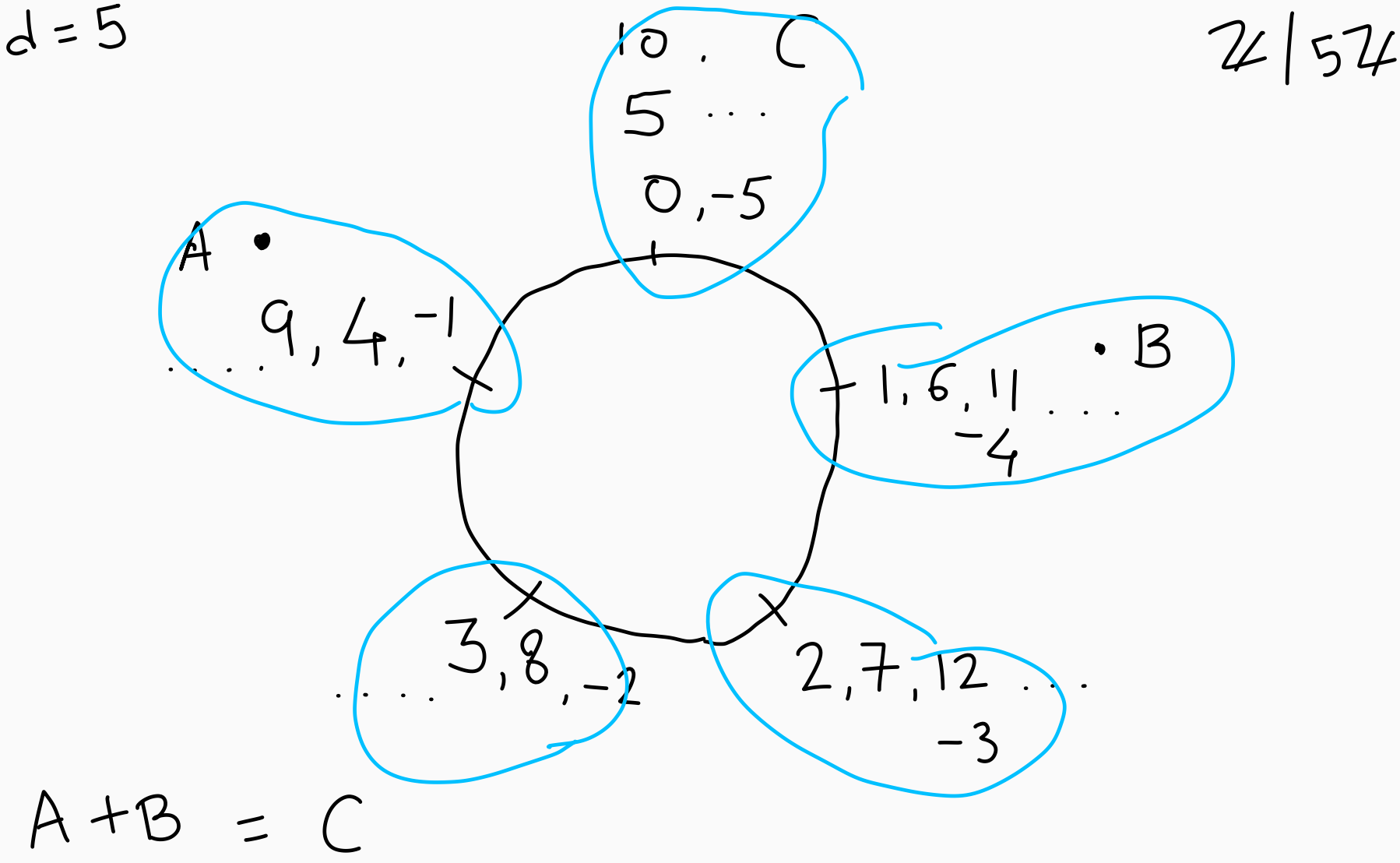
Games, graphs, and machines

Modular arithmetic

July 31, 2024

Visualising modular arithmetic



Arithmetic modulo 10

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

positive

$$\overline{7} \cdot \overline{6} = \overline{2} \pmod{10}$$

$a \sim_{10} b$

$a \equiv b \pmod{10}$

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 $\overline{3} \times \overline{5} - \overline{13} \pmod 8$.

1. $-\overline{3} = \overline{4}$ $\pmod 7$

$\overline{3} + \overline{4} = \overline{0}$

$-\overline{3} = \overline{-3}$

2. $\overline{2} = \overline{-6}$

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 $\overline{4} \neq \overline{0} \pmod 8$.

By definition, $\overline{4} \times \overline{4} = \overline{4 \times 4}$

$= \overline{16}$.

Now $\overline{16} = \overline{0}$, because $16 \equiv 0 \pmod 8$.

But $\overline{4} \neq \overline{0}$ because $4 \not\equiv 0 \pmod 8$

(8 does not divide 4).

Squares

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

$|\mathbb{Z}/d\mathbb{Z}| = d$ $\quad \mathbb{Z}/d\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{d-1}\}$

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

$d = 7$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

✓ ✓ ✓ ✓

Square roots

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

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