Quiz :

Determine if the following equation has an integer solution or not .

$$42x + 78y = 9$$

$$\left.\begin{aligned} 78 &= 1\cdot 42 + 36 \\ 42 &= 1\cdot 36 + 6 \\ 36 &= 6\cdot 6 + 0 \end{aligned}\right\} \quad GCD(78, 42) = 6$$

$6 \nmid 9 \Rightarrow$ No integer solution!

Theorem.

Let a, b & c be integers. The equation $ax + by = c$ has an integer solution iff c is a multiple of $GCD(a, b)$

Q: Find ALL the integer solutions of $ax + by = c$.

Suppose (x_0, y_0) is an integer solution, i.e.

$$ax_0 + by_0 = c \qquad \text{(Eq. 0)}$$

Suppose (x_1, y_1) is another integer solution, i.e.

$$ax_1 + by_1 = c \qquad \text{(Eq. 1)}$$

Then substract (Eq 0) from (Eq 1) gives

$$a(x_1 - x_0) + b(y_1 - y_0) = 0$$

Hence $(x_1 - x_0, y_1 - y_0)$ is an integer solution of the homogenious equation.

$$ax + by = 0$$

Lemma: Suppose (x_0, y_0) is an integer soluttion of $ax + by = c$.

Then we have

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

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

$$\{(x_0, y_0) + (x',y') \mid \cdots\}$$

That is to say:

any integer solution (x,y) of $ax + by = c$ can be written as

$(x_0, y_0) + (x', y')$ uniquely,

where (x',y') is an integer solution of $ax + by = 0$. Vice versa.

Proof: Exerice.

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

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

$$a\cdot 0+b\cdot 0=0.$$

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

$$\left.\begin{aligned} ax+by&=0 \\ ax'+by'&=0 \end{aligned}\right\} \Rightarrow a(x+x')+b(y+y')=0$$

In other words, $\{(x,y)\in\mathbb{Z}^2 \mid ax+by=0\}$ is an Abelian group.

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

$$ax+by=0 \Rightarrow amx+bmy=0$$

In other words, $\{(x,y)\in\mathbb{Z}^2 \mid ax+by=0\}$ is a $\mathbb{Z}$-module.

Def. of Abelian group

Optional

An **Abelian group** is a triple $(A, \oplus, 0)$ where A is a set, $\oplus$ is a binary operator $\oplus : A \times A \longrightarrow A$, and 0 is an element of A.

Axioms: (identity) $\forall a \in A, \; a \oplus 0 = 0 \oplus a = a$

(associativity) $\forall a, b, c \in A. \; (a \oplus b) \oplus c = a \oplus (b \oplus c)$

(commutativity) $\forall a, b \in A. \; a \oplus b = b \oplus a$

Example: 1) $(\mathbb{Z}, +, 0)$ 2) $(\mathbb{Z}^2, +, (0,0))$.

Def. of $\mathbb{Z}$-module

An **$\mathbb{Z}$-module** is an abelian group A with an action of $\mathbb{Z}$

$$\rho : \mathbb{Z} \times A \longrightarrow A$$

Axioms: (nullity) $\forall a \in A. \; \rho(0, a) = 0$

(identity) $\forall a \in A, \; \rho(1, a) = a$

(associtivity) $\forall a \in A, m, n \in \mathbb{Z}. \; \rho(m, \rho(n, a)) = \rho(mn, a)$

Example: 1) $(\mathbb{Z}, \times)$ 2) $(\mathbb{Z}^2, \rho)$ $\rho(m, (x, y)) = (mx, my)$

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

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

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.

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

Pf: If (x,y) is an integer solution, then $ax = b \cdot (-y)$. So the set $\{(x,y) \in \mathbb{Z}^2 \mid ax + by = 0\}$ is totally ordered according to x.

$$\text{"}(x,y) \propto (x',y')\text{"} \Longleftrightarrow x < x'$$

Let $(x_0, y_0) \in \{(x,y) \in \mathbb{Z}^2 \mid ax + by = 0\}$ be the smallest positive one.

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

" $\supset$ " is (c)

" $\subset$ ": Suppose $(x', y') \in \{(x,y) \in \mathbb{Z}^2 \mid ax + by = 0\}$ but

$(x', y') \notin \mathbb{Z} \cdot (x_0, y_0)$.

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

$\cdot\cdot)$ There is a positive one in $(x', y') + \mathbb{Z}(x_0, y_0)$ which is less than (x_0, y_0)

$x' + m_0 x_0$ smallest positive

$x' + (m_0 - 1) x_0 < 0$

$\Rightarrow x' + m_0 x_0 < x_0$

$(x', y') + m_0 (x_0, y_0)$ smallest.

$(x', y') + (m_0 - 1)(x_0, y_0) \prec (0, 0) \Rightarrow (x', y') + m_0 (x_0, y_0) \prec (x_0, y_0)$

$\Rightarrow\!\!\!\!\!\times$ $\boxtimes$

Rmk: (x_0, y_0) is Not unique. Indeed, $\pm(x_0, y_0)$ works.

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 <u>Antisymmetric</u> property of $\mid$, $l = l'$.

$\boxtimes$

Solutions of homogenious 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 $l = LCM(a,b)$

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

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

We may assume $a>0$

Proof: If (x,y) is an integer solution, then $ax = b\cdot(-y)$ is a common multiple of a & b.

Therefore $l \mid a\cdot x$ (by (ii) of LCM). Then $l \leqslant a|x|$, and hence $\frac{l}{a} \leq |x|$.

But $\left(\frac{l}{a}, -\frac{l}{b}\right)$ is an integer solution of $ax+by=0$. Hence

$\left(\frac{l}{a}, -\frac{l}{b}\right)$ is the smallest positive one in the solution set.

After-class Readings.

- Today's topic: the **LCM** and the **solution set** of the **homogeneous** linear Diophantine equation $ax + by = 0$.
  - For **LCM**: compare with GCD on their defining properties and proofs.
  - For **solution set**: note that how we deduce its properties and how we use them to give a concrete description. The main idea is that the solution set of the homogeneous linear Diophantine equation $ax + by = 0$ is a **free $\mathbb{Z}$-module of rank one**, namely
    1. it contains a null element $(0, 0)$;
    2. it is equipped with an associative commutative addition operation;
    3. it is equipped with an action of $\mathbb{Z}$, namely multiplied by an integer;
    4. it is exactly all the multiple of one specific element.

    Please compare this with the following fact from linear algebra:

    > The set of real solutions of the homogeneous linear equation $ax + by = 0$ is a one-dimensional real vector space.
  - In the proof, we essentially use the fact that we can **totally order** the solution set. Note that, **order** means the relation $\preceq$ is **reflexive**, **antisymmetric**, and **transitive**; **total** means any two elements can be compared.
- I encourage you to read the rest of Chapter 1 preparing for our next meeting.