DIVISIBILITY OF GENERALIZED FIBONACCI AND LUCAS NUMBERS BY THEIR SUBSCRIPTS

Richard André-Jeannin
Ecole Nationale d'Ingénieurs de Sfax, Tunisia
(Submitted February 1990)

1. Introduction

In this paper, we shall extend some previous results ([2], [3], [4]) concerning divisibility of terms of certain recurring sequences based on their subscripts. We shall use the generalized Fibonacci and Lucas numbers, defined for $n \geq 0$ by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n,$$

where α and β are two complex numbers such that $P = \alpha + \beta$ and $Q = \alpha\beta$ are relatively prime nonzero integers. We shall exclude from consideration the case in which and are roots of unity. Then U_n and V_n are always different from zero [1]. We shall also give some applications to the equation

$$a^n \pm b^n \equiv 0 \pmod{n},$$

where $a > b \geq 1$ are relatively prime *integers*.

In what follows, $\omega(q)$ [resp. $\overline{\omega}(q)$] denotes the rank of apparition of the positive integer q in the sequence $\{U_m\}$ (resp. $\{V_m\}$), i.e., the least positive index ω (resp. $\overline{\omega}$) for which $q \mid U_\omega$ (resp. $q \mid V_{\overline{\omega}}$). Recall that the integer b is an odd multiple of the integer a if $a \mid b$ and $2 \nmid (b/a)$. The main result, which generalizes the one of Jarden [3], can be stated as follows.

Theorem 1: Let $n = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k} \geq 2$ be a natural integer.

(i) If $n \geq 2$ divides some member of the sequence $\{U_m\}$, then $U_n \equiv 0 \pmod{n}$ if and only if the rank of apparition of any prime divisor of n also divides n.

(ii) If $n \geq 3$ divides some member of the sequence $\{V_m\}$, then $V_n \equiv 0 \pmod{n}$ if and only if n is an odd multiple of $\operatorname{lcm}(\overline{\omega}(p_1), \ldots, \overline{\omega}(p_k))$.

2. Preliminary Results

The following well-known properties will be necessary for our future proofs. Proofs of these results can be found in the papers of Lucas [5] or Carmichael [1].

(i) For each integer $n \geq 1$, $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$.

(ii) If p is a prime number such that $p \nmid Q$, then $\omega(p) = p$ if and only if $p \mid (\alpha - \beta)^2$, and $\gcd(\omega(p), p) = 1$ otherwise.

(iii) If q is a prime divisor of $\omega(p)$, with $p \neq 2$ and $p \nmid (\alpha - \beta)^2$, then $q < p$. Moreover, we have

(a) $\omega(p^\lambda) = \omega(p)p^\mu$, $0 \leq \mu < \lambda$,

(b) $\omega(p_1^{\lambda_1} \ldots p_k^{\lambda_k}) = \operatorname{lcm}(\omega(p_1^{\lambda_1}), \ldots, \omega(p_k^{\lambda_k}))$, and

(c) $n \mid U_m$ if and only if $\omega(n) \mid m$.

(iv) If the prime number p divides some member of the sequence $\{V_m\}$, then

(a) $\overline{\omega}(p) < p$,

(b) $\gcd(\overline{\omega}(p), p) = 1$,

(c) $\overline{\omega}(p^\lambda) = \overline{\omega}(p)p^\mu$, $0 \le \mu < \lambda$, p odd,

(d) If $2^\lambda | V_m$, then $\overline{\omega}(2) = \overline{\omega}(2^\lambda)$, and

(e) If $n = p_1^{\lambda_1} \ldots p_k^{\lambda_k}$ divides some member of the sequence $\{V_m\}$, then $\overline{\omega}(n) = \text{lcm}(\overline{\omega}(p_1^{\lambda_1}), \ldots, \overline{\omega}(p_k^{\lambda_k}))$, and, for $n \ge 3$, $n | V_m$ if and only if m is an odd multiple of $\overline{\omega}(n)$.

3. Proof of Theorem 1

(i) Let $n = p_1^{\lambda_1} \ldots p_k^{\lambda_k} \ge 2$ be an integer which divides some member of the sequence $\{U_m\}$. First, assume that $n | U_n$. Then, for each $1 \le i \le k$, $p_i | U_n$, and $\omega(p_i) | n$. Second, assume that, for each i, $\omega(p_i) | n$.

If $p_i | (\alpha - \beta)^2$, then

$$\omega(p_i^{\lambda_i}) = \omega(p_i)p_i^{\mu_i} = p_i^{\mu_i + 1} | n,$$

since $\mu_i < \lambda_i$; otherwise,

$$\omega(p_i^{\lambda_i}) = \omega(p_i)p_i^{\mu_i} | n,$$

since $\gcd(\omega(p_i), p_i) = 1$, and $\mu_i < \lambda_i$. Thus,

$$\omega(n) = \text{lcm}(\omega(p_1^{\lambda_1}), \ldots, \omega(p_k^{\lambda_k})) | n, \quad \text{and} \quad n | U_n.$$

(ii) Now, let $n = p_1^{\lambda_1} \ldots p_k^{\lambda_k} \ge 3$ be an integer which divides some member of the sequence $\{V_m\}$. First, assume that n is an odd multiple of $\text{lcm}(\overline{\omega}(p_1), \ldots, \overline{\omega}(p_k))$. If $p = 2$, then $\overline{\omega}(p_i^{\lambda_i}) = \overline{\omega}(p_i) | n$, whereas if $p_i \ne 2$, then $\overline{\omega}(p_i^{\lambda_i}) = \overline{\omega}(p_i)p_i^{\mu_i} | n$, since $\gcd(\overline{\omega}(p_i), p_i) = 1$, and $\mu_i < \lambda_i$. Therefore, n is an odd multiple of $\overline{\omega}(n) = \text{lcm}(\overline{\omega}(p_1^{\lambda_1}), \ldots, \overline{\omega}(p_k^{\lambda_k})$, since n is an odd multiple of $\text{lcm}(\overline{\omega}(p_1), \ldots, \overline{\omega}(p_k))$. Second, assume that $n | V_n$, with $n \ge 3$. We know that n is an odd multiple of $\text{lcm}(\overline{\omega}(p_1^{\lambda_1}), \ldots, \overline{\omega}(p_k^{\lambda_k})) = \overline{\omega}(n)$. Therefore, n is an odd multiple of $\text{lcm}(\overline{\omega}(p_1), \ldots, \overline{\omega}(p_k))$, since $\overline{\omega}(p_i^{\lambda_i}) = \overline{\omega}(p_i)p_i^{\mu_i}$, p_i odd, or $\overline{\omega}(p_i^{\lambda_i}) = \overline{\omega}(p_i)$, if $p_i = 2$. This concludes the proof of Theorem 1.

Theorem 1 immediately yields the following Corollary, due to Jarden [3].

Corollary 1: (i) If $U_n \equiv 0 \pmod{n}$, and m is composed of only prime factors of n, then also $U_{mn} \equiv 0 \pmod{mn}$.

(ii) If $V_n \equiv 0 \pmod{n}$, and m is composed of only odd prime factors of n, then also $V_{mn} \equiv 0 \pmod{mn}$.

Remark 1: By application of Theorem 1 and Corollary 1, numerical examples can be obtained. For instance, let $n = p_1^{\lambda_1} \ldots p_k^{\lambda_k}$ be an odd number, such that $3 \le p_1 < \cdots < p_k$, and $n | U_n$. We have $\omega(p_1) \ne 1$, since $U_1 = 1$, and by §2(iii), $\omega(p_1) = p_1$, and $p_1 | (\alpha - \beta)^2$, since $\omega(p_1)$ is a factor of n. This case can occur only if $(\alpha - \beta)^2$ admits an odd prime divisor. Moreover, we have

$$\omega(p_i) = p_i,$$

or

$$\omega(p_i) = p_1^{\mu_1} \ldots p_{i-1}^{\mu_{i-1}}, \quad i = 2, \ldots, k; \quad \mu_j \le \lambda_j, \quad j = 1, \ldots, i - 1.$$

Theorem 1 also yields the following Corollary.

Corollary 2: If $n | U_n$, then $U_n | U_{U_n}$.

Proof: If $n | U_n$, and if p is a prime number such that $p | U_n$, then $\omega(p) | n | U_n$, and the result follows by Theorem 1.

4. The Congruence $a^n \pm b^n \equiv 0 \pmod{n}$

In what follows, we assume that $a > b \geq 1$ are relatively prime integers and that $e(n)$ denotes the rank of apparition of n in the sequence $\{a^m - b^m\}$. The next result generalizes the main theorem of [4].

Theorem 2: Let n and ab be relatively prime. Then the following statements are equivalent:

(i) $U_n \equiv 0 \pmod{n}$.
(ii) $a^n - b^n \equiv 0 \pmod{n}$.
(iii) $n \equiv 0\ [\text{mod } e(n)]$.
(iv) $n \equiv 0\ [\text{mod } e(p)]$, for each prime factor p of n.

Proof: It is clear that (i) ⇒ (ii) ⇒ (iii) ⇒ (iv). Now, assume that $n \equiv 0$ [mod $e(p)$] for each prime factor of n. If $p|a - b$, then [§2(ii)] $\omega(p) = p|n$. On the other hand, if $p\nmid a - b$, then $p|U_n$ if and only if $p|a^n - b^n$. Thus, $\omega(p) = e(p)|n$. The conclusion follows by Theorem 1.

Corollary 3: The equation $a^n - b^n \equiv 0 \pmod{n}$ has

(i) no solution if $a = b + 1$ and $n \geq 2$,
(ii) infinitely many solutions otherwise.

Proof: If $a - b$ admits at least one prime divisor p, then $p^\lambda | U_{p^\lambda}$, for each positive integer λ, by Corollary 1. On the other hand, if $a - b = 1$, then $Q = ab$ is even and n must be odd. But this case cannot occur since, if p was the least prime factor of n, we would have, by Remark 1 above,

$$\omega(p) \,|\, (a - b)^2. \quad \text{Q.E.D.}$$

Corollary 4: The equation $a^n + b^n \equiv 0 \pmod{n}$ admits infinitely many solutions.

Proof: If $V_1 = a + b$ admits an odd prime divisor p, then $p^\lambda | V_{p^\lambda}$, for each $\lambda \geq 1$, by Theorem 1 and Corollary 1. On the other hand, suppose that

$$V_1 = a + b = 2^m, \quad m \geq 2.$$

Thus a and b are odd and

$$V_2 = (a + b)^2 - 2ab = 2(2^{2m-1} - Q),$$

where $2^{2m-1} - Q > 1$ is odd, since Q is also odd. Thus, V_2 admits an odd prime divisor p, and $2p$ is an odd multiple of $\text{lcm}(\overline{\omega}(2), \overline{\omega}(p)) = 2$. By Theorem 1 and Corollary 1, we have

$$2p^\alpha | V_{2p^\alpha}, \quad \alpha \geq 1. \quad \text{Q.E.D.}$$

References

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetical Forms $\alpha^n \pm \beta^n$." *Ann of Math.* *2.15* (1913):30-70.
2. V. E. Hoggatt, Jr. & G. E. Bergum. "Divisibility and Congruence Relations." *Fibonacci Quarterly* *12.2* (1974):189-95.
3. D. Jarden. *Recurring Sequences.* 3rd ed. Jerusalem: Riveon Lematematika, 1973.
4. R. E. Kennedy & G. N. Cooper. "Niven Repunits and $10^n \equiv 1 \pmod{n}$." *Fibonacci Quarterly* *27.2* (1989):139-43.
5. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* *1* (1878):184-220, 289-321.

*****