

# 密码数学基础：初等数论篇

刘仁章

北京原语科技有限公司

2023 年 9 月 16 日

# 目录

- 1 整除与同余
- 2 素数与算术基本定理
- 3 最大公因子与欧几里得算法
- 4 线性同余方程与中国剩余定理
- 5 阶与原根

# 目录

- 1 整除与同余
- 2 素数与算术基本定理
- 3 最大公因子与欧几里得算法
- 4 线性同余方程与中国剩余定理
- 5 阶与原根

# 整除关系

如果整数  $a \neq 0, b$  满足“存在整数  $c$ , 使得  $b = ac$ ”, 则称  $a$  整除  $b$ , 或者  $b$  能被  $a$  整除, 记做  $a|b$ 。整除是一种二元关系。

- 自反性 (反身性):  $a|a$ 。
- 反对称性。如果  $a|b$  且  $b|a$ , 那么  $a = \pm b$ 。
- 传递性。如果  $a|b, b|c$ , 那么  $a|c$ 。

整除是一种偏序关系 (集合的包含关系, 小于等于关系等)。

- $1|a, b|0$  对任意的整数  $a$  和  $b \neq 0$  成立。
- 如果  $a|b$  则称  $a$  是  $b$  的一个因子,  $b$  是  $a$  的一个倍数。

# 带余除法

对于整数  $a$  和  $b > 0$ , 存在唯一的整数  $q$  和  $r$  满足  $a = bq + r$  且  $0 \leq r < b$ 。称  $a$  为被除数,  $b$  是除数,  $q$  为商,  $r$  为余数。

- $b|a$  当且仅当  $r = 0$ 。

给定了除数  $b$ , 可以将所有的整数按照除以  $b$  所得到的余数进行划分。这就是我们下面所说的“同余”。

# 同余关系

如果整数  $a$  和  $b$  除以  $m$  后得到的余数相同, 称  $a$  与  $b$  模  $m$  同余, 记做  $a \equiv b \pmod{m}$ 。同余也是一种二元关系。

- 自反性 (反身性):  $a \equiv a \pmod{m}$ 。
- 对称性。如果  $a \equiv b \pmod{m}$ , 那么  $b \equiv a \pmod{m}$ 。
- 传递性。如果  $a \equiv b \pmod{m}$ ,  $b \equiv c \pmod{m}$ , 那么  $a \equiv c \pmod{m}$ 。

同余关系是一种等价关系。于是, 可以将所有的整数按模  $m$  是否同余划分为一些等价类, 即模  $m$  的完全剩余系。

# 模 $m$ 的完全剩余系

令  $m$  为大于 0 的整数。

- $\{0, \dots, m-1\}$  是模  $m$  的最小非负剩余。
- $\{0, \pm 1, \dots, \pm \frac{m-1}{2}\}$  ( $m$  为奇数),  $\{0, \pm 1, \dots, \pm \frac{m-2}{2}, \frac{m}{2}\}$  ( $m$  为偶数) 是模  $m$  的最小绝对剩余。
- 模  $m$  的完全剩余系包含  $m$  个元素, 两两不同余, 从而任意的整数模  $m$  都与完全剩余系中的唯一一个元素同余。

# 目录

- 1 整除与同余
- 2 素数与算术基本定理**
- 3 最大公因子与欧几里得算法
- 4 线性同余方程与中国剩余定理
- 5 阶与原根



# 素数

如果正整数  $p$  有且仅有 1 和它本身两个（正）因子，则称  $p$  是素数。

- 素数是数论的重要研究对象。
- 如果一个正整数有多于两个（正）因子，则称其为合数。
- 2 是唯一的偶素数，1 既不是素数也不是合数。
- 任何大于 1 的整数都有素因子。
- 素数有无穷个。

# 素数

素数有无穷多个。

- 假定素数只有有限多个，设为  $p_1, \dots, p_k$ 。
- 考虑  $Q = p_1 \cdots p_k + 1$ 。
- $p_i \nmid Q$ 。
- $Q$  有异于  $p_1, \dots, p_k$  的素因子。
- 矛盾。于是素数有无穷个。

# 一些特殊的数

Dirichlet 证明了, 对于互素的正整数  $a, b$ ,  $an + b$  包含无穷多个素数。  
有没有只生成素数的表达式?

- 费马数:  $F_n = 2^{2^n} + 1$ 。

- ▶ 如果考虑形如  $2^N + 1$  的素数, 可以推出  $N = 2^n$ : 如果  $N$  是奇素数, 那么 3 是  $2^N + 1$  的真因子。如果  $N$  包含奇因子  $1 < l < N$ , 那么  $(2^l + 1) | (2^N + 1)$ 。
- ▶  $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$  都是素数。费马猜测,  $F_n$  都是素数。然而, 欧拉证明了  $641 | F_5$ 。实际上目前已知的费马素数只有  $F_0 \sim F_4$ , 不知道是否有无穷多个费马素数, 也不知道  $F_n (n > 4)$  是否都是合数。
- ▶ 费马素数与尺规作图问题紧密相关。正  $N$  边形可尺规作图当且仅当  $N$  可以写成 2 的任意幂次与任意多不同费马素数的乘积形式。

# 一些特殊的数

梅森数： $M_p = 2^p - 1$ ， $p$  为素数。

- 如果考虑形如  $2^N - 1$  的素数，可以推出  $N$  必须为素数：如果  $N$  包含素因子  $2 \leq l < N$ ，那么  $(2^l - 1) | (2^N - 1)$ 。
- 梅森数有一种高效的素性判定算法，称为“Lucas-Lehmer 判定法”。
- 通过梅森数找大素数（《2017 年最大的素数》， $M_{77232917}$ ）。目前还不知道是否存在无穷多个梅森素数。
- 梅森素数与偶完全数一一对应。
- 梅森素数可以用来做优化。如 ZUC 中就使用  $M_{31}$ 。
- $p = h2^u \pm f$ ， $h$  和  $f$  都很小。

# 算术基本定理

任何大于 1 的正整数都可以分解为素数幂的乘积。在不考虑顺序的情形下，该分解是唯一的：

$$n = p_1^{e_1} \cdots p_k^{e_k}, p_i \text{ 为素数}, e_i > 0$$

- 对任意的  $n$ ，要完全分解是困难的。
- 对于**随机**的  $n$ ，找到一个素因子相对是容易的 (如约 50% 的概率  $n$  是偶数，约 1/3 的概率  $n$  是 3 的倍数)。
- 随机选一个很大的整数，有大素因子的概率也是比较高的。

# 目录

- 1 整除与同余
- 2 素数与算术基本定理
- 3 最大公因子与欧几里得算法**
- 4 线性同余方程与中国剩余定理
- 5 阶与原根

# 最大公因子

两个不同时为 0 的整数  $a, b$  的最大公因子是同时整除  $a, b$  的最大整数, 记做  $(a, b)$ 。规定  $(0, 0) = 0$ 。

- 如果  $(a, b) = 1$ , 则称  $a, b$  互素。
- 对于负数, 定义  $(a, b) = (|a|, |b|)$ 。
- $(0, a) = |a|$ 。

# 最大公因子

- 如果  $(a, b) = d$ , 则  $(a/d, b/d) = 1$ 。
- $(a, b) = (a + bc, b)$ 。
- $(a, b) = \min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$ 。
- Bezout 定理: 存在整数  $m, n$  使得  $ma + nb = (a, b)$ 。
  - ▶ 如果对  $m, n$  不加限制, 则有无穷多组解  $(m_0 + kb, n_0 - ka), k = 0, 1, \dots$ 。
  - ▶ 怎么求  $m_0, n_0, (a, b)$ ?



# 欧几里得算法

对于  $a \geq b > 0$ ,

- $r_0 = a, r_1 = b$ 。
- $r_j = q_{j+1}r_{j+1} + r_{j+2}, 0 < r_{j+2} < r_{j+1}, j = 0, \dots$ 。
- $r_{n+1} = 0$ 。
- 则  $r_n = (a, b)$ 。

欧几里得算法又叫辗转相除法，是第一个有记录的算法。

# 欧几里得算法

很多时候，需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法

# 欧几里得算法

很多时候，需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心：计算  $s_j, t_j$ ，满足  $s_j a + t_j b = r_j$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。
- $r_j = q_{j+1}r_{j+1} + r_{j+2} \Rightarrow r_j - q_{j+1}r_{j+1} = r_{j+2}$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。
- $r_j = q_{j+1} r_{j+1} + r_{j+2} \Rightarrow r_j - q_{j+1} r_{j+1} = r_{j+2}$ 。
- $(s_j a + t_j b) - q_{j+1}(s_{j+1} a + t_{j+1} b) = r_{j+2}$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。
- $r_j = q_{j+1}r_{j+1} + r_{j+2} \Rightarrow r_j - q_{j+1}r_{j+1} = r_{j+2}$ 。
- $(s_j a + t_j b) - q_{j+1}(s_{j+1} a + t_{j+1} b) = r_{j+2}$ 。
- $(s_j - q_{j+1}s_{j+1})a + (t_j - q_{j+1}t_{j+1})b = r_{j+2}$ 。



# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。
- $r_j = q_{j+1}r_{j+1} + r_{j+2} \Rightarrow r_j - q_{j+1}r_{j+1} = r_{j+2}$ 。
- $(s_j a + t_j b) - q_{j+1}(s_{j+1} a + t_{j+1} b) = r_{j+2}$ 。
- $(s_j - q_{j+1}s_{j+1})a + (t_j - q_{j+1}t_{j+1})b = r_{j+2}$ 。
- $s_{j+2} = s_j - q_{j+1}s_{j+1}, t_{j+2} = t_j - q_{j+1}t_{j+1}$ 。

# 欧几里得算法

很多时候, 需要求出  $m, n, (a, b)$  使得  $ma + nb = (a, b)$ 。

- 扩展欧几里得算法
- 核心: 计算  $s_j, t_j$ , 满足  $s_j a + t_j b = r_j$ 。
- $a = r_0, s_0 = 1, t_0 = 0$ 。
- $b = r_1, s_1 = 0, t_1 = 1$ 。
- $r_j = q_{j+1} r_{j+1} + r_{j+2}$ 。
- 
- 
- $s_{j+2} = s_j - q_{j+1} s_{j+1}, t_{j+2} = t_j - q_{j+1} t_{j+1}$ 。

# 目录

- 1 整除与同余
- 2 素数与算术基本定理
- 3 最大公因子与欧几里得算法
- 4 线性同余方程与中国剩余定理
- 5 阶与原根

# 整除和同余的一些性质

- 如果  $a|b, c|d$ , 那么  $ac|bd$ 。
- 如果  $a|bc$  且  $(a, b) = 1$ , 那么  $a|c$ 。
- 如果  $a \equiv b \pmod{m}, c \equiv d \pmod{m}$ , 那么  $a + c \equiv b + d \pmod{m}$ 。
- 如果  $a \equiv b \pmod{m}, d|m$ , 那么  $a \equiv b \pmod{d}$ 。
- 如果  $a \equiv b \pmod{m}$ , 那么  $ac \equiv bc \pmod{mc}$ , 从而  $ac \equiv bc \pmod{m}$ 。
- 如果  $ac \equiv bc \pmod{m}$ , 那么  $a \equiv b \pmod{\frac{m}{(c, m)}}$ 。当  $(c, m) = 1$  时, 消去律才成立。
- 如果  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}$ , 那么  $a \equiv b \pmod{\frac{m_1 m_2}{(m_1, m_2)}}$ , 实际上  $\frac{m_1 m_2}{(m_1, m_2)}$  就是  $m_1, m_2$  的最小公倍数。
- 同余性质的证明很多时候可以通过定义进行:

$$a \equiv b \pmod{m} \iff m|(a - b) \iff a = b + mk, k \in \mathbb{Z}$$

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。
- $\frac{a}{(a, m)}x + \frac{m}{(a, m)}y = \frac{b}{(a, m)}$ , 其中  $(\frac{a}{(a, m)}, \frac{m}{(a, m)}) = 1$ 。



# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。
- $ax_0 + my_0 = 1$ ,  $ax + my = 0$ 。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。
- $ax_0 + my_0 = 1$ ,  $ax + my = 0$ 。
- $a(bx_0) + m(by_0) = b$ ,  $a(m) + m(-a) = 0$ 。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。
- $ax_0 + my_0 = 1, ax + my = 0$ 。
- $a(bx_0) + m(by_0) = b, a(m) + m(-a) = 0$ 。
- 从而  $(bx_0 + mk, by_0 - ak), k \in \mathbb{Z}$ 。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = 1$ 。
- $\frac{a}{(a, m)}x + \frac{m}{(a, m)}y = \frac{b}{(a, m)}$ , 其中  $(\frac{a}{(a, m)}, \frac{m}{(a, m)}) = 1$ 。
- $ax_0 + my_0 = 1$ ,  $ax + my = 0$ 。
- $a(bx_0) + m(by_0) = b$ ,  $a(m) + m(-a) = 0$ 。
- 从而  $(bx_0 + mk, by_0 - ak), k \in \mathbb{Z}$ 。

# 丢番图方程

对于整数  $a, b, m$ , 考虑方程  $ax + my = b$  的整数解。

- 当且仅当  $(a, m) | b$  时, 方程有整数解。
- 不失一般性, 考虑  $ax + my = b$  的整数解, 其中  $(a, m) = d$ 。
- $\frac{a}{(a, m)}x + \frac{m}{(a, m)}y = \frac{b}{(a, m)}$ , 其中  $(\frac{a}{(a, m)}, \frac{m}{(a, m)}) = 1$ 。
- $ax_0 + my_0 = d$ ,  $ax + my = 0$ 。
- $a((b/d)x_0) + m((b/d)y_0) = b/d$ ,  $a(m/d) + m(-a/d) = 0$ 。
- 从而  $((b/d)x_0 + (m/d)k, (b/d)y_0 - (a/d)k), k \in \mathbb{Z}$ 。

# 线性同余方程

注意上面的丢番图方程中有:  $x_0(\frac{a}{d}) + y_0(\frac{m}{d}) = 1$ ,  $x = \frac{b}{d}x_0 + \frac{m}{d}k$ 。

线性同余方程  $ax \equiv b \pmod{m}$  可以转化为上面的丢番图方程。

- 令  $d = (a, m)$ 。则当且仅当  $d|b$  时, 线性同余方程有解, 且其解为  $x \equiv \frac{b}{d}(\frac{a}{d})^{-1} \pmod{\frac{m}{d}}$ 。(如果还写成模  $m$  的解呢?)
- 当  $d = (a, m) = 1$  时, 即大家熟知的  $x \equiv ba^{-1} \pmod{m}$ 。

# 中国剩余定理

- 物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？
- 三人同行七十稀，五树梅花廿一枝，七子团圆正半月，除百零五便得知。
- 孙子定理，秦九韶定理（《数书九章》大衍术），中国剩余定理

# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$



# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$

- 根据  $x \bmod 3 = 2$  得到  $x = 3k + 2, k \in \mathbb{Z}$ 。

# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$

- 根据  $x \bmod 3 = 2$  得到  $x = 3k + 2, k \in \mathbb{Z}$ 。
- 代入  $x \bmod 5 = 3$  得到  $3k \bmod 5 = 1$ , 于是  $k \bmod 5 = 2$ 。

# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$

- 根据  $x \bmod 3 = 2$  得到  $x = 3k + 2, k \in \mathbb{Z}$ 。
- 代入  $x \bmod 5 = 3$  得到  $3k \bmod 5 = 1$ , 于是  $k \bmod 5 = 2$ 。
- $k = 5m + 2, m \in \mathbb{Z}, x = 15m + 8$ 。

# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$

- 根据  $x \bmod 3 = 2$  得到  $x = 3k + 2, k \in \mathbb{Z}$ 。
- 代入  $x \bmod 5 = 3$  得到  $3k \bmod 5 = 1$ , 于是  $k \bmod 5 = 2$ 。
- $k = 5m + 2, m \in \mathbb{Z}, x = 15m + 8$ 。
- 代入  $x \bmod 7 = 2$  得到  $m \bmod 7 = 1$ 。

# 中国剩余定理

假设为  $x$ , 则问题为  $x \bmod 3 = 2, x \bmod 5 = 3, x \bmod 7 = 2$

- 根据  $x \bmod 3 = 2$  得到  $x = 3k + 2, k \in \mathbb{Z}$ 。
- 代入  $x \bmod 5 = 3$  得到  $3k \bmod 5 = 1$ , 于是  $k \bmod 5 = 2$ 。
- $k = 5m + 2, m \in \mathbb{Z}, x = 15m + 8$ 。
- 代入  $x \bmod 7 = 2$  得到  $m \bmod 7 = 1$ 。
- $m = 7n + 1, n \in \mathbb{Z}, x = 105n + 23, n \in \mathbb{Z}$ 。

# 中国剩余定理

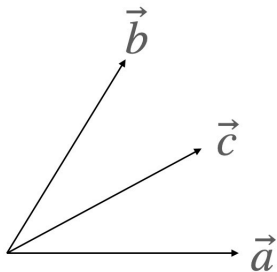
令  $m_1, \dots, m_r$  为两两互素的整数。则同余方程组

$$x \equiv a_i \pmod{m_i} (1 \leq i \leq r)$$

在模  $M = m_1 \cdots m_r$  意义下有唯一解。

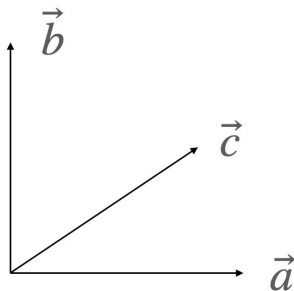
- 令  $M_i = \frac{M}{m_i}$ ,  $u_i \equiv M_i^{-1} \pmod{m_i}$ , 则  $x \equiv a_1(u_1 M_1) + \cdots + a_r(u_r M_r) \pmod{M}$ 。
- 前例中,  $u_1 M_1 = 70$ ,  $u_2 M_2 = 21$ ,  $u_3 M_3 = 15$ ,  $M = 105$ 。

# 向量在一组基下的表示



$$\vec{c} = x\vec{a} + y\vec{b}?$$

# 向量在一组基下的表示



$$\vec{c} = \frac{\langle \vec{c}, \vec{a} \rangle}{\langle \vec{a}, \vec{a} \rangle} \vec{a} + \frac{\langle \vec{c}, \vec{b} \rangle}{\langle \vec{b}, \vec{b} \rangle} \vec{b}$$



# 中国剩余定理

将整数  $x$  表示为向量

$$(x \bmod m_1, \dots, x \bmod m_r) = (a_1, a_2, \dots, a_r)$$

关键找到一组“标准正交”基。

- 如果知道了  $\vec{e}_i = (0, \dots, 0, 1, 0, \dots)$  对应的整数，那么根据  $(a_1, \dots, a_r) = a_1 \vec{e}_1 + \dots + a_r \vec{e}_r$ ，很容易求出  $x$ 。

# 中国剩余定理

实际上  $\vec{e}_i$  对应的整数就是  $u_i M_i \bmod M$ 。

- $\vec{e}_i = (0, \dots, 0, 1, 0, \dots)$  对应的整数  $U_i$  能被其他  $r-1$  个模整除, 从而也可以被它们的最小公倍数整除。
- 若干个两两互素的整数, 其最小公倍数就是它们的乘积。于是  $U_i \equiv 0 \bmod M_i$ , 假定  $U_i = kM_i, k \in \mathbb{Z}$ 。
- 根据  $U_i \bmod m_i = 1$ , 知道  $kM_i \equiv 1 \bmod m_i$ , 于是  $k \equiv u_i \bmod m_i$ 。

# 中国剩余定理

- “正交”？独立性！
- 如果  $m_i$  不互素，会怎么样？
- 可能无解。
- 当有解的时候，在模  $m_1 \cdots m_r$  的意义下有多个解。但是在模  $(m_1, \cdots, m_r)$ （最小公倍数）意义下是唯一的。

# 中国剩余定理

如果  $m_i$  不互素，如何计算？

- $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$  有解当且仅当  $(m_1, m_2) | (a_1 - a_2)$ 。
- 当方程组有解时候，解在模  $[m_1, m_2]$ （最小公倍数）意义下是唯一的。
- 将  $x = a_1 + k_1 m$  代入到第二个式子中，用前述的解线性同余方程的方式求解。
- 课后习题中还给出了两个算法，有兴趣的可以了解一下。

高次同余方程的求解，将放在后面的内容中介绍。

# 一些特殊的同余式

- Fermat 小定理：对素数  $p$  和任意不被  $p$  整除的  $a$ ,  $a^{p-1} \equiv 1 \pmod p$  成立。
- 欧拉定理：  $a^{\varphi(m)} \equiv 1 \pmod m$ , 其中  $(a, m) = 1$ ,  $\varphi(m)$  (欧拉 phi 函数, 欧拉 totient 函数) 是指  $\{1, 2, \dots, m-1\}$  中与  $m$  互素的元素个数 (实际上也就是模  $m$  可逆的元素个数)。
- Wilson 定理：若  $p$  是素数,  $(p-1)! \equiv -1 \pmod p$ 。其逆命题也成立。

# 欧拉函数 $\varphi(m)$

- 积（乘）性函数：  $(m, n) = 1$ ,  $\varphi(mn) = \varphi(m)\varphi(n)$ 。
- 如果  $n = p_1^{a_1} \cdots p_r^{a_r}$ ,  
 $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_r^{a_r}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$ 。
- $\sum_{d|n} \varphi(d) = n$ 。

# 目录

- 1 整除与同余
- 2 素数与算术基本定理
- 3 最大公因子与欧几里得算法
- 4 线性同余方程与中国剩余定理
- 5 阶与原根

- 对于  $(a, n) = 1$ ,  $a$  模  $n$  的阶是满足  $a^k \equiv 1 \pmod{n}$  的最小正整数  $k$ , 记做  $\text{ord}_n(a)$ 。当  $(a, n) \neq 1$  时, 不存在整数  $k$ , 使得  $a^k \equiv 1 \pmod{n}$ 。
- 因此, 这里考虑的是与  $n$  互素的那些剩余类, 也称模  $n$  的一个约化剩余系, 其中包含  $\varphi(n)$  个元素, 常常记做  $\mathbb{Z}_n^*$ 。
- 由欧拉定理:  $a^{\varphi(n)} \equiv 1 \pmod{n}$ ,  $(a, n) = 1$ ,  $\text{ord}_n(a) | \varphi(n)$ 。即  $a$  的阶是  $\varphi(n)$  的一个因子。
- $a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{\text{ord}_n(a)}$ 。



# 原根

$a$  的阶是  $\varphi(n)$  的一个因子。如果  $\text{ord}_n(a) = \varphi(n)$ ，则称  $a$  是模  $n$  的一个（本）原根。换句话说，当模  $n$  的约化剩余系可以由一个元素通过乘法生成时候（乘法循环群），原根就是这个生成元。

- $(r, n) = 1$ ， $r$  是模  $n$  的一个原根，当且仅当  $r, \dots, r^{\varphi(n)}$  形成模  $n$  的一个约化剩余系。
- $\text{ord}_n(a^t) = \frac{\text{ord}_n(a)}{(t, \text{ord}_n(a))}$ 。
- $r$  是模  $n$  的原根，即  $\text{ord}_n(r) = \varphi(n)$ 。那么  $r^u$  也是原根，当且仅当  $(u, \varphi(n)) = 1$ 。于是，如果模  $n$  有原根  $r$ ，那么模  $n$  有  $\varphi(\varphi(n))$  个不同的原根。

# 原根

哪些模  $n$  有原根？

- 模  $n$  有原根当且仅当  $n = 2, 4, p^t, 2p^t$ ，其中  $p$  是奇素数。

# 原根

哪些模  $n$  有原根？

- 模  $n$  有原根当且仅当  $n = 2, 4, p^t, 2p^t$ ，其中  $p$  是奇素数。
- 对上述的  $n$ ，其分解是明显的。如果知道  $\varphi(n)$  的分解，则原根的判定是简单的。

# 原根

哪些模  $n$  有原根？

- 模  $n$  有原根当且仅当  $n = 2, 4, p^t, 2p^t$ ，其中  $p$  是奇素数。
- 对上述的  $n$ ，其分解是明显的。如果知道  $\varphi(n)$  的分解，则原根的判定是简单的。
- 对  $n = p^t, 2p^t$ ， $r$  是模  $n$  的原根当且仅当对任意的素数  $q | \varphi(n)$ ， $r^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$ 。

# 原根

哪些模  $n$  有原根？

- 模  $n$  有原根当且仅当  $n = 2, 4, p^t, 2p^t$ ，其中  $p$  是奇素数。
- 对上述的  $n$ ，其分解是明显的。如果知道  $\varphi(n)$  的分解，则原根的判定是简单的。
- 对  $n = p^t, 2p^t$ ， $r$  是模  $n$  的原根当且仅当对任意的素数  $q| \varphi(n)$ ， $r^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$ 。
- 1 和 3 分别是模 2 和 4 的原根。

# 原根

- 如果  $r$  是模奇素数  $p$  的原根, 那么  $r$  或  $r + p$  中必有模  $p^2$  的原根。

# 原根

- 如果  $r$  是模奇素数  $p$  的原根, 那么  $r$  或  $r + p$  中必有模  $p^2$  的原根。
- 如果  $r$  是模  $p^2$  的原根,  $p$  为奇素数, 那么,  $r$  也是模  $p^k$  的原根,  $k \geq 3$ 。

# 原根

- 如果  $r$  是模奇素数  $p$  的原根, 那么  $r$  或  $r + p$  中必有模  $p^2$  的原根。
- 如果  $r$  是模  $p^2$  的原根,  $p$  为奇素数, 那么,  $r$  也是模  $p^k$  的原根,  $k \geq 3$ 。
- 如果  $r$  是模  $p^t$  的原根,  $p$  为奇素数, 那么,  $r + p^t, r$  中为奇数的那个也是模  $2p^t$  的原根。



# 原根

- 如果  $r$  是模奇素数  $p$  的原根, 那么  $r$  或  $r + p$  中必有模  $p^2$  的原根。
- 如果  $r$  是模  $p^2$  的原根,  $p$  为奇素数, 那么,  $r$  也是模  $p^k$  的原根,  $k \geq 3$ 。
- 如果  $r$  是模  $p^t$  的原根,  $p$  为奇素数, 那么,  $r + p^t, r$  中为奇数的那个也是模  $2p^t$  的原根。
- $\mathbb{Z}_{p^t}^*$  是模  $p^t$  的约化剩余系, 由所有小于  $p^t$  且不能被  $p$  整除的正整数组成, 其有原根。后面会证明有限域  $\mathbb{F}_{p^t}$  中也有原根。两者的结构完全不同, 千万不可混淆。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k=3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k=3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .
- 假设结论对  $k_0$  成立, 即  $a^{\varphi(2^{k_0})/2} = a^{2^{k_0-2}} \equiv 1 \pmod{2^{k_0}}$ .

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k=3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .
- 假设结论对  $k_0$  成立, 即  $a^{\varphi(2^{k_0})/2} = a^{2^{k_0-2}} \equiv 1 \pmod{2^{k_0}}$ .
- 令  $a^{2^{k_0-2}} = 1 + d2^{k_0}$ .

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k=3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .
- 假设结论对  $k_0$  成立, 即  $a^{\varphi(2^{k_0})/2} = a^{2^{k_0-2}} \equiv 1 \pmod{2^{k_0}}$ .
- 令  $a^{2^{k_0-2}} = 1 + d2^{k_0}$ .
- 两边平方得到,  $a^{2^{k_0-1}} = 1 + d2^{k_0+1} + d^2 2^{2k_0}$ .

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k = 3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .
- 假设结论对  $k_0$  成立, 即  $a^{\varphi(2^{k_0})/2} = a^{2^{k_0-2}} \equiv 1 \pmod{2^{k_0}}$ .
- 令  $a^{2^{k_0-2}} = 1 + d2^{k_0}$ .
- 两边平方得到,  $a^{2^{k_0-1}} = 1 + d2^{k_0+1} + d^2 2^{2k_0}$ .
- 于是  $a^{\varphi(2^{k_0+1})/2} = a^{2^{k_0-1}} \equiv 1 \pmod{2^{k_0+1}}$ , 即结论对  $k_0 + 1$  也成立.



## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 对于奇数  $a$  和整数  $k \geq 3$ ,  $a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .
- (数学归纳法) 当  $k=3$  时, 显然  $a^2 \equiv 1 \pmod{8}$ ,  
 $\varphi(2^k)/2 = 2^{k-2} = 2$ .
- 假设结论对  $k_0$  成立, 即  $a^{\varphi(2^{k_0})/2} = a^{2^{k_0-2}} \equiv 1 \pmod{2^{k_0}}$ .
- 令  $a^{2^{k_0-2}} = 1 + d2^{k_0}$ .
- 两边平方得到,  $a^{2^{k_0-1}} = 1 + d2^{k_0+1} + d^2 2^{2k_0}$ .
- 于是  $a^{\varphi(2^{k_0+1})/2} = a^{2^{k_0-1}} \equiv 1 \pmod{2^{k_0+1}}$ , 即结论对  $k_0+1$  也成立.
- 从而模  $2^k (k \geq 3)$  没有原根.

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 但是模  $2^k (k \geq 3)$  总存在阶为  $\varphi(2^k)/2 = 2^{k-2}$  的元素。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 但是模  $2^k (k \geq 3)$  总存在阶为  $\varphi(2^k)/2 = 2^{k-2}$  的元素。
- 由于 3 是模 4 的原根, 根据之前的定理, 猜测 5 可能是这样的元素。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 但是模  $2^k$  ( $k \geq 3$ ) 总存在阶为  $\varphi(2^k)/2 = 2^{k-2}$  的元素。
- 由于 3 是模 4 的原根, 根据之前的定理, 猜测 5 可能是这样的元素。
- 只需要证明  $5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ 。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 但是模  $2^k$  ( $k \geq 3$ ) 总存在阶为  $\varphi(2^k)/2 = 2^{k-2}$  的元素。
- 由于 3 是模 4 的原根, 根据之前的定理, 猜测 5 可能是这样的元素。
- 只需要证明  $5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ 。
- 实际上可以通过数学归纳法证明  $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$ 。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- 但是模  $2^k$  ( $k \geq 3$ ) 总存在阶为  $\varphi(2^k)/2 = 2^{k-2}$  的元素。
- 由于 3 是模 4 的原根, 根据之前的定理, 猜测 5 可能是这样的元素。
- 只需要证明  $5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ 。
- 实际上可以通过数学归纳法证明  $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$ 。
- 于是  $\text{ord}_{2^k}(5) = 2^{k-2}$ ,  $k \geq 3$ 。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- $\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\} = \{-1, 1\} \times \{5, 5^2, \dots, 5^{2^{k-2}}\}.$
- 即任何一个小于  $2^k$  的奇数都可以写成  $(-1)^a 5^b \pmod{2^k}$  的形式。

## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- $\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\} = \{-1, 1\} \times \{5, 5^2, \dots, 5^{2^{k-2}}\}.$
- 即任何一个小于  $2^k$  的奇数都可以写成  $(-1)^a 5^b \pmod{2^k}$  的形式。
- SEAL 中用的是几?



## $\mathbb{Z}_{2^k}^*$ , $k \geq 3$ 的结构

$$\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\}, \varphi(2^k) = 2^{k-1}.$$

- $\mathbb{Z}_{2^k}^* = \{1, 3, \dots, 2^k - 1\} = \{-1, 1\} \times \{5, 5^2, \dots, 5^{2^{k-2}}\}.$
- 即任何一个小于  $2^k$  的奇数都可以写成  $(-1)^a 5^b \pmod{2^k}$  的形式。
- SEAL 中用的是几?
- 答案是 3。请在课后的习题中证明 3 也具有上面的性质。

# 原根

设  $p$  是奇素数，利用模  $p$  的原根  $g$  的存在性，我们可以证明

$$S_n = \sum_{j=0}^{p-1} j^n \pmod{p} \equiv \begin{cases} -1 & (p-1) \mid n \\ 0 & (p-1) \nmid n \end{cases}$$

- 进一步地，如果  $p-1 = 2^k r$ ，那么模  $p$  存在  $2^k$  次单位根  $g^r$ 。
- $u = g^r$  也存在上述类似地指数和 (请仿照 FFT 的形式，猜测  $u$  满足哪些性质，并证明之)。
- 快速数论变换 (NTT) 的理论基础。

# “模”：数学 v.s. 英语

数学中有很多“模”相关的词，对应的英语表达却有所不同，你能区分吗？

- modular
- module
- moduli
- modulus
- modulo
- mod.
- 模运算、模格、模数、模空间、模形式.....

# 课后题

习题及课件: <https://github.com/primihub/crypto-learning>

# 谢谢