$\sum_{i=1}^{n} \frac{n}{i} \approx n \ln(n)$

质数

若大于 1 的正整数 p 仅有两个因子 1 和 p，则称 p 是一个质数。否则，若 $p > 1$，则称 p 是一个合数。

质数

若大于 1 的正整数 p 仅有两个因子 1 和 p ，则称 p 是一个质数。
否则，若 $p > 1$ ，则称 p 是一个合数。
质数有无穷多个
不大于 n 的质数约有 $n/\ln(n)$ 个
每个数都可以被唯一分解为一些质数的乘积

唯一分解定理

每个数都可以被唯一分解为一些质数的乘积

把正整数 n 写成质数的乘积

$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$，其中 p 为互不相同的质数，这样的表示是唯一的

唯一分解定理

每个数都可以被唯一分解为一些质数的乘积

把正整数 n 写成质数的乘积

$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$，其中 p 为互不相同的质数，这样的表示是唯一的

质因数分解

质因数分解

https://www.luogu.com.cn/problem/P1075

例子：质因数分解

将 $N!$ 分解质因数
$N \leq 10^6$

例子：质因数分解

将 $N!$ 分解质因数
$N \leq 10^6$
只包含小于等于 N 的素数
素数 p 出现了多少次

例子：质因数分解

将 $N!$ 分解质因数
$N \leq 10^6$
只包含小于等于 N 的素数
素数 p 出现了多少次
$\lfloor \frac{N}{p} \rfloor + \lfloor \frac{N}{p^2} \rfloor + \lfloor \frac{N}{p^3} \rfloor + \cdots$
$\sum_i i * \#(ANS = i) = \sum_i \#(ANS \geq i)$

带余除法

对于整数 a, m，($m > 0$)，存在唯一的整数 q, r，满足 $a = qm + r$，其中 $0 \leq r < m$。称 q 为商，r 为余数

余数用 $a \bmod m$ 表示

同余

若两数 a, b 除以 c 的余数相等，则称 a, b 模 c 同余
记做 $a \equiv b \pmod{c}$

同余

若两数 a, b 除以 c 的余数相等，则称 a, b 模 c 同余
记做 $a \equiv b \pmod{c}$
$a \equiv b \pmod{c}$ 与 $c | a - b$ 等价
若 $a \equiv b, c \equiv d$，则有 $a + c \equiv b + d, ac \equiv bd$

最大公因数

设 a, b 是不都为 0 的整数，c 为满足 $c|a$ 且 $c|b$ 的最大整数，则称 c 是 a, b 的最大公约数，记为 (a, b)

若 $(a, b) = 1$ ，则称 ab 两数互质

最大公因数

设 a, b 是不都为 0 的整数，c 为满足 $c|a$ 且 $c|b$ 的最大整数，则称 c 是 a, b 的最大公约数，记为 (a, b)

若 $(a, b) = 1$ ，则称 ab 两数互质

$(a, b) = g \Leftrightarrow (a/g, b/g) = 1$

最大公因数

设 a, b 是不都为 0 的整数，c 为满足 $c|a$ 且 $c|b$ 的最大整数，则称 c 是 a, b 的最大公约数，记为 (a, b)

若 $(a, b) = 1$ ，则称 ab 两数互质

$(a, b) = g \Leftrightarrow (a/g, b/g) = 1$

$(a, b) = (a, a + b) = (a, ka + b)$

最大公因数

设 a, b 是不都为 0 的整数，c 为满足 $c|a$ 且 $c|b$ 的最大整数，则称 c 是 a, b 的最大公约数，记为 (a, b)

若 $(a, b) = 1$ ，则称 ab 两数互质

$(a, b) = g \Leftrightarrow (a/g, b/g) = 1$

$(a, b) = (a, a + b) = (a, ka + b)$

$(a, c) = 1$，$(a, b) = (a, cb)$

欧几里德算法

$(a, b) = (b, a \bmod b)$
递归求两数 gcd
复杂度 $O(\log n)$

欧几里德算法

$(a, b) = (b, a \bmod b)$
递归求两数 gcd
复杂度 $O(\log n)$
$a > b/2$
$a < b/2$

最大公因数的质因数分解

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$$

最大公因数的质因数分解

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$$
$$gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} p_3^{\min\{\alpha_3,\beta_3\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

最大公因数的质因数分解

$$
\begin{aligned}
&a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k} \\
&b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k} \\
&gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} p_3^{\min\{\alpha_3,\beta_3\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}} \\
&lcm(a, b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} p_3^{\max\{\alpha_3,\beta_3\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}
\end{aligned}
$$

最大公因数的质因数分解

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$$
$$gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} p_3^{\min\{\alpha_3,\beta_3\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$
$$lcm(a, b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} p_3^{\max\{\alpha_3,\beta_3\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}$$
$$a * b = gcd(a, b) * lcm(a, b)$$

最大公因数的性质

https://www.luogu.com.cn/problem/P3598

最大公因数的性质

https://www.luogu.com.cn/problem/P3598

$(x^a - 1, x^b - 1) = x^{(a,b)} - 1$

最大公因数的性质

https://www.luogu.com.cn/problem/P3598

$(x^a-1, x^b-1) = x^{(a,b)}-1$

不妨假设 $b<a$，数学归纳法对 a 进行归纳

$(x^a-1, x^b-1) = (x^a-1, x^a-x^b) = (x^a-1, x^b(x^{a-b}-1))$

最大公因数 + 整除

https://atcoder.jp/contests/agc046/tasks/agc046_a

最大公因数 + 质因数分解

https://www.luogu.com.cn/problem/P1029

最大公因数 + 质因数分解

https://www.luogu.com.cn/problem/P1372

Eratosthenes 筛

从小到大枚举处理 $i = 2 \sim n$，枚举到 i 时，若 i 未被标记则记 i 为质数，并且标记 i 的倍数不是质数。

时间复杂度：$O(n \log\log n)$

线性筛

DP 求 $1 \sim n$ 每个数的最小质因子 $f[i]$
枚举 $i = 2 \sim n$，枚举到 i 时若 $f[i]$ 尚未求出则 i 为质数，且 $f[i] = i$
然后枚举 $1 \sim f[i]$ 的所有素数 p，可以求得 $f[i * p] = p$
每个 $f[i]$ 只会被其最小质因数求一次，因此时间复杂度为 $O(n)$

线性筛

DP 求 $1 \sim n$ 每个数的最小质因子 $f[i]$
枚举 $i = 2 \sim n$，枚举到 i 时若 $f[i]$ 尚未求出则 i 为质数，且 $f[i] = i$
然后枚举 $1 \sim f[i]$ 的所有素数 p，可以求得 $f[i * p] = p$
每个 $f[i]$ 只会被其最小质因数求一次，因此时间复杂度为 $O(n)$
https://www.luogu.com.cn/problem/P3912

质因数分解

已知最小质因子为 $f[i]$
$O(\log n)$ 的质因数分解

质因数分解

已知最小质因子为 $f[i]$
$O(\log n)$ 的质因数分解
$n = n/f[n]$

线性筛 ++

https://oj.shiyancang.cn/Problem/781.html
$1 \leq L < R < 2^{31}, R-L \leq 10^6$

线性筛 ++

https://oj.shiyancang.cn/Problem/781.html

$1 \le L < R < 2^{31}, R - L \le 10^6$

考虑筛的是“最小”质因数，对于一个非质数，其最小质因数只有 $O(\sqrt{N})$ 级别

线性筛 ++

https://oj.shiyancang.cn/Problem/331.html

线性筛 ++

https://oj.shiyancang.cn/Problem/331.html

$gcd(n, (n-1)!)? = 1$

线性筛 ++

https://oj.shiyancang.cn/Problem/331.html
$gcd(n,(n-1)!)? = 1$
n 为质数：YES，否则：NO

线性筛 ++

https://oj.shiyancang.cn/Problem/331.html
$gcd(n,(n-1)!)? = 1$
n 为质数：YES，否则：NO
和上一题一样

Thanks

谢谢大家。