The Biggest Known Prime Number

Keith Conrad

May 29, 2018

News about primes

The ancient Greeks (Euclid's *Elements*, Book IX, Proposition 20) knew that the sequence of primes never ends:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29, \ldots, 14221, 14243, 14249, \ldots$$

There is no largest prime, but there's always a largest *known* prime.

In January this year, a new largest known prime was announced:

$$2^{77,232,917} - 1 = \underbrace{46733 \ldots 79071}_{\text{23,249,425 digits}}.$$

Verifying its primality took 6 days (by independent computations on 4 computers as a consistency check).

Primes of the form $2^n - 1$ are *Mersenne primes*. Interest in them is mainly driven by curiosity. Large primes are used in cryptography, but with hundreds of digits rather than millions.

What some news websites said in articles on the new prime

1. "*After using the formula to create a number, you then have to go through the arduous process of testing it, dividing it by every number that could possibly be a factor.*"

   That is incorrect. The efficient way of testing if $2^n - 1$ is prime is **not** based on trial division.

2. "*Mathematicians found that if n is prime then with high probability the corresponding Mersenne number is prime.*"

   That is incorrect. Newest found Mersenne prime is 50th we know, but over 4,500,000 values $2^n - 1$ for prime n are lower.

3. "*[Although] too large to be useful for this purpose, encryption uses large prime numbers simply because they are so difficult to find.*"

   That is incorrect. Primes for cryptographic uses are not hard to find using a probabilistic test (so really "probable primes"). What is hard, to break cryptography, is *factoring*.

Record Mersenne primes

The five largest known prime numbers are all Mersenne primes.

Prime	Number of digits	Found
$2^{77232917} - 1$	23,249,425	2017
$2^{74207281} - 1$	22,338,618	2015
$2^{57885161} - 1$	17,425,170	2013
$2^{43112609} - 1$	12,978,189	2008
$2^{42643801} - 1$	12,837,064	2009

Here is $2^{74207281} - 1$ on 745 back-to-back pages of *very small* type.

Since 1876, the largest known prime has been a Mersenne prime except during 1951-52 and 1989-92.

Marin Mersenne

In 1600s, before academies or journals, the French priest Marin Mersenne was a resource for many on the latest work in science.

In 1644, Mersenne claimed $2^n - 1$ is prime for the following 11 exponents $n \leq 257$ and no others up to that bound:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257.$$

Cases up to 19 were known in 1500s: $2^{19} - 1 = 524{,}287$ has square root ≈ 724 and there are 128 primes below that to test as factors. Primality of $2^{31} - 1 = 2{,}147{,}483{,}647$ in the 1600s was speculation.

Historical role for Mersenne primes: finding perfect numbers

An integer $n > 1$ is *perfect* if it is the sum of its proper factors.

Examples. $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$.

The ancient Greeks knew 4 perfect numbers: 6, 28, 496, and 8128.

Theorem. (Euclid) $2^n - 1$ *prime* $\Rightarrow 2^{n-1}(2^n - 1)$ *is perfect*.

n	2	3	5	7	13	17
$2^{n-1}(2^n - 1)$	6	28	496	8128	33550336	8589869056

Theorem. (Euler, 1747) *Every even perfect number has the form* $2^{n-1}(2^n - 1)$ *where* $2^n - 1$ *is prime.*

So even perfect numbers correspond to Mersenne primes: 50 now.

After proving this theorem, Euler wrote:

Utrum autem praeter hos dentur numeri perfecti impares nec ne, difficillima est quaestio.

Historical role for Mersenne primes: finding perfect numbers

An integer $n > 1$ is *perfect* if it is the sum of its proper factors.

Examples. $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$.

The ancient Greeks knew 4 perfect numbers: 6, 28, 496, and 8128.

Theorem. (Euclid) $2^n - 1$ *prime* $\Rightarrow 2^{n-1}(2^n - 1)$ *is perfect*.

n	2	3	5	7	13	17
$2^{n-1}(2^n - 1)$	6	28	496	8128	33550336	8589869056

Theorem. (Euler, 1747) *Every even perfect number has the form* $2^{n-1}(2^n - 1)$ *where* $2^n - 1$ *is prime.*

So even perfect numbers correspond to Mersenne primes: 50 now.

After proving this theorem, Euler wrote:

Whether in addition to these there are any odd perfect numbers is a most difficult problem.

Any odd perfect number would have over 1500 digits.

When can $2^n - 1$ be prime?

Theorem. *For $2^n - 1$ to be prime, n is prime.*

Proof. If $n = k\ell$ with $1 < k < n$ then

$$2^n - 1 = (2^k)^\ell - 1 = (2^k - 1)(2^{k(\ell-1)} + 2^{k(\ell-2)} + \cdots + 2^k + 1),$$

so $2^k - 1$ is a factor of $2^{k\ell} - 1$ and $1 < 2^k - 1 < 2^{k\ell} - 1$. □

The converse is **false**: if n is prime then $2^n - 1$ need not be prime.

Examples.

$$2^{11} - 1 = 2047 = 23 \cdot 89, \quad 2^{23} - 1 = 8{,}388{,}607 = 47 \cdot 178481.$$

Remark. That $2^{11} - 1$ has factor 23 is related to an important construction in coding theory called the perfect binary Golay code (a special subset of 23-dimensional space over integers mod 2).

There are 25 primes $p < 100$ and $2^p - 1$ is prime for 10 of them:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89.$$

Early examples are misleading: p being prime does not tend to make $2^p - 1$ prime.

Settling Mersenne's claim

Here is Mersenne's list of n making $2^n - 1$ prime for $n \leq 257$:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257.$$

Cases $n \leq 19$ were known before Mersenne. What happened later?

1. 1772: Euler proved $2^{31} - 1$ (10 digits) is prime. (Ask later.)
2. 1876: Lucas proved $2^{67} - 1$ (21 digits) is composite *without* factoring it and $2^{127} - 1$ (39 digits) is prime; it would be the largest known prime until the 1950s.
3. 1883: Pervushin proved $2^{61} - 1$ is prime (Mersenne missed).
4. 1911: Powers proved $2^{89} - 1$ is prime (Mersenne missed). Lucas (1891) had claimed this to be composite.
5. 1914: Powers proved $2^{107} - 1$ is prime (Mersenne missed).
6. 1927: Lehmer proved $2^{257} - 1$ (78 digits) is composite.

So Mersenne's list had 5 mistakes: 2 composites included, 3 primes missing. It took over 250 years to settle this.

Factoring a Mersenne number

When Lucas (1876) proved $2^{67} - 1$ is composite he **didn't** factor it.

A factorization of $2^{67} - 1$ was given in 1903 by Frank Nelson Cole: $2^{67} - 1 = 193{,}707{,}721 \cdot 761{,}838{,}257{,}287$. (The factors are prime.)

When asked how he found this, he said (?) "3 years of Sundays."

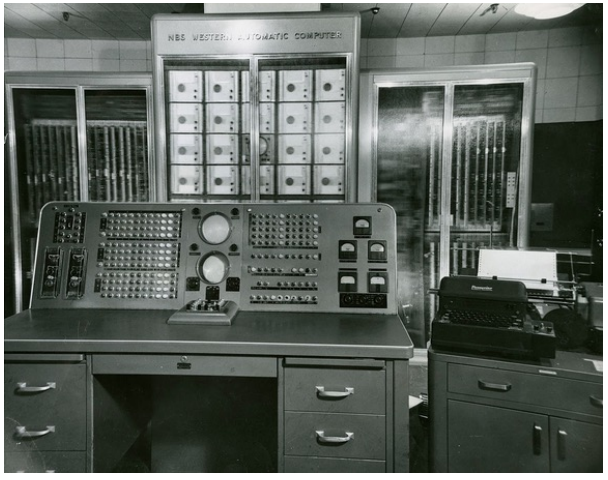
In fact, Cole's paper uses standard techniques in number theory (modular arithmetic and quadratic residues). In the end he found a way to write $2^{67} - 1$ as a difference of squares: it equals

$$380151598250^4 - 380822274783^2 = u^2 - v^2 = (u - v)(u + v).$$

See the MO post "How did Cole factor $2^{67} - 1$ in 1903."

Moving into the modern era

Until 1950s, 12 Mersenne primes were known (max $= 2^{127} - 1$). In 1952, SWAC (Standards Western Automatic Computer) found five new ones: $2^n - 1$ for $n = 521$, 607, 1279, 2203, and 2281.



After primality of $2^{11213} - 1$ was verified in 1963 at UIUC, the math department's outgoing mail stamp changed for a while.

Mersenne primes by computer

In 1927 Lehmer showed Mersenne's "prime" $2^{257} - 1$ is composite without finding a factor. It was factored in 1979 (partially) and 1980 (completely): a product of 3 primes. Today, in a few seconds the free version of Wolfram Alpha finds a prime factor of $2^{257} - 1$ and knows the complementary factor is composite.

In 1996 a distributed computing project called the Great Internet Mersenne Prime Search (`https://www.mersenne.org/`) was launched and has found every new Mersenne prime since the 35th.

The frequency of Mersenne primes found by computers:

Decade	50s	60s	70s	80s	90s	00s	10s
Found	6	5	4	4	7	9	3

Almost as many Mersenne primes were found in 1950s and 1960s as had ever been found before computers!

Infinitude of Mersenne primes?

We present a non-rigorous argument for (i) why there should be infinitely many Mersenne primes and (ii) why they should be rare.

The main idea is the Prime Number Theorem, which says

$$|\{\text{primes} \leq x\}| \sim \frac{x}{\log x}.$$

This suggests the probabilistic heuristic (going back to Gauss)

$$\text{Prob}(m \text{ prime}) = \frac{1}{\log m}$$

for $m \geq 2$ (really, $m \geq 3$), which in return predicts the *expected* number of primes up to x to be

$$\sum_{2 \leq m \leq x} \frac{1}{\log m} \sim \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x},$$

which *is* correct. Let's apply this heuristic to predict a count of Mersenne primes: how should $|\{n \leq x : 2^n - 1 \text{ is prime}\}|$ grow?

Infinitude of Mersenne primes?

Using the heuristic Prob(m prime) $= \dfrac{1}{\log m}$ with $m = 2^n - 1$, the expected number of $n \leq x$ making $2^n - 1$ prime should grow like

$$\sum_{1<n\leq x} \frac{1}{\log(2^n - 1)} \quad \sim \quad \sum_{n\leq x} \frac{1}{n \log 2}$$

Infinitude of Mersenne primes?

Using the heuristic Prob(m prime) $= \dfrac{1}{\log m}$ with $m = 2^n - 1$, the expected number of $n \le x$ making $2^n - 1$ prime should grow like

$$\begin{aligned}
\sum_{1<n\le x} \frac{1}{\log(2^n-1)} &\sim \sum_{n\le x} \frac{1}{n\log 2} \\
&= \frac{1}{\log 2}\sum_{n\le x}\frac{1}{n} \\
&\sim \frac{1}{\log 2}\int_1^x \frac{dt}{t} \\
&= \frac{1}{\log 2}\log x \;=\; \log_2 x.
\end{aligned}$$

This suggests the count $\to \infty$, but *slowly*. (And if $m = 3^n - 1$?)

Infinitude of Mersenne primes?

Using the heuristic Prob(m prime) $= \dfrac{1}{\log m}$ with $m = 2^n - 1$, the expected number of $n \le x$ making $2^n - 1$ prime should grow like

$$\begin{aligned}
\sum_{1<n\le x} \frac{1}{\log(2^n-1)} &\sim \sum_{n\le x} \frac{1}{n\log 2} \\
&= \frac{1}{\log 2}\sum_{n\le x}\frac{1}{n} \\
&\sim \frac{1}{\log 2}\int_1^x \frac{dt}{t} \\
&= \frac{1}{\log 2}\log x \;=\; \log_2 x.
\end{aligned}$$

This suggests the count $\to \infty$, but *slowly*. (And if $m = 3^n - 1$?)

A precise conjecture (of Lenstra, Pomerance, and Wagstaff) is that number of $n \le x$ with $2^n - 1$ prime is $\sim e^\gamma \log_2 x$, where $\gamma \approx .577$ is Euler's constant ($e^\gamma \approx 1.78$). At $x = 80{,}000{,}000$ it's ≈ 46.7.

Infinitude of Mersenne composites?

There is a reason to expect infinitely many composite $2^n - 1$.

Theorem. (Euler) *If p and $2p+1$ are prime, and $p = 4m+3$, then $2^p - 1$ is divisible by $2p+1$.*

Proof. Let $M = 2^p - 1$ and $q = 2p+1$. Then

$$q = 2(4m+3)+1 = 8m+7 \equiv 7 \bmod 8,$$

so by quadratic reciprocity $\left(\frac{2}{q}\right) = 1$. Then

$$2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) = 1 \bmod q,$$

which says

$$2^p \equiv 1 \bmod q,$$

so $2^p - 1$ is divisible by $q = 2p+1$. □

Example. The hypotheses hold for $p = 11$ and $p = 23$. We saw earlier that $2^{11} - 1$ is divisible by $23 = 2 \cdot 11 + 1$ and $2^{23} - 1$ is divisible by $47 = 2 \cdot 23 + 1$.

Infinitude of Mersenne composites?

Theorem. (Euler) *If p and $2p+1$ are prime, and $p = 4m+3$, then $2^p - 1$ is divisible by $2p+1$.*

If $p = 4m+3$ then $2p+1 = 8m+7$.

- Known that $4m+3$ and $8m+7$ each prime infinitely often: special cases of Dirichlet's theorem.
- It is expected that $4m+3$ and $8m+7$ are prime for the same m infinitely often: a special case of Dickson's conjecture.

Dickson's conjecture would imply $2^p - 1$ is composite infinitely often: use $p = 4m+3$ where p and $2p+1$ are both prime.

The Lucas–Lehmer test

The search for enormous primes focuses on numbers $2^n - 1$ because of a primality test tailor-made for them: the *Lucas–Lehmer test*.

Define $M_n = 2^n - 1$ and positive integers s_i by the recursion

$$s_1 = 4, \quad s_i = s_{i-1}^2 - 2$$

for $i \geq 2$: s_i begins as 4, 14, 194, 37634, 1416317954, ...

Theorem. *For odd prime p, M_p is prime* $\Leftrightarrow s_{p-1} \equiv 0 \bmod M_p$.

Key point is that the test works in *both* directions. Lucas found a weaker version of it in 1876 if $p = 4m + 3$ (*e.g.*, $p = 67$ and 127).

Using Lucas–Lehmer test ($s_n = 4,\ 14,\ 194,\ 37634,\ 1416317954, \ldots$)

Lucas–Lehmer test: M_p is prime $\iff s_{p-1} \equiv 0 \bmod M_p$.

Check by modular arithmetic: find $s_1, s_2, s_3, \ldots, s_{p-1} \bmod M_p$ by squaring, subtracting 2, and reducing $p-1$ times. The numbers never exceed M_p^2. Want to check if $s_{p-1} \stackrel{?}{\equiv} 0 \bmod M_p$.

Using Lucas–Lehmer test ($s_n = 4,\ 14,\ 194,\ 37634,\ 1416317954, \ldots$)

Lucas–Lehmer test: M_p is prime $\iff s_{p-1} \equiv 0 \bmod M_p$.

Check by modular arithmetic: find $s_1, s_2, s_3, \ldots, s_{p-1} \bmod M_p$ by squaring, subtracting 2, and reducing $p-1$ times. The numbers never exceed M_p^2. Want to check if $s_{p-1} \stackrel{?}{\equiv} 0 \bmod M_p$.

Example. Is $2^{11} - 1 = 2047$ prime? Compute s_n mod 2047 using its recursion modulo 2047:

i	3	4	5	6	7	8	9	10
$s_i \bmod 2047$	194	788	701	119	1877	240	282	1736

Since $1736 \not\equiv 0 \bmod 2047$, the test says $2^{11} - 1$ is not prime (but this does **not** give us a factor of 2047).

Example. Is $2^{13} - 1 = 8191$ prime? We compute s_n mod 8191:

i	5	6	7	8	9	10	11	12
$s_i \bmod 8191$	3953	5970	1857	36	1294	3470	128	0

Since $s_{12} \equiv 0 \bmod 8191$, the test says $2^{13} - 1$ is prime.

Lucas–Lehmer test combined with other tests

How the Great Internet Mersenne Prime Search tests primality of $2^n - 1$:

1. Trial division of $2^n - 1$ by primes up to a specific bound.
2. If trial division doesn't reveal a factor then apply another factoring algorithm, the "$p - 1$ test" (explained in tomorrow's plenary lecture).
3. If no factor of $2^n - 1$ is found in steps 1 or 2, then apply the Lucas–Lehmer test to $2^n - 1$. It tells us if $2^n - 1$ is or is not prime, but do not get a factor if it's not prime.

There are *probabilistic* primality tests that report "not prime" with absolute certainty and "prime" with very low probability of error. George Woltman, the founder of the Great Internet Mersenne Prime Search, says the Search may start using a probabilistic primality test before the Lucas–Lehmer step, so LL step would only be applied to almost certain primes.

Beyond Lucas–Lehmer I: Gross' test

Proof of Lucas–Lehmer test uses a formula for s_n:

$$s_i = (2+\sqrt{3})^{2^{i-1}} + (2-\sqrt{3})^{2^{i-1}} = \frac{(2+\sqrt{3})^{2^i}+1}{(2+\sqrt{3})^{2^{i-1}}}.$$

The coefficients $(2,1)$ of $2+\sqrt{3}$ satisfy $x^2-3y^2=1$, and all $x+y\sqrt{3}$ with $x,y \in \mathbf{Z}$ satisfying $x^2-3y^2=1$ are a group under multiplication (Pell's equation).

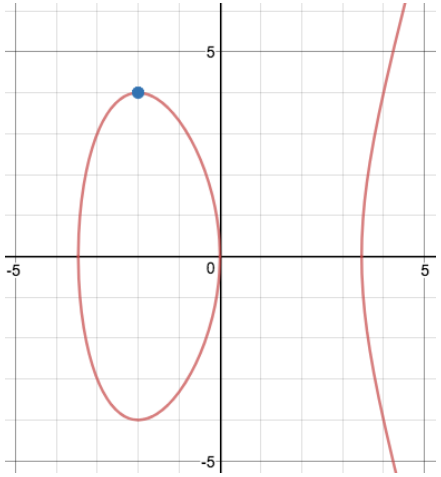
Beyond Lucas–Lehmer I: Gross' test

Proof of Lucas–Lehmer test uses a formula for s_n:

$$s_i = (2+\sqrt{3})^{2^{i-1}} + (2-\sqrt{3})^{2^{i-1}} = \frac{(2+\sqrt{3})^{2^i}+1}{(2+\sqrt{3})^{2^{i-1}}}.$$

The coefficients $(2,1)$ of $2+\sqrt{3}$ satisfy $x^2-3y^2=1$, and all $x+y\sqrt{3}$ with $x,y \in \mathbf{Z}$ satisfying $x^2-3y^2=1$ are a group under multiplication (Pell's equation).

In 2005, B. H. Gross was inspired to use rational points on the elliptic curve $y^2 = x^3 - 12x$, which is a group, to make a new primality test for 2^n-1 using repeated doubling of $(-2,4)$.



Beyond Lucas–Lehmer II: Lucas–Lehmer–Riesel test

Riesel generalized the Lucas–Lehmer test to test primality of

$$k \cdot 2^n - 1$$

for odd k and large enough n ($2^n > k$). Primality no longer requires n to be prime, *e.g.*, $7 \cdot 2^{45} - 1$ is prime.
The LLR test is like the LL-test:

$$k \cdot 2^n - 1 \text{ is prime} \iff s_{n-1} \equiv 0 \bmod k \cdot 2^n - 1$$

where $s_1, s_2, s_3, \ldots$ is a recursive sequence with $s_i = s_{i-1}^2 - 2$. The *initial value* s_1 depends on k.

- For k not divisible by 3, can use $s_1 = (2+\sqrt{3})^k + (2-\sqrt{3})^k$.
  $k = 1$: $s_1 = (2+\sqrt{3}) + (2-\sqrt{3}) = 4$
  $k = 5$: $s_1 = (2+\sqrt{3})^5 + (2-\sqrt{3})^5 = 724$
  $k = 7$: $s_1 = (2+\sqrt{3})^7 + (2-\sqrt{3})^7 = 10084$
- For k divisible by 3, selection of s_1 is more subtle (involves Jacobi symbols).

Changing -1 to $+1$

If we switch $2^n - 1$ to $2^n + 1$, and $k \cdot 2^n - 1$ to $k \cdot 2^n + 1$, the primality behavior can change radically.

1. $2^n + 1$ appears to have *very few* prime values: n must be a power of 2 and only known primes are at $n = 1, 2, 4, 8, 16$ (called Fermat primes – inspired Gauss to focus on math!).
2. for some odd k, $k \cdot 2^n + 1$ is provably composite for *all* $n \geq 1$!

An example of 2nd effect is $k = 78557$: for $n \geq 1$, $78557 \cdot 2^n + 1$ is divisible by 3, 5, 7, 13, 19, 37, or 73.

Sierpinski problem: show 78557 is the smallest such k. For each odd $k < 78557$ we want to find a prime of the form $k \cdot 2^n + 1$.

There is a distributed computing project working on this task at PrimeGrid (`http://www.primegrid.com/`), and only five k remain to be settled: 21181, 22699, 24737, 55459, and 67607.

Questions?

Appendix: primality of one Mersenne number

How did Euler show $2^{31} - 1 = 2{,}147{,}483{,}647$ is prime? If it is not prime, it has prime factor $p \leq \sqrt{2^{31} - 1} \approx 46340.9$. There are 4792 such primes. Euler cut down the search space a lot!

From $p \mid 2^{31} - 1$ we have $2^{31} \equiv 1 \bmod p$, so $31 \mid (p - 1)$. Thus $p = 1 + 31k$. Since p odd, k is even: $p = 1 + 62\ell$. Then

$$2^{(p-1)/2} = 2^{31\ell} \equiv 1 \bmod p,$$

so by Euler's criterion $\left(\frac{2}{p}\right) = 1$, which implies $p \equiv 1, 7 \bmod 8$.

The congruence conditions $p \equiv 1 \bmod 62$ and $p \equiv 1, 7 \bmod 8$ are the same as $p \equiv 1, 63 \bmod 248$, so

$$p = 1 + 248m \text{ or } p = 63 + 248m.$$

The number of primes $1 + 248m \leq 46340$ and $63 + 248m \leq 46340$ is 84 total: manageable for Euler to check by hand.