PSEUDOPRIMES, PERFECT NUMBERS, AND A PROBLEM OF LEHMER

Walter Carlip
Ohio University, Athens, OH 45701

Eliot Jacobson
Ohio University, Athens, OH 45701

Lawrence Somer
Catholic University of America, Washington, D.C. 20064

(*Submitted December 1996-Final Revision April 1997*)

1. INTRODUCTION

Two classical problems in elementary number theory appear, at first, to be unrelated. The first, posed by D. H. Lehmer in [7], asks whether there is a composite integer N such that $\phi(N)$ divides $N-1$, where $\phi(N)$ is Euler's totient function. This question has received considerable attention and it has been demonstrated that such an integer, if it exists, must be extraordinary. For example, in [2] G. L. Cohen and P. Hagis, Jr., show that an integer providing an affirmative answer to Lehmer's question must have at least 14 distinct prime factors and exceed 10^{20}.

The second is the ancient question whether there exists an odd perfect number, that is, an odd integer N, such that $\sigma(N)=2N$, where $\sigma(N)$ is the sum of the divisors of N. More generally, for each integer $k>1$, one can ask for odd multiperfect numbers, i.e., odd solutions N of the equation $\sigma(N)=kN$. This question has also received much attention and solutions must be extraordinary. For example, in [1] W. E. Beck and R. M. Rudolph show that an odd solution to $\sigma(N)=3N$ must exceed 10^{50}. Moreover, C. Pomerance [9], and more recently D. R. Heath-Brown [4], have found explicit upper bounds for multiperfect numbers with a bounded number of prime factors.

In recent work [13], L. Somer shows that for fixed d there are at most finitely many composite integers N such that some integer a relatively prime to N has multiplicative order $(N-1)/d$ modulo N. A composite integer N with this property is a Fermat d-pseudoprime. (See [12], p. 117, where Fermat d-pseudoprimes are referred to as Somer d-pseudoprimes.) More recently, Somer [14] showed that under suitable conditions, there are at most finitely many Lucas d-pseudoprimes, i.e., pseudoprimes that arise via tests employing recurrence sequences. (Lucas d-pseudoprimes are discussed on pp. 131-132 of [12] where they are also called Somer-Lucas d-pseudoprimes. For a complete discussion of these and other pseudoprimes that arise from recurrence relations, see [12] or [11].)

The methods used by Somer in his papers motivated the present work. While attempting to simplify and extend the arguments in [13] and [14] we discovered that, in fact, Lehmer's problem, the existence of odd multiperfect numbers, and Somer's theorems about pseudoprimes are intimately related. In this paper we present a unified approach to the study of these four questions.

2. PRELIMINARIES

We adopt the convention that p always represents a prime number. Define the set $\delta(N)=\{p \mid p \text{ divides } N\}$ and for each i such that $1 \le i \le |\delta(N)|$, define $\delta_i(N)$ to the i^{th} largest prime in the decomposition of N. Thus, if N has decomposition

$$N = \prod_{i=1}^{t} p_i^{k_i}, \tag{2.1}$$

with $p_1 < p_2 < \cdots < p_t$, then $\delta_i(N) = p_i$. If Ω is a set of natural numbers, define

$$\delta(\Omega) = \cup_{N \in \Omega} \delta(N)$$

and, similarly, $\delta_i(\Omega) = \{\delta_i(N) \mid N \in \Omega\}$.

In the arguments below we will have need to extract the square-free part of certain integers. If N has decomposition (2.1), we will write

$$N_1 = \prod_{i=1}^{t} p_i \quad \text{and} \quad N_2 = \prod_{i=1}^{t} p_i^{k_i - 1}, \tag{2.2}$$

so that $N = N_1 N_2$ with N_1 square-free.

In the definitions and lemmas below, we will need a semigroup homomorphism from the natural numbers **N** to the multiplicative semigroup $\{-1, 0, 1\}$. Such a function will be called a *signature* function, and we will single out the case in which $\varepsilon = 1$, the constant function. Clearly, a signature function is determined by its values on the primes. We say that N is *supported* by ε if $\varepsilon(N) \neq 0$ or, equivalently, if $\varepsilon(p) \neq 0$ for all p that divide N. Similarly, a set Ω of natural numbers is *supported* by ε if $\varepsilon(N) \neq 0$ for all $N \in \Omega$. Note that if D is a fixed integer, the Jacobi symbol $\varepsilon(i) = (\frac{D}{i})$ is a signature function.

If N is any natural number and ε is a signature function, define the number theoretic function $\xi(N)$ as follows:

$$\xi(N) = \xi_\varepsilon(N) = \frac{1}{N} \prod_{p \mid N} (p - \varepsilon(p)). \tag{2.3}$$

Note that if N has decomposition (2.1), we can write $N = N_1 N_2$ as in (2.2) and

$$\xi(N) = \frac{1}{N_2} \prod_{i=1}^{t} \left(\frac{p_i - \varepsilon(p_i)}{p_i} \right) = \frac{1}{N_2} \prod_{i=1}^{t} \left(1 - \frac{\varepsilon(p_i)}{p_i} \right). \tag{2.4}$$

We will be interested in certain limiting values of $\xi(N)$ for N in a set Ω. In particular, if Ω is an infinite set of positive integers, then

$$\lim_{N \in \Omega} \xi(N) = L \tag{2.5}$$

means that for every $\varepsilon > 0$ there is an M such that $|\xi(N) - L| < \varepsilon$ whenever $N > M$ and $N \in \Omega$. Although in most applications the signature ε will be fixed, we also allow ε to vary with N, requiring only that N be supported by its associated signature.

The following elementary lemma is an easy exercise.

Lemma 2.1: Suppose that Ω is a set of positive integers and $f : \Omega \to \mathbf{R}$ a function such that $\lim_{N \in \Omega} f(N) = L$. Suppose as well that there exist functions f_1 and $f_2 : \Omega \to \mathbf{R}$ such that

(a) $f(N) = f_1(N) f_2(N)$ for all $N \in \Omega$;
(b) $\{f_2(N) \mid N \in \Omega\}$ has finite cardinality; and
(c) $\lim_{N \in \Omega} f_1(N) = 1$.

Then $f_2(N) = L$ for some $N \in \Omega$.

Lemma 2.2: If $N > 1$ is an integer supported by the signature ε and (c, d) is a pair of integers such that $\xi(N) = c/d$, then $(N, d) \neq 1$.

Proof: If $\xi(N) = c/d$, then

$$d\prod_{p|N}(p - \varepsilon(p)) = cN.$$

Since N is supported by ε, it follows that $\varepsilon(p) \neq 0$ for all p dividing N. Thus, if p is the largest prime divisor of N, then $p|d$. □

Theorem 2.3: Suppose that Ω is an infinite set of positive integers with each $N \in \Omega$ supported by corresponding signature ε and for which $|\delta(N)| = t$ for all $N \in \Omega$. Suppose as well that $\{N_2 \mid N \in \Omega\}$ is bounded. If c and d are integers such that $(N, d) = 1$ for all $N \in \Omega$ and

$$\lim_{N \in \Omega} \xi(N) = c/d, \tag{2.6}$$

then $c = d$.

Proof: If $\delta_t(\Omega)$ is bounded, then $\delta(\Omega)$ is bounded. Since $\{N_2 \mid N \in \Omega\}$ is bounded, it follows from (2.4) that $\xi(N)$ takes on finitely many values as N ranges over Ω. It follows that $\lim_{N \in \Omega} \xi(N) = \xi(N_0)$ for some $N_0 \in \Omega$, and $\xi(N_0) = c/d$, contrary to Lemma 2.2.

Consequently $\delta_t(\Omega)$ is unbounded. Choose s to be minimal such that $\delta_s(\Omega)$ is unbounded. Since $\delta_s(\Omega)$ is unbounded, we can find an infinite subset of Ω such that $\delta_s(N)$ is increasing and, without loss of generality, we may replace Ω with this subset. Now, if

$$f_1(N) = \prod_{i=s}^{t} \frac{\delta_i(N) - \varepsilon(\delta_i(N))}{\delta_i(N)},$$

then

$$\lim_{N \in \Omega} f_1(N) = 1. \tag{2.7}$$

Since $\delta_k(\Omega)$ is bounded for all $k < s$ and $\{N_2 \mid N \in \Omega\}$ is bounded, it follows that

$$f_2(N) = \begin{cases} \dfrac{1}{N_2} \displaystyle\prod_{i=1}^{s-1} \frac{\delta_i(N) - \varepsilon(\delta_i(N))}{\delta_i(N)} & \text{if } s > 1 \\ \dfrac{1}{N_2} & \text{if } s = 1 \end{cases} \tag{2.8}$$

takes on finitely many values. Since, in both cases, $\xi(N) = f_1(N) f_2(N)$, Lemma 2.1 implies that $f_2(N) = c/d$ for some $N \in \Omega$. If $s > 1$, it follows that

$$d\prod_{i=1}^{s-1}(\delta_i(N) - \varepsilon(\delta_i(N))) = cN_2 \prod_{i=1}^{s-1} \delta_i(N). \tag{2.9}$$

But then $\delta_{s-1}(N)$ divides d, contrary to the hypothesis that $(N, d) = 1$. It now follows that $s = 1$. But then Lemma 2.1 implies that $d = cN_2$ for some $N \in \Omega$. Since $(N_2, d) = 1$ for all $N \in \Omega$, this implies that $N_2 = 1$ and $c = d$, as desired. □

Corollary 2.4: Suppose that Ω is an infinite set of positive integers that is supported by the signature ε and for which $\{|\delta(N)|\}_{N\in\Omega}$ is bounded. Suppose as well that $\{N_2 \mid N \in \Omega\}$ is bounded. If c and d are integers such that $(N, d) = 1$ for all $N \in \Omega$ and

$$\lim_{N\in\Omega} \xi(N) = c/d, \tag{2.10}$$

then $c = d$.

Proof: If Ω is infinite and $\{|\delta(N)|\}_{N\in\Omega}$ is bounded, then there is some integer t such that $\hat{\Omega} = \{N \in \Omega \mid t = |\delta(N)|\}$ is infinite. We can now apply Theorem 2.3 to $\hat{\Omega}$. □

3. FERMAT PSEUDOPRIMES

Suppose that N is a composite integer and $a > 1$ is an integer such that $(N, a) = 1$ and $a^{N-1} \equiv 1 \pmod N$. Then N is called a *Fermat pseudoprime* to the base a. Moreover, if a has multiplicative order $(N-1)/d$ in $(\mathbf{Z}/N\mathbf{Z})^*$, then N is said to be a *Fermat d-pseudoprime* to the base a. In general, if there exists an integer $a > 1$ such that N is a Fermat d-pseudoprime to the base a, then we call N a Fermat d-pseudoprime.

If N has prime decomposition (2.1), then the structure of the unit group $(\mathbf{Z}/N\mathbf{Z})^*$ is well known. If N is not divisible by 8, then $(\mathbf{Z}/N\mathbf{Z})^*$ is a product of cyclic groups of order $p_i^{k_i-1}(p_i - 1)$, while if N is divisible by 8, then $p_1 = 2$ and $(\mathbf{Z}/N\mathbf{Z})^*$ has an additional factor that is a product of a cyclic group of order 2 and a cyclic group of order 2^{k_1-2}. It follows that the multiplicative orders of integers a relatively prime to N in $(\mathbf{Z}/N\mathbf{Z})^*$ are just the divisors of $\lambda(N) = \mathrm{lcm}\{p_i^{s_i}(p_i - 1)\}$, where $s_i = k_i - 1$ when p_i is odd, $s_1 = k_1 - 1$ if $p_1 = 2$ and $k_1 = 1$ or 2, and $s_1 = k_1 - 2$ if $p_1 = 2$ and $k_1 \geq 3$. Therefore N is a Fermat d-pseudoprime if and only if $(N-1)/d$ divides $\lambda(N)$. Moreover, since $(N, N-1) = 1$, a composite integer N is a Fermat d-pseudoprime if and only if $(N-1)/d$ divides $\lambda'(N) = \mathrm{lcm}\{p_i - 1\}$.

If N has decomposition (2.1), define

$$\psi(N) = \frac{1}{2^s}\prod_{i=1}^{t}(p_i - 1),$$

where $s = t-2$ when $2|N$ and $t \geq 2$, and $s = t-1$ otherwise. It is easy to see that if N is composite, then $\psi(N)$ is an integer and $\lambda'(N)$ divides $\psi(N)$. Therefore, if N is a Fermat d-pseudoprime, then $(N-1)/d$ divides $\psi(N)$, and hence, there is an integer c such that

$$\frac{\psi(N)}{N-1} = \frac{c}{d}. \tag{3.1}$$

We will need several lemmas concerning the properties of Fermat d-pseudoprimes and $\psi(N)$. Similar lemmas appear in [13], but the proofs are short and we include them here for completeness.

Lemma 3.1: If N is a Fermat d-pseudoprime with prime decomposition (2.1), then $(N, d) = 1$ and there exists an integer c such that

$$\frac{\psi(N)}{N-1} = \frac{c}{d} < \frac{1}{2^{t-1}}. \tag{3.2}$$

Proof: If $t=1$, then (3.2) follows immediately from the definition of $\psi(N)$ and the fact that N is composite. Assume that $t>1$. By (3.1) and the preceding comments, it suffices to show that $c/d<1/2^{t-1}$. This is immediate from the observation that

$$\frac{\prod_{p|N}(p-1)}{\prod_{p|N}p-1}<1$$

in general, and

$$\frac{\prod_{p|N}(p-1)}{\prod_{p|N}p-1}<\frac{1}{2}$$

when $2|N$. □

Lemma 3.2: If N is a Fermat d-pseudoprime with prime decomposition (2.1), then $t<\log_2(d)+1$.

Proof: By Lemma 3.1,

$$\frac{1}{d}\le\frac{c}{d}<\frac{1}{2^{t-1}},$$

and hence $d>2^{t-1}$. Thus $t-1<\log_2(d)$, and therefore $t<\log_2(d)+1$. □

Lemma 3.3: If N is a Fermat d-pseudoprime with prime decomposition (2.1) and $k_i\ge 2$, then

$$p_i^{k_i-1}<\frac{p_i^{k_i}}{p_i-1}\le d+1. \tag{3.3}$$

Proof: Clearly,

$$\begin{aligned}p_i^{k_i-1}<\prod_{j=1}^{t}\frac{p_j^{k_j}}{p_j-1}&=\frac{1}{2^s}\left(\frac{\Pi p_j^{k_j}}{\frac{1}{2^s}\Pi(p_j-1)}\right)=\frac{1}{2^s}\left(\frac{N}{\psi(N)}\right)\\&=\frac{1}{2^s}\left(\frac{N-1}{\psi(N)}\right)+\frac{1}{2^s\psi(N)}=\frac{1}{2^s}\left(\frac{d}{c}\right)+\frac{1}{2^s\psi(N)}\\&\le\frac{d}{2^s}+\frac{1}{2^s}=\frac{1}{2^s}(d+1)\le d+1.\ \square\end{aligned}$$

The following theorem first appeared in [13].

Theorem 3.4: For fixed positive integer d, there are at most a finite number of Fermat d-pseudoprimes.

Proof: By way of contradiction, suppose that there are an infinite number of Fermat d-pseudoprimes. By Lemma 3.2, there exists an integer t, with $t<\log_2(d)+1$, such that an infinite number of these Fermat d-pseudoprimes have exactly t distinct prime divisors. Moreover, an infinite number of these Fermat d-pseudoprimes have the same parity. Then (3.2) is satisfied by an infinite number of integers N of the same parity. There are, however, only a finite number of possible values for c, and it follows that there is some value of c for which (3.2) has an infinite number of solutions N of the same parity. Fix this value of c and let Ω be an (infinite) set of positive integers N of the same parity that satisfy (3.2) for these fixed values of c and d.

If $\delta(\Omega)$ is bounded, then, by Lemma 3.3, Ω is finite, contrary to our choice of c. Consequently $\delta(\Omega)$ is unbounded. Moreover, by Lemma 3.2, $\{|\delta(N)|\}_{N\in\Omega}$ is bounded, and it follows that

$$\lim_{N\in\Omega}\frac{1}{\psi(N)}=0.$$

Consequently, with constant signature $\varepsilon=1$, and $s=t-2$ if the elements of Ω are even and $t\geq 2$, and $s=t-1$ otherwise, we obtain

$$\begin{aligned}\frac{2^s c}{d}&=2^s\lim_{N\in\Omega}\left(\frac{\psi(N)}{N-1}\right)=2^s\lim_{N\in\Omega}\frac{1}{\left(\frac{N-1}{\psi(N)}\right)}\\&=2^s\lim_{N\in\Omega}\frac{1}{\left(\frac{N}{\psi(N)}-\frac{1}{\psi(N)}\right)}=2^s\lim_{N\in\Omega}\left(\frac{\psi(N)}{N}\right)=\lim_{N\in\Omega}\xi(N).\end{aligned}\tag{3.4}$$

By Lemma 3.3, $\{N_2\mid N\in\Omega\}$ is bounded and, by Lemma 3.1, $(N,d)=1$ for all $N\in\Omega$. Clearly, Ω is supported by the constant signature $\varepsilon=1$. Therefore Theorem 2.3 implies that $2^s c/d=1$.

Finally, by (3.2),

$$1=\frac{2^s c}{d}<\frac{2^s}{2^{t-1}}\leq 1,\tag{3.5}$$

a contradiction. □

4. LUCAS PSEUDOPRIMES

Let $U(P,Q)$ be the recurrence sequence defined by $U_0=0$, $U_1=1$, and

$$U_{n+2}=PU_{n+1}-QU_n\tag{4.1}$$

for all $n\geq 0$. The sequence $U(P,Q)$ is called a *Lucas sequence* with parameters P and Q. Associated with $U(P,Q)$ is an integer $D=P^2-4Q$ known as the *discriminant* of $U(P,Q)$ and, as noted above, the function $\varepsilon(i)=\left(\frac{D}{i}\right)$ is a signature function. For the duration of this section, $\varepsilon(N)$ will be the Jacobi symbol.

If N is an integer and $U(P,Q)$ a Lucas sequence, we define $\rho_U(N)$ to be the least positive integer n such that N divides U_n. The number $\rho(N)$ is called the *rank of appearance* (or simply the *rank*) of N in $U(P,Q)$. If $(N,Q)=1$, then it is well known that $U(P,Q)$ is purely periodic modulo N and, since $U_0=0$, $\rho(N)$ exists. Moreover, in this case $U_n\equiv 0 \pmod N$ if and only if $\rho(N)$ divides n. It was proven by Lucas [8] that, if a prime p does not divide $2QD$, then $U_{p-\varepsilon(p)}\equiv 0 \pmod p$ and hence $\rho(p)$ divides $p-\varepsilon(p)$.

Motivated by Lucas' theorem, we say that an odd composite integer N is a *Lucas pseudoprime* if there is a Lucas sequence $U(P,Q)$ with discriminant D such that $(N,QD)=1$ and $U_{N-\varepsilon(N)}\equiv 0 \pmod N$, where $\varepsilon(N)=\left(\frac{D}{N}\right)$. Moreover, if $\rho(N)=(N-\varepsilon(N))/d$, then N is said to be a *Lucas d-pseudoprime*.

Suppose that ε is any signature function and N an odd integer with decomposition (2.1) that is supported by ε. Analogous to the functions λ, λ', and ψ defined in the previous section, define

$$\lambda(N) = \mathrm{lcm}\{p_i^{k_i-1}(p_i - \varepsilon(p_i))\},$$
$$\lambda'(N) = \mathrm{lcm}\{p_i - \varepsilon(p_i)\}, \text{ and}$$
$$\psi(N) = \frac{1}{2^{t-1}}\prod_{i=1}^{t}(p_i - \varepsilon(p_i)).$$

In [14], L. Somer shows that an integer N is a Fermat d-pseudoprime if and only if it is a Lucas d-pseudoprime with a signature ε satisfying $\varepsilon(p) = 1$ for all primes p dividing N. Since for each d there are only a finite number of Fermat d-pseudoprimes, it may seem reasonable to conjecture that there are also a finite number of Lucas d-pseudoprimes. This conjecture seems highly unlikely, however, since d-pseudoprimes with three prime divisors and d divisible by 4 are easy to construct.

If k is an even integer with the property that $p = 3k - 1$, $q = 3k + 1$, and $r = 3k^2 - 1$ are prime, set $N = pqr$ and choose D relatively prime to N and congruent to 0 or 1 (mod 4) such that $\varepsilon(p) = 1$ and $\varepsilon(q) = \varepsilon(r) = -1$. Then

$$\begin{aligned} N - \varepsilon(N) &= pqr - 1 = (3k-1)(3k+1)(3k^2-1) - 1 \\ &= 3k^2(9k^2 - 4) = (3k-2)(3k+2)(3k^2) \\ &= (p-1)(q+1)(r+1). \end{aligned}$$

It is a consequence of elementary properties of Lucas sequences and a theorem of H. C. Williams [15] that for any odd integer N and discriminant D relatively prime to N and satisfying $D \equiv 0$ or 1 (mod 4), there is a Lucas sequence U satisfying $\rho_U(N) = \lambda(N)$. Thus, for

$$d = \frac{(p-1)(q+1)(r+1)}{\mathrm{lcm}(p-1), (q+1), (r+1)} = \frac{N - \varepsilon(N)}{\lambda(N)},$$

Williams' theorem implies that N is a Lucas d-pseudoprime. Since $p - 1, q + 1$, and $r + 1$ are all even, it is clear that d is divisible by 4, and when $\lambda(N)$ is maximal, $d = 4$. For example, taking $k = 4$ yields the Lucas 4-pseudoprime $N = 11 \cdot 13 \cdot 47 = 6721$ and $k = 60$ yields the 4-pseudoprime $N = 179 \cdot 181 \cdot 10799 = 349876801$.

More general algorithms for generating Lucas d-pseudoprimes are described in [14] and will be discussed in detail in a future paper. It is worth noting that the computational evidence presented in [14] suggests that there are infinitely many Lucas d-pseudoprimes with exactly three distinct prime divisors when 4 divides d and d is a square, and that there is a relationship between the number of Lucas d-pseudoprimes N, the precise power of 2 that divides d, and the number of prime divisors of N. We prove below that there are at most a finite number of Lucas d-pseudoprimes N such that $2^r \| N$ and $|\delta(N)| \geq r + 2$. In light of the computational evidence presented in [14], the requirement that $|\delta(N)| \geq r + 2$ appears to be best possible.

As in the previous section, we require a few lemmas that describe properties of Lucas d-pseudoprimes and $\psi(N)$. The following three lemmas can be proved by methods analogous to those used to prove Lemma 3.1, Lemma 3.2, and Lemma 3.3.

Lemma 4.1: If N is a Lucas d-pseudoprime, then $(N, d) = 1$ and there exist integers b and c such that

$$\frac{\lambda'(N)}{N - \varepsilon(N)} = \frac{b}{d} \leq \frac{\psi(N)}{N - \varepsilon(N)} = \frac{c}{d} < 2\left(\frac{2}{3}\right)^t. \tag{4.2}$$

Lemma 4.2: If N is a Lucas d-pseudoprime with prime decomposition (2.1), then $t < \log_{3/2}(2d)$.

Lemma 4.3: If N is a Lucas d-pseudoprime with prime decomposition (2.1) and $k_i \geq 2$, then

$$p_i^{k_i-1} < 2(2/3)^t(d+1). \tag{4.3}$$

The following theorem is new; it sharpens a result of the third author in [14].

Theorem 4.4: Let d be a fixed positive integer and suppose that 2^r exactly divides d. Then there are at most a finite number of Lucas d-pseudoprimes N such that $|\delta(N)| \geq r+2$.

Proof: Suppose that there are an infinite number of Lucas d-pseudoprimes N with $|\delta(N)| \geq r+2$. By Lemma 4.2, there exists an integer t, with $r+1 < t < \log_{3/2}(2d)$, such that an infinite number of these Lucas d-pseudoprimes have exactly t distinct prime divisors. Thus (4.2) is satisfied by an infinite number of integers N. There are, however, only a finite number of possible values for c, and it follows that there is some value of c for which (4.2) has an infinite number of solutions N. Fix this value of c and let Ω be the (infinite) set of positive integers N that satisfy (4.2) for these fixed values of c and d.

If $\delta(\Omega)$ is bounded, then, by Lemma 4.3, Ω is finite, contrary to our choice of c. Consequently $\delta(\Omega)$ is unbounded. Moreover, by Lemma 4.2, $\{|\delta(N)|\}_{N\in\Omega}$ is bounded and it follows that

$$\lim_{N\in\Omega}\frac{\varepsilon(N)}{\psi(N)} = 0.$$

It then follows that

$$\frac{2^{t-1}c}{d} = 2^{t-1}\lim_{N\in\Omega}\left(\frac{\psi(N)}{N-\varepsilon(N)}\right) = 2^{t-1}\lim_{N\in\Omega}\frac{1}{\left(\frac{N-\varepsilon(N)}{\psi(N)}\right)}$$
$$= 2^{t-1}\lim_{N\in\Omega}\frac{1}{\left(\frac{N}{\psi(N)}-\frac{\varepsilon(N)}{\psi(N)}\right)} = 2^{t-1}\lim_{N\in\Omega}\left(\frac{\psi(N)}{N}\right) = \lim_{N\in\Omega}\xi(N). \tag{4.4}$$

By Lemma 4.3, $\{N_2 | N \in \Omega\}$ is bounded and, by Lemma 4.1, $(N,d)=1$ for all $N\in\Omega$. Moreover, since $\varepsilon(N) = \left(\frac{D}{N}\right)$ and, by definition of Lucas d-pseudoprime, $(D,N)=1$, it follows that Ω is supported by ε. Therefore Theorem 2.3 implies that $2^{t-1}c/d = 1$. Thus $d = 2^{t-1}c$. Since 2^r exactly divides d, the hypothesis that $t > r+1$ implies that $r \geq t-1 > (r+1)-1 = r$, a contradiction. □

The following two corollaries are stated in [14].

Corollary 4.5: If d is odd, then there are at most finitely many Lucas d-pseudoprimes.

Proof: Theorem 4.4 handles the case in which N has at least 2 distinct prime divisors and Lemma 4.3 handles the case in which N is a prime power. □

Corollary 4.6: If 2 exactly divides d, then there are at most finitely many Lucas d-pseudoprimes.

Proof: Suppose otherwise and fix d such that $d \equiv 2 \pmod 4$ and there are infinitely many d-pseudoprimes N. Then, by Theorem 4.4 and Lemma 4.3, there are infinitely many d-pseudoprimes with $|\delta(N)| = 2$. By Lemma 4.1 and the argument in the proof of Theorem 4.4,

$$\frac{\psi(N)}{N-\varepsilon(N)} = \frac{1}{2}; \tag{4.5}$$

and hence, if N has decomposition (2.1),

$$\frac{(p_1-\varepsilon(p_1))(p_2-\varepsilon(p_2))}{N-\varepsilon(N)}=1. \tag{4.6}$$

If either $k_1>1$ or $k_2>1$, then

$$\begin{aligned}\frac{(p_1-\varepsilon(p_1))(p_2-\varepsilon(p_2))}{N-\varepsilon(N)}&=\frac{(p_1-\varepsilon(p_1))(p_2-\varepsilon(p_2))}{p_1^{k_1}p_2^{k_2}-\varepsilon(N)}\\&\leq\frac{(p_1+1)(p_2+1)}{p_1^2p_2-1}\leq\frac{(3+1)(5+1)}{9\cdot5-1}=\frac{24}{44}<1,\end{aligned} \tag{4.7}$$

a contradiction. Therefore $k_1=k_2=1$.

It now follows that

$$\begin{aligned}(p_1-\varepsilon(p_1))(p_2-\varepsilon(p_2))&=p_1p_2-\varepsilon(p_1)\varepsilon(p_2),\ \text{and}\\ p_1\varepsilon(p_2)+p_2\varepsilon(p_1)&=2\varepsilon(p_1)\varepsilon(p_2).\end{aligned} \tag{4.8}$$

If $\varepsilon(p_1)=\varepsilon(p_2)$, then $p_1+p_2=\pm2$, which is impossible. Hence, $\varepsilon(p_1)=-\varepsilon(p_2)$.

Since $p_2>p_1$, it now follows that $p_2-p_1=2$, i.e., p_1 and p_2 are twin primes.

Now, by Lemma 4.1,

$$\frac{b}{d}=\frac{\lambda'(N)}{N-\varepsilon(N)}=\frac{\operatorname{lcm}\{(p_1+1),(p_1+2-1)\}}{p_1(p_1+2)+1}=\frac{1}{p_1+1}. \tag{4.9}$$

It follows that $d=b(p_1+1)$. Clearly, there are only finitely many prime twins p_1 and p_1+2 such that p_1+1 divides d. This final contradiction completes the proof of the corollary. □

5. LEHMER'S PROBLEM

In [7], D. H. Lehmer asks whether there exist composite integers N such that $\phi(N)$ divides $N-1$. If N has prime decomposition (2.1), then

$$\phi(N)=N\prod_{p|N}\frac{p-1}{p}. \tag{5.1}$$

Consequently, if $d\phi(N)=N-1$, it follows that

$$dN\prod_{p|N}(p-1)=(N-1)\prod_{p|N}p, \tag{5.2}$$

and therefore

$$dN_2\prod_{p|N}(p-1)=(N-1). \tag{5.3}$$

Since $(N,N-1)=1$, this implies that $N_2=1$, i.e., N is square-free.

The following theorem was first proven by C. Pomerance in [10].

Theorem 5.1: For any integers $t>1$ and $d>1$, there are at most a finite number of integers $N>2$ such that $d\phi(N)=N-1$ and $|\delta(N)|\leq t$.

Proof: Fix positive integers t and d, and let Ω be the set of all positive integers N such that $d\phi(N) = N-1$ and $|\delta(N)| \le t$. By way of contradiction, assume that Ω has infinite cardinality.

It follows from the hypotheses that $(N, d) = 1$ for all $N \in \Omega$ and, from the remarks above, that N is square-free. Moreover, since $\phi(N)$ is even for N greater than 2, every element of Ω is odd.

It now follows for each $N \in \Omega$ that $\phi(N)/(N-1) = 1/d$. As in the previous sections, replacing Ω with a subset if necessary, we obtain

$$\frac{1}{d} = \frac{\phi(N)}{N-1} = \lim_{N\in\Omega} \frac{\phi(N)}{N-1} = \lim_{N\in\Omega} \frac{N\xi(N)}{N-1} = \lim_{N\in\Omega} \xi(N). \tag{5.4}$$

It now follows from Corollary 2.4 that $d = 1$, a contradiction. □

6. PERFECT NUMBERS

If N is a positive integer, define $\sigma(N)$ to be the sum of the positive divisors of N. A positive integer N is called a *perfect number* if $\sigma(N) = 2N$. It is well known that every even perfect number is a Euclid number, i.e., an integer of the form $2^n(2^{n+1}-1)$, where $2^{n+1}-1$ is a Mersenne prime. Moreover, it is well known that every odd perfect number can be written in the form $N = pM^2$ for some integer $M > 1$. It follows that 6 is the only square-free perfect number.

Recall that if N has decomposition (2.1), then

$$\sigma(N) = \prod_{p|N} \frac{p^{k_i+1}-1}{p-1}. \tag{6.1}$$

If N is square-free, then (6.1) becomes

$$\sigma(N) = \prod_{p|N} \frac{p^2-1}{p-1} = \prod_{p|N} (p+1) = N\xi(N), \tag{6.2}$$

where the signature function ε is given by $\varepsilon(p) = -1$ for all primes p. Thus, for N square-free, N is a perfect number if and only if

$$\xi(N) = 2. \tag{6.3}$$

More generally, we can ask for square-free k-perfect integers N, that is, solutions N of

$$\xi(N) = k. \tag{6.4}$$

L. E. Dickson [3] and I. S. Gradstein [5] have both proven that there are only a finite number of odd perfect numbers N with $|\delta(N)|$ bounded, and Dickson [3] generalized this result to primitive abundant numbers. H.-J. Kanold [6] has studied (6.4) for k rational, and proved that there are only finitely many primitive (and hence only finitely many odd) solutions N with a fixed number of prime factors. As mentioned in the introduction, these results have recently been generalized by Pomerance [9] and D. R. Heath-Brown [4]. Here we apply the methods developed above to prove a similar result for multiperfect numbers.

Theorem 6.1: For fixed k and t, there exist at most finitely many square-free integers N such that $|\delta(N)| \le t$ and

$$\sigma(N) = kN. \tag{6.5}$$

Proof: By the remarks preceding the theorem, the condition $\sigma(N) = kN$ is equivalent to $\xi(N) = k$. Let $\Omega = \{N \mid \xi(N) = k, |\delta(N)| \le t$, and N is square-free$\}$. By way of contradiction, suppose that Ω has infinite cardinality. Since each $N \in \Omega$ is square-free, $\{N_2 \mid N \in \Omega\}$ is bounded. It is clear that Ω satisfies the hypotheses of Corollary 2.4, and we conclude that $k = 1$. But, clearly, $\sigma(N) \ge N + 1 > kN$, a contradiction. □

REFERENCES

1. Walter E. Beck & Rudolph M. Najar. "A Lower Bound for Odd Triperfects." *Math. Comp.* **38** (1982):249-51.
2. G. L. Cohen & P. Hagis. "On the Number of Prime Factors of n if $\phi(n)$ Divides $n-1$." *Nieuw Arch. Wisc.* (4) **28** (1980):177-85.
3. L. E. Dickson. "Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Divisors." *Amer. J. Math.* **35** (1913):413-22.
4. D. R. Heath-Brown. "Odd Perfect Numbers." *Math. Proc. Cambridge Philos. Soc.* **115** (1994):191-96.
5. I. S. Gradstein. "On Perfect Numbers" (in Russian) *Mat. Sb.* **32** (1925):476-510.
6. Hans-Joachim Kanold. "Über einen Satz von L. E. Dickson." *Math. Annalen* **131** (1956): 167-79.
7. D. H. Lehmer. "On Euler's Totient Function." *Bull. Amer. Math. Soc.* (N.S.) **38** (1932): 745-51.
8. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-250.
9. Carl Pomerance. "Multiple Perfect Numbers, Mersenne Primes, and Effective Computability." *Math. Ann.* **226** (1977):195-206.
10. Carl Pomerance. "On Composite n for Which $\phi(n)$ Divides $n-1$, II." *Pacific J. Math.* **69** (1977):177-86.
11. Paulo Ribenboim. *The Little Book of Big Primes*. New York: Springer-Verlag, 1991.
12. Paulo Ribenboim. *The New Book of Prime Number Records*. New York: Springer-Verlag, 1996.
13. Lawrence Somer. "On Fermat *d*-Pseudoprimes." In *Number Theory*, pp. 841-60. Ed. J.-M. De Koninck & C. Levesque. Berlin: Walter de Gruyter, 1989.
14. Lawrence Somer. "On Lucas *d*-Pseudoprimes." In *Applications of Fibonacci Numbers* **7**. Ed. A. N. Philippou, A. F. Horadam, & G. E. Bergum. Dordrecht: Kluwer, 1998.
15. H. C. Williams. "On Numbers Analogous to the Carmichael Numbers." *Can. Math. Bull.* **20** (1977):133-43.

AMS Classification Numbers: 11B39, 11A25, 11A51, 11B36

❖❖❖