

Games, graphs, and machines

Modular arithmetic

July 29, 2025

Visualising modular arithmetic

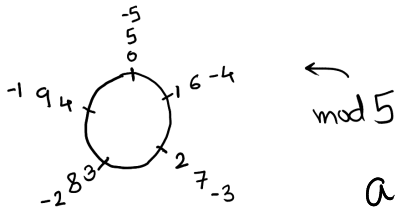
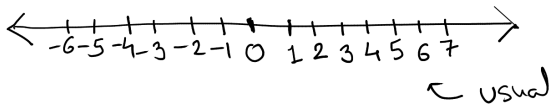


Number
line



Number
circle

Visualising modular arithmetic



$a - b$ is a multiple of 5.



$a \equiv b \pmod{5}$
if a & b land at the same pt on 5-step circle.

Modular operations $+$ and \times

To find $A + B$ —

1. Pick $a \in A$ and $b \in B$.
2. Compute $a + b$.
3. The answer is the resulting equivalence class.

To find $A \times B$ — Same thing.

Key point Consistency

The answer does not depend on which a or b was chosen.

Laws of arithmetic

Both $+$ and \times satisfy the usual laws (commutativity, associativity, distributivity).

For example,

1. What is the negative of $\bar{3}$ modulo 7?

2. Compute $\bar{3} \times \bar{5} - \bar{13}$ (mod 8).

Additive id
= $\bar{0}$
mult. id = $\bar{1}$

$$1. \quad \bar{4} = \overline{-3} = \overline{11} = \overline{-10}$$

$$2. \quad \begin{array}{l} \bar{2} \\ \bar{10} \end{array} \quad \begin{array}{l} (3 \times 5 - 13) \\ (3 \times 5 - 5) \end{array}$$

Laws of arithmetic: surprises

Some things are different! For example, it may happen that $a \times b = 0$ but $a \neq 0$ and $b \neq 0$.

Let $S = \mathbb{Z}/12\mathbb{Z}$. Find $A, B \in S$ such that $A \neq \bar{0}$ and $B \neq \bar{0}$ but

$$A \cdot B = 0.$$

Ex.

$$\begin{array}{cc} \bar{2} & \& \bar{6} \\ \bar{3} & \& \bar{4} \\ \bar{9} & \& \bar{8} \end{array}$$

Laws of arithmetic: surprises

What are the square-roots of $\bar{1}$ in $\mathbb{Z}/8\mathbb{Z}$?

$\bar{3}$, $\bar{1}$, $\bar{7}$, $\bar{5}$

Trial and error.

← Four!

Modular equations

1. Solve $2x + 7 = 0$ in $\mathbb{Z}/5\mathbb{Z}$.

$$\begin{array}{l} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \checkmark$$

2. Solve $2x + 7 = 0$ in $\mathbb{Z}/6\mathbb{Z}$.

~~~~~

$$x \in \mathbb{Z}/5\mathbb{Z}$$

$$\begin{aligned} \bar{2}x + \bar{7} &= \bar{0} \\ + \bar{3} &= + \bar{3} \end{aligned}$$

$$\bar{2}x = \bar{3}$$

$$\begin{array}{cc} \bar{3} \times & \times \bar{3} \end{array}$$

$$\boxed{x = \bar{9}}$$