# Linear Diophantine equation

## Linear Diophantine equation

**Question Binary linear Diophantine equation.**

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

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

When $c$ is the output of the division algorithm of $(a, b)$, then we can use the (Euclidean) division algorithm to find a solution $(x_0, y_0)$.

$$a x_0 + b y_0 = c$$

1. By the *2-out-of-3 principle* of divisibility of integers, if the problem has a solution $(x_0, y_0)$, then for any common divisor $d$ of $a$ and $b$, we must have $d \mid c$.
   Conversely, if $c$ is not a multiple of common divisors of $a$ and $b$, then the problem has no solution.

2. If we can find a solution $(x_0, y_0)$ to the Diophantine equation

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

Then for any integer $z$, $(zx_0, zy_0)$ is a solution of the Diophantine equation

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

$$azx_0 + bzy_0 = zc$$

# Greatest common divisor

**Definition 1.2.1 Greatest common divisor.**

Let $a, b$ be two integers (not all zero). Then a positive integer $g$ is called a *greatest common divisor* of $a$ and $b$ if it satisfies the following two *defining properties*:

1. $g \mid a$ and $g \mid b$, i.e. $g$ is a common divisor of $a$ and $b$; and
2. if $d$ is any common divisor of $a$ and $b$, then $d \mid g$.

For a given pair $(a, b)$, the greatest common divisor is unique, we use $\gcd(a, b)$ to denote it. In particular, we use $\gcd(a, b) = g$ to mean the greatest common divisor exists and equals to $g$.

**Theorem 1.2.2.**

*Let $a, b$ be two positive integers. The output (namely, the last non-zero remainder $r$) of the (Euclidean) division algorithm of $(a, b)$ is a greatest common divisor of $a$ and $b$.*

In particular, since the (Euclidean) division algorithm always halts in finite steps, the greatest common divisor of any pairs of positive integers always exists.

**Theorem 1.2.2.**

*Let $a, b$ be two positive integers. The output (namely, the last non-zero remainder $r$) of the (Euclidean) division algorithm of $(a, b)$ is a greatest common divisor of $a$ and $b$.*

If we combine this theorem with our observations before, we see that: 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 $\gcd(a, b)$.

Let's start with a lemma.

**Lemma 1.2.3.**

*Let $a, b$ be two positive integers. If there are integers $q$ and $r$ such that $a = qb + r$, then we have*

$$\gcd(a, b) = g \iff \gcd(b, r) = g.$$

**Lemma 1.2.3.**

*Let $a, b$ be two positive integers. If there are integers $q$ and $r$ such that $a = qb + r$, then we have*

$$\gcd(a, b) = g \iff \gcd(b, r) = g.$$

**Proof.** ($\Longrightarrow$) Suppose $\gcd(a, b) = g$, let's prove $\gcd(b, r) = g$ by verifying the two defining properties.

1. Since $\gcd(a, b) = g$, we have $g \mid a$ and $g \mid b$. Since $a = qb + r$, by the 2-out-of-3 principle, we have $g \mid r$.
2. Let $d \mid b$ and $d \mid r$. Since $a = qb + r$, by the 2-out-of-3 principle, we have $d \mid a$. Since $\gcd(a, b) = g$, we have $d \mid g$.

A very similar argument gives you ($\Longleftarrow$). $\square$

Let's assume $a \geqslant b$. The division algorithm gives us the following

$$
\begin{aligned}
a &= q_1 b + r_1 && \text{(Step 1)}\\
b &= q_2 r_1 + r_2 && \text{(Step 2)}\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r && \text{(Step } n-1\text{)}\\
r_{n-2} &= q_n r + 0 && \text{(Step } n\text{)}
\end{aligned}
$$

Our lemma 1.2.3 tells us that

$$
\begin{aligned}
\gcd(a, b) &= \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots\\
&= \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-2}, r) = \gcd(r, 0) = r. \qquad \square
\end{aligned}
$$

# (Euclidean) division algorithm, backward

Note that, if we work the division algorithm backward, we have

$$
\begin{aligned}
r &= r_{n-3} + (-q_{n-1}) \cdot r_{n-2} \\
&= r_{n-3} + (-q_{n-1}) \cdot (r_{n-4} - q_{n-2} r_{n-3}) && \text{substitute in } r_{n-2} \\
&= (\cdots) \cdot r_{n-4} + (\cdots) \cdot r_{n-3} && \text{collect the coefficients} \\
&\vdots \\
&= x_0 \cdot a + y_0 \cdot b.
\end{aligned}
$$

Hence, the division algorithm gives us a solution $(x_0, y_0)$ of the Diophantine equation $a \cdot x + b \cdot y = \gcd(a, b)$.

**Theorem 1.2.4 Bézout's identity.**

*Given non-zero integers $a, b$, there exist integers $x_0, y_0$ such that*

$$a \cdot x_0 + b \cdot y_0 = \gcd(a, b).$$

**Theorem 1.2.4 Bézout's identity.**

*Given non-zero integers $a, b$, there exist integers $x_0, y_0$ such that*

$$a \cdot x_0 + b \cdot y_0 = \gcd(a, b).$$

**Proof.** When $a, b$ are both positive, the integers $x_0, y_0$ are obtained by working the division algorithm backward.

In general, we solve this problem for the positive integers $|a|, |b|$, producing integers $x_0, y_0$, then we have

$$a \cdot (\operatorname{sign}(a)x_0) + b \cdot (\operatorname{sign}(a)y_0) = \gcd(a, b),$$

where $\operatorname{sign}(\,\cdot\,)$ eats an integer and gives its signature, is a solution for our Diophantine equation. $\square$

# Summarizing

# Summarizing

- Let $a, b$ be two nonzero integers. 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 $\gcd(a, b)$.

# Summarizing

- Let $a, b$ be two nonzero integers. 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.

# Summarizing

- Let $a, b$ be two nonzero integers. 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.
- It remains to study what are *all* the solutions. Namely, to study the *solution set*

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