PERFECT NUMBERS AND MERSENNE PRIMES

KEITH CONRAD

1. Introduction

A positive integer n is called a *perfect number* when it is equal to the sum of its proper factors. The first two perfect numbers are 6 and 28 since

$$1 + 2 + 3 = 6, \quad 1 + 2 + 4 + 7 + 14 = 28.$$

There is a close connection between perfect numbers and primes of the form $2^n - 1$. To see this, we first show $2^n - 1$ can be prime only when $n = p$ is a prime number. When n is composite, write $n = ab$ with $a \geq 2$ and $b \geq 2$, so $2^n - 1 = (2^a)^b - 1$. The polynomial identity $x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \cdots + x + 1)$ at $x = 2^a$ gives us

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

and the two factors on the right are greater than 1. Thus n being composite makes $2^n - 1$ composite, so $2^n - 1$ being prime implies n is prime. For small primes p, $2^p - 1$ is prime:

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127.$$

However, $2^{11} - 1 = 23 \cdot 89$, so primality of p is a necessary condition for $2^p - 1$ to be prime but it is *not* a sufficient condition. The table below indicates for primes $p \leq 47$ when $2^p - 1$ is prime.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$2^p - 1$ prime?	✓	✓	✓	✓		✓	✓	✓			✓				

The first ten primes of the form $2^p - 1$ occur for $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, and 89. When $2^p - 1$ is prime, it is denoted M_p and called a *Mersenne prime* after Marin Mersenne, a French priest who wrote about them in 1644. It is expected that there are infinitely many Mersenne primes, and this remains an open problem. Just 52 primes values of M_p have been found, with the largest being $2^p - 1$ for $p = 136{,}279{,}841$ and has over 41 million digits. There is currently a $150,000 prize for the first prime number (of any kind) found with over 100 million digits. A table of all known Mersenne primes is at https://t5k.org/mersenne/.

Here is the link between perfect numbers and Mersenne primes.

Theorem 1.1. *For an even positive integer n, n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime.*

The direction ($\Longleftarrow$) was known to the ancient Greeks, as it is Prop. 9 of Book IX of Euclid's *Elements*. The direction ($\Longrightarrow$) is due to Euler [1, Sect. 8] in 1747, although Euler's paper was published around 100 years later.

Proof. ($\Longleftarrow$) Let $n = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime, so p is prime. Write $2^p - 1$ as q. The factors of n in $\mathbf{Z}^+$ are $1, 2, \ldots, 2^{p-1}$ and $q, 2q, \ldots, 2^{p-1}q$, so the sum of the factors of n

is

$$1 + 2 + \ldots + 2^{p-1} + q + 2q + \ldots + 2^{p-1}q = (1 + 2 + \ldots + 2^{p-1})(1 + q) = (2^p - 1)2^p = 2n.$$

Thus n is perfect.

($\Longrightarrow$) Let n be an even perfect number. Since it is even, $n = 2^k\ell$ where $k \geq 1$ and ℓ is odd. Then

$$\sigma(n) = 2n \Longrightarrow \sigma(2^k)\sigma(\ell) = 2n \Longrightarrow (2^{k+1} - 1)\sigma(\ell) = 2^{k+1}\ell. \tag{1.1}$$

Thus $(2^{k+1} - 1) \mid 2^{k+1}\ell$ and $2^{k+1} - 1$ is relatively prime to 2^{k+1}, so $(2^{k+1} - 1) \mid \ell$: we can write $\ell = (2^{k+1} - 1)m$. Since $(2^{k+1} - 1) > 1$, m is a proper factor of ℓ. By (1.1),

$$(2^{k+1} - 1)\sigma(\ell) = 2^{k+1}\ell = 2^{k+1}(2^{k+1} - 1)m \Longrightarrow \sigma(\ell) = 2^{k+1}m.$$

Since m is a proper factor of ℓ and

$$\ell + m = (2^{k+1} - 1)m + m = 2^{k+1}m = \sigma(\ell),$$

the *only* factors of ℓ in $\mathbf{Z}^+$ are ℓ and m. Thus $m = 1$ and ℓ is prime. This implies $\ell = (2^{k+1} - 1)m = 2^{k+1} - 1$, so $2^{k+1} - 1$ is prime and $n = 2^k\ell = 2^k(2^{k+1} - 1)$. That makes $2^{k+1} - 1$ a Mersenne prime, so $p := k + 1$ is prime and $n = 2^k\ell = 2^{p-1}(2^p - 1)$. □

This theorem shows even perfect numbers and Mersenne primes naturally go together. (It is expected, but not proved, that there are no odd perfect numbers.) Mersenne's work on Mersenne primes in 1644 was in fact work on perfect numbers. He claimed that $2^{p-1}(2^p - 1)$ is perfect, or equivalently $2^p - 1$ is prime, for the following 11 values of $p \leq 257$ and no other p in that range: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257. Cataldi had checked the 6-digit numbers $2^{17} - 1$ and $2^{19} - 1$ are prime in 1588. Checking the 10-digit number $2^{31} - 1$ or larger examples are prime was a very error-prone task in the 1600s and the first accepted proof that $2^{31} - 1$ is prime is credited to Euler in 1772.

Mersenne's list of p where $2^p - 1$ is prime is partly right and partly wrong when $p \geq 31$:

- $2^{31} - 1$ (10 digits) and $2^{127} - 1$ (39 digits) are prime,
- $2^{67} - 1$ (21 digits) and $2^{257} - 1$ (78 digits) are composite,
- Mersenne missed three examples with $p < 257$: $2^{61} - 1$ (19 digits), $2^{89} - 1$ (27 digits), and $2^{107} - 1$ (33 digits) are prime.

The largest Mersenne prime whose primality was proved entirely by hand calculation is $2^{127} - 1$ by Lucas in 1876, and he was not completely confident in his work, writing "je pense avoir démontré que le nombre $A = 2^{127} - 1$ est premier" (I think I have demonstrated that the number $A = 2^{127} - 1$ is prime) [5, p. 167]. This was not the *last* Mersenne prime to have its primality proved by hand calculation since Mersenne primes have not always been discovered in numerical order, *e.g.*, primality of $2^{107} - 1$ was proved by Powers in 1914 [6].

A computer was first applied to the search for Mersenne primes by Raphael Robinson in 1952. It found five new Mersenne primes that year: $2^p - 1$ for $p = 521$, 607, 1279, 2203, and 2281 [2, 3, 4]. The first two examples were found on the first day of testing. This computer also determined that earlier manual checks that $2^p - 1$ is composite when $p = 101$, 103, 109, 137, and 167 had errors [7, p. 844], but these numbers are nevertheless composite.

The verification by Lehmer in 1930 that Mersenne's last example $2^{257} - 1$ is composite, but without factoring it, took hundreds of hours with a desk calculator. Robinson's computer verified Lehmer's work on $2^{257} - 1$ in under a minute. Today Wolfram Alpha can explicitly factor $2^{257} - 1$ in a few seconds.

References

[1] L. Euler, "De numeris amicibilibus," *Commentationes arithmeticae* **2** (1849), 627-636. URL https://scholarlycommons.pacific.edu/euler-works/798/.

[2] D. H. Lehmer, "Recent discoveries of large primes," *Mathematical Tables and Other Aids to Computation*, **6** (1952), 61. URL https://www.ams.org/journals/mcom/1952-06-037/S0025-5718-52-99403-9/S0025-5718-52-99403-9.pdf.

[3] D. H. Lehmer, "A new Mersenne prime," *Mathematical Tables and Other Aids to Computation*, **6** (1952), 205. URL https://www.ams.org/journals/mcom/1952-06-039/S0025-5718-52-99387-3/S0025-5718-52-99387-3.pdf.

[4] D. H. Lehmer, "Two new Mersenne primes," *Mathematical Tables and Other Aids to Computation*, **7** (1953), 72. URL https://www.ams.org/journals/mcom/1953-07-041/S0025-5718-53-99372-7/S0025-5718-53-99372-7.pdf.

[5] É. Lucas, "Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers," *C. R. Acad. Sci. Paris*, **82** (1876), 165–167. URL https://www.biodiversitylibrary.org/item/24897#page/171/mode/1up.

[6] R. E. Powers, "A Mersenne Prime," *Bull. Amer. Math. Soc.* **20** (1914), p. 531. https://www.ams.org/journals/bull/1914-20-10/S0002-9904-1914-02547-9/S0002-9904-1914-02547-9.pdf.

[7] R. M. Robinson, "Mersenne and Fermat Numbers," *Proc. Amer. Math. Soc.* **5** (1954), 842–846. URL https://t5k.org/mersenne/LukeMirror/lit/lit_024s.htm.