初等数论习题

Lemma：对 $\forall x\in\mathbb{Z}$，有：$\gcd(x)=|x|$.

Proof：当 $x=0$ 时，$\gcd(x)=\gcd(0)=0=|0|=|x|$

当 $x\neq 0$ 时，$\gcd(x)=\max\{d\in\mathbb{Z}_{\geq 1}: d\mid x\}=|x|$

$(\because d\in\mathbb{Z}_{\geq1}$，$x\in\mathbb{Z}$ 且 $x\neq0$，$d\mid x$ $\quad\therefore |d|\leqslant|x|$ $\quad\therefore d\leqslant|x|$.

$\because |x|\mid x$ $\quad\therefore \gcd(x)=\max\{d\in\mathbb{Z}_{\geq1}: d\mid x\}=|x|$.) $\quad\square$

Lemma：$n\in\mathbb{Z}_{\geq1}$，$x_1,\cdots,x_n\in\mathbb{Z}$，则有：

$$\gcd(\gcd(x_1,\cdots,x_n))=\gcd(x_1,\cdots,x_n).$$

Proof：当 $x_1,\cdots,x_n$ 全为0时，

$\gcd(\gcd(x_1,\cdots,x_n))=\gcd(\gcd(0,\cdots,0))=\gcd(0)=0=\gcd(x_1,\cdots,x_n)$

当 $x_1,\cdots,x_n$ 不全为0时，有：$\gcd(x_1,\cdots,x_n)\in\mathbb{Z}_{\geq1}$

$\therefore \gcd(\gcd(x_1,\cdots,x_n))=|\gcd(x_1,\cdots,x_n)|=\gcd(x_1,\cdots,x_n)$ $\quad\square$

Lemma（最大公因数前k个元的分组）$n\in\mathbb{Z}_{\geq1}$，$x_1,\cdots,x_n\in\mathbb{Z}$，$k\in\{1,\cdots,n\}$，则有：

$$\gcd(x_1,\cdots,x_n)=\gcd(\gcd(x_1,\cdots,x_k),x_{k+1},\cdots,x_n)$$

当 $k=n$ 时，右边 $=\gcd(\gcd(x_1,\cdots,x_n))=\gcd(x_1,\cdots,x_n)=$ 左边．结论得证．

当 $k=2$ 时，结论已证．

当 $k=1$ 时，$\gcd(x_1)=|x_1|$．分两种情况讨论：

(i). $x_1,\cdots,x_n$ 全为0．此时左边 $=\gcd(x_1,\cdots,x_n)=\gcd(0,\cdots,0)=0=\gcd(|x_1|,x_2,\cdots,x_n)$

$=\gcd(\gcd(x_1),x_2,\cdots,x_n)=$ 右边．结论得证．

(ii) $x_1,\cdots,x_n$ 不全为0．此时左边 $=\gcd(x_1,\cdots,x_n)=\max\{d\in\mathbb{Z}_{\geq1}: d\mid x_1$ 且 $d\mid x_2$ 且 $\cdots$ 且 $d\mid x_n\}$

$= \max\{d \in \mathbb{Z}_{\geq 1} : d \mid |x_1| \text{ 且 } d \mid x_2 \text{ 且} \cdots \text{且 } d \mid x_n\}$

$= \gcd(|x_1|, x_2, \cdots, x_n) = \gcd(\gcd(x_1), x_2, \cdots, x_n) =$ 右边，结论得证.

($x_1, x_2, \cdots, x_n$ 不全为0 $\Longleftrightarrow$ $|x_1|, x_2, \cdots, x_n$ 不全为0

$x_1, x_2, \cdots, x_n$ 不全为0

$\Rightarrow \begin{cases} \text{若 } x_1 \neq 0 \Rightarrow |x_1| \neq 0 \Rightarrow |x_1|, x_2, \cdots, x_n \text{ 不全为0} \\ \text{若 } x_1 = 0 \Rightarrow x_2, \cdots, x_n \text{ 不全为0} \Rightarrow |x_1|, x_2, \cdots, x_n \text{ 不全为0} \end{cases}$

$|x_1|, x_2, \cdots, x_n$ 不全为0

$\Rightarrow \begin{cases} \text{若 } x_1 \neq 0 \Rightarrow x_1, x_2, \cdots, x_n \text{ 不全为0} \\ \text{若 } x_1 = 0 \Rightarrow |x_1| = 0 \Rightarrow x_2, \cdots, x_n \text{ 不全为0} \Rightarrow x_1, x_2, \cdots, x_n \text{ 不全为0.} \end{cases}$)

$\therefore k=1$ 时结论得证.

当 $k \in \{3, \cdots, n-1\}$ 时，分情况讨论如下：

① $x_1, \cdots, x_n$ 全为0. 此时有：

左边 $= \gcd(x_1, \cdots, x_n) = \gcd(0, \cdots, 0) = 0$ ~~$= \gcd(|x_1|$~~

右边 $= \gcd(\gcd(x_1, \cdots, x_k), x_{k+1}, \cdots, x_n) = \gcd(\gcd(\underbrace{0, \cdots, 0}_{k\text{个}0}), \underbrace{0, \cdots, 0}_{(n-k)\text{个}0})$

$= \gcd(0, \underbrace{0, \cdots, 0}_{(n-k)\text{个}0}) = 0 =$ 左边. 结论得证.

② $x_1, \cdots, x_n$ 不全为0. 此时再分两种情况讨论.

(i) $x_1, \cdots, x_k$ 全为0. $\therefore x_{k+1}, \cdots, x_n$ 中必有非零的整数.

$\therefore$ 左边 $= \gcd(x_1, \cdots, x_n) = \gcd(x_1, \cdots, x_k, x_{k+1}, \cdots, x_n) = \gcd(\underbrace{0, \cdots, 0}_{k\text{个}0}, x_{k+1}, \cdots, x_n)$

$= \max\{d \in \mathbb{Z}_{\geq 1} : \underbrace{d \mid 0 \text{ 且} \cdots \text{且 } d \mid 0}_{k\text{个}\text{“}d \mid 0\text{”}} \text{ 且 } d \mid x_{k+1} \text{ 且} \cdots \text{且 } d \mid x_n\}$

$= \max\{d \in \mathbb{Z}_{\geq 1} : d \mid 0 \text{ 且 } d \mid x_{k+1} \text{ 且} \cdots \text{且 } d \mid x_n\} = \gcd(0, x_{k+1}, \cdots, x_n)$

$= \gcd(\gcd(\underbrace{0, \cdots, 0}_{k\text{个}0}), x_{k+1}, \cdots, x_n) = \gcd(\gcd(x_1, \cdots, x_k), x_{k+1}, \cdots, x_n) =$ 右边. 结论得证.

(ii) $x_1, \cdots, x_k$ 不全为0. 此时有 $\gcd(x_1, \cdots, x_k) \in \mathbb{Z}_{\geqslant 1}$

对 $\forall d \in \mathbb{Z}$, $d \neq 0$, 有:

若 $d \mid x_1$ 且 $\cdots$ 且 $d \mid x_k$, 则 $d \mid \gcd(x_1, \cdots, x_k)$

若 $d \mid \gcd(x_1, \cdots, x_k)$, 则 $\because$ $\gcd(x_1, \cdots, x_k) \mid x_1$ 且 $\cdots$ 且 $\gcd(x_1, \cdots, x_k) \mid x_k$

$\therefore$ $d \mid x_1$ 且 $\cdots$ 且 $d \mid x_k$

$\therefore$ 对 $\forall d \in \mathbb{Z}$, $d \neq 0$, 有: $(d \mid x_1$ 且 $\cdots$ 且 $d \mid x_k) \iff d \mid \gcd(x_1, \cdots, x_k)$

$\therefore$ 左边 $= \gcd(x_1, \cdots, x_n) = \gcd(x_1, \cdots, x_k, x_{k+1}, \cdots, x_n)$

$= \max\{d \in \mathbb{Z}_{\geqslant 1} : d \mid x_1$ 且 $\cdots$ 且 $d \mid x_k$ 且 $d \mid x_{k+1}$ 且 $\cdots$ 且 $d \mid x_n\}$

$= \max\{d \in \mathbb{Z}_{\geqslant 1} : d \mid \gcd(x_1, \cdots, x_k)$ 且 $d \mid x_{k+1}$ 且 $\cdots$ 且 $d \mid x_n\}$

$= \gcd(\gcd(x_1, \cdots, x_k), x_{k+1}, \cdots, x_n) =$ 右边. 结论得证. $\square$

Lemma: 对 $\forall a, b, c \in \mathbb{Z}$, a,b不全为0, 有: $\gcd(a, b, c) \leqslant \gcd(a, b)$

Proof: 分如下情况讨论.

① a, b, c 全为0. 此时 $\gcd(a, b, c) = \gcd(0, 0, 0) = 0 = \gcd(0, 0) = \gcd(a, b)$

结论得证.

② a, b, c 不全为0. 此时再分两种情况讨论:

(i) a, b 全为0 $\therefore$ $c \neq 0$. $\therefore$ $\gcd(a, b, c) = \gcd(0, 0, c) = |c| \in \mathbb{Z}_{\geqslant 1}$

$\because$ $\gcd(a, b) = \gcd(0, 0) = 0$

$\therefore$ $\gcd(a, b, c) > 0 = \gcd(a, b)$

(ii) a, b 不全为0 $\therefore$ $\gcd(a, b) \in \mathbb{Z}_{\geqslant 1}$ $\because$ a, b, c 不全为0 $\therefore$ $\gcd(a, b, c) \in \mathbb{Z}_{\geqslant 1}$

$\because$ $\gcd(a, b, c) \mid a$ 且 $\gcd(a, b, c) \mid b$ $\therefore$ $\gcd(a, b, c) \mid \gcd(a, b)$

$\therefore$ $|\gcd(a, b, c)| \leqslant |\gcd(a, b)|$ $\therefore$ $\gcd(a, b, c) \leqslant \gcd(a, b)$ $\square$

问题：对$\forall a,b,c\in\mathbb{Z}$，探究 $\operatorname{lcm}(a,b,c)$ 与 $\operatorname{lcm}(a,b)$ 的大小关系.

Proof：如果 a,b 中有一个或两个为0，则 $\operatorname{lcm}(a,b)=0$，$\operatorname{lcm}(a,b,c)=0$.

此时 $\operatorname{lcm}(a,b,c)=\operatorname{lcm}(a,b)$.

如果 a,b 全不为0，则再分两种情况讨论：

(i) $c=0$. 此时 $a\neq0$，$b\neq0$，$c=0$. 此时 $\operatorname{lcm}(a,b,c)=0$，$\operatorname{lcm}(a,b)\in\mathbb{Z}_{\geq1}$

此时 $\operatorname{lcm}(a,b,c)<\operatorname{lcm}(a,b)$

(ii) $c\neq0$. 此时 $a\neq0$，$b\neq0$，$c\neq0$. $\therefore\operatorname{lcm}(a,b,c)\in\mathbb{Z}_{\geq1}$，$\operatorname{lcm}(a,b)\in\mathbb{Z}_{\geq1}$

$\because\operatorname{lcm}(a,b,c)\in\mathbb{Z}_{\geq1}$，$a\mid\operatorname{lcm}(a,b,c)$，$b\mid\operatorname{lcm}(a,b,c)$

$\therefore\operatorname{lcm}(a,b)\leq\operatorname{lcm}(a,b,c)$ $\quad\therefore\operatorname{lcm}(a,b,c)\geq\operatorname{lcm}(a,b)$ $\quad\square$