EXTENSIONS OF SOME RESULTS CONCERNING ODD PERFECT NUMBERS

G. L. COHEN and R. J. WILLIAMS
The New South Wales Institute of Technology,
Broadway, New South Wales, 2007, Australia
(Submitted July 1983)

1. INTRODUCTION

Throughout this paper we shall suppose that N is an odd perfect number, so that N is an odd integer and $\sigma(N) = 2N$, where σ is the positive-divisor-sum function. There is no known example of an odd perfect number, and it has not been proved that none exists. However, a great number of necessary conditions which must be satisfied by N have been established. The first of these, due to Euler, is that

$$N = p^{\alpha} q_1^{2\beta_1} \ \dots \ q_t^{2\beta_t}$$

for distinct odd primes $p, q_1, \dots, q_t$, with $p \equiv \alpha \equiv 1 \pmod 4$. (We shall always assume this form for the prime factor decomposition of N). Many writers have found conditions which must be satisfied by the exponents $2\beta_1, \dots, 2\beta_t$, and it is our intention here to extend some of those results. We shall find it necessary to call on a number of conditions of other types, some of which have only recently been found. These are outlined in Section 2.

It is known (see [8]) that we cannot have $\beta_i \equiv 1 \pmod 3$ for all i or (see [9]) $\beta_i \equiv 17 \pmod{35}$ for all i. Also, if $\beta_1 = \cdots = \beta_t = \beta$, then: from [6], $\beta \neq 2$; from [4], $\beta \neq 3$; and from [9], $\beta \neq 5$, 12, 24, or 62. We shall prove

Theorem 1. If N as above is an odd perfect number and $\beta_1 = \cdots = \beta_t = \beta$, then $\beta \neq 6$, 8, 11, 14, or 18.

The possibility that $\beta_2 = \cdots = \beta_t = 1$ (with $\beta_1 > 1$) has also been considered. In this case, it is known (see [1]) that $\beta_1 \neq 2$ and (see [7]) that $\beta_1 \neq 3$; by a previously mentioned result [8], we also have that $\beta_1 \not\equiv 1 \pmod 3$. We shall prove

Theorem 2. If N as above is an odd perfect number and $\beta_2 = \cdots = \beta_t = 1$, then $\beta_1 \neq 5$ or 6.

The computations required to prove these two theorems were mostly carried out on the Honeywell 66/40 computer at The New South Wales Institute of Technology. We also made use of some factorizations in [10].

Finally, we shall introduce a theorem whose proof is quite elementary, but it is a result which, to our knowledge, has not been noted previously. Euler's form for N, shown above, follows quickly by considering the equation $\sigma(N) = 2N$, modulo 4. Using the modulus 8 instead, we will obtain

Theorem 3. If N as above is an odd perfect number and x is the number of prime powers $q_i^{2\beta_i}$ in which both $q_i \equiv 1 \pmod 4$ and $\beta_i \equiv 1 \pmod 2$, then

$$p - \alpha \equiv 4x \pmod 8.$$

To obtain the following corollary, we then only need to notice that $x = 0$.

Corollary. If N as above is an odd perfect number and $\beta_i \equiv 0 \pmod 2$ for all i, then $p \equiv \alpha \pmod 8$.

2. PRELIMINARY RESULTS

Since we are assuming that $\sigma(N) = 2N$, it is clear in the first place that any odd divisor of $\sigma(N)$ is also a divisor of N. The proof of Theorem 1 makes use of the following facts.

(i) N is divisible by $(p + 1)/2$ (since α is odd).

(ii) If q and $2\beta + 1 = r$ are primes, then $r|\sigma(q^{2\beta})$ if and only if $q \equiv 1$ (mod r). Furthermore, if $r|\sigma(q^{2\beta})$, then $r\|\sigma(q^{2\beta})$. If $s|\sigma(q^{2\beta})$ and $s \neq r$, then $s \equiv 1$ (mod r). (This is a special case of results given, for example, in [9].)

(iii) If $\beta_1 = \cdots = \beta_t = \beta$ and $2\beta + 1 = r$ is prime, then $r^4|N$ and $p \equiv 1$ (mod r). In particular, $p \neq r$. (See [6] for generalizations of this.)

(iv) If $n|N$, then $\sigma(n)/n \leqslant 2$.

The proof of Theorem 2 uses (i), (ii), and (iv), as well as the following results.

(v) The second greatest prime factor of N is at least 1009 (see [3]) and the greatest at least 100129 (see [5]).

(vi) The equation $q^2 + q + 1 = p^a$ has no solution in primes p and q if a is an integer greater than 1 (see [1]).

3. PROOF OF THEOREM 1

We shall assume that $\beta = 6, 8, 11, 14$, and 18, in turn, and in each case obtain a contradiction, usually along the following lines. In each case, $2\beta + 1 = r$ is prime so that, by (iii), $r^{2\beta}\|N$. Then $\sigma(r^{2\beta})|N$. If s is prime, $s \neq p$ and $s|\sigma(r^{2\beta})$, then $s \equiv 1$ (mod r) and $s^{2\beta}\|N$, so that $r\|\sigma(s^{2\beta})$, by (ii). Applying the same process to other prime factors of $\sigma(s^{2\beta})$ and repeating it sufficiently often, we find that $r^{2\beta+1}|N$, which is our contradiction.

Except in the case $\beta = 8$, we were not able to carry out sufficiently many factorizations explicitly. (We generally restricted ourselves to seeking prime factors less than 5×10^6.) However, we were able to test whether unfactored quotients were pseudoprime (base 3) or not. Each P below is a pseudoprime and each M is an unfactored quotient which is not a pseudoprime, and hence is not a prime. We checked that each M was not a perfect power so that the existence of two distinct prime factors of each M was assured. We checked also that no M's or P's within each case had any prime factors in common with each other or with known factors of N. In this way, we could distinguish sufficiently many distinct prime factors of N to imply that $r^{2\beta+1}|N$. There is a slightly special treatment required when $\beta = 6$.

We shall give the details of the proof here only in the cases $\beta = 6$ and $\beta = 11$. These illustrate well the methods involved. The other parts of the proof are available from the first named author.

(a) Suppose $\beta = 6$, so that $13^{12}\|N$; $\sigma(13^{12}) = 53 \cdot 264031 \cdot 1803647$. The relevant factorizations are given in Table 1. We distinguish two main cases.

Table 1

	q	Some factors of $\sigma(q^{12})/13$
	53	3297113, P_1
	264031	P_2
	1803647	131, M_1
	131	79, Q
	79	M_2
(A)	131	$Q = M_3$
(B)	131	$Q = q_9$
	q_9	q_{10}

Suppose first that $p \neq 53$. We may assume that $q_{2i-1}q_{2i} | M_i$ (i = 1, 2) and $q_{j+4} | P_j$ (j = 1, 2). In Table 1, Q is also a pseudoprime (base 3) and we need to consider two distinct alternatives. In (A), we suppose that $Q = M_3$ is composite, so that $q_7q_8 | M_3$, say. (We checked that Q was not a perfect power.) In (B), we suppose that Q is prime, so we write $Q = q_9$. If this is so, then $q_9 \neq p$, since $Q \equiv 3 \pmod 4$. Thus, we have 14 primes:

53, 79, 131, 264031, 1803647, 3297113, q_i $(1 \leqslant i \leqslant 6)$

with q_7 and q_8, or with q_9 and q_{10}. Each of these primes is congruent to 1 (mod 13) and at most one of them might be p. Put

$$\Lambda = \{53, 79, 131, 264031, 1803647, 3297113, M_1, M_2, P_1, P_2, Q, (Q^{13}-1)/(Q-1)\}.$$

We checked that no two elements of Λ had a common prime factor; therefore, the 14 primes above are distinct. Hence, $13^{13} | N$, the desired contradiction.

Now suppose that $p = 53$. By (i), $3 | N$ and so $\sigma(3^{12}) = 797161 | N$. Certainly there is a prime q_{11} dividing $\sigma(797161^{12})/13$. We thus have 13 primes:

79, 131, 264031, 797161, 1803647, q_i $(1 \leqslant i \leqslant 4)$, q_6, q_{11}

with q_7 and q_8, or with q_9 and q_{10}. Each of these is congruent to 1 (mod 13), and we checked that no two elements of the set

$$(\Lambda - \{53, 3297113, P_1\}) \cup \{797161, \sigma(797161^{12})/13\}$$

had a common prime factor. Hence, again, $13^{13} | N$.

(b) Suppose $\beta = 11$, so that $23^{22} \| N$, and note that

$$\sigma(23^{22}) = 461 \cdot 1289 \cdot M_1.$$

Now refer to Table 2, where an asterisk signifies that the prime is 1 (mod 4), when that is relevant.

There are three cases to consider. First, suppose that $p = 1289$. By (i), $3 \cdot 5 | N$ so that $n_1 | N$ where $n_1 = (3 \cdot 5 \cdot 23 \cdot 47)^{22}$; but $\sigma(n_1)/n_1 > 2$, contradicting (iv). Similarly, if $p = 461$, then we have $3 \cdot 7 \cdot 11 | N$ so that $n_2 | N$ where $n_2 = (3 \cdot 7 \cdot 11 \cdot 23)^{22}$; but $\sigma(n_2)/n_2 > 2$.

Now suppose that $p \neq 461$ and $p \neq 1289$. We may suppose that $q_{2i-1}q_{2i} | M_i$ $(1 \leqslant i \leqslant 7)$ and $q_{15} | P$. Thus, N is divisible by the following 24 primes, each 1 (mod 23):

47, 139, 461, 1289, 37123, 133723, 281153, 300749, 2258831, q_i $(1 \leqslant i \leqslant 15)$.

Table 2

q	Some factors of $\sigma(q^{22})/23$
461*	139, 133723, P
133723	47, 37123, 2258831, $461 \cdot M_2$
2258831	300749,* M_3
1289*	281153,* M_4
47	M_5
139	M_6
37123	M_7

We checked that the 24 primes given above were distinct. One of them might be p, so $23^{23} | N$, our usual contradiction.

This shows that $\beta \neq 11$. We remark that we also looked at the remaining possible values of β less than 15, namely, 9, 15, 20, 21, and 23, without further success.

4. PROOF OF THEOREM 2

We begin by proving more than is stated in Theorem 2 in the case in which $3 \nmid N$.

Lemma. If N as before is an odd perfect number, $3 \nmid N$ and $\beta_2 = \cdots = \beta_t = 1$, then $\beta_1 \neq 5$, 6, or 8.

Proof: We will show first that, if $\beta_1 = 5$, 6, or 8, then $7 \nmid N$. Notice that $q_i \equiv 2 \pmod 3$ $(2 \leqslant i \leqslant t)$, since, otherwise, $3 | \sigma(q_i^2) | N$. In particular, $7^2 \nmid N$, so that $q_1 = 7$ if $7 | N$. In that case, we obtain contradictions, as follows.

If $\beta_1 = 5$, then $7^{10} | N$. But $1123 | \sigma(7^{10}) | N$ and $p \neq 1123$, so $1123^2 \| N$. But $1123 \equiv 1 \pmod 3$. If $\beta_1 = 6$, then $7^{12} \| N$. Then $r = \sigma(7^{12}) = 16148168401 | N$; if $r = p$, then $103 | N$, by (i). However, $103 \equiv r \equiv 1 \pmod 3$. If $\beta_1 = 8$, then $7^{16} \| N$, $14009 | \sigma(7^{16}) | N$. Then $p \neq 14009$, else $3 | N$ by (i), so $14009^2 \| N$. But $223 | \sigma(14009^2)$ and $223 \equiv 1 \pmod 3$.

Now we can show that $13 \nmid N$ for any of these values of β_1. Since N is not divisible by either 3 or 7, we must have $q_1 = 13$ if $13 | N$. Then $\beta_1 \neq 5$, else $23 | \sigma(13^{10}) | N$ and $7 | \sigma(23^2) | N$. Also, $\beta_1 \neq 6$, else $264031 | \sigma(13^{12}) | N$ and $264031 \equiv 1 \pmod 3$. Similarly, $\beta_1 \neq 8$, else $103 | \sigma(13^{16}) | N$.

Notice next that, by (ii), divisors of $\sigma(q_i^2)$ $(2 \leqslant i \leqslant t)$ are congruent to $1 \pmod 3$, so that $\sigma(q_i^2) = p^{a_i} q_1^{b_i}$ for some a_i, b_i $(0 \leqslant a_i \leqslant \alpha,\ 0 \leqslant b_i \leqslant 2\beta_1)$ and for each i $(2 \leqslant i \leqslant t)$. There can be at most $2\beta_1$ values of $i \geqslant 2$ such that $q_1 | \sigma(q_i^2)$; by (vi), there is at most one value of $i \geqslant 2$ such that $\sigma(q_i^2) = p^c$ $(c \geqslant 1)$. It follows that N has at most $2\beta_1 + 3$ distinct prime factors. Of these, at most two are congruent to $1 \pmod 3$, namely, p and q_1. By (i), certainly $p \equiv 1 \pmod 3$, so that in fact $p \equiv 1 \pmod{12}$.

In our case, when $\beta_1 = 5$, 6, or 8, we must have $p \geqslant 37$ (since $13 \nmid N$) and has at most 19 distinct prime factors. Using (v), we can now obtain the final contradiction which proves the lemma:

$$2 = \frac{\sigma(N)}{N} = \frac{p - p^{-\alpha}}{p - 1} \prod_{i=1}^{t} \frac{q_i - q_i^{-2\beta_i}}{q_i - 1} < \frac{p}{p - 1} \prod_{i=1}^{t} \frac{q_i}{q_i - 1}$$

(continued)

$$< \frac{5}{4}\,\frac{11}{10}\,\frac{17}{16}\,\frac{19}{18}\,\frac{23}{22}\,\frac{29}{28}\,\frac{37}{36}\,\frac{41}{40}\,\frac{47}{46}\,\frac{53}{52}\,\frac{59}{58}\,\frac{71}{70}\,\frac{83}{82}\,\frac{89}{88}\,\frac{101}{100}\,\frac{107}{106}\,\frac{113}{112}\,\frac{1009}{1008}\,\frac{100129}{100128} < 2.$$

We shall give the remaining details only in the case $\beta_1 = 6$; the proof for the case $\beta_1 = 5$ is available from the first named author. By the Lemma, we can assume that $3|N$.

We will assume first that $q_1 = 3$. Then $797161 = \sigma(3^{12})|N$. We cannot have $p = 797161$ because then, by (i), $398581^2\|N$: $1621|\sigma(398581^2)$, $7 \cdot 13|\sigma(1621^2)$, $19|\sigma(7^2)$, and $127|\sigma(19^2)$, so that $n|N$, where $n = 3^{12}(7 \cdot 13 \cdot 19 \cdot 127)^2$; but $\sigma(n)/n > 2$ and (iv) is contradicted. Hence, $797161^2\|N$.

Notice that $\sigma(797161^2) = 3 \cdot 61 \cdot 151 \cdot 22996651$; also note that $7|\sigma(151^2)$ and $19|\sigma(7^2)$. Thus, $7^2 19^2\|N$. Making use of (i), we then see that $p \neq 1693$, since then $(p + 1)/2 = 7 \cdot 11^2$ and $7|\sigma(11^2)$, so that $7^3|N$, and $p \neq 433$, since then $(p + 1)/2 = 7 \cdot 31$, $331|\sigma(31^2)$ and $7|\sigma(331^2)$, so that again $7^3|N$. We now observe that

$$43|\sigma(22996651^2),\quad 631|\sigma(43^2),\quad 433|\sigma(631^2),\quad 1693|\sigma(433^2),\quad 13|\sigma(1693^2),$$

so that $n|N$, where $n = 3^{12}13(7 \cdot 19 \cdot 43)^2$; but $\sigma(n)/n > 2$, contradicting (iv).

Now, we assume that $3^2\|N$, so that we can have at most two values of $i \geqslant 2$ with $q_i \equiv 1 \pmod 3$. We have $13 = \sigma(3^2)|N$.

First, we will suppose that $p = 13$, so that, by (i), $7|N$. We cannot have $q_1 = 7$, because $\sigma(7^{12}) = 16148168401 = r$ is prime, $433|\sigma(r^2)$, $37|\sigma(433^2)$, and $37 \equiv 433 \equiv r \equiv 1 \pmod 3$. Hence, $7^2\|N$, so $19|\sigma(7^2)|N$. Again, $q_1 \neq 19$, because $599 \cdot 29251|\sigma(19^{12})$, $51343|\sigma(599^2)$, and $29251 \equiv 51343 \equiv 1 \pmod 3$. Thus, $19^2\|N$ and for no further values of i can be have $q_i \equiv 1 \pmod 3$. Therefore, we have $127|\sigma(19^2)|N$.

Clearly, $127^2 \nmid N$, so $q_1 = 127$. Setting $q_2 = 7$ and $q_3 = 19$, we must have, for $i \geqslant 4$, $\sigma(q_i^2) = 7^{a_i}13^{b_i}19^{c_i}127^{d_i}$ where $a_i \leqslant 1$, $b_i \leqslant \alpha$, $c_i \leqslant 1$, and $d_i \leqslant 11$, since, by (ii), any other prime divisors of $\sigma(q_i^2)$ would be congruent to 1 (mod 3). Using (vi), as in the proof of the Lemma, it follows that there are at most 14 primes q_i with $i \geqslant 4$. We cannot have $11|N$ [although $\sigma(11^2) = 7 \cdot 19$], since then $n|N$, where $n = 3^2 7^2 11^2 13 \cdot 19^2$; but $\sigma(n)/n > 2$, contradicting (iv). Possibly $107|N$, since $\sigma(107^2) = 7 \cdot 13 \cdot 127$, but we find that no other prime less than 500 can be q_i for some $i \geqslant 4$. Then we have our contradiction: there are 13 primes q, $503 \leqslant q \leqslant 653$, that are congruent to 2 (mod 3); thus,

$$2 = \frac{\sigma(N)}{N} < \frac{\sigma(3^2 7^2 19^2)}{3^2 7^2 19^2}\,\frac{13}{12}\,\frac{107}{106}\,\frac{127}{126} \prod_{\substack{q=503 \\ q \equiv 2 \pmod 3}}^{653} \frac{q}{q-1} < 2.$$

This shows that $p \neq 13$.

We cannot have $q_1 = 13$, because $53 \cdot 264031|\sigma(13^{12})$, $p \neq 53$ [else $3^3|N$, by (i)], $\sigma(53^2) = 7 \cdot 409$ and $7 \equiv 409 \equiv 264031 \equiv 1 \pmod 3$. Hence, $13^2\|N$, so we have $62|\sigma(13^2)|N$.

Suppose that $p = 61$, so that, by (i), $31|N$. Then $q_1 \neq 31$, since $\sigma(31^{12}) = 42407 \cdot 2426789 \cdot 7908811$, $43|\sigma(7908811^2)$, and $13 \equiv 43 \equiv 7908811 \equiv 1 \pmod 3$. Thus, $31^2\|N$ and $331|\sigma(31^2)|N$. Since $13 \equiv 31 \equiv 331 \equiv 1 \pmod 3$, then $q_1 = 331$. But $53|\sigma(331^{12})$, $7|\sigma(53^2)$, and $7 \equiv 13 \equiv 31 \equiv 1 \pmod 3$. This shows that $p \neq 61$. Also, $q_1 \neq 61$, since $187123|\sigma(61^{12})$, $19|\sigma(187123^2)$, and $13 \equiv 19 \equiv 187123 \equiv 1 \pmod 3$. Hence, $61^2\|N$, so $97|\sigma(61^2)|N$, and we can have no further values of $i \geqslant 2$ with $q_i \equiv 1 \pmod 3$. In particular, $97^2 \nmid N$.

If $p = 97$, then $7|N$ by (i), so $q_1 = 7$; but $\sigma(7^{12}) = r$ (above) $\equiv 1 \pmod 3$. Thus, $q_1 = 97$. But $79|\sigma(97^{12})$ and $79 \equiv 1 \pmod 3$.

This completes the proof.

5. PROOF OF THEOREM 3

We note first that, modulo 8,

$$\sigma(q_i^{2\beta_i}) = 1 + q_i + q_i^2 + \cdots + q_i^{2\beta_i} \equiv 1 + q_i + 1 + \cdots + q_i + 1$$
$$= 1 + \beta_i(q_i + 1),$$

and, writing $\alpha = 4a + 1$,

$$\sigma(p^\alpha) = 1 + p\sigma(p^{4a}) \equiv 1 + p(1 + 2a(p + 1)) \equiv (2a + 1)(p + 1).$$

Since $\sigma(N) = 2N$, we have

$$(2a + 1)(p + 1)\prod_{i=1}^{t}(1 + \beta_i(q_i + 1)) \equiv 2p \pmod 8,$$

or, since $p \equiv 1 \pmod 4$,

$$(2a + 1)\frac{p + 1}{2}\prod_{i=1}^{t}(1 + \beta_i(q_i + 1)) \equiv 1 \pmod 4.$$

If $q_i \equiv 1 \pmod 4$ and $\beta_i \equiv 1 \pmod 2$, then $1 + \beta_i(q_i + 1) \equiv 3 \pmod 4$; otherwise, $1 + \beta_i(q_i + 1) \equiv 1 \pmod 4$. Thus,

$$3^x(2a + 1)\frac{p + 1}{2} \equiv 1 \pmod 4.$$

We see that $3^x \equiv 2x + 1 \pmod 4$, so now

$$(2a + 2x + 1)\frac{p + 1}{2} \equiv 1 \pmod 4.$$

Considering separately the possibilities $p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$, we find that this is equivalent to

$$a + x \equiv \frac{p - 1}{4} \pmod 2,$$

or $p - \alpha = p - 4a - 1 \equiv 4x \pmod 8$, as required.

Note: Since this paper was prepared for publication, we have noticed that Ewell [2] has also given a form of Theorem 3. Both his statement of the theorem and his proof are more complicated than the above.

REFERENCES

1. A. Brauer. "On the Non-Existence of Odd Perfect Numbers of Form $p^\alpha q_1^2 q_2^2 \ldots q_{t-1}^2 q_t^4$." *Bull. Amer. Math. Soc.* 49 (1943):712-18.

2. J. A. Ewell. "On the Multiplicative Structure of Odd Perfect Numbers." *J. Number Th.* 12 (1980):339-42.

3. P. Hagis, Jr. "On the Second Largest Prime Divisor of an Odd Perfect Number." In *Analytic Number Theory*, Lecture Notes in Mathematics, Vol. 899, pp. 254-63. Berlin & New York: Springer-Verlag, 1981.

4. P. Hagis, Jr., & W. L. McDaniel. "A New Result Concerning the Structure of Odd Perfect Numbers." *Proc. Amer. Math. Soc.* 32 (1972):13-15.

5. P. Hagis, Jr., & W. L. McDaniel. "On the Largest Prime Divisor of an Odd Perfect Number, II." *Math. Comp.* **29** (1975):922-24.

6. H.-J. Kanold. "Untersuchungen über ungerade vollkommene Zahlen." *J. Reine Angew. Math.* **183** (1941):98-109.

7. H.-J. Kanold. "Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme, II." *J. Reine Angew. Math.* **188** (1950): 129-46.

8. W. L. McDaniel. "The Non-Existence of Odd Perfect Numbers of a Certain Form." *Arch. Math.* **21** (1970):52-53.

9. W. L. McDaniel & P. Hagis, Jr. "Some Results Concerning the Non-Existence of Odd Perfect Numbers of the Form $p^{\alpha}M^{2\beta}$." *The Fibonacci Quarterly* **13**. no. 1 (1975):25-28.

10. B. Tuckerman. "Odd-Perfect-Number Tree to 10^{36}, To Supplement 'A Search Procedure and Lower Bound for Odd Perfect Numbers,'" IBM Research Report RC-4695, 1974.

♦◇♦◇♦