MATHEMATICS OF COMPUTATION
VOLUME 40, NUMBER 161
JANUARY 1983, PAGES 399-404

# Sketch of a Proof That an Odd Perfect Number Relatively Prime to 3 Has at Least Eleven Prime Factors

By Peter Hagis, Jr.

**Abstract.** An argument is outlined which demonstates that every odd perfect number which is not divisible by 3 has at least eleven distinct prime factors.

**1. Introduction.** A positive integer $n$ is said to be perfect if $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of the positive divisors of $n$. No *odd* perfect numbers have been found, but it has not been proved that none exists. Throughout this paper $N$ will represent an odd perfect number, and $\omega(N)$ will denote the number of distinct prime factors of $N$. It was shown in [1] that $\omega(N) \geqslant 8$, while if $3 \nmid N$ it was proved by Kishore [6] that $\omega(N) \geqslant 10$. The purpose of the present paper is to sketch a proof of the following improvement of Kishore's result.

THEOREM. *If $N$ is an odd perfect number and $3 \nmid N$, then $\omega(N) \geqslant 11$.*

We shall omit most of the details of the proof of this theorem. The complete proof, in the form of a handwritten manuscript [3] of approximately forty-five pages, has been deposited in the UMT file.

Our plan of attack is rather obvious. We assume the existence of an odd perfect number $N$ such that $3 \nmid N$ and $\omega(N) = 10$ and show that such an assumption is untenable. In conjunction with Kishore's result this yields our theorem. Our proof is largely computational and the necessary calculations and searches were carried out on the CDC CYBER 174 at the Temple University Computing Center. The total amount of computer time used was about 45 minutes.

**2. Some Basic Facts.** In what follows the letters $p$ and $q$, with or without subscripts, denote odd primes. If

$$N = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} \tag{1}$$

where $p_1 < p_2 < \cdots < p_t$ and $a_i > 0$ then $p_i^{a_i}$ is called a component of $N$. Euler showed that for every component except one, $2 \mid a_i$. For this *special* component, which we shall denote by $\pi^m$, it is true that $\pi \equiv m \equiv 1 \pmod 4$.

It was proved in [4] that

$$p_t \geqslant 100129, \tag{2}$$

and in [2] it was shown that

$$p_{t-1} \geqslant 1009. \tag{3}$$

Received August 7, 1981; revised June 21, 1982.
1980 *Mathematics Subject Classification.* Primary 10A20.

Now, let $F_d$ be the $d$th cyclotomic polynomial and let $E = E(p; q)$ be the exponent to which $p$ belongs modulo $q$. References for the following facts may be found in [1] and/or [8].

$$2N = \sigma(N) = \prod_{i=1}^{t} \sigma(p_i^{a_i}) = \prod_{i=1}^{t} \prod_{d} F_d(p_i) \tag{4}$$

where $d$ runs over the divisors of $a_{i+1}$ which exceed 1.

$$q \mid F_k(p) \quad \text{if and only if } k = q^{\beta} \cdot E(p; q). \tag{5}$$

If $\beta > 0$ then $q \parallel F_k(p)$; if $\beta = 0$ then $q \equiv 1 \pmod{k}$.

(6) If $k \geqslant 3$ then $F_k(p)$ has at least one prime factor $q$ such that $q \equiv 1 \pmod{k}$.

(7) If $q_1 \mid F_{k_1}(p)$ and $q_2 \mid F_{k_2}(p)$ where $k_1 > k_2 \geqslant 2$ and $q_i \nmid k_i$ then $q_1 \neq q_2$.

If $q$ is a Fermat prime and $p^a \parallel N$; and we write $b = v_q(K)$ if $q^b \parallel K$, then:

$$v_q(\sigma(p^a)) = \begin{cases} v_q(a+1) & \text{if } E = 1, \\ v_q(a+1) + v_q(p+1) & \text{if } E = 2 \text{ and } p = \pi, \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

If $h(k) = \sigma(k)/k$, so that $k$ is perfect if and only if $h(k) = 2$, and $h(p^{\infty}) = p/(p-1)$, then

$$1 \leqslant h(p^a) < h(p^b) < h(q^c) \tag{9}$$

if $0 \leqslant a < b \leqslant \infty$, $1 \leqslant c \leqslant \infty$ and $p > q$.

**3. Three Important Lemmas.** We remind the reader that $N$ is an odd perfect number with special prime factor $\pi$.

LEMMA 1. *If $5^b \parallel N$, where $b \geqslant 5$, and $5^{b-4} \mid (\pi + 1)$, then $\pi \nmid \sigma(5^b)$.*

LEMMA 2. *If $17^c \parallel N$, where $c \geqslant 6$, and $17^{c-3} \mid (\pi + 1)$, then $\pi \nmid \sigma(17^c)$.*

*Proof.* Since $17^{c-3} \mid (\pi + 1)$, we see that $\pi + 1 = J \cdot 17^{c-3}$ where $J \geqslant 2$. Also, since $17^3 \mid (\pi + 1)$, it follows that $\pi + 1 \leqslant 9826\pi/9825$. Therefore,

$$\sigma(17^c) = (17^{c+1} - 1)/16 < 17^{c+1}/16 = 17^{c-3}17^4/16 \leqslant (\pi + 1)17^4/32 < 2611\pi.$$

Now assume that $\pi \mid \sigma(17^c)$. Then $\sigma(17^c) = S\pi$ where $S < 2611$. Since $\sigma(17^c) = 1 + 17 + 17^2 + \cdots + 17^c$ and $17^3 \mid (\pi + 1)$, we see that $307 \equiv S\pi \equiv -S \pmod{17^3}$. Therefore, $S \geqslant 4606$ which is impossible.

LEMMA 3. *If $N = Mp^{\alpha}$ where $(M, p) = 1$, and $G(M) = 2/(2 - h(M))$, then: (i) $p = G(M) - 1$ if $\alpha = 1$; (ii) $G(M) - (p+1)^{-1} \leqslant p < G(M)$ if $\alpha > 1$.*

A few remarks concerning Lemma 3 are in order. First, the fact that $p < G(M)$ is proved in Section 1.4 of [8]; and a slightly erroneous version of the lemma is stated in [5]. Second, in (i) it is clear that $p = \pi$. Third, referring to (1) we see that if $2 \leqslant s \leqslant t$ and $p = p_s$ then from (ii), $G(M) - (p_{s-1} + 3)^{-1} \leqslant p_s$.

**4. Some Preliminary Results.** We assume from now on that $3 \nmid N$ and $\omega(N) = 10$. Note first that from (2) and (3), $p_9 \geqslant 1009$ and $p_{10} \geqslant 100129$. Also, $p_1 = 5$, $p_2 = 7$

and $p_3 = 11$ since otherwise it would follow from (9) that $h(N) < h(5^\infty 7^\infty 13^\infty 17^\infty 19^\infty 23^\infty 29^\infty 31^\infty 1009^\infty 100129^\infty) < 2$ which is impossible since $N$ is perfect. Likewise, $p_4 = 13$ or 17 since $h(5^\infty 7^\infty 11^\infty 19^\infty 23^\infty 29^\infty 31^\infty 37^\infty 1009^\infty 100129^\infty) < 2$, and similar arguments show that $p_5 = 17$, 19 or 23 and $19 \leqslant p_6 \leqslant 31$ and $p_7 \leqslant 79$. From Lemma 1 in [6] we have

$$\pi \equiv 1 \pmod{12} \tag{10}$$

and

$$\text{if } p \equiv 1 \pmod 3 \text{ and } p^a \,\|\, N \text{ then } a \not\equiv 2 \pmod 3. \tag{11}$$

It follows that $p_7 \geqslant 29$. For if $p_7 = 23$, $h(N) > h(5^2 7^4 11^2 13 \cdot 17^2 19^4 23^2) > 2$.

A more elaborate argument now shows that $p_4 = 13$, and the following lemma can then be proved.

LEMMA 4. *If $5^b \,\|\, N$ and $b > 6$, then $\sigma(5^b)$ has a prime factor $Q \geqslant 100129$.*

With the aid of this lemma we can show that $p_5 \neq 23$, and we have

PROPOSITION 1. *If $N = \prod_{i=1}^{10} p_i^{a_i}$ is an odd perfect number with $3 < p_1 < p_2 < \cdots < p_{10}$, then $p_1 = 5$, $p_2 = 7$, $p_3 = 11$, $p_4 = 13$, $p_5 = 17$ or 19, $19 \leqslant p_6 \leqslant 31$, and $29 \leqslant p_7 \leqslant 79$. $p_9 \geqslant 1009$ and $p_{10} \geqslant 100129$.*

**5. Permissible Exponents.** It can be shown that

$$\text{if } 19 \mid N, \text{ then } 19^{10} \mid N. \tag{12}$$

Also,

$$5^8 \nmid\nmid N. \tag{13}$$

For otherwise $\sigma(5^8) = 19 \cdot 31 \cdot 829 \mid N$, and if $p_5 = 17$, then $h(N) > 2$ while if $p_5 = 19$, then $h(N) < 2$.

Similarly, it can be proved that

$$13^9 \nmid\nmid N. \tag{14}$$

Referring to (11), (12), (13), (14) we define in Table I for each (possible) prime factor $p$ of $N$ a finite set, $S(p)$, of "permissible" exponents for $p$. The entry 1* indicates that $1 \in S(p)$ if and only if $p$ *might* be $\pi$, while 2* indicates that $2 \in S(p)$ if and only if $p \equiv 2 \pmod 3$. We also tabulate $m(p)$, the maximum element in $S(p)$.

TABLE I

| $p$ | $S(p)$ | $m(p)$ |
|---|---|---|
| 5 | 2, 4, 6, 10 | 10 |
| 7 | 4, 6, 10 | 10 |
| 11 | 2, 4, 6, 8 | 8 |
| 13 | 1, 4, 6, 10 | 10 |
| 17 | 2, 4, 6 | 6 |
| 19 | 10 | 10 |
| 37 | 1, 4, 6 | 6 |
| $p_6$ ($\neq 19$) | 2*, 4, 6 | 6 |
| $p_7$ ($\neq 37$) | 2*, 4, 6 | 6 |
| $p_8$ | 1*, 2*, 4, 6 | 6 |
| $p_9$ | 1*, 2 | 2 |
| $p_{10}$ | 1*, 2 | 2 |

**6. A Revised Version of Lemma 3.** Suppose that $N = \prod_{i=1}^{10} p_i^{a_i}$. With $m(p_i)$ as given in Table I we define $b_i = \min(a_i, m(p_i))$; and $c_i = a_i$ if $a_i < m(p_i)$ and $c_i = \infty$, otherwise. Let $B_9$ and $B_{10}$ be lower bounds for $p_9$ and $p_{10}$, respectively. If $M = N/p_8^{a_8}$, we (formally) define $M_L$ and $M_U$ as follows. $M_L = Q_9 Q_{10} \prod_{i=1}^{7} p_i^{b_i}$ where $Q_i = p_i^{b_i}$ if the value of $p_i$, for $i = 9$ or 10, is specified (known) and $Q_i = 1$ otherwise. $M_U = R_9 R_{10} \prod_{i=1}^{7} p_i^{c_i}$ where $R_i = p_i^{\infty}$ if $p_i$ is specified and $R_i = B_i^{\infty}$ otherwise. From Lemma 3 we have

LEMMA 3*. *If* $N = Mp_8^{a_8}$ *where* $p_8 \nmid M$ *and* $h(M_U) < 2$, *then*
(i) $G(M_L) - 1 \leqslant p_8 \leqslant G(M_U) - 1$ *if* $a_8 = 1$;
(ii) $G(M_L) - (p_7 + 3)^{-1} \leqslant p_8 < G(M_U)$ *if* $a_8 > 1$.
*Moreover, if* $F(M_L) = G(M_L) - (p_7 + 3)^{-1}$, *then*
(iii) $G(M_L) - (F(M_L) + 1)^{-1} \leqslant p_8 < G(M_U)$ *if* $a_8 > 1$.

**7. An Upper Bound For $p_9$.** Our immediate objective is to prove that $p_9 < 10^5$. With this in mind assume that $p_9 > 10^5$. Then (see Section 6) we may take $B_9 = 100003$ and $B_{10} = 100129$. Assuming that $p_5 = 19$ a computer program utilizing double-precision arithmetic was written which used Lemma 3* to bound $p_8$ for every *possible* value of $N$. (Only a finite number of cases, determined by the values of $p_i$ as given in Proposition 1 and the elements of $S(p_i)$ as given in Table I, had to be considered.) It was found that if $p_9 > 10^5$ and $p_5 = 19$ then $11^2 \| N$, $5^{10}7^{10}13^6 19^{10} 29^4 37^6 \mid N$ and $p_8 = 41$. Since $F_5(41) = 5 \cdot 579281$ and $h(5^{10}7^{10}11^2 13^6 19^{10} 29^4 37^6 41^4 579281) > 2$, we see that $5 \nmid (a_8 + 1)$. Therefore, if $5^b \| N$ it follows from (8), (4) and (6) that $5^b \mid \sigma(p_9^{a_9} p_{10}^{a_{10}})$ *and* that $5^{b-2} \mid (\pi + 1)$. Thus, $\pi > 2 \cdot 5^8 - 1 = 781249$ and, from Lemma 1, $\pi \nmid \sigma(5^b)$. If $p$ is the smallest prime factor of $b + 1$ then, since $F_3(5) = 31$, $F_5(5) = 11 \cdot 71$ and $F_7(5) = 19531$, we see from (4) that $p \geqslant 11$. Using (5) it is not difficult to verify that $p_i \nmid F_p(5)$ for $i \leqslant 8$. Therefore, (assuming without loss of generality that $\pi = p_{10}$) $F_p(5) = p_9^{\alpha}$. According to the table in [7] either $\alpha = 1$, so that $p_9 = F_p(5) \geqslant F_{11}(5) = 12207031$ or $p_9 > 2^{29}$. It follows that $h(N) < h(5^\infty 7^\infty 11^2 13^\infty 19^\infty 29^\infty 37^\infty 41^\infty 12207031^\infty 781249^\infty) < 2$ and this contradiction shows that $p_9 < 10^5$ if $p_5 = 19$. A similar, but lengthier, argument shows that $p_9 < 10^5$ if $p_5 = 17$. Thus, we have

LEMMA 5. *If* $N = \prod_{i=1}^{10} p_i^{a_i}$ *is odd and perfect and* $3 < p_1 < p_2 < \cdots < p_{10}$, *then* $10^3 < p_9 < 10^5$.

**8. A Proof That $p_5 = 19$.** The proofs of the following two lemmas are omitted here.

LEMMA 6. *If* $17 \mid N$, *then* $17^2 \| N$ *or* $17^4 \| N$.

LEMMA 7. *If* $5 \mid \sigma(N/\pi^m)$, *then* $p_{10} \equiv 1 \pmod 5$. *Also, if* $5 \mid \sigma(p_i^{a_i})$ *where* $i \leqslant 7$, *then* $p_i = p_7 = 41$ *and* $p_{10} = F_5(41)/5 = 579281$.

Assume that $p_5 = 17$ and $17^2 \| N$. Then $p_8 = 307$ since $\sigma(17^2) = 307$. With $B_9 = 1009$ and $B_{10} = 100129$, Lemma 3* was employed in order to bound $p_8$ for all possible values of $N$. In no case was 307 a permissible value of $p_8$. Therefore, if $p_5 = 17$, then $17^4 \| N$. Since it can be shown that $17^4 \nparallel N$, we have

LEMMA 8. $p_5 = 19$.

**9. The Proof of Our Theorem Concluded.** The proofs of the following two lemmas are omitted here.

LEMMA 9. *If* $p_9 = \pi$, *then* $p_9 \not\equiv -1 \pmod 5$.

LEMMA 10. *If* $5^b \parallel N$, *then* $b = 2, 4$ *or* 6.

With $p_5 = 19$, $B_9 = 1009$, $B_{10} = 100129$ and making use of Lemma 10, Lemma 3* was utilized to determine $p_8$ for all possible values of $N$. The results are given in Table IV. The notation $p_8^*$ means that $p_8 \parallel N$.

TABLE IV

| Restrictions on $N$ | $p_8$ |
|---|---|
| $5^2 \parallel N$; $7^{10}11^2 13^6 19^{10} 23^4 31^6 \mid N$ | 59 or 61 |
| $5^4 \parallel N$; $7^{10}11^8 13^6 19^{10} 23^4 37^6 \mid N$ | 71 |
| $5^2 11^2 13 \parallel N$; $7^{10} 19^{10} 23^4 31^6 \mid N$ | 43 |
| $5^2 11^2 \parallel N$; $7^{10} 13^6 19^{10} 29^4 31^6 \mid N$ | 37* |
| $5^2 \parallel N$; $7^{10}11^8 13^6 19^{10} 23^4 31^6 \mid N$ | 61* |

For the case $p_8 = 43$ a modified version of Lemma 3* was used to bound $p_9$. It was found that $2647 \leqslant p_9 \leqslant 2707$. Since the only prime in this range congruent to 1 modulo 5 is 2671 and since $571 \mid F_5(2671)$ it follows from Lemma 7, (8) and (4) that $5^2 \mid \sigma(p_{10}^{a_{10}})$. This is impossible since $p_i \not\equiv 1 \pmod{5^2}$ for $i < 10$. Therefore, $p_8 \neq 43$.

If $p_8 = 71$, then $p_9 = 1399$ or 1409. From (10), $\pi \neq p_9$. Since $211 \mid F_5(71)$ it follows from (8) and Lemma 7 that $5^4 \mid \sigma(p_{10}^{a_{10}})$. Since $p_i \not\equiv 1 \pmod{5^2}$ if $i \leqslant 9$, we see that $\pi = p_{10}$. Now, $E(11; 7) = 3$ and $F_3(11) = 7 \cdot 19$ while $1723 \mid F_{21}(11)$. $E(13; 7) = E(1399; 7) = 2$ and $E(19; 7) = 6$. $E(23; 7) = E(37; 7) = E(1409; 7) = 3$ while $79 \mid F_3(23)$, $3 \mid F_3(37)$ and $283813 \mid F_3(1409)$ (while $F_2(283813) = 2 \cdot 141907$). Also, $E(71; 7) = 1$ and $883 \mid F_7(71)$. From (4) and (5), $7^2 \nmid \sigma(p_1^{a_1} \cdots p_9^{a_9})$. Therefore, $7^9 \mid \sigma(p_{10}^{a_{10}})$. If $E(p_{10}; 7) = 1$, then from (4), (5), (6) and (7) $N$ has at least nine prime factors congruent to 1 modulo 7. If $E(p_{10}; 7) = 3$ or 6, then (since $\pi \equiv 1 \pmod 3$) $3 \mid N$. Therefore, $E(p_{10}; 7) = 2$ *and* $7^9 \mid (\pi + 1)$. It follows that $\pi \geqslant 2 \cdot 7^9 - 1 = 80707213$, and since $h(5^4 7^\infty 11^\infty 13^\infty 19^\infty 23^\infty 37^\infty 71^\infty 1399^\infty 80707213^\infty) < 2$, we see that $p_8 \neq 71$.

Since it can also be shown that $p_8 \neq 37$ or 59 or 61, the proof of our theorem is now complete.

**10. Some Concluding Remarks.** This paper is one of many which have appeared in the last ten years which indicate that if an odd perfect number exists then it must be "complicated" (i.e., it must be very large, possess many prime factors (some of which are large), etc.) To the best of my knowledge, the last of these papers which did not make extensive use of a high-speed digital computer was [8]. I may be wrong, but it seems to me that we are near the boundaries of what can be achieved in this area given our present knowledge concerning questions relating to the factors of a cyclotomic polynomial with a prime argument and the present-day "state of the art" in computer hardware and software. Thus, I would be surprised if someone were to prove in the next five years or so that every odd perfect number is greater than $10^{500}$, or has at least 9 prime factors, or has a prime factor which exceeds $10^6$. These results *are* all obtainable, I believe, but both the sheer effort and the computer time required are, in my opinion, prohibitive at present.

Department of Mathematics
Temple University
Philadelphia, Pennsylvania 19122

1. P. HAGIS, JR., "Outline of a proof that every odd perfect number has at least eight prime factors," *Math. Comp.*, v. 35, 1980, pp. 1027–1032.

2. P. HAGIS, JR., "On the second largest prime divisor of an odd perfect number," *Analytic Number Theory*, Lecture Notes in Math., vol. 899, Springer-Verlag, Berlin and New York, 1981, pp. 254–263.

3. P. HAGIS, JR., "Every odd perfect number not divisible by 3 has at least eleven distinct prime factors." (Copy deposited in UMT file.)

4. P. HAGIS, JR. & W. L. MCDANIEL, "On the largest prime divisor of an odd perfect number. II," *Math. Comp.*, v. 29, 1975, pp. 922–924.

R. P. JERRARD & N. TEMPERLEY, "Almost perfect numbers," *Math. Mag.*, v. 46, 1973, pp. 84–87.

6. M. KISHORE, "Odd perfect numbers not divisible by 3 are divisible by at least ten distinct primes," *Math. Comp.*, v. 31, 1977, pp. 274–279.

7. W. L. MCDANIEL, "On multiple prime divisors of cyclotomic polynomials," *Math. Comp.*, v. 28, 1974, pp. 847–850.

8. C. POMERANCE, "Odd perfect numbers are divisible by at least seven distinct primes," *Acta Arith.*, v. 25, 1974, pp. 265–300.