THE G.C.D. IN LUCAS SEQUENCES AND LEHMER NUMBER SEQUENCES

Wayne L. McDaniel
University of Missouri-St. Louis, St. Louis, MO 63121
(Submitted December 1988)

1. Introduction

Let P and Q be relatively prime integers, α and β ($\alpha > \beta$) be the zeros of $x^2 - Px + Q$, and, for $k = 0, 1, 2, 3, \ldots$, let

$$(1) \qquad U_k = U_k(P, Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{and} \quad V_k = V_k(P, Q) = \alpha^k + \beta^k.$$

The following result is well known.

Theorem 0: Let m and n be positive integers, and $d = \gcd(m, n)$.

(i) $\gcd(U_m, U_n) = U_d$;

(ii) if $\frac{m}{d}$ and $\frac{n}{d}$ are odd, $\gcd(V_m, V_n) = V_d$;

(iii) if $m = n$, $\gcd(U_m, V_n) = 1$ or 2.

Using basic identities, Lucas proved Theorem 0 in the first of his two 1878 articles in which he developed the general theory of second-order linear recurrences [5]; Lucas had previously proven parts (i) and (iii) in his 1875 article [4]. Nearly four decades later, Carmichael [1] used the theory of cyclotomic polynomials to obtain both new results and results confirming and generalizing many of Lucas' theorems; Theorem 0 was among the results obtained using cyclotomic polynomials.

Curiously, the value of $\gcd(V_m, V_n)$ when m and n are not divisible by the same power of 2, and of $\gcd(U_m, V_n)$ for $m \neq n$, do not appear in the literature, and have, apparently, never been established. It is interesting that the values of all three of these gcd's can be rather easily found, for *all* pairs of positive integers m and n, by the application of an approach similar to that used in establishing the Euclidean algorithm to a single sequence of equations. We shall prove the following result.

Main Theorem: Let $m = 2^a m'$, $n = 2^b n'$, m' and n' odd, a and $b \geq 0$, and let $d = \gcd(m, n)$. Then

(i) $\gcd(U_m, U_n) = U_d$,

(ii) $\gcd(V_m, V_n) = \begin{cases} V_d & \text{if } a = b, \\ 1 \text{ or } 2 & \text{if } a \neq b; \end{cases}$

(iii) $\gcd(U_m, V_n) = \begin{cases} V_d & \text{if } a > b, \\ 1 \text{ or } 2 & \text{if } a \leq b. \end{cases}$

The value of $\gcd(V_m, V_n)$ is even if any only if Q is odd and either P is even or $3|d$; $\gcd(U_m, V_n)$ is even if and only if Q is odd and (1) P and d are even, or (2) P is odd and $3|d$.

Our definition of U_k and V_k assures that the above result holds for all second-order linear recurring sequences $\{U_k\}$ and $\{V_k\}$ satisfying

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = PU_{n+1} - QU_n,$$

and

$$V_0 = 2,\ V_1 = P,\ V_{n+2} = PV_{n+1} - QV_n.$$

If $P = 1$ and $Q = -1$, the sequences are the Fibonacci and Lucas number sequences, respectively; for this case, a nice alternate proof of (ii) has been communicated to the author by Paulo Ribenboim, and appears now in [6]. If one defines the sequence $\{U_n\}$ more generally, by

$$U_1 = a,\ U_2 = b,\ U_{n+2} = cU_{n+1} + dU_n,$$

then Lucas' result [(i) above] will hold under certain circumstances: P. Horak & L. Skula [2] have characterized those sequences for which (i) holds.

In our last section, we shall observe that a result analogous to Theorem 1 holds for Lehmer numbers and the "associated" Lehmer numbers.

2. Preliminary Results

We base our proof on the following formulas, all of which are well-known, and are easily verified directly from the definition (1) of U_k and V_k.

Property L: Let $r > s \geq 0$, $e = \min\{r - s, s\}$, and $D = P^2 - 4Q$.

L(i) $\quad U_r = V_{r-s}U_s \pm Q^eU_{|r-2s|}$, where the + sign is used iff $r - 2s \geq 0$,

L(ii) $\quad V_r = V_{r-s}V_s - Q^eV_{|r-2s|}$,

L(iii) $\quad U_r = U_{r-s}V_s \pm Q^eU_{|r-2s|}$, where the + sign is used iff $r - 2s < 0$,

L(iv) $\quad V_r = DU_{r-s}U_s + Q^eV_{|r-2s|}$,

L(v) $\quad V_r^2 = DU_r^2 + 4Q^r$.

We will use the fact that, for $k > 0$,

(2) $\quad \gcd(U_k, Q) = \gcd(V_k, Q) = 1$,

which is also readily shown from (1) [or see [1], Th. I].

Finally, we require this result concerning the parity of U_k and V_k, which is easily deduced from (1), using $P = \alpha + \beta$ and $Q = \alpha\beta$ (or see [1], Th. III):

Parity Conditions: If $k = 0$, $U_k = 1$ and $V_k = 2$. Let $k > 0$.

(i) If Q is even, both U_k and V_k are odd;

(ii) If Q is odd and P is even, then V_k is even, and U_k is even iff k is;

(iii) If Q is odd and P is odd, then U_k and V_k are both even iff $3|k$.

3. The Basic Result

Let $\{\gamma_i\}$ and $\{\delta_i\}$ ($i \geq 0$) be sequences of integers. Let $m_0 = 2^AM$ and $n_0 = 2^BN$ be positive integers with A and $B \geq 0$, M and N odd, and $m_0 > n_0$, and let

$$d_0 = |m_0 - 2n_0| \quad \text{and} \quad d = \gcd(m_0, n_0);$$

let G_{m_0} and H_{n_0} be integers, and K_{d_0} be defined by

$$G_{m_0} = \gamma_0H_{n_0} + \delta_0K_{d_0}.$$

Theorem 1: For $j = 1, 2, 3, \ldots$, let

$$m_j = n_{j-1},\ n_j = d_{j-1},\ G_{m_j} = H_{n_{j-1}} \text{ and } H_{n_j} = K_{d_{j-1}}, \quad \text{if } n_{j-1} \geq d_{j-1},$$

or

$$m_j = d_{j-1},\ n_j = n_{j-1},\ G_{m_j} = K_{d_{j-1}} \text{ and } H_{n_j} = H_{n_{j-1}}, \quad \text{if } n_{j-1} < d_{j-1},$$

let $d_j = |m_j - 2n_j|$, and let K_{d_j} be defined by

$$G_{m_j} = \gamma_jH_{n_j} + \delta_jK_{d_j}.$$

If, for $j \geq 0$, $\gcd(G_{m_j}, \delta_j) = 1$, then

$$\gcd(G_{m_0}, H_{n_0}) = \begin{cases} \gcd(H_d, K_d) & \text{if } A = B, \\ \gcd(H_d, K_0) & \text{if } A \neq B. \end{cases}$$

Proof: For each pair of integers r and s, we let (r, s) denote $\gcd(r, s)$. The definitions of m_j, n_j, and d_j imply that $\{m_j\}$ is a nonincreasing sequence of positive integers; let k be the least integer such that $m_{k-1} = m_k$. Now, it is clear, from our definitions above, that

$$\begin{aligned}(m_0, n_0) &= (n_0, d_0) = (m_1, n_1) = (n_1, d_1) = \cdots \\ &= (m_{k-1}, n_{k-1}) = (n_{k-1}, d_{k-1}).\end{aligned}$$

Furthermore, by our assumptions that $G_{m_j} = \gamma_j H_{n_j} + \delta_j K_{d_j}$ and $(G_{m_j}, \delta_j) = 1$, we have, similarly

$$(G_{m_0}, H_{n_0}) = (H_{n_0}, K_{d_0}) = \cdots = (H_{n_{k-1}}, K_{d_{k-1}}).$$

Since, by definition, $m_k = \max\{n_{k-1}, d_{k-1}\}$, $m_{k-1} = n_{k-1}$ or d_{k-1}.

Case 1. If $m_{k-1} = n_{k-1}$, then $d_{k-1} = |m_{k-1} - 2n_{k-1}| = m_{k-1}$ also, so

$$(m_0, n_0) = (n_{k-1}, d_{k-1}) = m_{k-1};$$

that is, $d = m_{k-1} = n_{k-1} = d_{k-1}$. Hence, in Case 1,

$$(G_{m_0}, H_{n_0}) = (H_d, K_d).$$

Case 2. If $m_{k-1} = d_{k-1} \neq n_{k-1}$, then $d_{k-1} = |m_{k-1} - 2n_{k-1}|$ implies $n_{k-1} = 0$. But, then, since $n_{k-1} = \min\{n_{k-2}, d_{k-2}\}$, $d_{k-2} = 0$; this implies

$$d = (m_0, n_0) = (n_{k-2}, 0) = n_{k-2}.$$

Hence, in Case 2,

$$(G_{m_0}, H_{n_0}) = (H_{n_{k-2}}, K_{d_{k-2}}) = (H_d, K_0).$$

For $j \geq 0$, let $M_j = m_j/d$, $N_j = n_j/d$, and $D_j = d_j/d$. If $A = B$, M_0, N_0, and D_0 are each odd; consequently, M_j, N_j, and D_j are odd for $j = 0, 1, 2, 3, \ldots$. This is possible only in Case 1, since, in Case 2, $d_{k-2} = 0$, implying that D_{k-2} is even. If $A \neq B$, it is easy to see that, for each j, exactly one or exactly two of the three integers M_j, N_j, and D_j is (are) even, and this is possible only in Case 2, since, in Case 1, $M_{k-1} = N_{k-1} = D_{k-1}$. This proves the theorem.

4. Proof of the Main Theorem

For $j \geq 0$, we assume that m_j, n_j, d_j, G_{m_j}, H_{n_j}, and K_{d_j} are as defined in Section 3, and M_j, N_j, and D_j are as defined in the proof of Theorem 1. Let $S(r)$ denote the number of integers j, $0 < j \leq k$, such that $n_{j-1} \geq d_{j-1}$, and for each positive integer i, let $p(i)$ denote the parity of i.

Lemma 1: If $A \neq B$, and if there exists an integer k such that $d_k = 0$, then $S(k)$ is even if and only if $A > B$.

Proof: Assume $A \neq B$ and that there exists an integer k such that d_k (and hence, D_k) equals 0. It is clear that the number of integers j, $0 < j \leq k$ such that $N_{j-1} \geq D_{j-1}$ is $S(k)$. Now, $A \neq B$ implies that, for each j,

$$(p(M_j), p(N_j), p(D_j)) = (\text{even, odd, even}) \text{ or } (\text{odd, even, odd}),$$

and it is clear from the definitions of m_j and n_j that $S(k)$ is precisely the number of changes from one of these two forms to the other, as j assumes the values $0, 1, 2, \ldots, k$. Since $d_k = 0$,

$$(p(M_k), p(N_k), p(D_k)) = (\text{even, odd, even});$$

it follows that $S(k)$ is even if and only if M_0 is even; that is, if and only if $A > B$.

Proof of the Main Theorem: Let $e_j = \min\{m_j - n_j, n_j\}$.

(i) We assume without loss of generality that $m \geq n$, let $m = m_0$, $n = n_0$, and apply Theorem 1 with $G_{m_0} = U_{m_0}$, $H_{n_0} = U_{n_0}$, $\gamma_j = V_{m_j - n_j}$, and $\delta_j = \pm Q^{e_j}$, where the + sign is chosen if and only if $m_j - 2n_j \geq 0$, for $j \geq 0$. For each $j \geq 0$, $G_{m_j} = \gamma_j H_{n_j} + \delta_j K_{d_j}$ implies that $K_{d_j} = U_{d_j}$, by property L(i); since $(G_{m_j}, \delta_j) = 1$, as observed in Section 2,

$$\gcd(U_m, U_n) = \gcd(U_d, U_d) = U_d, \text{ if } a = b,$$

and

$$\gcd(U_m, U_n) = \gcd(U_d, U_0) = \gcd(U_d, 0) = U_d, \text{ if } a \neq b.$$

(ii) Assume, again without loss of generality, that $m \geq n$, and let $m = m_0$ and $n = n_0$. Defining G_{m_0}, H_{n_0}, K_{d_j}, γ_j, and δ_j as V_{m_0}, V_{n_0}, V_{d_j}, $V_{m_j - n_j}$, and $-Q^{e_j}$, for $j \geq 0$, respectively, we have, by Theorem 1 and L(ii),

$$\gcd(V_m, V_n) = \gcd(V_d, V_d) = V_d \text{ if } a = b,$$

and

$$\gcd(V_m, V_n) = \gcd(V_d, 2) = 1 \text{ or } 2 \text{ if } a \neq b,$$

proving (ii).

(iii) Case 1. Assume $m \geq n$, let $m = m_0$ and $n = n_0$, and define G_{m_0}, H_{n_0}, K_{d_0}, γ_0, and δ_0 as U_{m_0}, V_{n_0}, U_{d_0}, $U_{m_0 - n_0}$ and $\pm Q^{e_0}$, where the + sign is used if and only if $m_0 - 2n_0 < 0$. For $j = 1, 2, 3, \ldots$, let $\gamma_j = DU_{m_j - n_j}$, $\delta_j = Q^{e_j}$, and $K_{d_j} = V_{d_j}$ *if* $G_{m_j} = V_{n_{j-1}}$; and $\gamma_j = U_{m_j - n_j}$, $\delta_j = \pm Q^{e_j}$, and $K_{d_j} = U_{d_j}$ *if* $G_{m_j} = U_{n_{j-1}}$, where the + sign is used if and only if $m_j - 2n_j < 0$. Corresponding to each j $(j \geq 0)$, then, $G_{m_j} = \gamma_j H_{n_j} + \delta_j K_{d_j}$ is either L(iii) or L(iv).

If $a = b$, Theorem 1 implies

$$\gcd(U_m, V_n) = \gcd(V_d, U_d) \text{ [or, } \gcd(U_d, V_d)],$$

and it is immediate from (2) and L(v) that this integer is either 1 or 2.

If $a \neq b$, Theorem 1 implies

$$\gcd(U_m, V_n) = \gcd(V_d, U_0) = \gcd(V_d, 0) = V_d,$$

or

$$\gcd(U_m, V_n) = \gcd(U_d, V_0) = \gcd(U_d, 2) = 1 \text{ or } 2.$$

Now, $G_{m_r} = \gamma_r H_{n_r} + \delta_r K_{d_r}$ changes from one of the forms L(iii) or L(iv) to the other as r changes from $j - 1$ to j if and only if $n_{j-1} \geq d_{j-1}$; hence, the number of such changes as j assumes the values $0, 1, 2, \ldots, k$, is $S(k)$. Since $K_{d_0} = U_{d_0}$, the integer k such that $K_{d_k} = U_0$ exists if and only if $S(k)$ is even, and, by Lemma 1, this happens if and only if $a > b$; that is, if $a \neq b$, $\gcd(U_m, V_n) = V_d$ if and only if $a > b$.

Case 2. Assume $n > m$, let $n = m_0$ and $m = n_0$, and define G_{m_0}, H_{n_0}, K_{d_0}, γ_0, and δ_0 to be V_{m_0}, U_{n_0}, V_{d_0}, $DU_{m_0 - n_0}$, and Q^{e_0}, respectively. All the remaining definitions parallel those in Case 1 in the obvious way, and the proof is similar.

The conditions determining whether $\gcd(V_m, V_n)$ or $\gcd(U_m, V_n)$ is 1 or 2 follow immediately from the parity conditions in Section 2.

Letting $F_k = U_k(1, -1)$ and $L_k = V_k(1, -1)$ represent the k^{th} Fibonacci and Lucas numbers, respectively, we have the following corollary.

Corollary: If $m = 2^a m'$, $n = 2^b n'$, m' and n' odd, a and $b \geq 0$, and $d = \gcd(m, n)$, then

(i) $\gcd(F_m, F_n) = F_d$;

(ii) $\gcd(L_m, L_n) = L_d$ if $a = b$, 2 if $a \neq b$ and $3 \mid d$, and 1 if $a \neq b$ and $3 \nmid d$;

(iii) $\gcd(F_m, L_n) = L_d$ if $a > b$, 2 if $a \le b$ and $3 | d$, and 1 if $a \le b$ and $3 \nmid d$.

5. Lehmer Numbers

Let R be an integer relatively prime to Q. We let α and β denote the zeros of $x^2 - \sqrt{R}x + Q$, and redefine

$$U_k = U_k(\sqrt{R}, Q) = \begin{cases} (\alpha^k - \beta^k)/(\alpha - \beta), & \text{if } k \text{ is odd,} \\ (\alpha^k - \beta^k)/(\alpha^2 - \beta^2), & \text{if } k \text{ is even,} \end{cases}$$

and

$$V_k = V_k(\sqrt{R}, Q) = \begin{cases} (\alpha^k + \beta^k)/(\alpha + \beta), & \text{if } k \text{ is odd,} \\ (\alpha^k + \beta^k), & \text{if } k \text{ is even.} \end{cases}$$

The numbers U_k and V_k were defined by Lehmer, who developed many of the properties of this generalization of Lucas sequences in his 1930 paper [3]. The numbers are known, respectively, as Lehmer numbers and the "associated" Lehmer numbers.

The Main Theorem is true for Lehmer numbers and the associated Lehmer numbers, except that appropriate changes must be made in the statement concerning the parity of the greatest common divisors. We shall not restate the theorem, and refer the reader to [3], Theorem 1.3, for the parity conditions for U_k and V_k.

Both U_k and V_k are prime to Q ([3], Th. 1.1), and it is not difficult to show, directly from the definitions above, the following counterpart of Property L:

Property L': Let $r > s \ge 0$, $e = \min\{r - s, s\}$, and $\Delta = R - 4Q$.

L'(i) $U_r = RV_{r-s}U_s \pm Q^e U_{|r-2s|}$, if r is odd and s is even,
$U_r = V_{r-s}U_s \pm Q^e U_{|r-2s|}$, otherwise;

L'(ii) $V_r = RV_{r-s}V_s - Q^e V_{|r-2s|}$, if r is even and s is odd,
$V_r = V_{r-s}V_s - Q^e V_{|r-2s|}$, otherwise;

L'(iii) $U_r = RU_{r-s}V_s \pm Q^e U_{|r-2s|}$, if r and s are odd,
$U_r = U_{r-s}V_s \pm Q^e U_{|r-2s|}$, otherwise;

L'(iv) $V_r = R\Delta U_{r-s}U_s + Q^e V_{|r-2s|}$, if r and s are even,
$V_r = \Delta U_{r-s}U_s + Q^e V_{|r-2s|}$, otherwise;

L'(v) $RV_r^2 = \Delta U_r^2 + 4Q^r$, if r is odd,
$V_r^2 = R\Delta U_r^2 + 4Q^r$, if r is even.

The + sign is used in L'(i) if and only if $r - 2s \ge 0$, and in L'(iii) if and only if $r - 2s < 0$.

Each of the identities L'(i) through L'(iv) is of the form

$$G_{m_j} = \gamma_j H_{n_j} + \delta_j K_{d_j}.$$

The proof that $\gcd(U_m, U_n)$, $\gcd(V_m, V_n)$, and $\gcd(U_m, V_n)$ are set forth in the Main Theorem is, then, precisely the same as that given in Section 4, with the slight changes required as the above identities replace the identities of Property L.

References

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Annals of Math.* *15* (1913):30-70.
2. P. Horak & L. Skula. "A Characterization of the Second-Order Strong Divisibility Sequences." *Fibonacci Quarterly* *23* (1985):126-32.
3. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Annals of Math.* *31* (1930):419-48.
4. E. Lucas. "Sur la theorie des nombres premiers." *Atti R. Accad. Sc. Torino* (Math). *11* (1875-1876):928-37.
5. E. Lucas. "Theorie des fonctions numeriques simplement periodiques." *Amer. J. Math.* *1* (1878):184-240, 289-321.
6. P. Ribenboim. "Square Classes of Fibonacci and Lucas Numbers." *Port. Math.* *46* (1989):159-75.

*****