Are short proofs hard to find?



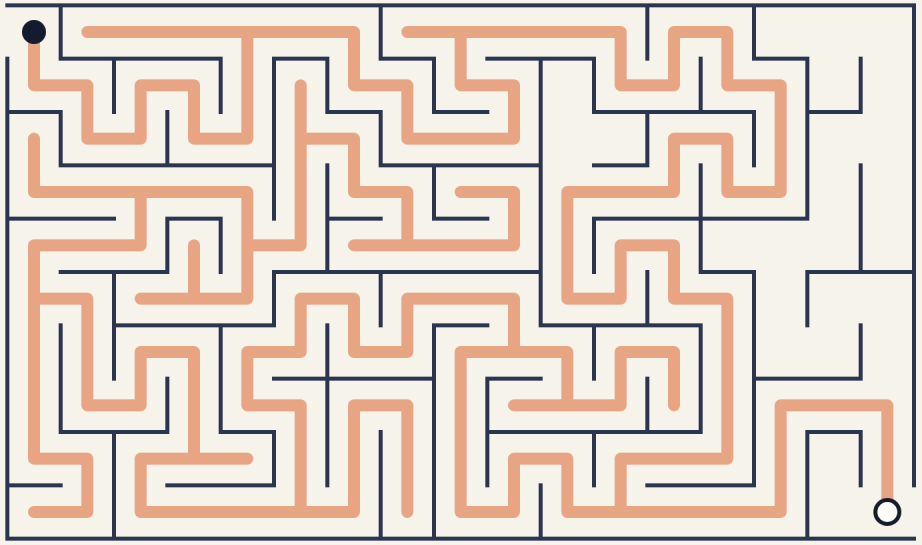
Andrew V. Sutherland · MIT · RESI

Joint work with Alexa McLain, part of the DARPA expMath program

Computations implemented with LLM coding agents.
Claude Fable 5.2 wrote the first draft of these slides.

Finding a proof, checking a proof

FIND search for a proof

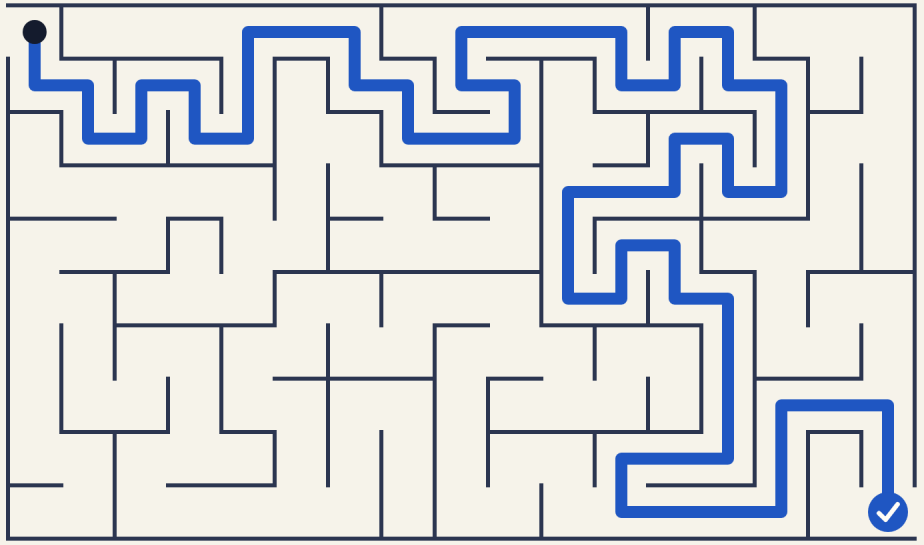


once — by anyone, or anything

may be ✓ randomized ✓ heuristic ✓ occasionally wrong

proof

VERIFY follow the proof



every time — by everyone

must be deterministic rigorous fast

With superhuman provers: ↑ let finding get harder → ↓ if it makes checking easier

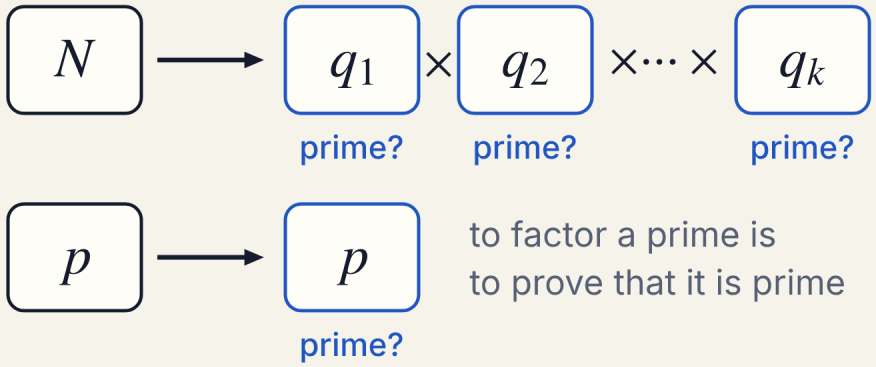
A test case: is p prime?

$$p = 2^{255} - 19 =$$

$$57896044618658097711785492$$
$$50434395392663499233282028$$
$$20197287920039565648 19949$$

77 digits. The prime under Curve25519: TLS, SSH, Signal, WireGuard.

Proving primality is the base case of factoring



every factor must be proved prime

to factor a prime is to prove that it is prime

rests on

your secure connection
HTTPS · SSH · private messaging

key exchange and signatures

an elliptic curve over $\mathbb{F}_p$

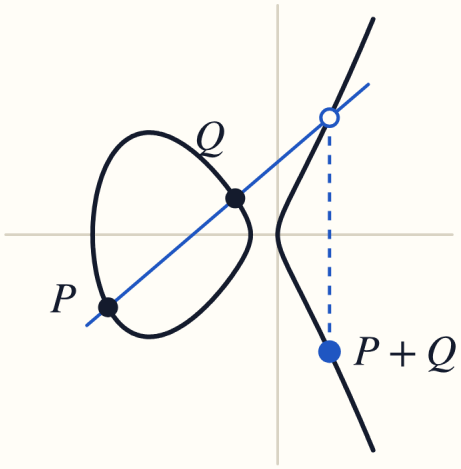
p is prime — needs a proof

A probable-prime test is not a proof.

A formally verified stack needs a certificate that a small, trusted checker can confirm.

The elliptic curve idea

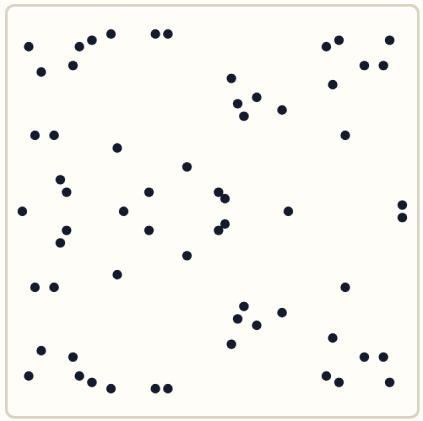
1 An elliptic curve



$y^2 = x^3 + Ax^2 + x$

its points can be added

2 Its points mod a prime ℓ

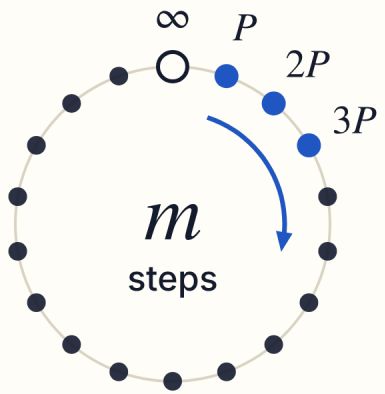


$\ell = 61$: 64 points

at most $\ell + 1 + 2\sqrt{\ell}$ points

Hasse's bound

3 The order of a point

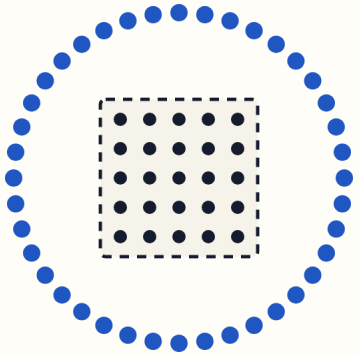


$[m]P = \infty$

and no sooner

4 A factor $\ell \le \sqrt{p}$?

the orbit of P : m points



the curve mod ℓ : too small

$m > (\sqrt[4]{p} + 1)^2$

no such ℓ , so p **is prime**

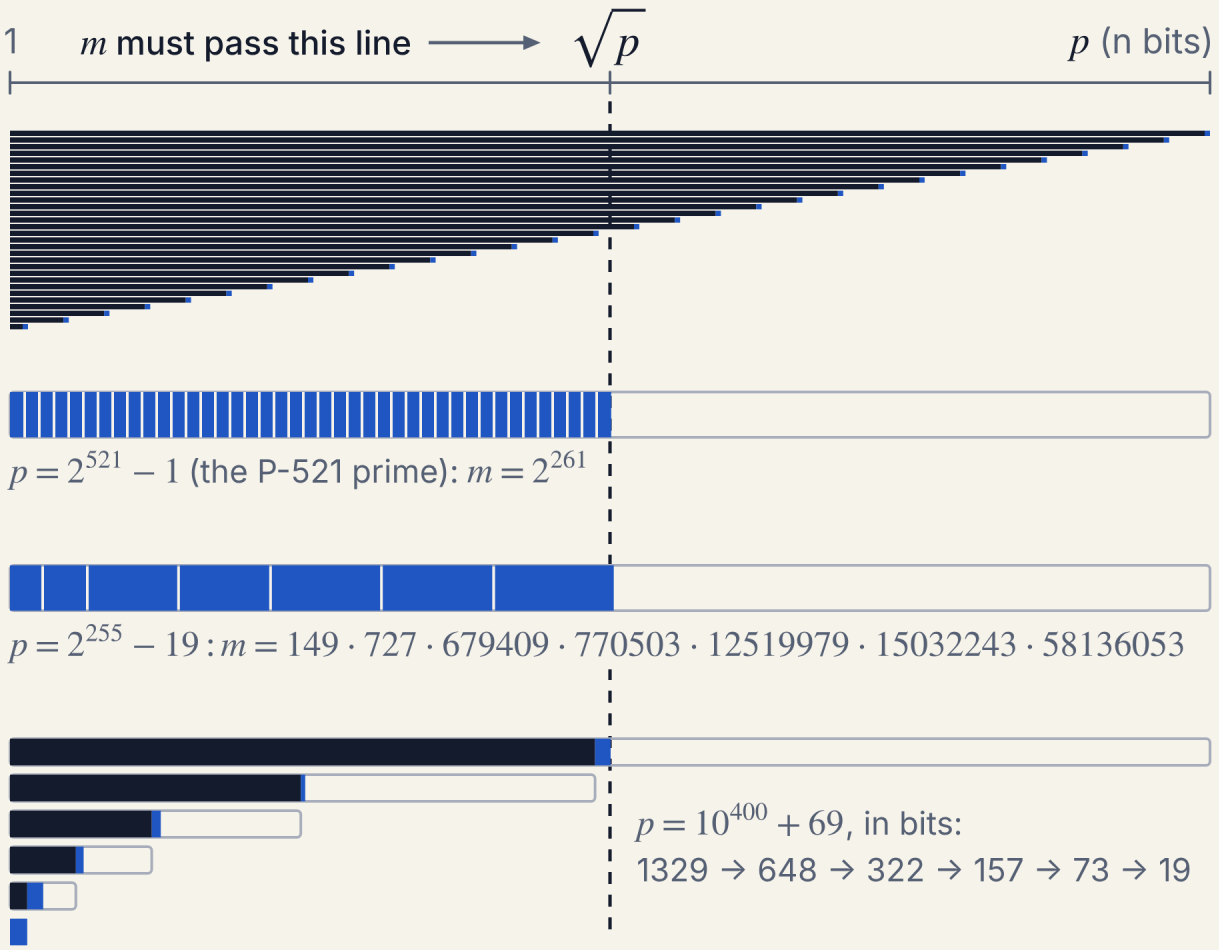
The verifier computes modulo p and never needs to know ℓ

- ✓ $[m]P = \infty$
- ✓ $[m/q]P \neq \infty$ for every prime $q \mid m$, checked with a gcd: $\gcd(Z,\ p) = 1$

the checker needs the prime factors of m

factoring p → factoring m

Four shapes of certificate

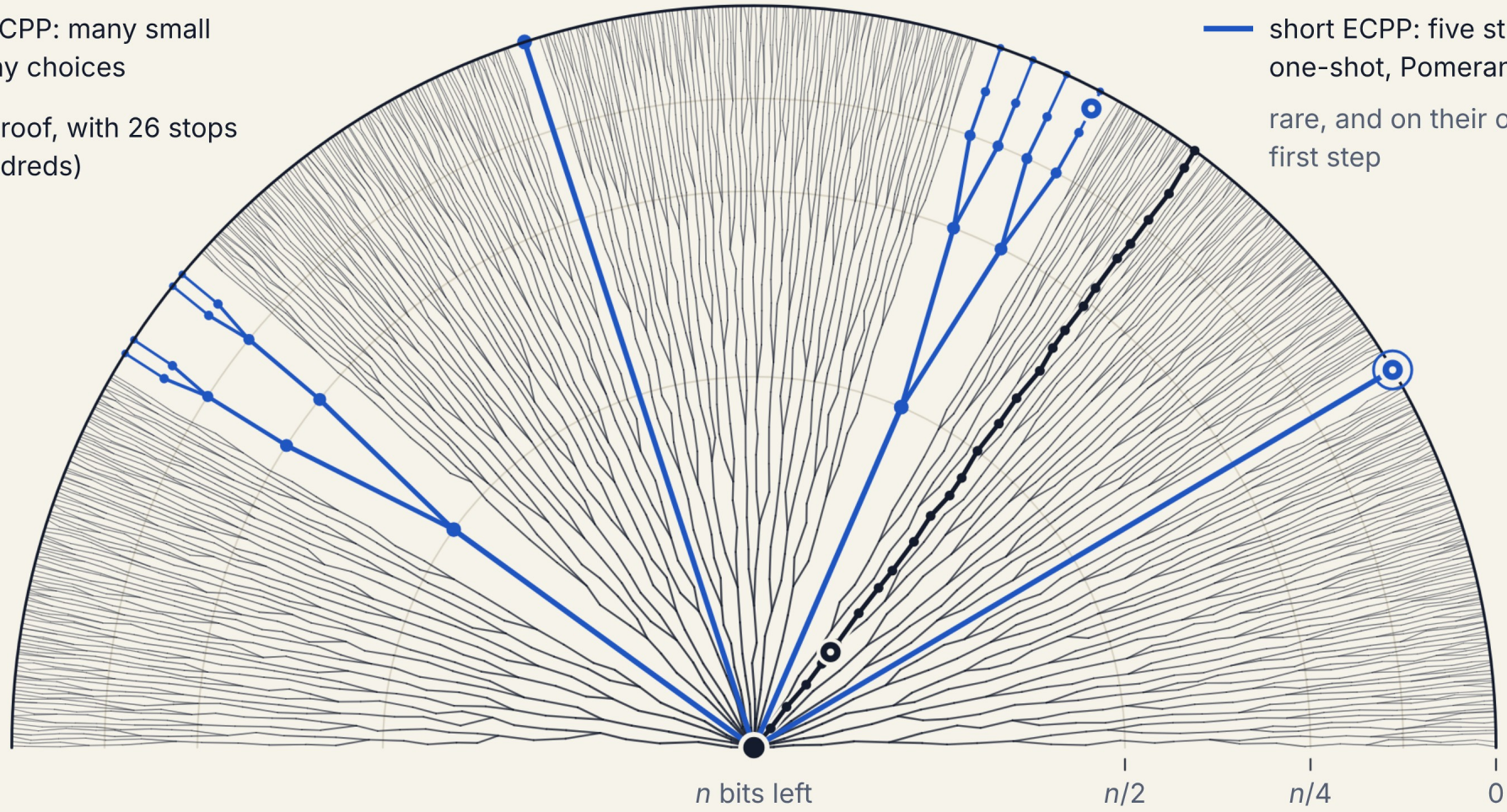


Bars are to scale in bits. Verification cost in bit operations, up to logarithmic factors.

The shape of proof space

classical ECPP: many small steps, many choices

one long proof, with 26 stops (really hundreds)

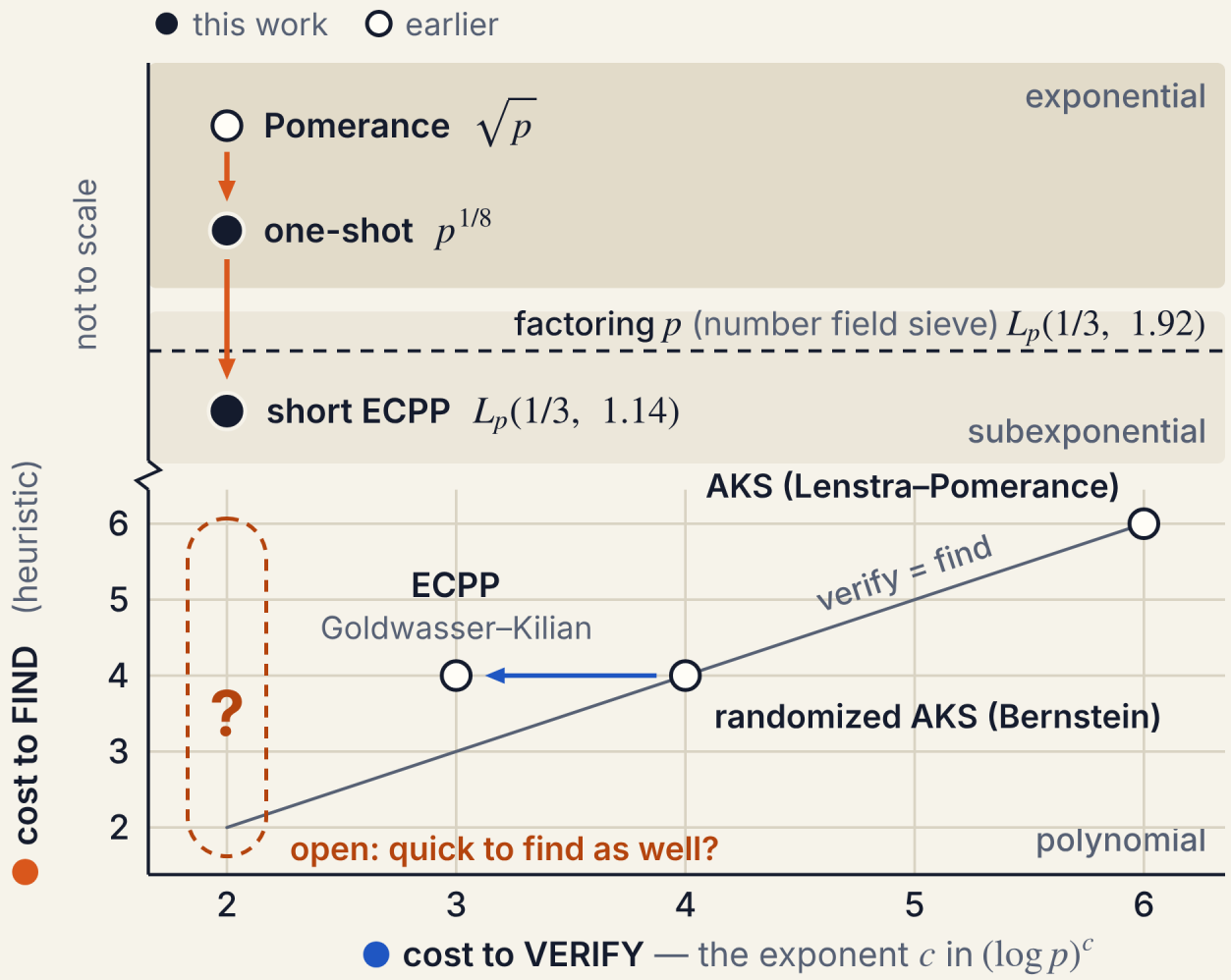


short ECPP: five strides one-shot, Pomerance: one leap

rare, and on their own from the first step

Schematic and not to scale: short proofs are a vanishing share. Mapping proof space in general is an open problem.

The price of a short proof



Cheaper than factoring

find a short proof (heuristic)

$c = (3/2)^{1/3} \approx 1.14$

factor p (number field sieve)

$c = (64/9)^{1/3} \approx 1.92$

$$L_p(1/3,\ c) = \exp\left((c + o(1))\,(\ln p)^{1/3}(\ln \ln p)^{2/3}\right)$$

Already past AKS in practice

largest primes proved so far

short ECPP	1,329 bits
AKS	1,025 bits

Finding costs are heuristic. Exponents are up to o(1).

Short primality proofs cost more to find, but less than factoring.

Open: a certificate that is quick to verify and quick to find.

POMERANCE TRIPLES	github.com/AndrewVSutherland/DANGER3
ONE-SHOT CERTIFICATES	github.com/AndrewVSutherland/OneShotPrimalityProofs
SHORT CERTIFICATES	github.com/AndrewVSutherland/ShortPrimalityProofs

Certificates welcome. Joint work with Alexa McLain, part of the DARPA expMath program.