

The remarkable arithmetic of recurrence sequences



Marin Mersenne (1588–1648)

Image taken from

<http://sh1.stanford.edu/Eyes/kircher/mersenne.html>

Mersenne noticed that $2^2 - 1$, $2^3 - 1$, $2^5 - 1$, and $2^7 - 1$ are all primes.

He suggested on the basis of experiments that $2^p - 1$ would be a prime whenever p is a prime that exceeds by 3 or less an even power of 2.

Lemma: If $n = ab$ is composite, then $2^n - 1$ is composite.

Proof: $\frac{2^n - 1}{2^a - 1} = 2^{n-a} + 2^{n-2a} + \dots + 2^a + 1.$

Mersenne was wrong: Lucas (1876) showed that $2^{67} - 1$ is not prime (without factoring it).

Cole (1903) at the American Mathematical Society showed that $2^{67} - 1$ is equal to

$$193707721 \times 761838257287.$$

It's a little easier now:

```
? factor(2^(67)-1)
```

```
time = 14 ms.
```

```
%1 = [193707721 1] [761838257287 1]
```

Impressive results were known earlier: as a simple example, Fermat proved that

$$47 \mid 2^{23} - 1.$$

How?

Write M_n for $2^n - 1$.

Lemma: If p is a prime, and q is a prime dividing M_p , then $q \equiv 1 \pmod{p}$.

The proof is an application of Fermat's Little Theorem.

For $2^{23} - 1$, Fermat would have looked for possible divisors among the primes of the form $23n + 1$ smaller than $\sqrt{2^{23} - 1}$:

47, 277, 461, ...

and then was lucky!

Mersenne primes (primes of the form $2^p - 1$) have special properties that make them easy to check for primality.

The largest known prime is usually one of these: the current record holder is

$$2^{25964951} - 1,$$

a number with 7816230 decimal digits.

These large primes are found using idle time on thousands of PCs; see

www.mersenne.org/prime.htm

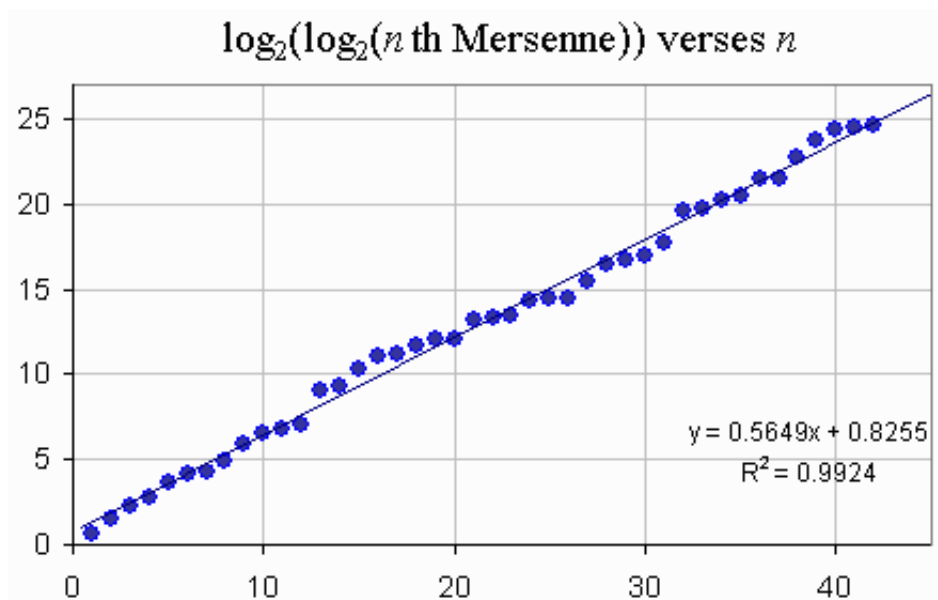
The Mersenne Prime Conjecture

Numerical evidence and a careful (but not rigorous) heuristic argument suggest:

- There are infinitely many Mersenne primes.
- If p_1, p_2, \dots are the primes for which

$$M_{p_1}, M_{p_2}, \dots$$

are primes, then $\log \log(M_{p_n})$ is approximately a constant times n .



Graph taken from Chris Caldwell's Prime Pages

<http://www.utm.edu/research/primes/>

An easier problem

The Mersenne prime conjecture, even in a weak form, seems very difficult.

However, the sequence does produce infinitely many new primes.

Given any sequence a_1, a_2, \dots a prime p that divides a_n but does not divide any earlier a_m with $m < n$ is called a **primitive divisor** of a_n .

Zsigmondy's Theorem: For $n \neq 6$, M_n has a primitive divisor.

The next page shows the first few.

n	M_n	Factorization
2	3	3
3	7	7
4	15	3 · 5
5	31	31
6	63	3 ² · 7
7	127	127
8	255	3 · 5 · 17
9	511	7 · 73
10	1023	3 · 11 · 31
11	2047	23 · 89
12	4095	3 · 5 · 7 · 13
13	8191	8191
14	16383	3 · 43 · 127
15	32767	7 · 31 · 151
16	65535	3 · 5 · 17 · 257
17	131071	131071
18	262143	3 ³ · 7 · 19 · 73
19	524287	524287
20	1048575	3 · 5 ² · 11 · 31 · 41
21	2097151	7 · 127 · 337
22	4194303	3 · 23 · 89 · 683
23	8388607	47 · 178481
24	16777215	3 · 5 · 7 · 13 · 17 · 241

Table taken from “An Introduction to Number Theory”, Everest and Ward, Springer-Verlag(2005).

The proof is not very difficult, but uses a little more machinery. It ends up with a statement:

if M_n does not have a primitive divisor, then

$$\log n < 2 \log \log n + C$$

for some explicit constant C . This bounds n , and then remaining cases can be checked.

Zsigmondy proved a more general result, but essentially no magic is involved.

Deep magic

Diophantine analysis asks: if α is not a rational number for some special reason, how small could

$$\left| \alpha - \frac{p}{q} \right|$$

be, with integers p and q ?

Naive answer: as small as you please!

Sophisticated answer: how big is q allowed to be?

It turns out that you can always find infinitely many different p s and q s with

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Roth's Theorem: (1950s) If α is not rational, but is a zero of a polynomial with integer coefficients (an **algebraic number**), then for any small number $\epsilon > 0$, there are only finitely many ps and qs with

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}.$$

Laurent–Mignotte–Nesterenko: (1990s)
If α and β are algebraic numbers with the property that $\alpha^n = \beta^m \implies n = m = 0$, then for any rational numbers a and b ,

$$|a \log \alpha - b \log \beta| \geq \square$$

where \square is a complicated explicit expression involving information about α and β and the denominators of a and b .

Using this result, and a great deal of other high-powered machinery, Zsigmondy's Theorem has been updated for the new millenium.

Bilu–Hanrot–Voutier: (2001) If L_1, L_2, \dots is any Lucas or Lehmer sequence, then for $n > 30$, L_n has a primitive divisor.

This is a huge class of sequences, including:

- The Fibonacci sequence $1, 1, 2, 3, \dots$
- The Lucas sequence $1, 3, 4, \dots$
- For integers P, Q with $P^2 - 4Q > 0$, and

$$(x - \alpha)(x - \beta) = x^2 - Px + Q,$$

the sequences defined by

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$$

or

$$V_n = \alpha^n + \beta^n.$$

What is surprising is the uniformity (the 30) and the modest size of the bound: for any given sequence in this class, you can check the remaining cases.