一、整数的算数.

$a \mid b$: $\exists m \in \mathbb{Z}$, $b = am$.

$a, b \in \mathbb{Z}^+$, $d = gcd(a,b)$: ① d 是 a, b 的公因子;

② $\forall c \in \mathbb{Z}$, 若 c 是 a, b 的公因子, 则 $c \mid d$.

最大公因子的等价刻画: 设 $d \in \mathbb{Z}^+$

命题1. 若 ① d 是 a, b 的公因子

② $\exists u, v \in \mathbb{Z}$, $ua + vb = d$,

则 $d = gcd(a,b)$.

证: 首先 d 是 a, b 的公因子. 设 $c \mid a$ 且 $c \mid b$. 则 $c \mid ua + vb$. 即 $c \mid d$.

所以 $d = gcd(a,b)$.

命题2. 若 ① $\exists a_1, b_1 \in \mathbb{Z}$, 使得 $da_1 = a$, $db_1 = b$.

② $gcd(a_1, b_1) = 1$.

则 $d = gcd(a,b)$

证明: 首先 d 是 a, b 的公因子. 又因为 $gcd(a_1, b_1) = 1$, 则存在 $u, v \in \mathbb{Z}$,

$$ua_1 + vb_1 = 1,$$

所以 $ua_1 d + vb_1 d = 1$, 由命题1可知, $d = gcd(a,b)$.

命题3 设 $a = p_1^{n_1} \cdots p_s^{n_s}$, $b = q_1^{m_1} \cdots q_t^{m_t}$, ($p_i, q_i$ 为素数) 分别为 a, b 的素因子分解. 若 a, b 有相同素因子, 不妨设 $p_i = q_i$, $i = 1, \cdots, l$. 且 a 的其它素因子与 b 不同, 则

$$gcd(a,b) = p_1^{\min\{n_1, m_1\}} \cdots p_l^{\min\{n_l, m_l\}}.$$

习题5 设 $a_1, \cdots, a_n \in \mathbb{Z}^+$，则

(1) $\gcd(a_1, \cdots, a_n) = \gcd(\gcd(a_1, \cdots, a_{n-1}), a_n)$

(2) $\exists u_1, \cdots, u_n \in \mathbb{Z}$，使得

$$u_1 a_1 + \cdots + u_n a_n = \gcd(a_1, \cdots, a_n), \quad n \geq 2.$$

证明：

(1) 设 $\gcd(a_1, \cdots, a_n) = g$，则 $g \mid a_i$，$i = 1, \cdots, n$，所以 g 是 $a_1, \cdots, a_{n-1}$ 的公因子，则 $g \mid \gcd(a_1, \cdots, a_{n-1})$. 则 g 是 $\gcd(a_1, \cdots, a_{n-1})$ 的公因子. 设 h 是 $\gcd(a_1, \cdots, a_{n-1})$ 和 a_n 的公因子，则

$$h \mid \gcd(a_1, \cdots, a_{n-1}), \quad h \mid a_n$$

由 $h \mid \gcd(a_1, \cdots, a_{n-1})$ 可得 h 是 $a_1, \cdots, a_{n-1}$ 的公因子，则 h 是 $a_1, \cdots, a_{n-1}, a_n$ 的公因子，因为 g 是 $a_1, \cdots, a_n$ 的最大公因子，所以 $h \mid g$. 由定义可知

$$g = \gcd(\gcd(a_1, \cdots, a_{n-1}), a_n)$$

(2) 当 $n = 2$ 时，由扩展 Euclidean 算法可知命题成立.

假设 $n = k$ 时 ($k \geq 2$)，命题成立，

当 $n = k+1$ 时，由

$$\gcd(a_1, \cdots, a_{k+1}) = \gcd(\gcd(a_1, \cdots, a_k), a_{k+1})$$

则存在 $u, v \in \mathbb{Z}$，使得

$$u \cdot \gcd(a_1, \cdots, a_k) + v a_{k+1} = \gcd(\gcd(a_1, \cdots, a_k), a_{k+1}) = \gcd(a_1, \cdots, a_{k+1})$$

由归纳假设得 $\exists u_1', \cdots, u_k' \in \mathbb{Z}$

$$\gcd(a_1, \cdots, a_k) = u_1' a_1 + \cdots + u_k' a_k$$

所以 $\gcd(a_1, \cdots, a_{k+1}) = u(u_1' a_1 + \cdots + u_k' a_k) + v a_{k+1}$

$$= u u_1' a_1 + \cdots + u u_k' a_k + v a_{k+1}$$

令 $u_i = u u_i'$，$i = 1, \cdots, k$，$u_{k+1} = v$，则命题对于 $n = k+1$ 也成立.

□

习题4　计算 $gcd(60,35)$，u，v，$lcm(60,35)$.

解：

	$r_0 = 60$	$u_0 = 1$	$v_0 = 0$
	$r_1 = 35$	$u_1 = 0$	$v_1 = 1$
$q_2 = 1$	$r_2 = r_0 - q_2 r_1$ $= 25$	$u_2 = u_0 - q_2 u_1$ $= 1$	$v_2 = v_0 - q_2 v_1$ $= -1$
$q_3 = 1$	$r_3 = r_1 - q_3 r_2$ $= 10$	$u_3 = u_1 - q_3 u_2$ $= -1$	$v_3 = v_1 - q_3 v_2$ $= 2$
$q_4 = 2$	$r_4 = r_2 - q_4 r_3$ $= 5$	$u_4 = u_2 - q_4 u_3$ $= 3$	$v_4 = v_2 - q_4 v_3$ $= -5$
$q_5 = 2$	$r_5 = 0$		

所以 $gcd(60,35) = 5$，且

$$5 = 3 \cdot 60 + (-5) \cdot 35$$

最小公倍数为 $\frac{60 \cdot 35}{5} = 420$.

□

Warning：设 $g = gcd(a_1, a_2, a_3)$，$a_1 = a_1' d$，$a_2 = a_2' d$，$a_3 = a_3' d$，$lcm(a_1, a_2, a_3)$ 和 $a_1' a_2' a_3' d$ 一般情况下不相等

注：刚才讲的命题1，2，3对多个 a_i 也成立.

素数：　a 和 b 互素 $\Leftrightarrow gcd(a,b) = 1$ ☆ $\Leftrightarrow \exists u, v \in \mathbb{Z}$，$ua + vb = 1$

p 为素数，$p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$.

二. 线性相关与线性无关

设 $v_1, \cdots, v_k \in \mathbb{R}^n$，则

$v_1, \cdots, v_k$ 线性相关 $\Leftrightarrow$ 存在不全为0的 $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$，使得 $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$

$\Leftrightarrow$ $(v_1, \cdots, v_k)$ 为系数矩阵的齐次线性方程组为非零解.

$\Leftrightarrow$ $(v_1, \cdots, v_k)$ 化为阶梯型矩阵后非0行个数小于 k

$\Leftrightarrow$ $A = (v_1, \cdots, v_k)$，$\mathrm{rank}(A) < k$

$v_1, \cdots, v_k$ 线性无关 $\Leftrightarrow$ "若 $\alpha_1, \cdots, \alpha_k \in R$，$\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$，则 $\alpha_1 = \cdots = \alpha_k = 0$."

(例1.4, 例1.5)

习题2. (例1.10), 习题3.

例：设 $v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$，$v_2 = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$，$v_3 = \begin{pmatrix} 0 \\ 1 \\ 5 \end{pmatrix}$，判定 v_1, v_2, v_3 是否线性相关.

解：$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix}$，由 Gauss 消去法可知

$$A \to \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

于是以 A 为系数矩阵的齐次线性方程组有非平凡解.

故 v_1, v_2, v_3 线性相关.

□

习题4　证明：$v_1, v_2, v_3 \in \mathbb{R}^n$ 线性无关 $\Leftrightarrow$ $v_1+v_2, v_1+v_3, v_2+v_3$ 也线性无关.

证明：$\Rightarrow$ 设 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}^n$，$\alpha_1(v_1+v_2)+\alpha_2(v_1+v_3)+\alpha_3(v_2+v_3)=0$.

则 $(\alpha_1+\alpha_2)v_1+(\alpha_1+\alpha_3)v_2+(\alpha_2+\alpha_3)v_3=0$

因为 v_1, v_2, v_3 线性无关，所以

$$\alpha_1+\alpha_2=0,\ \alpha_1+\alpha_3=0,\ \alpha_2+\alpha_3=0,$$

得 $\alpha_1=\alpha_2=\alpha_3=0$. 所以 $v_1+v_2, v_1+v_3, v_2+v_3$ 线性无关.

$\Leftarrow$ 设 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}^n$，$\alpha_1v_1+\alpha_2v_2+\alpha_3v_3=0$.

则 $\left(\frac{\alpha_1+\alpha_2-\alpha_3}{2}\right)(v_1+v_2)+\left(\frac{\alpha_1-\alpha_2+\alpha_3}{2}\right)(v_1+v_3)+\left(\frac{-\alpha_1+\alpha_2+\alpha_3}{2}\right)(v_2+v_3)=0$

因为 $v_1+v_2, v_1+v_3, v_2+v_3$ 线性无关，所以

$$\frac{\alpha_1+\alpha_2-\alpha_3}{2}=\frac{\alpha_1-\alpha_2+\alpha_3}{2}=\frac{-\alpha_1+\alpha_2+\alpha_3}{2}=0.$$

得 $\alpha_1, \alpha_2, \alpha_3=0$，所以 v_1, v_2, v_3 线性无关.

□

$\Leftarrow$ 因为 $v_1+v_2, v_1+v_3, v_2+v_3$ 线性无关，所以任意 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$，

$$\alpha_1(v_1+v_2)+\alpha_2(v_1+v_3)+\alpha_3(v_2+v_3)=0$$

可以推出 $\alpha_1=\alpha_2=\alpha_3=0$，则

$$(\alpha_1+\alpha_2)v_1+(\alpha_1+\alpha_3)v_2+(\alpha_2+\alpha_3)v_3=0$$

可以推出 $\alpha_1+\alpha_2=\alpha_1+\alpha_3=\alpha_2+\alpha_3=0$. 又因为 $\forall \beta_1, \beta_2, \beta_3 \in \mathbb{R}$

$$\begin{aligned}\alpha_1+\alpha_2 &= \beta_1\\ \alpha_1+\alpha_3 &= \beta_2\\ \alpha_2+\alpha_3 &= \beta_3\end{aligned}$$

有解. 所以 $\forall \beta_1, \beta_2, \beta_3 \in \mathbb{R}$，若

$$\beta_1v_1+\beta_2v_2+\beta_3v_3=0,$$

存在 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$，使得 $\alpha_1+\alpha_2=\beta_1$，$\alpha_1+\alpha_3=\beta_2$，$\alpha_2+\alpha_3=\beta_3$，则

$$(\alpha_1+\alpha_2)v_1+(\alpha_1+\alpha_3)v_2+(\alpha_2+\alpha_3)v_3=0 \Rightarrow \beta_1=\beta_2=\beta_3=0$$

所以 v_1, v_2, v_3 线性无关.

□

如果是反证法，需要说明前面系数不全为0.

关于线性表出和线性相关的一些命题：

1. 若 $v_1, \cdots, v_k$ 线性无关，$v, v_1, \cdots, v_k$ 线性相关，则 v 可以被 $v_1, \cdots, v_k$ 唯一线性表出.

2. $v_1, \cdots, v_k$ 线性无关 $\Leftrightarrow$ 任意 $\{v_{i_1}, \cdots, v_{i_k}\} \subset \{v_1, \cdots, v_k\}$. $v_{i_1}, \cdots, v_{i_k}$ 线性无关.

3. $v_1, \cdots, v_k$ 线性相关 $\Leftrightarrow$ 存在 $\{v_{i_1}, \cdots, v_{i_k}\} \subset \{v_1, \cdots, v_k\}$ $v_{i_1}, \cdots, v_{i_k}$ 线性相关.

4. 若 $v_1, \cdots, v_k$ 线性无关，v 不可以被 $v_1, \cdots, v_k$ 线性表出，则 $v_1, \cdots, v_k, v$ 线性无关.

5. 若 $v_1, \cdots, v_k$ 的每一个 v_i 都不能被前 $i-1$ 个向量线性表出，则 $v_1, \cdots, v_k$ 线性无关.

6. 若 $w_1, \cdots, w_l$ 可以被 $v_1, \cdots, v_k$ 线性表出，$k < l$，则 $w_1, \cdots, w_l$ 线性相关. (引理1.13)

7. 若 $v_1, \cdots, v_m \in \mathbb{R}^n$，$m > n$，则 $v_1, \cdots, v_m$ 线性相关.

8. 若 $v_1, \cdots, v_k$ 线性无关，$w_1, \cdots, w_l$ 线性无关，而且 $v_1, \cdots, v_k$ 和 $w_1, \cdots, w_l$ 可以相互线性表出，则 $k = l$.