A NOTE ON ODD PERFECT NUMBERS

JOSE ARNALDO B. DRIS AND FLORIAN LUCA

Abstract. In this note, we show that if N is an odd perfect number and q^α is some prime power exactly dividing it, then $\sigma(N/q^\alpha)/q^\alpha > 5$. In general, we also show that if $\sigma(N/q^\alpha)/q^\alpha < K$, where K is any constant, then N is bounded by some function depending on K.

1. Introduction

For a positive integer N we write $\sigma(N)$ for the sum of the divisors of N. A number N is *perfect* if $\sigma(N) = 2N$. Even perfect numbers have been characterized by Euler. Namely, N is an even perfect number if and only if $N = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime. Hence, the only obstruction in proving that there are infinitely many of them lies with proving that there exist infinitely many primes of the form $2^p - 1$.

We know less about odd perfect numbers. No example has been found, nor do we have a proof that they don't exist. If they exist, then they must have at least 7 distinct prime factors, a result of Pomerance from [7]. The bound 7 has been raised to 9 recently in [5]. Brent et. al. [2] showed that $N > 10^{300}$. The exponent 300 has been raised to 1500 in the recent work [6].

Let N be perfect and let $q^\alpha \| N$, where q is prime. Recall that the notation $q^\alpha \| N$ stands for the power of q exactly dividing N, namely $q^\alpha \mid N$ but $q^{\alpha+1} \nmid N$. Then

$$2N = 2q^\alpha \left(\frac{N}{q^\alpha}\right) = \sigma(N) = \sigma(q^\alpha)\sigma\left(\frac{N}{q^\alpha}\right),$$

and since q^α is coprime to $\sigma(q^\alpha)$, it follows that $\sigma(N/q^\alpha)/q^\alpha$ is an integer divisor of $2N$. When $N = 2^{p-1}(2^p - 1)$ is even, then

$$\frac{\sigma(N/q^\alpha)}{q^\alpha} = \begin{cases} 2, & \text{if} \quad q = 2; \\ 1, & \text{if} \quad q = 2^p - 1. \end{cases}$$

Here, we study this statistic when N is an odd perfect number. We prove the following theorem.

Theorem 1.1. *If N is an odd perfect number and $q^\alpha \| N$ is a prime power exactly dividing N, then $\sigma(N/q^\alpha)/q^\alpha > 5$.*

This improves on a previous lower bound obtained by the first author in his M. S. thesis [3].

The lower bound 5 can likely be easily improved although it is not clear to us what the current numerical limit of this improvement should be. We leave this as a problem for other researchers. In light of the above result, one may ask whether it could be the case that by imposing an upper bound on the amount $\sigma(N/q^\alpha)/q^\alpha$, the number N ends up being bounded as well. This is indeed so as shown by the following result.

Theorem 1.2. *For every fixed $K > 5$, there are only finitely many odd perfect numbers N such that for some prime power $q^\alpha \| N$ we have that $\sigma(N/q^\alpha)/q^\alpha < K$. All such N are bounded by some effectively computable number depending on K.*

The proof of Theorem 1.1 is elementary. The proof of Theorem 1.2 uses the arguments from the proof of the particular case Theorem 1.1 together with two more ingredients. The first ingredient is a result of Heath–Brown [4] to the effect that an odd perfect number N with s distinct prime factors cannot exceed $4^{4^{s+1}}$. The second ingredient is a well-known result from the theory of Exponential Diophantine Equations (for the main results in this area, see [8]) regarding the largest prime factor of $f(n)$ for large n, where $f(X) \in \mathbb{Z}[X]$ is a polynomial with at least two distinct roots.

One of the main tools for the proof of both Theorems 1.1 and 1.2 is the following result due to Bang (see [1]).

Lemma 1.3. *Let $a > 1$ be an integer. For all $n \geq 7$, there is a prime factor p of $a^n - 1$ which does not divide $a^m - 1$ for any $1 \leq m < n$. Moreover, such a prime p is congruent to 1 modulo n.*

Throughout the paper, we use p, q, r, P and Q with or without subscripts for prime numbers.

2. Preliminaries

Let $N = p_1^{\lambda_1} \cdots p_s^{\lambda_s} q^{\alpha}$, where the primes $p_1, \ldots, p_s$, q are distinct and not necessarily ordered increasingly. We write

$$\sigma(p_i^{\lambda_i}) = m_i q^{\beta_i}, \quad i = 1, \ldots, k, \quad \text{and} \qquad \sigma(p_i^{\lambda_i}) = q^{\beta_i}, \qquad i = k+1, \ldots, s, \tag{2.1}$$

where $m_i \geq 2$ for $i = 1, \ldots, k$, and $\alpha = \beta_1 + \cdots + \beta_s$. For both proofs of Theorem 1.1 and 1.2 we will need facts about equations (2.1) for some i either in $\{1, \ldots, k\}$ and with a fixed value of $m_i \geq 2$, or with $i \in \{k+1, \ldots, s\}$. Observe that λ_i is even for all $i = k+1, \ldots, s$, and λ_i is even for at most one $i \in \{1, \ldots, k\}$.

We treat first the case of a fixed $m_i \geq 2$. For simplicity, let $p := p_i$, $\beta := \beta_i$, $m := m_i$, and $\lambda := \lambda_i$ for some $i = 1, \ldots, k$. Then the first equation (2.1) for the index i is

$$\frac{p^{\lambda+1} - 1}{p - 1} = m q^{\beta}. \tag{2.2}$$

Here, p and q are odd. We prove the following lemma.

Lemma 2.1. *In equation (2.2), we have $\lambda + 1 \leq m^2$.*

Proof. For a positive integer n coprime to p let $\ell_p(n)$ be the multiplicative order of p modulo n. Let $u_n := (p^n - 1)/(p - 1)$. Then m divides $u_{\lambda+1}$. It is then well-known that $\lambda + 1$ is divisible by the number $z_p(m)$ defined as

$$z_p(m) := \operatorname{lcm}[z_p(r^{\delta}),\ r^{\delta} \| m],$$

where

$$z_p(r^{\delta}) = \begin{cases} r^{\delta} & \text{if } p \equiv 1 \pmod{r}, \\ \ell_p(r^{\delta}) & \text{otherwise.} \end{cases}$$

Clearly, $2 \leq z_p(m) \leq m$. Equality is achieved if and only if each prime factor of m is also a prime factor of $p - 1$. Assume that $\lambda + 1 > m^2$. Write $\lambda + 1 = z_p(m) d$, where $d > z_p(m)$. We look at $u_d = (p^d - 1)/(p - 1)$ which is a divisor of $m q^{\beta}$. If $d \geq 7$, then by Lemma 1.3 there is a prime factor P of u_d which does not divide $u_{z_p(m)}$. Since all prime factors of m divide $u_{z_p(m)}$, we must have that $P = q$. But then all prime factors of $u_{\lambda+1}$ divide either q; hence, u_d, or m; hence $u_{z_p(m)}$, contradicting Lemma 1.3. So, we have a contradiction if $d \geq 7$.

Thus, all prime factors of u_d are among the prime factors of $u_{z_p(m)}$ and so $d \le 6$. In particular, the prime factors of d must be among the prime factors of $z_p(m)$, for otherwise, namely if there is some prime factor Q of d which does not divide $z_p(m)$, then $u_Q = (p^Q - 1)/(p-1)$ is a divisor of $u_d = (p^d - 1)/(p-1)$ which is coprime to $u_{z_p(m)}$, a multiple of m, which in turn is false. Thus, all prime factors of d are indeed among the prime factors of $z_p(m)$, and since $d > z_p(m)$, there is a prime factor Q of d which appears in the factorization of d with an exponent larger than the exponent with which it appears in the factorization of $z_p(m)$. Hence, $d \ge Q^2$, and since $d \le 6$, we get that $Q = 2$. This implies that $u_{\lambda+1}$ is a multiple of u_4; hence, a multiple of 4, which is false. This shows that indeed $\lambda + 1 \le m^2$. $\square$

We next treat the case of $i \in \{k+1, \ldots, s\}$.

Lemma 2.2. *The equations*

$$\frac{p^{\lambda+1} - 1}{p - 1} = q^{\beta} \qquad \textit{and} \qquad p^{\lambda} \mid \frac{q^{\alpha+1} - 1}{q - 1} \tag{2.3}$$

imply that $\alpha + 1$ *is a multiple of* $p^{\lambda-1}$.

Proof. The left equation in (2.3) is

$$p^{\lambda} + \cdots + p^2 + p = q^{\beta} - 1,$$

showing that $p \| q^{\beta} - 1$. This implies easily that $p \| q^{\ell_q(p)} - 1$. Now the conclusion follows immediately from the divisibility relation from the right-hand side of equation (2.3). $\square$

Let $m := m_1 \cdots m_k$. We let $M := \prod_{i=k+1}^{s} p_i^{\lambda_i}$. We label the numbers $\lambda_1, \ldots, \lambda_k$ such that $\beta_1 \le \beta_2 \le \cdots \le \beta_k$. Applying Lemma 2.2 for $i = k+1, \ldots, s$, we get that

$$\alpha + 1 \ge \prod_{i=2}^{s} p_i^{\alpha_i - 1} \ge \prod_{i=2}^{s} p_i^{\alpha_i/2} = M^{1/2}. \tag{2.4}$$

Let $\Lambda := \mathrm{lcm}[\lambda_i + 1 : i = 1, \ldots, k]$. Then $\Lambda \le \prod_{i=1}^{k} m_i^2 = m^2$. Observe that $p_i^{\lambda_i} \equiv 1 \pmod{q^{\beta_i}}$ for $i = 1, \ldots, k$. In particular,

$$p_i^{\Lambda} \equiv 1 \pmod{q^{\beta_i}} \qquad \text{for all} \quad i = 1, \ldots, k. \tag{2.5}$$

Lemma 2.3. *One of the following holds:*

(i) $q \mid m$;
(ii) $q^{\beta_i} < (2Mqm)^{(m^2+1)^i}$ *for* $i = 1, \ldots, k$.

Proof. If $q \mid m$, we are through. So suppose that $q \nmid m$. We write

$$\frac{q^{\alpha+1} - 1}{q - 1} = \sigma(q^{\alpha}) = \left(\frac{2M}{m}\right) p_1^{\lambda_1} \cdots p_k^{\lambda_k}.$$

We raise the above equation to the power Λ and use congruences (2.5) obtaining

$$\left(\frac{-1}{q-1}\right)^{\Lambda} \equiv \left(\frac{2M}{m}\right)^{\Lambda} \pmod{q^{\beta_1}}.$$

Hence, $q^{\beta_1} \mid (2M(q-1))^{\Lambda} \pm m^{\Lambda}$. The last expression is nonzero, since if it were zero, we would get $2M(q-1) = m$, which is impossible because $2M(q-1)$ is a multiple of 4, whereas m is a divisor of $2N$, so it is not a multiple of 4. Thus,

$$q^{\beta_1} \le (2M(q-1))^{\Lambda} + m^{\Lambda} < (2M(q-1) + m)^{\Lambda} < (2Mqm)^{\Lambda} < (2Mqm)^{m^2}.$$

This takes care of the case $i = 1$ of (ii). For the case of a general i in (ii), suppose, by induction, that $i \geq 2$ and that we have proved that

$$q_j^{\beta_j} < (2Mqm)^{(m^2+1)^j} \quad \text{holds for all} \quad j = 1, \ldots, i-1.$$

Then $p_j^{\lambda_j} < \sigma(p_j^{\lambda_j}) = m_j q^{\beta_j}$ for $j = 1, \ldots, i-1$. Thus,

$$\frac{q^{\alpha+1}-1}{q-1} = \left(\frac{2Mp_1^{\lambda_1} \cdots p_{i-1}^{\lambda_{i-1}}}{m}\right) p_i^{\lambda_i} \cdots p_k^{\lambda_k}. \tag{2.6}$$

We raise congruence (2.6) to the power Λ and reduce it modulo q^{β_i} obtaining

$$q_i^{\beta_i} \mid (2M(q-1)p_1^{\lambda_1} \cdots p_{i-1}^{\lambda_{i-1}})^{\Lambda} \pm m^{\Lambda}.$$

The last expression above is not zero since $2M(q-1)p_1^{\lambda_1} \cdots p_{i-1}^{\lambda_{i-1}}$ is a multiple of 4 and m is not. Hence,

$$\begin{aligned} q^{\beta_i} &\leq (2M(q-1)p_1^{\lambda_1} \cdots p_{i-1}{}^{\lambda_{i-1}})^{\Lambda} + m^{\Lambda} \\ &\leq m^{\Lambda}((2M(q-1)^{\Lambda}+1)(q^{\beta_1} \cdots q_{i-1}{}^{\beta_{i-1}})^{\Lambda} \\ &\leq (2qMm)^{\Lambda} q^{\Lambda(\beta_1+\cdots+\beta_{i-1})} \\ &< (2qMm)^{m^2(1+(m^2+1)+\cdots+(m^2+1)^{i-1})} \\ &< (2qMm)^{(m^2+1)^i}, \end{aligned}$$

which is what we wanted to prove. □

3. The Proof of Theorem 1.1

Since $m \leq 5$ and at most one of the m_i's is even for $i = 1, \ldots, k$, we get that $k \leq 1$. Then Lemma 2.3 shows that either $q \leq 5$, or

$$q^{\beta_i} \leq (20Mq)^{25^i} \qquad \text{for all } i = 1, \ldots, k. \tag{3.1}$$

Assume that $q > 5$. Then

$$\begin{aligned} q^{\sqrt{M}-1} \leq q^{\alpha} = \left(\frac{2M}{m}\right) p_1^{\lambda_1} \cdots p_k^{\lambda_k} &< 2Mq^{\beta_1+\cdots+\beta_k} \\ &< 2M(20qM)^{25} < (20qM)^{26}, \end{aligned}$$

leading to

$$3^{\sqrt{M}-27} \leq q^{\sqrt{M}-27} < (20M)^{26},$$

which implies that $M < 2 \times 10^5$. Since $s \geq 8$ and $k \leq 1$, there exists $j \in \{k+1, \ldots, s\}$ such that $p_j^{\beta_j} < M^{1/7} \leq 6$. This is false because $p_j^{\beta_j} \geq 3^2 = 9$. Thus, $q \in \{3, 5\}$.

The equation from the right-hand side of (2.1) with $p := p_2$, $\lambda := \lambda_2$ and $\beta := \beta_2$ becomes

$$\frac{p^{\lambda+1}-1}{p-1} = q^{\beta}.$$

Observe that $\lambda + 1$ is odd. If $\lambda + 1 \geq 7$, we get a contradiction from Lemma 1.3 because $q \leq 5$. Thus, $\lambda \in \{2, 4\}$ and we get one of the four equations

$$\begin{aligned} p^2 + p + 1 = 3^{\beta}, &\qquad p^4 + p^3 + p^2 + p + 1 = 3^{\beta}, \\ p^2 + p + 1 = 5^{\beta}, &\qquad p^4 + p^3 + p^2 + p + 1 = 25^{\beta}. \end{aligned}$$

Arguments modulo 9 and 25 show first that the exponents β from the above equations are in $\{0,1\}$, which immediately implies that none of the above equations has in fact any solutions.

4. The Proof of Theorem 1.2

Here, we have $m = m_1 \cdots m_k \le K$, so $m \le K$ and $k \le (\log K)/(\log 2)$. Heath–Brown proved that $N < 4^{4^{s+1}}$ (see [4]). Hence, we may assume that $s > k$. Then $M \ge 2^{s-k}$. Now the argument from the proof of Theorem 1.1 shows that either $q \le K$, or

$$q^{\sqrt{M}-1} \le q^{\alpha} < \sigma(q^{\alpha}) < 2Mq^{\beta_1+\cdots+\beta_k} < (2KMq)^{(K^2+1)^{k+1}}.$$

In the second case, we get that M is bounded, hence s is bounded, so N is bounded by Heath-Brown's result.

In the first case, Lemma 1.3 shows that in equations appearing in the right-hand side of equations (2.1), the numbers $\lambda_i + 1$ are bounded for $i = k+1, \ldots, s$. Let Γ be a bound for λ_i for $i = k+1, \ldots, s$. For each $\lambda \in \{2, \ldots, \Gamma\}$ and fixed value of $q \le K$, equation

$$\frac{p^{\lambda+1}-1}{p-1} = p^{\lambda} + p^{\lambda-1} + \cdots + p + 1 = q^{\beta}$$

in the unknowns p and β have only finitely many effectively computable solutions (p, β). Indeed, this follows because if we write $P(t)$ for the largest prime factor of the positive integer t, then it is known that if $f(X) \in \mathbb{Z}[X]$ is a polynomial with at least two distinct roots, then $P(f(n))$ tends to infinity with n in an effective way. Now we only have to invoke this result for the polynomial $f(X) = (X^{\lambda+1}-1)/(X-1)$ whose $\lambda \ge 2$ roots are all distinct, and for the equation $P(f(p)) = q \le K$. Thus, all primes $p_{k+1}, \ldots, p_s$ are bounded, and therefore so is their number $s - k$. Hence, s is bounded, therefore N is bounded by Heath–Brown's result.

Acknowledgements

The authors thank Luis Gallardo for correcting an error in an earlier version of the paper. F. L. thanks Professor Arnold Knopfmacher for useful advice. This paper was written while F. L. was in sabbatical from the Mathematical Institute UNAM from January 1 to June 30, 2011 and supported by a PASPA fellowship from DGAPA.

References

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

[2] 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), 857–868.

[3] J. A. B. Dris, *Solving the odd perfect number problem: some old and new approaches*, M. S. Math thesis, De La Salle University, Manila, Philippines, 2008.

[4] D. R. Heath–Brown, *Odd perfect numbers*, Math. Proc. Cambridge Philos. Soc., **115** (1994), 191–196.

[5] P. P. Nielsen, *Odd perfect numbers have at least nine prime factors*, Math. Comp., **76** (2007), 2109–2126.

[6] P. Ochem and M. Rao, *Odd perfect numbers are greater than* 10^{1500}, Math. Comp., **81** (279), 1869–1877.

[7] C. Pomerance, *Odd perfect numbers are divisible by at least 7 primes*, Acta Arith., **25** (1974), 265–300.

[8] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

MSC2010: 11A25.

Far Eastern University, Manila, Philippines
E-mail address: `jadris@feu.edu.ph or josearnaldobdris@gmail.com`

School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa
E-mail address: `florian.luca@wits.ac.za`