Primes, Proofs and Computers

Antrittsvorlesung

Floris van Doorn

Mathematical Institute

15.05.2024

Computers in science and math

Computers are used extensively in science:

- To compute
- To simulate
- To record data
- To perform statistical analysis
- To write papers and books
- To exchange ideas online

$\vdots$

Computers in science and math

Computers are used extensively in science:

- To compute
- To simulate
- To record data
- To perform statistical analysis
- To write papers and books
- To exchange ideas online

$\vdots$

Mathematicians prove theorems about abstract mathematical concepts.

However, computers are rarely used for finding or checking proofs.

Formalization

A proof assistant is a program that can reason with mathematical definitions, theorems and proofs, provided a user writes these in a language that the program can understand.

This is called formalization.

Formalization

A proof assistant is a program that can reason with mathematical definitions, theorems and proofs, provided a user writes these in a language that the program can understand.

This is called formalization.

The first proof assistant Automath was developed by Dutch Mathematician De Bruijn in 1968.

A proof assistant that is popular among mathematicians is Lean, an open source program in development since 2013.

Overview of the talk

- Infinitude of primes: Euclid's proof
- Infinitude of primes: proof in Lean
- More on formalization

Primes

Definition

A natural number $(0, 1, 2, \ldots)$ is prime if it is greater than 1 and it cannot be written as the product of two smaller natural numbers.

The first few prime numbers are $2, 3, 5, 7, 11, 13, \ldots$
117 is not prime, since $117 = 3 \times 39 = 3 \times 3 \times 13$.
Every natural number greater than 1 can be written as a product of one or more prime numbers.

Primes

Definition

A natural number $(0, 1, 2, \ldots)$ is prime if it is greater than 1 and it cannot be written as the product of two smaller natural numbers.

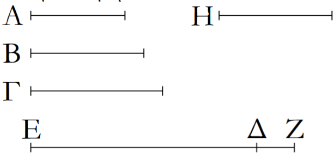
The first few prime numbers are $2, 3, 5, 7, 11, 13, \ldots$
117 is not prime, since $117 = 3 \times 39 = 3 \times 3 \times 13$.
Every natural number greater than 1 can be written as a product of one or more prime numbers.

Theorem (Euclid)

There are infinitely many prime numbers.

κ΄.

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.



Ἔστωσαν οἱ προτεθέντες πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ· λέγω, ὅτι τῶν Α, Β, Γ πλείους εἰσὶ πρῶτοι ἀριθμοί.

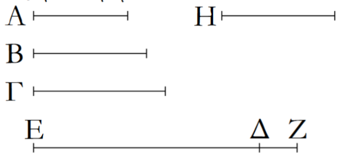
Εἰλήφθω γὰρ ὁ ὑπὸ τῶν Α, Β, Γ ἐλάχιστος μετρούμενος καὶ ἔστω ΔΕ, καὶ προσκείσθω τῷ ΔΕ μονὰς ἡ ΔΖ. ὁ δὴ ΕΖ ἤτοι πρῶτός ἐστιν ἢ οὔ. ἔστω πρότερον πρῶτος· εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ, ΕΖ πλείους τῶν Α, Β, Γ.

Ἀλλὰ δὴ μὴ ἔστω ὁ ΕΖ πρῶτος· ὑπὸ πρώτου ἄρα τινὸς ἀριθμοῦ μετρεῖται. μετρείσθω ὑπὸ πρώτου τοῦ Η· λέγω, ὅτι ὁ Η οὐδενὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. εἰ γὰρ δυνατόν, ἔστω. οἱ δὲ Α, Β, Γ τὸν ΔΕ μετροῦσιν· καὶ ὁ Η ἄρα τὸν ΔΕ μετρήσει. μετρεῖ δὲ καὶ τὸν ΕΖ· καὶ λοιπὴν τὴν ΔΖ μονάδα μετρήσει ὁ Η ἀριθμὸς ὤν· ὅπερ ἄτοπον. οὐκ ἄρα ὁ Η ἑνὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. καὶ ὑπόκειται πρῶτος. εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ πλείους τοῦ προτεθέντος πλήθους τῶν Α, Β, Γ οἱ Α, Β, Γ, Η· ὅπερ ἔδει δεῖξαι.

(Book IX, Proposition 20)

κʹ.

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.



Ἔστωσαν οἱ προτεθέντες πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ· λέγω, ὅτι τῶν Α, Β, Γ πλείους εἰσὶ πρῶτοι ἀριθμοί.

Εἰλήφθω γὰρ ὁ ὑπὸ τῶν Α, Β, Γ ἐλάχιστος μετρούμενος καὶ ἔστω ΔΕ, καὶ προσκείσθω τῷ ΔΕ μονὰς ἡ ΔΖ. ὁ δὴ ΕΖ ἤτοι πρῶτός ἐστιν ἢ οὔ. ἔστω πρότερον πρῶτος· εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ, ΕΖ πλείους τῶν Α, Β, Γ.

Ἀλλὰ δὴ μὴ ἔστω ὁ ΕΖ πρῶτος· ὑπὸ πρώτου ἄρα τινὸς ἀριθμοῦ μετρεῖται. μετρείσθω ὑπὸ πρώτου τοῦ Η· λέγω, ὅτι ὁ Η οὐδενὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. εἰ γὰρ δυνατόν, ἔστω. οἱ δὲ Α, Β, Γ τὸν ΔΕ μετροῦσιν· καὶ ὁ Η ἄρα τὸν ΔΕ μετρήσει. μετρεῖ δὲ καὶ τὸν ΕΖ· καὶ λοιπὴν τὴν ΔΖ μονάδα μετρήσει ὁ Η ἀριθμὸς ὤν· ὅπερ ἄτοπον. οὐκ ἄρα ὁ Η ἑνὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. καὶ ὑπόκειται πρῶτος. εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ πλείους τοῦ προτεθέντος πλήθους τῶν Α, Β, Γ οἱ Α, Β, Γ, Η· ὅπερ ἔδει δεῖξαι.

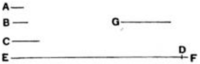
(Book IX, Proposition 20)

PROPOSITION 20.

Prime numbers are more than any assigned multitude of prime numbers.

Let *A*, *B*, *C* be the assigned prime numbers;

I say that there are more prime numbers than *A*, *B*, *C*.



For let the least number measured by *A*, *B*, *C* be taken,

and let it be *DE*;

let the unit *DF* be added to *DE*.

Then *EF* is either prime or not.

First, let it be prime;

then the prime numbers *A*, *B*, *C*, *EF* have been found which are more than *A*, *B*, *C*.

Next, let *EF* not be prime;

therefore it is measured by some prime number. [VII. 31]

Let it be measured by the prime number *G*.

I say that *G* is not the same with any of the numbers *A*, *B*, *C*.

For, if possible, let it be so.

Now *A*, *B*, *C* measure *DE*;

therefore *G* also will measure *DE*.

But it also measures *EF*.

Therefore *G*, being a number, will measure the remainder, the unit *DF*:

which is absurd.

Therefore *G* is not the same with any one of the numbers *A*, *B*, *C*.

And by hypothesis it is prime.

Therefore the prime numbers *A*, *B*, *C*, *G* have been found which are more than the assigned multitude of *A*, *B*, *C*.

Q. E. D.

(translation by Thomas Little Heath, 1908)

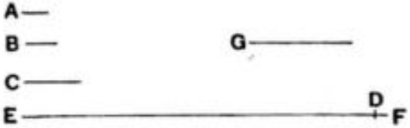
PROPOSITION 20.

Prime numbers are more than any assigned multitude of prime numbers.

Let A, B, C be the assigned prime numbers;

I say that there are more prime numbers than A, B, C.

For let the least number measured by A, B, C be taken,



and let it be DE;

let the unit DF be added to DE.

Then EF is either prime or not.

First, let it be prime;

then the prime numbers A, B, C, EF have been found which are more than A, B, C.

Next, let EF not be prime;

therefore it is measured by some prime number. [VII. 31] are more than A, B, C.

Next, let EF not be prime;

therefore it is measured by some prime number. [VII. 31]

Let it be measured by the prime number G.

I say that G is not the same with any of the numbers A, B, C.

For, if possible, let it be so.

Now A, B, C measure DE;

therefore G also will measure DE.

But it also measures EF.

Therefore G, being a number, will measure the remainder, the unit DF:

which is absurd.

Therefore G is not the same with any one of the numbers A, B, C.

And by hypothesis it is prime.

Therefore the prime numbers A, B, C, G have been found which are more than the assigned multitude of A, B, C.

Q. E. D.

Proof in Lean

Demo:

```
theorem Euclid
  (P : finite subset of ℕ)
  (hP : for all p in P, p is prime) :
  exists p,
  p is prime and p is not in P
```

Lean's mathematical library

Lean has a mathematical library with results from many fields in mathematics:
algebra, analysis, geometry, probability theory, combinatorics, logic, topology, category theory, ...

It is large: Mathlib has over 1 million lines of code, with thousands of definitions and theorems written by over 300 contributors.

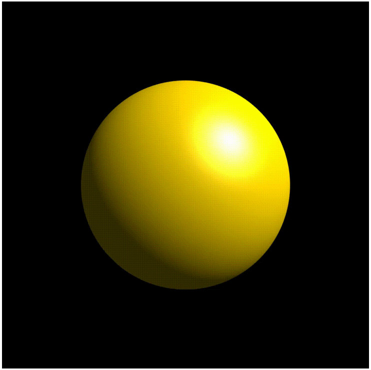
It is actively developed: There are more than 100 contributions every week, reviewed by the maintainers.

Sphere eversion

Can we turn a sphere inside out?

Rules:

- No tears or sharp creases;
- It is allowed to self-intersect.

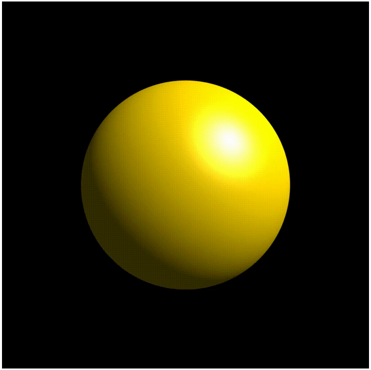


Sphere eversion

Can we turn a sphere inside out?

Rules:

- No tears or sharp creases;
- It is allowed to self-intersect.



Sphere eversion

Theorem (Smale, 1957)

There is a smooth transformation of immersions

$$\mathbb{S}^2 \to \mathbb{R}^3$$

from the inclusion map to the antipodal map.

This follows from a deep result in differential geometry.

Theorem (Gromov, 1973)

If $\mathcal{R}$ is an open and ample partial differential relation for functions between manifolds M and N then $\mathcal{R}$ satisfies the homotopy principle.

In 2022 I formalized these theorems in Lean together with Patrick Massot and Oliver Nash.

Why formalize mathematics?

1. Collaboratively create a unified mathematical library
   - We are creating a large repository of mathematical knowledge.

Why formalize mathematics?

1. Collaboratively create a unified mathematical library
   - We are creating a large repository of mathematical knowledge.
2. Check proofs
   - A proof assistant ensures the correctness of results.
   - A computer-verified result is easier to peer-review.

Why formalize mathematics?

1. Collaboratively create a unified mathematical library
   - We are creating a large repository of mathematical knowledge.
2. Check proofs
   - A proof assistant ensures the correctness of results.
   - A computer-verified result is easier to peer-review.
3. Teach mathematics
   - The proof assistant forces students to write structured proofs and gives immediate feedback.

Why formalize mathematics?

1. Collaboratively create a unified mathematical library
   - We are creating a large repository of mathematical knowledge.
2. Check proofs
   - A proof assistant ensures the correctness of results.
   - A computer-verified result is easier to peer-review.
3. Teach mathematics
   - The proof assistant forces students to write structured proofs and gives immediate feedback.
4. Create new mathematics
   - Being forced to write rigorous proofs leads one to gain new insights in mathematics.
   - Potentially in the future by AI.

Thanks for listening

Questions?

Sphere eversion, formalized

```
theorem sphere_eversion :
  ∃ f : ℝ → 𝕊² → ℝ³,
  smooth (↿f : ℝ × 𝕊² → ℝ³) ∧
  f 0 = (coe : 𝕊² → ℝ³) ∧
  f 1 = (-coe : 𝕊² → ℝ³) ∧
  ∀ t, immersion (f t)
```

The homotopy principle

Theorem (Gromov, 1973)

If $\mathcal{R}$ is an open and ample[1] *partial differential relation for functions between manifolds M and N then $\mathcal{R}$ satisfies the homotopy principle, i.e. any formal solution can be smoothly deformed into a holonomic one inside $\mathcal{R}$.*

[1] Ampleness is a geometric condition that ensures that certain convex hulls are large enough for the convex integration argument to work.