A NEW APPROACH TO LOWER BOUNDS FOR ODD PERFECT NUMBERS

By 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, we are able to extend the computations in an earlier paper to show that $N > 10^{200}$.

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 or not there exist odd perfect numbers. 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 discussed in [1], 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 $N > q^k\sigma(q^k) > q^{2k}$. Since the previous methods require the explicit factorisations of $\sigma(q^k)$ for increasingly large values of k, this gives a practical limit to their effectiveness. 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 $N > q^{5k/2}$.

We are thus enabled to prove

THEOREM 1. *There is no odd perfect number less than* 10^{200}.

The proof 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 prove Theorem 1 required the factorisation of the 81-digit composite number $\sigma(13^{72})$; but $13^{180} > 10^{200}$, so our new result allows this factorisation to be avoided. Apart from this and one other instance, the original algorithm, with the "q^{2k}" result, was sufficient for our purposes.

All letters in this paper, except E, S and ϵ, denote nonnegative integers.

To describe the new method, we need the

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

$$E(q,k) = \{\, p^\beta \mid p \text{ odd prime},\ \beta \geq 2,\ \beta \text{ even or } \beta \equiv p \equiv 1 \pmod 4,\\ (\exists j)(0 < j \leq k,\ p^\beta < q^{2j} \text{ and } q^j \parallel \sigma(p^\beta)) \,\}$$

and

$$\epsilon(q,k) = \sum_{p^\beta \in E(q,k)} \log_q(q^{2j}/p^\beta).$$

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

We can compute $\epsilon(q,k)$ in time polynomial in q and k by an efficient "lifting" algorithm, described in Hardy and Wright [2, Theorem 123]. Usually, $\epsilon(q,k)$ is quite small; numerical results will be given later.

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 $k \equiv \beta_2 \equiv \cdots \equiv \beta_j \equiv 0 \pmod 2$.

Our new result is

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 $N > q^{5k/2}$.*

2. Proof of Theorem 2. The proof depends on a number of Lemmas.

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 $p+1 = 2\alpha q^m$ for some $\alpha > 0$. Then, since $p \mid \sigma(q^k) = (q^{k+1}-1)/(q-1)$,

$$q^{k+1} - 1 = (2\alpha q^m - 1)R$$

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

Thus

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

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

We also have

$$q^{k+1-m} = 2\alpha\beta q^m + 2\alpha - \beta,$$

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

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

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

From (1), if $2\alpha > q^m$, 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 $\beta \geq q^m$, 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.

LEMMA 2. *Let q be an odd prime and let $S = \{ p_i^{\beta_i} \mid p_i$ distinct odd primes, $\beta_i \geq 2$, β_i even or $\beta_i \equiv p_i \equiv 1 \pmod 4 \}$. If $q^{k_i} \parallel \sigma(p_i^{\beta_i})$ for each i and $k \geq \sum k_i$, then*

$$\prod_{p_i^{\beta_i} \in S} \sigma(p_i^{\beta_i}) > q^{2\sum k_i - \epsilon(q,k)}.$$

Proof. We have quite generally that

$$\begin{aligned} \sigma(p_i^{\beta_i}) > p_i^{\beta_i} &= q^{2k_i - (2k_i - \log_q p_i^{\beta_i})} \\ &= q^{2k_i - \log_q (q^{2k_i}/p_i^{\beta_i})}, \end{aligned}$$

while if $p_i^{\beta_i} \in S \backslash E(q,k)$, then $p_i^{\beta_i} > q^{2k_i}$. Thus, where $E = E(q,k)$,

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

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 above. Then $N > q^{8k/3 - \epsilon(q,k)}$, provided either*

(i) *$\beta_1 > 1$, or*

(ii) *$\beta_1 = 1$ and $p_1 \mid \sigma(q^k)$.*

Proof. (i) We shall apply Lemma 2 with S equal to the set of maximal prime power divisors of N, other than q^k. Then, in Lemma 2, $\sum k_i = k$ and

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

Since $k \geq 2$ and $q \geq 3$, we have $q^{k/3} > 2$, and the result follows.

(ii) We again apply Lemma 2, this time with S equal to the set of maximal prime power divisors of N, other than q^k and p_1. Suppose $q^{k_1} \parallel p_1 + 1$. Then, in Lemma 2, $\sum k_i = k - k_1$. Also, $p_1 + 1 \geq 2q^{k_1}$. Thus,

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

But, from Lemma 1, $k \geq 3k_1$ so the result follows since $3k - k_1 \geq 3k - k/3 = 8k/3$.

LEMMA 4. *Let N, q^k and p_1 be as above. Suppose $q^{k_1} \parallel p_1 + 1$ and that $\sigma(q^k)$ is not a perfect square and is not divisible by p_1 or any prime number less than B. Then*

$$N > \sqrt{2Bq^{5k-\epsilon(q,k)}}.$$

Proof. Suppose $k_1 > 0$. 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

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

This result is true also if $k_1 = 0$. From the first part of the proof of Lemma 3(ii), we also have $N > q^{3k-k_1-\epsilon(q,k)}$. Hence

$$N^2 > 2Bq^{5k-\epsilon(q,k)},$$

as required.

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