Games, graphs, and machines

Modular arithmetic

July 31, 2024

Visualising modular arithmetic

Arithmetic modulo 10

- $a \equiv b \pmod 1)0$ if and only if a and b have the same units digit (when written in base 10).
- Arithmetic modulo 10 = units digit arithmetic

$$\overline{7} \cdot \overline{6} = \overline{2}$$

Laws of arithmetic:

Fix d. All the usual laws of arithmetic for $\mathbb{Z}$ hold for equivalence classes modulo d. That is, $+$ and $\times$ are commutative and associative, have identity elements, and $\times$ distributes over $+$.

1. What is the negative of $\overline{3}$ modulo 7?
2. Compute $\overline{3} \times \overline{5} - \overline{1}3 \pmod 8$.

Laws of arithmetic: surprises

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

Prove that $\overline{4} \cdot \overline{4} = \overline{0} \pmod 8$ but $\overline{4} \neq \overline{0} \pmod 8$.

Squares

Notation: $\mathbb{Z}/d\mathbb{Z}$ denotes the equivalence classes of $\mathbb{Z}$ under the equivalence relation $\sim_d$.

Of the 7 elements of $\mathbb{Z}/d\mathbb{Z}$, which ones are perfect squares?

Square roots

What are the sqaure roots of $\overline{-1}$ . . .

1. modulo 5?
2. modulo 7?
3. modulo 8?