Elliptic Curves: From Primality Proofs to Cryptography

Nandan Surabhi

July 10th 2026

Motivation: "Probably" prime is not the same as prime

The practical problem

Cryptographic systems need large primes, but trial division checks factors up to $\sqrt{n}$, which is exponential in the bit-length of n.

Importance

The goal is not just to avoid composites. It is to produce a short reason that anyone else can verify.

- Miller–Rabin is fast and useful.
- But in its randomized form, it gives evidence, not a certificate.
- A primality proof should be independently checkable.

Table of Contests

Big idea

How can elliptic curve arithmetic be used both to prove that an integer is prime and to build secure cryptographic systems?

1. Why classical primality tests motivate certificates.
2. How elliptic curves form finite abelian groups over $\mathbb{F}_p$.
3. How Hasse's theorem turns point orders into a primality proof.
4. How scalar multiplication gives elliptic curve cryptography.
5. Why Baby-Step Giant-Step explains the square-root attack barrier.

Fermat test

If p is prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

So if $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.

- Fermat can prove compositeness.
- Some composites still pass for many bases.
- Miller–Rabin fixes this probabilistically.

Importance

A fast test is useful for searching, but a proof needs data that forces every possible factorization to fail.

Curve over a prime field

For a prime p, an elliptic curve is

$$E : y^2 = x^3 + Ax + B \pmod{p}, \qquad 4A^3 + 27B^2 \not\equiv 0 \pmod{p}.$$

The point set is

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + Ax + B\} \cup \{O\}.$$

- O is the identity point.
- Points can be added geometrically and algebraically.
- The result is a finite abelian group.

Importance

Once points form a group, we can talk about point orders, large prime factors, and scalar multiplication.

The group law and scalar multiplication

For distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Over $\mathbb{F}_p$, division means multiplying by a modular inverse.

Scalar multiplication

$$[k]P = \underbrace{P + P + \cdots + P}_{k \text{ times}}$$

Double-and-add computes this in $O(\log k)$ group operations.

Importance

This one operation is the bridge: ECPP verifies equations like $[m]P = O$; ECC publishes points like $[d]G$.

Hasse's theorem: the size of the group is tightly controlled

Hasse's bound

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

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

Equivalently,

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

- Heuristic center: for each x, roughly half the values are quadratic residues, giving about one y on average.
- The extra $+1$ comes from the point at infinity O.

Importance

Hasse's theorem converts "a point has large order" into a numerical contradiction for possible prime divisors of n.

Proof of Hasse's Theorem

3 Cases

Case 1: $f(x) \equiv 0$	(mod p)	
Case 2: $f(x) \equiv s$	(mod p)	where s is a quadratic residue modulo p
Case 3: $f(x) \equiv t$	(mod p)	where t is not a quadratic residue modulo p

- $\mathbb{Z}/p\mathbb{Z}$ modulo p satisifes satisfies $|\mathbb{Z}/p\mathbb{Z}| \cup O = p + 1$
- For the sake of approximation, take the probability that a given residue is a quadratic residue modulo p is $\frac{1}{2}$. Each quadratic residue gives 2 values(negative and positive), while a non quadratic residue gives none.
- $\frac{1}{2} \cdot 2 \cdot (p + 1) = p + 1$

How a point order can prove primality

Setup

Let n be the number to prove prime. Choose a curve modulo n with proposed order

$$m = kq,$$

where q is a large prime. Find a point P such that

$$[m]P = O, \qquad [k]P \neq O.$$

- The first equation says the order of P divides m.
- The second says the order still contains the factor q.
- Reducing modulo any prime divisor $p \mid n$, the same large factor must appear in $\#E(\mathbb{F}_p)$.

Importance

If n were composite, its smallest prime factor p would be small. Hasse then says $\#E(\mathbb{F}_p)$ cannot be large enough to contain q.

Goldwasser–Kilian criterion: the contradiction

Primality criterion

Suppose $m = kq$ and

$$q > \left(n^{1/4} + 1\right)^2.$$

If $[m]P = O$ and $[k]P$ is strongly nonzero modulo every prime divisor of n, then n is prime.

If n were composite, let p be its smallest prime divisor. Then $p \le \sqrt{n}$, so Hasse gives

$$\#E(\mathbb{F}_p) \le (\sqrt{p} + 1)^2 \le (n^{1/4} + 1)^2.$$

But the point order forces

$$q \mid \#E(\mathbb{F}_p),$$

so $q \le \#E(\mathbb{F}_p)$, contradicting the size bound.

Example: Proving 11 is prime

Curve and point

Consider

$$E : y^2 = x^3 + 3x + 2 \pmod{11}, \qquad P = (4, 1).$$

This curve has 13 points, and repeated addition gives

$$P + 4P + 8P = [13]P = O, \qquad [1]P \neq O.$$

- Let $m = q = 13$ and $k = 1$.
- The size condition holds: $13 > (11^{1/4} + 1)^2 \approx 7.96$.
- If 11 had a prime divisor $p \leq \sqrt{11}$, then Hasse would force $\#E(\mathbb{F}_p) < 13$, impossible because $13 \mid \#E(\mathbb{F}_p)$.

Importance

The example is tiny, but it shows the main mechanism: point order plus Hasse bound produces a contradiction.

Why ECPP improves the search

Random-curve difficulty

Goldwasser–Kilian may try many curves before finding one whose order has a large prime factor.

ECPP reversal

ECPP uses complex multiplication to predict possible group orders first, then constructs a curve with a useful order.

Core equation

For a negative discriminant D, ECPP searches for

$$4n = u^2 - Dv^2 = u^2 + |D|v^2.$$

This gives candidate orders

$$m = n + 1 - u \quad \text{or} \quad m = n + 1 + u.$$

Importance

Certificates: hard to find, easy to verify

What an ECPP certificate records

A certificate includes the curve data, a proposed order $m = kq$, a point P, the size condition on q, and a recursive certificate that q is prime.

Producer does the search:

- choose discriminants,
- find roots and curves,
- factor candidate orders,
- build the recursion chain.

Verifier checks:

- algebraic identities,
- nonsingularity,
- $[m]P = O$ and $[k]P \neq O$,
- primality of the next q.

Importance

This asymmetry is the point: expensive discovery becomes a compact, auditable proof.

Same group, different purpose: ECPP versus ECC

Feature	ECPP	ECC
Goal	Prove n is prime	Create keys and shared secrets
Group order	Known or sufficiently factored	Has a large prime-order subgroup
Large prime factor	Used to force a contradiction	Used to resist attacks
Output	Certificate	Public key or shared secret
Main operation	Verify scalar multiples	Compute scalar multiples

Importance

ECPP reveals the curve order to make a proof checkable. ECC hides the scalar to make a one-way function.

Elliptic Curve Diffie–Hellman

Publicly agree on E, a base point G, and the prime order r of G.

$$\text{Alice: } A = [a]G$$
$$\text{Bob: } B = [b]G$$

Alice computes

$$[a]B = [a]([b]G) = [ab]G.$$

Bob computes

$$[b]A = [b]([a]G) = [ab]G.$$

Shared secret

Both obtain the same point $[ab]G$.

Importance

An eavesdropper sees G, A, and B, but recovering a or b means solving the elliptic curve discrete logarithm problem.

The elliptic curve discrete logarithm problem

ECDLP

Given G and

$$Q = [k]G,$$

find the unknown scalar k.

- Computing Q from k is fast: double-and-add takes $O(\log k)$ operations.
- Recovering k is believed hard for properly chosen curves.
- Secure systems choose G with large prime order r so attacks cannot split into small factors.

Importance

The same scalar multiplication that makes ECPP verification efficient becomes a one-way operation in cryptography.

Baby-Step Giant-Step: why the attack is square-root sized

Decompose the unknown

Let G have order r, set $m = \lceil \sqrt{r} \rceil$, and write

$$k = im + j, \qquad 0 \le i, j < m.$$

Then

$$Q - [i]([m]G) = [j]G.$$

Baby steps: store $[j]G$ for $0 \le j < m$.

Giant steps: test $Q - [i]([m]G)$ until a stored point appears.

Importance

Instead of trying all r scalars, the attack uses about $\sqrt{r}$ time and $\sqrt{r}$ memory. This is why a 256-bit subgroup gives about 128-bit generic security.

Worked Baby-Step Giant-Step example

Use the same curve

$$E : y^2 = x^3 + 3x + 2 \pmod{11}, \qquad G = (4, 1), \qquad |G| = 13.$$

Let the secret be $k = 9$, so

$$Q = [9]G = (2, 7).$$

Set $m = \lceil \sqrt{13} \rceil = 4$.

Baby steps

$0G = O$
$1G = (4, 1)$
$2G = (7, 5)$
$3G = (3, 4)$

Giant steps

$Q = (2, 7)$: no match
$Q - [4]G = (10, 8)$: no match
$Q - [8]G = (4, 1) = 1G$

Thus $k = 2 \cdot 4 + 1 = 9$.

Takeaways

1. Classical tests motivate a distinction between probable primes and certified primes.
2. Elliptic curves over finite fields give finite abelian groups with useful point orders.
3. Hasse's theorem is the key bound that lets a large point-order factor prove primality.
4. ECPP makes Goldwasser–Kilian practical by constructing curves with useful orders.
5. ECC uses the same group law differently: scalar multiplication is easy, but reversing it is hard.

Big idea

In ECPP, point orders create certificates of correctness; in ECC, the difficulty of recovering scalars creates security.

Thanks for listening!