数论

余杰

2026.7.30

目录

1 整除
- 整除理论
- 最大公因数
- 互素与素数

2 同余
- 定义
- 乘法逆元
- 线性同余方程
- 二次剩余

3 组合数相关
- 卢卡斯定理
- 库默尔定理

4 阶与原根
- 阶
- 原根

5 数论函数
- 定义与积性函数
- 狄利克雷卷积
- 贝尔级数

6 莫比乌斯反演
- 整除分块
- 莫比乌斯反演

7 积性函数前缀和
- 杜教筛
- PN 筛

8 其他
- 类欧几里得算法
- 连分数

1 整除
- 整除理论
- 最大公因数
- 互素与素数

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

整除

我们知道任意两个整数的和、差、积以至任意有限个整数的加、减、乘的混合运算结果仍是整数，但是整数除整数不一定仍为整数。

整除

我们知道任意两个整数的和、差、积以至任意有限个整数的加、减、乘的混合运算结果仍是整数，但是整数除整数不一定仍为整数。

为了应对整数除法的不封闭性，我们引入整除的概念。

Definition 1.1 (整除)

设 a, b 是任意两个整数，其中 $b \neq 0$，若存在整数 q 使得 $a = bq$，则称 b 整除 a 或 a 被 b 整除，记作 $b \mid a$。

Definition 1.1 (整除)

设 a, b 是任意两个整数，其中 $b \neq 0$，若存在整数 q 使得 $a = bq$，则称 b 整除 a 或 a 被 b 整除，记作 $b \mid a$。

此时称 b 为 a 的因数，a 为 b 的倍数。

Definition 1.1 (整除)

设 a, b 是任意两个整数，其中 $b \neq 0$，若存在整数 q 使得 $a = bq$，则称 b 整除 a 或 a 被 b 整除，记作 $b \mid a$。

此时称 b 为 a 的因数，a 为 b 的倍数。

Theorem 1.1

$$d \mid a, d \mid b \implies d \mid ua + vb \ (u, v \in \mathbb{Z})$$

Definition 1.2 (带余除法)

设 a, b 是任意两个整数，其中 $b \neq 0$，存在唯一的整数对 (q, r) 使得 $a = bq + r$ 且 $0 \leq r < |b|$。记作 $a \div b = q \cdots r$。

Definition 1.2 (带余除法)

设 a, b 是任意两个整数，其中 $b \neq 0$，存在唯一的整数对 (q, r) 使得 $a = bq + r$ 且 $0 \leq r < |b|$。记作 $a \div b = q \cdots r$。

此时称 q 为 a 除以 b 的商，r 为 a 除以 b 的余数。记 $a \bmod b = r$。

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

下面是几条性质：

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

下面是几条性质：

- $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$，$x - 1 < \lfloor x \rfloor \leq x$

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

下面是几条性质：

- $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$，$x - 1 < \lfloor x \rfloor \le x$
- $\lfloor n + x \rfloor = n + \lfloor x \rfloor$，$n$ 为整数

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

下面是几条性质：

- $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$，$x - 1 < \lfloor x \rfloor \le x$
- $\lfloor n + x \rfloor = n + \lfloor x \rfloor$，$n$ 为整数
- $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor$

取整函数

对于任意 $x \in \mathbb{R}$，用 $[x]$ 或 $\lfloor x \rfloor$ 表示不大于 x 的最大整数。用 $\lceil x \rceil$ 表示不小于 x 的最小整数。用 $\{x\} = x - \lfloor x \rfloor$ 表示 x 的小数部分。

下面是几条性质：

- $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$，$x - 1 < \lfloor x \rfloor \le x$
- $\lfloor n + x \rfloor = n + \lfloor x \rfloor$，$n$ 为整数
- $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor$
- $a, b \in \mathbb{Z}, b > 0$，则 $a = b \left\lfloor \dfrac{a}{b} \right\rfloor + b \left\{ \dfrac{a}{b} \right\}$

Theorem 1.2 (复合性质)

- $m \in \mathbb{Z}^+, x \in \mathbb{R}$，则 $\left\lfloor \frac{x}{m} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor$
- $a \in \mathbb{Z}, b, c \in \mathbb{Z}^+$，则 $\left\lfloor \frac{a}{bc} \right\rfloor = \left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor$

这两条性质在后面的数论分块中很重要。

1 整除
- 整除理论
- 最大公因数
- 互素与素数

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

最大公因数

Definition 2.1 (gcd & lcm)

$a, b \in \mathbb{Z}$，若 $d \mid a, d \mid b$，则称 d 为 a, b 的公因数。

最大公因数

Definition 2.1 (gcd & lcm)

$a, b \in \mathbb{Z}$，若 $d \mid a, d \mid b$，则称 d 为 a, b 的公因数。

当 a, b 不全为 0 时公因数个数是有限的，故存在最大公因数，记为 $\gcd(a, b)$ 或 (a, b)。

最大公因数

Definition 2.1 (gcd & lcm)

$a, b \in \mathbb{Z}$，若 $d \mid a, d \mid b$，则称 d 为 a, b 的公因数。

当 a, b 不全为 0 时公因数个数是有限的，故存在最大公因数，记为 $\gcd(a, b)$ 或 (a, b)。

特别地，若 $a = b = 0$，定义 $\gcd(0, 0) = 0$。

最大公因数

Definition 2.1 (gcd & lcm)

$a, b \in \mathbb{Z}$，若 $d \mid a, d \mid b$，则称 d 为 a, b 的公因数。

当 a, b 不全为 0 时公因数个数是有限的，故存在最大公因数，记为 $\gcd(a, b)$ 或 (a, b)。

特别地，若 $a = b = 0$，定义 $\gcd(0, 0) = 0$。

同理定义最小公倍数，记为 $\operatorname{lcm}(a, b)$ 或 $[a, b]$。

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

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

- $\gcd(a, b) = \gcd(|a|, |b|)$
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$
- $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$

- $\gcd(a, b) = \gcd(|a|, |b|)$
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$
- $\mathrm{lcm}(\mathrm{lcm}(a, b), c) = \mathrm{lcm}(a, \mathrm{lcm}(b, c))$
- $\gcd(a, b)\mathrm{lcm}(a, b) = ab$

- $\gcd(a, b) = \gcd(|a|, |b|)$
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$
- $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$
- $\gcd(a, b)\operatorname{lcm}(a, b) = ab$
- $d \mid a, d \mid b \iff d \mid \gcd(a, b)$

- $\gcd(a, b) = \gcd(|a|, |b|)$
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$
- $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$
- $\gcd(a, b)\operatorname{lcm}(a, b) = ab$
- $d \mid a, d \mid b \iff d \mid \gcd(a, b)$
- $\gcd(ma, mb) = m\gcd(a, b)$

- $\gcd(a, b) = \gcd(|a|, |b|)$
- $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$
- $\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$
- $\gcd(a, b)\operatorname{lcm}(a, b) = ab$
- $d \mid a, d \mid b \iff d \mid \gcd(a, b)$
- $\gcd(ma, mb) = m\gcd(a, b)$
- $\gcd(a^n, b^n) = \gcd(a, b)^n$

欧几里得算法

gcd 有以下性质：

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

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

欧几里得算法

gcd 有以下性质：

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

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

由此得到求 gcd 的欧几里得算法：

```
int gcd(int a, int b) {
    if (b == 0) return a;
    return gcd(b, a % b);
}
```

每次操作后 ab 至少会变为原来的 $1/2$，故时间复杂度 $O(\log a + \log b)$。

每次操作后 ab 至少会变为原来的 $1/2$，故时间复杂度 $O(\log a + \log b)$。
精细的分析是 $O(\log \min\{a, b\})$。

每次操作后 ab 至少会变为原来的 $1/2$，故时间复杂度 $O(\log a + \log b)$。
精细的分析是 $O(\log \min\{a, b\})$。

更加精细的分析是递归次数不超过 $\log_\phi \dfrac{\min\{a, b\}}{\gcd(a, b)} + O(1)$。其中 $\phi = \dfrac{1+\sqrt{5}}{2}$。

例题

求 $\gcd(2^{120}-1, 2^{100}-1)$。

例题

求 $\gcd(2^{120}-1, 2^{100}-1)$。

$$\begin{aligned}\gcd(a^n-1, a^m-1) &= \gcd(a^n-a^m, a^m-1)\\ &= \gcd(a^m(a^{n-m}-1), a^m-1)\\ &= \gcd(a^{n-m}-1, a^m-1)\end{aligned}$$

例题

求 $\gcd(2^{120}-1, 2^{100}-1)$。

$$\begin{aligned}\gcd(a^n-1, a^m-1) &= \gcd(a^n-a^m, a^m-1)\\ &= \gcd(a^m(a^{n-m}-1), a^m-1)\\ &= \gcd(a^{n-m}-1, a^m-1)\end{aligned}$$

对指数使用辗转相除法，可证 $\gcd(a^n-1, a^m-1) = a^{\gcd(n,m)}-1$。

例题

求 $\gcd(2^{120}-1, 2^{100}-1)$。

$$\begin{aligned}\gcd(a^n-1, a^m-1) &= \gcd(a^n-a^m, a^m-1)\\ &= \gcd(a^m(a^{n-m}-1), a^m-1)\\ &= \gcd(a^{n-m}-1, a^m-1)\end{aligned}$$

对指数使用辗转相除法，可证 $\gcd(a^n-1, a^m-1) = a^{\gcd(n,m)}-1$。
可以再思考证明：若 $\gcd(a,b)=1$，则有

$$\gcd(a^m-b^m, a^n-b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$$

裴蜀定理

Theorem 2.1 (裴蜀定理)

若 a, b 为整数且 $\gcd(a, b) = d$，则 $\forall x, y \in \mathbb{Z}, d \mid ax + by$。且存在一组 x, y 使得 $ax + by = d$。

裴蜀定理

Theorem 2.1 (裴蜀定理)

若 a, b 为整数且 $\gcd(a, b) = d$，则 $\forall x, y \in \mathbb{Z}, d \mid ax + by$。且存在一组 x, y 使得 $ax + by = d$。

裴蜀定理告诉我们存在这样的 x, y。下面的扩展欧几里得算法可以找出一组特定的 x, y。

扩展欧几里得算法

```
int exgcd(int a, int b, int &x, int &y) {
    if (b == 0) {
        x = 1; y = 0;
        return a;
    }
    int d = exgcd(b, a % b, y, x);
    y -= a / b * x;
    return d;
}
```

扩展欧几里得算法

```
int exgcd(int a, int b, int &x, int &y) {
    if (b == 0) {
        x = 1; y = 0;
        return a;
    }
    int d = exgcd(b, a % b, y, x);
    y -= a / b * x;
    return d;
}
```

利用归纳法，可知求出的 x, y 满足 $|x| \le b, |y| \le a$。

二元一次不定方程

对于方程 $ax + by = c$，其有解的充要条件是 $\gcd(a, b) \mid c$。

二元一次不定方程

对于方程 $ax + by = c$，其有解的充要条件是 $\gcd(a, b) \mid c$。
调用 exgcd，得到的结果记为 x_0, y_0。

二元一次不定方程

对于方程 $ax + by = c$，其有解的充要条件是 $\gcd(a, b) \mid c$。
调用 exgcd，得到的结果记为 x_0, y_0。

一组特解为 $x_1 = \dfrac{x_0 c}{\gcd(a, b)}, y_1 = \dfrac{y_0 c}{\gcd(a, b)}$。

二元一次不定方程

对于方程 $ax + by = c$，其有解的充要条件是 $\gcd(a, b) \mid c$。
调用 exgcd，得到的结果记为 x_0, y_0。

一组特解为 $x_1 = \dfrac{x_0 c}{\gcd(a, b)}, y_1 = \dfrac{y_0 c}{\gcd(a, b)}$。

通解为 $x = x_1 + k\dfrac{b}{\gcd(a, b)}, y = y_1 - k\dfrac{a}{\gcd(a, b)}$。其中 k 为任意整数。

P3518 [POI 2011] SEJ-Strongbox

有一个密码箱，0 到 $n-1$ 中的某些整数是它的密码。且满足：若 a 和 b 是它的密码，则 $(a+b) \bmod n$ 也是它的密码（a, b 可以相等）。某人试了 k 次密码 $m_1, \ldots, m_k$，前 $k-1$ 次都失败了，最后一次成功了。问，该密码箱最多有多少种不同的密码。

$1 \le k \le 2.5 \times 10^5, k \le n \le 10^{14}$。

设最小非零的密码为 d，则所有 d 的倍数也是密码。若存在密码 x 不是 d 的倍数，则由裴蜀定理 $\gcd(x, d) < d$ 也是密码，与 d 的最小性矛盾。故所有密码恰是 d 的所有倍数。进一步可知 $d \mid n$。

设最小非零的密码为 d，则所有 d 的倍数也是密码。若存在密码 x 不是 d 的倍数，则由裴蜀定理 $\gcd(x, d) < d$ 也是密码，与 d 的最小性矛盾。故所有密码恰是 d 的所有倍数。进一步可知 $d \mid n$。

故枚举 $\gcd(n, m_k)$ 的所有因子，找到最小的 d 满足 $d \nmid m_i$ $(i < k)$ 即为答案。精细实现可将复杂度优化至 $O(d(n)\omega(n))$。

1 整除
- 整除理论
- 最大公因数
- 互素与素数

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

a, b 互素的充要条件是 $\exists u, v \in \mathbb{Z}, ua + vb = 1$。

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

a, b 互素的充要条件是 $\exists u, v \in \mathbb{Z}, ua + vb = 1$。

Theorem 3.1

- 如果 $a \mid bc$ 且 $(a, b) = 1$，则 $a \mid c$

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

a, b 互素的充要条件是 $\exists u, v \in \mathbb{Z}, ua + vb = 1$。

Theorem 3.1

- 如果 $a \mid bc$ 且 $(a, b) = 1$，则 $a \mid c$
- 如果 $a \mid c, b \mid c$ 且 $(a, b) = 1$，则 $ab \mid c$

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

a, b 互素的充要条件是 $\exists u, v \in \mathbb{Z}, ua + vb = 1$。

Theorem 3.1

- 如果 $a \mid bc$ 且 $(a, b) = 1$，则 $a \mid c$
- 如果 $a \mid c, b \mid c$ 且 $(a, b) = 1$，则 $ab \mid c$
- 如果 $(a, c) = 1, (b, c) = 1$，则 $(ab, c) = 1$

Definition 3.1 (互素)

对于整数 a, b，如果 $\gcd(a, b) = 1$，则称 a, b 互素。

a, b 互素的充要条件是 $\exists u, v \in \mathbb{Z}, ua + vb = 1$。

Theorem 3.1

- 如果 $a \mid bc$ 且 $(a, b) = 1$，则 $a \mid c$
- 如果 $a \mid c, b \mid c$ 且 $(a, b) = 1$，则 $ab \mid c$
- 如果 $(a, c) = 1, (b, c) = 1$，则 $(ab, c) = 1$

这些性质可以轻易用算术基本定理证明，但是我建议大家先用最基础最本质的整除与互素的定义来做。因为算术基本定理并不是显然的，证明需要用到本页内容。

素数

Definition 3.2

一个大于 1 的整数，如果其正因数只有 1 和自身，则称其为素数。

素数

Definition 3.2

一个大于 1 的整数，如果其正因数只有 1 和自身，则称其为素数。

准确来说，这是不可约数的定义。素数的定义如下：

Definition 3.3

在正整数集 $\mathbb{Z}^+$ 中，一个大于 1 的整数 p 被称为素数，如果满足：对于任意 $a, b \in \mathbb{Z}^+$，若 $p \mid ab$，则必有 $p \mid a$ 或 $p \mid b$。

素数

Definition 3.2

一个大于 1 的整数，如果其正因数只有 1 和自身，则称其为素数。

准确来说，这是不可约数的定义。素数的定义如下：

Definition 3.3

在正整数集 $\mathbb{Z}^+$ 中，一个大于 1 的整数 p 被称为素数，如果满足：对于任意 $a, b \in \mathbb{Z}^+$，若 $p \mid ab$，则必有 $p \mid a$ 或 $p \mid b$。

在一般的代数系统中，素不等同于不可约。$\mathbb{Z}$ 中二者恰好等价，是由于 $\mathbb{Z}$ 本身有良好的结构。

素数

Definition 3.2

一个大于 1 的整数，如果其正因数只有 1 和自身，则称其为素数。

准确来说，这是不可约数的定义。素数的定义如下：

Definition 3.3

在正整数集 $\mathbb{Z}^+$ 中，一个大于 1 的整数 p 被称为素数，如果满足：对于任意 $a, b \in \mathbb{Z}^+$，若 $p \mid ab$，则必有 $p \mid a$ 或 $p \mid b$。

在一般的代数系统中，素不等同于不可约。$\mathbb{Z}$ 中二者恰好等价，是由于 $\mathbb{Z}$ 本身有良好的结构。

“良好”怎么定义？环 $<$ 交换环 $<$ 整环 $<$ 唯一分解环 $<$ 主理想环 $<$ 欧几里得整环。

算术基本定理

下面证明算术基本定理。为此我们先证明两个引理：

Theorem 3.2

若 p 为素数，a 是任一整数，则要么 $p \mid a$，要么 $\gcd(p, a) = 1$。

算术基本定理

下面证明算术基本定理。为此我们先证明两个引理：

Theorem 3.2

若 p 为素数，a 是任一整数，则要么 $p \mid a$，要么 $\gcd(p, a) = 1$。

Theorem 3.3 (欧几里得引理)

若素数 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$。

Theorem 3.4 (算术基本定理)

任一大于 1 的整数 a 都能表示为如下形式：

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

其中 $p_1 < p_2 < \cdots < p_s$ 是素数，$\alpha_1, \dots, \alpha_s$ 是正整数。

Theorem 3.4 (算术基本定理)

任一大于 1 的整数 a 都能表示为如下形式：

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

其中 $p_1 < p_2 < \cdots < p_s$ 是素数，$\alpha_1, \dots, \alpha_s$ 是正整数。

同样的，一般的代数系统中不一定存在这种唯一分解定理。

Theorem 3.4 (算术基本定理)

任一大于 1 的整数 a 都能表示为如下形式：

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

其中 $p_1 < p_2 < \dots < p_s$ 是素数，$\alpha_1, \dots, \alpha_s$ 是正整数。

同样的，一般的代数系统中不一定存在这种唯一分解定理。

分解质因数是数论问题的重要思考方向。将素数从小到大排列为 $p_1 = 2, p_2 = 3, p_3 = 5, \dots$，则任一正整数 $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ 可映射为一个每维都是非负整数的无穷维向量 $(\alpha_1, \alpha_2, \dots)$。

正整数的乘法与向量的加法形成同构，gcd 对应于每维分别取 min，lcm 对应于取 max。

P8255 [NOI Online 2022 入门组] 数学游戏

T 组询问，每组询问给定 x, z，求最小的正整数 y 使得 $z = x \times y \times \gcd(x, y)$，或判断无解。

$1 \le T \le 5 \times 10^5, 1 \le x \le 10^9, 1 \le z < 2^{63}$。

对于每个 p，记 $v_p(x)$ 为 x 的分解式中 p 上的指数。则可知有解的必要条件是 $\forall p \in \mathbb{P}, v_p(x) \le v_p(z)$，并且若 $3v_p(x) \le v_p(z)$，则 $v_p(y) = v_p(z) - 2v_p(x)$，否则 $2v_p(y) = v_p(z) - v_p(x)$。

对于每个 p，记 $v_p(x)$ 为 x 的分解式中 p 上的指数。则可知有解的必要条件是 $\forall p \in \mathbb{P}, v_p(x) \le v_p(z)$，并且若 $3v_p(x) \le v_p(z)$，则 $v_p(y) = v_p(z) - 2v_p(x)$，否则 $2v_p(y) = v_p(z) - v_p(x)$。

将两种情况统一起来，可得 $v_p(y) = \dfrac{2v_p(z) - v_p(x) - \min\{v_p(z), 3v_p(x)\}}{2}$。对所有 p 并行处理，$y = \sqrt{\dfrac{z^2}{x\gcd(z, x^3)}}$。若不为整数则无解。

1 整除

2 同余
- 定义
- 乘法逆元
- 线性同余方程
- 二次剩余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

好的符号体系可以大大降低描述问题的难度，使得我们能把更多精力放在问题本身上。例如下面是一套不好的符号体系：

19.（17 分）

离散对数在密码学中有重要的应用．设 p 是素数，集合 $X=\{1,2,\cdots,p-1\}$，若 $u,v\in X$，$m\in\mathbf{N}$，记 $u\otimes v$ 为 uv 除以 p 的余数，$u^{m,\otimes}$ 为 u^m 除以 p 的余数；设 $a\in X$，$1,a,a^{2,\otimes},\cdots,a^{p-2,\otimes}$ 两两不同，若 $a^{n,\otimes}=b\ (n\in\{0,1,\cdots,p-2\})$，则称 n 是以 a 为底 b 的离散对数，记为 $n=\log(p)_a b$．

（1）若 $p=11$，$a=2$，求 $a^{p-1,\otimes}$；

（2）对 $m_1,m_2\in\{0,1,\cdots,p-2\}$，记 $m_1\oplus m_2$ 为 m_1+m_2 除以 $p-1$ 的余数（当 m_1+m_2 能被 $p-1$ 整除时，$m_1\oplus m_2=0$）．证明：$\log(p)_a(b\otimes c)=\log(p)_a b\oplus\log(p)_a c$，其中 $b,c\in X$；

（3）已知 $n=\log(p)_a b$．对 $x\in X$，$k\in\{1,2,\cdots,p-2\}$，令 $y_1=a^{k,\otimes}$，$y_2=x\otimes b^{k,\otimes}$．证明：$x=y_2\otimes y_1^{n(p-2),\otimes}$．

同余

Definition 1.1 (同余)

给定一个正整数 m，若整数 a, b 除以 m 的余数相同，则称 a, b 关于模 m 同余，记为 $a \equiv b \pmod{m}$。

同余

Definition 1.1 (同余)

给定一个正整数 m，若整数 a, b 除以 m 的余数相同，则称 a, b 关于模 m 同余，记为 $a \equiv b \pmod{m}$。

使用同余的符号体系，可以在处理加、减、乘等运算时像普通的等式一样方便地进行代数变形。

同余

Definition 1.1 (同余)

给定一个正整数 m，若整数 a, b 除以 m 的余数相同，则称 a, b 关于模 m 同余，记为 $a \equiv b \pmod{m}$。

使用同余的符号体系，可以在处理加、减、乘等运算时像普通的等式一样方便地进行代数变形。

若 $a \equiv b \pmod{m}, c \equiv d \pmod{m}$，则 $a + c \equiv b + d \pmod{m}$，$a - c \equiv b - d \pmod{m}$，$ac \equiv bd \pmod{m}$，$a^n \equiv b^n \pmod{m}$。

同余

Definition 1.1 (同余)

给定一个正整数 m，若整数 a, b 除以 m 的余数相同，则称 a, b 关于模 m 同余，记为 $a \equiv b \pmod{m}$。

使用同余的符号体系，可以在处理加、减、乘等运算时像普通的等式一样方便地进行代数变形。

若 $a \equiv b \pmod{m}, c \equiv d \pmod{m}$，则 $a + c \equiv b + d \pmod{m}$，$a - c \equiv b - d \pmod{m}$，$ac \equiv bd \pmod{m}$，$a^n \equiv b^n \pmod{m}$。

若 $ac \equiv bc \pmod{m}$，且 $\gcd(c, m) = d$，则 $a \equiv b \pmod{\frac{m}{d}}$。

Definition 1.2 (剩余类)

设 m 是一个正整数，任意整数除以 m 所得的余数有 m 中可能 $0, 1, \ldots, m-1$。对于一种余数 r，所有模 m 与 r 同余的整数形成集合 $[r] = \{km + r \mid k \in \mathbb{Z}\}$，称为模 m 的一个剩余类。

Definition 1.2 (剩余类)

设 m 是一个正整数，任意整数除以 m 所得的余数有 m 中可能 $0, 1, \ldots, m-1$。对于一种余数 r，所有模 m 与 r 同余的整数形成集合 $[r] = \{km + r \mid k \in \mathbb{Z}\}$，称为模 m 的一个剩余类。

Definition 1.3 (完全剩余系)

设 $a_0, a_1, \ldots, a_{m-1}$ 是 m 个整数，若其中任意两数都不在同一个剩余类中，则称 $\{a_0, a_1, \ldots, a_{m-1}\}$ 为模 m 的一个完全剩余系，简称完系。

Definition 1.2 (剩余类)

设 m 是一个正整数，任意整数除以 m 所得的余数有 m 中可能 $0, 1, \ldots, m-1$。对于一种余数 r，所有模 m 与 r 同余的整数形成集合 $[r] = \{km + r \mid k \in \mathbb{Z}\}$，称为模 m 的一个剩余类。

Definition 1.3 (完全剩余系)

设 $a_0, a_1, \ldots, a_{m-1}$ 是 m 个整数，若其中任意两数都不在同一个剩余类中，则称 $\{a_0, a_1, \ldots, a_{m-1}\}$ 为模 m 的一个完全剩余系，简称完系。

特别地，$\{0, 1, \ldots, m-1\}$ 称为模 m 的最小非负完系。

Definition 1.4 (欧拉函数)

欧拉函数 $\varphi(a)$ 为定义在正整数上的函数，$\varphi(a)$ 等于 $0, 1, \ldots, a-1$ 中与 a 互素的数的个数。

Definition 1.4 (欧拉函数)

欧拉函数 $\varphi(a)$ 为定义在正整数上的函数，$\varphi(a)$ 等于 $0, 1, \ldots, a-1$ 中与 a 互素的数的个数。

Definition 1.5 (简化剩余系)

设 $a_0, a_1, \ldots, a_{\varphi(m)-1}$ 是 $\varphi(m)$ 个整数，若其中任意两数都不在同一剩余类中，且每个数都与 m 互素，则称 $\{a_0, a_1, \ldots, a_{\varphi(m)-1}\}$ 为模 m 的一个简化剩余系或既约剩余系，简称缩系。

尝试证明以下性质：

尝试证明以下性质：

Theorem 1.1

- 若 $\gcd(a, m) = 1$，x 取遍模 m 的完全剩余系，则 $ax + b$ 也取遍模 m 的完全剩余系。

尝试证明以下性质：

Theorem 1.1

- 若 $\gcd(a, m) = 1$，x 取遍模 m 的完全剩余系，则 $ax + b$ 也取遍模 m 的完全剩余系。
- 若 $\gcd(a, m) = 1$，x 取遍模 m 的简化剩余系，则 ax 也取遍模 m 的简化剩余系。

尝试证明以下性质：

Theorem 1.1

- 若 $\gcd(a, m) = 1$，x 取遍模 m 的完全剩余系，则 $ax + b$ 也取遍模 m 的完全剩余系。
- 若 $\gcd(a, m) = 1$，x 取遍模 m 的简化剩余系，则 ax 也取遍模 m 的简化剩余系。
- 若 m_1, m_2 互素，x_1, x_2 分别取遍模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 取遍模 m_1m_2 的完全剩余系。

尝试证明以下性质：

Theorem 1.1

- 若 $\gcd(a, m) = 1$，x 取遍模 m 的完全剩余系，则 $ax + b$ 也取遍模 m 的完全剩余系。
- 若 $\gcd(a, m) = 1$，x 取遍模 m 的简化剩余系，则 ax 也取遍模 m 的简化剩余系。
- 若 m_1, m_2 互素，x_1, x_2 分别取遍模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 取遍模 m_1m_2 的完全剩余系。
- 若 m_1, m_2 互素，x_1, x_2 分别取遍模 m_1, m_2 的简化剩余系，则 $m_2x_1 + m_1x_2$ 取遍模 m_1m_2 的简化剩余系。

尝试证明以下性质：

Theorem 1.1

- 若 $\gcd(a, m) = 1$，x 取遍模 m 的完全剩余系，则 $ax + b$ 也取遍模 m 的完全剩余系。
- 若 $\gcd(a, m) = 1$，x 取遍模 m 的简化剩余系，则 ax 也取遍模 m 的简化剩余系。
- 若 m_1, m_2 互素，x_1, x_2 分别取遍模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 取遍模 m_1m_2 的完全剩余系。
- 若 m_1, m_2 互素，x_1, x_2 分别取遍模 m_1, m_2 的简化剩余系，则 $m_2x_1 + m_1x_2$ 取遍模 m_1m_2 的简化剩余系。

推论：$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$。

1 整除

2 同余
- 定义
- 乘法逆元
- 线性同余方程
- 二次剩余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

Example 1 (从 $\mathbb{Z}$ 到 $\mathbb{Q}$)

计算 $9396 \times 14 \div 21$。

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

Example 1 (从 $\mathbb{Z}$ 到 $\mathbb{Q}$)

计算 $9396 \times 14 \div 21$。

这是一个 $\mathbb{Z}$ 上的问题，完全限制在 $\mathbb{Z}$ 上也能做但是运算复杂。引入 $\mathbb{Q}$ 可以简化运算。

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

Example 1 (从 $\mathbb{Z}$ 到 $\mathbb{Q}$)

计算 $9396 \times 14 \div 21$。

这是一个 $\mathbb{Z}$ 上的问题，完全限制在 $\mathbb{Z}$ 上也能做但是运算复杂。引入 $\mathbb{Q}$ 可以简化运算。

Example 2 (从 $\mathbb{R}$ 到 $\mathbb{C}$)

求三次方程 $x^3 - 3x + 1 = 0$。

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

Example 1 (从 $\mathbb{Z}$ 到 $\mathbb{Q}$)

计算 $9396 \times 14 \div 21$。

这是一个 $\mathbb{Z}$ 上的问题，完全限制在 $\mathbb{Z}$ 上也能做但是运算复杂。引入 $\mathbb{Q}$ 可以简化运算。

Example 2 (从 $\mathbb{R}$ 到 $\mathbb{C}$)

求三次方程 $x^3 - 3x + 1 = 0$。

看函数图像可知该方程有三个实根。但是完全限制在 $\mathbb{R}$ 上不容易求出，引入 $\mathbb{C}$ 后可以通过求根公式快速求出。中间过程会产生虚数单位 i，但最后全部消掉，结果回到 $\mathbb{R}$ 中。

有些问题在一个数系中难以解决，但通过数系的扩张可以变简单。

Example 1 (从 $\mathbb{Z}$ 到 $\mathbb{Q}$)

计算 $9396 \times 14 \div 21$。

这是一个 $\mathbb{Z}$ 上的问题，完全限制在 $\mathbb{Z}$ 上也能做但是运算复杂。引入 $\mathbb{Q}$ 可以简化运算。

Example 2 (从 $\mathbb{R}$ 到 $\mathbb{C}$)

求三次方程 $x^3 - 3x + 1 = 0$。

看函数图像可知该方程有三个实根。但是完全限制在 $\mathbb{R}$ 上不容易求出，引入 $\mathbb{C}$ 后可以通过求根公式快速求出。中间过程会产生虚数单位 i，但最后全部消掉，结果回到 $\mathbb{R}$ 中。

引入逆元也是出于类似的考虑。我们希望在模 m 的意义下进行类似数系的扩张来简化运算。

乘法逆元

Definition 2.1 (逆元)

设 m 是一个大于 1 的正整数，a 是任意一个整数。若存在整数 x 使得 $ax \equiv 1 \pmod{m}$ 成立，则称 x 为 a 模 m 的乘法逆元，记为 a^{-1}。

乘法逆元

Definition 2.1 (逆元)

设 m 是一个大于 1 的正整数，a 是任意一个整数。若存在整数 x 使得 $ax \equiv 1 \pmod{m}$ 成立，则称 x 为 a 模 m 的乘法逆元，记为 a^{-1}。

$ax \equiv 1 \pmod{m} \iff ax + m\xi = 1$。由裴蜀定理，$a$ 存在逆元的充要条件是 $\gcd(a, m) = 1$。

乘法逆元

Definition 2.1 (逆元)

设 m 是一个大于 1 的正整数，a 是任意一个整数。若存在整数 x 使得 $ax \equiv 1 \pmod{m}$ 成立，则称 x 为 a 模 m 的乘法逆元，记为 a^{-1}。

$ax \equiv 1 \pmod{m} \iff ax + m\xi = 1$。由裴蜀定理，$a$ 存在逆元的充要条件是 $\gcd(a, m) = 1$。

所有逆元属于同一个剩余类。

乘法逆元

Definition 2.1 (逆元)

设 m 是一个大于 1 的正整数，a 是任意一个整数。若存在整数 x 使得 $ax \equiv 1 \pmod{m}$ 成立，则称 x 为 a 模 m 的乘法逆元，记为 a^{-1}。

$ax \equiv 1 \pmod{m} \iff ax + m\xi = 1$。由裴蜀定理，$a$ 存在逆元的充要条件是 $\gcd(a, m) = 1$。

所有逆元属于同一个剩余类。

模为素数 p 时，每个整数 $0 < x < p$ 均有逆元。

Example 3

求解线性同余方程 $3x \equiv 4 \pmod{101}$。

Example 3

求解线性同余方程 $3x \equiv 4 \pmod{101}$。
原来需要解二元一次方程，现在只需两边同乘 3 的逆元即可。

Example 3

求解线性同余方程 $3x \equiv 4 \pmod{101}$。
原来需要解二元一次方程，现在只需两边同乘 3 的逆元即可。

乘法逆元可以在同余的体系下引入人造分数，在运算上和 $\mathbb{Q}$ 保持高度一致。以后可以使用 $\dfrac{a}{b}$ 来表示 $a \cdot b^{-1} \bmod m$。

逆元求解

求逆元的第一种方法是使用 exgcd 求二元一次方程，前面已经介绍过。下面介绍 OI 中更常用的利用欧拉定理的方法。

逆元求解

求逆元的第一种方法是使用 exgcd 求二元一次方程，前面已经介绍过。下面介绍 OI 中更常用的利用欧拉定理的方法。

Theorem 2.1 (欧拉定理)

对于大于 1 的正整数 m 和与 m 互素的整数 a，有 $a^{\varphi(m)} \equiv 1 \pmod{m}$。

逆元求解

求逆元的第一种方法是使用 exgcd 求二元一次方程，前面已经介绍过。下面介绍 OI 中更常用的利用欧拉定理的方法。

Theorem 2.1 (欧拉定理)

对于大于 1 的正整数 m 和与 m 互素的整数 a，有 $a^{\varphi(m)} \equiv 1 \pmod{m}$。

Proof.

由前面的结论，当 x 取遍模 m 的简化剩余系时，ax 也取遍模 m 的简化剩余系。设 $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ 是一个简化剩余系，则 $r_1 r_2 \ldots r_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \pmod{m}$。又 $\gcd(r_1, m) = \gcd(r_2, m) = \cdots = \gcd(r_{\varphi(m)}, m) = 1$，故 $\gcd(r_1 r_2 \ldots r_{\varphi(m)}, m) = 1$。于是 $a^{\varphi(m)} \equiv 1 \pmod{m}$。 □

Theorem 2.2 (费马小定理)

对于素数 p 和模 p 不为 0 的整数 a，$a^{p-1} \equiv 1 \pmod{p}$。

Theorem 2.2 (费马小定理)

对于素数 p 和模 p 不为 0 的整数 a，$a^{p-1} \equiv 1 \pmod{p}$。

于是 a 的逆元可以直接表示为 $a^{\varphi(m)-1}$ 或 a^{p-2}。

Theorem 2.2 (费马小定理)

对于素数 p 和模 p 不为 0 的整数 a，$a^{p-1} \equiv 1 \pmod p$。

于是 a 的逆元可以直接表示为 $a^{\varphi(m)-1}$ 或 a^{p-2}。

exgcd 和快速幂都需要 log 时间复杂度，下面介绍一种离线的线性预处理、$O(1)$ 查询的逆元求法。

离线逆元：有 n 个整数 $a_1, a_2, \ldots, a_n$，用线性时间求出它们在模 m 意义下的逆元 $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$。

离线逆元：有 n 个整数 $a_1, a_2, \ldots, a_n$，用线性时间求出它们在模 m 意义下的逆元 $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$。

记 $A = a_1 a_2 \ldots a_n$。由于每个 a_i 都有逆元，A 也有逆元 A^{-1}。

离线逆元：有 n 个整数 $a_1, a_2, \ldots, a_n$，用线性时间求出它们在模 m 意义下的逆元 $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$。

记 $A = a_1 a_2 \ldots a_n$。由于每个 a_i 都有逆元，A 也有逆元 A^{-1}。

维护序列的前缀积 $p_i = a_1 a_2 \ldots a_{i-1}$ 和后缀积 $s_i = a_{i+1} a_{i+2} \ldots a_n$。则 $a_i^{-1} \equiv A^{-1} p_i s_i \pmod{m}$。

离线逆元：有 n 个整数 $a_1, a_2, \ldots, a_n$，用线性时间求出它们在模 m 意义下的逆元 $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$。

记 $A = a_1 a_2 \ldots a_n$。由于每个 a_i 都有逆元，A 也有逆元 A^{-1}。

维护序列的前缀积 $p_i = a_1 a_2 \ldots a_{i-1}$ 和后缀积 $s_i = a_{i+1} a_{i+2} \ldots a_n$。则 $a_i^{-1} \equiv A^{-1} p_i s_i \pmod{m}$。

特别地，$1 \sim n$ 中所有数的逆元、$1 \sim n$ 中所有数的阶乘的逆元也可以线性预处理。

SOJ123 水题

给定奇质数 P 和 n 个整数 $a_1, \ldots, a_n$，支持两种操作：

- 对于所有 $l \le i \le r$，将 a_i 加上 x。
- 对于所有 $l \le i \le r$，将 a_i 变成 a_i^{P-2}。

每次操作后输出 $\sum_{i=1}^{n} a_i \bmod P$。$n \le 2000$，操作次数 $m \le 2000$。

SOJ123 水题

给定奇质数 P 和 n 个整数 $a_1, \ldots, a_n$，支持两种操作：

- 对于所有 $l \le i \le r$，将 a_i 加上 x。
- 对于所有 $l \le i \le r$，将 a_i 变成 a_i^{P-2}。

每次操作后输出 $\sum_{i=1}^{n} a_i \bmod P$。$n \le 2000$，操作次数 $m \le 2000$。

将每个 a_i 以分数的形式维护，每次查询的时候线性求出每个分母的逆元。复杂度 $O(nm + m \log P)$。

1 整除

2 同余
- 定义
- 乘法逆元
- 线性同余方程
- 二次剩余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

线性同余方程

形如 $ax \equiv b \pmod{m}$ 的方程，称为线性同余方程。

线性同余方程

形如 $ax \equiv b \pmod{m}$ 的方程，称为线性同余方程。
将其改写为 $ax + m\xi = b$ 的形式，易知有解的充要条件是 $\gcd(a, m) \mid b$。

线性同余方程

形如 $ax \equiv b \pmod{m}$ 的方程，称为线性同余方程。
将其改写为 $ax + m\xi = b$ 的形式，易知有解的充要条件是 $\gcd(a, m) \mid b$。
用 exgcd 可以求出 $ax + m\xi = \gcd(a, m)$ 的一个特解 x_0，并表示出通解

$$x = \frac{x_0 b}{\gcd(a, m)} + k\frac{m}{\gcd(a, m)}$$

线性同余方程

形如 $ax \equiv b \pmod{m}$ 的方程，称为线性同余方程。
将其改写为 $ax + m\xi = b$ 的形式，易知有解的充要条件是 $\gcd(a, m) \mid b$。
用 exgcd 可以求出 $ax + m\xi = \gcd(a, m)$ 的一个特解 x_0，并表示出通解

$$x = \frac{x_0 b}{\gcd(a, m)} + k\frac{m}{\gcd(a, m)}$$

或者写成

$$x \equiv \frac{x_0 b}{\gcd(a, m)} \pmod{\frac{m}{\gcd(a, m)}}$$

线性同余方程组

求解线性同余方程组：

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

线性同余方程组

求解线性同余方程组：

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

考虑不断合并两个同余方程 $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$。

将其转化为不定方程 $x = a_1 + \xi_1 m_1 = a_2 + \xi_2 m_2$，即 $\xi_1 m_1 - \xi_2 m_2 = a_2 - a_1$。有解的充要条件是 $\gcd(m_1, m_2) \mid a_2 - a_1$。

还是一样使用 exgcd 求出一个特解 ξ_1', ξ_2'，并表示出通解

$$\xi_1 = \frac{\xi_1'(a_2 - a_1)}{\gcd(m_1, m_2)} + k\frac{m_2}{\gcd(m_1, m_2)}$$

还是一样使用 exgcd 求出一个特解 ξ_1', ξ_2'，并表示出通解

$$\xi_1 = \frac{\xi_1'(a_2 - a_1)}{\gcd(m_1, m_2)} + k\frac{m_2}{\gcd(m_1, m_2)}$$

于是

$$x = a_1 + \frac{m_1\xi_1'(a_2 - a_1)}{\gcd(m_1, m_2)} + k\frac{m_1 m_2}{\gcd(m_1, m_2)}$$

$$x \equiv a_1 + \frac{m_1\xi_1'(a_2 - a_1)}{\gcd(m_1, m_2)} \pmod{\operatorname{lcm}(m_1, m_2)}$$

中国剩余定理

$m_1, \ldots, m_n$ 互素时，可以直接形式化地给出解：

$$x \equiv \sum_{i=1}^{n} (a_i \prod_{j \neq i} m_j^{-1} \bmod m_i) \prod_{j \neq i} m_j \pmod{\prod_{i=1}^{n} m_i}$$

CF338D GCD Table

给出序列 $a_1, \ldots, a_k$，判断是否存在 x, y，满足 $1 \le x \le n, 1 \le y \le m$，且对于 $i = 1, 2, \ldots, k$，均有 $\gcd(x, y + i - 1) = a_i$。

$k \le 10^4, n, m, a_i \le 10^{12}$。

$\gcd(x, y+i-1) = a_i$ 的必要条件是 $a_i \mid x, a_i \mid y+i-1$。由此列出关于 x 和 y 的线性方程组。

$\gcd(x, y+i-1) = a_i$ 的必要条件是 $a_i \mid x, a_i \mid y+i-1$。由此列出关于 x 和 y 的线性方程组。

求解得到 $x = k_1 \cdot \mathrm{lcm}(a_1, \ldots, a_k), y = k_2 \cdot \mathrm{lcm}(a_1, \ldots, a_k) + y_0$。

$\gcd(x, y+i-1) = a_i$ 的必要条件是 $a_i \mid x, a_i \mid y+i-1$。由此列出关于 x 和 y 的线性方程组。

求解得到 $x = k_1 \cdot \operatorname{lcm}(a_1, \ldots, a_k), y = k_2 \cdot \operatorname{lcm}(a_1, \ldots, a_k) + y_0$。

此时有 $a_i \mid \gcd(x, y+i-1)$，要求 k_1, k_2 的值使 gcd 恰好等于 a_i。$k_1 > 1$ 一定不优，故 $k_1 = 1$。$\gcd(x, y+i-1) = \gcd(\operatorname{lcm}(a_1, \ldots, a_k), y_0 + i - 1)$，和 k_2 取值无关，令 $k_2 = 0$。对每个 i 判定即可。

P5330 [SNOI2019] 数论

给定正整数 P, Q, T，大小为 n 的整数集 A 和大小为 m 的整数集 B。求

$$\sum_{i=0}^{T-1}[(i \bmod P) \in A \wedge (i \bmod Q) \in B]$$

即求有多少个小于 T 的非负整数满足除以 P 的余数属于 A 且除以 Q 的余数属于 B。

$1 \le n, m \le 10^6, 1 \le P, Q \le 10^6, 1 \le T \le 10^{18}$。

对满足条件的 x，存在 i, j, u, v，$x = a_i + uP = b_j + vQ$，即 $uP - vQ = b_j - a_i$。记 $g = \gcd(P, Q)$，必有 $g \mid b_j - a_i$。故把 A, B 中的所有元素按模 g 分组，$A_r = \{a_i \mid a_i \equiv r \pmod{g}\}$。接下来将问题限制在 A_r, B_r 上，统计所有模 g 余 r 的 x。

对满足条件的 x，存在 i, j, u, v，$x = a_i + uP = b_j + vQ$，即 $uP - vQ = b_j - a_i$。记 $g = \gcd(P, Q)$，必有 $g \mid b_j - a_i$。故把 A, B 中的所有元素按模 g 分组，$A_r = \{a_i \mid a_i \equiv r \pmod g\}$。接下来将问题限制在 A_r, B_r 上，统计所有模 g 余 r 的 x。

对 $uP - vQ = b_j - a_i$，使用 exgcd 返回一个解 u_0, v_0，所有可能的 u 为 $u = \dfrac{u_0(b_j - a_i)}{g} + k \cdot \dfrac{Q}{g}$。于是解得

$$x \equiv a_i + \frac{Pu_0(b_j - a_i)}{g} \equiv (g - Pu_0)\frac{a_i - r}{g} + Pu_0\frac{b_j - r}{g} + r \pmod{\operatorname{lcm}(P, Q)}$$

其中 u_0 只与 P, Q 有关。将 A_r 中的每个元素 a 变为 $(g - Pu_0)\dfrac{a-r}{g}$ 即 $Qv_0\dfrac{a-r}{g}$，B_r 中的每个元素 b 变为 $Pu_0\dfrac{b-r}{g}$。问题变成求有多少 x 满足 $\exists a, b,\ \text{s.t. } x \equiv a + b + r \pmod{\operatorname{lcm}(P, Q)}$。

其中 u_0 只与 P, Q 有关。将 A_r 中的每个元素 a 变为 $(g - Pu_0)\dfrac{a-r}{g}$ 即 $Qv_0\dfrac{a-r}{g}$，B_r 中的每个元素 b 变为 $Pu_0\dfrac{b-r}{g}$。问题变成求有多少 x 满足 $\exists a, b,\ \text{s.t. } x \equiv a + b + r \pmod{\operatorname{lcm}(P, Q)}$。

注意到不会有两对不同的 a, b 撞在一起，于是容易解决。

1 整除

2 同余
- 定义
- 乘法逆元
- 线性同余方程
- 二次剩余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

素数模的同余式

下面考虑素数模下多项式和同余式的一些一般性质。

素数模的同余式

下面考虑素数模下多项式和同余式的一些一般性质。
高次同余式：

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \pmod{p}$$

其中 p 是素数，$a_n \not\equiv 0 \pmod{p}$。

素数模的同余式

下面考虑素数模下多项式和同余式的一些一般性质。
高次同余式：

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \pmod{p}$$

其中 p 是素数，$a_n \not\equiv 0 \pmod{p}$。
对 $f(x)$ 作带余除法 $f(x) = (x^p - x)q(x) + r(x)$，其中 $r(x)$ 次数不超过 $p-1$。

素数模的同余式

下面考虑素数模下多项式和同余式的一些一般性质。

高次同余式：

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \pmod{p}$$

其中 p 是素数，$a_n \not\equiv 0 \pmod{p}$。

对 $f(x)$ 作带余除法 $f(x) = (x^p - x)q(x) + r(x)$，其中 $r(x)$ 次数不超过 $p-1$。

任意整数 x 满足 $x^p - x \equiv 0 \pmod{p}$，故 $f(x) \equiv r(x) \pmod{p}$，这意味着 $f(x)$ 与一个次数不超过 $p-1$ 的多项式等价。下面可以令 $n < p$。

Theorem 4.1 (因式定理)

设 $k \le n$，$x \equiv r_i \pmod p$ $(i = 1, 2, \ldots, k)$ 是同余方程的 k 个不同解。则存在首项系数为 a_n 的 $n-k$ 次多项式 $f_k(x)$，使得 $f(x) \equiv (x-r_1)(x-r_2)\ldots(x-r_k)f_k(x) \pmod p$。

Theorem 4.1 (因式定理)

设 $k \le n$，$x \equiv r_i \pmod p$ $(i = 1, 2, \ldots, k)$ 是同余方程的 k 个不同解。则存在首项系数为 a_n 的 $n-k$ 次多项式 $f_k(x)$，使得 $f(x) \equiv (x-r_1)(x-r_2)\ldots(x-r_k)f_k(x) \pmod p$。

由此立刻得出以下推论：

Corollary 4.1 (费马小定理的推论)

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod p$$

Theorem 4.2 (威尔逊定理)

$$(p-1)! \equiv -1 \pmod{p}。$$

Theorem 4.2 (威尔逊定理)

$(p-1)! \equiv -1 \pmod{p}$。

Theorem 4.3 (拉格朗日定理)

同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \pmod{p} \quad (n < p, p \nmid a_n)$$

的解数不超过 n。

二次剩余

现在来研究二次同余方程 $Ax^2 + Bx + C \equiv 0 \pmod{m}$。通过使用配方法和拆分模数，我们只需要研究核心问题 $x^2 \equiv a \pmod{p}$，其中 p 为奇素数。若该方程有解，称 a 为模 p 的二次剩余，否则称为二次非剩余。

先判断方程 $x^2 \equiv a \pmod p$ 有没有解，即判断 a 是不是模 p 的二次剩余。

先判断方程 $x^2 \equiv a \pmod p$ 有没有解，即判断 a 是不是模 p 的二次剩余。

Theorem 4.4

$1, 2, \ldots, p-1$ 中恰好有 $\frac{p-1}{2}$ 个二次剩余。

先判断方程 $x^2 \equiv a \pmod p$ 有没有解，即判断 a 是不是模 p 的二次剩余。

Theorem 4.4

$1, 2, \ldots, p-1$ 中恰好有 $\frac{p-1}{2}$ 个二次剩余。

设有不同的 $x, y < p$ 满足 $x^2 \equiv y^2 \pmod p$，则 $(x-y)(x+y) \equiv 0 \pmod p$，故必有 $y = p - x$。于是可知 $1^2, 2^2, \ldots, (\frac{p-1}{2})^2 \bmod p$ 恰为所有的二次剩余。

Theorem 4.5 (欧拉判别法)

若 $\gcd(a,p)=1$，则 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 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$。

Theorem 4.5 (欧拉判别法)

若 $\gcd(a,p)=1$，则 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 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$。

Proof.

由费马小定理，$x^{p-1}-1 \equiv (x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1) \equiv 0 \pmod p$。故 $a^{\frac{p-1}{2}}$ 模 p 的结果一定为 ± 1。

Theorem 4.5 (欧拉判别法)

若 $\gcd(a,p)=1$，则 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 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$。

Proof.

由费马小定理，$x^{p-1}-1 \equiv (x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1) \equiv 0 \pmod p$。故 $a^{\frac{p-1}{2}}$ 模 p 的结果一定为 ± 1。

若 a 是二次剩余，有 $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$。

Theorem 4.5 (欧拉判别法)

若 $\gcd(a,p)=1$，则 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 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$。

Proof.

由费马小定理，$x^{p-1}-1 \equiv (x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1) \equiv 0 \pmod p$。故 $a^{\frac{p-1}{2}}$ 模 p 的结果一定为 ± 1。

若 a 是二次剩余，有 $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$。

所有 $\frac{p-1}{2}$ 个二次剩余都是方程 $x^{\frac{p-1}{2}}-1 \equiv 0 \pmod p$ 的根。由拉格朗日定理，不存在任何一个二次非剩余再是 $x^{\frac{p-1}{2}}-1 \equiv 0 \pmod p$ 的根。故所有二次非剩余 a 满足 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$。 □

勒让德符号

勒让德符号 $\left(\frac{a}{p}\right)$（读作 a 对 p 的勒让德符号）是一个对于给定的奇素数 p 定义在一切整数 a 上的函数，值为

$$\left(\frac{a}{p}\right)=\begin{cases}1, & a\text{ 是模}p\text{ 的二次剩余},\\ -1, & a\text{ 是模}p\text{ 的二次非剩余},\\ 0, & p\mid a.\end{cases}$$

Theorem 4.6

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Theorem 4.6

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$（完全积性）

Theorem 4.6

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$（完全积性）
- $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Theorem 4.7 (二次互反律)

设 p, q 是两个不同的奇素数，则

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

Cipolla 算法

接下来求解 $x^2 \equiv a \pmod p$。已知 a 为二次剩余。

Cipolla 算法

接下来求解 $x^2 \equiv a \pmod p$。已知 a 为二次剩余。

先找到一个整数 r，使得 $r^2 - a$ 是二次非剩余。由于二次非剩余个数占一半，故可直接不断随机 r 直到满足条件。

Cipolla 算法

接下来求解 $x^2 \equiv a \pmod p$。已知 a 为二次剩余。

先找到一个整数 r，使得 $r^2 - a$ 是二次非剩余。由于二次非剩余个数占一半，故可直接不断随机 r 直到满足条件。

构造复数 $\omega = \sqrt{r^2 - a}$。下面进行域扩张，定义 $\mathbb{F}_{p^2} = \{A + B\omega \mid A, B \in \mathbb{F}_p\}$，在该域中取模操作为 A, B 分别取模。有 $\omega^2 \equiv r^2 - a \pmod p$。

Theorem 4.8 (Freshman's Dream)

在特征为素数 p 的代数系统中，$(x+y)^p = x^p + y^p$。

Theorem 4.8 (Freshman's Dream)

在特征为素数 p 的代数系统中，$(x+y)^p = x^p + y^p$。

$\mathbb{F}_{p^2}$ 的特征与 $\mathbb{F}_p$ 相同，均为 p。于是 $\forall x, y \in \mathbb{F}_{p^2}, (x+y)^p \equiv x^p + y^p \pmod{p}$。

Theorem 4.8 (Freshman's Dream)

在特征为素数 p 的代数系统中，$(x+y)^p = x^p + y^p$。

$\mathbb{F}_{p^2}$ 的特征与 $\mathbb{F}_p$ 相同，均为 p。于是 $\forall x, y \in \mathbb{F}_{p^2}, (x+y)^p \equiv x^p + y^p \pmod{p}$。

Theorem 4.9

$\omega^p \equiv -\omega \pmod{p}$。

直接令 $x = (r+\omega)^{\frac{p+1}{2}} \bmod p$。下证 $x^2 \equiv a \pmod p$ 以及 $x \in \mathbb{F}_p$。

直接令 $x = (r+\omega)^{\frac{p+1}{2}} \bmod p$。下证 $x^2 \equiv a \pmod p$ 以及 $x \in \mathbb{F}_p$。

$x^2 \equiv (r+\omega)^{p+1} \equiv (r+\omega)(r^p+\omega^p) \equiv (r+\omega)(r-\omega) \equiv r^2-\omega^2 \equiv a \pmod p$。

直接令 $x = (r+\omega)^{\frac{p+1}{2}} \bmod p$。下证 $x^2 \equiv a \pmod p$ 以及 $x \in \mathbb{F}_p$。

$x^2 \equiv (r+\omega)^{p+1} \equiv (r+\omega)(r^p+\omega^p) \equiv (r+\omega)(r-\omega) \equiv r^2-\omega^2 \equiv a \pmod p$。

在 $\mathbb{F}_{p^2}$ 中考察同余式 $y^{p-1}-1 \equiv 0 \pmod p$，由拉格朗日定理，其有不超过 $p-1$ 个根，且一定都在 $\mathbb{F}_p$ 中。而 $x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p$，故 $x \in \mathbb{F}_p$。

P6610 [Code+#7] 同余方程

n 次询问，每次给出正整数 p 和 x，求方程 $a^2 + b^2 \equiv x \pmod p$ 关于 a, b 在模 p 意义下解的组数。其中 p 是奇数，且不含平方因子。

$n \le 10^5, p \le 10^7$。

p 是不含平方因子的奇数，意味着可以分解为若干奇素数的乘积。可以拆开分别求解，再用中国剩余定理拼起来。答案为模数取遍 p 的所有素因子时答案之积。

p 是不含平方因子的奇数，意味着可以分解为若干奇素数的乘积。可以拆开分别求解，再用中国剩余定理拼起来。答案为模数取遍 p 的所有素因子时答案之积。

下面设 p 为奇素数。枚举 $u = a^2, v = b^2$，则 u, v 需要同时为二次剩余。当 u 为二次剩余时，对应着两个 a。v 同理。可以用勒让德符号把二者统一起来：

$$ans = \sum_{u+v\equiv x} \left(\left(\frac{u}{p}\right) + 1\right)\left(\left(\frac{v}{p}\right) + 1\right)$$

模奇素数时二次剩余与二次非剩余数量相等，即 $\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)=0$。结合勒让德符号的完全积性，上式变成

$$ans=p+\sum_{u+v\equiv x}\left(\frac{uv}{p}\right)=p+\sum_{u=0}^{p-1}\left(\frac{u(x-u)}{p}\right)$$

模奇素数时二次剩余与二次非剩余数量相等，即 $\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)=0$。结合勒让德符号的完全积性，上式变成

$$ans=p+\sum_{u+v\equiv x}\left(\frac{uv}{p}\right)=p+\sum_{u=0}^{p-1}\left(\frac{u(x-u)}{p}\right)$$

再由 $\left(\frac{u(x-u)}{p}\right)=\left(\frac{\frac{x}{u}-1}{p}\right)$，$u$ 取遍模 p 的简化剩余系时 $\frac{x}{u}$ 也取遍模 p 的简化剩余系，$\frac{x}{u}-1$ 取遍 $0\sim p-2$。故

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

1 整除

2 同余

3 组合数相关
- 卢卡斯定理
- 库默尔定理

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

卢卡斯定理

Theorem 1.1 (卢卡斯定理)

对于素数 p，有

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

Proof.

考虑 $(1+x)^n$，有

$$\begin{aligned}
\binom{n}{m} &\equiv [x^m](1+x)^n \pmod p \\
&\equiv [x^m](1+x)^{p\lfloor n/p\rfloor}(1+x)^{n \bmod p} \pmod p \\
&\equiv [x^m](1+x^p)^{\lfloor n/p\rfloor}(1+x)^{n \bmod p} \pmod p \\
&\equiv [x^{p\lfloor m/p\rfloor}](1+x^p)^{\lfloor n/p\rfloor}\cdot[x^{m \bmod p}](1+x)^{n \bmod p} \pmod p \\
&\equiv \binom{\lfloor n/p\rfloor}{\lfloor m/p\rfloor}\binom{n \bmod p}{m \bmod p} \pmod p
\end{aligned}$$

□

该定理可以自然地从二项式系数 $\binom{n}{m}$ 推广到多项式系数

$$\binom{n}{a_1, a_2, \ldots, a_m} = [x_1^{a_1} \ldots x_m^{a_m}](x_1 + \cdots + x_m)^n。$$

该定理可以自然地从二项式系数 $\binom{n}{m}$ 推广到多项式系数

$$\binom{n}{a_1, a_2, \ldots, a_m} = [x_1^{a_1} \ldots x_m^{a_m}](x_1 + \cdots + x_m)^n。$$

Corollary 1.1

$$\binom{n}{a_1, a_2, \ldots, a_m} \equiv \binom{\lfloor n/p \rfloor}{\lfloor a_1/p \rfloor, \ldots, \lfloor a_m/p \rfloor} \binom{n \bmod p}{a_1 \bmod p, \ldots, a_m \bmod p} \pmod{p}$$

P5598 混乱度

有 n 种颜色的球，其中第 i 种颜色的球有 a_i 个，同色的球不区分。

定义第 $l \sim r$ 种颜色的球的混乱度 $f(l,r)$ 为：将第 $l \sim r$ 种颜色的球排成一排的方案数对 p 取模的结果。

求 $\sum\limits_{l=1}^{n}\sum\limits_{r=l}^{n} f(l,r)$。$n \le 5 \times 10^5, a_i \le 10^{18}, p \in \{2,3,5,7\}$。

$f(l,r)=\binom{a_l+\cdots+a_r}{a_l,\ldots,a_r} \bmod p$。由卢卡斯定理，在 p 进制下若 $a_l+\cdots+a_r$ 发生了进位，则 $f(l,r)=0$。而若 $r-l>p\log a$，一定会发生进位。于是可知对于固定的 l，所有 $f(l,r)\neq 0$ 的 r 一定距离 l 很近。

$f(l,r)=\binom{a_l+\cdots+a_r}{a_l,\ldots,a_r} \bmod p$。由卢卡斯定理，在 p 进制下若 $a_l+\cdots+a_r$ 发生了进位，则 $f(l,r)=0$。而若 $r-l>p\log a$，一定会发生进位。于是可知对于固定的 l，所有 $f(l,r)\neq 0$ 的 r 一定距离 l 很近。

$f(l,r)$ 可由 $f(l,r-1)$ 增量求出。故枚举左端点，移动右端点即可。

P4345 [SHOI2015] 超能粒子炮・改

t 次询问，每次求 $\sum_{i=0}^{k}\binom{n}{i} \bmod p$。$p=2333, t\le 10^5, n,k\le 10^{18}$。

P4345 [SHOI2015] 超能粒子炮・改

t 次询问，每次求 $\sum_{i=0}^{k}\binom{n}{i} \bmod p$。$p=2333, t\le 10^5, n,k\le 10^{18}$。

记 $f(n,k)=\sum_{i=0}^{k}\binom{n}{i}$。有：

卢卡斯定理

$$f(n,k)=\sum_{i=0}^{k}\binom{n}{i}$$

$$
\begin{aligned}
f(n,k) &= \sum_{i=0}^{k} \binom{n}{i} \\
&\equiv \sum_{i=0}^{k} \binom{\lfloor n/p \rfloor}{\lfloor i/p \rfloor} \binom{n \bmod p}{i \bmod p}
\end{aligned}
$$

$$
\begin{aligned}
f(n,k) &= \sum_{i=0}^{k} \binom{n}{i} \\
&\equiv \sum_{i=0}^{k} \binom{\lfloor n/p \rfloor}{\lfloor i/p \rfloor} \binom{n \bmod p}{i \bmod p} \\
&\equiv \sum_{i=0}^{\lfloor k/p \rfloor - 1} \binom{\lfloor n/p \rfloor}{i} \cdot \sum_{j=0}^{p-1} \binom{n \bmod p}{j} + \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \sum_{j=0}^{k \bmod p} \binom{n \bmod p}{j}
\end{aligned}
$$

$$
\begin{aligned}
f(n,k) &= \sum_{i=0}^{k} \binom{n}{i} \\
&\equiv \sum_{i=0}^{k} \binom{\lfloor n/p \rfloor}{\lfloor i/p \rfloor} \binom{n \bmod p}{i \bmod p} \\
&\equiv \sum_{i=0}^{\lfloor k/p \rfloor - 1} \binom{\lfloor n/p \rfloor}{i} \cdot \sum_{j=0}^{p-1} \binom{n \bmod p}{j} + \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \sum_{j=0}^{k \bmod p} \binom{n \bmod p}{j} \\
&\equiv f(\lfloor n/p \rfloor, \lfloor k/p \rfloor - 1) \cdot f(n \bmod p, p-1) + \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} f(n \bmod p, k \bmod p)
\end{aligned}
$$

$$
\begin{aligned}
f(n,k) &= \sum_{i=0}^{k} \binom{n}{i} \\
&\equiv \sum_{i=0}^{k} \binom{\lfloor n/p \rfloor}{\lfloor i/p \rfloor} \binom{n \bmod p}{i \bmod p} \\
&\equiv \sum_{i=0}^{\lfloor k/p \rfloor - 1} \binom{\lfloor n/p \rfloor}{i} \cdot \sum_{j=0}^{p-1} \binom{n \bmod p}{j} + \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \sum_{j=0}^{k \bmod p} \binom{n \bmod p}{j} \\
&\equiv f(\lfloor n/p \rfloor, \lfloor k/p \rfloor - 1) \cdot f(n \bmod p, p-1) + \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} f(n \bmod p, k \bmod p)
\end{aligned}
$$

预处理出每个 $i, j < p$ 的 $f(i,j)$，每次查询 $O(\log^2 n)$。

扩展卢卡斯定理

对于模数 m 是合数的情况，如何化简 $\binom{n}{m}$？

扩展卢卡斯定理

对于模数 m 是合数的情况，如何化简 $\binom{n}{m}$？

先将 m 质因数分解 $M = \prod p_i^{\alpha_i}$。对每个 $p_i^{\alpha_i}$ 求出 $\binom{n}{m} \bmod p_i^{\alpha_i}$，再用中国剩余定理拼起来。

扩展卢卡斯定理

对于模数 m 是合数的情况，如何化简 $\binom{n}{m}$？

先将 m 质因数分解 $M = \prod p_i^{\alpha_i}$。对每个 $p_i^{\alpha_i}$ 求出 $\binom{n}{m} \bmod p_i^{\alpha_i}$，再用中国剩余定理拼起来。

$$\binom{n}{m} \bmod p^k = \frac{n!}{m!(n-m)!} \bmod p^k$$

由于 $m!$ 与 $(n-m)!$ 不一定有逆元，所以尝试先把分子分母中的 p 因子全部提出来。

设 $f(x)$ 表示 $x!$ 除掉所有 p 因子后的结果，$g(x)$ 表示 $x!$ 中因子 p 的个数。则有

$$\binom{n}{m} \bmod p^k = \frac{f(n)}{f(m)f(n-m)} p^{g(n)-g(m)-g(n-m)} \bmod p^k$$

拆分 $n!$ 来求 f 和 g

$$
\begin{aligned}
n! &= \prod_{i=1}^{\lfloor n/p \rfloor} pi \prod_{i=1, i\perp p}^{n} i \\
&= p^{\lfloor n/p \rfloor} (\lfloor \frac{n}{p} \rfloor)! \prod_{i=1, i\perp p}^{n} i \\
&\equiv p^{\lfloor n/p \rfloor} (\lfloor \frac{n}{p} \rfloor)! (\prod_{i=1, i\perp p}^{p^k} i)^{\lfloor n/p^k \rfloor} \prod_{i=1, i\perp p}^{n \bmod p^k} i \pmod{p^k}
\end{aligned}
$$

最后一个式子右边后两项不含因子 p。故有

$$f(n) \equiv f(\lfloor \frac{n}{p} \rfloor)(\prod_{i=1, i\perp p}^{p^k} i)^{\lfloor n/p^k \rfloor} \prod_{i=1, i\perp p}^{n \bmod p^k} i \pmod{p^k}$$

$$g(n) = \lfloor \frac{n}{p} \rfloor + g(\lfloor \frac{n}{p} \rfloor)$$

最后一个式子右边后两项不含因子 p。故有

$$f(n) \equiv f(\lfloor \frac{n}{p} \rfloor)(\prod_{i=1, i\perp p}^{p^k} i)^{\lfloor n/p^k \rfloor} \prod_{i=1, i\perp p}^{n \bmod p^k} i \pmod{p^k}$$

$$g(n) = \lfloor \frac{n}{p} \rfloor + g(\lfloor \frac{n}{p} \rfloor)$$

对每个 p^k，预处理复杂度 $O(p^k)$，每次查询 $O(\log^2 n)$。

最后一个式子右边后两项不含因子 p。故有

$$f(n) \equiv f(\lfloor \frac{n}{p} \rfloor)(\prod_{i=1, i\perp p}^{p^k} i)^{\lfloor n/p^k \rfloor} \prod_{i=1, i\perp p}^{n \bmod p^k} i \pmod{p^k}$$

$$g(n) = \lfloor \frac{n}{p} \rfloor + g(\lfloor \frac{n}{p} \rfloor)$$

对每个 p^k，预处理复杂度 $O(p^k)$，每次查询 $O(\log^2 n)$。
其中一个 log 来自于快速幂，可以使用威尔逊定理除掉，变成 $O(\log n)$。

1 整除

2 同余

3 组合数相关
- 卢卡斯定理
- 库默尔定理

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

Theorem 2.1 (勒让德定理)

记 $v_p(x)$ 为 x 质因数分解后 p 的指数，$s_p(x)$ 表示 p 进制下 x 各数位之和。则

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

Theorem 2.1 (勒让德定理)

记 $v_p(x)$ 为 x 质因数分解后 p 的指数，$s_p(x)$ 表示 p 进制下 x 各数位之和。则

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

Proof.

第一个等号

$$v_p(n!) = \sum_{i=1}^{n} v_p(i) = \sum_{i=1}^{n} \sum_{j=1}^{\infty} [p^j \mid i] = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$$

第二个等号容易用归纳法证明。 □

库默尔定理

Theorem 2.2 (库默尔定理)

$v_p\left(\binom{n+m}{n}\right)$ 等于 n 与 m 在 p 进制下相加的进位次数。

Proof.

令 $n=\sum_{i=0}^{\infty}a_ip_i, m=\sum_{i=1}^{\infty}b_ip^i$。于是

$$
\begin{aligned}
v_p\left(\binom{n+m}{n}\right) &= v_p((n+m)!)-v_p(n!)-v_p(m!)\\
&= \sum_{i=1}^{\infty}\lfloor\frac{n+m}{p^i}\rfloor-\lfloor\frac{n}{p^i}\rfloor-\lfloor\frac{m}{p^i}\rfloor\\
&= \sum_{i=1}^{\infty}\lfloor\frac{\sum_{j=0}^{i-1}(a_j+b_j)p^j}{p^i}\rfloor+\sum_{j=i}^{\infty}(a_j+b_j)p^{j-i}-\sum_{j=i}^{\infty}a_jp^{j-i}-\sum_{j=i}^{\infty}b_jp^{j-i}\\
&= \sum_{i=1}^{\infty}[\sum_{j=0}^{i-1}(a_j+b_j)p^j\geq p_i]
\end{aligned}
$$

SOJ2028 梅子

有一个 n 行 m 列的迷宫，第 x 行 y 列的坐标为 (x, y)，每个格子有 $0, 1$ 两种状态，初始所有格子都是 0。

进行 $10^{1233^{1337}}$ 次找宝藏，每次从 $(1, 1)$ 出发。在 (x, y) 时若当前格子是 0 则走到 $(x+1, y)$，否则走到 $(x, y+1)$。移动后将原 (x, y) 格子的状态取反。走出迷宫则本次找宝藏结束，并记录当前迷宫状态。

求 $10^{1233^{1337}}$ 次找宝藏后，本质不同的迷宫状态个数，对 998244353 取模。

多测，$T \le 2 \times 10^5$。$1 \le n, m \le 10^{18}$。

我们可以通过一个状态推向另一个状态，同时可以通过一个状态反推回上一个状态，所以迷宫的状态一定会变成最开始的状态。

我们可以通过一个状态推向另一个状态，同时可以通过一个状态反推回上一个状态，所以迷宫的状态一定会变成最开始的状态。

设经过 ans 次后第一次变成初始状态。设 $f(x,y)(0 \le x < n, 0 \le y < m)$ 表示前 ans 次有几次经过 $(x+1, y+1)$。每个格子一定都被经过偶数次，且向右和向上分别占一半。故

$$f(x,y) = \begin{cases} 0 & x < 0 \lor y < 0 \\ \text{ans} & x = 0 \land y = 0 \\ \dfrac{f(x-1,y) + f(x,y-1)}{2} & \text{otherwise} \end{cases}$$

由此可得 $f(x,y)=\dfrac{\mathsf{ans}\cdot\binom{x+y}{x}}{2^{x+y}}$。约束条件为 $\forall x<n, y<m, 2\mid f(x,y)$。故 ans 为 2 的整数幂，$\log_2\mathsf{ans}=\max\limits_{x,y}(x+y-v_2\left(\binom{x+y}{x}\right)+1)$。

由此可得 $f(x,y)=\dfrac{\mathsf{ans}\cdot\binom{x+y}{x}}{2^{x+y}}$。约束条件为 $\forall x<n, y<m, 2\mid f(x,y)$。故 ans 为 2 的整数幂，$\log_2 \mathsf{ans}=\max\limits_{x,y}(x+y-v_2\left(\binom{x+y}{x}\right)+1)$。

$v_2\left(\binom{x+y}{x}\right)=s_2(x)+s_2(y)-s_2(x+y)$。可以使用数位 dp 在 $O(\log n)$ 解决。

由此可得 $f(x,y)=\dfrac{\mathsf{ans}\cdot\binom{x+y}{x}}{2^{x+y}}$。约束条件为 $\forall x<n, y<m, 2\mid f(x,y)$。故 ans 为 2 的整数幂，$\log_2 \mathsf{ans}=\max\limits_{x,y}(x+y-v_2\left(\binom{x+y}{x}\right)+1)$。

$v_2\left(\binom{x+y}{x}\right)=s_2(x)+s_2(y)-s_2(x+y)$。可以使用数位 dp 在 $O(\log n)$ 解决。

可以发现 $x+y$ 相同的格子上 $f(x,y)$ 都是同奇偶的。故可固定一维再枚举，更加简化。

CF582D Number of Binominal Coefficients

给定一个素数 p 和整数 α, A，计算有多少对整数 (n, k)，满足 $0 \le k \le n \le A$，且 $\binom{n}{k}$ 可以被 p^α 整除。

$1 \le p, \alpha \le 10^9$，$0 \le A < 10^{1000}$。

答案要求 $v_p\left(\binom{n}{k}\right)$ 大于等于 α 的 (n,k) 数量。由库默尔定理，$v_p\left(\binom{n}{k}\right)$ 等于 $n-k$ 和 k 在 p 进制下相加的进位次数。

答案要求 $v_p\left(\binom{n}{k}\right)$ 大于等于 α 的 (n,k) 数量。由库默尔定理，$v_p\left(\binom{n}{k}\right)$ 等于 $n-k$ 和 k 在 p 进制下相加的进位次数。

A 很大，考虑在 p 进制下数位 DP。设 $f(i,j,0/1,0/1)$ 表示前 i 位，进位 j 次，$n-k$ 和 k 的和是否小于 A 的前 i 位，是否向前进位的方案数。转移方程略去。

复杂度 $O(\log^2 A)$。

1 整除

2 同余

3 组合数相关

4 阶与原根
- 阶
- 原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

Definition 1.1 (阶)

令 $a^x \equiv 1 \pmod{m}$ 成立的最小正整数 x 称为 a 模 m 的阶，记作 $\delta_m(a)$。

Definition 1.1 (阶)

令 $a^x \equiv 1 \pmod{m}$ 成立的最小正整数 x 称为 a 模 m 的阶，记作 $\delta_m(a)$。

容易看出存在阶的充要条件是 $\gcd(a, m) = 1$。故下面只考虑 a 与 m 互素的情况。

Definition 1.1 (阶)

令 $a^x \equiv 1 \pmod{m}$ 成立的最小正整数 x 称为 a 模 m 的阶，记作 $\delta_m(a)$。

容易看出存在阶的充要条件是 $\gcd(a, m) = 1$。故下面只考虑 a 与 m 互素的情况。

Theorem 1.1

$a, a^2, \ldots, a^{\delta_m(a)}$ 对模 m 两两不同余。

Definition 1.1 (阶)

令 $a^x \equiv 1 \pmod{m}$ 成立的最小正整数 x 称为 a 模 m 的阶，记作 $\delta_m(a)$。

容易看出存在阶的充要条件是 $\gcd(a, m) = 1$。故下面只考虑 a 与 m 互素的情况。

Theorem 1.1

$a, a^2, \ldots, a^{\delta_m(a)}$ 对模 m 两两不同余。

Corollary 1.1

- $a^x \equiv a^y \pmod{m}$ 当且仅当 $x \equiv y \pmod{\delta_m(a)}$。

Definition 1.1 (阶)

令 $a^x \equiv 1 \pmod{m}$ 成立的最小正整数 x 称为 a 模 m 的阶，记作 $\delta_m(a)$。

容易看出存在阶的充要条件是 $\gcd(a, m) = 1$。故下面只考虑 a 与 m 互素的情况。

Theorem 1.1

$a, a^2, \ldots, a^{\delta_m(a)}$ 对模 m 两两不同余。

Corollary 1.1

- $a^x \equiv a^y \pmod{m}$ 当且仅当 $x \equiv y \pmod{\delta_m(a)}$。
- 若 $a^r \equiv 1 \pmod{m}$，则 $\delta_m(a) \mid r$。

阶还有以下有趣的性质：

- $\delta_m(a^k) = \dfrac{\delta_m(a)}{\gcd(\delta_m(a), k)}$

阶还有以下有趣的性质：

- $\delta_m(a^k) = \dfrac{\delta_m(a)}{\gcd(\delta_m(a), k)}$
- 若 $\gcd(\delta_m(a), \delta_m(b)) = 1$，则 $\delta_m(ab) = \delta_m(a)\delta_m(b)$

阶还有以下有趣的性质：

- $\delta_m(a^k) = \dfrac{\delta_m(a)}{\gcd(\delta_m(a), k)}$
- 若 $\gcd(\delta_m(a), \delta_m(b)) = 1$，则 $\delta_m(ab) = \delta_m(a)\delta_m(b)$
- $\delta_m(a) = \delta_m(a^{-1})$

阶的计算

由欧拉定理，$a^{\varphi(m)} \equiv 1 \pmod{m}$。又有 $a^r \equiv 1 \pmod{m}$ 当且仅当 r 是 $\delta_m(a)$ 的倍数。

阶的计算

由欧拉定理，$a^{\varphi(m)} \equiv 1 \pmod{m}$。又有 $a^r \equiv 1 \pmod{m}$ 当且仅当 r 是 $\delta_m(a)$ 的倍数。

故令 $x = \varphi(m)$，不断尝试用 $\varphi(m)$ 的素因子去除 x，得到最小的 x 满足 $a^x \equiv 1 \pmod{m}$。此时 x 即为 $\delta_m(a)$。

离散对数判定

给定素数 p 和整数 a, b，形如 $a^x \equiv b \pmod p$ 的方程称为离散对数方程。利用阶可以快速判定其是否有解。

离散对数判定

给定素数 p 和整数 a, b，形如 $a^x \equiv b \pmod p$ 的方程称为离散对数方程。利用阶可以快速判定其是否有解。

Theorem 1.2

$a^x \equiv b \pmod p$ 有解当且仅当 $\delta_p(b) \mid \delta_p(a)$。

离散对数判定

给定素数 p 和整数 a, b，形如 $a^x \equiv b \pmod p$ 的方程称为离散对数方程。利用阶可以快速判定其是否有解。

Theorem 1.2

$a^x \equiv b \pmod p$ 有解当且仅当 $\delta_p(b) \mid \delta_p(a)$。

Proof.

必要性：$b^{\delta(a)} \equiv (a^{\delta(a)})^x \equiv 1 \pmod p$。故 $\delta_p(b) \mid \delta_p(a)$。

离散对数判定

给定素数 p 和整数 a, b，形如 $a^x \equiv b \pmod p$ 的方程称为离散对数方程。利用阶可以快速判定其是否有解。

Theorem 1.2

$a^x \equiv b \pmod p$ 有解当且仅当 $\delta_p(b) \mid \delta_p(a)$。

Proof.

必要性：$b^{\delta(a)} \equiv (a^{\delta(a)})^x \equiv 1 \pmod p$。故 $\delta_p(b) \mid \delta_p(a)$。
充分性：记 $d = \delta_p(a)$，$a, a^2, \ldots, a^d$ 在模 p 意义下两两不同余。由 $\delta_p(b) \mid \delta_p(a)$ 知 $b^d \equiv 1 \pmod p$。拉格朗日定理保证了 $b \equiv a^i \pmod p, i \in \{1, 2, \ldots, d\}$。 □

ABC335G Discrete Logarithm Problems

给定 n 个整数 $a_1, \ldots, a_n$ 和素数 p，求有多少对 $i, j (1 \le i, j \le n)$ 满足存在某个正整数 k，使得 $a_i^k \equiv a_j \pmod p$。

$2 \le n \le 2 \times 10^5, p \le 10^{13}$。

ABC335G Discrete Logarithm Problems

给定 n 个整数 $a_1, \ldots, a_n$ 和素数 p，求有多少对 $i, j (1 \le i, j \le n)$ 满足存在某个正整数 k，使得 $a_i^k \equiv a_j \pmod p$。

$2 \le n \le 2 \times 10^5, p \le 10^{13}$。

一道算法竞赛中罕见的和阶有关的题（

ABC335G Discrete Logarithm Problems

给定 n 个整数 $a_1, \ldots, a_n$ 和素数 p，求有多少对 $i, j (1 \le i, j \le n)$ 满足存在某个正整数 k，使得 $a_i^k \equiv a_j \pmod p$。

$2 \le n \le 2 \times 10^5, p \le 10^{13}$。

一道算法竞赛中罕见的和阶有关的题（

利用前面的结论，分别求出每个 a_i 的阶 δ_i，数有多少对 i, j 满足 $\delta_i \mid \delta_j$ 即可。

1 整除

2 同余

3 组合数相关

4 阶与原根
- 阶
- 原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

原根

若 a 模 m 的阶恰好等于 $\varphi(m)$，则称 a 为模 m 的一个原根。

原根

若 a 模 m 的阶恰好等于 $\varphi(m)$，则称 a 为模 m 的一个原根。

检验一个数 a 是否为原根，只需枚举 $\varphi(m)$ 的所有素因子 p_i，判断是否有 $a^{\varphi(m)/p_i} \not\equiv 1 \pmod{m}$ 同时成立即可。

原根

若 a 模 m 的阶恰好等于 $\varphi(m)$，则称 a 为模 m 的一个原根。

检验一个数 a 是否为原根，只需枚举 $\varphi(m)$ 的所有素因子 p_i，判断是否有 $a^{\varphi(m)/p_i} \not\equiv 1 \pmod{m}$ 同时成立即可。

一个模数存在原根当且仅当其为 $2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇素数，$\alpha \geq 1$。

Theorem 2.1 (原根个数)

一个模数 m 如果存在原根，则恰有 $\varphi(\varphi(m))$ 个原根。

Theorem 2.1 (原根个数)

一个模数 m 如果存在原根，则恰有 $\varphi(\varphi(m))$ 个原根。

Proof.

取一个原根 g。已知，$1, g, g^2, \ldots, g^{\varphi(m)-1}$ 两两不同余，且均和 m 互素，故构成模 m 的简化剩余系。

Theorem 2.1 (原根个数)

一个模数 m 如果存在原根，则恰有 $\varphi(\varphi(m))$ 个原根。

Proof.

取一个原根 g。已知，$1, g, g^2, \ldots, g^{\varphi(m)-1}$ 两两不同余，且均和 m 互素，故构成模 m 的简化剩余系。

所有原根均在简化剩余系中，设 g^k 为一个原根，有 $\delta_m(g^k) = \dfrac{\delta_m(g)}{\gcd(\delta_m(g), k)}$，则 $\gcd(\delta_m(g), k) = 1$。于是可知恰有 $\varphi(\delta_m(g)) = \varphi(\varphi(m))$ 个原根。 □

Theorem 2.1 (原根个数)

一个模数 m 如果存在原根，则恰有 $\varphi(\varphi(m))$ 个原根。

Proof.

取一个原根 g。已知，$1, g, g^2, \ldots, g^{\varphi(m)-1}$ 两两不同余，且均和 m 互素，故构成模 m 的简化剩余系。

所有原根均在简化剩余系中，设 g^k 为一个原根，有 $\delta_m(g^k) = \dfrac{\delta_m(g)}{\gcd(\delta_m(g), k)}$，则 $\gcd(\delta_m(g), k) = 1$。于是可知恰有 $\varphi(\delta_m(g)) = \varphi(\varphi(m))$ 个原根。 □

从中也可以得到从一个原根求出所有原根的算法。

更加广泛的结论是：

Theorem 2.2

若 m 存在原根，则使得 $\delta_m(a) = l$ 的 a 的个数为 $\begin{cases} 0 & l \nmid \varphi(m) \\ \varphi(l) & l \mid \varphi(m) \end{cases}$。

原根的计算

最小原根不会很大。因此可以暴力地从小到大枚举每个 a，若 $\gcd(a, m) = 1$ 且 $\delta_m(a) = \varphi(m)$，则其为一个原根。进而可以求出所有原根。

原根的计算

最小原根不会很大。因此可以暴力地从小到大枚举每个 a，若 $\gcd(a, m) = 1$ 且 $\delta_m(a) = \varphi(m)$，则其为一个原根。进而可以求出所有原根。

对于素数 p，其最小原根在 $O(p^{1/4})$ 级别。

原根的计算

最小原根不会很大。因此可以暴力地从小到大枚举每个 a，若 $\gcd(a, m) = 1$ 且 $\delta_m(a) = \varphi(m)$，则其为一个原根。进而可以求出所有原根。

对于素数 p，其最小原根在 $O(p^{1/4})$ 级别。

如果假设广义黎曼猜想成立，最小原根在 $O((\ln p)^2 \cdot d((p-1)^2))$ 级别。$d(n)$ 在 $O(n^\epsilon)$ 级别，对于所有 $\epsilon > 0$。

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

下面给出关于指标的一些性质：

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

下面给出关于指标的一些性质：

- 所有 x 以 g 为底的指标都在同一个模 $\varphi(m)$ 的剩余类中。

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

下面给出关于指标的一些性质：

- 所有 x 以 g 为底的指标都在同一个模 $\varphi(m)$ 的剩余类中。
- $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{\varphi(m)}$。

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

下面给出关于指标的一些性质：

- 所有 x 以 g 为底的指标都在同一个模 $\varphi(m)$ 的剩余类中。
- $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{\varphi(m)}$。
- $\mathrm{ind}_g(a^n) \equiv n \cdot \mathrm{ind}_g(a) \pmod{\varphi(m)}$。

指标

对于模数 m，原根 g 的幂次覆盖模 m 的简化剩余系。因此对于所有 $\gcd(x, m) = 1$ 的 x，存在一个整数 k 使得 $x \equiv g^k \pmod{m}$。这个 k 称为 x 以 g 为底的指标，记为 $\mathrm{ind}_g(x)$。

下面给出关于指标的一些性质：

- 所有 x 以 g 为底的指标都在同一个模 $\varphi(m)$ 的剩余类中。
- $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{\varphi(m)}$。
- $\mathrm{ind}_g(a^n) \equiv n \cdot \mathrm{ind}_g(a) \pmod{\varphi(m)}$。

这意味着在有原根的模数下，乘法等同于指标的加法。

BSGS 算法

如何求指标？$g^k \equiv x \pmod{m}$ 是一个离散对数问题，可以使用下面的 BSGS 算法。

BSGS 算法

如何求指标？$g^k \equiv x \pmod m$ 是一个离散对数问题，可以使用下面的 BSGS 算法。

令 $S = \lceil \sqrt{\varphi(m)} \rceil$，则 $\forall k$，可以将 k 唯一写成 $iS + j\ (0 \le i, j < S)$ 的形式。故只需找到一组 i, j 使得 $g^{iS} \equiv xg^{-j} \pmod m$。

BSGS 算法

如何求指标？$g^k \equiv x \pmod m$ 是一个离散对数问题，可以使用下面的 BSGS 算法。

令 $S = \lceil \sqrt{\varphi(m)} \rceil$，则 $\forall k$，可以将 k 唯一写成 $iS + j\ (0 \le i, j < S)$ 的形式。故只需找到一组 i, j 使得 $g^{iS} \equiv xg^{-j} \pmod m$。

将所有的 xg^{-j} 加入哈希表，再遍历所有 g^{iS}，查看是否有 xg^{-j} 与之相同即可。复杂度 $O(\sqrt{p})$。

高次剩余

对于素数 p 和整数 a, b，求 $0 \le x < p, x^a \equiv b \pmod p$ 的所有整数 x。

高次剩余

对于素数 p 和整数 a, b，求 $0 \le x < p, x^a \equiv b \pmod p$ 的所有整数 x。

先找到一个原根 g，$\mathrm{ind}_g(x)$ 记为 x'，$\mathrm{ind}_g(b)$ 记为 b'。则原方程等价于求所有满足 $ax' \equiv b' \pmod{\varphi(p)}$ 的 x'。容易解决。

UOJ525 平行四边形

一个 $n \times n$ 的棋盘，放入 n 个棋子使得没有两个棋子在同行或同列，没有四个棋子构成平行四边形（包括退化）。保证 $n+1$ 为素数。

$n \leq 1000$。

题目要求等价于：构造一个 $1 \sim n$ 的排列 $p_1, \ldots, p_n$，使得对于任意固定的间距 $k = i - j$，$p_i - p_j$ 两两不同。

题目要求等价于：构造一个 $1 \sim n$ 的排列 $p_1, \ldots, p_n$，使得对于任意固定的间距 $k = i - j$，$p_i - p_j$ 两两不同。

取 $n+1$ 的一个原根 g，直接令 $p_i = g^i \bmod (n+1)$。对于某个固定的间距 k，$p_i - p_j \equiv g^{j+k} - g^j \equiv g^j(g^k - 1) \pmod{n+1}$。$g^k - 1 \not\equiv 0 \pmod{n+1}$，且遍历所有 j 时 g^j 两两不同。故 $p_i - p_j$ 两两不同。

CF360D Levko and Sets

给定素数 p 以及两个整数数组 $a_1, \ldots, a_n$ 和 $b_1, \ldots, b_m$。现在要生成 n 个集合，第 i 个集合生成方式如下：

- 开始元素只有 1。
- 从集合中选出一个元素 c，对于所有 j，若 $c \times a_i^{b_j} \bmod p$ 不在当前集合中，将其加入集合。
- 不断重复上述操作直到集合中元素不变。

求 n 个集合并的大小。

$n \le 10^4, m \le 10^5, p \le 10^9, a_i < p, b_i \le 10^9$。

取 p 的一个原根 g，对所有 a_i 求指标 d_i，即 $g^{d_i} \equiv a_i \pmod p$。则构造集合的方式变成：初始元素 0，每次加上 $d_i \cdot b_j$，对 $p-1$ 取模。

取 p 的一个原根 g，对所有 a_i 求指标 d_i，即 $g^{d_i} \equiv a_i \pmod p$。则构造集合的方式变成：初始元素 0，每次加上 $d_i \cdot b_j$，对 $p-1$ 取模。

由裴蜀定理，集合里最终的元素为所有 $s_i = \gcd(\gcd(b_1, \ldots, b_m) \cdot d_i, p-1)$ 的倍数。

取 p 的一个原根 g，对所有 a_i 求指标 d_i，即 $g^{d_i} \equiv a_i \pmod p$。则构造集合的方式变成：初始元素 0，每次加上 $d_i \cdot b_j$，对 $p-1$ 取模。

由裴蜀定理，集合里最终的元素为所有 $s_i = \gcd(\gcd(b_1, \ldots, b_m) \cdot d_i, p-1)$ 的倍数。

所有 s_i 均为 $p-1$ 的因数，最终要求有多少 $1 \le x \le p-1$ 满足 $\exists s_i \mid x$。可以 $O(\sqrt{p} \log p)$ 解决。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数
- 定义与积性函数
- 狄利克雷卷积
- 贝尔级数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

Definition 1.1 (数论函数)

数论函数是一种定义域为正整数的函数。

Definition 1.1 (数论函数)

数论函数是一种定义域为正整数的函数。

Definition 1.2 (积性函数)

若函数 f 满足对任意 $\gcd(x, y) = 1$，有 $f(xy) = f(x)f(y)$，则称 f 是积性函数。

Definition 1.1 (数论函数)

数论函数是一种定义域为正整数的函数。

Definition 1.2 (积性函数)

若函数 f 满足对任意 $\gcd(x, y) = 1$，有 $f(xy) = f(x)f(y)$，则称 f 是积性函数。
若函数 f 满足对任意 x, y，有 $f(xy) = f(x)f(y)$，则称 f 是完全积性函数。

简单运算

- 加法：$(f+g)(n)=f(n)+g(n)$

简单运算

- 加法：$(f+g)(n)=f(n)+g(n)$
- 点乘：$(f\cdot g)(n)=f(n)\cdot g(n)$

简单运算

- 加法：$(f+g)(n)=f(n)+g(n)$
- 点乘：$(f\cdot g)(n)=f(n)\cdot g(n)$
- 狄利克雷卷积：$(f*g)(n)=\sum_{d|n}f(d)g(\frac{n}{d})$

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id
- $1(n) = 1$

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id
- $1(n) = 1$
- $\sigma_k(n) = \sum_{d|n} d^k$，$\sigma_0$ 常记作 d，σ_1 常记作 σ

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id
- $1(n) = 1$
- $\sigma_k(n) = \sum_{d|n} d^k$，$\sigma_0$ 常记作 d，σ_1 常记作 σ
- $\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id
- $1(n) = 1$
- $\sigma_k(n) = \sum\limits_{d \mid n} d^k$，$\sigma_0$ 常记作 d，σ_1 常记作 σ
- $\varphi(n) = \sum\limits_{i=1}^{n} [\gcd(i, n) = 1]$
- $\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \exists d > 1, d^2 \mid n\text{，其中 } \omega(n) \text{ 为 } n \text{ 含有的不同素因子个数} \\ (-1)^{\omega(n)} & \mathsf{otherwise} \end{cases}$

下面是一些常见的积性函数：

- $\epsilon(n) = [n = 1]$
- $\mathsf{id}_k(n) = n^k$，id_1 常记作 id
- $1(n) = 1$
- $\sigma_k(n) = \sum\limits_{d \mid n} d^k$，$\sigma_0$ 常记作 d，σ_1 常记作 σ
- $\varphi(n) = \sum\limits_{i=1}^{n} [\gcd(i, n) = 1]$
- $\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \exists d > 1, d^2 \mid n\text{，其中 } \omega(n) \text{ 为 } n \text{ 含有的不同素因子个数} \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$
- $\chi_k(n) = [\gcd(n, k) = 1]$

积性函数线性筛

一个积性函数 f 完全由其在各个素数幂处的取值 $f(p^i)$ 决定。若知道了所有 $f(p^i)$ 处的取值，可以 $O(n)$ 得到 f 在 $1 \sim n$ 上的取值。

积性函数线性筛

一个积性函数 f 完全由其在各个素数幂处的取值 $f(p^i)$ 决定。若知道了所有 $f(p^i)$ 处的取值，可以 $O(n)$ 得到 f 在 $1 \sim n$ 上的取值。

回顾欧拉筛。对于整数 x，记 p 为 x 的最小素因子，k 表示该素因子在 x 分解式中的幂次。若 x 不为素数的幂，则会在 x/p 处被筛掉。此时 f 在 $1 \sim x/p$ 上的取值都已确定，故令 $f(x) = f(p^k)f(x/p^k)$ 即可。显然该方法复杂度与欧拉筛相同，是线性的。

积性函数线性筛

一个积性函数 f 完全由其在各个素数幂处的取值 $f(p^i)$ 决定。若知道了所有 $f(p^i)$ 处的取值，可以 $O(n)$ 得到 f 在 $1 \sim n$ 上的取值。

回顾欧拉筛。对于整数 x，记 p 为 x 的最小素因子，k 表示该素因子在 x 分解式中的幂次。若 x 不为素数的幂，则会在 x/p 处被筛掉。此时 f 在 $1 \sim x/p$ 上的取值都已确定，故令 $f(x) = f(p^k)f(x/p^k)$ 即可。显然该方法复杂度与欧拉筛相同，是线性的。

容易发现该筛法不仅适用于积性函数，只要有 $f(\prod_{i=1}^{k} p_i^{\alpha_i}) = f(p_1^{\alpha_1}) \oplus \cdots \oplus f(p_k^{\alpha_k})$，其中 $\oplus$ 是一个可以 $O(1)$ 计算的右结合二元运算，就可以线性筛。例如素因子个数函数 $\omega(n)$，素因子之和函数 $s_\omega(n)$。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数
- 定义与积性函数
- 狄利克雷卷积
- 贝尔级数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

狄利克雷卷积

Definition 2.1

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

Definition 2.1

定义两个数论函数 f, g 的狄利克雷卷积为

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

一些性质：

- 狄利克雷卷积满足交换律、结合律，对加法有分配律。

狄利克雷卷积

Definition 2.1

定义两个数论函数 f, g 的狄利克雷卷积为

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

一些性质：

- 狄利克雷卷积满足交换律、结合律，对加法有分配律。
- 封闭性：两个积性函数的狄利克雷卷积仍是积性函数。

狄利克雷卷积

Definition 2.1

定义两个数论函数 f, g 的狄利克雷卷积为

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

一些性质：

- 狄利克雷卷积满足交换律、结合律，对加法有分配律。
- 封闭性：两个积性函数的狄利克雷卷积仍是积性函数。
- 分配律：对于积性函数 f, g 和完全积性函数 h，有 $(f * g) \cdot h = (f \cdot h) * (g \cdot h)$。

事实上，把所有的数论函数记作集合 $\mathcal{A}$，$(\mathcal{A}, +, *)$ 构成一个带单位元的交换环。乘法单位元为 ϵ。

事实上，把所有的数论函数记作集合 $\mathcal{A}$，$(\mathcal{A}, +, *)$ 构成一个带单位元的交换环。乘法单位元为 ϵ。

其中，所有非零积性函数构成子集 $\mathcal{M}$，$(\mathcal{M}, *)$ 构成一个阿贝尔群。

逆函数

对于函数 f，若存在函数 g 满足 $\epsilon = f * g$，则称 g 为 f 的逆函数，记为 $g = f^{-1}$。

逆函数

对于函数 f，若存在函数 g 满足 $\epsilon = f * g$，则称 g 为 f 的逆函数，记为 $g = f^{-1}$。

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

$$g(n) = \frac{1}{f(1)}(\epsilon(n) - \sum_{d|n, d<n} g(d) f(\frac{n}{d}))$$

上面给出求逆函数的方法。可见逆函数唯一，且有逆函数的充要条件是 $f(1) \neq 0$。

逆函数

对于函数 f，若存在函数 g 满足 $\epsilon = f * g$，则称 g 为 f 的逆函数，记为 $g = f^{-1}$。

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

$$g(n) = \frac{1}{f(1)}(\epsilon(n) - \sum_{d|n, d<n} g(d) f(\frac{n}{d}))$$

上面给出求逆函数的方法。可见逆函数唯一，且有逆函数的充要条件是 $f(1) \neq 0$。

- 积性函数都有逆函数，且逆函数仍是积性函数。

逆函数

对于函数 f，若存在函数 g 满足 $\epsilon = f * g$，则称 g 为 f 的逆函数，记为 $g = f^{-1}$。

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

$$g(n) = \frac{1}{f(1)}(\epsilon(n) - \sum_{d|n, d<n} g(d) f(\frac{n}{d}))$$

上面给出求逆函数的方法。可见逆函数唯一，且有逆函数的充要条件是 $f(1) \neq 0$。

- 积性函数都有逆函数，且逆函数仍是积性函数。
- 定义狄利克雷除法 $f/g = f * g^{-1}$。

逆函数

对于函数 f，若存在函数 g 满足 $\epsilon = f * g$，则称 g 为 f 的逆函数，记为 $g = f^{-1}$。

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

$$g(n) = \frac{1}{f(1)}(\epsilon(n) - \sum_{d|n, d<n} g(d) f(\frac{n}{d}))$$

上面给出求逆函数的方法。可见逆函数唯一，且有逆函数的充要条件是 $f(1) \neq 0$。

- 积性函数都有逆函数，且逆函数仍是积性函数。
- 定义狄利克雷除法 $f/g = f * g^{-1}$。
- 1 函数的逆为 μ。

狄利克雷前缀和

给定一个函数 f，求 $f * 1$。

狄利克雷前缀和

给定一个函数 f，求 $f*1$。

把 n 以内的每个素数看做一维，对每个 $x=\prod_{i=1}^{k} p_i^{\alpha_i}$，将其视作高维空间内的一个点 $(\alpha_1,\ldots,\alpha_k)$。所有满足每一维都不超过该点的点恰好构成 x 的所有因数。

狄利克雷前缀和

给定一个函数 f，求 $f*1$。

把 n 以内的每个素数看做一维，对每个 $x=\prod_{i=1}^{k} p_i^{\alpha_i}$，将其视作高维空间内的一个点 $(\alpha_1,\ldots,\alpha_k)$。所有满足每一维都不超过该点的点恰好构成 x 的所有因数。

类似高维前缀和的处理方法，枚举每个素数 p_i，再从小到大枚举每个 p_i 的倍数 x，将 $f(x)$ 加上 $f(\frac{x}{p_i})$。复杂度 $O(\sum_{i=1}^{k}\frac{n}{p_i})=O(n\log\log n)$。

狄利克雷前缀和

给定一个函数 f，求 $f*1$。

把 n 以内的每个素数看做一维，对每个 $x=\prod_{i=1}^{k} p_i^{\alpha_i}$，将其视作高维空间内的一个点 $(\alpha_1,\ldots,\alpha_k)$。所有满足每一维都不超过该点的点恰好构成 x 的所有因数。

类似高维前缀和的处理方法，枚举每个素数 p_i，再从小到大枚举每个 p_i 的倍数 x，将 $f(x)$ 加上 $f(\frac{x}{p_i})$。复杂度 $O(\sum_{i=1}^{k}\frac{n}{p_i})=O(n\log\log n)$。

求 $f*\mu$，可以类比高维差分。一样可以 $O(n\log\log n)$。

GYM101741F GCD

给定 $a_1, \ldots, a_n$ 与 k，删除至多 k 个元素，最大化所有元素的 gcd。
$n \le 10^5, k \le n/2, a_i \le 10^{18}$。

若 a_i 没被删除，则答案一定是 a_i 的因数。同时，令 $b_j = \gcd(a_j, a_i)$，答案为满足 $\sum_{j=1}^{n}[x \mid b_j] \geq n - k$ 的最大的 x。

若 a_i 没被删除，则答案一定是 a_i 的因数。同时，令 $b_j = \gcd(a_j, a_i)$，答案为满足 $\sum_{j=1}^{n}[x \mid b_j] \geq n - k$ 的最大的 x。

设最优解剩下的元素集合为 S。注意到随机选一个 a_i，其有至少一半的概率落在 S 中。故随机常数次即可以高概率保证某次随机的 a_i 在 S 中。

记 a_i 的所有因子构成集合 D，在 D 上定义函数 $f(x) = \sum_{j=1}^{n} [x = b_j]$。对 f 做狄利克雷后缀和得到 $g(x) = \sum_{x|y} f(y)$，答案即为最大的 x 满足 $g(x) \geq n - k$。复杂度 $O(d(a) \log \log a)$。

记 a_i 的所有因子构成集合 D，在 D 上定义函数 $f(x)=\sum_{j=1}^{n}[x=b_j]$。对 f 做狄利克雷后缀和得到 $g(x)=\sum_{x|y}f(y)$，答案即为最大的 x 满足 $g(x)\geq n-k$。复杂度 $O(d(a)\log\log a)$。

求因子时可以先对 a_i 进行质因数分解，再组合出所有因子。这样复杂度为 $d(a)$ 而不是 $\sqrt{a}$。

卷积复杂度

- 对两个积性函数 f, g 求 $f * g$，复杂度 $O(n)$。

卷积复杂度

- 对两个积性函数 f, g 求 $f * g$，复杂度 $O(n)$。

先处理 $f * g$ 在素数幂处的值，这一部分复杂度不到 $O(n)$。然后 $f * g$ 是积性函数，可以线筛。

卷积复杂度

- 对两个积性函数 f, g 求 $f * g$，复杂度 $O(n)$。

先处理 $f * g$ 在素数幂处的值，这一部分复杂度不到 $O(n)$。然后 $f * g$ 是积性函数，可以线筛。

常见的复杂度分析：$1 \sim n$ 中素数个数，素数幂个数，所有素数幂的幂次和，都是 $O(\frac{n}{\log n})$。

卷积复杂度

- 对两个积性函数 f, g 求 $f * g$，复杂度 $O(n)$。

  先处理 $f * g$ 在素数幂处的值，这一部分复杂度不到 $O(n)$。然后 $f * g$ 是积性函数，可以线筛。

  常见的复杂度分析：$1 \sim n$ 中素数个数，素数幂个数，所有素数幂的幂次和，都是 $O(\frac{n}{\log n})$。

- 对普通函数 f 和积性函数 g 求 $f * g$，复杂度 $O(n \log \log n)$。

卷积复杂度

- 对两个积性函数 f, g 求 $f * g$，复杂度 $O(n)$。

  先处理 $f * g$ 在素数幂处的值，这一部分复杂度不到 $O(n)$。然后 $f * g$ 是积性函数，可以线筛。

  常见的复杂度分析：$1 \sim n$ 中素数个数，素数幂个数，所有素数幂的幂次和，都是 $O(\frac{n}{\log n})$。

- 对普通函数 f 和积性函数 g 求 $f * g$，复杂度 $O(n \log \log n)$。

  用类似高维前缀和的方式处理即可。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数
- 定义与积性函数
- 狄利克雷卷积
- 贝尔级数

6 莫比乌斯反演

7 积性函数前缀和

8 其他

贝尔级数

对于积性函数 f 和给定的素数 p，定义其贝尔级数为

$$f_p(x) = \sum_{k=0}^{\infty} f(p^k) x^k$$

贝尔级数

对于积性函数 f 和给定的素数 p，定义其贝尔级数为

$$f_p(x) = \sum_{k=0}^{\infty} f(p^k) x^k$$

由定义可知，对于固定的 p，f 做狄利克雷卷积，对应于 f_p 做多项式乘法。

下面给出一些常见积性函数的贝尔级数：

- ϵ：1

下面给出一些常见积性函数的贝尔级数：

- ϵ：1
- 1：$\dfrac{1}{1-x}$

下面给出一些常见积性函数的贝尔级数：

- ϵ： 1
- 1： $\dfrac{1}{1-x}$
- id： $\dfrac{1}{1-px}$

下面给出一些常见积性函数的贝尔级数：

- ϵ： 1
- 1： $\dfrac{1}{1-x}$
- id： $\dfrac{1}{1-px}$
- d： $\dfrac{1}{(1-x)^2}$

下面给出一些常见积性函数的贝尔级数：

- ϵ： 1
- 1： $\dfrac{1}{1-x}$
- id： $\dfrac{1}{1-px}$
- d： $\dfrac{1}{(1-x)^2}$
- σ： $\dfrac{1}{(1-x)(1-px)}$

下面给出一些常见积性函数的贝尔级数：

- ϵ： 1
- 1： $\dfrac{1}{1-x}$
- id： $\dfrac{1}{1-px}$
- d： $\dfrac{1}{(1-x)^2}$
- σ： $\dfrac{1}{(1-x)(1-px)}$
- φ： $\dfrac{1-x}{1-px}$

下面给出一些常见积性函数的贝尔级数：

- ϵ： 1
- 1： $\dfrac{1}{1-x}$
- id： $\dfrac{1}{1-px}$
- d： $\dfrac{1}{(1-x)^2}$
- σ： $\dfrac{1}{(1-x)(1-px)}$
- φ： $\dfrac{1-x}{1-px}$
- μ： $1-x$

贝尔级数可以用来证明一些经典恒等式，比如 $\varphi * 1 = \mathsf{id}$，$\mu * 1 = \epsilon$。

贝尔级数可以用来证明一些经典恒等式，比如 $\varphi * 1 = \mathsf{id}$，$\mu * 1 = \epsilon$。
还可以用来处理逆元，求一个函数 f 使得 $f * d = \epsilon$。

贝尔级数可以用来证明一些经典恒等式，比如 $\varphi * 1 = \mathrm{id}$，$\mu * 1 = \epsilon$。
还可以用来处理逆元，求一个函数 f 使得 $f * d = \epsilon$。

Example 4

给定两个积性函数 $f(p^i) = p^i(p^i - 1), g(p^i) = p^i\varphi(p^i)$。求 f/g 的表达式。

$$f_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^i)x^i = 1 + \frac{p^2x}{1-p^2x} - \frac{px}{1-px}$$

$$f_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^i)x^i = 1 + \frac{p^2x}{1-p^2x} - \frac{px}{1-px}$$

$$g_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^{2i-1})x^i = \frac{1-px}{1-p^2x}$$

$$f_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^i)x^i = 1 + \frac{p^2x}{1-p^2x} - \frac{px}{1-px}$$

$$g_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^{2i-1})x^i = \frac{1-px}{1-p^2x}$$

$$h_p(x) = \frac{f_p(x)}{g_p(x)} = \frac{1}{1-px} - \frac{px(1-p^2x)}{(1-px)^2} = 1 + \sum_{i=2}^{\infty}(i-1)(p-1)p^ix^i$$

$$f_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^i)x^i = 1 + \frac{p^2x}{1-p^2x} - \frac{px}{1-px}$$

$$g_p(x) = 1 + \sum_{i=1}^{\infty}(p^{2i} - p^{2i-1})x^i = \frac{1-px}{1-p^2x}$$

$$h_p(x) = \frac{f_p(x)}{g_p(x)} = \frac{1}{1-px} - \frac{px(1-p^2x)}{(1-px)^2} = 1 + \sum_{i=2}^{\infty}(i-1)(p-1)p^ix^i$$

后面讲杜教筛，对于 f 要找到两个可块筛的函数 g, h 使得 $f * g = h$。可以根据 f 贝尔级数的封闭形式来配凑。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演
- 整除分块
- 莫比乌斯反演

7 积性函数前缀和

8 其他

整除分块

Theorem 1.1

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

整除分块

Theorem 1.1

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

Theorem 1.2

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

Theorem 1.3

对于给定的正整数 n, m，所有满足 $\left\lfloor \frac{n}{x} \right\rfloor = m$ 的正整数 x 恰为 $\left\lfloor \frac{n}{m+1} \right\rfloor + 1 \sim \left\lfloor \frac{n}{m} \right\rfloor$ 之间的所有整数。

P2260 模积和

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}(n \bmod i)(m \bmod j), i \neq j$。

$n, m \leq 10^9$。

先忽略 $i \neq j$ 的条件，原式等价于 $(\sum_{i=1}^{n} n \bmod i)(\sum_{j=1}^{m} m \bmod j)$。

先忽略 $i \neq j$ 的条件，原式等价于 $(\sum_{i=1}^{n} n \bmod i)(\sum_{j=1}^{m} m \bmod j)$。

$\sum_{i=1}^{n} n \bmod i = \sum_{i=1}^{n}(n - i\lfloor\frac{n}{i}\rfloor)$，由于 $\lfloor\frac{n}{i}\rfloor$ 只有 $O(\sqrt{n})$ 种不同的取值，故枚举每种取值 d，所有 $\lfloor\frac{n}{i}\rfloor = d$ 的 i 构成一个区间，可以快速计算。

先忽略 $i \neq j$ 的条件，原式等价于 $(\sum_{i=1}^{n} n \bmod i)(\sum_{j=1}^{m} m \bmod j)$。

$\sum_{i=1}^{n} n \bmod i = \sum_{i=1}^{n}(n - i\lfloor\frac{n}{i}\rfloor)$，由于 $\lfloor\frac{n}{i}\rfloor$ 只有 $O(\sqrt{n})$ 种不同的取值，故枚举每种取值 d，所有 $\lfloor\frac{n}{i}\rfloor = d$ 的 i 构成一个区间，可以快速计算。

再减掉 $i = j$ 的情况 $\sum_{i=1}^{\min\{n,m\}}(n - i\lfloor\frac{n}{i}\rfloor)^2$，同样使用整除分块方法。

先忽略 $i \neq j$ 的条件，原式等价于 $(\sum_{i=1}^{n} n \bmod i)(\sum_{j=1}^{m} m \bmod j)$。

$\sum_{i=1}^{n} n \bmod i = \sum_{i=1}^{n}(n - i\lfloor\frac{n}{i}\rfloor)$，由于 $\lfloor\frac{n}{i}\rfloor$ 只有 $O(\sqrt{n})$ 种不同的取值，故枚举每种取值 d，所有 $\lfloor\frac{n}{i}\rfloor = d$ 的 i 构成一个区间，可以快速计算。

再减掉 $i = j$ 的情况 $\sum_{i=1}^{\min\{n,m\}}(n - i\lfloor\frac{n}{i}\rfloor)^2$，同样使用整除分块方法。

复杂度 $O(\sqrt{n})$。

ARC068E Snuke Line

有一趟列车有 $m+1$ 个车站，从 0 到 m 编号。有 n 种商品，第 i 种只在编号 $[l_i, r_i]$ 的车站出售。一辆列车有一个预设好的系数 d，从 0 出发，只会在 d 的倍数车站停车。对于 d 从 1 到 m 的列车，求最多能买到多少种商品。

$1 \le n \le 3 \times 10^5, 1 \le m \le 10^5$。

ARC068E Snuke Line

有一趟列车有 $m+1$ 个车站，从 0 到 m 编号。有 n 种商品，第 i 种只在编号 $[l_i, r_i]$ 的车站出售。一辆列车有一个预设好的系数 d，从 0 出发，只会在 d 的倍数车站停车。对于 d 从 1 到 m 的列车，求最多能买到多少种商品。

$1 \le n \le 3 \times 10^5, 1 \le m \le 10^5$。

第 i 个商品会对满足 $\lfloor \frac{l_i - 1}{d} \rfloor < \lfloor \frac{r_i}{d} \rfloor$ 的 d 产生贡献。两个除式把 $1 \sim m$ 分成了 $O(\sqrt{m})$ 个区间，d 在每个区间里遍历时 $\lfloor \frac{l_i - 1}{d} \rfloor$ 和 $\lfloor \frac{r_i}{d} \rfloor$ 都不变。若二者不相等，则给该区间里每个 d 都加上 1 的贡献。差分即可。

线性预处理

如何在线性时间内对 $1 \sim n$ 中的每个 x 预处理出 $\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor$？

线性预处理

如何在线性时间内对 $1 \sim n$ 中的每个 x 预处理出 $\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor$？

观察到一个重要结论：$\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor = \sum_{i=1}^{x} d(i)$。然后递推即可。

线性预处理

如何在线性时间内对 $1 \sim n$ 中的每个 x 预处理出 $\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor$？

观察到一个重要结论：$\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor = \sum_{i=1}^{x} d(i)$。然后递推即可。

对所有 k，$\sum_{i=1}^{x} i^k \lfloor \frac{x}{i} \rfloor$ 均可线性预处理。

线性预处理

如何在线性时间内对 $1 \sim n$ 中的每个 x 预处理出 $\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor$？

观察到一个重要结论：$\sum_{i=1}^{x} \lfloor \frac{x}{i} \rfloor = \sum_{i=1}^{x} d(i)$。然后递推即可。

对所有 k，$\sum_{i=1}^{x} i^k \lfloor \frac{x}{i} \rfloor$ 均可线性预处理。

这种手法在马上要讲的莫比乌斯反演中有应用。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演
- 整除分块
- 莫比乌斯反演

7 积性函数前缀和

8 其他

莫比乌斯反演

如果有函数 $f = g * 1$，可以反推出 $g = f * \mu$。写成求和式就是：

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

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

莫比乌斯反演

如果有函数 $f = g * 1$，可以反推出 $g = f * \mu$。写成求和式就是：

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

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

反演是一个函数与积性函数的卷积，由前面的分析，复杂度为 $O(n \log \log n)$。

对于倍数的求和式，有类似的反演形式：

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

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

gcd 卷积

给定数列 a, b，求数列 f，满足 $f(n) = \sum_{\gcd(i,j)=n} a_i b_j$。

gcd 卷积

给定数列 a, b，求数列 f，满足 $f(n) = \sum\limits_{\gcd(i,j)=n} a_i b_j$。

先求 $g(n) = \sum\limits_{n|\gcd(i,j)} a_i b_j = (\sum\limits_{n|i} a_i)(\sum\limits_{n|j} b_j)$，可以 $O(n \log\log n)$ 求出。

gcd 卷积

给定数列 a, b，求数列 f，满足 $f(n) = \sum\limits_{\gcd(i,j)=n} a_i b_j$。

先求 $g(n) = \sum\limits_{n|\gcd(i,j)} a_i b_j = (\sum\limits_{n|i} a_i)(\sum\limits_{n|j} b_j)$，可以 $O(n \log\log n)$ 求出。
又由 $g(n) = \sum\limits_{n|d} f(d)$，可以 $O(n \log\log n)$ 反演得到 f。

gcd 求和

Example 5 (引例)

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

gcd 求和

Example 5 (引例)

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

莫比乌斯反演可以处理这类和 gcd 求和相关的问题。

利用 $\mu * 1 = \epsilon$，即 $\sum_{d|n} \mu(d) = [n = 1]$，进行如下变换：

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

一般形式：

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

更一般地，若 f, g 为完全积性函数：

$$
\begin{aligned}
&\sum_{i=1}^{n}\sum_{j=1}^{m} f(i)g(j)h(\gcd(i,j)) \\
=&\sum_{i=1}^{n}\sum_{j=1}^{m} f(i)g(j)(h*\mu*1)(\gcd(i,j)) \\
=&\sum_{d=1}^{n}(h*\mu)(d)\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor m/d\rfloor} f(id)g(jd) \\
=&\sum_{d=1}^{n}(h*\mu)(d)f(d)g(d)(\sum_{i=1}^{\lfloor n/d\rfloor} f(i))(\sum_{j=1}^{\lfloor m/d\rfloor} g(j))
\end{aligned}
$$

P2257 YY 的 GCD

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)\in\mathbb{P}]$。$1\le n,m\le 10^7$。

P2257 YY 的 GCD

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)\in\mathbb{P}]$。$1\le n,m\le 10^7$。

令 $f(n)=[n\in\mathbb{P}]$，需要求 $g=f*\mu$。

P2257 YY 的 GCD

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)\in\mathbb{P}]$。$1\le n,m\le 10^7$。

令 $f(n)=[n\in\mathbb{P}]$，需要求 $g=f*\mu$。

发现若 $x=\prod p_i^{\alpha_i}$ 中有两个 α_i 大于 1，则 $g(x)$ 一定为 0。简单分析知 g 可以线筛。

P6156 简单题

求 $\sum_{i=1}^{n}\sum_{j=1}^{n}(i+j)^k\mu^2(\gcd(i,j))\gcd(i,j)$。

$n \le 5\times 10^6, k \le 10^{18}$。

沿用之前的方法，记 $f=\mu^2\cdot\mathsf{id}, g=f*\mu$。原式化为 $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}(i+j)^k\sum\limits_{d|i,j}g(d)$，即 $\sum_{d=1}^{n}g(d)d^k\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor n/d\rfloor}(i+j)^k$。后面的二重求和式记作 $S(x)=\sum\limits_{i=1}^{x}\sum\limits_{j=1}^{x}(i+j)^k$，容易在线性时间内预处理出 S 在 $1\sim n$ 上每个点的取值。

沿用之前的方法，记 $f=\mu^2\cdot\mathsf{id}, g=f*\mu$。原式化为 $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}(i+j)^k\sum\limits_{d|i,j}g(d)$，即 $\sum_{d=1}^{n}g(d)d^k\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor n/d\rfloor}(i+j)^k$。后面的二重求和式记作 $S(x)=\sum\limits_{i=1}^{x}\sum\limits_{j=1}^{x}(i+j)^k$，容易在线性时间内预处理出 S 在 $1\sim n$ 上每个点的取值。

再来处理 g。可以看出 g 是积性函数，故只需求出 g 在素数幂处的取值即可线筛。$1\sim n$ 中所有素数幂的幂次和在 $O(\dfrac{n}{\log n})$ 级别，故暴力处理即可。

沿用之前的方法，记 $f=\mu^2\cdot\mathsf{id}, g=f*\mu$。原式化为 $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}(i+j)^k\sum\limits_{d|i,j}g(d)$，即 $\sum_{d=1}^{n}g(d)d^k\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor n/d\rfloor}(i+j)^k$。后面的二重求和式记作 $S(x)=\sum\limits_{i=1}^{x}\sum\limits_{j=1}^{x}(i+j)^k$，容易在线性时间内预处理出 S 在 $1\sim n$ 上每个点的取值。

再来处理 g。可以看出 g 是积性函数，故只需求出 g 在素数幂处的取值即可线筛。$1\sim n$ 中所有素数幂的幂次和在 $O(\dfrac{n}{\log n})$ 级别，故暴力处理即可。

复杂度 $O(n)$。

SOJ1985 拼图

对于正整数对 (a,b)，定义一次操作将其变为 $(\min(a,b),\max(a,b)-\min(a,b))$。设 $f(a,b)$ 为最小的操作次数，使得某一个数变成 0。

给定正整数 n，求 $\sum_{i=1}^{n}\sum_{j=1}^{n} f(i,j)$。$n \le 2\times 10^7$。

对于 (a,b)，$a \geq b$ 时将其变换为 $(a-b,b)$，否则变换为 $(a,b-a)$。答案显然不变。

对于 (a, b)，$a \geq b$ 时将其变换为 $(a-b, b)$，否则变换为 $(a, b-a)$。答案显然不变。

把每个点向其变换后的点连一条边，形成二叉树结构。对于点 (a, b)，其左儿子为 $(a+b, b)$，右儿子为 $(a, a+b)$。答案即为所有点的子树大小之和。

对于 (a,b)，$a \geq b$ 时将其变换为 $(a-b,b)$，否则变换为 $(a,b-a)$。答案显然不变。

把每个点向其变换后的点连一条边，形成二叉树结构。对于点 (a,b)，其左儿子为 $(a+b,b)$，右儿子为 $(a,a+b)$。答案即为所有点的子树大小之和。

Theorem 2.1 (结论)

(a,b) 子树大小为 $1+2\sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j)=1][ai+bj\leq n]$。

Proof.

记 $L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$。则 $\begin{pmatrix} a \\ b \end{pmatrix}$ 子树中的点为 $M\begin{pmatrix} a \\ b \end{pmatrix}$，$M$ 为 L, R 连乘得到的任意矩阵。答案即为求有多少个 M 使得 $M\begin{pmatrix} a \\ b \end{pmatrix} \le \begin{pmatrix} n \\ n \end{pmatrix}$。

Proof.

记 $L=\begin{pmatrix}1&1\\0&1\end{pmatrix},R=\begin{pmatrix}1&0\\1&1\end{pmatrix}$。则 $\begin{pmatrix}a\\b\end{pmatrix}$ 子树中的点为 $M\begin{pmatrix}a\\b\end{pmatrix}$，$M$ 为 L,R 连乘得到的任意矩阵。答案即为求有多少个 M 使得 $M\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}n\\n\end{pmatrix}$。

$M=I$ 时显然可以，$M\ne I$ 时，记 $M=PM_1$，P 为 L 或 R。可知 $M\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}n\\n\end{pmatrix}$ 等价于 $\begin{pmatrix}1&1\end{pmatrix}M_1\begin{pmatrix}a\\b\end{pmatrix}\le n$。于是答案为 $1+2\sum\limits_{M}[\begin{pmatrix}1&1\end{pmatrix}M\begin{pmatrix}a\\b\end{pmatrix}\le n]$。

Proof.

记 $L=\begin{pmatrix}1&1\\0&1\end{pmatrix},R=\begin{pmatrix}1&0\\1&1\end{pmatrix}$。则 $\begin{pmatrix}a\\b\end{pmatrix}$ 子树中的点为 $M\begin{pmatrix}a\\b\end{pmatrix}$，$M$ 为 L,R 连乘得到的任意矩阵。答案即为求有多少个 M 使得 $M\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}n\\n\end{pmatrix}$。

$M=I$ 时显然可以，$M\ne I$ 时，记 $M=PM_1$，P 为 L 或 R。可知 $M\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}n\\n\end{pmatrix}$ 等价于 $\begin{pmatrix}1&1\end{pmatrix}M_1\begin{pmatrix}a\\b\end{pmatrix}\le n$。于是答案为 $1+2\sum\limits_M[\begin{pmatrix}1&1\end{pmatrix}M\begin{pmatrix}a\\b\end{pmatrix}\le n]$。

$\begin{pmatrix}1&1\end{pmatrix}M$ 构成的集合与 $\{\begin{pmatrix}i&j\end{pmatrix}\mid\gcd(i,j)=1\}$ 相等，且存在一个双射。因此答案即为 $1+2\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n}[\gcd(i,j)=1][ai+bj\le n]$。 □

开始化式子：

$$\sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j)=1][ai+bj\le n]$$

开始化式子：

$$\sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j)=1][ai+bj\le n]$$

$$=\sum_{a=1}^{n}\sum_{n=1}^{n}\sum_{d=1}^{n}\mu(d)\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor n/d\rfloor}[ai+bj\le\lfloor\frac{n}{d}\rfloor]$$

开始化式子：

$$\sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[\gcd(i,j)=1][ai+bj\le n]$$

$$=\sum_{a=1}^{n}\sum_{n=1}^{n}\sum_{d=1}^{n}\mu(d)\sum_{i=1}^{\lfloor n/d\rfloor}\sum_{j=1}^{\lfloor n/d\rfloor}[ai+bj\le\lfloor\frac{n}{d}\rfloor]$$

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

其中

$$S(n)=\sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[ai+bj\le n]$$

其中

$$
\begin{aligned}
S(n) &= \sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[ai+bj\le n] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n-i} d(i)\,d(j)
\end{aligned}
$$

其中

$$
\begin{aligned}
S(n) &= \sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[ai+bj\le n] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n-i} d(i)\,d(j) \\
&= \sum_{i=1}^{n} d(i)\,S_d(n-i)
\end{aligned}
$$

其中

$$
\begin{aligned}
S(n) &= \sum_{a=1}^{n}\sum_{b=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[ai+bj\le n] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n-i} d(i)\,d(j) \\
&= \sum_{i=1}^{n} d(i)\,S_d(n-i)
\end{aligned}
$$

S_d 为 d 的前缀和，可以线性预处理。总复杂度为所有不同的 $\lfloor \frac{n}{d} \rfloor$ 求和，是 $O(n\log n)$ 的，常数很小。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和
- 杜教筛
- PN 筛

8 其他

块筛

记 $S_f(n) = \sum_{i=1}^{n} f(i)$。块筛定义为：对于一个 n，求出

$$\{(\lfloor \frac{n}{i} \rfloor, S_f(\lfloor \frac{n}{i} \rfloor)) \mid i \in \{1, 2, \ldots, n\}\}$$

块筛

记 $S_f(n) = \sum_{i=1}^{n} f(i)$。块筛定义为：对于一个 n，求出

$$\{(\lfloor \frac{n}{i} \rfloor, S_f(\lfloor \frac{n}{i} \rfloor)) \mid i \in \{1, 2, \ldots, n\}\}$$

集合大小是 $O(\sqrt{n})$ 的。

杜教筛

杜教筛的核心思想是寻找 $f = g/h$，满足 g, h 可块筛，则可以用 $O(n^{2/3})$ 复杂度块筛 f。

杜教筛

杜教筛的核心思想是寻找 $f = g/h$，满足 g, h 可块筛，则可以用 $O(n^{2/3})$ 复杂度块筛 f。

$$S_g(n) = \sum_{i=1}^{n} \sum_{d|i} h(d) f(\frac{i}{d})$$

杜教筛

杜教筛的核心思想是寻找 $f = g/h$，满足 g, h 可块筛，则可以用 $O(n^{2/3})$ 复杂度块筛 f。

$$
\begin{aligned}
S_g(n) &= \sum_{i=1}^{n} \sum_{d|i} h(d) f(\frac{i}{d}) \\
&= \sum_{d=1}^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor)
\end{aligned}
$$

杜教筛

杜教筛的核心思想是寻找 $f = g/h$，满足 g, h 可块筛，则可以用 $O(n^{2/3})$ 复杂度块筛 f。

$$
\begin{aligned}
S_g(n) &= \sum_{i=1}^{n} \sum_{d|i} h(d) f(\frac{i}{d}) \\
&= \sum_{d=1}^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor) \\
&= S_f(n) h(1) + \sum_{d=2}^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor)
\end{aligned}
$$

杜教筛

杜教筛的核心思想是寻找 $f = g/h$，满足 g, h 可块筛，则可以用 $O(n^{2/3})$ 复杂度块筛 f。

$$
\begin{aligned}
S_g(n) &= \sum_{i=1}^{n} \sum_{d|i} h(d) f(\frac{i}{d}) \\
&= \sum_{d=1}^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor) \\
&= S_f(n) h(1) + \sum_{d=2}^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor)
\end{aligned}
$$

$$
S_f(n) = \frac{1}{h(1)} (S_g(n) - \sum^{n} h(d) S_f(\lfloor \frac{n}{d} \rfloor))
$$

对上式整除分块，枚举 $m = \lfloor \frac{n}{d} \rfloor$，满足 $\lfloor \frac{n}{d} \rfloor = m$ 的 d 为 $\lfloor \frac{n}{m+1} \rfloor + 1 \sim \lfloor \frac{n}{m} \rfloor$。由于 h 可块筛，故 h 在该区间的和可以 $O(1)$ 计算，$S_f(n)$ 可以 $O(\sqrt{n})$ 计算。

对上式整除分块，枚举 $m = \lfloor \frac{n}{d} \rfloor$，满足 $\lfloor \frac{n}{d} \rfloor = m$ 的 d 为 $\lfloor \frac{n}{m+1} \rfloor + 1 \sim \lfloor \frac{n}{m} \rfloor$。由于 h 可块筛，故 h 在该区间的和可以 $O(1)$ 计算，$S_f(n)$ 可以 $O(\sqrt{n})$ 计算。

分析复杂度。在每个 n 处复杂度都是 $O(\sqrt{n})$，总复杂度为 $O(\sum_{i=1}^{\sqrt{n}} \sqrt{i} + \sqrt{n/i}) = O(n^{3/4})$。

对上式整除分块，枚举 $m = \lfloor \frac{n}{d} \rfloor$，满足 $\lfloor \frac{n}{d} \rfloor = m$ 的 d 为 $\lfloor \frac{n}{m+1} \rfloor + 1 \sim \lfloor \frac{n}{m} \rfloor$。由于 h 可块筛，故 h 在该区间的和可以 $O(1)$ 计算，$S_f(n)$ 可以 $O(\sqrt{n})$ 计算。

分析复杂度。在每个 n 处复杂度都是 $O(\sqrt{n})$，总复杂度为 $O(\sum_{i=1}^{\sqrt{n}} \sqrt{i} + \sqrt{n/i}) = O(n^{3/4})$。

如果使用线筛预处理出前 $n^{2/3}$ 项，则复杂度降为 $O(\sum_{i=1}^{n^{1/3}} \sqrt{n/i}) = O(n^{2/3})$。

对上式整除分块，枚举 $m = \lfloor \frac{n}{d} \rfloor$，满足 $\lfloor \frac{n}{d} \rfloor = m$ 的 d 为 $\lfloor \frac{n}{m+1} \rfloor + 1 \sim \lfloor \frac{n}{m} \rfloor$。由于 h 可块筛，故 h 在该区间的和可以 $O(1)$ 计算，$S_f(n)$ 可以 $O(\sqrt{n})$ 计算。

分析复杂度。在每个 n 处复杂度都是 $O(\sqrt{n})$，总复杂度为 $O(\sum_{i=1}^{\sqrt{n}} \sqrt{i} + \sqrt{n/i}) = O(n^{3/4})$。

如果使用线筛预处理出前 $n^{2/3}$ 项，则复杂度降为 $O(\sum_{i=1}^{n^{1/3}} \sqrt{n/i}) = O(n^{2/3})$。

实际计算中可以在计算 $S_f(n)$ 时递归计算每个 $S_f(\lfloor \frac{n}{d} \rfloor)$。求出 $S_f(n)$ 的同时得出所有块筛。

如果不是 $f = g/h$ 而是 $f = g * h$，同样可以求 $S_f(n)$ 的块筛。

如果不是 $f = g/h$ 而是 $f = g * h$，同样可以求 $S_f(n)$ 的块筛。

$$
\begin{aligned}
S_f(n) &= \sum_{i=1}^{n} \sum_{d|i} g(d) h(\frac{i}{d}) \\
&= \sum_{d=1}^{n} g(d) S_h(\lfloor \frac{n}{d} \rfloor)
\end{aligned}
$$

如果不是 $f = g/h$ 而是 $f = g * h$，同样可以求 $S_f(n)$ 的块筛。

$$\begin{aligned} S_f(n) &= \sum_{i=1}^{n} \sum_{d|i} g(d) h(\frac{i}{d}) \\ &= \sum_{d=1}^{n} g(d) S_h(\lfloor \frac{n}{d} \rfloor) \end{aligned}$$

如果已知 g, h 的块筛，则对 S_f 求单点需要 $O(\sqrt{n})$，求块筛同样可以预处理前 $n^{2/3}$ 项达到 $O(n^{2/3})$。

练习

用 $O(n^{2/3})$ 复杂度求以下函数的块筛：

- φ
- μ
- σ_k
- $\varphi \cdot \mathsf{id}_k$
- $d \cdot \mathsf{id}_k$

练习

用 $O(n^{2/3})$ 复杂度求以下函数的块筛：

- φ
- μ
- σ_k
- $\varphi \cdot \mathsf{id}_k$
- $d \cdot \mathsf{id}_k$

提示：使用贝尔级数来找合适的 $f = g/h$。

P4318 完全平方数

$\mu^2(n) = \mu(n) \cdot \mu(n)$。求 $S_{\mu^2}(n)$。

P4318 完全平方数

$\mu^2(n) = \mu(n) \cdot \mu(n)$。求 $S_{\mu^2}(n)$。

n 可以被唯一地分解为 $x^2 y$，其中 $\mu^2(y) = 1$。

P4318 完全平方数

$\mu^2(n) = \mu(n) \cdot \mu(n)$。求 $S_{\mu^2}(n)$。

n 可以被唯一地分解为 $x^2 y$，其中 $\mu^2(y) = 1$。
令 $f(n) = [\exists d, d^2 = n]$，则 $1 = f * \mu^2$。

P4318 完全平方数

$\mu^2(n) = \mu(n) \cdot \mu(n)$。求 $S_{\mu^2}(n)$。

n 可以被唯一地分解为 $x^2 y$，其中 $\mu^2(y) = 1$。
令 $f(n) = [\exists d, d^2 = n]$，则 $1 = f * \mu^2$。
$S_f(n) = \lfloor \sqrt{n} \rfloor$ 可以 $O(1)$ 计算，故可以杜教筛。复杂度 $O(n^{2/3})$。

更优秀的做法：

$$\mu^2(n) = [x = 1] = \sum_{d|x} \mu(d) = \sum_{d^2|n} \mu(d)$$

$$S_{\mu^2}(n) = \sum_{i=1}^{n} \sum_{d^2|i} \mu(d) = \sum_{d=1}^{\sqrt{n}} \mu(d) \lfloor \frac{n}{d^2} \rfloor$$

更优秀的做法：

$$\mu^2(n) = [x = 1] = \sum_{d|x} \mu(d) = \sum_{d^2|n} \mu(d)$$

$$S_{\mu^2}(n) = \sum_{i=1}^{n} \sum_{d^2|i} \mu(d) = \sum_{d=1}^{\sqrt{n}} \mu(d) \lfloor \frac{n}{d^2} \rfloor$$

复杂度 $O(\sqrt{n})$。

不明来源题

将 n 质因数分解为 $\sum_{i=1}^{k} p_i^{\alpha_i}$，定义 $f(n) = (-1)^{\sum_{i=1}^{k} \alpha_i}$。杜教筛 S_f。

不明来源题

将 n 质因数分解为 $\sum_{i=1}^{k} p_i^{\alpha_i}$，定义 $f(n) = (-1)^{\sum_{i=1}^{k} \alpha_i}$。杜教筛 S_f。

显然 f 是积性函数。

计算其贝尔级数 $f_p(x) = \sum_{i=0}^{\infty} (-1)^i x^i = \frac{1}{1+x}$。于是 $f = \epsilon / \mu^2$。

不明来源题

将 n 质因数分解为 $\sum_{i=1}^{k} p_i^{\alpha_i}$，定义 $f(n) = (-1)^{\sum_{i=1}^{k} \alpha_i}$。杜教筛 S_f。

显然 f 是积性函数。

计算其贝尔级数 $f_p(x) = \sum_{i=0}^{\infty} (-1)^i x^i = \frac{1}{1+x}$。于是 $f = \epsilon / \mu^2$。

由上题，μ^2 可块筛。故 S_f 可以 $O(n^{2/3})$ 求。

51nod1220 约数之和

求 $\sum_{i=1}^{n}\sum_{j=1}^{n}\sigma(ij)$。$n \le 10^9$。

Theorem 1.1

$$\sigma(xy) = \sum_{i|x} \sum_{j|y} \frac{x}{i} \cdot j[\gcd(i,j) = 1]$$

Theorem 1.1

$$\sigma(xy) = \sum_{i|x} \sum_{j|y} \frac{x}{i} \cdot j[\gcd(i,j) = 1]$$

Proof.

在集合 $S = \{(i,j) \mid i|x, j|y, \gcd(i,j) = 1\}$ 与 $D = \{d \mid xy\}$ 之间构造映射。(i,j) 对应于 $d = \frac{x}{i} \cdot j$，d 对应于 $(\frac{x}{\gcd(d,x)}, \frac{d}{\gcd(d,x)})$。

Theorem 1.1

$$\sigma(xy) = \sum_{i|x} \sum_{j|y} \frac{x}{i} \cdot j[\gcd(i,j) = 1]$$

Proof.

在集合 $S = \{(i,j) \mid i|x, j|y, \gcd(i,j) = 1\}$ 与 $D = \{d \mid xy\}$ 之间构造映射。(i,j) 对应于 $d = \frac{x}{i} \cdot j$，d 对应于 $(\frac{x}{\gcd(d,x)}, \frac{d}{\gcd(d,x)})$。

分别在每个素因子上考虑，可以发现两个映射都是单射，且互为逆映射。故为双射。将每个 d 替换为对应的 (i,j) 即得。 □

根据引理，原式化为

$$\sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{i|x}\sum_{j|y}\frac{x}{i}j\sum_{d|i,j}\mu(d)$$

根据引理，原式化为

$$\sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{i|x}\sum_{j|y}\frac{x}{i}j\sum_{d|i,j}\mu(d)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|i}\sum_{i|x}\frac{x}{i})(\sum_{d|j}\sum_{j|y}j)$$

根据引理，原式化为

$$\sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{i|x}\sum_{j|y}\frac{x}{i}j\sum_{d|i,j}\mu(d)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|i}\sum_{i|x}\frac{x}{i})(\sum_{d|j}\sum_{j|y}j)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|x}\sum_{d|i|x}\frac{x}{i})(\sum_{d|y}\sum_{d|j|y}d\cdot\frac{j}{d})$$

根据引理，原式化为

$$\sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{i|x}\sum_{j|y}\frac{x}{i}j\sum_{d|i,j}\mu(d)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|i}\sum_{i|x}\frac{x}{i})(\sum_{d|j}\sum_{j|y}j)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|x}\sum_{d|i|x}\frac{x}{i})(\sum_{d|y}\sum_{d|j|y}d\cdot\frac{j}{d})$$

$$=\sum_{d=1}^{n}\mu(d)\cdot d\cdot S_{\sigma}^{2}(\lfloor\frac{n}{d}\rfloor)$$

根据引理，原式化为

$$\sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{i|x}\sum_{j|y}\frac{x}{i}j\sum_{d|i,j}\mu(d)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|i}\sum_{i|x}\frac{x}{i})(\sum_{d|j}\sum_{j|y}j)$$

$$=\sum_{d=1}^{n}\mu(d)(\sum_{d|x}\sum_{d|i|x}\frac{x}{i})(\sum_{d|y}\sum_{d|j|y}d\cdot\frac{j}{d})$$

$$=\sum_{d=1}^{n}\mu(d)\cdot d\cdot S_{\sigma}^{2}(\lfloor\frac{n}{d}\rfloor)$$

求 $\mu\cdot\mathrm{id}$ 和 σ 的块筛即可。复杂度 $O(n^{2/3})$。

P1587 [NOI2016] 循环之美

给定 n, m, k，求在 k 进制下，有多少个数值上互不相等的纯循环小数，可以用分数 $\frac{x}{y}$ 表示，其中 $1 \le x \le n, 1 \le y \le m$，且 $x, y \in \mathbb{Z}$。

一个数是纯循环的，当且仅当它在 k 进制下可以写成 $a.\dot{c}_1 c_2 c_3 \ldots c_{l-1} \dot{c}_l$。

$n, m \le 10^9, k \le 2000$。

设 $\dfrac{x}{y}$ 是纯循环小数，循环节长度为 l。有 $\dfrac{xk^l}{y}-\dfrac{x}{y}\in\mathbb{Z}$，即 $xk^l\equiv x \pmod{y}$。而 $\gcd(x,y)=1$，故 $k^l\equiv 1 \pmod{y}$，等价于 $\gcd(k,y)=1$。易知这也是充分条件。

设 $\frac{x}{y}$ 是纯循环小数，循环节长度为 l。有 $\frac{xk^l}{y}-\frac{x}{y}\in\mathbb{Z}$，即 $xk^l\equiv x \pmod y$。而 $\gcd(x,y)=1$，故 $k^l\equiv 1 \pmod y$，等价于 $\gcd(k,y)=1$。易知这也是充分条件。

故答案为

$$\sum_{x=1}^{n}\sum_{y=1}^{m}[\gcd(x,y)=1][\gcd(y,k)=1]$$

$$
\begin{aligned}
\mathsf{ans} &= \sum_{d=1}^{n} \mu(d) \sum_{d|x} \sum_{d|y} [\gcd(y,k)=1] \\
&= \sum_{d=1}^{n} \mu(d) \cdot \chi_k(d) \cdot \lfloor \frac{n}{d} \rfloor \cdot S_{\chi_k}(\lfloor \frac{m}{d} \rfloor)
\end{aligned}
$$

$$\begin{aligned}\mathsf{ans} &= \sum_{d=1}^{n} \mu(d) \sum_{d|x} \sum_{d|y} [\gcd(y,k)=1] \\ &= \sum_{d=1}^{n} \mu(d) \cdot \chi_k(d) \cdot \lfloor \frac{n}{d} \rfloor \cdot S_{\chi_k}(\lfloor \frac{m}{d} \rfloor)\end{aligned}$$

其中 $\chi_k(x) = [\gcd(x,k)=1]$，是一个完全积性函数。

$$\begin{aligned}\mathsf{ans} &= \sum_{d=1}^{n} \mu(d) \sum_{d|x} \sum_{d|y} [\gcd(y,k)=1] \\ &= \sum_{d=1}^{n} \mu(d) \cdot \chi_k(d) \cdot \lfloor \frac{n}{d} \rfloor \cdot S_{\chi_k}(\lfloor \frac{m}{d} \rfloor)\end{aligned}$$

其中 $\chi_k(x) = [\gcd(x,k)=1]$，是一个完全积性函数。

$S_{\chi_k}(x) = \lfloor \frac{x}{k} \rfloor \varphi(k) + S_{\chi_k}(x \bmod k)$，可以 $O(k)$ 预处理后 $O(1)$ 查询。

$$\begin{aligned}\mathsf{ans} &= \sum_{d=1}^{n} \mu(d) \sum_{d|x} \sum_{d|y} [\gcd(y,k)=1] \\ &= \sum_{d=1}^{n} \mu(d) \cdot \chi_k(d) \cdot \lfloor \frac{n}{d} \rfloor \cdot S_{\chi_k}(\lfloor \frac{m}{d} \rfloor)\end{aligned}$$

其中 $\chi_k(x) = [\gcd(x,k)=1]$，是一个完全积性函数。

$S_{\chi_k}(x) = \lfloor \frac{x}{k} \rfloor \varphi(k) + S_{\chi_k}(x \bmod k)$，可以 $O(k)$ 预处理后 $O(1)$ 查询。

于是只需再块筛 $\mu \cdot \chi_k$。$(\mu \cdot \chi_k) * \chi_k = (\mu \cdot \chi_k) * (1 \cdot \chi_k) = (\mu * 1) \cdot \chi_k = \epsilon$。杜教筛即可。复杂度 $O(n^{2/3})$。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和
- 杜教筛
- PN 筛

8 其他

Powerful Number

将 n 质因数分解，若每个素数的指数均大于等于 2，则称 n 是一个 Powerful Number。

Powerful Number

将 n 质因数分解，若每个素数的指数均大于等于 2，则称 n 是一个 Powerful Number。

Theorem 2.1

n 以内的 *PN* 数量为 $O(\sqrt{n})$ 级别。

Powerful Number

将 n 质因数分解，若每个素数的指数均大于等于 2，则称 n 是一个 Powerful Number。

Theorem 2.1

n 以内的 *PN* 数量为 $O(\sqrt{n})$ 级别。

Proof.

一个 PN 可以被分解为 a^2b^3 的形式。

$$O(\sum_{a=1}^{\sqrt{n}}\sqrt[3]{\frac{n}{a^2}}) = O(n^{1/3}\int_1^{n^{1/2}} x^{-2/3}\mathrm{d}x) = O(\sqrt{n})$$

□

如何找 n 以内所有 PN？取出 $\sqrt{n}$ 以内所有素数，用 DFS 对这些素数及其素数幂进行组合即可。复杂度 $O(\sqrt{n})$。

素数拟合

给定一个积性函数 f，求 $S_f(n)$。

素数拟合

给定一个积性函数 f，求 $S_f(n)$。

做法：构造一个易块筛的积性函数 g，满足 g 在所有素数处都与 f 相等。称为 g 与 f 素数拟合。

素数拟合

给定一个积性函数 f，求 $S_f(n)$。

做法：构造一个易块筛的积性函数 g，满足 g 在所有素数处都与 f 相等。称为 g 与 f 素数拟合。

再令 $h = f/g$，此时 h 也是积性函数。由 $f(p) = g(p)h(1) + g(1)h(p), g(p) = f(p)$，知 $h(p) = 0$。于是 h 只在 PN 处有值。

素数拟合

给定一个积性函数 f，求 $S_f(n)$。

做法：构造一个易块筛的积性函数 g，满足 g 在所有素数处都与 f 相等。称为 g 与 f 素数拟合。

再令 $h = f/g$，此时 h 也是积性函数。由 $f(p) = g(p)h(1) + g(1)h(p), g(p) = f(p)$，知 $h(p) = 0$。于是 h 只在 PN 处有值。

$$
\begin{aligned}
S_f(n) &= \sum_{i=1}^{n} \sum_{d|i} h(d) g(\frac{i}{d}) \\
&= \sum_{d \in \mathsf{PN}} h(d) S_g(\lfloor \frac{n}{d} \rfloor)
\end{aligned}
$$

接下来求 h。因为 h 有积性，故只需要求出其在素数幂处的取值。

接下来求 h。因为 h 有积性，故只需要求出其在素数幂处的取值。

$$f(p^k) = \sum_{i=0}^{k} h(p^i) g(p^{k-i})$$

$$h(p^k) = f(p^k) - \sum_{i=1}^{k-1} h(p^i) g(p^{k-i})$$

接下来求 h。因为 h 有积性，故只需要求出其在素数幂处的取值。

$$f(p^k) = \sum_{i=0}^{k} h(p^i) g(p^{k-i})$$

$$h(p^k) = f(p^k) - \sum_{i=1}^{k-1} h(p^i) g(p^{k-i})$$

所有的 $h(p^k)$ 都可以在找 PN 的过程中暴力求出。这部分的复杂度为 $O(\sum_{p\in\mathbb{P}, p\le\sqrt{n}} \log_p^2(n)) = O(\frac{\sqrt{n}}{\log n})$，不为瓶颈。

一般复杂度瓶颈在于块筛 g。常为 $O(n^{2/3})$。

一般复杂度瓶颈在于块筛 g。常为 $O(n^{2/3})$。
特别地，如果 $S_g(x)$ 能在 $O(\sqrt{x})$ 内求出，则复杂度优化至

$$O(\sum_{d\in\mathsf{PN}}\sqrt{\frac{n}{d}}) = O(\sum_{a,b}\sqrt{\frac{n}{a^2b^3}}) = O(n^{1/2}\sum_a\frac{1}{a}) = O(\sqrt{n}\log n)$$

P5325 【模板】Min_25 筛

定义积性函数 f，$f(p^k) = p^k(p^k - 1)$。求 $S_f(n)$。$n \le 10^{10}$。

P5325 【模板】Min_25 筛

定义积性函数 f，$f(p^k) = p^k(p^k - 1)$。求 $S_f(n)$。$n \le 10^{10}$。

令 $g = \mathsf{id} \cdot \varphi$。则 g 与 f 素数拟合。

P5325 【模板】Min_25 筛

定义积性函数 f，$f(p^k) = p^k(p^k - 1)$。求 $S_f(n)$。$n \le 10^{10}$。

令 $g = \mathsf{id} \cdot \varphi$。则 g 与 f 素数拟合。
$\mathsf{id} \cdot \varphi = \mathsf{id} \cdot (\mathsf{id}/1) = \mathsf{id}_2/\mathsf{id}$，可以使用杜教筛求出块筛。复杂度 $O(n^{2/3})$。

LOJ6053 简单的函数

定义积性函数 f，$f(p^c) = p \oplus c$，其中 $\oplus$ 为异或。求 $S_f(n)$。
$n \le 10^{10}$。

当 p 为 2 时，$f(p) = 3$。当 p 为奇素数时，$f(p) = p - 1$。

当 p 为 2 时，$f(p)=3$。当 p 为奇素数时，$f(p)=p-1$。

于是构造 $g(x)=\begin{cases}3\varphi(x) & 2\mid x\\ \varphi(x) & 2\nmid x\end{cases}$，则 g 为积性函数且与 f 素数拟合。

当 p 为 2 时，$f(p)=3$。当 p 为奇素数时，$f(p)=p-1$。

于是构造 $g(x)=\begin{cases}3\varphi(x) & 2\mid x\\ \varphi(x) & 2\nmid x\end{cases}$，则 g 为积性函数且与 f 素数拟合。

只需块筛 $S_g(n)=\sum\limits_{i=1}^{n}\varphi(i)+2\sum\limits_{i=1}^{\lfloor n/2\rfloor}\varphi(2i)$。第一部分 S_φ 可以用杜教筛。

当 p 为 2 时，$f(p)=3$。当 p 为奇素数时，$f(p)=p-1$。

于是构造 $g(x)=\begin{cases}3\varphi(x) & 2\mid x\\ \varphi(x) & 2\nmid x\end{cases}$，则 g 为积性函数且与 f 素数拟合。

只需块筛 $S_g(n)=\sum\limits_{i=1}^{n}\varphi(i)+2\sum\limits_{i=1}^{\lfloor n/2\rfloor}\varphi(2i)$。第一部分 S_φ 可以用杜教筛。

第二部分 $F(n)=\sum\limits_{i=1}^{n}\varphi(2i)=\sum\limits_{i\le n,2\mid i}2\varphi(i)+\sum\limits_{i\le n,2\nmid i}\varphi(i)=S_\varphi(n)+\sum\limits_{i=1}^{\lfloor n/2\rfloor}\varphi(2i)$。于是得到递推式 $F(n)=S_\varphi(n)+F(\lfloor n/2\rfloor)$。递归计算的复杂度为 $O(\log n)$，不为瓶颈。

当 p 为 2 时，$f(p)=3$。当 p 为奇素数时，$f(p)=p-1$。

于是构造 $g(x)=\begin{cases}3\varphi(x) & 2\mid x\\ \varphi(x) & 2\nmid x\end{cases}$，则 g 为积性函数且与 f 素数拟合。

只需块筛 $S_g(n)=\sum\limits_{i=1}^{n}\varphi(i)+2\sum\limits_{i=1}^{\lfloor n/2\rfloor}\varphi(2i)$。第一部分 S_φ 可以用杜教筛。

第二部分 $F(n)=\sum\limits_{i=1}^{n}\varphi(2i)=\sum\limits_{i\le n,2\mid i}2\varphi(i)+\sum\limits_{i\le n,2\nmid i}\varphi(i)=S_\varphi(n)+\sum\limits_{i=1}^{\lfloor n/2\rfloor}\varphi(2i)$。于是得到递推式 $F(n)=S_\varphi(n)+F(\lfloor n/2\rfloor)$。递归计算的复杂度为 $O(\log n)$，不为瓶颈。

总复杂度为块筛 S_φ 的 $O(n^{2/3})$。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他
- 类欧几里得算法
- 连分数

直线下整点个数

求解如下函数

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

直线下整点个数

求解如下函数

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

实际上这是类欧几里得算法的一部分。由于形式简单，应用相对较多，故单独讲解。

若 $a \geq c$ 或 $b \geq c$，可以转化为 $a < c, b < c$ 的情况：

$$
\begin{aligned}
f(a,b,c,n) &= \sum_{i=0}^{n} \lfloor \frac{ai+b}{c} \rfloor \\
&= \sum_{i=0}^{n} \lfloor \frac{(\lfloor \frac{a}{c} \rfloor c + (a \bmod c))i + \lfloor \frac{b}{c} \rfloor c + (b \bmod c)}{c} \rfloor \\
&= \frac{n(n+1)}{2} \lfloor \frac{a}{c} \rfloor + (n+1) \lfloor \frac{b}{c} \rfloor + \sum_{i=0}^{n} \lfloor \frac{(a \bmod c)i + (b \bmod c)}{c} \rfloor \\
&= \frac{n(n+1)}{2} \lfloor \frac{a}{c} \rfloor + (n+1) \lfloor \frac{b}{c} \rfloor + f(a \bmod c, b \bmod c, c, n)
\end{aligned}
$$

接下来考虑一般情况 $a < c$ 且 $b < c$:

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

接下来考虑一般情况 $a < c$ 且 $b < c$:

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

$$
j < \lfloor \frac{ai+b}{c} \rfloor \iff \frac{jc+c-b-1}{a} < i
$$

令 $m = \lfloor \frac{an+b}{c} \rfloor$，有

$$
\begin{aligned}
f(a,b,c,n) &= \sum_{j=0}^{m-1} n - \lfloor \frac{jc+c-b-1}{a} \rfloor \\
&= nm - f(c, c-b-1, a, m-1)
\end{aligned}
$$

令 $m = \lfloor \frac{an+b}{c} \rfloor$，有

$$
\begin{aligned}
f(a, b, c, n) &= \sum_{j=0}^{m-1} n - \lfloor \frac{jc + c - b - 1}{a} \rfloor \\
&= nm - f(c, c - b - 1, a, m - 1)
\end{aligned}
$$

于是可以递归计算。复杂度 $O(\log n)$。

CF1912J Joy of Pok´emon Observation

给定 l_1, l_2, l_3, t，求满足 $l_1x + l_2y + l_3z = t$ 的非负整数对 (x, y, z) 的数量。
$l_1, l_2, l_3 \le 16, t \le 10^9$。

将 x, y 在 $\bmod l_3$ 意义下考虑，设 $x = pl_3 + x', y = ql_3 + y'$，则 $l_3(l_1 p + l_2 q + z) = t - l_1 x' - l_2 y'$。

将 x, y 在 $\bmod l_3$ 意义下考虑，设 $x = pl_3 + x', y = ql_3 + y'$，则 $l_3(l_1p + l_2q + z) = t - l_1x' - l_2y'$。

枚举 x', y'，若 $l_3 \nmid t - l_1x' - l_2y'$ 则无解，否则记 $K = \dfrac{t - l_1x' - l_2y'}{l_3}$，变为求有多少 (p, q, z) 满足 $l_1p + l_2q + z = K$。

将 x, y 在 $\bmod l_3$ 意义下考虑，设 $x = pl_3 + x', y = ql_3 + y'$，则 $l_3(l_1p + l_2q + z) = t - l_1x' - l_2y'$。

枚举 x', y'，若 $l_3 \nmid t - l_1x' - l_2y'$ 则无解，否则记 $K = \dfrac{t - l_1x' - l_2y'}{l_3}$，变为求有多少 (p, q, z) 满足 $l_1p + l_2q + z = K$。

一旦确定了 p, q，则唯一确定了 z。故答案为求有多少 (p, q) 满足 $l_1p + l_2q \le K$。即为

$$\sum_{p=0}^{t}\left(\left\lfloor \frac{K - l_1p}{l_2} \right\rfloor + 1\right)$$

将 x, y 在 $\bmod l_3$ 意义下考虑，设 $x = pl_3 + x', y = ql_3 + y'$，则 $l_3(l_1p + l_2q + z) = t - l_1x' - l_2y'$。

枚举 x', y'，若 $l_3 \nmid t - l_1x' - l_2y'$ 则无解，否则记 $K = \dfrac{t - l_1x' - l_2y'}{l_3}$，变为求有多少 (p, q, z) 满足 $l_1p + l_2q + z = K$。

一旦确定了 p, q，则唯一确定了 z。故答案为求有多少 (p, q) 满足 $l_1p + l_2q \le K$。即为

$$\sum_{p=0}^{t}\left(\left\lfloor \frac{K - l_1p}{l_2} \right\rfloor + 1\right)$$

复杂度 $O(l_3^2 \cdot \log t)$。

万能欧几里得算法

很多类欧几里得问题都可以归结为以下模型：

在平面直角坐标系内，有一条直线 $y = \dfrac{ax+b}{c}$，作出所有网格线 $x = k(k \in \mathbb{N}^*), y = k(k \in \mathbb{N}^*)$。

在 $(0, n]$ 中从左往右扫描该直线，与一条横的网格线有交点时进行一次 U 操作，与一条竖的网格线有交点时进行一次 R 操作。特别地，若同时与横线竖线有交点（即经过整点），规定先 U 后 R。

其中 U 和 R 都是半群元素，即满足结合律。

用 $f(n, a, b, c, U, R)$ 表示当前问题的答案。直线上下平移整数不影响答案，这意味着 b 可对 c 取模。以下默认 $b < c$。

用 $f(n,a,b,c,U,R)$ 表示当前问题的答案。直线上下平移整数不影响答案，这意味着 b 可对 c 取模。以下默认 $b<c$。

若 $a \geq c$，则每跨过一条竖线，会至少跨过 $\lfloor \frac{a}{c} \rfloor$ 条横线。

用 $f(n,a,b,c,U,R)$ 表示当前问题的答案。直线上下平移整数不影响答案，这意味着 b 可对 c 取模。以下默认 $b<c$。

若 $a \geq c$，则每跨过一条竖线，会至少跨过 $\lfloor \frac{a}{c} \rfloor$ 条横线。

$y = \frac{ax+b}{c} = \frac{(a \bmod c)x+b}{c} + \lfloor \frac{a}{c} \rfloor x$，故

$$f(n,a,b,c,U,R) = f(n, a \bmod c, b, c, U, U^{\lfloor \frac{a}{c} \rfloor} R)$$

若 $a < c$，考虑将直线沿 $y = x$ 对称。记 $m = \lfloor \frac{an+b}{c} \rfloor$，一共会产生 m 个 U。第 j 个 U 发生在跨过 $y = j$ 时，此时对应的 x 坐标为 $\frac{jc-b}{a}$，故第 j 个 U 之前 R 的数量为 $k_j = \lfloor \frac{jc-b-1}{a} \rfloor$。

若 $a < c$，考虑将直线沿 $y = x$ 对称。记 $m = \lfloor \frac{an+b}{c} \rfloor$，一共会产生 m 个 U。第 j 个 U 发生在跨过 $y = j$ 时，此时对应的 x 坐标为 $\frac{jc-b}{a}$，故第 j 个 U 之前 R 的数量为 $k_j = \lfloor \frac{jc-b-1}{a} \rfloor$。

现在整个操作序列被 m 个 U 分割，第一个 U 前有 k_1 个 R，最后一个 U 后有 $n - k_m$ 个 R，中间可以通过翻转坐标系变成 $a \geq c$ 的版本。故

$$f(n, a, b, c, U, R) = R^{k_1} \cdot U \cdot f(m-1, c, c-b-1, a, R, U) \cdot R^{n-k_m}$$

P5170【模板】类欧几里得算法

给定 n, a, b, c，分别求 $\sum_{i=0}^{n}\lfloor\frac{ai+b}{c}\rfloor, \sum_{i=0}^{n}\lfloor\frac{ai+b}{c}\rfloor^2, \sum_{i=0}^{n} i\lfloor\frac{ai+b}{c}\rfloor$。$t$ 组数据。

$t \le 10^5$，$0 \le n, a, b, c \le 10^9$，$c \ne 0$。

以 $\sum_{i=0}^{n}\lfloor\frac{ai+b}{c}\rfloor$ 为例。

设计二元组 (y, ans)，U 操作会让 $y \leftarrow y+1$，R 操作会让 $ans \leftarrow ans+y$。用矩阵描述 U 和 R，显然是满足结合律的。故可直接套用万欧。

QOJ8706 解方程

求方程 $(a+bx) \bmod p \in [0, c_2), x \in [0, c_1)$ 的所有解。
a, b 随机生成，$p \in [9 \times 10^{17}, 10^{18}]$ 且是质数，$c_1, c_2 \le 100\sqrt{p}$。

可以发现解的数量不多。对 x 的区间进行分治判定，假设有 k 个解，则将问题转化为 $O(k\log c_1)$ 次判定一个 x 的区间中是否存在解。

可以发现解的数量不多。对 x 的区间进行分治判定，假设有 k 个解，则将问题转化为 $O(k\log c_1)$ 次判定一个 x 的区间中是否存在解。

将 $(a+bx) \bmod p < c$ 改写为 $bx - p\left\lfloor \dfrac{a+bx}{p} \right\rfloor < c - a$。只需记录在一个 x 的区间中 $S = bx - p\left\lfloor \dfrac{a+bx}{p} \right\rfloor$ 的最小值。

可以发现解的数量不多。对 x 的区间进行分治判定，假设有 k 个解，则将问题转化为 $O(k\log c_1)$ 次判定一个 x 的区间中是否存在解。

将 $(a+bx) \bmod p < c$ 改写为 $bx - p\left\lfloor \dfrac{a+bx}{p} \right\rfloor < c-a$。只需记录在一个 x 的区间中 $S = bx - p\left\lfloor \dfrac{a+bx}{p} \right\rfloor$ 的最小值。

使用万欧的模型，维护二元组 (S, M)，直线 $y = \dfrac{a+bx}{p}$ 遇到竖线则 $S \leftarrow S + b, M = \min\{M, S\}$，遇到横线则 $S \leftarrow S - p$。R 与 U 操作可以用 $\min, +$ 矩阵表示。

1 整除

2 同余

3 组合数相关

4 阶与原根

5 数论函数

6 莫比乌斯反演

7 积性函数前缀和

8 其他
- 类欧几里得算法
- 连分数

连分数

形如

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

的分数被称为连分数，简记为 $[a_0, a_1, \cdots, a_n]$。若其中每个 a_i 均为正整数，则称为简单连分数。下面所说的连分数均指简单连分数。并定义 $x_k = [a_0, a_1, \cdots, a_k]$ 为 x 的 k 阶渐近分数。

有理数表示

Theorem 2.1

一个有理数有且仅有两种连分数表示。

有理数表示

Theorem 2.1

一个有理数有且仅有两种连分数表示。

用辗转相除法构造连分数：令 $r_0 = x$，$a_k = \lfloor r_k \rfloor$，$r_{k+1} = \dfrac{1}{r_k - a_k}$，当 r 为整数时停止。

有理数表示

Theorem 2.1

一个有理数有且仅有两种连分数表示。

用辗转相除法构造连分数：令 $r_0 = x$，$a_k = \lfloor r_k \rfloor$，$r_{k+1} = \dfrac{1}{r_k - a_k}$，当 r 为整数时停止。

这种方式可以构造出一个连分数，且位数是 log 级别的。

有理数表示

Theorem 2.1

一个有理数有且仅有两种连分数表示。

用辗转相除法构造连分数：令 $r_0 = x$，$a_k = \lfloor r_k \rfloor$，$r_{k+1} = \dfrac{1}{r_k - a_k}$，当 r 为整数时停止。

这种方式可以构造出一个连分数，且位数是 log 级别的。

若最后一位 $a_n \neq 1$，则 $[a_0, a_1, \cdots, a_n - 1, 1]$ 是另一种连分数表示。若 $a_n = 1$，则 $[a_0, a_1, \cdots, a_{n-1} + 1]$ 是另一种连分数表示。

Proof.

证明任意有理数不存在大于两种不同的连分数表示。

Proof.

证明任意有理数不存在大于两种不同的连分数表示。
只需证：若规定连分数的最后一位大于 1，则连分数表示唯一。

Proof.

证明任意有理数不存在大于两种不同的连分数表示。

只需证：若规定连分数的最后一位大于 1，则连分数表示唯一。

假设 $x = [a_0, a_1, \cdots, a_n] = [b_0, b_1, \cdots, b_m]$，其中 $a_n > 1, b_m > 1$。由于 $[a_1, \cdots, a_n] > 1$，知 $[a_1, \cdots, a_n]^{-1} < 1$，则 $a_0 = \lfloor x \rfloor$。同理 $b_0 = \lfloor x \rfloor$。

Proof.

证明任意有理数不存在大于两种不同的连分数表示。
只需证：若规定连分数的最后一位大于 1，则连分数表示唯一。
假设 $x = [a_0, a_1, \cdots, a_n] = [b_0, b_1, \cdots, b_m]$，其中 $a_n > 1, b_m > 1$。由于 $[a_1, \cdots, a_n] > 1$，知 $[a_1, \cdots, a_n]^{-1} < 1$，则 $a_0 = \lfloor x \rfloor$。同理 $b_0 = \lfloor x \rfloor$。
归纳即证。 □

Proof.

证明任意有理数不存在大于两种不同的连分数表示。
只需证：若规定连分数的最后一位大于 1，则连分数表示唯一。
假设 $x = [a_0, a_1, \cdots, a_n] = [b_0, b_1, \cdots, b_m]$，其中 $a_n > 1, b_m > 1$。由于 $[a_1, \cdots, a_n] > 1$，知 $[a_1, \cdots, a_n]^{-1} < 1$，则 $a_0 = \lfloor x \rfloor$。同理 $b_0 = \lfloor x \rfloor$。
归纳即证。 □

一般将 $a_n > 1$ 的连分数表示称为标准表示。

渐近分数

对于有理数 x，其 k 阶渐近分数为 $x_k = \dfrac{p_k}{q_k} = [a_0, \cdots, a_k]$。直接使用定义计算渐近分数并不方便。一般有如下递推公式：

$$\begin{cases} p_0 = a_0, p_1 = a_0 a_1 + 1 \\ p_k = a_k \cdot p_{k-1} + p_{k-2} \quad (k \geq 2) \\ q_0 = 1, q_1 = a_1 \\ q_k = a_k \cdot q_{k-1} + q_{k-2} \quad (k \geq 2) \end{cases}$$

Proof.

当 $a_{0\sim k-1}$ 确定，p_k, q_k 可以被表示为 a_k 的一次式，设 $p_k = A_k a_k + B_k$,，$q_k = C_k a_k + D_k$。则有：

$$\frac{p_{k+1}}{q_{k+1}} = [a_0, a_1, \cdots, a_k + \frac{1}{a_{k+1}}]$$

Proof.

当 $a_{0\sim k-1}$ 确定，p_k, q_k 可以被表示为 a_k 的一次式，设 $p_k = A_k a_k + B_k$,，$q_k = C_k a_k + D_k$。则有：

$$\begin{aligned}\frac{p_{k+1}}{q_{k+1}} &= [a_0, a_1, \cdots, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{A_k(a_k + \frac{1}{a_{k+1}}) + B_k}{C_k(a_k + \frac{1}{a_{k+1}}) + D_k}\end{aligned}$$

Proof.

当 $a_{0\sim k-1}$ 确定，p_k, q_k 可以被表示为 a_k 的一次式，设 $p_k = A_k a_k + B_k$,，$q_k = C_k a_k + D_k$。则有：

$$\begin{aligned}\frac{p_{k+1}}{q_{k+1}} &= [a_0, a_1, \cdots, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{A_k(a_k + \frac{1}{a_{k+1}}) + B_k}{C_k(a_k + \frac{1}{a_{k+1}}) + D_k} \\ &= \frac{(A_k a_k + B_k)a_{k+1} + A_k}{(C_k a_k + D_k)a_{k+1} + C_k}\end{aligned}$$

Proof.

当 $a_{0\sim k-1}$ 确定，p_k, q_k 可以被表示为 a_k 的一次式，设 $p_k = A_k a_k + B_k$,，$q_k = C_k a_k + D_k$。则有：

$$\begin{aligned}\frac{p_{k+1}}{q_{k+1}} &= [a_0, a_1, \cdots, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{A_k(a_k + \frac{1}{a_{k+1}}) + B_k}{C_k(a_k + \frac{1}{a_{k+1}}) + D_k} \\ &= \frac{(A_k a_k + B_k)a_{k+1} + A_k}{(C_k a_k + D_k)a_{k+1} + C_k}\end{aligned}$$

则 $B_{k+1} = A_k, A_{k+1} = p_k$。于是 $p_k = A_k a_k + B_k = p_{k-1}a_k + A_{k-1} = p_{k-1}a_k + p_{k-2}$。$q_k$ 同理。 □

P10788 [NOI2024] 分数

定义正分数为分子分母都为正整数的既约分数。定义完美正分数集合 S 为满足以下五条性质的集合：

- $\frac{1}{2} \in S$
- 对于 $\frac{1}{2} < x < 2$，$x \notin S$
- 对于所有 $x \in S$，$\frac{1}{x} \in S$
- 对于所有 $x \in S$，$x + 2 \in S$
- 对于所有 $x \in S$ 且 $x > 2$，$x - 2 \in S$

求 $1 \le i \le n, 1 \le j \le m$ 的完美正分数 $\frac{i}{j}$ 数量。$2 \le n, m \le 3 \times 10^7$。

把分数用标准连分数表示，取倒数相当于在连分数前面增加或删除一个 0，± 2 相当于对连分数的第一位 ± 2。于是可知：$x \in S \iff x = [2k_0, 2k_1, \cdots, 2k_n]$，其中 $k_0 \geq 0, k_1, \ldots, k_n \geq 1$。

把分数用标准连分数表示，取倒数相当于在连分数前面增加或删除一个 0，± 2 相当于对连分数的第一位 ± 2。于是可知：$x \in S \iff x = [2k_0, 2k_1, \cdots, 2k_n]$，其中 $k_0 \geq 0, k_1, \ldots, k_n \geq 1$。

由于有理数的标准连分数表示是唯一的，直接 DFS 搜索所有可能的连分数就能得到答案。具体地，从右到左加入连分数的每一位，实时维护其分数表示 $\frac{a}{b}$。这样的复杂度为 $O(ans)$，已经可以获得 90 分。

把分数用标准连分数表示，取倒数相当于在连分数前面增加或删除一个 0，± 2 相当于对连分数的第一位 ± 2。于是可知：$x \in S \iff x = [2k_0, 2k_1, \cdots, 2k_n]$，其中 $k_0 \geq 0, k_1, \ldots, k_n \geq 1$。

由于有理数的标准连分数表示是唯一的，直接 DFS 搜索所有可能的连分数就能得到答案。具体地，从右到左加入连分数的每一位，实时维护其分数表示 $\frac{a}{b}$。这样的复杂度为 $O(ans)$，已经可以获得 90 分。

后续的优化方式是考虑枚举连分数表示数列的最大值位置，然后可以一次统计好多个完美正分数。复杂度可能还是 $O(ans)$，但是常数小很多。