数论初步

HocRiser

吉林大学 20 级唐计

2021 年 1 月 27 日

1. 概述
   - 符号与约定
   - 同余与模运算
   - 素数
2. 数论定理
3. 数论算法

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \le a$，$b + 1 > a$，则称 $b = \lfloor a \rfloor$

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \leq a$，$b + 1 > a$，则称 $b = \lfloor a \rfloor$
- $a, b \in \mathbb{Z}$，定义 $a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \leq a$，$b + 1 > a$，则称 $b = \lfloor a \rfloor$
- $a, b \in \mathbb{Z}$，定义 $a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$
- $a, b \in \mathbb{N}*$，若 $b \bmod a = 0$，则称 a 整除 b，记为 $a|b$，并称 a 为 b 的约数，b 为 a 的倍数。

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \leq a$，$b+1 > a$，则称 $b = \lfloor a \rfloor$
- $a, b \in \mathbb{Z}$，定义 $a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$
- $a, b \in \mathbb{N}*$，若 $b \bmod a = 0$，则称 a 整除 b，记为 $a|b$，并称 a 为 b 的约数，b 为 a 的倍数。
- $a, b \in \mathbb{N}*$，最大的 $n(n \in \mathbb{N}*)$ 使得 $n|a$，$n|b$，则称 n 为 a 与 b 的最大公约数，记为 $n = gcd(a, b)$

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \leq a$，$b+1>a$，则称 $b=\lfloor a \rfloor$
- $a, b \in \mathbb{Z}$，定义 $a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$
- $a, b \in \mathbb{N}*$，若 $b \bmod a = 0$，则称 a 整除 b，记为 $a|b$，并称 a 为 b 的约数，b 为 a 的倍数。
- $a, b \in \mathbb{N}*$，最大的 $n(n \in \mathbb{N}*)$ 使得 $n|a$，$n|b$，则称 n 为 a 与 b 的最大公约数，记为 $n = gcd(a, b)$
- $a, b \in \mathbb{N}*$，最小的 $n(n \in \mathbb{N}*)$ 使得 $a|n$，$b|n$，则称 n 为 a 与 b 的最小公倍数，记为 $n = lcm(a, b)$

- $a \in \mathbb{R}$，$b \in \mathbb{Z}$，$b \leq a$，$b+1 > a$，则称 $b = \lfloor a \rfloor$
- $a, b \in \mathbb{Z}$，定义 $a \bmod b = a - \lfloor \frac{a}{b} \rfloor * b$
- $a, b \in \mathbb{N}*$，若 $b \bmod a = 0$，则称 a 整除 b，记为 $a|b$，并称 a 为 b 的约数，b 为 a 的倍数。
- $a, b \in \mathbb{N}*$，最大的 $n(n \in \mathbb{N}*)$ 使得 $n|a$，$n|b$，则称 n 为 a 与 b 的最大公约数，记为 $n = gcd(a, b)$
- $a, b \in \mathbb{N}*$，最小的 $n(n \in \mathbb{N}*)$ 使得 $a|n$，$b|n$，则称 n 为 a 与 b 的最小公倍数，记为 $n = lcm(a, b)$
- $a, b \in \mathbb{N}*$，若 $gcd(a, b) = 1$，则称 a, b 互素，记为 $a \perp b$

1 概述
- 符号与约定
- 同余与模运算
- 素数

2 数论定理

3 数论算法

- 设 $a, b \in \mathbb{Z}$，若 $a \bmod c = b \bmod c$，则称 a 与 b 同余，记为 $a \equiv b \pmod c$

- 设 $a, b \in \mathbb{Z}$，若 $a \bmod c = b \bmod c$，则称 a 与 b 同余，记为 $a \equiv b \pmod{c}$
- 自然数域下的模运算的性质有：

- 设 $a, b \in \mathbb{Z}$，若 $a \bmod c = b \bmod c$，则称 a 与 b 同余，记为 $a \equiv b \pmod{c}$
- 自然数域下的模运算的性质有：
  - $(a \bmod c) + (b \bmod c) \bmod c = (a + b) \bmod c$

- 设 $a, b \in \mathbb{Z}$，若 $a \bmod c = b \bmod c$，则称 a 与 b 同余，记为 $a \equiv b \pmod{c}$
- 自然数域下的模运算的性质有：
  - $(a \bmod c) + (b \bmod c) \bmod c = (a + b) \bmod c$
  - $(a \bmod c)(b \bmod c) \bmod c = (ab) \bmod c$

- 设 $a, b \in \mathbb{Z}$，若 $a \bmod c = b \bmod c$，则称 a 与 b 同余，记为 $a \equiv b \pmod{c}$
- 自然数域下的模运算的性质有：
  - $(a \bmod c) + (b \bmod c) \bmod c = (a + b) \bmod c$
  - $(a \bmod c)(b \bmod c) \bmod c = (ab) \bmod c$
  - $(a \bmod c)^b \bmod c = a^b \bmod c$

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod{c}$，则 $a - b \equiv 0 \pmod{c}$

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod{c}$，则 $a - b \equiv 0 \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a + n \equiv b + n \pmod{c}$

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod{c}$，则 $a - b \equiv 0 \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a + n \equiv b + n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a - n \equiv b - n \pmod{c}$

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod{c}$，则 $a - b \equiv 0 \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a + n \equiv b + n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a - n \equiv b - n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a \times n \equiv b \times n \pmod{c}$

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod c$，则 $a - b \equiv 0 \pmod c$
- 若 $a \equiv b \pmod c$，则 $a + n \equiv b + n \pmod c$
- 若 $a \equiv b \pmod c$，则 $a - n \equiv b - n \pmod c$
- 若 $a \equiv b \pmod c$，则 $a \times n \equiv b \times n \pmod c$
- 若 $a \equiv b \pmod c$，则 $a^n \equiv b^n \pmod c$（$n \in \mathbb{N}*$）

- 由此，我们可以得到同余的性质。设 $c \in \mathbb{N}*$，$n \in \mathbb{Z}$:
- 若 $a \equiv b \pmod{c}$，则 $a - b \equiv 0 \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a + n \equiv b + n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a - n \equiv b - n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a \times n \equiv b \times n \pmod{c}$
- 若 $a \equiv b \pmod{c}$，则 $a^n \equiv b^n \pmod{c}$（$n \in \mathbb{N}*$）
- $a + nc \equiv a \pmod{c}$

- 同时我们可以定义模意义下的运算。

- 同时我们可以定义模意义下的运算。
- 对于模 m 意义下的运算，任意 $n \in \mathbb{N}$，可以找到 $n' \in [0, m)$ 使得 $n \equiv n' \pmod{m}$。

- 同时我们可以定义模意义下的运算。
- 对于模 m 意义下的运算，任意 $n \in \mathbb{N}$，可以找到 $n' \in [0, m)$ 使得 $n \equiv n' \pmod{m}$。
- 传统的加法、减法、乘法，仍然具有封闭性，结合律，分配律，“1 元素”，“0 元素”等性质。

- 同时我们可以定义模意义下的运算。
- 对于模 m 意义下的运算，任意 $n \in \mathbb{N}$，可以找到 $n' \in [0, m)$ 使得 $n \equiv n' \pmod{m}$。
- 传统的加法、减法、乘法，仍然具有封闭性，结合律，分配律，“1 元素”，“0 元素”等性质。
- 若 $ac = bc$，则当 $gcd(c, m) = 1$ 时，$a = b$

- 对于 $n \in \mathbb{N}*$，一个整数集中的数模 n 所得的余数域，称为剩余系。

- 对于 $n \in \mathbb{N}*$，一个整数集中的数模 n 所得的余数域，称为剩余系。
- 设 $m \in \mathbb{N}*$，若 $r_0, r_1, \cdots, r_{m-1}$ 为 m 个整数，并且两两模 m 不同余，则 $r_0, r_1, \cdots, r_{m-1}$ 叫作模 m 的一个完全剩余系。

- 对于 $n \in \mathbb{N}*$，一个整数集中的数模 n 所得的余数域，称为剩余系。
- 设 $m \in \mathbb{N}*$，若 $r_0, r_1, \cdots, r_{m-1}$ 为 m 个整数，并且两两模 m 不同余，则 $r_0, r_1, \cdots, r_{m-1}$ 叫作模 m 的一个完全剩余系。
- 设 $m \in \mathbb{N}*$，以 $C_r(r = 0, 1, \cdots, m-1)$ 表示所有形如 $km + r(k \in \mathbb{Z}$ 的整数组成的集合，则 $C_0, C_1, \cdots, C_{m-1}$ 称为 m 的剩余类。

- 对于 $n \in \mathbb{N}*$，一个整数集中的数模 n 所得的余数域，称为剩余系。
- 设 $m \in \mathbb{N}*$，若 $r_0, r_1, \cdots, r_{m-1}$ 为 m 个整数，并且两两模 m 不同余，则 $r_0, r_1, \cdots, r_{m-1}$ 叫作模 m 的一个完全剩余系。
- 设 $m \in \mathbb{N}*$，以 $C_r(r = 0, 1, \cdots, m-1)$ 表示所有形如 $km + r(k \in \mathbb{Z}$ 的整数组成的集合，则 $C_0, C_1, \cdots, C_{m-1}$ 称为 m 的剩余类。
- m 个剩余类每个取一个代表元，即为完全剩余系。

- 对于 $n \in \mathbb{N}*$，一个整数集中的数模 n 所得的余数域，称为剩余系。
- 设 $m \in \mathbb{N}*$，若 $r_0, r_1, \cdots, r_{m-1}$ 为 m 个整数，并且两两模 m 不同余，则 $r_0, r_1, \cdots, r_{m-1}$ 叫作模 m 的一个完全剩余系。
- 设 $m \in \mathbb{N}*$，以 $C_r(r = 0, 1, \cdots, m-1)$ 表示所有形如 $km + r(k \in \mathbb{Z}$ 的整数组成的集合，则 $C_0, C_1, \cdots, C_{m-1}$ 称为 m 的剩余类。
- m 个剩余类每个取一个代表元，即为完全剩余系。
- 与 m 互素的各个等价类中取一个代表元，称为缩系。$\varphi(m)$ 表示这样的数的个数，称为 *Euler* 函数。

1 概述
- 符号与约定
- 同余与模运算
- 素数

2 数论定理

3 数论算法

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。
- Euler 函数 $\varphi(n)$ 基本性质：

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。
- *Euler* 函数 $\varphi(n)$ 基本性质：
  - $\varphi(n) = n\prod(1-\frac{1}{p_i})$

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。
- *Euler* 函数 $\varphi(n)$ 基本性质：
  - $\varphi(n) = n\prod(1 - \frac{1}{p_i})$
  - 若 $m \perp n$，则 $\varphi(mn) = \varphi(m)\varphi(n)$

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。
- *Euler* 函数 $\varphi(n)$ 基本性质：
  - $\varphi(n) = n\prod(1 - \frac{1}{p_i})$
  - 若 $m \perp n$，则 $\varphi(mn) = \varphi(m)\varphi(n)$
  - 若 $p|n$，则 $\varphi(pn) = p\varphi(n)$

- 当一个数 $n(n \in \mathbb{Z}\ n > 1)$ 的约数只有 2 个（1 和他本身）时，称之为素数/质数。当一个数的约数大于 2 个时，称之为合数。
- *Euler* 函数 $\varphi(n)$ 基本性质：
  - $\varphi(n) = n\prod(1 - \frac{1}{p_i})$
  - 若 $m \perp n$，则 $\varphi(mn) = \varphi(m)\varphi(n)$
  - 若 $p|n$，则 $\varphi(pn) = p\varphi(n)$
  - 若 $p \in \mathbb{P}$，则 $\varphi(p) = p - 1$

1 概述

2 数论定理

- 算术基本定理
- 费马小定理、欧拉定理与威尔逊定理
- 中国剩余定理

3 数论算法

1. 概述
2. **数论定理**
   - **算术基本定理**
   - 费马小定理、欧拉定理与威尔逊定理
   - 中国剩余定理
3. 数论算法

- 算术基本定理（唯一分解定理）：

约数个数的上界

$n \le$	10^1	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$\max\{\omega(n)\}$	2	3	4	5	6	7	8	8	9
$\max\{d(n)\}$	4	12	32	64	128	240	448	768	1344
$n \le$	10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}	10^{16}	10^{17}	10^{18}
$\max\{\omega(n)\}$	10	10	11	12	12	13	13	14	15
$\max\{d(n)\}$	2304	4032	6720	10752	17280	26880	41472	64512	103680

- 算术基本定理（唯一分解定理）:
  - 任意大于 1 的自然数都可以唯一地写为若干素数的积的形式（从小到大）

约数个数的上界

$n \le$	10^1	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$\max\{\omega(n)\}$	2	3	4	5	6	7	8	8	9
$\max\{d(n)\}$	4	12	32	64	128	240	448	768	1344
$n \le$	10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}	10^{16}	10^{17}	10^{18}
$\max\{\omega(n)\}$	10	10	11	12	12	13	13	14	15
$\max\{d(n)\}$	2304	4032	6720	10752	17280	26880	41472	64512	103680

1 概述

2 数论定理
- 算术基本定理
- 费马小定理、欧拉定理与威尔逊定理
- 中国剩余定理

3 数论算法

- 费马小定理:

- 费马小定理：
  - $p \in \mathbb{P}$，$a \in \mathbb{N}*$，$p \nmid a$，则 $a^{p-1} \equiv 1 \pmod p$

- 费马小定理：
  - $p \in \mathbb{P}$，$a \in \mathbb{N}*$，$p \nmid a$，则 $a^{p-1} \equiv 1 \pmod p$
- 欧拉定理：

- 费马小定理：
  - $p \in \mathbb{P}$，$a \in \mathbb{N}*$，$p \nmid a$，则 $a^{p-1} \equiv 1 \pmod p$
- 欧拉定理：
  - $p, a \in \mathbb{N}*$，$p \perp a$，则 $a^{\varphi(p)} \equiv 1 \pmod p$

- 费马小定理：
  - $p \in \mathbb{P}$，$a \in \mathbb{N}*$，$p \nmid a$，则 $a^{p-1} \equiv 1 \pmod p$
- 欧拉定理：
  - $p, a \in \mathbb{N}*$，$p \perp a$，则 $a^{\varphi(p)} \equiv 1 \pmod p$
- 威尔逊定理：

- 费马小定理：
  - $p \in \mathbb{P}$，$a \in \mathbb{N}*$，$p \nmid a$，则 $a^{p-1} \equiv 1 \pmod p$
- 欧拉定理：
  - $p, a \in \mathbb{N}*$，$p \perp a$，则 $a^{\varphi(p)} \equiv 1 \pmod p$
- 威尔逊定理：
  - $p \in \mathbb{P}$ 等价于 $(p-1)! \equiv -1 \pmod p$，否则余数为 0，$p = 4$ 时例外。

1 概述

2 数论定理
- 算术基本定理
- 费马小定理、欧拉定理与威尔逊定理
- 中国剩余定理

3 数论算法

- 对于线性同余方程组 $x \equiv a_i \pmod{m_i}$ 且 m_i 两两互质，无论 a_i 取值如何一定有解。

- 对于线性同余方程组 $x \equiv a_i \pmod{m_i}$ 且 m_i 两两互质，无论 a_i 取值如何一定有解。
- $x \equiv \sum a_i m_i m_i^{-1} \pmod{M} (M = \prod m_i)$

- 对于线性同余方程组 $x \equiv a_i \pmod{m_i}$ 且 m_i 两两互质，无论 a_i 取值如何一定有解。
- $x \equiv \sum a_i m_i m_i^{-1} \pmod{M} (M = \prod m_i)$
- 扩展中国剩余定理：https://blog.csdn.net/clove_unique/article/details/54571216

- 设 $a > b$， $d = gcd(a, b)$， 则 $d|a$， $d|b$， 故 $d|a - b$

- 设 $a > b$， $d = gcd(a, b)$，则 $d|a$，$d|b$，故 $d|a - b$
- 由此得到辗转相减法：每次将大的数减去小的数，直到一个数为 0，此时另一个数即为 gcd

- 设 $a > b$， $d = gcd(a, b)$，则 $d|a$，$d|b$，故 $d|a - b$
- 由此得到辗转相减法：每次将大的数减去小的数，直到一个数为 0，此时另一个数即为 gcd
- 令 $d = gcd(a, b)$，则 $d|(a \bmod b)$

- 设 $a > b$， $d = gcd(a, b)$，则 $d|a$，$d|b$，故 $d|a-b$
- 由此得到辗转相减法：每次将大的数减去小的数，直到一个数为 0，此时另一个数即为 gcd
- 令 $d = gcd(a, b)$，则 $d|(a \bmod b)$
- 由此得到辗转相除法：每次将大的数对小的数取模，直到一个数为 0，此时另一个数即为 gcd

- 设 $a > b$， $d = gcd(a, b)$， 则 $d|a$， $d|b$， 故 $d|a - b$
- 由此得到辗转相减法：每次将大的数减去小的数，直到一个数为 0，此时另一个数即为 gcd
- 令 $d = gcd(a, b)$， 则 $d|(a \bmod b)$
- 由此得到辗转相除法：每次将大的数对小的数取模，直到一个数为 0，此时另一个数即为 gcd
- 每次大的数至少缩小一半，故复杂度为 $\log(\max(a, b))$

1. 概述
2. 数论定理
3. 数论算法
   - 辗转相减与辗转相除
   - 扩展欧几里得算法
   - BSGS 算法
   - Eratosthenes 筛法与线性筛法
   - 递推求逆元

- 裴蜀定理：$a, b \in \mathbb{Z}$，存在无穷多组整数对 (x, y) 满足不定方程 $ax + by = d$，其中 $d = gcd(a, b)$

- 裴蜀定理：$a, b \in \mathbb{Z}$，存在无穷多组整数对 (x, y) 满足不定方程 $ax + by = d$，其中 $d = gcd(a, b)$
- 在求 $gcd(a, b)$ 的同时，可以求出上述方程的一组整数解。

- 裴蜀定理：$a, b \in \mathbb{Z}$，存在无穷多组整数对 (x, y) 满足不定方程 $ax + by = d$，其中 $d = gcd(a, b)$
- 在求 $gcd(a, b)$ 的同时，可以求出上述方程的一组整数解。
- 递归计算：假设已经求出 $(b \bmod a, a)$ 的一组解 (x_0, y_0)，满足 $(b \bmod a)x_0 + ay_0 = d$

- 裴蜀定理：$a, b \in \mathbb{Z}$，存在无穷多组整数对 (x, y) 满足不定方程 $ax + by = d$，其中 $d = gcd(a, b)$
- 在求 $gcd(a, b)$ 的同时，可以求出上述方程的一组整数解。
- 递归计算：假设已经求出 $(b \bmod a, a)$ 的一组解 (x_0, y_0)，满足 $(b \bmod a)x_0 + ay_0 = d$
- 可以得到 $(b - a\lfloor \frac{b}{a} \rfloor)x_0 + ay_0 = d$

- 裴蜀定理：$a, b \in \mathbb{Z}$，存在无穷多组整数对 (x, y) 满足不定方程 $ax + by = d$，其中 $d = gcd(a, b)$
- 在求 $gcd(a, b)$ 的同时，可以求出上述方程的一组整数解。
- 递归计算：假设已经求出 $(b \bmod a, a)$ 的一组解 (x_0, y_0)，满足 $(b \bmod a)x_0 + ay_0 = d$
- 可以得到 $(b - a\lfloor \frac{b}{a} \rfloor)x_0 + ay_0 = d$
- 整理得到 $a(y_0 - \lfloor \frac{b}{a} \rfloor x_0) + bx_0 = d$

问题

给定a,b,p，求最小的非负整数x，满足$a^x \equiv b \pmod p$

题解

这就是经典的BSGS算法，方法如下：

令$x = im - j$，$m = \lceil \sqrt{p} \rceil$，则$a^{im-j} \equiv b \pmod p$

移项，得$(a^m)^i \equiv ba^j \pmod p$

首先，从$0 - m$枚举j，将得到的ba^j的值存入hash表；

然后，从$1 - m$枚举i，计算$(a^m)^i$，查表，如果有值与之相等，则当时得到的$im - j$是最小值。

讨论

1、讨论无解的情况？

方程有解的充要条件是p为质数且$(a,p) = 1$

可以发现这是费马小定理的条件，会在问题2中讨论。

2、为什么m取$\lceil \sqrt{p} \rceil$就可以？

我们先考虑枚举的思路：如果要是枚举x的值的话应该何时停止？

首先证明：$a^{k \mod p-1} \equiv a^k \pmod p$

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

$\frac{a^k}{a^{m(p-1)}} \equiv a^k \pmod p$

即使$(a^{p-1})^m \equiv 1 \pmod p$

由费马小定理知当p为质数且$(a,p)=1$时$a^{p-1} \equiv 1 \pmod p$

推出p为质数且$(a,p)=1$这个条件，并证明结论$a^{k \mod p-1} \equiv a^k \pmod p$

即我们得到：枚举x的话枚举到p即可。

所以使$im-j <= p$，即$m=\lceil\sqrt{p}\rceil$，i,j最大值也为m。

3、为什么第一个枚举到的$im-j$是最小值？

首先要明确的一点是，枚举j时算出来的值有可能重复，那么我们在hash表里就要用新的值覆盖原来的值。正确性显而易见，要保证$im-j$最小，就要保证j最大。

为什么枚举到最小的i就是最小值呢？思考每枚举到一个i，im的值实际上是在原来的基础上增加了m，而j的范围是$[0,m]$，也就是说im增加的幅度一定比j增加的幅度大，从而保证了首先枚举到的一定是最小值。

4、为什么从$0-m$枚举j，而从$1-m$枚举i？

i不能为0，否则$im-j$有可能出现负数的情况

EXBSGS

现在考虑 P 不为质数的情况。

设 $d = gcd(A, P)$

如果 $d \nmid B$，唯一可能的解是 $x = 0$，如果 $B = 1$，方程有解。

如果 $d \mid B$ 且 $d = 1$，此时 A 与 P 互质，直接用 BSGS 解即可。

如果 $d \mid B$ 且 $d \neq 1$ 有

$$A^x \equiv B \; (mod \; P)$$
$$A^{x-1} * \frac{A}{d} \equiv \frac{B}{d} \; (mod \; \frac{P}{d})$$

此时 A 与 $\frac{P}{d}$ 可能不互质，继续分解，直到 A 与 $\frac{P}{\prod_{i=1}^{k} d_i}$ 互质。

$$A^{x-k} * \frac{A^k}{\prod_{i=1}^{k} d_i} \equiv \frac{B}{\prod_{i=1}^{k} d_i} \; (mod \; \frac{P}{\prod_{i=1}^{k} d_i})$$

BSGS 算法

如果 $\prod_{i=1}^{k} d_i \nmid B$，则唯一可能的解是 $x = 0$

如果 $\prod_{i=1}^{k} d_i \mid B$，首先我们暴力枚举 $x \in [0, k)$ 是否为解。(很显然 $k \le log_2 B$)

对于 $x \ge k$ 的情况，有：

$$A^{x-k} \equiv B * A^{-k} \; (mod \; \frac{P}{\prod_{i=1}^{k} d_i})$$

然后换元：$x' = x - k, B' = B * A^{-k}, P' = \frac{P}{\prod_{i=1}^{k} d_i}$，得：

$$A^{x'} \equiv B' \; (mod \; P')$$

此时 A 与 P' 互质，套用 BSGS 解方程即可，原方程的解为 $x = x' + k$。

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$
- Eratosthenes 筛法：从 2 到 n，枚举每个素数的倍数（除去自身）并标记为合数

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
    - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$
- Eratosthenes 筛法：从 2 到 n，枚举每个素数的倍数（除去自身）并标记为合数
    - 时间复杂度：$O(n \ln n \ln n)$

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$
- Eratosthenes 筛法：从 2 到 n，枚举每个素数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n \ln n \ln n)$
- Euler 筛法：对于每个素数 p，从小到大枚举它的所有倍数 $i * p (i > 1)$ 并标记为合数，直到 $p|i$

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$
- Eratosthenes 筛法：从 2 到 n，枚举每个素数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n \ln n \ln n)$
- Euler 筛法：对于每个素数 p，从小到大枚举它的所有倍数 $i * p(i > 1)$ 并标记为合数，直到 $p|i$
  - 每一个数只会被它最小的质因子筛到一次

- 朴素素数判定：$\forall n \notin \mathbb{P}$，$\exists y \in (1, \sqrt{n}]$，使得 $y|n$
- 朴素筛法：从 2 到 n，枚举每个数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n + \frac{n}{2} + \cdots + \frac{n}{n})$ $O(n \ln n)$
- Eratosthenes 筛法：从 2 到 n，枚举每个素数的倍数（除去自身）并标记为合数
  - 时间复杂度：$O(n \ln n \ln n)$
- Euler 筛法：对于每个素数 p，从小到大枚举它的所有倍数 $i * p(i > 1)$ 并标记为合数，直到 $p|i$
  - 每一个数只会被它最小的质因子筛到一次
  - 时间复杂度：$O(n)$

1. 概述
2. 数论定理
3. 数论算法
   - 辗转相减与辗转相除
   - 扩展欧几里得算法
   - BSGS 算法
   - Eratosthenes 筛法与线性筛法
   - 递推求逆元

- 若 $ab \equiv 1 \pmod{p}$，则称 b 为 a 在 $\bmod p$ 意义下的乘法逆元，记为 $a^{-1} \equiv b \pmod{p}$

- 若 $ab \equiv 1 \pmod p$，则称 b 为 a 在 $\bmod p$ 意义下的乘法逆元，记为 $a^{-1} \equiv b \pmod p$
- $\frac{a}{b} = a \times b^{-1} \pmod p$

- 若 $ab \equiv 1 \pmod p$，则称 b 为 a 在 $\bmod p$ 意义下的乘法逆元，记为 $a^{-1} \equiv b \pmod p$
- $\frac{a}{b} = a \times b^{-1} \pmod p$
- 由欧拉定理：$a^{\varphi(p)} \equiv a^{-1} \pmod p (a \perp p)$

- 若 $ab \equiv 1 \pmod p$，则称 b 为 a 在 $\bmod p$ 意义下的乘法逆元，记为 $a^{-1} \equiv b \pmod p$
- $\frac{a}{b} = a \times b^{-1} \pmod p$
- 由欧拉定理：$a^{\varphi(p)} \equiv a^{-1} \pmod p (a \perp p)$
- 不互素时考虑用 exgcd 解不定方程