

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?

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 $A + B = [a + b]$.

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 $A \cdot B = [a \cdot b]$.

Back to modular whole numbers

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

Multiplicative inverse

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

| n | 2 has an inverse |
|-----|------------------|
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 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 | |

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.