最大公因数理论

Lemma：$\lambda, x_1, \cdots, x_n \in \mathbb{Z}$，$x_1, \cdots, x_n$ 全不为 0，$x_1, \cdots, x_n$ 两两互素，

$x_1 | \lambda, \cdots, x_n | \lambda$. 则有：$x_1 \cdots x_n | \lambda$

Proof：$\because x_1 | \lambda$ $\therefore \exists q_1 \in \mathbb{Z}$, s.t. $\lambda = x_1 q_1$

$\because x_2, x_1, q_1 \in \mathbb{Z}$，$x_2 \neq 0$，$\gcd(x_2, x_1) = 1$，$x_2 | x_1 q_1$ $\therefore x_2 | q_1$

$\because x_2 | q_1$ $\therefore \exists q_2 \in \mathbb{Z}$, s.t. $q_1 = x_2 q_2$ $\therefore \lambda = x_1 q_1 = x_1 (x_2 q_2) = (x_1 x_2) q_2$

$\because x_3, x_1, x_2 \in \mathbb{Z}$，$\gcd(x_3, x_1) = 1$ $\therefore \gcd(x_3, x_1 x_2) = \gcd(x_3, x_2) = 1$

$\because x_3, x_1 x_2, q_2 \in \mathbb{Z}$，$x_3 \neq 0$，$\gcd(x_3, x_1 x_2) = 1$，$x_3 | (x_1 x_2) q_2$ $\therefore x_3 | q_2$

$\because x_3 | q_2$ $\therefore \exists q_3 \in \mathbb{Z}$, s.t. $q_2 = x_3 q_3$ $\therefore \lambda = (x_1 x_2) q_2 = (x_1 x_2)(x_3 q_3) = (x_1 x_2 x_3) q_3$

$\because x_4, x_1, x_2 \in \mathbb{Z}$，$\gcd(x_4, x_1) = 1$ $\therefore \gcd(x_4, x_1 x_2) = \gcd(x_4, x_2) = 1$

$\because x_4, x_1 x_2, x_3 \in \mathbb{Z}$，$\gcd(x_4, x_1 x_2) = 1$，$\therefore \gcd(x_4, x_1 x_2 x_3) = \gcd(x_4, x_3) = 1$

$\because x_4, x_1 x_2 x_3, q_3 \in \mathbb{Z}$，$x_4 \neq 0$，$\gcd(x_4, x_1 x_2 x_3) = 1$，$x_4 | (x_1 x_2 x_3) q_3$ $\therefore x_4 | q_3$

$\because x_4 | q_3$ $\therefore \exists q_4 \in \mathbb{Z}$, s.t. $q_3 = x_4 q_4$ $\therefore \lambda = (x_1 x_2 x_3) q_3 = (x_1 x_2 x_3 x_4) q_4$

将上述证明过程继续下去，可得：$\lambda = (x_1 x_2 \cdots x_{n-1}) q_{n-1}$.（其中 $q_{n-1} \in \mathbb{Z}$）

$\because x_n, x_1, x_2 \in \mathbb{Z}$，$\gcd(x_n, x_1) = 1$ $\therefore \gcd(x_n, x_1 x_2) = \gcd(x_n, x_2) = 1$

$\because x_n, x_1 x_2, x_3 \in \mathbb{Z}$，$\gcd(x_n, x_1 x_2) = 1$ $\therefore \gcd(x_n, x_1 x_2 x_3) = \gcd(x_n, x_3) = 1$

$\because x_n, x_1 x_2 x_3, x_4 \in \mathbb{Z}$，$\gcd(x_n, x_1 x_2 x_3) = 1$ $\therefore \gcd(x_n, x_1 x_2 x_3 x_4) = \gcd(x_n, x_4) = 1$

$\because x_n, x_1 x_2 x_3 x_4, x_5 \in \mathbb{Z}$，$\gcd(x_n, x_1 x_2 x_3 x_4) = 1$ $\therefore \gcd(x_n, x_1 x_2 x_3 x_4 x_5) = \gcd(x_n, x_5) = 1$

…… 可得：$\gcd(x_n, x_1 \cdots x_{n-2}) = \gcd(x_n, x_{n-2}) = 1$

$\because x_n, x_1 \cdots x_{n-2}, x_{n-1} \in \mathbb{Z}$，$\gcd(x_n, x_1 \cdots x_{n-2}) = 1$ $\therefore \gcd(x_n, x_1 \cdots x_{n-1}) = \gcd(x_n, x_{n-1}) = 1$

$\because x_n, x_1\cdots x_{n-1}, q_{n-1}\in\mathbb{Z}$, $x_n\neq 0$, $\gcd(x_n, x_1\cdots x_{n-1})=1$, $x_n \mid (x_1\cdots x_{n-1})q_{n-1}$ $\therefore x_n \mid q_{n-1}$

$\because x_n \mid q_{n-1}$ $\therefore \exists q_n\in\mathbb{Z}$, s.t. $q_{n-1}=x_n q_n$

$\therefore \lambda = (x_1\cdots x_{n-1})q_{n-1} = (x_1\cdots x_{n-1})(x_n q_n) = (x_1\cdots x_n)q_n$

$\because \lambda\in\mathbb{Z}$, $q_n\in\mathbb{Z}$, $x_1\cdots x_n\in\mathbb{Z}$, $x_1\cdots x_n\neq 0$ $\therefore x_1\cdots x_n \mid \lambda$ $\square$

Lemma (~~两~~两个数的最大公因数和最小公倍数的积等于它们乘积的绝对值) 对 $\forall x_1, x_2\in\mathbb{Z}$, 有:

$$\operatorname{lcm}(x_1,x_2)\cdot\gcd(x_1,x_2) = |x_1 x_2|$$

proof: 分4种情况讨论:

① $x_1=0$ 且 $x_2=0$. 此时 $\gcd(x_1,x_2)=\gcd(0,0)=0$ $\therefore$ 左边 $=0=$ 右边

② $x_1=0$ 且 $x_2\neq 0$. 此时 $\operatorname{lcm}(x_1,x_2)=\operatorname{lcm}(0,x_2)=0$ $\therefore$ 左边 $=0=$ 右边

③ $x_1\neq 0$ 且 $x_2=0$. 此时 $\operatorname{lcm}(x_1,x_2)=\operatorname{lcm}(x_1,0)=0$ $\therefore$ 左边 $=0=$ 右边

④ $x_1\neq 0$ 且 $x_2\neq 0$ 此时再分两种情况讨论:

(i) x_1 与 x_2 互素. $\therefore \gcd(x_1,x_2)=1$

$\because x_1, x_2\in\mathbb{Z}$, x_1, x_2 全不为0, $x_1x_2\in\mathbb{Z}$, $x_1 \mid x_1x_2$, $x_2 \mid x_1x_2$

$\therefore \operatorname{lcm}(x_1,x_2) \mid x_1x_2$ $\because \operatorname{lcm}(x_1,x_2)\in\mathbb{Z}_{\geq 1}$

$\therefore \operatorname{lcm}(x_1,x_2) \mid |x_1x_2|$

$\because x_1 \mid \operatorname{lcm}(x_1,x_2)$ $\therefore \exists q_1\in\mathbb{Z}$, s.t. $\operatorname{lcm}(x_1,x_2)=x_1q_1$

$\because x_2 \mid \operatorname{lcm}(x_1,x_2)$ $\therefore x_2 \mid x_1q_1$

$\because x_2, x_1, q_1\in\mathbb{Z}$, $x_2\neq 0$, $\gcd(x_2,x_1)=1$, $x_2 \mid x_1q_1$ $\therefore x_2 \mid q_1$

$\therefore \exists q_2\in\mathbb{Z}$, s.t. $q_1=x_2q_2$ $\therefore \operatorname{lcm}(x_1,x_2)=x_1q_1=x_1(x_2q_2)=(x_1x_2)q_2$

$\because \operatorname{lcm}(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$, $x_1 x_2 \in \mathbb{Z}$, $x_1 x_2 \neq 0$, $q_2 \in \mathbb{Z}$

$\therefore x_1 x_2 \mid \operatorname{lcm}(x_1, x_2)$ $\qquad \therefore |x_1 x_2| \mid \operatorname{lcm}(x_1, x_2)$

$\because \operatorname{lcm}(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$, $|x_1 x_2| \in \mathbb{Z}_{\geqslant 1}$, $\operatorname{lcm}(x_1, x_2) \mid |x_1 x_2|$, $|x_1 x_2| \mid \operatorname{lcm}(x_1, x_2)$

$\therefore \operatorname{lcm}(x_1, x_2) = |x_1 x_2|$

$\therefore \operatorname{lcm}(x_1, x_2) \cdot \gcd(x_1, x_2) = |x_1 x_2|$

(ii) x_1 与 x_2 不互素. $\therefore \gcd(x_1, x_2) \neq 1$.

$\because x_1 \neq 0$ 且 $x_2 \neq 0$ $\qquad \therefore \operatorname{lcm}(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$, $\gcd(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$

$\because \gcd(x_1, x_2) \mid x_1$ $\qquad \therefore \dfrac{x_1}{\gcd(x_1, x_2)} \in \mathbb{Z}$ $\qquad \because \gcd(x_1, x_2) \mid x_2$ $\qquad \therefore \dfrac{x_2}{\gcd(x_1, x_2)} \in \mathbb{Z}$

$\because x_1, x_2 \in \mathbb{Z}$, $x_1 \neq 0$ 且 $x_2 \neq 0$ $\qquad \therefore \gcd\left(\dfrac{x_1}{\gcd(x_1, x_2)}, \dfrac{x_2}{\gcd(x_1, x_2)}\right) = 1$

$\because \dfrac{x_1}{\gcd(x_1, x_2)} \in \mathbb{Z}$, $\dfrac{x_2}{\gcd(x_1, x_2)} \in \mathbb{Z}$, $\dfrac{x_1}{\gcd(x_1, x_2)} \neq 0$, $\dfrac{x_2}{\gcd(x_1, x_2)} \neq 0$

$\gcd\left(\dfrac{x_1}{\gcd(x_1, x_2)}, \dfrac{x_2}{\gcd(x_1, x_2)}\right) = 1$

$\therefore$ 由 (i) 知 $\operatorname{lcm}\left(\dfrac{x_1}{\gcd(x_1, x_2)}, \dfrac{x_2}{\gcd(x_1, x_2)}\right) = \left|\dfrac{x_1}{\gcd(x_1, x_2)} \cdot \dfrac{x_2}{\gcd(x_1, x_2)}\right|$

$$\therefore \operatorname{lcm}\left(\frac{x_1}{\gcd(x_1, x_2)}, \frac{x_2}{\gcd(x_1, x_2)}\right) = \frac{|x_1 x_2|}{(\gcd(x_1, x_2))^2}$$

$\because \dfrac{x_1}{\gcd(x_1, x_2)} \in \mathbb{Z}$, $\dfrac{x_2}{\gcd(x_1, x_2)} \in \mathbb{Z}$, $\gcd(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$

$$\therefore \operatorname{lcm}\left(\gcd(x_1, x_2) \cdot \frac{x_1}{\gcd(x_1, x_2)}, \gcd(x_1, x_2) \cdot \frac{x_2}{\gcd(x_1, x_2)}\right) = \gcd(x_1, x_2) \cdot \operatorname{lcm}\left(\frac{x_1}{\gcd(x_1, x_2)}, \frac{x_2}{\gcd(x_1, x_2)}\right)$$

$$\therefore \operatorname{lcm}(x_1, x_2) = \gcd(x_1, x_2) \cdot \frac{|x_1 x_2|}{(\gcd(x_1, x_2))^2} = \frac{|x_1 x_2|}{\gcd(x_1, x_2)}$$

$\because \gcd(x_1, x_2) \in \mathbb{Z}_{\geqslant 1}$

$\therefore \operatorname{lcm}(x_1, x_2) \cdot \gcd(x_1, x_2) = |x_1 x_2|$ $\square$