2000

Odd perfect numbers

Anh Minh Nguyen
San Jose State University

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI®

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

ODD PERFECT NUMBERS

A Thesis

Presented to

The Faculty of the Department of Mathematics

San Jose State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science

by

Anh Minh Nguyen

August 2000

Bell & Howell Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

APPROVED FOR THE DEPARTMENT OF
MATHEMATICS AND COMPUTER SCIENCE

Dr. Daniel Goldston

Dr. Vladimir Drobot

Dr. Brian Peterson

APPROVED FOR THE UNIVERSITY

ABSTRACT

ODD PERFECT NUMBERS

by Anh minh Nguyen

A perfect number is a positive integer which is equal to the sum of its proper divisors. For example, six is perfect since $6 = 1 + 2 + 3$. No one has ever discovered an odd perfect number yet (if one exists it must be larger than 10^{300}), and most mathematicians believe there are no odd perfect numbers. In this direction, many results have been proved which limit the type of odd numbers which might be perfect. For example, any odd perfect number must have at least 8 distinct prime factors. In 1994 Heath-Brown proved the remarkable result that an odd perfect number N with k prime factors must satisfy the bound $N < 4^{4^k}$. This thesis will give a proof of Heath-Brown's result and other related results.

Contents

Chapter 1

An Introduction to Perfect Numbers

1.1 A quick look at the history of the study of perfect numbers

It is not known when perfect numbers were first studied and indeed the first studies may go back to earliest times when people started to be curious about numbers. Perfect numbers were studied by Pythagoras and his followers, more for their mystical properties than for their number theoretic properties.

Today the usual definition of a perfect number is in terms of its divisors; *a positive integer is called a perfect number when it is equal to the sum of its proper divisors.* For instance, six is the first perfect number and the second is 28, since $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$, but early definitions were in terms of the *aliquot parts* of a number. An *aliquot parts* of a number is a proper quotient of the number. So for example the *aliquot parts* of 10 are $1, 2,$ and 5. A perfect number was defined to be one which is equal to the sum of its *aliquot parts* in the earlier time.

The four perfect numbers $6, 28, 496$ and 8128 seem to have been known from ancient times and there is no record of these discoveries. The first recorded mathematical result concerning perfect numbers which is known occurs in Euclid's Elements written around 300 BC.

The next significant study of perfect numbers was made by Nicomachus of Gerasa around 100AD. Nicomachus had some results concerning perfect numbers. All of these were given without any attempt at a proof.

(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 Algorithm to generate perfect numbers will give all even perfect numbers, i.e. every perfect number is of the form $2^{n-1}(2^n - 1)$, for some $n > 1$, where $2^n - 1$ is prime.

(5) There are infinitely many perfect numbers.

The fifth perfect number has been discovered and written down in a manuscript dated 1461.

J.Scheyble gave the sixth perfect number in 1555 in his commentary to a translation of Euclid's Elements.

The next major contribution was made by Fermat around 1640. His Little Theorem shows that for any prime p and an integer a not divisible by p, $a^{p-1} - 1$ is divisible by p. Certainly Fermat found his Little Theorem as a consequence of his investigations into perfect numbers.

Mersenne was very interested in the results that Fermat sent him on perfect numbers and soon produced a claim of his own which was to fascinate mathematicians for a great many years. In 1644 he published Cogitata Physica Mathematica in which he claimed that $2^p - 1$ is prime (and so $2^{p-1}(2^p - 1)$ is a perfect number) for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and for no other value of p up to 257. Primes of the form $2^p - 1$ are called Mersenne primes.

The next person to make a major contribution to the question of perfect numbers was Euler. In 1732 he proved that the eighth perfect number was $2^{30}(2^{31}-1) = 2305843008139952128$. It was the first new perfect number discovered for 125 years. Euler also proved the converse of Euclid's result by showing that every even perfect number had to be of the form $2^{p-1}(2^p-1)$.

In 1883 Pervusin showed that $2^{60}(2^{61}-1)$ is a perfect number. This was shown independently three years later by Seelhoff. Many mathematicians leapt to defend Mersenne saying that the number 67 was a misprint for 61.

Further mistakes made by Mersenne were found. In 1911 Power showed that $2^{88}(2^{89}-1)$ was a perfect number, then a few years later he showed that $2^{101}-1$ is a prime and so $2^{100}(2^{101}-1)$ is a perfect number. In 1922 Kraitchik showed that Mersenne was wrong in his claims for his largest prime of 257 when he showed that $2^{257}-1$ is not prime.

Many people have followed the progress of finding even perfect numbers but there was also attempts to show that an odd perfect number could not exist. In fact Sylvester proved in 1888 that any odd perfect number must have at least four distinct prime factors. It is also known that such a number would have more than 300 digits and a prime divisor greater than 10^6. The problem of whether an odd perfect number exists, however, remains unsolved.

Today 38 even perfect numbers are known, $2^{88}(2^{89}-1)$ being the last to be discovered by hand calculations in 1911, after that, all others being found using a computer.

In January 27, 1998, the 37^{th} was found. It is $(2^{3021376})(2^{3021377}-1)$ and has 1,819,050 digits. The 38^{th} was found in 1999 . It is $(2^{6972592})(2^{6972593}-1)$ and has 4,197,919 digits.

1.2 Some Notation for Arithmetic Function

An *arithmetic function* is a function having the natural numbers as its domain. The range of values of an arithmetic function is often a set of integers, but occasionally is the set of reals or complexes.

Here are some notable examples (in all examples, divisor means positive divisor):

$P_r(n) := n^r$ for a fixed integer r.

$d(n) :=$ the number of distinct divisors of n.

$\sigma(n) :=$ the sum of distinct divisors of n.

$\sigma_r(n) :=$ the sum of the r^{th} powers of the divisors of n.

$\omega(n) :=$ the number of distinct prime factors of n.

$\Omega(n) :=$ the total number of prime factors of n (counting multiplicity).

$\phi(n) :=$ the number of positive integers at most n that are relatively prime to n.

For instance, let $n = 90 = 2 \cdot 3^2 \cdot 5$. Then

$$P_2(90) = 90^2 = 8100,$$

$$\omega(90) = 3,$$

$$\Omega(90) = 4.$$

The positive divisors of n are $1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45$, and 90. So

$$\sigma(90) = 1 + 2 + 3 + 5 + 6 + 9 + 10 + 15 + 18 + 30 + 45 + 90 = 234,$$

and

$$d(90) = 12.$$

Note that if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then

$$\phi(n) = p_1^{(a_1-1)}(p_1 - 1)p_2^{(a_2-1)}(p_2 - 1) \cdots p_k^{(a_k-1)}(p_k - 1).$$

Thus

$$\phi(90) = (2^{(1-1)}1)(3^{(2-1)}2)(5^{(1-1)}4) = 1 \cdot 3 \cdot 2 \cdot 1 \cdot 4 = 24.$$

1.3 Euclid

Theorem 1.3.1 *If $2^{n+1}-1$ is prime, then $2^n(2^{n+1}-1)$ is perfect.*

Proof. Let $P = 2^{n+1}-1$, and suppose P is an odd prime. Let $N = 2^nP$. To prove that N is perfect, the first step is to show

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

The divisors of 2^n are just 1 and the powers of 2 up to 2^n. Thus

$$\sigma(2^n) = 1 + 2^1 + 2^2 + 2^3 + \cdots + 2^n.$$

Using the formula for a finite geometric series

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}, \quad \text{if } x \neq 1, \tag{1.2}$$

(1.1) is obtained by taking $x = 2$. Next, for any prime p, $\sigma(p) = 1 + p$. It is easy to see that $\sigma(n)$ is a *multiplicative* function, which is a function with the property that $f(ab) = f(a)f(b)$ whenever $\gcd(a,b) = 1$. (The proof of this will be given in Chapter 2.) Hence

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

and hence N is perfect.

Here is another way to prove this theorem without using the multiplicative property of $\sigma(n)$. Notice that the divisor of $N = 2^n P$ are 1, 2, 2^2, ..., 2^n, P, $2P$, 2^2P, ..., 2^nP. Thus

$$\begin{aligned}
\sigma(2^nP) &= (1+2+2^2+\cdots+2^n)+(P+2P+2^2P+\cdots+2^nP) \\
&= (1+P)(1+2+2^2+\cdots+2^n) \\
&= 2^{n+1}(2^{n+1}-1) \\
&= 2(2^n)(2^{n+1}-1) \\
&= 2(2^n)(P) \\
&= 2N
\end{aligned} \tag{1.3}$$

1.4 Euler

The following theorem of Euler completely determines the nature of even perfect numbers by linking their existence to the Mersenne primes.

Theorem 1.4.1 *Any even perfect number is a Euclid number, that is to say of the form* $2^n(2^{n+1}-1)$, *where* $P = 2^{n+1}-1$ *is a prime.*

Example:

$$\begin{aligned} 28 &= 2^2(2^3-1) \\ 496 &= 2^4(2^5-1) \\ 8128 &= 2^6(2^7-1). \end{aligned}$$

Proof. For any even integer N, write $N = 2^n b$, where $n \geq 1$ and $(b,2) = 1$, so that b is odd. Then since $\sigma(N)$ is multiplicative (see Chapter 2), it follows by (1.1) that

$$\begin{aligned} \sigma(N) &= \sigma(2^n b) \\ &= \sigma(2^n)\sigma(b) \\ &= (2^{n+1}-1)\sigma(b). \end{aligned} \tag{1.4}$$

Now assume N is perfect. Then

$$\begin{aligned} \sigma(N) &= 2N \\ &= 2^{n+1}b. \end{aligned} \tag{1.5}$$

Thus, (1.4) and (1.5) imply

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

which can be rewritten as

$$\frac{b}{\sigma(b)} = \frac{2^{n+1} - 1}{2^{n+1}}. \tag{1.6}$$

The fraction on the right-hand side is in reduced form since the numerator is odd while the denominator is a power of two. The fraction on the left-hand side of (1.6) needs to be in reduced form and is the next thing to be shown. Assume that it is not in the reduced form, then there exists an integer c such that

$$b = (2^{n+1} - 1)c \qquad \text{and} \qquad \sigma(b) = 2^{n+1}c. \tag{1.7}$$

If $c > 1$, then b has at least the divisors 1, b, and c. Thus

$$\begin{aligned} \sigma(b) &\geq 1 + c + b \\ &= 1 + c + (2^{n+1} - 1)c \\ &= 1 + 2^{n+1}c \\ &> 2^{n+1}c \\ &= \sigma(b), \end{aligned}$$

which is a contradiction. Hence $c = 1$, so

$$b = 2^{n+1} - 1$$

and

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

Therefore,

$$N = 2^n b = 2^n(2^{n+1} - 1).$$

Any even perfect number must be of the form

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

and

$$\sigma(b) = \sigma(2^{n+1} - 1) = 2^{n+1}. \tag{1.8}$$

was proved.

The next thing to be proved is that $(2^{n+1} - 1)$ is a prime. For if not, then $(2^{n+1} - 1)$ has at least one divisor other than 1 and itself and hence

$$\sigma(b) = \sigma(2^{n+1} - 1) > 1 + (2^{n+1} - 1) = 2^{n+1},$$

which contradicts (1.7). Therefore, $(2^{n+1} - 1)$ must be a prime, and the theorem is proved.

There is a simplier formulation of the result just proved, based on the fact that $2^n - 1$ can never be a prime if n is a composite number. This follows easily from (1.2), since if $n = rs$ with $r \geq 2$ and $s \geq 2$, then

$$\begin{aligned} 2^n - 1 &= 2^{rs} - 1 \\ &= (2^r)^s - 1 \\ &= (2^r - 1)(1 + 2^r + 2^{2r} + \cdots + (2^r)^{s-1}) \end{aligned}$$

which is composite. In conclusion, the only time that $2^n - 1$ can be prime is if $n = p$ a prime. The results on even perfect numbers can be summarized in the following theorem.

Theorem 1.4.2 *The even perfect numbers are precisely the numbers of the form*

$$2^{p-1}(2^p - 1) \tag{1.9}$$

where p is a prime and $2^p - 1$ is also a prime.

1.5 An interesting result on perfect numbers

Theorem 1.5.1 *If you sum the digits of any even perfect number (other than six), then sum the digits of the resulting number, and repeat this process until you get a single digit, that digit will be one.*

Examples.

$$\begin{aligned} 28 &\rightarrow 10 \rightarrow 1 \\ 496 &\rightarrow 19 \rightarrow 10 \rightarrow 1 \\ 8128 &\rightarrow 19 \rightarrow 10 \rightarrow 1 \\ 33,550,336 &\rightarrow 28 \rightarrow 10 \rightarrow 1 \\ 8,589,869,056 &\rightarrow 64 \rightarrow 10 \rightarrow 1 \end{aligned}$$

Proof.

Let $s(n)$ be the sum of the digits of n, where the digits of n in decimal notation are $a_0, a_1, \cdots, a_k$ then,

$$n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k.$$

Since

$$10^1 \equiv 1 (\text{mod } 9)$$

$$10^2 \equiv 1 (\text{mod } 9)$$

$$10^3 \equiv 1 (\text{mod } 9)$$

$$\vdots$$

$$10^k \equiv 1(\text{mod } 9),$$

Also,

$$n \equiv a_0 + a_1 + \cdots + a_k(\text{mod } 9)$$

or

$$a_0 + a_1 + \cdots + a_k \equiv n(\text{mod } 9)$$

or

$$s(n) \equiv n(\text{mod } 9).$$

Thus, this theorem can be proved by showing: perfect numbers are congruent to one modulo nine.

If n is a perfect number, then n has the form $2^{p-1}(2^p - 1)$, where p is prime (see Theorem 1.3.2 in this chapter).

From Euler's Theorem,

$$a^{\phi(n)} \equiv 1(\text{mod n}) \quad \text{if} \quad \gcd(\text{a}, \text{n}) = 1.$$

So

$$2^{\phi(9)} \equiv 1(\text{mod } 9)$$

since

$$\phi(9) = 6,$$

thus

$$2^6 \equiv 1(\text{mod } 9).$$

Hence,

$$2^m \equiv 1(\text{mod } 9) \quad \text{if} \quad m \equiv 0(\text{mod } 6).$$

Case 0. If $p = 2$, then

$$\begin{aligned} 2^{p-1}(2^p - 1) &= 2^{2-1}(2^2 - 1) \\ &= 2(3) \\ &= 6 \equiv 6(\text{mod } 9). \end{aligned}$$

Thus p can not be equal 2.

Case 1. If $p \equiv 1(\text{mod } 6)$, then

$$p - 1 \equiv 0(\text{mod } 6)$$

Thus

$$2^{p-1} \equiv 1(\text{mod } 9), \text{ where } p = 6j + 1, \text{ for some } j \in N.$$

And

$$2^p - 1 = (2^{1+6j} - 1) \equiv (2^1 - 1)(\text{mod } 9)$$

Therefore,

$$2^{p-1}(2^p - 1) \equiv 1(2^1 - 1)(\text{mod } 9) \equiv 1(\text{mod } 9)$$

Case 2. If $p \equiv 3(\text{mod } 6)$, then

$$\begin{aligned} p - 1 &\equiv 2(\text{mod } 6) \\ 2^{p-1} &\equiv 2^2(\text{mod } 9) \end{aligned}$$

$$\equiv 4(\text{mod } 9)$$

$$\text{and} \quad 2^p - 1 \equiv 2^3 - 1(\text{mod } 9)$$

$$\equiv 7(\text{mod } 9)$$

Hence,

$$2^{p-1}(2^p - 1) \equiv 28(\text{mod } 9)$$

$$\equiv 1(\text{mod } 9)$$

Case 3. If $p \equiv 5(\text{mod } 6)$, then

$$p - 1 \equiv 4(\text{mod } 6)$$

$$2^{p-1} \equiv 2^4(\text{mod } 9) \equiv 7(\text{mod } 9)$$

$$2^p \equiv 2^5 \equiv 5(\text{mod } 9)$$

$$2^{p-1} \equiv 4(\text{mod } 9)$$

Hence,

$$2^{p-1}(2^p - 1) \equiv 28(\text{mod } 9) \equiv 1(\text{mod } 9).$$

Chapter 2

Some results on arithmetic functions

2.1 Multiplicative functions

Let n be a positive integer. The divisor function $d(n)$ counts the number of positive integers which divide n (including 1 and n itself). Let $\sigma(n)$ be the sum of positive divisors of n (including 1 and n). In Table 1 below, $d(n)$ and $\sigma(n)$ were evaluated for n in the range from 1 to 10.

n	1	2	3	4	5	6	7	8	9	10
$d(n)$	1	2	2	3	2	4	2	4	3	4
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18

Table 1

Table 1 shows that there are times that $d(mn)$ can be determined from $d(n)$ and $d(m)$, and similarly for $\sigma(mn)$. For example,

$$d(2 \cdot 5) = d(10) = 4 = d(2)d(5)$$

$$d(2 \cdot 3) = d(6) = 4 = d(2)d(3)$$

$$\sigma(2 \cdot 5) = \sigma(10) = 18 = \sigma(2)\sigma(5)$$

$$\sigma(2 \cdot 3) = \sigma(6) = 12 = \sigma(2)\sigma(3).$$

On the other hand, this can not always be done, as the following examples illustrate:

$$d(2 \cdot 4) = d(8) = 4 \neq d(2)d(4) = 2 \cdot 3 = 6$$

$$\sigma(2 \cdot 4) = \sigma(8) = 15 \neq \sigma(2)\sigma(4) = 3 \cdot 7 = 21.$$

In the above examples, it shows that

$$d(mn) = d(m)d(n) \tag{2.1}$$

and

$$\sigma(mn) = \sigma(m)\sigma(n), \tag{2.2}$$

in every case that $\gcd(m, n) = 1$. This can be proved shortly. These examples motivate the following definition.

Definition 2.1 An arithmetical function f is *multiplicative* if f is not identically zero and $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. If $f(mn) = f(m)f(n)$ for all m, n, then f is said to be a *completely multiplicative* function.

One example of a *completely multiplicative function* is $f_r(n) = n^r$.

Theorem 2.1.1 *If f is multiplicative, then f(1)=1.*

Proof. Assuming that f is multiplicative, then

$$f(n) = f(1 \cdot n) = f(1)f(n)$$

since $\gcd(1, n) = 1$, for all n. Since $f(n) \neq 0$ for some n; thus $f(1) = 1$.

Because of the multiplicative property, the evaluation of a multiplicative function f at a positive integer is reduced to that of evaluating f at the prime powers that divide n. Thus, if $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, then

$$f(n) \;=\; f(p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t})$$

$$
\begin{aligned}
&= f(p_1^{a_1})(p_2^{a_2}\cdots p_t^{a_t}) \\
&= f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3}\cdots p_t^{a_t}) \\
&\vdots \\
&= f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3})\cdots f(p_t^{a_t}).
\end{aligned}
$$

The next theorem shows how to construct a new multiplicative function from a known multiplicative function.

Theorem 2.1.2 *Let f be a multiplicative function and suppose*

$$g(n) = \sum_{d|n} f(d). \tag{2.3}$$

Then $g(n)$ is multiplicative.

Proof. Suppose $n \geq 1, m \geq 1$, where $\gcd(m,n) = 1$. The goal is to show that $g(m)g(n) = g(mn)$. First,

$$g(m)g(n) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2). \tag{2.4}$$

If $d_1|m$, $d_2|n$ and $\gcd(m,n) = 1$, then

$$\gcd(d_1, d_2) = 1.$$

Thus by the definition of multiplicative function

$$f(d_1)f(d_2) = f(d_1d_2),$$

and (2.4) becomes

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

Let $d = d_1 d_2$, where d_1, d_2 are positive. If $d_1|m$ and $d_2|n$, then $d = d_1 d_2 | mn$, and every divisor of mn is of this form. Therefore,

$$g(m)g(n) = \sum_{d|mn} f(d) = g(mn),$$

and hence $g(n)$ is multiplicative. As an immediate consequences of Theorem 2.1.2, the next theorem is followed

Theorem 2.1.3 *The functions $d(n)$ and $\sigma(n)$ are multiplicative.*

Proof. The function $f(n) = 1$ for all n is multiplicative and

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

Thus by Theorem 2.1.2 $d(n)$ is multiplicative.

The function $f(n) = n$ is completely multiplicative and

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

Hence, $\sigma(n)$ is also multiplicative.

2.2 Divisors and Sums of Divisors

Definition 2.1 The generalized divisor function $\sigma_\alpha(n)$ for any real (or complex) number α is defined by

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha. \tag{2.5}$$

When $\alpha = 0$, it is easy to see that $d(n) = \sigma_0(n)$ and $\sigma(n) = \sigma_1(n)$.

Theorem 2.2.1 *If the factorization of n into primes is given by*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t},$$

then

$$d(n) = (a_1+1)(a_2+1)(a_3+1)\cdots(a_t+1) = \prod_{i=1}^{t}(a_i+1) \tag{2.6}$$

and

$$\sigma_\alpha(n) = \prod_{i=1}^{t}\left(\frac{p_i^{(a_i+1)\alpha}-1}{p_i^\alpha - 1}\right). \tag{2.7}$$

Proof. If p is a prime and $a \geq 1$, then the divisors of p^a are $1, p, p^2, p^3, \cdots p^a$. Thus $d(p^a) = a+1$. Since $d(n)$ is multiplicative,

$$\begin{aligned} d(n) &= d(p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}) \\ &= d(p_1^{a_1}) d(p_2^{a_2}) \cdots d(p_t^{a_t}) \\ &= (a_1+1)(a_2+1)(a_3+1)\cdots(a_t+1). \end{aligned}$$

Therefore,

$$d(n) = \prod_{i=1}^{t}(a_i+1)$$

which proves (2.6).

Next, $\sigma_\alpha(n)$ is a multiplicative function since it is a divisor sum of the multiplicative function $f(n) = n^\alpha$. Thus

$$\sigma_\alpha(p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}) = \sigma_\alpha(p_1^{a_1})\sigma_\alpha(p_2^{a_2})\cdots\sigma_\alpha(p_t^{a_t}).$$

As before the divisors of p^a are 1, p, $p^2, \cdots, p^a$, and hence by (1.2)

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

Thus

$$\sigma_\alpha(n) = \left(\frac{p_1^{(a_1+1)\alpha}-1}{p_1^\alpha-1}\right)\left(\frac{p_2^{(a_2+1)\alpha}-1}{p_2^\alpha-1}\right)\cdots\left(\frac{p_t^{(a_t+1)\alpha}-1}{p_t^\alpha-1}\right) = \prod_{i=1}^{t}\left(\frac{p_i^{(a_i+1)\alpha}-1}{p_i^\alpha-1}\right)$$

which gives (2.7).

This section is concluded with an inequality for $\sigma(n)$ which can often be used in the arguments in place of (2.7) and does not depend on the powers of the primes that divide n.

Lemma 2.1. For $n \geq 2$,

$$\frac{n}{\sigma(n)} > \prod_{p|n}\left(1-\frac{1}{p}\right). \tag{2.8}$$

Proof. The notation $a^m \parallel b$ means that $a^m|b$ but $a^{m+1} \not| b$.

$$\begin{aligned}\frac{n}{\sigma(n)} &= \prod_{p^m\parallel n}\frac{p^m}{\sigma(p^m)} \\ &= \prod_{p^m\parallel n}\frac{p^m}{\frac{p^{m+1}-1}{p-1}}\end{aligned}$$

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

Note that the product on the right-hand side of (2.8) is actually $\phi(n)/n$, where $\phi(n)$ is the Euler phi function which equals the number of numbers less than or equal to n and relatively prime to n.

Chapter 3

Odd Perfect Numbers Have at Least 4 Distinct Prime Factors

This chapter will prove that odd perfect numbers, if they exist, must have at least 4 distinct prime factors. This result was first proved by James Sylvester in 1888. The best current result of this type replaces 4 by 8. Heath-Brown's theorem in the next chapter shows that all theorems of this type can be obtained through a finite search. In the first two sections, it will be proved that an odd perfect number cannot have one or two distinct prime factors. These proofs were proceeded from scratch to demonstrate how one would first approach this problem. In the third section, a general result of Euler on odd perfect numbers that simplifies the cases that need to be considered will be proved. In the last section, this result will be applied to prove that no odd perfect number has three distinct prime factors.

3.1 The case of one prime factor

Let $n \geq 3$ be an odd perfect number that has only one prime factor.

Case 1. If $n = p$, then

$$\sigma(n) = \sigma(p) = 1 + p,$$

while since n is perfect, it follows that

$$\sigma(n) = \sigma(p) = 2p.$$

Thus

$$1 + p = 2p$$

which implies $p = 1$, which contradicts both the fact that $p \geq 3$, and that p is a prime.

Case 2. If $n = p^2$, then

$$\sigma(n) = \sigma(p^2) = 1 + p + p^2,$$

while since n is perfect, it follows that

$$\sigma(n) = \sigma(p^2) = 2p^2.$$

Thus

$$1 + p + p^2 = 2p^2,$$

which implies $1 + p = p^2$ or

$$p(p - 1) = 1,$$

which is impossible since $p \geq 3$.

Case 3. If $n = p^m$, where $m > 2$, then

$$\sigma(n) = \sigma(p^m) = 1 + p + p^2 + \cdots p^m,$$

while since n is perfect , it follows that

$$\sigma(n) = \sigma(p^m) = 2p^m.$$

Thus

$$1 + p + p^2 + \cdots + p^{m-1} = p^m$$

or

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

Therefore $p|1$ which is impossible.

3.2 The case of two prime factors

Let n be an odd perfect number that has two distinct prime factors. Then

$$\sigma(n) = 2n. \tag{3.1}$$

Consider the special case of $n = pq$ before doing the general case when $n = p^a q^b$.

Case 1. If $n = pq$, where $\gcd(p, q) = 1$, then

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

and thus by (3.1)

$$(1 + p)(1 + q) = 2pq. \tag{3.2}$$

Simplifying gives

$$\begin{aligned} 1 + p + q + pq &= 2pq, \\ 1 + p + q &= pq, \\ \frac{1}{pq} + \frac{1}{q} + \frac{1}{p} &= 1. \end{aligned} \tag{3.3}$$

Since $p, q \geq 3$, implies

$$\frac{1}{pq} \leq \frac{1}{3} \cdot \frac{1}{3} = \frac{1}{9}$$

which gives

$$\begin{aligned} \frac{1}{pq} + \frac{1}{q} + \frac{1}{p} &\leq \frac{1}{9} + \frac{1}{3} + \frac{1}{3} \\ &= \frac{7}{9} \\ &< 1 \end{aligned}$$

contradicting (3.3).

A second method to see that (3.2) is impossible is to consider the prime factorization implied by this relation. Since p does not divide $(1 + p)$, it follows that

$$p|(1 + q)$$

and similarly q does not divide $1 + q$, so

$$q|(1 + p).$$

But since $p \neq q$, either

$$p \geq 2 + q$$

or

$$q \geq 2 + p$$

which contradicts either

$$p|1 + q$$

or

$$q|(1+p).$$

A third method to show that (3.2) is false is simply to note that since p and q are odd, the left-hand side of (3.2) is divisible by 4 but the right hand side is not divisible by 4. This method will be used again in the next section to prove a more general result.

Case 2. The General Case: If $n = p^a q^b$, where $\gcd(p,q) = 1$, then

$$\begin{aligned}
\sigma(n) &= \sigma(p^a q^b) \\
&= \sigma(p^a)\sigma(q^b) \\
&= \left(\frac{p^{a+1}-1}{p-1}\right)\left(\frac{q^{b+1}-1}{q-1}\right) \\
&= \frac{p^{a+1}q^{b+1} - p^{a+1} - q^{b+1} + 1}{(p-1)(q-1)} \\
&= \frac{pqp^a q^b}{(p-1)(q-1)} - \frac{p^{a+1}}{(p-1)(q-1)} - \frac{q^{b+1}}{(p-1)(q-1)} + \frac{1}{(p-1)(q-1)} \\
&= \frac{pq}{(p-1)(q-1)}n - \frac{p^{a+1}}{(p-1)(q-1)} - \frac{1}{(p-1)(q-1)}(q^{b+1}-1) \\
&< \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)n. \qquad (3.4)
\end{aligned}$$

This last equation is actually just a special case of Lemma 2.1. If n is a perfect number then $\sigma(n) = 2n$, and this will be impossible by (3.4) when

$$\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right) < 2. \qquad (3.5)$$

The function $f(x) = \frac{x}{x-1}$ is a decreasing function for $x > 1$ since its derivative is $-(x-1)^{-2} < 0$. Since $p \geq 3$ and $q \geq 5$ (on taking p to be the smaller of the two

distinct primes), hence

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

so that (3.5) is satisfied and therefore n is not perfect.

The simplicity of the above argument might suggest that one can easily proceed to more prime factors. The problem that arises is that the analogue of (3.4) no longer produces a factor less than 2 when small prime factors occur. These small prime factors require separate arguments which become increasingly complicated. This occurs in the case of 3 distinct prime factors and will appear in section 3.4.

3.3 A Result of Euler on Odd Perfect Numbers

Now consider the prime factorization of an odd perfect number. In section 3.1 a proof (the third method) based on the main idea that will be used here. That idea is that $\sigma(n)$ is divisible by 2 but not by 4, and this will impose conditions on the factorization of n through equation (2.7). The simplest result of this type is that a square-free number can not be an odd perfect number. To see this, notice that if n is square free then $n = p_1 p_2 \dots p_t$ with distinct primes, and thus

$$\sigma(n) = (p_1 + 1)(p_2 + 1) \dots (p_t + 1).$$

This expression is a product of t even numbers, and thus is divisible by 2^t, which contradicts $4 \not| \sigma(n)$ unless $t = 1$, and $t = 1$ was eliminated in section 3.1. Here is a general result of Euler and its proof.

Theorem 3.3.1 *If n is an odd perfect number, then $n = p^a s^2$ where p is a prime,* $\gcd(p, s) = 1$, *and*

$$p \equiv 1 (\text{mod } 4), \qquad \text{and} \qquad a \equiv 1 (\text{mod } 4).$$

Proof. Let n be an odd perfect number, where $n = \prod_{i=1}^{t} p_i^{a_i}$. Then $\sigma(n) = 2n$, and since n is odd, $2 \parallel \sigma(n)$, or equivalently,

$$\sigma(n) \equiv 2 (\text{mod } 4).$$

Since σ is multiplicative,

$$\sigma(n) \;=\; \sigma(p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t})$$

$$= \sigma(p_1^{a_1})\sigma(p_2^{a_2})\cdots\sigma(p_t^{a_t}).$$

Hence

$$\sigma(p_1^{a_1})\sigma(p_2^{a_2})\cdots\sigma(p_t^{a_t}) \equiv 2(\text{mod } 4). \tag{3.6}$$

From this equation one can see that precisely one of the factors on the left must be divisible by 2 (but not 4) and thus there exists a unique p with $p^a \parallel n$ and

$$\sigma(p^a) \equiv 2(\text{mod } 4). \tag{3.7}$$

Since p is odd, it must be congruent to either 1 or 3 modulo 4. But if $p \equiv 3(\text{mod } 4)$, then

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

which contradicts (3.7). Hence $p \equiv 1(\text{mod } 4)$ as stated in Theorem 3.3.1. With $p \equiv 1(\text{mod } 4)$, it follows that

$$\begin{aligned}
\sigma(p^a) &= 1 + p^1 + p^2 + p^3 + \cdots + p^a \\
&\equiv \underbrace{1 + 1 + 1 + \cdots + 1}_{(a+1) \text{ terms}}(\text{mod } 4) \\
&\equiv (a + 1) \text{ (mod } 4)
\end{aligned}$$

which implies by (3.7) that $a \equiv 1(\text{mod } 4)$.

It remains to show that $n = p^a s^2$. Let $n = mp^a$. Then, by multiplicativity and (3.6)

$$\sigma(n) = \sigma(m)\sigma(p^a) \equiv 2(\text{mod } 4), \tag{3.8}$$

which by (3.7) implies $\sigma(m)$ is odd. Suppose q is an odd prime such that $q^b \| m$. Then $\sigma(q^b)$ is also odd by multiplicativity. Now either

$$q \equiv 1 (\text{mod } 4)$$

or

$$q \equiv 3 (\text{mod } 4).$$

Two cases below will show that b must be even.

Case 1. If $q \equiv 1 (\text{mod } 4)$, then

$$\begin{aligned} \sigma(q^b) &= 1 + q^1 + q^2 + \cdots + q^b \\ &\equiv \underbrace{1 + 1 + 1 + \cdots + 1}_{(b+1) \text{ terms}} (\text{mod } 4) \\ &\equiv (1 + b) (\text{mod } 4). \end{aligned}$$

Thus $(1 + b)$ must be odd and so b must be even.

Case 2. If $q \equiv 3 (\text{mod } 4)$, then

$$\begin{aligned} \sigma(q^b) &= 1 + q + q^2 + \cdots + q^b \\ &= \underbrace{1 + 3 + 1 + 3 + \cdots + 1}_{(b+1) \text{ terms}} (\text{mod } 4) \end{aligned}$$

which is odd only when b is even.

Therefore, in either case, b must be even. Since this argument applies for every prime dividing m, thus

$$m = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$$

$$= (q_1^{c_1} q_2^{c_2} \cdots q_r^{c_r})^2$$

$$= s^2,$$

where since each b_i is even, it is true that $b_i = 2c_i$.

3.4 The case of three prime factors

Let $n = p^a q^b r^c$ be an odd perfect number that has three prime factors, and assume $p < q < r$. Then by Lemma 2.1

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

and therefore in this case, it is true that

$$\sigma(n) < \left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)\left(\frac{r}{r-1}\right)n. \tag{3.9}$$

Thus n can not be perfect when

$$\left(\frac{p}{p-1}\right)\left(\frac{q}{q-1}\right)\left(\frac{r}{r-1}\right) < 2. \tag{3.10}$$

As in section 2 each factor in (3.10) is a decreasing function. First consider the case that p and q are as small as possible. Then $p \geq 3$, $q \geq 5$, and thus (3.10) holds if

$$\left(\frac{3}{2}\right)\left(\frac{5}{4}\right)\left(\frac{r}{r-1}\right) < 2$$

which simplifies to

$$\frac{15}{16} < 1 - \frac{1}{r}$$

which gives

$$\frac{1}{r} < \frac{1}{16}$$

and thus

$$r > 16.$$

Therefore (3.10) holds and n is not perfect if

$$p \geq 3, \quad q \geq 5, \quad r \geq 17. \tag{3.11}$$

Next, consider when $p \geq 3$, $q \geq 7$ and $r \geq 11$ which when substituted into (3.10) gives

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

and hence (3.10) holds and n can not be perfect for

$$p \geq 3 \quad q \geq 7 \quad r \geq 11. \tag{3.12}$$

On combining (3.11) and (3.12), the cases left to be considered are the sets of primes $\{3,5,7\}$, $\{3,5,11\}$, and $\{3,5,13\}$. In place of Theorem 3.3.1 which fails to handle these cases, so to take account of the powers of these primes is a need. Thus,

$$\begin{aligned} \sigma(n) &= \sigma(3^a)\sigma(5^b)\sigma(r^c) \\ &= \left(\frac{3^{a+1}-1}{2}\right)\left(\frac{5^{b+1}-1}{4}\right)\left(\frac{r^{c+1}-1}{r-1}\right), \end{aligned} \tag{3.13}$$

while if n is perfect then

$$\sigma(n) = 2n = 2(3^a 5^b r^c). \tag{3.14}$$

Combining (3.13) and (3.14) and simplifying gives that if n is perfect then

$$\left(3-\frac{1}{3^a}\right)\left(5-\frac{1}{5^b}\right)\left(\frac{r-\frac{1}{r^c}}{r-1}\right) = 16. \tag{3.15}$$

Now proceed to deal with three cases separately.

Case 1. Suppose $p = 3$, $q = 5$ and $r = 7$ and thus $n = 3^a 5^b 7^c$. Substituting into (3.15) and simplifying gives

$$\left(3 - \frac{1}{3^a}\right)\left(5 - \frac{1}{5^b}\right)\left(7 - \frac{1}{7^c}\right) = 96. \tag{3.16}$$

Since of the primes 3, 5, and 7 only $5 \equiv 1 (\mathrm{mod}\ 4)$, by Theorem 3.3.1, both 3^a and 7^c must be squares, and hence a and c are even, which in particular imply that

$$a \geq 2, \quad c \geq 2.$$

Using these and the trivial $b \geq 1$ it shows that the left-hand side of (3.16) is

$$\geq \left(3 - \frac{1}{3^2}\right)\left(5 - \frac{1}{5}\right)\left(7 - \frac{1}{7^2}\right) = \frac{26}{9}\frac{24}{5}\frac{242}{49} = 96.7836\ldots > 96$$

which contradicts (3.16)

Case 2. Suppose $p = 3$, $q = 5$, and $r = 11$, and thus $n = 3^a 5^b 11^c$ where a and c must be even by Theorem 3.3.1 as in Case 1. If the inequalities $a \geq 2$, $b \geq 1$, and $c \geq 2$ were used as in Case 1, a contradiction to (3.15) can not be seen. To solve this problem, first show that

$$a \geq 4.$$

To see this, notice by multiplicativity

$$\sigma(n) = \sigma(3^a 5^b 11^c) = \sigma(3^a)\sigma(5^b)\sigma(11^c)$$

and so

$$\sigma(3^a) | \sigma(n) = 2(3^a 5^b 11^c)$$

since n is perfect. But if $a = 2$ then

$$\sigma(3^2) = 1 + 3 + 3^2 = 13$$

which does not divide $2(3^a 5^b 11^c)$. Therefore $a \neq 2$ and since a is even $a \geq 4$.

Now consider two sub cases: $b = 1$ and $b \geq 2$. First, if $b \geq 2$, then with $a \geq 4$ and $c \geq 2$ the left-hand side of (3.15) is

$$\geq \left(3 - \frac{1}{3^4}\right)\left(5 - \frac{1}{5^2}\right)\left(\frac{11 - \frac{1}{11^2}}{10}\right) = \frac{242}{81}\frac{124}{25}\frac{133}{121} = 16.28839\ldots > 16,$$

which is a contradiction. Next, if $b = 1$ by (3.15) that

$$\left(3 - \frac{1}{3^a}\right)\left(5 - \frac{1}{5^1}\right)\left(11 - \frac{1}{11^c}\right) = 160$$

which implies

$$\left(3 - \frac{1}{3^a}\right)\left(11 - \frac{1}{11^c}\right) = \frac{100}{3} > 33$$

which is impossible since

$$\left(3 - \frac{1}{3^a}\right)\left(11 - \frac{1}{11^c}\right) < 3 \cdot 11 = 33.$$

Case 3. Suppose $p = 3$, $q = 5$, and $r = 13$, and thus $n = 3^a 5^b 13^c$. By Theorem 3.3.1, a is even since $3 \not\equiv 1 (\text{mod } 4)$. Suppose $c \geq 2$. If not, then by multiplicativity

$$\sigma(n) = \sigma(3^a 5^b 13^c) = \sigma(3^a)\sigma(5^b)\sigma(13^c),$$

which since

$$\sigma(13^1) = 1 + 13 = 14$$

implies that

$$7|\sigma(n) = 2(3^a 5^b 13^c)$$

which is impossible. Hence $c \geq 2$.

Thus $a \geq 2$, a even, $b \geq 1$, and $c \geq 2$. Divide these into three sub cases: i) $a \geq 4$, $b \geq 2$, and $c \geq 2$, ii) $a \geq 4$, $b = 1$, $c \geq 2$, and iii) $a = 2$, $b \geq 1$, and $c \geq 2$. Let $r = 13$ in (3.15) in order to obtain

$$\left(3 - \frac{1}{3^a}\right)\left(5 - \frac{1}{5^b}\right)\left(13 - \frac{1}{13^c}\right) = 192. \tag{3.17}$$

i) Suppose $a \geq 4$, $b \geq 2$, and $c \geq 2$. Then the left-hand side of (3.17) is

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

which exceeds the right-hand side of (3.17).

ii) If $a \geq 4$, $b = 1$, and $c \geq 2$ then (3.17) becomes

$$\left(3 - \frac{1}{3^a}\right)\left(13 - \frac{1}{13^c}\right) = 40,$$

which is impossible since the left-hand side is < 39.

iii) If $a = 2$, $b \geq 1$, $c \geq 2$, then (3.17) becomes

$$\left(5 - \frac{1}{5^b}\right)\left(13 - \frac{1}{13^c}\right) = \frac{864}{13} = 66.461\ldots,$$

which is impossible since the left-hand side is < 65.

Chapter 4

Heath-Brown's Lemma 1

Heath-Brown's Lemma 1

Let r be a positive integer and let $n_1, \cdots, n_r$ be integers such that $1 < n_1 < \cdots < n_r$. Suppose that $\frac{a}{b}$ is a rational number in the range

$$\prod_{i=1}^{r}(1 - \frac{1}{n_i}) \leq \frac{a}{b} < \prod_{i=1}^{r-1}(1 - \frac{1}{n_i}). \tag{4.1}$$

Then

$$\prod_{i=1}^{r} n_i \leq (4a)^{2^r - 1}.$$

Before proving Heath-Brown's Lemma 1, the following lemmas are needed:

Lemma 4.1

If $0 \leq a_i \leq 1$, then

$$\prod_{i=1}^{r}(1 - a_i) \geq 1 - \sum_{i=1}^{r} a_i.$$

Proof. (By induction on r.)

If $r = 1$, then $1 - a_1 \geq 1 - a_1$, so the lemma is true for the case $r = 1$.

Now assuming the lemma is true for the case $r = k - 1$, so

$$\prod_{i=1}^{k-1}(1 - a_i) \geq 1 - \sum_{i=1}^{k-1} a_i,$$

and then

$$\begin{aligned}
\prod_{i=1}^{k}(1 - a_i) &= \left(\prod_{i=1}^{k-1}(1 - a_i)\right)(1 - a_k) \\
&\geq \left(1 - \sum_{i=1}^{k-1} a_i\right)(1 - a_k) \\
&= 1 - \sum_{i=1}^{k-1} a_i - a_k + a_k \sum_{i=1}^{k-1} a_i
\end{aligned}$$

$$= 1 - \sum_{i=1}^{k} a_i + a_k \sum_{i=1}^{k-1} a_i$$
$$\geq 1 - \sum_{i=1}^{k} a_i.$$

Lemma 4.2

For any positive integer k, it is true that $k + 1 \leq 2^k$.

Proof. (By induction on k)

For $k = 1$,

$$1 + 1 = 2 = 2^1.$$

Thus the lemma is true for the case $k = 1$.

Now assume it is true for the case $k = r - 1$, so that

$$r - 1 + 1 = r \leq 2^{r-1}.$$

Then

$$r \leq \frac{2^r}{2}$$

or

$$r + 1 \leq 2r \leq 2^r,$$

and so

$$r + 1 \leq 2^r$$

is also true.

Lemma 4.3

For any positive integer k, it is true that $1 + \frac{k(k+1)}{2} \leq 2^k$.

Proof.

If $k = 1$, then

$$1 + \frac{1(1+1)}{2} = 2$$

and the lemma is true for $k = 1$. Now assume $k = r - 1$ is true. Then

$$1 + \frac{(r-1)r}{2} \leq 2^{r-1}.$$

Now if $k = r$ then

$$\begin{aligned} 1 + \frac{r(r+1)}{2} &= \left(1 + \frac{(r-1)r}{2}\right) + r \\ &\leq 2^{r-1} + r \\ &\leq 2^{r-1} + 2^{r-1} \\ &= 2(2^{r-1}) \\ &= 2^r, \end{aligned}$$

where Lemma 4.2 was used.

Proof of Heath-Brown's lemma 1: (By induction on r.)

When $r = 1$, (4.1) implies

$$1 - \frac{1}{n_1} \leq \frac{a}{b} < 1,$$

and using the right-hand inequality gives $a < b$. Since a and b are both integers, it is true that

$$a + 1 \leq b,$$

hence,

$$\frac{1}{b} \leq \frac{1}{a+1}$$

or

$$\frac{a}{b} \leq \frac{a}{a+1}.$$

Thus

$$1 - \frac{1}{n_1} \leq \frac{a}{b} \leq \frac{a}{a+1}$$

Therefore, if

$$1 - \frac{1}{n_1} \leq \frac{a}{a+1}$$

then

$$1 - \frac{1}{n_1} \leq \frac{a+1}{a+1} - \frac{1}{a+1} = 1 - \frac{1}{a+1}$$

or

$$\frac{-1}{n_1} \leq \frac{-1}{a+1}$$

which gives

$$\frac{1}{n_1} \geq \frac{1}{a+1}$$

or

$$n_1 \leq a+1 \leq 4a = (4a)^{2^1-1}.$$

Thus the case $r = 1$ is true. For the induction step, suppose that some integer n_i must satisfy

$$n_i \leq 2^{i+1}a. \tag{4.2}$$

Assume on the contrary that $n_i > 2^{i+1}a$ for every i. From (4.1)

$$\prod_{i=1}^{r}(1 - \frac{1}{n_i}) \leq \frac{a}{b} < \prod_{i=1}^{r-1}(1 - \frac{1}{n_i}) \leq 1.$$

It follows that $a < b$, hence $a + 1 \leq b$ so that

$$\frac{a}{a+1} \geq \frac{a}{b} \geq \prod_{i=1}^{r}(1 - \frac{1}{n_i}).$$

By lemma 4.1

$$\frac{a}{a+1} \geq \frac{a}{b} \geq \prod_{i=1}^{r}(1 - \frac{1}{n_i}) > 1 - \sum_{i=1}^{n}\frac{1}{n_i}.$$

From the assumption

$$n_i > 2^{i+1}a,$$

which gives

$$\frac{1}{n_i} < \frac{1}{2^{i+1}a}$$

and thus,

$$1 - \frac{1}{n_i} > 1 - \frac{1}{2^{i+1}a}.$$

Hence,

$$\frac{a}{a+1} > 1 - \sum_{i=1}^{n}\frac{1}{n_i} > 1 - \sum_{i=1}^{\infty}\frac{1}{2^{i+1}a} = 1 - \frac{1}{2a}$$

since $\sum_{i=1}^{\infty}\frac{1}{2^{i+1}}$ is a geometric series which converges to $\frac{1}{2}$ Thus,

$$\frac{a}{a+1} > 1 - \frac{1}{2a}$$

which implies

$$\frac{a}{a+1} > \frac{2a-1}{2a}$$

or

$$2a^2 > (2a-1)(a+1)$$

$$\begin{aligned} 2a^2 &> 2a^2 + a - 1 \\ -a &> -1 \\ a &< 1 \\ 2a &< a + 1. \end{aligned}$$

This is a contradiction since $2a \geq 1 + a$.

Now take k to be the smallest integer i for which $n_i \leq 2^{i+1}a$ holds. Thus

$$n_1 n_2 \cdots n_k \leq n_k^k \leq (2^{k+1}a)^k \tag{4.3}$$

and if $r = k$, then

$$\prod_{i=1}^{r} n_i \leq (2^{r+1}a)^r. \tag{4.4}$$

Next, if $1 \leq k \leq r-1$, then $\frac{a}{b}$ is a rational number in the range

$$\prod_{i=1}^{r}\left(1 - \frac{1}{n_i}\right) \leq \frac{a}{b} < \prod_{i=1}^{r-1}\left(1 - \frac{1}{n_i}\right),$$

which is equivalent to

$$\prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right)\prod_{i=k+1}^{r}\left(1 - \frac{1}{n_i}\right) \leq \frac{a}{b} < \prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right)\prod_{i=k+1}^{r-1}\left(1 - \frac{1}{n_i}\right).$$

It follows that

$$\prod_{i=k+1}^{r}\left(1 - \frac{1}{n_i}\right) \leq \frac{\frac{a}{b}}{\prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right)} < \prod_{i=k+1}^{r-1}\left(1 - \frac{1}{n_i}\right).$$

But

$$\frac{1}{\prod_{i=1}^{k}\left(1 - \frac{1}{n_i}\right)} = \frac{1}{(1 - \frac{1}{n_1})(1 - \frac{1}{n_2})\cdots(1 - \frac{1}{n_k})}$$

$$= \frac{n_1 n_2 \cdots n_k}{n_1 n_2 \cdots n_k (1-\frac{1}{n_1})(1-\frac{1}{n_2})\cdots(1-\frac{1}{n_k})}$$
$$= \frac{\prod_{i=1}^{k} n_i}{\prod_{i=1}^{k}(n_k-1)},$$

and hence

$$\frac{\frac{a}{b}}{\prod_{i=1}^{k}\left(1-\frac{1}{n_i}\right)} = \frac{a}{b}\cdot\frac{\prod_{i=1}^{k} n_i}{\prod_{i=1}^{k}(n_k-1)}.$$

Let

$$\frac{a'}{b'} = \frac{a\prod_{i=1}^{k} n_i}{b\prod_{i=1}^{k}(n_k-1)}.$$

If $1 \le k \le r-1$, then

$$\prod_{i=k+1}^{r}\left(1-\frac{1}{n_i}\right) \le \frac{a'}{b'} < \prod_{i=k+1}^{r-1}\left(1-\frac{1}{n_i}\right).$$

It therefore follows from the induction assumption that

$$\prod_{i=k+1}^{r-1} n_i \le (4a')^{2^{r-k}-1} = (4a\prod_{i=1}^{k} n_i)^{2^{r-k}-1}$$
$$= (4a)^{2^{r-k}-1}(\prod_{i=1}^{k} n_i)^{2^{r-k}-1}$$
$$= (4a)^{2^{r-k}-1}(\prod_{i=1}^{k} n_i)^{2^{r-k}}(\prod_{i=1}^{k} n_i)^{-1}.$$

Thus

$$(\prod_{i=k+1}^{r-1} n_i)(\prod_{i=1}^{k} n_i) \le (4a)^{2^{r-k}-1}(\prod_{i=1}^{k} n_i)^{2^{r-k}}, \quad \text{which implies}$$
$$\prod_{i=1}^{r} n_i \le (4a)^{2^{r-k}-1}(\prod_{i=1}^{k} n_i)^{2^{r-k}},$$

and by (4.3)

$$\prod_{i=1}^{r} n_i \le (4a)^{2^{r-k}-1}(2^{k+1}a)^{k(2^{r-k})}.$$

This estimate also holds when $k = r$ by (4.4).

To complete the induction, it is necessary to have

$$\prod_{i=1}^{r} n_i \leq (4)^{2^r-1} a^{2^r-1} = (4a)^{2^r-1}.$$

Therefore, if

$$(4^{2^{r-k}-1}) \left(2^{k(k+1)2^{r-k}}\right) \leq 4^{2^r-1} \tag{4.5}$$

and

$$a^{2^{r-k}-1} a^{k2^{r-k}} \leq a^{2^r-1}, \tag{4.6}$$

can be shown then the proof is completed.

Proof of (4.5): Since

$$\begin{aligned} (4^{2^{r-k}-1}) \left(2^{k(k+1)2^{r-k}}\right) &= 2^{2(2^{r-k}-1)} 2^{k(k+1)2^{r-k}} \\ &= 2^{(2^{r-k+1}-2)} 2^{k(k+1)2^{r-k}}. \end{aligned}$$

By Lemma 4.3, this last expression is $\leq 2^{(2^{r-k+1}-2)} 2^{(2^{k+1}-2)2^{r-k}}$.

$$\begin{aligned} &= 2^{(2^{r-k+1}-2)+2^{r+1}-2^{r-k+1}} \\ &= 2^{2^{r+1}-2} \\ &= 2^{2(2^r-1)} \\ &= 4^{2^r-1}. \end{aligned}$$

Proof of (4.6):

Lemma 4.2 $k + 1 \leq 2^k$, gives

$$a^{(2^{r-k}-1)} a^{k2^{r-k}} = a^{(2^{r-k}-1)+k2^{r-k}}$$

$$= a^{2^{r-k}(1+k)-1}$$

$$\leq a^{2^{r-k}2^k-1}$$

$$= a^{2^r-1}.$$

Chapter 5

Heath-Brown's Lemma 2

Heath Brown's Lemma 2:

Let $N \geq 3$ be an odd number divisible by a set S of primes, and suppose that

$$\frac{\sigma(N)}{N} = \frac{n}{d} > 1.$$

Then N is the product of two coprime factors U and V with the following properties.

(i) $\omega(V) = v$ is at least 1.

(ii) U is divisible by a set T of primes, where $v + \#T - \#S = w$ is non-negative.

(iii) $\frac{\sigma(U)}{U} = \frac{\nu}{\delta}$, with $d\sigma(V)|\delta$.

(iv) $4\delta \prod(T) \leq (4d \prod(S))^{2^{v+w}}$.

Proof.

Let $\prod(S) = \prod_{p \in S} p$.

If S is the empty set,

$$\prod_{p \in S} \left(1 - \frac{1}{p}\right) = 1.$$

If S is not the empty set and since $2 \notin S$, then

$$\prod_{p \in S} \left(1 - \frac{1}{p}\right) = \prod_{p \in S} \left(\frac{p-1}{p}\right)$$

is a product of even numbers divided by a product of odd numbers and therefore has even numerator when written as a fraction in lowest terms. On the other hand $\frac{d}{n} = \frac{N}{\sigma(N)}$ is less than 1 since N is less than $\sigma(N)$, and $\frac{N}{\sigma(N)} = \frac{odd}{\sigma(N)}$ has odd numerator when written as a fraction in lowest terms, since reducing a fraction to lowest terms does not change an odd numerator to an even one. It follows that

$$\prod_{p \in S} \left(1 - \frac{1}{p}\right) \neq \frac{d}{n}.$$

Case 1.

$$\prod_{p\in S}\left(1-\frac{1}{p}\right) > \frac{d}{n}. \tag{5.1}$$

In this case, first construct a non empty set S' of primes which is disjoint from S and also dividing N. By lemma 2.1

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

Dividing out the contribution to the product of the primes in S, one obtains

$$\begin{aligned}\frac{\prod_{p|N}(1-\frac{1}{p})}{\prod_{p\in S}(1-\frac{1}{p})} &= \prod_{p|N,p\notin S}\left(1-\frac{1}{p}\right)\\ &< \frac{\frac{d}{n}}{\prod_{p\in S}(1-\frac{1}{p})}\\ &< 1,\end{aligned}$$

since $\prod_{p\in S}(1-\frac{1}{p}) > \frac{d}{n}$.

Thus

$$\prod_{p|N,p\notin S}\left(1-\frac{1}{p}\right) < \frac{d\prod_{p\in S}p}{n\prod_{p\in S}(p-1)} = \frac{d'}{n'} < 1,$$

where

$$d' = d\prod_{p\in S}p = d\prod(S), \text{and} \quad n' = n\prod_{p\in S}(p-1) \tag{5.2}$$

Since $\prod_{p|N,p\notin S}(1-\frac{1}{p}) < 1$, the product is not empty and therefore the set of primes $p|N$ and $p \notin S$ is not the empty set. Some elements in this set are selected to

construct a subset $S' = \{p_1, p_2, p_3, \cdots, p_w\}$ with the properties that

$$\prod_{i=1}^{w} \left(1 - \frac{1}{p_i}\right) \leq \frac{d'}{n'} < \prod_{i=1}^{w-1} \left(1 - \frac{1}{p_i}\right). \tag{5.3}$$

First, pick a prime p_1 such that $p_1|N$ and $p_1 \notin S$. Then either

$$\left(1 - \frac{1}{p_1}\right) \leq \frac{d'}{n'} < 1$$

or else

$$\frac{d'}{n'} < \left(1 - \frac{1}{p_1}\right).$$

If the first situation holds, take $S' = \{p_1\}$ and the proof is completed. Otherwise, the set $p|N, p \notin S, p \neq p_1$, is not empty, and a second prime p_2 is picked from this set. Then

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) < \left(1 - \frac{1}{p_1}\right)$$

and either

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) < \frac{d'}{n'}$$

or else

$$\frac{d'}{n'} < \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).$$

In the first case, take $S' = \{p_1, p_2\}, w = 2$ and have

$$\prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right) \leq \frac{d'}{n'} < \prod_{i=1}^{1} \left(1 - \frac{1}{p_i}\right) = \left(1 - \frac{1}{p_1}\right).$$

Otherwise, a third prime p_3 is picked as before, let $S' = \{p_1, p_2, p_3\}$, so that

$$\prod_{i=1}^{w=3} \left(1 - \frac{1}{p_i}\right) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) < \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

and either

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right) < \frac{d'}{n'}$$

or else

$$\frac{d'}{n'} < \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right).$$

Again, in the first case

$$\prod_{i=1}^{3}\left(1-\frac{1}{p_i}\right) \leq \frac{d'}{n'} < \prod_{i=1}^{2}\left(1-\frac{1}{p_i}\right) = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right).$$

Otherwise, take $S' = \{p_1, p_2, p_3, p_4\}$ and keep repeating on this process. At the k^{th} stage,

$$\frac{d'}{n'} < \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

But if m is the number of primes $p|N$ and $p \notin S$, then

$$\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right) = \prod_{p|N, p\notin S}\left(1-\frac{1}{p_i}\right) < \frac{d'}{n'}$$

and hence $k < m$. Thus, there is some w where

$$\prod_{i=1}^{w}\left(1-\frac{1}{p_i}\right) \leq \frac{d'}{n'} < \prod_{i=1}^{w-1}\left(1-\frac{1}{p_i}\right)$$

for $S' = \{p_1, p_2, \cdots, p_w\}, p_i|N$, and $S \cap S' = \emptyset$.

Thus by Heath-Brown's Lemma 1,

$$\prod_{i=1}^{w} p_i = \prod(S') \leq (4d')^{2^w - 1}$$

and hence by (5.2)

$$\prod(S' \cup S) \;=\; \prod(S')\prod(S)$$

$$\begin{aligned} &\leq (4d')^{2^w-1} \prod(S) \\ &= \left(4d \prod(S)\right)^{2^w-1} \prod(S) \\ &= (4d)^{2^w-1} \prod(S)^{2^w}. \end{aligned} \tag{5.4}$$

Moreover

$$\prod_{i=1}^{w} \left(1 - \frac{1}{p_i}\right) \leq \frac{d'}{n'}$$

implies

$$\prod_{p \in S'} \left(1 - \frac{1}{p}\right) \prod_{p \in S} \left(1 - \frac{1}{p}\right) \leq \frac{d'}{n'} \prod_{p \in S} \left(1 - \frac{1}{p}\right)$$

and thus

$$\begin{aligned} \prod_{p \in (S \cup S')} \left(1 - \frac{1}{p}\right) &\leq \frac{d \prod_{p \in S} p}{n \prod_{p \in S} (p-1)} \prod_{p \in S} \left(1 - \frac{1}{p}\right) \\ &= \frac{d}{n} \prod_{p \in S} \left(\frac{p}{p-1}\right) \prod_{p \in S} \left(\frac{p-1}{p}\right) \\ &= \frac{d}{n}. \end{aligned}$$

Equality is not allowed here, since as before, d is odd but the product has an even numerator. Hence

$$\prod_{p \in (S \cup S')} \left(1 - \frac{1}{p}\right) < \frac{d}{n}. \tag{5.5}$$

Case 2.

Suppose

$$\prod_{p \in S} \left(1 - \frac{1}{p}\right) < \frac{d}{n}.$$

(5.4) and (5.5) must hold in this case, which will be shown by taking $S' = \emptyset, w = 0$.

If $S' = \emptyset, w = 0$, with these choices, (5.4) holds trivially because

$$\begin{aligned} \prod(S \cup S') &= \prod(S) \\ &\leq (4d)^{2^0 - 1} \prod(S)^{2^0} \\ &= \prod(S). \end{aligned}$$

Further (5.5) holds because

$$\prod_{p \in (S \cup S')} \left(1 - \frac{1}{p}\right) = \prod_{p \in S} \left(1 - \frac{1}{p}\right) < \frac{d}{n}.$$

Now, for every prime p, take e(p) to be the exponent of p in N, where $N = \prod_{i=1}^{r} p_i^{a_i}$.

Here,

$$\begin{aligned} \prod_{p \in (S \cup S')} \left(\frac{1 - p^{-e(p)-1}}{1 - \frac{1}{p}}\right) &= \prod_{p \in (S \cup S')} \left(\frac{1 - \frac{1}{p^{e(p)+1}}}{\frac{p-1}{p}}\right) \\ &= \prod_{p \in (S \cup S')} \left(\frac{p^{e(p)+1} - 1}{p^{e(p)+1}}\right)\left(\frac{p}{p-1}\right) \\ &= \prod_{p \in (S \cup S')} \left(\frac{p^{e(p)+1} - 1}{p-1}\right)\left(\frac{p}{p^{e(p)+1}}\right) \\ &= \prod_{p \in (S \cup S')} \left(\frac{p^{e(p)+1} - 1}{p-1}\right)\left(\frac{1}{p^{e(p)}}\right) \\ &\leq \prod_{i=1}^{r} \left(\frac{p^{a_i+1} - 1}{p_i - 1}\right)\left(\frac{1}{p_i^{a_i}}\right) \\ &= \frac{\sigma(N)}{N} \\ &= \frac{n}{d} \end{aligned}$$

Thus

$$\prod_{p \in (S \cup S')} (1 - p^{-e(p)-1}) \leq \frac{n}{d} \prod_{p \in (S \cup S')} \left(\frac{p-1}{p}\right) = \frac{n''}{d''}$$

where

$$n'' = n \prod_{p \in (S \cup S')} (p-1), \quad and \quad d'' = d \prod_{p \in (S \cup S')} p. \tag{5.6}$$

Moreover from (5.5)

$$\frac{n}{d} \prod_{p \in (S \cup S')} \left(\frac{p-1}{p} \right) < \frac{n}{d} \cdot \frac{d}{n} = 1.$$

Therefore,

$$\frac{n''}{d''} < 1.$$

Again, in the same way as before it can be shown that $S \cup S'$ contains a non-empty subset $S'' = \{p_1, p_2, \cdots, p_v\}$ such that

$$\prod_{i=1}^{v} \left(1 - \frac{1}{p_i^{e(p_i)+1}} \right) \leq \frac{n''}{d''} < \prod_{i=1}^{v-1} \left(1 - \frac{1}{p_i^{e(p_i)+1}} \right).$$

By Heath-Brown's Lemma 1

$$\prod_{p \in S''} p^{e(p)+1} \leq (4n'')^{2^v - 1}.$$

Since

$$\frac{n''}{d''} < 1,$$

hence

$$n'' < d''$$

Therefore,

$$\prod_{p \in S''} p^{e(p)+1} \leq (4d'')^{2^v - 1}, \tag{5.7}$$

where $v = \#S''$.

Let

$$V = \prod_{p \in S''} p^{e(p)},$$

$$U = \frac{N}{V},$$

then $\gcd(U, V) = 1$ since U has no primes in common with V.

Let

$$T = (S \cup S') \setminus S''.$$

Then

(i) $v = \omega(V) =$ the number of distinct prime factors of V is at least 1, since S'' is not empty.

(ii) Since $S \cap S' = \emptyset, S'' \subset S \cup S'$ and thus by the definition of T,

$$S \cup S' = T \cup S''.$$

Hence

$$\#S + \#S' = \#T + \#S''$$

or

$$\#S + w = \#T + v.$$

Hence

$$v + \#T - \#S = w \geq 0.$$

Also

$$\sigma(N) = \sigma(UV) = \sigma(U)\sigma(V)$$

and thus

$$\sigma(U) = \frac{\sigma(N)}{\sigma(V)}.$$

Thus

$$\begin{aligned}
\frac{\sigma(U)}{U} &= \frac{\sigma(N)}{\sigma(V)} \cdot \frac{1}{U} \\
&= \frac{\sigma(N)}{\sigma(V)} \cdot \frac{V}{N} \\
&= \frac{\sigma(N)}{N} \cdot \frac{V}{\sigma(V)} \\
&= \frac{n}{d} \cdot \frac{V}{\sigma(V)} \\
&= \frac{n}{d} \cdot \frac{V}{\prod_{p \in S''} \sigma(p^{e(p)})} \\
&= \frac{n}{d} \cdot \frac{V}{\prod_{p \in S''} (\frac{p^{e(p)+1}-1}{p-1})} \\
&= \frac{n}{d} \frac{V \prod_{p \in S''} (p-1)}{\prod_{p \in S''} (p^{e(p)+1}-1)} \\
&= \frac{\nu}{\delta},
\end{aligned}$$

where

$$\delta = d \prod_{p \in S''} (p^{e(p)+1} - 1) = d\sigma(V) \prod_{p \in s''} (p-1).$$

Thus, $d\sigma(V)|\delta$ as required for property (iii).

Finally,

$$\begin{aligned}
\delta &= d \prod_{p \in S''} (p^{e(p)+1} - 1) \\
&\leq d \prod_{p \in S''} p^{e(p)+1}
\end{aligned}$$

$$
\begin{aligned}
&\leq d(4d')^{2^v-1} && \text{by (5.7)}\\
&= d\left(4d\prod(S\cup S')\right)^{2^v-1} && \text{by (5.6)}\\
&\leq d\left(4d(4d)^{2^w-1}\prod(S)^{2^w}\right)^{2^v-1} && \text{by (5.4)}\\
&= d\left((4d)^{2^w}\right)^{2^v-1}\left(\prod(S)\right)^{2^w(2^v-1)}\\
&= d\left(4d\prod(S)\right)^{2^w(2^v-1)}.
\end{aligned}
$$

Thus

$$
\begin{aligned}
4\delta &\leq 4d\left(4d\prod(S)\right)^{2^w(2^v-1)},\\
4\delta\prod(T) &\leq 4d\left(4d\prod(S)\right)^{2^w(2^v-1)}\prod(S\cup S')\\
&\leq 4d\left(4d\prod(S)\right)^{2^w(2^v-1)}(4d)^{2^w-1}\prod(S)^{2^w} && \text{by (5.4)}\\
&= (4d)^{2^w}(4d)^{2^{w+v}-2^w}\prod(S)^{2^{w+v}-2^w}\prod(S)^{2^w}\\
&= (4d)^{2^{w+v}}\prod(S)^{2^{w+v}}\\
&= \left(4d\prod(S)\right)^{2^{v+w}},
\end{aligned}
$$

as required for property (iv) of Lemma 2. This completes the proof.

Chapter 6

Heath-Brown's Theorem:

Completion of the Proof

Heath-Brown's Theorem

Let α be a rational number. Let N be an odd number with at most k prime factors, and suppose that

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

Then

$$N < (4d)^{4^k},$$

where d is the denominator of α. In particular, if $\alpha = 2$, so that N is an odd perfect number, then

$$N < 4^{4^k}.$$

Proof.

Let $\alpha = \frac{n}{d} > 1$. Let N be an odd number with at most k prime factors, and suppose that

$$\sigma(N) = \alpha N = \frac{n}{d} N.$$

Let N be divisible by a set S of primes. Lemma 2 will be applied repeatedly to decompose N. The process is started by using Lemma 2 with $N = N_0, S = S_0 = \emptyset$, and $\alpha = \frac{n_0}{d_0} = \frac{n}{d}$.

By Lemma 2,

$$N = N_0 = UV, \quad \text{where} \quad \gcd(U, V) = 1. \tag{6.1}$$

Also, by (i) of Lemma 2, $\omega(V)$ = the number of distinct prime factors of V is at least 1 and there exists a set T of primes dividing U as specified in Lemma 2. Take

$S_1 = T, V_1 = V$ and $N_1 = U$ to produce the next set of values to be used in Lemma 2. By (iii) of Lemma 2,

$$\frac{\sigma(U)}{U} = \frac{\sigma(N_1)}{N_1} = \frac{\nu}{\delta} = \frac{n_1}{d_1}$$

and

$$d_0\sigma(V_1)|d_1, \quad \text{where} \quad d_1 = \delta.$$

Thus (6.1) and Lemma 2 imply

$$N = N_0 = N_1V_1 = U_2V_2V_1.$$

By taking $N_2 = U_2$, which gives

$$\frac{\sigma(U_2)}{U_2} = \frac{\sigma(N_2)}{N_2} = \frac{\nu'}{\delta'} = \frac{n_2}{d_2}$$

and

$$d_1\sigma(V_2)|d_2, \quad \text{where} \quad d_2 = \delta',$$

and there exists a new set T' of primes dividing U_2. Take $S_2 = T'$ and apply Lemma 2 again to obtain.

$$N = N_0 = N_1V_1 = U_2V_2V_1 = N_2V_2V_1 = U_3V_3V_2V_1 = N_3V_3V_2V_1.$$

This procedure continues and at the i^{th} stage that have N_i, S_i, n_i, d_i; which will then produce the next set of values $N_{i+1}, S_{i+1}, n_{i+1}, d_{i+1}$, where $\gcd(V_j, V_h) = 1$ if $j \neq h$, S_{i+1} is a set of primes that divides N_{i+1}, and

$$N = N_{i+1}V_{i+1}V_iV_{i-1}\cdots V_2V_1. \tag{6.2}$$

Lemma 2 also produces the numbers $v_{i+1} = \omega(V_{i+1})$ and the number w_{i+1} given by

$$w_{i+1} = v_{i+1} + \#S_{i+1} - \#S_i. \tag{6.3}$$

The next step is to show that this process terminates in s steps, where $s \leq k$. This follows from part(i) of Lemma 2, since each V_i has at least one prime factor, and N has at most k prime factors, which from (6.2) implies for any i

$$\begin{aligned} k \geq \omega(N) &\geq \omega(N_{i+1}) + \sum_{j=1}^{i+1} \omega(V_j) \\ &\geq \omega(N_{i+1}) + i + 1 \\ &\geq i + 1. \end{aligned}$$

Thus $s \leq k$.

The process terminates when $U_s = N_s = 1$ for the first time, where

$$N = V_1 V_2 \cdots V_s.$$

By (iii) of Lemma 2

$$\frac{\sigma(N_i)}{N_i} = \frac{n_i}{d_i} \quad \textit{and} \quad d_{i-1}\sigma(V_i)|d_i.$$

Starting with $i = 1$, it follows that

$$d_0\sigma(V_1)|d_1,$$

$$d_1\sigma(V_2)|d_2,$$

and thus

$$d_0\sigma(V_1)\sigma(V_2)|d_2.$$

Next,

$$d_2\sigma(V_3)|d_3$$

and

$$d_0\sigma(V_1)\sigma(V_2)\sigma(v_3)|d_3.$$

Continuing this process, $d_0\sigma(V_1)\sigma(V_2)\cdots\sigma(V_s)|d_s$ is obtained, and hence

$$\sigma(V_1)\sigma(V_2)\cdots\sigma(V_s)|d_s.$$

Recall that at the i^{th} stage where N_i, S_i, d_i, n_i; which will then produce $T = S_{i+1}, N_{i+1} = U_{i+1}$ and

$$\frac{\sigma(N_{i+1})}{N_{i+1}} = \frac{\nu}{\delta} = \frac{n_{i+1}}{d_{i+1}}, \quad \textit{where} \quad \delta = d_{i+1}.$$

Thus by (iv) of Lemma 2,

$$4d_{i+1}\prod(S_{i+1}) \leq \left(4d_i\prod(S_i)\right)^{2^{v_{i+1}+w_{i+1}}}.$$

If $i = 0$, then

$$4d_1\prod(S_1) \leq \left(4d_0\prod(S_0)\right)^{2^{v_1+w_1}},$$

and if $i = 1$, then

$$4d_2\prod(S_2) \leq \left(4d_1\prod(S_1)\right)^{2^{v_2+w_2}}.$$

It follows that

$$\begin{aligned} 4d_2\prod(S_2) &\leq \left(4d_1\prod(S_1)\right)^{2^{(v_2)+(w_2)}} \\ &\leq \left((4d_0\prod(S_0))^{2^{(v_1)+(w_1)}}\right)^{2^{(v_2)+(w_2)}} \\ &= \left(4d_0\prod(S_0)\right)^{2^{v_1+w_1+v_2+w_2}} \\ &= \left(4d_0\prod(S_0)\right)^{2^{(v_1+v_2)+(w_1+w_2}}. \end{aligned}$$

Continuing in this way until

$$4d_s\prod(S_s) \leq \left(4d_0\prod(S_0)\right)^{2^\Lambda},$$

where $\Lambda = \sum_{i=1}^{s}(v_i + w_i)$.

Also,

$$N \leq \sigma(N) = \sigma(V_1)\sigma(V_2)\cdots\sigma(V_s)|d_s,$$

which implies

$$\begin{aligned} N \leq d_s &\leq \frac{(4d_0\prod(S_0))^{2^\Lambda}}{4\prod(S_s)} \\ &= \frac{(4d_0\cdot 1)^{2^\Lambda}}{4\prod(S_s)} \qquad \text{(since } S_0 \text{ is an empty set.)} \\ &< (4d_0)^{2^\Lambda}, \qquad \text{since } 4\prod(S_s) > 1. \\ &= (4d)^{2^\Lambda}, \qquad \text{where } d = d_0. \end{aligned}$$

The proof is finished by showing $\Lambda \leq 2k$. First $v_i = \omega(V_i)$, hence

$$\sum_{i=1}^{s} v_i = \omega(N) \leq k.$$

Next,

$$w_i = v_i + \#S_i - \#S_{i-1}, \qquad (1 \leq i \leq s).$$

Summing gives

$$\begin{aligned}
\sum_{i=1}^{s} w_i &= \sum_{i=1}^{s} v_i + (\#S_1 + \#S_2 + \cdots \#S_s) - (\#S_0 + \#S_1 + \cdots \#S_{s-1}) \\
&= \sum_{i=1}^{s} v_i + \#S_s - \#S_0. \\
&= \omega(N) \leq k.
\end{aligned}$$

Since S_0 and S_s is a set of primes that divides $N_s = 1$ and so $S_s = \emptyset$ also,

$$\Lambda = \sum_{i=1}^{s}(v_i + w_i) \leq k + k = 2k.$$

Therefore,

$$N \leq (4d)^{2^{2k}} = (4d)^{4^k}.$$

In conclusion, if $\alpha > 1$ is a rational number with a denominator in the lowest terms and N is an odd number with at most k prime factors such that

$$\sigma(N) = \alpha N$$

then

$$N \leq (4d)^{4^k}.$$

In particular, if N is an odd perfect number; i.e,

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

then

$$N < 4^{4^k}.$$

References

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

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

3. D. R. Heath-Brown, *Odd perfect numbers*, Math. Proc. Camb. Phil. Soc. (1994), **115**, 191–196.

4. P. Schumer, *Introduction to Number Theory*, PWS Publishing Co., 1996.

5. W. Sierpinski, *Elementary Theory of Numbers*, Hafner Publishing Company, New York., 1964.