A SIMPLE PROOF OF CARMICHAEL'S THEOREM ON PRIMITIVE DIVISORS

Minoru Yabuta

46-35 Senriokanaka Suita-si, Osaka 565-0812, Japan

(Submitted September 1999-Final Revision March 2000)

1. INTRODUCTION

For arbitrary positive integer n, numbers of the form $D_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ are called the *Lucas numbers*, where α and β are distinct roots of the polynomial $f(z) = z^2 - Lz + M$, and L and M are integers that are nonzero. The Lucas sequence (D): $D_1, D_2, D_3, \ldots$ is called *real* when α and β are real. Throughout this paper, we assume that L and M are coprime. Each D_n is an integer. A prime p is called a *primitive divisor* of D_n if p divides D_n but does not divide D_m for $0 < m < n$. Carmichael [2] calls it a *characteristic factor* and Ward [9] an *intrinsic divisor*. As Durst [4] observed, in the study of primitive divisors, it suffices to take $L > 0$. Therefore, we assume $L > 0$ in this paper.

In 1913, Carmichael [2] established the following.

Theorem 1 (Carmichael): If α and β are real and $n \neq 1, 2, 6$, then D_n contains at least one primitive divisor except when $n = 12$, $L = 1$, $M = -1$,

In 1974, Schinzel [6] proved that if the roots of f are complex and their quotient is not a root of unity and if n is sufficiently large then the n^{th} term in the associated Lucas sequence has a primitive divisor. In 1976, Stewart [7] proved that if $n = 5$ or $n > 6$ there are only finitely many Lucas sequences that do not have a primitive divisor, and they may be determined. In 1995, Voutier [8] determined all the exceptional Lucas sequences with n at most 30. Finally, Bilu, Hanrot, and Voutier [1] have recently shown that there are no other exceptional sequences that do not have a primitive divisor for the n^{th} term with n larger than 30.

The aim of this paper is to give an elementary and simple proof of Theorem 1. To prove that Theorem 1 is true for all real Lucas sequences, it is sufficient to discuss the two special sequences, namely, the Fibonacci sequence and the so-called Fermat sequence.

2. A SUFFICIENT CONDITION THAT D_n HAS A PRIMITIVE DIVISOR

Let $n > 1$ be an integer. Following Ward [9], we call the numbers

$$Q_1 = 1,\ Q_n = Q_n(\alpha, \beta) = \prod_{\substack{1 \le r \le n \\ (r,n)=1}} (\alpha - e^{2\pi i r/n}\beta) \ \text{ for } n \ge 2$$

the cyclotomic numbers associated with the Lucas sequence, where α, β are the roots of the polynomial $f(z) = z^2 - Lz + M$ and the product is extended over all positive integers less than n and prime to n. Each Q_n is an integer, and $D_n = \prod_{d|n} Q_n$, where the product is extended over all divisors d of n. Hence, p is a primitive divisor of D_n if and only if p is a primitive divisor of Q_n.

Lemma 1 below was shown by several authors (Carmichael, Durst, Ward, and others).

Lemma 1: Let p be prime and let k be the least positive value of the index i such that p divides D_i. If $n \neq 1, 2, 6$ and if p divides Q_n and some Q_m with $0 < m < n$, then p^2 does not divide Q_n and $n = p^r k$ with $r \geq 1$.

Now suppose that n has a prime-power factorization $n = p_1^{e_1} p_2^{e_2} \ldots p_l^{e_l}$, where $p_1, p_2, \ldots, p_l$ are distinct primes and $e_1, e_2, \ldots, e_l$ are positive integers. Lemma 1 leads us to the following lemma (cf. Halton [5], Ward [9]).

Lemma 2: Let $n \neq 1, 2, 6$. A sufficient condition that D_n contains at least one primitive divisor is that $|Q_n| > p_1 p_2 \cdots p_l$.

Proof: We prove the contraposition. Suppose that D_n has no primitive divisors. If p is an arbitrary prime factor of Q_n, then p divides some Q_m with $0 < m < n$. Therefore, p divides n and p^2 does not divide Q_n. Hence, Q_n divides $p_1 p_2 \cdots p_l$, so $|Q_n| \leq p_1 p_2 \cdots p_l$. □

Our proof of Carmichael's theorem is based on the following.

Theorem 2: If $n \neq 1, 2, 6$ and if both the n^{th} cyclotomic number associated with $z^2 - z - 1$ and that associated with $z^2 - 3z + 2$ are greater than the product of all prime factors of n, then, for every real Lucas sequence, D_n contains at least one primitive divisor.

Now assume that n is an integer greater than 2 and that α and β are real, that is, $L^2 - 4M$ is positive. As Ward observed,

$$Q_n(\alpha, \beta) = \prod(\alpha - \zeta^r \beta)(\alpha - \zeta^{-r} \beta) \tag{1}$$

$$= \prod((\alpha + \beta)^2 - \alpha\beta(2 + \zeta^r + \zeta^{-r})), \tag{2}$$

where $\zeta = e^{2\pi i/n}$ and the products are extended over all positive integers less than $n/2$ and prime to n. Since $\alpha + \beta = L$ and $\alpha\beta = M$, by putting $\theta_r = 2 + \zeta^r + \zeta^{-r}$, we have

$$Q_n = Q_n(\alpha, \beta) = \prod(L^2 - M\theta_r). \tag{3}$$

Fix an arbitrary $n > 2$. Then Q_n can be considered as the function of variables L and M. We shall discuss for what values of L and M the n^{th} cyclotomic number Q_n has its least value.

Lemma 3: Let $n > 2$ be an arbitrary fixed integer. If α and β are real, then Q_n has its least value either when $L = 1$ and $M = -1$ or when $L = 3$ and $M = 2$.

Proof: Take an arbitrary θ_r and fix it. Since $n > 2$, we have $0 < \theta_r < 4$. Thus, if $M < 0$, we have $L^2 - M\theta_r \geq 1 + \theta_r$, with equality holding only in the case $L = 1$, $M = -1$. When $M > 0$, consider the cases $M = 1$, $M > 1$. In the first case we have $L \geq 3$, so that

$$L^2 - M\theta_r \geq 9 - \theta_r > 9 - 2\theta_r.$$

Now assume $M > 1$. Then, since $L^2 \geq 4M + 1$, we have

$$L^2 - M\theta_r \geq 4M + 1 - M\theta_r = 9 - 2\theta_r + (M - 2)(4 - \theta_r) \geq 9 - 2\theta_r$$

with equality holding only in the case $M = 2$, $L = 3$. Hence, by formula (3), we have completed the proof. □

Combining Lemma 2 with Lemma 3, we complete the proof of Theorem 2.

3. CARMICHAEL'S THEOREM

We call the Lucas sequence generated by $z^2 - z - 1$ the *Fibonacci sequence* and that generated by $z^2 - 3z + 2$ the *Fermat sequence*. Theorem 2 implies that to prove Carmichael's theorem it is sufficient to discuss the Fibonacci sequence and the Fermat sequence.

Now we suppose that n has a prime-power factorization $n = p_1^{e_1} p_2^{e_2} \ldots p_l^{e_l}$, and let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial.

Lemma 4: If $n > 2$ and if a is real with $|a| < 1/2$, then $\Phi_n(a) \geq 1 - |a| - |a|^2$.

Proof: We have

$$\Phi_n(a) = \prod_{d|n} (1 - a^{n/d})^{\mu(d)},$$

where μ denotes the Möbius function and the product is extended over all divisors d of n. Since $|a| < 1/2$ and $(1 - a^{n/d})^{\mu(d)} \geq 1 - |a|^{n/d}$,

$$\Phi_n(a) \geq \prod_{i=1}^{\infty} (1 - |a|^i) \geq (1 - |a|)(1 - |a|^2 - |a|^3 - |a|^4 - \cdots)$$
$$= (1 - |a|)\left(1 - \frac{|a|^2}{1 - |a|}\right) = 1 - |a| - |a|^2.$$

Here we have used the fact that if $0 \leq x \leq 1$ and $0 \leq y \leq 1$ then $(1 - x)(1 - y) \geq 1 - x - y$. We have thus proved the lemma. □

Theorem 3: If $n \neq 1, 2, 6, 12$, then the n^{th} term of the Fibonacci sequence contains at least one primitive divisor.

Proof: Assume $n > 2$. We shall determine for what n the inequality $|Q_n| > p_1 p_2 \ldots p_l$ is satisfied, where Q_n is the n^{th} cyclotomic number associated with the Fibonacci sequence. The roots of the polynomial $z^2 - z - 1$ are $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Since $|\beta / \alpha| = (3 - \sqrt{5})/2 < 1/2$, Lemma 4 gives

$$\Phi_n(\beta / \alpha) \geq 1 - |\beta / \alpha| - |\beta / \alpha|^2 = 2\sqrt{5} - 4 > 2/5.$$

In addition, since $\alpha > 3/2$, we have

$$Q_n(\alpha, \beta) = \alpha^{\phi(n)} \Phi_n(\beta / \alpha) > (2/5)(3/2)^{\phi(n)},$$

where $\phi(n)$ denotes the Euler function: $\phi(n) = \prod_{i=1}^{l} p_i^{e_i - 1}(p_i - 1)$. Thus, $|Q_n| > p_1 p_2 \ldots p_l$ is true for n satisfying

$$(2/5)(3/2)^{\phi(n)} > p_1 p_2 \ldots p_l. \tag{4}$$

We first suppose $p_1 > 7$ without loss of generality. Then $(2/5)(3/2)^{\phi(p_1)} > 2p_1$ is true, and consequently $(2/5)(3/2)^{\phi(n)} > p_1 p_2 \ldots p_l$. Here we have used the fact that if x, y are real with $x > y > 3$ and if m is integral with $m > 2$ then $x^{m-1} > my$. We next suppose $p_1^{e_1} = 2^4, 3^3, 5^2$, or 7^2 without loss of generality. Therefore, $(2/5)(3/2)^{\phi(p_1^{e_1})} > 2p_1$ is true, and consequently $(2/5)(3/2)^{\phi(n)} > p_1 p_2 \ldots p_l$. Hence, inequality (4) is true unless n is of the form

$$n = 2^a 3^b 5^c 7^d, \tag{5}$$

where $0 \le a \le 3$, $0 \le b \le 2$, $0 \le c \le 1$, and $0 \le d \le 1$. By substituting (5) into (4), we verify that inequality (4) is true for $n \ne 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 30$. However, by direct computation, we have

$$\begin{array}{lllll} Q_2 = 1, & Q_3 = 2, & Q_4 = 3, & Q_5 = 5, & Q_6 = 4, \\ Q_7 = 13, & Q_8 = 7, & Q_9 = 17, & Q_{10} = 11, & Q_{12} = 6, \\ Q_{14} = 29, & Q_{15} = 61, & Q_{18} = 19, & Q_{30} = 31. & \end{array}$$

Hence, $|Q_n| > p_1 p_2 \dots p_l$ holds for $n \ne 1, 2, 3, 5, 6, 12$. It follows from Lemma 2 that if $n \ne 1, 2, 3, 5, 6, 12$ then the n^{th} Fibonacci number F_n contains at least one primitive divisor. In addition, since $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 2^3$, $F_{12} = 2^4 \cdot 3^2$, the numbers F_3 and F_5 have a primitive divisor, and F_1, F_2, F_6, and F_{12} do not. □

Theorem 4: If $n \ne 1, 2, 6$, then the n^{th} term of the Fermat sequence contains at least one primitive divisor.

Proof: The roots of the polynomial $z^2 - 3z + 2$ are $\alpha = 2$ and $\beta = 1$. By Lemma 4,

$$\Phi_n(\beta/\alpha) \ge 1 - |\beta/\alpha| - |\beta/\alpha|^2 = 1/4.$$

Therefore,

$$Q_n(\alpha, \beta) = \alpha^{\phi(n)} \Phi_n(\beta/\alpha) > (1/4) \cdot 2^{\phi(n)}.$$

Now the inequality $(1/4) \cdot 2^{\phi(n)} > (2/5)(3/2)^{\phi(n)}$ is true for all $n > 2$. As shown in the proof of Theorem 3, the inequality $(2/5)(3/2)^{\phi(n)} > p_1 p_2 \dots p_l$ is true for $n \ne 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 30$. Moreover, by direct computation, we observe that $(1/4) \cdot 2^{\phi(n)} > p_1 p_2 \dots p_l$ is true for $n = 7, 8, 9, 14, 15, 18, 30$, and furthermore, we have

$$Q_3 = 7,\ Q_4 = 5,\ Q_5 = 31,\ Q_6 = 3,\ Q_{10} = 11,\ Q_{12} = 13.$$

Hence, $|Q_n| > p_1 p_2 \dots p_l$ holds for $n \ne 1, 2, 6$. It follows from Lemma 2 that if $n \ne 1, 2, 6$ then the n^{th} term of the Fermat sequence contains at least one primitive divisor. □

Now we are ready to prove Carmichael's theorem.

Proof of Carmichael's Theorem: As observed previously, for $n \ne 1, 2, 3, 5, 6, 12$, both the n^{th} cyclotomic number associated with the Fibonacci sequence and that associated with the Fermat sequence are greater than $p_1 p_2 \dots p_l$. It follows from Theorem 2 that if $n \ne 1, 2, 3, 5, 6, 12$ then D_n contains at least one primitive divisor. In addition, $Q_3 = L - M > 3$ except when $L = 1$, $M = -1$. Moreover, since $Q_5 = 5$ and $Q_{12} = 6$ when $L = 1$, $M = -1$, and $Q_5 = 31$ and $Q_{12} = 13$ when $L = 3$, $M = 2$, Lemma 3 gives $Q_5 > 5$ and $Q_{12} > 6$ except for the Fibonacci sequence.

Therefore, by Lemma 2, if $n \ne 1, 2, 6$ then D_n contains at least one primitive divisor except when $L = 1$, $M = -1$. Combining with Theorem 3, we complete the proof. □

4. APPENDIX

In 1955, Ward [9] proved the theorem below for the Lehmer numbers defined by

$$P_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}, \end{cases}$$

where α and β are distinct roots of the polynomial $z^2 - \sqrt{L}z + M$, and L and M are coprime integers with L positive and M nonzero. Here a sufficient condition $n \neq 6$ was pointed out by Durst [3].

Theorem 5 (Ward): If α and β are real and $n \neq 1, 2, 6$, then P_n contains at least one primitive divisor except when $n = 12$, $L = 1$, $M = -1$ and when $n = 12$, $L = 5$, $M = 1$.

We can also give an elementary proof of this theorem. It parallels the proof of Carmichael's theorem. The essential observation is that if $n \neq 1, 2, 6$ and if both the n^{th} cyclotomic number associated with $z^2 - z - 1$ and that associated with $z^2 - \sqrt{5}z + 1$ are greater than the product of all prime factors of n then, for all real Lehmer sequences, P_n contains at least one primitive divisor.

ACKNOWLEDGMENTS

I am grateful to Mr. Hajime Kajioka for his valuable advice regarding the proof of Lemma 4. In addition, I thank the anonymous referees for their useful suggestions.

REFERENCES

1. Yu Bilu, G. Hanrot, & P. M. Voutier. "Existence of Primitive divisors of Lucas and Lehmer Numbers." *J. Reine Angew. Math.* (to appear).
2. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. of Math.* **15** (1913):30-70.
3. L. K. Durst. "Exceptional Real Lehmer Sequences." *Pacific J. Math.* **9** (1959):437-41.
4. L. K. Durst. "Exceptional Real Lucas Sequences." *Pacific J. Math.* **11** (1961):489-94.
5. J. H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *The Fibonacci Quarterly* **4.3** (1966):217-40.
6. A. Schinzel. "Primitive Divisors of the Expression $A^n - B^n$ in Algebraic Number Fields." *J. Reine Angew. Math.* **268/269** (1974):27-33.
7. C. L. Stewart. "Primitive Divisors of Lucas and Lehmer Sequences." In *Transcendence Theory: Advances and Applications*, pp. 79-92. Ed. A. Baker & W. Masser. New York: Academic Press, 1977.
8. P. M. Voutier. "Primitive Divisors of Lucas and Lehmer Sequences." *Math. Comp.* **64** (1995):869-88.
9. M. Ward. "The Intrinsic Divisors of Lehmer Numbers." *Ann. of Math.* **62** (1955):230-36.

AMS Classification Numbers: 11A41, 11B39

❖❖❖