SOME RESULTS CONCERNING THE NON-EXISTENCE OF ODD PERFECT NUMBERS OF THE FORM $p^{\alpha}M^{2\beta}$

WAYNE L. McDANIEL
University of Missouri, St. Louis Missouri 63121
and
PETER HAGIS, JR.
Temple University, Philadelphia, Pennsylvania 19122

ABSTRACT

It is shown here that if n is an odd number of the form $p^{\alpha}M^{10}$, $p^{\alpha}M^{24}$, $p^{\alpha}M^{34}$, $p^{\alpha}M^{48}$ or $p^{\alpha}M^{124}$, where M is square-free and p is a prime which does not divide M, then n is not perfect.

1. INTRODUCTION

Euler (see page 19 in [1]) proved that if n is odd and perfect (that is, if n has the property that its positive divisor sum $\sigma(n)$ is equal to $2n$) then $n = p^{\alpha}N^2$ where $p \nmid N$ and $p \equiv \alpha \equiv 1 \pmod 4$. In considering the still unanswered question as to whether or not an odd perfect number exists, several investigators have focused their attention on the conditions which must be satisfied by the exponents in the prime decomposition of N. If M is square-free and β is a natural number then it is known that $n = p^{\alpha}M^{2\beta}$ is not perfect if β has any of the following values: 1 (Steuerwald in [8]), 2 (Kanold in [3]), 3 (Hagis and McDaniel in [2]), $3k + 1$ where k is a non-negative integer (McDaniel in [5]). Our purpose here is to show that n is not perfect for five additional values of β. Thus, we shall prove the following result.

Theorem. Let $n = p^{\alpha}M^{2\beta}$ where M is an odd square-free number, $p \nmid M$, and $p \equiv \alpha \equiv 1 \pmod 4$. Then n is not perfect if (A) $\beta = 5$, (B) $\beta = 12$ or 62, (C) $\beta = 24$, (D) $\beta = 17$.

2. SOME PRELIMINARY RESULTS AND REMARKS

For the reader's convenience we list several well-known facts concerning the sigma function, cyclotomic polynomials, and odd perfect numbers which will be needed. If q is a prime the notation $q^C \| K$ means that $q^C | K$ but $q^{C+1} \nmid K$.

(1) If P is a prime, then

$$\sigma(P^s) = \prod_m F_m(P),$$

where $F_m(x)$ is the m^{th} cyclotomic polynomial and m ranges over the positive divisors other than 1 of $s + 1$. (See Chapter 8 in [7].) If n is odd and perfect and q is an odd prime then it is immediate, since $\sigma(n) = 2n$, that $q | n$ if and only if $q | F_m(P)$ where P^s is a prime power such that $P^s \| n$ and $m | (s + 1)$.

(2) If $m = q^C$ where q is a prime then $q | F_m(P)$ if and only if $P \equiv 1 \pmod q$. Furthermore, if $q | F_m(P)$ and $m > 2$, then $q \| F_m(P)$. (See Theorem 95 in [6].)

(3) If $q | F_m(P)$ and $q \nmid m$, then $q \equiv 1 \pmod m$. (See Theorem 94 in [6].)

(4) If $n = p^{\alpha}p_1^{2\beta_1} \cdots p_t^{2\beta_t}$ is odd and perfect then the fourth power (at least) of any common divisor of the numbers $2\beta_i + 1$ $(i = 1, 2, \cdots, t)$ divides n. (See Section III in [3].)

(5) If n is an odd perfect number then n is divisible by $(p + 1)/2$.

We shall also require the following lemma which, to the best of our knowledge, is new.

Lemma. Let $n = p^{\alpha}M^{2\beta}$ be an odd perfect number with M square-free. If $2\beta + 1 = RQ^a$ where Q is a prime different from p and $Q \nmid R$, then at most $2\beta/a$ distinct prime factors of M are congruent to 1 modulo Q.

Proof. Since $Q^4 | n$, by (4), and $Q \neq p$ we have $Q^{2\beta} \| n$. If P is a prime factor of M then from (1) we see that $F_{Q^j}(P) | n$ for $j = 1, 2, \cdots, a$.

Thus, if $P \equiv 1 \pmod{Q}$ then $Q^a | n$, by (2). It now follows that if M is divisible by C distinct primes, each congruent to 1 modulo Q, then $Q^{aC} | n$. Since $Q^{2\beta} \| n$, $C \leq 2\beta / a$.

We are now prepared to prove our theorem. Our proof utilizes the principle of *reductio ad absurdum* with Kanold's result (4) furnishing a starting point and our lemma providing a convenient "target" for contradiction. The prime factors of the cyclotomic polynomials encountered in the sequel were obtained using the CDC 6400 at the Temple University Computing Center. For the most part only those prime factors of $F_m(P)$ were sought which did not exceed 10^5.

3. THE PROOF OF (A)

We begin by noting that

$$F_{11}(199) = 11R_1 \quad \text{and} \quad F_{11}(463) = 11 \cdot 23 \cdot 5479 R_2 ,$$

where every prime which divides $R_1 R_2$ exceeds 10^5. Since

$$R_1 / R_2 \doteq (8.899 \cdot 10^{21}) / (3.273 \cdot 10^{20}) \doteq 27.2$$

we see that $R_2 \nmid R_1$ from which it follows that $R_1 R_2$ has at least two distinct prime divisors P_1 and P_2, both greater than 10^5. By (3), $P_1 \equiv P_2 \equiv 1 \pmod{11}$. We also remark that if

$$P_3 = 1806113 \quad \text{and} \quad P_4 = 3937230404603 = F_{11}(23)/11$$

then it can be verified that neither of the primes P_3 or P_4 divides either R_1 or R_2.

Now assume that $n = p^\alpha M^{10}$ is perfect. From (4) we see that $11^4 | n$ and, therefore, that

$$F_{11}(11) = 15797 \cdot 1806113 | n.$$

We now consider three possibilities.

CASE 1. $p = 15797$. By (5), $3 \cdot 2633 | n$. It was found that

$$2113 | F_{11}(2633), \quad 683 \cdot 7459 | F_{11}(2113), \quad 23 \cdot 99859 | F_{11}(683), \quad \text{and} \quad 3719 \cdot 8999 | F_{11}(99859).$$

Also,

$$463 | F_{11}(3719) \quad \text{and} \quad 199 | F_{11}(1806113).$$

It follows from (1) that n is divisible by each of the following eleven primes, all congruent to 1 modulo 11:

$$23,\ 199,\ 463,\ 683,\ 2113,\ 3719,\ 7459,\ 8999,\ 99859,\ P_3,\ P_4 .$$

But this is impossible since, according to our lemma, M has at most 10 prime divisors congruent to 1 modulo 11.

CASE 2. $p = 1806113$. By (5), $3 \cdot 17 \cdot 17707 | n$. $1013 | F_{11}(17707)$ and $199 | F_{11}(1013)$; while

$$463 | F_{11}(15797), \quad 23 \cdot 5479 | F_{11}(463), \quad \text{and} \quad 1277 \cdot 18701 | F_{11}(5479).$$

From (1) and the discussion in the first paragraph of this section we see that each of the eleven primes

$$23,\ 199,\ 463,\ 1013,\ 1277,\ 5479,\ 15797,\ 18701,\ P_1,\ P_2,\ P_4$$

divides n. Our lemma has been contradicted again.

CASE 3. $p \neq 15797$ and $p \neq 1806113$. Since $199 | F_{11}(1806113)$ and $463 | F_{11}(15797)$ we see from the discussion thus far that n is divisible by the following eleven primes:

$$23,\ 199,\ 463,\ 1277,\ 5479,\ 15797,\ 18701,\ P_1,\ P_2,\ P_3,\ P_4 .$$

If $p = 18701$ then $3 | n$ and, therefore, 3851 (a factor of $F_{11}(3)$) divides n. If $p \neq 18701$ then n is divisible by 34607, a factor of $F_{11}(18701)$. In either case n is divisible by twelve primes, each congruent to 1 modulo 11, at most one of which is p. This contradiction to our lemma completes the proof of (A).

4. THE PROOF OF (B)

If we assume that $n = p^\alpha M^{2\beta}$ is perfect, where $\beta = 12$ or 62, then $5^4 | n$ by (4). If $p \equiv 2 \pmod{3}$ then from (5) we have $3 | n$, and since $F_5(3) = 11^2$ it follows from (1) that $3 \cdot 5^2 \cdot 11 | n$. But this contradicts a well known result of Kanold's ((2) Hilfssatz in [4]). We conclude, since $p \equiv 1 \pmod{4}$, that $p \equiv 1 \pmod{12}$.

Since $5^4 | n$ we have $5^{24} \| n$ (or $5^{124} \| n$), and from (1) we see that

$$F_5(5) = 11\cdot 71 \quad \text{and} \quad F_{25}(5) = 101\cdot 251\cdot 401\cdot 9384251$$

both divide n.

Proceeding as in the proof of (A) and referring to Table 1 we see that n is divisible by at least 43 different primes congruent to 1 modulo 5. (Here, and in our other tables, the presence of an asterisk indicates that the prime *might* be p.) Since at most one of these primes can be p, and since our lemma implies that M has at most 12 (or 41) prime factors congruent to 1 modulo 5, we have a contradiction.

TABLE 1

Selected Prime Factors of $F_5(q)$ and $F_{25}(q)$

q	$F_5(q)$	$F_{25}(q)$
5	11, 71	101, 251, 401, 9384251
11	3221	3001*, 24151
71	211, 2221*	
101	31, 491, 1381*	
401	1231	
9384251	181*, 191	1051, 70051
3221		151, 601*, 1301, 1601
211	1361	
31	17351	4951
1231	3491	55351
191	1871, 13001	5101*, 10151, 38351
1051	241*	2351, 19751
1301	61*	701, 6451
13001	1801*, 5431, 17981, 32491	

5. THE PROOF OF (C)

Assume that $n = p^{\alpha}M^{48}$ is perfect. Then $7^{48}\| n$ by (4), and if $p \equiv 2 \pmod 3$ then $3^{48}\| n$ by (5). (We note that $p \neq 29$ since otherwise $3\cdot 5\cdot 7 | n$ which is impossible.) According to Table 2, in which the upper half is applicable if $p \equiv 2 \pmod 3$ and the bottom half if $p \equiv 1 \pmod 3$, we see that n is divisible by at least 26 primes congruent to 1 modulo 7, at most one of which can be p. This is a contradiction since, by our lemma. M is divisible by at most 24 such primes.

6. THE PROOF OF (D)

We shall prove a more general result which includes (D) as a special case. Thus, suppose that

$$n = p^{\alpha}p_1^{2\beta_1}\cdots p_t^{2\beta_t} \quad \text{and that} \quad 35 | (2\beta_i + 1) \quad \text{for} \quad i = 1, 2, \cdots, t.$$

If n is perfect then $35^4 | n$ by (4). As in the proof of (B), $p \equiv 1 \pmod{12}$, and from (1) we see that $F_5(5) = 11\cdot 71$ and $F_7(7) = 29\cdot 4733$ each divides n. Referring to Table 3 and noting that either 181 or 86353 is *not* p we see that n is divisible by the primes

$$5, 7, 11, 29, 31, 41, 43, 61^*, 71, 101, 113, 127, 131, 151, 191, 197, 211, 241^*, 251, 271, 281, 491, 911.$$

If m is the product of the primes in this list which are not congruent to 1 modulo 12, then

$$\sigma(n)/n > \sigma(61\cdot 241m^4)/(61\cdot 241m^4) > 2.$$

This contradiction shows that n is not perfect.

7. CONCLUDING REMARKS

From the results obtained to date we see that if $n = p^{\alpha}M^{2\beta}$ is perfect then either $2\beta + 1 = q \geqslant 13$ where q is a prime, or $2\beta + 1 = m \geqslant 55$ where m is composite. Thus, it seems reasonable to conjecture that an odd number of the form $p^{\alpha}M^{2\beta}$, M square-free, cannot be perfect. It is clear, however, that the proof must await the development of a new approach: the magnitude of the numbers encountered for which factors must be found makes the attack of

TABLE 2

Selected Prime Factors of $F_7(q)$ and $F_{49}(q)$

q	$F_7(q)$	$F_{49}(q)$
7	29, 4733*	3529
3	1093	491, 4019, 8233, 51157, 131713
29	88009573	197*
3529	7883	16759
1093	14939	883
491	617*, 1051	
131713	43, 239	8527
88009573	71, 22807	4999
16759	701* 6959	6763
7	29, 4733	3529*
29	88009573*	197
4733	70001	83203
197	97847,2957767	1373
70001	50359, 263621	
83203	43	83497*
2957767	127·	
1373	281, 659	
50359	71, 1093*	16759
43	5839	491
16759	701, 6959	883, 6763

TABLE 3

Selected Prime Factors of $F_5(q)$ and $F_7(q)$

q	$F_5(q)$	$F_7(q)$
5	11, 71	
7		29, 4733
71	211	
4733	41, 101	70001
211	292661	
101	31, 491	
70001	61*, 181*	
292661	191, 241*	
191	1871	127, 197
1871	151	911
127		43, 86353*
181*		281
86353*	281	
151		1499
281	271	
1499	131	113
113	251	

the present paper impractical for "large" *deficient* values of $2\beta + 1$ (m is deficient of $\sigma(m) < 2m$), even with the aid of a high-speed computer. Six is perhaps the only value of β for which $2\beta + 1$ is a prime power within reach at present. If, on the other hand, $2\beta + 1 = m$ is abundant (that is, $\sigma(m) > 2m$) then it is trivial that $n = p^{\alpha}M^{2\beta}$ cannot be perfect; for by (4), $m \mid n$ and this implies that $\sigma(n)/n > \sigma(m)/m > 2$.

REFERENCES

1. L.E. Dickson, *History of the Theory of Numbers,* Vol. 1, Washington, D.C., Carnegie Institute, 1919.
2. P. Hagis, Jr., and W.L. McDaniel, "A New Result Cocnerning the Structure of Odd Perfect Numbers," *Proc. Am. Math. Soc.,* Vol. 32 (1972), pp. 13–15.
3. H.J. Kanold, "Untersuchungen über ungerade vollkommene Zahlen," *J. Reine Angew. Math.,* Vol. 183, 1941, pp. 98–109.
4. H.J. Kanold, "Folgerungen aus dem Vorkommen einen Gauss'schen Primzahl in der Primfaktorenzerlegung einen ungeraden vollkommenen Zahl," *J. Reine Angew. Math.,* Vol. 186, 1944, pp. 25–29.
5. W.L. McDaniel, "The Non-existence of Odd Perfect Numbers of a Certain Form," *Arch. Math.,* Vol. 21, 1970, pp. 52–53.
6. T. Nagell, *Introduction to Number Theory,* New York, 1951.
7. H. Rademacher, *Lectures on Elementary Number Theory,* New York, 1964.
8. R. Steuerwald, "Verscharfung einen notwendigen Bedingung für die Existenz einen ungeraden vollkommenen Zahl," *S.-Ber. Math.-Nat. Abt. Bayer Acad. Wiss.,* 1937, pp. 69–72.

****