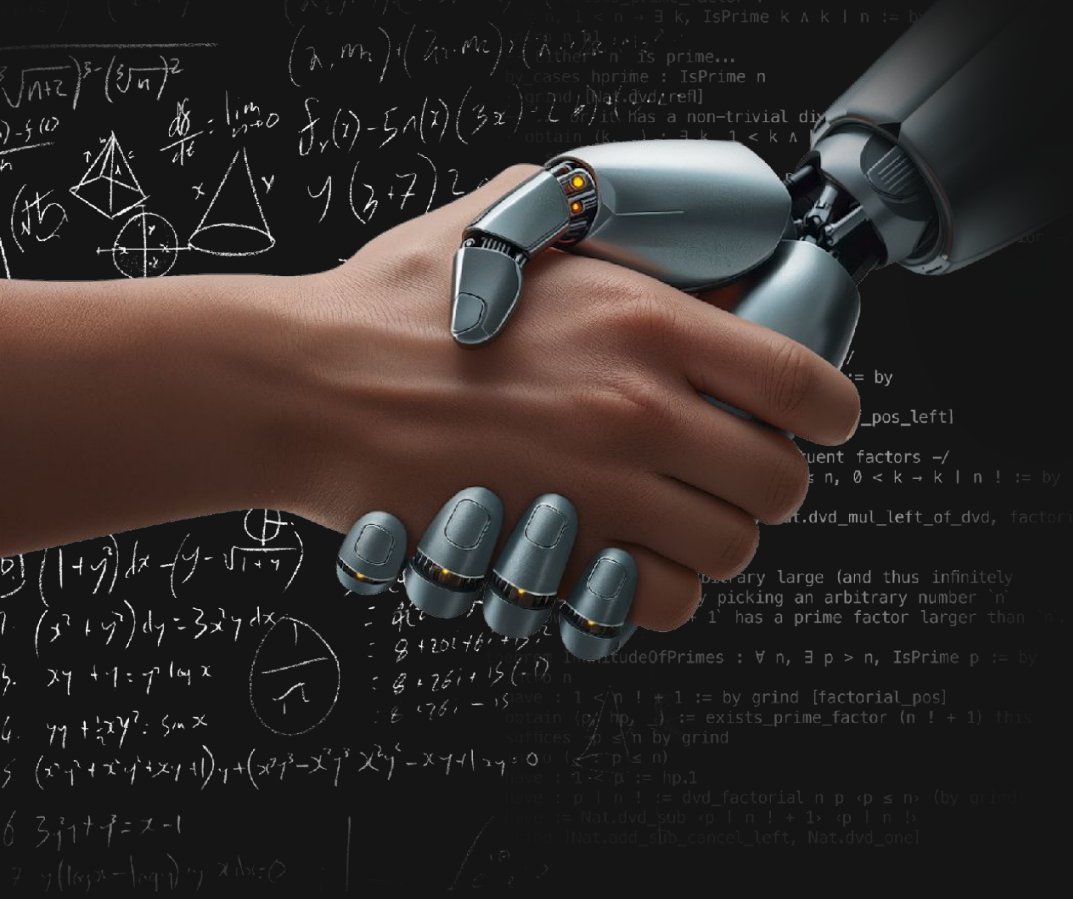


ItaLean 2025

Bridging Formal Mathematics and AI

Bologna, Italy | December 9-12, 2025

The Formal Conjectures Project

Moritz Firsching

formal-conjectures

Lean formalisations

formal-conjectures

Lean formalisations of (mostly) unsolved math problems

https://github.com/google-deepmind/formal-conjectures/

Goals:

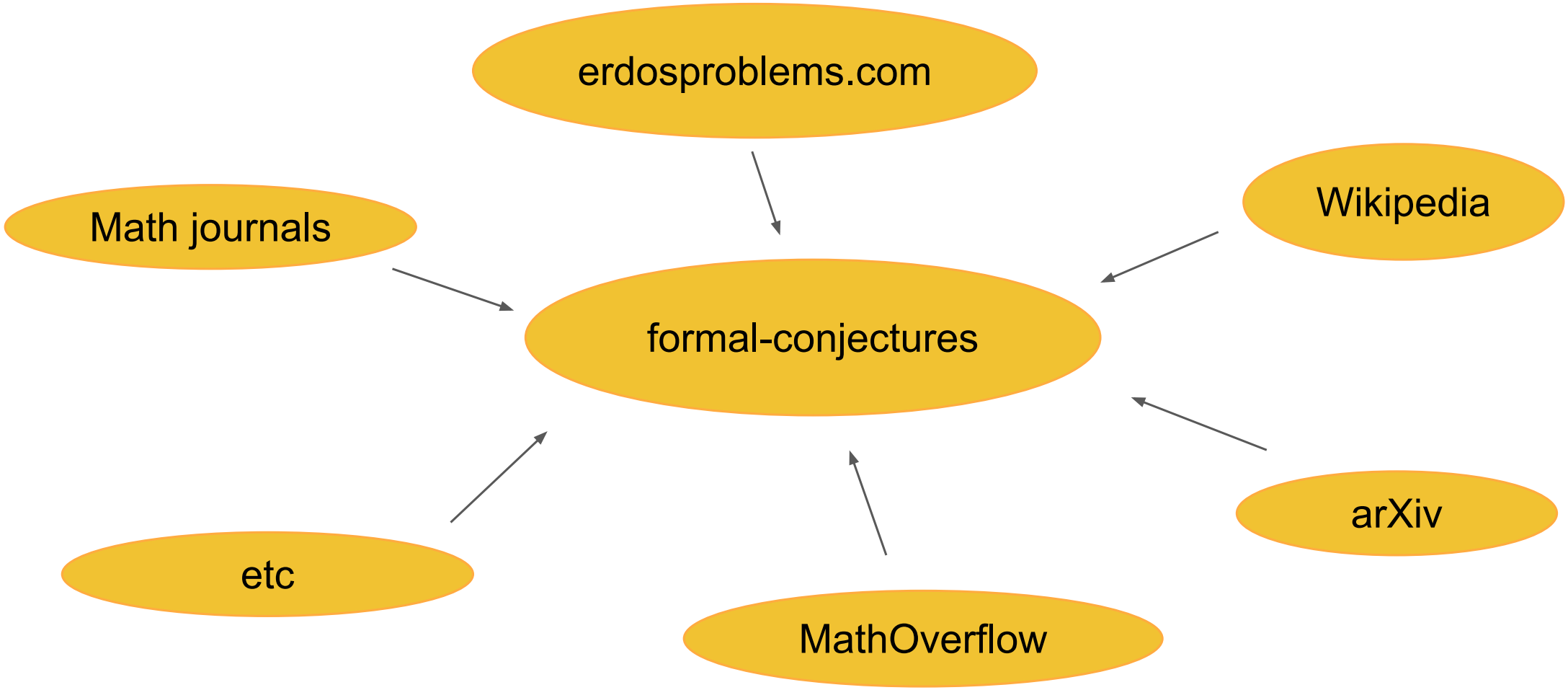
1. Community-driven universal library of formal statements of conjectures
2. Benchmark for automated theorem-proving & autoformalisation
3. Way for community to interact with proving agents

Challenges:

1. Misformalisations
2. limits of Mathlib
3. Review bottleneck

Sources

let’s collect every interesting conjecture!



High level overview

What kind of problems?

- Open problems
- Solved research problems
- When useful (e.g. sanity checks), easier related problems

Format:

- Allow problems requiring an answer (“find the largest n such that…”) ✅
- Can add definitions/results missing from Mathlib ✅
  - Useful testing ground before adding to Mathlib!

Examples: super famous conjecture simple to state

```
/--
The Odd Perfect Number Conjecture states that all perfect numbers are even.
-/
@[category research open, AMS 11]
theorem odd_perfect_number_conjecture (n : ℕ) (hn : Perfect n) : Even n := by
  sorry
```

Examples: open ended questions

Common case: “Is is true that ...” (used for every conjecture phrased as question)

```
/--
Are there infinitely many primes p such that p + 2 is prime?
-/
@[category research open, AMS 11]
theorem twin_primes :
    {p : ℕ | Prime p ∧ Prime (p + 2)}.Infinite ↔ answer(sorry) := by
  sorry
```

Examples: open ended questions

Asking for a numeric answer: In this example you'd need to put 5, 6 or 7.

```
/--
The Hadwiger–Nelson problem asks: How many colors are required to color the plane
such that no two points at distance 1 from each other have the same color?
-/
@[category research open, AMS 52]
theorem HadwigerNelsonProblem :
    (UnitDistancePlaneGraph ℝ).chromaticNumber = answer(sorry) := by
  sorry
```

Examples: open ended questions

Asking for asymptotics

```
@[category research open, AMS 11]
theorem erdos_409.parts.i.variants.isTheta (c : ℕ → ℕ)
    (h : ∀ n > 0, IsLeast { i | (φ · + 1)^[i] n |>.Prime } (c n)) :
    (fun n => (c n : ℝ)) =θ[atTop] (answer(sorry) : ℕ → ℝ) := by
  sorry
```

Additional information

Each problem is annotated with some metadata:

- Informal problem statement
- Area(s) of mathematics (AMS MSC classification)
- Category (solved/unsolved research question, etc)
- Source

Future ideas for additional information:

- expected hardness? Objectively: time since stated, subjectively: ?
- for solved problems: pointer to solution (informal/formal)

Reference

```
/-!
# Mathoverflow 21003

Is there any polynomial $f(x, y) \in \mathbb{Q}[x, y]$ such that
$f : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ is a bijection?

*Reference:* [mathoverflow/21003](https://mathoverflow.net/questions/21003)
asked by user [*Z.H.*](https://mathoverflow.net/users/5098/z-h)
-/

Paul Lezeau, 4 months ago | 2 authors (Bhavik Mehta and one other)
namespace Mathoverflow21003

/--
Is there any polynomial $f(x, y) \in \mathbb{Q}[x, y]$ such that
$f : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ is a bijection?
-/
@[category research open, AMS 12]
theorem mathoverflow_21003 :
    (∃ f : MvPolynomial (Fin 2) ℚ, Function.Bijective fun x ↦ f.eval x) ↔ answer(sorry) := by
  sorry

end Mathoverflow21003
```

Informal statement

Answer
(here true or false)

Category and subject

Current stats

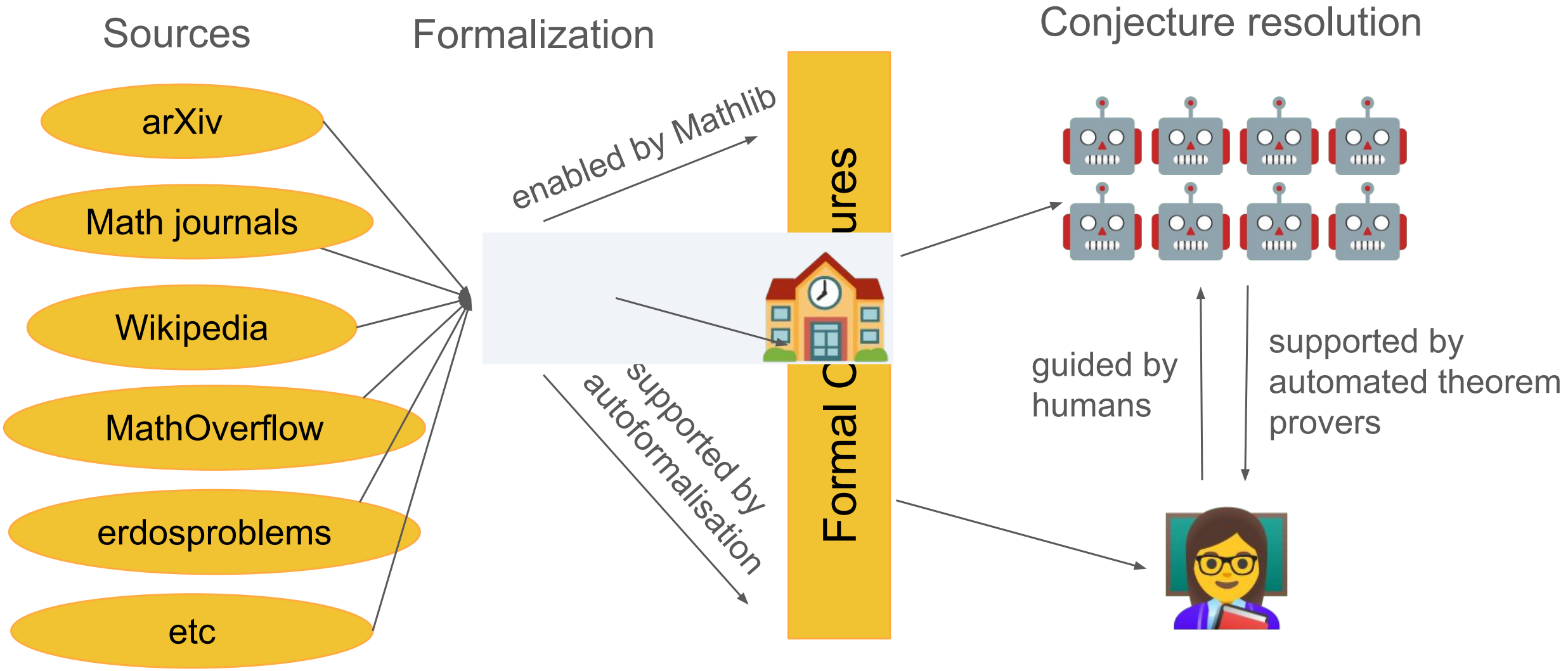
592 open conjectures and

395 solved problems, i.e. statements where an informal proof is available.

Mainly number theory and combinatorics currently.

Most statements require little definitions on top of mathlib to formulate them.

Formal Conjectures as interface between humans and AI



Challenge: misformalisations

Misformalisation: “A disagreement between the *intended* informal statement and the formalised statement.”

Different kinds of misformalization:

- Lean/mathlib footguns (e.g. 1/2 in Nat, Nat.digits, dummy values in general)
- typos
- misunderstanding of implicit assumptions
- literal interpretation of informal statement

Mitigations:

- use AlphaProof to find some misformalisations
- Test statements / known results with formal proofs

Example 1: Erdős Problem #477 (AlphaProof)

OPEN

Let $f : \mathbb{Z} \to \mathbb{Z}$ be a polynomial of degree at least 2. Is there a set A such that every $z \in \mathbb{Z}$ has exactly one representation as $z = a + f(n)$ for some $a \in A$ and $n \in \mathbb{Z}$?

#477: [ErGr80] number theory

```
-/
@[category research open, AMS 12]
theorem erdos_477 : (∀ (f : Polynomial ℤ), 2 ≤ f.degree →
-     (∃ (A : Set ℤ), ∀ z, ∃! a ∈ A ×ˢ Set.range f.eval, z = a.1 + a.2)) ↔ answer(sorry) := by
+     (∃ (A : Set ℤ), ∀ z, ∃! a ∈ A ×ˢ (f.eval '' {n | 0 < n}), z = a.1 + a.2)) ↔ answer(sorry) := by
+   sorry
+
```

OPEN

Let $f : \mathbb{Z} \to \mathbb{Z}$ be a polynomial of degree at least 2. Is there a set A such that every $z \in \mathbb{Z}$ has exactly one representation as $z = a + f(n)$ for some $a \in A$ and $n \geq 1$?

#477: [ErGr80,p.95] number theory

Example 2: Erdős Problem #728 (AlphaProof)

OPEN

Let $C > 0$ and $\epsilon > 0$ be sufficiently small. Are there infinitely many integers a, b, n with $a \geq \epsilon n$ and $b \geq \epsilon n$ such that

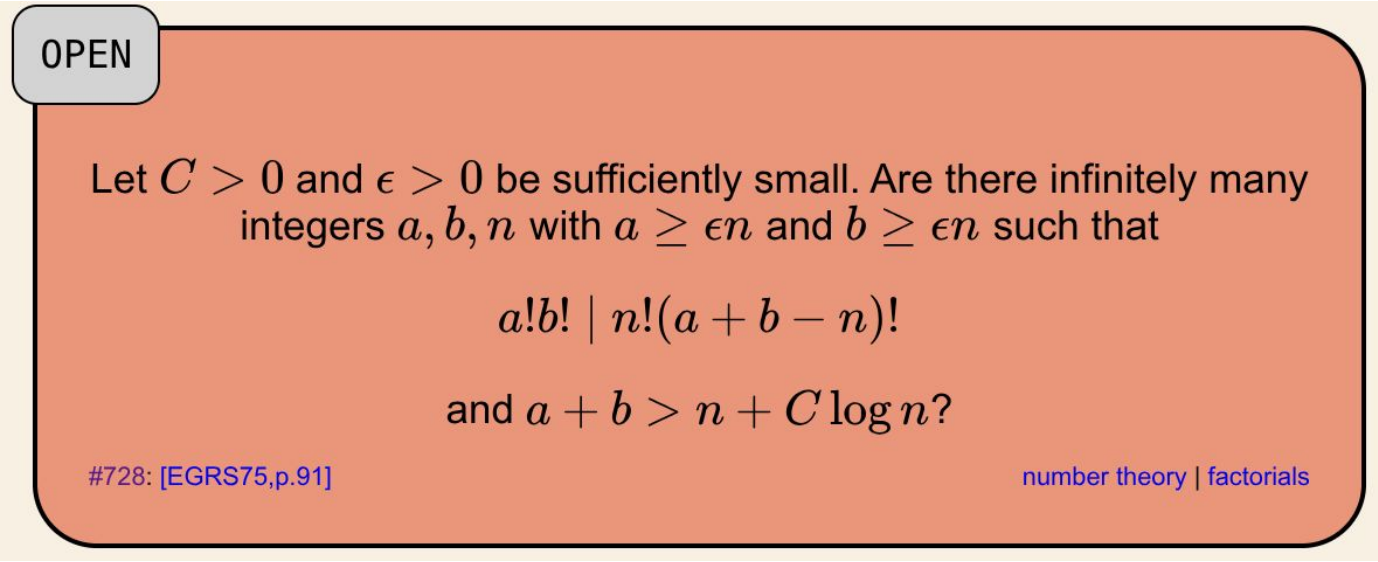
$$a!b! \mid n!(a+b-n)!$$

and $a + b > n + C \log n$?

#728: [EGRS75,p.91]

number theory | factorials

Example 2: Erdős Problem #728 (AlphaProof)



trivially provable: works even for n=0 and n=1
AlphaProof found that trivial proof
Clearly this was not intended:
Should be quantified differently: “for all n” instead of “there is an n”

=> Look at the original paper of Erdős, Graham, Ruzsa, and Straus

Example 2: Erdős Problem #728 (AlphaProof)

More precisely, is the following result true: To every c there is a k so that for infinitely many n (all $n > n_0(k, c)$?) there are suitable a and b such that $a + b > n + c \log n$ and $n!/a!b!$ has no prime factor $> k$ in its denominator? Also, suppose $a > \epsilon n$, $b > \epsilon n$, and $a + b > n + c \log n$. Can it happen that $n!(a + b - n)!/a!b!$ is an integer?

For real constants $\epsilon, C > 0$ and all integers $n > 0$, there are integers a, b such that $a > \varepsilon n$, $b > \varepsilon n$,

$$a!b! \mid n!(a+b-n)!$$

and $a + b > n + C \log n$.

AlphaProof can solve that version

```
/--
Let $\varepsilon, C > 0$. Let $n > 0$ be an integer. Are there integers $a, b$ such that
$$a > \varepsilon n,\quad b > \varepsilon n, \quad a!\, b! \mid n!\, (a + b - n)!, $$
and
$$ a + b > n + C \log n ?$$
-/
@[category test, AMS 11]
theorem erdos_728.variants.forall :
    (∀ (ε C : ℝ) (hε : 0 < ε) (hC : 0 < C) (n : ℕ) (_: 0 < n),
    ∃ a b : ℕ, ε * n < a ∧ ε * n < b ∧
    Nat.factorial a * Nat.factorial b | Nat.factorial n * Nat.factorial (a + b - n) ∧
    a + b > n + C * Real.log n) := by
    classical (aesop)
    cases exists_nat_gt<|ε*n⊔C*.log n
    simp_rw [max_lt_iff]at*
    use n+ (by valid+1)
    simp_all[mul_assoc, add_assoc,←Nat.choose_mul_factorial_mul_factorial le_self_add]
    aesop
    · {linarith only [@@ left] }
    · use(n+(w+1)).choose n*(w+1)-1,left.trans_le (mod_cast w.le_pred_of_lt
      ((Nat.le_mul_of_pos_left _)<|Nat.choose_pos le_self_add))
      use (by field_simp [mul_assoc, mul_left_comm, mul_dvd_mul,Nat.succ_le,
        Nat.choose_pos]),by linarith
/--
```

Example 2: Erdős Problem #728 (AlphaProof)

More precisely, is the following result true: To every c there is a k so that for infinitely many n (all $n > n_0(k, c)$?) there are suitable a and b such that $a + b > n + c \log n$ and $n!/a!b!$ has no prime factor $> k$ in its denominator? Also, suppose $a > \epsilon n$, $b > \epsilon n$, and $a + b > n + c \log n$. Can it happen that $n!(a + b - n)!/a!b!$ is an integer?

For real constants ε close to 0, and for infinitely many integers n, there are integers a, b such that $\varepsilon n < a < n$ and $\varepsilon n < b < n$

$$a!b! \mid n!(a+b-n)!$$

and $a + b > n + C \log n$.

AlphaProof can solve that version too

```
theorem erdos_728 (C : ℝ) (hC : 0 < C) :
    ∀ᶠ ε : ℝ in 𝓝[>] 0, ∃ᶠ n : ℕ in atTop,
      ∃ a < n, ∃ b < n,
        ε * n < a ∧ ε * n < b ∧
        a.factorial * b.factorial | n.factorial * (a + b - n).factorial ∧
        n + C * Real.log n < a + b := by
  nontriviality ℝ
  filter_upwards[Ioo_mem_nhdsGT (by bound: (1: ℝ)/16 > 0)] with S ⟨a, _⟩
  apply Filter.frequently_atTop.2 fun and=>((((Real.tendsto_log_atTop.comp
    (tendsto_natCast_atTop_atTop)).const_mul_atTop (by bound: 1/16-S > 0)).eventually_gt_atTop
    C).exists_forall_of_atTop.elim) ?_
  use fun A B=> (and+A+4).exists_infinite_primes.elim fun a s=> ⟨a*2,by valid, a*2-1,by valid,?_⟩
  obtain ⟨k, rfl⟩:=a.exists_eq_succ_of_ne_zero (by valid)
  field_simp[add_mul,Real.log_mul,Nat.factorial] at B⊢
  use (k + 1),by valid,by nlinarith, (@Nat.cast_succ ℝ _ _).symm▸by nlinarith
  constructor
  · exact (by valid : (k : ℕ)* (2)+1+ (k + 1) -(k *2+ (2))= k).symm▸
    (k : ℕ).factorial_succ▸(2, (by ring!))
  have:=(k*2+2 :ℝ).exp_log<|by bound
  have:=(k*2+2 :ℝ).log.sum_le_exp_of_nonneg (by bound) (3)
  norm_num[ Finset.sum_range_succ,Nat.factorial,show k*2+2+C*.log (k*2+2)<k*2+1+
    (k + 1)by nlinarith[mul_pos a (by bound:Real.log (k*2+2)>0),(B (k + 1) (by valid))] + 1]
  have:=(k*2+2 :ℝ).log.sum_le_exp_of_nonneg (by bound) 4
  simp_all![Finset.sum_range_succ]
  nlinarith[ (by bound: S*.log (k*2+2)≥0),show(k*2+2 : ℝ) = _ by norm_cast▸ (B _) (by valid),
    (mod_cast (by valid): 1 ≤(k : ℝ))]
```

Example 2: Erdős Problem #728 (AlphaProof)

More precisely, is the following result true: To every c there is a k so that for infinitely many n (all $n > n_0(k, c)$?) there are suitable a and b such that $a + b > n + c \log n$ and $n!/a!b!$ has no prime factor $> k$ in its denominator? Also, suppose $a > \epsilon n$, $b > \epsilon n$, and $a + b > n + c \log n$. Can it happen that $n!(a + b - n)!/a!b!$ is an integer?

For real constants ε close to 0, and for infinitely many integers n, there are integers a, b such that $\varepsilon n < a < n(1 - \varepsilon)$ and $\varepsilon n < b < n(1 - \varepsilon)$

$$a!b! \mid n!(a + b - n)!$$

and $a + b > n + C \log n$.

Unclear if this is the intended version.
=> Clarify questions by formalizing statements

Autoformalisation

- yes, please!
- more than half of the contributions from the last month used at least some kind of autoformalisation
- focus on reviewing (also potentially AI assisted?)

Community contributions ❤️

- 84 contributors
- 41 returning contributors (i.e. > 1 commit)

For some contributors their first lean experience!

Easy start for mathematicians not fluent in Lean.

Has been used in a class setting
(Floris van Doorn & Michael Rothgang)

What are your favorite conjectures?!

Moritz Firsching
Paul Lezeau
Salvatore Mercuri
Calle Sönne
Eric Wieser
Bhavik Mehta
Reklle
Yaël Dillies
Seewoo Lee
Junyan Xu
Anirudh Rao
Divyanshu Ranjan
Bolton Bailey
Ed Wagstaff
Yan Yablonovskiy
peabrainiac
Alex Kontorovich
…

You?

Questions?
Suggestions?

github.com/google-deepmind/formal-conjectures


Thanks to the organizers!