Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 13, 2023

What we have shown last time

Question (Binary linear Diophantine equation)

Given integers a, b, c, find integers x, y such that

$$a \cdot x + b \cdot y = c.$$

- First, the Diophantine equation

  $$a \cdot x + b \cdot y = c$$

  has a solution (in $\mathbb{Z}$) if and only if c is a multiple of $\gcd(a, b)$.
- If this is the case, the ***Bézout's identity*** gives a pair of integers (x_0, y_0) such that $ax_0 + by_0 = \gcd(a, b)$. Suppose $c = m \gcd(a, b)$. Then (mx_0, my_0) is a solution of our Diophantine equation.

Today's topics

- Homogeneous linear equation
- Least common multiple
- Solution set of the linear Diophantine equation

Homogeneous linear equations

Homogeneous linear equations

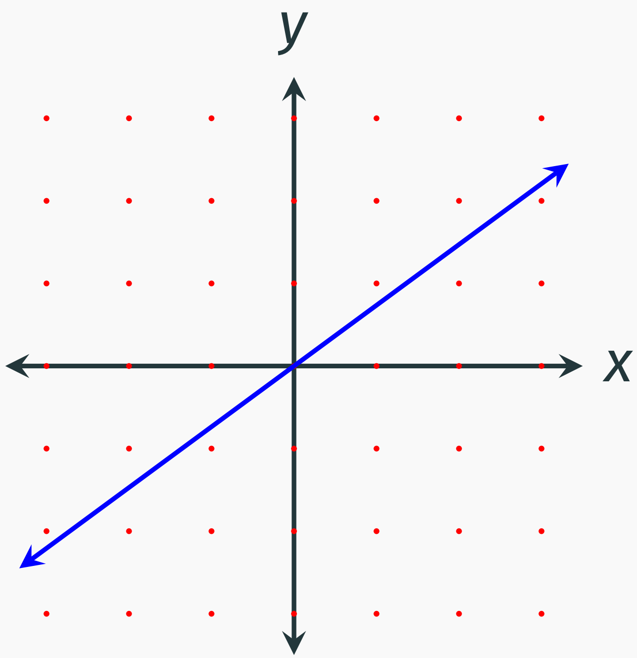
We first consider the case $c = 0$. We say the following equation is ***homogeneous***:

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

Before we move to the integer solutions, let's consider the set

$$\{(x, y) \in \mathbb{R}^2 \mid a \cdot x + b \cdot y = 0\}.$$

Geometrically, it is a line in the plane. Find the integer solutions = find the integer points on the line.



Homogeneous linear equations

By linear algebra, we can parameterize the line:

$(\frac{1}{a}, -\frac{1}{b})$ a vector repns the line.

$$\{(x, y) \in \mathbb{R}^2 \mid a \cdot x + b \cdot y = 0\} = \{(\tfrac{1}{a}t, -\tfrac{1}{b}t) \mid t \in \mathbb{R}\}.$$

Now, the problem becomes:

For which t, the pair $(\frac{1}{a}t, -\frac{1}{b}t)$ is a pair of integers?

$\frac{1}{a}t = x \iff t = ax$

1. t has to be an integer.
2. We then must have $a \mid t$ and $b \mid t$.
3. Namely, t has to be a common multiple of a, b.

Answer!

Least common multiple

Least common multiple

Definition 3.1 (Least common multiple)

Let a, b be two nonzero integers. Then a positive integer l is called a ***least common multiple*** of a and b if it satisfies the following two ***defining properties***:

1. $a \mid l$ and $b \mid l$, i.e. l is a common multiple of a and b; and
2. if m is any common multiple of a and b, then $l \mid m$.

$l \mid l'$ & $l' \mid l \Rightarrow l = l'$

For a given pair (a, b), the least common multiple is unique, we use $\operatorname{lcm}(a, b)$ to denote it. In particular, we use $\operatorname{lcm}(a, b) = l$ to mean the least common multiple exists and equals to l.

Theorem 3.2

For any integers a, b, we have $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$.

Proof. Let l be the right-hand. We need to verify it satisfies the two defining properties. $l = \frac{ab}{\gcd(a,b)}$

1. Since $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are integers, we have $b \mid l$ and $a \mid l$.
2. Suppose m is a common multiple of a and b. By ***Bézout's identity***, we can find integers x, y such that $ax + by = \gcd(a,b)$. Then we have $m \cdot \gcd(a,b) = \underset{\bar{b}}{m}ax + \underset{\bar{a}}{m}by$. Note that ab divides the right-hand side. Hence, we must have $l \mid m$. $\square$

Solution set of homogeneous linear Diophantine equation

Theorem 3.3

Let a, b be two nonzero integers. Then the solution set of the homogeneous linear Diophantine equation

$$a \cdot x + b \cdot y = 0$$

can be parameterized as

$$\left\{ \left(\frac{\operatorname{lcm}(a,b)}{a} t, -\frac{\operatorname{lcm}(a,b)}{b} t \right) \,\middle|\, t \in \mathbb{Z} \right\}.$$

Proof. This is because $\operatorname{lcm}(a, b)t$ ($t \in \mathbb{Z}$) are all the common multiples of a and b. $\square$

Solution set (general case)

Solution set (general case)

$$\text{``}\alpha + S\text{''} = \{\alpha + e \mid e \in S\}$$

set

Now, we back to the general case:

$$a \cdot x + b \cdot y = c.$$

Lemma 3.4

Suppose (x_1, y_1) is a solution of above Diophantine equation. Then the solution set $\left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = c\right\}$ can be expressed as

$$(x_1, y_1) + \left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = 0\right\}.$$

$$= \{(x_1, y_1) + (x, y) \mid (x, y) \in \mathbb{Z}^2 \text{ and } ax + by = 0\}$$

$$= \{(x_1 + x, y_1 + y) \mid (x, y) \in \mathbb{Z}^2 \text{ and } ax + by = 0\}$$

Solution set (general case)

Before we move to the proof, let's consider the corresponding proposition in geometry:

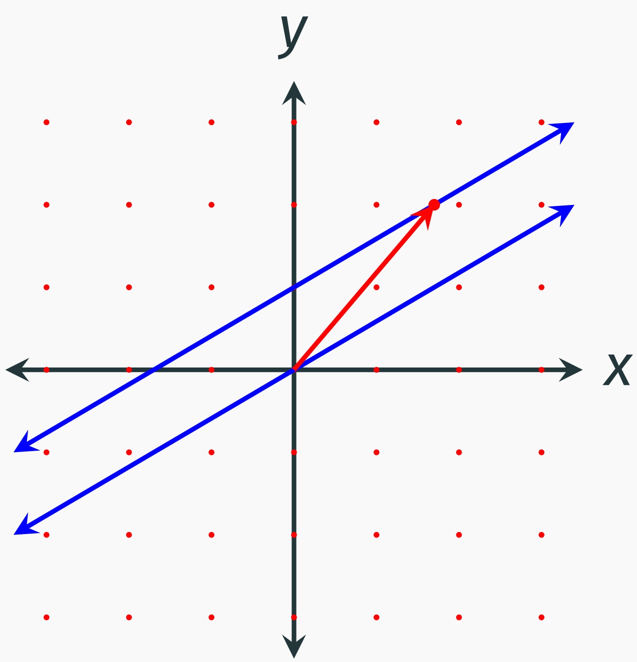
The line defined by the equation

$$a \cdot x + b \cdot y = c$$

can be obtained from the line

$$a \cdot x + b \cdot y = 0$$

by adding a vector $\langle x_1, y_1 \rangle$ from the origin to a point (x_1, y_1) on the first line.



Proof of the lemma

(x_1, y_1) is given

Suppose (x_2, y_2) is a solution of our Diophantine equation $a \cdot x + b \cdot y = c$, then we have:

Solset of "general"
$- (x_1, y_1)$
$\subseteq$ Solset of "homo"

$$a \cdot (x_1 - x_2) + b \cdot (y_1 - y_2) = 0.$$

Namely, $(x_1 - x_2, y_1 - y_2)$ is a solution of the corresponding homogeneous Diophantine equation $a \cdot x + b \cdot y = 0$.

Conversely, if (x_2, y_2) is a solution of the corresponding homogeneous Diophantine equation $a \cdot x + b \cdot y = 0$, then we have

Solset of "homo"
$+ (x_1, y_1)$
$\subseteq$ Solset of "gener"

$$a \cdot (x_1 + x_2) + b \cdot (y_1 + y_2) = c.$$

Namely, $(x_1 + x_2, y_1 + y_2)$ is a solution of our Diophantine equation $a \cdot x + b \cdot y = c$. $\square$

Solution set (general case) i

Now, we can give a general algorithm

Theorem 3.5

Given integers a, b, c, the solutions of the Diophantine equation

$$a \cdot x + b \cdot y = c$$

can be obtained through the following steps:

1. *Using division algorithm to find* $\gcd(a, b)$ *and then determine whether the Diophantine equation has an integer solution by whether* c *is a multiple of* $\gcd(a, b)$.
2. *If this is the case, the* **Bézout's identity** *gives a pair of integers* (x_0, y_0) *such that* $ax_0 + by_0 = \gcd(a, b)$. *Suppose* $c = m \gcd(a, b)$. *Then* (mx_0, my_0) *is a solution of our Diophantine equation.*

Theorem 3.5

3. *Once we have a solution* (x_1, y_1) *of our Diophantine equation, the solution set can be expressed as*[2]

$$(x_1, y_1) + \mathbb{Z}\left(\frac{\operatorname{lcm}(a,b)}{a}, -\frac{\operatorname{lcm}(a,b)}{b}\right).$$

$$= \left\{ (x_1, y_1) + t\left(\frac{\operatorname{lcm}(a,b)}{a}, -\frac{\operatorname{lcm}(a,b)}{b}\right) \;\middle|\; t \in \mathbb{Z} \right\}$$

Namely, the general solution is

$$\begin{cases} x = x_1 + \frac{\operatorname{lcm}(a,b)}{a} t \\ y = y_1 - \frac{\operatorname{lcm}(a,b)}{b} t \end{cases} \quad (t \in \mathbb{Z}).$$

Proof. The first two are proved in previous lecture, the third is the combination of theorem 3.3 and lemma 3.4. □

[2] Recall the conventions on set notations

Let's continue the example

$$\overset{a}{\underline{133}}x + \overset{b}{\underline{85}}y = 1.$$

We have seen that $\gcd(133, 85) = 1$ and that

$$133 \cdot (-23) + 85 \cdot (36) = 1.$$

Since $\gcd(133, 85) = 1$, we have $\operatorname{lcm}(133, 85) = 133 \cdot 85.$ Therefore, the general solution is (§7 3.2)

$$\begin{cases} x = -23 + 85t \\ y = 36 - 133t \end{cases} \qquad (t \in \mathbb{Z}).$$

After Class Work

After Class Work

1. So far, we have finished chapter 1 of the textbook.
2. The analogy and difference between ***solving linear equations*** (in Linear Algebra course) and ***solving linear Diophantine equations*** (in Number Theory course) worth thinking.
3. We will move to ***prime factorization***, please read chapter 2 for next week.
4. Please read the ***Hasse diagram*** part of chapter 0.
5. Please use knowledge from this week to solve HW 1.

Here we provide another approach to theorem 3.3.

Exercise 3.1

Show that the solution set $S = \left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = 0\right\}$ has the following properties:

1. $(0, 0) \in S$;
2. if both $(x_1, y_1) \in S$ and $(x_2, y_2) \in S$, then $(x_1 + x_2, y_1 + y_2) \in S$;
3. if $(x, y) \in S$ and $m \in \mathbb{Z}$, then $(mx, my) \in S$.

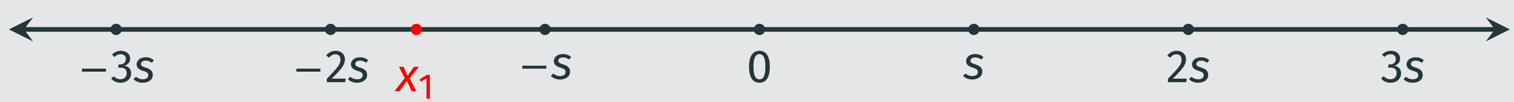
In the language of linear algebra, S is a $\mathbb{Z}$-submodule of $\mathbb{Z}^2$.

Another proof of theorem 3.3 ii

Exercise 3.2

Define a map $S \to \mathbb{N}$ as follows: $(x, y) \mapsto |x|$. Suppose $s \in \mathbb{Z}_+$ is the smallest positive integer in the image of the map and $(x_0, y_0) \in S$ is a preimage of s. Show that $S = \mathbb{Z}(x_0, y_0)$ as follows:

1. Suppose there is $(x_1, y_1) \in S$ which is not a multiple of (x_0, y_0). Show that there is an integer n such that $ns < |x_1| < (n+1)s$.



2. Show that $(x_1 - nx_0, y_1 - ny_0) \in S$ but $|x_1 - nx_0| < s$.
3. Conclude that this is a contradiction and hence $S = \mathbb{Z}(x_0, y_0)$.

Terminology

A ***group*** is a monoid $(M, *, e)$ satisfying

- (***invertibility***) for any element $a \in M$, there is an element $a^{-1} \in M$ such that $a * a^{-1} = a^{-1} * a = e$.

A monoid $(M, *, e)$ is ***abelian*** if it satisfies

- (***commutativity***) $a * b = b * a$ for all $a, b \in M$.

An ***abelian group*** is an abelian monoid which is a group.

Exercise 3.3

Determine whether the following monoids are groups/abelian: (endomaps of a set S, composition, id), $(\mathbb{N}$, multiplication, $1)$, $(\mathbb{Z}$, multiplication, $1)$, $(\mathbb{N}$, addition, $0)$, $(\mathbb{Z}$, addition, $0)$.

Terminology

A $\mathbb{Z}$***-module*** is an abelian group $(M, +, e)$ together with an action of integers $\rho\colon \mathbb{Z} \times M \longrightarrow M$ satisfying

- (***associativity***) $\rho(mn, a) = \rho(m, \rho(n, a))$ for all $m, n \in \mathbb{Z}$ and $a \in M$;
- (***neutrality***) $\rho(m, e) = e$ for all $m \in \mathbb{Z}$.

Exercise 3.4 (†)

Show that any abelian group is automatically a $\mathbb{Z}$-module. (Hint: how to define the action ρ?)

We usually write $m.e$ or me instead of $\rho(m, e)$ for simplicity.

Exercise 3.5

Fix a positive integer n and let $(M, +, 0, \rho)$ be a $\mathbb{Z}$-module. Show that the triple gives a $\mathbb{Z}$-module:

- the set is $M^n := \{(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in M\}$;
- the operation is componentwise addition:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) := (a_1 + b_1, \cdots, a_n + b_n);$$

- the neutral element is $(0, \cdots, 0)$;
- the action is componentwise multiplication:

$$\rho(m, (a_1, \cdots, a_n)) = (ma_1, \cdots, ma_n).$$

In particular, we have $\mathbb{Z}$-module structures on $\mathbb{Z}^n$, $\mathbb{R}^n$, etc.

Terminology

A subset N of a monoid $(M, *, e)$ is a ***submonoid*** if $e \in N$ and N is closed under the operation: $\forall a, b \in M : a, b \in N \implies a * b \in N$.

A subset N of a group $(M, *, e)$ is a ***subgroup*** if it is a submonoid and is closed under taking inverse: $\forall a \in M : a \in N \implies a^{-1} \in N$.

A subset N of a $\mathbb{Z}$-module $(M, +, 0, \rho)$ is a ***submodule*** if it is a subgroup and is closed under the action:

$$\forall a \in M, m \in \mathbb{Z} \colon a \in N \implies ma \in N.$$

Exercise 3.6

Show that a subset N of a $\mathbb{Z}$-module $(M, +, 0, \rho)$ is a submodule if it is a submonoid and is closed under the action.

Terminology

A $\mathbb{Z}$-module M is ***free of rank one*** if there is an element $x_0 \in M$ such that $M = \mathbb{Z}x_0$. Namely, any element of M is a multiple of x_0.

More generally, fix a natural number n, a $\mathbb{Z}$-module M is ***free of rank n*** if there are elements $x_1, \cdots, x_n \in M$ such that any element of M can be *uniquely* expressed as a $\mathbb{Z}$-linear combination of $x_1, \cdots, x_n$.

Example 3.6

- The $\mathbb{Z}$-module $\mathbb{Z}^n$ is free of rank n.
- Exercise 3.2 shows that the solution set S of $a \cdot x + b \cdot y = 0$ is free of rank one.