IMPROVED TECHNIQUES FOR LOWER BOUNDS FOR ODD PERFECT NUMBERS

R. P. Brent, G. L. Cohen and H. J. J. te Riele

Abstract. If N is an odd perfect number, and $q^k \parallel N$, q prime, k even, then it is almost immediate that $N > q^{2k}$. We prove here that, subject to certain conditions verifiable in polynomial time, in fact $N > q^{5k/2}$. Using this and related results, we are able to extend the computations in an earlier paper to show that $N > 10^{300}$.

1. Introduction. A natural number N is *perfect* if $\sigma(N) = 2N$, where σ is the positive divisor sum function. It is not known whether odd perfect numbers exist. In an earlier paper [2], the first two authors described an algorithm for demonstrating that there is no odd perfect number less than a given bound K, and applied it with $K = 10^{160}$.

That paper, and others referenced in it, are dependent on the simple observation that if N is an odd perfect number and $q^k \parallel N$, where q is prime and k is even, then $N \geq q^k\sigma(q^k) > q^{2k}$. Methods based on this observation require the explicit factorisation of $\sigma(q^k)$ for large values of q^k, which imposes a practical limit on their effectiveness. Fewer factorisations would be required if it were known that $N > q^l$ for $l > 2k$. We shall prove below that, under certain conditions which are readily tested computationally and easily satisfied in the cases to be considered, we in fact have $N > q^{5k/2}$ (Theorem 2, below). In some cases the exponent on q can be raised almost to $3k$ (Theorem 3).

The main result of this paper (Theorem 1) is still heavily dependent on the algorithm in [2], and we assume familiarity with that paper. It was stated at the end of that work that to continue the algorithm to obtain any substantial improvement of the earlier result required the factorisation of the 81-decimal-digit composite number $\sigma(13^{72})$; this factorisation has been completed and the result given in a postscript to [2]. But as our targeted lower bound increased, numerous other "unattainable" factorisations appeared to bar our way. One example is the factorisation of $\sigma(3169^{36})$, a composite number of 127 digits; since $3169^{5\cdot 36/2} = 3169^{90} > 10^{315}$, this factorisation could be avoided by application of Theorem 2. This approach was still not sufficient in some instances, but more powerful results along the same lines allowed us to avoid these factorisations as well.

We have thus been able to prove

THEOREM 1. *There is no odd perfect number less than* 10^{300}.

1980 Mathematics Subject Classification. Primary 11A25; Secondary 11Y05, 11Y70.

Appeared in *Mathematics of Computation* 57 (1991), 857–868.

rpb116 typeset using AMS-TEX

To prove Theorem 1, there were nine cases, all detailed in Section 4, requiring special attention. Apart from these, the original algorithm of [2], with the "q^{2k}" result, was sufficient.

A preliminary version of the present work is contained in [3]. There, the lower bound 10^{200} was obtained.

To describe the new method, we need the definition below. For each $\alpha \geq 0$, f_α is a function defined on the positive integers and satisfying $1 \leq f_\alpha(n) \leq 2^\alpha$ (so in particular $f_0(n) = 1$). We shall choose f_α as appropriate later.

Definition. *Let q be an odd prime and k a positive integer. Define*

$$\begin{aligned} E_\alpha(q,k) = \{\, p^\beta \mid\ & p \text{ odd prime}, \ \beta \geq 2, \ \beta \text{ even or } \beta \equiv p \equiv 1 \pmod 4, \\ & (\exists j)(0 < j \leq k, \ p^\beta / f_\alpha(p) < q^{2j} \text{ and } q^j \parallel \sigma(p^\beta)) \,\} \end{aligned}$$

and

$$\epsilon_\alpha(q,k) = \sum_{p^\beta \in E_\alpha(q,k)} \log_q(q^{2j} f_\alpha(p)/p^\beta).$$

(The value of j in the sum is that for which $q^j \parallel \sigma(p^\beta)$.)

Write ϵ for ϵ_0.

We can compute an upper bound on $\epsilon_\alpha(q,k)$ in time polynomial in q and k by an efficient "lifting" algorithm, described in Hardy and Wright [7, Theorem 123]. Usually, $\alpha = 0$ and $\epsilon(q,k)$ is quite small; numerical results will be given in Section 3.

We assume in the following that N is an odd perfect number. According to Euler, we may write

$$N = q^k \prod_{i=1}^{j} p_i^{\beta_i},$$

where q and the p_i are distinct odd primes, $p_1 \equiv \beta_1 \equiv 1 \pmod 4$ and $k \equiv \beta_2 \equiv \cdots \equiv \beta_j \equiv 0 \pmod 2$. It is easy to show that $j \geq 2$, and we make implicit use of this below; in fact, it is known that $j \geq 7$ (Hagis [6]). Each $p_i^{\beta_i}$, and q^k, are called components of N.

Our new results follow.

Theorem 2. *Let N, q^k and $\epsilon(q,k)$ be as above. Then, provided $k \geq 6\epsilon(q,k)$ and $\sigma(q^k)$ is not a square and has no prime factors less than $\frac{1}{2}q^{\epsilon(q,k)}$, we have $N > q^{5k/2}$.*

Theorem 3. *Let N, q^k, $\epsilon(q,k)$ and p_1 be as above. Let M be a unitary divisor of N (that is, $M \mid N$ and $\gcd(M, N/M) = 1$), such that $q \nmid M$, $q \nmid \sigma(M)$ and $p_1 \nmid M$. Then*

$$N > \tfrac{1}{2} M q^{3k - k_1 - \epsilon(q,k)},$$

where $q^{k_1} \parallel p_1 + 1$.

2. Proofs of Theorems 2 and 3. The proofs depend on a number of lemmas, some of which will also be used independently in the proof of Theorem 1.

Lemma 1. *If p and q are odd primes with $p \mid \sigma(q^k)$ and $q^m \mid p+1$, then $k \geq 3m$.*

Proof. Since $q^m \mid p+1$, we have $p+1 = 2aq^m$ for some $a > 0$. Then, since $p \mid \sigma(q^k) = (q^{k+1}-1)/(q-1)$,

$$q^{k+1} - 1 = (2aq^m - 1)R,$$

where $R > 0$, and this implies $k \geq m$. From the preceding equation, we have $R \equiv 1 \pmod{q^m}$, so $R = bq^m + 1$ say, and clearly $b > 0$.

Thus

$$q^{k+1} - 1 = (2aq^m - 1)(bq^m + 1), \tag{1}$$

so $q^{k+1} > aq^m \cdot bq^m \geq q^{2m}$, from which $k \geq 2m$.

We also have

$$q^{k+1-m} = 2abq^m + 2a - b,$$

so $b = 2a + \lambda q^m$, where $\lambda = 2ab - q^{k+1-2m}$, the latter implying $\lambda \neq 0$. Then we cannot have both $b < q^m$ and $2a < q^m$, since in that case

$$|\lambda| = \frac{|b-2a|}{q^m} < 1,$$

a contradiction. Hence, $b \geq q^m$ or $2a > q^m$.

From (1), if $2a > q^m$, then

$$q^{k+1} - 1 > (q^{2m} - 1)(q^m + 1),$$

so $q^{k+1} > q^{3m} + q^{2m} - q^m \geq q^{3m}$; and if $b \geq q^m$, then

$$q^{k+1} - 1 \geq (2q^m - 1)(q^{2m} + 1),$$

so $q^{k+1} \geq 2q^{3m} + 2q^m - q^{2m} > q^{3m}$. Either way, we infer that $k \geq 3m$, as required.

The example $p = 5$, $q = 3$, $k = 3$, $m = 1$ shows this result to be best possible.

Lemma 2. *Let q be an odd prime and let S be any nonempty set of prime powers p^β, with p odd and β at least 2 and either even or satisfying $\beta \equiv p \equiv 1 \pmod 4$. For each $p_i^{\beta_i} \in S$, suppose $q^{k_i} \parallel \sigma(p_i^{\beta_i})$ and $k \geq \sum k_i$. Then*

$$\log_q \prod_{p_i^{\beta_i} \in S} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} > 2\sum k_i - \epsilon_\alpha(q,k).$$

Proof. We have quite generally that

$$\frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} > \frac{p_i^{\beta_i}}{f_\alpha(p_i)} = q^{2k_i - (2k_i - \log_q(p_i^{\beta_i}/f_\alpha(p_i)))} = q^{2k_i - \log_q(q^{2k_i} f_\alpha(p_i)/p_i^{\beta_i})},$$

while if $p_i^{\beta_i} \in S \backslash E_\alpha(q,k)$, then $p_i^{\beta_i}/f_\alpha(p_i) \geq q^{2k_i}$. Thus, where $E_\alpha = E_\alpha(q,k)$,

$$\begin{aligned}\log_q \prod_{p_i^{\beta_i} \in S} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} &> 2\sum k_i - \sum_{p_i^{\beta_i} \in S \cap E_\alpha} \log_q(q^{2k_i} f_\alpha(p_i)/p_i^{\beta_i}) \\ &\geq 2\sum k_i - \sum_{p_i^{\beta_i} \in E_\alpha} \log_q(q^{2k_i} f_\alpha(p_i)/p_i^{\beta_i}) \\ &\geq 2\sum k_i - \epsilon_\alpha(q,k),\end{aligned}$$

as required.

We remark that Lemmas 1 and 2 require no reference to odd perfect numbers.

LEMMA 3. *Let N, q^k and $p_1^{\beta_1}$ be as in Section 1.*
(i) *If $\beta_1 > 1$ then*

$$N > \tfrac{1}{2} q^{3k-\epsilon_\alpha(q,k)} \prod_{i=1}^{j} f_\alpha(p_i).$$

(ii) *If $\beta_1 = 1$ then*

$$N > q^{3k-k_1-\epsilon_\alpha(q,k)} \prod_{i=2}^{j} f_\alpha(p_i),$$

where $q^{k_1} \parallel p_1 + 1$.

Proof. (i) Apply Lemma 2 with S equal to the set of components of N/q^k. Then, in Lemma 2, $\sum k_i = k$ and

$$\begin{aligned}2N = \sigma(N) &= \sigma(q^k) \prod_{i=1}^{j} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} \prod_{i=1}^{j} f_\alpha(p_i) \\ &> q^k \cdot q^{2k-\epsilon_\alpha(q,k)} \cdot \prod_{i=1}^{j} f_\alpha(p_i).\end{aligned}$$

(ii) We again apply Lemma 2, this time with S equal to the set of components of $N/q^k p_1$. Then $\sum k_i = k - k_1$ and

$$\begin{aligned}2N = \sigma(N) &= \sigma(q^k)\sigma(p_1) \prod_{i=2}^{j} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} \prod_{i=2}^{j} f_\alpha(p_i) \\ &> q^k \cdot (p_1+1) \cdot q^{2(k-k_1)-\epsilon_\alpha(q,k)} \cdot \prod_{i=2}^{j} f_\alpha(p_i).\end{aligned}$$

Since $p_1 + 1 \geq 2q^{k_1}$, the result follows.

COROLLARY 1. *Let N, q^k and $p_1^{\beta_1}$ be as above. If either* (i) *$\beta_1 > 1$, or* (ii) *$\beta_1 = 1$ and $p_1 \mid \sigma(q^k)$, then*

$$N > q^{8k/3-\epsilon(q,k)}.$$

Proof. Take $\alpha = 0$ in Lemma 3. (i) Since $k \geq 2$ and $q \geq 3$, we have $q^{k/3} > 2$ and the result follows from Lemma 3 (i). (ii) From Lemma 1, $k \geq 3k_1$ so the result follows from Lemma 3 (ii) since $3k - k_1 \geq 3k - k/3 = 8k/3$.

LEMMA 4. *Let N, q^k and p_1 be as in Section 1. Suppose that $\sigma(q^k)$ is not a perfect square and is not divisible by p_1 or any prime number less than B. Then*

$$N^2 > 2Bq^{5k-\epsilon_\alpha(q,k)} \prod_{i=2}^{j} f_\alpha(p_i).$$

Proof. We shall prove this lemma in the case where $q \mid p_1 + 1$ and $p_1 \parallel N$. (Minor adjustments are needed for the other cases.) Suppose $q^{k_1} \parallel p_1 + 1$. Since $\sigma(q^k)$ is not a perfect square, there is a prime, p_2 say, but not p_1, which divides $\sigma(q^k)$ to an odd power and so divides N to a higher (even) power. Also $p_1 + 1 \geq 2q^{k_1}$ and $p_2 \geq B$, so

$$\begin{aligned} N &\geq q^k \sigma(q^k) p_1 p_2 \\ &\geq q^k \cdot q^k(1 + q^{-1}) \cdot 2q^{k_1}(1 - \tfrac{1}{2}q^{-k_1}) \cdot B \\ &> 2Bq^{2k+k_1}. \end{aligned}$$

From Lemma 3 (ii), we also have $N > q^{3k-k_1-\epsilon_\alpha(q,k)} \prod_{i=2}^{j} f_\alpha(p_i)$. Hence

$$N^2 > 2Bq^{5k-\epsilon_\alpha(q,k)} \prod_{i=2}^{j} f_\alpha(p_i),$$

as required.

Proof of Theorem 2. Take $\alpha = 0$. Since $k \geq 6\epsilon(q,k)$, we have $8k/3 - \epsilon(q,k) \geq 5k/2$, and the theorem follows from Corollary 1, unless $\beta_1 = 1$ and $\sigma(q^k)$ is not divisible by p_1. But then the result follows from Lemma 4, with $B \geq \frac{1}{2}q^{\epsilon(q,k)}$.

Proof of Theorem 3. As in the proof of Lemma 3, we consider two cases. If $\beta_1 > 1$ then apply Lemma 2 with S equal to the set of components of N/Mq^k. Then $\sum k_i = k$, since $q \nmid \sigma(M)$, and

$$\begin{aligned} 2N = \sigma(N) = \sigma(M)\sigma\left(\frac{N}{M}\right) &= \sigma(M)\sigma(q^k) \prod_{\substack{i=1 \\ p_i \nmid M}}^{j} \sigma(p_i^{\beta_i}) \\ &> M \cdot q^k \cdot q^{2k-\epsilon(q,k)} = Mq^{3k-\epsilon(q,k)}. \end{aligned}$$

If $\beta_1 = 1$, then apply Lemma 2 with S equal to the set of components of $N/Mq^k p_1$. Then $\sum k_i = k - k_1$ and

$$\begin{aligned} 2N &= \sigma(M)\sigma(q^k)\sigma(p_1) \prod_{\substack{i=2 \\ p_i \nmid M}}^{j} \sigma(p_i^{\beta_i}) \\ &> M \cdot q^k \cdot 2q^{k_1} \cdot q^{2(k-k_1)-\epsilon(q,k)} = 2Mq^{3k-k_1-\epsilon(q,k)}. \end{aligned}$$

The result follows.

3. Computation of $\epsilon_\alpha(q,k)$. Theorem 2 is useful because an upper bound on $\epsilon_\alpha(q,k)$ can be computed in time which is bounded by a low degree polynomial in q and k. We first outline an algorithm for this computation, and then give a numerical example.

Suppose $p^\beta \in E_\alpha(q,k)$, where $E_\alpha(q,k)$ is defined in Section 1. Since $p \ge 3$ and $p^\beta < 2^\alpha q^{2k}$, we have $\beta < \alpha + 2k \log_3 q$. Thus, to establish the polynomial-time result, it is sufficient to suppose that β is fixed.

Define $F(x) = 1+x+x^2+\cdots+x^\beta$. We can enumerate the set S_j of least positive residues modulo q^j of $F(x) \equiv 0 \pmod{q^j}$ by the "lifting" algorithm described in [7, §8.3]. If $j = 1$, we can simply check all possible solutions 1, 2, ... , $q-1$ (although faster methods, using a primitive root (mod q), are preferable if q is large). If $j > 1$, we apply Theorem 123 of [7] to obtain S_j from S_{j-1}, using what is essentially an application of Newton's method. Since $F(x)$ is a polynomial of degree β, the number $|S_j|$ of solutions is bounded by β.

Define $T_j = \{\, s + \lambda q^j \mid s \in S_j,\ \lambda \ge 0,\ (s+\lambda q^j)^\beta < f_\alpha(s+\lambda q^j) q^{2j} \,\}$. Clearly, $|T_j| \le \lceil 2^{\alpha/\beta} \rceil\, |S_j|$. Since $p^\beta \in E_\alpha(q,k)$, there is some j, $0 < j \le k$, such that $q^j \parallel \sigma(p^\beta)$ and $p^\beta < f_\alpha(p) q^{2j}$. Thus, to enumerate such p^β, we need only check the elements of T_1, T_2, ... , T_k for primality. In order to obtain an upper bound on $\epsilon_\alpha(q,k)$, it is sufficient to use a polynomial-time probabilistic primality test, for the inclusion of a composite p will only increase the computed sum $\sum \log_q(q^{2j} f_\alpha(p)/p^\beta)$. In practice, below, the upper bounds on each $\epsilon_\alpha(q,k)$ are in fact exact results, rounded up if not zero, since each p used was shown to be prime.

Example. To illustrate the algorithm, consider the computation of $\epsilon(3169, 36)$. If $\beta = 2$, $F(x) = 1 + x + x^2$, so $S_1 = \{97, 3071\}$ is the set of solutions of $F(x) \equiv 0 \pmod{3169}$. We construct the sets S_2, S_3, ... , S_{36} as in [7, §8.3], and in each case $|S_j| = 2$. (In this example $\alpha = 0$ so $T_j = S_j$; in general we would add a small number of multiples of q^j to the elements of S_j in order to obtain the set T_j.) Applying a probabilistic primality test to the elements of T_1, T_2, ... , T_{36} rules out all but three possible odd prime p such that $3169^j \parallel \sigma(p^2)$:

$$j = 1,\ \ p = 97;$$
$$j = 3,\ \ p = 5875516237;\ \text{and}$$
$$j = 11,\ p = 26660239989363054908671257959481699820 1.$$

The contributions $\log_{3169}(3169^{2j}/p^2)$ from these three pairs (j, p) are respectively bounded above by 0.8651, 0.4192, and 0.0482.

For $\beta \ge 4$, we proceed similarly, but we find no solutions satisfying all the constraints. (This is typical, since it is unlikely that the constraint $p^\beta < f_\alpha(p) q^{2j}$ will be satisfied if $\beta \ge 4$.) We conclude that only the three pairs given above can contribute to $\epsilon(3169, 36)$, so $\epsilon(3169, 36) \le 1.3325$.

Table 1 gives the details of all nonzero contributions to $\epsilon_\alpha(q,k)$ in the cases relevant to the proof of Theorem 1. Note that there is only one case with $\beta > 2$.

TABLE 1. Nonzero contributions to $\epsilon_\alpha(q,k)$, $q^j \parallel \sigma(p^\beta)$

α	q	k	j	β	$\log_q(q^{2j}f_\alpha(p)/p^\beta)$	p (see below)
0	7	172	8	2	0.5496 ...	3376853
			19	2	0.0607 ...	10744682090246617
			25	2	0.3689 ...	936579478224094047977
			61	2	1.7036 ...	6778 ...
			119	2	1.0771 ...	1292 ...
			150	2	0.3796 ...	4020 ...
0	3221	42	1	4	0.8125 ...	11
0	612067	22	1	2	0.3398 ...	63601
			17	2	0.2253 ...	5291 ...
0	3169	36	1	2	0.8650 ...	97
			3	2	0.4191 ...	5875516237
			11	2	0.0481 ...	2666 ...
221	3	240	1	2	0.9380 ...	37

Large primes p occurring above

677822686658425215407071060694728215733634249273881

1292705670586158487568763039916765694399830534390031_
9630427909162956962804028786608263511417448696587

40205637668275700485119982296550937753326347643003642516228059494_
71752457774955475739650336310509313359098137765181615640612833

52915283185303600217046163660913353511950087333134_
106429889256916343584191707324489815681786937851

266602399893630549086712579594816998201

4. Proof of Theorem 1. Except for the nine cases to be discussed below, the proof is a straight-forward extension of the algorithmic method given in [2]. In particular, it is still valid that the theorem will follow once the primes 127, 19, 7, 11, 31, 13, 3 and 5 are eliminated as possible divisors of N. (As in [2], the elimination of these primes was carried out in the order given.)

The computer output towards the proof of Theorem 1 has 12655 lines. Some relevant extracts are shown below. In these, D means the indicated divisor has already been considered; for details, see [2]. The cases requiring special attention are the following.

(i) Line 7343 concerns the possibility that $3221^{42} \parallel N$. Note that $\sigma(3221^{42}) = c_{148}$, a composite number with 148 decimal digits, unable to be factorised at this time. We have $\epsilon(3221, 42) = \log_{3221}(3221^2/11^4) \leq 0.8126$ (see Table 1); the conditions of Theorem 2 are satisfied, so

$$N > 3221^{105} > 10^{368}.$$

(Such discussions will subsequently be much abbreviated.)

(ii) Line 7163, $\sigma(7^{172}) = c_{146}$, $\epsilon(7,172) \leq 4.1400$. By Theorem 2,

$$N > 7^{430} > 10^{363}.$$

(iii) Line 7985, $\sigma(612067^{22}) = c_{128}$, $\epsilon(612067,22) \leq 0.5652$. By Theorem 2,

$$N > 612067^{55} > 10^{318}.$$

(iv) Line 8866, $\sigma(3169^{36}) = c_{127}$, $\epsilon(3169,36) \leq 1.3324$. By Theorem 2,

$$N > 3169^{90} > 10^{315}.$$

(v) Line 4479, $\sigma(467^{46}) = c_{123}$. We apply Lemma 3, with $\alpha = 0$. The antecedents of this case (see Figure 1) show that $p_1 = 2801$ and $k_1 = 1$. Since $\epsilon(467,46) = 0$,

$$N > 467^{137} > 10^{365}.$$

Figure 1. $\sigma(467^{46})$

4340: $7^2 \Rightarrow 19\ldots,$ D

4341: $7^4 \Rightarrow 2801$

4342: $\quad 2801^1 \Rightarrow 3 \cdot 467$

4343: $\quad\quad 467^2 \Rightarrow 19\ldots,$ D

$\quad\quad$ (some lines omitted)

4479: $\quad\quad 467^{46} \Rightarrow c_{123},$ case (v)

(vi) Line 9527, $\sigma(191^{46}) = c_{105}$. See Figure 2. Lemma 3, with $\alpha = 0$, $p_1 = 30941$, $k_1 = 1$ and $\epsilon(191,46) = 0$, gives

$$N > 191^{137} > 10^{312}.$$

(vii) Line 11343, $\sigma(36389^{22}) = c_{101}$. Observing the antecedents of this case (Figure 3), we may apply Theorem 3 with $M = 3^{\beta_2} \geq 3^{18}$, $p_1 = 363889$, $k_1 = 1$ and $\epsilon(36389,22) = 0$. (Since 3 is a primitive root (mod 36389) and β_2 is even, we know that $36389 \nmid \sigma(3^{\beta_2})$.) Then

$$N > \tfrac{1}{2} \cdot 3^{18} 36389^{65} > 10^{304}.$$

Figure 2. $\sigma(191^{42})$ and $\sigma(191^{46})$

8653: $13^1 \Rightarrow 7,$ D

8654: $13^2 \Rightarrow 3 \cdot 61$

(some lines omitted)

9473: $13^4 \Rightarrow 30941$

9474: $\quad 30941^1 \Rightarrow 3^4 \cdot 191$

9475: $\quad\quad 191^2 \Rightarrow 7\ldots,$ D

$\quad\quad$ (some lines omitted)

9526: $\quad\quad 191^{42} \Rightarrow c_{96},$ case (viii)

9527: $\quad\quad 191^{46} \Rightarrow c_{105},$ case (vi)

(viii) Line 9526, $\sigma(191^{42}) = c_{96}$. The antecedents of this case (Figure 2) show that $p_1 = 30941$ and $191 \parallel \sigma(p_1)$. Then, in Lemma 3, $k_1 = 1$ and $f_\alpha(p_1) \geq 1$, so that

$$N > q^{3k-1-\epsilon_\alpha(q,k)} \prod_{i=2}^{j} f_\alpha(p_i),$$

with $q = 191$, $k = 42$. The bound obtainable from Lemma 3 with $\alpha = 0$ is not quite good enough, so (for the first time) we need to take $\alpha > 0$. For any prime p, we set

$$f_\alpha(p) = \begin{cases} \left(\dfrac{p}{p-1}\right)^\alpha & \text{if } p \mid N,\ p \neq 191 \text{ or } 30941, \\ 1 & \text{otherwise.} \end{cases}$$

Since

$$2 = \frac{\sigma(N)}{N} < \prod_{p \mid N} \frac{p}{p-1} = \frac{191}{190}\,\frac{30941}{30940} \prod_{i=2}^{j} \frac{p_i}{p_i - 1},$$

we have

$$\prod_{i=2}^{j} f_\alpha(p_i) > \left(2 \cdot \frac{190}{191} \cdot \frac{30940}{30941}\right)^\alpha.$$

We need to take α large enough that $\prod_{i=2}^{j} f_\alpha(p_i)$ is large but not so large that $\epsilon_\alpha(191, 42) > 0$. After some experimentation, we find that with $\alpha = 50$ we have $\epsilon_{50}(191, 42) = 0$ and

$$N > 191^{125} \left(2 \cdot \frac{190}{191} \cdot \frac{30940}{30941}\right)^{50} > 10^{300}.$$

Figure 3. $\sigma(36389^{22})$

10615:	$3^2 \Rightarrow 13,\quad \mathrm{D}$
	(some lines omitted)
11214:	$3^{18} \Rightarrow 1597 \cdot 363889$
11215:	$\quad 363889^1 \Rightarrow 5 \cdot 36389$
11216:	$\qquad 36389^2 \Rightarrow 1429 \cdot 926659$
	(some lines omitted)
11343:	$\qquad 36389^{22} \Rightarrow c_{101},\quad$ case (vii)

(ix) Line 12201, $\sigma(3^{240}) = c_{115}$. Since $\epsilon(3, 240) = 0$ and

$$3^{8 \cdot 240/3} = 3^{640} > 10^{305},$$

by Corollary 1 we may assume that $\beta_1 = 1$ and $p_1 \nmid \sigma(3^{240})$. Then, from Lemma 3 (ii),

$$N > 3^{720-k_1} > 10^{300}$$

if $k_1 \leq 91$. Thus we may assume further that $k_1 \geq 92$, so that $p_1 > 3^{92}$. For any prime p, we set

$$f_\alpha(p) = \begin{cases} \left(\dfrac{p}{p-1}\right)^\alpha & \text{if } p \mid N,\ p \neq 3 \text{ or } p_1, \\ 1 & \text{otherwise.} \end{cases}$$

Then, as in (viii),

$$\prod_{i=2}^{j} f_\alpha(p_i) > \left(2 \cdot \frac{2}{3} \cdot \frac{p_1 - 1}{p_1}\right)^\alpha .$$

We find that with $\alpha = 221$ we have $\epsilon_{221}(3, 240) \leq 0.9381$. (It is relevant for this calculation that 7, 13, 19, 31 are "forbidden" divisors. Otherwise, there would be contributions from these primes to the sum defining $\epsilon_{221}(3, 240)$.) Using Lemma 4 with $B = 1$, we have

$$N^2 > 2 \cdot 3^{1200-0.9381} \left(2 \cdot \frac{2}{3} \cdot \frac{3^{92}-1}{3^{92}}\right)^{221} > 10^{600}.$$

This completes the proof of Theorem 1.

The entire computer output is printed in [4]. A copy has been deposited in the UMT file of this journal.

We should mention that the size of the task precluded us from being as fastidious as we were in [2]. The proof contains 199 partial factorisations. We estimate that at most 1658 lines would have been saved if those factorisations were completed. In most cases, the extra lines result from expanding the proof tree using a smaller prime than would be available if the complete factorisation at the relevant line were known. In ten cases, the program had to backtrack from an assumed prime divisor q to another in the same or an earlier branch in order to avoid a composite $\sigma(q^k)$ for which we could find no useful factors. The nine special cases (i)–(ix) arose because this option was not available or was impractical. (This can be seen in Figures 1 and 2.) On the other hand, there were three cases where the proof was shortened by branching on a prime smaller than the largest available (but there was no systematic search for such possibilities).

The program for the proof of Theorem 1 differs from that used in [2] in that, besides calculating bounds named B1, B2 and B3 there, it also calculates, when necessary, "bounds" named B25 and B30, which are $\lfloor \log_{10} q^{5k/2} \rfloor$ and $\lfloor \log_{10} q^{3k} \rfloor$, respectively, for the current assumed component q^k. However, the B25 and B30 "bounds" need not exceed 10^{300}, and the program does not incorporate the calculation of values of ϵ_α, so that they are not rigorous and are used only to flag the need for special discussions, such as those above.

A supplement published with [2] contained the output for that proof. In [4], we include a list of factors of $p^n - 1$ for p prime, $13 \leq p < 10000$, and those values of n (all prime) which arose in our work. This complements the lists in [5] and should prove similarly useful. We take this opportunity to announce the availability of a machine-readable database of factors [1], including all those necessary for the proof of Theorem 1.

Acknowledgments. Some of the factorisations required for the proof of Theorem 1 were obtained using the Fujitsu VP-100 of the Australian National University Supercomputer Facility. Some others were obtained from [5]. We thank the referee for his assistance in improving the exposition.

Computer Sciences Laboratory
Research School of Physical Sciences
The Australian National University
GPO Box 4
Canberra, ACT 2601, Australia

School of Mathematical Sciences
University of Technology, Sydney
PO Box 123
Broadway, NSW 2007, Australia

Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ Amsterdam, The Netherlands

1. R. P. Brent, “Factor: an integer factorization program for the IBM PC”, Report TR-CS-89-23, Computer Sciences Laboratory, Australian National University, October 1989.

2. R. P. Brent and G. L. Cohen, “A new lower bound for odd perfect numbers”, *Math. Comp.*, v. 53, 1989, pp. 431–437, S7–S24.

3. R. P. Brent, G. L. Cohen and H. J. J. te Riele, “An improved technique for lower bounds for odd perfect numbers”, Report TR-CS-88-08, Computer Sciences Laboratory, Australian National University, August 1988.

4. R. P. Brent, G. L. Cohen and H. J. J. te Riele, “Improved techniques for lower bounds for odd perfect numbers”, Report CMA-R50-89, Centre for Mathematical Analysis, Australian National University, August 1988.

5. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to High Powers*, American Mathematical Society, Providence, Rhode Island, Second Edition, 1988.

6. P. Hagis, Jr., “Outline of a proof that every odd perfect number has at least eight prime factors”, *Math. Comp.*, v. 34, 1980, pp. 1027–1032.

7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford University Press, 1962.