- 近代密码涉及到许多数学分支, 如数理统计、信息论、数论、有限域理论、复杂性理论、甚至于代数、几何等.
- 数学是近代密码学中不可或缺的工具.

1 数论

1.1 数的 m 进制表示

1. 十进制表示

   - 十进制是最方便的一种整数表示法

     例如: $1987 = 1 \times 10^3 + 9 \times 10^2 + 8 \times 10 + 7$, $53721 = 5 \times 10^4 + 3 \times 10^3 + 7 \times 10^2 + 2 \times 10 + 1$
   - 实际上, 可以用任何进制表示一个数.

   定理 1.1 *设 m 是大于 1 的正整数, 则每一个正整数 n 可唯一表示为*

   $$n = c_k m^k + c_{k-1} m^{k-1} + \cdots + c_1 m + c_0$$

   其中 $c_j (j = 0, 1, 2, \cdots, k)$ 是整数, 且 $0 \le c_j < m, c_k \neq 0$. 记作: $n = (c_k c_{k-1} \cdots c_1 c_0)_m$

2. m 进制表示的具体做法

   - 将一个整数 n 表示为 m 进制时, 主要是确定 $c_0, c_1, \cdots, c_{k-1}, c_k$
   - $\lfloor \frac{n}{m} \rfloor$ 表示 n 除以 m 后, 取其整数部分 (也就是比 $\frac{n}{m}$ 小的最大整数), 确定 $c_0, c_1, c_2 \cdots, c_{k-1}, c_k$ 的方法如下:

     (a) 令 $r_1 = c_0, n_0 = n$, 则有

     $$n_1 = \lfloor \frac{n_0}{m} \rfloor = c_k m^{k-1} + c_{k-1} m^{k-2} + \cdots + c_1 m + c_0$$

     (b) 令 $r_2 = c_1$, 则有

     $$n_2 = \lfloor \frac{n_1}{m} \rfloor = c_k m^{k-2} + c_{k-1} m^{k-3} + \cdots + c_2 m + c_1$$

     (c) 令 $r_3 = c_2, \cdots\cdots$

(d) 若 $n_i > m$, 令 $r_{i+1} = c_i, i = 0, 1, 2, \cdots$

$$n_{i+1} = \lfloor \frac{n_i}{m} \rfloor = c_k m^{k-i-1} + c_{k-1} m^{k-i-2} + \cdots + c_{i+2} m + c_{i+1}$$

(e) 直到

$$n_{k+1} = \lfloor \frac{n_k}{m} \rfloor = 0, c_k = r_{k+1}$$

即 $n_k < m$ 为止

3. 举例

例如 $n = 389, m = 5$

解令 $n_0 = n = 389$

则有

$$n_1 = \lfloor \frac{n_0}{5} \rfloor = \lfloor \frac{389}{5} \rfloor = 77, r_1 = 4 = c_0$$
$$n_2 = \lfloor \frac{n_1}{5} \rfloor = \lfloor \frac{77}{5} \rfloor = 15, r_2 = 2 = c_1$$
$$n_1 = \lfloor \frac{n_0}{5} \rfloor = \lfloor \frac{389}{5} \rfloor = 77, r_3 = 0 = c_2$$
$$n_1 = \lfloor \frac{n_0}{5} \rfloor = \lfloor \frac{389}{5} \rfloor = 77, r_4 = 3 = c_3$$

故 $389 = 3 \times 5^3 + 0 \times 5^2 + 2 \times 5^1 + 4 = (3024)_5$

例如 $n = 389, m = 2$

则有

$$n_1 = \lfloor \frac{n_0}{2} \rfloor = \lfloor \frac{389}{2} \rfloor = 194, c_0 = 1$$
$$n_2 = \lfloor \frac{n_1}{2} \rfloor = \lfloor \frac{194}{2} \rfloor = 97, c_0 = 0$$
$$n_3 = \lfloor \frac{n_2}{2} \rfloor = \lfloor \frac{97}{2} \rfloor = 48, c_0 = 1$$
$$n_4 = \lfloor \frac{n_3}{2} \rfloor = \lfloor \frac{48}{2} \rfloor = 24, c_0 = 0$$
$$n_5 = \lfloor \frac{n_4}{2} \rfloor = \lfloor \frac{24}{2} \rfloor = 12, c_0 = 0$$
$$n_6 = \lfloor \frac{n_5}{2} \rfloor = \lfloor \frac{12}{2} \rfloor = 6, c_0 = 0$$
$$n_7 = \lfloor \frac{n_6}{2} \rfloor = \lfloor \frac{6}{2} \rfloor = 3, c_0 = 0$$
$$n_8 = \lfloor \frac{n_7}{2} \rfloor = \lfloor \frac{3}{2} \rfloor = 1, c_0 = 1$$
$$n_9 = \lfloor \frac{n_8}{2} \rfloor = \lfloor \frac{1}{2} \rfloor = 0, c_0 = 1$$

故 $389 = 2^8 + 2^7 + 2^2 + 1 = (110000101)_2$

1.2 数的因数分解

定义 1.1 素数 只能被 *1* 和其自身除尽的正整数称为
素数 $(1, 2, 3, 5, \cdots)$

定义 1.2 合数 不是 *1* 且非素数的正整数称为
合数 $(4, 6, 8, 9, 10, \cdots)$

a 除尽 b 表示 $a|b$.
以后不特别说明英文字母 $a, b, c, \cdots$ 等都表示正整数.

定义 1.3 公因子 若 $a|b$, 且 $a|c$, 则称 a 是 b 和 c 的公因子

定义 1.4 最大公因子 若 a 是 b 和 c 的公因子, 且 b 和 c 的每一个公因子都能除尽 a, 则称 a 是 b 和 c 的最大公因子, 表示为 $a = gcd(b, c)$ 或者 $a = (b, c)$

定义 1.5 倍数 若 $a|c$, 则称 c 是 a 的倍数, 若 $a|c$ 且 $b|c$, 则称 c 是 a 和 b 的公倍数

定义 1.6 最小公倍数 若 a 和 b 的公倍数 c 能除尽 a 和 b 的任意公倍数, 则称 c 是 a 和 b 的最小公倍数, 表示为 $c = lcm\{a, b\}$ 或 $c = [a, b]$

定理 1.2 若 $a = bq + r$, 则 $gcd\{a, b\} = \pm gcd\{b, r\}$

定理 1.3 每一对不全为零的整数, 必有一个正的最大公因数.

例: 求 $gcd\{726, 393\}$
解: 辗转相除法

$$
\begin{aligned}
&gcd\{726, 393\} = gcd\{393, 333\} \\
&gcd\{393, 333\} = gcd\{333, 60\} \\
&gcd\{60, 33\} = gcd\{33, 27\} \\
&gcd\{33, 27\} = gcd\{27, 6\} \\
&gcd\{27, 6\} = gcd\{6, 3\} \\
&gcd\{6, 3\} = 3
\end{aligned}
$$

定理 1.4 *若 $d = gcd\{a, b\}$, 则存在整数 p 和 q, 使得 $d = pa + qb$*
若 $gcd\{a, b\} = \pm 1$, 则称 a 和 b 互素. 1 和任意整数互素
若 a 和 b 互素, 则必存在整数 p 和 q, 使得 $pa + qb = 1$

例: 以 $3 = gcd\{726, 393\}$ 为例.
解:

$$\begin{aligned}
3 &= 27 - 4 \times 6 \\
&= 27 - 4 \times (33 - 27) \\
&= -4 \times 33 + 5 \times 27 \\
&= -4 \times 33 + 5 \times (60 - 33) \\
&= 5 \times 60 - 9 \times 33 \\
&= 5 \times 60 - 9 \times (333 - 5 \times 60) \\
&= -9 \times 333 + 50 \times 60 \\
&= -9 \times 333 + 50 \times (393 - 333) \\
&= 50 \times 393 - 59 \times 333 \\
&= 50 \times 393 - 59 \times (726 - 393) \\
&= -59 \times 726 + 109 \times 393
\end{aligned}$$

所以, $3 \equiv -59 \times 726 + 109 \times 393$

1.3 同余类

- 若 $m|a-b$, 即 $a - b = km$, 就称 a 和 b 模 m 同余, 记作: $a \equiv b \bmod m$. m 被称为这个同余式的模
- 同余关系和通常意义的相等颇为相似, 但实质不同.
- a 和 b 模 m 同余表示 a 和 b 除以 m 的余数相同, 或 $a - b$ 是 m 的倍数.

例如 $5 \equiv 2 \bmod 3, 8 \equiv 2 \bmod 3, 11 \equiv 2 \bmod 3$ 即 $a \equiv b \bmod m$, 实际上是说明存在一个整数 k, 使得 $a \equiv km + b$

定理 1.5 *模 m 的同余关系满足*

(1) *自反性, 即 $a \equiv a \bmod m$.*

(2) 对称性, 即若 $a \equiv b \bmod m$, 则 $b \equiv a \bmod m$.

(3) 传递性, 即若 $a \equiv b \bmod m$, $b \equiv c \bmod m$, 则 $a \equiv c \bmod m$.

定理 1.6 若 $a \equiv b \bmod m, c \equiv d \bmod m$, 则

(1) $a \pm c \equiv b \pm d \bmod m$

(2) $ac \equiv bd \bmod m$

定理 1.7 若 $ac \equiv bc \bmod m$, 且 c 和 m 互素, 则 $a \equiv b \bmod m$.

定理 1.8 若 $ac \equiv bc \bmod m, d = (c, m)$, 则 $a \equiv b \bmod (m/d)$

例如: $\because \begin{array}{l} 42 \equiv 7 \bmod 5 \\ 6 \times 7 \equiv 1 \times 7 \bmod 5 \end{array}$

$\therefore 6 \equiv 1 \bmod 5$

1.4 线性同余方程

- 线性同余方程为: $ax \equiv b \bmod m$
- 若整数 x_1 满足线性同余方程, 即 $ax_1 \equiv b \bmod m$, 则模 m 与 x_1 同余的所有整数 $x(x \equiv x_1 \bmod m)$ 都满足这个线性同余方程.
- 若 x_2 是模 m 与 x_1 的同余整数, 即 $x_2 \equiv x_1 \bmod m$, 则 $ax_2 \equiv b \bmod m$

例如: $2x \equiv 3 \bmod 5, x \equiv 4 \bmod 5$ 是这个线性同余式的解.

定理 1.9 同余式

$$ax = b \bmod m$$

有解的充要条件是 $d|b$, 其中 $d = (a, m)$. 令 $m' = \frac{m}{d}$, 若 x_0 是 $ax = b \bmod m$ 的一个解, 则其所有解 x 均满足

$$x \equiv x_0 (\bmod m')$$

推论 1.1 设 $(a, m) = 1$, 则同余式 $ax \equiv b (\bmod m)$ 恰有唯一解

$$x \equiv x_o (\bmod m)$$

1.5 联立的同余式和中国剩余定理

定理 1.10 下列两个同余式

$$x \equiv b_1 \bmod m_1, x \equiv b_2 \bmod m_2$$

有一个共同解的充要条件为

$$b_1 \equiv b_2 \bmod d, d = (m_1, m_2)$$

即

$$(m_1, m_2)|(b_1, b_2)$$

对于 n 个联立同余式有类似结果

定理 1.11 联立同余式

$$x \equiv b_i \bmod m_i, i = 1, 2, \cdots, n$$

有一个共同解的充要条件为

$$(m_i, m_j)|(b_i, b_j), i \neq j, i, j = 1, 2, 3, \cdots, n$$

定理 1.12 若 $a \equiv b \bmod m_1, a \equiv b \bmod m_2, \cdots, a \equiv b \bmod m_k$, 则

$$a \equiv b \bmod [m_1, m_2, \cdots, m_k]$$

式中 $[m_1, m_2, \cdots, m_k]$ 表示最小公倍数.

定义 1.7 中国剩余定理 设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数, $M = m_1 m_2 \cdots m_k$, $M_i = \frac{M}{m_i}(i = 1, 2, \cdots, k)$, 则同余式方程组

$$x \equiv b_i \bmod m_i, i = 1, 2, \cdots, k$$

有唯一解

$$x \equiv b_1 M_1 y_1 + b_2 M_2 y_2 + \cdots + b_k M_k y_k (modM)$$

其中 $M_i y_i \equiv 1(\text{mod} m_i), i = 1, 2, \cdots, k.$

证明 1.1 令 $M = m_1 m_2 \cdots m_k$

$$M_j = \frac{M}{m_j} = m_1 m_2 \cdots m_{j-1} m_{j+1} \cdots m_k$$

求 y_j 使得

$$M_i y_i \equiv 1 \bmod m_j, j = 1, 2, \cdots, k$$

由于 $(M_j, m_j) = 1$, 故 y_j 存在. 令

$$x = b_1 M_1 y_1 + b_2 M_2 y_2 + \cdots + b_k M_k y_k$$

例题求下列方程组的解

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

由上述方程可以得到

$$b_1 = 1, b_2 = 2, b_3 = 3$$

$$m_1 = 2, m_2 = 3, m_3 = 5$$

所以

$$\begin{aligned} &M = m_1 \cdot m_2 \cdot m_3 = 2 \times 3 \times 5 = 30 \\ &M_1 = \frac{M}{m_1} = \frac{30}{2} = 15 \\ &M_2 = \frac{M}{m_2} = \frac{30}{3} = 10 \\ &M_3 = \frac{M}{m_3} = \frac{30}{5} = 6 \end{aligned}$$

因而

$$\begin{cases} 15y_1 \equiv 1 \bmod 2, y_1 = 1 \\ 10y_2 \equiv 1 \bmod 3, y_2 = 1 \\ 6y_3 \equiv 1 \bmod 5, y_3 = 1 \end{cases}$$

可得

$$\begin{aligned} x &= b_1 M_1 y_1 + b_2 + M_2 y_2 + b_3 M_3 y_3 \\ &= 1 \times 15 \times 1 + 2 \times 10 \times 1 + 3 \times 6 \times 1 \\ &= 15 + 20 + 18 \\ &= 53 \equiv 23 \bmod 30 \end{aligned}$$

例题: 求解方程

$$\begin{cases} x \equiv 0(\mathrm{mod}3) \\ x \equiv 1(\mathrm{mod}5) \\ x \equiv 2(\mathrm{mod}7) \end{cases}$$

解: 由题目条件可知

$$m_1 = 3, m_2 = 5, m_3 = 7, b_1 = 0, b_2 = 1, b_3 = 2$$

故有

$$\begin{aligned} &M = m_1 \cdot m_2 \cdot m_3 = 3 \times 5 \times 7 = 105 \\ &M_1 = \frac{M}{m_1} = \frac{105}{3} = 35 \\ &M_2 = \frac{M}{m_2} = \frac{105}{5} = 21 \\ &M_3 = \frac{M}{m_3} = \frac{105}{7} = 15 \end{aligned}$$

则

$$35y_1 = 1(\mathrm{mod}3), y_1 = 2$$

$$21y_2 = 1(\mathrm{mod}5), y_2 = 1$$

$$15y_3 = 1(\mathrm{mod}7), y_3 = 1$$

最后得到解

$$\begin{aligned} x &\equiv y_1M_1b_1 + y_2M_2b_2 + y_3M_3b_3(\mathrm{mod}M) \\ &\equiv [2 \times 35 \times 0 + 1 \times 21 \times 1 + 1 \times 15 \times 2](\mathrm{mod}105) \\ &\equiv 51(\mathrm{mod}105) \end{aligned}$$