MATHEMATICS OF COMPUTATION
Volume 76, Number 260, October 2007, Pages 2109–2126
S 0025-5718(07)01990-4
Article electronically published on May 9, 2007

ODD PERFECT NUMBERS HAVE AT LEAST NINE DISTINCT PRIME FACTORS

PACE P. NIELSEN

ABSTRACT. An odd perfect number, N, is shown to have at least nine distinct prime factors. If $3 \nmid N$ then N must have at least twelve distinct prime divisors. The proof ultimately avoids previous computational results for odd perfect numbers.

1. INTRODUCTION

A perfect number is one where $\sigma(N) = 2N$. In other words, the sum of the divisors of N is twice N. These numbers have been studied since antiquity. A number N is an even perfect number if and only if $N = (2^p - 1)2^{p-1}$ with $2^p - 1$ prime. Sufficiency was proven by Euclid and necessity by Euler. A prime number of the form $2^p - 1$ is called a Mersenne prime, and there are currently 44 that have been found. There is an ongoing, online, distributed search for such primes at `http://www.mersenne.org`.

The search for odd perfect numbers has not been as successful. None have been found, making their existence the oldest unanswered question in mathematics. However, there are a great number of necessary conditions for their existence, which go through periodic improvements. The list of conditions given here is the same list as in [25], but with recent improvements included.

Let N be an odd perfect number (if such exists). Write $N = \prod_{i=1}^{k} p_i^{a_i}$ where each p_i is prime, $p_1 < p_2 < \ldots < p_k$, and $k = \omega(N)$ is the number of distinct prime factors. The factors $p_i^{a_i}$ are called the *prime components* of N. Then:

- *Eulerian Form:* We have $N = \pi^{\alpha} m^2$ for some integers $\pi, \alpha, m \in \mathbb{Z}_+$, with $\pi \equiv \alpha \equiv 1 \pmod 4$ and π prime. The prime π is called the *special* prime of N.
- *Lower Bound:* Brent, Cohen, and te Riele [3] using a computer search found that $N > 10^{300}$. William Lipp, using the same techniques, is close to pushing the bound to $N > 10^{500}$, and plans to start a distributed search at the website `http://www.oddperfect.org`.
- *Upper Bound:* Dickson [7] proved that there are finitely many odd perfect numbers with a fixed number of distinct prime factors. Pomerance [24] gave an effective bound in terms of k. This was improved in succession by Heath-Brown [12], Cook [6], and finally Nielsen [22] to $N < 2^{4^k}$.

Received by the editor April 1, 2006 and, in revised form, September 1, 2006.
2000 *Mathematics Subject Classification.* Primary 11N25; Secondary 11Y50.
Key words and phrases. Abundant, deficient, odd perfect.

©2007 American Mathematical Society
Reverts to public domain 28 years from publication

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

- *Large Factors:* Jenkins [15] proved that $p_k > 10^7$, and Iannucci [13], [14] proved $p_{k-1} > 10^4$ and $p_{k-2} > 10^2$. (T. Goto and Y. Ohno recently announced they have a proof that $p_k > 10^8$.)
- *Small Factors:* The smallest prime factor satisfies $p_1 < \frac{2}{3}k + 2$ as proved by Grün [8]. For $2 \leqslant i \leqslant 6$, Kishore [17] showed that $p_i < 2^{2^{i-1}}(k - i + 1)$, and this has been slightly improved by Cohen and Sorli [5].
- *Number of Total Prime Factors:* Hare [11] proved that the total number of (not necessarily distinct) prime factors of N must be at least 47. In unpublished work he has improved this to 75.
- *Number of Distinct Prime Factors:* Chein [4] and Hagis [9] independently proved that $\omega(N) \geqslant 8$. Hagis [10] and Kishore [18] showed that if $3 \nmid N$, then $\omega(N) \geqslant 11$. This paper improves both of these bounds by 1.
- *The Exponents:* For the non-special primes, p_i, write $a_i = 2b_i$. If $d = \gcd(2b_i + 1)$, then $d \not\equiv 0 \pmod 3$ by a result of McDaniel [19].

With such a number of conditions, it might seem that an odd perfect number could not exist. Pomerance has given an interesting heuristic, available at Lipp's website, suggesting that odd perfect numbers are very unlikely.

Much of the terminology, notation, and lemmas of the early sections of this paper match those found in [25] (which in turn match those in [13], and earlier work like [23]) in an effort to establish a sense of both continuity and improvement. I would like to thank John Voight for some interesting conversations on topics related to his paper. I would also like to thank William Lipp for providing some of the factorizations given in the lemmas. Finally, I thank the referee for useful comments and suggestions concerning the presentation of this material.

2. Fixed notations, conventions, and the algorithm

Let N be an odd perfect number and $k = \omega(N)$. We will write π for the special prime. By $\mathbb{N}$ we mean the non-negative integers and by $\mathbb{Z}_+$ the positive integers. The subscripts on the prime divisors p_i of N will no longer have any relationship to their relative sizes, unless explicitly assumed otherwise. We will use a computer run algorithm to prove our results. The main idea of the algorithm is to use a factor chain argument, as given in both [5] and [25]. For the benefit of the reader, we will describe the algorithm here. Basically, we consider every possible combination of k distinct prime divisors of an odd perfect number, and finds contradictions in each case.

We start by needing a prime divisor of N. In Section 6 we develop machinery (Lemmas 19 and 20) which can yield a lower and upper bound on a prime divisor of N. In our case we find $2 < p_1 < k + 2$. (Alternately, we could have used Grün's result which was quoted above, but this leads to only trivial improvements on the algorithm. We will instead rely on as few previous results as possible.)

So for example, if $k = 4$, then $p = 3$ or 5. By considering the Eulerian form, we see that the cases

$$3^2||N, 3^4||N, 3^6||N, 3^8||N, \ldots, 5^1||N, 5^2||N, 5^4||N, 5^5||N, \ldots$$

are the only ones possible. There is a benefit and cost to considering each of these cases individually. The cost is that there are an infinite number of cases, and hence we simply cannot consider them all. The benefit is that in each individual case we do not have to rely on the results of Section 6 to find bounds on p_2. For example,

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

in the case $3^2||N$, since $13 = \sigma(3^2)|2N$, we find that $13|N$, and so we can take $p_2 = 13$. (Note that the subscript does not mean that 13 is the second smallest prime divisor of N. Only that 13 is the second prime divisor we found for N in this case.)

As a matter of terminology, we think of each of the cases

$$3^2||N, 3^4||N, 3^6||N, 3^8||N, \ldots, 5^1||N, 5^2||N, 5^4||N, 5^5||N, \ldots$$

as branches on a tree, with each branch providing new factors for our algorithm and hence branching further. As the tree branches out, we eventually arrive at cases which are contradictory in some way. However, we still have to deal with the fact that there are an infinite number of branches. To get around this problem, we combine all the branches with large powers of primes into one composite branch. In other words, if p is a prime divisor of N, we combine all the cases $p^n||N$, for large n, together into one case. More precisely, we let B be a large integer (which will be around the size 10^{50}) which we fix at the beginning of the algorithm, and then we combine all the branches p^n together, for all $n \geqslant n_0$, where n_0 is minimal so that $p^{n_0} > B$. On this combined branch we are not assuming $p^n||N$ for any specific n, but rather we just assume $p^a|N$ for some $a \geqslant n_0$. In this way, we deal with all the remaining cases at once. As a matter of notation we label this conglomerated branch by p^∞.

For example, if we take $k = 4$ and $B = 50$, then we have five initial branches

$$3^2, 3^\infty, 5^1, 5^2, 5^\infty.$$

The first case $3^2||N$ branches further into two sub-branches $13^1, 13^\infty$, and we can continue this branching process. When we are on a branch with p^∞ we say p is an *infinite prime* (not to be confused with the infinite primes of algebraic number theory). Notice that infinite primes do not provide more factors for the factor chain, since we don't have $\sigma(p^n)|2N$ for any specific n, so we have to rely on the intervals of Section 6 to find bounds for the next prime. If we set B too low, then the primes on our branches become infinite too quickly, and we may have the case that the intervals of Section 6 are very large, or even that there is no upper bound for the next prime! (This corresponds to the case when $\Delta_0 > 2$ in Lemma 20.) If we make B large enough, the intervals will always have upper bounds (for a proof see [5]), and the algorithm will only have to consider a finite number of cases.

At each stage in the algorithm there will be prime divisors of N that are *known* and some that are *unknown*, meaning that the prime divisors are either specified by the algorithm or they are not, respectively. This set of known primes will change at every stage of the algorithm as it runs through different cases, and so the known and unknown primes are constantly changing. We let k_1 be the number of known, distinct prime divisors of N (at any given stage), and let $k_2 = k - k_1$ be the number of unknown, distinct prime divisors. Among the known prime divisors of N, some of the prime *components* are also known (again, *known* being a technical term meaning *specified by the algorithm*). In other words, if p is a known prime divisor of N and if our algorithm yields some $n \in \mathbb{Z}_+$ so that $p^n||N$, we say p^n is a known prime component. We let ℓ_1 be the number of known prime components of N, and let $\ell_2 = k - \ell_1$ be the number of unknown prime components.

A word of warning: In some theorems we will assume p is a prime with $p^n||N$, but this doesn't even mean that p is a known prime, let alone that the prime component is known. This is because, while p^n is, by hypothesis, a component of

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

N, the prime p and the number n might not have been specified by the algorithm. Throughout, we will only use the phrases "known prime" and "known component" to mean known to us *through our algorithm*, rather than by hypothesis.

More formally, the known components are those prime components which occur on the branch we are on, which are not infinite. The known primes are the primes we have branched upon, along with the primes coming from σ of the known components. For example, if we are on the branch $3^\infty 5^4$, then the known primes are $3, 5, 11, 71$ (the primes 11 and 71 come from $\sigma(5^4)|2N$), and the only known component is 5^4. In this case we say that 3 and 5 are *on* while 11 and 71 are *off*. In other words, the *on* primes are exactly the known primes for which we have started the branching process. Note that $k_1 - \ell_1$ is exactly the number of (known) primes which are infinite or off. In this example, since 11 is the smallest off prime we continue the branching process first on this prime, rather than 71. When there are no off primes we use the interval bounds of Section 6 to arrive at more primes, as explained earlier. Whenever we reach a contradiction, we go to the next available branch.

To clarify the previous exposition, we do the case when $k = 4$, $B = 50$. The following is the entire output, which is explained after the printout.

```
3^2 => 13^1
   13^1 => 2^1 7^1  N: 9 < p_3 < 11
   13^∞ : 3 < p_3 < 9
      5^1 => 2^1 3^1 : 15 < p_4 < 17  F
      5^2 => 31^1  A
      5^∞ : 42 < p_4 < 46  SF1: 42 < p_4 < 46
      7^2 => 3^1 19^1  D
      7^∞ : 10 < p_4 < 12
         11^∞  A
3^∞ : 3 < p_2 < 11
   5^1 => 2^1 3^1 : 8 < p_3 < 13  F
   5^2 => 31^1  SF1: 22 < p_4 < 26
   5^∞ : 14 < p_3 < 17  N: 14 < p_3 < 17
   7^2 => 3^1 19^1  N: 11 < p_3 < 13
   7^∞ : 7 < p_3 < 16
      11^∞ : 22 < p_4 < 27  SF1: 22 < p_4 < 27
      13^1 => 2^1 7^1 : 15 < p_4 < 18
         17^∞  F
      13^∞ : 16 < p_4 < 20
         17^1 => 2^1 3^2  F
         17^∞  A
         19^∞  No contradiction.  The number B is too small.
```

We start with the case $3^2||N$. Since $13 = \sigma(3^2)|N$, we go to the sub-branch (represented by the indentation on the second line) with $13||N$. On this branch we could further branch off on the new prime 7 coming from $\sigma(13)$, but the letter `N` means that there are no primes in the interval given by the bounds of Section 6, which is a contradiction. So, we backtrack to the next possible branch, which is $3^2 13^\infty$. On this branch we have no off primes, and so we again use the interval bounds, and find $3 < p_3 < 9$, hence $p_3 = 5$ or 7. The next four cases are all contradictory, as represented by the different letters near the ends of the lines. All

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

of the different contradictions will be explained in Section 7. The rest of the output is self-explanatory except the very last branch $3^\infty 7^\infty 13^\infty 19^\infty$, which doesn't yield a contradiction. Thus the algorithm terminates unsuccessfully because the bound B was chosen too small. One must increase B and rerun the program to successfully complete this case.

We close this section with a brief outline of the rest of the paper, so that the reader can understand how the results interrelate, and which results are new and which are standard. Section 3 discusses congruence relations that arise naturally when considering perfect numbers. All of that section's material is standard knowledge. Sections 4 and 5 use the congruence relations of Section 3 to prove that if certain primes become infinite, then N must have one or two large prime factors. The first half of Section 4 follows the paper [25], and Proposition 7 is an improvement on [25, Proposition 3.1]. The second half of Section 4 and all of Section 5 are new, including Propositions 10, 14, and 17. In Section 6 we develop lower and upper bounds, given in Lemmas 19 and 20, respectively, on the next unknown prime of N. These bounds are standard, except we modify the upper bound (Lemma 20) to take into account the possible large divisors of N that arise due to the results of Sections 4 and 5. In the last three sections we discuss our actual implementation, including a list of the contradictions used, the results obtained, and possible future improvements. It is important to keep in mind that the contradictions are of secondary importance; it is the strength of the interval bounds of Section 6, in conjunction with the large factors we find in Sections 4 and 5, that make the results of this paper obtainable.

3. Cyclotomic integers

The equation $\sigma(N) = 2N$ can be (trivially) rewritten as $\sigma(N)/N = 2$ which tells us that each odd prime divisor of $\sigma(N)$ must somehow divide N, and vice versa. Thus, we want to study the prime factorization of

$$\sigma(N) = \prod_{i=1}^{k} \sigma(p_i^{a_i}) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Letting $\Phi_n(x)$ be the nth cyclotomic polynomial (i.e. the minimal polynomial over $\mathbb{Q}$ for a primitive nth root of unity), we have the partial factorization

$$p^n - 1 = \prod_{d|n} \Phi_d(p)$$

and so

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} = \prod_{d|(a+1),\, d>1} \Phi_d(p). \tag{1}$$

We are further interested in the factorization of $\Phi_d(p)$. If c and d are integers with $d > 1$ and $\gcd(c, d) = 1$ we write $o_d(c)$ for the multiplicative order of c modulo d. If p is prime, we write v_p for the valuation associated to p. In other words, for $n \in \mathbb{Z}_+$ we have $p^{v_p(n)} || n$. The following results of Nagell [21] are fundamental and are often left as exercises in modern abstract algebra books.

Lemma 1 ([25, Lemma 2.3])**.** *Let $m > 1$ be an integer, and let q be prime. Write $m = q^b n$ with $\gcd(q, n) = 1$.*

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

If $b = 0$, then

$$\Phi_m(x) \equiv 0 \pmod{q}$$

is solvable if and only if $q \equiv 1 \pmod{m}$. The solutions are those x with $o_q(x) = m$. Furthermore, $v_q(\Phi_m(x)) = v_q(x^m - 1)$ for such solutions.

If $b \neq 0$, then

$$\Phi_m(x) \equiv 0 \pmod{q}$$

is solvable if and only if $q \equiv 1 \pmod{n}$. The solutions are those x with $o_q(x) = n$. Furthermore, if $m > 2$, then $v_q(\Phi_m(x)) = 1$ for such solutions.

As a result of Lemma 1 and Equation (1) we get the following lemma (for a proof see [25, Lemma 2.4]):

Lemma 2. *Let p and q be primes, $q \geqslant 3$, and $a \in \mathbb{Z}_+$. Then*

$$v_q(\sigma(p^a)) = \begin{cases} v_q(p^{o_q(p)} - 1) + v_q(a+1) & \text{if } o_q(p) | (a+1) \text{ and } o_q(p) \neq 1, \\ v_q(a+1) & \text{if } o_q(p) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In our work we will want a prime divisor q of $\Phi_d(p)$ with $o_q(p) = d$. In other words, we want to reduce to the first case of Lemma 1 (when $b = 0$). To make sure we can always reduce to that case, we need the following result, usually attributed to Bang [1], but given other proofs such as in [2].

Lemma 3. *Let $m, x \in \mathbb{Z}_+$ with $x \geqslant 2$. Then $\Phi_m(x)$ is divisible by a prime q with $o_q(x) = m$, except if $x = 2$ and $m = 1$ or 6, or if $x = 2^i - 1$ (for some $i \in \mathbb{Z}_+$) and $m = 2$.*

Note that we are only interested in this lemma when $x = p$ is a prime dividing an odd perfect number N. Thus, the case $x = 2$ never happens. Also, if $m = 2$, this corresponds to the case that x is the special prime (in the Eulerian form), so $x = \pi \equiv 1 \pmod{4}$ and hence cannot be of the form $2^i - 1$. Thus, both exceptions in the lemma do not affect our work.

Define $\sigma_i(n) = \sum_{d|n} d^i$, for $i \in \mathbb{Z}$ and $n \in \mathbb{Z}_+$. It is clear that each of these functions is multiplicative, $\sigma_1 = \sigma$ is the usual sum of divisors function, and σ_0 is the number of divisors function. The following is immediate:

Lemma 4. *Let N be an odd perfect number. If $p^a || N$, where p is prime, then for each $d|(a+1)$ the number $\Phi_d(p)$ is divisible by a prime q with $o_q(p) = d$ and $q \equiv 1 \pmod{d}$. In particular, $\sigma(p^a)$ has at least $\sigma_0(a+1) - 1$ distinct prime factors in common with N.*

Note that if $q|\Phi_d(p)$ and $o_q(p) = d$, then the relation $q \equiv 1 \pmod{d}$ holds necessarily, from Lemma 2.

4. Fermat primes

A prime q is called a *Fermat prime* if it is of the form $q = 2^j + 1$ for some $j \in \mathbb{Z}_+$. One can show it is necessary that $j = 2^i$ for some $i \in \mathbb{N}$. It is easily seen that if $i = 0, 1, 2, 3, 4$, then $2^{2^i} + 1$ is prime (i.e. $q = 3, 5, 17, 257, 65537$). No other Fermat primes have been found. These primes play a special role in the study of odd perfect numbers. This is because the prime factorization of $q - 1$ is exactly a power of 2.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

The first thing we can do is restate Lemma 2 in terms of divisors of N, and Fermat primes.

Lemma 5 ([23], [25, Lemma 2.5]). *Let N be an odd perfect number, $p^a||N$ with p prime, and let q be a Fermat prime. Then:*

$$v_q(\sigma(p^a)) = \begin{cases} v_q(p+1) + v_q(a+1) & \text{if } \pi = p \equiv -1 \pmod{q}, \\ v_q(a+1) & \text{if } p \equiv 1 \pmod{q}, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5 tells us that there are only a few sources in $\sigma(N)$ for copies of q, either the special prime or primes which are congruent to 1 modulo the Fermat prime. In particular, if $q^n|N$ for some large n, we can force the size of the special prime to be large. To prove this we first need another lemma.

Lemma 6 (cf. [25, Proposition 2.8]). *Let N be an odd perfect number, let q be a Fermat prime, and suppose $p^a||N$ with p prime.*

(i) *If $p \neq \pi$ and $q^b|\sigma(p^a)$, then $\sigma(p^a)$ is divisible by b distinct primes $r_1, r_2, \ldots, r_b$ with $r_i \equiv 1 \pmod{q^i}$.*

(ii) *If $p = \pi$, $p \equiv -1 \pmod{q}$, and $q^c|(a+1)$, then $\sigma(p^a)$ is divisible by $2c$ distinct primes $r_1, r_1', \ldots, r_c, r_c'$ with $r_i \equiv r_i' \equiv 1 \pmod{q^i}$.*

Proof. For part (i), by Lemma 5 (which we can use since q is Fermat) we have $q^b|(a+1)$. So we take r_i to be the divisor of $\Phi_{q^i}(p)$ specified by Lemma 4. Part (ii) follows from the same lemmas, noticing that since $p = \pi$ is special we have $2|(a+1)$, and hence we can take r_i and r_i' to be the factors specified by Lemma 4 of $\Phi_{q^i}(p)$ and $\Phi_{2q^i}(p)$, respectively. □

Proposition 7 (cf. [25, Proposition 3.1]). *Let N be an odd perfect number, and let q be a Fermat prime with $q^n||N$. Suppose k, k_1, k_2, ℓ_1, and ℓ_2 have their usual meanings. Further suppose $q^b||\sigma(\text{known prime components of } N)$. Finally, let k_1' (respectively, ℓ_1') be the number of distinct prime factors, r, among the k_1 known prime divisors (respectively, among the ℓ_1 known prime components) for which we have $r \equiv 1 \pmod{q}$.*

If

$$\tau = n - b - (k_1' - \ell_1' + k_2)(k_1' + k_2 - 1) > 0,$$

then $\pi \equiv -1 \pmod{q}$ and π is among the unknown prime components. If, furthermore, each known prime, p, with unknown component and with $p \equiv 1 \pmod{4}$ satisfies $p \not\equiv -1 \pmod{q^{\tau - \lfloor (k_1'+k_2)/2 \rfloor}}$, then π is among the unknown primes, and

$$v_q(\pi + 1) \geqslant n - b - (k_1' - \ell_1' + k_2 - 1)(k_1' + k_2 - 2) - \lfloor (k_1' + k_2 - 1)/2 \rfloor = \tau'.$$

Proof. First, we will show the contrapositive of the initial statement. Suppose either π is among the known components or $\pi \not\equiv -1 \pmod{q}$. Let p^a be an unknown component of N. Lemma 5, combined with what we have just said, implies $v_q(\sigma(p^a)) = v_q(a+1)$ if $p \equiv 1 \pmod{q}$, and equals 0 otherwise. Using the equation $\sigma(N)/N = 2$, there are $n - b$ copies of q that must be accounted for by σ of the unknown components. Note that there are at most $k_1' + k_2$ distinct prime factors of N that are congruent to 1 $\pmod{q}$. Thus, by Lemma 6, at most $k_1' + k_2 - 1$ copies of q divide $a+1$ if $p \equiv 1 \pmod{q}$ (since p itself cannot divide $\sigma(p^a)$), otherwise we end up with too many distinct prime divisors of N which are congruent to 1 $\pmod{q}$. There are at most $k_1' - \ell_1' + k_2$ primes p with unknown component

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

satisfying $p \equiv 1 \pmod{q}$. Hence at most $(k_1' - \ell_1' + k_2)(k_1' + k_2 - 1)$ copies of q can be accounted for by σ of the unknown components. Therefore,

$$\tau = n - b - (k_1' - \ell_1' + k_2)(k_1' + k_2 - 1) \leqslant 0$$

or we will have left over copies of q not accounted for in $\sigma(N)$.

To get the last statement, now suppose $\tau > 0$, $\pi \equiv -1 \pmod{q}$, and π is among the unknown components. Lemma 5 tells us that the only place the extra τ copies of q can be accounted for is $v_q(\pi+1) + v_q(\alpha+1)$. But at most $\lfloor (k_1' + k_2)/2 \rfloor$ copies of q divide $\alpha+1$ by Lemma 6, part (ii). Hence $q^{\tau - \lfloor (k_1'+k_2)/2 \rfloor} | (\pi+1)$, and so $\pi \equiv -1 \pmod{q^{\tau - \lfloor (k_1'+k_2)/2 \rfloor}}$.

This means, if no known primes satisfy this congruence, that when we counted the maximum number of possible unknown prime divisors $\equiv 1 \pmod{q}$ we included one too many. Thus there are at most $k_1' + k_2 - 1$ primes dividing N that are congruent to $1 \pmod{q}$, and hence at most $(k_1' - \ell_1' + k_2 - 1)(k_1' + k_2 - 2)$ copies of q can be accounted for by σ of the unknown, non-special components. For the special component π^α, by Lemma 6, part (ii) we see that at most $(k_1' + k_2 - 1)/2$ copies of q can divide $\alpha + 1$, otherwise we once again obtain too many factors of N congruent to $1 \pmod{q}$. Since, in fact, an integer number of copies of q divide $\alpha + 1$, we can again take the floor function. Putting this all together, τ' copies of q must divide $\pi + 1$. □

Thus, if a large power of a Fermat prime divides N, we see that $\pi + 1$, and hence π, must be large. This isn't quite good enough to simplify our search to a manageable number of cases. We need a way to find another large prime divisor of N. The trick is to consider divisors of $\sigma(q^n)$. Suppose q is a Fermat prime, with $q^n || N$, and n very large. Then using the previous lemma, we can force π to be very large. One might wonder if $\pi | \sigma(q^n)$. The following result speaks to this issue.

Lemma 8 ([3, Lemma 1])**.** *If p and q are odd primes with $p | \sigma(q^k)$ and $q^m | (p+1)$, then $k \geqslant 3m$.*

So, using the terminology of Proposition 7, if $\tau > 0$, $q^{\tau - \lfloor (k_1'+k_2)/2 \rfloor} \nmid (p+1)$ for the known primes, and also $3\tau' > n$, then $\pi \nmid \sigma(q^n)$ by Lemma 8. But since n is big we would expect a large prime divisor of N which divides $\sigma(q^n)$. The following work clarifies how large a divisor we can find for $\sigma(q^n)$.

Lemma 9. *Let p be an odd prime and let $q = 3$ or 5. If $q^{p-1} \equiv 1 \pmod{p^2}$, then either $(q,p) = (3,11)$ or $q^{o_p(q)} - 1$ has a prime divisor greater than 10^{13}. If $q = 17$ and $q^{p-1} \equiv \pmod{p^2}$, then either $(q,p) = (17,3)$ or $q^{o_p(q)} - 1$ has a prime divisor greater than 10^{11}.*

Proof. The papers [20] and [16] give a list of (q,p) for which $q^{p-1} \equiv 1 \pmod{p^2}$ and $p < 10^{13}$ with $q = 3$ or 5 (or $p < 10^{11}$ with $q = 17$). In the cases $(q,p) \neq (3,11), (17,3)$ the following table gives the requisite factor of $q^{o_p(q)} - 1$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

q	p	Large factor of $q^{o_p(q)}-1$
3	1006003	154680726732318637
5	20771	625552508473588471
5	40487	625552508473588471
5	53471161	60081451169922001
5	1645333507	52082118058261
5	6692367337	8930008316757509
5	188748146801	40093613041379
17	46021	1365581260423071390161
17	48947	63895279579889

□

For use shortly, we make the following definition. Letting p and q be odd primes, with $p \neq q$, we set

$$o'_q(p) = \begin{cases} & \text{if } 2 \nmid o_q(p), \\ & \text{or } 4 \nmid o_q(p) \text{ and either} \\ o_q(p) & \quad \text{(i) } p = \pi \text{ and } \pi \text{ is among the known components,} \\ & \text{or} \\ & \quad \text{(ii) } p \equiv 1 \pmod 4 \text{ and } \pi \text{ is not among the} \\ & \qquad \text{known components,} \\ 0 & \text{otherwise.} \end{cases}$$

In other words, $o'_q(p)$ is the usual order function, unless it is impossible for both $p^a || N$ and $o_q(p) \mid (a+1)$ to hold, due to consideration of the Eulerian form.

Proposition 10. *Let N be an odd perfect number with k, k_1, and k_2 having their usual meanings. Suppose $q = 3$ or 5 is a known prime divisor of N, $q^n || N$, $q \neq \pi$ and $\pi \nmid \sigma(q^n)$. Suppose $p_1, \ldots, p_{k_1-1}$ are the other known prime factors of N, besides q. For each $i = 1, 2, \ldots, k_1 - 1$ define*

$$\epsilon_i = \begin{cases} 0 & \text{if } o'_{p_i}(q) = 0, \\ \max(s+t-1, 1) & \text{if } o'_{p_i}(q) \neq 0, \text{ where } s = v_{p_i}(\sigma(q^{o_{p_i}(q)-1})) \\ & \qquad \text{and } t \in \mathbb{Z}_+ \text{ is minimal so that } p_i^t > 100. \end{cases}$$

Set $V = \prod_{i=1}^{k_1-1} p_i^{\epsilon_i}$. Suppose π is among the k_2 unknown prime factors, and $k_2 > 1$. Finally, assume that all unknown prime factors are greater than 100.

If

$$\min\left(10^{13}, \left(\frac{\sigma(q^n)}{V}\right)^{\frac{1}{k_2-1}}, \left(\frac{\sigma(q^{100})}{V}\right)^{\frac{1}{k_2-1}}\right) > 1,$$

then $\sigma(q^n)$ has a prime divisor among the unknown primes at least as big as the above minimum. If $q = 17$ one can replace 10^{13} with 10^{11}, and then the result still holds.

Proof. We only do the case when $q = 3$, since the other cases are similar. First suppose $\sigma(q^n) = (q^{n+1}-1)/(q-1)$ is at most divisible by $p_i^{\epsilon_i}$ for the known primes, and square-free for the unknown primes. Then since $\pi, q \nmid \sigma(q^n)$, the

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

largest unknown prime divisor of $\sigma(q^n)$ is at least

$$\left(\frac{\sigma(q^n)}{V}\right)^{\frac{1}{k_2-1}},$$

unless this quantity is $\leqslant 1$ (in which case there might be no unknown factors).

So we may assume there is some prime $p|N$, $o'_p(q) \neq 0$, so that $\sigma(q^n)$ is divisible by p^2 if p is unknown, or $p^{\epsilon+1}$ if p is known (and ϵ is the corresponding ϵ_i), with p *maximal* among such primes. By Lemma 9 we may also assume that if $p^2|(q^{n+1}-1)$ and p is unknown, then $p|(n+1)$. (This is where 10^{13} comes into the minimum.)

Thus, in either case, $p^t|(n+1)$ where $p^t > 100$ (taking $t = 1$ if p is an unknown prime). Then we have

$$\sigma(q^{p^t-1})|\sigma(q^n).$$

Thus it suffices to find a large divisor of $(q^{p^t}-1)/(q-1)$. By Lemma 1, the quantity $(q^{p^t}-1)/(q-1)$ is only divisible by primes larger than p, or p itself to the first power. (In this case, q being Fermat means the quantity is not divisible by p, and we could replace $\max(s+t-1,1)$ by $s+t-1$ in the definition of ϵ_i. But to keep similar notations later when we take q to be an arbitrary prime, we do not use this fact.) But then, by the maximality condition on p, $(q^{p^t}-1)/(q-1)$ is not divisible by more than $p_i^{\epsilon_i}$ for known primes and the first power for all the unknown primes. So the analysis we used in the first paragraph goes through by only changing $n+1$ to p^t. Finally, note that $p^t > 100$, so we have the appropriate bound. □

The most useful case when we will use Proposition 10 is when n is very large and k_1 is close to k. So, in practice, we will usually end up with 10^{13} as the lower bound on a divisor of $\sigma(q^n)$. A lot of work could be saved if this number was significantly improved by increasing the bounds given in [16], or there was some means to work around square divisors.

5. Non-fermat primes

Sometimes our candidate for an odd perfect number will not be divisible by a large power of a Fermat prime, but rather by a large power of some arbitrary prime, q. Unfortunately, we don't have Lemma 5 for non-Fermat primes, and so we cannot put all of the "extra" factors of q into $\pi+1$. This causes two problems. First, we have to spread the extra factors of q among the unknown primes, thus reducing the number of extra factors we have at hand, exponentially. Second, if $p \not\equiv 1 \pmod{q}$ is one of our unknown primes, we cannot reduce to the case $q|\Phi_2(p)$, but rather $q|\Phi_d(p)$ for some (arbitrary) $d > 1$, $d|(q-1)$. Thus, we need a way of bounding the size of p for which $q^n|\Phi_d(p)$. This second problem is easily dealt with.

Lemma 11 ([16, Theorem 2])**.** *Let q be an odd prime. Let a_1 be a primitive root modulo q. For $r \geqslant 2$, define $a_r = a_1^{q^{r-1}} \pmod{q^r}$. Then $\{a_r^m \pmod{q^r} \,|\, m = 0,\ldots,q-2\}$ gives a complete set of incongruent solutions to $a^{q-1} \equiv 1 \pmod{q^r}$.*

Lemma 12. *Let $q < 1000$ be an odd prime. If $p^{q-1} \equiv 1 \pmod{q^n}$ for some $n \in \mathbb{Z}_+$ and some odd prime p, then $p \geqslant \min(q^{n-2}, 10^{50})$ except when*

$$(p,q) = (406633727665706113898462943559144 21, 7).$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Proof. Let $q < 1000$ be an odd prime. Fix $m \in \mathbb{N}$ so that $q^{m-2} > 10^{50}$ and m is minimal. A computer search using Lemma 11 demonstrates that every positive solution to $x^{q-1} \equiv 1 \pmod{q^m}$ with $x \neq 1$ satisfies $x > 10^{50}$. Hence the same is true if we replace m with a larger integer. Thus, it suffices to search for prime solutions to $x^{q-1} \equiv 1 \pmod{q^n}$ for $n \leqslant m$. Again, a computer search yields the stated result. □

The choice of 1000 in Lemma 12 is easily improved, but it is large enough for our needs. Also, the exceptional (p, q) in the lemma is irrelevant to our work, since in this case we find $o_q(p) = 6$ and $\sigma(p^5)$ gives rise to 12 additional prime factors of N besides p and q.

Lemma 13. *Let N be an odd perfect number, let q be an odd prime, and suppose $p^a||N$ with p prime.*

(i) *If $p \equiv 1 \pmod{q}$ and $q^b|\sigma(p^a)$, then $\sigma(p^a)$ is divisible by b distinct primes $r_1, r_2, \ldots, r_b$ with $r_i \equiv 1 \pmod{q^i}$.*

(ii) *If $p \not\equiv 1 \pmod{q}$, $o_q(p)|(a+1)$, and $q^c|(a+1)$, then $\sigma(p^a)$ is divisible by $c \cdot \sigma_0(o_q(p))$ distinct primes divisors $r_{i,j}$, $i \in [1, c]$, $j \in [1, \sigma_0(o_q(p))]$, with $r_{i,j} \equiv 1 \pmod{q^i}$.*

Proof. Analogous to Lemma 6. □

Proposition 14. *Let N be an odd perfect number, and let $q < 1000$ be a prime divisor of N with $q^n||N$. Suppose b, k, k_1, k_2, ℓ_1, ℓ_2, k_1', and ℓ_1', have the same meanings as in Proposition 7. Suppose further that the exceptional case of Lemma 12 doesn't hold. Let T be the set of known primes with unknown component, different from q, and $\not\equiv 1 \pmod{q}$. Let*

$$\tau = n - b - \sum_{p \in T,\, o_q'(p) \neq 0} \left(v_q(p^{o_q(p)} - 1) + \left\lfloor \frac{k_1' + k_2}{\sigma_0(o_q(p))} \right\rfloor \right) - (k_1' - \ell_1' + k_2)(k_1' + k_2 - 1).$$

If $\tau > 0$, then one of the unknown primes is not congruent to $1 \pmod{q}$. Furthermore, in this case, one of the unknown primes is at least as large as $\min(q^{\tau'-2}, 10^{50})$ where

$$\tau' = \min_{1 \leqslant m \leqslant k_2} \left\lceil \left(n - b - \sum_{p \in T,\, o_q'(p) \neq 0} \left(v_q(p^{o_q(p)} - 1) + \left\lfloor \frac{k_1' + k_2 - m}{\sigma_0(o_q(p))} \right\rfloor \right) - (k_1' - \ell_1' + k_2 - m)(k_1' + k_2 - m - 1) - m \left\lfloor \frac{k_1' + k_2 - m}{2} \right\rfloor \right) / m \right\rceil.$$

Proof. The proof is similar to Proposition 7. From the equation $\sigma(N)/N = 2$ we see that $q^n|\sigma(N)$, and so we try to account for as many copies of q in $\sigma(N)$ as we can. The quantity τ is exactly how many copies of q are unaccounted for, if all of the unknown primes are $\equiv 1 \pmod{q}$, and we try to account for as many copies of q as possible from the known primes using Lemmas 2 and 13. If $\tau > 0$, this means we actually have left over copies of q, which yields a contradiction, and hence not all of the unknown primes are $\equiv 1 \pmod{q}$.

In this case, let m be the number of unknown primes $\not\equiv 1 \pmod{q}$. Lemma 2 tells us that there are two sources of copies of q in $\sigma(N)$; the exponents of the

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

primes, and $p^{o_q(p)}-1$. The quantity

$$n-b-\sum_{p\in T,\, o'_q(p)\neq 0}\left(v_q(p^{o_q(p)}-1)+\left\lfloor\frac{k'_1+k_2-m}{\sigma_0(o_q(p))}\right\rfloor\right) - (k'_1-\ell'_1+k_2-m)(k'_1+k_2-m-1)-m\left\lfloor\frac{k'_1+k_2-m}{2}\right\rfloor \tag{2}$$

is the number of copies of q in $\sigma(N)$ not yet accounted for, after we account for as many copies of q as we can (again using Lemmas 2 and 13) except those copies of q which come from $\sigma(p^{o_q(p)-1})$ for the unknown primes p with $p\not\equiv 1 \pmod q$. Thus, if we divide Equation (2) by m, and take the ceiling, we have a number of copies of q that must be accounted for by $p^{o_q(p)}-1$ for an unknown prime p with $o_q(p)\neq 1$. Since m is unspecified by the hypotheses, we take the minimum over all possibilities. Finally, we apply Lemma 12. □

Next we want to prove a result analogous to Proposition 10, except for arbitrary primes. However, there have to be a few differences. First, we need something to play the role of Lemma 8. It turns out that it doesn't hurt much to just assume that the large prime, call it p, coming from Proposition 14 may in fact divide $\sigma(q^n)$. So we can write $q^{n+1}-1=(q-1)p^cm$ for some $c\in\mathbb{N}$ and $m\in\mathbb{Z}_+$. Power this equation to the $(q-1)$st power. Since $p^{q-1}\equiv 1 \pmod{q^{\tau'}}$ and $\tau'\leqslant n$, we have

$$((q-1)m)^{q-1}\equiv((q-1)mp^c)^{q-1}=(q^{n+1}-1)^{q-1}\equiv 1 \pmod{q^{\tau'}}$$

and hence we can bound $(q-1)m$ using an analogue of Lemma 12 (where we look for solutions to the equation $x^{q-1}\equiv 1 \pmod{q^n}$ which are divisible by $q-1$, rather than prime solutions). The following lemma provides this result:

Lemma 15. *Let $q<1000$ be an odd prime. Suppose $a^{q-1}\equiv 1 \pmod{q^n}$ for some $n\in\mathbb{Z}_+$ and some integer a with $(q-1)|a$. If $q\geqslant 11$, then $a\geqslant\min(q^{n-2},10^{50})$. If $q=7$, then $a\geqslant\min(q^{n-3},10^{50})$.*

Proof. An easy computer search as in Lemma 12. □

Next we need to work with possible square factors of $\sigma(q^n)$, similar to what was done with Lemma 9.

Lemma 16. *Let p and q be primes with $10^2<p<10^{11}$ and $q=7$, 11 or 13. If $q^{p-1}\equiv 1 \pmod{p^2}$, then $\sigma(q^{o_p(q)-1})$ is divisible by two primes greater than 10^{11}.*

Proof. By [16], there are only 3 pairs (p,q) satisfying the conditions, namely

$$(p,q)=(491531,7),(863,13),(1747591,13).$$

In the first case, since $65|o_p(q)$, just factor $\sigma(7^{64})$ to find the two factors 4446437759531 and 434502978835771. In the second case, $o_p(q)=862$. One factor, 16002623839393, is easily found and another is

$$\frac{13^{431}+1}{14\cdot 863^3\cdot 68099}.$$

In the last case, since $195|o_p(q)$, one factors $\sigma(13^{38})$ to find 57745124662681 and factors $\sigma(13^{64})$ to find 71442881968439190301. □

We are now ready to prove:

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Proposition 17. *Let N be an odd perfect number and let $q = 11$ or 13 be a known prime divisor of N, with $q^n || N$. Let τ, τ' be as in Proposition 14, suppose all the hypotheses of that proposition are met, and let p be the guaranteed unknown prime. Let $p_1, \ldots, p_{k_1-1}$ be the known primes different from q. Let ϵ_i be defined as before, and put $V = \prod_{i=1}^{k_1-1} p_i^{\epsilon_i}$. Suppose $k_2 > 1$. Finally, assume that all unknown prime factors are greater than 100.*

If

$$\min\left(10^{11}, \left(\frac{10^{50}}{(q-1)V}\right)^{\frac{1}{k_2-1}}, \left(\frac{q^{\tau'-2}}{(q-1)V}\right)^{\frac{1}{k_2-1}}\right) > 1,$$

then $\sigma(q^n)$ has a prime divisor, different from p, among the unknown primes, at least as big as the above minimum. If $q = 7$, the same result holds if we replace $q^{\tau'-2}$ by $q^{\tau'-3}$.

Proof. We do the case $q = 11$ or 13, the other being similar. So assume the above minimum is > 1. First note that if $d|(n+1)$, then $\sigma(q^{d-1})|\sigma(q^n)$ and so it suffices to show that $\sigma(q^{d-1})$ has a prime divisor larger than the above minimum, different from p, for some $d|(n+1)$.

By the method of proof given in Proposition 10, we may assume that at most ϵ_i copies of p_i divide $\sigma(q^{d-1})$, for some d either greater than 100 or equal to $n+1$. Furthermore, because 10^{11} occurs in the above minimum, we may assume that the only unknown prime greater than 10^{11} that may divide $\sigma(q^n)$ is p. Then by Lemma 16 and the fact that the unknown primes are greater than 100, we may assume $\sigma(q^n)$ is square-free for unknown primes, except possibly p.

From the proof for Proposition 14, we have $p^{q-1} \equiv 1 \pmod{q^{\tau'}}$ and $\tau' \leqslant n$. Write $q^d - 1 = (q-1)mp^c$ with $c \in \mathbb{N}$, $m \in \mathbb{Z}_+$, and $\gcd(p, m) = 1$. Powering this equation to the $(q-1)$st power, we have

$$((q-1)m)^{q-1} \equiv ((q-1)mp^c)^{q-1} = (q^d-1)^{q-1} \equiv 1 \pmod{q^{\min(\tau', 100)}}.$$

By Lemma 15, $(q-1)m \geqslant \min(q^{\tau'-2}, q^{98}, 10^{50}) = \min(q^{\tau'-2}, 10^{50})$. Thus

$$\frac{m}{V} \geqslant \min\left(\frac{q^{\tau'-2}}{(q-1)V}, \frac{10^{50}}{(q-1)V}\right).$$

Since m/V is at least as big as the part of $\sigma(q^{d-1})$ made up from the unknown primes, different from p, if we take the $k_2 - 1$ root of the minimum we have the appropriate lower bound. □

6. Abundance and deficiency

Let $n \in \mathbb{Z}_+$. Recall the multiplicative function $\sigma_{-1}(n) = \sum_{d|n} d^{-1}$ we introduced earlier. This function can alternatively be written using the formula $\sigma_{-1}(n) = \sigma(n)/n$, and so $\sigma(n)/n = 2$ if and only if $\sigma_{-1}(n) = 2$. A number n is called *abundant* when $\sigma_{-1}(n) > 2$ and *deficient* when $\sigma_{-1}(n) < 2$. We can use abundance and deficiency computations to limit choices on possible prime factors of an odd perfect number N. First, we extend the definition of σ_{-1} by setting

$$\sigma_{-1}(p^\infty) = \lim_{a\to\infty} \sigma_{-1}(p^a) = \frac{p}{p-1}.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Lemma 18 ([25, Proposition 2.2])**.** *Let p and q be odd primes. If $1 \leqslant a < b \leqslant \infty$, then $1 < \sigma_{-1}(p^a) < \sigma_{-1}(p^b)$. If $a, b \in [1, \infty]$ and $p < q$, then $\sigma_{-1}(q^b) < \sigma_{-1}(p^a)$.*

Lemma 19. *Let N be an odd perfect number. Suppose $p_1, \ldots, p_{k_1}$ are the known prime factors of N, $p_i^{a_i} | N$, and $k_1 < k = \omega(N)$. If $\Pi = \prod_{i=1}^{k_1} \sigma_{-1}(p_i^{a_i}) < 2$, then the smallest unknown prime is*

$$p_{k_1+1} \geqslant \frac{\Pi}{2 - \Pi}.$$

Proof. We find

$$2 = \sigma_{-1}(N) \geqslant \left(\prod_{i=1}^{k_1} \sigma_{-1}(p_i^{a_i}) \right) \sigma_{-1}(p_{k_1+1}) = \Pi \cdot \frac{p_{k_1+1} + 1}{p_{k_1+1}},$$

where the inequality in the middle follows from Lemma 18. Noting $\Pi \geqslant 1$, we obtain $\frac{2}{\Pi} \geqslant 1 + \frac{1}{p_{k_1+1}}$. Therefore $\frac{2-\Pi}{\Pi} \geqslant \frac{1}{p_{k_1+1}}$ and taking reciprocals gives us the result, since $2 - \Pi > 0$. □

Note that in the lemma if $\Pi > 2$, then $\prod_{i=1}^{k_1} p_i^{a_i}$ is abundant, hence N is abundant. If $\Pi = 2$, then $\prod_{i=1}^{k_1} p_i^{a_i}$ is already an odd perfect number.

The following lemma is the true key to our search for odd perfect numbers, as simple as the proof is (after wading through the hypotheses). This is because we built up machinery in the last few sections to find bounds for large prime divisors of N.

Lemma 20 (cf. [5, Lemma 2.2])**.** *Let N be an odd perfect number. Let $p_1, \ldots, p_k$ be the prime divisors of N, and let a_i be such that $p_i^{a_i} || N$. Fix the numbering on the indices so that $p_1, \ldots, p_{\ell_1}$ are the primes with known prime component, $p_{\ell_1+1}, \ldots, p_{k_1}$ are the other known primes, and $p_{k_1+1} < \ldots < p_k$ are the unknown primes. Suppose among the unknown primes we have bounds $p_k > P_1 > 1, \ldots, p_{k-v+1} > P_v > 1$, with $v < k_2$. For each $u = 0, 1, \ldots, v$, set*

$$\Delta_u = \left(\prod_{i=1}^{\ell_1} \sigma_{-1}(p_i^{a_i}) \right) \left(\prod_{i=\ell_1+1}^{k_1} \frac{p_i}{p_i - 1} \right) \left(\prod_{i=1}^{u} \frac{P_i}{P_i - 1} \right).$$

Finally, suppose $k_2 > 0$.

If $\Delta_u < 2$, then the smallest unknown prime is

$$p_{k_1+1} \leqslant \frac{\Delta_u (k_2 - u)}{2 - \Delta_u} + 1.$$

Therefore,

$$p_{k_1+1} \leqslant \min_{u \in [0,v],\, \Delta_u < 2} \left(\frac{\Delta_u (k_2 - u)}{2 - \Delta_u} + 1 \right).$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Proof. We compute

$$\begin{aligned}
2 = \sigma_{-1}(N) &= \prod_{i=1}^{k} \sigma_{-1}(p_i^{a_i}) \\
&\leqslant \left(\prod_{i=1}^{\ell_1} \sigma_{-1}(p_i^{a_i})\right)\left(\prod_{i=\ell_1+1}^{k-u} \sigma_{-1}(p_i^{\infty})\right)\left(\prod_{i=k-u+1}^{k} \sigma_{-1}(P_{k-i+1}^{\infty})\right) \\
&= \Delta_u \prod_{i=k_1+1}^{k-u} \sigma_{-1}(p_i^{\infty}) \leqslant \Delta_u \prod_{i=0}^{k-u-k_1-1} \sigma_{-1}((p_{k_1+1}+i)^{\infty}) \\
&= \Delta_u \frac{p_{k_1+1}+k-u-k_1-1}{p_{k_1+1}-1} = \Delta_u\left(1+\frac{k_2-u}{p_{k_1+1}-1}\right).
\end{aligned}$$

Now, recall that $u \leqslant v < k_2$ which implies $k_2 - u \geqslant 1$. Also $0 < \Delta_u < 2$, so we solve the main inequality as we did in the previous lemma, finding

$$p_{k_1+1} \leqslant \frac{\Delta_u(k_2-u)}{2-\Delta_u} + 1.$$

The last statement follows. □

One major difference between Lemma 20 and Lemma 19 is that if $\Delta_u > 2$, then that doesn't necessarily imply N is abundant. (It is true that if $k_1 = k$ and $\Delta_0 < 2$, then N is deficient, however.) This means that we might end up with $\Delta_0 > 2$, and hence we have no upper bound on p_{k_1+1}.

7. An implementation

There are three major differences between our implementation of this algorithm, and the implementations in [5] and [25]:

First, we do not allow the bound B to increase within the algorithm. Allowing the computer to vary B fully automates the algorithm at the expense of unnecessary complexity. We fix the number B at the outset, and only increase it manually if needed.

Second, the use of Lemma 20 allows for stronger upper bounds on intervals for primes. In the terminology of that lemma, our implementation always has $v \in [0, 2]$, the exact number depending on if we find large prime divisors for N from Sections 4 and 5.

Third, some of the contradictions are different. Here is a complete list of the contradictions in our implementation:

- MT There are too many total factors.
- MS There are too many copies of a single prime with known component.
- S There is an off prime smaller than an on prime coming from interval computations.
- A The number is abundant.
- D There are k known primes, and $\Delta_0 < 2$, hence N is deficient.
- F The special prime π belongs to a known component, but the hypotheses of Proposition 7 hold showing π must be in an unknown component due to a Fermat prime.
- N There are no primes in the interval given by Lemmas 19 and 20, or there are primes in the interval but they are already known, on primes.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

SF1 There are $k-1$ known primes, and the interval formula gives an upper bound of $p_k < C$, but we know from the fact that a large power of a small Fermat prime divides N that some unknown prime is larger than C by Proposition 7.

SF2 Similar to SF1 except we have a contradiction between the interval formula and Proposition 10.

SNF1 Similar to SF1, except we have a contradiction from a small non-Fermat prime, using Proposition 14.

SNF2 Similar, using Proposition 17.

The first seven contradictions are all standard, while the last four are new. There were other contradictions we might have included, but they either rely heavily on the extensive computations of others or do not present a significant increase in the speed of the algorithm.

8. Points of improvement on the algorithm and the results

The algorithm was implemented in Mathematica on a Pentium 4 personal computer. The factorizations of $\sigma(p^a)$ were carried out using a probable primality test, definitive for integers $< 10^{16}$. Thus, if a factor of $\sigma(p^a)$ was larger than this bound, Mathematica's primality proving routine was also run.

After a few trial runs of the algorithm it became clear that certain modifications would speed up the process. First, the bound B was too uniform. So, B was replaced by two bounds B_1 and B_2, where a prime $p < 1000$ became infinite when $p^a | N$ and $p^a > B_1$, while a prime $p > 1000$ became infinite when $p^a | N$ and $p^a > B_2$. We took $B_1 = 10^{50}$ and $B_2 = 10^{30}$. To further speed up the algorithm, all factorizations $\sigma(p^n)$ for $p < 1000$ and $p^n < B_1$ were put in a table beforehand. Also, to save time when computing $o'_q(p)$ and $o_q(p)$, we replaced them with $q-1$ whenever $q > 10^{40}$ (which, while inaccurate, does not make bounds invalid, only weaker).

Running the algorithm gives an output of 2857959 lines, taking about two days to finish. One of the longest cases (besides $3^\infty 5^\infty 17^\infty 257^\infty$) is $3^4 11^\infty 5^1$. This is because the bound given in Proposition 17 depends on taking (k_2-1)st roots. So, when $k_2 = 3$ the bound is really around the square-root of where it should be. To get around this problem, B_1 can be further increased only for the primes 7 and 11. After this is done the overall output is significantly reduced. With these improvements, and doing all the cases $1 \leqslant k \leqslant 8$, there are 1465127 lines of computation (about half of the previous run) taking about 18 hours. Thus we obtain:

Theorem 21. *An odd perfect number has at least* 9 *distinct prime divisors.*

Running the algorithm with $B_1 = 10^{50}$, $B_2 = 10^{30}$, $1 \leqslant k \leqslant 11$, and forcing $3 \nmid N$, also terminates without finding any odd perfect numbers, with 1679607 lines of output. Thus:

Theorem 22. *An odd perfect number N with $3 \nmid N$ has at least* 12 *distinct prime divisors.*

With the way we have chosen the contradictions and propositions, the only results we used, which are proved outside of this paper consist of:

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(i) the easy to prove non-computational lemmas, such as the Eulerian form, the results of Section 3, Lemma 8, Lemma 11, and Lemma 18;
(ii) the results of [16] for primes no greater than 17.

Files containing the printouts demonstrating the validity of Theorems 21 and 22 are available on the author's website at:

`http://www.math.uiowa.edu/~ppnielse/pace.html`

9. Future results

This paper has shown that $\omega(N) \geqslant 9$. To do the next case $\omega(N) \geqslant 10$ we would have to show that $\omega(N) = 9$ gives rise to a contradiction. To do this case with these techniques, in a reasonable amount of time, it would be necessary to find a strong upper bound for p_{k-2}, or significantly increase the lower bound on p_{k-1}. For example, consider the case of

$$3^{\infty}5^{\infty}17^{\infty}257^{\infty}65537^{\infty}4294967311^{\infty}.$$

We can make the powers on these primes so large that we may, for all intents and purposes, assume p_k is as big as we like (except not quite big enough to use [22]). However, the best we can do with our tools for p_{k-1} is 10^{13}, which is already smaller than the lower bound already given by the interval formula for p_{k-2}! The interval for p_{k-2} has a length of about 10^{18}, which is much too large to check one prime at a time, in any reasonable amount of time (even if the project was distributed over the internet).

One might try to improve the results of [16] to get around this problem, but it is currently computationally unfeasible to make large enough gains to affect the case $\omega(N) = 9$. Another possible line of attack would be to suppose that two primes q_1, q_2 divide N, each to a high power. Then one might be able to prove that $\sigma(q_1^{n_1})$ and $\sigma(q_2^{n_2})$ must each have large divisors, different from one another, once n_1 and n_2 are large enough. Another alternative would be to show that the square part of $\sigma(q^n)$ is small.

The algorithm and methods described here have other uses that could be implemented immediately. For example, one could add additional contradictions to prove results such as the following: "If $\omega(N) = 9$, then N must have at least 100 (not necessarily distinct) prime divisors." Since the purpose of this paper is to introduce new ideas, and not merely improve existing results, such improvements are left to the interested reader to explore.

References

1. A. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math. **5 IV** (1886), 70–80, 130–137.
2. Geo. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2) **5** (1904), no. 4, 173–180. MR1503541
3. R. P. Brent, G. L. Cohen, and H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp. **57** (1991), no. 196, 857–868. MR1094940 (92c:11004)
4. Joseph E. Z. Chein, *An odd perfect number has at least 8 prime factors*, Ph.D. thesis, Pennsylvania State University, 1979.
5. Graeme L. Cohen and Ronald M. Sorli, *On the number of distinct prime factors of an odd perfect number*, J. Discrete Algorithms **1** (2003), no. 1, 21–35, Combinatorial algorithms. MR2016472 (2004h:11003)
6. R. J. Cook, *Bounds for odd perfect numbers*, Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 67–71. MR1684591 (2000d:11010)

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

7. Leonard Eugene Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Amer. J. Math. **35** (1913), no. 4, 413–422. MR1506194
8. Otto Grün, *Über ungerade vollkommene Zahlen*, Math. Z. **55** (1952), 353–354. MR0053123 (14,724g)
9. Peter Hagis, Jr., *Outline of a proof that every odd perfect number has at least eight prime factors*, Math. Comp. **35** (1980), no. 151, 1027–1032. MR572873 (81k:10004)
10. ———, *Sketch of a proof that an odd perfect number relatively prime to* 3 *has at least eleven prime factors*, Math. Comp. **40** (1983), no. 161, 399–404. MR679455 (85b:11004)
11. Kevin G. Hare, *More on the total number of prime factors of an odd perfect number*, Math. Comp. **74** (2005), no. 250, 1003–1008 (electronic). MR2114661 (2005h:11010)
12. D. R. Heath-Brown, *Odd perfect numbers*, Math. Proc. Cambridge Philos. Soc. **115** (1994), no. 2, 191–196. MR1277055 (96b:11130)
13. Douglas E. Iannucci, *The second largest prime divisor of an odd perfect number exceeds ten thousand*, Math. Comp. **68** (1999), no. 228, 1749–1760. MR1651761 (2000i:11200)
14. ———, *The third largest prime divisor of an odd perfect number exceeds one hundred*, Math. Comp. **69** (2000), no. 230, 867–879. MR1651762 (2000i:11201)
15. Paul M. Jenkins, *Odd perfect numbers have a prime factor exceeding* 10^7, Math. Comp. **72** (2003), no. 243, 1549–1554 (electronic). MR1972752 (2004a:11002)
16. Wilfrid Keller and Jörg Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. **74** (2005), no. 250, 927–936 (electronic). MR2114655 (2005i:11004)
17. Masao Kishore, *On odd perfect, quasiperfect, and odd almost perfect numbers*, Math. Comp. **36** (1981), no. 154, 583–586. MR606516 (82h:10006)
18. ———, *Odd perfect numbers not divisible by* 3. *II*, Math. Comp. **40** (1983), no. 161, 405–411. MR679456 (84d:10009)
19. Wayne L. McDaniel, *The non-existence of odd perfect numbers of a certain form*, Arch. Math. (Basel) **21** (1970), 52–53. MR0258723 (41:3369)
20. Peter L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), no. 203, 361–363. MR1182246 (94d:11003)
21. Trygve Nagell, *Introduction to Number Theory*, John Wiley & Sons Inc., New York, 1951. MR0043111 (13,207b)
22. Pace P. Nielsen, *An upper bound for odd perfect numbers*, Integers **3** (2003), A14, 9 pp. (electronic). MR2036480 (2004k:11009)
23. Carl Pomerance, *Odd perfect numbers are divisible by at least seven distinct primes*, Acta Arith. **25** (1973/74), 265–300. MR0340169 (49:4925)
24. ———, *Multiply perfect numbers, Mersenne primes, and effective computability*, Math. Ann. **226** (1977), no. 3, 195–206. MR0439730 (55:12616)
25. John Voight, *On the nonexistence of odd perfect numbers*, MASS selecta, Amer. Math. Soc., Providence, RI, 2003, pp. 293–300. MR2027187 (2004j:11006)

Department of Mathematics, University of Iowa, Iowa City, Iowa 52242
E-mail address: pace_nielsen@hotmail.com

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use