Homogeneous linear equations

Homogeneous linear equations

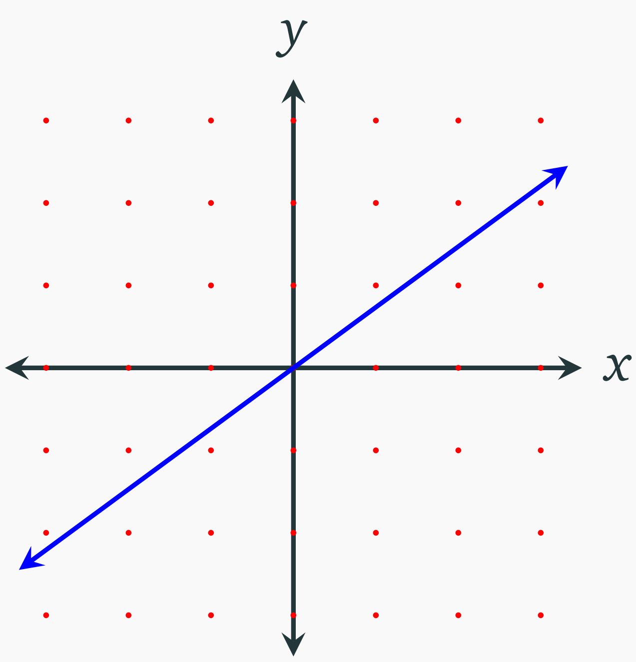
We first consider the case $c = 0$. We say the following equation is *homogeneous*:

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

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.



By linear algebra, we can parameterize the line:

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

Now, the problem becomes:

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

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.

Least common multiple

Definition 1.3.1 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 $l \mid m$.

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 1.3.2.

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

Proof. Let l be the right-hand. We need to verify it satisfies the two defining properties.

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 $l \mid m$.

$\square$

Theorem 1.3.2.

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.

1. Since $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are integers, we have $b \mid l$ and $a \mid l$.

$$l = \frac{a}{\gcd(a,b)} \cdot b = a \cdot \frac{b}{\gcd(a,b)}$$

□

Theorem 1.3.2.

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.

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 $m \cdot \gcd(a,b) = \underline{max} + \underline{mby}$. Note that ab divides the right-hand side. Hence, we must have $l \mid m$. □

$ab \mid m \cdot \gcd(a,b)$

Theorem 1.3.3.

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