1965

On Perfect Numbers

David Thomas Eastham
College of William & Mary - Arts & Sciences

ON PERFECT NUMBERS

A Thesis

Presented to

The Faculty of the Department of Mathematics

The College of William and Mary in Virginia

In Partial Fulfillment

Of the Requirements for the Degree of

Master of Arts

By

David Thomas Eastham

August 1965

APPROVAL SHEET

This thesis is submitted in partial fulfillment of
the requirements for the degree of
Master of Arts

David T. Eastham

Author

Approved, August 1965:

Thomas L. Reynolds

Thomas L. Reynolds, Ph.D.

Hugh B. Easler

Hugh B. Easler, M.A.

Luther T. Conner

Luther T. Conner, M.A.

ACKNOWLEDGMENT

The writer wishes to express his grateful appreciation to Professor Thomas L. Reynolds for his personal guidance and assistance throughout the compilation of this manuscript. The author is also indebted to Professor Luther T. Conner and Professor Hugh B. Easler for their helpful comments and corrections. He also wishes to thank his wife, Kathleen, for the typing of this manuscript.

TABLE OF CONTENTS

	Page
ACKNOWLEDGMENT	iii
ABSTRACT	v
INTRODUCTION	2
Chapter	
I. EVEN PERFECT NUMBERS	3
II. ODD PERFECT NUMBERS	9
III. TECHNIQUES OF PROOF	25
BIBLIOGRAPHY	35

ABSTRACT

A perfect number is a number the sum of whose divisors is equal to twice the number. Even numbers that are perfect have been known for centuries. However, the existence or non-existence of odd numbers that are perfect has never been established. In this paper, some of the properties of perfect numbers are discussed together with conditions for their existence.

Chapter I lists the main result concerning even perfect numbers together with some minor conclusions concerning their properties.

In Chapter II some of the basic principles are set forth concerning the question of odd perfect numbers. This is accompanied by a brief historical review of the progress in various areas.

In order to illustrate the means employed in the attack on odd perfect numbers, Chapter III selects the most comprehensive and most important of a variety of methods and explains their structure.

In the light of the evidence presented, it would seem unlikely that any odd perfect number exists. This, however has not yet been proved.

INTRODUCTION

The aliquot parts of a number are the divisors which are less than the number. If a given natural number is equal to the sum of its aliquot parts it is termed <u>perfect</u>, which is equivalent to saying that the sum of its divisors is equal to twice the number. If this aliquot sum is less than the given number it is termed <u>deficient</u>. If the sum of the divisors is greater than twice the given number, it is termed <u>abundant</u>.

The quality of such a number that equals the sum of its parts has for hundreds of years been associated with perfection, and hence its name. The establishment of a simple criterion by which one could determine whether or not a given natural number is perfect has been a goal sought by mathematicians since the days of the early Greeks. We will discuss, during the next few chapters, the results which have been established concerning such numbers and the methods employed in their establishment.

ON PERFECT NUMBERS

CHAPTER I

EVEN PERFECT NUMBERS

Euclid [6][1] gave a sufficient condition for an even number to be perfect with:

Theorem 1: If p and $2^p - 1$ are primes, then $N = (2^{p-1})(2^p - 1)$ is perfect and even.

Proof: Obviously, $(2^{p-1})(2^p - 1)$ is divisible by

$$1, 2, \ldots\ldots, 2^{p-1}, 2^p - 1, 2(2^p - 1), \ldots\ldots, (2^{p-2})(2^p - 1)$$

but not by any other number less than $(2^{p-1})(2^p - 1)$. The sum of these divisors is $(2^{p-1})(2^p - 1)$. Clearly N is even.

Euler [6] later proved that this condition was also necessary. Hence,

Theorem 2: If N is even and perfect, then $N = (2^{p-1})(2^p - 1)$, where p and $2^p - 1$ are primes.

Proof: We will denote $\sum_{d|N} d$ by $\sigma(N)$. Letting

$$N = 2^k\mu,$$

where

$$(2^k, \mu) = 1,$$

we have

$$\sigma(N) = 2N = \sigma(2^k\mu) = \sigma(2^k)\sigma(\mu),$$

giving

$$\text{(A)} \qquad \frac{2^{k+1} - 1}{2-1}\sigma(\mu) = 2^{k+1}\mu.$$

---

[1]The numbers in brackets refer to the bibliography.

But $2^{k+1}-1$ is odd and must be a factor of μ. So

$$\mu = (2^{k+1}-1)V$$

or

$$(2^{k+1}-1)\sigma(\mu) = 2^{k+1}[(2^{k+1}-1)V],$$

whence

$$\sigma(\mu) = (2^{k+1})V.$$

But also

$$\sigma(\mu) = \sigma[(2^{k+1}-1)V].$$

Now, either $V = 1$ or $V > 1$. Assume $V > 1$. The divisors of $(2^{k+1}-1)V$ are:

$$(2^{k+1}-1)V,\ 2^{k+1}-1,\ V,\ 1,\ \ldots\ldots .$$

Their sum, S, is:

$$S = (2^{k+1})V - V + 2^{k+1}-1 + V + 1 + \ldots\ldots$$

$$= (2^{k+1})V + (2^{k+1} + \ldots\ldots\ldots+.)$$

$$= \sigma[(2^{k+1}-1)V] = \sigma(\mu)$$

which from a previous equation is equal to

$$(2^{k+1})V,$$

or

$$(2^{k+1})V = (2^{k+1})V + (2^{k+1} + \ldots\ldots\ldots+.)$$

which is impossible, therefore $V = 1$, and $\mu = 2^{k+1}-1$.

From (A),

$$\sigma(\mu) = 2^{k+1}$$

or

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

Now, the divisors of $2^{k+1} - 1$ are:

$$2^{k+1} - 1, 1, \ldots\ldots,$$

Adding, we get

$$\sigma(2^{k+1} - 1) = 2^{k+1} - 1 + 1 + (\text{extra terms})$$

$$= 2^{k+1} + (\text{extra terms}),$$

thus (extra terms) = 0. So $2^{k+1} - 1$ must be prime.

To show that k + 1 is a prime we assume $k + 1 = a \cdot b$. Then

$$2^{k+1} - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 = x^b - 1.$$

This $x^b - 1$ is divisible by

$$x - 1 = 2^a - 1,$$

but

$$x^b - 1 = 2^{k+1} - 1$$

was prime, hence a contradiction and k + 1 is prime.

Primes of the form $p = 1 + 2 + 2^2 + \ldots + 2^{p-1} = 2^p - 1$ are called Mersenne primes and since the time of Euler the search for even perfect numbers has been reduced to the search for Mersenne primes. Due to the difficulty of ascertaining whether or not a number of the form $2^p - 1$ is a prime, few correct lists of Mersenne primes were published until the advent of the modern computers. Even now the only even perfect numbers known are those corresponding to p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, and 4423 [1]. It is still not known whether there is a finite number of even perfect numbers.

Some of the properties of even perfect numbers follow:

Theorem 3: Every multiple of an even perfect number is abundant.

Proof: Let $N = (2^{p-1})(2^p-1)$ be perfect.

Then

$$NK = (2^{p-1})(2^p-1)K$$

and

$$\sum_{\substack{d|N \\ d<N}} K(2^{p-1})(2^p-1)$$

$= 2(2^p-1)K + 2^2(2^p-1)K +.+ 2^{p-2}(2^p-1)K + N + K + 2K +.+ (2^{p-1})K$

$= (2^p-1)(2^{p-1}-1)K + N + (2^p-1)K$

Let

$$(2^{p-1})(2^p-1)K = (2^p-1)(2^{p-1}-1)K + N + K(2^p-1)$$

$$= (2^p-1)(2^{p-1}-1)K + (2^{p-1})(2^p-1) + (2^p-1)K,$$

hence,

$$(2^{p-1})K = (2^{p-1}-1)K + 2^{p-1} + K$$

$$= K\cdot 2^{p-1} - K + 2^{p-1} + K$$

$$= (2^{p-1})K + 2^{p-1}.$$

This holds only for $p = 1$, which does not make N perfect. Otherwise NK is obviously abundant.

Theorem 4: Every divisor of an even perfect number is deficient.

Proof: Let $N = (2^p - 1)(2^{p-1})$ be perfect. The conclusion is immediate since, if p is prime, then

(a) $$\sum_{\substack{d|p \\ d<p}} d = 1$$

and

(b) $$\sum_{\substack{d|2^k \\ d<2^k}} 2^k = 1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1.$$

Theorem 5: If $(2^{p-1})(2^p - 1)$ is perfect, then

$$(2^{p-1})(2^p - 1) \equiv 1 \pmod 9.$$

Proof: We shall denote the ultimate sum of the digits of a number by S(N).

Example: $S(398) = 3 + 9 + 8 = 20$; $2 + 0 = 2$ and $S(398) = 2$.

Brooke [4] showed that $S[(2^{n-1})(2^n - 1)]$ forms the sequence 1, 3, 1, 9, 1, 6, 1, 3, ... etc., for $n \geqslant 3$. However, if $(2^{n-1})(2^n - 1)$ is to be perfect, n must be prime and those elements occupying the positions in the sequence generated when n was even would be eliminated. Hence the only numbers to be considered are those such that $S(N) = 1$. The result follows from the easily proven fact that if

$$S(N) \equiv 1 \pmod 9,$$

then

$$N \equiv 1 \pmod 9.$$

Theorem 6: Every even perfect number is triangular.

Proof: Triangular numbers are of the form

$$1/2[n(n+1)],\ n > 0.$$

Given an even perfect number it is of the form

$$(2^p-1)(2^{p-1})$$

by Theorem 2 and

$$(2^p-1)(2^{p-1}) = 1/2[2^p(2^p-1)].$$

Theorem 7: For any integer of the form $2^{n-1}(2^n-1)$, $2^{n-1}<2^n-1$ for every positive integer $n > 1$. In particular, this holds for any even perfect number $N = 2^{p-1}(2^p-1)$ where p is a prime.

Proof: If $n = 2$, $2 < 3$. Assume that

$$2^{k-1} < 2^k-1$$

for some integer $k > 2$. Then

$$2^k < 2^{k+1}-2$$

or

$$2^k < 2^{k+1}-1$$

and the induction is complete.

An alternate result may be found in [1].

Theorem 7*: Six is the only square free even perfect number.

Proof: In Theorem 2 we proved that for $N = (2^{p-1})(2^p-1)$ to be perfect, 2^p-1 and p had to be prime. For N to be square free it is necessary that $p-1<2$, hence $p = 2$ and $N = 6$.

CHAPTER II
ODD PERFECT NUMBERS

In the case of even numbers the desired criteria have been established to determine if the number is perfect. However, there does not exist any such determining equation for an odd perfect number despite centuries of effort by professional and amateur mathematicians. In fact, no odd perfect number has ever been discovered and it is seriously doubted that one even exists.

Among the many earlier statements made concerning odd perfect numbers (usually erroneous), the first significant fact pertaining to their existance was established by Euler [6] who proved that:

<u>Theorem 8</u>: If N is an odd perfect number, then

$$N = p^{\alpha} q_1^{2\beta_1} q_2^{2\beta_2} \ldots q_n^{2\beta_n},$$

where

p_1, $q_1, \ldots q_n$ are distinct odd primes and $\alpha \equiv 1 \equiv p (\mathrm{mod}\ 4)$.

<u>Proof</u>: We first remark that since p is odd and $p > 2$, then

$$(p^s) = p^s + p^{s-1} + \ldots + p^2 + p + 1$$

is odd when s is even and even when s is odd. Thus we need only one prime raised to an odd power, where the σ of this number, $\sigma(p^s)$, is of the form 2K, K being odd.

Now assume p is of the form $4x - 1$. Let n be odd, then

$$\sigma[(4x-1)^n] = (4x-1)^n + (4x-1)^{n-1} +..+ (4x-1)^2 + (4x-1) +1$$

which has an even number of terms as shown but the constant term in each binomial expansion alternates sign, thus all the terms not containing x are gone.

Hence

$$\sigma[(4x-1)^n] = 4 \cdot M,$$

giving p the form $4x+1$ as prime.

If $p = 4x+1$, we now assume an odd exponent n.

$$\sigma[(4x+1)^n] = (4x+1)^n + (4x+1)^{n-1} +..+ (4x+1)^2 + (4x+1) +1$$

$$= 4A + (n+1).$$

If n is of the form $4K + 3$, then

$$\sigma[(4x+1)^{4K+3}] = 4A + (4K+3+1) = 4Q,$$

which cannot be a product of 2 and an odd number. Hence the exceptional prime is of the form $4x+1$ and its exponent must have the form $4K+1$.

We will assume the prime factorization given by Theorem 8 for any odd perfect number, denoted by N, throughout this chapter. We continue denoting the sum of the divisors of N, by $\sigma(N)$ and establish some elementary facts about this sum in relation to odd perfect numbers.

In Theorem 8 assume that

$$p<q_1<q_2<\ldots<q_n.$$

Then the sum of the divisors of N,

$$\sigma(N) = (1+p+p^2+..+p^\alpha)\ldots(1+q_n+q_n^2+..+q_n^{2\beta_n}) =$$

$$\text{(A)} \qquad \frac{p^{\alpha+1}-1}{p-1}\cdot\frac{q_1^{2\beta_1+1}-1}{q_1-1}\cdot\ldots\cdot\frac{q_n^{2\beta_n+1}-1}{q_n-1}.$$

<u>Theorem 9</u>: The odd number $p^\alpha q^\beta$ is not perfect.

<u>Proof</u>: We first give an elementary inequality needed in the proof.

Assume that $q_1<q_2$, where q_1 and q_2 are primes each greater than 2.

Then,

$$q_1q_2-q_1>q_1q_2-q_2$$

or

$$q_1(q_2-1)>q_2(q_1-1)$$

whence

$$\text{(B)} \qquad \frac{q_1}{q_1-1} > \frac{q_2}{q_2-1}$$

Also if

$$q_1<q_2<q_3,$$

then from (B) and

$$\frac{q_2}{q_2-1} > \frac{q_3}{q_3-1},$$

we have

(C) $$\frac{q_1}{q_1-1}\cdot\frac{q_2}{q_2-1} > \frac{q_2}{q_2-1}\cdot\frac{q_3}{q_3-1}.$$

Now assume $p^\alpha q^\beta$ is perfect.

Then

$$\sigma(p^\alpha q^\beta) = \frac{p^{\alpha+1}-1}{p-1} \cdot \frac{q^{\beta+1}-1}{q-1} = 2p^\alpha q^\beta,$$

and

$$\frac{p^{\alpha+1}}{p-1}\cdot\frac{q^{\beta+1}}{q-1} > 2p^\alpha q^\beta$$

implies that

$$\frac{p}{p-1}\cdot\frac{q}{q-1} > 2.$$

This fraction reaches its maximum for smallest values of p at p=3 and q=5 by (C), but this gives $\frac{3}{2}\cdot\frac{5}{4} = \frac{15}{8} < 2$.

Theorem 10: $\frac{(p+1)}{2}$ divides N where p is the exceptional prime.

Proof: $$\sigma(p^{4K+1}) = \frac{p^{4K+1}-1}{p-1} = (p+1)\left(\frac{p^{2K+1}+1}{p+1}\right)\left(\frac{p^{2K+1}-1}{p-1}\right)$$

These last three factors are integers, so that each divides $\sigma(N)$ and $\frac{p+1}{2}$ divides N by the statement above.

These elementary results give a basis for the development of different methods of attack on the properties of an odd perfect number. We continue by giving a historical review of these approaches and by proving some of the basic ideas.

The first such attack was an attempt to develop relationships between the number of factors n of N and the smallest factor p.

The initiator of this method seems to have been Desboves [6], who proved in 1878:

Theorem 11: In an odd perfect number which is divisible by just n distinct primes the least prime, p, is less than 2^n.

However, using statement (A) we may improve this as follows:

Theorem 12: Let p be the smallest prime divisor of an odd perfect number N, then N has at least p distinct prime divisors.

Proof: Under the same assumptions as statement (A), we know that:

$$2p^{\alpha}q_1^{2\beta_1}q_2^{2\beta_2}\cdots q_n^{2\beta_n} = \frac{p^{\alpha+1}-1}{p-1}\cdot\frac{q_1^{2\beta_1+1}-1}{q_1-1}\cdots\frac{q_n^{2\beta_n+1}-1}{q_n-1},$$

however,

$$p^{\alpha+1}>p^{\alpha+1}-1,\ q_1^{2\beta_1+1}>q_1^{2\beta_1+1}-1,\ \text{etc.},$$

giving

$$\text{(D)} \qquad 2<\frac{p}{p-1}\cdot\frac{q_1}{q_1-1}\cdot\frac{q_2}{q_2-1}\cdots\frac{q_n}{q_n-1}$$

Also,

$$\frac{q_1}{q_1-1}<\frac{p+1}{p},\ \frac{q_2}{q_2-1}<\frac{p+2}{p+1},\cdots\frac{q_n}{q_n-1}<\frac{p+n-1}{p+n-2},$$

so that,

$$\frac{p}{p-1}\cdot\frac{q_1}{q_1-1}\cdots\frac{q_n}{q_n-1}<\frac{p}{p-1}\cdot\frac{p+1}{p}\cdot\frac{p+2}{p+1}\cdots\frac{p+n-1}{p+n-2} = \frac{p+n-1}{p-1}$$

or

$$2 < \frac{p+n-1}{p-1},$$

hence

$$p<n+1$$

This result was given by Servais [6] in 1888 and in 1952 Otto Grün [6] proved that $p<\frac{2}{3}n + 2$, by utilizing the fact that odd primes differ by at least two. Using this last result, the fact that 3, 5 and 7 cannot occur together in N (See Chapter 3) and that alternate primes differ by at least 6, Muskat [8], in 1955, showed that $p < 1/7(3n+36)$.

Uhler [13] in 1952 proved:

<u>Theorem 13</u>: If $N = p^{\alpha}q_1^{2\beta_1}q_2^{2\beta_2}\cdots q_n^{2\beta_n}$ is perfect, then

$$2< \frac{p}{p-1}\prod_{i=1}^{n}\left(\frac{q_i}{q_i-1}\right) < (1+\epsilon)\log p_n/\log p_1,$$

where $p_1 = p$ and p_n is the n-th consecutive prime beginning with p.

<u>Proof</u>: The proof follows from the inequality:

$$2 < \frac{p}{p-1}\prod_{i=1}^{n}\left(\frac{q_i}{q_i-1}\right),$$

which is a result of Theorem 12 when N is perfect; and the fact that asymptotically,

$$\prod_{p < n} \frac{p}{p-1} \approx (\log n)e^{\gamma}$$

From this result we know

$$p_n > p^{2/1+\epsilon}$$

The best results to date in this area have been given by Karl K. Norton [9] who, employing analytic methods and assisted by ILLIAC (the University of Illinois Automatic Digital Computer), proved the following theorems:

First we clarify the notation:

Suppose

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots \cdot p_k^{\alpha_k} \text{ is perfect,}$$

where

$$3 \leq p_1 < p_2 < \cdots p_k$$

so that

$$\text{(E)} \qquad 2 = \prod_{r=1}^{k} \frac{p_r^{a_r+1} - 1}{p_r^{a_r}(p_r - 1)} < \prod_{r=1}^{k} \frac{p_r}{p_r - 1}$$

When

$$p_1 = p_n,$$

$$\text{(F)} \qquad 2 < \prod_{r=n}^{n+k-1} \frac{p_r}{p_r-1} .$$

Let the function $\alpha(n)$ be defined for $n \geqslant 2$ by the following double inequality:

$$\text{(G)} \qquad \prod_{r=n}^{n+\alpha(n)-2} \frac{p_r}{p_r-1} < 2 < \prod_{r=n}^{n+\alpha(n)-1} \frac{p_r}{p_r-1} .$$

From (E), (F) and (G) it follows that if p_n is the smallest prime factor of N, then N has at least $\alpha(n)$ different prime factors. Also, N must have a prime factor at least as large as

$$p_{n+\alpha(n)+1} = p_s$$

($s = s(n)$ represents $n + \alpha(n) + 1$).

Norton's results are given in the following:

Theorem 14: If p_n is the smallest prime factor of N, then

$$N \geqslant p_n^6 p_{n+1}^4 (p_{n+2} p_{n+3} \cdots p_{s-1})^2 p_s .$$

Theorem 15: If p_n is the smallest prime factor of N, where $2 \leqslant n < e^{42}$ or $n > e^{1993}$, then

$$\log N > 2p_s\left(1 - \frac{1}{\log p_s}\right) - 2p_n\left(1 + \frac{1}{\log p_n}\right) + 6(\log p_n)$$

$$+ 2(\log p_{n+1}) - \log p_s .$$

Theorem 16: $a(n) > n^2 - 2n - \frac{n+1}{\log n} - 5/4 - 1/2n$

$- 1/4n (\log n).$

Theorem 17: Suppose that $t(1 - \frac{a}{\log t}) < \theta(t) < t(1 + \frac{b}{\log t})$ for $p_n \leqslant t \leqslant p_s$, where a and b are constants and $0 < a \leqslant 3$, $0 < b \leqslant 3$.

Then,

$$p_s > e^{-b} p_n^2 \left\{ 1 - \frac{4a + 3b + b^2}{2(\log p_n)} - \frac{4(\log p_n)}{p_n} \right\}.$$

In particular,

$$p_s > e^{-b} p_n^2 \left\{ 1 - \frac{4a + 3b + b^3}{2(\log 547)} - \frac{4(\log 547)}{547} \right\}, \text{ for } n \geqslant 4.$$

Using this same approach Professor Paul T. Bateman [9], gives a theorem which indicates a lower bound for log N:

Theorem 18: Let N have a smallest prime factor p_n and let b be any number less than 4/7.

Then,

1) N has at least $\alpha(N)$ different prime factors, where

$$\alpha(N) = l_i(p_n^2) + O(n^2 e^{-\log^b n}).$$

2) N has a prime factor at least as large as

$$p_s = p_n^2 + O(n^2 e^{-\log^b n}).$$

3) $\log N > 2\, p_n^2 + O(n^2 e^{-\log^b n}).$

Many papers have appeared examining the size of n under various conditions on N. We have already shown (Theorem 9) that any odd perfect number has at least 3 distinct prime factors. Desboves [6] stated that no odd perfect number is divisible by only 3 distinct primes.

J. J. Sylvester [6] proved there are none with 4 distinct primes and stated that there is no N with fewer than 6 distinct prime divisors and proved that there is none, not divisible by 3 with less than 8 distinct prime divisors.

Kühnel [8] and Webber [8] proved later that if 3 divides N, $n \geqslant 5$.

E. Catalan [6] proved that if 3, 5 or 7 does not divide N, $n \geqslant 26$, with N having at least 45 digits.

T. Pepin [6] proved that an odd perfect number relatively prime to $3 \cdot 7$, $3 \cdot 5$, or $3 \cdot 5 \cdot 7$ contains at least 11, 14 or 19 distinct prime factors respectively, and cannot have the form $6K + 5$.

By 1855 Sylvester [6] had raised the number of distinct primes to 5 and Gradstein [8] pushed this to 6. Later, Kühnel [8] and Webber [8] produced the same latter result.

T. L. Reynolds [10] proved that if $5 \nmid N$, $n > 6$.

In this area, although much later, Kanold [6] showed that if N is odd and perfect, such that

$$\beta_2 = \ldots\ldots = \beta_n = 1,$$

then

$$n \geqslant 9,$$

and if

$$\alpha = 1, \ \beta_2 = \ldots\ldots = \beta_n = 1,$$

then

$$n \geqslant 13.$$

Muskat [8] illustrated a proof that for any N, $n \geqslant 7$.

An obvious result of the previous section is the establishment of lower bounds for N. Among the first such bound was $N > 2(10)^6$ given by Turcaninov [7] in 1908. This was raised to 10^8 by Bernhard [2], $1.4(10)^{14}$ by Kanold [7], 10^{18} by Muskat [7], 10^{20} by Kanold [9] and to 10^{36} by Kanold [7] if $\beta_2 = \ldots\ldots\ldots = \beta_n = 1$.

During the period from 1912 to the late thirties there seems to have been a lack of interest in the problem of odd perfect numbers. The revival of this interest began with Steuerweld [7] who introduced greater restrictions on N by examining the forms allowed the exponents of the primes. His first proof was that N is not perfect if $\beta_1 = \ldots\ldots = \beta_n = 1$.

Kanold [7] then showed that if $\alpha = 1$, or $\alpha = 5$, then N is not perfect if $\beta_1 = 2$ and $\beta_2 = \ldots\ldots = \beta_n = 1$.

Brauer [7] and Kanold [7] then proved independently that N is not perfect if $\beta_1 = 2$ and $\beta_2 = \ldots\ldots = \beta_n = 1$. Kanold [7] later showed that N is not perfect if $\beta_1 = \ldots\ldots = \beta_n = 2$, and also if $2\beta_i + 1$, $i = 1, 2, \ldots, n$, have a common divisor 9, 15, 21 or 33. In addition he proved [7] that N is not perfect if $\beta_1 = \beta_2 = 2$ and $\beta_3 = \ldots = \beta_n = 1$, or if $\alpha = 5$, $\beta_i = 1$, where $i = 1, 2, \ldots, n$.

Kanold [7] proved that N is not perfect if it is relatively prime to 3, i.e., $(N,3) = 1$ and $\beta_2 = \ldots = \beta_n = 1$, or if $\alpha = 1$ or 5, $\beta_2 = \ldots = \beta_n = 1$ and $2\beta_1 < 10$. He pointed out that if N is perfect and $\beta_2 = \ldots = \beta_n = 1$, then $\alpha + 2\beta_1 + 2(n + 1) \geqslant 37$. Also if N is perfect, $\alpha = 1$, and $\beta_2 = \ldots = \beta_n = 1$, then $q_1 = 3$, $2\beta_1 \geqslant 12$.

McCarthy [7] showed that if N is perfect, $(N,3) = 1$, and $\beta_2 = \ldots = \beta_n = 1$, then $q_1 \equiv 1 \pmod 3$.

Of a slightly different nature Kanold [7] proved that if N is perfect, then the maximum prime divisor of N is greater than twice the maximum of $\alpha + 1$ and $2\beta_i + 1$, $i = 1, 2, \ldots, n$. He also proved here that if $2\beta_i + 1 = r^{\lambda i}$, $i = 1, 2, \ldots, n$, where r is a prime, then both $p \equiv 1 \pmod r$ and $1/2(\alpha + 1) \equiv 0$ or $1 \pmod r$ are necessary conditions for N to be perfect.

The next area of research, which has led to many valuable conclusions concerning odd perfect numbers, is a result of the study of certain cyclotomic polynomials and Diophantine equations. We give here some definitions and elementary results of this area while delaying a more detailed explanation of the methods used until the next chapter.

For any natural number m, the $m^{\underline{th}}$ cyclotomic polynomial is defined by

$$F_m(x) = \prod_{i=1}^{\varphi(m)} (x - \epsilon_i),$$

where the ϵ_i are the $\varphi(m)$ primitive $m^{\underline{th}}$ roots of unity.

$F_m(x)$ is an irreducible polynomial with integral coefficients, and when rewritten in the following form:

$$x^s + x^{s-1} + \ldots\ldots + x^2 + x + 1 = \prod_{\substack{m \mid s+1 \\ m \neq 1}} F_m(x)$$

we can see its importance to our problem, remembering that if N is perfect, and that

$$\sigma(p^\alpha) \cdot \prod_{i=1}^{n} \sigma(q_i^{2\beta_i}) = 2p^\alpha q_1^{2\beta_1} \cdot q_2^{2\beta_2} \ldots . q_n^{2\beta_n}.$$

Hence every prime factor of an odd perfect number N is a prime factor of some $F_m(x)$ where $m \mid \alpha + 1$ or $m \mid 2\beta_i + 1$.

The fundamental result is due to Kronecker and is in reference to the divisibility properties of these polynomials. Kronecker proved that if s is a prime divisor of $F_m(x)$, then either $s \mid m$ or $s \equiv 1 (\mathrm{mod}\ m)$. Kanold [7] then generalized this by proving that if

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_k^{\alpha_k} \geqslant 3$$

with

$$p_1 < p_2 < \cdots\cdots < p_k$$

and if r is a prime divisor of $F_m(x)$,

then

$$p_k \equiv 1 (\text{mod } p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_k^{\alpha_k - 1})$$

is a necessary condition that $r = p_k$, and

$$p_k \equiv 1 (\text{mod } p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_k^{\alpha_k - 1})$$

is a sufficient condition that $r \equiv 1 (\text{mod } m)$. In case $p_k | F_m(a)$ for some integer a, then p_k^2 does not divide $F_m(a)$. As a corollary, he proved that if $m \geqslant 3$ and $a \geqslant 3$ is an integer, then $F_m(a)$ has at least one prime divisor $r \equiv 1 (\text{mod } m)$. He improved on this last result by showing that if $m \geqslant 3$ and $a = \pm 2$ then $F_m(a)$ has at least one prime divisor $r \equiv 1 (\text{mod } m)$.

In the consideration of certain Diophantine equations, T. Nagell [3] proved:

If $m > 1$ is not a power of 3, then the equation $x^2 + x + 1 = y^m$ has no solutions in integers x, y with $y \neq \pm 1$.

Brauer [3] improved on Nagell's theorem by establishing, as a lemma, the following:

Let r and s be different positive integers and p be a prime. The system of simultaneous Diophantine equations $x^2 + x + 1 = 3p^r$, $y^2 + y + 1 = 3p^s$, has no solutions in positive integers x, y.

Kanold [7] then proved that the Diophantine equation

$$x^\beta + x^{\beta-1} + \dots + x^2 + x + 1 = y^r$$

has no solution with x a prime and $r > 1$ except $x = 3$, $\beta = 1$, $y = r = 2$.

In addition to the various areas covered above there are a few miscellaneous results which we list below.

Shapiro [11] and Dickson [5] proved independently, giving different proofs, that there are only a finite number of odd perfect numbers with a given number of primes.

If N is given, then

1) Kanold [7] proved that N has a square factor greater than or equal to $1/2(r + 1)$, where r is the largest prime divisor of N.

2) $N \equiv 1 \pmod{12}$ or $N \equiv 9 \pmod{36}$, which was proved by Touchard [7].

We know that N is not perfect if

$$1/2[\sigma(p^\alpha)] \text{ and } \sigma(q_i^{2\beta_i}),$$

$i = 1, 2, \dots, n$ are prime powers. [Levit].

Kanold, McCarthy and Volkman showed the density of the set of all perfect numbers to be zero [7].

CHAPTER III

TECHNIQUES OF PROOF

In discussing the techniques used in the proofs of the previous statements we remark first that many of these results were arrived at by using the elementary items.

For instance, when the number n + 1 of distinct prime factors was relatively small, knowing that no perfect number having less than n + 1 distinct prime factors existed, and desiring to prove that no number with n + 1 distinct prime factors could exist, a process of elimination was instituted as follows:

First, all combinations of n + 1 factors satisfying

$$2 < \frac{p}{p-1} \prod_{i=1}^{n} \frac{q_i}{q_i-1},$$

were eliminated by systematically ruling out the lower values of the exponents until

$$\frac{\sigma(N)}{N} > 2.$$

These exponents were usually removed by using the fact that any odd divisor of $\sigma(N)$ also must divide N.

If this failed, then N was selected with fixed exponents and

$$\frac{\sigma(N)}{N}$$

was shown to be less than 2.

Following this, one would choose N with larger exponents and repeat the process.

To demonstrate this procedure we will construct part of the proof of Desbove's statement (Chapter II) that there does not exist an odd perfect number with only three distinct prime divisors.

To simplify notation we define the function

$$F(N) = \frac{\sigma(N)}{N} .$$

Thus, for an odd perfect number N,

$$F(N) = 2.$$

For obvious reasons we prove:

Theorem 19: If for any N, $F(N) > 2$, then for any multiple KN of N, $F(KN) > F(N) > 2$.

Proof: If $(K, N) = 1$, then $F(KN) = F(K) \cdot F(N) > F(N) > 2$. If KN contains higher powers of the same factors as N, then, since

$$F(Z^{x+y}) = \frac{Z^{x+y+1}-1}{Z^{x+y}(Z-1)} > \frac{Z^{x+1}-1}{Z^{x}(Z-1)} = F(Z^{x}),$$

$$F(KN) > F(N) > 2.$$

If KN contains both new factors and the present factors of N to higher powers, let

$$KN = K_1K_2N$$

where K_1 contains the new factors and K_2 contains the higher powers of factors of N.

Then

$$F(KN) = F(K_1)\cdot F(K_2N) > F(K_1)\cdot F(N) > 2.$$

We now wish to show that if N is perfect then

$$N \neq p^{\alpha}q_1^{2\beta_1}q_2^{2\beta_2}.$$

Proof: We first remark that by Theorem 12 the smallest prime divisor of N is less than n + 1 = 3 + 1 implying that if

$$N = p^{\alpha}q_1^{2\beta_1}q_2^{2\beta_2},$$

and perfect,

$$q_1 = 3.$$

(1) $5\cdot 3\cdot 7$ does not divide N.

Proof: By Theorem 8, the smallest values of the exponents would give $5\cdot 3^2\cdot 7^2$. But

$$F(5\cdot 3^2\cdot 7^2) = \frac{494}{245} > 2,$$

and by Theorem 19,

$$F[K(5\cdot 3^2\cdot 7^2)] > 2.$$

(2) If $p = 13$, then $13\cdot 3\cdot x$, where x is a prime not equal to 7, does not divide N.

Proof: By Theorem 10, $1/2(p+1) = 7$ divides N.

(3) $5\cdot 3\cdot 11$ does not divide N.

Proof: If $N = 5\cdot 3^2\cdot 11^2$, then

$$\sigma(N) = x\cdot \frac{11^3 - 1}{10} = x\cdot 7\cdot 19,$$

thus 7 and 19 must divide N, a contradiction.

If $N = 5\cdot 3^2\cdot 11^4$, then

$$\sigma(N) = x\cdot \frac{3^2 - 1}{2} = x\cdot 13,$$

forcing 13 to divide N, which is impossible.

If $N = 5\cdot 3^4\cdot 11^4$, then

$$\sigma(N) = x\cdot \frac{11^5 - 1}{10} = x\cdot 2^3\cdot 3\cdot 61,$$

where 61 does not divide N.

If $N = 5\cdot 3^4\cdot 11^6$, then

$$F(N) < 2.$$

If $N = 5\cdot 3^6\cdot 11^6$, then

$$\sigma(N) = x\cdot \frac{3^7 - 1}{2} = x\cdot 1093,$$

where 1093 is prime and does not divide N.

If $N = 5\cdot 3^8\cdot 11^6$, then

$$\sigma(N) = x\cdot \frac{3^9 - 1}{2} = x\cdot 13\cdot 757,$$

where 13 does not divide N.

$$\text{If } N = 5 \cdot 3^{10} \cdot 11^{6}, \text{ then}$$

$$F(N) < 2.$$

$$\text{If } N = 5 \cdot 3^{10} \cdot 11^{8}, \text{ then}$$

$$F(N) > 2$$

and by Theorem 19,

$$F[K(N)] > 2.$$

We have thus far illustrated the usage of the basic items, knowing that $N \neq p^{\alpha} q_1^{2\beta_1}$ in the beginning of the proof. To complete the proof one need only to continue the elimination process.

However, it is obvious, that as the number of factors increase, the amount of work necessary to eliminate the proportionally increasing combinations of factors becomes impractical. These elementary techniques would produce results but as one would suspect, additional means have been developed to aid in this work.

One of the strangest, perhaps, of these means resulted from the study of differential equations, the outcome of which allows to classify all odd perfect numbers into two classes.

In Chapter II we stated that:

If odd perfect numbers exist, they are of the form $12M + 1$ or $36M + 9$.

<u>Proof</u>: Balth van der Pol [11] in 1951 showed that the function

$$\text{(A)} \qquad \alpha(t) = 1 - 24\sum_{1}^{\infty} \sigma(k)e^{-kt},$$

satisfies the differential equation:

$$\text{(B)} \qquad 2\frac{d^3\alpha}{dt^3} + 2\alpha\frac{d^2\alpha}{dt^2} - 3\left(\frac{d\alpha}{dt}\right)^2 = 0,$$

and substituting (A) into (B) he shows that the numbers $\sigma(k)$ satisfy the relation:

$$\text{(C)} \qquad \frac{n^2(n-1)}{12}\sigma(n) = \sum_{k=1}^{n-1} [5k(n-k)-n^2]\sigma(k)\sigma(n-k),$$

for $n > 1$.

For example:

$\sigma(2) = 3[\sigma(1)]^2 = 3.$

$3\sigma(3) = 4\sigma(1)\cdot\sigma(2) = 4\cdot1\cdot3 = 12.$

$2\sigma(4) = -\sigma(1)\cdot\sigma(3) + 2[\sigma(2)]^2 = -4 + 18 = 14.$

$5\sigma(5) = -6\sigma(1)\sigma(4) + 6\sigma(2)\sigma(3) = -6\cdot1\cdot7 + 6\cdot3\cdot4$

$= -42 + 72 = 30.$

These are the first few cases for n.

Van der Pol later showed that relation (C) can also be written:

$$\text{(D)} \qquad \frac{n^2(n-1)}{6}\sigma(n) = \sum_{k=1}^{n-1} (3n^2-10k^2)\sigma(k)\sigma(n-k).$$

The rearrangement is the first of a family of modifications which are derived as follows:

Let

$$S_p = S_p(n-1) = \sum_{k=1}^{n-1} k^p\sigma(k)\sigma(n-k),$$

then, letting k be n-k gives:

$$S_p = \sum_{k=1}^{n-1} (n-k)^p\sigma(n-k)\sigma(n)$$

$$= n^pS_o - pn^{p-1}S_1 + \frac{p}{2}n^{p-2}S_2 - \cdot\cdot + (-1)^pS_p.$$

From this we may derive the equations:

$$S_1 = nS_o - S_1,$$

or

(E) $$2S_1 = nS_o,$$

and

(F) $$4S_3 = 6nS_2 - n^3S_o.$$

Using equations (E) and (F) Touchard gives (C) the following form:

(G) $$n^3(n-1)\sigma(n) - 48nS_2 + 72S_3 = 0.$$

Now, if n is perfect, then $\sigma(n) = 2n$ and (G) becomes:

$$2n^4(n-1) = 48nS_2 - 72S_3$$

or

$$1/12n^4(n-1) = 2nS_2 - 3S_3,$$

where $2nS_2 - 3S_3$ is an integer.

If n is odd, $n \equiv 0 \pmod 3$, then $n \equiv 1 \pmod 4$, whence $n \equiv 9 \pmod{12}$. However, for n odd, such that $n \not\equiv 0 \pmod 3$, then $n \equiv 1 \pmod{12}$.

We conclude this chapter with a brief discussion of the use of cyclotomic sums of the form

$$\sum_{i=0}^{n-1} q^i = 1 + q + q^2 + \ldots + q^{n-1} = \frac{q^n - 1}{q-1}$$

in proving the non-existence of odd perfect numbers when the exponents of the prime factors of N are specified.

In Chapter II we gave two lemmas concerning Diophantine equations, namely:

(1) If $m > 1$ is not a power of 3, then the equation $x^2 + x + 1 = y^m$ has no solutions in integers x, y with $y = \pm 1$.

(2) Let r and s be different positive integers and p be a prime. The system of simultaneous equations $x^2 + x + 1 = 3p^r$, $y^2 + y + 1 = 3p^s$, has no solutions in positive integers x, y.

We now illustrate the use of these lemmas by discussing several cases of the proof of the following theorem due to Brauer [2].

<u>Theorem</u>: An odd number of the form $N = p^{\alpha} q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$ is not perfect.

<u>Proof</u>: We will denote N by

$$N = p^{\alpha} q_1^2 q_2^2 \cdots q_k^2 r_1^2 r_2^2 \cdots r_t^2 s^4, \quad (k \geqslant 0,\ t \geqslant 0)$$

where

$$q_n \equiv 1 (\mathrm{mod}\ 3),\ (1 \leqslant n \leqslant k)$$

and

$$r_\lambda \not\equiv 1 (\mathrm{mod}\ 3)$$

for

$$(1 \leqslant \lambda \leqslant t).$$

If we assume that N is perfect then

$$2N = \sigma(N) = \sigma(p^\alpha)\sigma(q_1^2)\cdots\sigma(q_k^2)\sigma(r_1^2)\cdots\sigma(r_t^2)\sigma(s^4) =$$

(3)

$$\sigma(p^\alpha)\prod_{n=1}^{k}(1 + q_n + q_n^2)\prod_{\lambda=1}^{t}[(1 + r_\lambda + r_\lambda^2)](1 + s + s^2 + s^3 + s^4).$$

Here $(1 + q_n + q_n^2) \equiv 0 (\mathrm{mod}\ 3)$, $(1 \leqslant n \leqslant k)$ but $(1 + q_n + q_n^2) \not\equiv 0 (\mathrm{mod}\ 9)$, for $(1 \leqslant n \leqslant k)$. Also $(1 + r_\lambda + r_\lambda^2) \not\equiv 0 (\mathrm{mod}\ 3)$ for $(1 \leqslant \lambda \leqslant t)$.

We now consider some cases.

I. $N \not\equiv 0 (\mathrm{mod}\ 3)$. Here we have that $k = 0$, and since 3 does not divide N we know from a previous theorem due to Sylvester that N must contain at least 8 different primes, hence $t \geqslant 6$. Since $k = 0$, then by (3)

$$\prod_{\lambda=1}^{t}(1 + r_\lambda + r_\lambda^2)$$

divides

$$p^\alpha s^4.$$

One of the factors of this product could be a power of p, but none of the remaining factors could be a power of p by Lemma 1. This implies that each of these t-1 factors must be divisible by s, and hence their product would be divisible by s^5, a contradiction.

II. In the following cases it is first assumed that $N \equiv 0 \pmod 3$ where $N \not\equiv 0 \pmod{27}$ and secondly, that $s = 3$. This last case is easily disposed of by considering the necessary prime divisors of N. However, the first of these two cases is more difficult. It is disposed of in the following manner.

First a value for p is chosen and then the allowable values for q_n and s are ruled out and this is followed by new selections for p and further elimination of the values for q_n, r_λ and s. These eliminations are usually performed by using the elementary procedures already discussed. However, once the numbers become too large to be conveniently removed in this manner then the form of the divisors of (q_λ^2) is regulated by Lemma 2 which in turn lowers the number of factors of N until either t or k is below the necessary value, thus eliminating the remaining possibilities.

BIBLIOGRAPHY

1. Andree, V. Richard. Selections from Modern Abstract Algebra, Henry Holt and Company, 30-31, New York, 1958.

2. Bernhard, H. A. "On the Least Possible Odd Perfect Number," American Mathematical Monthly, Vol. 56, 628-629, 1949.

3. Brauer, Alfred. "On the Non-Existence of Odd Perfect Numbers of Form $p^{\alpha}q_1^2q_2^2 \cdots q_{t-1}^2q_t^4$," Bull. Amer. Math. Soc., Vol. 49, 712-718, 1943.

4. Brooke, Maxey. "On the Digital Roots of Perfect Numbers," Mathematics Magazine, Vol. 34, No. 2, 100-124, Nov.-Dec., 1960.

5. Dickson, Leonard Eugene. "Finiteness of Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors," Amer. Jour. Math., Vol. 35, 413-422, 1913.

6. Dickson, Leonard Eugene. History of the Theory of Numbers, Vol. I, 3-35, Carnegie Institute of Washington, Washington, 1919.

7. McCarthy, Paul J. "Odd Perfect Numbers," Scripta Mathematics, Vol. 23, 43-47, 1957.

8. Muskat, Joseph Baruch. "Results on Odd Perfect Numbers," Masters Thesis, Massachusetts Institute of Technology, 1956.

9. Norton, Karl K. "Remarks on the Number of Factors of an Odd Perfect Number," Acta Arithmetica, VI 4, 365-374, 1961.

10. Reynolds, Thomas L., "On the Non-Existence of an Odd Perfect number N, not Divisible by 5, with Six Different Prime Divisors," Ph.D. Dissertation, University of North Carolina, 1950.

11. Shapino, H. N. "Note on a Theorem of Dickson," Bull. Amer. Math. Soc., Vol. 55, 450-452, 1949.

12. Touchard, Jacques. "On Prime Numbers and Perfect Numbers," Scripta Mathematics, Vols. 19-20, 35-39, 1953-54.

13. Uhler, Horace S. "A Brief History of the Investigations on Mersenne Numbers and the Latest Immense Primes," Scripta Mathematics, Vol. 18, 122-131, 1952.

VITA

David Thomas Eastham

Born in Charlotte, North Carolina, November 8, 1940. Graduated from Warsaw High School, Warsaw, Virginia, June, 1959; B. A.; College of William and Mary, 1963. In January 1964, the author entered the College of William and Mary as a M. A. candidate in mathematics. From 1964-1965 the author held a part-time instructorship at the College of William and Mary.