辗转相除法

定理 2：对正整数 a, b，令 $d = (a, b)$，则 d 是 S 中的最小元素，其中 $S = \{ax+by : x, y \in \mathbb{Z}, ax + by > 0\}$.

证明： 显然 S 非空

由良序引理，它包含最小元素，记为 $c = ax_0 + by_0$

下证 $d = c$

一方面，由 $d \mid a, d \mid b$，有 $d \mid c$, 则 $d \leq c$

另一方面，令 $a = cq + r, 0 \leq r \leq c - 1$

若 $r \neq 0$，则 $r = a - cq = a - (ax_0 + by_0)q = a(1 - x_0) - by_0q$

$\therefore r \in S$，这与 c 为 S 中最小元素矛盾　$\therefore r = 0$，故 $c \mid a$

类似地，有 $c \mid b$

$\therefore c \leq d$

$\therefore d = c$.

定理 3（最大公因数的刻画定理）： 对正整数 a, b，$d = (a, b)$ 当且仅当 $d > 0, d \mid a, d \mid b$，且对任何的 $f \mid a, f \mid b$，有 $f \mid d$

证明： 必要性：由最大公因数的定义，$d > 0, d \mid a, d \mid b$ 显然

若 $f \mid a, f \mid b$，由定理 2 知 $d = ax + by, x, y \in \mathbb{Z}$

$\therefore f \mid d$.

充分性: 由 $f \mid d$ 可得 $f \leq d$

由 $f \mid a, f \mid b$ 及 f 的任意性知 f 是 a, b 的任意公因子

因此由最大公因子的定义知 $d = (a, b)$

推论（辗转相除法）： 若

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$

$$\vdots$$
$$r_{k-2} = r_{k-1}q_k + r_k$$
$$r_{k-1} = r_k q_{k+1}$$

令 $d = (a, b)$，则 $r_k = d$.

证明： 一方面，注意到 $r_k \mid r_{k-1}, r_k \mid r_{k-2}, r_k \mid r_{k-3}, \cdots, r_k \mid r_1, r_k \mid b, r_k \mid a$

可知 r_k 为 a, b 的公因子

由定理 3，$r_k \mid d$.

另一方面，

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_k \\ &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k \\ &= r_{k-3}(-q_k) + r_{k-2}(1 + q_k q_{k-1}) \\ &= \cdots \\ &= ax + by \end{aligned}$$

由 $d = (a, b)$ 知 $d \mid a, d \mid b$, 故 $d \mid r_k$

$\therefore d = r_k$.