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. $a \mid l$, $b \mid l$

ii) If m is a common multiple of a and b, then $l \mid m$

Notation: $LCM(a, b)$.

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 $\mid$, $l = l'$.

$\blacksquare$

Implement of GCD & LCM

Input: a & b two integers.

$GCD(a, b)$:

by Euclidean Algorithm

$LCM(a, b)$:

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

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

$(m = ax = by) \cdot \underbrace{GCD(a,b)}_{\parallel}$

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

Solutions of homogenious 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

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

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

Exercice: 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 $l = LCM(a, b)$

That is to say,

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

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

Proof: We may assume $a > 0$.

All we need to show is that $\left(\frac{l}{a}, -\frac{l}{b}\right)$ 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 $\left(\frac{l}{a}, -\frac{l}{b}\right)$ is a positive integer solution!

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

$\square$

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

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

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

$$a x_0' + b y_0' = c \quad \text{(Bézout's Identity)}$$

3) The general integer solutions can be written as

$$\begin{cases} x = x_0' + m \cdot \dfrac{LCM(a, b)}{a} \\ y = y_0' + m \cdot \left(- \dfrac{LCM(a, b)}{b} \right) \end{cases} \quad (m \in \mathbb{Z})$$

Quiz 3

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

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

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

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

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

Question: Using above to find ALL integer solution of

$$36x + 21y = 9$$

Solution to Quiz 3 :

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

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

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

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

$$
\begin{aligned}
3 &\overset{(3)}{=} 15 - 2 \cdot 6 \\
&\overset{(2)}{=} 15 - 2 \cdot (21 - 1 \cdot 15) \\
&= -2 \cdot 21 + 3 \cdot 15 \\
&\overset{(1)}{=} -2 \cdot 21 + 3 \cdot (36 - 1 \cdot 21) \\
&= 3 \cdot 36 - 5 \cdot 21
\end{aligned}
$$

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 LCM(36, 21)

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

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

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

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

$\overline{\ast}$ Optional

Let a & b be two integers. Consider the expression

$$ax + by$$

$\mathbb{R}$ $\mathbb{R}$

$$ax + by$$

$\mathbb{R}$.

a linear function

$\mathbb{Z}$ $\mathbb{Z}$

$$ax + by$$

$\mathbb{Z}$

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

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

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

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

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

General Solutions of $ax+by=c$

$(x_0,y_0) +$ Null$(ax+by)$.

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

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.