The Lucas-Lehmer Primality Test

An Efficient Algorithm for Discovering Large Primes

Abdur Rehman Cheema

Euler Circle

July 11, 2025

Agenda

Why Primes Matter

- Building blocks of arithmetic and key to number theory.
- Vital in modern cryptography and computer science.

Challenge: Efficiently test very large numbers for primality.

Primality Testing Methods

- **Probabilistic (e.g., Miller-Rabin)**: Fast but not guaranteed.
- **Deterministic (e.g., AKS, LLT)**: Guaranteed results, sometimes slow.

Goal: Find fast, deterministic tests for special classes of numbers.

Mersenne Primes and Perfect Numbers

Mersenne Number

$M_p = 2^p - 1$, where p is prime.

- Examples: $M_3 = 7$, $M_5 = 31$, $M_7 = 127$
- $M_{11} = 2047 = 23 \times 89$ (composite)

Perfect Number

Equal to sum of its proper divisors.
Example: $28 = 1 + 2 + 4 + 7 + 14$

Euclid-Euler Theorem:
M_p prime $\Rightarrow 2^{p-1}(2^p - 1)$ is perfect.

Historical Origins of the Test

- **Édouard Lucas (1876):** Developed the first primality test for Mersenne numbers.
- Proved $M_{127} = 2^{127} - 1$ is prime — the largest known prime for 75 years.
- Used by hand — extremely laborious!

Legacy

Lucas laid the theoretical foundation for efficient primality testing.

From Lucas to Lehmer

- **Derrick Lehmer (1930s–1950s):** Refined Lucas's method for the digital age.
- Introduced the recurrence relation now called the **Lucas-Lehmer Test**.
- First implemented the test on early computers like the ENIAC.

Modern Impact

LLT is now the fastest deterministic method for testing Mersenne primes.

The Lucas-Lehmer Test

To test if $M_p = 2^p - 1$ is prime:

- Start: $S_0 = 4$
- Recurrence: $S_{k+1} = S_k^2 - 2 \mod M_p$
- If $S_{p-2} \equiv 0$, then M_p is prime

Fast, deterministic, efficient for Mersenne numbers.

Example: $M_5 = 31$

- $S_0 = 4$
- $S_1 = 14$
- $S_2 = 8$
- $S_3 = 0$

Since $S_3 \equiv 0 \mod 31$, M_5 is **prime**.

Mathematical Foundation

Lucas Sequences: $S_k = \omega^{2^k} + \bar{\omega}^{2^k}$
Where $\omega = 2 + \sqrt{3}$, $\bar{\omega} = 2 - \sqrt{3}$

This recurrence generates S_k satisfying $S_{k+1} = S_k^2 - 2$

Why LLT Works

- Based on group theory: large cycle length only possible if M_p is prime.
- Uses elements with order 2^p.
- A composite M_p cannot sustain such long cycles.

Therefore: $S_{p-2} \equiv 0 \Rightarrow M_p$ is prime

Why It's So Efficient

- Only $p - 2$ iterations.
- Uses Fast Fourier Transform for big multiplication.
- Modulo $2^p - 1$ is fast with bitwise operations.

Ideal for testing very large Mersenne primes.

Cryptographic Significance

- LLT itself not used in RSA, but...
- Drives innovation in big-number libraries and multiplication algorithms.
- Forms the foundation for testing large prime candidates.

Hardware Stress Testing

Prime95 Software:

- Uses LLT for GIMPS
- Tests CPU, RAM, and system stability
- Common in overclocking and hardware validation

The GIMPS Project

- Global network of volunteers
- Discovered every largest known prime since 1996
- Shows the power of distributed computing

Record-Breaking Discoveries

Example: $M_{82,589,933}$

Found in 2018, has **24,862,048 digits**!

LLT makes verifying such primes possible.

Key Takeaways

- LLT: Fast, deterministic, and elegant
- Optimized for Mersenne numbers
- Drives research in mathematics and computing
- Powers GIMPS and real-world cryptographic tools

Q&A

Questions?