ON THE TOTAL NUMBER OF PRIME FACTORS OF AN ODD PERFECT NUMBER

D. E. IANNUCCI AND R. M. SORLI

ABSTRACT. We say $n \in \mathbb{N}$ is perfect if $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of the positive divisors of n. No odd perfect numbers are known, but it is well known that if such a number exists, it must have prime factorization of the form $n = p^{\alpha} \prod_{j=1}^k q_j^{2\beta_j}$, where p, q_1, \ldots, q_k are distinct primes and $p \equiv \alpha \equiv 1 \pmod{4}$. We prove that if $\beta_j \equiv 1 \pmod{3}$ or $\beta_j \equiv 2 \pmod{5}$ for all $j, 1 \leq j \leq k$, then $3 \nmid n$. We also prove as our main result that $\Omega(n) \geq 37$, where $\Omega(n) = \alpha + 2 \sum_{j=1}^k \beta_j$. This improves a result of Sayers $\Omega(n) \geq 29$ given in 1986.

1. Introduction

A natural number n is said to be *perfect* if $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of the positive divisors of n. Euclid in Book IX of his *Elements* showed that $2^{p-1}(2^p-1)$ is perfect if 2^p-1 is a (Mersenne) prime; Euler showed that every even perfect number has this form.

The status of odd perfect numbers remains completely unknown. No odd perfect numbers are known, and a proof of their nonexistence remains elusive. In the meantime, many necessary conditions for their existence have been found. One such condition is a lower bound for the number of distinct prime factors of an odd perfect number.

If n has the unique prime factorization $\prod_{j=1}^k p_j^{\alpha_j}$, we write $\omega(n) = k$ and $\Omega(n) = \sum_{j=1}^k \alpha_j$, the number of distinct prime factors and the *total* number of prime factors, respectively. Chein [2] and Hagis [6] each showed that if n is an odd perfect number, then $\omega(n) \geq 8$. Furthermore, Hagis [7] and Kishore [9] each showed that if $3 \nmid n$, then $\omega(n) \geq 11$.

A related problem is that of finding a lower bound on $\Omega(n)$ for an odd perfect number n. The first significant result of this type was obtained by Cohen [3] in 1982 when he proved that $\Omega(n) \geq 23$. In 1986, Sayers [12] improved this result to obtain $\Omega(n) \geq 29$. In this paper, we will improve this lower bound to 37, and we state our result here:

Theorem 1. If n is an odd perfect number, then $\Omega(n) \geq 37$.

For the past several decades, necessary conditions for the existence of odd perfect numbers have been established with the extensive aid of computers, and Theorem 1

Received by the editor November 7, 2001.

²⁰⁰⁰ Mathematics Subject Classification. Primary 11A25, 11Y70.

Key words and phrases. Odd perfect numbers, factorization.

The authors are grateful for the advice and assistance given by Graeme Cohen.

is no exception. The proof, to be outlined in Sections 3 and 4, was obtained by writing and executing several programs with the *Mathematica* software system.

2. Preliminaries

Without further explicit mention, we will let N denote an odd perfect number. It is due to Euler, and it is well known that N has the shape given by

(1)
$$N = p^{\alpha} q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_k^{2\beta_k}$$

where p, q_1, \ldots, q_k are distinct primes, $\alpha, \beta_1, \ldots, \beta_k$ are positive integers, and $p \equiv \alpha \equiv 1 \pmod{4}$. The prime p is referred to as special. From (1), it follows that $\omega(N) = k+1$ and $\Omega(N) = \alpha+2\sum_{j=1}^k \beta_j$. We will assume that $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_k$. Since N is perfect and σ is multiplicative, we have

(2)
$$2N = \sigma(p^{\alpha}) \prod_{j=1}^{k} \sigma(q_j^{2\beta_j}).$$

It is clear from (1) and (2) that if r is an odd prime divisor of $\sigma(p^{\alpha})$ or of $\sigma(q_j^{2\beta_j})$ for some $j, 1 \leq j \leq k$, then $r \mid N$.

We shall use the notation

$$\sigma_{-1}(n) = \frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$$

for any natural number n. Thus $\sigma_{-1}(N) = 2$. It is easy to show that $\sigma_{-1}(d) < 2$ for any proper divisor d of N.

For prime p and natural number a, we have

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

It is clear that

$$\frac{p+1}{p} \le \sigma_{-1}(p^a) < \frac{p}{p-1}$$

and that $\sigma_{-1}(p^a) < \sigma_{-1}(p^b)$ if a < b. For odd primes p < q, we have q/(q-1) < (p+1)/p and thus

$$\sigma_{-1}(q^b) < \sigma_{-1}(p^a)$$

for any natural numbers a and b.

Referring back to (1), McDaniel [11] proved that if $\beta_j = 1$ or 2 for all j, then N has no prime factor less than 101. This result was extended by Cohen [4] who showed that N has no prime factor less than 739 under the same conditions. Cohen's result then implies that $\omega(N) \geq 47326$; this follows from (2), (3) and (4) since

$$2 = \sigma_{-1}(N) = \sigma_{-1}(p^a) \prod_{j=1}^k \sigma_{-1}(q_j^{2\beta_j}) < \frac{p}{p-1} \prod_{j=1}^k \frac{q_j}{q_j - 1}$$

and

$$\prod_{739$$

where the product is taken over the 47325 consecutive primes indicated. It follows (from McDaniel's result, in fact) that

(5) if
$$\beta_j = 1$$
 or 2 for all j , then $\Omega(N) > 35$.

Many similar results regarding the exponents β_j have appeared in the literature. We will apply some of these results to prove Theorem 1.

We first introduce some notation for the sake of brevity. For nonnegative integers $m, j, a_i \ge 1 \ (1 \le i \le m \text{ if } m > 0)$ and $b_i \ge 1 \ (1 \le i \le m + j \text{ if } m + j > 0)$, we let the expression

$$b_1(a_1), b_2(a_2), \ldots, b_m(a_m), b_{m+1}(*), \ldots, b_{m+j}(*)$$

represent the following: Of the set $\{\beta_1, \beta_2, \ldots, \beta_k\}$ of decreasing numbers,

- (i) at most a_i can equal b_i , $1 \le i \le m$,
- (ii) any element not equal to b_i , $1 \le i \le m$, must belong to $\{b_{m+1}, \ldots, b_{m+j}\}$ for which each member can occur an unrestricted number of times.

Then for x = 1, 3, or 5, we let the expression

(6)
$$[x:b_1(a_1),b_2(a_2),\ldots,b_m(a_m),b_{m+1}(*),\ldots,b_{m+j}(*)]$$

represent the following:

If x = 1, then items (i) and (ii) above are impossible.

If x = 3 and (i) and (ii) are true, then $3 \nmid N$.

If x = 5 and (i) and (ii) are true, then $3 \nmid N$ and $5 \nmid N$.

Some of the results we shall apply are then given as follows.

McDaniel [10] showed it is impossible to have $\beta_j \equiv 1 \pmod{3}$ for all $j, 1 \leq j \leq k$. This implies, sufficient for our purposes,

$$[1:10(*),7(*),4(*),1(*)],$$

that is, the exponents $2\beta_1, \ldots, 2\beta_k$ cannot all belong to $\{2, 8, 14, 20\}$. (Steuerwald [13] had previously obtained [1:1(*)].) Cohen and Williams [5] showed it is impossible to have $\beta_1 = 5$ or 6 and $\beta_j = 1$ for all $j, 2 \le j \le k$. These results give us, respectively,

$$[1:5(1),1(*)],$$

(9)
$$[1:6(1),1(*)].$$

Brauer [1] showed that $\beta_1 = 2$, $\beta_j = 1$ for all j, $2 \le j \le k$, is impossible, and Kanold [8] showed that $\beta_1 = 3$, $\beta_j = 1$ for all j, $2 \le j \le k$, is impossible. Cohen [3] showed that $\beta_1 = 3$, $\beta_2 = 2$, $\beta_j = 1$ for all j, $3 \le j \le k$, is impossible. These three results, combined with that of Steuerwald, give us

$$[1:3(1),2(1),1(*)].$$

Steuerwald's result, along with Theorem 2 in Sayers [12], gives us

$$[1:3(3),1(*)].$$

3. The proof of Theorem 1, part 1

We first assume that $\Omega(N) = 35$. Then (5) becomes equivalent to

$$[1:2(*),1(*)],$$

and this, in conjunction with Theorem 3 in Sayers [12], then gives us

$$[1:4(1),2(4),1(*)].$$

There are exactly 686 possible cases for the exponents in (1) when $\Omega(N) = 35$; these range from $\alpha = 33$, k = 1, $\beta_1 = 1$, to $\alpha = 1$, k = 17, $\beta_1 = \cdots = \beta_{17} = 1$. The condition $\omega(N) \geq 8$ eliminates exactly 439 of these cases. Of the remaining 247 cases, exactly 81 are further eliminated by conditions (7) through (13). This leaves 166 cases to consider.

Of these 166 cases, exactly 136 satisfy $\omega(N) \leq 10$. Recalling that $\omega(N) \geq 11$ if $3 \nmid N$, 120 of these 136 cases are eliminated once we prove the following fourteen lemmata:

- [3:3(5),1(*)],
- [3:4(1),3(3),2(1),1(*)],
- [3:5(2),3(1),1(*)],
- [3:5(2),2(2),1(*)],
- [3:5(1),4(2),1(*)],
- [3:5(1),3(3),2(2),1(*)],
- [3:6(2),1(*)],
- [3:6(1),5(1),4(1),3(1),2(*),1(*)],
- [3:6(1),3(2),2(1),1(*)],
- [3:7(1),5(1),1(*)],
- [3:7(1),3(2),1(*)],
- [3:8(1),3(1),2(*),1(*)],
- [3:9(1),3(1),2(*),1(*)],
- [3:11(1),1(*)].

(For example, (14) states: If, in (1), $2\beta_1 = \cdots = 2\beta_l = 6$ for $1 \leq l \leq 5$ and $2\beta_{l+1} = \cdots = 2\beta_k = 2$, then $3 \nmid N$.)

The remaining sixteen cases (of the 136 mentioned above) are eliminated once we prove three further lemmata, namely

- [3:4(3),2(1),1(*)],
- [3:7(1),4(1),2(1),1(*)],
- [3:10(1),2(1),1(*)],

and these are all special cases of the following:

Theorem 2. If $N = p^{\alpha} \prod_{j=1}^{k} q_j^{2\beta_j}$ is an odd perfect number and $\beta_j \equiv 1 \pmod{3}$ or $\beta_j \equiv 2 \pmod{5}$ for all $j = 1, 2, \ldots, k$, then $3 \nmid N$.

This leaves exactly 30 cases to consider. In each of these remaining cases, we have $\omega(N) \leq 14$. It follows from (3) and (4) that $\omega(N) \geq 15$ if $3 \nmid N$ and $5 \nmid N$

since

$$\prod_{7$$

the product being over the 14 primes indicated. The remaining 30 cases are then eliminated once we prove the following five lemmata:

$$[5:3(4),2(*),1(*)],$$

$$[5:4(2),3(2),2(*),1(*)],$$

$$[5:6(1),5(1),4(1),3(1),2(*),1(*)],$$

$$[5:7(1),3(1),2(*),1(*)],$$

$$[5:8(1),4(1),1(*)].$$

Lemmata (7) through (35) will also eliminate every possible case for the exponents in (1) if we assume any one of $\Omega(N) = 29$, 31, or 33. Therefore, recalling that it is known that $\Omega(N) \geq 29$ (Sayers [12]), it suffices, for the proof of Theorem 1, to prove the lemmata stated in (14) through (35); we outline these proofs in the following section.

The lemmata (14) through (35) are all independent and quite specific for our purposes, although they all contain some generality in allowing an unrestricted number of exponents equal to 2, and in some cases an unrestricted number of exponents equal to 4. Theorem 2, by which we prove (28) through (30), would have greater applicability.

4. The proof of Theorem 1, part 2

Theorem 2 and the lemmata are all proved by contradiction.

For lemmata (14) through (27), we assume separately in each case that $3 \mid N$ and we obtain a contradiction at the end of a chain of factorizations, in manners to be described shortly.

Call an exact prime-power divisor p^a of N a component of N and write $p^a \parallel$ N; then $p^{a+1} \nmid N$. The factorization chains are constructed systematically, one component at a time, beginning with 3^2 , or 3^4 , or ..., with, in practice, each new component implying at least one additional candidate prime divisor (since an odd perfect number was not found!). For example, if N is an odd perfect number and, by assumption, $3^2 \parallel N$, then $13 \mid N$ since $\sigma(3^2) = 13$ and $\sigma_{-1}(3^2 \cdot 13^a) < 2$ for any natural number a. Then $13 \parallel N$ (since 13 may be the special prime) so $7 \mid N$ since $\sigma(13) = 2.7$ and $\sigma_{-1}(3^2 \cdot 13 \cdot 7^a) < 2$; or $13^2 \parallel N$ so $61 \mid N$ since $\sigma(13^2) = 3.61$ and $\sigma_{-1}(3^2\cdot 13^2\cdot 61^a) < 2$; or $13^4 \parallel N$ so (The algorithm is illustrated in Table 1.) If there is more than one candidate prime divisor available, then choosing the smallest as the basis for the next component of N results in the greatest increase in $\sigma_{-1}(N')$ (and hence usually the shortest path to a contradiction), where N' is the product of the components so far assumed or as yet unexplored (and in the latter case, for the purpose of calculating $\sigma_{-1}(N')$, they are given their smallest possible exponent). For each prime chosen to continue a chain, exponents are investigated as allowed by the exponent pattern for the lemma under consideration. (If the candidate prime might be the special prime, then only the exponent 1 is considered for it, since $p+1=\sigma(p)\mid \sigma(p^{\alpha}), \text{ when } p\equiv \alpha\equiv 1\pmod{4}.$

Table 1. Beginning the proof of [3:5(1),2(1),1(*)].

```
3^2 \Rightarrow 13^a
 13^1 \Rightarrow 7^b
  7^2 \Rightarrow 3 \cdot 19
   19^2 \Rightarrow 3 \cdot 127
    127^2 \Rightarrow 3 \cdot 5419 \text{ xs}=3^{\circ}
    127^4 \Rightarrow 262209281
     262209281^2 \Rightarrow 13 \cdot 1231 \cdot 4296301150081^d
      1231^2 \Rightarrow 3 \cdot 13 \cdot 37 \cdot 1051 \text{ xs} = 3
       1231^{10} \Rightarrow 23 \cdot 67 \cdot 3323 \cdot 38237 \cdot 40842910222965466771 \text{ S} = 2.04507^{\text{e}}
     6865379200955135391524384965083073728767674853 S = 2.04490^{f}
    127^{10} \Rightarrow 23 \cdot 47834644354838156839 \text{ S} = 2.01226
    19^4 \Rightarrow 151 \cdot 911
    151^2 \Rightarrow 3 \cdot 7 \cdot 1093
     911^2 \Rightarrow 830833^g
       1093^2 \Rightarrow 3 \cdot 39858 \text{ xs} = 3
       1093^{10} \Rightarrow 23 \cdot 6491 \cdot 2608387 \cdot 6254429058851062673 \text{ S} = 2.01438
     911^{10} \Rightarrow 67 \cdot 472319 \cdot 50390258557 \cdot 247174661801
      67^2 \Rightarrow 3 \cdot 7^2 \cdot 31 \text{ xs} = 3
    151^{10} \Rightarrow 23 \cdot 14864609 \cdot 18145704541823 S=2.01223
    19^{10} \Rightarrow 104281 \cdot 62060021
    104281^2 \Rightarrow 3 \cdot 7 \cdot 43 \cdot 67 \cdot 179743
     43^2 \Rightarrow 3.631 \text{ xs}=3
     43^4 \Rightarrow 3500201
      67^2 \Rightarrow 3 \cdot 7^2 \cdot 31 \text{ xs} = 3
    104281^4 \Rightarrow 5 \cdot 41 \cdot 3181 \cdot 181345750520141 \text{ S} = 2.42843
  7^4 \Rightarrow 2801
   2801^2 \Rightarrow 37 \cdot 43 \cdot 4933
    37^2 \Rightarrow 3 \cdot 7 \cdot 67
     43^2 \Rightarrow 3 \cdot 631
      67^2 \Rightarrow 3 \cdot 7^2 \cdot 31 \text{ xs} = 3
      67^{10} \Rightarrow 11 \cdot 89 \cdot 1890149702927663 \text{ S} = 2.15947
     43^{10} \Rightarrow 60381099 \cdot 3664405207
      67^2 \Rightarrow 3 \cdot 7^2 \cdot 31 \text{ S} = 2.00408
    37^{10} \Rightarrow 2663 \cdot 1855860368209
     43^2 \Rightarrow 3 \cdot 631
      631^2 \Rightarrow 3 \cdot 307 \cdot 433
       307^2 \Rightarrow 3 \cdot 43 \cdot 733 \text{ xs} = 3
```

^aConvenient notation for odd prime factors of $\sigma(3^2) = 13$; further factorizations in the chain are indicated by indentations.

b13 could be the special prime.

^cContradiction: an excess of 3's.

^dAlthough $262209281 \equiv 1 \pmod 4$, the smallest possible exponent is 2, since 13 is currently the special prime.

eContradiction: $S = \sigma_{-1}(3^2 13^1 7^2 19^2 127^4 262209281^2 1231^{10} \cdot 23^2 67^2 \dots) > 2$.

^fThe program would not need to fully factorize $\sigma(262209281^{10})$: it would calculate $S=\sigma_{-1}(3^213^17^219^2127^4262209281^{10}\cdot 23^267^2947^2)>2$.

gThe smallest unexplored prime, 911 here rather than 1093, is used to continue the chain.

If $q^{2\beta}$ (or p^{α}) is the new additional assumed component of N, then the set of assumed prime divisors of N needs to be updated with the prime divisors of $\sigma(q^{2\beta})$ (or of $\sigma(p)/2$). A chain is continued while $\sigma_{-1}(N') < 2$. However, it can be observed that the larger assumed primes make little contribution to the value of $\sigma_{-1}(N')$. We can take advantage of this by finding only the "small" prime divisors of $\sigma(q^{2\beta})$ (or of $\sigma(p)/2$), perhaps leaving a single "hard" composite. Any such composites are easily identified and then excluded from the calculation of $\sigma_{-1}(N')$. This underestimates the value of $\sigma_{-1}(N')$ and may lead to slightly longer chains in some cases but this is more than offset by the substantial reduction in factorization time. If there is no unexplored prime available from earlier factorizations with which to continue the chain, then it is necessary to factor one of the composites carried forward (and in practice the most recently added composite was used).

For the proofs of lemmata (14) through (27), an additional constraint, that each (nonspecial) prime factor q of N occurred to a given exponent 2β , so that $q^b \parallel \sigma(N')$ for $b \leq 2\beta$, was employed to allow another contradiction that could terminate a chain. A violation of this constraint (when so many primes q arose from factorizations as to imply $b > 2\beta$) was described as saying there was an excess of the prime q.

For the proofs of each of lemmata (31) through (35), we first showed that $3 \nmid N$, as above, and then assumed that $5 \mid N$; in a similar manner, this was also shown to lead to a contradiction.

The proof of Theorem 2 was accomplished by assuming $3 \mid N$, ignoring the second possible contradiction (of an excess of primes), and employing the facts that $\sigma(q^2) \mid \sigma(q^{2\beta})$ when $\beta \equiv 1 \pmod{3}$ and $\sigma(q^4) \mid \sigma(q^{2\beta})$ when $\beta \equiv 2 \pmod{5}$. Only exponents with $\beta = 1$ or 2 were assumed (on nonspecial primes), and the only contradiction used to terminate a chain was $\sigma_{-1}(N') > 2$.

5. Implementation

The most novel feature of the algorithm is the effective use of incomplete factorizations. This was implemented as follows. If the composite was less than a chosen bound, usually 10^{15} , then the complete factorization was carried out (with minimal effort). For composites greater than the bound, a stored list of complete factorizations was searched. If the desired factorization was not found, then an incomplete factorization was carried out using the FactorComplete->False option of the FactorInteger[] function of Mathematica. (Maple has a similar `easy` option for its ifactor() function.) In Mathematica, for incomplete factorization, only the trial division, Pollard p-1, Pollard rho and continued fraction methods of factorization are applied to find "small" factors, in some combination not detailed in the accompanying documentation.

To help clarify the algorithm, see Table 1, which shows the beginning of the computational proof of [3:5(1),2(1),1(*)] (in fact subsumed by lemma (17)). In this example, full factorizations are shown although the opportunity for partial factorization is noted.

If it became necessary for the continuation of a chain to have the full factorization of a composite, then this was established separately either by looking up known tables or by calculation. A list of needed, complete factorizations would then be updated within the program.

The most difficult factorization required was that of $\sigma(\sigma(61^6)^{16})$, the product of a 73-digit prime and a 100-digit prime. This was realized through the assistance of Herman te Riele and Peter Montgomery at CWI, to whom we are most grateful.

6. ECONOMIZATION

The patterns of exponents represented by the lemmata are the result of amalgamation through generalization of the patterns of the original 166 cases. Initially, we experimented with generalizations of the form [3:...,1(*)], that is, an unrestricted number of components with an exponent of 2. Then patterns like [3:...,2(*),1(*)] were selectively tried. This was followed by generalizations such as [3:3(1),2(*),1(*)],...,[3:3(4),2(*),1(*)]. Another series of generalizations investigated was [3:3(1),2(*),1(*)],...,[3:6(1),5(1),4(1),3(1),2(*),1(*)]. This last pattern (lemma (21)) involved the generation of a computational proof of almost nine million lines. In each case, practical considerations determined how comprehensive the generalization could be made.

REFERENCES

- [1] A. Brauer, On the nonexistence of odd perfect numbers of the form $p^{\alpha}q_1^2q_2^2\cdots q_{t-1}^2q_t^4$ Bull. Amer. Math. Soc. **49** (1943), 712–718. MR **9:**90b
- [2] E. Z. Chein, Ph.D. Thesis, Pennsylvania State University (1979).
- [3] G. L. Cohen, On the total number of prime factors of an odd perfect number Appendix A.3, Ph.D. Thesis, University of New South Wales (1982).
- [4] ______, On the largest component of an odd perfect number J. Austral. Math. Soc. Ser. A 42 (1987), 280–286. MR 87m:11005
- [5] G. L. Cohen and R. J. Williams, Extensions of some results concerning odd perfect numbers
 J. Fibonacci Quart. 23 (1985), 70–76. MR 86f:11009
- [6] P. Hagis, Outline of a proof that every odd perfect number has at least eight prime factors Math. Comp. 35 (1980), 1027–1032. MR 81k:10004
- [7] P. Hagis, Sketch of a proof that every odd perfect number relatively prime to 3 has at least eleven prime factors Math. Comp. 40 (1983), 399-404. MR 85b:11004
- [8] H.-J. Kanold, Sätze über kreisteilungspolynome und ihre andwendungen auf einiger zahlentheoretische problem II J. Reine Angew. Math. 188 (1950), 129-146. MR 13:443b
- [9] M. Kishore, Odd perfect numbers not divisible by three are divisible by at least eleven distinct primes Math. Comp. 40 (1983), 405-411. MR 84d:10009
- [10] W. McDaniel, The nonexistence of odd perfect numbers of a certain form Arch. Math. 21 (1970), 52-53. MR 41:3369
- [11] W. McDaniel, On the divisibility of an odd perfect number by the sixth power of a prime Math. Comp. 25 (1971), 383–385. MR 45:5074
- [12] M. Sayers, M.App.Sc. Thesis, New South Wales Institute of Technology (1986).
- [13] R. Steuerwald, Verschärfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl S.-B. Math.-Nat. Abt. Bayer. Akad. Wiss. (1937), 68-73.

UNIVERSITY OF THE VIRGIN ISLANDS, St. THOMAS, VIRGIN ISLANDS 00802 $E\text{-}mail\ address:}$ diannuc@uvi.edu

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF TECHNOLOGY, SYDNEY, BROADWAY, 2007, AUSTRALIA

E-mail address: rons@maths.uts.edu.au