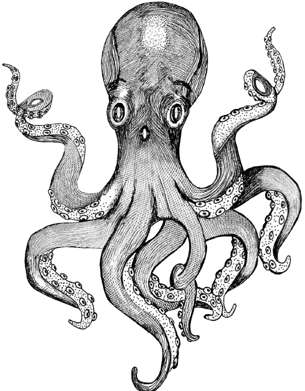
Formalizing Fundamental Algebraic Number Theory

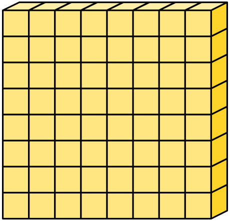
Anne Baanen

Vrije Universiteit Amsterdam

29th January 2024

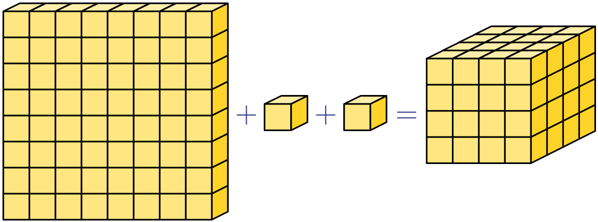


I have a set of little cubes that I can arrange into a square shape.



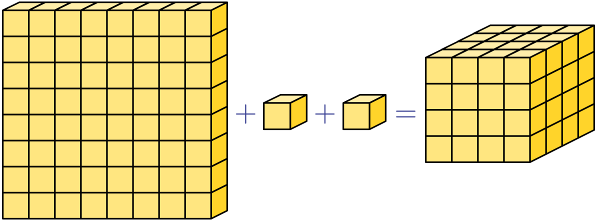
A puzzle

I have a set of little cubes that I can arrange into a square shape.
If I add two more little cubes, I can arrange them into a cube shape.



A puzzle

I have a set of little cubes that I can arrange into a square shape.
If I add two more little cubes, I can arrange them into a cube shape.



How many little cubes did I start with?

Number theory

This puzzle can be solved with number theory, studying the counting numbers $0, 1, 2, \ldots,$ addition and multiplication.
Number theory has been around for thousands of years.

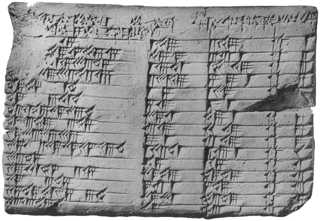


Figure: A Babylonian tablet listing solutions to $x^2 + y^2 = z^2$, 1800 BCE.

Number theory

This puzzle can be solved with number theory, studying the counting numbers $0, 1, 2, \ldots,$ addition and multiplication.
Number theory has been around for thousands of years.

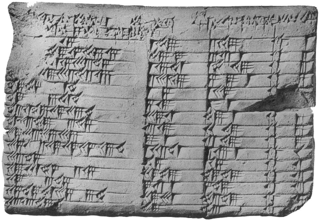


Figure: A Babylonian tablet listing solutions to $x^2 + y^2 = z^2$, 1800 BCE.

I studied algebraic number theory, using modern concepts to solve questions ancient people could have understood.

Mechanizing mathematics

Mathematicians use computers to calculate quickly and accurately.

Factor the number 44203.

`44203 is a prime number.`

Mechanizing mathematics

Mathematicians use computers to calculate quickly and accurately.

Factor the number 44203.

`44203 is a prime number.`

But we care much more about proving by logical reasoning.

Check my proof that $1 + 1 = 3$.

Mistake on line 37: missing argument $ha : a \neq 0$.

Software for checking and analyzing your proofs is called a proof assistant.

A virtual library of mathematics

The Mathlib project wants to translate ("formalize") all mathematics into the language of the proof assistant Lean.
Mathlib contains hundreds of thousands of definitions and theorems, written by hundreds of contributors, including myself.

A virtual library of mathematics

The Mathlib project wants to translate ("formalize") all mathematics into the language of the proof assistant Lean.
Mathlib contains hundreds of thousands of definitions and theorems, written by hundreds of contributors, including myself.

To formalize a proof, we need to explain all details. Computers don't have common sense!

A virtual library of mathematics

The Mathlib project wants to translate ("formalize") all mathematics into the language of the proof assistant Lean.
Mathlib contains hundreds of thousands of definitions and theorems, written by hundreds of contributors, including myself.

To formalize a proof, we need to explain all details. Computers don't have common sense!

Lemma 5.1. $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. Ask a toddler on the street.

Figure: Unfortunately Lean doesn't accept this proof tactic.

My research

I sat down with mathematicians to make the first formalization of the fundamentals of algebraic number theory (that I am aware of).

As a consequence, we:

- expanded Mathlib with more definitions and theorems.
- discovered where formalizing is still difficult.
- made formalizing easier by identifying useful idioms.
- improved the capabilities of Lean itself.

Practical applications

For mathematicians, proof assistants verify proofs are correct.
Lean can analyze proofs: “this hypothesis is not necessary”.

Practical applications

For mathematicians, proof assistants verify proofs are correct.
Lean can analyze proofs: "this hypothesis is not necessary".

For students, proof checking means instant feedback on your exercises.
Lean is interactive: click on a symbol you don't know to go to its definition.

Practical applications

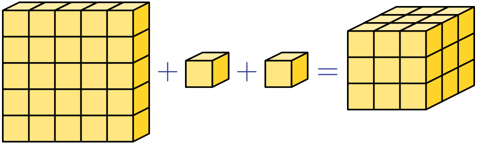
For mathematicians, proof assistants verify proofs are correct.
Lean can analyze proofs: "this hypothesis is not necessary".

For students, proof checking means instant feedback on your exercises.
Lean is interactive: click on a symbol you don't know to go to its definition.

For AI researchers, the logical reasoning of proof assistants balances the free association of large language models.
Train your model to reason logically by checking against Lean.
Or search through Mathlib if you need a fact.

The puzzle solution

I started with 25 little cubes in a 5×5 square,
and added two to get a $3 \times 3 \times 3$ cube.



This is the only solution! Read my thesis to find out why.

Sources, notes and credits

Slide 2: the clay tablet is known as Plimpton 322. Source: `https://personal.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html`

Slide 3: Robot icon by Mutant Standard, modified as part of Robomoji, CC-BY-NC-SA 4.0.

Slide 4: Lemma 5.1 comes from the study notes for *Introduction to Modular Representation Theory*, Zhiyuan Bai, `https://zb260.user.srcf.net/notes/III/modrep.pdf`.
This result has been formalized in Mathlib as `IsCyclotomicExtension.autEquivPow`.