Linear Combination of Integers.

i.e. $ax+by=d$ has int. sol^{n} x,y. (解就是 x,y)

1. L.C. of Int. : We say that d is a lin. comb. of the integers a and b if there exist integers x and y s.t. $ax+by=d$.

1). Lemma 0: For any $a,b \in \mathbb{Z}$, $\exists x,y \in \mathbb{Z}$, s.t. $\gcd(a,b)=ax+by$.
($\gcd(a,b)$ is lin. comb. of themselves).

→ Extended Euclid Theorem:

① Input: (a,b).

② Output: (x,y,d) where $ax+by=d$, $\gcd(a,b)=d$.

e.g. Find $d=\gcd(1239,735)$. and integer x,y s.t. $1239x+735y=d$.

① Use GCDWR.

$\gcd(1239,735)$.
$=\gcd(735,504)$.
$=\gcd(504,231)$.
$=\gcd(231,42)$.
$=\gcd(42,21)$.
$=21$.

$1239=1\times735+504$.
$735=1\times504+231$.
$504=2\times231+42$.
$231=5\times42+21$.
$42=2\times21$.

② Solve. $1239x+735y=21$.

Starting from the next to last equation. substitute.

$21=231-5\times42$.
$=231-5\times(504-2\times231)$.
$=-5\times504+11\times231$.
$=-5\times504+11\times(735-504)$
$=11\times735-16\times504$.
$=11\times735-16\times(1239-735)$.
$=-16\times1239+27\times735$.

$\therefore x=-16,\ y=27$.

2. Linear Diophantine Equation: an equation of the form $ax+by=c$, where $a,b,c \in \mathbb{Z}$ and we seek sol^{n} (x,y) with $x,y \in \mathbb{Z}$.

1) Thm. 7.2.8: The Diophantine Equation $ax+by=c$ with $a,b,c \in \mathbb{Z}$, has integer sol^{n} iff $\gcd(a,b)$ divides c.

proof: Let $\gcd(a,b)=d$.

① Assume $ax+by=c$ has integer solution

WTS: $d \mid c$.

Since $d=\gcd(a,b)$ gives $d \mid a \wedge d \mid b$, which $\exists k_1, k_2 \in \mathbb{Z}$, $dk_1=a$, $dk_2=b$, gives

$$dk_1x+dk_2y=c$$

$$\Rightarrow d(k_1x+k_2y)=c \text{, which } d \mid c$$

② Assume $d \mid c$.

WTS: $ax+by=c$ has integer sol^{n}.

Since $d \mid c$ gives $\exists k \in \mathbb{Z}$ s.t. $dk=c$.

Since $d=\gcd(a,b)$, from Lemma 0, gives $\exists x^*, y^* \in \mathbb{Z}$ s.t.

$$ax^*+by^*=d$$

$$\Rightarrow kax^*+kby^*=dk=c.$$

Since $k, x^*, y^* \in \mathbb{Z}$, $\exists x=kx^*$, $y=ky^*$, s.t.

$ax+by=c$ has int. sol^{n}.

3. General sol^{n} of L.D.E:

Let $\gcd(a,b)=d$. The L.D.E. $ax+by=c$ has sol^{n} iff $d \mid c$. If $d \mid c$ and (x_0,y_0) is a sol^{n}, then the integral sol^{n} of the equation are all the pairs $(x_0+m\frac{b}{d}, y_0-m\frac{a}{d})$, where m assumes all int. values. ↘有无数解.

proof: ① $(x_0+m\frac{b}{d}, y_0-m\frac{a}{d})$ is sol^{n} of L.D.E. for any $m \in \mathbb{Z}$.

Assume (x_0,y_0) is a sol^{n} of L.D.E., i.e. $ax_0+by_0=c$.

Substitute gives $a(x_0+\frac{b}{d}m)+b(y_0-\frac{a}{d}m)=c$.

$$\Rightarrow ax_0 + \frac{ba}{d}m + by_0 - \frac{ab}{d}m = c.$$

$$\Rightarrow ax_0 + by_0 = c.$$

② No other solutions.

Assume (x_0^*, y_0^*) is other sol^n than (x_0, y_0) to $ax_0+by_0=c$.

$$\begin{cases} ax_0 + by_0 = c. & ① \\ ax_0^* + by_0^* = c. & ② \end{cases} \xrightarrow{① - ②} a(x_0 - x_0^*) + b(y_0 - y_0^*) = 0.$$

$$\Rightarrow \quad a(x_0 - x_0^*) = b(y_0^* - y_0)$$

$$\Rightarrow \quad \frac{a}{d}(x_0 - x_0^*) = \frac{b}{d}(y_0^* - y_0).$$

Since $\gcd(a,b) = d$, gives $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, gives

1. $\frac{a}{d} \mid y_0^* - y_0$. $\exists m \in \mathbb{Z}$ s.t.
$\Rightarrow \frac{a}{d} m = y_0^* - y_0$.
$\Rightarrow y_0^* = \frac{a}{d}m + y_0$.

2. $\frac{b}{d} \mid x_0 - x_0^*$. $\exists m \in \mathbb{Z}$ s.t.
$\Rightarrow \frac{b}{d} \cdot m = x_0 - x_0^*$
$\Rightarrow x_0^* = x_0 - \frac{b}{d}m$.

Since $m \in \mathbb{Z}$, they has the same form as expected. ■