MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 151
JULY 1980, PAGES 1027–1032

Outline of a Proof That Every Odd Perfect Number Has at Least Eight Prime Factors

By Peter Hagis, Jr.

Abstract. An argument is outlined which demonstrates that every odd perfect number is divisible by at least eight distinct primes.

1. **Introduction.** A positive integer is said to be perfect if it is equal to the sum of its proper divisors. Over a period of time spanning more than two thousand years only twenty-seven perfect numbers have been discovered, all of them *even*. Whether or not any *odd* perfect numbers exist is a very old and as yet unanswered question. Many persons have investigated the properties which must be possessed by an odd perfect number (*if* one exists), and particular attention has been paid to the question, "If N is odd and perfect how many prime divisors does N have?" Let R denote the number of distinct prime factors of the odd perfect number N, and let $P(K)$ denote the set of all odd perfect numbers with exactly K distinct prime factors. In 1888 Sylvester proved that $R \geqslant 5$ (so that $P(K)$ is empty if $K \leqslant 4$), and in 1913 L. E. Dickson showed that $P(K)$ is finite for every natural number K. In 1972 Robbins (Brooklyn Polytechnical Institute) and Pomerance (Harvard) each wrote a doctoral dissertation in which he proved that $R \geqslant 7$. For a more complete history of these matters and references to the literature the interested reader is referred to [8]. It should, perhaps, be mentioned here that Pomerance [10] has shown that no member of $P(K)$ can exceed $(4K)e(4K)e(2)e(K)e(2)$ where $(x)e(y) = x^y$.

In the present paper a proof is sketched that $R \geqslant 8$. The complete proof, in the form of a hand-written manuscript [3] of almost two hundred pages, has been deposited in the UMT file. Our plan of attack is simple. We assume the existence of an odd perfect number with exactly seven prime divisors and then show that such an assumption is untenable. In conjunction with the result of Pomerance-Robbins mentioned above this yields the desired result.

2. **Some Notation.** In what follows we shall try to be consistent in our use of the following notation. $a, b, c, \ldots$ and $\alpha, \beta, \gamma, \ldots$ will be used to represent nonnegative integers with odd primes being symbolized by $p, q, r, \ldots$. M will denote an odd integer with the property that if $p \mid M$, then $p \geqslant 100129$. N will represent an odd perfect number, and n will represent an odd perfect number with exactly seven distinct prime factors. If $p^a \| N$, we shall call p^a a *component* of N. The largest prime

Received May 14, 1979; revised November 14, 1979.
1980 *Mathematics Subject Classification.* Primary 10A20.

factor of N will be denoted by P. The dth cyclotomic polynomial will be symbolized by F_d (so that, $F_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$). As usual, $\sigma(k)$ will denote the sum of the positive divisors of the positive integer k. We shall write $h(k) = \sigma(k)/k$ so that k is perfect if and only if $h(k) = 2$. $h(p^\infty) = \lim_{a\to\infty} h(p^a) = p/(p-1)$ and it is easy to see that:

(i) $1 \leqslant h(p^a) < h(p^b)$ if $0 \leqslant a < b \leqslant \infty$;

(ii) $h(p^a) < h(q^b)$ if $p > q$ and $0 \leqslant a \leqslant \infty$, $1 \leqslant b \leqslant \infty$;

(iii) $h(p_1^{a_1} p_2^{a_2} \cdots p_j^{a_j}) = h(p^{a_1})h(p_2^{a_2}) \cdots h(p_j^{a_j})$ if the p_i are distinct primes and $0 \leqslant a_i \leqslant \infty$.

3. **The Key Steps.** We shall now state, and in a *very few* cases prove, the most important results which lead to the conclusion that every odd perfect number has eight prime factors. The nomenclature is that of [3].

From Theorems 94 and 95 in [7]:

(2) $q \mid F_k(p)$ if and only if $k = q^\beta \cdot E(p; q)$, where $E(p; q)$ is the exponent to which p belongs modulo q. If $\beta > 0$, then $q \,\|\, F_k(p)$; if $\beta = 0$, then $q \equiv 1(k)$.

As a special case of (2) we have:

(2a) If q is a Fermat prime ($q = 2^a + 1$) and $k > 1$ is odd, then $q \mid F_k(p)$ if and only if $k = q^\beta$ and $p \equiv 1(q)$.

(4) If $k \geqslant 3$, then $F_k(p)$ has at least one prime factor q such that $q \equiv 1(k)$. (This result is (21) in [5]. Other references are given in 1.8 of [8].)

The next result appears in [6].

(15) If $q^2 \mid F_p(11)$, then $q > 2^{28}$.

If N is odd and perfect, Euler showed that

(22) $N = p_0^{a_0} p_1^{a_1} \cdots p_t^{a_t}$, where $p_0 \equiv a_0 \equiv 1(4)$ and $2 \mid a_i$ if $i > 0$. We shall follow Pomerance [8] and usually write $p_0 = \pi$ and $a_0 = m$. π is called the *special* prime divisor of N.

Since N is perfect, $\sigma(N) = 2N$; and since σ is multiplicative and $\sigma(p^a) = \Pi F_d(p)$, where $d \mid (a+1)$ and $d > 1$:

$$2N = \prod_{i=0}^{t} \sigma(p_i^{a_i}) = \prod_{i=0}^{t} \prod_{d} F_d(p_i). \tag{23}$$

Here d runs over the divisors of $a_i + 1$ which exceed 1. The set of p_i in (22) is identical with the set of odd prime factors of the $F_d(p_i)$ in (23).

If P is the largest prime factor of N, it is proved in [4] that

(25) $P \geqslant 100129$.

The following result is proved in [2]:

(28) If $3 \cdot 5 \cdot 11 \mid N$, then $5 \,\|\, N$. Also, $p \nmid N$ if $13 \leqslant p \leqslant 71$.

1.13 in [8] states that

(34) If $17^c \,\|\, N$ and $17^c \nmid (\pi + 1)$, then N has (at least) two prime factors $\equiv 1(17)$. (We note that 103 is the smallest prime $\equiv 1(17)$.)

PROPOSITION 6.1. *If $3 \mid N$ and $5^b \,\|\, N$ where $b \neq 0, 1, 2, 6$ or 13, then $\sigma(5^b)$ (and N) is divisible either by two primes $\geqslant 100129$ or by a prime $q \geqslant 100129$ such that $q \not\equiv 1(4)$ or $5^5 \nmid (q+1)$.*

PROPOSITION 6.2. *If* $3 | N$ *and* $5^2 | \sigma(N/\pi^m)$, *then* N *has (at least) three prime factors* $\equiv 1(5)$.

Proof. Let p^α and q^β be nonspecial components of N such that $5^2 | \sigma(p^\alpha q^\beta)$. If $5 \| \sigma(p^\alpha)$ and $5 \| \sigma(q^\beta)$ *and* N does not have three prime factors $\equiv 1(5)$ it follows from (2) and (2a) that $F_5(p) = 5q^a$ and $F_5(q) = 5p^b$. Thus, $5q^a \equiv 1(p)$ and $q^5 \equiv 1(p)$, *and* it follows that $1 \equiv 5^5 q^{5a} \equiv 5^5(p)$. Therefore, $p | 3124$ so that $p = 11$ or 71. Since $11 | F_5(71)$ it follows that $3 \cdot 5^2 \cdot 11 | N$ which contradicts (28).

If $5^2 | \sigma(p^\alpha)$, then from (2), (2a), (4) and (23) we see that $F_5(p) | N$, $F_{25}(p) | N$ *and* N has three prime factors (including p) $\equiv 1(5)$. □

PROPOSITION 6.3. *If* $3 | N$ *and* $5^4 | \sigma(N/\pi^m)$, *then* N *has (at least) four prime factors* $\equiv 1(5)$.

PROPOSITION 6.4. *If* $3 | N$, $5^b \| N$ *(where* $b > 0$*) and* N *has at most two prime factors* $\equiv 1(5)$, *then* $5^{b-2} | (\pi + 1)$ *and* $\pi \nmid \sigma(5^b)$.

PROPOSITION 6.5. *Suppose that* $3 \cdot 5 | N$ *and the special component of* N *is* π^m. *If* $3 | (m + 1)$, *then* $\pi \equiv 1(7)$; *if* $5 | (m + 1)$, *then* $\pi \equiv 1(11)$.

Proof. Assume first that $3 | (m + 1)$. From (23), $(F_2F_3F_6)(\pi) | 2N$. If $\pi \equiv 6(7)$, then $7 | F_2(\pi)$; if $\pi \equiv 2, 4(7)$, then $7 | F_3(\pi)$; if $\pi \equiv 3, 5(7)$, then $7 | F_6(\pi)$. Since $3 \cdot 5 \cdot 7 \nmid N$, we see that $\pi \equiv 1(7)$. If $5 | (m + 1)$ then $(F_2F_5F_{10})(\pi) | 2N$. If $\pi \equiv 10(11)$ then $11 | F_2(\pi)$; if $\pi \equiv 3, 4, 5, 9(11)$, then $11 | F_5(\pi)$; if $\pi \equiv 2, 6, 7, 8(11)$, then $11 | F_{10}(\pi)$. Since $3 \cdot 5^2 \cdot 11 \nmid N$, it follows that $\pi \equiv 1(11)$. □

The next result is due to E. Z. Chein [1].

PROPOSITION 6.6. *If* $3^3 | \sigma(N/\pi^m)$, *then* N *has (at least) four prime factors* $\equiv 1(3)$.

If n is a seven-component odd perfect number, then according to Theorem 2 in [9] either

(35) $3 \cdot 5 | n$ or $3 \cdot 7 | n$.

PROPOSITION 7.1. *If* $p^\alpha \| n$ *and* $p \neq \pi$, *then* $5^4 \nmid \sigma(p^\alpha)$.

PROPOSITION 7.2. *If* $\pi = 5$, *then* $5 \| n$.

Proof. Suppose that $5^m \| n$ where $m \equiv 1(4)$. From Proposition 7.1 and (35) at most $5^{15} | \sigma(n/\pi^m)$ so that $m \leqslant 13$. From Proposition 6.5, $m \neq 5$ and $m \neq 9$. If $m = 13$, $\sigma(5^{13})/2 = 3 \cdot 29 \cdot 449 \cdot 19531 | n$ *and*, from Proposition 7.1 and (2a), at most $5^9 | n$. This contradicts the assumption that $5^{13} \| n$. Therefore, $m = 1$. □

PROPOSITION 7.3. *Let* $P^g \| n$ *where* P *is the largest prime factor of* n, *and assume that* $P \neq \pi$. *Then* $3^3 \nmid \sigma(P^g)$. *If* $3^2 \| \sigma(P^g)$ *then* n *has (at least) four prime factors* $\equiv 1(3)$. *If* $3^2 \| \sigma(P^g)$ *and* n *has exactly four prime factors* $\equiv 1(5)$, *then* $5 | n$ *and* $s | n$ *where* $s \equiv 1(3)$ *and* $P > s > P/\sqrt{3}$.

PROPOSITION 7.4. *If* π^m *is the special component of* n, $3^2 \nmid (m + 1)$.

PROPOSITION 8.1. *If* $\pi = 5$, *then* $3^7 \nmid n$.

PROPOSITION 8.2. *If* $F_{3J}(p) = 3q^a$ *and* $p \mid F_{3K}(q)$, *where* $K = 1$ *or* 2, *then* $p =$ 13 *or* 757.

PROPOSITION 8.3. *If* $3 \cdot 5 \mid n$, *then* $\pi \neq 17$.

PROPOSITION 8.4. *If* $3^4 \mid \sigma(n/\pi^m)$, *then n has (at least) five prime factors* $\equiv 1(3)$.

PROPOSITION 9.1. *If* $3^8 \mid n$, *then* $\pi \equiv -1(3)$ *and* $\pi \neq 5$.

PROPOSITION 9.2. *If* $5^b \| n$ $(b \geqslant 2)$ *and* $\pi \equiv -1(3)$, *then* $3^2 \| n$ *or* $3^6 \| n$ *or* $3^{12} \mid n$. *If* $3^{12} \mid n$ *then* $\pi \geqslant 511757$.

PROPOSITION 9.3. *If* $7 \mid n$ *and* $3^8 \mid n$, *then* $\pi \geqslant 13121$.

PROPOSITION 10.1. *If* $5 \mid n$, $\pi^m \| n$ *and* $\pi \equiv \pm 1(5)$, *then* $5^2 \nmid (m + 1)$.

PROPOSITION 10.2. *If* $5^b \| n$ $(b > 0)$ *and* $5^b \nparallel \sigma(\pi^m)$, *then n has (at least) two prime factors* $\equiv 1(5)$, *one of which exceeds* 100129.

PROPOSITION 10.3. *If* $5 \mid n$ *and* p^α *and* q^β *are nonspecial components of n, then* $5^3 \mid \sigma(p^\alpha)$ *and* $5^3 \mid \sigma(q^\beta)$ *is impossible.*

PROPOSITION 11.1. *If* $\pi \equiv -1(5)$ *and* $5^\beta \| (\pi + 1)$, *then at most* $5^{\beta+4} \mid n$ *and at most* $5^3 \mid \sigma(n/\pi^m)$. *Moreover: if* $\beta < 4$, *then* $5^2 \| n$; *if* $\beta = 4$, *then* $5^6 \| n$ *and* $\pi \geqslant 100129$; *if* $\beta > 4$, *then* $\pi \geqslant 100129$.

PROPOSITION 12.1. *If* $5^{10} \mid n$, *then n has a nonspecial prime factor* $\geqslant 100129$.

PROPOSITION 12.2. *If* $3^{12} \mid n$, *then n has a nonspecial prime factor* $\geqslant 100129$.

PROPOSITION 13.1. *If* $7 \mid n$, *then* $11 \mid n$ *or* $13 \mid n$.

Proof. Let $n = 3^a 7^b p^c q^d r^e s^f P^g$ where $p < q < r < s < P$. Since $F_3(3) = 13$ and $F_5(3) = 11^2$, we may assume in what follows that $a \neq 2, 4, 8$.

If $a = 6$, then $\sigma(3^6) = 1093 \mid n$. If $a = 10$, then $\sigma(3^{10}) = 23 \cdot 3851 n$ and, from Proposition 9.3, $\pi \geqslant 13121$. If $a \geqslant 12$, then $\pi \geqslant 13121$ *and*, from Proposition 12.2, n has a nonspecial prime factor $\geqslant 100129$. Thus, $s \geqslant 1093$ and, since $h(3^\infty 7^\infty 1093^\infty 100129^\infty 23^\infty 29^\infty 31^\infty) < 2$, we see that if $p \neq 11$ or 13, then $p = 17$ or 19.

Suppose that $p = 19$. Then $q = 23$ and $r = 29$ since otherwise $h(n) < h(3^\infty 7^\infty 19^\infty 1093^\infty 100129^\infty 23^\infty 31^\infty) < 2$. Since $127 \mid F_3(19)$, $79 \mid F_3(23)$ and $67 \mid F_3(29)$, we see that $(19 \cdot 23 \cdot 29)^4 \mid n$. If $7^2 \| n$, then

$$h(n) < h(3^\infty 7^2 19^\infty 23^\infty 29^\infty 1093^\infty 100129^\infty) < 2.$$

If $7^4 \mid n$ and $a = 6$, then $h(n) > h(3^6 7^4 19^4 23^4 29^4 1093) > 2$. If $7^4 \mid n$ and $\alpha \geqslant 10$, then $h(n) > h(3^{10} 7^4 19^4 23^4 29^4) > 2$. These contradictions show that $p \neq 19$.

Suppose that $p = 17$. Then $q = 19$ or 23 since

$$h(3^\infty 7^\infty 17^\infty 1093^\infty 100129^\infty 29^\infty 31^\infty) < 2.$$

If $17 \| n$, then $\pi = 17$, and from Proposition 9.3 $3^6 \| n$. From (34) it follows that $h(n) < h(3^6 7^\infty 17 \cdot 19^\infty 1093^\infty 100129^\infty 103^\infty) < 2$. If $17^2 \| n$, then $\sigma(17^2) = 307 \mid n$, and $h(n) < h(3^\infty 7^\infty 17^2 19^\infty 307^\infty 1093^\infty 100129^\infty) < 2$. We conclude that $17^4 \mid n$.

Now suppose that $7^2 \| n$. Then $q = 19$ since $19 | \sigma(7^2)$. Also, $r = 47$ since $h(3^6 7^2 17^4 19^2 43^2) > 2$ and $h(3^\infty 7^2 17^\infty 19^\infty 1093^\infty 100129^\infty 53^\infty) < 2$. Since $23 | \sigma(3^{10})$ and $r \neq 23$, we see that $a \neq 10$. If $a = 6$, then

$$h(n) > h(3^6 7^2 17^4 19^2 47^2 1093) > 2.$$

If $a \geqslant 12$, then $h(n) < h(3^\infty 7^2 17^\infty 19^\infty 47^\infty 13121^\infty 100129^\infty) < 2$.

If $7^4 | n$, then $q = 19$. For if $q = 23$ then either $h(n) > h(3^6 \cdot 7^4 17^4 23^2 31^2) > 2$ or $h(n) < h(3^\infty 7^\infty 17^\infty 23^\infty 1093^\infty 100129^\infty 37^\infty) < 2$ since there are no primes between 31 and 37. Also, $r \leqslant 53$ since $h(3^\infty 7^\infty 17^\infty 19^\infty 1093^\infty 100129^\infty 59^\infty) < 2$. Therefore, either $a = 6$ and $h(n) > h(3^6 7^4 17^4 19^2 1093 \cdot 53) > 2$ or $a \geqslant 10$ and $h(n) > h(3^{10} 7^4 17^4 19^4 53^2) > 2$ ($19^2 \nparallel n$ since $\sigma(19^2) = 3 \cdot 127$). These contradictions show that $p \neq 17$ so that $p = 11$ or 13. □

PROPOSITION 14.1. $11 \cdot 13 \nmid n$.

PROPOSITION 16.1. $3 \cdot 7 \cdot 13 \nmid n$.

PROPOSITION 18.1. $3 \cdot 7 \cdot 11 \nmid n$.

PROPOSITION 20.1. $3 \cdot 5^2 \nmid n$.

PROPOSITION 21.1. $5 \| n$.

LEMMA 21.2. *If* $3^4 \| n$, *then* $11^{12} | n$ and $P > V = 2^{28} + 1$.

Proof. Assume that $n = 3^4 5 \cdot 11^c q^d r^e s^f P^g$. From Proposition 6.6, $q \equiv r \equiv s \equiv P \equiv 1(3)$. Since $h(3^4 5 \cdot 11^\infty 100129^\infty 211^\infty 223^\infty 229^\infty) < 2$, it follows from (28) that $73 \leqslant q \leqslant 199$. Since $h(3^4 5 \cdot 11^\infty 73^\infty 100129^\infty 5407^\infty 5413^\infty) < 2$, $r \leqslant 5347$. Now, let t be the smallest prime factor of $c + 1$. Of course, $F_t(11) | n$. Since $7 | F_3(11)$, $3221 | F_5(11)$, $43 | F_7(11)$, $15797 | F_{11}(11)$ *and* since $3221 \equiv 15797 \equiv 2(3)$ we see that $t \geqslant 13$ so that $11^{12} | n$. $F_{13}(11) = 1093 \cdot 3158528101$, $F_{17}(11) = 50544702849929377$, and $F_{19}(11) = M$ where $M \approx 6.11 \cdot 10^{18}$ and every prime factor of M exceeds 10^7. Therefore, if $t \leqslant 19$, we see that $P \geqslant \sqrt{M} > 10^9 > V$. If $t \geqslant 23$ and $F_t(11)$ is not square-free, then, from (15), $P > V$. If $t \geqslant 23$ and $F_t(11)$ is square-free, then $F_t(11) = q^\alpha r^\beta W$ where $0 \leqslant \alpha, \beta \leqslant 1$ and W has at most two prime factors (since n has exactly seven prime divisors). Therefore, $W \geqslant F_{23}(11)/qr > 11^{22}/(199 \cdot 5347) > 7.6 \cdot 10^{16}$ *and* $P > \sqrt{W} > V$. □

PROPOSITION 21.2. $3^2 \| n$.

THEOREM 22.1. *Every odd perfect number has at least eight distinct prime factors.*

4. Concluding Remarks. The referee has informed me that E. Z. Chein in his 1979 doctoral dissertation (Pennsylvania State University) has also proved Theorem 22.1. It might be pertinent to point out that the present author announced the result of this paper in a talk at the 81st Annual Meeting of the American Mathematical Society held in Washington, D. C. in January, 1975. An abstract appeared in the January, 1975 issue of the *Notices of the American Mathematical Society*.

Department of Mathematics
Temple University
Philadelphia, Pennsylvania 19122

1. E. Z. CHEIN, "Non-existence of odd perfect numbers of the form $q_1^{a_1}q_2^{a_2} \cdots q_6^{a_6}$ and $5^{a_1}q_2^{a_2} \cdots q_9^{a_9}$." (Unpublished manuscript.)

2. P. HAGIS, JR., "If n is odd and perfect then $n > 10^{45}$. A case study proof with a supplement in which the lower bound is improved to 10^{50}." (Copy deposited in UMT file.)

3. P. HAGIS, JR., "Every odd perfect number has at least eight 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.

5. H. J. KANOLD, "Untersuchungen über ungerade volkommene Zahlen," *J. Reine Angew. Math.*, v. 183, 1941, pp. 98–109.

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

7. T. NAGELL, *Introduction to Number Theory*, Wiley, New York, 1951.

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

9. C. POMERANCE, "The second largest prime factor of an odd perfect number," *Math. Comp.*, v. 29, 1975, pp. 914–921.

10. C. POMERANCE, "Multiply perfect numbers, Mersenne primes, and effective computability," *Math. Ann.*, v. 226, 1977, pp. 195–206.