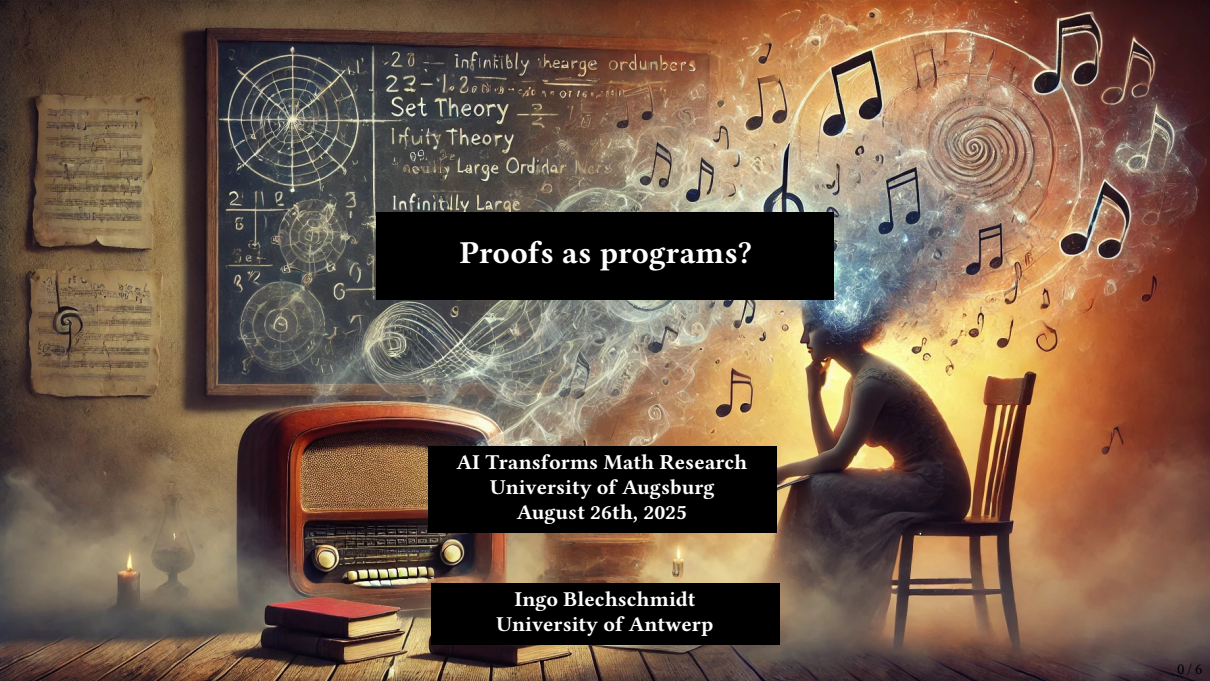
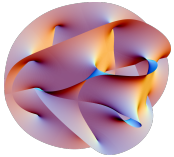


Proofs as programs?

AI Transforms Math Research
University of Augsburg
August 26th, 2025

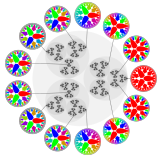
Ingo Blechschmidt
University of Antwerp

In this talk



commutative algebra and number theory

numerical content



a fractal without points

foundational crisis

traveling the multiverse

monadic side effects

proof assistants

alien algorithms

A first glimpse of proof mining

Theorem. For every natural number n, there is a prime number larger than n.

Proof (Euclid). Every prime factor of $n! + 1$ will do. □

A first glimpse of proof mining

Theorem. For every natural number n, there is a prime number larger than n.

Proof (Euclid). Every prime factor of $n! + 1$ will do. □

Let $p_0, p_1, p_2, \ldots$ be the sequence of prime numbers.
Scholium. $p_{n+1} \leq p_n! + 1$.
Scholium. $p_n \leq 2^{2^n}$.

A first glimpse of proof mining

Theorem. For every natural number n, there is a prime number larger than n.

Proof (Euclid). Every prime factor of $n! + 1$ will do. □

Let $p_0, p_1, p_2, \ldots$ be the sequence of prime numbers.
Scholium. $p_{n+1} \leq p_n! + 1$.
Scholium. $p_n \leq 2^{2^n}$.

Proof (Euler). If there were only finitely many primes, the identity

$$\prod_p \frac{1}{1 - 1/p} = \sum_{n \geq 1} \frac{1}{n}$$

would imply that the harmonic series converges. □

Scholium. $p_n \leq \lceil e^{n+1-\gamma} \rceil$.

Proof mining in convex analysis

Theorem (zero displacement conjecture). Let H be a Hilbert space. Let $C_1, \ldots, C_N \subseteq H$ be nonempty closed convex subsets with orthogonal projections P_{C_i}. Let $T = P_{C_N} \circ \ldots \circ P_{C_1}$. Then for every $x \in H$,

$$\|T^{n+1}x - T^n x\| \xrightarrow{n\to\infty} 0.$$

Proof. See [Bauschke 2003], employing Minty's theorem, the Brézis–Haraux theorem, Rockafellar's maximal monotonicity and sum theorems, strongly nonexpansive mappings, conjugate functions, normal cones, … □

Proof mining in convex analysis

Theorem (zero displacement conjecture). Let H be a Hilbert space. Let $C_1, \ldots, C_N \subseteq H$ be nonempty closed convex subsets with orthogonal projections P_{C_i}. Let $T = P_{C_N} \circ \ldots \circ P_{C_1}$. Then for every $x \in H$,

$$\|T^{n+1}x - T^n x\| \xrightarrow{n\to\infty} 0.$$

Proof. See [Bauschke 2003], employing Minty's theorem, the Brézis–Haraux theorem, Rockafellar's maximal monotonicity and sum theorems, strongly nonexpansive mappings, conjugate functions, normal cones, … □

Scholium [Kohlenbach 2018]. In this situation, let b be an upper bound on the norm of x and let K be an upper bound on the norm of N arbitrary points $c_i \in C_i$. Then

$$\forall \varepsilon > 0.\, \forall n \geq \phi(\varepsilon, N, b, K).\, \|T^{n+1}x - T^n x\| < \varepsilon,$$

where $\phi(\varepsilon, N, b, K)$ is given by a certain explicit formula.

Proof mining in approximation theory

Let $n \in \mathbb{N}$. Let P_n be the space of polynomials of degree at most n.
Let $f \in C[0,1]$ be a continuous function.

Theorem. There is a **unique** best L^1-approximation of f in P_n.

Proof mining in approximation theory

Let $n \in \mathbb{N}$. Let P_n be the space of polynomials of degree at most n.
Let $f \in C[0,1]$ be a continuous function.

Theorem. There is a **unique** best L^1-approximation of f in P_n.

Let ω be a **modulus of uniform continuity** for f, i.e. a function $\mathbb{R}^+ \to \mathbb{R}^+$ such that

$$\forall x, \tilde{x} \in [0,1].\, \forall \varepsilon > 0.\, \big(|x - \tilde{x}| < \omega(\varepsilon) \Longrightarrow |f(x) - f(\tilde{x})| < \varepsilon\big).$$

Scholium [Kohlenbach 1990]. $\forall \varepsilon > 0.\, \forall p_1, p_2 \in P_n.$

$$\bigwedge_{i=1}^{2} \big(\|f - p_i\|_1 - \mathrm{dist}_1(f, P_n) < \phi(\omega, n, \varepsilon)\big) \Longrightarrow \|p_1 - p_2\|_1 \leq \varepsilon,$$

where $\phi(\omega, n, \varepsilon)$ is given by a certain explicit formula.

Backed by logical metatheorems?

Metatheorems for backing proof mining have been and are being developed which …

- 🧮 guarantee the **extractability** of suitable numerical information in principle (bounds, convergence rates, moduli of uniqueness, rates of asymptotic regularity, …),
- 🤖 describe an **algorithm** for carrying out the extraction and
- 📦 support **modular treatments** of auxiliary lemmas,

provided the input proof is **formally** supplied in a **certain system**.
[Kohlenbach–Oliva 2002]

Backed by logical metatheorems?

Metatheorems for backing proof mining have been and are being developed which …

- 🧮 guarantee the **extractability** of suitable numerical information in principle (bounds, convergence rates, moduli of uniqueness, rates of asymptotic regularity, …),
- 🤖 describe an **algorithm** for carrying out the extraction and
- 📦 support **modular treatments** of auxiliary lemmas,

provided the input proof is **formally** supplied in a **certain system**.
[Kohlenbach–Oliva 2002]

In practice (2025): Algorithms **not** used, only followed as **rough guidelines**, combined with hand-rolled optimizations. **Let us explore tool support!**

Backed by logical metatheorems?

Metatheorems for backing proof mining have been and are being developed which …

- 🧮 guarantee the **extractability** of suitable numerical information in principle (bounds, convergence rates, moduli of uniqueness, rates of asymptotic regularity, …),
- 🤖 describe an **algorithm** for carrying out the extraction and
- 📦 support **modular treatments** of auxiliary lemmas,

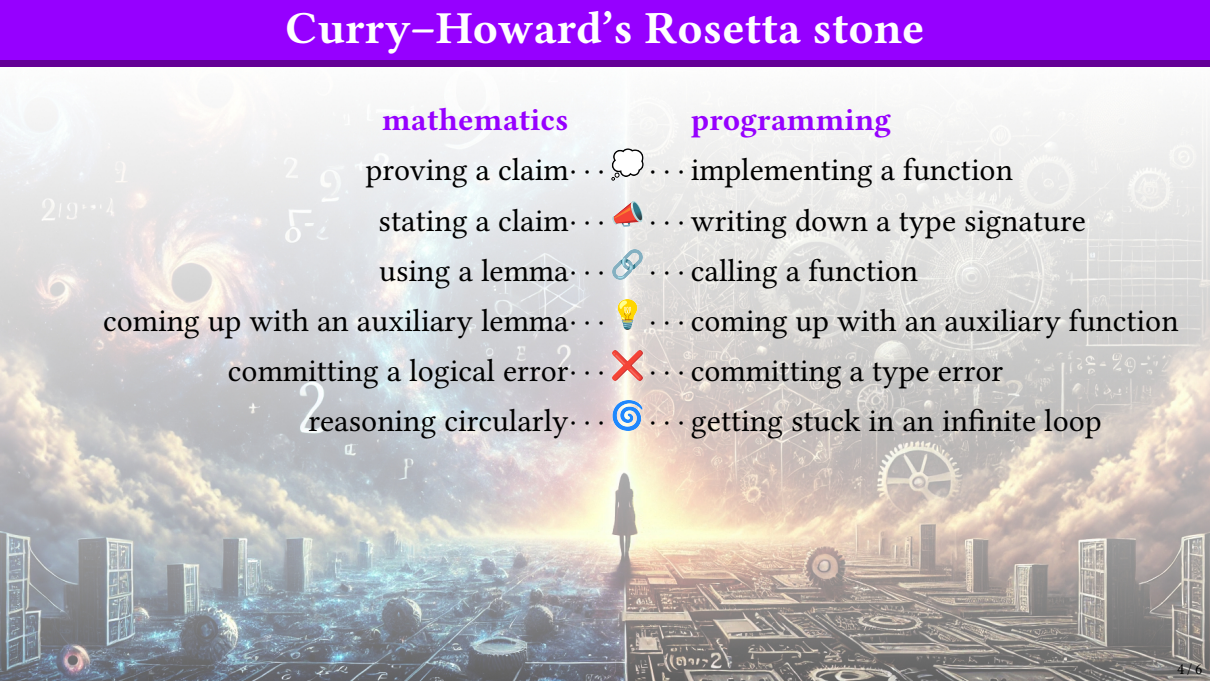
provided the input proof is **formally** supplied in a **certain system**.
[Kohlenbach–Oliva 2002]

In practice (2025): Algorithms **not** used, only followed as **rough guidelines**, combined with hand-rolled optimizations. **Let us explore tool support!**

NB: The **quality** of the extracted data depends on the **sophistication** of the **logical principles** used in the proof (Heine–Borel, Bolzano–Weierstraß, …).

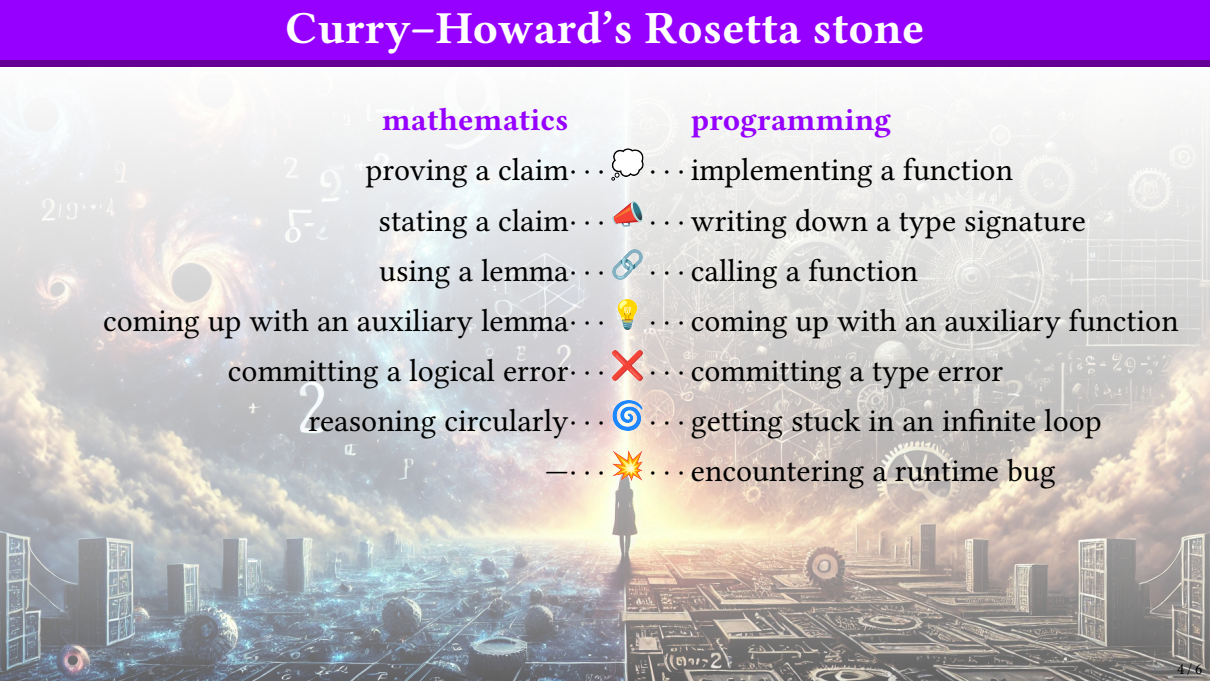
Curry–Howard's Rosetta stone

mathematics		programming
proving a claim	💭	implementing a function
stating a claim	📣	writing down a type signature
using a lemma	🔗	calling a function
coming up with an auxiliary lemma	💡	coming up with an auxiliary function
committing a logical error	❌	committing a type error
reasoning circularly	🌀	getting stuck in an infinite loop



Curry–Howard's Rosetta stone

mathematics		programming
proving a claim	💭	implementing a function
stating a claim	📣	writing down a type signature
using a lemma	🔗	calling a function
coming up with an auxiliary lemma	💡	coming up with an auxiliary function
committing a logical error	❌	committing a type error
reasoning circularly	🌀	getting stuck in an infinite loop
—	💥	encountering a runtime bug

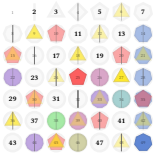


Curry–Howard's Rosetta stone

mathematics		programming
proving a claim	💭	implementing a function
stating a claim	📣	writing down a type signature
using a lemma	🔗	calling a function
coming up with an auxiliary lemma	💡	coming up with an auxiliary function
committing a logical error	❌	committing a type error
reasoning circularly	🌀	getting stuck in an infinite loop
—	💥	encountering a runtime bug

To extract numerical data from a proof,
run the proof.

Three case studies

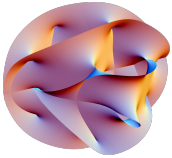


Theorem. For every natural number n, there is a prime larger than n.

Proof. Every prime factor of $n! + 1$ will do. □

Theorem. Every infinite sequence $f : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $f(i) \leq f(j)$.

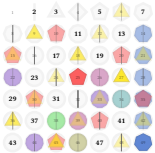
Proof. There is a minimal value $f(i)$. Set $j := i + 1$. □



Theorem. Let M be a surjective matrix with more rows than columns over a commutative ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is still surjective over $A/\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, this is a contradiction to basic linear algebra. □

Three case studies

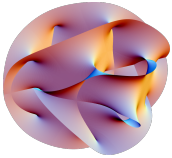


Theorem. For every natural number n, there is a prime larger than n.

Proof. Every prime factor of $n! + 1$ will do. □

Theorem. Every infinite sequence $f : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $f(i) \leq f(j)$.

Proof. There is a minimal value $f(i)$. Set $j := i + 1$. □



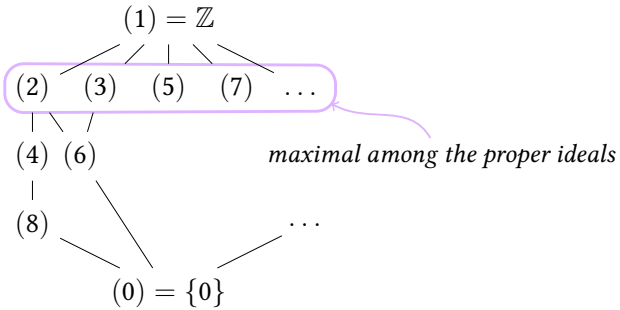
Theorem. Let M be a surjective matrix with more rows than columns over a commutative ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is still surjective over $A/\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, this is a contradiction to basic linear algebra. □

A case study in commutative algebra

Theorem. Let M be a surjective matrix with more rows than columns over a commutative ring A. Then $1 = 0$ in A.

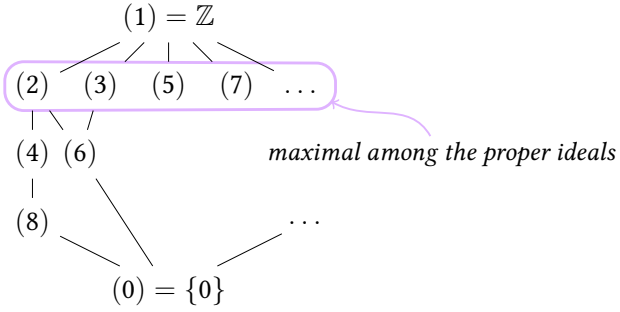
Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is still surjective over $A/\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, this is a contradiction to basic linear algebra. □



A case study in commutative algebra

Theorem. Let M be a surjective matrix with more rows than columns over a commutative ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is still surjective over $A/\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, this is a contradiction to basic linear algebra. □



Proof. Write $M = \binom{x}{y}$. By surjectivity, have $u, v \in A$ with $u\binom{x}{y} = \binom{1}{0}$ and $v\binom{x}{y} = \binom{0}{1}$. Hence $1 = (vy)(ux) = (uy)(vx) = 0$. □

Maximal ideals as convenient fictions?

- In classical mathematics, every ring has a maximal ideal by Zorn's lemma.

Maximal ideals as convenient fictions?

- In classical mathematics, every ring has a maximal ideal by Zorn's lemma.
- Without Zorn, at least every countable ring $A = \{x_0, x_1, \ldots\}$ has a maximal ideal.
  – Iterative construction given an ideal membership test [Krull 1929]:

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

Maximal ideals as convenient fictions?

- In classical mathematics, every ring has a maximal ideal by Zorn's lemma.
- Without Zorn, at least every countable ring $A = \{x_0, x_1, \ldots\}$ has a maximal ideal.
  – Iterative construction given an ideal membership test [Krull 1929]:

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

  – Also without membership test! [Krivine 1996], [Berardi–Valentini 2004]

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \mathfrak{m}_n + \underbrace{(\{x_n \mid 1 \notin \mathfrak{m}_n + (x_n)\})}_{\text{a certain subsingleton set}}$$

Maximal ideals as convenient fictions?

- In classical mathematics, every ring has a maximal ideal by Zorn's lemma.
- Without Zorn, at least every countable ring $A = \{x_0, x_1, \ldots\}$ has a maximal ideal.
  – Iterative construction given an ideal membership test [Krull 1929]:

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

  – Also without membership test! [Krivine 1996], [Berardi–Valentini 2004]

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \mathfrak{m}_n + (\underbrace{\{x_n \mid 1 \notin \mathfrak{m}_n + (x_n)\}}_{\text{a certain subsingleton set}})$$

- Without Zorn, **every** ring has a maximal ideal in a "suitable **forcing extension** of the universe" [B.–Schuster 2024]. In plain terms: **Approximate** a (perhaps non-existing) surjection $\mathbb{N} \twoheadrightarrow A$ by partial functions which can **grow on demand**.