Part I

Linear Diophantine Equations

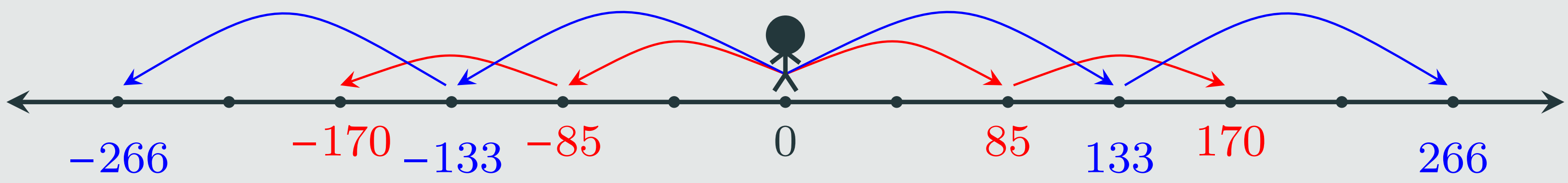
A motivating example

A motivating example

Question.

Suppose you are standing at 0 on the number axis, and you can

- *hop 133 steps left (-133) or right (+133)*
- *skip 85 steps left (-85) or right (+85)*



Can you hop x-many times and skip y-many times to get to 1?

- For example, hopping twice to the right and skipping thrice to the left gets you

$$(2) \cdot 133 + (-3) \cdot 85 = 266 - 255 = 11$$

- For example, hopping twice to the right and skipping thrice to the left gets you

$$(+2) \cdot 133 + (-3) \cdot 85 = 266 - 255 = 11$$

- If you can hop x-many times and skip y-many times to get to 1, then you can hop xz-many times and skip yz-many times to get to z for any integer $z \in \mathbb{Z}$.

- For example, hopping twice to the right and skipping thrice to the left gets you

$$(+2) \cdot 133 + (-3) \cdot 85 = 266 - 255 = 11$$

- If you can hop x-many times and skip y-many times to get to 1, then you can hop xz-many times and skip yz-many times to get to z for any integer $z \in \mathbb{Z}$.
- The answer is *Yes*. We can solve this problem using *(Euclidean) Division Algorithm*.

(Euclidean) division algorithm

(Euclidean) division algorithm

1. Start with two positive integers a, b, assume $a \geq b$.
2. Divide a by b
$$a = q \cdot b + r, \quad 0 \leqslant r < b, \quad q \in \mathbb{Z}.$$
3. If $r = 0$, *halt*. Otherwise, repeat the previous steps with the pair (a, b) replaced by (b, r).
4. Continue until your remainder is 0, this process will terminate in finite steps. Output the last nonzero remainder.

Now, we apply the (Euclidean) Division Algorithm to our example.

$$133 = (1) \cdot 85 + 48$$

$$85 = (1) \cdot 48 + 37$$

$$48 = (1) \cdot 37 + 11$$

$$37 = (3) \cdot 11 + 4$$

$$11 = (2) \cdot 4 + 3$$

$$4 = (1) \cdot 3 + 1$$

$$3 = (3) \cdot 1 + \underline{0}$$

Now, we apply the (Euclidean) Division Algorithm to our example.

$$133 = (1) \cdot 85 + 48$$
$$85 = (1) \cdot 48 + 37$$
$$48 = (1) \cdot 37 + 11$$
$$37 = (3) \cdot 11 + 4$$
$$11 = (2) \cdot 4 + 3$$
$$4 = (1) \cdot 3 + 1$$
$$3 = (3) \cdot 1 + 0$$

$$\begin{aligned}
1 &= 4 + (-1) \cdot 3 \\
&= 4 + (-1) \cdot (11 - 2 \cdot 4) \\
&= (-1) \cdot 11 + (3) \cdot 4 \\
&= (-1) \cdot 11 + (3) \cdot (37 - 3 \cdot 11) \\
&= (3) \cdot 37 + (-10) \cdot 11 \\
&= (3) \cdot 37 + (-10) \cdot (48 - 1 \cdot 37) \\
&= (-10) \cdot 48 + (13) \cdot 37 \\
&= (-10) \cdot 48 + (13) \cdot (85 - 1 \cdot 48) \\
&= (13) \cdot 85 + (-23) \cdot 48 \\
&= (13) \cdot 85 + (-23) \cdot (133 - 1 \cdot 85) \\
&= (-23) \cdot 133 + (36) \cdot 85
\end{aligned}$$

(Euclidean) Division Algorithm

Now, we apply the (Euclidean) Division Algorithm to our example.

$$
\begin{aligned}
133 &= (1)\cdot 85 + 48\\
85 &= (1)\cdot 48 + 37\\
48 &= (1)\cdot 37 + 11\\
37 &= (3)\cdot 11 + 4\\
11 &= (2)\cdot 4 + 3\\
4 &= (1)\cdot 3 + 1\\
3 &= (3)\cdot 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 4 + (-1)\cdot 3\\
&= 4 + (-1)\cdot (11 - 2\cdot 4)\\
&= (-1)\cdot 11 + (3)\cdot 4\\
&= (-1)\cdot 11 + (3)\cdot (37 - 3\cdot 11)\\
&= (3)\cdot 37 + (-10)\cdot 11\\
&= (3)\cdot 37 + (-10)\cdot (48 - 1\cdot 37)\\
&= (-10)\cdot 48 + (13)\cdot 37\\
&= (-10)\cdot 48 + (13)\cdot (85 - 1\cdot 48)\\
&= (13)\cdot 85 + (-23)\cdot 48\\
&= (13)\cdot 85 + (-23)\cdot (133 - 1\cdot 85)\\
&= (\underbrace{-23}_{x})\cdot 133 + (\underbrace{36}_{y})\cdot 85
\end{aligned}
$$