Perfect Numbers

Joe Luquette

June 20, 2008

History

A perfect number n is a number whose positive divisors (sans the number itself) sum to n. Equivalently, if we consider n to be a divisor of itself (which it is!), we call n perfect if the sum of all of its divisors is $2n$. These numbers have been studied for thousands of years, as ancient Greek mathematicians spent much time studying the relationship between a number and its divisors. Many classes of numbers arose from these studies, including *deficient* numbers, whose divisors' sum is less than the number itself, *abundant* numbers, whose divisors sum to more than the number itself, and, of course, *perfect numbers*.

An example of a perfect number is 6: the divisors of 6 are 1, 2, 3 and 6. Adding these together, we see that

$$1 + 2 + 3 = 6, \quad \text{or} \quad 1 + 2 + 3 + 6 = 2 \cdot 6.$$

The next few perfect numbers are small, and were easy to find by exhaustive search: 6, 28, 496 and 8128. In fact, Euclid himself discovered that these perfect numbers are generated by the formula

$$2^{n-1}(2^n - 1),$$

whenever $2^n - 1$ is prime. In the 17th century, the monk Marin Mersenne began studying primes of the form $2^n - 1$, and these primes have become known as *Mersenne primes*.

It is easy to see that any perfect number generated by this formula must be even: 2^{n-1} is always even and $2^n - 1$ is always odd.[1] Since the product of an even and odd number is even, we see that this formula can only render *even perfect numbers*. Even glancing again at our initial list of four perfect numbers, we see that each of these values is indeed even. This begs the obvious question: do odd perfect numbers exist?

Technical Details

There is a bit of standard notation for dealing with perfect numbers and their properties. The first such object is the *divisor function* $\sigma(n)$. The divisor function on any value n is the sum of every natural number which divides n—including n itself. Thus,

$$\begin{aligned}
\sigma(1) &= 1, \\
\sigma(2) &= 1 + 2, \\
\sigma(3) &= 1 + 3, \\
\sigma(4) &= 1 + 2 + 4, \\
\sigma(5) &= 1 + 5, \\
\sigma(6) &= 1 + 2 + 3 + 6,
\end{aligned}$$

and so on. We can then formally define the divisor function as follows.

[1] Unless $n = 1$, in which case $2^0(2^1 - 1) = 2$ is not a perfect number.

Definition. Let $n \in \mathbb{N}$. Then we denote the summation over all of n's natural divisors by

$$\sigma(n) = \sum_{d \in N : d | n} d,$$

and refer to $\sigma : \mathbb{N} \to \mathbb{N}$ as the *divisor function*.

With the divisor function well-defined, a more exacting definition of a perfect number can be given.

Definition. Let $n \in \mathbb{N}$ such that

$$\sigma(n) = 2n,$$

then we say that n is a *perfect number*.

Mersenne Primes and Even Perfect Numbers

As we discovered earlier, the first four perfect numbers are given by the formula

$$2^{n-1}(2^n - 1),$$

when $2^n - 1$ is prime. Primes of this form are referred to as *Mersenne primes* and are deeply related to even perfect numbers. Mathematicians had previously been interested in primes of the form $a^n - 1$ for arbitrary $a \in \mathbb{N}$. However, it is easy to see that for $n > 1$, the only possible value for a is 2. This is due to the following factorization:

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

Thus, for any number of the form $a^n - 1$ with $n > 2$, we know immediatley that $a - 1 \mid a^n - 1$. When $a = 2$, we have $a - 1 = 1$, which does not pose a problem for a prime number. However, for any other value of $a > 2$, this divisor will destroy the primality of $a^n - 1$.

Thus, the study of primes of the form $2^n - 1$ began. The singularity of the subject of Mersenne primes and even perfect numbers had been realized by mathematicians as early as 1000AD; but it was not until the 18th century that Euler provided a bijection between the Mersenne primes and the even perfect numbers. That is to say, due to Euler's result, we have a complete description of *all* even perfect numbers.

Theorem (Euler)**.** *Let $n \in \mathbb{N}$ be an even perfect number. Then there exists a $k \in \mathbb{N}$ such that*

$$n = 2^{k-1}(2^k - 1).$$

Odd Perfect Numbers

Up until this point, we have been very careful to point out that the perfect numbers generated by Mersenne primes are always even. Even more amazingly, we've provided a complete description of the set of even perfect numbers. But what about odd perfect numbers?

These objects have proven to be very elusive. Many results have shown that, if an odd perfect number were to exist, that it would have an extremely limited form. For example, Euler also showed that if n were an odd perfect number, that its prime factorization must be given by

$$n = q^{\alpha} p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k},$$

where $q \equiv \alpha \equiv 1 \pmod 4$ and $q, p_1, \ldots, p_k$ are distinct primes. To give an example of a less elegant property of an odd perfect number, Nielsen and Hare showed that n would have to have at least 75 prime factors; at least 9 of which are distinct.

Given these sometimes powerful and sometimes ludicrous restrictions on odd perfect numbers, it is widely believe that no odd perfect numbers can exist. A large distributed computing is currently performing an exhaustive search to increase the range of numbers in which we know there exist no odd perfect numbers. So far, the project has verified that no odd perfect numbers exist in the interval $[1, 10^{300}] \subset \mathbb{N}$.

Further Questions

Upon studying numbers $n \in \mathbb{N}$ which satisfy $\sigma(n) = 2n$, the question naturally arises: what is so important about the coefficient 2? Can we describe other classes of numbers by changing the coefficient or using a different function of n altogether? Here, we examine a few different options.

First, what about numbers that satisfy $\sigma(n) = n$? In reality, this defines an extremely narrow class of numbers: the only natural number to satisfy this is 1. To see why no natural number greater than 1 can satisfy $\sigma(n) = n$, consider that for every $n \in \mathbb{N}$, we know that both $1 \mid n$ and $n \mid n$. When $n > 1$, we then know that

$$\sigma(n) \geq 1 + n > n, \qquad n > 1.$$

Thus, $\sigma(n) \neq n$ for any $n > 1$.

What about trying some other arbitrary coefficient? Let us consider the set of natural numbers

$$\{n \in \mathbb{N} \mid \sigma(n) = 3n\}.$$

This set is much harder to analyze. It is, however, non-trivial and non-empty. The first three such numbers are 120, 672 and 523,776. An exhaustive search by computer has shown that no more such numbers exist in the interval $[776, 10^8]$.

An interesting property shared by these three numbers is the structure of their prime factorization. We have

$$\begin{aligned} 120 &= 2^3 \cdot 3^1 \cdot 5^1, \\ 672 &= 2^5 \cdot 3^1 \cdot 7^1, \\ 523,776 &= 2^9 \cdot 3^1 \cdot 11^1 \cdot 31^1. \end{aligned}$$

We may perhaps conjecture that all numbers satisfying $\sigma(n) = 3n$ are of the form

$$n = 2^\alpha \cdot p_1^1 \cdot p_2^1 \cdot \cdots \cdot p_k^1.$$

Clearly, α need not be prime and the primes $p_1, \ldots, p_k$ need not all be 1 or 3 modulo 4. An attempt at a proof of this conjecture is beyond the scope of this paper.

Now we consider a different function of n altogether: a quadratic function. So, we look at the following set of naturals:

$$\{n \in \mathbb{N} \mid \sigma(n) = n^2\}.$$

This unfortunately also defines an extremely trivial set of natural numbers. To begin, clearly 1 satisfies this property and belongs to the above set. We claim that no other number can have this property. First, recall the value of the following summation:

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

The above defines the sum of all natural numbers less than or equal to n; it is then a clear consequence of the definition of the divisor function that

$$\sigma(n) \leq \sum_{k=0}^{n} k,$$

since the divisors of n form a subset of the numbers less than or equal to n. Clearly, then if we can show that $\sum_{k=0}^{n} k < n^2$ for all $n > 1$, we see that

$$\sigma(n) \leq \sum_{k=0}^{n} k < n^2 \quad \text{implies} \quad \sigma(n) \neq n^2, \quad n > 1$$

We prove exactly this in the following lemma.

Lemma. *Let $n \in \mathbb{N}$ be greater than 1. Then $\sum_{k=0}^{n} k < n^2$.*

Proof. We can prove this inductively. Consider the base case $n = 2$: then a direct check shows that

$$\frac{n(n+1)}{2} = 3 < 4 = n^2, \quad n = 2.$$

Now suppose inductively that $n(n+1)/2 < n^2$ for some n. Consider the result of adding $2n+1$ to each side of our inductive hypothesis:

$$\frac{n(n+1)+4n+2}{2} = \frac{n(n+1)}{2} + 2n + 1 < n^2 + 2n + 1 = (n+1)^2. \tag{1}$$

The far left-hand term of the above display can be rewritten:

$$\frac{n(n+1)+4n+2}{2} = \frac{n^2+5n+2}{2}.$$

Now we are almost done: we know that $(n+1)(n+2)/2 = (n^2+3n+2)/2$ and clearly

$$\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2} < \frac{n^2+5n+2}{2}, \quad n > 0. \tag{2}$$

Combining equations (1) and (2), we arrive at

$$\frac{(n+1)(n+2)}{2} < (n+1)^2.$$

By induction, we have $\sum_{k=0}^{n} k < n^2$ for all $n > 2$. □

Now we consider one final class of numbers: those defined by

$$\{p \in \mathbb{N} \mid \sigma(p) = p + 1\}.$$

The variable p used in the set definition above is meant to be suggestive: this set is exactly the set of prime numbers. The proof is extremely simple and straightforward.

Proof. Suppose that $n \in \mathbb{N}$ is such that $\sigma(n) = n+1$. First, it is clear that 1 cannot satisfy this statement: $\sigma(1) = 1$. So let us consider $n > 1$. If $n > 1$, then we know that there are *at least* two distinct divisors of n: 1 and n itself. Thus $\sigma(n) \geq n+1$ for all $n > 1$. Recall that we chose n such that $\sigma(n) = n+1$. But then this means that 1 and n are the *only*[2] divisors of n! This is exactly the definition of a prime number, and thus we are done. □

[2]If there existed another divisor, $d \in \mathbb{N}$, then $\sigma(n) = 1 + n + d > 1 + n$, refuting our selection of n.