J. Austral. Math. Soc. (Series A) **42** (1987), 280–286

ON THE LARGEST COMPONENT OF AN ODD PERFECT NUMBER

GRAEME L. COHEN

(Received 25 June 1985; revised 20 September 1985)

Communicated by J. H. Loxton

Abstract

It is shown that any odd perfect number has a component greater than 10^{20}.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 11 A 25.

1

Let $\sigma(N)$ be the sum of the positive divisors of a natural number N. We say N is perfect if $\sigma(N) = 2N$. No odd perfect numbers have been found, nor has a proof of their nonexistence. However a great many necessary conditions that an odd perfect number, if there is one, must satisfy have been found.

Many of these conditions have a qualitative nature. For example, assuming henceforth that N is odd and perfect, Euler showed that

$$N = \prod_{i=0}^{u} q_i^{b_i},$$

where $q_0, \ldots, q_u$ are distinct odd primes, and where (say) $q_0 \equiv b_0 \equiv 1 \pmod 4$ and $b_i \equiv 0 \pmod 2$ $(1 \leqslant i \leqslant u)$. We shall take this as our standard form for N. Also, Steuerwald [10] showed that we cannot have $b_i = 2$ for $1 \leqslant i \leqslant u$, and McDaniel [6] generalised this by showing that we cannot have $b_i \equiv 2 \pmod 6$ for $1 \leqslant i \leqslant u$. The other conditions are numerical, and most have been steadily improved over the last twenty years. They concern, for example, lower bounds for N, u and the largest prime factor of N. (See Guy [3] for details.)

Probably the most longstanding of these numerical conditions is the often-quoted result of Muskat [8] that N must be divisible by a prime power greater than 10^{12}. This bound was improved to 10^{18} by Tuckerman [11] for the special case in which 3 or 5 divides N. We shall call each $q_i^{b_i}$ a component of N, and in this paper will prove

THEOREM 1. *Any odd perfect number has a component greater than* 10^{20}.

To prove this using Muskat's approach (which depended on Steuerwald's result, above) would require the investigation of each odd prime less than 10^5. Instead, we shall use another result of McDaniel [7] and consider first those N with $b_i = 2$ or 4 for $1 \leqslant i \leqslant u$. Having shown that for such N there must be a component greater than 10^{20}, we may then assume that $b_i \geqslant 6$ for at least one $i (1 \leqslant i \leqslant u)$, so that, since $2161^6 > 10^{20}$, we need only investigate each odd prime less than 2160.

The large amount of computational work necessary for the proof of Theorem 1 is given separately in [2], which consists of 38 typed pages in six appendices. The computations were carried out on the Honeywell Level 66 computer at the New South Wales Institute of Technology and, by using the multiprecision capabilities of the algebraic manipulation package MuMATH, on an Apple II.

Most of the computing involved factorisation (we used trial division and Fermat's method, with sieve) and primality testing (based on Fermat's theorem), with numbers of up to 20 digits. It is the number of factorisations required, rather than their individual difficulty if modern methods are used, which would be daunting if our lower bound of 10^{20} were to be improved by the method described in this paper.

2

We give here some notation and known results which will be used often in what follows. Since $\sigma(N) = 2N$, any odd divisor of $\sigma(N)$ is also a divisor of N. It is well known that

$$\sigma(N) = \prod_{i=0}^{u} \sigma\left(q_i^{b_i}\right) \quad \text{and} \quad \sigma\left(q_i^{b_i}\right) = \prod_{m_i} F_{m_i}(q_i) \qquad (0 \leqslant i \leqslant u),$$

where $m_i > 1$, $m_i \mid b_i + 1$ and F_{m_i} is the cyclotomic polynomial of order m_i. In particular (when $m_0 = 2$), we have $(q_0 + 1)/2 \mid N$.

The letters p and q will always denote odd primes.

The prime factors of N are the odd prime factors of the $F_{m_i}(q_i)$. Divisor properties of cyclotomic polynomials were given by Nagell [9] and summarised by McDaniel [7] as follows: If $m = p^a d$, where $p \nmid d$, then $p \mid F_m(q)$ if and only if

$p \equiv 1 \pmod{d}$ and q belongs to $d \pmod{p}$; further, if $a > 0$ and $p \mid F_m(q)$, then $p \| F_m(q)$. In the special case when p is a Fermat prime (that is, of the form $2^c + 1$) and $p \mid F_m(q)$ (where $m > 1$ is odd), we must have $p \| F_m(q)$ and $m = p^a$.

3

In [7], McDaniel proved that if $b_i = 2$ or 4 for all i, $1 \leqslant i \leqslant u$, then N has no prime divisor smaller than 100. We shall later extend this, but first we use McDaniel's result to prove

THEOREM 2. *Suppose* $N = q_0^{b_0}\prod_{i=1}^{t} q_i^2 \prod_{i=t+1}^{u} q_i^4$ *is an odd perfect number. Then*

$$\tfrac{1}{4}(t-1) \leqslant u - t \leqslant 2t + \sqrt{b_0}\,.$$

PROOF. Since $3 \nmid N$, we have $q_i \equiv 2 \pmod 3$ for $1 \leqslant i \leqslant t$. Further, for $1 \leqslant i \leqslant t$, we also have

$$\sigma\left(q_i^2\right) = q_0^{a_i}\prod_{j=t+1}^{u} q_j^{b_{i,j}}, \qquad 0 \leqslant a_i \leqslant b_0,\, 0 \leqslant b_{i,j} \leqslant 4 \quad (t+1 \leqslant j \leqslant u),$$

since divisors of $\sigma(q_i^2) = F_3(q_i)$ are congruent to $1 \pmod 3$. At most $4(u-t)$ values of i ($1 \leqslant i \leqslant t$) are such that $q_j \mid \sigma(q_i^2)$ for some j ($t+1 \leqslant j \leqslant u$). Then, if $t > 4(u-t)$, we have $\sigma(q_i^2) = q_0^{a_i}$ for the remaining values of i ($1 \leqslant i \leqslant t$). Brauer [1] showed that this equation is solvable (for primes q_i, q_0) only when $a_i = 1$, so there is at most one such i. Hence $t \leqslant 4(u-t) + 1$, which gives the left-hand inequality in the theorem. (This is all that is required below, but the right-hand inequality is also of interest.)

Since $5 \nmid N$, $q_i \not\equiv 1 \pmod 5$ for $t+1 \leqslant i \leqslant u$. Then, for $t+1 \leqslant i \leqslant u$, we have

$$\sigma\left(q_i^4\right) = q_0^{c_i}\prod_{j=1}^{t} q_j^{d_{i,j}}, \qquad 0 \leqslant c_i \leqslant b_0,\, 0 \leqslant d_{i,j} \leqslant 2 \quad (1 \leqslant j \leqslant t),$$

since divisors of $\sigma(q_i^4) = F_5(q_i)$ are congruent to $1 \pmod 5$. At most $2t$ values of i ($t+1 \leqslant i \leqslant u$) are such that $q_j \mid \sigma(q_i^4)$ for some j ($1 \leqslant j \leqslant t$). If $u - t > 2t$, then $\sigma(q_i^4) = q_0^{c_i}$ for the remaining values of i ($t+1 \leqslant i \leqslant u$). Since $3 \nmid N$, c_i is odd (Inkeri [5]), and $1 + 3 + 5 + \cdots + (2k-1) = k^2 > b_0$ if $k > \sqrt{b_0}$, so there are at most $\sqrt{b_0}$ such values of i. Thus $u - t \leqslant 2t + \sqrt{b_0}$, which completes the proof of Theorem 2.

Suppose still that N has the form given in Theorem 2.

If the smallest prime factor of N is 739 or greater, then N has at least 47326 prime factors, for there are exactly 47325 primes from 739 to 578309, inclusive, and, if there are fewer prime factors of N, then

$$\frac{\sigma(N)}{N} < \prod_{i=0}^{u} \frac{q_i}{q_i - 1} \leqslant \prod_{p=739}^{578309} \frac{p}{p-1} < 2.$$

Then, using Theorem 2, we obtain

$$47326 \leqslant u + 1 \leqslant 5(u - t) + 2,$$

so that $u - t \geqslant 9465$. Write P_i for the ith prime. Then $P_{131} = 739$ and $P_{9465+131-1} = P_{9595} = 100043$, so that N has a prime factor at least as large as 100043 occurring to the fourth power. Hence N has a component greater than 10^{20}.

It remains here to show that N, as given in Theorem 2, can have no prime factor less than 739. The details of this may be found in Appendix 1 of [2]. Therefore we have proved

LEMMA 1. *Any odd perfect number with all even exponents equal to* 2 *or* 4 *has a component greater than* 10^{20}.

REMARK 1. As in [7], it now follows, by using the numbers above, that any odd perfect number less than 10^{482711} is divisible by the sixth power of a prime.

4

Suppose further now that all components of N are less than 10^{20}. According to Lemma 1, we may assume that $b_i \geqslant 6$ for at least one i $(1 \leqslant i \leqslant u)$. Further, for such i, $q_i \leqslant 2153$, for otherwise N has a component equal to at least $2161^6 > 10^{20}$. Let A be the set of odd primes less than 2160. To complete the proof of Theorem 1, we consider all prime powers q^b, for $q \in A$, b even, $b \geqslant 6$, as possible components of N, in each case obtaining a contradiction to the definition of N.

In practice, it is convenient to eliminate entirely certain primes in A as divisors of N. Our starting point for this is Tuckerman's table of computations [12] in which, if 3 or 5 divides N, he showed that N has a component exceeding 10^{18}. There are 49 "nodes" (Tuckerman's word) at which more work is required to extend this bound to 10^{20}. The details are given in Appendix 2 of [2]. This proves

LEMMA 2. *Any odd perfect number divisible by* 3 *or* 5 *has a component greater than* 10^{20}.

REMARK 2. From Lemma 2, it follows quickly that any odd perfect number is greater than 10^{40}. The best currently accepted lower bound is 10^{50} (Hagis [4]).

In Table 1, we list all the primes eliminated in similar fashion as possible divisors of N. Previously eliminated primes are used in subsequent eliminations: the primes in each row of Table 1, after the first, are eliminated by reference to some primes in preceding rows. Table 1 includes all odd primes less than 315. The details of the eliminations are given in Appendix 3 of [2].

TABLE 1

3
5
7, 991
11, 211, 631, 701, 967, 1009, 1051, 1471
13, 31, 71, 163, 229, 241, 307, 379, 421, 1303, 1373
43, 61, 101, 113, 127, 137, 167, 173, 179, 233, 337, 521
29, 59, 97, 109, 191, 251, 269, 293, 743, 911
19, 53, 103, 107, 149, 181, 199, 223, 257, 281, 431, 449
17, 23, 37, 79, 193, 197, 239, 547, 1499, 2003
47, 67, 73, 83, 151, 157, 263, 271, 283, 311, 491, 617, 1723
41, 227, 313, 541
131, 139, 953, 1289, 2087
89, 277

5

Since $317^8 > 10^{20}$, all that remains for the proof of Theorem 1 is to show that if $q^6 \| N$ for $317 \leqslant q \leqslant 2153$ (with q not in Table 1), then N has a component greater than 10^{20}.

For some of these primes q, we have $p \mid \sigma(q^6)$ for some p in Table 1; such q are thereby eliminated. The list of primes eliminated in this way is given in Table 2 where, by $p(\ldots, q, \ldots)$, we mean $p \mid \sigma(q^6)$.

Of the remaining primes q, we list in Table 3 those for which $p \mid \sigma(q^6)$, where $p \equiv 3 \pmod 4$ and $p > 10^{10}$, so that $p^2 \mid N$ if $q^6 \| N$. An asterisk means $\sigma(q^6)$ is prime; if $\sigma(q^6)$ is composite, its factorisation is given in Appendix 4 of [2]. In Table 4 we give primes q for which $\sigma(q^6)$ has a factor p with $p > 10^{10}$ and $p \equiv 5 \pmod{12}$ or $p \equiv 9 \pmod{20}$, so that 3 or 5 divides $F_2(p)$. The factorisations of $\sigma(q^6)$ for these q are given in Appendix 5 of [2]. All these primes q are thus eliminated.

TABLE 2

7(463, 659, 673, 757, 827, 883, 1093, 1163, 1429, 1583, 1597, 1667, 1709, 1877, 1933, 2017, 2129, 2143); 29(373, 397, 401, 487, 509, 571, 587, 661, 683, 691, 719, 761, 857, 877, 919, 977, 1031, 1039, 1069, 1097, 1109, 1151, 1213, 1283, 1301, 1321, 1399, 1531, 1553, 1619, 1669, 1747, 1789, 1823, 1847, 1879, 1901, 1979, 1997, 2053, 2083, 2111, 2113, 2137, 2141, 2153); 43(317, 557, 563, 613, 643, 709, 809, 821, 881, 907, 1091, 1129, 1153, 1423, 1483, 1559, 1607, 1693, 1741, 1913, 1951, 1999, 2099); 71(811, 829, 971, 1181, 1237, 1381, 1511, 1523, 1663, 1949, 2089); 113(367, 593, 727, 787, 1013, 1033, 1123, 1259, 1801, 2027); 127(383, 389, 1907); 197(769, 1021, 1493, 1543); 211(359, 1621, 1811); 239(1697); 281(641, 1867); 337(1019, 1063, 1427); 379(1223, 1231); 421(1759, 1931, 2069); 449(467, 773); 491(823); 547(1103); 617(1993); 631(601); 743(433); 911(1871); 953(1481); 967(1193); 1009(859); 1051(1447, 1453); 1289(1657); 1303(1187); 1373(1049); 1471(1217); 2003(733); 2087(2011)

TABLE 3

349*, 353*, 419, 547, 461*, 751, 839, 941*, 1117*, 1201, 1229*, 1249, 1277*, 1297*, 1307, 1319, 1327, 1409*, 1433, 1459, 1487, 1489*, 1549, 1609*, 1613, 1753*, 1777, 1973, 1987

TABLE 4

479, 503, 577, 797, 929, 937, 983, 1367, 1601, 1699, 1721, 1787, 1861, 1873, 2063, 2081

Only 40 primes in A are not included in Tables 1 to 4. Their elimination as divisors of N follows from the computations given in Appendix 6 of [2].

This completes the proof of Theorem 1.

References

[1] A. Brauer, 'On the non-existence of odd perfect numbers of form $p^\alpha q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$', *Bull. Amer. Math. Soc.* **49** (1943), 712–718.

[2] G. L. Cohen, 'Appendices for "On the largest component of an odd perfect number" ' (available from the author).

[3] R. K. Guy, *Unsolved Problems in Number Theory* (Springer-Verlag, New York, 1981).

[4] P. Hagis, Jr., 'A lower bound for the set of odd perfect numbers', *Math. Comp.* **27** (1973), 951–953.

https://doi.org/10.1017/S1446788700028251 Published online by Cambridge University Press

[5] K. Inkeri, 'On the diophantine equation $a(x^n - 1)/(x - 1) = y^m$', *Acta Arith.* **21** (1972), 299–311.
[6] W. L. McDaniel, 'The non-existence of odd perfect numbers of a certain form', *Arch. Math.* **21** (1970), 52–53.
[7] W. L. McDaniel, 'On the divisibility of an odd perfect number by the sixth power of a prime', *Math. Comp.* **25** (1971), 383–385.
[8] J. B. Muskat, 'On divisors of odd perfect numbers', *Math. Comp.* **20** (1966), 141–144.
[9] T. Nagell, *Introduction to Number Theory* (Wiley, New York, 1951).
[10] R. Steuerwald, 'Verschärfung einer notwendigen Bedigung für die Existenz einer ungeraden vollkommenen Zahl', *S.-Ber. Math.-Nat. Abt. Bayer. Acad. Wiss.* (1937), 68–72.
[11] B. Tuckerman, 'A search procedure and lower bound for odd perfect numbers', *Math. Comp.* **27** (1973), 943–949.
[12] 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, copy deposited in UMT file, reviewed *Math. Comp.* **27** (1973), 1004–1005).

School of Mathematical Sciences
The New South Wales Institute of Technology
Broadway, New South Wales 2007
Australia

https://doi.org/10.1017/S1446788700028251 Published online by Cambridge University Press