Mersenne Primes

Definition. A *Mersenne prime* is a prime of the form $2^n - 1$.

- Equivalently, ... of the form $2^p - 1$ where p is a prime.
- The largest known prime is $2^{57885161} - 1$ (17425170 digits).

The Lucas-Lehmer Test. *Let p be an odd prime, and define recursively*

$$L_0 = 4 \quad \text{and} \quad L_{n+1} = L_n^2 - 2 \bmod (2^p - 1) \quad \text{for} \quad n \geq 0.$$

Then $2^p - 1$ is a prime if and only if $L_{p-2} = 0$.

Other Primality Tests

Theorem (Selfridge-Weinberger). *Assume that the Extended Riemann Hypothesis holds. Let n be an odd integer > 1. A necessary and sufficient condition for n to be prime is that for all positive integers $a < \min\{70(\log n)^2, n\}$, we have $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$ with at least one occurrence of -1.*

Theorem (Lucas). *Let n be a positive integer. If there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and for all primes p dividing $n-1$ we have $a^{(n-1)/p} \not\equiv 1 \pmod{n}$, then n is prime.*

Revised Theorem. *Let n be a positive integer. Suppose that for each prime p dividing $n-1$, there is an $a \in \mathbb{Z}$ such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/p} \not\equiv 1 \pmod{n}$. Then n is prime.*

Theorem (Lucas). *Let n be a positive integer. If there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and for all primes p dividing $n-1$ we have $a^{(n-1)/p} \not\equiv 1 \pmod{n}$, then n is prime.*

Theorem (Pepin Test). *Let $F_n = 2^{2^n} + 1$ with n a positive integer. Then F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

($\Longrightarrow$): Use $\left(\frac{3}{F_n}\right) = -1$.

($\Longleftarrow$): Use $\mathrm{ord}_{F_n}(3) = 2^{2^n}$. (Or use the theorem of Lucas.)

Theorem (Proth, Pocklington, Lehmer Test). *Let $n \in \mathbb{Z}^+$. Suppose $n - 1 = FR$ where all the prime factors of F are known and $\gcd(F, R) = 1$. Suppose further that there exists an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and for all primes p dividing F we have $\gcd(a^{(n-1)/p} - 1, n) = 1$. Then every prime factor of n is congruent to 1 modulo F.*

Note: If $F \geq \sqrt{n}$ and the conclusion holds, then n is prime.

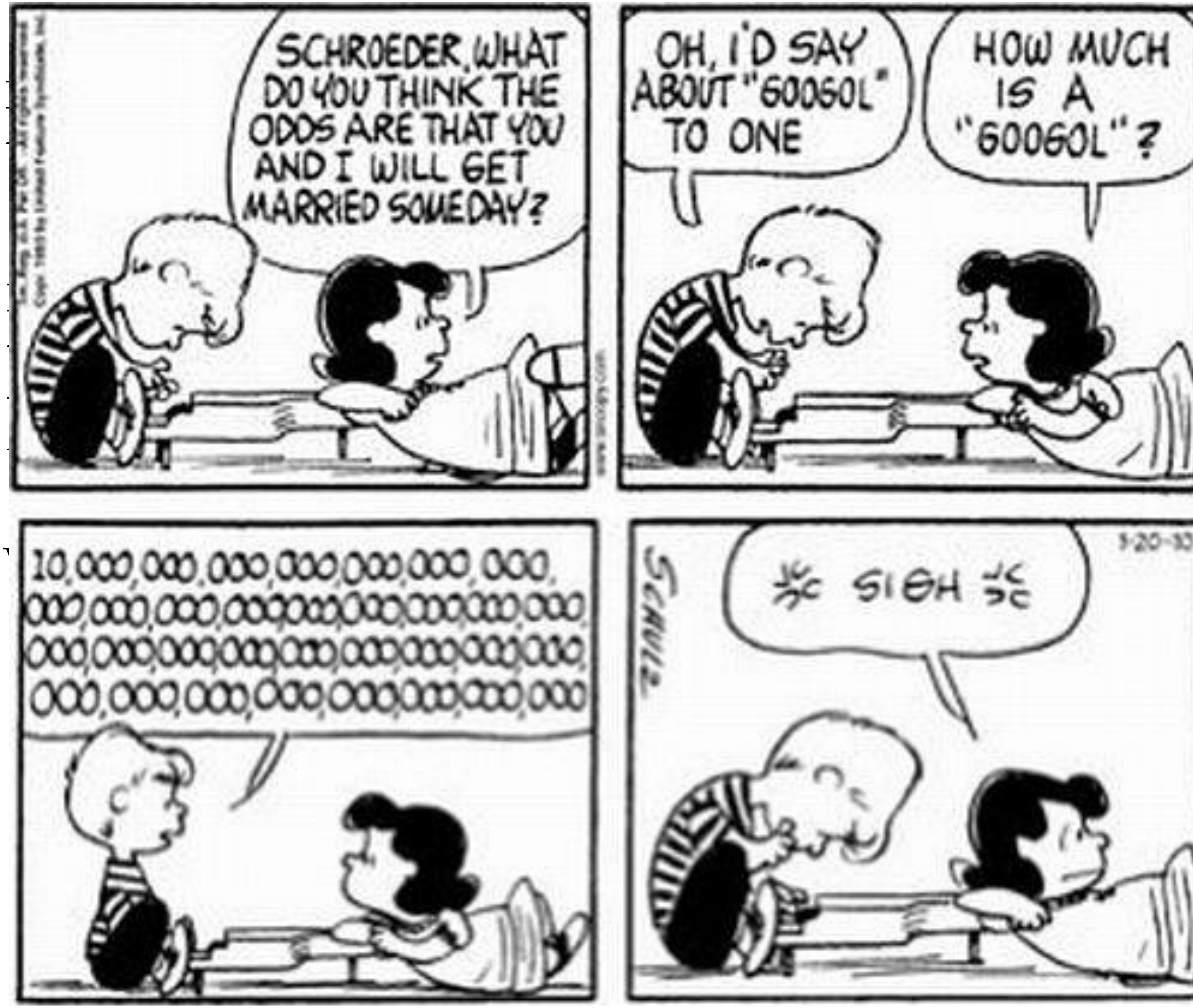
- Suppose $q|n$ (q prime), and let $m = \operatorname{ord}_q(a)$.
- If $p^e \| F$, then $p^e \| m$.
- Deduce $F|m$, so $F|(q-1)$.

In 1980, Adleman, Pomerance, and Rumely found a primality test that determines if n is prime in $\ll (\log n)^{c \log\log\log n}$ steps (shown by Odlyzko).

In 2002, Agrawal, Kayal, and Saxena developed a polynomial time primality test. Pomerance and Lenstra gave a variant that runs in $\ll (\log n)^6$ steps where n is the number being tested.

Which test is better?

Note: If n has a googol digits, then $\log\log\log n < 5.5$.


SCHROEDER, WHAT DO YOU THINK THE ODDS ARE THAT YOU AND I WILL GET MARRIED SOMEDAY?
OH, I'D SAY ABOUT "GOOGOL" TO ONE
HOW MUCH IS A "GOOGOL"?
10,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000
SCHULZ
SIGH

In 1980, Adleman, Pomerance, and Rumely found a primality test that determines if n is prime in $\ll (\log n)^{c \log\log\log n}$ steps (shown by Odlyzko).

In 2002, Agrawal, Kayal, and Saxena developed a polynomial time primality test. Pomerance and Lenstra gave a variant that runs in $\ll (\log n)^6$ steps where n is the number being tested.

Which test is better?

Note: If n has a googol digits, then $\log\log\log n < 5.5$.

Primality Testing in Polynomial Time

(Recyclization of an OLD Lecture, 2002)

PRIMALITY TESTING IN POLYNOMIAL TIME

A Theorem of

M. AGRAWAL, N. KAYAL, AND N. SAXENA
Department of Computer Science & Engineering
Indian Institute of Technology in Kanpur

PRIMALITY TESTING IN POLYNOMIAL TIME

CAUTION: This is a theoretical result.

Primality Testing in Polynomial Time

Caution: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps

PRIMALITY TESTING IN POLYNOMIAL TIME

CAUTION: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps, a truly remarkable result.

PRIMALITY TESTING IN POLYNOMIAL TIME

CAUTION: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps, a truly remarkable result. There is, however, no claim that if $n < 10^{1000}$, then the algorithm takes less than n steps.

Primality Testing in Polynomial Time

Another Caution:

Primality Testing in Polynomial Time

Another Caution:

$$\log x = \log_2 x$$

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Comments: Verifying the congruence requires too much running time as the LHS contains $n + 1$ non-zero terms.

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Comments: Verifying the congruence requires too much running time as the LHS contains $n + 1$ non-zero terms.

$$(x - a)^n \equiv x^n - a \pmod{n}$$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

$$(x - a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

What does this mean?

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

What does this mean?

- The difference $(x-a)^n - (x^n - a)$ is an element in the ideal $\left(x^r - 1, n\right)$ in the ring $\mathbb{Z}[x]$.

$$(x - a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

What does this mean?

- The difference $(x - a)^n - (x^n - a)$ is an element in the ideal $\left(x^r - 1, n\right)$ in the ring $\mathbb{Z}[x]$.
- It is the same as the assertion

  $\mathtt{Rem}\left(\left(\mathtt{x} - \mathtt{a}\right)^{\mathtt{n}} - \left(\mathtt{x}^{\mathtt{n}} - \mathtt{a}\right), \mathtt{x}^{\mathtt{r}} - \mathtt{1}, \mathtt{x}\right)\ \mathtt{mod\ n\ =\ 0}$

  in MAPLE.

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

What does this mean?

- The difference $(x-a)^n - (x^n - a)$ is an element in the ideal $(x^r - 1, n)$ in the ring $\mathbb{Z}[x]$.
- It is the same as the assertion

  $\texttt{Rem}((\texttt{x}-\texttt{a})^{\texttt{n}} - (\texttt{x}^{\texttt{n}} - \texttt{a}), \texttt{x}^{\texttt{r}} - 1, \texttt{x})\ \texttt{mod n = 0}$

  in MAPLE.

```
> Rem((x-2)^15-(x^15-2),x^3-1,x) mod 15
```

$$12\,x^2 + 9\,x + 9$$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

r denotes a prime of size $\ll \log n$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

r denotes a prime of size $\ll \log n$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

Idea for Checking this Congruence:

r denotes a prime of size $\ll \log n$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

Idea for Checking this Congruence:

- Write $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_{t-1}} + 2^{k_t}$, where $k_1 < k_2 < \cdots < k_t$.

r denotes a prime of size $\ll \log n$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

Idea for Checking this Congruence:

- Write $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_{t-1}} + 2^{k_t}$, where $k_1 < k_2 < \cdots < k_t$.
- Compute $f_j(x) = (x-a)^{2^j} \pmod{x^r - 1, n}$ for $j \in \{0, 1, \ldots, k_t\}$ successively by squaring.

r denotes a prime of size $\ll \log n$

$$(x - a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

Idea for Checking this Congruence:

- Write $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_{t-1}} + 2^{k_t}$, where $k_1 < k_2 < \cdots < k_t$.
- Compute $f_j(x) = (x - a)^{2^j} \pmod{x^r - 1, n}$ for $j \in \{0, 1, \ldots, k_t\}$ successively by squaring.
- Compute $\prod_{j=1}^{t} f_{k_j} \pmod{x^r - 1, n}$ and compare to $x^{n \bmod r} - (a \bmod n)$.

Conjecture: Suppose r does not divide $n(n^2-1)$ where r is prime. Then n is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

Conjecture: Suppose r does not divide $n(n^2-1)$ where r is prime. Then n is a prime if and only if

$$(*) \quad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

$$n \text{ prime} \implies (*) \text{ holds}$$

$$(*) \text{ holds} \implies n \text{ prime}$$

Conjecture: Suppose r does not divide $n(n^2 - 1)$ where r is prime. Then n is a prime if and only if

$$(*) \quad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

$$n \text{ prime} \quad \overset{\checkmark}{\Longrightarrow} \quad (*) \text{ holds}$$

$$(*) \text{ holds} \quad \overset{?}{\Longrightarrow} \quad n \text{ prime}$$