

Def. Let a and b be two integers.

The **least common multiple** of a and b is a natural number $l \in \mathbb{N}$ satisfying the following properties:

- i) l is a common multiple of a and b , i.e. $a|l$, $b|l$
- ii) If m is a common multiple of a and b , then $l|m$

Notation: $\text{LCM}(a, b)$.

Rmk The properties i) & ii) together are called the **defining property** or the **universal property** of the notion 'the least common multiple of a and b '

Prop (uniqueness of LCM)

There is at most **ONE** natural number $l \in \mathbb{N}$ satisfying i) & ii).

Proof: Suppose l & l' are LCM of a and b .

By i), we have $a \mid l$, $b \mid l$, $a \mid l'$, $b \mid l'$.

By ii), we have $l \mid l'$ and $l' \mid l$.

By Antisymmetric property of \mid , $l = l'$.



Implement of GCD & LCM

Input: a & b two integers.

GCD(a, b):

by Euclidean Algorithm

LCM(a, b):

$$\text{by } \text{LCM}(a, b) = \frac{ab}{\text{GCD}(a, b)} = a \cdot \frac{b}{\text{GCD}(a, b)} = b \cdot \frac{a}{\text{GCD}(a, b)}$$

m be any common multiple of a & b , $a \mid m$, $b \mid m$

$$(m = az = by) \cdot \frac{\text{GCD}(a, b)}{1} = \frac{by}{1} + \frac{ax}{1} \Rightarrow \frac{ab}{\text{GCD}(a, b)} \mid m$$
$$m \cdot (az + bw) = m \cdot az + m \cdot bw$$

Solutions of homogenous equation $ax + by = 0$.

a) $(0,0)$ is an integer solution.

b) If (x,y) and (x',y') are two integer solutions, then $(x+x', y+y')$ is also an integer solution.

c) If (x,y) is an integer solution, then so is (mx, my) for any $m \in \mathbb{Z}$.

d) There is an solution $(x_0, y_0) \in \mathbb{Z}^2$ s.t.

$$\{(x,y) \in \mathbb{Z}^2 \mid ax + by = 0\} = \mathbb{Z} \cdot (x_0, y_0)$$

Indeed, the solution set is totally ordered according to first components

$$(x,y) \prec (x',y') \Leftrightarrow x < x'$$

and (x_0, y_0) can be taken to be the smallest positive one
(or the largest negative one)

Exercise:
Why this is NOT
an order on the
entire \mathbb{Z}^2 .

Theorem (General Solutions of the **homogenous** linear Diophantine equation
 $ax + by = 0$)

$$\{(x, y) \in \mathbb{Z}^2 \mid ax + by = 0\} = \mathbb{Z} \cdot \left(\frac{l}{a}, -\frac{l}{b} \right)$$

where $l = \text{LCM}(a, b)$

That is to say,

any integer solution of $ax + by = 0$ is a multiple of

$$\left(\frac{\text{LCM}(a, b)}{a}, -\frac{\text{LCM}(a, b)}{b} \right)$$

Proof: We may assume $a > 0$.

All we need to show is that $(\frac{l}{a}, -\frac{l}{b})$ is the smallest positive element in the solution set.

If (x, y) is a positive integer solution, then

$$ax = b \cdot (-y)$$

is a common multiple of a & b . Therefore $l \mid ax$ (by (ii) of LCM)

Then $l \leq ax$, and hence $\frac{l}{a} \leq x$.

But $(\frac{l}{a}, -\frac{l}{b})$ is a positive integer solution!

hence it is the smallest positive element in the solution set.



Theorem (General solutions of $ax + by = c$)

1) If $\text{GCD}(a, b) \nmid c$, then there is no integer solution.

2) If $\text{GCD}(a, b) \mid c$, then the Euclidean Algorithm gives one particular integer solution of $ax + by = \text{GCD}(a, b)$ say (x_0, y_0) . Then $(\frac{c \cdot x_0}{\text{GCD}(a, b)}, \frac{c \cdot y_0}{\text{GCD}(a, b)})$ is an integer solution of $ax + by = c$. Denote it by (x'_0, y'_0) .

$$ax'_0 + by'_0 = c \quad (\text{Bézout's Identity})$$

3) The general integer solutions can be written as

$$\begin{cases} x = x'_0 + m \cdot \frac{\text{LCM}(a, b)}{a} \\ y = y'_0 + m \cdot \left(-\frac{\text{LCM}(a, b)}{b} \right) \end{cases} \quad (m \in \mathbb{Z})$$

Quiz 3

The following shows the implementation of the Euclidean Algorithm for (36, 21)

$$1) \quad 36 = 1 \cdot 21 + 15$$

$$2) \quad 21 = 1 \cdot 15 + 6$$

$$3) \quad 15 = 2 \cdot 6 + 3$$

$$4) \quad 6 = 2 \cdot 3 + \underline{0} \text{ Halt!}$$

Question: Using above to find ALL integer solution of

$$36x + 21y = 9$$

Solution to Quiz 3 :

$$1) \quad 36 = 1 \cdot 21 + 15$$

$$2) \quad 21 = 1 \cdot 15 + 6$$

$$3) \quad 15 = 2 \cdot 6 + 3$$

$$4) \quad 6 = 2 \cdot 3 + \underline{0} \text{ Halt!}$$

$$3 \stackrel{(3)}{=} 15 - 2 \cdot 6$$

$$\stackrel{(2)}{=} 15 - 2 \cdot (21 - 1 \cdot 15)$$

$$= -2 \cdot 21 + 3 \cdot 15$$

$$\stackrel{(1)}{=} -2 \cdot 21 + 3 \cdot (36 - 1 \cdot 21)$$

$$= 3 \cdot 36 - 5 \cdot 21$$

Since $9 = 3 \cdot 3$, we obtain an integer solution

$$\begin{cases} x = 3 \cdot 3 = 9 \\ y = 3 \cdot (-5) = -15 \end{cases}$$

To give ALL integer solutions,

first compute $\text{LCM}(36, 21)$

$$= 36 \cdot 21 / \text{gcd}(36, 21) = \frac{36 \cdot 21}{3} = 252$$

Then the general solution of $36x + 21y = 9$ is

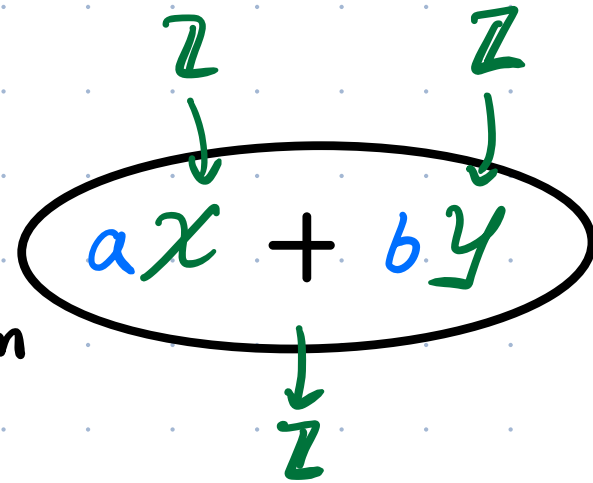
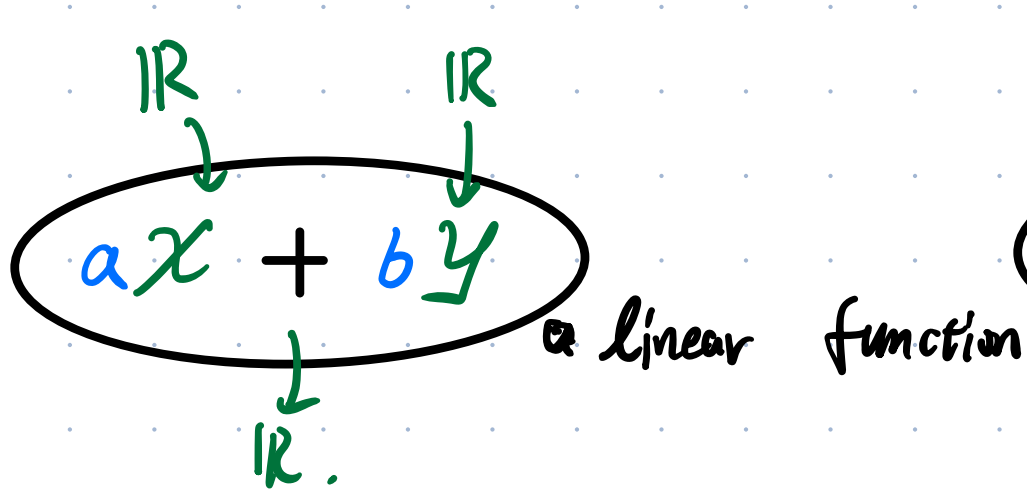
$$\begin{cases} x = 9 + m \cdot \frac{252}{36} = 9 + m \cdot 7 \\ y = -15 + m \cdot \left(-\frac{252}{21}\right) = -15 - m \cdot 12 \end{cases}$$

$(m \in \mathbb{Z})$

* Optional

Let a & b be two integers. Consider the expression

$$ax + by$$



Range? either \mathbb{R} (if $(a,b) \neq (0,0)$)
or 0 (if $a,b=0$)

$$\text{Null? } \{ (x,y) \in \mathbb{R}^2 \mid ax + by = 0 \}$$

one dimensional (if $(a,b) \neq (0,0)$)
two dimensional (if $a,b=0$)

General Solutions of $ax + by = c$
 $(x_0, y_0) + \text{Null}(ax + by).$

either $\mathbb{Z} \cdot \text{GCD}(a,b)$ (if $(a,b) \neq (0,0)$)
or 0 ($a,b=0$)

$$\{ (x,y) \in \mathbb{Z}^2 \mid ax + by = 0 \}$$

$$= \mathbb{Z} \cdot \left(\frac{d}{a}, -\frac{d}{b} \right) \quad (\text{if } a \neq 0, b \neq 0)$$

$$(x_0, y_0) + \mathbb{Z} \cdot \left(\frac{d}{a}, -\frac{d}{b} \right)$$

Reading Suggestions

- The analogy and difference between **solving linear equations** (in Linear Algebra course) and **solving linear Diophantine equations** (in Number Theory course) worth thinking.
- In the study of solutions of homogeneous Diophantine equation $ax + by = 0$, we **define** a total order (**total** means any two elements can be compared) on the solution set.
 1. The totalness says that the elements form a line according to the order, and the null element $(0, 0)$ plays the role of the origin.
 2. Then we pick up the **smallest positive element**. This certainly relies on a special property of the set \mathbb{N} of natural numbers: the **Least Element Principle**, which says that any nonempty set of natural numbers has a smallest element.
 3. But we are talking about the solution set, but the set \mathbb{N} itself, so how are they related? The reason is: the solution set equipped with the total order and the origin $(0, 0)$ form a mathematical structure which is **isomorphic** to the set \mathbb{Z} equipped with its natural order and the origin 0. Then the non-negative elements are corresponding to the natural numbers.
- Next week, we will study **prime numbers** and **prime factorization**. As a preliminary, please read the last part of Chapter 0, on **Hasse diagram**. Then read Chapter 2 for the next week.