

Games, graphs, and machines

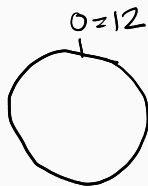
Modular arithmetic

July 30, 2025

Modular real numbers

Let $a, b \in \mathbb{R}$. Say $a \equiv b \pmod{12}$ if $a - b$ is an integer multiple of 12. Is $\equiv \pmod{12}$ an equivalence relation?

- Reflexive ✓
- Symmetric ✓
- Transitive ✓



Modular real operations

Let $\mathbb{R}/12$ be the set of equivalence classes. Try to define $+$ and \times on $\mathbb{R}/12$ by the usual process.

Which one works and which one does not work?



To find $A + B$

1. Pick $a \in A$ and $b \in B$.
2. Calculate $a + b$.
3. Check that $[a + b]$ does not change even if we pick different a and b .
4. Set $A + B = [a + b]$.



$$\begin{array}{l} a \\ \hline 12K_1 \end{array} \quad \begin{array}{l} b \\ \hline 12K_2 \end{array} \rightsquigarrow \begin{array}{l} a+b \\ \hline 12(K_1+K_2) \end{array}$$



To find $A \cdot B$

1. Pick $a \in A$ and $b \in B$.
2. Calculate $a \cdot b$.
3. Check that $[a \cdot b]$ does not change even if we pick different a and b .
4. Set $A \cdot B = [a \cdot b]$.



$$\begin{array}{l} a = \frac{1}{2} \\ a' = \frac{1}{2} \end{array} \quad \begin{array}{l} b = 0 \\ b' = 12 \end{array} \quad \begin{array}{l} ab = 0 \\ a'b' = 6 \end{array}$$

Back to modular whole numbers

Can you solve $2x + 4 = 0$ in $\mathbb{Z}/12\mathbb{Z}$?

$$x = 4, -2 = 10$$

$$2x + 4 = 0 \quad (\mathbb{Z}/12\mathbb{Z})$$

$$2x = -4$$

can't divide by 2!

$$x = -2$$

$$2 = [2] \in \mathbb{Z}/12\mathbb{Z}$$

to $\rightarrow 0$

~~$x = 2$~~

2
4
6
8
10

||

Multiplicative inverse

For which n does 2 have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$?

n	2 has an inverse
2	X
3	✓
4	X
5	✓
6	X
7	✓
8	X
9	✓
10	·
11	·
12	·
13	·
14	
15	

Square roots

For which n does 2 have a square root in $\mathbb{Z}/n\mathbb{Z}$?

n	2 has a square root
2	✓
3	✗
4	✗
5	✗
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

trickier

The world of modular arithmetic

- Modular square roots \rightsquigarrow quadratic reciprocity theorem.
- Modular n -th roots \rightsquigarrow class field theory.
- Modular equations in 2-variables \rightsquigarrow elliptic curves and post-quantum cryptography.