COLLOQUIUM MATHEMATICUM

VOL. 103 2005 NO. 2

ODD PERFECT NUMBERS OF A SPECIAL FORM

BY

TOMOHIRO YAMADA (Kyoto)

Abstract. We show that there is an effectively computable upper bound of odd perfect numbers whose Euler factors are powers of fixed exponent.

1. Introduction. We denote by $\sigma(N)$ the sum of divisors of N. We say that N is *perfect* if $\sigma(N) = 2N$. Though it is not known whether or not an odd perfect number exists, many conditions which must be satisfied by such a number are known. Suppose N is an odd perfect number. Euler has shown that $N = p^\alpha q_1^{2\beta_1} \cdots q_t^{2\beta_t}$ for distinct odd primes $p, q_1, \ldots, q_t$ with $p \equiv \alpha \equiv 1 \pmod 4$. Steuerwald [12] proved that we cannot have $\beta_1 = \cdots = \beta_t = 1$. McDaniel [8] proved that we cannot have $\beta_1 \equiv \cdots \equiv \beta_t \equiv 1 \pmod 3$. If $\beta_1 = \cdots = \beta_t = \beta$, then it is known that $\beta \neq 2$ (Kanold [6]), $\beta \neq 3$ (Hagis and McDaniel [5]), $\beta \neq 5, 12, 17, 24, 62$ (McDaniel and Hagis [9]), and $\beta \neq 6, 8, 11, 14, 18$ (Cohen and Williams [2]). In their paper [5], Hagis and McDaniel conjecture that $\beta_1 = \cdots = \beta_t = \beta$ does not occur. We have not been able to prove this conjecture. But we can prove that for any *fixed* β, all of the odd perfect numbers N can be effectively determined. Our result is as follows.

THEOREM 1.1. *Let $\beta \geq 1$. If $N = p^\alpha q_1^{2\beta} \cdots q_t^{2\beta}$ is an odd perfect number, then*

$$\omega(N) \leq 4\beta^2 + 2\beta + 3 \tag{1}$$

and

$$N \leq 2^{4^{4\beta^2+2\beta+3}}. \tag{2}$$

2. Lemmas. Let us denote by $v_p(n)$ the solution e of $p^e \parallel n$. For distinct primes p and q, we denote by $o_q(p)$ the exponent of p mod q and we define $a_q(p) = v_q(p^d - 1)$, where $d = o_q(p)$. Clearly $o_q(p)$ divides $q - 1$ and $a_q(p)$ is a positive integer. Now we quote some elementary properties of $v_q(\sigma(p^x))$. Lemmas 2.1 and 2.2 are well known. Lemma 2.1 follows from Theorems 94

2000 *Mathematics Subject Classification*: 11A05, 11A25.

Key words and phrases: odd perfect number.

and 95 in Nagell [10]. Lemma 2.2 has been proved by Zsigmondy [13] and rediscovered by many authors such as Dickson [4] and Kanold [7].

Lemma 2.1. *Let p, q be distinct primes with $q \neq 2$ and c be a positive integer. If $p \equiv 1 \pmod{q}$, then $v_q(\sigma(p^c)) = v_q(c+1)$. Moreover, if $p \not\equiv 1 \pmod{q}$, then $v_q(\sigma(p^c)) = a_q(p) + v_q(c+1)$ if $o_q(p) \mid (c+1)$ and $v_q(\sigma(p^c)) = 0$ otherwise.*

Lemma 2.2. *If $a > b \geq 1$ are coprime integers, then $a^n - b^n$ has a prime factor which does not divide $a^m - b^m$ for any $m < n$, unless $(a, b, n) = (2, 1, 6)$ or $a - b = n = 1$, or $n = 2$ and $a + b$ is a power of 2.*

By Lemma 2.2, we obtain the following lemmas.

Lemma 2.3. *Suppose p is a prime and n is a positive integer. If $d \mid (n+1)$, $d > 1$ and (p, d) satisfies neither $(p, d) = (2, 6)$ nor $(p, d) = (2^m - 1, 2)$ for some integer m, then there exists a prime q with $o_q(p) = d$ and $q \mid \sigma(p^n)$.*

Proof. We can apply Lemma 2.2 with $(a, b) = (p, 1)$ and we see that there exists a prime p such that $o_p(q) = d$. Furthermore, q does not divide $p - 1$ since $o_p(q) = d > 1$. On the other hand, q divides $p^{n+1} - 1$ since $1 < d \mid (n+1)$. Hence $q \mid \sigma(p^n)$. ∎

Lemma 2.4. *If p is a prime and n is a positive integer, then $\omega(\sigma(p^n)) \geq \tau(n+1) - 1$ unless $p = 2$ and $n \equiv 5 \pmod{6}$, or p is a Mersenne prime and n is odd.*

Proof. If $d \mid (n+1)$ and $d \neq 1$, then (p, n, d) satisfies the condition of Lemma 2.3. Hence $\sigma(p^n)$ has a prime factor q_d satisfying $o_p(q_d) = d$. Thus we have $\omega(\sigma(p^n)) \geq \#\{d : d \mid (n+1),\ d > 1\} = d(n+1) - 1$. ∎

The following is Lemma 2 of Danpat, Hunsucker and Pomerance [3].

Lemma 2.5. *If p, q are distinct primes with $q \neq 2$ satisfying $\sigma(q^x) = p^y$ for some positive integers x, y, then $p \equiv 1 \pmod{q}$ or $a_q(p) = 1$.*

From this lemma and Lemma 2.1, we immediately deduce the following result.

Lemma 2.6. *Let p, q be distinct primes satisfying the condition of Lemma 2.5 and $q^f \mid \sigma(p^e)$. Then $q^{f-1} o_q(p)$ divides $e + 1$.*

Proof. By Lemma 2.5, $p \equiv 1 \pmod{q}$ or $a_q(p) = 1$. If $p \equiv 1 \pmod{q}$, then $q^f \mid \sigma(p^e)$ implies $q^f = q^f o_q(p) \mid (e+1)$ by Lemma 2.1. If $a_q(p) = 1$, then $o_q(p) \mid (e+1)$ and $v_q(e+1) \geq f - a_q(p) = f - 1$ by Lemma 2.1. In both cases, $q^{f-1} o_q(p)$ divides $e + 1$. ∎

Moreover, we quote a result of Kanold [6].

LEMMA 2.7. *Let* $N = p^{\alpha} q_1^{2\beta_1} \cdots q_r^{2\beta_r}$ *be an odd perfect number and* l *be a common divisor of* $2\beta_1 + 1, \ldots, 2\beta_r + 1$. *Then* $l^4 \mid N$. *Moreover, if* l *is a power of a prime* q, *then* $p \neq q$.

3. Proof of Theorem 1.1. Let $N = p^{\alpha} q_1^{2\beta} \cdots q_r^{2\beta}$ be an odd perfect number.

First assume that $2\beta + 1 = l^{\gamma}$, where l is a prime and γ is a positive integer. Various results recalled in the Introduction allow us to assume that $\beta \geq 8$ without loss of generality.

By Lemma 2.7, $p \neq l$ and $l^{4\gamma}$ divides N. Hence $l = q_{i_0}$ for some i_0 and $v_l(N) = 2\beta$. We divide $q_1, \ldots, q_r$ into four disjoint sets. Let

$$S = \{i : q_i \equiv 1 \pmod{l}\},$$
$$T = \{i : q_i \not\equiv 1 \pmod{l},\ i \neq i_0,\ q_j \mid \sigma(q_i^{2\beta}) \text{ for some } 1 \leq j \leq r\},$$
$$U = \{i : q_i \not\equiv 1 \pmod{l},\ i \neq i_0,\ q_j \nmid \sigma(q_i^{2\beta}) \text{ for any } 1 \leq j \leq r\}.$$

Then $i \in S \cup T \cup U \cup \{i_0\}$ and thus we have

$$r \leq \#S + \#T + \#U + 1. \tag{3}$$

LEMMA 3.1.
$$\#S \leq 2\beta.$$

Proof. For $i \in S$, we have $l \mid \sigma(q_i^{2\beta})$ by Lemma 2.1. Hence

$$\#S \leq v_l\Big(\prod_{i \in S} \sigma(q_i^{2\beta})\Big) \leq v_l(2N) = v_l(N) = 2\beta. \ \blacksquare$$

LEMMA 3.2.
$$\#T \leq (2\beta)^2.$$

Proof. If $i \in T$, then $q_j \mid \sigma(q_i^{2\beta})$ for some $j \in S$. Hence $\sum_{j \in S} v_{q_j}(\sigma(q_i^{2\beta})) \geq 1$ for $i \in T$. By Lemma 3.1 we have

$$\begin{aligned}\#T &\leq \sum_{i \in T} \sum_{j \in S} v_{q_j}(\sigma(q_i^{2\beta})) = \sum_{j \in S} v_{q_j}\Big(\prod_{i \in T} \sigma(q_i^{2\beta})\Big) \\ &\leq \sum_{j \in S} v_{q_j}(2N) = \sum_{j \in S} v_{q_j}(N) \leq (2\beta)^2. \ \blacksquare\end{aligned}$$

LEMMA 3.3.
$$\#U \leq 1.$$

Proof. If $i \in U$ and q is a prime dividing $\sigma(q_i^{2\beta})$, then $q = p$ since $q \mid 2N$, $\sigma(q_i^{2\beta})$ is odd, and $q \neq q_j$ for any j. Thus $\sigma(q_i^{2\beta}) = p^{\zeta_i}$ for some positive integer ζ_i.

We shall show $q_i^{2\beta} \mid \sigma(p^{\alpha})$. If q_i divides $\sigma(q_j^{2\beta})$ for some j, then q_i divides $2\beta + 1 = l^{\gamma}$ or $1 < o_{q_i}(q_j) \mid (2\beta + 1) = l^{\gamma}$ by Lemma 2.1. The former case cannot occur since $q_i \neq q_{i_0} = l$. If $1 < o_{q_i}(q_j) \mid (2\beta + 1) = l^{\gamma}$, then $o_{q_i}(p) = l^t$

for some integer $t > 0$ and therefore $q_i \equiv 1 \pmod{l}$, which is inconsistent with the assumption $q_i \in U$. Since $q_i^{2\beta} \mid N \mid \sigma(N)$, we conclude that $q_i^{2\beta} \mid \sigma(p^\alpha)$.

We can apply Lemma 2.6 with $(q, f, e) = (q_i, 2\beta, \alpha)$ and deduce that $q_i^{2\beta-1}$ divides $(\alpha+1)/2$ since q_i is odd and $\alpha \equiv 1 \pmod{4}$. Hence $(\alpha+1)/2$ must be divisible by $\prod_{i\in U} q_i^{2\beta-1}$ and therefore $d(\alpha+1) \geq 2(2\beta)^{\#U}$. By Lemma 2.4, we have $\omega(\sigma(p^\alpha)) \geq 2(2\beta)^{\#U} - 1$.

On the other hand, we have $\omega(\sigma(p^\alpha)) \leq \omega(N)+1$ since $\sigma(p^\alpha) \mid 2N$. Thus, from Lemmas 3.1 and 3.2 we obtain

$$2(2\beta)^{\#U} - 1 \leq \omega(N) + 1 \leq \#S + \#T + \#U + 3 \leq \#U + (2\beta)^2 + 2\beta + 3.$$

Since $\#U \leq (2\beta)^{\#U-1} \leq (2\beta)^{\#U}/16$ by the assumption that $\beta \geq 8$, we have

$$\frac{31}{16}(2\beta)^{\#U} \leq 2(2\beta)^{\#U} - \#U \leq (2\beta)^2 + 2\beta + 4 \leq \frac{21}{16}(2\beta)^2, \tag{4}$$

and therefore $\#U \leq 1$. ∎

By Lemmas 3.1–3.3 and by (3), we have $\omega(N) \leq r + 1 \leq 4\beta^2 + 2\beta + 3$, which is the desired result.

Next we assume that $2\beta + 1 = l_1^{\gamma_1} l_2^{\gamma_2} \cdots l_s^{\gamma_s}$ with $s \geq 2$, where $l_1, \ldots, l_s$ are distinct primes. By Lemma 2.7, $l_i^{4\gamma_i}$ divides N for each i. This clearly implies that there are at least $s-1$ primes among the l_i's each of which is equal to q_j for some j. Hence we may assume that $l_i = q_i$ for $i = 1, \ldots, s-1$.

Let $S = \{i : q_i \equiv 1 \pmod{l_1}\}$. As in the prime-power case, we derive that $\#S \leq 2\beta$. By Lemma 2.4, each $\sigma(q_j^{2\beta})$ has at least one prime factor q with $o_q(q_j) = d$ for any $d > 1$ dividing $2\beta + 1$. If we denote by w the number of divisors of $2\beta+1$ divisible by l_1, then $w = \gamma_1(\gamma_2+1)\cdots(\gamma_s+1) \geq 2^{s-1}$. Thus each $\sigma(q_j^{2\beta})$ has at least $2^{s-1} - 1$ prime factors $\equiv 1 \pmod{l_1}$ and different from p, namely, belonging to S.

Hence we conclude that $r \leq 2\beta\#S/(2^{s-1} - 1) \leq (2\beta)^2$ and therefore $\omega(N) \leq 4\beta^2 + 1$, which is more than we desired. This completes the proof of the first part of Theorem 1.1.

To obtain the second part of our theorem it remains to apply the result of Nielsen [11], who has shown that $M \leq (d+1)^{4^l}$ for any positive integer n, d, M, l satisfying $\sigma(M)/M = n/d$ and $\omega(M) = l$.

REFERENCES

[1] A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math. 5 IV (1886), 70–80 and 130–137.

[2] G. L. Cohen and R. J. Williams, *Extensions of some results concerning odd perfect numbers*, Fibonacci Quart. 23 (1985), 70–76.

[3] G. G. Dandapat, J. L. Hunsucker and C. Pomerance, *Some new results on odd perfect numbers*, Pacific J. Math. 57 (1975), 359–364.

[4] L. E. Dickson, *On the cyclotomic functions*, Amer. Math. Monthly 12 (1905), 86–89.
[5] P. Hagis Jr. and W. L. McDaniel, *A new result concerning the structure of odd perfect numbers*, Proc. Amer. Math. Soc. 32 (1972), 13–15.
[6] H.-J. Kanold, *Untersuchungen über ungerade vollkommene Zahlen*, J. Reine Angew. Math. 183 (1941), 98–109.
[7] —, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme*, *I*, ibid. 187 (1950), 169–182.
[8] W. L. McDaniel, *The non-existence of odd perfect numbers of a certain form*, Arch. Math. (Basel) 21 (1970), 52–53.
[9] W. L. McDaniel and P. Hagis Jr., *Some results concerning the non-existence of odd perfect numbers of the form* $p^a M^{2\beta}$, Fibonacci Quart. 13 (1975), 25–28.
[10] T. Nagell, *Introduction to Number Theory*, 2nd ed., Chelsea, New York, 1964.
[11] P. P. Nielsen, *An upper bound for odd perfect numbers*, Integers 3 (2003), #A14.
[12] R. Steuerwald, *Verschärfung einer notwendigen Bedingung für die Existenz einen ungeraden vollkommenen Zahl*, Sitzungsber. Bayer. Akad. Wiss. Math.-Naturwiss. Abt. 1937, no. 2, 69–72.
[13] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Department of Mathematics
Faculty of Science
Kyoto University
Kyoto, 606-8502, Japan
E-mail: tyamada@math.kyoto-u.ac.jp

Received 30 November 2004;
revised 16 May 2005 (4537)