MATHEMATICS OF COMPUTATION
Volume 72, Number 243, Pages 1549–1554
S 0025-5718(03)01496-0
Article electronically published on January 8, 2003

ODD PERFECT NUMBERS HAVE A PRIME FACTOR EXCEEDING 10^7

PAUL M. JENKINS

ABSTRACT. It is proved that every odd perfect number is divisible by a prime greater than 10^7.

1. INTRODUCTION

A perfect number is a positive integer N which satisfies $\sigma(N) = 2N$, where $\sigma(N)$ denotes the sum of the positive divisors of N. All known perfect numbers are even; it is well known that even perfect numbers have the form $N = 2^{p-1}(2^p - 1)$, where p is prime and $2^p - 1$ is a Mersenne prime. It is conjectured that no odd perfect numbers exist, but this has yet to be proven. However, certain conditions that a hypothetical odd perfect number must satisfy have been found. Brent, Cohen, and teRiele [3] proved that such a number must be greater than 10^{300}. Chein [4] and Hagis [6] each showed that an odd perfect number must have at least 8 distinct prime factors.

The best known lower bound for the largest prime divisor of an odd perfect number was raised from 100110 in 1975 by Hagis and McDaniel [8] to 300000 in 1978 by Condict [5] to 500000 in 1982 by Brandstein [2]. Most recently, Hagis and Cohen [7] proved that the largest prime divisor of an odd perfect number must be greater than 10^6. Iannucci [9], [10] showed that the second largest prime divisor must exceed 10^4 and that the third largest prime divisor must be greater than 100.

This paper improves the lower bound for the largest prime divisor of an odd perfect number, proving that

Theorem 1.1. *The largest prime divisor of an odd perfect number exceeds* 10^7.

The proof follows the method used by Hagis and Cohen.

2. RAISING THE BOUND TO 10^7

The proof of Theorem 1.1 is by contradiction. Let N denote an odd perfect number with no prime divisors exceeding 10^7.

Nonnegative integers will be symbolized by $a, b, c, \ldots$, and p, q and r will represent odd prime numbers. The notation $p^a \| n$ means that $p^a | n$ and $p^{a+1} \nmid n$. The dth cyclotomic polynomial will be denoted by F_d, so that $F_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. If p and m are relatively prime, $h(p, m)$ will represent the order of p modulo m.

It is well known that $N = p_0^{a_0} p_1^{a_1} \cdots p_u^{a_u}$, where the p_i are distinct odd primes, $p_0 \equiv a_0 \equiv 1 \mod 4$, and $2 | a_i$ if $i > 0$. We call p_0 the *special* prime.

Received by the editor November 7, 2001.
2000 *Mathematics Subject Classification.* Primary 11A25, 11Y70.

Hagis and Cohen [7] give the equation

$$2N = \prod_{i=0}^{u} \sigma(p_i^{a_i}) = \prod_{i=0}^{u} \prod_{\substack{d|(a_i+1)\\ d>1}} F_d(p_i), \tag{2.1}$$

where $p_i|N$.

Theorems 94 and 95 in Nagell [12] state that

Lemma 2.1. *It is true that $q|F_m(p)$ if and only if $m = q^b h(p;q)$. If $b > 0$, then $q\|F_m(p)$. If $b = 0$, then $q \equiv 1 \pmod{m}$.*

It follows from Lemma 2.1 that, for r prime,

Lemma 2.2. *If $q|F_r(p)$, then either $r = q$ and $p \equiv 1 \pmod{q}$, so that $q\|F_r(p)$, or $q \equiv 1 \pmod{r}$.*

Lemma 2.3. *If $q = 3$ or 5 and $m > 1$ is odd, then $q|F_m(p)$ (and $q\|F_m(p)$) if and only if $m = q^b$ and $p \equiv 1 \pmod{q}$.*

A result originally from Bang [1], as documented by Pomerance [13], shows that

Lemma 2.4. *If p is an odd prime and $m \geq 3$, then $F_m(p)$ has at least one prime factor q such that $q \equiv 1 \pmod{m}$.*

It is obvious that the set of primes p_i dividing N is identical to the set of odd prime factors of the $F_d(p_i)$ in (2.1), so all prime factors of each $F_d(p_i)$ must be less than 10^7. In particular, if r is a prime divisor of $a_i + 1$, then every prime factor of $F_r(p_i)$ must be less than 10^7.

Define $F_r(p)$ to be *acceptable* if every prime divisor of $F_r(p)$ is less than 10^7. It follows that if $r > 5000000$, then $F_r(p)$ is unacceptable for an odd prime p.

Computer searches showed that if $3 \leq p < 10^7$ and $r \geq 7$, then $F_r(p)$ is unacceptable except for 143 pairs of values of p and r. This table appears in [11], which can be found online at `http://www.math.byu.edu/OddPerf`.

We will show that for each of these 143 pairs (r, p), $F_r(p)$ cannot appear as a factor of N on the right-hand side of 2.1.

Lemma 2.5. *No prime in the set X of "small" primes*

$$X = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 43, 61,$$
$$71, 113, 127, 131, 151, 197, 211, 239, 281, 1093\}.$$

divides N.

These primes are considered in the order

$$1093, 151, 31, 127, 19, 11, 7, 23, 31, 37, 43, 61,$$
$$13, 3, 5, 29, 43, 17, 71, 113, 197, 211, 239, 281.$$

A contradiction is derived in the case that each of these primes divides N. For example, after proving that $1093 \nmid N$, the proof that $151 \nmid N$ is as follows:

Assume that $151|N$. One value of $F_r(151)$ must divide $2N$, where r is prime. List the values of $F_r(151)$ from the table of acceptable values of $F_r(p)$ and for $r = 3, 5$. ($r = 2$ is not considered because $151 \not\equiv 1 \mod 4$, so 151 is not the special prime.)

No such values appear in the table, $F_3(151) = 3 \cdot 7 \cdot 1093$ (contradicting $1093 \nmid N$), and $F_5(151) = 5 \cdot 104670301$ is unacceptable. Thus $151 \nmid N$. If an acceptable value of $F_r(151)$ existed, each of its odd prime factors would divide N, and we would select one such factor and iterate this process until a contradiction is reached. The complete proof of this lemma appears in the appendix to [11].

When these primes are eliminated as factors of $F_r(p)$, most pairs (r, p) in the table are eliminated. From the remaining values, it follows that if $r > 5$, then

$$p \in \{67, 173, 607, 619, 653, 1063, 1453, 2503, 4289, 5953, 9103, 9397,$$
$$10889, 12917, 19441, 63587, 109793, 113287, 191693, 6450307, 7144363\}.$$

Each of these primes is then eliminated in a manner similar to that used to eliminate the "small" primes. This proves

Lemma 2.6. *If $p^a \| N$ and p is not the special prime p_0, then $a + 1 = 3^b \cdot 5^c$, where $(b + c) > 0$. If $p_0^{a_0} \| N$, then $a_0 + 1 = 2 \cdot 3^b \cdot 5^c$, where $(b + c) \geq 0$.*

Let $S = \{47, 53, 59, \ldots\}$ be the set of all primes p such that $p \not\equiv 1 \pmod 3$, $p \not\equiv 1 \pmod 5$ and $37 < p < 10^7$.

If $p|N$ and $p|F_d(p_i)$ and $d \neq 2$; then, since $d|(a_i + 1)$, either $3|d$ or $5|d$ by Lemma 2.6. By Lemmas 2.1 and 2.5, either $p \equiv 1 \pmod 3$ or $p \equiv 1 \pmod 5$, so $p \notin S$.

Suppose that $p_i \in S$ and $p_i^{a_i} \| N$ and $p_i | F_2(p_0)$. Then $p_i^{a_i} \| F_2(p_0)$ from the previous statement, and if two elements of S were divisors of $F_2(p_0)$, then $F_2(p_0) = p_0 + 1 \geq 2 \cdot 47^2 \cdot 53^2 = 12410162$. This is impossible, since $p_0 < 10^7$. Thus, at most one element of S can divide $F_2(p_0)$. Note also that if $p_0 \in S$, then $p_0 \equiv 2 \pmod 3$ and $3|(p_0 + 1) = F_2(p_0)$, contradicting Lemma 2.5. Thus, $p_0 \notin S$.

We have proved

Lemma 2.7. *The number N is divisible by at most one element of S. If there is such an element s, then $s \neq p_0$ and $s \geq 47$.*

A computer search showed that S has 249278 elements, and that

$$S^* = \prod_{p \in S} \frac{p}{p - 1} > 1.7331909144375899931. \tag{2.2}$$

Let $T = \{61, 151, 181, \ldots\}$ be the set of all primes p such that $p \equiv 1 \pmod{15}$ and $37 < p < 10^7$.

Suppose that $p_i \in T$ and $p_i \neq p_0$. If $p_i^{a_i} \| N$, then either $3|(a_i + 1)$ or $5|(a_i + 1)$ by Lemma 2.6. By (2.1) and Lemma 2.3, either $F_3(p_i)|N$, in which case $3|N$, or $F_5(p_i)|N$, in which case $5|N$. In either case Lemma 2.5 is contradicted, so $p_i \nmid N$.

Thus,

Lemma 2.8. *The number N is divisible by at most one element of T. If there is such an element it is p_0, and then $p_0 \geq 61$.*

A computer search showed that T has 83002 elements, and that

$$T^* = \prod_{p \in T} \frac{p}{p - 1} > 1.1791835683407662159. \tag{2.3}$$

Let $U = \{73, 79, 103, \ldots\}$ be the set of all primes p such that $p \equiv 1 \pmod 3$, $p \not\equiv 1 \pmod 5$, $F_5(p)$ has a prime factor greater than 10^7, and $37 < p < 10^7$.

Suppose $p_i \in U$ and $p_i \neq p_0$. If $p_i^{a_i} \| N$, then by Lemma 2.6 either $3|(a_i + 1)$ or $5|(a_i + 1)$. If $3|(a_i + 1)$, then $F_3(p_i)|N$ and $3|N$, contradicting Lemma 2.5. If $5|(a_i + 1)$, then $F_5(p_i)|N$ and N has a factor greater than 10^7, a contradiction. Thus, $p_i \nmid N$.

It is, therefore, true that

Lemma 2.9. *The number N is divisible by at most one element of U. If there is such an element it is p_0, and then $p_0 \geq 73$.*

A computer search showed that U has 694 elements less than 20000, and that

$$U^* = \prod_{p \in U} \frac{p}{p-1} > \prod_{\substack{p \in U \\ p < 20000}} \frac{p}{p-1} > 1.239225225. \tag{2.4}$$

Let $V = \{3221, 3251, 3491, \ldots\}$ be the set of all primes p such that $p \equiv 1 \pmod 5), p \not\equiv 1 \pmod 3), F_3(p)$ has a prime factor greater than 10^7, and $37 < p < 10^7$.

Suppose $p_i \in V$. Since $p_i \not\equiv 1 \pmod 3$, it must be true that $p_i \equiv 2 \pmod 3$ and thus that $3|(p_i + 1) = F_2(p_i)$. But $F_2(p_0)|N$ and $3 \nmid N$, so $p_i \neq p_0$. If $p_i^{a_i} \| N$, then by Lemma 2.6 either $3|(a_i + 1)$ or $5|(a_i + 1)$. If $5|(a_i + 1)$, then $F_5(p_i)|N$ and $5|N$, contradicting Lemma 2.5. If $3|(a_i + 1)$, then $F_3(p_i)|N$ and N has a factor greater than 10^7, a contradiction. Thus, $p_i \nmid N$.

It is, therefore, true that

Lemma 2.10. *The number N is not divisible by any element of V.*

A computer search showed that V has 57 elements less than 20000, and that

$$V^* = \prod_{p \in V} \frac{p}{p-1} > \prod_{\substack{p \in V \\ p < 20000}} \frac{p}{p-1} > 1.006054597. \tag{2.5}$$

Note that S, T, U, and V are pairwise disjoint.

There are 664567 primes p such that $37 < p < 10^7$, and

$$P^* = \prod_{41 \leq p < 10^7} \frac{p}{p-1} < 4.269448664996309337. \tag{2.6}$$

If $p^a \| N$, then

$$1 < \sigma(p^a)/p^a = (p^{a+1} - 1)/(p^a(p-1)) < p/(p-1).$$

Since σ is a multiplicative function,

$$\frac{\sigma(N)}{N} = \frac{\sigma(p_0^{a_0})\sigma(p_1^{a_1}) \cdots}{p_0 p_1 \cdots} < \prod_{i=0}^{u} \frac{p_i}{p_i - 1}.$$

From Lemma 2.5, $p_i > 37$. Since $x/(x-1)$ is monotonic decreasing for $x > 1$, it follows that if $p_i \in S$, then $p_i/(p_i - 1) < 47/46$, and if $p_i \in T$ or U, then $p_i/(p_i - 1) < 61/60$. Thus, it follows from Lemmas 2.7–2.10, and inequalities (2.1)–(2.6) that

$$2 = \frac{\sigma(N)}{N} < \prod_{i=0}^{u} \frac{p_i}{p_i - 1} \leq \frac{47}{46} \frac{61}{60} \frac{P^*}{S^* T^* U^* V^*} < 1.740567 \tag{2.7}$$

This contradiction proves Theorem 1.1.

3. Interesting details on the computer searches

These arguments follow closely those appearing in Section 7 of Hagis and Cohen's paper [7].

Let $Q(r)$ be the product of all primes less than 10^7 and congruent to $1 \pmod r$. If $2142 < r < 5000000$, a computer search showed that if $10^2 < p < 10^7$, then $Q(r)^2 < 10^{2(r-1)} < p^{r-1} < F_r(p)$. Additionally, if $q < 10^7$, then $q^3 \nmid F_r(p)$, except that $60647^3 \| F_{30323}(6392117)$ and $10709^3 \| F_{2677}(6619441)$.

These and other elementary computations lead to the conclusion that if $r > 2142$ and $10^2 < p < 10^7$, then $F_r(p)$ has a prime factor greater than 10^7.

Suppose that $1472 < r < 2142$ and $10^2 < p < 10^7$. A computer search showed that if $q < 10^7$, then $q^3 \nmid F_r(p)$, except that $3119^3 \| F_{1559}(146917)$ and $2999^3 \| F_{1499}(8474027)$, and $q^2 \| F_r(p)$ for at most one q for each $F_r(p)$. Searches also showed that $10^7 \cdot Q(r) < 10^{2(r-1)}$ for all r in this range.

Again, it follows after additional computations that if $1472 < r < 2142$ and $10^2 < p < 10^7$, then $F_r(p)$ has a prime factor greater than 10^7.

For $7 \leq r < 1472$ and $p < 10^7$, more computation was necessary. For each $F_r(p)$, the primes $q < 10^7$ that divide $F_r(p)$ were determined. It is easily seen that $F_r(p)$ has a prime factor greater than 10^7 if and only if

$$\prod_{\substack{q^b \| F_r(p) \\ q < 10^7}} q^b < p^{r-1}.$$

In this manner, a table of acceptable values of $F_r(p)$ was generated.

The UBASIC and MAPLE programs used in the proof of Theorem 1.1 can be found online at `http://www.math.byu.edu/OddPerf`.

4. Concluding remarks

Let R be the largest prime factor of the odd perfect number N. It has been shown here that $R > 10^7$. It seems probable that this proof could be extended to raise the lower bound for R, using the same methods, since the inequality proving the theorem is much stronger than is necessary and could be strengthened even further by calculating U^* and V^* for the entire sets U and V instead of just the elements less than 20000. Unfortunately, the time that would be required to find acceptable values of $F_r(p)$ for $r \geq 7$ for a larger lower bound seems to be great enough to make this computation impractical. If $\pi(x)$ is the number of primes not exceeding x, then to generate this table for a lower bound of R for the largest prime divisor of N, $\pi(R) \cdot \pi(R/2)$ values of $F_r(p)$ must be examined for acceptability.

Hagis and Cohen [7] used approximately 700 hours of computing time proving that $R \geq 10^6$, using a CYBER 860 and a 486 PC. The computations in this paper required approximately 2930 hours of processor time on a dual-processor 866 MHz Pentium III and approximately 22870 hours of processor time on twenty-two 300 MHz Pentium II's. The bound was increased only by a factor of 10, but the time required, even with advances in computer technology, increased by a factor of 36.

References

1. A. Bang, *Taltheoretiske undersøgelser*, Tidsskrift Math. **5 IV** (1886), 70–80, 130–137.
2. M. Brandstein, *New lower bound for a factor of an odd perfect number*, Abstracts Amer. Math. Soc. **3** (1982), 257, 82T-10-240.

3. R. P. Brent, G. L. Cohen, and H. J. J. te Reile, *Improved techniques for lower bounds for odd perfect numbers*, Mathematics of Computation **57** (1991), 857–868. MR **92c:**11004
4. E. Chein, *An odd perfect number has at least 8 prime factors*, Ph.D. thesis, Pennsylvania State University, 1979.
5. J. Condict, *On an odd perfect number's largest prime divisor*, Senior Thesis, Middlebury College, 1978.
6. P. Hagis, Jr., *Outline of a proof that every odd perfect number has at least eight prime factors*, Mathematics of Computation **35** (1980), 1027–1032. MR **81k:**10004
7. P. Hagis, Jr. and G. L. Cohen, *Every odd perfect number has a prime factor which exceeds* 10^6, Mathematics of Computation **67** (1998), 1323–1330. MR **98k:**11002
8. P. Hagis, Jr. and W. McDaniel, *On the largest prime divisor of an odd perfect number II*, Mathematics of Computation **29** (1975), 922–924. MR **51:**8021
9. D. E. Iannucci, *The second largest prime divisor of an odd perfect number exceeds ten thousand*, Mathematics of Computation **68** (1999), 1749–1760. MR **2000i:**11200
10. ______, *The third largest prime divisor of an odd perfect number exceeds one hundred*, Mathematics of Computation **69** (2000), 867–879. MR **2000i:**11201
11. Paul M. Jenkins, *Odd perfect numbers have a prime factor exceeding* 10^7, Senior Thesis, Brigham Young University, 2000.
12. T. Nagell, *Introduction to number theory*, second ed., Chelsea, New York, 1964. MR **30:**4714
13. C. Pomerance, *Odd perfect numbers are divisible by at least seven distinct primes*, Acta. Arith. **25** (1974), 265–300, MR **49:**4925

Department of Mathematics, Brigham Young University, Provo, Utah 84602
E-mail address: `pmj5@math.byu.edu`