A NOTE ON THE DIVISIBILITY OF THE GENERALIZED LUCAS SEQUENCES

Pingzhi Yuan
Dept. of Math. and Mechanics, Central South University, Hunan Changsha, 410075, P.R. China
e-mail: yuanpz@csru.edu.cn

(Submitted January 2000-Final Revision March 2001)

In this paper we discuss the divisibility theory of the generalized Lucas sequences U_n and V_n which were defined by D. H. Lehmer [1] as follows:

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \tag{1}$$

$$V_n = \alpha^n + \beta^n, \quad V_0 = 2, \tag{2}$$

where $\alpha = (\sqrt{R} + \sqrt{\Delta})/2$, $\beta = (\sqrt{R} - \sqrt{\Delta})/2$ are the roots of $x^2 - R^{1/2}x + Q = 0$, R and Q are coprime integers, $R > 0$, the discriminant $\Delta = R - 4Q$, and $n \geq 0$ is an integer.

The main theorem of this paper is a complement of that of Lehmer [1], and this result is essential in the applications to exponential Diophantine equations, as we will show in another paper. Moreover, the main results of McDaniel [2] will be extended, and this can be deduced easily from the main theorem of this paper.

It is easy to see that U_{2k+1} and V_{2k} are rational integers and that U_{2k} and V_{2k+1} are integral multiples of $R^{1/2}$. Let Z be the set of integers, $R^{1/2}Z = \{aR^{1/2} \mid a \in Z\}$. If we define the divisibility of the elements of the set $Z \cup R^{1/2}Z$ as follows: For any A, $B \in Z \cup R^{1/2}Z$, $A|B \Leftrightarrow B = A \cdot C$, and $C \in Z \cup R^{1/2}Z$, then most of the propositions below are well known (see, e.g., [3], Chapter 2). Proposition 1(e) was recently proved in [2]; however, as we will show, this proposition is not true for the most general definition of the generalized Lucas sequences as defined above.

Proposition 1: Let m and n be arbitrary integers:

(a) $V_n^2 - \Delta U_n^2 = 4Q^n$.

(b) If $m|n$, then $U_m | U_n$; if n/m is odd, then $V_m | V_n$.

(c) $U_{2n} = U_n V_n$; $V_{2n} = V_n^2 - 2Q^n$.

(d) If $d = \gcd(m, n)$, then $\gcd(U_m, U_n) = U_d$.

(e) If $d = \gcd(m, n)$, then $\gcd(V_m, V_n) = V_d$ if m/d and n/d are odd, and 1, or 2, otherwise.

(f) If p is a prime and ω is the minimal positive integer with $p|U_\omega$ ([1] defined ω to be the appearance of p in U_n), then for any positive integers k and λ, we have $p^{\lambda+1} | U_{k\omega p^\lambda}$.

(g) If an odd prime p, with $p \nmid R\Delta$, $\varepsilon = (\Delta R/p)$ is the Kronecker symbol, then $U_{p-\varepsilon} \equiv 0 \pmod{p}$.

For any prime p, $A \in Z \cup R^{1/2}Z$, $\mathrm{ord}_p A$ is defined to be the rational number s with $2s$ being an integer and $p^{2s} \| A^2$, denoted by $\mathrm{ord}_p A = s$. We now have the following theorem.

Theorem 1: If p, q are odd primes and s, t are positive integers with $p^s \| \Delta$, $q^t \| R$, then:

(a) If $p^s > 3$, then $\mathrm{ord}_p U_m = \mathrm{ord}_p m$, $\mathrm{ord}_p V_m = 0$.

(b) For $q^t > 3$: if m is odd, then $\mathrm{ord}_q U_m = 0$, $\mathrm{ord}_q V_m / V_1 = \mathrm{ord}_q m$; if m is even, then $\mathrm{ord}_q V_m = 0$, $\mathrm{ord}_q U_m = \mathrm{ord}_q m + t/2$.

(c) Suppose $p^s = 3$ and λ is an integer with $3^\lambda \| 3R+\Delta$, then $\mathrm{ord}_3 V_m = 0$, $\mathrm{ord}_3 U_{3m} = \lambda + \mathrm{ord}_3 m$; if $3 \nmid m$, then $\mathrm{ord}_3 U_m = 0$.
(d) Suppose now that $q^t = 3$ and μ is an integer with $3^\mu \| 3\Delta + R$. If m is odd, then $\mathrm{ord}_3 U_m = 0$, $\mathrm{ord}_3 V_{3m}/V_1 = \mathrm{ord}_3 m + \mu$, and $\mathrm{ord}_3 V_m / V_1 = 0$ with $3 \nmid m$; if m is even, then $\mathrm{ord}_3 V_m = 0$, $\mathrm{ord}_3 U_{3m} = \mathrm{ord}_3 m + \mu + 1/2$, and $\mathrm{ord}_3 U_m = 1/2$ with $3 \nmid m$.
(e) Let $2 \| R$: if $2 \nmid m$, then $\mathrm{ord}_2 U_m = \mathrm{ord}_2 V_m / V_1 = 0$ $(2 \nmid m)$; if $2 \| m$, then $\mathrm{ord}_2 V_m = \mathrm{ord}_2 V_2$ and $\mathrm{ord}_2 U_m = 1/2$; if $4 | m$, then $\mathrm{ord}_2 V_m = 1/2$ and $\mathrm{ord}_2 U_m = \mathrm{ord}_2 m - 1/2$.
(f) Let $4 | R$: if m is odd, then $\mathrm{ord}_2 U_m = 0$ and $\mathrm{ord}_2 V_m = \mathrm{ord}_2 V_1$; if m is even, then $\mathrm{ord}_2 U_m = \mathrm{ord}_2 m + \frac{1}{2}\mathrm{ord}_2 R - 1$ and $\mathrm{ord}_2 V_m = 1$.

Proof: We divide the proof of the theorem into three parts:

(I) If m is odd, subtracting the m^{th} power of $2\beta = R^{1/2} - \Delta^{1/2}$ from the m^{th} power of $2\alpha = R^{1/2} + \Delta^{1/2}$, we get

$$2^{m-1}U_m = \sum_{i=0}^{(m-1)/2} \binom{m}{2i+1} \Delta^i R^{(m-2i-1)/2} = mR^{(m-1)/2} + \sum_{i=1}^{(m-1)/2} \frac{m}{2i+1}\binom{m-1}{2i} \Delta^i R^{(m-2i-1)/2}. \tag{3}$$

Let u be a positive integer with $p^u \| m$, $u > 0$, and notice that

$$\mathrm{ord}_p \frac{m}{2i+1}\Delta^i = si + u - \mathrm{ord}_p(2i+1) \ge si + u - \log_p(2i+1). \tag{4}$$

If $p^s \ne 3$, then $p^{si} > 2i+1$ for any $i \ge 1$, so from (4) we know that every term of the summation of (3) is a multiple of p^{u+1}; therefore, $\mathrm{ord}_p U_m = \mathrm{ord}_p m = u$. This result together with Proposition 1(a) and $(R, Q) = 1$ implies that $\mathrm{ord}_p V_m = 0$, i.e., Theorem 1(a) holds for odd m.

If $p^s = 3$, then $4U_3 = 3R + \Delta$, so from (3) we conclude that $3 | U_m$ when $3 | m$. Subtracting the m^{th} power of $2\beta^3 = V_3 - \Delta^{1/2}U_3$ from the m^{th} power of $2\alpha^3 = V_3 + \Delta^{1/2}U_3$, we get

$$2^{m-1}U_{3m}/U_3 = \sum_{i=0}^{(m-1)/2} \binom{m}{2i+1} (\Delta U_3^2)^i V_3^{m-2i-1}. \tag{5}$$

Similar to the above, we have $\mathrm{ord}_3 U_{3m}/U_3 = \mathrm{ord}_3 m$ and $\mathrm{ord}_3 V_m = 0$, i.e., Theorem 1(c) holds for odd m.

If m is odd, from [1] and Proposition 1(a) we have

$$2^{m-1}V_m/V_1 = \sum_{i=0}^{(m-1)/2} \binom{m}{2i+1} R^i \Delta^{(m-2i-1)/2}, \tag{6}$$

$$R(V_m/V_1)^2 - \Delta U^2 = 4Q^m. \tag{7}$$

Symmetrically, from (6) and (7) we conclude that Theorem 1(b) and (d) hold for odd m.

(II) Now suppose that m is even, then $U_2^2 = R$, so $R | U_m^2$ for any even m; therefore, $\mathrm{ord}_p V_m = 0 = \mathrm{ord}_q V_m$ by Proposition 1(a). Let $m = 2^a m_1$, $2 \nmid m_1$, $a \ge 1$, be an integer, and notice that by Proposition 1(c) we have

$$U_{2^a m_1} = U_{m_1} V_{m_1} V_{2m_1} \dots V_{2^{a-1}m_1}. \tag{8}$$

Thus, $\mathrm{ord}_p U_m = \mathrm{ord}_p U_{m_1}$ and $\mathrm{ord}_q U_m = \mathrm{ord}_q V_{m_1}$, and from the above result of the odd number m_1 we know that Theorem 1(a)-(d) hold for even m.

(III) For Theorem 1(e), it is well-known that $\{U_m\}$ satisfies the following recurrence relation,

$$U_{m+2} = R^{1/2}U_{m+1} - QU_m, \quad U_0 = 0, \ U_1 = 1. \tag{9}$$

Since $(R, Q) = 1$ and $2 \| R$, we have $Q \equiv 1 \pmod 2$ and $\Delta = R - 4Q \equiv 2 \pmod 4$. Taking modulo 2 for the sequence (9), we obtain a sequence with a period 4,

$$U_m \equiv 0, 1, R^{1/2}, 1, 0, 1, R^{1/2}, 1, \ldots. \tag{10}$$

If $2 \nmid m$, then (10) implies that $\mathrm{ord}_2 U_m = 0$, and from $2 \| \Delta$ and $V_m^2 - \Delta U_m^2 = 4Q^m$ we have $\mathrm{ord}_2 V_m = 1/2$; if $4|m$, then (10) implies that $\mathrm{ord}_2 U_m \geq 1$, and from $2\|\Delta$ and $V_m^2 - \Delta U_m^2 = 4Q^m$ we have $\mathrm{ord}_2 V_m = 1$. Then from (8) we have

$$\mathrm{ord}_2 U_m = \mathrm{ord}_2 U_{m_1} + \mathrm{ord}_2 V_{m_1} + \sum_{i=1}^{a-1} \mathrm{ord}_2 V_{2^i m_1} = 0 + \frac{1}{2} + (a-1) = \mathrm{ord}_2 m - \frac{1}{2}.$$

If $2\|m$, say, $m = 2m_1$, $2 \nmid m_1$, then $V_2 \equiv R - 2Q \equiv 0 \pmod 4$, and adding the m^{th} powers of $2\alpha^2 = V_2 + (R\Delta)^{1/2}$ and $2\beta^2 = V_2 - (R\Delta)^{1/2}$, we get

$$2^{m_1 - 1} V_{2m_1} / V_2 = \sum_{i=0}^{(m_1-1)/2} \binom{m_1}{2i+1} V_2^{2i} (\Delta R)^{(m_1 - 2i - 1)/2} \tag{11}$$

and $\mathrm{ord}_2(V_2^{2i}(\Delta R)^{(m_1-2i-1)/2}) \geq m_1 - 1$, and the equality holds if and only if $i = 0$. Thus, by taking modulo 2^{m_1} for (11), we get $\mathrm{ord}_2 V_{2m_1}/V_2 = 0$, and from (8) we have $\mathrm{ord}_2 V_{2m_1} = \mathrm{ord}_2 V_{m_1} = 1/2$. Summing the above result we complete the proof of Theorem 1(e).

For Theorem 1(f), if $4|R$, put $R = 4R_1$, then $\Delta = R - 4Q = 4\Delta_1$ and Q is odd, so $2|R_1\Delta_1$, and if m is odd,

$$U_m = \sum_{i=0}^{(m-1)/2} \binom{m}{2i+1} \Delta_1^i R_1^{(m-2i-1)/2} = mR_1^{(m-1)/2} + \sum_{i=1}^{(m-3)/2} \frac{m}{2i+1}\binom{m-1}{2i} \Delta_1^i R_1^{(m-2i-1)/2} + \Delta_1^{(m-1)/2}.$$

Therefore, $\mathrm{ord}_2 U_m = 0$. Similarly, $\mathrm{ord}_2 V_m = \mathrm{ord}_2 V_1$. If m is even, then from (8) we have $2|U_m$, and $V_m^2/4 - \Delta_1 U_m^2 = Q^m$ implies that $V_m/2$ is odd, i.e., $\mathrm{ord}_2 V_m = 1$. From the results for odd m and again using (8) we have $\mathrm{ord}_2 U_m = \mathrm{ord}_2 m - 1 + \mathrm{ord}_2 V_1 = \mathrm{ord}_2 m + \frac{1}{2}\mathrm{ord}_2 R - 1$. This completes the proof of Theorem 1.

Remark 1: Put $\alpha_1 = \alpha^m$, $\beta_1 = \beta^m$, $R_1 = \alpha_1 + \beta_1$, $\Delta_1 = (\alpha_1 - \beta_1)^2$, $U_n^{(1)} = (\alpha_1^n - \beta_1^n)/(\alpha_1 - \beta_1)$, and $V_n^{(1)} = \alpha_1^n + \beta_1^n$. Then we have $U_n^{(1)} = U_{mn}/U_m$, $V_n^{(1)} = V_{mn}$, and $\Delta_1 = \Delta U_m^2$. Applying Theorem 1 to $U_n^{(1)}$, $V_n^{(1)}$, we obtain the largest power of q in U_n or V_n if $q|U_m$ or $q|V_m$.

Now let us remark that if $2 \nmid R$ then $2 \nmid \Delta$, since U_n and V_n satisfy recurrence relation (9) and the following one, respectively,

$$V_{n+2} = R^{1/2} V_{m+1} - QV_m, \quad V_0 = 2, \ V_1 = R^{1/2}. \tag{12}$$

Taking modulo 2, we have $2 \nmid U_m V_m$ when $m > 0$, and if $2 \nmid Q$ then $2|U_m$ and $2|V_m$ if and only if $3|m$ and $3|n$, respectively. Hence, from Remark 1 and the above discussion, we need only consider the case of $2|R$ when we study the behavior of the 2-part of U_m and V_n.

We will now prove the following corollary which is an extension of Proposition 1(e) above.

Corollary: If $d = \gcd(m, n)$, then $\gcd(V_m, V_n) = V_d$ if m/d and n/d are odd, and 1, $\sqrt{2}$, or 2, otherwise.

Proof: For $d = \gcd(m, n)$, we may suppose without loss of generality that $km = d + \ell n$, where k and ℓ are positive integers. If k is odd, notice that $V_m | V_{km}$ and $(U_m, V_m) | 2$ for any $m \geq 0$ and

$$2V_{km} = (\alpha^d - \beta^d)(\alpha^{\ell n} - \beta^{\ell n}) + V_d V_{\ell n} \tag{13}$$

and $V_n | V_{\ell n}$ if ℓ is odd, $V_n | U_{\ell n}$ if ℓ is even. Thus,

$$(V_m, V_n) | ((\alpha^d - \beta^d)(\alpha^{\ell n} - \beta^{\ell n}),\ V_d V_{\ell n}) | 8V_d. \tag{14}$$

If k is even, then ℓn is an odd multiple of d, and we see that

$$2(\alpha^{km} - \beta^{km}) / (\alpha^d - \beta^d) = V_d(\alpha^{\ell n} - \beta^{\ell n}) / (\alpha^d - \beta^d) + V_{\ell n}, \tag{15}$$

$V_m | 2(\alpha^{km} - \beta^{km}) / (\alpha^d - \beta^d)$, and $V_n | V_{\ell n}$, so

$$(V_m, V_n) | 2V_d. \tag{16}$$

Furthermore, for any prime divisor p of $2V_d$ from Remark 1, applying Theorem 1 to V_m and V_n we obtain the desired results.

Remark 2: Lehmer proved the following theorem.

Theorem A (Lehmer [1], Theorem 1.6): If 2α is a positive integer such that q^α is the highest power of a prime q dividing U_m, and if k is any integer not divisible by q, then for any integer λ, U_{kmq^λ} is divisible by $q^{\alpha+\lambda}$, and if $q^\alpha \neq 2$, this is the highest power of q dividing U_{kmq^λ}.

Comparing Theorem A with Theorem 1 of this paper, we can easily find out that: If $q^\alpha = 3$, $m = 2$, $3 \| R$, and $9 | 3\Delta + R$, and we put $\lambda = 1$ in Theorem A, then the last conclusion of Theorem A is incorrect. This is indispensable in its applications to exponential Diophantine equations, as will be shown in a future paper.

Example: Let $R = 2$ and $\Delta = -1$, then we have

$$V_0 = 2,\ V_1 = \sqrt{2},\ V_2 = 4,\ V_3 = 5\sqrt{2},\ V_4 = 14,\ V_5 = 19\sqrt{2}, \ldots,$$

which means that $\gcd(V_4, V_5) = \sqrt{2}$.

ACKNOWLEDGMENT

The author is very grateful to the anonymous referee from valuable suggestions.

REFERENCES

1. D. H. Lehmer. "An Extended Theory of Lucas Functions." *Ann. Math.* **31** (1930):419-48.
2. W. L. McDaniel. "The g.c.d. in Lucas Sequences and Lehmer Number Sequences." *The Fibonacci Quarterly* **29.1** (1991):24-29.
3. P. Ribenboim. *The Book of Prime Number Records.* New York: Springer-Verlag, 1989.

AMS Classification Numbers: 11B37, 11A07

❖❖❖