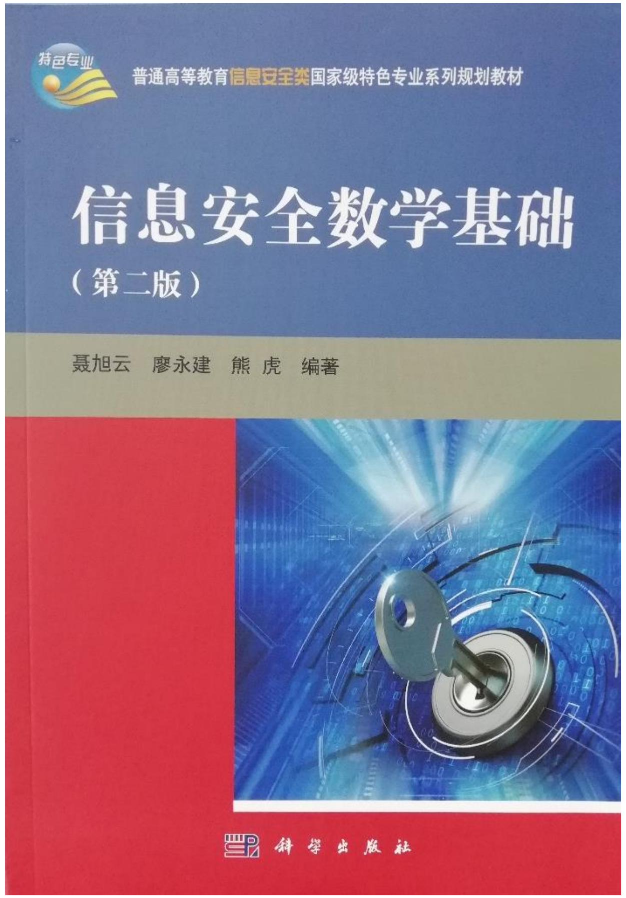
现代密码学

模整数乘法逆元

信息与软件工程学院

参考资料

- 《信息安全数学基础（第二版）》，聂旭云，廖永建，熊虎编著，科学出版社，2019
- 第一章 整除 1.2节
- 第二章 同余 2.2节



1.2 欧几里得算法及其扩展算法

辗转相除法（欧几里得算法）

该算法是用来求解给定整数a和b的最大公因数

设a,b是两个整数，$b\neq 0$，依次做带余数除法

$$a = bq_1 + r_1, 0 < r_1 < |b|$$

$$b = r_1 q_2 + r_2, 0 < r_2 < r_1$$

$$\vdots$$

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, 0 < r_{k+1} < r_k$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1}, r_{n+1} = 0$$

经过有限步运算，必然存在n使得$r_{n+1} = 0$，这是因为

$$0 \le r_{n+1} < r_n < \cdots < r_1 < |b|$$

1.2 欧几里得算法及其扩展算法

定理1.2.1 设a,b 是两个整数，不妨设$a>b$ ，则 $(a,b)=r_n$ ，其中r_n 是上述辗转相除法中得到的最后一个非零余数。

证明：根据最大公因数的性质（4），有

$$\begin{aligned}(a,b)&=(b,r_1)\\&=(r_1,r_2)\\&\ \ \vdots\\&=(r_{n-1},r_n)\\&=r_n\end{aligned}$$

1.2 欧几里得算法及其扩展算法

算法 1.2.1 计算两个整数得最大公因子的欧几里得算法。

输入：两个非负整数 a，b，且 $a \geq b$；

输出：a，b 的最大公因子。

1、 当 $b \neq 0$ 作

1.1 $r \leftarrow a \bmod b, a \leftarrow b, b \leftarrow r$；

2、返回 (a)

例1.2.1 计算 $(4864, 3458)$ 。

$$
\begin{aligned}
4864 &= 1 \times 3458 + 1406, & q_1 &= 1, r_1 = 1406 \\
3458 &= 2 \times 1406 + 646, & q_2 &= 2, r_2 = 646 \\
1406 &= 2 \times 646 + 114, & q_3 &= 2, r_3 = 114 \\
646 &= 5 \times 114 + 76, & q_4 &= 5, r_4 = 76 \\
114 &= 1 \times 76 + 38, & q_5 &= 1, r_5 = 38 \\
76 &= 2 \times 38, & q_6 &= 2
\end{aligned}
$$

所以 $(4864, 3458) = r_5 = 38$ 。

1.2 欧几里得算法及其扩展算法

注意：当 a, b 中有负整数时，可根据最大公因数的性质（1）可将其中的负整数转变为正整数来求其最大公因数。

例1.2.2 用辗转相除法求 $(-123, 17)$ 。

解： $(-123, 17) = (123, 17)$

做辗转相除法：

$$
\begin{aligned}
123 &= 7 \times 17 + 4, \quad q_1 = 7, r_1 = 4, \\
17 &= 4 \times 4 + 1, \quad q_2 = 4, r_2 = 1, \\
4 &= 4 \times 1, \quad q_3 = 4
\end{aligned}
$$

因此， $(123, 17) = r_2 = 1$

1.2 欧几里得算法及其扩展算法

定理 **1.2.2** 对于任意两个整数 a,b ，存在整数 x,y 使得

$$(a,b)=xa+yb$$ 。

证明：设 Z 是全体整数集合。做一个如下集合：

$$S=\{|xa+yb||x,y\in Z\}$$

S 中的元素显然大于等于**0**。

设 d 为 S 中的最小正整数，则 d 可表示为 a,b 的组合，设

$$d=ua+vb$$

现在我们证明 $d|a$ 且 $d|b$ 。

做带余除法：

$$a=qd+r, 0\le r<d$$

于是

$$r=a-qd=a-q(ua+vb)=(1-qu)a-qvb$$

这说明 r 也可表示为 a,b 的组合，则 $r\in S$。由于 d 是 S 中最小正整数，所以只有 $r=0$ 。故 $d|a$ 。同理 $d|b$ 。

设 c 是 a,b 的任意公因子，由 $c|a$ 和 $c|b$ 得 $c|d=ua+vb$。故 d 是 a,b 的最大公因子，证毕。

1.2 欧几里得算法及其扩展算法

定理1.2.2 对于任意两个整数 a, b，存在整数 x, y 使得

$$(a,b) = xa + yb$$

证明 根据辗转相除法，有

$$r_1 = a - bq_1, r_2 = b - r_1 q_2 = -q_2 a + (1 + q_1 q_2) b$$

一般地，对于任意的 r_i，都存在两个整数 x_i, y_i，使 $r_i = x_i a + y_i b$ 可利用如下递推公式得到：

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= (x_{i-2} a + y_{i-2} b) - q_i (x_{i-1} a + y_{i-1} b) \\ &= (x_{i-2} - q_i x_{i-1}) a + (y_{i-2} - q_i y_{i-1}) b \end{aligned}$$

可见

$$x_i = x_{i-2} - q_i x_{i-1}, y_i = y_{i-2} - q_i y_{i-1}, i = 1, 2, 3, \cdots$$

1.2 欧几里得算法及其扩展算法

由式（1.2）可知

$$x_{-1} = 1, x_0 = 0,$$

$$y_{-1} = 0, y_0 = 1$$

利用这几个初始值及递推关系式（1.3），就可依次计算出

$$(x_1, y_1)(x_2, y_2), \cdots, (x_n, y_n)$$

最后得到

$$(a, b) = r_n = x_n a + y_n b$$

令 $x = x_n, y = y_n$，定理得证。

1.2 欧几里得算法及其扩展算法

算法 1.2.2 扩展的欧几里得算法

输入：两个非负整数 a，b，且 $a \ge b$；

输出：$d=(a,b)$ 与满足 $ax+by=d$ 的整数 x 与 y;

1、若 $b=0$，则 $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$，返回 (d,x,y)

2、设 $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$；

3、当 $b>0$ 时，作

3.1 $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a-qb, x \leftarrow x_2-qx_1, y \leftarrow y_2-qy_1$；

3.2 $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$；

4、$d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$，返回 (d,x,y)。

1.2 欧几里得算法及其扩展算法

例 求整数 x,y 使得，$(17,26)=17x+26y$ 。

$$26=17\times 1+9$$
$$17=9\times 1+8$$
$$9=8\times 1+1$$
$$8=1\times 8$$

1=9-8 ×1

=9-（17-9 ×1）

=9 ×2-17

=（26-17 ×1） ×2-17

=26 ×2-17 ×3

例1.2.3 求整数 x, y ，使 $(4864, 3458) = 4864x + 3458y$ 。

解：回顾例1.2.1 中

$$\begin{aligned}
4864 &= 1 \times 3458 + 1406, & q_1 &= 1, r_1 = 1406 \\
3458 &= 2 \times 1406 + 646, & q_2 &= 2, r_2 = 646 \\
1406 &= 2 \times 646 + 114, & q_3 &= 2, r_3 = 114 \\
646 &= 5 \times 114 + 76, & q_4 &= 5, r_4 = 76 \\
114 &= 1 \times 76 + 38, & q_5 &= 1, r_5 = 38 \\
76 &= 2 \times 38, & q_6 &= 2
\end{aligned}$$

$$(4864, 3458) = r_5 = 38$$

根据例1.2.1，有

1.2 欧几里得算法及其扩展算法

$$
\begin{aligned}
1406 &= 4864 - 1 \times 3458 \\
646 &= 3458 - 2 \times 1406 \\
&= 3458 - 2 \times (4864 - 1 \times 3458) \\
&= 3 \times 3458 - 2 \times 4864 \\
114 &= 1406 - 2 \times 646 \\
&= 4864 - 1 \times 3458 - 2 \times (3 \times 3458 - 2 \times 4864) \\
&= 5 \times 4864 - 7 \times 3458 \\
76 &= 646 - 5 \times 114 \\
&= 3 \times 3458 - 2 \times 4864 - 5 \times (5 \times 4864 - 7 \times 3458) \\
&= 38 \times 3458 - 27 \times 4864 \\
38 &= 114 - 76 \\
&= 5 \times 4864 - 7 \times 3458 - (38 \times 3458 - 27 \times 4864) \\
&= 32 \times 4864 - 45 \times 3458
\end{aligned}
$$

即：

$$
\begin{aligned}
38 &= 114 - 76 \\
&= 114 - (646 - 5 \times 114) \\
&= -646 + 6 \times (1406 - 2 \times 646) \\
&= 6 \times 1406 - 13 \times (3458 - 2 \times 1406) \\
&= -13 \times 3458 + 32 \times (4864 - 3458) \\
&= 32 \times 4864 - 45 \times 3458
\end{aligned}
$$

因此整数 $x = 32, y = -45$ 满足 $(4864, 3458) = 4864x + 3458y$ 。

1.2 欧几里得算法及其扩展算法

定理1.2.3 设a, b是两个不全为**0**的整数，则 $(a,b)=1$ 当且仅当存在整数 u, v 使得

$$ua+vb=1$$

证明 必要性式定理 **1.2.1** 的特例。下证充分性。
如果存在整数 u, v ，使得$ua+vb=1$
则根据整除的性质有 $(a,b)|ua+vb$ ，即有 $(a,b)|1$ ，因此有 $(a,b)=1$ 。

定理2.2.7 设 m是正整数，$r \in \mathbf{Z}_m$，若 $(r, m) = 1$，则存在整数$s \in \mathbf{Z}_m$，使得

$$rs \equiv 1 (\bmod\ m)$$

整数s也称为 r模整数m 下的乘法逆元。

证明：因为 $(r, m) = 1$，根据定理**1.2.3**存在整数s_1，t_1，使得

$$s_1 r + t_1 m = 1$$

因此有$s_1 r \equiv 1 (\bmod\ m)$。取$s$为$s_1$模去$m$后的最小正整数，即可得证。

例2.2.4 求 $15 \pmod{26}$ 的乘法逆元。

解：15与26互素，存在乘法逆元。做辗转相除法，可得

$$26 = 1 \times 15 + 11$$

$$15 = 1 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

因此有

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \times 4) \\ &= 3 \times 4 - 11 = 3 \times (15 - 11) - 11 \\ &= 3 \times 15 - 4 \times 11 = 3 \times 15 - 4 \times (26 - 15) \\ &= 7 \times 15 - 4 \times 26 \end{aligned}$$

所以 $15 \pmod{26}$ 的乘法逆元为7。

例2.2.5 求$11 \pmod{26}$的乘法逆元。

解：11与26互素，存在乘法逆元。做辗转相除法

$$26 = 2 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

因此有

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \times 4) \\ &= 3 \times 4 - 11 \\ &= 3 \times (26 - 2 \times 11) - 11 \\ &= 3 \times 26 - 7 \times 11 \end{aligned}$$

又因为$-7 \equiv 19 \pmod{26}$，所以$11 \pmod{26}$的乘法逆元为19。

感 谢 聆 听!

xynie@uestc.edu.cn