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

Improved techniques for lower bounds for odd perfect numbers
The Centre for Mathematics and Computer Science is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Research (N.W.O.).

Copyright © Stichting Mathematisch Centrum, Amsterdam
IMPROVED TECHNIQUES FOR LOWER BOUNDS FOR ODD PERFECT NUMBERS

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

G.L. Cohen
School of Mathematical Sciences
University of Technology, Sydney
PO Box 123, Broadway, NSW 2007, Australia

H.J.J. te Riele
Centre for Mathematics and Computer Science
PO Box 4079, 1009 AB Amsterdam, The Netherlands

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 \( N > 10^{300} \).

1980 Mathematics Subject Classification: Primary 11A25; Secondary 11Y05, 11Y70.
Key Words and Phrases: Odd perfect numbers.
Note: This report has been submitted for publication elsewhere.
1. **Introduction.** A natural number $N$ is *perfect* if $\sigma(N) = 2N$, where $\sigma$ is the positive divisor sum function. It is not known whether odd perfect numbers exist. In an earlier paper [1], 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 $q^k \mid N$, 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 computed 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 [1], 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 results required the factorisation of the 81-decimal-digit composite number $\sigma(13^{12})$; this factorisation has been completed and the result given in a postscript to [1]. 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 $10^{300}$.

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

A preliminary version of the present work is contained in [2]. There, the lower bound $10^{200}$ was obtained.

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

$$E_\alpha(q, k) = \{ p^\beta \mid p \text{ odd prime}, \beta \geq 2, \beta \text{ even or } \beta \equiv 1 \pmod{4},$$

$$(\exists j)(0 < j \leq k, p^\beta / f_\alpha(p) < q^{2j} \text{ and } q^j \mid \sigma(p^\beta)) \}$$

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 $q^j \mid \sigma(p^\beta)$.)

Write $\epsilon$ for $\epsilon_0$. 

We can compute $\epsilon_\alpha(q, k)$ in time polynomial in $q$ and $k$ by an efficient "lifting" algorithm, described in Hardy and Wright [5, Theorem 123]. Usually, $\epsilon(q, k)$ 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 [4]).

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

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

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

3
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 \( p | \sigma(q^k) \) and \( q^m | p + 1 \), then \( k \geq 3m \).

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

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

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

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

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 \( \lambda = 2ab - q^{k+1-m} \), 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 \( q^{k+1} \geq 2q^{3m} + 2q^m - q^{2m} > q^{5m} \). 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 the form \( \{ p_i^{\beta_i} \mid p_i \) distinct odd primes, \( \beta_i \geq 2 \), \( \beta_i \) even or \( \beta_i \equiv 1 \pmod{4} \} \). If \( q^{k_i} | \sigma(p_i^{\beta_i}) \) for each \( i \) and \( k \geq \sum k_i \), then

\[
\prod_{\beta_i \in S} \frac{\sigma(p_i^{\beta_i})}{\phi(p_i)} > q^{2\sum_{i} k_i - \epsilon_{q,k}}.
\]

4
Proof. We have quite generally that
\[
\frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} = \frac{p_i^{\beta_i}}{f_\alpha(p_i)} = q^{2k_i-\log_q(p_i^{\beta_i}/f_\alpha(p_i))} = q^{2k_i-\log_q(q^{2k_i}f_\alpha(p_i)/p_i^{\beta_i})},
\]
while if \(p_i^{\beta_i} \in S \setminus E_\alpha(q,k)\), then \(f_i^{\beta_i}/f_\alpha(p_i) \geq q^{2k_i}\). Thus, where \(E_\alpha = E_\alpha(q,k)\),
\[
\log_q \prod_{p_i^{\beta_i} \in S \setminus E_\alpha} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} > 2 \sum k_i - \sum_{p_i^{\beta_i} \in S \setminus E_\alpha} \log_q(q^{2k_i}f_\alpha(p_i)/p_i^{\beta_i}) \\
\geq 2 \sum k_i - \sum_{p_i^{\beta_i} \in E_\alpha} \log_q(q^{2k_i}f_\alpha(p_i)/p_i^{\beta_i}) \\
\geq 2 \sum k_i - \epsilon_\alpha(q,k),
\]
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
\[
N > \frac{1}{2}q^{2k-\epsilon_\alpha(q,k)} \prod_{i=1}^{j} f_\alpha(p_i).
\]

(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
\[
2N = \sigma(N) = \sigma(q^k) \prod_{i=1}^{j} \frac{\sigma(p_i^{\beta_i})}{f_\alpha(p_i)} \prod_{i=1}^{j} f_\alpha(p_i) \\
> q^k \cdot q^{2k-\epsilon_\alpha(q,k)} \prod_{i=1}^{j} f_\alpha(p_i).
\]

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

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

**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

\[
N^2 > 2Bq^{5k - \epsilon_0(q,k)} \prod_{i=2}^j f_\alpha(p_i).
\]

**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

\[
N \geq q^k \sigma(q^k) p_1 p_2 \\
\geq q^k \cdot q^k(1 + q^{-1}) \cdot 2q^k(1 - \frac{1}{q}q^{-k_1}) \cdot B \\
> 2Bq^{2k+k}.
\]

From Lemma 3(ii), we also have \( N > q^{3k-k_1 - \epsilon_0(q,k)} \prod_{i=2}^j f_\alpha(p_i) \). Hence

\[
N^2 > 2Bq^{5k - \epsilon_0(q,k)} \prod_{i=2}^j f_\alpha(p_i),
\]

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 \( B \geq \frac{1}{2}q^{(q,k)} \).

**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

\[
2N = \sigma(N) = \sigma(M) \sigma\left(\frac{N}{M}\right) = \sigma(M) \sigma(q^k) \prod_{i=1}^j \sigma(p_i^{\beta_i}) \\
> M \cdot q^k \cdot q^{2k - \epsilon(q,k)} = Mq^{3k - \epsilon(q,k)}.
\]
If $\beta_1 = 1$, then apply Lemma 2 with $S$ equal to the set of components of $N/M q^k p_1$. Then $\sum k_i = k - k_1$ and 

$$2N = \sigma(M)\sigma(q^k)\sigma(p_1) \prod_{i=2}^{j} \sigma(p_i^\beta)$$

$$> M^2 q^k \cdot 2q^{k_1} \cdot q^{2(k-k_1)-\epsilon(q,k)} = 2Mq^{3k-k_1-\epsilon(q,k)}.$$

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 $p \geq 3$ and $p^\beta < 2^\alpha q^{2k}$, we have $\beta < \alpha + 2k \log_2 q$. Thus, to establish the polynomial-time result, it is sufficient to suppose that $\beta$ is fixed.

Define $F(x) = 1 + x + x^2 + \cdots + x^\beta$. We can enumerate the set $S_\beta$ of solutions modulo $q^\beta$ of $F(x) = 0$ by the "lifting" algorithm described in [5, §8.3]. If $\beta = 1$, we can simply check all possible solutions $1, 2, \ldots, q - 1$ (although faster methods, using a primitive root (mod $q$), are preferable if $q$ is large). If $\beta > 1$, we apply Theorem 123 of [5] to obtain $S_\beta$ from $S_{\beta-1}$, using what is essentially an application of Newton's method. Since $F(x)$ is a polynomial of degree $\beta$, the number $|S_\beta|$ of solutions is bounded by $\beta$.

Define $T_\beta = \{ s + \lambda q^j \mid s \in S_\beta, \lambda \geq 0, (s + \lambda q^j)^\beta < f_\alpha(s + \lambda q^j)q^{2j} \}$. Clearly, $|T_\beta| \leq 2^{\alpha/\beta}|S_\beta|$. Since $p^\beta \in E_\alpha(q,k)$, there is some $j, 0 < j \leq k$, such that $q^j \| \sigma(p^\beta)$ and $p^\beta < f_\alpha(p)q^{2j}$. Thus, to enumerate such $p^\beta$, we need only check the elements of $T_1, T_2, \ldots, T_k$ 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 $\sum \log_q(q^{2j}f_\alpha(p)/p^\beta)$.

**Example.** To illustrate the algorithm, consider the computation of $\epsilon(3159,36)$. If $\beta = 2$, $F(x) = 1 + x + x^2$, so $S_1 = \{97, 3071\}$ is the set of solutions of $F(x) = 0$ (mod 3169). We construct the sets $S_2, S_3, \ldots, S_{36}$ as in [5, §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 $T_1, T_2, \ldots, T_{36}$ rules out all but three possible odd prime $p$ such that $3169^j \| \sigma(p^2)$:

- $j = 1$, $p = 97$;
- $j = 3$, $p = 9875516237$; and
- $j = 11$, $p = 2666023998360549086712579594816998201$. 


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 \( \beta \geq 4 \), 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 \( \beta \geq 4 \).) We conclude that only the three pairs given above can contribute to \( \epsilon(3169, 36) \), so \( \epsilon(3169, 36) \leq 1.3325 \).

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

<table>
<thead>
<tr>
<th>( \alpha )</th>
<th>( q )</th>
<th>( k )</th>
<th>( j )</th>
<th>( \beta )</th>
<th>( \log_q(q^{2j}f_\alpha(p)/p^\beta) )</th>
<th>( p ) (see below)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>172</td>
<td>8</td>
<td>2</td>
<td>0.5495 \ldots</td>
<td>3376853</td>
</tr>
<tr>
<td>0</td>
<td>19</td>
<td>2</td>
<td>0.0607 \ldots</td>
<td>1074458209246617</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>2</td>
<td>0.3689 \ldots</td>
<td>936579478224094047977</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>2</td>
<td>1.7035 \ldots</td>
<td>6778 \ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>2</td>
<td>1.0771 \ldots</td>
<td>1292 \ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>150</td>
<td>2</td>
<td>0.3795 \ldots</td>
<td>4020 \ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>3221</td>
<td>42</td>
<td>1</td>
<td>4</td>
<td>0.8125 \ldots</td>
<td>11</td>
</tr>
<tr>
<td>0</td>
<td>612067</td>
<td>22</td>
<td>1</td>
<td>2</td>
<td>0.3398 \ldots</td>
<td>63601</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>0.2253 \ldots</td>
<td>5291 \ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>3169</td>
<td>36</td>
<td>1</td>
<td>2</td>
<td>0.8650 \ldots</td>
<td>97</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0.4191 \ldots</td>
<td>5875516237</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>0.0481 \ldots</td>
<td>2666 \ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>221</td>
<td>3</td>
<td>249</td>
<td>1</td>
<td>2</td>
<td>0.9380 \ldots</td>
<td>37</td>
</tr>
</tbody>
</table>

Large primes \( p \) occurring above

677822686658425215407071060694728215733634249273881
1292705670586158487568763039916765694399830534390031
9630427099162956962804028786608263511417448696587
4020563766827570048511998229655093775323634764366342516228059494
717524577495475739650336310509313359098137765181615640612833
52915283185303600217046163660933353195087333134
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 [1]. 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 [1], 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. 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 $\epsilon(3221, 42) = \log_{3221}(3221^{2}/11^{4}) = 0.8125\ldots$ (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, $\sigma(7^{172}) = c_{146}$, $\epsilon(7, 172) = 4.1398\ldots$. By Theorem 2,

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

(iii) Line 7985, $\sigma(612067^{22}) = c_{128}$, $\epsilon(612067, 22) = 0.5651\ldots$. By Theorem 2,

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

(iv) Line 8866, $\sigma(3169^{34}) = c_{27}$, $\epsilon(3169, 36) = 1.3323\ldots$. By Theorem 2,

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

<table>
<thead>
<tr>
<th>Figure 1. $\sigma(467^{46})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4340: $7^{2} \Rightarrow 19\ldots$, D</td>
</tr>
<tr>
<td>4341: $7^{4} \Rightarrow 2801$, B1 6</td>
</tr>
<tr>
<td>4342: $2801^{1} \Rightarrow 3 \cdot 467$, B1 13</td>
</tr>
<tr>
<td>4343: $467^{2} \Rightarrow 19\ldots$, D</td>
</tr>
<tr>
<td>(some lines omitted)</td>
</tr>
<tr>
<td>4479: $467^{46} \Rightarrow c_{123}$, case (v)</td>
</tr>
</tbody>
</table>

(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 $\epsilon(467, 46) = 0$,

$$N > 467^{137} > 10^{365}.$$
(vi) Line 9527, $\sigma(191^{46}) = c_{105}$. See Figure 2. Lemma 3, with $\alpha = 0$, $p_1 = 30941$, $k_1 = 1$ and $\varepsilon(191, 46) = 0$, 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 $M = 3^{22} \geq 3^{18}$, $p_1 = 363889$, $k_1 = 1$ and $\varepsilon(36389, 22) = 0$. (Since 3 is a primitive root $\pmod{36389}$ and $\beta_2$ is even, we know that $36389 \nmid \sigma(3^{22})$.) Then

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

(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

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

10
with \( q = 191, k = 42 \). For any prime \( p \), we set

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

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

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

After some experimentation, we find that with \( \alpha = 50 \) we have \( \epsilon_{90}(191, 42) = 0 \) and

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

(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),

\[
N > 3^{726 - k_1} > 10^{300}
\]

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

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

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 \( \epsilon_{221}(3, 240) = 0.9380 \ldots \). (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 obtainable from the first author.

We should mention that the size of the task precluded us from being as fastidious as we were in [1]. 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 [1] 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 $\epsilon_4$, 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 [1] contained the output for that proof. With the present paper, 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 [3] and should prove similarly useful.

Acknowledgements. 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 [3]. Moreover, some were obtained using a Cyber 205 and a NEC SX/2, the CPU-time on these computers being provided by the Dutch Working Group on the Use of Supercomputers.


3. 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

