

# 数论总结

## D. Same GCDs

<https://codeforces.com/problemset/problem/1295/D>

- 前置知识

### 辗转相除法（欧几里得算法）

$$\gcd(\text{较大数}, \text{较小数}) = \gcd(\text{较小数}, \text{二者余数})$$

通俗的数学语言表示：

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

PS：有 gcd 出现要想到辗转相除法，每次都会忘记

### 欧拉函数

对于一个正整数  $n$ ，欧拉函数  $\phi(n)$  等于小于等于  $n$  的正整数中于  $n$  互质的数的数目

计算过程如下：

1. 首先将给定的数拆分为标准分解式的格式：

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$$

2. 计算欧拉函数

$$\phi(n) = \prod_{i=1}^r p_i^{k_i-1} (p_i - 1)$$

补充欧拉函数的性质：

$$\phi(a \times b) = \phi(a) \times \phi(b), \text{当 } n \text{ 为奇数时 } \phi(2n) = \phi(n)$$

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

$$\text{若 } n = p^k \text{ (} p \text{ 为质数)}, \phi(n) = p^k - p^{k-1}$$

- 拓展

### 更相减损术

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

优化后的结果：

如果： $(2 \mid a) \wedge (2 \mid b)$  则有  $\gcd(a, b) = 2 \gcd(\frac{a}{2}, \frac{b}{2})$

如果： $(2 \mid a) \wedge (2 \nmid b)$ ，则有  $\gcd(\frac{a}{2}, b)$

此算法的复杂度为  $O(\log n)$

- 本题思路如下:

$$\sum_{x=0}^{m-1} [\gcd(a, m) = \gcd(a + x, m)] \implies \sum_{x=0}^{m-1} [\gcd(a, m) = \gcd((a + x) \bmod m, m)]$$

$\implies \sum_{x=0}^{m-1} [\gcd(a, m) = \gcd(x, m)]$ ,  $(a + x)$  在  $x$  从  $0 \rightarrow m$  过程中会有且仅一次的覆盖整个取模空间

令  $\gcd(a, m) = \gcd(x, m) = q \implies \frac{\gcd(x, m)}{q} = 1$ , 这个  $q$  我们是知道的

即求  $\sum_{x=0}^{m-1} [\frac{\gcd(x, m)}{q} = 1]$ , 稍微转化一下:  $\sum_{0 \leq i \leq m} [\gcd(i, \frac{m}{q}) = 1]$

因为  $x < m$ , 所以  $\sum_{0 \leq i \leq m} [\gcd(i, \frac{m}{q}) = 1]$  实际上的范围就是  $1 \sim \frac{m}{q} - 1$

这实际就是  $\phi(\frac{m}{q})$

## D. Dima and Lisa

<https://codeforces.com/problemset/problem/584/D>

- 前置知识

### 哥德巴赫猜想

一个任意大于 2 的整数都可以分解成三个质数之和

附属猜想, 任何一个大于 2 的偶数都可以分解为两个质数之和

### 质数密度情况

通过数学证明证明出两两素数间的平均距离大致为  $\log n$