Bull. Korean Math. Soc. **50** (2013), No. 6, pp. 1981–1988
http://dx.doi.org/10.4134/BKMS.2013.50.6.1981

GENERALIZED CULLEN NUMBERS WITH THE LEHMER PROPERTY

Dae-June Kim and Byeong-Kweon Oh

Abstract. We say a positive integer n satisfies the Lehmer property if $\phi(n)$ divides $n-1$, where $\phi(n)$ is the Euler's totient function. Clearly, every prime satisfies the Lehmer property. No composite integer satisfying the Lehmer property is known. In this article, we show that every composite integer of the form $D_{p,n} = np^n + 1$, for a prime p and a positive integer n, or of the form $\alpha 2^\beta + 1$ for $\alpha \le \beta$ does not satisfy the Lehmer property.

1. Introduction

A composite integer n is called a *Lehmer number* if $\phi(n)$ divides $n-1$, where $\phi(n)$ is the Euler's totient function. Hence every Lehmer number is a Carmichael number and it is a product of distinct odd primes. In 1932 Lehmer proved in [5] that every Lehmer number is a product of at least 7 distinct odd primes and asked whether or not a Lehmer number exists. In 1980 Cohen and Hagis [2] extended Lehmer's result in such a way that every Lehmer number is a product of at least 14 distinct odd primes. At present no Lehmer number is known. Recently it was proved that certain sequences of integers such as the Fibonacci sequence do not contain a Lehmer number (see, for example, [1], [6]).

An integer of the form $C_n = n2^n + 1$ for some integer n is called a *Cullen number*. Though Hooley proved in [4] that almost all Cullen numbers are composite in some sense, it is conjectured that there are infinitely many prime Cullen numbers. Recently, Grau Ribas and Luca proved in [3] that every Cullen number is not a Lehmer number. Motivated their proof, we prove that there does not exist a Lehmer number of the form $D_{p,n} := np^n + 1$, where n is an arbitrary integer and p is prime. Also we show that an integer of the form $\alpha 2^\beta + 1$ for $\alpha \le \beta$ is not a Lehmer number, where α is an odd integer.

Received August 24, 2012; Revised April 9, 2013.
2010 *Mathematics Subject Classification.* 11A05, 11N25.
Key words and phrases. Euler's totient function, generalized Cullen number, Lehmer property.
This work was supported by the Korea Foundation for the Advancement of Science & Creativity(KOFAC), and funded by the Korean Government(MEST).

2. Generalized Cullen numbers with the Lehmer property

We say an integer n satisfies the Lehmer property if $\phi(n)$ divides $n-1$. Clearly every prime satisfies the Lehmer property, and a Lehmer number is a composite integer satisfying the Lehmer property. An integer of the form $D_{p,n} := np^n + 1$ is called a generalized Cullen number, where n and p are positive integers. In this section we show that every generalized Cullen number satisfying the Lehmer property is prime, where p is an odd prime. Assume that $\phi(D_{p,n})$ divides $D_{p,n} - 1 = np^n$. Then we have $D_{p,n} = \prod_{i=1}^{k} p_i$, where p_i's are distinct odd primes. Since $k \geq 14$ by [2], the integer n is divisible by 2^{14}.

Lemma 2.1. *With the above notations, we have*

$$\min\left(\frac{n^{1/2}}{s_{p,n}}, 1 + \frac{2n^{1/2}}{3s_{p,n}}\right) < k < 1.45 \log n,$$

where $s_{p,n} = (3.005 + 2/\log p)(\log n)^{1/2}$.

Proof. Though the proof of this lemma is quite similar to that of Section 2 of [3], we provide the proof in detail for reader's convenience.[1]

Assume that $n = p^\alpha n_1$ $(p \nmid n_1)$. Then $D_{p,n} = n_1 p^{n_2} + 1 = \prod_{i=1}^{k} p_i$ where $n_2 = \alpha + n$. Let $q = p_i$ be a prime factor of $D_{p,n}$. Since $q - 1 | D_{p,n} - 1 = n_1 p^{n_2}$, we may write $q = m_q p^{n_q} + 1$, where m_q is an even factor of n_1.

First, we show the inequality in the right hand side holds. Since $\prod_{q|D_{p,n}} m_q$ divides n and $m_q \geq 2$, the number of prime factors of $D_{p,n}$ is at most $\frac{\log n}{\log 2}$. Therefore we have $k \leq \frac{\log n}{\log 2} < 1.45 \log n$.

Now we prove the inequality in the left hand side. First, suppose that $n_q > n$. If we write $D_{p,n} = q\lambda$, then we have

$$\lambda = \frac{D_{p,n}}{q} \leq \frac{np^n + 1}{p^{n+1} + 1} < n.$$

Furthermore, since

$$D_{p,n} = q\lambda = np^n + 1 \equiv 1 \equiv (m_q p^{n_q} + 1)\lambda \equiv \lambda \pmod{p^n},$$

the integer $\lambda - 1$ is divisible by p^n, which is a contradiction. Therefore we have $n_q \leq n$.

For an integer $N = \lfloor \sqrt{\frac{n}{\log n}} \rfloor$, consider all pairs (a, b) of integers such that $0 \leq a, b \leq N$. Clearly, the number of such pairs (a, b) is $(N+1)^2 > \frac{n}{\log n}$. For each pair (a, b), define $L(a, b) := an + bn_q$. Since $0 \leq L(a, b) \leq \frac{2n^{3/2}}{(\log n)^{1/2}}$ for each possible pair (a, b), there exist two pairs $(a, b) \neq (a_1, b_1)$ such that

$$|(a-a_1)n + (b-b_1)n_q| = |L(a,b) - L(a_1,b_1)| \leq \frac{2n^{3/2}/(\log n)^{1/2}}{n/\log n - 1} < 3(n \log n)^{1/2}.$$

[1] Some part of the proof in Section 2 of [3] is not correct. Professor Luca kindly sent an erratum to the first author.

If we define $u = a - a_1, v = b - b_1$, then $(u, v) \neq (0, 0)$ and $|un + vn_q| < 3(n \log n)^{1/2}$. Furthermore we may assume that $\gcd(u, v) = 1$ and $u \geq 0$ by changing (u, v) suitably.

Since

$$np^n \equiv -1 \pmod{q} \qquad \text{and} \qquad m_q p^{n_q} \equiv -1 \pmod{q},$$

we have $n^u m_q^v p^{nu+n_q v} \equiv (-1)^{u+v} (\text{mod } q)$. Now we define

$$A_q := n^u m_q^v p^{nu+n_q v} - (-1)^{u+v} = n_1^u m_q^v p^{(n+\alpha)u+n_q v} - (-1)^{u+v}.$$

First, suppose that $A_q = n_1^u m_q^v p^{(n+\alpha)u+n_q v} - (-1)^{u+v} = 0$. Then we have

$$n_1^u m_q^v = 1, \quad (n+\alpha)u + n_q v = 0 \;\text{ and }\; u + v \equiv 0 \pmod{2}.$$

Therefore there exists a positive integer ρ such that $n_1 = \rho^{-v}$, $m_q = \rho^u$. Since u, v are relatively prime and $u+v$ is even, both u and v are odd. Since $m_q | n_1$, we have $u \leq -v$. Furthermore since $(p^\alpha \rho^{-v} + \alpha)u + n_q v = 0$, n_q is divisible by u. Thus $q = m_q p^{n_q} + 1 = \rho^u p^{n_q} + 1 = X^u + 1$, where $X = \rho p^{n_q/u}$ is an integer. If $u > 1$, then $q = X^u + 1$ has a divisor $X + 1$, which is a contradiction. Thus $u = 1$. If $v = -1$, then $m_q = n_1 = \rho$ and $n_q = p^\alpha \rho + \alpha = n + \alpha$. This implies that $q = D_{p,n}$, which is a contradiction to the assumption that $D_{p,n}$ is a composite number. Thus $v \leq -3$, $n_1 = \rho^{-v}$ and $q = \rho p^{-(\alpha+n)/v} + 1 = (np^n)^{-1/v} + 1$.

Now we will show that there is at most one prime factor q of $D_{p,n}$ satisfying the above properties. To show this, assume that q_1, q_2 are such prime factors. Let $q_i = (np^n)^{1/w_i} + 1$ for each $i = 1, 2$ and without loss of generality, assume that $w_1 < w_2$. Note that $n_1 = \rho_i^{w_i}$ and $w_i \mid (n + \alpha)$ for each $i = 1, 2$. If we define $W := \operatorname{lcm}(w_1, w_2)$, then there exists a ρ_0 such that $n_1 = \rho_0^W$. If we write $W = w_1 \lambda$ for some positive odd integer λ, then $\rho_0^\lambda = \rho_1$. Thus $q_1 = \rho_1 p^{(\alpha+n)/w_1} + 1 = Y^\lambda + 1$, where $Y = \rho_0 p^{(\alpha+n)/W}$. This is a contradiction for the prime $q_1 = Y^\lambda + 1$ has a divisor $Y + 1$. Thus there is at most one prime factor q of $D_{p,n}$ such that $A_q = 0$. Furthermore such a prime exists, then $n_1 = \rho^w$ for some $w \geq 3$ and $q = (np^n)^{1/w} + 1 \leq (np^n)^{1/3} + 1$.

If $A_q \neq 0$, then we have

$$\begin{aligned} q &\leq \text{numerator of } A_q \leq p^{1+|nu+n_q v|} n^u m_q^{|v|} \\ &\leq p^{1+3(n \log n)^{1/2}} n^{2(n/\log n)^{1/2}} < p^{1+3(n \log n)^{1/2} + (2/\log p)(n \log n)^{1/2}} \\ &< p^{(3.005+2/\log p)(n \log n)^{1/2}} = p^{s_{p,n} n^{1/2}}. \end{aligned}$$

Note that since n is divisible by 2^{14}, $1 < 0.005(n \log n)^{1/2}$. Therefore if $A_q \neq 0$ for every prime factor q of $D_{p,n}$, then

$$p^n \leq D_{p,n} = \prod_{i=1}^{k} p_i < \prod_{i=1}^{k} p^{s_{p,n} n^{1/2}} = p^{k(s_{p,n} n^{1/2})},$$

which implies that $k > \frac{n^{1/2}}{s_{p,n}}$. Suppose that there exists a prime factor q' of $D_{p,n}$ such that $A_{q'} = 0$. Since $q' \le (np^n)^{1/3} + 1$, we have

$$p^{2n/3} < \frac{np^n}{(np^n)^{1/3} + 1} < \frac{D_{p,n}}{q'} < \prod_{\substack{1 \le i \le k \\ p_i \ne q'}} p^{s_{p,n} n^{1/2}} \le p^{(k-1)s_{p,n} n^{1/2}},$$

which implies that $k > 1 + \frac{2n^{1/2}}{3s_{p,n}}$. Therefore we have

$$k > \min\left(\frac{n^{1/2}}{s_{p,n}}, 1 + \frac{2n^{1/2}}{3s_{p,n}}\right),$$

which is the desired result. □

Lemma 2.2. *Let p be an odd prime. If $D_{p,n}$ satisfies the Lehmer property, then $n = 2^m$ for some integer m greater than* 13.

Proof. Assume that $D_{p,n} = \prod_{i=1}^{k} p_i$, where p_i's are distinct odd primes. Since $\phi(D_{p,n}) = \prod_{i=1}^{k}(p_i - 1)$ divides $D_{p,n} - 1 = np^n$, we may write $p_i = m_i p^{n_i} + 1$, where $\prod_{i=1}^{k} m_i$ divides n and is relatively prime to p. We assume that $m_i \ge m_j$ if and only if $i \le j$.

Since $3.005 + 2/\log p < 4.83$, we have

$$\min\left(\frac{n^{1/2}}{4.83(\log n)^{1/2}}, 1 + \frac{n^{1/2}}{7.25(\log n)^{1/2}}\right) < k < 1.45 \log n.$$

Therefore we may assume that $n < 180,000$. Suppose that n is divisible by an odd prime q. Since

$$k < 1 + \frac{\log(n/q)}{\log 2} \le 1 + \frac{\log(180,000/3)}{\log 2} < 16.9,$$

we have $k \le 16$. Furthermore since

$$\min\left(\frac{n^{1/2}}{4.83(\log n)^{1/2}}, 1 + \frac{n^{1/2}}{7.25(\log n)^{1/2}}\right) < 16,$$

we have $n < 150,000$. Consequently $14 \le k \le 16$.

Since other cases can be done in a similar manner, we only provide the proof of the case when $k = 14$. From the inequality

$$\min\left(\frac{n^{1/2}}{4.83(\log n)^{1/2}}, 1 + \frac{n^{1/2}}{7.25(\log n)^{1/2}}\right) < 14,$$

we have $n < 110,000$. Furthermore since n is divisible by 2^{14}, the integer n is of the form $n = 2^{14} \times 3, 2^{15} \times 3$ or $2^{14} \times 5$.

Assume that $n = 2^{14} \times 3$. Since $\prod_{i=1}^{14} m_i \mid n = 2^{14} \times 3$ and m_i is even for any $1 \le i \le 14$, $m_i = 2$ or 6. Thus p_i is of the form $2p^{\alpha} + 1$ or $6p^{\alpha} + 1$.

Moreover there is at most one i such that p_i is of the form of $6p^\alpha+1$. Assume that $p_1 < p_2 < \cdots < p_{14}$. Then from the above observation, we have

$$p_1, p_2 \geq 7, \quad p_3, p_4 \geq 19, \quad p_5, p_6 \geq 163, \quad p_7, p_8 \geq 487,$$
$$p_9, p_{10} \geq 1459, \quad p_{11}, p_{12} \geq 13123 \quad \text{and} \quad p_{13}, p_{14} \geq 39367.$$

From this follows

$$2 \leq \frac{D_{p,n}-1}{\phi(D_{p,n})} = \prod_{i=1}^{14}\left(1+\frac{1}{p_i-1}\right) < 1.6,$$

which is a contradiction. The proofs for the remaining two cases are quite similar. □

Theorem 2.3. *If an integer $D_{p,n}$ satisfies the Lehmer property, then it is prime.*

Proof. Since $n = 2^m < 180,000$ for some integer m by the above lemma, we have $14 \leq m \leq 17$. Moreover since $k < 1.45 \log n < 17.6$, we have $14 \leq k \leq 17$. On the other hand, since $\prod_{i=1}^k m_i \mid n \mid 2^{17}$ and m_i is even, we have following seven possibilities: $m_i = 2$ for all $i \geq 4$ and

$$(m_1, m_2, m_3) = (2^s, 2, 2) \text{ where } 1 \leq s \leq 4, \quad (8,4,2), \; (4,4,2) \quad \text{and} \quad (4,4,4).$$

Since all the other cases can be done in a similar manner, we only consider the case when $(m_1, m_2, m_3) = (4,4,2)$. In this case

$$p_1 = 4p^{n_1}+1, \quad p_2 = 4p^{n_2}+1 \quad \text{and} \quad p_i = 2p^{n_i}+1 \text{ for } 3 \leq i \leq k.$$

Without loss of generality, we assume that $n_1 < n_2$ and $n_3 < \cdots < n_k$. Note that

$$2^m p^{2^m} + 1 = (4p^{n_1}+1)(4p^{n_2}+1)(2p^{n_3}+1)\cdots(2p^{n_k}+1).$$

If $n_1 \neq n_3$, then $1 \equiv 4p^s+1 \pmod{p^{s+1}}$ or $1 \equiv 2p^s+1 \pmod{p^{s+1}}$, where $s = \min(n_1, n_3)$. This is a contradiction. Therefore we have $n_1 = n_3$. If $n_i \geq 1$ for any i, then

$$\begin{aligned} 2 \leq \frac{D_{p,n}-1}{\phi(D_{p,n})} &= \prod_{i=1}^{k}(1+\frac{1}{p_i-1}) = (1+\frac{1}{4p^{n_1}})(1+\frac{1}{4p^{n_2}})\prod_{i=3}^{k}(1+\frac{1}{2p^{n_i}}) \\ &\leq (1+\frac{1}{12})(1+\frac{1}{12})\prod_{i=3}^{17}(1+\frac{1}{2\times 3^{i-2}}) < 1.51, \end{aligned}$$

which is a contradiction. Thus $n_1 = n_3 = 0$. Since

$$2^m p^{2^m} + 1 = (4+1)(2+1)(4p^{n_2}+1)(2p^{n_4}+1)\cdots(2p^{n_k}+1),$$

the prime p should be 7. This is also contradiction because $p_i = 2 \times 7^{n_i}+1$ is divisible by 3. This completes the proof. □

3. Arbitrary case

Assume that an integer n satisfies the Lehmer property. Let α be a positive odd integer and let β be an integer such that $n-1=\alpha 2^{\beta}$. Let us write $n=\prod_{i=1}^{k} p_i$, where p_i's are distinct odd primes. Then $\phi(n)=\prod_{i=1}^{k}(p_i-1)$ divides $n-1=\alpha 2^{\beta}$. Since (p_i-1) divides $\alpha 2^{\beta}$, there exist an odd integer $m_{p_i}|\alpha$ and $n_{p_i}\le\beta$ such that $p_i=m_{p_i}2^{n_{p_i}}+1$ for any $i=1,2,\dots,k$.

Lemma 3.1. *With the above notations, we have*

$$k<1+\frac{\log\beta}{\log 2}+\frac{\log\alpha}{\log 3}.$$

Proof. Let $p=p_i$ be a prime dividing n. Assume that $m_p=1$. Since $p=2^{n_p}+1$ is prime. the integer n_p should be a power of 2. Let $n_p=2^{\gamma}$ for some integer γ. Since $n_p\le\beta$, we have $0\le\gamma<\frac{\log\beta}{\log 2}$. Thus there are at most $\frac{\log\beta}{\log 2}+1$ prime factors of n such that $m_p=1$.

Now assume that $m_p>1$. Since $\prod_{p|n} m_p$ divides α, the number of such prime factors is less than or equal to $\frac{\log\alpha}{\log 3}$. Therefore we have

$$k<1+\frac{\log\beta}{\log 2}+\frac{\log\alpha}{\log 3},$$

which is the desired result. □

Lemma 3.2. *With the above notations, if $\beta\ge 30$, then we have*

$$k>\min\left(\frac{\beta^{1/2}}{t_{\alpha,\beta}},1+\frac{2\beta^{1/2}}{3t_{\alpha,\beta}}\right),$$

where $t_{\alpha,\beta}=3.1(\log\beta)^{1/2}+(2.9\log\alpha)/(\log\beta)^{1/2}$.

Proof. First we let $N=\lfloor\sqrt{\frac{\beta}{\log\beta}}\rfloor$. By applying the same argument in Lemma 2.1, we may find a pair (u,v) of integers satisfying $u\ge 0$, $\gcd(u,v)=1$, $|u|,|v|<(\beta/\log\beta)^{1/2}$ and $|u\beta+vn_p|<3(\beta\log\beta)^{1/2}$.

Let $p=p_i$ be a prime factor of n. Since

$$\alpha 2^{\beta}\equiv -1 \pmod p \qquad\text{and}\qquad m_p 2^{n_p}\equiv -1 \pmod p,$$

we have $\alpha^u m_p^v 2^{\beta u+n_p v}\equiv(-1)^{u+v} (\mathrm{mod}\ p)$. Now we define

$$A_p:=\alpha^u m_p^v 2^{\beta u+n_p v}-(-1)^{u+v}.$$

By replacing α and β with n_1 and n in Lemma 2.1, respectively, one may easily show the following: there is at most one prime factor p of n such that $A_p=0$, and in this case, α is of the form ρ^{-v} for a suitable integer ρ, and $p=(\alpha 2^{\beta})^{-1/v}+1\le(\alpha 2^{\beta})^{1/3}+1$. Moreover, when $A_p\ne 0$, we have

$$\begin{aligned} p &\le \text{numerator of } A < 2^{1+|\beta u+n_p v|}\alpha^u m_p^{|v|}\le 2^{1+3(\beta\log\beta)^{1/2}}\alpha^{2(\beta/\log\beta)^{1/2}}\\ &< 2^{1+3(\beta\log\beta)^{1/2}+(2\log\alpha)(\beta\log\beta)^{1/2}}\\ &< 2^{3.1(\beta\log\beta)^{1/2}+(2.9\log\alpha)(\beta/\log\beta)^{1/2}}=2^{t_{\alpha,\beta}\beta^{1/2}}. \end{aligned}$$

Note that since $\beta \geq 30$, $1 < 0.1(\beta \log \beta)^{1/2}$. Thus, if $A_p \neq 0$ for every prime factor p of n, then

$$2^\beta < n = \prod_{i=1}^{k} p_i < \prod_{i=1}^{k} 2^{t_{\alpha,\beta}\beta^{1/2}} = 2^{kt_{\alpha,\beta}\beta^{1/2}},$$

which implies that $k > \frac{\beta^{1/2}}{t_{\alpha,\beta}}$. Suppose that there exists a prime factor p' of n with $A_{p'} = 0$. Since $p' \leq (\alpha 2^\beta)^{1/3} + 1$, we have

$$2^{2\beta/3} < \frac{\alpha 2^\beta + 1}{(\alpha 2^\beta)^{1/3} + 1} \leq \frac{n}{p'} = \prod_{\substack{1 \leq i \leq k \\ p_i \neq p'}} p_i < 2^{(k-1)t_{\alpha,\beta}\beta^{1/2}},$$

which implies that $k > 1 + \frac{2\beta^{1/2}}{3t_{\alpha,\beta}}$. The lemma follows. □

Corollary 3.3. *If* $\max(\alpha, 30) \leq \beta$*, then we have*

$$\min\left(\frac{\beta^{1/2}}{6(\log \beta)^{1/2}}, 1 + \frac{\beta^{1/2}}{9(\log \beta)^{1/2}}\right) < k < 1 + 2.4 \log \beta.$$

Proof. This is a direct consequence of Lemmas 3.1 and 3.2. □

Theorem 3.4. *If* $n = \alpha 2^\beta + 1$ $(\alpha \leq \beta)$ *satisfies the Lehmer property, then it is prime.*

Proof. Since the number of prime factors of n is greater than or equal to 14, we may assume that $\beta \geq 30$. From Corollary 3.3, we have $\beta < 1.4 \times 10^6$. Assume that a Fermat prime $2^{2^\gamma} + 1$ is a factor of n. Since 2^{2^γ} divides $\alpha 2^\beta$, we have $2^\gamma < \beta < 1.4 \times 10^6$. Thus we have $\gamma \leq 20$, and in fact, $\gamma \in \{0, 1, 2, 3, 4\}$. On the other hand, the number of prime factors p of n with $m_p > 1$ is less than or equal to $\frac{\log \alpha}{\log 3} < \frac{\log \beta}{\log 3} \leq 12.9$. Hence, we have $k \leq 5 + 12 = 17$. Again by Corollary 3.3, we have

$$\min\left(\frac{\beta^{1/2}}{6(\log \beta)^{1/2}}, 1 + \frac{\beta^{1/2}}{9(\log \beta)^{1/2}}\right) < 17.$$

Hence, $\beta < 260,000$.

Suppose that α is not divisible by 3. Then the number of prime factors p of n such that $m_p > 1$ is less than or equal to $\frac{\log 260{,}000}{\log 5} < 7.8$. Hence $k \leq 5 + 7 = 12$, which is a contradiction by [2]. Therefore α is divisible by 3 and n is not divisible by 3. Consequently, $\gamma \neq 0$ and $k \leq 4 + 11 = 15$. Now by Corollary 3.3 again, we have

$$\min\left(\frac{\beta^{1/2}}{6(\log \beta)^{1/2}}, 1 + \frac{\beta^{1/2}}{9(\log \beta)^{1/2}}\right) < 15.$$

Therefore we have $\beta < 200,000$.
Assume that there is a prime $q > 3$ dividing m_{p_i} for some i. Then

$$3^9 \cdot q \leq 3^{k-5} \cdot q \leq \prod_{i=1}^{k} m_{p_i} \leq \alpha \leq \beta < 200,000.$$

Hence, $q = 5$ or 7. If $\prod_{i=1}^{k} m_{p_i} = 3^a \cdot 5^b \cdot 7^c$, then

$$3^a \cdot 5^b \cdot 7^c \leq \alpha \leq 200,000 \quad \text{and} \quad 10 \leq a + b + c.$$

Therefore all possible (a, b, c)'s are

$$(11, 0, 0),\ (10, 0, 0),\ (9, 1, 0),\ (9, 0, 1) \quad \text{and} \quad (8, 2, 0).$$

Assume that $b \neq 0$. Since $\gamma \neq 1$ in this case, we have $k \leq 13$. This is a contradiction. For each remaining (a, b, c), one may easily check that

$$3^a \cdot 5^b \cdot 7^c \cdot 2^\beta + 1 \not\equiv 0 \pmod{257} \quad \text{and} \quad 3^{11} \cdot 2^\beta + 1 \not\equiv 0 \pmod{17}$$

for any β. Hence, $\gamma \neq 3$ and $\gamma \neq 2$ if $a = 11$. Therefore $k \leq 13$ in all cases. This completes the proof. $\square$

Remark 3.5. If $e^{\beta^{3/14}/6} > \alpha > \beta \geq 10^{10}$, then one may also show that a composite $n = \alpha 2^\beta + 1$ does not satisfy the Lehmer property by using a similar method.

References

[1] J. Cilleruelo and F. Luca, *Repunit Lehmer numbers*, Proc. Edinb. Math. Soc. (2) **54** (2011), no. 1, 55–65.

[2] G. L. Cohen and P. Hagis Jr., *On the number of prime factors of n if $\phi(n)|(n-1)$*, Nieuw. Arch. Wisk. (3) **28** (1980), no. 2, 177–185.

[3] J. M. Grau Ribas and F. Luca, *Cullen numbers with the Lehmer property*, Proc. Amer. Math. Soc. **140** (2012), no. 1, 129–134.

[4] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics, No. 70. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[5] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), no. 10, 745–757.

[6] F. Luca, *Fibonacci numbers with the Lehmer property*, Bull. Pol. Acad. Sci. Math. **55** (2007), no. 1, 7–15.

Dae-June Kim
Department of Mathematical Sciences
Seoul National University
Seoul 151-747, Korea
E-mail address: goodkdj@snu.ac.kr

Byeong-Kweon Oh
Department of Mathematical Sciences and Research Institute of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail address: bkoh@snu.ac.kr