On the Multiplicative Structure of Odd Perfect Numbers*

JOHN A. EWELL

Department of Mathematical Sciences, Northern Illinois University,
De Kalb, Illinois 60115

Communicated by H. Zassenhaus

Received July 10, 1978; revised February 26, 1979

Starting with Euler's theorem that any odd perfect number $n$ has the form $n = p^e_1 p^e_2 \cdots p^e_k$, where $p, p_1, \ldots, p_k$ are distinct odd primes and $p \equiv e \equiv 1 \pmod{4}$, we show that extensive subsets of these numbers (so described) can be eliminated from consideration. A typical result says: if $p^e_1, p^e_2, \ldots, p^e_k$ are all of the prime-power divisors of such an $n$ with $p \equiv p_1 \equiv 1 \pmod{4}$, then the ordered set $(e_1, \ldots, e_k)$ contains an even number or odd number of odd numbers according as $e \equiv p$ or $e \not\equiv p \pmod{8}$.

1. Introduction

For each positive integer $n$, $\sigma(n)$ denotes the sum of the positive divisors of $n$. A number $n$ is called perfect if and only if $\sigma(n) = 2n$. One of the celebrated open questions of number theory is whether or not there exist any odd perfect numbers. Like most papers on odd perfect numbers the present one takes as its point of departure the following theorem of Euler.

**Theorem 1.** If $n$ is an odd perfect number (if indeed such numbers exist), then

$$n = p^e \prod_{i=1}^{k} p_i^{2e_i},$$

where $p, p_1, \ldots, p_k$ are distinct odd primes and $p \equiv e \equiv 1 \pmod{4}$.

For proof see [1, p. 231]. The purpose of this note is to establish several refinements of Euler's theorem, among which the following theorem is typical.

* AMS (MOS) subject classifications (1970). Primary 10A20; Secondary 10A35.
THEOREM 2. Let \( n \) denote an odd perfect number described as in Euler's theorem. If the primes \( p_1, \ldots, p_k \) (together with their corresponding exponents) are relabeled as \( p_1, \ldots, p_r, q_1, \ldots, q_s \), so that each \( p_i \) \((i = 1, \ldots, r)\) is of the form \( 4x + 1 \) and each \( q_j \) \((j = 1, \ldots, s)\) is of the form \( 4x - 1 \), say,

\[
n = p^e \prod_{i=1}^{r} p_i^{2e_i} \prod_{j=1}^{s} q_j^{2f_j},
\]

then: (i) the ordered set \( S(r) = \{e_1, \ldots, e_r\} \) contains an even number of odd numbers, provided \( e \) and \( p \) belong to the same residue class \((\text{mod } 8)\); but, (ii) \( S(r) \) contains an odd number of odd numbers, provided \( e \) and \( p \) belong to different classes \((\text{mod } 8)\).

In Section 2 we prove this result, sharpen it, and finally establish a similar result which follows from examination of the congruence \( \sigma(n) \equiv 2n \) (mod 3).

2. PROOF OF THEOREM 2

Assume that \( n \) is an odd perfect number and write: \( n = p^e \prod_{i=1}^{k} p_i^{2e_i} \), \( p = 4\pi + 1, e = 4\varepsilon + 1, p_i = 2\pi_i - 1 \) \((i = 1, \ldots, k)\). Then, using the congruences \( p^2 \equiv p_i^2 \equiv 1 \) (mod 8), we get

\[
2n \equiv 2p \pmod{16},
\]

\[
\sigma(n) \equiv (1 + p + \cdots + p^{4\varepsilon + 1}) \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{2e_i})
\]

\[
\equiv (1 + p)(2\varepsilon + 1) \prod_{i=1}^{k} (1 + (1 + p_i)e_i)
\]

\[
\equiv 2(2\pi + 1)(2\varepsilon + 1) \prod_{i=1}^{k} (1 + 2\pi_i e_i) \pmod{16}.
\]

These congruences imply

\[
4\pi + 1 \equiv (4\pi \varepsilon + 2\pi + 2\varepsilon + 1) \left(1 + 2 \sum_{i=1}^{k} \pi_i e_i + 4 \sum_{i<j} \pi_i \pi_j e_i e_j\right) \pmod{8}. \quad (1)
\]

[Throughout this investigation we interpret \( i < j \) under a sigma-sum as \( 1 \leq i < j \leq k \).] Hence,

\[
\pi + \varepsilon + \sum_{i=1}^{k} \pi_i e_i \equiv 0 \pmod{2}. \quad (2)
\]

Now, the terms \( \pi_i e_i \) with \( \pi_i \) even correspond to the \( q_j \) \((j = 1, \ldots, s)\). Since
these terms vanish (mod 2), we therefore interpret (2) as just the conclusion of our theorem.

In order to realize a somewhat stronger result we use (2) to write \( \sum \pi_i e_i = n + \varepsilon + 2\lambda \), for some integer \( \lambda \). Hence,

\[
2 \sum_{i < j} \pi_i \pi_j e_i e_j \equiv (n + \varepsilon)^2 - \sum_{i=1}^{k} \pi_i^2 e_i^2 \pmod{4}
\]

We then use (1) and the foregoing congruence to obtain

\[
2n \equiv 2n + 2\varepsilon + 2\lambda + 2\pi \varepsilon + 3(n + \varepsilon)^2 - \sum_{i=1}^{k} \pi_i^2 e_i^2 \pmod{4}
\]

or

\[
\sum_{i=1}^{k} \pi_i^2 e_i^2 \equiv 3n^2 3\varepsilon^2 + 2\varepsilon + 2\lambda \pmod{4}. \tag{3}
\]

This is the desired sharpening of (2).

If \( n = p^e \prod_{i=1}^{k} p_i^{2e_i} \) is an odd perfect number, notation is the same as before and \( p_i \neq 3 \) (\( i = 1, \ldots, k \)), then: \( p^2 \equiv p_i^2 \equiv 1 \pmod{3} \) and

\[
\pi + 1 \equiv (1 - \pi)(1 - \varepsilon) \prod_{i=1}^{k} (1 - \pi_i e_i) \pmod{3}.
\]

The only condition compatible with hypothesis is \( \pi \equiv 0 \pmod{3} \), whence \( p \equiv 1 \pmod{12} \), whence

\[
1 \equiv (1 - \varepsilon) \prod_{i=1}^{k} (1 - \pi_i e_i) \pmod{3}. \tag{4}
\]

Interpretation of (4) thus yields the following.

**Theorem 3.** If \( n = p^e \prod_{i=1}^{k} p_i^{2e_i} \) is an odd perfect number such that \( e = 4\varepsilon + 1 \), \( p_i = 2\pi_i - 1 \) and \( p_i \neq 3 \) (\( i = 1, \ldots, k \)), then \( p \equiv 1 \pmod{12} \); \( \varepsilon \equiv 0 \) or \(-1 \pmod{3} \); each \( \pi_i e_i \equiv 0 \) or \(-1 \pmod{3} \); and the number of elements in the set \( \{ \pi_1 e_1, \pi_2 e_2, \ldots, \pi_k e_k \} \) for which \( \pi_i e_i \equiv -1 \pmod{3} \) is even or odd according as \( \varepsilon \equiv 0 \) or \(-1 \pmod{3} \).

**Acknowledgments**

The author would like to thank the referee for suggested improvement of the exposition. Special thanks are given to Professor E. G. Straus.
REFERENCES