The Perfect Numbers

Tseliso Paul Lekhoaela (tseliso@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Prof Florian Breuer
Stellenbosch University, South Africa

22 May 2014
Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

Abstract

The most interesting object in this essay would be the problem of odd perfect numbers, but some discussions based on the results of even perfect numbers which are well understood and are in bijection with the Mersenne primes will be included. Are there any odd perfect numbers? The answer to this question is still unknown, but it is known that odd perfect numbers, if they exist, would have to satisfy a number of unlikely properties. Some of those unlikely properties are: (i) An odd perfect numbers must have at least four distinct prime factors. (ii) The lower bounds of the distinct prime factors of an odd perfect numbers must exceed 10^7 (iii) An odd perfect numbers must be greater than 10^{300}.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Tseliso Paul Lekhoaela, 22 May 2014

Contents

1. Introduction

One of the oldest problems which is still unsolved in number theory is to determine whether odd perfect numbers (OPN) exist. It is not known when the first general studies of perfect numbers took place. Perhaps they could have been the earliest times when people began to be interested in the properties of integers. Like Pythagoras and his followers who examined perfect numbers not specifically on the number theoretic properties, but more for their mystical properties.

A positive integer N is called a perfect number if it is equal to the sum of its proper divisors. The smallest known perfect number is 6, since 6=1+2+3 and the second is 28 because 28=1+2+4+7+14. In earlier times, a definition of perfect numbers was provided in terms of aliquot parts of the number. Aliquot parts of a number are the proper quotients of that number. For example, 1, 2 and 4 are aliquot parts of 8. The first four perfect numbers that were discovered in ancient times are 6, 28, 496, 8128, and around 300BC in Euclid's Elements, the first attempt dealing with perfect numbers was thoroughly understood and recorded.

In 100AD, Nicomachus of Gerasa in a significant investigation of perfect numbers observed some necessary results which he provided without any evidence for their truth. Thus, they are listed below as follows:

- All perfect numbers are even.
- All perfect numbers terminate with a number 6 or 8 alternatively.
- The n^{th} perfect number is composed of n digits.
- There exist infinitely many perfect numbers.
- Every perfect number is in the form $2^{p-1}(2^p - 1)$, for some $p > 1$, where $2^p - 1$ is prime. This result was later proved and shown that p must be prime.

In 1461 and 1555, the fifth and sixth perfect numbers were respectively obtained. The sixth was discovered unexpectedly by J. Scheyble. Moreover, around 1640, Fermat came up with a good idea from his little theorem which states that, "If a is not divisible by a prime p, then $a^{p-1} - 1$ is divisible by p". This little theorem was the source for Fermat to examine systematically the outstanding problem of the perfect numbers.

Mersenne was highly attracted and motivated by the results he received from Fermat about the perfect numbers and soon formulated an important declaration that if $2^n - 1$ is prime , then $2^{n-1}(2^n - 1)$ is an even perfect number. It is known that all prime numbers of the form $2^n - 1$ are Mersenne primes. In 1732, Euler showed that the eighth perfect number is $2^{30}(2^{31} - 1)$ and he further showed that every even perfect numbers should have the form $2^{p-1}(2^p - 1)$, which in turn leads to the fact that the search for even perfect number is equivalent to the search for Mersenne primes. Hence, even perfect numbers are bijective with Mersenne primes and recently by the use of computers, 39 even perfect numbers have been discovered. The last even perfect number which was calculated in 1911 by hand is $2^{88}(2^{89} - 1)$.

In spite of some interesting contributions that have been made on the even perfect numbers, there are also great attempts considered in proving that an OPN might not exist. In 1888, Sylvester showed that an OPN should have a minimum of four distinct prime factors and it is known that if OPN exists it must be greater than 10^{300} with its largest component (which means divisor p^a with prime p) bigger than 10^{62}. Furthermore, it has been proved that an OPN must have 101 prime factors without necessarily considering distinct prime factors only. In the next section, we would describe some crucial definitions and provide the proof of theorems that will enable us to justify some necessary conditions on the existence or non-existence of an OPN.

1.1 Preliminaries

Definition 1.1.1. An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$. A function f is called multiplicative if it is not identically zero with $f(ab) = f(a)f(b)$, where a and b are relatively prime. Moreover, if $f(ab) = f(a)f(b)$ for all positive integers a and b, then f is called a completely multiplicative function.
Proposition 1.1.2. Let f be multiplicative function, then f(1) $= 1$.

Proof. Suppose that f is multiplicative function. For any positive integer n, $n = 1 \cdot n$. Since f is not identically zero, for some n, $f(n) \neq 0$. For that n,

$$f(n) = f(1 \cdot n) = f(1)f(n), \quad \text{where} \quad \gcd(n, 1) = 1.$$

Therefore, $f(1) = 1$. □

Let f be a multiplicative arithmetic function and take a positive integer n written uniquely as a product of its prime factors as follows,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where $p_1, p_2, \ldots, p_r$ are distinct prime numbers and $\alpha_1, \alpha_2, \ldots, \alpha_r$ are non-negative integers. It can easily be seen that $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ iff $i \neq j$. Then we have,

$$\begin{aligned} f(n) &= f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ &= f(p_1^{\alpha_1}) f(p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ &= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) f(p_3^{\alpha_3} \cdots p_r^{\alpha_r}) \\ &\ \ \vdots \\ &= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) f(p_3^{\alpha_3}) \cdots f(p_r^{\alpha_r}). \end{aligned}$$

Particularly, a multiplicative arithmetic function is totally determined by its values at the exponents of the primes which permits us to get more compact formulas for multiplicative arithmetic functions.
Theorem 1.1.3. *Suppose that f is an arithmetic function for positive integers n and*

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

If f is multiplicative, then F is multiplicative too.

Proof. Take two positive integers m, n where $gcd(m, n) = 1$. To prove that F is multiplicative, we need to demonstrate that $F(mn) = F(m)F(n)$. By using the definition we get,

$$F(m)F(n) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2).$$

Since $gcd(m, n) = 1$ and if d_1 divides m, d_2 divides n, it follows that $gcd(d_1, d_2) = 1$. Since f is multiplicative,

$$f(d_1)f(d_2) = f(d_1 d_2).$$

Then, it follows that

$$F(m)F(n) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2).$$

Take $d = d_1 d_2$. Since $d_1|m$ and $d_2|n$ and $gcd(m, n) = 1$, $gcd(d_1, d_2) = 1$, then $d = d_1 d_2|mn$.

$$F(m)F(n) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{d|mn} f(d) = F(mn)$$

Hence, F is multiplicative. □

1.2 Divisors and Sum of Divisors

Definition 1.2.1. A sum of positive divisors function $\sigma_\alpha(n)$, is defined as

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

where $\alpha \in \mathbb{C}$.

There are some special cases that can be deduced from Definition 1.2.1, that is, when $\alpha = 1$ and $\alpha = 0$, we get the following:

$$\sigma_1(n) = \sum_{d|n} d^1 = \sigma(n) \qquad \text{and} \qquad \sigma_0(n) = \sum_{d|n} d^0 = \tau(n)$$

where

- $\sigma(n)$ is a function defined as a sum of positive divisors of an integer n with 1 and n inclusive.
- $\tau(n)$ is a function which counts the number of distinct divisors of an integer n.

For instance,
Example 1.2.2. Let $n = 10$. Its positive divisors are $1, 2, 5, 10$, so by definition:

$$\tau(10) = \sigma_0(10) = \sum_{d|10} d^0 = 1 + 1 + 1 + 1 = 4$$

and

$$\sigma(10) = \sigma_1(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18$$

Lemma 1.2.3. $\tau(n)$ and $\sigma(n)$ are multiplicative functions.

Proof. The constant function, $f(n) = 1$ is multiplicative, $\forall\, n \in \mathbb{N}$. So now

$$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} f(d).$$

Hence, from Theorem 1.1.3, it follows that $\tau(n)$ is multiplicative.

On the other hand, it is known that an identity function, $f(d) = d$ is completely multiplicative thus,

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

Therefore, $\sigma(n)$ is a multiplicative function. □

Utilizing Lemma 1.2.3 we can derive formulas for $\tau(n)$ and $\sigma(n)$. Let p be prime. Then the positive divisors of p^a are $1,\ p,\ p^2,\ \cdots,\ p^a$, thus just using the method of inspection we get,

$$\tau(p^a) = 1 + a.$$

By the way, to derive the formula for σ we will use the finite geometric series formula,

$$\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} = \frac{p^{(1+a)\alpha} - 1}{p^\alpha - 1}.$$

Hence this formulas motivates the proof of the following theorem.

Theorem 1.2.4. *Suppose that a prime factorization of an integer n is given as*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Then

$$\tau(n) = \prod_{i=1}^{r} (1 + a_i)$$

and

$$\sigma_\alpha(n) = \prod_{i=1}^{r} \left(\frac{p_i^{(1+a_i)\alpha} - 1}{p_i^\alpha - 1} \right).$$

Proof. Since τ is multiplicative, from Lemma 1.2.3 and the little motivation created above,

$$\begin{aligned}
\tau(n) &= \tau(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \\
&= \tau(p_1^{a_1})\tau(p_2^{a_2}) \cdots \tau(p_r^{a_r}) \\
&= (1 + a_1)(1 + a_2) \cdots (1 + a_r) \\
&= \prod_{i=1}^{r} (1 + a_i).
\end{aligned}$$

Hence, it is shown that $\tau(n) = \prod_{i=1}^{r}(1 + a_i)$. Similarly σ_α is a multiplicative function, so from Lemma 1.2.3 and small motivation above,

$$\begin{aligned}
\sigma_\alpha(n) &= \sigma_\alpha(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \\
&= \sigma_\alpha(p_1^{a_1})\sigma_\alpha(p_2^{a_2}) \cdots \sigma_\alpha(p_r^{a_r}) \\
&= \left(\frac{p_1^{(1+a_1)\sigma} - 1}{p_1^{\alpha} - 1}\right)\left(\frac{p_2^{(1+a_2)\sigma} - 1}{p_2^{\alpha} - 1}\right) \cdots \left(\frac{p_r^{(1+a_r)\sigma} - 1}{p_r^{\alpha} - 1}\right) \\
&= \prod_{i=1}^{r}\left(\frac{p_i^{(1+a_i)\alpha} - 1}{p_i^{\alpha} - 1}\right).
\end{aligned}$$

□

At this juncture, it is very important to give a bound $\frac{\sigma(n)}{n}$.
Lemma 1.2.5. For every positive integer $n \geq 2$, we have

$$\frac{\sigma(n)}{n} < \prod_{p|n}\left(\frac{p}{p-1}\right)$$

Proof. Let's define the following notation $t^m \parallel r$ if $t^m | r$ but $t^{m+1} \nmid r$. so now,

$$\begin{aligned}
\frac{n}{\sigma(n)} &= \prod_{p^m \| n} \frac{p^m}{\sigma(p^m)} = \prod_{p^m \| n} \frac{p^m}{\frac{p^{m+1}-1}{p-1}} \\
&= \prod_{p^m \| n} \frac{p^m(p-1)}{p^{m+1} - 1} = \prod_{p^m \| n} \frac{p^{m+1}(1 - \frac{1}{p})}{p^{m+1}(1 - \frac{1}{p^{m+1}})} \\
&= \prod_{p^m \| n} \frac{(1 - \frac{1}{p})}{(1 - \frac{1}{p^{m+1}})} \\
&> \prod_{p^m \| n}\left(1 - \frac{1}{p}\right) = \prod_{p|n}\left(1 - \frac{1}{p}\right).
\end{aligned}$$

Hence, it is proved that

$$\frac{\sigma(n)}{n} < \prod_{p|n}\left(\frac{p}{p-1}\right).$$

□

Lastly, consider a definition of Euler phi function.
Definition 1.2.6. $\phi(n)$ is the number of positive integers less than n that are relatively prime to n.

Let's give an example for illustration.
Example 1.2.7. $\phi(4) = \#\{1, 3\} = 2$. But in fact, knowing a little more about ϕ, we can observe that

$$\phi(4) = \phi(2^2) = (2-1)(2^{(2-1)}) = 2.$$

If p is prime, then $\phi(p) = p - 1$ because all of the following numbers $1,\ 2,\ \ldots,\ p-1$ are relatively prime to p.

2. Perfect Numbers

2.1 Even Perfect Numbers

The problem of the perfect numbers was first examined by the great Greek mathematician Euclid over 2000 years ago. He was the first to group perfect numbers and he observed that the first four perfect numbers are of the form;

$$\begin{aligned}
6 &= 2(1+2) = 2 \cdot 3 \\
28 &= 2^2(1+2+2^2) = 4 \cdot 7 \\
496 &= 2^4(1+2+2^2+2^3+2^4) = 16 \cdot 31 \\
8128 &= 2^6(1+2+2^2+2^3+2^4+2^5+2^6) = 64 \cdot 127.
\end{aligned}$$

From four perfect numbers mentioned above, it was discovered that a general form of even perfect numbers would be $2^{p-1}(2^p-1)$ and this will be proved later in this section.

Definition 2.1.1. A positive integer N is called a perfect number if it is equal to the sum of its positive divisors excluding itself. That is,

$$\sigma(N) = 2N.$$

Theorem 2.1.2. (Euclid) *Let n be an integer ≥ 2 with $2^n - 1$ a prime number, then $N = 2^{n-1}(2^n - 1)$ is a perfect number.*

Proof. Since $2^n - 1$ is prime, it is obvious that the only prime factors of N are 2 and $2^n - 1$. Let $P = 2^n - 1$, so $N = 2^{n-1}P$. To show that N is perfect, we commence by showing that

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

All factors of 2^{n-1} are $1,\ 2,\ \ldots,\ 2^{n-1}$. Adding all of them we get

$$\begin{aligned}
\sigma(2^{n-1}) &= 1 + 2 + 2^2 + \cdots + 2^{n-1} \\
&= \frac{2^n - 1}{2 - 1} \\
&= 2^n - 1.
\end{aligned}$$

This result is just obtained by using the formula of the finite geometric series. Since every prime has two divisors, one and the prime number itself, we get that $\sigma(P) = 1 + P$. It has been shown that σ is multiplicative. Thus,

$$\begin{aligned}
\sigma(N) &= \sigma(2^{n-1}P) \\
&= \sigma(2^{n-1})\sigma(P) \\
&= (2^n - 1)(1 + P) \\
&= (2^n - 1)(1 + 2^n - 1) \\
&= 2^n(2^n - 1) \\
&= 2 \cdot 2^{n-1}(2^n - 1) \\
&= 2N.
\end{aligned}$$

Therefore, N is a perfect number. □

The task of finding an even perfect numbers has also brought a complete control over getting the Mersenne primes. These Mersenne primes are of the form $2^n - 1$ for some positive integer n. There is a lemma below to be proved with the fact that if $2^n - 1$ is prime, then n is not a composite number.

Lemma 2.1.3. (Cataldi-Fermat) Let $2^n - 1$ be prime. Then n is prime.

Proof. Suppose that n is composite number. Then $n = \lambda\beta$ where $\lambda \geq 2$, and $\beta \geq 2$. Thus

$$2^n - 1 = 2^{\lambda\beta} - 1 \tag{2.1.1}$$

By considering the following factorisation

$$x^n - 1 = (x-1)(1 + x + \cdots + x^{n-1})$$

Equation (2.1.1) becomes

$$\begin{aligned} 2^{\lambda\beta} - 1 &= (2^\lambda)^\beta - 1 \\ &= (2^\lambda - 1)(1 + 2^\lambda + \cdots + (2^\lambda)^{\beta-2} + (2^\lambda)^{\beta-1}), \end{aligned}$$

which implies that $2^\lambda - 1$ is the factor of $2^n - 1$. But $2^n - 1$ is a prime, so its only divisors are 1 and itself. Thus, there is a contradiction. Hence, the only way that $2^n - 1$ is prime, could be when $n = p$ being a prime. □

The theorem of Euler justifies a fact that prove to be indispensable that even perfect numbers are bijective with Mersenne Primes.

Theorem 2.1.4. (Euler) *The even perfect numbers are precisely the numbers constructed in the following way,* $2^{p-1}(2^p - 1)$, *where* $2^p - 1$ *is prime.*

Proof. Assume that $N = 2^{p-1}a$ where $p \geq 2$ and $\gcd(2, a) = 1$, which implies that a is odd and it is also relatively prime to 2^{p-1}. Then,

$$\begin{aligned} \sigma(N) &= \sigma(2^{p-1}a) \\ &= \sigma(2^{p-1})\sigma(a) \\ &= (2^p - 1)\sigma(a). \end{aligned}$$

If N is a perfect number, then

$$\begin{aligned} \sigma(N) &= 2N \\ &= 2(2^{p-1}a) \\ &= 2^p a. \end{aligned}$$

Thus,

$$\sigma(N) = (2^p - 1)\sigma(a) = 2^p a. \tag{2.1.2}$$

Since $2^p - 1$ is odd, then $2^p - 1$ divides a and we can write a as

$$a = (2^p - 1)k, \tag{2.1.3}$$

where k is a positive integer. Then substituting Equation (2.1.3) into (2.1.2) we get

$$\begin{aligned}(2^p-1)\sigma(a) &= 2^p(2^p-1)k \\ \Rightarrow \sigma(a) &= 2^p k \\ &= (2^p-1)k+k \\ &= a+k.\end{aligned}$$

It is clear that k divides a which shows that a has only two divisors and k should be equal to one. Thus $\sigma(a)=1+a$ and a is prime. Since 2^p-1 divides a, then it forces $a=2^p-1$. In conclusion,

$$N = 2^{p-1}(2^p-1) \text{ where } 2^p-1 \text{ is prime,}$$

and p is prime by Lemma 2.1.3. □

2.2 Odd Perfect Numbers

The problem for odd perfect numbers (OPNs) stays still unanswered, that is, it is not known whether OPNs exist or not. There are some good attempts made by Euler on the results of OPNs.

Theorem 2.2.1. (Euler) *Let N be an odd perfect number (if it exists). Then N must be of the form $p^b s^2$ where p is prime and gcd$(p,s)=1$ with*

$$p \equiv 1 \pmod 4 \quad \textit{and} \quad b \equiv 1 \pmod 4.$$

Proof. Since N is an odd perfect number, N can be written as

$$N = \prod_{i=1}^{t} p_i^{b_i}.$$

So $\sigma(N)=2N$ and N is odd, then $2|\sigma(N)$ but $4 \nmid \sigma(N)$. On the other hand, it can be written as $\sigma(N) \equiv 2 \pmod 4$. From Lemma 1.2.3 we have,

$$\begin{aligned}\sigma(N) &= \sigma(p_1^{b_1}p_2^{b_2}p_3^{b_3}\cdots p_r^{b_r}) \\ &= \sigma(p_1^{b_1})\sigma(p_2^{b_2})\sigma(p_3^{b_3})\cdots\sigma(p_r^{b_r})\end{aligned}$$

which implies that

$$\sigma(p_1^{b_1})\sigma(p_2^{b_2})\sigma(p_3^{b_3})\cdots\sigma(p_r^{b_r}) \equiv 2 \pmod 4.$$

The integer N is odd, therefore all p_i are also odd. Thus, there is a unique prime p satisfying the following condition $p^b \parallel N$ and

$$\sigma(p^b) \equiv 2 \pmod 4. \tag{2.2.1}$$

Since p is odd, it must be congruent 1 modulo 4 or congruent 3 modulo 4. Let us suppose that $p \equiv 3 \pmod 4$. We have,

$$\sigma(p^b) = 1+p+p^2+\cdots+p^b.$$

this is the sum of $b+1$ odd numbers which is understood that it will be odd if b is even. The proof will follow later in this proof. Then,

$$\begin{aligned}\sigma(p^b) &= 1+p+p^2+\cdots+p^b \\ &\equiv 1+3+1+3+\cdots+1 \pmod 4 \\ &\equiv 0 \quad \text{or} \quad 1 \pmod 4,\end{aligned}$$

and this result which is obtained here contradicts Equation (2.2.1) and we make a conclusion that $p \equiv 1 \pmod 4$. It follows that for $p \equiv 1 \pmod 4$ we have,

$$\begin{aligned}\sigma(p^b) &= 1+p+p^2+\cdots+p^b \\ &\equiv 1+1+1+\cdots+1 \pmod 4 \\ &\equiv (b+1) \pmod 4.\end{aligned}$$

Since $\sigma(p^b) \equiv 2 \pmod 4$, then $b \equiv 1 \pmod 4$. Now the task is to prove that $\frac{N}{p^b}$ is square. Let $\frac{N}{p^b} = s'$. Then,

$$\sigma(N) = \sigma(p^b s') = \sigma(p^b)\sigma(s') \equiv 2 \pmod 4.$$

Assume we have an odd prime k with crucial condition that $k^{m'}|s'$ but $k^{m'+1} \nmid s'$. Then both $\sigma(s')$ and $\sigma(k^{m'})$ are odd by multiplicativity and Equation (2.2.1). So there are two cases stated as follows;

- either $k \equiv 1 \pmod 4$
- or $k \equiv 3 \pmod 4$.

Let's start by showing when $k \equiv 1 \pmod 4$. If $k \equiv 1 \pmod 4$,then

$$\begin{aligned}\sigma(k^{m'}) &= 1+k+k^2+\cdots+k^{m'} \\ &\equiv 1+1+1\cdots+1 \pmod 4 \\ &\equiv (1+m') \pmod 4.\end{aligned}$$

Since $1+m'$ must be odd then it is enough to say that m' should be even. Moreover, for the case when $k \equiv 3 \pmod 4$. Suppose m' is odd. Then

$$\sigma(k^{m'}) = 1+k+k^2+\cdots+k^{m'} \equiv 0 \pmod 4$$

and it contradicts both cases, hence m' must be even. So

$$s' = \prod_{i=1}^{t} k_i^{m_i'} = \prod_{i=1}^{t} k_i^{2n_i'} = \left(\prod_{i=1}^{t} k_i^{n_i'}\right)^2 = s^2$$

□

The prime p is called the special prime or Euler prime of N and p^b is Euler's factor of N.

3. Attempts of OPNs

In this chapter, we will concentrate more on how the great researchers have long ago formulated some theorems on the problem of odd perfect numbers. In 1888, James Sylvester proved that OPNs if they exist must have at least 4 distinct prime factors. This result was recently improved to 9 distinct prime divisors by P. P. Nielsen in 2007. In the second section, we would show that an OPN N must be greater than 10^{300}, a result by Brent, Cohen and te Riele in 1991.

3.1 The Least Distinct Prime Divisors of OPNs

We will commence by showing that an OPN does not have less than four distinct prime factors and this would be done by proving three cases. In the first case, we will show that an OPN cannot have one prime factor and in second case, show that it doesn't have two distinct prime factors. Lastly in the third case, we will prove that it doesn't have three distinct prime factors.

3.1.1 The Case of One Prime Divisor for OPN. For an OPN $N \geq 3$, assume that N has only one prime factor, that is, $N = p$. Then

$$\sigma(N) = \sigma(p) = 1 + p, \tag{3.1.1}$$

and since N is a perfect number, it suffices from the definition of perfect numbers to show that,

$$\sigma(N) = 2N = 2p. \tag{3.1.2}$$

Then equating Equation (3.1.1) to Equation (3.1.2) we obtain

$$\sigma(N) = 2p = p + 1 \Rightarrow \; p = 1,$$

which results in a contradiction since $p \geq 3$ and also p is prime. Moreover, consider the sub-case when the prime factor is squared and follow the same procedure as above. Suppose that $N = p^2$. Then

$$\sigma(N) = \sigma(p^2) = 1 + p + p^2$$

and

$$\sigma(N) = 2N = 2p^2,$$

so it follows that

$$\begin{aligned} &2p^2 = 1 + p + p^2 \\ \Rightarrow\ &p^2 = 1 + p \\ \Rightarrow\ &p(p-1) = 1. \end{aligned}$$

The result obtained is definitely incapable of being true since $p \geq 3$. Lastly on this sub-case, by applying same argument but in a general way, we assume that $N = p^m$ where m is any positive integer greater than 2, then

$$\sigma(N) = \sigma(p^m) = 1 + p + \cdots + p^m$$

and we already know that

$$\sigma(N) = 2N = 2p^m,$$

then if we equate them, we figure out that

$$\begin{aligned} &1 + p + \cdots + p^m = 2p^m \\ \Rightarrow\ &1 + p + \cdots + p^{m-1} = p^m \\ \Rightarrow\ &p^m - p^{m-1} - \cdots - p = 1 \\ \Rightarrow\ &p(p^{m-1} - p^{p-2} \cdots - 1) = 1. \end{aligned}$$

Then this implies that 1 is a product of two factors, but we have $p \geq 3$ and $3 \nmid 1$ so p is not a factor of one. Hence, an OPN does not have one prime factor.

3.1.2 The Case of Two Prime Divisors for OPN. Let's consider the case where an OPN has two distinct prime factors. So, let $N = pq$, where gcd$(p, q) = 1$. Then

$$\sigma(N) = \sigma(pq) = \sigma(p)\sigma(q) = (1 + p)(1 + q) = 1 + p + q + pq$$

and

$$\sigma(N) = \sigma(pq) = 2pq.$$

It follows that

$$\begin{aligned} 1 + p + q + pq &= 2pq \\ 1 + p + q &= pq, \end{aligned}$$

then dividing by pq both sides we get that,

$$\frac{1}{pq} + \frac{1}{p} + \frac{1}{q} = 1. \tag{3.1.3}$$

It is known that $p \geq 3$, $q \geq 5$ since gcd$(p, q) = 1$ and both are primes. Take $p = 3$ and $q = 5$. Then $\frac{1}{pq} \leq \frac{1}{3} \cdot \frac{1}{5} = \frac{1}{15}$, so

$$\frac{1}{pq} + \frac{1}{p} + \frac{1}{q} \leq \frac{1}{15} + \frac{1}{3} + \frac{1}{5} = \frac{9}{15} < 1,$$

which contradicts Equation (3.1.3). Furthermore, granting that $N = p^m q^n$ where gcd$(p, q) = 1$,

$$\begin{aligned} \sigma(N) &= \sigma(p^m q^n) = \sigma(p^m)\sigma(q^n) \\ &= \left(\frac{p^{m+1} - 1}{p - 1}\right)\left(\frac{q^{n+1} - 1}{q - 1}\right) = \frac{p^{m+1}q^{n+1} - q^{n+1} - p^{m+1} + 1}{(p-1)(q-1)} \\ &= \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)p^m q^n - \left(\frac{q^{n+1} + p^{m+1} - 1}{(p-1)(q-1)}\right) \\ &< \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)p^m q^n = \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)N \\ \therefore \frac{\sigma(N)}{N} &< \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right). \end{aligned}$$

The result precisely satisfies Lemma 1.2.5. The ratio $\sigma_{-1}(N) = \frac{\sigma(N)}{N}$ is called an abundancy index and when $\sigma_{-1}(N) = 2$, the number N is called a perfect number, but in case that

$$\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right) < 2, \tag{3.1.4}$$

N will never be perfect. It has been mentioned earlier that $p \geq 3$ and $q \geq 5$, so let $p = 3$ and $q = 5$. Then

$$\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right) = \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

Hence, Inequality (3.1.4) is satisfied and N is a deficient number, which contradicts the fact that N is a perfect number. In general cases it is concluded that an OPN does not have two distinct prime divisors.

Remark 3.1.3. If the abundancy ratio $\sigma_{-1}(N) < 2$, then N is said to be deficient while for $\sigma_{-1}(N) \geq 2$, N is said to be a primitive abundant. It is clear that every perfect number is a primitive abundant. We also recall that

$$\sigma_{-1}(p^{\infty}) = \lim_{q \to +\infty} \sigma_{-1}(p^q) = \frac{p}{p-1}.$$

Moreover, in the next sub-section we would show that there is no OPN with three distinct prime factors.

3.1.4 The Case of Three Prime Divisors for OPN. Lastly, consider the case of three distinct prime factors of an OPN and allow $N = p^m q^n r^l$ an OPN such that $p < q < r$. From the recent case, where we dealt with two prime factors and also by Lemma 1.2.5, it is true that

$$\begin{aligned} \frac{\sigma(N)}{N} &< \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)\left(\frac{r}{r-1}\right) \\ \Rightarrow \sigma(N) &< \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)\left(\frac{r}{r-1}\right) N. \end{aligned}$$

It has been emphasized that N could not be an OPN if

$$\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)\left(\frac{r}{r-1}\right) < 2. \tag{3.1.5}$$

Consider small possible values of p, q and find the lower bound on the prime factor r for which Inequality (3.1.5) will be satisfied. Let $p \geq 3$, $q \geq 5$ and substitute into Inequality (3.1.5), so that we get

$$\begin{aligned} &\left(\frac{3}{2}\right)\left(\frac{5}{4}\right)\left(\frac{r}{r-1}\right) < 2 \\ \Rightarrow &\frac{r}{r-1} < \frac{16}{15} \\ \Rightarrow &\frac{1}{r} < \frac{1}{16} \\ \therefore\ &r > 16. \end{aligned}$$

Since r is a prime number, it is sufficient to take $r \geq 17$. Thus, N is not an OPN if $p \geq 3$, $q \geq 5$ and $r \geq 17$. There are prime numbers less than 17, so it is necessary to look at other combinations for those prime factors. Consider when $p \geq 3$, $q \geq 7$ and $r \geq 11$, then also by substituting into (3.1.5) we obtain

$$\left(\frac{3}{2}\right)\left(\frac{7}{6}\right)\left(\frac{11}{10}\right) = \frac{231}{120} < 2,$$

from which follows that Inequality (3.1.5) is satisfied, whence N is not a perfect number by selecting such a combination. Moreover, if we further unite $p \geq 3$, $q \geq 7$, $r \geq 11$ and $p \geq 3$, $q \geq 5$, $r \geq 13$, we find that there are some of the combinations requiring a special attention and they are listed as a sets of primes: $\{3,5,7\}$, $\{3,5,11\}$ and $\{3,5,13\}$. Let $N = 3^m5^nr^l$. If N is perfect, then

$$\begin{aligned}\sigma(N) &= \sigma(3^m5^nr^l)\\ &= \sigma(3^m)\sigma(5^n)\sigma(r^l)\\ &= \left(\frac{3^{m+1}-1}{2}\right)\left(\frac{5^{n+1}-1}{4}\right)\left(\frac{r^{l+1}-1}{r-1}\right)\\ &= 2(3^m5^nr^l)\\ &= 2N.\end{aligned}$$

After performing arithmetically some simple manipulations, we get the following results

$$\left(3-\frac{1}{3^m}\right)\left(5-\frac{1}{5^n}\right)\left(\frac{r-\frac{1}{r^l}}{r-1}\right) = 16. \tag{3.1.6}$$

Since there are three sets mentioned above, we progress by looking at the three possible sub-cases with an OPN $N = p^mq^nr^l$. In the first sub-case, let $p=3$, $q=5$, $r=7$, so that $N = 3^m5^n7^l$. Replace those values into (3.1.6) to get

$$\left(3-\frac{1}{3^m}\right)\left(5-\frac{1}{5^n}\right)\left(7-\frac{1}{7^l}\right) = 96. \tag{3.1.7}$$

It is known that N is odd and $4 \nmid \sigma(N)$, and precisely, $4 \nmid \sigma(3^m)$ and $4 \nmid \sigma(7^l)$. In spite, for some cases when $m = l = 1$, we get that $\sigma(3) = 1+3 = 4$ and $\sigma(7) = 1+7 = 8$ in which both of them are divisible by 4. These specifically imply that $m \geq 2$ and $l \geq 2$. It is also true that $5 \equiv 1 \pmod 4$ and by Theorem 2.2.1 n is not necessarily even. In this way, take $n \geq 1$ with $m \geq 2$ and $l \geq 2$ to get,

$$96 = \left(3-\frac{1}{3^m}\right)\left(5-\frac{1}{5^n}\right)\left(7-\frac{1}{7^l}\right) \geq \left(3-\frac{1}{3^2}\right)\left(5-\frac{1}{5}\right)\left(7-\frac{1}{7^2}\right) = 96.7836... > 96,$$

which gives a contradiction. Hence, there is no OPN in the form $N = 3^m5^n7^l$. Moreover, in this second sub-case, let $p=3$, $q=5$, $r=11$ such that $N = 3^m5^n11^l$. By using Theorem 2.2.1, m and l must be even like they were in first sub-case discussed. If we consider the inequalities $m \geq 2$, $l \geq 2$ and $n \geq 1$ again, the contradiction is not easily recognised. Hence to solve this, we need to prove that $m \geq 4$. Note that

$$\sigma(N) = \sigma(3^m5^n11^l) = \sigma(3^m)\sigma(5^n)\sigma(11^l)$$

and since N is perfect

$$\sigma(N) = 2N = 2\cdot 3^m\cdot 5^n\cdot 11^l,$$

then $\sigma(3^m)|\sigma(N)$.

For $m = 1,\ 2,\ 3$, we have $\sigma(3^m) = 1+3 = 4$, $\sigma(3^2) = 1+3+3^2 = 13$ and $\sigma(3^3) = 1+3+3^2+3^3 = 40$. Since $4 \nmid \sigma(N)$, $m \neq 1$ and $m \neq 3$. Also, $13 \nmid (2\cdot 3^m\cdot 5^n\cdot 11^l)$ thus, $13 \nmid \sigma(3^m)$. Therefore $m \neq 2$ and m is even, which implies that $m \geq 4$. Analogously, when $l = 1$, $\sigma(11^l) = 12$, which is divisible by 4 and it contradicts the fact that $4 \nmid \sigma(11^l)$. Hence, $l \geq 2$. Now taking into account when

- $n = 1$
- $n \geq 2$.

Firstly take $m \geq 4$, $n \geq 2$, $l \geq 2$, then substituting into (3.1.6) to get,

$$\left(3 - \frac{1}{3^m}\right)\left(5 - \frac{1}{5^n}\right)\left(11 - \frac{1}{11^l}\right) = 160. \tag{3.1.8}$$

Then

$$160 = \left(3 - \frac{1}{3^m}\right)\left(5 - \frac{1}{5^n}\right)\left(11 - \frac{1}{11^l}\right) \geq \left(3 - \frac{1}{3^4}\right)\left(5 - \frac{1}{5^2}\right)\left(11 - \frac{1}{11^2}\right) = 162.8839... > 160$$

which resulted in a contradiction. Secondly choose $n = 1$ and place it into Equation (3.1.8) and make some little simplification to get,

$$\left(3 - \frac{1}{3^m}\right)\left(11 - \frac{1}{11^l}\right) = \frac{100}{3} > 33.$$

It is easily seen by inspection that

$$\left(3 - \frac{1}{3^m}\right)\left(11 - \frac{1}{11^l}\right) < 3 \cdot 11 = 33,$$

for $m \geq 4$ and $l \geq 2$ which is a contradiction. Therefore, there is no OPN of the form $N = 3^m 5^n 11^l$. In this last sub-case, let $p = 3$, $q = 5$, $r = 13$ so that $N = 3^m 5^n 13^l$. By using Theorem 2.2.1, m is even since $3 \not\equiv 1 \mod 4$. Assume $l = 1$, then $\sigma(13^l) = 1 + 13 = 14$ which implies that

$$\begin{aligned} & 7 | \sigma(N) \\ \Rightarrow \quad & 7 | 2 \cdot 3^m \cdot 5^n \cdot 13^l \end{aligned}$$

which is impossible. Therefore, $7 \nmid \sigma(13^l)$ and it is adequate to justify that $l \geq 2$. Thus, $m \geq 2$, $n \geq 1$ and $l \geq 2$. Like in previous sub-case, we would categorise this sub-case into small categories as, (i) $m \geq 4$, $n \geq 2$ and $l \geq 2$, (ii) $m \geq 4$, $n = 1$ and $l \geq 2$ and (iii) $m = 2$, $n \geq 1$ and $l \geq 2$. From Equation (3.1.6) and when $r = 13$, the following equation is obtained,

$$\left(3 - \frac{1}{3^m}\right)\left(5 - \frac{1}{5^n}\right)\left(13 - \frac{1}{13^l}\right) = 192. \tag{3.1.9}$$

(i) Let $m \geq 4$, $n \geq 2$, $l \geq 2$ and then from Equation (3.1.9)

$$192 = \left(3 - \frac{1}{3^m}\right)\left(5 - \frac{1}{5^n}\right)\left(13 - \frac{1}{13^l}\right) \geq \left(3 - \frac{1}{3^4}\right)\left(5 - \frac{1}{5^2}\right)\left(13 - \frac{1}{13^2}\right) = 192.5562... > 192$$

which is a contradiction.

(ii) If $m \geq 4$, $n = 1$, $l \geq 2$ and it follows from equation (3.1.9)

$$\left(3 - \frac{1}{3^m}\right)\left(13 - \frac{1}{13^l}\right) = 40$$

which is not true since $\left(3 - \frac{1}{3^m}\right)\left(13 - \frac{1}{13^l}\right) < 3 \cdot 13 = 39$ for $m \geq 4$ and $l \geq 2$.

(iii) Lastly, if $m = 2$, $n \geq 1$, $l \geq 2$ then equation (3.1.9) becomes

$$\left(5 - \frac{1}{5^n}\right)\left(13 - \frac{1}{13^l}\right) = 66.4615...$$

which is impossible since $\left(5 - \frac{1}{5^n}\right)\left(13 - \frac{1}{13^l}\right) < 5 \cdot 13 = 65$, hence there is no OPN of the form $N = 3^m 5^n 13^l$. It is concluded that an OPN must have at least four distinct prime factors.

3.2 The Lower Bounds for an OPNs

The problem of OPNs which has been demonstrated using several results is totally based on an argument created by Euler about the form of OPNs. As in previous section, postulate that N is an OPN and p is a prime factor of N.
Theorem 3.2.1. *There is no OPN less than* 10^{300}.

We would make some slim changes to improve the proof of Theorem 3.2.1 which is given in (Brent et al., 1991). The proof follows from an algorithm provided in (Brent et al., 1989) and it is basically done by considering lots of computations which are obtained by using Sage. Table 3.1 below shows some results from our calculation and see (Brent et al., 1991).

In case that $p^{\alpha} \parallel N$ where $\alpha > 0$, then $\sigma(p^{\alpha})|2N$. Moreover, if a prime $q > 2$ divides $\sigma(p^{\alpha})$, then we could create more prime divisors of N, definitely the odd primes dividing $\sigma(p^{\alpha})$. We then claim that α' is a power of q such that $\sigma(q^{\alpha'})$ is factorizable so as more primes dividing N could be produced. This process is advanced till the contradiction is obtained.

Furthermore, suppose we have a prime p. Then $\sigma(p^{\alpha_1})|\sigma(p^{\alpha_2})$ if $(\alpha_1+1)|(\alpha_2+1)$. So, it is adequate in claiming an exponent α_1 of a prime p with a target that α_1+1 is prime, where $p|N$. All this process discussed above is called the factor-chain method and it depends mostly on an explicit factorisation of $\sigma(p^{\alpha})$. It is observed that identical factorisation could occur many times, which is too costly and to prevent it, we get rid of the following primes if they divide N: 127, 19, 7, 11, 31, 13, 3, 5.

Moreover, we need to clarify how primes listed above would be eliminated. N is taken as an OPN and p is a prime. So if $p^a \parallel N$, it follows that $\sigma(p^a)|N$ and $\sigma(p^a)$ is then prime factorized. The lowest common multiple of all factors of $\sigma(p^a)$ appearing during that time is obtained. Then we use LCM to find the floor of $\log_{10}(\text{lower bound on } N \text{ if } p^a \parallel N)$, (that is $\lfloor\log_{10}(\text{lower bound on } N \text{ if } p^a \parallel N)\rfloor$. We further find an integer part of $\log_{10} p^{2a}$ and suppose we denote it by v, such that 10^v is the lower bound of N in case that $p^a|N$. In addition, we find the floor of $\log_{10}(\text{lower bound on } N \text{ valid to such an extend})$. Then another prime factor would be considered and similar procedure followed. Also if $\sigma(N) > 2N$,this is considered as the worst-case where relevant factors of N will just come after. For more details see (Brent et al., 1989).

In case that, none of the prime listed is a factor of N, then N must have at least 101 distinct prime factors.

Let's assume that the number of prime divisors is less than 101. Then we know by use of sage and Lemma 1.2.5 that

$$\begin{aligned}\frac{\sigma(N)}{N} &= \prod_{i=0}^{t} \frac{p_i - p_i^{-a_i}}{p_i - 1} \\ &< \prod_{i=0}^{t} \frac{p_i}{p_i - 1} \\ &\leq \frac{17}{16}\frac{23}{22}\frac{29}{28} \prod_{p \in P} \frac{p}{p-1} \\ &= 1.99696032809974 < 2,\end{aligned}$$

where $P = \{p| \quad p \quad \text{is a prime}, \quad 37 \leq p \leq 599 \quad \text{and} \quad p \neq 127\}$. Hence, a contradiction. It follows that,

$$N \geq \left(17 \cdot 23 \cdot 29 \cdot \prod_{P} p\right)^2 \cdot 601 > 10^{473},$$

in the way that eight possible prime factors of N removed would prove the theorem.

For more details see Brent et al. (1989). The main objective for this section is to show that every OPN must exceed 10^{300}. Thus, the following definition is required to make the proof of Theorem 3.2.1 be completed easily. Let $\lambda \geq 0$. Then a function $f_\lambda : \mathbb{N} \to \mathbb{R}$ is defined such that $1 \leq f_\lambda(n) \leq 2^\lambda$, $\forall \quad n \in \mathbb{N}$ with $f_0(n) = 1$.

Definition 3.2.2. Allow q to be an odd prime and n a positive integer. Then

$$E_\lambda(q,n) = \{p^a |\ p \text{ odd prime, } a \text{ even or } a \equiv p \equiv 1 \pmod 4,\ \exists\ j\ \ni\ 0 < j \leq n,\ \frac{p^a}{f_\lambda(p)} < q^{2j} \text{ and } q^j \parallel \sigma(p^a)\}$$

and

$$\varepsilon_\lambda(q,n) = \sum_{p^a \in E_\lambda(q,n)} \log_q \left(\frac{f_\lambda(p) q^{2j}}{p^a}\right) \text{ which implies that } \varepsilon_0(q,n) = \sum_{p^a \in E_\lambda(q,n)} \log_q \left(\frac{q^{2j}}{p^a}\right).$$

N is taken as an OPN and by Euler it is in the form;

$$N = q^n \prod_{i=1}^{j} p_i^{a_i}$$

with q, p_i are distinct odd primes and $p_1 \equiv a_1 \equiv 1 \pmod 4$ and $n \equiv a_2 \equiv \cdots \equiv a_j \equiv 0 \pmod 2$.

Lemma 3.2.3. For the odd primes p and q, if $p|\sigma(q^n)$ and $q^m|p+1$, then $n \geq 3m$.

Proof. Given that p and q are odd primes with a supposition that $q^m|p+1$, it follows that

$$p + 1 = 2dq^m \Rightarrow p = 2dq^m - 1 \quad \text{for some} \quad d > 0, \tag{3.2.1}$$

where $2d$ is another positive factor of $p+1$. Similarly, since $p|\sigma(q^n)$ with $\sigma(q^n) = \frac{q^{n+1}-1}{q-1}$, then

$$\begin{aligned} \frac{q^{n+1}-1}{q-1} &= py \quad \text{for } y > 0 \\ \Rightarrow\ q^{n+1} - 1 &= (2dq^m - 1)y(q-1) \quad \text{from Equation (3.2.1)} \\ &= (2dq^m - 1)T, \end{aligned}$$

where $y(q-1) = T > 0$ and $n \geq m$. Claim that $T \equiv 1 \pmod{q^m}$, then $T = bq^m + 1$ and b is positive. Thus, from above we get,

$$q^{n+1} - 1 = (2dq^m - 1)(bq^m + 1) \tag{3.2.2}$$

whence, $q^{n+1} > dq^m \cdot bq^m \geq q^{2m}$, thus $n \geq 2m$. Then, by expanding equation (3.2.2) and simplifying we obtain,

$$\begin{aligned} q^{n+1-m} &= 2bdq^m + 2d - b \\ \Rightarrow\ b &= 2d + 2bdq^m - q^{n-m+1} \\ &= 2d + q^m(2bd - q^{n+1-2m}) \\ &= 2d + a'q^m \\ \therefore\quad b &= 2d + a'q^m, \end{aligned}$$

where $a' = 2bd - q^{n-2m+1}$, so it is clear that $a' \neq 0$. Hence, there are no possibilities that both $b < q^m$ and $2d < q^m$, if that is the case, then we would have

$$\begin{aligned} b &= 2d + a'q^m \\ \Rightarrow \quad a' &= \frac{b-2d}{q^m} \\ \therefore \quad |a'| &= \frac{|b-2d|}{q^m} < 1 \end{aligned}$$

which resulted into a contradiction. Therefore, $b \geq q^m$ or $2d > q^m$. Assume that $2d > q^m$, then from Equation (3.2.2) we get

$$\begin{aligned} & q^{n+1} - 1 > (q^{2m}-1)(q^m+1) \\ \Rightarrow \quad & q^{n+1} - 1 > q^{3m} + q^{2m} - q^m - 1 \\ \therefore \quad & q^{n+1} > q^{3m} + q^{2m} - q^m \geq q^{3m} \end{aligned}$$

and in case that $b \geq q^m$, then

$$\begin{aligned} & q^{n+1} - 1 > (2q^m-1)(q^{2m}+1) \\ \Rightarrow \quad & q^{n+1} - 1 > 2q^{3m} - q^{2m} + 2q^m - 1 \\ \therefore \quad & q^{n+1} > 2q^{3m} - q^{2m} + 2q^m \geq q^{3m} \end{aligned}$$

Thus, from both cases, it is true that $n \geq 3m$. □

Lemma 3.2.4. For an odd prime q, a set

$$S = \{p_i^{a_i} : p_i \text{ odd primes},\ a_i \geq 2 \text{ either even or satisfying } a_i \equiv p_i \equiv 1 \pmod 4\}.$$

If $q^{n_i} \parallel \sigma(p_i^{a_i})$ and $n \geq \sum n_i$ for every $p_i^{a_i} \in S$, then

$$\log_q \prod_{p_i^{a_i} \in S} \frac{\sigma(p_i^{a_i})}{f_\lambda(p_i)} > 2\sum n_i - \varepsilon_\lambda(q,n).$$

Lemma 3.2.5. Allow N be an OPN, $p_1^{a_1} \in S$ and take q^n as in Definition 3.2.2.

(i) If $a_1 > 1$, then

$$N > \frac{1}{2} q^{3n-\varepsilon_\lambda(q,n)} \prod_{i=1}^{j} f_\lambda(p_i).$$

(ii) In case that $a_1 = 1$,then

$$N > q^{3n-n_1-\varepsilon_\lambda(q,n)} \prod_{i=2}^{j} f_\lambda(p_i),$$

in a way that $q^{n_1} \parallel p_1 + 1$.

For the proofs of Lemma 3.2.4 and 3.2.5 see (Brent et al., 1991).

Corollary 3.2.6. Let N, q^n and $p_1^{a_1}$ be the same as in Lemma 3.2.5.

In case that either, (i) $a_1 > 1$ or (ii) $a_1 = 1$ and $p_1 | \sigma(q^n)$, then

$$N > q^{\frac{8n}{3} - \varepsilon_\lambda(q,n)}.$$

Proof. From Lemma 3.2.5, let $\lambda = 0$, then

(i) For $a_1 > 1$, we know that $n \geq 2$ and $q \geq 3$, since q is an odd prime, so it is true that $q^{3n} > q^{\frac{n}{3}} > 2$. Then, lemma 3.2.5(i) states that

$$N > \frac{1}{2} q^{3n - \varepsilon_\lambda(q,n)}, \text{ since } f_0(p_i) = 1 \text{ implies that } \prod_{i=1}^{j} f_0(p_i) = 1$$

$$\Rightarrow \quad N > \frac{1}{2} q^{3n - \varepsilon_\lambda(q,n)} > q^{3n - \frac{n}{3} - \varepsilon_\lambda(q,n)}, \text{ dividing by } q^{\frac{n}{3}} \text{ instead of } 2.$$

$$\therefore \quad N > q^{\frac{8n}{3} - \varepsilon_\lambda(q,n)}$$

(ii) Consider $a_1 = 1$, lemma 3.2.3 stated that $n \geq 3n_1$. It is clear that,

$$3n - n_1 \geq 3n - \frac{n}{3} = \frac{8n}{3}$$

$$\therefore \quad 3n - n_1 \geq \frac{8n}{3}.$$

Then, utilise lemma 3.2.5(ii) to get

$$N > q^{\frac{8n}{3} - \varepsilon_\lambda(q,n)}, \text{ as it is required.}$$

□

Lemma 3.2.7. If $\sigma(q^n)$ is not a perfect square and $p_1 \nmid \sigma(q^n)$, or $p_1' \nmid \sigma(q^n)$ where p_1' is any prime less than B, then

$$N^2 > 2Bq^{5n - \varepsilon_\lambda(q,n)} \prod_{i=2}^{j} f_\lambda(p_i)$$

where N, q^n and p_1 are defined as before.

Proof. Assume that $q^{n_1} \parallel p_1 + 1$, which implies that $q^{n_1} | p_1 + 1$ but $q^{n_1+1} \nmid p_1 + 1$. Since $\sigma(q^n)$ is not a perfect square number, there exists a distinct prime p_2 such that $p_2 | \sigma(q^n)$ to an odd exponent and also $p_2 | N$ to the higher even exponent.

Moreover, $p_1 + 1 \geq 2q^{n_1}$ and $p_2 \geq B$. Then

$$\begin{aligned} N &\geq q^n \sigma(q^n) p_1 p_2 \\ &\geq q^n \cdot \left(\frac{q^{n+1} - 1}{q - 1} \right) \cdot (2q^{n_1} - 1) \cdot B \\ &\geq q^n \cdot q^n \left(\frac{q - q^{-n}}{q - 1} \right) \cdot 2q^{n_1} (1 - \frac{1}{2} q^{-n_1}) \cdot B \\ &> 2Bq^{2n + n_1} \end{aligned}$$

By using Lemma 3.2.5(ii), it follows that

$$N^2 > 2Bq^{5n-\varepsilon_\lambda(q,n)} \prod_{i=2}^{j} f_\lambda(p_i).$$

□

Theorem 3.2.8. *Let N, q^n and $\varepsilon_0(q,n)$ be defined as in Definition 3.2.2. Then $N > q^{\frac{5n}{2}}$ in conditions that $n \geq 6 \cdot \varepsilon_0(q,n)$ and $\sigma(q^n)$ is not a perfect square and has no prime factors less than $\frac{1}{2}q^{\varepsilon_0(q,n)}$.*

Proof. Let $\lambda = 0$ with a given conditions that $n \geq 6 \cdot \varepsilon_0(q,n)$, then

$$\frac{8n}{3} - \varepsilon_0(q,n) \geq \frac{48(\varepsilon_0(q,n))}{3} - \varepsilon_0(q,n) = 15 \cdot \varepsilon_0(q,n)$$

and

$$\frac{5n}{2} \geq \frac{30 \cdot \varepsilon_0(q,n)}{2} = 15 \cdot \varepsilon_0(q,n).$$

Hence

$$\frac{8n}{3} - \varepsilon_0(q,n) \geq \frac{5n}{2} \quad \text{since,} \quad n \geq 6 \cdot \varepsilon_0(q,n). \tag{3.2.3}$$

Thus from Corollary 3.2.6 and Inequality (3.2.3), we get

$$N > q^{\frac{8n}{3} - \varepsilon_0(q,n)} \geq q^{\frac{5n}{2}}$$
$$\therefore \quad N > q^{\frac{5n}{2}},$$

unless $a_1 = 1$ and $\sigma(q^n)$ is not divisible by p_1. But then the result will follow from Lemma 3.2.7 as $B \geq \frac{1}{2}q^{\varepsilon_0(q,n)}$. □

Theorem 3.2.9. *Take N, q^n, $\varepsilon_0(q,n)$ and p_1 as before. Let R be an unitary divisor of N, meaning that $R|N$ and gcd$\left(N, \frac{N}{R}\right) = 1$, such that $q \nmid R$, $q \nmid \sigma(R)$ and $p_1 \nmid R$. Then*

$$N > \frac{1}{2}Rq^{3n-n_1-\varepsilon_0(q,n)} \quad \textit{where} \quad q^{n_1} \parallel p_1 + 1.$$

Proof. See (Brent et al., 1991) □

A procedure for the computation of $\varepsilon_\lambda(q,n)$ is given as follows. Assume that $p^a \in \varepsilon_\lambda(q,n)$ and $p \geq 3$, then $p^a < 2^\lambda q^{2n}$. Let a polynomial of degree a,

$$F(x) = 1 + x + x^2 + \cdots + x^a,$$

where a is fixed, such that

$$F(x) \equiv 0 \pmod{q^j}.$$

Then, it must also be true that $q^j \parallel \sigma(p^a)$.

Table 3.1: Non-zero results to $\varepsilon_\lambda(q, n)$, $q^j \parallel \sigma(p^a)$

λ	q	n	j	a	$\log_q\left(\frac{q^{2j} f_\lambda(p)}{p^a}\right)$	p
0	7	172	8	2	0.5496...	3376853
			19	2	0.0607...	10744682090246617
			25	2	0.3689...	936579478224094047977
			61	2	1.7036...	6778...
			119	2	1.0771...	1292...
			150	2	0.3796...	4020...
0	3221	42	1	4	0.8125...	11
0	612067	22	1	2	0.3398...	63601
			17	2	0.2253...	5291...
0	3169	36	1	2	0.8650...	97
			3	2	0.4191...	5875516237
			11	2	0.0481...	2666...
221	3	240	1	2	0.9380...	37

Proof. Let D indicates a prime divisor which has been eliminated already and three dots (...) signal that the rest of other factors appearing are irrelevant. Also, a number N is assumed to be an OPN as before. We would prove Theorem 3.2.1 by considering some cases where special attention is needed. These cases are considered because when Theorem 3.2.8 is used the values obtained are getting closer and closer to 10^{300}. Since we have selected some of the cases it follows that the proof of lower bounds for OPNs is not complete in this work because not every case is included. For more convincing details see (Brent et al., 1991).

Case I: Suppose that $3221^{42} \parallel N$, then it implies that $\sigma(3221^{42})|2N$. Then

$$\begin{aligned}\sigma(3221^{42}) = \ &21664331653303852776686485860345118504113585502359004344672281026719\\&170619080128356159823273738435384217108793820294008781550292420927969\\&75832692103\end{aligned}$$

For simplicity, denote $\sigma(3221^{42})$ as c_{148} , where c_{148} stands for a composite number with 148 digits. By using Definition 3.2.2, we get that

$$\varepsilon_0(3221, 42) = \log_{3221}\left(\frac{3221^2}{11^4}\right) \leq 0.8126.$$

See Table 3.1. So all conditions of Theorem 3.2.8 are fulfilled. Therefore,

$$N > 3221^{\left(\frac{5\cdot 42}{2}\right)} \quad \Rightarrow \quad N > 3221^{105} > 10^{368}.$$

Case II: Similarly, assume that $7^{172} \parallel N$, then $\sigma(7^{172})|2N$. From the use of sage, it is obtained that $\sigma(7^{172}) = c_{146}$, where c_{146} is defined like in (case I) above. Thus, $\varepsilon_0(7, 172) \leq 4.1400$, by using Theorem 3.2.8 with all conditions in there are satisfied. Hence,

$$N > 7^{\left(\frac{5\cdot 172}{2}\right)} \quad \Rightarrow \quad N > 7^{430} > 10^{363}.$$

Case III: In this case, we take $612067^{22} \parallel N$, truly followed by $\sigma(612067^{22})|2N$. $\sigma(612067^{22}) = c_{128}$ is computed using sage and we found that $\varepsilon_0(612067, 22) \leq 0.5652$. Thus, from Theorem 3.2.8 we have

$$N > 612067^{\left(\frac{5 \cdot 22}{2}\right)} \quad \Rightarrow \quad N > 612067^{545} > 10^{318},$$

since all conditions stated in Theorem 3.2.8 are satisfied.

Case IV: It is quite clear that the exponent of 10 reduces as more cases are considered, so in the next case suppose that $3169^{36} \parallel N$, then $c_{127} = \sigma(3169^{36})|2N$ and $\varepsilon_0(3169, 36) \leq 1.3324$. From Theorem 3.2.8, we get

$$N > 3169^{\left(\frac{5 \cdot 36}{2}\right)} \quad \Rightarrow \quad N > 3169^{90} > 10^{315}.$$

Case V In addition, assume that $497^{46} \parallel N$, thus $c_{123} = \sigma(497^{46})|2N$ and following the same argument, we obtain that $\varepsilon_0(467, 46) = 0$. Let $\lambda = 0$ and use Lemma 3.2.5. The factor-chain method used here is precisely based on the elimination of the following prime numbers 127, 19,7,11,31,13,3,and 5. Consider

$$\begin{aligned}
&7^2 \Rightarrow \sigma(7^2) = 57 \Rightarrow 19 \ldots, \quad D \\
&7^4 \Rightarrow \sigma(7^4) = 2801^1 \\
&2801^1 \Rightarrow \sigma(2801^1) = 2802 \Rightarrow 3 \cdot 467 \\
&467^2 \Rightarrow \sigma(467^2) = 218557 \Rightarrow 19 \ldots, \quad D \\
&467^4 \Rightarrow \sigma(467^4) = 47664878041 \Rightarrow 2801 \ldots, \quad D \\
&\quad \vdots \\
&469^{46} \Rightarrow \sigma(469^{46}) = c_{123}
\end{aligned}$$

and this shows that $p_1 = 2801$ and $n_1 = 1$, then

$$N > 467^{(3 \cdot 42 - 1)} \quad \Rightarrow \quad N > 467^{137} > 10^{315}.$$

Case VI: For $191^{46} \parallel N$ and $\sigma(191^{46})|2N$, we would make use of Lemma 3.2.5 with $\lambda = 0$, $p_1 = 30941$, $n_1 = 1$ and $\varepsilon_0(191, 46) = 0$. Then $\sigma(191^{46}) = c_{105}$ and for more details see (Brent et al., 1991) Figure 2. Hence,

$$N > 191^{(3 \cdot 46 - 1)} \quad \Rightarrow \quad N > 191^{137} > 10^{312}.$$

Case VII: Consider the fact that $36389^{22} \parallel N$ and $c_{101} = \sigma(36389^{22})|2N$. Then

$$\begin{aligned}
&3^2 \;\; \Rightarrow \sigma(3^2) = 13, \quad D \\
&3^4 \;\; \Rightarrow \sigma(3^4) = 121 \quad \Rightarrow \quad 11\ldots, \quad D \\
&\quad \vdots \\
&3^{18} \;\; \Rightarrow \sigma(3^{18}) = 581130733 \quad \Rightarrow 1597 \cdot 363889 \\
&363889^1 \;\; \Rightarrow \sigma(363889^1) = 363890 \;\; \Rightarrow 5 \cdot 36389 \\
&\qquad\qquad \text{(proceeding till we get)} \\
&363889^{22} \;\; \Rightarrow \sigma(363889^{22}) = c_{101}
\end{aligned}$$

By using Theorem 3.2.9 and a selected computation above, we observe that, $R = 3^{n_2} \geq 3^{18}$, $p_1 = 363889$, $n_1 = 1$ and $\varepsilon_0(36389, 22) = 0$, then

$$N > \frac{1}{2}(3^{18}) \cdot 36389^{65} > 10^{304}.$$

Case VIII: In this case, take $191^{42} \parallel N$ such that $\sigma(191^{42}) = c_{96}$ and this is obtained as follows,

$$\begin{aligned}
&13^1 \ \Rightarrow \sigma(13) = 14 \Rightarrow 7, \quad D\\
&13^2 \ \Rightarrow \sigma(13^2) = 183 \Rightarrow 3 \cdot 61,\\
&\text{(some computations are left out of discussion here),}\\
&13^4 \ \Rightarrow \sigma(13^4) = 30941,\\
&30941^1 \ \Rightarrow \sigma(30941^1) = 30942 \ \Rightarrow 3^4 \cdot 191,\\
&191^2 \ \Rightarrow \sigma(191^2) = 36673 \ \Rightarrow 7..., \quad D\\
&\text{some computations are omitted,}\\
&191^{42} \ \Rightarrow \sigma(191^{42}) = c_{96},
\end{aligned}$$

then, $p_1 = 30941$ and $191 \parallel \sigma(p_1)$. From Lemma 3.2.5, $n_1 = 1$, $f_\lambda(p_1) \geq 0$ and $\lambda = 0$, then

$$N > q^{3n-1-\varepsilon_\lambda(q,n)} \prod_{i=2}^{j} f_\lambda(p_i).$$

When $q = 191$ and $n = 42$, the bound obtained is not sufficiently good, so we proceed by letting $\lambda > 0$. Suppose for all prime p

$$f_\lambda(p) = \begin{cases} \left(\frac{p}{p-1}\right)^\lambda & \text{if } \ p|N, \ \ p \neq 191 \ \text{ or } \ 30941 \\ 1 \ \ \text{otherwise} \end{cases}.$$

We know that

$$\begin{aligned}
2 = \frac{\sigma(N)}{N} < \prod_{p|N} \frac{p}{p-1} &= \frac{191}{190} \cdot \frac{30941}{30940} \prod_{i=2}^{j} \left(\frac{p_i}{p_i - 1}\right)\\
\Rightarrow \qquad 2 &< \frac{191}{190} \cdot \frac{30941}{30940} \prod_{i=2}^{j} \left(\frac{p_i}{p_i - 1}\right).
\end{aligned}$$

It follows that

$$\prod_{i=2}^{j} f_\lambda(p_i) > \left(2 \cdot \frac{190}{191} \frac{30940}{30941}\right)^\lambda.$$

Choose λ to be so large that it would generate $\prod_{i=2}^{j} f_\lambda(p_i)$ to be large also and making some experiments we conclude that

$$N > 191^{125} \left(2 \cdot \frac{190}{191} \frac{30940}{30941}\right)^{50} > 10^{300}.$$

□

3.3 An OPN Has a Prime Factor Exceeding 10^7

In this section, we would examine the components of an OPN again and primarily the lower bounds of its factors. We would start first by defining a cyclotomic polynomial. The nth cyclotomic polynomial, of order n, evaluated at x, would be symbolised by $\Phi_n(x)$. If n is prime, then

$$\Phi_n(x) = 1 + x + \cdots + x^{n-1}.$$

In general, the partial factorisation is given as,

$$p^n - 1 = \prod_{d|n} \Phi_d(p)$$

and so

$$\sigma(p^a) = \frac{p^{a+1}-1}{p-1} = \prod_{d} \Phi_d(p), \quad \text{where } d|a+1 \text{ and } d > 1,\ p \text{ is prime.} \tag{3.3.1}$$

Let N be an OPN with unique prime factorisation provided by $N = \prod_{i=1}^{r}(p_i^{a_i})$, then

$$2N = 2\prod_{i=1}^{r}(p_i^{a_i}) = \sigma\left(\prod_{i=1}^{r}(p_i^{a_i})\right) = \prod_{i=1}^{r} \prod_{\substack{d|a+1 \\ d>1}} \Phi_d(p_i). \tag{3.3.2}$$

Let p and q be positive integers such that $q > 1$ and $\gcd(p, q) = 1$, then $o_q(p)$ is called a multiplicative order of p modulo q. Suppose that q is prime, then we write $v_q(p)$ the valuation of p associated to q, which means, $v_q(p) = \gamma$ if $(q^\gamma \parallel p$. From Theorems 94 and 95 in (Nagell, 1964), we obtain;

Lemma 3.3.1. Let p and q be primes, then $q|\Phi_n(p)$ if and only if $n = rq^\beta$, where $r = o_q(p)$ with $\beta \geq 0$. Moreover, if $\beta > 0$, then $q \parallel \Phi_n(p)$.

By using Equation (3.3.1) and Lemma 3.3.1 the following result is obtained,

$$v_q(\sigma(p^a)) = \begin{cases} v_q(\Phi_r(p)) + v_q(a+1) & \text{if} \quad r|(a+1), \quad r \neq 1, \quad \text{where} \quad \Phi_r(p) = p^r - 1 \\ v_q(a+1) & \text{if} \quad r = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{3.3.3}$$

From Lemma 3.3.1, another lemma follows immediately and is stated as follows,

Lemma 3.3.2. In case that, $q|\Phi_{\alpha_1}(p)$ and $s|\Phi_{\alpha_2}(p)$ with $\alpha_1 \neq \alpha_2$, $q \equiv 1 \pmod{\alpha_1}$ and $s \equiv 1 \pmod{\alpha_2}$, then $q \neq s$.

Lemma 3.3.3. Take N be an OPN and p prime. If $p^a|N$, then for each $d|a+1$ the number $\Phi_d(p)$ is divisible by a prime q with $o_q(p) = d$ and $q \equiv 1 \pmod{d}$.

Let's give a little information about the Fermat primes. A prime q_1 is said to be a Fermat prime if it is of the form $q_1 = 2^\mu + 1$, for some positive integer μ. It is easily observed that $\mu = 2^i$ for some $i \in \mathbb{N}$. These primes contributed a lot towards the problem of OPNs. We would make few changes from Equation (3.3.3) in terms of factors of N and Fermat primes to obtain the following lemma.

Lemma 3.3.4. Let an OPN be N with $p^a \parallel N$ where p is prime and q is a Fermat prime. Then,

$$v_q(\sigma(p^a)) = \begin{cases} v_q(p+1) + v_q(a+1) & \text{if} \quad p \equiv -1 \pmod{q} \\ v_q(a+1) & \text{if} \quad p \equiv 1 \pmod{q} \\ 0 & \text{otherwise.} \end{cases}.$$

See (Nielsen, 2007) for the proof of this lemma.

Definition 3.3.5. Acceptable values of $\Phi_d(p)$: Let d and $p \geq 3$ be primes. Then $\Phi_d(p)$ is said to be acceptable if each prime divisor of $\Phi_d(p)$ is strictly less than 10^7.

On account that p is odd and $d > 5000000$, from lemma 3.3.3, $\Phi_d(p)$ has at least one prime factor q such that $q \equiv 1 \pmod d$. Moreover, since $d+1$ is even and 1 is not prime, then $q \geq 2d+1 > 10^7$ and thus, $\Phi_d(p)$ would not be acceptable. Any prime p is said to be inadmissible if $\Phi_d(p)$ is unacceptable for every d. The case when $d = 2$ is definitely looked at if p is a special prime for N.

From a computer search, a quick ascertainment was made that if $d \geq 7$ and $3 \leq p < 10^7$, then the cyclotomic number $\Phi_d(p)$ is unacceptable but excluding all values listed on Table A, on section for Appendix made by Jenkins, see (Jenkins, 2003). Next we would give a brief discussion of an inadmissible small primes and they will be listed below.

Lemma 3.3.6. Suppose that an OPN N has no prime factor exceeding 10^7. Then any element of the set

$$\mathsf{Y} = \{3, 5, 7, 13, 17, 19, 23, 29, 31, 37, 43, 61, 71, 113, 127, 131, 151, 197, 211, 239, 281, 1093\}.$$

would not be a prime factor of N.

To prove Lemma 3.3.6, since it is known that if $p \in \mathsf{Y}$, then $p \nmid N$. We would assume that each prime in the set divides N and obtain a contradiction, following the order below,

$$1093, 151, 31, 127, 19, 11, 7, 23, 31, 37, 43, 61, 13, 3, 5, 29, 43, 17, 71, 113, 197, 211, 239, 281.$$

Thus, we suppose that $p|N$, where $p \in \mathsf{Y}$ and attain acceptable values of $\Phi_d(p)$ by looking in Table A to get acceptable values with $d \geq 7$. Thus, we check acceptability of $\Phi_3(p)$, $\Phi_5(p)$ and also for $\Phi_2(p)$ where p satisfies the condition that $p \equiv 1 \pmod 4$. If the preceding special prime is found then the last special prime is no longer considered. Then, we write $\Phi_d(p)$ as the product of its prime factors to see which prime factors are greater than 10^7. The process is continued for several time till there is a contraction obtained. So, we would start by showing $1093 \nmid N$ and followed by $151 \nmid N$.

Proof. Suppose that $1093|N$. Note that $1093 \equiv 1 \pmod 4$, hence 1093 is a special prime. So,

$$\Phi_2(1093) = 1 + 1093 = 1094 = 2 \cdot 547,$$
$$\Phi_3(1093) = 1 + 1093 + 1093^2 = 1195743 = 3 \cdot 398581,$$
both $\Phi_2(1093)$ and $\Phi_3(1093)$ are acceptable then,
$$\Phi_5(1093) = 1 + 1093 + 1093^2 + 1093^3 + 1093^4 = 142849318030 = 11 \cdot 31 \cdot 4189129561,$$
$\Phi_5(1093)$ is unacceptable since $4189129561 > 10^7$.

Hence, we have $547|N$ or $398581|N$, start first by consider $547|N$. Assume that $547|N$ and $547 \not\equiv 1 \pmod 4$ so 547 is not special prime.

$$\Phi_3(547) = 1 + 547 + 547^2 = 299757 = 3 \cdot 163 \cdot 613,$$
$$\Phi_5(547) = 1 + 547 + 547^2 + 547^3 + 547^4 = 89689992761 = 431 \cdot 208097431,$$
$\Phi_5(547)$ is unacceptable while $\Phi_3(547)$ is acceptable.

Thus, $613|N$.

$$\Phi_3(613) = 1 + 613 + 613^2 = 376383 = 3 \cdot 7 \cdot 17923,$$
$$\Phi_5(613) = 1 + 613 + 613^2 + 613^3 + 613^4 = 141433064141 = 131 \cdot 20161 \cdot 53551,$$

Both values are acceptable and the short summery of the process till a contradiction is given below.

$$
\begin{aligned}
&1093^*, 547, 613, 17923 : \Phi_3(17923) = 3 \cdot 7 \cdot 31 \cdot 265717,\\
&1093^*, 547, 613, 17923, 265717 : 265717 \quad \text{is inadmissible},\\
&1093, 398581^* : \Phi_2(398581) = 2 \cdot 17 \cdot 19 \cdot 617,\\
&1093, 398581^*, 617 : \Phi_3(617) = 97 \cdot 3931,\\
&1093, 398581^*, 617, 3931 : \Phi_3(3931) = 3 \cdot 7 \cdot 31 \cdot 23743\\
&1093, 398581^*, 617, 3931, 23743 : 23743 \quad \text{is inadmissible}.\\
&151 \nmid N\\
&151 : \Phi_3(151) = 3 \cdot 7 \cdot 1093
\end{aligned}
$$

then we obtain a contradiction since 1093 does not divide N. Take note that a number with the star represents the recent special prime number considered. □

The next important issue to pay attention to is where a restriction on the exponents in the prime power decomposition of N is given. We make an assumption that $p^a \parallel N$ and $d|a+1$ where $d > 5$. From values of $\Phi_d(p)$ shown in Table A and Equation (3.3.2), then it follows that $\Phi_d(p)|N$. Moreover, from Table A and Lemma 3.3.6, we get that $d = 7$ and p is an element of the following set,

$$
\{67, 173, 607, 619, 653, 1063, 1453, 2503, 4289, 5953, 9103, 9397,\\
10889, 12917, 19441, 63587, 109793, 113287, 191693, 6450307, 7144363\}
$$

Lemma 3.3.7. If $p^a \parallel N$ and p is not the special prime p_0, then $a+1 = 3^b \cdot 5^c$ where $b + c > 0$. If $p_0^{a_0}$, then $a_0 + 1 = 2 \cdot 3^b \cdot 5^c$ where $b + c \geq 0$

Let $P = \{p| \quad 37 < p < 10^7\}$. Consider the following four subsets A, B, C and D of P which are defined as follows:

$$
\begin{aligned}
A &= \{p \in P| \quad p \not\equiv 1 \pmod 3 \text{ and } p \not\equiv 1 \pmod 5\} = \{47, 53, 59, \ldots\},\\
B &= \{p \in P| \quad p \equiv 1 \pmod{15}\} = \{61, 151, 181, \ldots\},\\
C &= \{p \in P| \quad p \equiv 1 \pmod 3, \quad p \not\equiv 1 \pmod 5 \text{ and } \Phi_5(p) \text{ has a prime divisor} \geq 10^7\}\\
&= \{73, 79, 103, \ldots\},\\
D &= \{p \in P| \quad p \not\equiv 1 \pmod 3, \quad p \equiv 1 \pmod 5 \text{ and } \Phi_3(p) \text{ has a prime divisor} \geq 10^7\}\\
&= \{3221, 3251, 3491, \ldots\}
\end{aligned}
$$

By using computer search we get that cardinality of set $A = 249278$, $B = 83002$, $C = 694$ and $D = 57$, then

$$
\begin{aligned}
A^* &= \prod_{p \in A} \frac{p}{p-1} > 1.7331909144375899931,\\
B^* &= \prod_{p \in B} \frac{p}{p-1} > 1.1791835683407662159,\\
C^* &= \prod_{p \in C} \frac{p}{p-1} > 1.239225225,\\
D^* &= \prod_{p \in D} \frac{p}{p-1} > 1.006054597.
\end{aligned}
$$

For the proof of the following proposition see (Hagis et al., 1998).

Proposition 3.3.8. Assume that an OPN has no prime factor greater than 10^7 and p_0 be a special prime. Then the following are satisfied:

- The number N is divisible by at most one element of A. If there is such an element a, then $a \neq p_0$ and $a \geq 47$.
- The number N is divisible by at most one element of B. If there is such an element it is p_0, and then $p_0 \geq 61$.
- The number N is divisible by at most one element of C. If there is such an element it is p_0, and then $p_0 \geq 73$.
- The number N is not divisible by any element of D.

Theorem 3.3.9. *If N is an OPN, then N has a prime factor greater than 10^7.*

Proof. The cardinality of the set P is 664567, thus

$$P^* = \prod_{p \in P} \frac{p}{p-1} < 4.269448664996309337$$

From Lemma 1.2.5, Proposition 3.3.8 and 3.3.1 it follows that,

$$2 = \frac{\sigma(N)}{N} < \prod_{i=0} \frac{p_i}{p_i - 1} \leq \frac{47}{46}\frac{61}{60}\frac{P^*}{A^* B^* C^* D^*} < 1.740567$$

This is contradiction. □

4. Conclusion

In this chapter, we will like to emphasize that all of the results discussed in this essay about OPN can be improved to obtain higher bounds. We will commence by the distinct prime factors of an OPN N. Let $\omega(N)$ be a function which counts the distinct prime divisors of N. We have shown that $\omega(N) \geq 4$, but there are some good results proven by Pace P. Nielsen which shows that an OPN must have at least nine distinct prime factors. There is a feeling that this bound can also be extended in future.

In addition, the study of the OPNs' problem involves many conditions, so the lower bound of an OPN which is discussed in Section 3.2 is indeed improved from that bound to the new bound stated as "an OPNs are greater than 10^{1500}." This was shown by Pascal Ochem and Michaël Rao; for more details see (Ochem and Rao, 2012). Hopefully this bound can still be further increased to higher power of 10 as it is mostly dependent to the quality of device used to make some computations. This can be possible since technology is always improved every day.

Lastly, let the largest component of N be greater than 10^7 and denote it by K. The criteria used in the last section on Chapter 3 is also applied to raise the power bound of K to eight. This was done by Takeshi Goto and Yasuo Ohno and for more information see (Goto and Ohno, 2008). The inequality is very powerful in proving Theorem 3.3.9; probably it can be extended even more to the powers larger than eight due to assistance of upgraded tools we have nowadays to generate all acceptable values shown on Table A; see (Hagis et al., 1998).

Acknowledgements

I wish to take this opportunity to pass my sincere gratitudes to my supervisor, Professor Florian Breuer, for the wonderful contribution he did in the process of writing my essay, and more specifically by proposing the essay-topic for me. I couldn't see me accomplishing my essay from the beginning, but with your superior I made it. I would also like to thank my tutor, Tovondrainy Christalin Razafindramahatsiaro, for his invaluable guidance and helpful remarks during my essay phase. Thank you brother for the motivation.

My special thankfulness goes to Professor Barry Green, Director of AIMS , Professor Jeff Sanders, Academic Director and the whole staff for giving me opportunity to study at AIMS with brilliant people from different countries in Africa. My profound gratitude goes to Jan Groenewald for the support he provided to me in terms of IT issues. I would also like to thank all my colleagues for the support they gave it to me.

Lastly and foremost, I would like to thank God for being with me through my stay at AIMS till the end of studies.Thank you LORD. I would like to say thanks to my family for their prayers and their support.

References

T. M. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York Inc, 1976.

R. P. Brent, G.L.Cohen, and H. te Riele. A new lower bound for odd perfect numbers. volume 53, pages 431–437. Computer Sciences Laboratory, Australia National University, 1989.

R. P. Brent, G.L.Cohen, and H. te Riele. Improved techniques for lower bounds of odd perfect numbers. volume 57, pages 857–868. Computer Sciences Laboratory, Australia National University, 1991.

T. Goto and Y. Ohno. Odd perfect numbers have a prime factor which exceeds 10^8. volume 77, pages 1859–1868. Math. comp, 2008.

P. Hagis, Jr, and G.L.Cohen. Every odd perfect number has a prime factor which exceeds 10^6. volume 67, pages 1323–1330. Math. comp, 1998.

G. H. Hardy and E. M. Wrigth. *An Introduction to the Theory of Numbers*. 5th Edition, Oxford Press, 1980.

P. Jenkins. Odd perfect numbers have a prime factor exceeding 10^7. *Math. Comp*, 72:1549–1554, 2003.

T. Nagell. *Introduction to Number Theory*. Wiley, New York, 1964.

A. M. Nguyen. *Odd Perfect Numbers*. Masters, San Jose State University, 2000.

P. P. Nielsen. Odd perfect numbers have a least nine distinct prime factors. volume 76, pages 2109–2126. Math. comp, 2007.

P. Ochem and M. Rao. Every odd perfect numbers are greater than 10^{1500}. volume 81, pages 1869–1877. Math. comp, 2012.