

# AI in Mathematics

## Lecture 1

Bar-Ilan University  
Nebius Academy | Stevens Institute of  
Technology  
March 18, 2025



**NEBIUS**

# Computers in Mathematics

## The Pioneering Era (Mid-20th Century)



# Computers in Mathematics

## The Four Color Theorem



# Computers in Mathematics

## Software and globalization



L<sup>A</sup>T<sub>E</sub>X



MATLAB®

arXiv



# Computers in Mathematics

## Formal Proof Assistants



L<sup>A</sup>T<sub>E</sub>X

LEAN



arXiv

# Computers in Mathematics

**AI and LLMs everywhere**



L<sup>A</sup>T<sub>E</sub>X

LEAN

LLaMA

MATLAB

arXiv



# AI IN MATHEMATICS

```
graph TD; A[AI IN MATHEMATICS] --> B[Large Language Models (LLMs)]; A --> C[Formal Proof Assistant]; A --> D[Machine Learning];
```

Large Language  
Models (LLMs)



Formal Proof Assistant



Machine Learning

## Algorithms

- Mathematical search engine
- Provides explanations
- Math Problem Solving

- Software tools for theorem proving
- Verifies proofs
- Makes you structure proofs

- Generates examples
- Discovers new structures and relationships
- Pushes the boundaries of solving methods

# Large Language Models (LLMs)

Examples:



 Claude

 Gemini



Predict the next “word” based on previously generated tokens and the given context.

Recent developments:

- Non-linear reasoning
- Usage of Agents



# Formal Proof Assistants

Examples:



Check out: <https://adam.math.hhu.de>

Verify mathematical proofs with absolute rigor.

Reduce the need  
in human reviews

Generate datasets  
of proofs

Allow simpler  
collaboration



# IMO Participation



AI won “silver” medal on International Math Olympiad

- Solved the **hardest** (for humans) problem of the Olympiad.
- Wrote proofs in Lean and scored **28/42** points (just **one point shy** of a gold medal).
- **Three days** to find the solution.
- **Didn't solve combinatorics.** Apparently, AI is not a fan of this field!

# AlphaProof solved

**Problem 1.** Determine all real numbers  $\alpha$  such that, for every positive integer  $n$ , the integer

$$\lfloor \alpha \rfloor + \lfloor 2\alpha \rfloor + \cdots + \lfloor n\alpha \rfloor$$

is a multiple of  $n$ . (Note that  $\lfloor z \rfloor$  denotes the greatest integer less than or equal to  $z$ . For example,  $\lfloor -\pi \rfloor = -4$  and  $\lfloor 2 \rfloor = \lfloor 2.9 \rfloor = 2$ .)

**Problem 2.** Determine all pairs  $(a, b)$  of positive integers for which there exist positive integers  $g$  and  $N$  such that

$$\gcd(a^n + b, b^n + a) = g$$

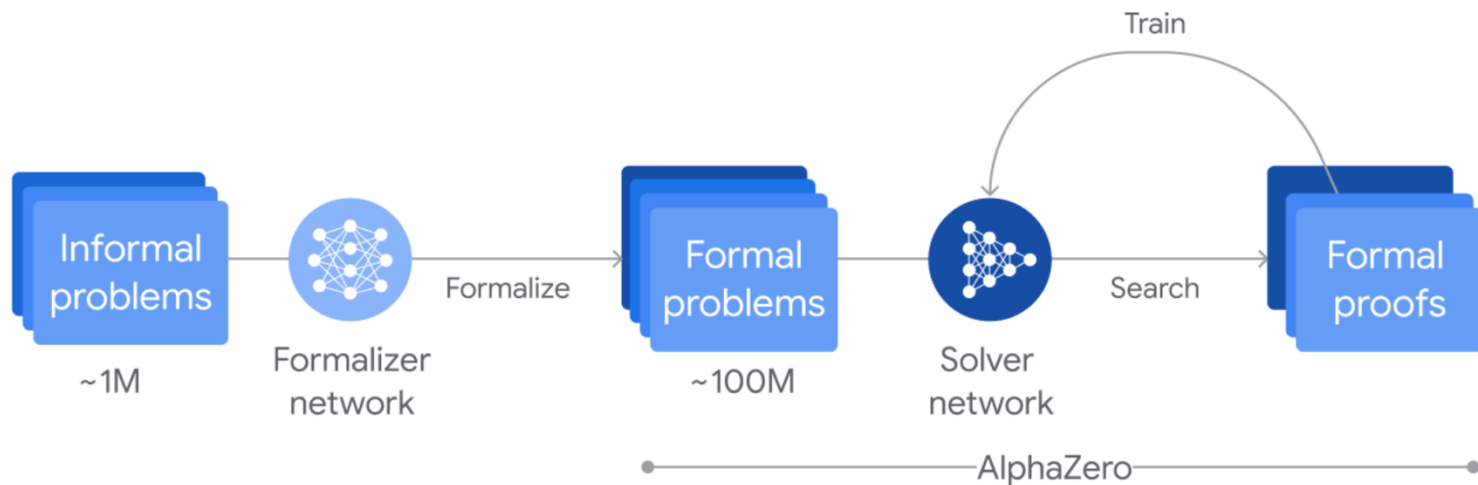
holds for all integers  $n \geq N$ . (Note that  $\gcd(x, y)$  denotes the greatest common divisor of integers  $x$  and  $y$ .)

**Problem 6.** Let  $\mathbb{Q}$  be the set of rational numbers. A function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is called *aquaesulian* if the following property holds: for every  $x, y \in \mathbb{Q}$ ,

$$f(x + f(y)) = f(x) + y \quad \text{or} \quad f(f(x) + y) = x + f(y).$$

Show that there exists an integer  $c$  such that for any aquaesulian function  $f$  there are at most  $c$  different rational numbers of the form  $f(r) + f(-r)$  for some rational number  $r$ , and find the smallest possible value of  $c$ .

# AlphaProof



# Problem 1

**Problem 1.** Determine all real numbers  $\alpha$  such that, for every positive integer  $n$ , the integer

$$\lfloor \alpha \rfloor + \lfloor 2\alpha \rfloor + \cdots + \lfloor n\alpha \rfloor$$

is a multiple of  $n$ . (Note that  $\lfloor z \rfloor$  denotes the greatest integer less than or equal to  $z$ . For example,  $\lfloor -\pi \rfloor = -4$  and  $\lfloor 2 \rfloor = \lfloor 2.9 \rfloor = 2$ .)

Solution ideas:

- Even integers satisfy the condition.
- Consider  $\alpha$  as a sum of integer  $k$  and  $0 \leq \epsilon < 1$ .
- Notice that we can take  $k$  out of the brackets.
- Consider case of even and odd  $k$  separately and prove that only even integers satisfy.

# Problem 2

**Problem 2.** Determine all pairs  $(a, b)$  of positive integers for which there exist positive integers  $g$  and  $N$  such that

$$\gcd(a^n + b, b^n + a) = g$$

holds for all integers  $n \geq N$ . (Note that  $\gcd(x, y)$  denotes the greatest common divisor of integers  $x$  and  $y$ .)

Let again  $K = ab + 1$ , which is coprime to both  $a$  and  $b$ . By Euler's theorem, for  $n = k \cdot \varphi(K) - 1$  we have

$$a(a^n + b) = (a^k)^{\varphi(K)} + ab \equiv 1 + ab = K \equiv 0 \pmod{K},$$

so  $K \mid a^n + b$  and similarly  $K \mid b^n + a$ . Hence  $K$  is a common divisor of  $a^n + b$  and  $b^n + a$ . If  $n$  is sufficiently large, the greatest common divisor is supposed to be  $g$ , so  $K \mid g$ .

Now, for sufficiently large  $n = k \cdot \varphi(K)$  we have  $K \mid g \mid a^n + b$  and therefore

$$0 \equiv a^n + b = (a^k)^{\varphi(K)} + b \equiv 1 + b \pmod{K},$$

so  $K = ab + 1 \mid b + 1$  and similarly  $ab + 1 \mid a + 1$ , which is possible only for  $a = b = 1$ ,

# Problem 6

**Problem 6.** Let  $\mathbb{Q}$  be the set of rational numbers. A function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is called *aquaesulian* if the following property holds: for every  $x, y \in \mathbb{Q}$ ,

$$f(x + f(y)) = f(x) + y \quad \text{or} \quad f(f(x) + y) = x + f(y).$$

Show that there exists an integer  $c$  such that for any aquaesulian function  $f$  there are at most  $c$  different rational numbers of the form  $f(r) + f(-r)$  for some rational number  $r$ , and find the smallest possible value of  $c$ .

Solution ideas:

- Example  $f(x) = [x] - \{x\}$  gives  $c \geq 2$ .
- Denote  $g(x) = f(x) + f(-x)$ .
- We want to show that it can not have more than 1 nonzero value.
- Show that  $f$  is a bijection with  $f(-f(-x)) = x$ .
- Derive the result for  $g(x)$  knowing that  $f^{-1}(x) = -f(-x)$ .

# AlphaGeometry solved

**Problem 4.** Let  $ABC$  be a triangle with  $AB < AC < BC$ . Let the incentre and incircle of triangle  $ABC$  be  $I$  and  $\omega$ , respectively. Let  $X$  be the point on line  $BC$  different from  $C$  such that the line through  $X$  parallel to  $AC$  is tangent to  $\omega$ . Similarly, let  $Y$  be the point on line  $BC$  different from  $B$  such that the line through  $Y$  parallel to  $AB$  is tangent to  $\omega$ . Let  $AI$  intersect the circumcircle of triangle  $ABC$  again at  $P \neq A$ . Let  $K$  and  $L$  be the midpoints of  $AC$  and  $AB$ , respectively.

Prove that  $\angle KIL + \angle YPX = 180^\circ$ .

in 19 seconds...

**Much stronger than AlphaProof:**

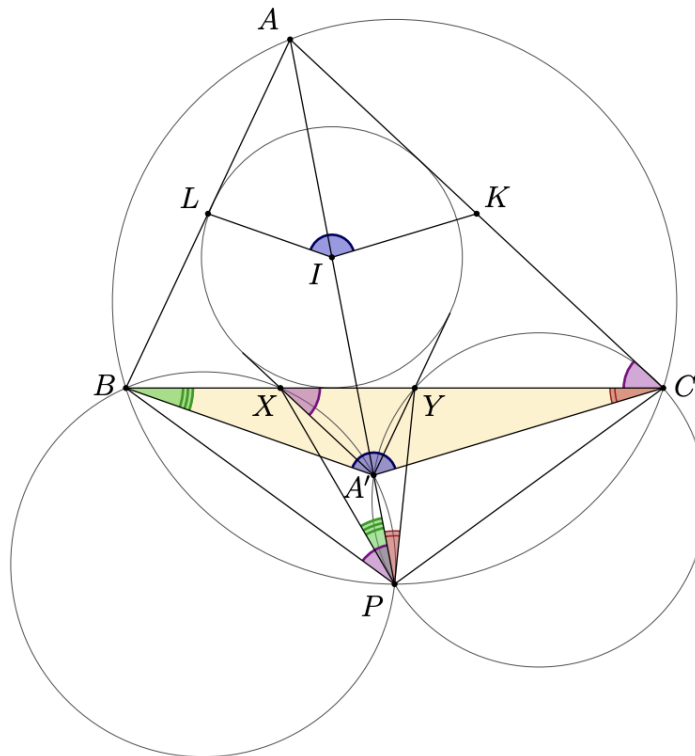
Solves almost all geometry problems from IMO this century.



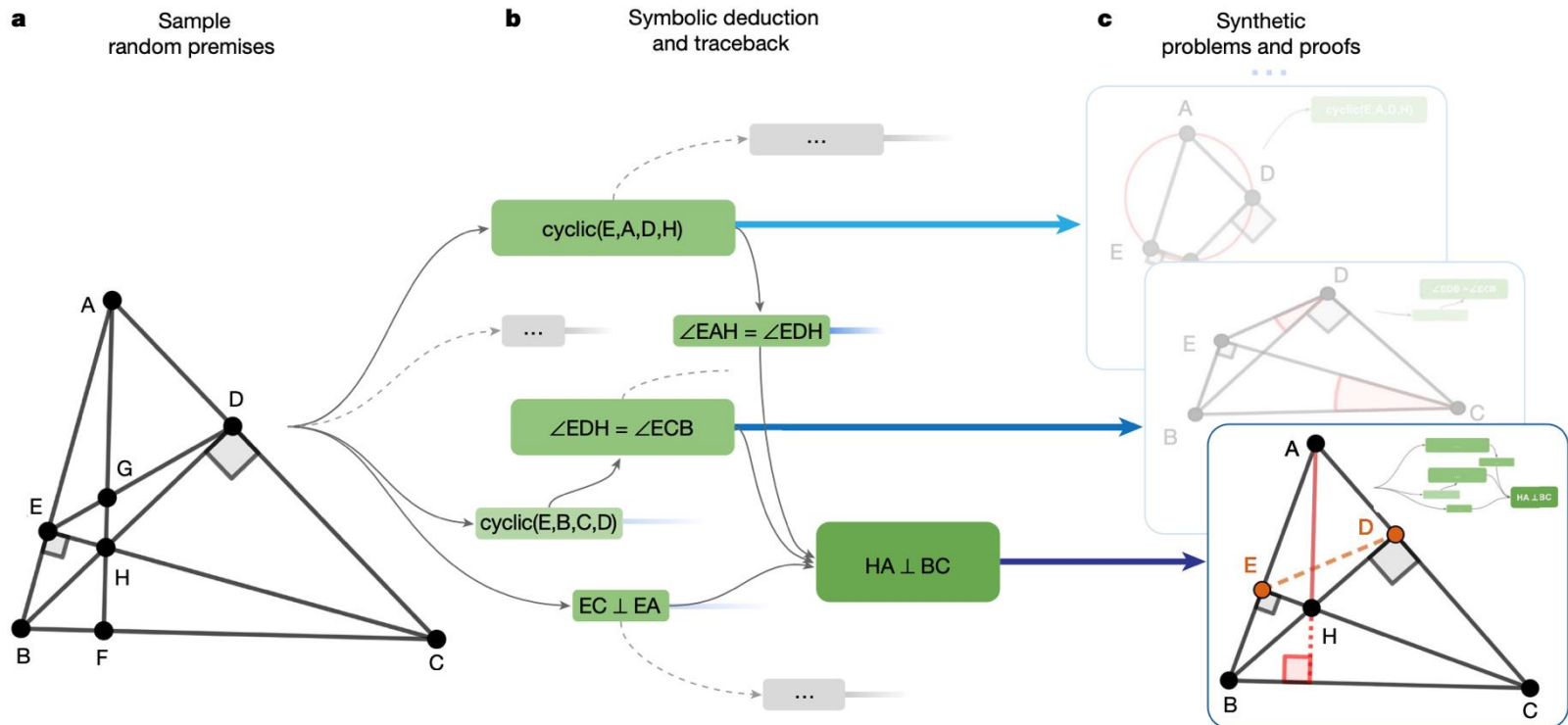
# AlphaGeometry solved

**Problem 4.** Let  $ABC$  be a triangle with  $AB < AC < BC$ . Let the incentre and incircle of triangle  $ABC$  be  $I$  and  $\omega$ , respectively. Let  $X$  be the point on line  $BC$  different from  $C$  such that the line through  $X$  parallel to  $AC$  is tangent to  $\omega$ . Similarly, let  $Y$  be the point on line  $BC$  different from  $B$  such that the line through  $Y$  parallel to  $AB$  is tangent to  $\omega$ . Let  $AI$  intersect the circumcircle of triangle  $ABC$  again at  $P \neq A$ . Let  $K$  and  $L$  be the midpoints of  $AC$  and  $AB$ , respectively.

Prove that  $\angle KIL + \angle YPX = 180^\circ$ .

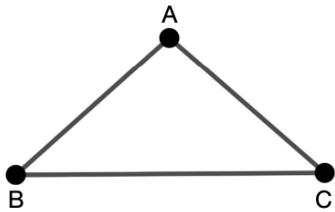


# AlphaGeometry



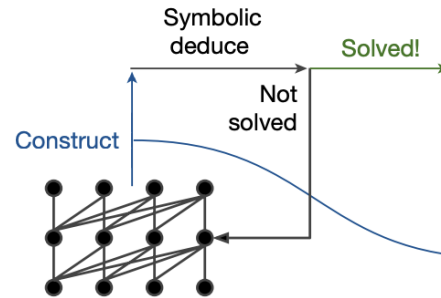
# AlphaGeometry

**a** A simple problem



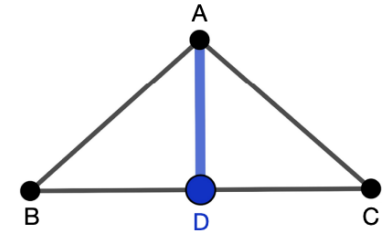
"Let ABC be any triangle with  $AB = AC$ .  
Prove that  $\angle ABC = \angle BCA$ ."

**b** AlphaGeometry



**c** Language model

**d** Solution



Construct D: midpoint BC,

$AB=AC, BD = DC, AD=AD \Rightarrow \angle ABD = \angle DCA$  [1]

[1],  $B C D$  collinear  $\Rightarrow \angle ABC = \angle BCA$

# AlphaProof didn't solve

**Problem 3.** Let  $a_1, a_2, a_3, \dots$  be an infinite sequence of positive integers, and let  $N$  be a positive integer. Suppose that, for each  $n > N$ ,  $a_n$  is equal to the number of times  $a_{n-1}$  appears in the list  $a_1, a_2, \dots, a_{n-1}$ .

Prove that at least one of the sequences  $a_1, a_3, a_5, \dots$  and  $a_2, a_4, a_6, \dots$  is eventually periodic.

(An infinite sequence  $b_1, b_2, b_3, \dots$  is *eventually periodic* if there exist positive integers  $p$  and  $M$  such that  $b_{m+p} = b_m$  for all  $m \geq M$ .)

**Problem 5.** Turbo the snail plays a game on a board with 2024 rows and 2023 columns. There are hidden monsters in 2022 of the cells. Initially, Turbo does not know where any of the monsters are, but he knows that there is exactly one monster in each row except the first row and the last row, and that each column contains at most one monster.

Turbo makes a series of attempts to go from the first row to the last row. On each attempt, he chooses to start on any cell in the first row, then repeatedly moves to an adjacent cell sharing a common side. (He is allowed to return to a previously visited cell.) If he reaches a cell with a monster, his attempt ends and he is transported back to the first row to start a new attempt. The monsters do not move, and Turbo remembers whether or not each cell he has visited contains a monster. If he reaches any cell in the last row, his attempt ends and the game is over.

Determine the minimum value of  $n$  for which Turbo has a strategy that guarantees reaching the last row on the  $n^{\text{th}}$  attempt or earlier, regardless of the locations of the monsters.

Is it too lazy to read so many words?)

# Problem 3

**Problem 3.** Let  $a_1, a_2, a_3, \dots$  be an infinite sequence of positive integers, and let  $N$  be a positive integer. Suppose that, for each  $n > N$ ,  $a_n$  is equal to the number of times  $a_{n-1}$  appears in the list  $a_1, a_2, \dots, a_{n-1}$ .

Prove that at least one of the sequences  $a_1, a_3, a_5, \dots$  and  $a_2, a_4, a_6, \dots$  is eventually periodic.

(An infinite sequence  $b_1, b_2, b_3, \dots$  is *eventually periodic* if there exist positive integers  $p$  and  $M$  such that  $b_{m+p} = b_m$  for all  $m \geq M$ .)

Ideas:

1. At least one integer appears infinitely often.
2. Only finitely many integers appear infinitely often.
3. Classify numbers and show the sequence eventually alternates between “big” and “small.”
4. Analyze the “small” terms to show eventual periodicity.

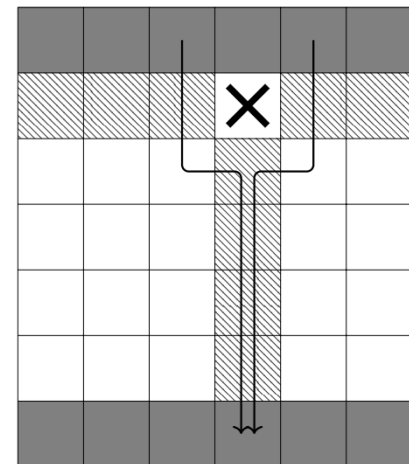
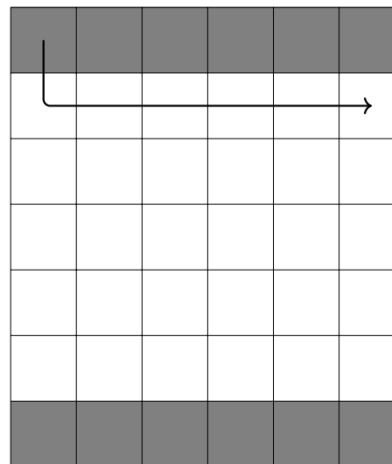
# Problem 5

**Problem 5.** Turbo the snail plays a game on a board with 2024 rows and 2023 columns. There are hidden monsters in 2022 of the cells. Initially, Turbo does not know where any of the monsters are, but he knows that there is exactly one monster in each row except the first row and the last row, and that each column contains at most one monster.

Turbo makes a series of attempts to go from the first row to the last row. On each attempt, he chooses to start on any cell in the first row, then repeatedly moves to an adjacent cell sharing a common side. (He is allowed to return to a previously visited cell.) If he reaches a cell with a monster, his attempt ends and he is transported back to the first row to start a new attempt. The monsters do not move, and Turbo remembers whether or not each cell he has visited contains a monster. If he reaches any cell in the last row, his attempt ends and the game is over.

Determine the minimum value of  $n$  for which Turbo has a strategy that guarantees reaching the last row on the  $n^{\text{th}}$  attempt or earlier, regardless of the locations of the monsters.

Answer:  $n = 3$





# AI and Mathematics



And now we will look at some examples how machine learning solves real mathematical problems

# AI and Matrix Multiplication

Consider multiplying two matrices:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

How many multiplications are needed in the classical approach?



# AI and Matrix Multiplication

We can do 7!!!!

$$M_1 = (a_{11} + a_{22}) \cdot (b_{11} + b_{22}), \quad M_2 = (a_{21} + a_{22}) \cdot b_{11}$$

$$M_3 = a_{11} \cdot (b_{12} - b_{22}), \quad M_4 = a_{22} \cdot (b_{21} - b_{11})$$

$$M_5 = (a_{11} + a_{12}) \cdot b_{22}, \quad M_6 = (a_{21} - a_{11}) \cdot (b_{11} + b_{12})$$

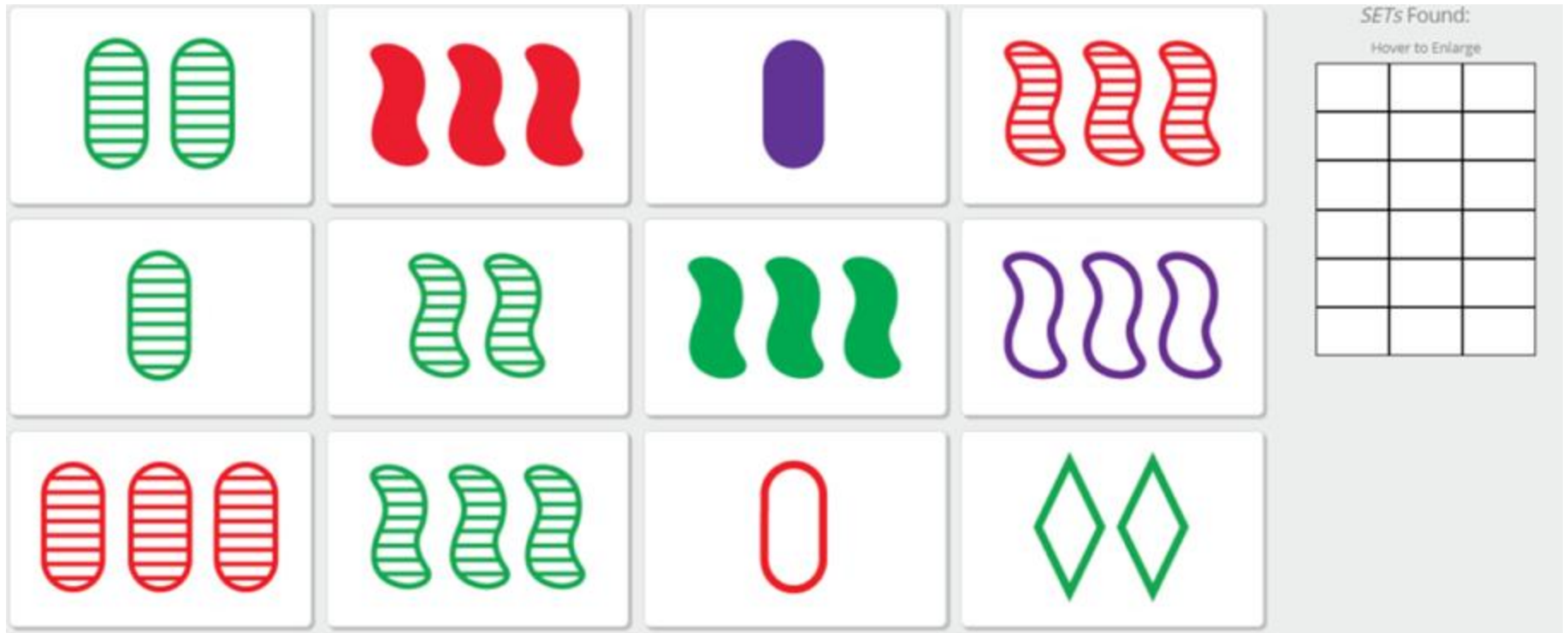
$$M_7 = (a_{12} - a_{22}) \cdot (b_{21} + b_{22})$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} M_1 + M_4 - M_5 + M_7 & M_3 + M_5 \\ M_2 + M_4 & M_1 - M_2 + M_3 + M_6 \end{pmatrix}.$$

# Alpha Tensor results

Size ( $n, m, p$ )	Best method known	Best rank known	AlphaTensor rank	
			Modular	Standard
(2, 2, 2)	(Strassen, 1969) <sup>2</sup>	7	7	7
(3, 3, 3)	(Laderman, 1976) <sup>15</sup>	23	23	23
(4, 4, 4)	(Strassen, 1969) <sup>2</sup> (2, 2, 2) $\otimes$ (2, 2, 2)	49	47	49
(5, 5, 5)	(3, 5, 5) + (2, 5, 5)	98	96	98
(2, 2, 3)	(2, 2, 2) + (2, 2, 1)	11	11	11
(2, 2, 4)	(2, 2, 2) + (2, 2, 2)	14	14	14
(2, 2, 5)	(2, 2, 2) + (2, 2, 3)	18	18	18
(2, 3, 3)	(Hopcroft and Kerr, 1971) <sup>16</sup>	15	15	15
(2, 3, 4)	(Hopcroft and Kerr, 1971) <sup>16</sup>	20	20	20
(2, 3, 5)	(Hopcroft and Kerr, 1971) <sup>16</sup>	25	25	25
(2, 4, 4)	(Hopcroft and Kerr, 1971) <sup>16</sup>	26	26	26
(2, 4, 5)	(Hopcroft and Kerr, 1971) <sup>16</sup>	33	33	33
(2, 5, 5)	(Hopcroft and Kerr, 1971) <sup>16</sup>	40	40	40
(3, 3, 4)	(Smirnov, 2013) <sup>18</sup>	29	29	29
(3, 3, 5)	(Smirnov, 2013) <sup>18</sup>	36	36	36
(3, 4, 4)	(Smirnov, 2013) <sup>18</sup>	38	38	38
(3, 4, 5)	(Smirnov, 2013) <sup>18</sup>	48	47	47
(3, 5, 5)	(Sedoglavic and Smirnov, 2021) <sup>19</sup>	58	58	58
(4, 4, 5)	(4, 4, 2) + (4, 4, 3)	64	63	63
(4, 5, 5)	(2, 5, 5) $\otimes$ (2, 1, 1)	80	76	76

# The SET Game



# The SET Game

What mathematical structure do the cards correspond to?

Each card represents a point in  $\mathbb{Z}_3^4$  (a four-dimensional vector space over  $\mathbb{Z}_3$ ). A “set” is a triple of cards whose sum in  $\mathbb{Z}_3^4$  is the zero vector.



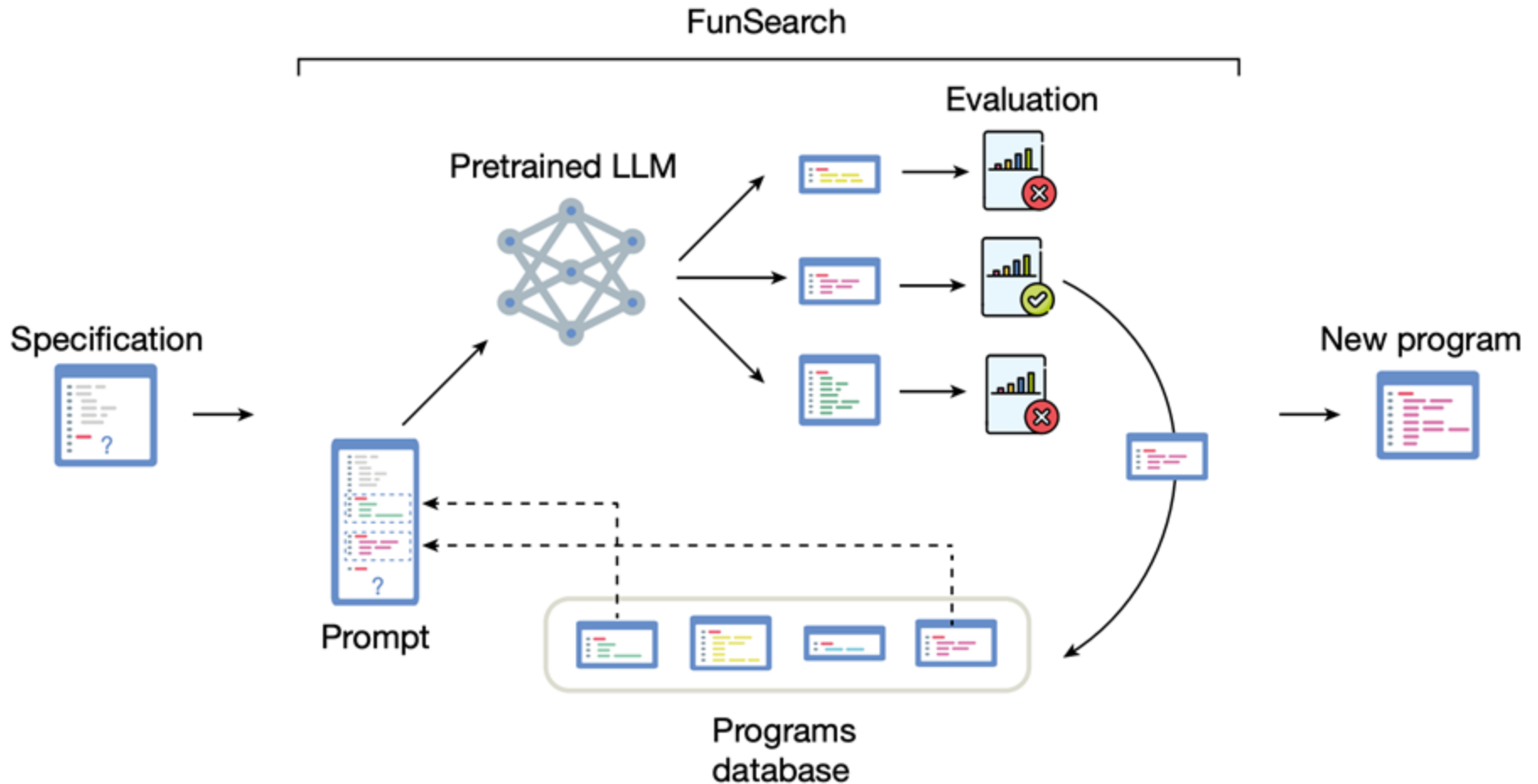
(diamond, 2, red, open)

# AI improved the results!

Find the largest possible subset of  $\mathbb{Z}_3^n$ , such that sum of any triplet doesn't equal to zero.

$n$	3	4	5	6	7	8
Best known	9	20	45	112	236	496
FunSearch	9	20	45	112	236	512

# How AI Helped in the Capset Problem?



# Lyapunov Functions

A Lyapunov function is a function associated with an ordinary differential equation (ODE):

$$\dot{x} = g(x), \quad x \in \mathbb{R}^n.$$

**Definition:** A function  $V : \mathbb{R}^n \rightarrow \mathbb{R}$  is called a **Lyapunov function** for the system if:

- $V(x) > 0$  for all  $x \neq 0$ ,
- $V(0) = 0$ ,
- $\dot{V}(x) = \langle \nabla V(x), \dot{x} \rangle \leq 0$ .

Why are they important?

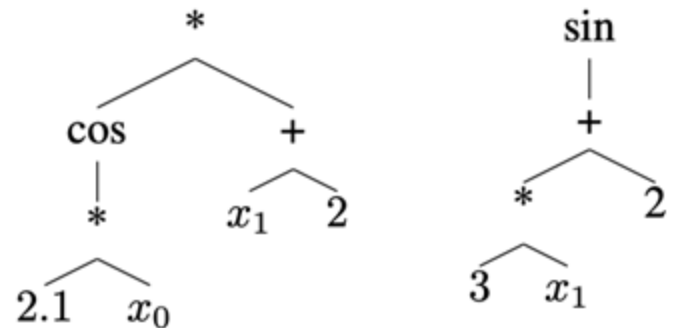
Lyapunov function  $\Leftrightarrow$  Stable system

# Lyapunov Functions

Even writing system of equation in a machine readable text is challenging:

$$\begin{cases} \dot{x}_0 = \cos(2.1x_0)(x_1 + 2) \\ \dot{x}_1 = \sin(3x_1 + 2) \end{cases}$$

is represented as



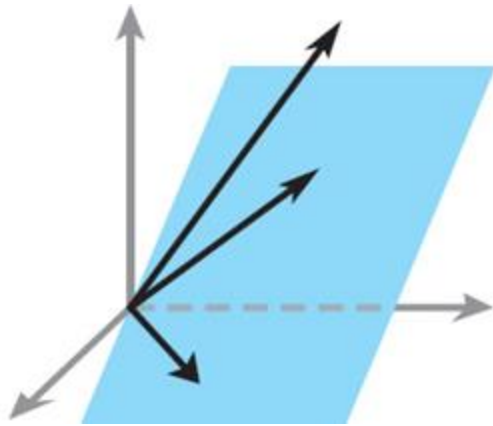


# Lyapunov Functions

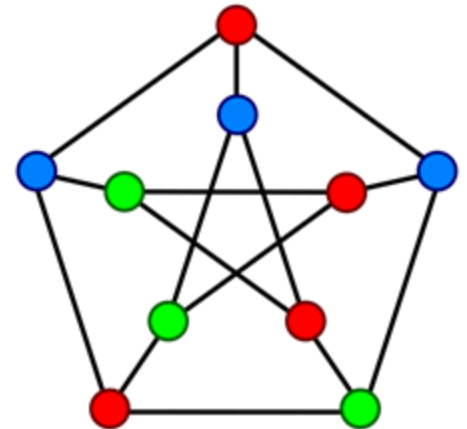
AI found Lyapunov functions on a test dataset **84%** of the time, while Master's students in relative field only solved **9.3%** of those equations.



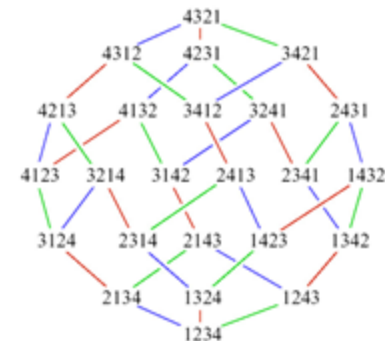
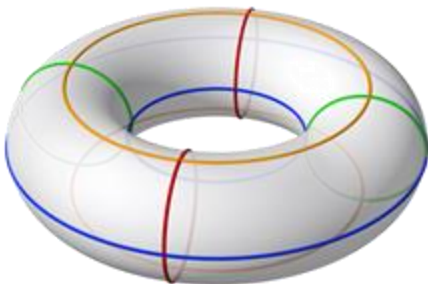
# Mathematical Data



$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$



$$f(x) = a_n x^n + \dots + a_1 x + a_0$$



# About This Course

1 week: Intro

2 weeks: Data Science in Mathematics

2 weeks: Deep Learning in Mathematics

3 weeks: Math as an NLP problem (LLMs etc.)

3 weeks: Reinforcement Learning (RL) in Math

1 week: Advanced AI topics

1 week: Project Presentations

**Thank you!**