数论基础

Bob Wang

UESTC, China

2024.6.8

目录

目录

数论要学些什么?

- 整除理论：整除，约数，公约数，公倍数……
- 同余理论：模意义下运算，同余方程（组），费马小定理……
- 积性函数与筛：线性筛素数，欧拉函数，莫比乌斯函数……

一般只涉及自然数。

数论要学些什么?

- 整除理论：整除，约数，公约数，公倍数……
- 同余理论：模意义下运算，同余方程（组），费马小定理……
- 积性函数与筛：线性筛素数，欧拉函数，莫比乌斯函数……

一般只涉及自然数。

数论要学些什么?

- 整除理论：整除，约数，公约数，公倍数……
- 同余理论：模意义下运算，同余方程（组），费马小定理……
- 积性函数与筛：线性筛素数，欧拉函数，莫比乌斯函数……

一般只涉及自然数。

数论要学些什么?

- 整除理论：整除，约数，公约数，公倍数……
- 同余理论：模意义下运算，同余方程（组），费马小定理……
- 积性函数与筛：线性筛素数，欧拉函数，莫比乌斯函数……

一般只涉及自然数。

目录

知识点

1. 整除
2. 约数与最大公约数、最小公倍数
3. 互质与质数
4. 算术基本定理

整除

整除的定义

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 $a \mid b$;
b 不可被 a 整除记作 $a \nmid b$.

性质：

1. 正整数上的整除关系是一种偏序关系：自反，反对称，传递
   自反：$a \mid a$
   反对称：若 $a \neq b, a \mid b$，则 $b \nmid a$
   传递：若 $a \mid b, b \mid c$，则 $a \mid c$.
2. $a \mid b \to a \mid bc$
3. $a \mid b, a \mid c \to a \mid (xb + yc)$

整除

整除的定义

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 $a \mid b$;
b 不可被 a 整除记作 $a \nmid b$.

性质:

1. 正整数上的整除关系是一种偏序关系：自反，反对称，传递
   自反：$a \mid a$
   反对称：若 $a \neq b, a \mid b$，则 $b \nmid a$
   传递：若 $a \mid b, b \mid c$，则 $a \mid c$.
2. $a \mid b \to a \mid bc$
3. $a \mid b, a \mid c \to a \mid (xb + yc)$

整除

整除的定义

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 $a \mid b$;
b 不可被 a 整除记作 $a \nmid b$.

性质:

1. 正整数上的整除关系是一种偏序关系：自反，反对称，传递
   自反：$a \mid a$
   反对称：若 $a \neq b, a \mid b$，则 $b \nmid a$
   传递：若 $a \mid b, b \mid c$，则 $a \mid c$.
2. $a \mid b \to a \mid bc$
3. $a \mid b, a \mid c \to a \mid (xb + yc)$

约数与倍数

约数与倍数的定义

若 $a \mid b$，则 a 是 b 的约数（因数），b 是 a 的倍数。
1 是任何数的约数，0 是任何数的倍数。

性质：

1. 一个数 n 的约数的上界为 $O(\sqrt{n})$.

约数与倍数

约数与倍数的定义

若 $a \mid b$，则 a 是 b 的约数（因数），b 是 a 的倍数。
1 是任何数的约数，0 是任何数的倍数。

性质：

1. 一个数 n 的约数的上界为 $O(\sqrt{n})$.

约数与倍数

约数与倍数的定义

若 $a \mid b$，则 a 是 b 的约数（因数），b 是 a 的倍数。
1 是任何数的约数，0 是任何数的倍数。

性质：

1. 一个数 n 的约数的上界为 $O(\sqrt{n})$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, \dots, a \mid n_m$，则 a 是 n_1、n_2、……n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, \dots, n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, \dots, n_m)$，可简写为 $(n_1, n_2, \dots, n_m)$。

性质：

1. $\gcd(n_1, n_2, \dots, n_m) = \gcd(\gcd(n_1, n_2, \dots, n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x \% y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, ..., a \mid n_m$，则 a 是 n_1、n_2、……n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, ..., n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, ..., n_m)$，可简写为 $(n_1, n_2, ..., n_m)$。

性质：

1. $\gcd(n_1, n_2, ..., n_m) = \gcd(\gcd(n_1, n_2, ..., n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x\%y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, ..., a \mid n_m$，则 a 是 n_1、n_2、……n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, ..., n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, ..., n_m)$，可简写为 $(n_1, n_2, ..., n_m)$。

性质：

1. $\gcd(n_1, n_2, ..., n_m) = \gcd(\gcd(n_1, n_2, ..., n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x \% y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, ..., a \mid n_m$，则 a 是 n_1、n_2、……n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, ..., n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, ..., n_m)$，可简写为 $(n_1, n_2, ..., n_m)$。

性质：

1. $\gcd(n_1, n_2, ..., n_m) = \gcd(\gcd(n_1, n_2, ..., n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x \% y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, ..., a \mid n_m$，则 a 是 n_1、n_2、……n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, ..., n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, ..., n_m)$，可简写为 $(n_1, n_2, ..., n_m)$。

性质：

1. $\gcd(n_1, n_2, ..., n_m) = \gcd(\gcd(n_1, n_2, ..., n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x \% y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公约数

若 $a \mid n_1, a \mid n_2, ..., a \mid n_m$，则 a 是 n_1、n_2、......n_m 的公约数 (公因数)。

最大公约数 (gcd)

$n_1, n_2, ..., n_m$ 最大的公约数（字面意义），
记为 $\gcd(n_1, n_2, ..., n_m)$，可简写为 $(n_1, n_2, ..., n_m)$。

性质:

1. $\gcd(n_1, n_2, ..., n_m) = \gcd(\gcd(n_1, n_2, ..., n_{m-1}), n_m)$.
2. 辗转相减：$\gcd(x, y) = \gcd(y, x - y)$.
3. 辗转相除：$\gcd(x, y) = \gcd(y, x\%y)$.

辗转相除法（欧几里得算法）求两个数 gcd 的时间复杂度为 $O(\log n)$.

约数与倍数

公倍数

若 $a_1 \mid n, a_2 \mid n, ..., a_m \mid n$，则 n 是 a_1、a_2、……a_m 的公倍数。

最小公倍数 (lcm)

$a_1, a_2, ..., a_m$ 最小的公倍数（字面意义），
记为 $\text{lcm}(a_1, a_2, ..., a_m)$，可简写为 $[a_1, a_2, ..., a_m]$。

性质：

1. $\text{lcm}(a_1, a_2, ..., a_m) = \text{lcm}(\text{lcm}(a_1, a_2, ..., a_{m-1}), a_m)$.
2. $\gcd(x, y) \times \text{lcm}(x, y) = xy$.

约数与倍数

公倍数

若 $a_1 \mid n, a_2 \mid n, ..., a_m \mid n$，则 n 是 a_1、a_2、……a_m 的公倍数。

最小公倍数 (lcm)

$a_1, a_2, ..., a_m$ 最小的公倍数（字面意义），
记为 $\operatorname{lcm}(a_1, a_2, ..., a_m)$，可简写为 $[a_1, a_2, ..., a_m]$。

性质：

1. $\operatorname{lcm}(a_1, a_2, ..., a_m) = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2, ..., a_{m-1}), a_m)$.
2. $\gcd(x, y) \times \operatorname{lcm}(x, y) = xy$.

约数与倍数

公倍数

若 $a_1 \mid n, a_2 \mid n, ..., a_m \mid n$，则 n 是 a_1、a_2、……a_m 的公倍数。

最小公倍数 (lcm)

$a_1, a_2, ..., a_m$ 最小的公倍数（字面意义），
记为 $\text{lcm}(a_1, a_2, ..., a_m)$，可简写为 $[a_1, a_2, ..., a_m]$。

性质：

1. $\text{lcm}(a_1, a_2, ..., a_m) = \text{lcm}(\text{lcm}(a_1, a_2, ..., a_{m-1}), a_m)$.
2. $\gcd(x, y) \times \text{lcm}(x, y) = xy$.

约数与倍数

公倍数

若 $a_1 \mid n, a_2 \mid n, ..., a_m \mid n$，则 n 是 a_1、a_2、……a_m 的公倍数。

最小公倍数 (lcm)

$a_1, a_2, ..., a_m$ 最小的公倍数（字面意义），
记为 $\operatorname{lcm}(a_1, a_2, ..., a_m)$，可简写为 $[a_1, a_2, ..., a_m]$。

性质：

1. $\operatorname{lcm}(a_1, a_2, ..., a_m) = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2, ..., a_{m-1}), a_m)$.
2. $\gcd(x, y) \times \operatorname{lcm}(x, y) = xy$.

互质与质数

互质的定义

若 $\gcd(x, y) = 1$，则称 x 与 y 互质。

质数与合数

如果一个大于 1 的数 n 的因数只有 1 和 n，则 n 为质数，否则 n 为合数。
1 既不是质数，也不是合数。

N 以内质数的数量级为 $\pi(N) = O(\frac{N}{\ln N})$.

互质与质数

互质的定义

若 $\gcd(x, y) = 1$，则称 x 与 y 互质。

质数与合数

如果一个大于 1 的数 n 的因数只有 1 和 n，则 n 为质数，否则 n 为合数。
1 既不是质数，也不是合数。

N 以内质数的数量级为 $\pi(N) = O(\frac{N}{\ln N})$.

互质与质数

互质的定义

若 $\gcd(x, y) = 1$，则称 x 与 y 互质。

质数与合数

如果一个大于 1 的数 n 的因数只有 1 和 n，则 n 为质数，否则 n 为合数。
1 既不是质数，也不是合数。

N 以内质数的数量级为 $\pi(N) = O(\frac{N}{\ln N})$.

唯一分解定理

算术基本引理

设 p 是质数，$p \mid a_1a_2$，那么 $p \mid a_1$ 和 $p \mid a_2$ 至少有一个成立。

算术基本定理（唯一分解定理）

大于 1 的正整数 a 一定可以表示为以下形式：

$$a = p_1p_2...p_s$$

其中 $p_i(1 \le i \le s)$ 为质数，且在不计次序的情况下该表示唯一。

唯一分解定理

算术基本引理

设 p 是质数，$p \mid a_1a_2$，那么 $p \mid a_1$ 和 $p \mid a_2$ 至少有一个成立。

算术基本定理（唯一分解定理）

大于 1 的正整数 a 一定可以表示为以下形式：

$$a = p_1p_2...p_s$$

其中 $p_i(1 \leq i \leq s)$ 为质数，且在不计次序的情况下该表示唯一。

唯一分解定理

质因数分解

正整数 a 的标准素因数分解式为：

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}, p_1 < p_2 < ... < p_s$$

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} ... p_s^{k_{a_s}}$，$b = p_1^{k_{b_1}} p_2^{k_{b_2}} ... p_s^{k_{b_s}}$，
则:

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

可推广至多个数的情况。
第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} \ldots p_s^{k_{a_s}}$， $b = p_1^{k_{b_1}} p_2^{k_{b_2}} \ldots p_s^{k_{b_s}}$，
则：

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

可推广至多个数的情况。
第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} ... p_s^{k_{a_s}}$，$b = p_1^{k_{b_1}} p_2^{k_{b_2}} ... p_s^{k_{b_s}}$，
则：

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

可推广至多个数的情况。
第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} \dots p_s^{k_{a_s}}$，$b = p_1^{k_{b_1}} p_2^{k_{b_2}} \dots p_s^{k_{b_s}}$，
则:

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

可推广至多个数的情况。
第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} \ldots p_s^{k_{a_s}}$， $b = p_1^{k_{b_1}} p_2^{k_{b_2}} \ldots p_s^{k_{b_s}}$，
则：

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

可推广至多个数的情况。

第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

设 $a = p_1^{k_{a_1}} p_2^{k_{a_2}} ... p_s^{k_{a_s}}$，$b = p_1^{k_{b_1}} p_2^{k_{b_2}} ... p_s^{k_{b_s}}$，
则:

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

可推广至多个数的情况。
第十五届蓝桥杯 C 与 C++ 国赛 F 题。

再探 gcd 与 lcm

题目描述：
给出三个数 x, y, n，求有序数对 $(a_1, a_2, ..., a_n)$ 的数量，满足：

$$\gcd(a_1, a_2, ..., a_n) = x, \operatorname{lcm}(a_1, a_2, ..., a_n) = y$$

.
$1 \le x \le y \le 10^9, 2 \le n \le 10^5$.

再探 gcd 与 lcm

题目分析:
根据 $\gcd(a_1, a_2, ..., a_n) = x$，将这 n 个数表示成以下形式:

$$a_1 = t_1 x, a_2 = t_2 x, ..., a_n = t_n x$$

其中 $\gcd(t_1, t_2, ...t_n) = 1$.
又由于 $\operatorname{lcm}(a_1, a_2, ..., a_n) = y$,
因此 $\operatorname{lcm}(t_1, t_2, ..., t_n) = \frac{y}{x} = d$.
根据前面提到的质因数分解，将 d 分解为 $p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$,
将 t_i 分解为 $p_1^{k_{t_{i_1}}} p_2^{k_{t_{i_2}}} ... p_s^{k_{t_{i_s}}}$,
则:

$$\min\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = 0, 1 \leq i \leq s$$

$$\max\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = k_i, 1 \leq i \leq s$$

再探 gcd 与 lcm

题目分析:
根据 $\gcd(a_1, a_2, ..., a_n) = x$，将这 n 个数表示成以下形式:

$$a_1 = t_1 x, a_2 = t_2 x, ..., a_n = t_n x$$

其中 $\gcd(t_1, t_2, ...t_n) = 1$.
又由于 $\operatorname{lcm}(a_1, a_2, ..., a_n) = y$,
因此 $\operatorname{lcm}(t_1, t_2, ..., t_n) = \frac{y}{x} = d$.
根据前面提到的质因数分解，将 d 分解为 $p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$,
将 t_i 分解为 $p_1^{k_{t_{i_1}}} p_2^{k_{t_{i_2}}} ... p_s^{k_{t_{i_s}}}$,
则:

$$\min\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = 0, 1 \le i \le s$$

$$\max\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = k_i, 1 \le i \le s$$

再探 gcd 与 lcm

题目分析:
根据 $\gcd(a_1, a_2, ..., a_n) = x$，将这 n 个数表示成以下形式:

$$a_1 = t_1 x, a_2 = t_2 x, ..., a_n = t_n x$$

其中 $\gcd(t_1, t_2, ...t_n) = 1$.
又由于 $\mathrm{lcm}(a_1, a_2, ..., a_n) = y$,
因此 $\mathrm{lcm}(t_1, t_2, ..., t_n) = \frac{y}{x} = d$.
根据前面提到的质因数分解，将 d 分解为 $p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$,
将 t_i 分解为 $p_1^{k_{t_{i_1}}} p_2^{k_{t_{i_2}}} ... p_s^{k_{t_{i_s}}}$,
则:

$$\min\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = 0, 1 \le i \le s$$

$$\max\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = k_i, 1 \le i \le s$$

再探 gcd 与 lcm

题目分析:
根据 $\gcd(a_1, a_2, ..., a_n) = x$，将这 n 个数表示成以下形式:

$$a_1 = t_1 x, a_2 = t_2 x, ..., a_n = t_n x$$

其中 $\gcd(t_1, t_2, ...t_n) = 1$.
又由于 $\mathrm{lcm}(a_1, a_2, ..., a_n) = y$,
因此 $\mathrm{lcm}(t_1, t_2, ..., t_n) = \frac{y}{x} = d$.
根据前面提到的质因数分解，将 d 分解为 $p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$,
将 t_i 分解为 $p_1^{k_{t_{i_1}}} p_2^{k_{t_{i_2}}} ... p_s^{k_{t_{i_s}}}$,
则:

$$\min\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = 0, 1 \leq i \leq s$$

$$\max\{k_{t_{1_i}}, k_{t_{2_i}}, ..., k_{t_{n_i}}\} = k_i, 1 \leq i \leq s$$

再探 gcd 与 lcm

对于每一个质因数 p_i，便可以单独讨论。
贡献即为 $t_j, 1 \leq j \leq n$ 分解到 p_i 上的指数的最小值为 0，最大值为 k_i 的方案数.
根据容斥原理:
贡献为指数从 0 到 k_i 任选的方案数，减去指数从 1 到 k_i 任选的方案数，减去指数从 0 到 $k_i - 1$ 任选的方案数, 加上指数从 1 到 $k_i - 1$ 任选的方案数。
答案为:

$$\prod_{i=1}^{s}((k_i+1)^n - 2 \times k_i^n + (k_i-1)^n)$$

.

再探 gcd 与 lcm

对于每一个质因数 p_i，便可以单独讨论。
贡献即为 $t_j, 1 \leq j \leq n$ 分解到 p_i 上的指数的最小值为 0，最大值为 k_i 的方案数.
根据容斥原理：
贡献为指数从 0 到 k_i 任选的方案数，减去指数从 1 到 k_i 任选的方案数，减去指数从 0 到 $k_i - 1$ 任选的方案数, 加上指数从 1 到 $k_i - 1$ 任选的方案数。
答案为：

$$\prod_{i=1}^{s}((k_i+1)^n - 2 \times k_i^n + (k_i-1)^n)$$

.

目录

知识点

1. 同余，剩余系
2. 模意义下运算：加减乘除，乘方，开根，取对数
3. 同余方程（组），裴蜀定理，拓展欧几里得，中国剩余定理
4. 威尔逊引理、费马小定理、欧拉定理
5. 阶与原根

从模意义下的运算入手，穿插定理的讲解。

知识点

1. 同余，剩余系
2. 模意义下运算：加减乘除，乘方，开根，取对数
3. 同余方程（组），裴蜀定理，拓展欧几里得，中国剩余定理
4. 威尔逊引理、费马小定理、欧拉定理
5. 阶与原根

从模意义下的运算入手，穿插定理的讲解。

正实数下的运算

- 加减乘除

  $a+b, a-b, a\times b, a\div b$
- 乘方，开方

  $a^b, \sqrt[b]{a}$
- 取对数

  $\log_b a$

模意义下的加减乘法

模运算的定义

也称取余运算，求一个数 a 除以另一个数 m 的余数，记作 $a\%m$ 或者 $a \bmod m$.

一般定义域为非负整数。在此定义域下，值域为 0 到 $m-1$ 之间的整数。模数 m 不能为 0.

模运算的性质：

1. $(a \pm b)\%m = ((a\%m) \pm (b\%m))\%m$
2. $(a \times b)\%m = (a\%m) \times (b\%m)\%m$

也就是说，可以一遍加减乘一边取模，防止溢出。同时这也是模意义下的加减乘法。

模意义下的加减乘法

模运算的定义

也称取余运算，求一个数 a 除以另一个数 m 的余数，
记作 $a\%m$ 或者 $a \bmod m$.

一般定义域为非负整数。在此定义域下，值域为 0 到 $m-1$ 之间的整数。模数 m 不能为 0.

模运算的性质:

1. $(a \pm b)\%m = ((a\%m) \pm (b\%m))\%m$
2. $(a \times b)\%m = (a\%m) \times (b\%m)\%m$

也就是说，可以一遍加减乘一边取模，防止溢出。同时这也是模意义下的加减乘法。

模意义下的加减乘法

模运算的定义

也称取余运算，求一个数 a 除以另一个数 m 的余数，记作 $a\%m$ 或者 $a \bmod m$.

一般定义域为非负整数。在此定义域下，值域为 0 到 $m-1$ 之间的整数。模数 m 不能为 0.

模运算的性质：

1. $(a \pm b)\%m = ((a\%m) \pm (b\%m))\%m$
2. $(a \times b)\%m = (a\%m) \times (b\%m)\%m$

也就是说，可以一遍加减乘一边取模，防止溢出。同时这也是模意义下的加减乘法。

模意义下的加减乘法

模运算的定义

也称取余运算，求一个数 a 除以另一个数 m 的余数，
记作 $a\%m$ 或者 $a \bmod m$.

一般定义域为非负整数。在此定义域下，值域为 0 到 $m-1$ 之间的整数。模数 m 不能为 0.
模运算的性质：

1. $(a \pm b)\%m = ((a\%m) \pm (b\%m))\%m$
2. $(a \times b)\%m = (a\%m) \times (b\%m)\%m$

也就是说，可以一遍加减乘一边取模，防止溢出。同时这也是模意义下的加减乘法。

模意义下的加减乘法

模运算的定义

也称取余运算，求一个数 a 除以另一个数 m 的余数，记作 $a\%m$ 或者 $a \bmod m$.

一般定义域为非负整数。在此定义域下，值域为 0 到 $m-1$ 之间的整数。模数 m 不能为 0.

模运算的性质：

1. $(a \pm b)\%m = ((a\%m) \pm (b\%m))\%m$
2. $(a \times b)\%m = (a\%m) \times (b\%m)\%m$

也就是说，可以一遍加减乘一边取模，防止溢出。同时这也是模意义下的加减乘法。

模意义下的乘方

如何快速求出 a^b 在模 m 意义下的值呢?

- 快速幂算法

基于二进制分解的思路。

假设我们要求 7^{10} 的值。10 的二进制表示为 $(1010)_2 = 2 + 8$，

因此 $7^{10} = 7^2 \times 7^8 = 7^2 \times ((7^2)^2)^2$.

这样我们便可以在将底数进行平方的过程中，根据指数该位的值，将乘方计算出来。注意一边乘的同时一边取模。

模意义下的乘方

如何快速求出 a^b 在模 m 意义下的值呢?

- 快速幂算法

基于二进制分解的思路。
假设我们要求 7^{10} 的值。10 的二进制表示为 $(1010)_2 = 2 + 8$，因此 $7^{10} = 7^2 \times 7^8 = 7^2 \times ((7^2)^2)^2$.
这样我们便可以在将底数进行平方的过程中，根据指数该位的值，将乘方计算出来。注意一边乘的同时一边取模。

模意义下的乘方

如何快速求出 a^b 在模 m 意义下的值呢?

- 快速幂算法

基于二进制分解的思路。
假设我们要求 7^{10} 的值。10 的二进制表示为 $(1010)_2 = 2 + 8$,
因此 $7^{10} = 7^2 \times 7^8 = 7^2 \times ((7^2)^2)^2$.
这样我们便可以在将底数进行平方的过程中，根据指数该位的值，将乘方计算出来。注意一边乘的同时一边取模。

模意义下的乘方

如何快速求出 a^b 在模 m 意义下的值呢?

- 快速幂算法

基于二进制分解的思路。
假设我们要求 7^{10} 的值。10 的二进制表示为 $(1010)_2 = 2 + 8$,
因此 $7^{10} = 7^2 \times 7^8 = 7^2 \times ((7^2)^2)^2$.
这样我们便可以在将底数进行平方的过程中，根据指数该位的值，将乘方计算出来。注意一边乘的同时一边取模。

模意义下的除法（乘法逆元）

在此之前，我们先来介绍一下同余的相关概念。

同余的定义

设模数为 $m, m > 0$，若 $m \mid (a - b)$，即 $a\%m = b\%m$，则称 a 同余于 b 模 m，b 是 a 对模数 m 的剩余，
记作 $a \equiv b \pmod m$.

同余的性质：

1. 同余关系是等价关系：自反，对称，传递
   自反：$a \equiv a \pmod m$
   对称：若 $a \equiv b \pmod m$，则 $b \equiv a \pmod m$
   传递：
   若 $a \equiv b \pmod m, b \equiv c \pmod m$，则 $a \equiv c \pmod m$
2. 线性运算：若 $a \equiv b \pmod m$，则：
   $a \pm c \equiv b \pm c \pmod m, a \times c \equiv b \times c \pmod m$

模意义下的除法（乘法逆元）

在此之前，我们先来介绍一下同余的相关概念。

同余的定义

设模数为 $m, m > 0$，若 $m \mid (a-b)$，即 $a\%m = b\%m$，则称 a 同余于 b 模 m，b 是 a 对模数 m 的剩余，
记作 $a \equiv b \pmod{m}$.

同余的性质：

1. 同余关系是等价关系：自反，对称，传递
   自反：$a \equiv a \pmod{m}$
   对称：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$
   传递：
   若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$
2. 线性运算：若 $a \equiv b \pmod{m}$，则：
   $a \pm c \equiv b \pm c \pmod{m}, a \times c \equiv b \times c \pmod{m}$

模意义下的除法（乘法逆元）

在此之前，我们先来介绍一下同余的相关概念。

同余的定义

设模数为 $m, m > 0$，若 $m \mid (a-b)$，即 $a\%m = b\%m$，则称 a 同余于 b 模 m，b 是 a 对模数 m 的剩余，
记作 $a \equiv b \pmod m$.

同余的性质：

1. 同余关系是等价关系：自反，对称，传递
   自反：$a \equiv a \pmod m$
   对称：若 $a \equiv b \pmod m$，则 $b \equiv a \pmod m$
   传递：
   若 $a \equiv b \pmod m, b \equiv c \pmod m$，则 $a \equiv c \pmod m$
2. 线性运算：若 $a \equiv b \pmod m$，则：
   $a \pm c \equiv b \pm c \pmod m, a \times c \equiv b \times c \pmod m$

模意义下的除法（乘法逆元）

在此之前，我们先来介绍一下同余的相关概念。

同余的定义

设模数为 $m, m > 0$，若 $m \mid (a - b)$，即 $a\%m = b\%m$，则称 a 同余于 b 模 m，b 是 a 对模数 m 的剩余，
记作 $a \equiv b \pmod{m}$.

同余的性质：

1. 同余关系是等价关系：自反，对称，传递
   自反：$a \equiv a \pmod{m}$
   对称：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$
   传递：
   若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$
2. 线性运算：若 $a \equiv b \pmod{m}$，则：
   $a \pm c \equiv b \pm c \pmod{m}, a \times c \equiv b \times c \pmod{m}$

模意义下的除法（乘法逆元）

在此之前，我们先来介绍一下同余的相关概念。

同余的定义

设模数为 $m, m > 0$，若 $m \mid (a-b)$，即 $a\%m = b\%m$，则称 a 同余于 b 模 m，b 是 a 对模数 m 的剩余，
记作 $a \equiv b \pmod{m}$.

同余的性质：

1. 同余关系是等价关系：自反，对称，传递
   自反：$a \equiv a \pmod{m}$
   对称：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$
   传递：
   若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$
2. 线性运算：若 $a \equiv b \pmod{m}$，则：
   $a \pm c \equiv b \pm c \pmod{m}, a \times c \equiv b \times c \pmod{m}$

模意义下的除法（乘法逆元）

问题：
假设 $a \times b \equiv c \pmod{m}$，我们希望找到一个数 a^{-1}，
使得 $b \equiv c \times a^{-1} \pmod{m}$，
这个数 a^{-1} 便为 a 在模 m 意义下的乘法逆元。
问题等价于求解线性同余方程：

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

.

模意义下的除法（乘法逆元）

问题：
假设 $a \times b \equiv c \pmod{m}$，我们希望找到一个数 a^{-1}，
使得 $b \equiv c \times a^{-1} \pmod{m}$，
这个数 a^{-1} 便为 a 在模 m 意义下的乘法逆元。
问题等价于求解线性同余方程：

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

.

线性同余方程

将线性同余方程的概念推广至一般形式：

线性同余方程

形如：

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

的方程称为线性同余方程。其中 a, b, m 为给定的整数，x 为需要求解的未知数。

线性同余方程可以改写为线性不定方程:

$$ax + my = b$$

x, y 为未知数，可以通过拓展欧几里得算法（exgcd）求解。

线性同余方程

裴蜀定理

设 a, b 是不全为零的整数，对任意整数 x, y，满足 $\gcd(a,b) \mid ax+by$，且存在整数 x, y, 使得 $ax+by=\gcd(a,b)$.

线性同余方程

proof.

$$ax + by = \gcd(a, b) \Rightarrow (a - b)x + b(x + y) = \gcd(a, b)$$

令 $x\prime = x + y, y\prime = x$，则上式化为：

$$bx\prime + (a - b)y\prime = \gcd(a, b) \Rightarrow (2b - a)x\prime + (a - b)(x\prime + y\prime) = \gcd(a, b)$$

令 $x\prime\prime = x\prime + y\prime, y\prime\prime = x\prime$，则上式化为：

$$(a - b)x\prime\prime + (2b - a)y\prime\prime = \gcd(a, b)$$

是不是很像辗转相除法?
最后一定会化简为形如 $\gcd(a, b)x^{(n)} = \gcd(a, b)$ 的形式，
代入 $x^{(n)} = 1, y^{(n)} = 0$，递归回去便可得到解。

线性同余方程

proof.

$$ax + by = \gcd(a,b) \Rightarrow (a-b)x + b(x+y) = \gcd(a,b)$$

令 $x' = x + y, y' = x$，则上式化为：

$$bx' + (a-b)y' = \gcd(a,b) \Rightarrow (2b-a)x' + (a-b)(x'+y') = \gcd(a,b)$$

令 $x'' = x' + y', y'' = x'$，则上式化为：

$$(a-b)x'' + (2b-a)y'' = \gcd(a,b)$$

是不是很像辗转相除法?
最后一定会化简为形如 $\gcd(a,b)x^{(n)} = \gcd(a,b)$ 的形式，
代入 $x^{(n)} = 1, y^{(n)} = 0$，递归回去便可得到解。

线性同余方程

proof.

$$ax+by=\gcd(a,b)\Rightarrow(a-b)x+b(x+y)=\gcd(a,b)$$

令 $x\prime=x+y,y\prime=x$，则上式化为：

$$bx\prime+(a-b)y\prime=\gcd(a,b)\Rightarrow(2b-a)x\prime+(a-b)(x\prime+y\prime)=\gcd(a,b)$$

令 $x\prime\prime=x\prime+y\prime,y\prime\prime=x\prime$，则上式化为：

$$(a-b)x\prime\prime+(2b-a)y\prime\prime=\gcd(a,b)$$

是不是很像辗转相除法?
最后一定会化简为形如 $\gcd(a,b)x^{(n)}=\gcd(a,b)$ 的形式，
代入 $x^{(n)}=1,y^{(n)}=0$，递归回去便可得到解。

线性同余方程

proof.

$$ax + by = \gcd(a,b) \Rightarrow (a-b)x + b(x+y) = \gcd(a,b)$$

令 $x\prime = x + y, y\prime = x$，则上式化为：

$$bx\prime + (a-b)y\prime = \gcd(a,b) \Rightarrow (2b-a)x\prime + (a-b)(x\prime + y\prime) = \gcd(a,b)$$

令 $x\prime\prime = x\prime + y\prime, y\prime\prime = x\prime$，则上式化为：

$$(a-b)x\prime\prime + (2b-a)y\prime\prime = \gcd(a,b)$$

是不是很像辗转相除法?

最后一定会化简为形如 $\gcd(a,b)x^{(n)} = \gcd(a,b)$ 的形式，代入 $x^{(n)} = 1, y^{(n)} = 0$，递归回去便可得到解。

线性同余方程

proof.

$$ax + by = \gcd(a, b) \Rightarrow (a - b)x + b(x + y) = \gcd(a, b)$$

令 $x\prime = x + y, y\prime = x$，则上式化为：

$$bx\prime + (a - b)y\prime = \gcd(a, b) \Rightarrow (2b - a)x\prime + (a - b)(x\prime + y\prime) = \gcd(a, b)$$

令 $x\prime\prime = x\prime + y\prime, y\prime\prime = x\prime$，则上式化为：

$$(a - b)x\prime\prime + (2b - a)y\prime\prime = \gcd(a, b)$$

是不是很像辗转相除法?
最后一定会化简为形如 $\gcd(a, b)x^{(n)} = \gcd(a, b)$ 的形式，
代入 $x^{(n)} = 1, y^{(n)} = 0$，递归回去便可得到解。

线性同余方程

下面我们来对 $ax + by = \gcd(a, b)$ 快速求解。

- 拓展欧几里得算法（exgcd）

根据裴蜀定理 $bx\prime + (a\%b)y\prime = \gcd(a, b)$ 一定有解，
而 $a\%b = a - b\lfloor \frac{a}{b} \rfloor$，代入上面的方程，化简：

$$ay\prime + b(x\prime - \lfloor \frac{a}{b} \rfloor y\prime) = \gcd(a, b)$$

因此 $x = y\prime, y = x\prime - \lfloor \frac{a}{b} \rfloor y\prime$.
递归的终止条件为 $b = 0$，返回解 $x = 1, y = 0$.
该算法时间复杂度为 $O(\log n)$.

线性同余方程

这样求出的解是一组特解，如何得到通解呢？

假设特解为 x_0, y_0，则通解可以表示为：

$$\begin{cases} x = x_0 + k \times \frac{b}{\gcd(a,b)} \\ y = y_0 - k \times \frac{a}{\gcd(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

理解：只有当 x 和 y 引起的改变量为 a 和 b 公倍数，x 和 y 引起的改变量之和才可能为 0.

线性同余方程

这样求出的解是一组特解，如何得到通解呢?
假设特解为 x_0, y_0，则通解可以表示为:

$$\begin{cases} x = x_0 + k \times \frac{b}{\gcd(a,b)} \\ y = y_0 - k \times \frac{a}{\gcd(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

理解：只有当 x 和 y 引起的改变量为 a 和 b 公倍数，x 和 y 引起的改变量之和才可能为 0.

线性同余方程

这样求出的解是一组特解，如何得到通解呢?
假设特解为 x_0, y_0，则通解可以表示为:

$$\begin{cases} x = x_0 + k \times \frac{b}{\gcd(a,b)} \\ y = y_0 - k \times \frac{a}{\gcd(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

理解：只有当 x 和 y 引起的改变量为 a 和 b 公倍数，x 和 y 引起的改变量之和才可能为 0.

线性同余方程

如何对一般的不定方程 $ax + by = m$ 求解呢?

定理

$ax + by = m$ 有解当且仅当 $\gcd(a, b) \mid m$.

用裴蜀定理很好证明。
对于 $ax + by = \gcd(a, b)$，我们得到了一组特解 x_0, y_0，则 $ax + by = m$ 有特解 $x_0{}' = \frac{m}{\gcd(a,b)} \times x_0, y_0{}' = \frac{m}{\gcd(a,b)} \times y_0$，
通解为:

$$\begin{cases} x = \frac{m}{\gcd(a,b)} \times x_0 + k \times \frac{b}{\gcd(a,b)} \\ y = \frac{m}{\gcd(a,b)} \times y_0 - k \times \frac{a}{\gcd(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

线性同余方程

如何对一般的不定方程 $ax + by = m$ 求解呢?

定理

$ax + by = m$ 有解当且仅当 $\gcd(a, b) \mid m$.

用裴蜀定理很好证明。

对于 $ax + by = \gcd(a, b)$，我们得到了一组特解 x_0, y_0，则 $ax + by = m$ 有特解 $x_0\prime = \frac{m}{\gcd(a,b)} \times x_0, y_0\prime = \frac{m}{\gcd(a,b)} \times y_0$，

通解为:

$$\begin{cases} x = \frac{m}{\gcd(a,b)} \times x_0 + k \times \frac{b}{\gcd(a,b)} \\ y = \frac{m}{\gcd(a,b)} \times y_0 - k \times \frac{a}{\gcd(a,b)} \end{cases} \quad k \in \mathbb{Z}$$

线性同余方程

如何对一般的不定方程 $ax+by=m$ 求解呢?

定理

$ax+by=m$ 有解当且仅当 $\gcd(a,b)\mid m$.

用裴蜀定理很好证明。

对于 $ax+by=\gcd(a,b)$，我们得到了一组特解 x_0,y_0，则 $ax+by=m$ 有特解 $x_0{}'=\frac{m}{\gcd(a,b)}\times x_0, y_0{}'=\frac{m}{\gcd(a,b)}\times y_0$，通解为:

$$\begin{cases} x=\frac{m}{\gcd(a,b)}\times x_0+k\times\frac{b}{\gcd(a,b)} \\ y=\frac{m}{\gcd(a,b)}\times y_0-k\times\frac{a}{\gcd(a,b)} \end{cases} \quad k\in\mathbb{Z}$$

线性同余方程

如何对一般的不定方程 $ax+by=m$ 求解呢?

定理

$ax+by=m$ 有解当且仅当 $\gcd(a,b)\mid m$.

用裴蜀定理很好证明。
对于 $ax+by=\gcd(a,b)$，我们得到了一组特解 x_0,y_0，则 $ax+by=m$ 有特解 $x_0\prime=\frac{m}{\gcd(a,b)}\times x_0, y_0\prime=\frac{m}{\gcd(a,b)}\times y_0$，
通解为:

$$\begin{cases} x=\frac{m}{\gcd(a,b)}\times x_0+k\times\frac{b}{\gcd(a,b)} \\ y=\frac{m}{\gcd(a,b)}\times y_0-k\times\frac{a}{\gcd(a,b)} \end{cases} \quad k\in\mathbb{Z}$$

线性同余方程

如何对一般的不定方程 $ax+by=m$ 求解呢?

定理

$ax+by=m$ 有解当且仅当 $\gcd(a,b)\mid m$.

用裴蜀定理很好证明。
对于 $ax+by=\gcd(a,b)$，我们得到了一组特解 x_0,y_0，则 $ax+by=m$ 有特解 $x_0\prime=\frac{m}{\gcd(a,b)}\times x_0, y_0\prime=\frac{m}{\gcd(a,b)}\times y_0$，
通解为：

$$\begin{cases} x=\frac{m}{\gcd(a,b)}\times x_0+k\times\frac{b}{\gcd(a,b)} \\ y=\frac{m}{\gcd(a,b)}\times y_0-k\times\frac{a}{\gcd(a,b)} \end{cases} \quad k\in\mathbb{Z}$$

模意义下除法（乘法逆元）

回到对乘法逆元的求解上，求一个数 a 在模 m 意义下的乘法逆元相当于求解线性同余方程：

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

显然当且仅当 $\gcd(a, m) = 1$ 时 a 才会有乘法逆元。
考虑简单情况：当 m 为一个质数时，a 的乘法逆元有什么简便的求法吗？
答案是肯定的，$a^{-1} \equiv a^{m-2} \pmod{m}$.

模意义下除法（乘法逆元）

回到对乘法逆元的求解上，求一个数 a 在模 m 意义下的乘法逆元相当于求解线性同余方程：

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

显然当且仅当 $\gcd(a, m) = 1$ 时 a 才会有乘法逆元。
考虑简单情况：当 m 为一个质数时，a 的乘法逆元有什么简便的求法吗？
答案是肯定的，$a^{-1} \equiv a^{m-2} \pmod{m}$.

模意义下除法（乘法逆元）

回到对乘法逆元的求解上，求一个数 a 在模 m 意义下的乘法逆元相当于求解线性同余方程：

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

显然当且仅当 $\gcd(a, m) = 1$ 时 a 才会有乘法逆元。
考虑简单情况：当 m 为一个质数时，a 的乘法逆元有什么简便的求法吗？
答案是肯定的，$a^{-1} \equiv a^{m-2} \pmod{m}$.

同余类与剩余系

同余类的定义

由于同余关系为等价关系，因此对于模数 m，可以把整数划分为 m 个等价类，其中第 $i, 0 \leq i < m$ 个等价类中的数模 m 等于 i. 这 m 个集合均称为 m 的同余类，也叫剩余类。

完全剩余系

对 m 个整数 $a_1, a_2, \ldots, a_m$，若对任意的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 m 个整数 $a_1, a_2, \ldots, a_m$ 为模 m 的完全剩余系，简称剩余系。

最小非负剩余系：$0, 1, \ldots m-1$.

同余类与剩余系

同余类的定义

由于同余关系为等价关系，因此对于模数 m，可以把整数划分为 m 个等价类，其中第 $i, 0 \le i < m$ 个等价类中的数模 m 等于 i. 这 m 个集合均称为 m 的同余类，也叫剩余类。

完全剩余系

对 m 个整数 $a_1, a_2, \ldots, a_m$，若对任意的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 m 个整数 $a_1, a_2, \ldots, a_m$ 为模 m 的完全剩余系，简称剩余系。

最小非负剩余系：$0, 1, \ldots m-1$.

同余类与剩余系

同余类的定义

由于同余关系为等价关系，因此对于模数 m，可以把整数划分为 m 个等价类，其中第 $i, 0 \leq i < m$ 个等价类中的数模 m 等于 i. 这 m 个集合均称为 m 的同余类，也叫剩余类。

完全剩余系

对 m 个整数 $a_1, a_2, \ldots, a_m$，若对任意的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 m 个整数 $a_1, a_2, \ldots, a_m$ 为模 m 的完全剩余系，简称剩余系。

最小非负剩余系：$0, 1, \ldots m-1$.

同余类与剩余系

完全剩余系的性质：
若 $\gcd(b,m)=1, a_1,\dots,a_m$ 为一个完全剩余系，则
$b\times a_i+c, 1\le i\le m$ 也为一个完全剩余系。
例题：若 p 为质数，a 为给定数，证明当 x 为 0 到 $p-1$，ax 在模 p 的意义下互不相同。
$0,a,2a,\dots,(p-1)a$ 构成一个模 p 意义下的完全剩余系。

同余类与剩余系

完全剩余系的性质：
若 $\gcd(b, m) = 1, a_1, \ldots, a_m$ 为一个完全剩余系，则 $b \times a_i + c, 1 \le i \le m$ 也为一个完全剩余系。
例题：若 p 为质数，a 为给定数，证明当 x 为 0 到 $p-1$，ax 在模 p 的意义下互不相同。
$0, a, 2a, \ldots, (p-1)a$ 构成一个模 p 意义下的完全剩余系。

同余类与剩余系

完全剩余系的性质：
若 $\gcd(b,m)=1, a_1,\ldots,a_m$ 为一个完全剩余系，则 $b\times a_i+c, 1\le i\le m$ 也为一个完全剩余系。
例题：若 p 为质数，a 为给定数，证明当 x 为 0 到 $p-1$，ax 在模 p 的意义下互不相同。
$0, a, 2a, \ldots, (p-1)a$ 构成一个模 p 意义下的完全剩余系。

同余类与剩余系

例题：$ax\%m$ 一定为 $\gcd(a,m)$ 的倍数，且当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时互不相同。

$$
\begin{aligned}
&ax\%m\\
=&(\gcd(a,m)\times\frac{a}{\gcd(a,m)}\times x)\%(\gcd(a,m)\times\frac{m}{\gcd(a,m)})\\
=&\gcd(a,m)(\frac{a}{\gcd(a,m)}\times x\%\frac{m}{\gcd(a,m)})
\end{aligned}
$$

由于 $\frac{a}{\gcd(a,m)}$ 与 $\frac{m}{\gcd(a,m)}$ 互质，
因此当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时，
$\frac{a}{\gcd(a,m)}\times x$ 构成了一个模 $\frac{m}{\gcd(a,m)}$ 意义下的完全剩余系。得证。

同余类与剩余系

例题：$ax\%m$ 一定为 $\gcd(a,m)$ 的倍数，且当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时互不相同。

$$
\begin{aligned}
&ax\%m\\
=&(\gcd(a,m)\times\frac{a}{\gcd(a,m)}\times x)\%(\gcd(a,m)\times\frac{m}{\gcd(a,m)})\\
=&\gcd(a,m)(\frac{a}{\gcd(a,m)}\times x\%\frac{m}{\gcd(a,m)})
\end{aligned}
$$

由于 $\frac{a}{\gcd(a,m)}$ 与 $\frac{m}{\gcd(a,m)}$ 互质，
因此当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时，
$\frac{a}{\gcd(a,m)}\times x$ 构成了一个模 $\frac{m}{\gcd(a,m)}$ 意义下的完全剩余系。得证。

同余类与剩余系

例题：$ax\%m$ 一定为 $\gcd(a,m)$ 的倍数，且当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时互不相同。

$$\begin{aligned}&ax\%m\\=&(\gcd(a,m)\times\frac{a}{\gcd(a,m)}\times x)\%(\gcd(a,m)\times\frac{m}{\gcd(a,m)})\\=&\gcd(a,m)(\frac{a}{\gcd(a,m)}\times x\%\frac{m}{\gcd(a,m)})\end{aligned}$$

由于 $\frac{a}{\gcd(a,m)}$ 与 $\frac{m}{\gcd(a,m)}$ 互质，
因此当 x 为 0 到 $\frac{m}{\gcd(a,m)}-1$ 时，
$\frac{a}{\gcd(a,m)}\times x$ 构成了一个模 $\frac{m}{\gcd(a,m)}$ 意义下的完全剩余系。得证。

同余类与剩余系

既约同余类

对同余类 $r \bmod m$，若 $(r,m)=1$，则称该同余类为既约同余类或既约剩余类。我们把模 m 既约剩余类的个数记作 $\varphi(m)$，$\varphi(m)$ 称为欧拉函数。

既约剩余系

对 $t=\varphi(m)$ 个整数 $a_1,a_2,\ldots,a_t$，若 $(a_i,m)=1,\forall 1\le i\le t$，且对任意满足 $(x,m)=1$ 的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 t 个整数 $a_1,a_2,\ldots,a_t$ 为模 m 的既约剩余系、缩剩余系或简化剩余系。

最小非负既约剩余系：$0,1,\ldots m-1$ 中与 m 互质的数构成的剩余系。

同余类与剩余系

既约同余类

对同余类 $r \bmod m$，若 $(r,m)=1$，则称该同余类为既约同余类或既约剩余类。我们把模 m 既约剩余类的个数记作 $\varphi(m)$，$\varphi(m)$ 称为欧拉函数。

既约剩余系

对 $t=\varphi(m)$ 个整数 $a_1,a_2,\ldots,a_t$，若 $(a_i,m)=1,\forall 1\le i\le t$，且对任意满足 $(x,m)=1$ 的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 t 个整数 $a_1,a_2,\ldots,a_t$ 为模 m 的既约剩余系、缩剩余系或简化剩余系。

最小非负既约剩余系：$0,1,\ldots m-1$ 中与 m 互质的数构成的剩余系。

同余类与剩余系

既约同余类

对同余类 $r \bmod m$，若 $(r, m) = 1$，则称该同余类为既约同余类或既约剩余类。我们把模 m 既约剩余类的个数记作 $\varphi(m)$，$\varphi(m)$ 称为欧拉函数。

既约剩余系

对 $t = \varphi(m)$ 个整数 $a_1, a_2, \ldots, a_t$，若 $(a_i, m) = 1, \forall 1 \leq i \leq t$，且对任意满足 $(x, m) = 1$ 的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 t 个整数 $a_1, a_2, \ldots, a_t$ 为模 m 的既约剩余系、缩剩余系或简化剩余系。

最小非负既约剩余系：$0, 1, \ldots m-1$ 中与 m 互质的数构成的剩余系。

三个重要数论定理

威尔逊定理

若 p 为素数，则 $(p-1)! \equiv -1 \pmod p$，相当于 $(p-1)! \equiv p-1 \pmod p$.

proof.

$p=2$ 时，显然成立。

p 为奇质数时，$\forall a \in [1, p-1]$，有且仅有一个 b，使得 $ab \equiv 1 \pmod p$.

因为 $0, a, 2a, \ldots (p-1)a$ 为模 p 意义下的一个完全剩余系，因此这些数互不相同，且遍历 0 到 $p-1$，其中 $a, 2a, \ldots (p-1)a$ 遍历 1 到 $p-1$.

当 $a=b$ 时，即 $a^2 \equiv 1 \pmod p$，$a=1$ 或 $-1(p-1)$.

因此 $(p-1)! \equiv 1 \times 1 \times (p-1) \equiv p-1 \equiv -1 \pmod p$.

证毕。

三个重要数论定理

威尔逊定理

若 p 为素数，则 $(p-1)! \equiv -1 \pmod{p}$，相当于 $(p-1)! \equiv p-1 \pmod{p}$.

proof.
$p=2$ 时，显然成立。
p 为奇质数时，$\forall a \in [1, p-1]$，有且仅有一个 b，使得 $ab \equiv 1 \pmod{p}$.
因为 $0, a, 2a, \ldots (p-1)a$ 为模 p 意义下的一个完全剩余系，因此这些数互不相同，且遍历 0 到 $p-1$，其中 $a, 2a, \ldots (p-1)a$ 遍历 1 到 $p-1$.
当 $a=b$ 时，即 $a^2 \equiv 1 \pmod{p}$，$a=1$ 或 $-1(p-1)$.
因此 $(p-1)! \equiv 1 \times 1 \times (p-1) \equiv p-1 \equiv -1 \pmod{p}$.
证毕。

三个重要数论定理

费马小定理

若 p 为素数，$\gcd(a,p)=1$，则 $a^{(p-1)} \equiv 1 \pmod{p}$.

proof.
由于 $\gcd(a,p)=1$，因此 $0,a,2a,\ldots,(p-1)a$ 为模 p 意义下的一个完全剩余系，因此有：

$$a \times 2a \times \cdots \times (p-1)a \equiv \times (p-1)! \pmod{p}$$

而 $a \times 2a \times \cdots \times (p-1)a = a^{p-1}(p-1)!$,
因此

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

证毕。

三个重要数论定理

费马小定理

若 p 为素数，$\gcd(a,p)=1$，则 $a^{(p-1)} \equiv 1 \pmod p$.

proof.
由于 $\gcd(a,p)=1$，因此 $0, a, 2a, \ldots, (p-1)a$ 为模 p 意义下的一个完全剩余系，因此有：

$$a \times 2a \times \cdots \times (p-1)a \equiv \times (p-1)! \pmod p$$

而 $a \times 2a \times \cdots \times (p-1)a = a^{p-1}(p-1)!$，
因此

$$\begin{aligned} a^{p-1}(p-1)! &\equiv (p-1)! \pmod p \\ a^{p-1} &\equiv 1 \pmod p \end{aligned}$$

证毕。

三个重要数论定理

拓展欧拉定理

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

证明略。

三个重要数论定理

例题：求

$$a^{a^{a^{\cdots}}} \mod m$$

的值，其中 a 一共有 k 层。

设 $f(a,k,m)$ 为 a 的 k 层幂塔对 m 取模的结果，则：

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1 \\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m) \\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m) \\ 1 & k=0\text{或}m=1 \end{cases}$$

三个重要数论定理

例题：求

$$a^{a^{a^{\cdots}}} \bmod m$$

的值，其中 a 一共有 k 层。
设 $f(a,k,m)$ 为 a 的 k 层幂塔对 m 取模的结果，则：

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1 \\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m) \\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m) \\ 1 & k=0\text{或}m=1 \end{cases}$$

三个重要数论定理

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1 \\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m) \\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m) \\ 1 & k=0\text{或}m=1 \end{cases}$$

$f(a,k-1,\varphi(m))$ 与 $\varphi(m)$ 的大小关系可以通过一直取以 a 为底的对数递归比较。

由于欧拉函数下降得非常快（不超过 $O(\log m)$ 层），因此递归的层数不会太多。

洛谷 P4139 上帝与集合的正确用法。

2019ICPC 南京网络赛 B super log。

三个重要数论定理

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1\\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m)\\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m)\\ 1 & k=0\text{或}m=1 \end{cases}$$

$f(a,k-1,\varphi(m))$ 与 $\varphi(m)$ 的大小关系可以通过一直取以 a 为底的对数递归比较。

由于欧拉函数下降得非常快（不超过 $O(\log m)$ 层），因此递归的层数不会太多。

洛谷 P4139 上帝与集合的正确用法。

2019ICPC 南京网络赛 B super log。

三个重要数论定理

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1 \\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m) \\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m) \\ 1 & k=0\text{或}m=1 \end{cases}$$

$f(a,k-1,\varphi(m))$ 与 $\varphi(m)$ 的大小关系可以通过一直取以 a 为底的对数递归比较。

由于欧拉函数下降得非常快（不超过 $O(\log m)$ 层），因此递归的层数不会太多。

洛谷 P4139 上帝与集合的正确用法。

2019ICPC 南京网络赛 B super log。

三个重要数论定理

$$f(a,k,m)=\begin{cases} a^{f(a,k-1,\varphi(m))}\%m, & \gcd(a,m)=1 \\ a^{f(a,k-1,\varphi(m))}\%m, & f(a,k-1,\varphi(m))<\varphi(m) \\ a^{f(a,k-1,\varphi(m))+\varphi(m)}\%m, & f(a,k-1,\varphi(m))\geq\varphi(m) \\ 1 & k=0\text{或}m=1 \end{cases}$$

$f(a,k-1,\varphi(m))$ 与 $\varphi(m)$ 的大小关系可以通过一直取以 a 为底的对数递归比较。
由于欧拉函数下降得非常快（不超过 $O(\log m)$ 层），因此递归的层数不会太多。
洛谷 P4139 上帝与集合的正确用法。
2019ICPC 南京网络赛 B super log。

模意义下除法（乘法逆元）

回到当 m 为一个质数时，a 的乘法逆元为 $a^{m-2}\%m$.
用费马小定理可以轻松证明。
至此，我们用大量的篇幅学习了乘法逆元的解法，使用拓展欧几里得算法或者快速幂都可以在 $O(\log n)$ 的时间内求出一个数的乘法逆元。

模意义下除法（乘法逆元）

回到当 m 为一个质数时，a 的乘法逆元为 $a^{m-2}\% m$.
用费马小定理可以轻松证明。
至此，我们用大量的篇幅学习了乘法逆元的解法，使用拓展欧几里得算法或者快速幂都可以在 $O(\log n)$ 的时间内求出一个数的乘法逆元。

模意义下开根（k 次剩余）

k 次剩余

令整数 $k \geq 2$，整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^k \equiv a \pmod{m}$$

则称 a 为模 m 的 k 次剩余，否则称 a 为模 m 的 k 次非剩余。

二次剩余

整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^2 \equiv a \pmod{m}$$

则称 a 为模 m 的二次剩余，否则称 a 为模的二次非剩余。

求解二次剩余可以使用 Cipolla 算法。

模意义下开根（k 次剩余）

k 次剩余

令整数 $k \geq 2$，整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^k \equiv a \pmod{m}$$

则称 a 为模 m 的 k 次剩余，否则称 a 为模 m 的 k 次非剩余。

二次剩余

整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^2 \equiv a \pmod{m}$$

则称 a 为模 m 的二次剩余，否则称 a 为模的二次非剩余。

求解二次剩余可以使用 Cipolla 算法。

模意义下开根（k 次剩余）

k 次剩余

令整数 $k \geq 2$，整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^k \equiv a \pmod{m}$$

则称 a 为模 m 的 k 次剩余，否则称 a 为模 m 的 k 次非剩余。

二次剩余

整数 a, m 满足 $\gcd(a, m) = 1$，若存在整数 x，使得

$$x^2 \equiv a \pmod{m}$$

则称 a 为模 m 的二次剩余，否则称 a 为模的二次非剩余。

求解二次剩余可以使用 Cipolla 算法。

模意义下取对数（离散对数）

离散对数

给定整数 a, b, m，求解

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

x 即为以 a 为底，模 m 意义下的离散对数。

当 p 为质数时，采用 BSGS（大步小步）算法，可在 $O(\sqrt{m})$ 的时间内解决该问题。
当 p 不保证为质数时，采用 exBSGS 算法可以解决该问题。

模意义下取对数（离散对数）

离散对数

给定整数 a, b, m，求解

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

x 即为以 a 为底，模 m 意义下的离散对数。

当 p 为质数时，采用 BSGS（大步小步）算法，可在 $O(\sqrt{m})$ 的时间内解决该问题。

当 p 不保证为质数时，采用 exBSGS 算法可以解决该问题。

模意义下取对数（离散对数）

离散对数

给定整数 a, b, m，求解

$$x^a \equiv b \pmod m$$

x 即为以 a 为底，模 m 意义下的离散对数。

当 p 为质数时，采用 BSGS（大步小步）算法，可在 $O(\sqrt{m})$ 的时间内解决该问题。
当 p 不保证为质数时，采用 exBSGS 算法可以解决该问题。

模意义下取对数（离散对数）

当模数为质数 p 时，采用 BSGS 算法。

$$x^a \equiv b \pmod p$$

令 $t = \lfloor \sqrt{p} \rfloor$，则 a 可以表示为 $i \times t - j, 0 \le i \le t, 0 \le j < t$。方程化为

$$x^{i \times t} \equiv b \times x^j \pmod p$$

其中 $b \times x^j \% p$ 共有 t 种取值，可以提前放进一个 hash 表里。然后枚举 $x^{i \times t} \% p$，在 hash 表里查找是否有这个值，若有，则找到了一个解。

模意义下取对数（离散对数）

当模数为质数 p 时，采用 BSGS 算法。

$$x^a \equiv b \pmod p$$

令 $t = \lfloor \sqrt{p} \rfloor$，则 a 可以表示为 $i \times t - j, 0 \le i \le t, 0 \le j < t$。
方程化为

$$x^{i \times t} \equiv b \times x^j \pmod p$$

其中 $b \times x^j \% p$ 共有 t 种取值，可以提前放进一个 hash 表里。
然后枚举 $x^{i \times t} \% p$，在 hash 表里查找是否有这个值，若有，则找到了一个解。

线性同余方程组

之前我们通过 exgcd 求解了线性同余方程，现在我们来试着对一组线性同余方程求解：

$$\begin{cases} x \equiv a_1 \pmod{m}_1 \\ x \equiv a_2 \pmod{m}_2 \\ \dots \\ x \equiv a_k \pmod{m}_k \end{cases}$$

若 $m_1, m_2, \dots, m_k$ 两两互质，则可以采用中国剩余定理（CRT）求解，否则采用拓展中国剩余定理（exCRT）求解。

线性同余方程组

例子：一群大学生分组完成小组作业。3 个人一组，会有 1 个人没有分到组；5 个人一组，会有 1 个人没有分到组；7 个人一组，会有 2 个人没有分到组。问最少有多少个大学生。

相当于解同余方程：

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

线性同余方程组

例子：一群大学生分组完成小组作业。3 个人一组，会有 1 个人没有分到组；5 个人一组，会有 1 个人没有分到组；7 个人一组，会有 2 个人没有分到组。问最少有多少个大学生。
相当于解同余方程：

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

线性同余方程组

我们可以构造三个值 x_1, x_2, x_3：

$$\begin{cases} x_1 \equiv 1 \pmod 3 \\ x_1 \equiv 0 \pmod 5 \\ x_1 \equiv 0 \pmod 7 \end{cases} \quad \begin{cases} x_2 \equiv 0 \pmod 3 \\ x_2 \equiv 1 \pmod 5 \\ x_2 \equiv 0 \pmod 7 \end{cases} \quad \begin{cases} x_3 \equiv 0 \pmod 3 \\ x_3 \equiv 0 \pmod 5 \\ x_3 \equiv 2 \pmod 7 \end{cases}$$

求解 x_3 相当于找到 15 在模 7 意义下的逆元，将 15 与逆元相乘后再乘上余数 2，即得到 x_3，x_3 一定满足上式。解 x_1, x_2 同理。
$x = (x_1 + x_2 + x_3)\%(3 \times 5 \times 7) = 16.$

线性同余方程组

我们可以构造三个值 x_1, x_2, x_3:

$$
\begin{cases} x_1 \equiv 1 \pmod 3 \\ x_1 \equiv 0 \pmod 5 \\ x_1 \equiv 0 \pmod 7 \end{cases}
\begin{cases} x_2 \equiv 0 \pmod 3 \\ x_2 \equiv 1 \pmod 5 \\ x_2 \equiv 0 \pmod 7 \end{cases}
\begin{cases} x_3 \equiv 0 \pmod 3 \\ x_3 \equiv 0 \pmod 5 \\ x_3 \equiv 2 \pmod 7 \end{cases}
$$

求解 x_3 相当于找到 15 在模 7 意义下的逆元，将 15 与逆元相乘后再乘上余数 2，即得到 x_3，x_3 一定满足上式。解 x_1, x_2 同理。
$x = (x_1 + x_2 + x_3)\%(3 \times 5 \times 7) = 16.$

线性同余方程组

中国剩余定理（CRT）的过程：

1. 计算所有模数的积 m.
2. 对于第 i 个方程：
   计算 $n_i = \frac{m}{m_i}$
   计算 n_i 在模 m_i 意义下的逆元 n_i^{-1}
   计算 $c_i = n_i n_i^{-1}$，不需要取模
3. $x = \sum_{i=1}^{k} c_i a_i \pmod{m}$

拓展中国剩余定理（exCRT）请自学。

线性同余方程组

中国剩余定理（CRT）的过程：

1. 计算所有模数的积 m.
2. 对于第 i 个方程：
   计算 $n_i = \frac{m}{m_i}$
   计算 n_i 在模 m_i 意义下的逆元 n_i^{-1}
   计算 $c_i = n_i n_i^{-1}$，不需要取模
3. $x = \sum_{i=1}^{k} c_i a_i \pmod{m}$

拓展中国剩余定理（exCRT）请自学。

阶与原根

阶的定义

设 $a > 2, \gcd(a, m) = 1$，d 为满足 $a^d \equiv 1 \pmod{m}$ 的最小正整数，则称 d 为 a 模 m 的阶，记为 $\delta_m(a)$.

性质：

1. 若 $a^c \equiv 1 \pmod{m}$，则 $\delta_m(a) \mid c$，显然 $\delta_m(a) \mid \varphi(m)$.
2. $a, a^2, \ldots, a^{\delta_m(a)}$ 两两不同余。

阶与原根

阶的定义

设 $a>2, \gcd(a,m)=1$，d 为满足 $a^d \equiv 1 \pmod m$ 的最小正整数，则称 d 为 a 模 m 的阶，记为 $\delta_m(a)$.

性质：

1. 若 $a^c \equiv 1 \pmod m$，则 $\delta_m(a) \mid c$，显然 $\delta_m(a) \mid \varphi(m)$.
2. $a, a^2, \ldots, a^{\delta_m(a)}$ 两两不同余。

阶与原根

原根的定义

若 $g>2, \gcd(g,m)=1, \delta_m(g)=\varphi(m)$，则称 g 为模 m 的原根。

性质：

1. $g^0, g^1, \ldots, g^{\varphi(m)}$ 遍历模 m 的既约剩余系。
   当 m 为质数时，遍历其完全剩余系。
2. 若模 m 有原根，则其原根个数为 $\varphi(\varphi(m))$
3. 若模 m 有原根，则其最小原根不超过 $O(m^{0.25})$ 数量级；

阶与原根

原根的定义

若 $g>2, \gcd(g,m)=1, \delta_m(g)=\varphi(m)$，则称 g 为模 m 的原根。

性质：

1. $g^0, g^1, \ldots, g^{\varphi(m)}$ 遍历模 m 的既约剩余系。
   当 m 为质数时，遍历其完全剩余系。
2. 若模 m 有原根，则其原根个数为 $\varphi(\varphi(m))$
3. 若模 m 有原根，则其最小原根不超过 $O(m^{0.25})$ 数量级；

阶与原根

原根判定定理

设 $m \geq 3, \gcd(g, m) = 1$，则 g 是模 m 的原根的充要条件是，对于 $\varphi(m)$ 的每个质因数 p，都有 $g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$.

原根存在定理

一个数 m 存在原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇质数，$\alpha \in \mathbb{N}^*$.

寻找原根可以用原根判定定理暴力枚举。

阶与原根

原根判定定理

设 $m \geq 3, \gcd(g, m) = 1$，则 g 是模 m 的原根的充要条件是，对于 $\varphi(m)$ 的每个质因数 p，都有 $g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$.

原根存在定理

一个数 m 存在原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇质数，$\alpha \in \mathbb{N}^*$.

寻找原根可以用原根判定定理暴力枚举。

阶与原根

原根判定定理

设 $m \geq 3, \gcd(g, m) = 1$，则 g 是模 m 的原根的充要条件是，对于 $\varphi(m)$ 的每个质因数 p，都有 $g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$.

原根存在定理

一个数 m 存在原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇质数，$\alpha \in \mathbb{N}^*$.

寻找原根可以用原根判定定理暴力枚举。

目录

知识点

1. 积性函数：欧拉函数，莫比乌斯函数……
2. 线性筛
3. 莫比乌斯反演，数论分块

积性函数

在讲既约剩余系的时候，我们提到了欧拉函数的概念。
$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的数量。
欧拉函数是数论当中一个非常重要的函数，它和其他的一类函数都具有一些有趣的性质。
这类函数称为积性函数。

积性函数

数论函数

定义域为正整数的函数称为数论函数。

积性函数

若函数 $f(n)$ 满足 $f(1)=1$ 且 $\forall x,y\in\mathbf{N}^*,\gcd(x,y)=1$ 都有 $f(xy)=f(x)f(y)$，则函数 $f(n)$ 为积性函数。

完全积性函数

若函数 $f(n)$ 满足 $f(1)=1$ 且 $\forall x,y\in\mathbf{N}^*$ 都有 $f(xy)=f(x)f(y)$，则函数 $f(n)$ 为完全积性函数。

积性函数

数论函数

定义域为正整数的函数称为数论函数。

积性函数

若函数 $f(n)$ 满足 $f(1) = 1$ 且 $\forall x, y \in \mathbf{N}^*, \gcd(x, y) = 1$ 都有 $f(xy) = f(x)f(y)$，则函数 $f(n)$ 为积性函数。

完全积性函数

若函数 $f(n)$ 满足 $f(1) = 1$ 且 $\forall x, y \in \mathbf{N}^*$ 都有 $f(xy) = f(x)f(y)$，则函数 $f(n)$ 为完全积性函数。

积性函数

数论函数

定义域为正整数的函数称为数论函数。

积性函数

若函数 $f(n)$ 满足 $f(1)=1$ 且 $\forall x,y\in\mathbf{N}^*,\gcd(x,y)=1$ 都有 $f(xy)=f(x)f(y)$，则函数 $f(n)$ 为积性函数。

完全积性函数

若函数 $f(n)$ 满足 $f(1)=1$ 且 $\forall x,y\in\mathbf{N}^*$ 都有 $f(xy)=f(x)f(y)$，则函数 $f(n)$ 为完全积性函数。

积性函数

积性函数的性质：
若 $f(n), g(n)$ 为积性函数，则以下函数也为积性函数：

1. $h(n) = f(n^p)$
2. $h(n) = f^p(n)$
3. $h(n) = f(n)g(n)$
4. $h(n) = \sum_{d|n} f(d)g(\frac{n}{d})$（狄利克雷卷积）

积性函数

积性函数的性质：
若 $f(n), g(n)$ 为积性函数，则以下函数也为积性函数：

1. $h(n) = f(n^p)$
2. $h(n) = f^p(n)$
3. $h(n) = f(n)g(n)$
4. $h(n) = \sum_{d|n} f(d)g(\frac{n}{d})$ (狄利克雷卷积)

积性函数

常见的积性函数：

1. 单位函数：$\varepsilon(n) = [n = 1]$（完全积性）
2. 恒等函数：$id_k(n) = n^k$，$id_1(n)$ 通常记为 $id(n)$（完全积性）
3. 常数函数：$I(n) = 1$（完全积性）
4. 除数函数：$\sigma_k(n) = \sum_{d|n} d^k$，$\sigma_0(n)$ 通常记为 $d(n)$ 或 $\tau(n)$，$\sigma_1(n)$ 通常记为 $\sigma(n)$
5. 欧拉函数：$\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$
6. 莫比乌斯函数：$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \exists d > 1, d^2 \mid n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$ 其中 $\omega(n)$ 表示 n 的本质不同的质因子个数。

积性函数

常见的积性函数：

1. 单位函数：$\varepsilon(n) = [n = 1]$（完全积性）
2. 恒等函数：$id_k(n) = n^k$，$id_1(n)$ 通常记为 $id(n)$（完全积性）
3. 常数函数：$I(n) = 1$（完全积性）
4. 除数函数：$\sigma_k(n) = \sum_{d|n} d^k$，$\sigma_0(n)$ 通常记为 $d(n)$ 或 $\tau(n)$，$\sigma_1(n)$ 通常记为 $\sigma(n)$
5. 欧拉函数：$\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$
6. 莫比乌斯函数：$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \exists d > 1, d^2 \mid n \text{ 其中} \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$

   $\omega(n)$ 表示 n 的本质不同的质因子个数。

欧拉函数

欧拉函数的定义

$$\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$$

欧拉函数的公式：
设 n 的本质不同的质因子分别为 $p_1, p_2, \dots, p_k$，
则：

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

因此求一个数的欧拉函数可以在分解质因数的同时求解，时间复杂度为 $O(\sqrt{n})$.

欧拉函数

欧拉函数的定义

$$\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$$

欧拉函数的公式：
设 n 的本质不同的质因子分别为 $p_1, p_2, \ldots, p_k$，
则：

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

因此求一个数的欧拉函数可以在分解质因数的同时求解，时间复杂度为 $O(\sqrt{n})$.

欧拉函数

欧拉函数的定义

$$\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$$

欧拉函数的公式：
设 n 的本质不同的质因子分别为 $p_1, p_2, \ldots, p_k$，
则：

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

因此求一个数的欧拉函数可以在分解质因数的同时求解，时间复杂度为 $O(\sqrt{n})$.

欧拉函数

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

proof.
设 n 的质因子为 p, q,
则与 n 互质的数的集合需要除去 $p, 2p, 3p, \ldots, \lfloor\frac{n}{p}\rfloor p$，共 $\lfloor\frac{n}{p}\rfloor$ 个数,
以及 $q, 2q, 3q, \ldots, \lfloor\frac{n}{q}\rfloor q$，共 $\lfloor\frac{n}{q}\rfloor$ 个数,
同时加上 $pq, 2pq, 3pq, \ldots, \lfloor\frac{n}{pq}\rfloor pq$，共 $\lfloor\frac{n}{pq}\rfloor$ 个数（容斥原理）,

欧拉函数

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

proof.
设 n 的质因子为 p, q,
则与 n 互质的数的集合需要除去 $p, 2p, 3p, \ldots, \lfloor\frac{n}{p}\rfloor p$，共 $\lfloor\frac{n}{p}\rfloor$ 个数，
以及 $q, 2q, 3q, \ldots, \lfloor\frac{n}{q}\rfloor q$，共 $\lfloor\frac{n}{q}\rfloor$ 个数，
同时加上 $pq, 2pq, 3pq, \ldots, \lfloor\frac{n}{pq}\rfloor pq$，共 $\lfloor\frac{n}{pq}\rfloor$ 个数（容斥原理），

欧拉函数

因此

$$\varphi(n) = n - \lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{q} \rfloor + \lfloor \frac{n}{pq} \rfloor$$
$$= n(1 - \frac{1}{p})(1 - \frac{1}{q})$$

同理可证 $\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$.

欧拉函数

因此

$$\varphi(n) = n - \lfloor\frac{n}{p}\rfloor - \lfloor\frac{n}{q}\rfloor + \lfloor\frac{n}{pq}\rfloor$$
$$= n(1 - \frac{1}{p})(1 - \frac{1}{q})$$

同理可证 $\varphi(n) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i})$.

欧拉函数

证明欧拉函数是积性函数。

proof.

设 n 的质因子为 $p_1, p_2, \ldots, p_l$，m 的质因子为 $q_1, q_2, \ldots, q_r$，且 $\gcd(n, m) = 1$

则 nm 的质因子为 $p_1, p_2, \ldots, p_l, q_1, q_2, \ldots, q_r$，

$$\begin{aligned}\varphi(nm) &= nm\prod_{i=1}^{l}(1-\frac{1}{p_i})\prod_{j=1}^{r}(1-\frac{1}{q_j}) \\ &= (n\prod_{i=1}^{l}(1-\frac{1}{p_i}))(m\prod_{j=1}^{r}(1-\frac{1}{q_j})) \\ &= \varphi(n)\varphi(m)\end{aligned}$$

欧拉函数

证明欧拉函数是积性函数。

proof.

设 n 的质因子为 $p_1, p_2, \ldots, p_l$， m 的质因子为 $q_1, q_2, \ldots, q_r$， 且 $\gcd(n, m) = 1$

则 nm 的质因子为 $p_1, p_2, \ldots, p_l, q_1, q_2, \ldots, q_r$，

$$
\begin{aligned}
\varphi(nm) &= nm \prod_{i=1}^{l}(1 - \frac{1}{p_i}) \prod_{j=1}^{r}(1 - \frac{1}{q_j}) \\
&= (n \prod_{i=1}^{l}(1 - \frac{1}{p_i}))(m \prod_{j=1}^{r}(1 - \frac{1}{q_j})) \\
&= \varphi(n)\varphi(m)
\end{aligned}
$$

欧拉函数

结论：

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

即 $\varphi * I = id$

proof.

若 $\gcd(a, b) = d$，则 $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

设 $f(x)$ 表示 $\gcd(k, n) = x$ 的 k 的个数，则 $n = \sum_{d|n} f(d)$

而 $f(d) = \varphi(\frac{n}{d})$，

因此 $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$.

欧拉函数

结论:

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

即 $\varphi * I = id$

proof.

若 $\gcd(a,b) = d$，则 $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

设 $f(x)$ 表示 $\gcd(k,n) = x$ 的 k 的个数，则 $n = \sum_{d|n} f(d)$

而 $f(d) = \varphi(\frac{n}{d})$，

因此 $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$.

莫比乌斯函数

莫比乌斯函数的定义

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \exists d > 1, d^2 \mid n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$$

其中 $\omega(n)$ 表示 n 的本质不同的质因子个数。

容易证明莫比乌斯函数是积性函数，只需针对以上三种情况分类讨论即可。

莫比乌斯函数的应用：容斥原理；莫比乌斯反演；

莫比乌斯函数

莫比乌斯函数的定义

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \exists d > 1, d^2 \mid n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$$

其中 $\omega(n)$ 表示 n 的本质不同的质因子个数。

容易证明莫比乌斯函数是积性函数，只需针对以上三种情况分类讨论即可。

莫比乌斯函数的应用：容斥原理；莫比乌斯反演；

莫比乌斯函数

莫比乌斯函数的定义

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \exists d > 1, d^2 \mid n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$$

其中 $\omega(n)$ 表示 n 的本质不同的质因子个数。

容易证明莫比乌斯函数是积性函数，只需针对以上三种情况分类讨论即可。

莫比乌斯函数的应用：容斥原理；莫比乌斯反演；

莫比乌斯函数

莫比乌斯函数的性质：

$$\sum_{d|n}\mu(d)=[n=1]$$

即 $\mu * I = \varepsilon$.

proof.

设 $n=\prod_{i=1}^{k}p_i^{c_i}, n\prime=\prod_{i=1}^{k}p_i$，

则 $\sum_{d|n}\mu(d)=\sum_{d|n\prime}\mu(d)=\sum_{i=0}^{k}\binom{k}{i}\cdot(-1)^i=(1+(-1))^k$

根据二项式定理，当 $k=0$，即 $n=1$ 时，上式为 0，其他时候为 1. 证毕。

莫比乌斯函数

莫比乌斯函数的性质：

$$\sum_{d|n} \mu(d) = [n = 1]$$

即 $\mu * I = \varepsilon$.

proof.

设 $n = \prod_{i=1}^{k} p_i^{c_i}, n\prime = \prod_{i=1}^{k} p_i$,

则 $\sum_{d|n} \mu(d) = \sum_{d|n\prime} \mu(d) = \sum_{i=0}^{k} \binom{k}{i} \cdot (-1)^i = (1 + (-1))^k$

根据二项式定理，当 $k = 0$，即 $n = 1$ 时，上式为 0，其他时候为 1. 证毕。

莫比乌斯函数

莫比乌斯函数的性质：

$$\sum_{d|n} \mu(d) = [n = 1]$$

即 $\mu * I = \varepsilon$.
proof.
设 $n = \prod_{i=1}^{k} p_i^{c_i}, n\prime = \prod_{i=1}^{k} p_i$,
则 $\sum_{d|n} \mu(d) = \sum_{d|n\prime} \mu(d) = \sum_{i=0}^{k} \binom{k}{i} \cdot (-1)^i = (1 + (-1))^k$
根据二项式定理，当 $k = 0$，即 $n = 1$ 时，上式为 0，其他时候为 1. 证毕。

莫比乌斯函数

莫比乌斯函数的性质：

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

即 $\mu * id = \varphi$.

proof.

已经证明 $\varphi * I = id$，以及 $\mu * I = \varepsilon$，

两边同时卷 μ，得：

$$\varphi * I * \mu = id * \mu$$

$$\varphi * \varepsilon = id * \mu$$

$$\varphi = id * \mu$$

莫比乌斯函数

莫比乌斯函数的性质：

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

即 $\mu * id = \varphi$.

proof.

已经证明 $\varphi * I = id$，以及 $\mu * I = \varepsilon$，

两边同时卷 μ，得：

$$\varphi * I * \mu = id * \mu$$

$$\varphi * \varepsilon = id * \mu$$

$$\varphi = id * \mu$$

莫比乌斯函数

莫比乌斯函数的性质：

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

即 $\mu * id = \varphi$.
proof.
已经证明 $\varphi * I = id$，以及 $\mu * I = \varepsilon$，
两边同时卷 μ，得：

$$\begin{aligned} \varphi * I * \mu &= id * \mu \\ \varphi * \varepsilon &= id * \mu \\ \varphi &= id * \mu \end{aligned}$$

莫比乌斯反演

莫比乌斯反演

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

莫比乌斯反演

proof.

$$
\begin{aligned}
&\sum_{d|n} \mu(d) g(\frac{n}{d}) \\
\Leftrightarrow &\sum_{d|n} \mu(\frac{n}{d}) g(d) \\
\Leftrightarrow &\sum_{k|n} \sum_{d|\frac{n}{k}} \mu(\frac{n}{kd}) f(k) \\
\Leftrightarrow &\sum_{k|n} \sum_{d|\frac{n}{k}} \mu(d) f(k) \\
\Leftrightarrow &\sum_{k|n} [\frac{n}{k} = 1] f(k) \\
\Leftrightarrow &f(n)
\end{aligned}
$$

莫比乌斯反演

例题：求

$$\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)=1]$$

莫比乌斯反演

根据 $\sum_{d|n}\mu(d)=[n=1]$

$$
\begin{aligned}
&\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)=1] \\
=&\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d|\gcd(i,j)}\mu(d) \\
=&\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d|i,d|j}\mu(d)
\end{aligned}
$$

莫比乌斯反演

$$
\begin{aligned}
&\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d|i,d|j}\mu(d)\\
=&\sum_{d=1}^{n}\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{d}\rfloor}\mu(d)\\
=&\sum_{d=1}^{n}\mu(d)\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{d}\rfloor}1\\
=&\sum_{d=1}^{n}\mu(d)\lfloor\frac{n}{d}\rfloor\lfloor\frac{m}{d}\rfloor
\end{aligned}
$$

线性筛

下面我们考虑这个问题：如何找出 1 到 n 之间所有的质数?

- 我会对每个数，通过枚举因数的方法判断是否为质数！$O(n\sqrt{n})$
- 我学过埃氏筛！$O(n \ln \ln n)$

那么，可以把复杂度降到 $O(n)$ 吗?

线性筛

下面我们考虑这个问题：如何找出 1 到 n 之间所有的质数？

- 我会对每个数，通过枚举因数的方法判断是否为质数！$O(n\sqrt{n})$
- 我学过埃氏筛！$O(n\ln\ln n)$

那么，可以把复杂度降到 $O(n)$ 吗？

线性筛

下面我们考虑这个问题：如何找出 1 到 n 之间所有的质数？

- 我会对每个数，通过枚举因数的方法判断是否为质数！ $O(n\sqrt{n})$
- 我学过埃氏筛！ $O(n\ln\ln n)$

那么，可以把复杂度降到 $O(n)$ 吗？

线性筛

下面我们考虑这个问题：如何找出 1 到 n 之间所有的质数?

- 我会对每个数，通过枚举因数的方法判断是否为质数！$O(n\sqrt{n})$
- 我学过埃氏筛！$O(n \ln \ln n)$

那么，可以把复杂度降到 $O(n)$ 吗?

线性筛

我们考虑通过对每个数打标记的方法，判断这个数是否是质数。

1. 从 2 开始枚举，如果一个数 i 没有被标记，那么这个数就是质数，将其存放进数组 $prime$；
2. 对于数 i，枚举已经筛出的质数 p_j，将 $i \cdot p_j$ 标记为合数；
3. 若 $p_j \mid i$，则枚举下一个数 $i+1$，即返回第 1 步；否则枚举下一个质数 p_{j+1}，即返回第 2 步；

对于每个合数，只会在枚举其最小质因数时被标记一次，因此时间复杂度为 $O(n)$。

线性筛

我们考虑通过对每个数打标记的方法，判断这个数是否是质数。

1. 从 2 开始枚举，如果一个数 i 没有被标记，那么这个数就是质数，将其存放进数组 $prime$；
2. 对于数 i，枚举已经筛出的质数 p_j，将 $i \cdot p_j$ 标记为合数；
3. 若 $p_j \mid i$，则枚举下一个数 $i+1$，即返回第 1 步；否则枚举下一个质数 p_{j+1}，即返回第 2 步；

对于每个合数，只会在枚举其最小质因数时被标记一次，因此时间复杂度为 $O(n)$。

线性筛

我们考虑通过对每个数打标记的方法，判断这个数是否是质数。

1. 从 2 开始枚举，如果一个数 i 没有被标记，那么这个数就是质数，将其存放进数组 $prime$；
2. 对于数 i，枚举已经筛出的质数 p_j，将 $i \cdot p_j$ 标记为合数；
3. 若 $p_j \mid i$，则枚举下一个数 $i+1$，即返回第 1 步；否则枚举下一个质数 p_{j+1}，即返回第 2 步；

对于每个合数，只会在枚举其最小质因数时被标记一次，因此时间复杂度为 $O(n)$。

线性筛

我们考虑通过对每个数打标记的方法，判断这个数是否是质数。

1. 从 2 开始枚举，如果一个数 i 没有被标记，那么这个数就是质数，将其存放进数组 $prime$；
2. 对于数 i，枚举已经筛出的质数 p_j，将 $i \cdot p_j$ 标记为合数；
3. 若 $p_j \mid i$，则枚举下一个数 $i+1$，即返回第 1 步；否则枚举下一个质数 p_{j+1}，即返回第 2 步；

对于每个合数，只会在枚举其最小质因数时被标记一次，因此时间复杂度为 $O(n)$。

线性筛

我们考虑通过对每个数打标记的方法，判断这个数是否是质数。

1. 从 2 开始枚举，如果一个数 i 没有被标记，那么这个数就是质数，将其存放进数组 $prime$；
2. 对于数 i，枚举已经筛出的质数 p_j，将 $i \cdot p_j$ 标记为合数；
3. 若 $p_j \mid i$，则枚举下一个数 $i+1$，即返回第 1 步；否则枚举下一个质数 p_{j+1}，即返回第 2 步；

对于每个合数，只会在枚举其最小质因数时被标记一次，因此时间复杂度为 $O(n)$。

线性筛

proof.
设 $m=\prod_{i=1}^{k} p_i^{c_i}$，其中 $p_i<p_{i+1}, 1\le i\le k$，
当第 1 步枚举到 $p_1^{c_1-1}\prod_{i=2}^{k} p_i^{c_i}$，第二步枚举到 p_1 时，
m 肯定会被标记。
当第 1 步枚举到 $m\prime=p_i^{c_i-1}\prod_{j=1,j\ne i}^{k} p_j^{c_j}, i\ne 1$ 时，
第 2 步会在枚举到 p_1 的时候，由于 $p_1\mid m\prime$，会停止枚举质数，
开始枚举 $m\prime+1$。
因此每个合数会且仅会被筛一次。

线性筛

```
for(int i=2;i<=n;i++)
{
    if(!mark[i])//是素数。
    prime[++tot]=i//增加一个素数。
    for(int j=1;j<=tot;j++)
    {
        int x=i*prime[j];
        if(x>n)
        break;
        mark[x]=1;//标记倍数为合数。
        if(i%prime[j]==0)
        break;
    }
}
```

图: 线性筛素数模板

线性筛

不止质数，任何积性函数 $f(n)$ 都可以通过线性筛在 $O(n)$ 的时间内将 $f(1)$ 到 $f(n)$ 都筛出来，只要知道以下信息即可：

- $f(p)$ 的求法，p 为质数；
- 当 $p \mid m$ 时 $f(mp)$ 的求法，p 为 m 的最小质因子；

线性筛

```
for(int i=2;i<=n;i++)
{
    if(!mark[i])
    f(i)=...//素数的情况
    for(int j=1;j<=tot;j++)
    {
        int x=i*prime[j];
        if(x>n)
        break;
        if(i%prime[j]==0)
        {
            f(x)=...//p|i的情况
            break;
        }
        else f(x)=f(p)*f(i);
    }
}
```

图: 线性筛积性函数模板

线性筛

以欧拉函数为例：

1. $\varphi(p) = p - 1$,p 为质数；
2. $\varphi(mp) = \varphi(m)\varphi(p) = (p-1)\varphi(m), p \nmid m$；
3. $\varphi(mp) = p\varphi(m), p \mid m$，且 p 为 m 的最小质因子。

数论分块

最后一个问题：
求

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

的值。

数论分块

先研究 $\lfloor \frac{n}{i} \rfloor$，打一个小表：

表: 12/i 下取整

i	1	2	3	4	5	6	7	8	9	10	11	12
$\lfloor \frac{12}{i} \rfloor$	12	6	4	3	2	2	1	1	1	1	1	1

发现可能的取值比较少。
事实上，可能的取值只有不超过 $\lfloor 2\sqrt{n} \rfloor$，即 $O(\sqrt{n})$ 个。
因此可以根据下取整的值进行分块处理。

数论分块

先研究 $\lfloor \frac{n}{i} \rfloor$，打一个小表：

表: 12/i 下取整

i	1	2	3	4	5	6	7	8	9	10	11	12
$\lfloor \frac{12}{i} \rfloor$	12	6	4	3	2	2	1	1	1	1	1	1

发现可能的取值比较少。

事实上，可能的取值只有不超过 $\lfloor 2\sqrt{n} \rfloor$，即 $O(\sqrt{n})$ 个。

因此可以根据下取整的值进行分块处理。

数论分块

先研究 $\lfloor \frac{n}{i} \rfloor$，打一个小表：

表: 12/i 下取整

i	1	2	3	4	5	6	7	8	9	10	11	12
$\lfloor \frac{12}{i} \rfloor$	12	6	4	3	2	2	1	1	1	1	1	1

发现可能的取值比较少。
事实上，可能的取值只有不超过 $\lfloor 2\sqrt{n} \rfloor$，即 $O(\sqrt{n})$ 个。
因此可以根据下取整的值进行分块处理。

数论分块

先研究 $\lfloor \frac{n}{i} \rfloor$，打一个小表：

表: 12/i 下取整

i	1	2	3	4	5	6	7	8	9	10	11	12
$\lfloor \frac{12}{i} \rfloor$	12	6	4	3	2	2	1	1	1	1	1	1

发现可能的取值比较少。
事实上，可能的取值只有不超过 $\lfloor 2\sqrt{n} \rfloor$，即 $O(\sqrt{n})$ 个。
因此可以根据下取整的值进行分块处理。

数论分块

结论：
对于常数 n，使得式子

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

成立且满足 $i \leq j \leq n$ 的 j 最大为 $\lfloor \frac{n}{\lfloor \frac{n}{i} \rfloor} \rfloor$，
即值 $\lfloor \frac{n}{i} \rfloor$ 所在的块的右端点为 $\lfloor \frac{n}{\lfloor \frac{n}{i} \rfloor} \rfloor$.

数论分块

回到问题 $\sum_{i=1}^{n} f(i)\lfloor\frac{n}{i}\rfloor$ 上，
对 $\lfloor\frac{n}{i}\rfloor$ 分块后，假设左右端点分别是 l,r，
那么 $\lfloor\frac{n}{i}\rfloor, l \le i \le r$ 是相等的，
因此该段的答案为 $\lfloor\frac{n}{l}\rfloor\sum_{i=l}^{r} f(i)$。
问题转化为快速求 $f(n)$ 的前缀和：套公式，杜教筛，min25 筛，洲阁筛……

数论分块

回到问题 $\sum_{i=1}^{n} f(i)\lfloor\frac{n}{i}\rfloor$ 上，
对 $\lfloor\frac{n}{i}\rfloor$ 分块后，假设左右端点分别是 l, r，
那么 $\lfloor\frac{n}{i}\rfloor, l \le i \le r$ 是相等的，
因此该段的答案为 $\lfloor\frac{n}{l}\rfloor\sum_{i=l}^{r} f(i)$。
问题转化为快速求 $f(n)$ 的前缀和：套公式，杜教筛，min25 筛，洲阁筛……

数论分块

回到问题 $\sum_{i=1}^{n} f(i)\lfloor\frac{n}{i}\rfloor$ 上，
对 $\lfloor\frac{n}{i}\rfloor$ 分块后，假设左右端点分别是 l, r，
那么 $\lfloor\frac{n}{i}\rfloor, l \le i \le r$ 是相等的，
因此该段的答案为 $\lfloor\frac{n}{l}\rfloor\sum_{i=l}^{r} f(i)$。
问题转化为快速求 $f(n)$ 的前缀和：套公式，杜教筛，min25 筛，洲阁筛……

推荐自学

- miller rabin 素性检测
- pollard rho 大整数质因数分解
- 高级筛：杜教筛 $O(n^{\frac{2}{3}})$，min25 筛 $O(\frac{n^{\frac{3}{4}}}{\ln n})$，洲阁筛 $O(\frac{n^{\frac{3}{4}}}{\ln n})$，PN 筛 $O(\sqrt{n})$……

感谢各位大佬莅临!