提高算法班

整除、质数、筛法、欧拉函数、最大公约数
最小公倍数、裴蜀定理、费马小定理

Mas

整除

设 $a,b \in \mathbb{Z}$, $a \neq 0$

若 $\exists q \in \mathbb{Z}$, 使得 $b = aq$ 则称 b 可被 a 整除 , 记作 $a \mid b$ 且 称 b 是 a 的倍数 也可称 a 是 b 的约数 (因数)

b 不被 a 整除 , 记作 $a \nmid b$

特殊地 0 是所有非 0 整数的倍数 , 即 $m \mid 0 \ (m \neq 0)$

对于整数 $b \neq 0$, b 的约数只有限个

平凡约数/因数

又称显然约数

对于整数 $b \neq 0$、 ± 1、 $\pm b$ 是 b 的显然约数

当 $b = \pm 1$ 时 , b 只有两个显然约数

对于整数 $b \neq 0$, b 的其他约数称为真约数 (真因数、非平凡约数、非平凡因数)

整除

整除的性质

- $a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b \Leftrightarrow |a| \mid |b|$
- $a \mid b \wedge b \mid c \Rightarrow a \mid c$
- $a \mid b \wedge a \mid c \Leftrightarrow \forall x, y \in \mathbb{Z}, a \mid (xb + yc)$
- $a \mid b \wedge b \mid a \Rightarrow b = \pm a$
- 设 $m \neq 0$，那么 $a \mid b \Leftrightarrow ma \mid mb$
- 设 $b \neq 0$，那么 $a \mid b \Rightarrow |a| \leq |b|$
- 设 $a \neq 0, b = qa + c$，那么 $a \mid b \Leftrightarrow a \mid c$

在具体问题中如无特别说明，约数总是指正约数

余数

设 a,b 为两个给定的整数 $a \neq 0$, d 是一个给定的整数

那么一定存在唯一的一对整数 q 和 r 满足

$$b = qa + r, d \leq r < |a| + d$$

无论整数 d 取何值 r 统称为**余数**

一般情况下 d 取 0 , 此时等式 $b = qa + r, 0 \leq r < |a|$ 称为**带余数除法**

如无特别说明 , 余数总是指最小非负余数

余数的性质

- 整数 b 被正整数 a 除后 , 余数一定是且仅是 $0 \sim a - 1$ 这 a 个数中的一个
- 相邻的 a 个整数被正整数 a 除后 , 恰好取到上述 a 个余数

  特别地 , 一定有且仅有一个数被 a 整除

质数

设整数 $p \neq 0, \pm 1$ 若 p 除了显然约数外没有其他约数，则称 p 为素数（不可约数）

若整数 $a \neq 0, \pm 1$ 且 a 不是素数，则称 a 为合数（p 和 $-p$ 总是同为素数或同为合数）

若无特别说明，素数总是指正的素数

整数的因数是素数,则该素数称为该整数的素因数 (素约数)

小于或等于 n 的素数的个数，用 $\pi(n)$ 表示

随着 n 的增大，有这样的近似结果： $\pi(n) \sim \frac{n}{\ln(n)}$

素数与合数的简单性质:

- 对于合数 a，一定存在素数 $p \leq \sqrt{a}$ 使得 $p \mid a$
- 素数有**无穷多**个
- 所有大于 3 的素数都可以表示为 $6n \pm 1 (n \in \mathbb{Z})$ 的形式

  任何整数都能表示为 $6n, 6n \pm 1, 6n \pm 2, 6n \pm 3$，其中 $6n, 6n \pm 2, 6n \pm 3$ 显然不为质数(**$6n \pm 1$ 不都为质数**)

质数

欧几里得《几何原本》片段：

欧几里得："对于任何有限的素数列表，至少有一个素数不在这个列表中"

证明

若质数数量有限，设 P 为一有穷质数集，记

$$S = \prod_{i \in \mathrm{P}} i$$

考虑数字 $S + 1$

若 $S + 1$ 为质数，说明存在不在 P 中的质数，与假设矛盾

若 $S + 1$ 不为质数，根据 **唯一分解定理** 必然存在质因子 $p \mid (S + 1)$

若 $p \in \mathrm{P}$

则 $p \mid (S + 1) \wedge p \mid S \Rightarrow p \mid 1$，显然不可能存在这样的 p，即 $p \notin P$

若 $p \notin \mathrm{P}$，说明存在不在 P 中的质数，与假设矛盾

命题得证

Eratosthenes 筛法

合数 一定可以写成 $p \times k$ 的形式，其中 p 是素数 k 是倍数$(k > 1)$

对于每一个 $1 \sim n$ 内的素数 p，枚举倍数 k $(k > 1)$，将 $p \times k$ 标记为合数

时间复杂度

$$O(\frac{n}{2} + \frac{n}{3} + \frac{\mathrm{n}}{5} + \cdots) = O(n \log \log n)$$

一些优化

- 仅筛至 $\sqrt{n}$
- 对于素数 p，只筛倍数 $x \geq p$ 的数

  若 $x < p$，则 x 中一定有比 p 小的素因子，$p \times x$ 会在前面筛选过程中被筛出
- 位级压缩

  可使用 vector < bool > 或 bitset 实现按位压缩标记减少内存占用

Euler 筛法

算法需保证每个合数仅被 **最小质因子** 筛除，可保证每个合数仅被筛一次

从下到大枚举 $2 \sim n$ 中的每一个数 i

- 若 i 是素数则加入素数表 p 中
- 顺序遍历素数表 p，利用 i 和 p 中素数 p_j 筛除 $i \times p_j$

  当 $p_j \mid i$ 时跳出循环（需先标记再跳出）

不重复

为确保仅被 **最小质因子** 筛除，仅需确保 p_j 为 $i \times p_j$ 中最小的质因子

即 i 中不能包含小于 p_j 的质因子

若 $p_j \mid i$ 有 $i = p_j \times x \Rightarrow \forall k > j$，$i \times p_k = x \times p_j \times p_k$

由于 $p_j < p_k$ 即 p_k 并非 $i \times p_k$ 最小质因子

所以当 $p_j \mid i$ 时不执行后续筛除，可保证合数仅被最小质因子筛除

```
void eulerSieve(int n)
{
  for (int i = 2; i <= n; i++)
  {
    if (!st[i])
      p[++pos] = i;
    for (LL j = 1; j <= pos && i * p[j] <= n; j++)
    {
      st[i * p[j]] = 1;
      if (i % p[j] == 0)
        break;
    }
  }
}
```

Euler 筛法

break 仅排除 非最小质因子 搭配时的情况，并非所有 $p \mid i$ 时

这也是为什么 $p \mid i$ 时，先标记再 break 的原因

借助该特性可同时求出 $2 \sim n$ 中所有数最小质因子

不遗漏

对于 $j < i$ 且 j 为合数 $j = p \times k$ 其中 p 为 j 的最小质因子显然 $p < i$ 同时也有 $k < i$

所以 j 将被 p 与 k 搭配筛除，既 $2 \sim i$ 的合数都被考虑

对于质数其显然不被标记，若遍历到 i 时未被标记则说明 i 为质数

不超过 i 的质数都已被加入质数表，既 $2 \sim i$ 的质数都被考虑

借助该特性，可在欧拉筛过程中进行顺序递推

综上欧拉筛不重不漏

时间复杂度 $O(n)$

#781、Prime Distance

题目描述

给定两个整数 L, R

求闭区间 $[L, R]$ 中相邻两个质数差值最小的数对与差值最大的数对

当存在多个时,输出靠前的素数对

输入格式

多组数据,每行两个数 L, R

输出格式

详见输出样例

样例输入

```
2 17
14 17
```

样例输出

```
2,3 are closest, 7,11 are most distant.
There are no adjacent primes.
```

数据范围

对于全部数据, $1 \leq L < R < 2^{31}, R - L \leq 10^6$

对于一个合数 x , 必然有一个质因子在 $[2, \sqrt{x}]$ 范围内

不妨预处理出 $[2, \sqrt{n}]$ 范围内所有质数

对于每个在 $[2, \sqrt{n}]$ 范围内的质数 p

其在 $[L, R]$ 范围内的最小倍数为

$$\max\left(2, \left\lceil \frac{L}{p} \right\rceil\right)$$

类似于埃氏筛处理出 $[L, R]$ 范围内的质数即可

算术基本定理

算术基本定理 (Fundamental theorem of arithmetic)

又称唯一分解定理

若整数 $N \geq 2$, 那么 N 一定可以唯一表示为若干素数的乘积 , 形如

$$N = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k} \ (p_i \in \mathbb{P}, p_1 < p_2 < \dots < p_k, c_i \geq 0)$$

算术基本引理

又称欧几里得引理

若 $p \in \mathbb{P} \wedge p \mid ab$ 那么 $p \mid a$ 和 $p \mid b$ 至少有一个成立

算术基本引理是素数的本质属性 , 也是素数的真正定义

证明

假设 $p \nmid a$, 根据质数性质显然有 $p \perp a$ 即 $(a, p) = 1$

根据 **裴蜀定理** 存在 $x, y \in \mathbb{Z}$

算术基本引理

$$ax + py = 1$$

两边同乘 b 可得

$$abx + bpy = b$$

由于 $p \mid ab$ 根据整除的性质

$$p \mid abx$$

即 $p \mid abx + bpy$ 即 $p \mid b$

同理可证 $p \nmid b$ 时 $p \mid a$

算术基本引理推论

若 p 为质数且 $p \mid \prod_{i=1}^{n} a_i$ ，那么至少存在一个 a_i 满足 $p \mid a_i$

不难通过数学归纳法证明

算术基本定理

存在性证明

设存在不能分解成有限个质数的乘积的合数，则其中必有一个最小数，设其为 n

$\exists\, a,b \in \mathbb{N}^+ \wedge 1 < a,b < n$ 满足 $n = ab$

- 若 a,b 都为质数

  与假设矛盾

- 若 a,b 至少有一个是合数

  因为 $1 < a,b < n$

  所以该合数可被分解成有限个质数乘积

  将乘积替换，可推出 n 可分解成有限个质数的乘积

  与假设矛盾

存在性成立

算术基本定理

唯一性证明

设存在某些数，它们能分解为两种 **根本不同** 的质数乘积

将其中最小的数设为 n（小于 n 的数都能被唯一分解）

$$n = p_1p_2p_3 \cdots p_r = q_1q_2q_3 \cdots q_s$$

不妨假设 $p_1 < p_2 < p_3 < \cdots < p_r$ ， $q_1 < q_2 < q_3 < \cdots < q_r$ 且有 $1 < p_1 < q_1$

记 $n' = n - p_1q_2q_3 \cdots q_s$

将 $n = p_1p_2p_3 \cdots p_r$ 代入有

$$n' = p_1p_2p_3 \cdots p_r - p_1q_2q_3 \cdots q_s = p_1(p_2p_3 \cdots p_r - q_2q_3 \cdots q_s) \qquad (1)$$

将 $n = q_1q_2q_3 \cdots q_s$ 代入有

$$n' = q_1q_2q_3 \cdots q_s - p_1q_2q_3 \cdots q_s = (q_1 - p_1)q_2q_3 \cdots q_s$$

由于 $p_1q_2q_3 \cdots q_s > 0 \Rightarrow n' < n$ 即 n' 能被唯一分解

算术基本定理

由 (1) 可知 p_1 为 n' 因子，所以 $p_1 \mid (q_1 - p_1)q_2q_3 \cdots q_s$

又由于 $p_1 < q_2 < q_3 < \cdots < q_r$ 且其都为质数

显然

$$p_1 \nmid q_2q_3 \cdots q_s$$

根据 **欧几里得引理** 推论

此时必有

$$p_1 \mid (q_1 - p_1)$$

即

$$kp_1 = (q_1 - p_1) \Rightarrow (k+1)p_1 = q_1$$

此时表明 p_1 为 q_1 因子，与 q_1 为质数矛盾

唯一性成立

另一形式证明算术基本定理: https://oj.shiyancang.cn/Public/25.html

算术基本定理

算术基本定理存在如下推论

N 的正约数的集合可以写作

$$p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k} \ (p_i \in \mathbb{P}, 0 \leq b_i \leq c_i)$$

N 的正约数个数为

$$(c_1 + 1) \times (c_2 + 1) \times \cdots \times (c_k + 1) = \prod_{i=1}^{k} (c_i + 1)$$

N 的正约数之和为

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{c_1}\right) \times \left(1 + p_2 + p_2^2 + \cdots + p_2^{c_2}\right) \times \cdots \times \left(1 + p_k + p_k^2 + \cdots + p_k^{c_k}\right) = \prod_{i=1}^{k} \sum_{j=0}^{c_i} p_i^j$$

#1696、阶乘分解

题目描述

给定整数 n

试把阶乘 $n!$ 分解质因数

按照底数 p_i 、指数 c_i 的形式输出分解结果

输入格式

一个整数 n

输出格式

$n!$ 分解质因数后的结果,共若干行

每行一对 p_i, c_i ,表示含有 $p_i^{c_i}$ 项

按照 p_i 从小到大的顺序输出

数据范围

对于全部数据 $1 \leq n \leq 10^6$

$n!$ 的质因子不超过 n

$n!$ 中质数 p 的指数为$1 \sim n$ 中包含因子 p 的个数

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

筛出 $2 \sim n$ 质数 p_i

对所有 p_i 求次数

Legendre 公式

Legendre 公式（**Legendre's formula**）

$n!$ 中质因子 p 出现次数记为 $v_p(n!)$

将 n 做 p 进制分解（$n = \sum_{i=0}^{k} \mathbf{d}_i p^i$）

令 $S_p(n) = \sum_{i=0}^{k} \mathbf{d}_i$

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - S_p(n)}{p - 1}$$

证明

仅证第二个等号

$$\left\lfloor \frac{n}{p^j} \right\rfloor = \mathbf{d}_k p^{k-j} + \mathbf{d}_{k-1} p^{k-j-1} + \cdots + \mathbf{d}_j$$

Legendre 公式

即 $\left\lfloor \frac{n}{p^j} \right\rfloor$ 表示截去 p 进制下 n 的最低 j 位的结果

那么

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \left(\mathbf{d}_k p^{k-1} + \mathbf{d}_{k-1} p^{k-2} + \cdots + \mathbf{d}_1\right) + \left(\mathbf{d}_k p^{k-2} + \mathbf{d}_{k-1} p^{k-3} + \cdots + \mathbf{d}_2\right) + \cdots + \left(\mathbf{d}_k p + \mathbf{d}_{k-1}\right) + \mathbf{d}_k$$

$$= \left(\mathbf{d}_k \sum_{i=0}^{k-1} p^i\right) + \left(\mathbf{d}_{k-1} \sum_{i=0}^{k-2} p^i\right) + \cdots + \mathbf{d}_2 (p+1) + \mathbf{d}_1$$

$$= \sum_{i=0}^{k} \left(\mathbf{d}_i \frac{p^i - 1}{p-1}\right) = \frac{1}{p-1}\left(\left(\sum_{i=0}^{k} \left(\mathbf{d}_i p^i\right)\right) - \left(\sum_{i=0}^{k} \mathbf{d}_i\right)\right)$$

$$= \frac{n - S_p(n)}{p-1}$$

最大公约数

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 $\gcd(a, b)$ 或 (a, b)

$$\gcd(a, b) = \gcd(b, a)$$

$$\gcd(a, b) = \gcd(-a, b)$$

$$\gcd(a, b) = \gcd(|a|, |b|)$$

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

$$\mathrm{d} \mid a \wedge d \mid b \iff \mathrm{d} \mid \gcd(a, b)$$

$$\gcd(a, 0) = a$$

$$\gcd(a, ka) = a$$

$$\gcd(an, bn) = n \gcd(a, b)$$

若 $\gcd(a, b) = 1$，称 a, b 互质，记为 $a \perp b$

上述性质证明见：https://oj.shiyancang.cn/Public/127.html

尝试证明

若 $a \perp b$，$\gcd(ab, k) = \gcd(a, k) \times \gcd(a, k)$

欧几里得算法

辗转相除法 / 欧几里得算法 (**Euclidean algorithm**) 算法核心为

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

证明

不妨设 $a > b$

若 $b \mid a$, 那么 $b = (a,b)$

若 b $\nmid a$, 即 $a = bq + r$, 其中 $0 \le r < b$

设 $a = bk + c$, 显然 $c = a \bmod b = a - bk$

设 $d \mid a$, $d \mid b$, 那么 $\frac{c}{d} = \frac{a}{d} - \frac{b}{d}k$

$\frac{a}{d}$ 、 $\frac{b}{d}$ 为整数$\Longrightarrow$ $\frac{c}{d}$ 也为整数 , 即 $d \mid c$

对于所有 a,b 的公约数,它也是 b , $a \bmod b$ 的公约数

在计算过程中若出现 $b = 0$

欧几里得算法

那么上一步为 $a \bmod b = 0$，本层的 a 即为所求

当 $a < b$ 时

$$\gcd(a, b) = \gcd(b, a \bmod b) = \gcd(b, a)$$

时间复杂度

- $a < b$

  此时 $\gcd(a, b) = \gcd(b, a)$

- $a \geq b$

  此时 $\gcd(a, b) = \gcd(b, a \bmod b)$

  $a \bmod b$ 将使得 a 至少折半

  当 $b \leq \frac{a}{2}$ 时显然成立

  当 $b > \frac{a}{2}$ 时 $\left\lfloor \frac{a}{b} \right\rfloor = 0$

欧几里得算法

$$\Rightarrow a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$$

即该过程至多发生 $O(\log a)$ 次

而 $a < b$ 发生后 $a \geq b$ 一定会发生

因此 $a < b$ 发生次数一定 不多于 $a \geq b$ 发生次数

综上时间复杂度 $O(\log \max(a, b))$

当求解 **斐波那契数列** 相邻两项的最大公约数，会使该算法达到最坏复杂度

另一形式证明与最坏情况分析见 https://oj.shiyancang.cn/Public/309.html

#2737、加值GCD

题目描述

给你两个正整数数组 $a_1, a_2, \cdots, a_n$ 和 $b_1, b_2, \cdots, b_m$

请你求出 $a_1 + b_i, a_2 + b_i, \cdots, a_n + b_i$ 的最大公约数

输入格式

第一行输入两个正整数 n, m

第二行输入 n 个正整数 a_i

第三行输入 m 个正整数 b_i

输出格式

输出 m 个数

第 i 行输出 $\gcd(a_1 + b_i, a_2 + b_i, \cdots, a_n + b_i)$

数据规模

对于 30% 的数据 $1 \leq n, m, \ a_i, b_j \leq 1000$

对于 100% 的数据 $1 \leq n, m \leq 2 \times 10^5, 1 \leq a_i, b_i \leq 10^{18}$

输入样例

```
4 4
1 25 121 169
1 2 7 23
```

输出样例

```
2
3
8
24
```

更相减损术

$$\forall a, \mathrm{b} \in \mathbb{N}, (a, b) = (b, a - b) = (a, a - b)$$

$$\forall a, b \in \mathbb{N}, (2a, 2b) = 2(a, b)$$

对于后者根据最大公约数的定义显然成立

对于a 与 b 任意公约数 d

$d \mid a, d \mid b \Rightarrow d \mid a - b$ 即 d 也是 b与 $a - b$的一个公约数

同理可证 $a, b - a$ 的情况

推广到多个数

$$(a_1, a_2, a_3, a_4, \cdots, a_n)$$

$$= (a_1, a_2 - a_1, a_3 - a_2, \cdots, a_n - a_{n-1})$$

#2737、加值GCD

要求 $(a_1 + b_j, a_2 + b_j, \cdots, a_n + b_j)$

根据结论有

$$(a_1 + b_j, a_2 + b_j, \cdots, a_n + b_j)$$

$$= (a_1 + b_j, a_2 + b_j - a_1 - b_j, \cdots, a_n + b_j - a_{n-1} - b_j)$$

$$= (a_1 + b_j, a_2 - a_1, \cdots, a_n - a_{n-1})$$

记 $(a_2 - a_1, \cdots, a_n - a_{n-1})$ 的值为 x

对于每一个 b_j，答案为 $(x, a_1 + b_j)$

为了避免出现负数，可将数组升序排序

最小公倍数

a 和 b 最小的正公倍数为 a 和 b 的**最小公倍数**,记作 $\mathrm{lcm}(a,b)$ 或 $[a,b]$

根据唯一分解定理

$$a = p_1^{k_{a_1}} p_2^{k_{a_2}} \cdots p_s^{k_{a_s}}, b = p_1^{k_{b_1}} p_2^{k_{b_2}} \cdots p_s^{k_{b_s}}$$

对于 a 和 b 根据定义

$$\gcd(a,b) = p_1^{\min(k_{a_1},k_{b_1})} p_2^{\min(k_{a_2},k_{b_2})} \cdots p_s^{\min(k_{a_s},k_{b_s})}$$

$$\mathrm{lcm}(a,b) = p_1^{\max(k_{a_1},k_{b_1})} p_2^{\max(k_{a_2},k_{b_2})} \cdots p_s^{\max(k_{a_s},k_{b_s})}$$

由于 $k_a + k_b = \max(k_a,k_b) + \min(k_a,k_b)$

即

$$(a,b)[\mathrm{a},\mathrm{b}] = ab$$

另一种形式证明上述结论: https://oj.shiyancang.cn/Public/24.html

#511、除法游戏

题目描述

小 A 和小 B 是一对好朋友,他们的爱好是研究数字

学过除法之后,他们就发明了一个新游戏:

两人各说一个数字分别为 a 和 b ,如果 a 能包含 b 的所有质数因子,那么 A 就获胜

但是当数字太大的时候,两个朋友的脑算速度就有点跟不上了

现在,请你写个程序,来判断胜负吧:

输入两个正整数,表示 a 和 b

如果 a 包含了 b 的所有质数因子,则输出 `Yes` ,否则输出 `No`

输入格式

输入两个正整数 a 和 b ,中间用一个空格隔开

输出格式

如果 a 包含了 b 的所有质数因子,则输出 `Yes` ,否则输出 `No`

数据规模

对于全部的数据 $2 \leq a, b \leq 10^{18}$

当$(a,b)=1$ 时显然不满足条件

当不满足条件时 设

$$a = p_1^{k_{a_1}} p_2^{k_{a_2}} \cdots p_s^{k_{a_s}} \ , b = p_1^{k_{b_1}} p_2^{k_{b_2}} \cdots p_s^{k_{b_s}} q$$

据定义 $(a,b) = p_1^{\min(k_{a_1},k_{b_1})} p_2^{\min(k_{a_2},k_{b_2})} \cdots p_s^{\min(k_{a_s},k_{b_s})}$

即 (a,b) 中包含 a,b 的公共因子

b 除以 (a,b) 仅会将 a,b 公共质因子指数减少

不断让 b 除以 (a,b) , 直到 $(a,b)=1$时停下

此时所有公共因子指数已变为 0

最后 b 就为 q

若不为 1 说明不满足条件

裴蜀定理

裴蜀定理（**Bézout's lemma**）是一个关于最大公约数的定理

若 $a, b \in \mathbb{N}$ 且 a, b 不同时为 0，存在 $x, y \in \mathbb{Z}$ 满足

$$ax + by = (a, b)$$

上述结论等价于

$$ax + by = 1 \Leftrightarrow (a, b) = 1$$

$ax + by = 1$ 等价于

$$ax \equiv 1 \pmod{b}$$

即 $(a, b) = 1$ 模 b 意义下必然存在整数意义的 a^{-1}

推论

- $ax + by = c$ 有解的充要条件为 $(a, b) \mid c$

  证明见 P46

- $ax + by = c$ 有解时必然有无穷多个整数解

裴蜀定理

证明

设 $a,b \in \mathbb{N}$ 且 $a \neq 0$，构造集合

$$S = \{ax + by : x,y \in \mathbb{Z}, ax + by > 0\}$$

容易发现 $S \subseteq \mathbb{N}^+$ 且 S 非空(若 $a > 0$ 则 $a \in S$；若 $a < 0$ 则 $-a \in S$)

根据自然数的良序公理，必然存在最小元素 $d \in S$

假设 $d \nmid a$，根据带余数除法性质存在

$$a = kd + r \ (r,k \in \mathbb{Z}, 0 < r < d)$$

带入 $d = ax + by$，整理得

$$r = a(1 - kx) + b(-ky)$$

显然 $r \in S$ 又由于 $r < d$ 与 d 为最小元素矛盾

所以 $d \mid a$

同理可证 $d \mid b$ 即 d 为 a,b 公约数

裴蜀定理

对于 a,b **任意**公约数 $d' \neq d$, 根据整除性质有

$$d' \mid a \wedge d' \wedge b \Rightarrow d' \mid ax+by$$

而 d 为 S 中元素(也为 $ax+by$ 形式) , 那么 $d' \mid d$

根据整除性质 $d' \mid d \Rightarrow d' \leq d$ 又由于$d' \neq d$

所以 $d' < d$

由于 d 为 S 中最小元素

所以 $d' \notin S$

即不存在整数 x,y 满足 $d' = ax+by$

综上存在唯一公约数 d 满足 $d = ax+by$ 有整数解

且 d 为所有公约数最大

得证

裴蜀定理

$ax+by=c$ 有解的**充要条件**为 $(a,b)\mid c$

对 $ax+by=(a,b)$ 将 x,y 同时扩大 $\frac{c}{(a,b)}$ 倍即可证明充分性

考虑其必要性

若存在 $ax+by=c$ 且 $(a,b)\nmid c$ 那么

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=\frac{c}{(a,b)}$$

其中 $\frac{a}{(a,b)},\frac{b}{(a,b)}y\in\mathbb{Z}$ 而 $\frac{c}{(a,b)}\notin\mathbb{Z}$ 显然矛盾

这意味这 裴蜀定理**逆定理** 也成立，即

若 $a,b\in\mathbb{N}$ 且 a,b 不同时为 0，存在 $x,y\in\mathbb{Z}$ 满足 $ax+by=d$ 同时有 $d\mid a$ 且 $d\mid b$

那么 $(a,b)=d$

#2747、裴蜀定理

题目描述

给定一个包含 n 个元素的**整数**序列 A，记作 $A_1, A_2, A_3, \ldots, A_n$

求另一个包含 n 个元素的待定**整数**序列 X，记 $S = \sum_{i=1}^{n} A_i \times X_i$，使得 $S > 0$ 且 S 尽可能的小

输入格式

第一行一个整数 n，表示序列元素个数。第二行 n 个整数，表示序列 A。

输出格式

一行一个整数，表示 $S > 0$ 的前提下 S 的最小值。

输入样例

```
2
4059 -1782
```

输出样例

```
99
```

说明

对于 100% 的数据，$1 \le n \le 20, |A_i| \le 10^5$，且 A 序列不全为 0。

当只有两项时，根据裴蜀定理答案为(A_1, A_2)

裴蜀定理可扩展到多项

答案为 $(A_1, A_2, A_3, \cdots, A_n)$

欧拉函数

欧拉函数（**Euler's totient function**），即 $\varphi(n)$ 表示小于等于 n 与 n 互质的数的个数

如 $\varphi(1) = 1, \varphi(8) = 4$

当 n 是质数的时候，显然有 $\varphi(n) = n - 1$

欧拉函数是 **积性函数**

函数 f 为积性函数，若 $(a,b) = 1$ 有 $f(nm) = f(n)f(m)$

若 $(n,m) = 1$ 有 $\varphi(nm) = \varphi(n)\varphi(m)$

当 n 为奇数时 $\varphi(2n) = \varphi(n)$

若 $n = p^k (p \in \mathbb{P})$，那么 $\varphi(n) = p^k - p^{k-1}$

对于 $1 \sim p^k$ 的所有整数中,除 p^{k-1} 个 p 的倍数外其它数都与 p^k 互质

故

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \times (p-1)$$

欧拉函数

若 $(n,m)=1$ 有 $\varphi(nm)=\varphi(n)\varphi(m)$

证明

构造包含 $1\sim nm$ 范围内整数的矩阵

$\varphi(nm)$ 即为矩阵内与 n,m 互质数的个数

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & mn \end{bmatrix}$$

每列都 $\bmod n$ 同余

根据最大公约数性质有 $(n,i)=(n,i+kn)$

那么 $(i,n)=1$ 则 $(i+kn,n)=1$

考虑第一行，其中有 $\varphi(n)$ 个元素与 n 互质，那么共有 $\varphi(n)$ 列且列内的数都与 n 互质

欧拉函数

同一列中的元素为 $r, r+n, r+2n, \cdots, r+(m-1)n$ 共 m 个元素

有 $\{0, 1, 2, \cdots, m-1\}$ 与 $\{r, r+n, r+2n, \cdots, r+(m-1)n\}$ 一一对应

若不然则存在 $0 \le i < j < m$ 且 $r+in \equiv r+jn \pmod m \Rightarrow in \equiv jn \pmod m$

由于 $(m,n)=1$ 则 n^{-1} 必然存在，同乘逆元则有 $i \equiv j \pmod m$，矛盾

即每一列中都有 $\varphi(m)$ 个元素与 m 互质

$\varphi(n)$ 列中的每一列都有 $\varphi(m)$ 个交点处的数都与 n, m 互质

这样的交点有 $\varphi(n) \times \varphi(m)$ 个，即

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

命题得证

欧拉函数

设

$$n = \prod_{i=1}^{s} p_i^{c_i} \ (c_i \in \mathbb{N}^+, p_i \in \mathbb{P})$$

有

$$\varphi(n) = n \prod_{i=1}^{s} \frac{p_i - 1}{p_i}$$

由唯一分解定理与欧拉函数的积性

$$\varphi(n) = \prod_{i=1}^{s} \varphi\left(p_i^{k_i}\right) = \prod_{i=1}^{s} \left(p_i^{k_i - 1}(p_i - 1)\right)$$

$$= \prod_{i=1}^{s} \left(p_i^{k_i}(1 - \frac{1}{p_i})\right) = \prod_{i=1}^{s} \left(p_i^{k_i}(\frac{p_i - 1}{p_i})\right)$$

$$= n \prod_{i=1}^{s} \frac{p_i - 1}{p_i}$$

#2397、最简分数

题目描述

求分子分母都不超过 n 且为真分数的最简分数有多少个

> *最简分数：分子分母互质的分数为最简分数*

输入格式

输入一行,输入一个整数 n

输出格式

输出一行,为所求的答案

样例输入

```
2
```

样例输出

```
1
```

数据规模

对于 10% 的数据 $1 \leq n \leq 1000$

对于 40% 的数据 $1 \leq n \leq 500000$

对于 100% 的数据 $1 \leq n \leq 10000000$

容易发现答案为

$$\sum_{i=2}^{n} \varphi(i)$$

对每个数分解质因数无法通过

考虑使用朴素埃氏筛优化

当枚举的数 p 为质数时 $2p, 3p, 4p, \ldots$为合数

对于每一个 $2p, 3p, 4p, \ldots$ 乘上 $\frac{p-1}{p}$ 即可

时间复杂度$O(n \log \log n)$

#2397、最简分数

在欧拉筛过程中

当 i 为质数时 $\varphi(i) = i - 1$

- 若 $p_j \mid i$

  i 的所有质因子其中必然包含了p_j

$$\varphi(i \times p_j) = i \times p_j \times \prod_{i=1}^{s} \frac{p_k - 1}{p_k} = p_j \times \varphi(i)$$

- 若 $p_j \nmid i$

  p_j 为质数 $(p_j, i) = 1$ 根据积性函数性质

$$\varphi(i \times p_j) = \varphi(p_j) \times \varphi(i) = (p_j - 1) \times \varphi(i)$$

时间复杂度 $O(n)$

#2397、最简分数

进一步的还存在如下性质

记 $\gcd(x,y)=d$

$$\varphi(x\times y)=\frac{\varphi(x)\times\varphi(y)\times d}{\varphi(d)}$$

证明

记 $P=\{p_1,p_2,\cdots,p_n\}$ 为 x 的质因子集合

$Q=\{q_1,q_2,\cdots,q_m\}$ 为 y 的质因子集合

记 $A=P\cap Q$ (A 为公共质因子集 , 其也为 d 的质因子集) , $B=P\cup Q$ (B 为 $x\times y$ 质因子集)

$$\varphi(x\times y)=x\times y\times\prod_{b\in B}\frac{b-1}{b}$$

#2397、最简分数

$$= x \times y \times \frac{\left(\prod_{p \in P} \frac{p-1}{p}\right) \times \left(\prod_{q \in Q} \frac{q-1}{q}\right)}{\prod_{a \in A} \frac{a-1}{a}}$$

$$= \frac{x \times \left(\prod_{p \in P} \frac{p-1}{p}\right) \times y \times \left(\prod_{q \in Q} \frac{q-1}{q}\right) \times d}{\left(\prod_{a \in A} \frac{a-1}{a}\right) \times d}$$

$$= \frac{\varphi(x) \times \varphi(y) \times d}{\varphi(d)}$$

命题得证

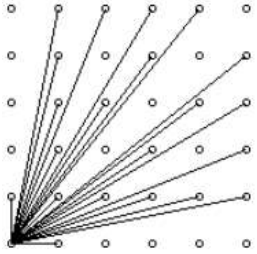
#2738、可见的点

题目描述

在一个平面直角坐标系的第一象限内
如果一个点 (x,y) 与原点 $(0,0)$ 的连线中没有通过其他任何点
则称该点在原点处是可见的

如点 $(4,2)$ 就是不可见的,因为它与原点的连线会通过点 $(2,1)$

部分可见点与原点的连线如下图所示:



编写一个程序,计算给定整数 N 的情况下,满足 $0 \leq x,y \leq N$ 的可见点 $x,y)$ 的数量

> *可见点不包括原点*

输入格式

第一行包含整数 C ,表示共有 C 组测试数据

每组测试数据占一行,包含一个整数 N

输出格式

每组测试数据的输出占据一行

输出可见点的数量

数据范围

对于 20% 的数据 $1 \leq n,T \leq 100$
对于 100% 的数据 $1 \leq T \leq 10000, 1 \leq N \leq 10^6$

光源位于 (0,0)

所有点与光源之间直线解析式为

$$y = kx$$

若一个点 (x',y') 被同一直线上 (x_0,y_0) 点遮挡

有

$$\frac{y_0}{x_0} = \frac{y'}{x'} = k\ (x' > x_0\ , y' > y_0)$$

显然 $(x_0,y_0) = 1$, $(x',y') \neq 1$

若点对满足 $(x,y) = 1$ 都可见

容易想到 $O(T\ n^2 \log n)$ 枚举

#2738、可见的点

- 当 $x = y$ 时

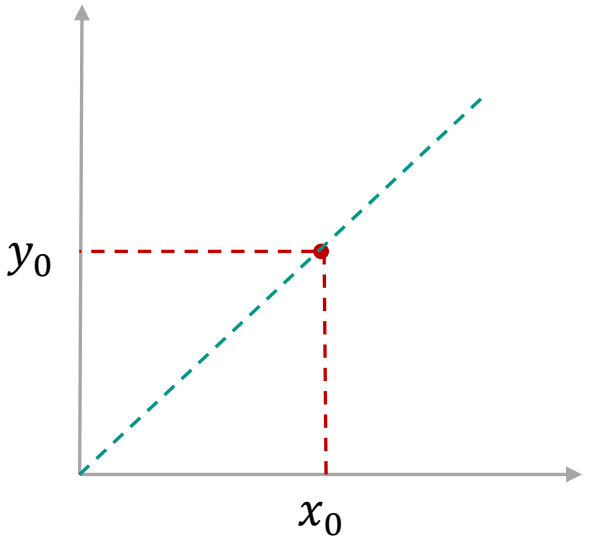
  互质点个数仅有一个

- 当 $x > y$ 时

  互质点的个数为 $\varphi(x)$

- 当 $x < y$ 时

  互质点的个数为 $\varphi(y)$



容易发现 整个正方形上的点都是关于 $y = x$ 对称

即答案为

$$1 + 2\sum_{i=1}^{n}\varphi(i)$$

使用前缀和维护时间复杂度 $O(\max(n) + T)$

同余

若 $a \bmod m = b \bmod m$ 且 $m \neq 0$

即 a, b 除以 m 所得的余数相等，记作 $a \equiv b \pmod m$，读作 a 同余与 b 模 m

若无特殊说明，模数总是正整数，余数为最小非负剩余

同余存在如下性质

若 $a \equiv b \pmod m$，则 $m \mid (a - b)$

若 $a \equiv b \pmod m$ 且 $b \equiv c \pmod m$，则 $a \equiv c \pmod m$

若 $a \equiv b \pmod m$ 且 $d \mid m$，则 $a \equiv b \pmod d$

若 $a \equiv b \pmod m$，则 $(a, m) = (b, m)$

若 $a \equiv b \pmod m$，对于整数 k 有

$$k + a \equiv k + b \pmod m$$

同余

若 $a \equiv b \pmod{m}$, 对于整数 k 有

$$ka \equiv kb \pmod{m}$$

若 $a \equiv b \pmod{m}$, 对于非零整数 k 有

$$ka \equiv kb \pmod{km}$$

若 $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m}$

那么下面的模运算律成立:

$$a \pm c \equiv b \pm d \pmod{m}$$

$$a \times c \equiv b \times d \pmod{m}$$

$$a^n \equiv b^n \pmod{m}$$

#1615、k倍区间

题目描述

给定一个长度为 n 的数列 $a_1, a_2, \ldots, a_n$

如果其中一段连续的子序列 $a_i, a_{i+1}, \ldots, a_j (i \le j)$ 之和是 K 的倍数

我们就称这个区间 $[i, j]$ 是 K 倍区间

你能求出数列中总共有多少个 K 倍区间吗?

输入格式

第一行包含两个整数 n 和 k

以下 n 行每行包含一个整数 a_i

输出格式

输出一个整数,代表 k 倍区间的数目

数据规模

对于 20% 的数据 $1 \le n \le k \le 100$

对于 60% 的数据 $1 \le n \le k \le 10000$

对于 100% 的数据 $1 \le n \le k \le 100000$

对于全部数据 $1 \le a_i \le 100000$

维护前缀和 sum_i

若

$$\text{sum}_i \equiv \text{sum}_j \pmod{k}$$

那么

$$(\text{sum}_i - \text{sum}_j) \mid k$$

维护所有的 $\text{sum}_i \bmod k$

令 $\text{cnt}_{\text{sum}_i \bmod k}$ 表示 $\text{sum}_i \bmod k$ 出现的次数

答案为

$$\sum_{i=0}^{k-1} \binom{\text{cnt}_i}{2}$$

时间复杂度 $O(n)$

费马小定理

若 p 为素数且 $(a,p)=1$ 有

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)$$

引理

构造序列 $A=\{1,2,3,\cdots,p-1\}$，存在如下性质

$$\prod_{i=1}^{p-1}A_i\equiv\prod_{i=1}^{p-1}(a\times A_i)\ (\mathrm{mod}\ p)$$

当 $i\neq j$ 时根据质数性质显然有 $A_i\not\equiv A_j\ (\mathrm{mod}\ p)$

由于 $(a,p)=1$，根据 **裴蜀定理** 必然存在整数 I 满足 $a\times I\equiv 1\ (\mathrm{mod}\ p)$

若存在 $a\times A_i\equiv a\times A_j\ (\mathrm{mod}\ p)$，两边同乘 I 可得 $A_i\equiv A_j\ (\mathrm{mod}\ p)$

与条件矛盾，即

$$a\times A_i\not\equiv a\times A_j\ (\mathrm{mod}\ p)$$

费马小定理

综上 $A_i \times a$ 与 A_i 在模 p 意义下一一对应

引理得证

证明

记 $f = (p-1)!$

$$a^{p-1} \times f \equiv f \pmod{p}$$

根据质数性质显然有 $(f, p) = 1$

根据 **裴蜀定理**，必然存在整数 I 满足 $f \times I \equiv 1 \pmod{p}$

两边同乘 I，可得

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

得证

乘法逆元

给定两个整数 a 和 p，若存在整数 x 使得

$$ax \equiv 1 \pmod{p}$$

称 x 为 $a \bmod p$ 的乘法逆元，记作 a^{-1}

当 $p \in \mathbb{P}$ 时，根据费马小定理

$$a \times x \equiv a \times a^{p-1} \pmod{p}$$

即

$$x \equiv a^{p-2} \pmod{p}$$

当 $(a, p) = 1$ 时 a^{-1} 必然存在

根据裴蜀定理必然存在 $ax + py = 1$

上式等价于 $ax \equiv 1 \pmod{p}$

命题得证

乘法逆元

当 $(a,p) \neq 1$ 时 a^{-1} 必然不存在

此时 $d = (a,p) > 1$

那么 $ax + py = 1$ 可写为

$$\frac{ax}{d} + \frac{py}{d} = \frac{1}{d}$$

显然 $\frac{ax}{d}, \frac{py}{d} \in \mathbb{Z}$ 而 $\frac{1}{d} \notin \mathbb{Z}$

命题得证

#1928、 计算题

题目描述

这是一道简单的计算题

给定整数 A, N 求

$$(A-1) \times \sum_{i=0}^{N} A^i$$

答案可能很大,输出时对 1000000007 取模

输入格式

一行两个正整数 A, N

输出格式

一个数,表示计算结果

数据范围

对于 5% 的数据 $N \leq 100$

对于 15% 的数据 $N \leq 2 \times 10^9$

对于 100% 的数据 $2 \leq N \leq 10^{100000}, 2 \leq A \leq 2 \times 10^9$ 保证 $A \neq 1000000007$

等比数列求和

$$\left(\sum_{i=0}^{N} A^i\right) = \frac{A^{N+1}-1}{A-1}$$

所求即为 $A^{N+1}-1$

费马小定理

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

这意味着指数存在周期，周期为 $p-1$

不难发现 $(A, 1000000007) = 1$ 且 1000000007 为质数

费马小定理降幂求解即可

整除分块

性质1

$\forall\, a,b,c \in \mathbb{Z}$, $\left\lfloor \frac{a}{bc} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor$

证明

$$\frac{a}{b} = \left\lfloor \frac{a}{b} \right\rfloor + r\ (0 \le r < 1) \Rightarrow \left\lfloor \frac{a}{b} \cdot \frac{1}{c} \right\rfloor = \left\lfloor \frac{1}{c} \cdot \left(\left\lfloor \frac{a}{b} \right\rfloor + r \right) \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} + \frac{r}{c} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor$$

性质2

$\forall\, n \in \mathbb{N}^+$, $\left| \left\{ \left\lfloor \frac{n}{d} \right\rfloor \mid d \in \mathbb{N}^+, d \le n \right\} \right| \le 2\sqrt{n}$

证明

对于 $d \le \sqrt{n}$, $\left\lfloor \frac{n}{d} \right\rfloor$ 至多有 $\sqrt{n}$ 种取值

对于 $d \ge \sqrt{n}$, $\left\lfloor \frac{n}{d} \right\rfloor < \sqrt{n}$ 至多有 $\sqrt{n}$ 种取值

整除分块

性质3

设 $k = \left\lfloor \frac{n}{l} \right\rfloor$，若有 $\left\lfloor \frac{n}{r} \right\rfloor = k$ 则满足 $l \le r \le n$ 的 r 最大为 $\left\lfloor \frac{n}{k} \right\rfloor$

证明

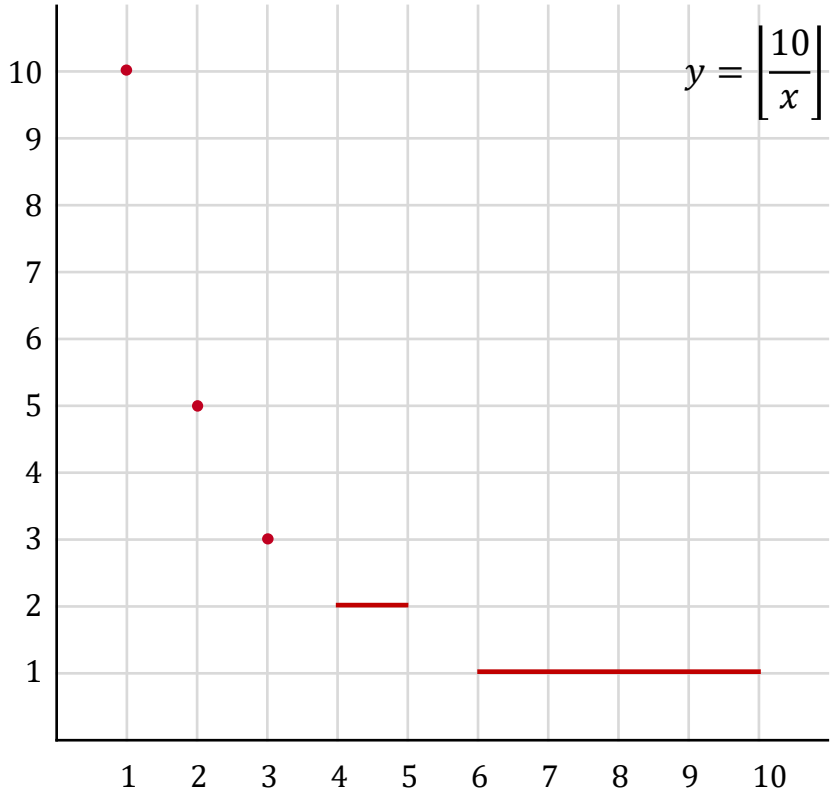
对于 $l \le x \le r$ 都有 $\left\lfloor \frac{n}{x} \right\rfloor = k$

n 可被写为 $kx + q\ (0 \le q < k)$

那么

$$kx \le n \Rightarrow x \le \left\lfloor \frac{n}{k} \right\rfloor$$

这意味着 $\left\lfloor \frac{n}{x} \right\rfloor$ 一定成块连续出现，对于 k 出现的范围为 $\left\lfloor \frac{n}{k+1} \right\rfloor + 1 \sim \left\lfloor \frac{n}{k} \right\rfloor$



#3825、 数论分块1

题目描述

定义 $f(i)$ 为 i 的正约数个数

给出正整数 N 请你求出

$$\sum_{i=1}^{N} f(i)$$

输入格式

输入一个整数 N

输出格式

输出一个整数表示 $\sum_{i=1}^{N} f(i)$

数据规模

对于 10% 的数据 $1 \le N \le 10^5$

对于 30% 的数据 $1 \le N \le 2 \times 10^7$

对于 100% 的数据 $1 \le N \le 10^{15}$

$f(i)$ 为积性函数，可在欧拉筛过程中求解

时间复杂度 $O(N)$ 但无法通过本题

$$f(i) = \sum_{j=1}^{i} [j \mid i]$$

那么

$$\sum_{i=1}^{N} f(i) = \sum_{i=1}^{N} \sum_{j=1}^{i} [j \mid i]$$

约数仅可能在 $1 \sim N$ 间

约数 d 在 $f(d)$，$f(2d)$，$\cdots$，$f\left(\left\lfloor \frac{N}{d} \right\rfloor d\right)$ 中分别产生贡献 1

共有 $\left\lfloor \frac{N}{d} \right\rfloor$ 的贡献

#3825、 数论分块1

即

$$\sum_{i=1}^{N} f(i) = \sum_{d=1}^{N} \left\lfloor \frac{N}{d} \right\rfloor$$

记 $k = \left\lfloor \frac{N}{d} \right\rfloor$ 根据 **性质3**

$l = k$, $r = \left\lfloor \frac{N}{k} \right\rfloor$ 在 $l \le d \le r$ 范围内 $\left\lfloor \frac{N}{d} \right\rfloor$ 都为定值 k (将 $\left\lfloor \frac{N}{d} \right\rfloor$ 都为 k 的部分称为一个 **块**)

初始时令 $l \leftarrow 1$

每次令 $k \leftarrow \left\lfloor \frac{N}{d} \right\rfloor, r \leftarrow \left\lfloor \frac{N}{k} \right\rfloor$ 累加贡献 $k \times (r - l + 1)$

再令 $l = r + 1$, 直到 l 超过 N

根据 **性质2** $\left\lfloor \frac{n}{d} \right\rfloor$ 仅有 $2\sqrt{N}$ 个取值 , 该过程时间复杂度 $O(\sqrt{N})$

#3826、 数论分块2

题目描述

定义 $f(i)$ 为 i 的正约数之和

给出正整数 N 请你求出

$$\sum_{i=1}^{N} f(i)$$

输入格式

输入一个整数 N

输出格式

输出一个整数表示 $\sum_{i=1}^{N} f(i)$

数据规模

对于 10% 的数据 $1 \leq N \leq 10^5$

对于 30% 的数据 $1 \leq N \leq 2 \times 10^7$

对于 100% 的数据 $1 \leq N \leq 2 \times 10^9$

$$f(i) = \sum_{d \mid i} d$$

那么

$$\sum_{i=1}^{N} f(i) = \sum_{i=1}^{N} \sum_{d \mid i} d$$

约数仅可能在 $1 \sim N$ 间

约数 d 在 $f(d)$，$f(2d)$，$\cdots$，$f\left(\left\lfloor \frac{N}{d} \right\rfloor\right)$ 中分别产生贡献 d

共有 $d \times \left\lfloor \frac{N}{d} \right\rfloor$ 的贡献

#3826、 数论分块2

即

$$\sum_{i=1}^{N} f(i) = \sum_{d=1}^{N} \left(d \times \left\lfloor \frac{N}{d} \right\rfloor \right)$$

记 $k = \left\lfloor \frac{N}{d} \right\rfloor$ 根据 **性质3**

$l = k, r = \left\lfloor \frac{N}{k} \right\rfloor$ 在 $l \le d \le r$ 范围内 $\left\lfloor \frac{N}{d} \right\rfloor$ 都为定值 k

此时 d 遍历 l~r 此部分贡献为等差数列

那么一个块的贡献为

$$\frac{(r-l+1)(l+r)}{2} \times k$$

时间复杂度 $O(\sqrt{N})$

谢谢观看