ON INEQUALITIES INVOLVING COUNTS OF THE PRIME FACTORS OF AN ODD PERFECT NUMBER

Graeme Clayton
Department of Mathematics, Brigham Young University, Provo, Utah
graemec@byu.edu

Cody Hansen
Department of Mathematics, Brigham Young University, Provo, Utah
hcodys@mathematics.byu.edu

Received: 3/14/23, Revised: 5/25/23, Accepted: 10/3/23, Published: 11/6/23

Abstract

Let N be an odd perfect number. Let $\omega(N)$ be the number of distinct prime factors of N and let $\Omega(N)$ be the total number (counting multiplicity) of prime factors of N. We prove that $\frac{99}{37}\omega(N) - \frac{187}{37} \leq \Omega(N)$ and that if $3 \nmid N$, then $\frac{51}{19}\omega(N) - \frac{46}{19} \leq \Omega(N)$.

1. Introduction

A positive integer is said to be *perfect* if the sum of its positive integer divisors is twice itself. For the purposes of this paper, we will assume that N is an odd perfect number, although it is a centuries-old open problem to prove that none exist. It was shown by Euler that for any such N we have

$$N = p_0^{e_0} m^2,$$

where $p_0 \equiv e_0 \equiv 1 \pmod 4$ and p_0 is a prime not dividing m. We call p_0 the *special* prime factor of N.

It is apparent from the previously displayed equation that the inequality

$$2\omega(N) - 1 \leq \Omega(N) \tag{1.1}$$

holds, where $\omega(N)$ is the number of distinct prime factors of N and $\Omega(N)$ is the total number (counting multiplicity) of prime factors of N. Since we are only concerned with the prime-counting functions ω and Ω applied to the argument N, for simplicity we will hereafter suppress N from the notation of these functions.

DOI: 10.5281/zenodo.10075859

In a paper by Ochem and Rao [2], and in two papers by Zelinsky [3, 4], inequalities of the form $a\omega + b \leq \Omega$, with $a, b \in \mathbb{Q}$ and $a > 2$, are obtained as improvements to Inequality (1.1). Prior to this paper, the best such (asymptotic) inequalities, as proven by Zelinsky, were

$$\frac{66}{25}\omega - 5 \leq \Omega, \qquad \text{if } 3 \mid N,$$

and

$$\frac{302}{113}\omega - \frac{286}{113} \leq \Omega, \qquad \text{if } 3 \nmid N.$$

These improvements over Inequality (1.1) are based on the fact that σ, the sum of divisors function, is multiplicative. Therefore, letting the prime factorization of N be given as $N = p_0^{e_0} p_1^{e_1} \cdots p_k^{e_k}$, we have that

$$2p_0^{e_0} p_1^{e_1} \cdots p_k^{e_k} = 2N = \sigma(N) = \sigma(p_0^{e_0} p_1^{e_1} \cdots p_k^{e_k}) = \prod_{i=0}^{k} \sigma(p_i^{e_i}).$$

From this we see that each odd prime q dividing N must divide some $\sigma(p_i^{e_i})$. Hence, we make the following definition.

Definition 1.2. Given an odd perfect number N, we say that a prime p dividing N *contributes* a prime q, or that q is *contributed* by p, if $q \mid \sigma(p^e)$, where $p^e \parallel N$ (meaning that $p^e \mid N$ but $p^{e+1} \nmid N$).

We observe that

$$\sigma(p^e) = p^e + p^{e-1} + \cdots + p + 1 = \frac{p^{e+1} - 1}{p - 1} = \prod_{\substack{d \mid (e+1) \\ d \neq 1}} \Phi_d(p),$$

where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial. Thus, the factorization of N is closely linked to the factorization of cyclotomic polynomials.

Our main improvement to previous bounds is a result of discovering new restrictions on such factorizations, as shown in Lemma 3.3, Lemma 3.6, and Lemmas 4.1 through 4.7. We use these restrictions to obtain a system of inequalities. We then optimize that system to get the following theorem.

Theorem 1.3. *If N is an odd perfect number, then*

$$\frac{99}{37}\omega - \frac{187}{37} \leq \Omega.$$

This improves Zelinsky's bound in the case when $3 \mid N$, but only asymptotically improves the bound when $3 \nmid N$. However, we are able to easily modify our system of inequalities to handle this case, resulting in the next theorem, which is a strict improvement over Zelinsky's bound.

Theorem 1.4. *If N is an odd perfect number and $3 \nmid N$, then*

$$\frac{51}{19}\omega - \frac{46}{19} \leq \Omega.$$

2. Definitions

Following notation from the previously cited papers, as well as from the introduction, let N be an odd perfect number, let ω be the number of distinct prime factors of N, and let Ω be the number of total prime factors of N. Let f_3 be the integer where $3^{f_3} \mid\mid N$ (i.e., f_3 is the 3-adic valuation of N). Also, let p_0 be the special prime of N.

We will focus on prime divisors of N that are neither 3 nor the special prime. Therefore, we make the following notational choice:

Definition 2.1. Let

$$P \coloneqq \{p \text{ prime } : \ p \mid N, \ p \neq p_0, \ p \neq 3\}.$$

We often need to consider the set of the primes contributed by P. Thus, we introduce the following notation.

Definition 2.2. Let

$$Q \coloneqq \{q \text{ prime } : \ q \text{ is contributed by some } p \in P\}.$$

We define a function that describes what primes are contributed by a prime in P.

Definition 2.3. Let f be the function from P to the power set of Q, defined by the rule

$$f(p) = \{q \in Q \ : \ p \text{ contributes } q\}.$$

By an abuse of notation, for any subset $P' \subseteq P$ we also define

$$f(P') = \bigcup_{p \in P'} f(p).$$

We now separate the primes in P based on how many times they divide N.

Definition 2.4. Let

$$S \coloneqq \left\{p \in P \ : \ p^2 \mid\mid N\right\}$$

and

$$T \coloneqq \left\{p \in P \ : \ p^4 \mid N\right\}.$$

Note that $S \cap T = \emptyset$ and $S \cup T = P$. Let g_4 be the number of primes factors p of N, counting multiplicity as divisors of N, where $p \in T$.

In order to further differentiate between elements of S, we introduce notation describing certain subsets of S.

Definition 2.5. Given an integer m, given sets $U_1, \ldots, U_n$, with $0 \le n \le m$, and given an integer $j \in \{1, 2\}$, we let $S_{m,j}^{U_1,\ldots,U_n}$ denote the set of all $p \in S$ that satisfy the following conditions:

1. p contributes exactly m primes (counting multiplicity), call them $q_1, \ldots, q_m$,
2. up to reordering, $q_i \in U_i$ for each $1 \le i \le n$, and
3. $p \equiv j \pmod 3$.

We allow $n < m$ because we do not always need to focus on all of the contributed primes of elements of S. We also allow $n = 0$ for when we do not need to focus on which sets these contributed primes belong to. For example, the set $S_{2,1}$ is the set of all p in S such that p contributes two primes and is congruent to 1 modulo 3. Also, notice that we do not allow $j = 0$, because $3 \notin S$.

Note that whenever $j = 1$, all elements of the set $S_{m,j}^{U_1,\ldots,U_n}$ will contribute the prime 3. This fact is proved in Lemma 2.6.

Lemma 2.6. *If $p \in S_{m,1}^{U_1,\ldots,U_n}$, then p contributes 3 exactly once.*

Proof. Since $j = 1$, we see that $p \equiv 1 \pmod 3$. As $p \in S$, we have

$$\sigma(p^2) = p^2 + p + 1 \equiv 1^2 + 1 + 1 \equiv 0 \pmod 3.$$

To see that p does not contribute 3 twice, note that p is congruent to one of $1, 4$, or 7 modulo 9, and in all cases $p^2 + p + 1$ is congruent to 3 modulo 9. Thus, in no case can p contribute 3 twice. $\square$

We now illustrate our newly-defined notation with the following example.

Example 2.7. Suppose that $7^2, 107^2, 557^2 \,||\, N$ and that $13^4, 127^4, 6343^4 \mid N$. We see that

$$\sigma(557^2) = 557^2 + 557 + 1 = 7^2 \cdot 6343,$$

so 557 contributes 7 twice. Since $557, 7 \in S$ and $557 \equiv 2 \pmod 3$, this means that $557 \in S_{3,2}^{S,S}$. We also have $6343 \in T$, so $557 \in S_{3,2}^{T}$, and $557 \in S_{3,2}^{S,S,T}$. Since

$$\sigma(107^2) = 107^2 + 107 + 1 = 7 \cdot 13 \cdot 127$$

and $7 \in S$, we have that 107 is an element of all of the following sets:

$$S_{3,2}^{S},\ S_{3,2}^{T},\ S_{3,2}^{T,T},\ \text{and } S_{3,2}^{S,T,T}.$$

However, since $13^4 \mid N$ and $127^4 \mid N$, we have $13, 127 \in T$, so $13, 127 \notin S$, meaning that $107 \notin S_{3,2}^{S,S}$. Similarly, since $7 \in S$ we have $7 \notin T$, so $557 \notin S_{3,2}^{T,T}$.

In order to more easily discuss the prime divisors of N without regard to their congruence modulo 3, we make the following definition.

Definition 2.8. Let

$$S_m^{U_1,\dots,U_n} := S_{m,1}^{U_1,\dots,U_n} \cup S_{m,2}^{U_1,\dots,U_n}.$$

Our methods work best when we consider small values of m. Thus, we introduce the following notation to consolidate the contrary cases.

Definition 2.9. Let

$$S_{\geq k,j}^{U_1,\dots,U_n} := \bigcup_{m \geq k} S_{m,j}^{U_1,\dots,U_n},$$

for a positive integer k.

In [3], Zelinsky proves that the following inequalities hold:

$$|S_1| + |S_{2,2}| \leq |T| + |S_{2,1}| + |S_{\geq 3,1}| + 1, \tag{2.10}$$

$$|S_1| \leq |T| + |S_{\geq 3,1}| + 1. \tag{2.11}$$

In doing so, he shows that if $p_1 \in S_1$ and $p_2 \in S_2$, then the largest contributed prime of p_2 is not contributed by p_1. Furthermore, if $p_3, p_4 \in S_{2,2}$, then the largest contributed prime of p_3 is also not the largest contributed prime of p_4. These results lead to the following definition.

Definition 2.12. For each $p \in S_1 \cup S_2 \cup S_{3,1}$, we define its *linked prime* ℓ_p as follows. Let ℓ_p be the largest prime contributed by p, except in the case where $p \in S_{2,2}$ and the largest prime contributed by p is contributed by an element of $S_{2,1}$ as well. In this exceptional case, we will take ℓ_p to be the smaller prime contributed by p instead.

Inequalities (2.10) and (2.11) hold if the linking map $p \mapsto \ell_p$ is injective when considered separately over the domains $S_1 \cup S_{2,1}$ and $S_1 \cup S_{2,2}$, respectively. One of our main results is that the linking map is still injective over the union of these domains, which we prove in Lemma 3.10.

3. Lemmas for Linked Primes

We start with a well-known fact that was mentioned on page 2436 of [2]. We leave the easy proof to the motivated reader.

Lemma 3.1. *Let $a, b,$ and c be primes such that*

$$a \mid \sigma(b^{c-1}).$$

Then, either $a = c$ or $a \equiv 1 \pmod{c}$. In particular, if $c = 3$, then either $a = 3$ or $a \equiv 1 \pmod 3$.

We will also often use the following simple fact without comment.

Lemma 3.2. *Let $a, b, c,$ and d be positive integers with $b \geq c$. If $a^2 + a + 1 = bcd$, then*

$$b > \frac{a}{\sqrt{d}}.$$

Proof. We have

$$b^2 \geq bc = \frac{a^2 + a + 1}{d}$$

and so

$$b \geq \sqrt{\frac{a^2 + a + 1}{d}} > \frac{a}{\sqrt{d}}.$$

□

The next lemma is a key tool that is used repeatedly in the proofs that follow.

Lemma 3.3. *Let $a, b, c, d,$ and e be positive integers, with c prime, that satisfy*

(1) $a^2 + a + 1 = cd$,

(2) $b^2 + b + 1 = ce$, *and*

(3) $c > d > e$.

Then, $c = a + b + 1$ and $a - b = d - e$.

Proof. Since $c > d$ and $cd > a^2$, it follows that $c > a$. Note that

$$c \mid (a^2 + a + 1) - (b^2 + b + 1) = (a - b)(a + b + 1).$$

As c is prime, either $c \mid a - b$ or $c \mid a + b + 1$. Clearly, $c \nmid a - b$, as $c > a$. Hence, $c \mid a + b + 1$. However, note that $2c > 2a \geq a + b + 1$, as $a > b$. Therefore, we must have that $c = a + b + 1$. Then, since

$$(a - b)c = (a - b)(a + b + 1) = (a^2 + a + 1) - (b^2 + b + 1) = cd - ce = c(d - e),$$

we have that $a - b = d - e$. □

We next show that the largest prime contributed by an element of S_2 is not contributed by an element of S_1.

Lemma 3.4 ([2, Lemma 3])**.** *Let $a, b, c,$ and d be positive integers, with $c > d > 1$, and with c prime. If*

$$a^2 + a + 1 = cd \quad \textit{and} \quad b^2 + b + 1 = c,$$

then $a = b^2$. In particular, a is not prime in this case.

Proof. Taking $e = 1$, we can apply Lemma 3.3 to get that $c = a + b + 1$. This implies that

$$b^2 + b + 1 = a + b + 1,$$

so $a = b^2$. Thus a is not prime. $\square$

We next show that two distinct elements of $S_{2,2}$ never share their largest contributed prime.

Lemma 3.5 ([2, Lemma 3])**.** *Let a, b, c, d, and f be odd primes greater than 3, with $c > d > f$. Then, it does not hold that*

$$a^2 + a + 1 = cd \quad \textit{and} \quad b^2 + b + 1 = cf.$$

Proof. By way of contradiction, suppose that the equalities do hold. Then, since $3 \nmid a^2 + a + 1$, we have that $a \equiv 2 \pmod 3$. Similarly, $b \equiv 2 \pmod 3$. By applying Lemma 3.3 with $e = f$, we have $a + b + 1 = c$, and so by Lemma 3.1 we have that $c \equiv 1 \pmod 3$ and hence

$$1 \equiv c = a + b + 1 \equiv 2 \pmod 3,$$

a contradiction. $\square$

Two distinct elements of $S_{2,1}$ clearly have distinct largest contributed primes. However, the case remains when a prime $p_1 \in S_{2,1}$ and another prime $p_2 \in S_{2,2}$ have the same largest contributed prime. For example, if $p_1 = 7$ and $p_2 = 11$, then we have $\sigma(7^2) = 3 \cdot 19$ and $\sigma(11^2) = 7 \cdot 19$. Nevertheless, we prove below that if this occurs, the smaller contributed prime from p_2 is distinct from all of the largest contributed primes of elements of $S_1 \cup S_2$. Further, we will see in Corollary 3.9 that the smaller contributed prime from p_2 is not contributed in this same way by another similar pair of primes.

Lemma 3.6. *Suppose we have odd primes a, b, c, and d, with $c > d$ and $d \neq 3$, that satisfy the equations*

$$a^2 + a + 1 = cd \quad \textit{and} \quad b^2 + b + 1 = 3c.$$

Then, there does not exist any odd prime g such that $g^2 + g + 1 = dh$, with $d > h$, where $h = 1$ or h is an odd prime.

Proof. By Lemma 3.3, we have $c = a + b + 1$ and $d - 3 = a - b$. Therefore, we have

$$b^2 + b + 1 = 3c = 3(a + b + 1) = 3a + 3b + 3,$$

and so $a = (b^2 - 2b - 2)/3$. We also have

$$d = \frac{b^2 - 2b - 2}{3} - b + 3 = \frac{b^2 - 5b + 7}{3}. \tag{3.7}$$

Now suppose g is an odd prime such that $g^2 + g + 1 = dh$ with $d > h$. We then have three cases.

Case 1. Suppose that $g \equiv 0 \pmod 3$. Then, $g = 3$, so we find that $d = 13$ and $h = 1$. We know that $d = (b^2 - 5b + 7)/3$, so $0 = b^2 - 5b - 32$. But this has no integer solutions, a contradiction.

Case 2. Suppose that $g \equiv 1 \pmod 3$. Then, $g^2 + g + 1 \equiv 0 \pmod 3$, so

$$g^2 + g + 1 = 3d = b^2 - 5b + 7.$$

Solving for g with the quadratic equation, we find that the only positive solution is $g = b - 3$. However, this contradicts the fact that g is odd.

Case 3. Suppose that $g \equiv 2 \pmod 3$. We will show that $2d > a$. To that end, observe that

$$2d - a = \frac{2b^2 - 10b + 14}{3} - \frac{b^2 - 2b - 2}{3} = \frac{b^2 - 8b + 16}{3} = \frac{(b-4)^2}{3},$$

which is greater than 0, since $b \neq 4$. Since

$$g^2 + g + 1 = dh < d^2 < cd = a^2 + a + 1,$$

we have $g < a$. Since $2d > a$ and $g < a$, we have that

$$a + g + 1 < 2a < 4d. \tag{3.8}$$

Hence, from our earlier factorization, we have

$$d(c - h) = cd - dh = (a^2 + a + 1) - (g^2 + g + 1) = (a - g)(a + g + 1),$$

which is positive. Hence, $d \mid a - g$ or $d \mid a + g + 1$. If $d \mid a - g$, then $d = a - g$, as $2d > a$. However, this means $d \equiv 0 \pmod 3$, a contradiction. Thus, we have $d \mid a + g + 1$, i.e., $kd = a + g + 1$ for some $k \in \mathbb{N}$. We see that $a \equiv 5 \pmod 6$ and $g \equiv 5 \pmod 6$. Thus, $a + g + 1 \equiv 5 \pmod 6$. Thus, $k \equiv 5 \pmod 6$ since $d \equiv 1 \pmod 6$. However, this means that $5d \leq a + g + 1$, contradicting (3.8). □

The following corollary shows that for $p_1 \in S_{2,1}$ and $p_2 \in S_{2,2}$, if ℓ_{p_2} is the smaller contributed prime of p_2 then p_1, p_2, and all other contributed primes of p_1 and p_2 are uniquely determined by ℓ_{p_2}.

Corollary 3.9. *Given an odd prime d, if there exist odd primes a, b, and c that satisfy*

(1) $a^2 + a + 1 = cd$,

(2) $b^2 + b + 1 = 3c$, *and*

(3) $c > d$,

they are unique.

Proof. From (3.7) we get that $d = (b^2 - 5b + 7)/3$. By the quadratic equation,

$$b = \frac{1}{2}\left(5 \pm \sqrt{12d - 3}\right).$$

Since $b > 0$ and $d > 3$, the only solution is

$$b = \frac{1}{2}\left(5 + \sqrt{12d - 3}\right).$$

Then, since $b^2 + b + 1 = 3c$, we can write c entirely in terms of d. Likewise, since $a^2 + a + 1 = cd$, we can solve for a in terms of d using the quadratic equation. Since $a > 0$, we have

$$a = \frac{1}{2}\left(-1 + \sqrt{4d^2 + 4d\sqrt{12d - 3} + 12d - 3}\right).$$

Thus, a, b, and c are all uniquely determined by d. □

Using the above lemmas we show that the linking map from $S_1 \cup S_2$ to Q is injective.

Lemma 3.10. *The linking map $\ell : S_1 \cup S_2 \to Q$ defined by the rule $p \mapsto \ell_p$ is injective.*

Proof. Suppose that we have $p_1, p_2 \in S_1 \cup S_2$ and suppose that $\ell_{p_1} = \ell_{p_2}$. Our goal is to show that $p_1 = p_2$. We have nine cases to consider.

`Case 1.` Suppose that $p_1, p_2 \in S_1$. We have that

$$p_1^2 + p_1 + 1 = \ell_{p_1} = \ell_{p_2} = p_2^2 + p_2 + 1,$$

and thus $p_1 = p_2$ since $p_1, p_2 > 0$.

`Case 2.` Suppose that $p_1, p_2 \in S_{2,1}$. We have that

$$p_1^2 + p_1 + 1 = 3\ell_{p_1} = 3\ell_{p_2} = p_2^2 + p_2 + 1,$$

and thus $p_1 = p_2$ since $p_1, p_2 > 0$.

`Case 3.` Suppose that $p_1, p_2 \in S_{2,2}$ and suppose that ℓ_{p_1} is the largest prime divisor of $\sigma(p_1^2)$ and that ℓ_{p_2} is the largest divisor of $\sigma(p_2^2)$. This case is handled by Lemma 3.5.

`Case 4.` Suppose that $p_1, p_2 \in S_{2,2}$ and suppose that ℓ_{p_1} is the largest prime divisor of $\sigma(p_1^2)$ and that ℓ_{p_2} is the smallest divisor of $\sigma(p_2^2)$. By the definition of linked primes, this means that there is some $p_3 \in S_{2,1}$ that shares its largest prime divisor with $\sigma(p_2^2)$. Hence, this case is handled by Lemma 3.6.

`Case 5.` Suppose that $p_1, p_2 \in S_{2,2}$, and suppose that ℓ_{p_1} and ℓ_{p_2} are the smallest prime divisors of $\sigma(p_1^2)$ and $\sigma(p_2^2)$ respectively. By the definition of linked primes, this means that there is some $p_3 \in S_{2,1}$ that shares its largest prime divisor with $\sigma(p_1^2)$. Similarly, there is some $p_4 \in S_{2,1}$ that shares its largest prime divisor with $\sigma(p_2^2)$. Hence, by Corollary 3.9 we must have $p_1 = p_2$.

`Case 6.` Suppose that $p_1 \in S_1$ and $p_2 \in S_{2,1}$. This case is handled by Lemma 3.4, by taking $d = 3$.

`Case 7.` Suppose that $p_1 \in S_1$ and $p_2 \in S_{2,2}$, and suppose that ℓ_{p_2} is the largest prime divisor of $\sigma(p_2^2)$. This case is also handled by Lemma 3.4.

`Case 8.` Suppose that $p_1 \in S_1$ and $p_2 \in S_{2,2}$, and suppose that ℓ_{p_2} is the smallest prime divisor of $\sigma(p_2^2)$. Then, there exists some $p_3 \in S_{2,1}$ such that $\sigma(p_3^2)$ shares its largest prime divisor with $\sigma(p_2^2)$. Hence, this case is handled by Lemma 3.6, taking $h = 1$.

`Case 9.` Suppose that $p_1 \in S_{2,1}$ and $p_2 \in S_{2,2}$. From the definition of linked primes, this means that ℓ_{p_2} is the smallest prime divisor of $\sigma(p_2^2)$. Hence, there exists some $p_3 \in S_{2,1}$ such that $\sigma(p_3^2)$ shares its largest prime divisor with $\sigma(p_2^2)$. We see that this is impossible due to Lemma 3.6, with $h = 3$ and $d = \ell_{p_1}$. □

4. A Generalization of the Linking Map

As linked primes are one of the most important tools we use in establishing our main inequality between Ω and ω, we naturally want to extend the domain of the linking map. However, we were not able to establish an injective map that links all primes in S to their contributed primes in Q.

Furthermore, in [1] it was shown that a linking map $S_1 \cup S_{4,2} \to Q$ may not be injective. Thus we do not expect that it is possible to generalize our injective linking map to the entire domain S using our methods. However, we are able to show that our linking map is nearly injective over the domain $S_1 \cup S_2 \cup S_{3,1}$, in the sense that for every contributed prime q, we have that $|\{p \in S_1 \cup S_2 \cup S_{3,1} \ : \ \ell_p = q\}| \leq 2$.

We now prove two lemmas analogous to Lemma 3.3 for use with primes from $S_{3,1}$.

Lemma 4.1. *Let $a, b, d, e,$ and f be positive integers, with a, b, d prime and with $d > e > f$, that satisfy $a^2 + a + 1 = 3de$ and $b^2 + b + 1 = df$. Then, $d = a + b + 1$ and $a - b = 3e - f$.*

Proof. From Lemma 3.2, we have that $d > a/\sqrt{3} > a/2$. Therefore,

$$d(3e - f) = 3de - df = (a^2 + a + 1) - (b^2 + b + 1) = (a - b)(a + b + 1).$$

Hence, either $d \mid (a-b)$ or $d \mid (a+b+1)$.

First, suppose $d \mid (a-b)$. Then, since $2d > a$, we have that $d = a-b$. But since $d \equiv 1 \pmod 3$ by Lemma 3.1, we have that $a-b = d \equiv 1 \pmod 3$. But $a \equiv 1 \pmod 3$ and $b \equiv 2 \pmod 3$ and so $a-b \equiv 2 \pmod 3$, a contradiction, so this case cannot occur.

Now, suppose $d \mid (a+b+1)$. We observe that since $a \equiv 1 \pmod 3$ and $b \equiv 2 \pmod 3$ that $a+b+1 \equiv 1 \pmod 3$. Then, $a+b+1 \le 2a < 4d$ and so $kd = a+b+1$ for some $k \in \{1,2,3\}$. But $k=3$ yields $3d = a+b+1 \equiv 1 \pmod 3$, a contradiction. Similarly, $k=2$ gives $2d = a+b+1 \equiv 1 \pmod 2$, a contradiction. Thus $d = a+b+1$, and therefore $a-b = 3e-f$. □

Lemma 4.2. *Let a, b, d, e, and f be positive integers, with a, b, d prime and with $d \ge e > f$, that $a^2+a+1 = 3de$ and $b^2+b+1 = 3df$. Then, $d = (a+b+1)/3$ and $a-b = e-f$.*

Proof. From Lemma 3.2, $d \ge a/\sqrt{3} > a/3$. Then, we have

$$3d(e-f) = 3de - 3df = (a^2+a+1) - (b^2+b+1) = (a-b)(a+b+1).$$

Note that in this case we have $a \equiv b \equiv 1 \pmod 3$. Hence, $a-b \equiv a+b+1 \equiv 0 \pmod 3$, so $d \mid (a-b)/3$ or $d \mid (a+b+1)/3$. However, $d > a/3 > (a-b)/3$, so $d \nmid (a-b)/3$. It follows that $d \mid (a+b+1)/3$. Note that

$$\frac{a+b+1}{3} \le \frac{2a}{3} < 2d.$$

Thus, $d = (a+b+1)/3$, and therefore $a-b = e-f$. □

We now show that the largest contributed prime of an element of $S_{3,1}$ is contributed by at most one other element of $S_{3,1}$.

Lemma 4.3. *There do not exist distinct odd primes a, b, c, d, e, f, and g that satisfy*

(1) $a^2+a+1 = 3de$,

(2) $b^2+b+1 = 3df$,

(3) $c^2+c+1 = 3dg$, *and*

(4) $d \ge e > f > g$.

Proof. Suppose to the contrary that such primes exist. By Lemma 4.2 we have that $d = (a+b+1)/3$ and $d = (a+c+1)/3$. Thus $b = c$ and so $f = g$, a contradiction. □

We next show that the largest contributed prime of an element from $S_{2,2}$ can only be the largest contributed prime of a single element from $S_{3,1}$.

Lemma 4.4. *There do not exist odd primes* $a, b, c, d, e, f,$ *and* g *that satisfy*

(1) $a^2 + a + 1 = 3de,$

(2) $b^2 + b + 1 = 3df,$

(3) $c^2 + c + 1 = dg,$

(4) $d \geq e, f, g,$ *and*

(5) $e \neq f.$

Proof. Suppose to the contrary that such primes exist. By Lemma 4.1 we have that $d = a + c + 1$ and $d = b + c + 1$. Thus $a = b$ and so $e = f$, a contradiction. □

We now show that the largest contributed prime of an element from $S_{3,1}$ is not also the contributed prime of an element from S_1.

Lemma 4.5. *There do not exist odd primes* a, b, d, *and* e *that satisfy*

(1) $a^2 + a + 1 = 3de,$

(2) $b^2 + b + 1 = d,$ *and*

(3) $d \geq e.$

Proof. Suppose to the contrary that such primes exist. By Lemma 4.1, with $f = 1$, we have that $d = a + b + 1$. Thus,

$$b^2 + b + 1 = a + b + 1$$

which implies $a = b^2$, a contradiction. □

We next show that shows that the largest contributed prime of an element from $S_{3,1}$ is not also the largest contributed prime of an element from $S_{2,1}$.

Lemma 4.6. *There do not exist odd primes* a, b, d, *and* e *that satisfy*

(1) $a^2 + a + 1 = 3de,$

(2) $b^2 + b + 1 = 3d,$ *and*

(3) $d \geq e.$

Proof. Suppose to the contrary that such primes exist. By Lemma 4.2, with $f = 1$, we have that $d = (a + b + 1)/3$ and $e = a - b + 1$. Then,

$$\begin{aligned} a^2 + a + 1 &= 3de \\ &= 3\left(\frac{a+b+1}{3}\right)(a - b + 1) \\ &= (a + b + 1)(a - b + 1) \\ &= a^2 + a + 1 + (a - b^2). \end{aligned}$$

Thus, $a = b^2$, a contradiction. □

We next show that in the exceptional case that an element of $S_{2,2}$ shares its largest contributed prime with an element of $S_{2,1}$, the smaller contributed prime of that element of $S_{2,2}$ is not the largest contributed prime of an element from $S_{3,1}$.

Lemma 4.7. *Let a, b, d, and f be odd primes such that $d > f > 3$, satisfying*

$$a^2 + a + 1 = df \quad \textit{and} \quad b^2 + b + 1 = 3d.$$

Then, there do not exist odd primes c and g such that

$$c^2 + c + 1 = 3fg,$$

with $f > g$.

Proof. Suppose to the contrary that such primes exist. Then, by Lemma 3.3 with $e = 3$, we have that $f = a - b + 3$. From the proof of Corollary 3.9, we can express a in terms of f. We see that since $f > 3$, we have that

$$\begin{aligned} a &= \frac{1}{2}\left(-1 + \sqrt{4f^2 + 4f\sqrt{12f - 3} + 12f - 3}\right) \\ &< 2f. \end{aligned}$$

From Lemma 3.2, we have $f \geq c/\sqrt{3}$.

We can now factor whichever is positive of $(a^2 + a + 1) - (c^2 + c + 1)$ and $(c^2 + c + 1) - (a^2 + a + 1)$, giving us two cases to consider.

Case 1. Suppose $a > c$. Thus we have

$$f(d - 3g) = df - 3fg = (a^2 + a + 1) - (c^2 + c + 1) = (a - c)(a + c + 1).$$

So $f \mid (a - c)$ or $f \mid (a + c + 1)$. Suppose $f \mid (a - c)$. Since we also have $f > a/2$ from above, we have that $f = a - c$. Then, $a - c = a - b + 3$ and so $b = c + 3$, a contradiction. Thus $f \mid (a + c + 1)$ and since

$$a + c + 1 \leq 2a < 4f,$$

we have that $kf = a+c+1$ for some $k \in \{1, 2, 3\}$. Then, $k = 3$ yields $3f = a+c+1 \equiv 1 \pmod 3$, a contradiction. Similarly, $k = 2$ gives $2f = a + c + 1 \equiv 1 \pmod 2$, a contradiction. Therefore, $k = 1$ and so $f = a + c + 1$. Hence, $a + c + 1 = a - b + 3$ and so $b + c = 2$, a contradiction.

`Case 2.` Suppose $a < c$. Thus we have

$$f(3g - d) = 3fg - df = (c^2 + c + 1) - (a^2 + a + 1) = (c - a)(a + c + 1).$$

So $f \mid (c - a)$ or $f \mid (a + c + 1)$. Suppose $f \mid (c - a)$. From Lemma 3.2 we have that $f > c/\sqrt{3}$, so $f > c/2$ and thus we have by Lemma 3.1 that $1 \equiv f = c - a \equiv 2 \pmod 3$, a contradiction. Thus $f \mid (a + c + 1)$ and since

$$a + c + 1 \leq 2c < 4f,$$

we have that $kf = a+c+1$ for some $k \in \{1, 2, 3\}$. Then, $k = 3$ yields $3f = a+c+1 \equiv 1 \pmod 3$, a contradiction. Similarly, $k = 2$ gives $2f = a + c + 1 \equiv 1 \pmod 2$, a contradiction. Thus $k = 1$ and so $f = a + c + 1$. Hence, $a + c + 1 = a - b + 3$ and so $b + c = 2$, a contradiction. □

Lemma 4.8. *Let the linking map $\ell : S_1 \cup S_2 \cup S_{3,1} \to Q$ be defined by the rule $p \mapsto \ell_p$. Then, for every $q \in Q$, $|\{p \in S_1 \cup S_{2,1} \ : \ \ell_p = q\}| = 1$ and $|\{p \in S_{2,2} \cup S_{3,1} \ : \ \ell_p = q\}| \leq 2$.*

Proof. Suppose that we have $p_1, p_2, p_3 \in S_1 \cup S_2 \cup S_{3,1}$, and suppose that $\ell_{p_1} = \ell_{p_2} = \ell_{p_3}$. All nine cases in Lemma 3.10 still apply, so we have five additional cases to consider.

`Case 10.` Suppose that $p_1, p_2, p_3 \in S_{3,1}$. Then, by Lemma 4.3, we have, without loss of generality, that $p_1 = p_3$. Thus the preimage of ℓ_{p_1} has at most two elements, p_1 and p_2.

`Case 11.` Suppose that $p_1 \in S_1$ and $p_2 \in S_{3,1}$. This case is handled by Lemma 4.5.

`Case 12.` Suppose that $p_1 \in S_{2,1}$ and $p_2 \in S_{3,1}$. This case is handled by Lemma 4.6.

`Case 13.` Suppose that $p_1 \in S_{2,2}$, $p_2 \in S_{3,1}$, and ℓ_{p_1} is the largest contributed prime of p_1. By the injectivity of the linking map over $S_1 \cup S_2$, we know that $p_3 \notin S_1 \cup S_2$. Hence, the only remaining possibility is that $p_3 \in S_{3,1}$; however, this case is handled by Lemma 4.4.

`Case 14.` Suppose that $p_1 \in S_{2,2}$, $p_2 \in S_{3,1}$, and ℓ_{p_1} is the smaller contributed prime of p_1. This case is handled by Lemma 4.7. □

5. Proofs of Theorem 1.3 and Theorem 1.4

To obtain the bound in [4], twenty-one inequalities were derived. We use thirteen of those inequalities as they appear in [4], modify one to eliminate unnecessary variables, and improve one other (Equation 35 in [4]). Further, we introduce four new inequalities. The correspondence between this paper and [4] is shown in Table 1 below. We now give brief explanations of the inequalities.

Our Equation	Corr. eqn. in [4]
(5.4)	(26)
(5.5)	(27)
(5.6)	(28)
(5.7)	(29)
(5.8)	(30)
(5.1)	(31)
(5.10)	(32)
(5.11)	(33)
(5.9)	(34)
(5.16)	(35)
(5.14)	(36)
(5.15)	(37)
(5.3)	(38)
(5.13)	(41)
(5.2)	(47)

Table 1: Equation correspondence

Inequalities (5.1) through (5.4) are all straightforward consequences of their associated definitions:

$$e_0 + f_3 + 2|S| + g_4 = \Omega, \tag{5.1}$$

$$\omega \le 2 + |S| + |T|, \tag{5.2}$$

$$4|T| \le g_4, \tag{5.3}$$

$$1 \le e_0. \tag{5.4}$$

Equations (5.5) through (5.10) are obtained by decomposing S, and some of its subsets, into disjoint subsets. Note there are similar decompositions for $S_{2,1}$ and $S_{2,2}$, but they do not contribute to our result. The following hold:

$$|S| = |S_1| + |S_2| + |S_3| + |S_{\ge 4}|, \tag{5.5}$$

$$|S_2| = |S_{2,1}| + |S_{2,2}|, \tag{5.6}$$

$$|S_3| = |S_{3,1}| + |S_{3,2}|, \tag{5.7}$$

$$|S_{\geq 4}| = |S_{\geq 4,1}| + |S_{\geq 4,2}|, \tag{5.8}$$
$$|S_1| = \left|S_1^S\right| + \left|S_1^T\right| + \left|S_1^{\{p_0\}}\right|, \tag{5.9}$$
$$|S_{3,1}| = \left|S_{3,1}^{S,S}\right| + \left|S_{3,1}^{T\cup\{p_0\},T\cup\{p_0\}}\right| + \left|S_{3,1}^{S,T\cup\{p_0\}}\right|. \tag{5.10}$$

Inequalities (5.11) and (5.12) are obtained by splitting sets into subsets, which may overlap. In particular, it was proven in [1] that for $p \in S_{3,2}$, with $f(p) = \{p_1, p_2, p_3\}$, that, without loss of generality, $p_1 \notin f(S_1)$. We make a distinction for when $p_1 \in S$ and when $p_1 \in T \cup \{p_0\}$, giving (5.12). Thus we have:

$$\left|S_{3,1}^{S,T\cup\{p_0\}}\right| \leq \left|S_{3,1}^{S\setminus f(S_1),T\cup\{p_0\}}\right| + \left|S_{3,1}^{S,(T\cup\{p_0\})\setminus f(S_1)}\right|, \tag{5.11}$$
$$|S_{3,2}| \leq \left|S_{3,2}^{S\setminus f(S_1)}\right| + \left|S_{3,2}^{(T\cup\{p_0\})\setminus f(S_1)}\right|. \tag{5.12}$$

We obtain Inequality (5.13) by noting that only one element of S_1 can contribute the special prime, i.e., $S_1^{\{p_0\}}$ has at most one element. Therefore:

$$\left|S_1^{\{p_0\}}\right| \leq 1. \tag{5.13}$$

Inequality (5.14) holds since every element of $S_{2,1} \cup S_{3,1} \cup S_{\geq 4,1}$ contributes exactly one 3, and thus 3 must divide N at least once for each element of these sets. Thus we have:

$$|S_{2,1}| + |S_{3,1}| + |S_{\geq 4,1}| \leq f_3. \tag{5.14}$$

Counting the number of primes unequal to 3 that are contributed by elements of S gives

$$\begin{aligned}|S_1| + 2\,|S_{2,2}| + 3\,|S_{3,2}| + 4\,|S_{\geq 4,2}| + |S_{2,1}| + 2\,|S_{3,1}| + 3\,|S_{\geq 4,1}|\\ \leq g_4 + e_0 + 2\,|S_{2,1}| + 2\,|S_{3,1}| + 2\,|S_{\geq 4,1}|,\end{aligned}$$

which simplifies to

$$|S_1| + 2\,|S_{2,2}| + 3\,|S_{3,2}| + 4\,|S_{\geq 4,2}| + |S_{\geq 4,1}| \leq g_4 + e_0 + |S_{2,1}|. \tag{5.15}$$

From Lemma 3.10 and Lemma 4.8, we get Inequality (5.16) and Inequality (5.17), respectively:

$$|S_1| + |S_2| \leq |T| + |S_{2,1}| + |S_{3,1}| + |S_{\geq 4,1}| + 1, \tag{5.16}$$
$$|S_1| + |S_{2,1}| + \frac{1}{2}(|S_{2,2}| + |S_{3,1}|) \leq |T| + |S_{2,1}| + |S_{3,1}| + |S_{\geq 4,1}| + 1. \tag{5.17}$$

Inequality (5.18) comes from establishing a lower bound for the total number of primes (counting multiplicity) which divide N exactly twice and are congruent 1 modulo 3. The right hand side of the inequality is exactly the total number of such primes (note that no elements of S_1 are congruent 1 modulo 3).

To justify the left hand side, note that every element of S_1^S will contribute one unique prime to S which is congruent to 1 modulo 3. Since all of these contributed primes are in S, by definition they must divide N exactly twice. We will show that all other sets used in the left-hand side of this inequality contribute at least one prime that is distinct from all of these primes contributed by S_1^S. Therefore, we are allowed to double the $\left|S_1^S\right|$ term in the inequality.

By Lemma 4.5, the largest prime contributed by an element of $S_{3,1}$ is not also contributed by an element of S_1. Therefore, each prime in $S_{3,1}^{S,S}$ will contribute at least one prime which is in S and is congruent to 1 modulo 3 and is distinct from any primes contributed by elements of S_1. Similarly, we have at least one such prime contributed by each element of $S_{3,1}^{S\setminus f(S_1),T\cup\{p_0\}}$ and by each element of $S_{3,2}^{S\setminus f(S_1)}$, simply by the definition of these sets. We express these relationships with the following inequality:

$$2\left|S_1^S\right| + \left|S_{3,1}^{S,S}\right| + \left|S_{3,1}^{S\setminus f(S_1),T\cup\{p_0\}}\right| + \left|S_{3,2}^{S\setminus f(S_1)}\right| \leq 2\left|S_{2,1}\right| + 2\left|S_{3,1}\right| + 2\left|S_{\geq 4,1}\right|. \tag{5.18}$$

Inequality (5.19) is very similar to (5.18). It comes from establishing a lower bound for the total number of primes (counting multiplicity) which divide N at least four times, or are equal to the special prime. The argument justifying (5.19) is identical to the above in almost every way, with $T\cup\{p_0\}$ and S interchanged, though we do use S_1^T rather than $S_1^{T\cup\{p_0\}}$, simply to ensure that each element of the set contributes a prime which divides N at least four times.

There is a notable difference between this inequality and the last one, however, in that g_4+e_0 is the total number of all primes which divide N at least four times, or are the special prime, not just those that are congruent to 1 modulo 3. This is simply because we have not utilized the same subdivisions of the set T as we have for S, and the argument still holds, resulting in the following inequality:

$$4\left|S_1^T\right| + \left|S_{3,1}^{T\cup\{p_0\},T\cup\{p_0\}}\right| + \left|S_{3,1}^{S,(T\cup\{p_0\})\setminus f(S_1)}\right| + \left|S_{3,2}^{(T\cup\{p_0\})\setminus f(S_1)}\right| \leq g_4+e_0. \tag{5.19}$$

Our goal is to get an inequality of the form $a\omega+b\leq\Omega$, with $a,b\in\mathbb{Q}$, with a as large as possible. Once we have found the maximum value of a, we would like to then maximize b. To that end, we rewrite all numbered inequalities (and equalities) of this section so that the right hand side is zero. We then set x_i to be equal to the left hand side of these rewritten inequalities for $1 \le i \le 19$. For example, for Inequality (5.14) we have that $x_{14} = |S_{2,1}| + |S_{3,1}| + |S_{\ge 4,1}| - f_3$.

We now multiply each x_i by a coefficient c_i and sum the products to get the linear combination:

$$\sum_{i=1}^{19} c_i x_i \le 0. \tag{5.20}$$

We set $c_1 = 1$, so that the coefficient of Ω is fixed. Next, for each i such that (5.i) is an inequality rather than an equality, we add the constraint $c_i \ge 0$. Finally, after expanding and collecting like terms in Inequality (5.20), we also constrain the coefficients of each term to be nonnegative. For example, to ensure that the coefficient of the term $|S|$ is nonnegative in Inequality (5.20), we add the constraint that $2c_1 - c_2 + c_5 \ge 0$. We then maximize c_2 subject to these constraints in Mathematica, which gives the values in Table 2.

$c_1 = 1$	$c_2 = 99/37$	$c_3 = 28/37$	$c_4 = 28/37$	$c_5 = 25/37$
$c_6 = 20/37$	$c_7 = 25/37$	$c_8 = 25/37$	$c_9 = 4/37$	$c_{10} = 1/37$
$c_{11} = 1/37$	$c_{12} = 1/37$	$c_{13} = 4/37$	$c_{14} = 1$	$c_{15} = 8/37$
$c_{16} = 5/37$	$c_{17} = 8/37$	$c_{18} = 2/37$	$c_{19} = 1/37$	

Table 2: Coefficients for the $3 \mid N$ case

Expanding Inequality (5.20) with these coefficients and multiplying by 37 gives

$$\left|S_{3,1}^{S,S}\right| + \left|S_{3,1}^{S\setminus f(S_1),T\cup\{p_0\}}\right| + \left|S_{3,2}^{S\setminus f(S_1)}\right| + 3\left|S_{\ge 4,1}\right| + 7\left|S_{\ge 4,2}\right| + 99\omega - 187 \le 37\Omega.$$

Then, since each quantity is nonnegative, we can simplify to

$$\frac{99}{37}\omega - \frac{187}{37} \le \Omega,$$

as desired.

To deal with the case when $3 \nmid N$, we need to add the equality

$$f_3 = 0 \tag{5.21}$$

and change Inequality (5.2) to the equality

$$\omega = 1 + |S| + |T|.$$

Using the modified system of equations, we get the coefficients displayed in Table 3 using Mathematica. These coefficients lead to the inequality

$$\frac{51}{19}\omega - \frac{46}{19} \le \Omega,$$

as claimed.

$c_1 = 1$	$c_2 = 51/19$	$c_3 = 14/19$	$c_4 = 10/19$	$c_5 = 13/19$
$c_6 = 8/19$	$c_7 = 13/19$	$c_8 = 13/19$	$c_9 = 4/19$	$c_{10} = 1/19$
$c_{11} = 1/19$	$c_{12} = 1/19$	$c_{13} = 4/19$	$c_{14} = 21/19$	$c_{15} = 4/19$
$c_{16} = 5/19$	$c_{17} = 0$	$c_{18} = 2/19$	$c_{19} = 1/19$	$c_{21} = 2/19$

Table 3: Coefficients for the $3 \nmid N$ case

6. Future Work

The improvements in this paper are based on the idea of linked primes. Further study into this concept could yield additional improvements. In particular, showing that the linking map extends to a larger domain would increase the numerics of this paper, although we know $S_{4,2}$ to be a natural boundary to the linking map due to the work in [1].

We were able to prove that a largest contributed prime can be shared among elements of $S_1 \cup S_2 \cup S_{3,1}$ only twice, and ideally we would extend this restriction to larger subsets of S. However, this is not possible for $S_{3,2}$, as there exists a set of five primes that could be in $S_{3,2}$ that share their largest contributed prime (these are 120587, 269561, 324143, 473117, and 833033, which share 16963). Indeed, we suspect that elements of $S_{3,2}$ could share their largest prime arbitrarily often. Therefore, extending the linking map to $S_{3,2}$ would likely require a change in the definition of a linked prime.

Our work has mainly focused on improving the linear term in Theorem 1.3, and more work could be done to improve the constant term. In discussion with the authors, Ochem and Rao suggested a method to improve the constant term with casework. They were able to get an improved constant term of $-75/37$ under the assumption $e_0 \geq 5$, and a constant term of $-124/37$ when $e_0 = 1$ and $p_0 \equiv 2 \pmod 3$. However, in the remaining case, $e_0 = 1$ and $p_0 \equiv 1 \pmod 3$, it is not obvious how to proceed.

In proving his bound for when $3 \nmid N$, Zelinsky uses the factorization

$$\Phi_3(\Phi_5(x)) = (x^2 - x + 1)(x^6 + 3x^5 + 5x^4 + 6x^3 + 7x^2 + 6x + 3).$$

It is not difficult to show that this factorization is part of a family of factorizations of compositions of cyclotomic polynomials or the product of cyclotomic polynomials. Namely:

Proposition 6.1. *Let $\Psi_n(x) = \sum_{i=0}^{n-1} x^i$, let r be an odd integer, and let t be an odd prime. If $r \equiv -1 \pmod{2t}$, then*

$$\Phi_{2t}(x) \mid \Phi_t(\Psi_r(x)).$$

Proof. Observe that for any $2t^{\text{th}}$ root of unity ζ_{2t},

$$\Psi_r(\zeta_{2t}) = \Psi_{2t-1}(\zeta_{2t}).$$

Note that

$$\Psi_{2t-1}(\zeta_{2t}) = \zeta_{2t}^{t-1}.$$

However, $\zeta_{2t}^{t-1} = \zeta_t$ for some primitive t^{th} root of unity. Thus,

$$\Phi_t(\Psi_r(\zeta_{2t})) = \Phi_t(\zeta_t) = 0.$$

Since ζ_{2t} was arbitrary, all primitive $2t^{\text{th}}$ roots of unity are zeros of $\Phi_t(\Psi_r(x))$. Hence,

$$\Phi_{2t}(x) \mid \Phi_t(\Psi_r(x)). \qquad \square$$

Proposition 6.1 implies that if $p^e \mid\mid N$ for some e such that $e+1$ is prime and $q = \sigma(p^e)$ is also prime, and if $q^m \mid\mid N$ for some even m, then $\sigma(q^m)$ has at least two factors. Thus, if we could prove that this situation occurs often enough, we could improve our result.

Acknowledgements. We thank our advisor Pace P. Nielsen for his invaluable assistance in preparing this paper. We thank Joshua Zelinsky, Pascal Ochem, Michaël Rao, the anonymous referee, and the editors for comments that improved this paper.

References

[1] Cody S. Hansen and Pace P. Nielsen, Prime factors of $\Phi_3(x)$ of the same form, *Integers* **22** (2022), #A71.

[2] Pascal Ochem and Michaël Rao, On the number of prime factors of an odd perfect number, *Math. Comp.* **83** (2014), no. 289, 2435–2439.

[3] Joshua Zelinsky, An improvement of an inequality of Ochem and Rao concerning odd perfect numbers, *Integers* **18** (2018), #A48.

[4] Joshua Zelinsky, On the total number of prime factors of an odd perfect number, *Integers* **21** (2021), #A76.