# Oddly Perfect

On the Oldest Open Problem in Mathematics

1500723

March 20, 2017

# Contents

# 1 Introduction

Simply put, a perfect number is a whole number which is the sum of its proper divisors, known as *aliquot parts*. So $6 = 1 + 2 + 3$ is perfect, but $8 \neq 1 + 2 + 4$ is not. Perfect numbers have fascinated mathematicians for over two millennia, to quote Martin Gardner; "One would be hard put to find a set of whole numbers with a more fascinating history" [2], and so we start by investigating these numbers from a historical viewpoint, before proceeding to uncover the underlying mathematics behind these intriguing numbers.

Although the idea of a perfect number was certainly known to Pythagoras and his followers, they viewed these numbers as mystical objects, rather than mathematical ones, linked with marriage and beauty [18, p. 1]. The first person to study perfect numbers in more detail was Euclid [4, p. 4], who recorded his results in his *Elements* c. 300 BC. The ancient Greeks knew of the first four perfect numbers [16, p. 128] which are $6, 28, 496$ and $8128$, and Euclid found a formula linking perfect numbers with primes [7, Book IX, pp. 227–228]. We shall look at his work in more detail in Section 3.

The next major contribution came from Nicomachus of Gerasa c. 100 AD who gave a classification of numbers based on perfect numbers in his *Introductio Arithmetica* as follows: if the sum of the aliquot parts is equal to the number, then the number is *perfect*. If the sum is greater than the number itself, then the number is *superabundant*, and if the sum is less than the number, it is said to be *deficient* [4, p. 3]. These terms are still used today, although superabundant numbers are usually simply referred to as abundant. Nicomachus then went on to describe the moral and biological properties of each type of number, something that seems very strange today! Perfect numbers were said to be objects of "measure, propriety, [and] beauty", whilst describing deficient numbers as having "a single eye" and "fewer than five fingers" and superabundant numbers as having "ten mouths" and "a hundred arms" [5, pp. 207–208].

Most importantly, Nicomachus made five conjectures in his *Introductio Arithmetica* without proof [13]:

1. The $n$th perfect number has n digits.
2. All perfect numbers are even.
3. All perfect numbers end in 6 and 8 alternately.
4. Euclid's formula holds.
5. There are infinitely many perfect numbers.

Unfortunately for Nicomachus, not all of his conjectures are correct, namely the first and third conjectures, as we shall see later. However, what

is astonishing is the fact that the second and fifth conjectures are still open problems, and the second is now commonly stated as the *oldest unsolved problem in mathematics* (much to the annoyance of the fifth!).

There is then a rather large gap in the history of this subject. It is known that some Arab mathematicians made progress around 1000 AD, but little is recorded of their feats [14, pp. 125–126]. It was not until the 15th and 16th centuries that interest started to grow again, with mathematicians such as Fermat, Cataldi, Descartes and Mersenne taking up the study of these numbers [4, § 1]. In fact, Fermat discovered his *Little Theorem* after investigating perfect numbers [13].

The major breakthrough in the subject came from Euler, who discovered that not only did Euclid's formula hold, but that all even perfect numbers could be found using his formula, and he also investigated the properties of odd perfect numbers [4, p. 10] which led to several other mathematicians, in particular Sylvester [9], finding restrictions on odd perfect numbers, a pursuit which today is still an active area of research. Throughout this essay we will provide more insight into the history of perfect numbers as we relive the discoveries of some of the great names we have just discussed.

## 2 The Divisor Function and Elementary Theory

Before we start looking at the exciting mathematics behind perfect numbers, we must cover some basic, but very useful, results and tools. Throughout this essay, we will be dealing with natural numbers and so any variable can be assumed to be a natural number unless otherwise stated.

**Definition 2.1.** The *sum of divisors function* $\sigma(n)$ is the sum of all the positive divisors of $n$, including 1 and $n$.

$$\sigma(n) = \sum_{d|n} d.$$

So $\sigma(22) = 1 + 2 + 11 + 22 = 36, \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$ and importantly we note that $\sigma(p) = p + 1$ if and only if $p$ is a prime number. We can also see that 22 is deficient and that 12 is abundant.

We can now formally define a perfect number using the sum of divisors function.

**Definition 2.2.** $N$ is said to be a *perfect number* if $\sigma(N) = 2N$.

Although this definition may at first seem a little strange, as we are no longer defining a perfect number using aliquot parts, it is equivalent and will simplify proofs, and shall be the way we define a perfect number from now on.

**Definition 2.3.** A function $f$ on the natural numbers is said to be *multiplicative* if $f(mn) = f(m)f(n)$ whenever $m$ and $n$ are coprime.

**Lemma 1.** *The sum of divisors function $\sigma$ is multiplicative.*

*Proof.* [15, p. 8]. Suppose $m$ and $n$ are coprime. Let $a_1, a_2, \ldots, a_r$ be the divisors of $m$ and $b_1, b_2, \ldots, b_s$ the divisors of $n$. Then for any $i, j$ with $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant s$, we have that $a_i b_j$ is a divisor of $mn$ and all divisors of $mn$ can be uniquely expressed in this form since $m$ and $n$ are coprime. So

$$\sigma(mn) = \sum_{i,j} a_i b_j = (a_1 + \cdots + a_r)(b_1 + \cdots + b_s) = \sum_{i}^{r} a_i \sum_{j}^{s} b_j = \sigma(m)\sigma(n).$$

□

The following lemma will prove (pun intended!) to be very useful for many upcoming results and so we state it as a lemma.

**Lemma 2.**

$$1 + x + x^2 + ... + x^n = \sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}$$

*Proof.* The proof is straightforward and so we shall omit it. This result is proved in Euclid's *Elements* [7, Book IX, Proposition 35], or for a very interesting geometric proof, see [1]. □

We can now find a formula for the sum of the divisors of any number in terms of its prime factorisation.

**Proposition 3.** *If $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ is the prime factorisation of $N$, then*

$$\sigma(N) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

*Proof.* [16, p. 90] This follows almost directly from the previous lemma and the multiplicity of $\sigma$. We have $\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1}-1}{p_i-1}$. So

$$\sigma(N) = \sigma(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \sigma(p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

□

## 3 Even Perfect Numbers

Now that we have covered some elementary results, we can look at the work of Euclid and Euler on even perfect numbers. Euclid was the first person to delve deeper into the mathematics of perfect numbers after noticing a pattern in the first four perfect numbers, those which were known to the Greeks at the time:

$$\begin{aligned} 6 &= 2^1(1+2) = 2\cdot 3, \\ 28 &= 2^2(1+2+2^2) = 4\cdot 7, \\ 496 &= 2^4(1+2+2^2+2^3+2^4) = 16\cdot 31, \text{and} \\ 8128 &= 2^6(1+2+\cdots+2^6) = 64\cdot 127. \end{aligned}$$

However, $90 = 2^3(1+2+2^2+2^3) = 8\cdot 15$, and $2016 = 2^5(1+2+\cdots+2^5) = 32\cdot 63$ are not included in this sequence, and similarly, $32640 = 2^7(1+2+\cdots+2^7)$ would be left out as well. In fact, the next number in this sequence is the 5th perfect number $33550336 = 2^{12}(1+2+\cdots+2^{12})$ — a rather big jump! — and unfortunately for Nicomachus, a number which disproves his first conjecture, since it has eight digits. Back to the topic at hand, the question is: *what is the pattern?* Euclid asked himself the same question and formulated the answer as the following proposition (translated by Heath [13]) in Book IX of his *Elements*, incidentally the very last number theory result in the (series of) books.

> If as many numbers as we please beginning from a unit be set out continuously in double proportion until the sum of all becomes a prime, and if the sum multiplied into the last make some number, then the product will be perfect.

Of course, this statement is a little different to how we write things nowadays, however the idea is identical. In today's language, the statement says: *if we add the powers of* 2*, starting from* $2^0 = 1$*, until we have a prime number, and then multiply this prime by the last power of* 2 *which was added, then we have a perfect number.* Let us instead state this mathematically!

**Theorem 4.** *(Euclid) If* $2^n - 1$ *is prime, then* $N = 2^{n-1}(2^n - 1)$ *is perfect.*

Note that $(1+2+\cdots+2^n) = 2^n - 1$ by the properties of geometric series (Lemma 2).

*Proof.* [16, p. 41]. Using the properties of the divisor function, the proof is straightforward. Our aim is of course to show that $\sigma(N) = 2N$.

The divisors of $2^{n-1}$ are $1, 2, \ldots, 2^{n-1}$, so $\sigma(2^{n-1}) = 2^n - 1$, and then $\sigma(2^n - 1) = (2^n - 1) + 1 = 2^n$ because $2^n - 1$ is prime (by assumption)

and we also see that $2^{n-1}$ and $2^n - 1$ are coprime. Using the fact that $\sigma$ is multiplicative we have:

$$\sigma(N) = \sigma(2^{n-1})\sigma(2^n - 1) = (2^n - 1)(2^n) = 2[(2^{n-1})(2^n - 1)] = 2N.$$

□

Thus far, we have shown that any number of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime, is perfect. What about the converse? Is every even perfect number of this form? A natural question, but one that was only first recorded a millennium later by Ibn al-Haytham c. 1000 AD [12], an Arab mathematician who conjectured that all even perfect numbers are of this form, but was unable to prove his statement rigorously.

Then in the 18th century (2000 years after Euclid!) Euler proved that every even perfect number can indeed be written in the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. Before seeing this proof, we first present the following lemma.

**Lemma 5.** *If $2^n - 1$ is prime, then $n$ is prime.*

*Proof.* [18, p. 4]. Recall the formula $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1)$, a rearrangement of the formula from Lemma 2. Suppose $2^n - 1$ is prime but that $n$ is not prime, that is to say there exists $a$ and $b$ with $a, b > 1$ such that $n = ab$. Then

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

which says that $2^n - 1$ is divisible by $2^a - 1$, a contradiction, since $2^a - 1 \neq 1$ (because $a \neq 1$) but $2^n - 1$ is prime. □

The converse to this lemma however, is false: $2^{11} - 1 = 2047 = 23 \cdot 89$. This seemingly simple factorisation, that had eluded mathematicians for centuries, was first found by Hudalrichus Regius in 1536 [13].

We are now in a position to state the following famous theorem for which many proofs exist, and the reader may wish to explore a slightly shorter proof in [3, pp. 220–221]. Here, we will follow Euler's own proof.

**Theorem 6.** *(Euler) Every even perfect number $N$ can be written in the form $N = 2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime.*

*Proof.* [18, p. 5]. We start by letting $N = 2^{n-1}m$ be a perfect number for some odd $m$. Our goal is to show that $m = 2^n - 1$ and that it is prime. Since $m$ is odd, $m$ and $2^{n-1}$ are coprime, so

$$\sigma(N) = \sigma(2^{n-1}m) = \sigma(2^{n-1})\sigma(m) = \frac{2^n - 1}{2 - 1}\sigma(m) = (2^n - 1)\sigma(m). \quad (\star)$$

We also know that $N$ is perfect, so $\sigma(N) = 2N = 2(2^{n-1}m) = 2^n m$, and then equating this with $(\star)$ gives

$$m = \frac{(2^n - 1)\sigma(m)}{2^n}. \qquad (*)$$

Clearly, $2^n \nmid 2^n - 1$, and so because $m$ is a whole number we must have $2^n \mid \sigma(m)$; that is to say that there exists some $q$ such that $\sigma(m) = 2^n q$. Substituting this into $(*)$ gives $m = (2^n - 1)q$.

If $q = 1$ then $m = 2^n - 1$ and it remains to show that $m$ is prime. Since $\sigma(m) = 2^n$ when $q = 1$, we have $\sigma(m) = m + 1$ and so $m$ is indeed prime.

Now, suppose instead that $q > 1$. Clearly, $1$ , $q$ , $2^n - 1$, and $(2^n - 1)q$ are all divisors of $m$ and so

$$\sigma(m) \geqslant 1 + q + (2^n - 1) + (2^n - 1)q = q + 2^n + 2^n q - q = 2^n(q + 1),$$

which then yields the following strict inequality:

$$\frac{m}{\sigma(m)} \leqslant \frac{(2^n - 1)q}{2^n(q + 1)} = \left(\frac{2^n - 1}{2^n}\right)\left(\frac{q}{q + 1}\right) < \frac{2^n - 1}{2^n}.$$

However, this contradicts the equality achieved in $(*)$ meaning that $q \not> 1$, that is $q = 1$, and so $N = 2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. □

Throughout this section, the importance of the prime number $2^n - 1$ is evident. This is no coincidence, and in fact, numbers of this form are called *Mersenne primes*. Even perfect numbers and Mersenne primes are closely linked since the search for even perfect numbers comes down to a search for Mersenne primes. More information about Mersenne primes can be found in [3, § 10.2] for example.

Now that we have had a look at even perfect numbers, we are in a position to explore their (possibly non-existent!) brothers, the odd perfect numbers, usually abbreviated to OPNs. However, before we enter this dangerous mathematical territory of the unknown, let us take a moment to appreciate the beauty of perfect numbers (the even ones at least) and look at some of their amazing properties.

## 4 Interesting Properties of Even Perfect Numbers

Perfect numbers exhibit some truly magnificent properties, most of which are very surprising at first. However, now that we have examined the structure of even perfect numbers in detail, we can understand the underlying mathematical structure of these properties.

Our first remark is that every perfect number can be written as the sum of consecutive integers, that is to say a triangle number. Of course, the converse is not true. Otherwise this essay would be rather short!

**Proposition 7.** *Every even perfect number is a triangle number.*

*Proof.* [18, p. 7]. Note that any triangle number $T$ is of the form $T = k(k-1)/2$. Let $N$ be an even perfect number. Then $N = 2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. We can rewrite this as

$$N = \frac{1}{2}2^n(2^n - 1)$$

and then simply setting $2^n = k$ gives the desired result. □

Our next result would make even our good friend Nicomachus proud.

**Proposition 8.** *Every even perfect number $N$ ends in a 6 or 28; that is*

$$N \equiv 6 \pmod{10} \qquad \text{or} \qquad N \equiv 28 \pmod{100}.$$

*Proof.* Similar to [3, pp. 222–223]. Again, we let $N$ be an even perfect number, and so $N = 2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime, and then by Lemma 5 we know that $n$ is prime. We split the proof into four cases:

*Case* 1. $n = 2$. We simply have $N = 2^{2-1}(2^2 - 1) = 2 \cdot 3 = 6$.

*Case* 2. $n = 3$. We simply have $N = 2^{3-1}(2^3 - 1) = 4 \cdot 7 = 28$.

*Case* 3. $n = 4m + 1$ for some $m \geqslant 1$. We then have

$$N = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m \equiv 2 \cdot 6^{2m} - 6^m \pmod{10},$$

and since by induction $6^m \equiv 6 \pmod{10}$ for all $m \geqslant 1$, we have that

$$N \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}.$$

*Case* 4. $n = 4m + 3$ for some $m \geqslant 1$. We first see that

$$2^{n-1} = 2^{4m+2} = 16^m \cdot 4 \equiv 6 \cdot 4 \equiv 4 \pmod{10},$$

and so the last digit of $2^{n-1}$ is a 4.

We also note that $4 \mid 2^{n-1}$ for $n > 2$, and so 4 must divide the number formed by the last two digits of $2^{n-1}$. These two conditions leave us with the following possibilities:

$$2^{n-1} \equiv 4, 24, 44, 64, \text{ or } 84 \pmod{100}.$$

This then gives us information about $2^n - 1$, the other part of $N$, since we can rewrite $2^n - 1$ as follows:

$$2^n - 1 = 2\left(2^{n-1}\right) - 1 \equiv 7, 47, 87, 27, \text{ or } 67 \pmod{100},$$

and so we have that

$$N = 2^{n-1}(2^n - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27, \text{ or } 84 \cdot 67 \pmod{100},$$

at which point it is easy to check that each of these products is congruent to $28 \pmod{100}$. For example: $44 \cdot 87 = 3828 \equiv 28 \pmod{100}$. □

*Remark.* Both the fifth and sixth perfect numbers end in the digit 6 [16, p. 129], disproving Nicomachus' third conjecture.

Finally, we come to what is perhaps the most surprising result of this section concerning the *digital root* of a number. This quantity is obtained by adding together the digits of a number again and again, until you end up with a single digit. For example, the digital root of 1352 is 2 because $1+3+5+2=11$ and $1+1=2$. The digital root of a number is also often referred to as the *iterative sum of the digits of a number*, which is perhaps a more instructive name, but certainly a lot less catchy. The following result is accredited to Wantzel [4, p. 20].

**Proposition 9.** *The digital root of every even perfect number other than* 6 *is* 1.

*Proof.* Adapted from [18, p. 8]. The trick in this proof is to simply view the digital root of a number as its congruence modulo 9, with the slight catch that if a number is divisible by 9 (and does not equal 0), then we set the digital root to be 9 rather than 0. The reason why this works is as follows: let $M = d_k \dots d_2 d_1 d_0$, where the $d_i$ are the digits of $M$ for $1 \leqslant i \leqslant k$. Then we have that

$$M = \sum_{i=0}^{k} d_i 10^i \equiv \sum_{i=0}^{k} d_i \pmod 9.$$

So $M$ is congruent to the sum of its digits modulo 9. Simply iterating this process gives the desired result due to the transitivity of congruence.

We have now reduced the problem to showing that if $N$ is an even perfect number, other than 6, then $N \equiv 1 \pmod 9$. As usual, we let $N = 2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. We know that $n$ is prime by Lemma 5, and that $n \neq 2$ as we are excluding $N = 6$. For $n = 3$, we get $N = 28 \equiv 1 \pmod 9$. For $n > 3$, we see that $3 \nmid n$, by the primality of $n$, and so we are left with two cases:

*Case* 1. $n = 3k+1$ for some $k \geqslant 1$. Since $n$ is odd, $k$ must be even. Setting $k = 2m$ gives $n = 6m+1$ for some $m \geqslant 1$, and so

$$N = 2^{6m}(2^{6m+1} - 1) = 64^m(2 \cdot 64^m - 1) \equiv 1(2-1) \equiv 1 \pmod 9.$$

*Case* 2. $n = 3k+2$ for some $k \geqslant 1$. Since $n$ is odd, $k$ must be odd too. Setting $k = 2m-1$ gives $n = 6m-1$ for some $m \geqslant 1$, and we have

$$N = 2^{6m-2}(2^{6m-1} - 1) = \left(16 \cdot 64^{m-1}\right)\left(32 \cdot 64^{m-1} - 1\right) \equiv 7(5-1) \equiv 1 \pmod 9.$$

□

With this, we have reached the end of our whistle-stop tour of these curious properties; not because we have covered them all, but because it is now time to move away from even perfect numbers and on to greater things

(well, greater by one to be precise, or maybe smaller by one, depending on your point of view), namely the odd perfect numbers. The reader is invited to find out more about even perfect numbers and their properties by looking at [18].

# 5 Odd Perfect Numbers

## 5.1 The Form of an Odd Perfect Number

The study of OPNs (odd perfect numbers) is rather intriguing, since they may well not exist, and one might wonder how to study something whose existence is uncertain. The answer lies in finding conditions that an odd perfect number would have to satisfy if it were to exist. There are now a huge number of restrictions that have been found on OPNs (and are still being found), and in this section we will discover some of the more (relatively) elementary ones. Of course, finding these conditions neither proves nor disproves our age–old question, but it gives us a flavour of how rare OPNs are if they do exist.

We start with the first known result proven about OPNs by none other than one of our heroes from Section 3: Leonhard Euler.

**Theorem 10.** *(Euler) If $N$ is an OPN, then*

$$N = p_1^{\alpha} p_2^{2\beta_2} \dots p_r^{2\beta_r},$$

*where the $p_i$ are distinct odd primes and $p_1 \equiv \alpha \equiv 1 \pmod 4$.*

*Proof.* Adapted from [6, pp. 32–33]. Let $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorisation of $N$. Firstly, all of the $p_i$ must be odd because $N$ is odd. Next, $N$ is perfect, so

$$2N = \sigma(N) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}),$$

and furthermore, because $N$ is odd, $N \equiv 1 \pmod 4$ or $N \equiv 3 \pmod 4$. Either way, $2N = \sigma(N) \equiv 2 \pmod 4$ meaning that $\sigma(N)$ is divisible by 2, but not divisible by 4, and so exactly one of the $\sigma(p_i^{k_i})$ must be divisible by 2 (but not divisible by 4). Let us set this to be $\sigma(p_1^{k_1})$, and so all of the other $\sigma(p_i^{k_i})$ must be odd.

Then consider $\sigma(p_i^{k_i}) = 1 + p_i + \cdots + p_i^{k_i}$ for some $i$ with $2 \leqslant i \leqslant r$. This is an odd number which is the sum of $k_i + 1$ odd terms, meaning that $k_i$ must be even for $2 \leqslant i \leqslant r$, since then $k_i + 1$ is odd, and the sum of an odd number of odd terms is indeed odd. So we can set $k_1 = \alpha$ and the other $k_i = 2\beta_i$, giving $N = p_1^{\alpha} p_2^{2\beta_2} \dots p_r^{2\beta_r}$.

We must now show that $p_1 \equiv \alpha \equiv 1 \pmod 4$. Since $p_1$ is odd, $\alpha$ must be odd. This is because $\sigma(p_1^{\alpha}) = 1 + p_1 + \cdots + p_1^{\alpha}$ is even, which is true

only if $\alpha$ is odd, as otherwise we would be summing an odd number of odd terms. Now, either $p_1 \equiv 1 \pmod 4$ or $p_1 \equiv 3 \equiv -1 \pmod 4$. If $p_1 \equiv -1 \pmod 4$, since $\alpha$ is odd,

$$\sigma(p_1^\alpha) = 1 + p_1 + \cdots + p_1^{\alpha-1} + p_1^\alpha \equiv 1 + (-1) + \cdots + 1 + (-1)^\alpha \equiv 0 \pmod 4,$$

which is a contradiction because $\sigma(p_1^\alpha)$ is not divisible by 4, and so $p_1 \equiv 1 \pmod 4$. Now we have that

$$\sigma(p_1^\alpha) = 1 + p_1 + \cdots + p_1^{\alpha-1} + p_1^\alpha \equiv 1 + 1 + \cdots + 1 + 1 \equiv \alpha + 1 \pmod 4,$$

meaning that if $\alpha \equiv -1 \pmod 4$, we would have a contradiction again, as this would imply that $\sigma(p_1^\alpha) \equiv 0 \pmod 4$, and so we are left with (since $\alpha$ is odd), $\alpha \equiv 1 \pmod 4$ thus completing the proof.

□

This theorem can in fact be proven rather quickly using an idea from the later section on Touchard's Theorem, but here we have followed Euler's original proof. From this theorem we obtain the following important result:

**Corollary 10.1.** *If $N$ is an OPN, then*

$$N = p^\alpha m^2,$$

*where $p$ is a prime number, $p \nmid m$, and $p \equiv \alpha \equiv 1 \pmod 4$; in particular, $N \equiv 1 \pmod 4$.*

*Proof.* [3, p. 232]. From the theorem we just proved, we can write

$$N = p_1^\alpha (p_2^{\beta_2} \ldots p_r^{\beta_r})^2 = p^\alpha m^2,$$

where we have rewritten $p_1$ as $p$. We already know that $p$ is a prime number, $p \nmid m$, and $p \equiv \alpha \equiv 1 \pmod 4$. It remains to show that $N \equiv 1 \pmod 4$. Note that $m$ is odd, so $m \equiv 1$ or $3 \pmod 4$; either way, $m^2 \equiv 1 \pmod 4$ and so $N \equiv 1 \cdot 1 \equiv 1 \pmod 4$.

□

## 5.2 Prime Factors

One way of finding conditions on OPNs is by looking at their prime factors. Sylvester famously proved in 1888 that an OPN must have at least four distinct prime factors in [9], and in the same year he increased this lower bound to five. In fact, we now know that an OPN can have no fewer than nine distinct prime factors due to Nielsen, in a paper published in 2007 [10]. In this section we prove a much more modest lower bound: an OPN has at least three distinct prime factors.

**Definition 5.1.** The number of distinct prime factors of a number $n$ is $\omega(n)$.

For example, $\omega(60) = 3$ because $60 = 2^2 \cdot 3 \cdot 5$. To find a lower bound on $\omega(n)$ we will use what is known as the *abundancy index* of a number, a simple concept that is currently leading modern research in this area.

**Definition 5.2.** The *abundancy index* of a number $n$ is given by the quotient

$$\frac{\sigma(n)}{n}.$$

Of course, $N$ is perfect if and only if its abundancy index is two. For a prime power, we obtain the following useful inequality from [6, p. 27] for which we provide our own proof:

**Lemma 11.** *[6, p. 27]. Let $p$ be a prime. Then*

$$\frac{\sigma(p^\alpha)}{p^\alpha} < \frac{p}{p-1}.$$

*Proof.* From Proposition 3, we know that

$$\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1} < \frac{p^{\alpha+1}}{p-1},$$

and then dividing both sides of the inequality by $p^\alpha$ gives the desired result. □

We now need one more result before proving our main theorem of this section.

**Lemma 12.** *Let $N$ be a perfect number (odd or even) with prime factorisation $N = \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}$, then*

$$2 < \prod_{i=1}^{\omega(N)} \frac{p_i}{p_i - 1} = \prod_{i=1}^{\omega(N)} \left(1 + \frac{1}{p_i - 1}\right).$$

*Proof.* [6, p. 36]. Since $N$ is perfect, $\frac{\sigma(N)}{N} = 2$. The inequality simply follows by applying Lemma 11 to each prime power in $N$'s prime factorisation. □

Our main result is now a fairly straightforward consequence of these two lemmas.

**Theorem 13.** *If $N$ is an OPN, then $\omega(N) \geqslant 3$.*

*Proof.* Adapted from [6, p. 37]. It is clear that $\omega(N) \neq 1$ since prime powers are deficient. Suppose $\omega(N) = 2$, so $N = p^\alpha q^\beta$ where $p$ and $q$ are prime numbers. Since $N$ is odd, neither $p$ nor $q$ equals two, and so (without any loss of generality) we can say that $p \geqslant 3$ and $q \geqslant 5$ since $p$ and $q$ are distinct. Then by our previous lemma,

$$2 < \left(1 + \frac{1}{p-1}\right)\left(1 + \frac{1}{q-1}\right) \leqslant \left(1 + \frac{1}{3-1}\right)\left(1 + \frac{1}{5-1}\right) = \frac{15}{8},$$

which is a clear contradiction since $2 > 15/8$, and so $\omega(N) \neq 2$ meaning that $\omega(N) \geqslant 3$ as required. □

The proof for $\omega(N) \geqslant 4$ uses the same idea as the proof above, but splits into several cases and is somewhat messy. It can be found in [6, pp. 38–40].

### 5.3 Congruence Conditions: Touchard's Theorem

In this section we prove a classic theorem on odd perfect numbers, proved by Jacques Touchard in 1953, which places rather strict conditions on the existence of an OPN. Touchard's original proof uses a complicated recurrence relation derived from a nonlinear partial differential equation [17]. We follow Holdener's proof from [8] instead. First we present the following proposition:

**Proposition 14.** *If $N$ is of the form $6k - 1$ then $N$ is not perfect.*

The main idea in this proof is to express $\sigma(N)$ as a sum of *divisor pairs*. For a number $m$, a divisor pair is any divisor $d$ (of $m$) and $m/d$. For example, 2 and 5 make up a divisor pair of 10. The important point to note is that unless $m$ is a square number, $\sigma(m)$ is the sum of all of $m$'s divisor pairs. If $m$ is a square number, however, then this is not true, since $\sqrt{m}$ would be counted twice in the sum of divisor pairs.

*Proof.* [8]. Assume $N = 6k - 1$ is perfect for some $k$. We have that $N \equiv -1 \pmod 3$ and so $N$ cannot be a square number since all square numbers are congruent to 0 or 1 modulo 3 (this is easy to see, since in $\mathbb{Z}_3$, $0^2 = 0, 1^2 = 1$, and $2^2 = 1$). Now, for any divisor $d$ of $N$, $N = (N/d) \cdot d \equiv -1 \pmod 3$ and so either $N/d \equiv 1 \pmod 3$ and $d \equiv -1 \pmod 3$ or $N/d \equiv -1 \pmod 3$ and $d \equiv 1 \pmod 3$. In both cases, $d + N/d \equiv 0 \pmod 3$, so

$$\sigma(N) = \sum_{d|N, d<\sqrt{N}} d + \frac{N}{d} \equiv 0 \pmod 3,$$

but this contradicts the fact that $\sigma(N) = 2N = 2(6k - 1) \equiv 1 \pmod 3$ and so $N$ is not perfect. □

**Theorem 15.** *(Touchard) If $N$ is an OPN, then $N$ is of the form $12m + 1$ or $36m + 9$.*

*Proof.* [8]. Let $N$ be an OPN. By the previous proposition, $N \not\equiv -1 \pmod 6$, and then using the fact that $N \equiv 1 \pmod 4$ (see section 5.1) we form two sets of simultaneous equations:

*Case* 1. $N = 6s + 1$ for some $s$ and $N = 4t + 1$ for some $t$. We have $6s + 1 = 4t + 1$ and so rearranging this equation gives $s = \frac{2t}{3}$, and since $s$ is a whole number, we must have $t = 3m$ for some $m$. Substituting this into the second equation gives $N = 12m + 1$.

*Case* 2. $N = 6s + 3$ for some $s$ and $N = 4t + 1$ for some $t$. We have $6s + 3 = 4t + 1$ and so rearranging this equation gives $t = \frac{3s}{2} + \frac{1}{2}$ which means that $s$ must be odd for $t$ to be a whole number; that is $s = 2m + 1$ for some $m$, which gives $N = 6(2m + 1) + 3 = 12m + 9$.

Currently we have that $N$ is of the form $12m + 1$ or $12m + 9$, which is not quite what we are trying to show. To continue, suppose $N = 12m + 9$ is perfect and that $3 \nmid m$. Then

$$\sigma(N) = \sigma(12m + 9) = \sigma(3(4m + 3)) = \sigma(3)\sigma(4m + 3) = 4\sigma(4m + 3),$$

where we have used the fact that 3 and $4m + 3$ must be coprime because $3 \nmid m$, and so we then see that $\sigma(N) \equiv 0 \pmod 4$. However, $N$ is perfect, so

$$\sigma(N) = 2N = 2(12m + 9) \equiv 2 \pmod 4,$$

which is a contradiction, and so we must have that $3 \mid m$, meaning that $m = 3k$ for some $k$, and so $N$ is of the form $12(3k) + 9 = 36k + 9$ as desired. □

# 6 Conclusion and a Look to the Future

We have reached the end of our journey and it is important to take a look at what we have seen, and what there still is to see. We have given a classification of even perfect numbers, investigated some of their properties and looked at odd perfect numbers in some detail. *What else is there to do?* Well, for even perfect numbers, probably not a great deal more. The *Great Internet Mersenne Prime Search*,[1] or GIMPS, uses the power of over a million computers to search for Mersenne primes (and anyone can help!). At the time of writing, we know of forty–nine Mersenne primes, and therefore of forty–nine even perfect numbers, the most recent one having been discovered on the 7th of January 2016, and this perfect number has an incredible $44,677,235$ digits!

As for odd perfect numbers, in 1888 Sylvester wrote that " ... a prolonged meditation on the subject has satisfied me that the existence of [an odd perfect number] — its escape, so to say, from the complex web of conditions

[1] `http://www.mersenne.org/`

which hem it in on all sides — would be little short of a miracle." [9, p. 6]. We currently know that if an OPN exists then it is of Euler's form, has at least nine distinct prime factors [10], is greater than $10^{1500}$ [11], and must satisfy a myriad of other highly restrictive conditions.

As was briefly mentioned in Section 5.2, current research is using the idea of the abundancy index of a number, as well as the concept of *abundancy outlaws* to find ever increasingly strict conditions on the existence of an OPN. Furthermore, modern research is using an idea of *factor chains* to find bounds, both upper and lower, on the size of the prime factors of OPNs [6, § 4]. Research does suggest that no odd perfect numbers exist, but of course, mathematicians will never be satisfied with such a statement, and so the search goes on.

## References


[1] A. Bennett and P. Denson. Visualizing the geometric series. *The Mathematics Teacher*, 82(2):130–136, 1989.

[2] J. Bezuszka and M. Kenney. Even perfect numbers:(update) 2. *The Mathematics Teacher*, 90(8):628–633, 1997.

[3] D. Burton. *Elementary Number Theory.* Allyn and Bacon, 1st edition, 1980.

[4] L. Dickson. *History of the Theory of Numbers*, volume 1. Washington, Carnegie Institution of Washington, 1919.

[5] F. Robbins, M. d'Ooge and L. Karpinski. *Nicomachus of Gerasa: Introduction to Arithmetic.* New York, The Macmillan Company, 1926.

[6] J. Dris. Solving the odd perfect number problem: some old and new approaches. *arXiv preprint arXiv:1204.1450*, 2012.

[7] R. Fitzpatrick. *Euclid's Elements of Geometry.* 2nd edition, 2008.

[8] J. Holdener. A theorem of Touchard on the form of odd perfect numbers. *The American Mathematical Monthly*, 109(7):661–663, 2002.

[9] S. Gimbel, J.Gimbel and J. Jaroma. Sylvester: ushering in the modern era of research on odd perfect numbers. *Integers: Electronic Journal of Combinatorial Number Theory*, 3(A16):2, 2003.

[10] P. Nielsen. Odd perfect numbers have at least nine distinct prime factors. *Mathematics of Computation*, 76(260):2109–2126, 2007.

[11] P. Ochem and M. Rao. Odd perfect numbers are greater than $10^{1500}$. *Mathematics of Computation*, 81(279):1869–1877, 2012.

[12] J. O'Connor and E. Robertson. Abu Ali al-hasan ibn al-Haytham. `http://www-history.mcs.st-andrews.ac.uk/Biographies/Al-Haytham.html`, University of St Andrews, November 1999. Accessed: 2016-12-16.

[13] J. O'Connor and E. Robertson. Perfect numbers. `http://www-history.mcs.st-andrews.ac.uk/HistTopics/Perfect_numbers.html`, University of St Andrews, May 2009. Accessed: 2016-12-16.

[14] E. Picutti. Pour l'histoire des sept premiers nombres parfaits. *Historia mathematica*, 16(2):123–136, 1989.

[15] C. Smyth. Maths 4 number theory notes. *University of Edinburgh*, 2012.

[16] J. Tattersall. *Elementary Number Theory in Nine Chapters*. Cambridge University Press, 1999.

[17] J. Touchard. On prime numbers and perfect numbers. *Scripta Math*, 19(1953):35–39, 1953.

[18] J. Voight. Perfect numbers: an elementary introduction. *University of California, Berkeley*, 1998.