MATHEMATICS OF COMPUTATION
Volume 77, Number 263, July 2008, Pages 1859–1868
S 0025-5718(08)02050-4
Article electronically published on February 12, 2008

ODD PERFECT NUMBERS HAVE A PRIME FACTOR EXCEEDING 10^8

TAKESHI GOTO AND YASUO OHNO

Abstract. Jenkins in 2003 showed that every odd perfect number is divisible by a prime exceeding 10^7. Using the properties of cyclotomic polynomials, we improve this result to show that every perfect number is divisible by a prime exceeding 10^8.

1. Introduction

A positive integer n is said to be *perfect* if $\sigma(n) = 2n$, where $\sigma(n)$ denotes the sum of positive divisors of n. As of November 2006, forty-four even perfect numbers are known. On the other hand, it is still open whether or not an odd perfect number exists. Many necessary conditions for existence of an odd perfect number have been found. For example, Euler showed that the prime factorization of an odd perfect number n must be of the form

$$n = p_0^{e_0} p_1^{2e_1} \cdots p_k^{2e_k}, \quad p_0 \equiv e_0 \equiv 1 \pmod 4.$$

Here p_0 is called the *special prime* of n. Brent, Cohen and te Riele [1] showed that $n > 10^{300}$. Chein [2] and Hagis [7] independently showed that n must have at least 8 distinct prime factors, and this bound was recently improved to 9 by Nielsen [18]. Hare [9] showed that n must have totally at least 47 prime factors, and he recently improved this bound to 75 in [10].

In the present paper, we focus our attention on the largest prime factor of an odd perfect number. In 1944, Kanold [15] showed that every odd perfect number is divisible by a prime exceeding 60. This lower bound was improved by Hagis and McDaniel [5] (resp. [6]) to 10^4 (resp. 10^5), by Hagis and Cohen [8] to 10^6, by Jenkins [13], [14] to 10^7. Jenkins reported that he needed about 25,800 hours for computing time. On the other hand, Ore [19] proved that every perfect number is a *harmonic number* (a positive integer is said to be harmonic if the harmonic mean of its positive divisors is an integer). Chishiki, Goto and Ohno [3] showed that every odd harmonic number is divisible by a prime exceeding 10^5. This is another extension of the result given by McDaniel [6]. The aim of the present paper is to show the following result.

Theorem 1.1. *Every odd perfect number is divisible by a prime exceeding* 10^8.

Received by the editor December 13, 2006 and, in revised form, February 26, 2007.
2000 *Mathematics Subject Classification.* Primary 11A25, 11Y70.
Key words and phrases. Odd perfect numbers, cyclotomic numbers.
This work was supported by Computing and Communications Center, Kyushu University.
The second author was supported in part by JSPS Grant-in-Aid No. 15740025 and No. 18740020.

In §2 and §3, we explain our proof of Theorem 1.1. For more details, see the note on the webpage `http://www.ma.noda.tus.ac.jp/u/tg/perfect.html`. The programs used in the computation are also available on this webpage. In §4, we discuss our algorithm.

2. Outline of the proof

In this paper, p, q will denote odd primes and r will denote a (possibly even) prime. The dth cyclotomic polynomial will be denoted by Φ_d, so that $\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \prod_{d|(e+1),d>1} \Phi_d(p)$. Let n be an odd perfect number whose prime factorization is $p_1^{e_1} \cdots p_k^{e_k}$ (note that this is different from the form in §1). Since σ is multiplicative, it easily follows from $\sigma(n) = 2n$ that

$$\prod_{i=1}^{k} \prod_{\substack{d \mid (e_i+1) \\ d>1}} \Phi_d(p_i) = 2\prod_{i=1}^{k} p_i^{e_i}. \tag{2.1}$$

For integers $a, d \geq 2$, the integer $\Phi_d(a)$ is often called a *cyclotomic number*. In the nineteenth century, cyclotomic numbers were studied by Sylvester, Kronecker et al. The following proposition is a summary of their results (cf. [20]).

Proposition 2.1. *Let q be a prime, and a, d be integers. Suppose that $a \geq 2, d \geq 3$. Then the following facts hold.*

1. *If $q \mid \Phi_d(a)$, then $q \mid d$ or $q \equiv 1 \pmod{d}$.*
2. *If $q \mid \Phi_d(a)$ and $q \mid d$, then $q^2 \nmid \Phi_d(a)$.*
3. *If $(a, d) \neq (2, 6)$, then the cyclotomic number $\Phi_d(a)$ has at least one prime factor q such that $q \equiv 1 \pmod{d}$.*

2.1. **Acceptable values.** Assume that n is an odd perfect number whose largest prime factor is less than 10^8. Then the right-hand side of (2.1) has no prime factors exceeding 10^8, hence so does the left-hand side. Since n is odd, the cyclotomic numbers in (2.1) are not divisible by 4.

Definition. For an odd prime p and a prime r, we say that $\Phi_r(p)$ is *acceptable* if the following two conditions hold.

1. $\Phi_r(p)$ has no prime factors exceeding 10^8.
2. $4 \nmid \Phi_r(p)$.

Clearly, cyclotomic numbers in (2.1) must be acceptable. Our first aim is to find all acceptable values $\Phi_r(p)$ with $3 \leq p < 10^8$.

Lemma 2.2. *Suppose that $3 \leq p < 10^8$, $r \geq 7$, and the cyclotomic number $\Phi_r(p)$ is acceptable. Then $\Phi_r(p)$ is one of 671 numbers listed in the online note mentioned in §1.*

The details of the proof of Lemma 2.2 can be found in §3. The basic techniques used for proving Lemma 2.2 is first to show that we can restrict our search to $r < 5 \times 10^7$ (hence we need search only finitely many numbers), and then to use properties of cyclotomic polynomials to further refine the search.

2.2. **Inadmissible small primes.** Under Lemma 2.2, we show the following.

Lemma 2.3. *Assume that n is an odd perfect number whose largest prime factor is less than 10^8. Then n is not divisible by any prime in the following set X.*

$$\begin{aligned} X = \{&3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 43, 61, 71, 113, 127, 131, 151, 197,\\ &211, 239, 281, 337, 379, 421, 449, 463, 491, 547, 617, 631, 659, 673, 743,\\ &757, 827, 911, 953, 967, 1051, 1093\}.\end{aligned}$$

In particular, n has no prime factors less than 41.

For the proof of this lemma, primes in X are considered in the order

$$\begin{aligned} &1093, 151, 31, 127, 19, 11, 7, 23, 131, 37, 61, 13, 3, 5, 29, 43, 1051, 17,\\ &71, 113, 197, 211, 239, 281, 337, 379, 421, 449, 463, 491, 547, 617, 631,\\ &659, 673, 743, 757, 827, 911, 953, 967.\end{aligned}$$

For example, after proving that $1093 \nmid n$, we prove $151 \nmid n$ as follows. Assume that $151 \mid n$. Then the left-hand side of (2.1) is divisible by a cyclotomic number $\Phi_r(151)$ for some prime r. Only $\Phi_3(151) = 3 \cdot 7 \cdot 1093$ is acceptable, however, it is contradictory to $1093 \nmid n$. Hence we have $151 \nmid n$. The proof of $1093 \nmid n$ has many branches. At each step, we only need to branch on r where $\Phi_r(p)$ is acceptable. We write p^* to indicate that p is the special prime. Note that two different primes cannot be special simultaneously.

(initial part of the proof of Lemma 2.3)

$(1093 \nmid n)$

$1093:\ \Phi_2(1093) = 2 \cdot 547;\ \Phi_3(1093) = 3 \cdot 398581.$

$1093^*, 547:\ \Phi_3(547) = 3 \cdot 163 \cdot 613.$

$1093^*, 547, 613:\ \Phi_3(613) = 3 \cdot 7 \cdot 17923;\ \Phi_5(613) = 131 \cdot 20161 \cdot 53551.$

$1093^*, 547, 613, 17923:\ \Phi_3(17923) = 3 \cdot 13 \cdot 31 \cdot 265717.$

$1093^*, 547, 613, 17923, 265717:$ Any $\Phi_r(265717)$ is unacceptable.

$1093^*, 547, 613, 20161:$ Any $\Phi_r(20161)$ is unacceptable.

$1093, 398581:\ \Phi_2(398581) = 2 \cdot 17 \cdot 19 \cdot 617;\ \Phi_3(398581) = 3 \cdot 1621 \cdot 32668561.$

$1093, 398581^*, 617:\ \Phi_3(617) = 97 \cdot 3931.$

$1093, 398581^*, 617, 3931:\ \Phi_3(3931) = 3 \cdot 7 \cdot 31 \cdot 23743.$

$1093, 398581^*, 617, 3931, 23743:\ \Phi_3(23743) = 3 \cdot 37 \cdot 5078863.$

$1093, 398581^*, 617, 3931, 23743, 5078863:$ Any $\Phi_r(5078863)$ is unacceptable.

$1093, 398581, 32668561:\ \Phi_2(32668561) = 2 \cdot 19 \cdot 43 \cdot 19993.$

$1093, 398581, 32668561^*, 19993:\ \Phi_3(19993) = 3 \cdot 73 \cdot 1825297.$

$1093, 398581, 32668561^*, 19993, 1825297:\ \Phi_3(1825297) = 3 \cdot 326863 \cdot 3397663.$

$1093, 398581, 32668561^*, 19993, 1825297, 326863:\ \Phi_3(326863) = 3 \cdot 67 \cdot 3313 \cdot 160441.$

$1093, 398581, 32668561^*, 19993, 1825297, 326863, 3313:\ \Phi_3(3313) = 3 \cdot 7 \cdot 7 \cdot 19 \cdot 3931.$

$1093, 398581, 32668561^*, 19993, 1825297, 326863, 3313, 3931:$
$\Phi_3(3931) = 3 \cdot 7 \cdot 31 \cdot 23743.$

$1093, 398581, 32668561^*, 19993, 1825297, 326863, 3313, 3931, 23743:$
$\Phi_3(23743) = 3 \cdot 37 \cdot 5078863.$

$1093, 398581, 32668561^*, 19993, 1825297, 326863, 3313, 3931, 23743, 5078863:$
Any $\Phi_r(5078863)$ is unacceptable.

$(153 \nmid n)$

$151:\ \Phi_3(151) = 3 \cdot 7 \cdot 1093.$

$151, 1093:$ contradiction to $1093 \nmid n$.

$(31 \nmid n)$

$31:\ \Phi_3(31) = 3 \cdot 331;\ \Phi_5(31) = 5 \cdot 11 \cdot 17351;\ \Phi_{13}(31) = 42407 \cdot 2426789 \cdot 7908811.$

$\cdots$

For the complete proof of Lemma 2.3, see the online note mentioned in §1.

2.3. **Restriction on exponents in the prime factorization.** Under Lemmas 2.2, 2.3, we show the following.

Lemma 2.4. *Assume that n is an odd perfect number whose largest prime factor is less than 10^8. Let the prime factorization of n be $p_1^{e_1} \cdots p_k^{e_k}$. Then every $e_i + 1$ has no prime factors greater than 5.*

Assume that some e_i+1 has a prime factor r greater than 5. Then the cyclotomic number $\Phi_r(p_i)$ is acceptable. Hence $\Phi_r(p_i)$ is one of the 671 numbers mentioned in the statement of Lemma 2.2. From Lemma 2.3, it follows that $p_i \notin X$, and $\Phi_r(p_i)$ is not divisible by any prime in X. There are 87 such cyclotomic numbers. It is sufficient to show that each of these 87 numbers cannot appear in (2.1). For example, we can check $\Phi_{13}(47)$ as follows. Assume that $\Phi_{13}(47) \mid n$. This implies $14050609 \mid n$ since

$$\Phi_{13}(47) = 53 \cdot 2237 \cdot 14050609 \cdot 71265169.$$

Only $\Phi_2(14050609) = 2 \cdot 5 \cdot 7 \cdot 200723$ is acceptable. Since $5 \in X$, this is contradictory to Lemma 2.3. For the complete proof of Lemma 2.4, see the online note mentioned in §1.

2.4. **Four sets.** We denote by $|A|$ the size of the set A. Let $P = \{p \mid p \text{ is prime}, 41 \le p < 10^8\}$. A computer search showed that $|P| = 5761443$ and

$$P^* := \prod_{p \in P} \frac{p}{p-1} < 4.87934286481804236682.$$

The four subsets S, T, U, V of P are defined by

$$\begin{aligned}
S &= \{p \in P \mid p \not\equiv 1 \pmod 3 \text{ and } p \not\equiv 1 \pmod 5\},\\
T &= \{p \in P \mid p \equiv 1 \pmod{15}\},\\
U &= \{p \in P \mid p \equiv 1 \pmod 3, p \not\equiv 1 \pmod 5 \text{ and } \Phi_5(p) \text{ is unacceptable}\},\\
V &= \{p \in P \mid p \not\equiv 1 \pmod 3, p \equiv 1 \pmod 5 \text{ and } \Phi_3(p) \text{ is unacceptable}\}.
\end{aligned}$$

Note that these subsets are disjoint and $S \cup T \cup U \cup T \neq P$. Computer searches showed that $|S| = 2160618, |T| = 719983, |U| = 2144188, |V| = 496701$ and

$$\begin{aligned}
S^* &:= \prod_{p \in S} \frac{p}{p-1} > 1.82219345901032950583,\\
T^* &:= \prod_{p \in T} \frac{p}{p-1} > 1.19902263543776496408,\\
U^* &:= \prod_{p \in U} \frac{p}{p-1} > 1.43699138263382743310,\\
V^* &:= \prod_{p \in V} \frac{p}{p-1} > 1.03750936160818766647.
\end{aligned}$$

Proposition 2.5. *Assume that n is an odd perfect number whose largest prime factor is less than 10^8. Then the following facts hold.*

1. *The number n is divisible by at most two elements of S. If there is such an element s, then it is not the special prime of n, and $s \ge 47$.*

(2) *The number n is divisible by at most one element of T. If there is such an element t, then it is the special prime of n, and $t \geq 61$.*
(3) *The number n is divisible by at most one element of U. If there is such an element u, then it is the special prime of n, and $u \geq 73$.*
(4) *The number n is not divisible by any element of V.*

Proof. These facts can be proven similarly to the paper [8]. Here we show only (1) since it is slightly different from the original one. Suppose that $p \in S$ and $p \mid n$. Then p divides some cyclotomic number $\Phi_d(p_j)$ in equation (2.1). Assume that $d \neq 2$. By Lemma 2.4, d is divisible by 3 or 5, and hence $p \equiv 1 \pmod 3$ or $p \equiv 1 \pmod 5$ from Proposition 2.1 (1). This is a contradiction to $p \in S$. Therefore $d = 2$. Because of the definition of the special prime, p_j is the special prime and p is not. Since the smallest element of S is 47, it holds that $p \geq 47$. Since $p \mid \Phi_2(p_j)$ and the other cyclotomic numbers in (2.1) are not divisible by p, we have $p^2 \mid (p_j + 1)$. If there are three such p, then $p_j + 1 \geq 2 \cdot 47^2 \cdot 53^2 \cdot 59^2 > 10^8$, a contradiction to $p_j < 10^8$. □

We define $\sigma_{-1}(n)$ by

$$\sigma_{-1}(n) := \sum_{d|n} d^{-1} = \frac{\sigma(n)}{n}.$$

An integer n is perfect if and only if $\sigma_{-1}(n) = 2$. The function σ_{-1} is multiplicative, and for any positive integer e,

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

Assume again that $n = p_1^{e_1} \cdots p_k^{e_k}$ is an odd perfect number whose largest prime factor is less than 10^8. From Proposition 2.5, n is divisible by at most three elements of $S \cup T \cup U \cup V$. Since $x/(x-1)$ is monotone decreasing for $x > 1$, if $p_i \in S$, then $\sigma_{-1}(p_i^\infty) \leq 47/46$, and if $p_i \in T \cup U$, then $\sigma_{-1}(p_i^\infty) \leq 61/60$. Therefore it follows from Proposition 2.5 that

$$2 = \sigma_{-1}(n) < \prod_i \frac{p_i}{p_i - 1} \leq \frac{47}{46} \cdot \frac{53}{52} \cdot \frac{61}{60} \cdot \frac{P^*}{S^* T^* U^* V^*} < 1.5859314817,$$

a contradiction. The proof of Theorem 1.1 is completed.

3. Details on the search for acceptable values

From Proposition 2.1 (3), the cyclotomic number $\Phi_r(p)$ has a prime factor q such that $q \geq 2r + 1$, hence if $\Phi_r(p)$ is acceptable, then $r < 5 \cdot 10^7$. Therefore we need to check only finitely many cyclotomic numbers, however, it is hard to directly determine whether or not each number is acceptable because of difficulty of prime factorization. The key point of the proof of Lemma 2.2 is the following lemma. The notation $p^e \parallel n$ means that $p^e \mid n$ and $p^{e+1} \nmid n$.

Lemma 3.1. *If $p, q < 10^8$ and $6679 < r < 5 \cdot 10^7$, then $q^4 \nmid \Phi_r(p)$ for all primes q and $q^3 \parallel \Phi_r(p)$ for at most one prime q. In fact, $q^3 \nmid \Phi_r(p)$ except for*

$$28499^3 \parallel \Phi_{14249}(70081199),\ 60647^3 \parallel \Phi_{30323}(6392117),\ 63587^3 \parallel \Phi_{31793}(42326917).$$

In the rest of this section, we prove Lemma 2.2 using Lemma 3.1. In §4, we discuss our algorithm to show Lemma 3.1.

Lemma 3.2. *If* $10^2 < p < 10^8$ *and* $6679 < r < 5 \cdot 10^7$*, then* $\Phi_r(p)$ *is unacceptable.*

Proof. For a prime r, we define $Q(r)$ by

$$Q(r) = \prod_{\substack{q < 10^8 \\ q \equiv 1 \pmod{r}}} q.$$

Note that $r \cdot Q(r)$ is the product of all primes which may divide an acceptable cyclotomic number $\Phi_r(p)$ in view of Proposition 2.1. Therefore, if $\Phi_r(p)$ is acceptable and squarefree, then $\Phi_r(p) \le r \cdot Q(r)$. Under the assumption of this lemma, we have $\Phi_r(p) < 10^8 r \cdot Q(r)^2$ from Lemma 3.1.

We show that if $6679 < r < 5 \cdot 10^7$, then $10^8 r \cdot Q(r)^2 < 10^{2(r-1)}$. A direct computation showed that if $6679 < r < 5 \cdot 10^4$, then the required inequality holds. Suppose that $r \ge 5 \cdot 10^4$. If $q \equiv 1 \pmod{r}$, then $q = 2kr + 1$ with $k < 10^3$, hence we have $10^4\sqrt{r} \cdot Q(r) < (10^8)^{10^3+2} < 10^{10^4} < 10^{r-1}$. The square of this inequality is the required one.

Hence it follows that $\Phi_r(p) < 10^8 r \cdot Q(r)^2 < 10^{2(r-1)}$. On the other hand, we have $\Phi_r(p) > p^{r-1} > 10^{2(r-1)}$, a contradiction. □

Lemma 3.3. *If* $10^2 < p < 10^8$ *and* $4723 < r \le 6679$*, then* $\Phi_r(p)$ *is unacceptable.*

Proof. A direct computation showed that if $4723 < r \le 6679$, then $10^8 r \cdot Q(r) < 10^{2(r-1)}$. Another computer search showed that if $4723 < r \le 6679$, then $q^3 \nmid \Phi_r(p)$ for all primes q and $q^2 \parallel \Phi_r(p)$ for at most one prime q. Assume that $10^2 < p < 10^8, 4723 < r \le 6679$ and $\Phi_r(p)$ is acceptable. Then it follows that $10^{2(r-1)} < p^{r-1} < \Phi_r(p) < 10^8 r \cdot Q(r) < 10^{2(r-1)}$, a contradiction. □

Lemma 3.4. (1) *If* $10^6 < p < 10^8$ *and* $2707 < r \le 4723$*, then* $\Phi_r(p)$ *is unacceptable.* (2) *If* $10^7 < p < 10^8$ *and* $2503 < r \le 2707$*, then* $\Phi_r(p)$ *is unacceptable.*

Proof. A computer search showed that if $p, q < 10^8$ and $2503 < r \le 4723$, then $q^2 \mid \Phi_r(p)$ for at most one prime q, and $q^3 \nmid \Phi_r(p)$ except for

$$10709^3 \parallel \Phi_{2677}(6619441), \quad 5939^3 \parallel \Phi_{2969}(41492783), \quad 6719^3 \parallel \Phi_{3359}(59698039),$$
$$8147^3 \parallel \Phi_{4073}(41112823), \quad 8147^3 \parallel \Phi_{4073}(41728717).$$

(1) A direct computation showed that if $2707 < r \le 4723$, then $(10^8)^2 r \cdot Q(r) < 10^{6(r-1)}$. Hence if $10^6 < p < 10^8, 2707 < r \le 4723$ and $\Phi_r(p)$ is acceptable, then it follows that $10^{6(r-1)} < p^{r-1} < \Phi_r(p) < (10^8)^2 r \cdot Q(r) < 10^{6(r-1)}$, a contradiction.

(2) A direct computation showed that if $2503 < r \le 2707$, then $(10^8)^2 r \cdot Q(r) < 10^{7(r-1)}$. Hence if $10^7 < p < 10^8, 2503 < r \le 2707$ and $\Phi_r(p)$ is acceptable, then it follows that $10^{7(r-1)} < p^{r-1} < \Phi_r(p) < (10^8)^2 r \cdot Q(r) < 10^{7(r-1)}$, a contradiction. □

Suppose that $p < 10^2$ and $q^2 \mid \Phi_r(p)$. Proposition 2.1 (1), (2) imply that $r \mid (q-1)$, and we have $p^r \equiv 1 \pmod{q^2}$ by the argument in the proof of Proposition 4.1. Hence it follows that $p^{q-1} \equiv 1 \pmod{q^2}$. According to the table of Montgomery [16], all solutions of $p^{q-1} \equiv 1 \pmod{q^2}, 3 \le p < 10^2, q < 10^8$ are given by Table 1. From the table, if $p < 10^2$ and $3 \le r < 5 \cdot 10^7$, then $\Phi_r(p)$ is squarefree except for

$$11^2 \parallel \Phi_5(3),\ 48947^2 \parallel \Phi_{24473}(17),\ 47^2 \parallel \Phi_{23}(53),\ 59^2 \parallel \Phi_{29}(53),$$
$$7^2 \parallel \Phi_3(67),\ 47^2 \parallel \Phi_{23}(71),\ 7^2 \parallel \Phi_3(79),\ 4871^2 \parallel \Phi_{487}(83).$$

Table 1

p	q	p	q
3	11, 1006003	43	5, 103
5	20771, 40487, 53471161	47	none
7	5, 491531	53	3, 47, 59, 97
11	71	59	2777
13	863, 1747591	61	none
17	3, 46021, 48947	67	7, 47, 268573
19	3, 7, 13, 43, 137, 63061489	71	3, 47, 331
23	13, 2481757, 13703077	73	3
29	none	79	7, 263, 3037, 1012573, 60312841
31	7, 79, 6451, 2806861	83	4871, 13691
37	3, 77867	89	3, 13
41	29, 1025273	97	7, 2914393

Using a program based on Algorithm 2 in §4, we showed this fact again without Montgomery's table.

For a prime p, we define $R(p)$ by

$$R(p) = \min\{a \in \mathbb{N} \mid 10^8 r \cdot Q(r) < p^{r-1} \text{ if } r \geq a\}.$$

It immediately follows that $R(p) \leq 5 \cdot 10^4$. In fact, if $r \geq 5 \cdot 10^4$, then

$$10^8 r \cdot Q(r) < (10^8)^{10^3+2} < (3^{17})^{10^3+2} < 3^{r-1} \leq p^{r-1}.$$

By directly checking each $r < 5 \cdot 10^4$, we have Table 2.

Table 2

p	$R(p)$	p	$R(p)$	p	$R(p)$
3	9650	29	5508	61	4952
5	7950	31	5508	67	4890
7	7238	37	5310	71	4878
11	6548	41	5262	73	4878
13	6318	43	5262	79	4818
17	5954	47	5108	83	4788
19	5882	53	5060	89	4734
23	5660	59	4988	97	4724

Lemma 3.5. *If $3 \leq p < 10^2$ and $R(p) \leq r < 5 \cdot 10^7$, then $\Phi_r(p)$ is unacceptable.*

Proof. Assume that $\Phi_r(p)$ is acceptable. Since $q^2 \mid \Phi_r(p)$ for at most one prime q, it follows that $p^{r-1} < \Phi_r(p) < 10^8 r \cdot Q(r) < p^{r-1}$, a contradiction. □

For a completion of the proof of Lemma 2.2, we must check r given in Table 3 for each p. We can do this by a direct search.

Table 3

p	r
$3 \leq p < 10^2$	$r \leq R(p) - 1$
$10^2 < p < 10^6$	$r \leq 4723$
$10^6 < p < 10^7$	$r \leq 2707$
$10^7 < p < 10^8$	$r \leq 2503$

4. Improved algorithm

It is the hardest task to show Lemma 3.1. In general, we consider the algorithm to find all triplets of odd primes (p, q, r) satisfying $p, q < M, r \geq c$ and $q^3 \mid \Phi_r(p)$ for some given integers M, c. From Proposition 2.1, it is necessary that $r < M/2$ and $q \equiv 1 \pmod{2r}$. The algorithm made by Jenkins [13] is described by Algorithm 1.

Algorithm 1 (original algorithm)

```
for $r = c$ to $M/2$ do
  if $r$ is prime then
    $q \leftarrow 2r + 1$
    while $q < M$
      if $q$ is prime then
        for $p = 3$ to $M$ do
          if $p$ is prime and $q^3 \mid \Phi_r(p)$ then print $(p, q, r)$
        end for
      end if
      $q \leftarrow q + 2r$
    end while
  end if
end for
```

By this algorithm, we will check triplets (p, q, r) in the set

$$\{(p, q, r) \,|\, p, q, r \text{ are primes}, p, q < M, c \leq r < M/2, q \equiv 1 \ (\mathrm{mod}\, 2r)\}. \tag{4.2}$$

Our improved algorithm is based on the following proposition.

Proposition 4.1. *Suppose that $q \mid \Phi_r(p)$ and $q \equiv 1 \pmod{r}$. Let g be a generator of the cyclic group $(\mathbb{Z}/q^m\mathbb{Z})^\times$, and put $w = (q-1)/r$. Then $q^m \mid \Phi_r(p)$ if and only if p belongs to the subgroup $\langle g^{wq^{m-1}} \rangle$ of $(\mathbb{Z}/q^m\mathbb{Z})^\times$.*

Proof. Note that w is an integer since $q \equiv 1 \pmod{r}$. Assume that $p \equiv 1 \pmod{q}$. Then it follows that $\Phi_r(p) \equiv r \pmod{q}$, a contradiction. Hence $p \not\equiv 1 \pmod{q}$ and

$$\begin{aligned} q^m \mid \Phi_r(p) &\iff q^m \mid (p-1)\Phi_r(p) \\ &\iff p^r \equiv 1 \pmod{q^m} \\ &\iff \text{the order of } p \in (\mathbb{Z}/q^m\mathbb{Z})^\times \text{ is } r \\ &\iff p \in \langle g^{wq^{m-1}} \rangle, \end{aligned}$$

as required. □

Our program is described by Algorithm 2. In the algorithm, we use Proposition 4.1 with $m = 2$ instead of $m = 3$, since we would not like to deal with large numbers.

By the improved algorithm, we will check triplets (p, q, r) in the set

$$\{(p, q, r) \,|\, p, q, r \text{ are primes}, p, q < M, c \leq r < M/2, q \equiv 1 \ (\mathrm{mod}\, 2r), p \in \langle g^{q(q-1)/r} \rangle\},$$

which is a subset of the set given by (4.2). Note that if $c > \sqrt{M}/2$, then $q \geq 2r + 1 > \sqrt{M}$ and hence $q^2 > M$. Therefore there exists at most one prime $p < M$ satisfying $p \equiv (g^{q(q-1)/r})^i \pmod{q^2}$ for each i. In [4], we estimate the amount of the computation for the improved algorithm. In §5, we give some data for the effect of the improvement.

ALGORITHM 2 (improved algorithm)

```
for $r = c$ to $M/2$ do
  if $r$ is prime then
    $q \leftarrow 2r + 1$
    while $q < M$
      if $q$ is prime then
        $p \leftarrow 1$
        $g \leftarrow$ a generator of the cyclic group $(\mathbb{Z}/q^2\mathbb{Z})^\times$
        for $i = 1$ to $r$ do
          $p \leftarrow p \times (g^{q(q-1)/r}) \bmod q^2$
          if $p < M$, $p$ is prime and $q^3 \mid \Phi_r(p)$ then print $(p, q, r)$
        end for
      end if
      $q \leftarrow q + 2r$
    end while
  end if
end for
```

5. Concluding remarks

For the proof of Lemma 3.1, we used PARI/GP and a computer AlpherServer GS320 (CPU: Alpha21264, 731MHz) which belongs to Computing and Communications Center, Kyushu University. The computation needed about 26,000 hours for total CPU time. Since we used ten CPU's simultaneously, it took about four months. For the bound 10^7, the same computer needed 274 hours. Using our UBASIC program and a PC (CPU: Pentium4, 3GHz), we needed 42 hours. For the bound 10^6, we needed 11 hours using the original UBASIC program made by Jenkins, and needed 35 minutes using our UBASIC program. These data show how our improved algorithm is effective.

Our UBASIC program is faster than our PARI/GP program, however, we cannot use UBASIC on UNIX machines. The authors do not have enough Windows machines, so we mainly used PARI/GP to show Lemma 3.1 and used UBASIC for the other computations.

The inequality at the end of §2 is much stronger than is needed and the theorem could be proved by only S and U. The referee of the paper [8] also pointed out this fact. However, it is considered that the four sets are worth being mentioned as Hagis and Cohen claimed.

Iannucci [11], [12] showed that the second (resp. third) largest prime factor of an odd perfect number must exceed 10^4 (resp. 10^2). He used the bound 10^6 of the largest prime factor, hence the new bound 10^8 is possibly useful to raise the bounds of the second and third largest prime factor.

In order to raise the lower bound to 10^9, we need much CPU time or a better method. In the case of the bound 10^8, it was shown that if $\Phi_r(p)$ is acceptable, then $r \leq 47$. Is it possible to eliminate the possibility of $47 < r < 5 \cdot 10^7$ without hard computations? The authors consider that a hint is in the paper by Murty and Wong [17]. They showed that if the ABC conjecture is true, then largest prime factors of cyclotomic numbers are large enough in a sense.

References

[1] R. P. Brent, G. L. Cohen, H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp. **57** (1991), 857-868. MR1094940 (92c:11004)

[2] J. E. Z. Chein, *An Odd Perfect Number has a Least* 8 *Prime Factors*, Ph.D. thesis, Pennsylvania State Univ., 1979.

[3] Y. Chishiki, T. Goto and Y. Ohno, *On the largest prime divisor of an odd harmonic number*, Math. Comp. **76** (2007), 1577–1587.

[4] T. Goto and Y. Ohno, *Perfect numbers, cyclotomic numbers and ABC conjecture* (Japanese), Trans. Japan Soc. Indust. Appl. Math. **16** (2006), 187-195.

[5] P. Hagis, Jr. and W. L. McDaniel, *On the largest prime divisor of an odd perfect number*, Math. Comp. **27** (1973), 955–957. MR0325508 (48:3855)

[6] P. Hagis, Jr. and W. L. McDaniel, *On the largest prime divisor of an odd perfect number II*, Math. Comp. **29** (1975), 922–924. MR0371804 (51:8021)

[7] P. Hagis, Jr., *Outline of a proof that every odd perfect number has at least eight prime factors*, Math. Comp. **35** (1980), 1027–1032. MR572873 (81k:10004)

[8] P. Hagis, Jr. and G. L. Cohen, *Every odd perfect number has a prime factor which exceeds* 10^6, Math. Comp. **67** (1998), 1323–1330. MR1484897 (98k:11002)

[9] K. G. Hare, *More on the total number of prime factors of an odd perfect number*, Math. Comp. **74** (2005), 1003–1008. MR2114661 (2005h:11010)

[10] K. G. Hare, *New techniques for bounds on the total number of prime factors of an odd perfect number*, Math. Comp., to appear.

[11] D. E. Iannucci, *The second largest prime divisor of an odd perfect number exceeds ten thousand*, Math. Comp., **68** (1999), 1749–1760. MR1651761 (2000i:11200)

[12] D. E. Iannucci, *The third largest prime divisor of an odd perfect number exceeds one hundred*, Math. Comp., **69** (2000), 867–879. MR1651762 (2000i:11201)

[13] P. M. Jenkins, *Odd perfect numbers have a prime factor exceeding* 10^7, Senior Thesis, Brigham Young University, 2000.

[14] P. M. Jenkins, *Odd perfect numbers have a prime factor exceeding* 10^7, Math. Comp. **72** (2003), 1549–1554. MR1972752 (2004a:11002)

[15] H. J. Kanold, *Folgerungen aus dem Vorkommen einer Gauss'schen Primzahl in der Primfaktorenzerlegung einer ungeraden vollkommenen Zahl*, J. Reine Angew. Math. **186** (1944), 25–29. MR0012079 (6:255c)

[16] P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), 361–363. MR1182246 (94d:11003)

[17] M. R. Murty and S. Wong, *The ABC conjecture and prime divisors of the Lucas and Lehmer sequences*, Number Theory for the Millenium, III, (Urbana, IL, 2000), A. K. Peters, Natick, MA, 2002, 43–54. MR1956267 (2003k:11058)

[18] Pace P. Nielsen, *Odd perfect numbers have at least nine distinct prime factors*, Math. Comp., to appear.

[19] O. Ore, *On the averages of the divisors of a number*, Amer. Math. Monthly, **55** (1948), 615–619. MR0027292 (10:284a)

[20] H. N. Shapiro, *Introduction to the Theory of Numbers*, Wiley, New York, 1983. MR693458 (84f:10001)

Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, Noda, Chiba, 278-8510, Japan
E-mail address: goto_takeshi@ma.noda.tus.ac.jp

Department of Mathematics, Kinki University Higashi-Osaka, Osaka 577-8502, Japan
E-mail address: ohno@math.kindai.ac.jp