

# 18.783 Elliptic Curves

## Lecture 11

Andrew Sutherland

October 9, 2025

## Primality proving

- Primality proving is one of the founding problems of computational number theory.
- A factorization cannot be considered complete without a proof of primality.
- Probabilistic factorization algorithms will typically not terminate on prime inputs.
- Elliptic curves play a crucial role in practical primality proving.
- Existing polynomial-time algorithms are not as practical and do not provide a useful [certificate](#) of primality.
- Algorithms for primes of specific forms such as Mersenne primes are very efficient but are not applicable in any generality.
- There are very efficient probabilistic algorithms for proving compositeness without providing a factorization, but these do not prove primality.

# Using Fermat's little theorem to prove compositeness

## Theorem (Fermat 1640)

*If  $N$  is prime then  $a^N \equiv a \pmod{N}$  for all integers  $a$ .*

## Example

The fact that  $2^{91} \equiv 37 \pmod{91}$  proves that 91 is not prime (without factoring it).

## Example

We have  $2^{341} \equiv 2 \pmod{341}$  (which proves nothing), but  $3^{341} \equiv 168 \pmod{341}$  proves that 341 is not prime (thus we may need to try different values of  $a$ ).

## Example

We have  $a^{561} \equiv a \pmod{561}$  for every integer  $a$ . But  $561 = 3 \cdot 11 \cdot 17$  is not prime!

# Carmichael numbers

## Definition

A composite  $N \in \mathbb{Z}$  such that  $a^N \equiv a \pmod{N}$  for all  $a \in \mathbb{Z}$  is a **Carmichael number**.

The sequence of Carmichael numbers begins 561, 1105, 1729, 2821, ..., and forms sequence [A002997](#) in the On-Line Encyclopedia of Integer Sequences (OEIS).

Statistics on the 20,138,200 Carmichael numbers less than  $10^{21}$  can be found [here](#).

## Theorem (Alford-Granville-Pomerance 1994)

*The sequence of Carmichael numbers is infinite.*

There are thus infinitely many composite integers that will pass any primality test based on Fermat's little theorem.

## A better test for compositeness

Recall the Euler function  $\phi(N) := \#(\mathbb{Z}/N\mathbb{Z})^\times$ .

### Theorem

*A positive integer  $N$  is prime if and only if  $\phi(N) = N - 1$ .*

**Proof:** Every nonzero residue class in  $\mathbb{Z}/N\mathbb{Z}$  is invertible if and only if  $N$  is prime.

### Lemma

*Let  $p = 2^s t + 1$  be prime with  $t$  odd and suppose  $a \in \mathbb{Z}$  is not divisible by  $p$ . Exactly one of the following holds:*

- (i)  $a^t \equiv 1 \pmod{p}$ .
- (ii)  $a^{2^i t} \equiv -1 \pmod{p}$  for some  $0 \leq i < s$ .

**Proof:** To the blackboard!

## A witness for compositeness

### Definition

Let  $N = 2^s t + 1$  with  $t$  odd. An integer  $a \not\equiv 0 \pmod{N}$  is a **witness** for  $N$  if

$$(i) a^t \not\equiv 1 \pmod{N} \quad \text{and} \quad (ii) a^{2^i t} \not\equiv -1 \pmod{N} \text{ for } 0 \leq i < s.$$

If  $N$  has a witness  $a$  then  $N$  is composite (and  $a$  is a certificate of this fact).

### Theorem (Monier-Rabin 1980)

*Let  $N$  be an odd composite integer.*

*A random integer  $a \in [1, N - 1]$  is a witness for  $N$  with probability at least  $3/4$ .*

Proof: See notes.

If we pick 100 random  $a \in [1, N - 1]$  we are nearly certain to find a witness if  $N$  is composite. But if we do not find one we cannot say whether  $N$  is prime or composite. 6

# The Miller-Rabin algorithm

## Algorithm

Given an odd integer  $N > 1$ :

1. Pick a random integer  $a \in [1, N - 1]$ .
2. Write  $N = 2^s t + 1$ , with  $t$  odd, and compute  $b = a^t \bmod N$ .  
If  $b \equiv \pm 1 \pmod N$ , return **true** ( $a$  is not a witness,  $N$  could be prime).
3. For  $i$  from 1 to  $s - 1$ :
  - 3.1 Set  $b \leftarrow b^2 \bmod N$ .
  - 3.2 If  $b \equiv -1 \pmod N$ , return **true** ( $a$  is not a witness,  $N$  could be prime).
4. Return **false** ( $a$  is a witness,  $N$  is definitely not prime).

On prime inputs this algorithm will always output **true**.

On composite inputs it will output **false** with probability at least  $3/4$ .

# The Miller-Rabin algorithm

## Example

For  $N = 561$  we have  $561 = 2^4 \cdot 35 + 1$ , so  $s = 4$  and  $t = 35$ , and for  $a = 2$  we have

$$2^{35} \equiv 263 \pmod{561},$$

which is not  $\pm 1 \pmod{561}$  so we continue and compute

$$263^2 \equiv 166 \pmod{561},$$

$$166^2 \equiv 67 \pmod{561},$$

$$67^2 \equiv 1 \pmod{561}.$$

We never hit  $-1$ , so  $a = 2$  is a witness for  $N = 561$  and we return **false**, since we have proved that 561 is not prime.

## How good is the Miller-Rabin test?

The Miller-Rabin test will detect composite inputs with probability at least  $3/4$ .  
By running it  $k$  times we can amplify this probability to  $1 - 2^{-2k}$ .  
But its performance on random composite inputs is much better than this.

### Theorem (Damgård-Landrock-Pomerance 1993)

*Let  $N$  be a random odd integer in  $[2^{k-1}, 2^k]$  and  $a$  a random integer in  $[1, N - 1]$ .  
Then  $\Pr[N \text{ is prime} \mid a \text{ is not a witness for } N] \geq 1 - k^2 \cdot 4^{2-\sqrt{k}}$ .*

Some typical values of  $k$ :

$$k = 256 : \quad 1 - k^2 \cdot 4^{2-\sqrt{k}} = 1 - 2^{-12},$$

$$k = 4096 : \quad 1 - k^2 \cdot 4^{2-\sqrt{k}} = 1 - 2^{-100}.$$

Note that this applies to just a single test and can be amplified!

# Elliptic curve primality proving

## Definition

Let  $P = (P_x : P_y : P_z) \in E(\mathbb{Q})$  with  $P_x, P_y, P_z \in \mathbb{Z}$  and  $\gcd(P_x, P_y, P_z) = 1$ .

For  $N \in \mathbb{Z}_{>0}$ , if  $P_z \equiv 0 \pmod{N}$  then we say that  $P$  is **zero mod  $N$** , and otherwise we say that  $P$  is **nonzero mod  $N$** . If  $\gcd(P_z, N) = 1$  then  $P$  is **strongly nonzero mod  $N$** .

If  $P$  is strongly nonzero mod  $N$ , then  $P$  is nonzero mod  $p$  for every prime  $p|N$ .

When  $N$  is prime, the notions of nonzero and strongly nonzero coincide.

## Theorem (Goldwasser-Kilian 1986)

*Let  $E/\mathbb{Q}$  be an elliptic curve, and let  $M, N > 1$  be integers with  $M > (N^{1/4} + 1)^2$  and  $N \perp \Delta(E)$ , and let  $P \in E(\mathbb{Q})$ . If  $MP$  is zero mod  $N$  and  $(M/\ell)P$  is strongly nonzero mod  $N$  for every prime  $\ell|M$  then  $N$  is prime.*

**Proof:** To the blackboard!

## Primality certificates

To apply the Goldwasser-Kilian theorem, we need to know the prime factors  $q$  of  $M$ . In particular, we need to be sure that these  $q$  are actually prime! To simplify matters, we restrict to the case that  $M = q$  is prime.

### Definition

An **elliptic curve primality certificate** for  $p$  is a tuple of integers

$$(p, A, B, x_1, y_1, q),$$

where  $P = (x_1 : y_1 : 1)$  is a point on the elliptic curve  $E: y^2 = x^3 + Ax + B$  over  $\mathbb{Q}$ , the integer  $p > 1$  is prime to  $\Delta(E)$ , and  $qP$  is zero mod  $p$  with  $q > (p^{1/4} + 1)^2$ .

Note that  $P = (x_1 : y_1 : 1)$  is strongly nonzero mod  $p$ , since its  $z$ -coordinate is 1. A primality certificate  $(p, \dots, q)$  reduces the question of  $p$ 's primality to that of  $q$ . A chain of such certificates can lead to a  $q$  that is small enough for trial division.

## Algorithm (Goldwasser-Kilian ECPP)

Given an odd integer  $p$  (a candidate prime), and a bound  $b$ , with  $p > b > 5$ , construct a primality certificate  $(p, A, B, x_1, y_1, q)$  with  $q \leq (\sqrt{p} + 1)^2/2$  or prove  $p$  composite.

1. Pick random integers  $A, x_0, y_0 \in [0, p - 1]$ , and set  $B = y_0^2 - x_0^3 - Ax_0$ .  
Repeat until  $\gcd(4A^3 + 27B^2, p) = 1$ , then define  $E: y^2 = x^3 + Ax + B$ .
2. Use Schoof's algorithm to compute  $m = \#E(\mathbb{F}_p)$  assuming that  $p$  is prime.  
If anything goes wrong (which it might!), or if  $m \notin \mathcal{H}(p)$ , then return **composite**.
3. Write  $m = cq$ , where  $c$  is  $b$ -smooth and  $q$  is  $b$ -coarse.  
If  $c = 1$  or  $q \leq (p^{1/4} + 1)^2$ , then go to step 1.
4. (optional) Perform a Miller-Rabin test on  $q$ . If it returns **false** then go to step 1.
5. Compute  $P = (P_x : P_y : P_z) = c \cdot (x_0 : y_0 : 1)$  on  $E$ , working modulo  $p$ .  
If  $\gcd(P_z, p) \neq 1$ , go to step 1, else let  $x_1 \equiv P_x/P_z \pmod{p}$ ,  $y_1 \equiv P_y/P_z \pmod{p}$ .
6. Compute  $Q = (Q_x : Q_y : Q_z) = q \cdot (x_1 : y_1 : 1)$  on  $E$ , working modulo  $p$ .  
If  $Q_z \not\equiv 0 \pmod{p}$  then return **composite**.
7. If  $q > b$ , then recursively verify that  $q$  is prime using inputs  $q$  and  $b$ ; otherwise, verify that  $q$  is prime by trial division. If  $q$  is found to be composite, go to step 1.
8. Output the certificate  $(p, A, \tilde{B}, x_1, y_1, q)$  such that  $y_1^2 = x_1^3 + Ax_1 + \tilde{B}$  (over  $\mathbb{Z}$ ).

## Complexity analysis and subsequent improvements

You will analyze the heuristic complexity of this algorithm assuming that  $m$  is a random integer (in which case it is a polynomial-time Las Vegas algorithm)

Goldwasser-Kilian proved this for all but a subexponentially small set of inputs.

Adleman-Huang proved this for all inputs by modifying the algorithm.

(they "reduce" the problem to proving the primality of a random prime  $p' \approx p^2$ ).

The Goldwasser-Kilian algorithm has been superseded by the "fast ECPP" algorithm developed by Atkin and Morain, which uses the theory of **complex multiplication** to obtain a much better heuristic expected running time:  $\tilde{O}(n^4)$ . This algorithm can handle primes with tens of thousands (but not millions) of digits.

The AKS algorithm (as originally proposed) has a deterministic complexity of  $\tilde{O}(n^{10.5})$ . This can be improved to  $\tilde{O}(n^6)$ , and there is a randomized version that can be shown to run in  $\tilde{O}(n^4)$  expected time, but it is still much slower than ECPP.

MIT OpenCourseWare

<https://ocw.mit.edu>

18.783 / 18.7831 Elliptic Curves

Fall 2025

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.