On a divisibility relation for Lucas sequences

Pante Stănică

(joint work with Yuri F. Bilu, Takao Komatsu, Florian Luca, Amalia Pizarro-Madariaga)

Naval Postgraduate School
Applied Mathematics Department
Monterey, CA 93943; pstanica@nps.edu
The objects of the investigation: Lucas Sequences

- Lucas sequence and its companion:
  \[ U := U(a, b) = \{ U_n \}_{n \geq 0}, \quad U_0 = 0, \quad U_1 = 1 \]
  \[ U_{n+2} = aU_{n+1} + bU_n \quad \text{for all} \quad n \geq 0, \quad b \in \{ \pm 1 \}. \quad (1) \]

- We put \( V(a, b) = \{ V_n \}_{n \geq 0} \) for the Lucas companion of \( U \):
  \( V_0 = 2, \ V_1 = a \), same recurrence;

- Characteristic equation is \( x^2 - ax - b = 0 \) with roots
  \[ (\alpha, \beta) = \left( \frac{a + \sqrt{a^2 + 4b}}{2}, \frac{a - \sqrt{a^2 + 4b}}{2} \right). \]

- The Binet formulas for \( U_n \) and \( V_n \) are
  \[ U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n \quad \text{for all} \quad n \geq 0. \]

- Assume \( \Delta = a^2 + 4b > 0 \) and that \( \alpha/\beta \) is not a root of unity (that is, \( (a, b) \not\in \{ (0, \pm 1), (\pm 1, -1), (2, -1) \} \)).
If $a = b = 1$, we get the Fibonacci, resp., Lucas sequences.

In this case, Cohn and, independently, Wyler (both in 1964) proved that $U_n = \square$ iff $n = 0, 1, 2, 12$. Cohn slightly generalized this result.

McDaniel and Ribenboim (1992) showed (using divisibility methods) that if $U_n = \square, 2 \square$, then $n \leq 12$.

Mignotte and Pethö (1993) using linear forms in logarithms showed that if $b = -1$, $n > 4$, then $U_n = w \square$ is impossible if $w \in \{1, 2, 3, 6\}$, and these equations have solutions for $n = 4$ only if $a = 338$, and then, $U_4 = (2 \cdot 13 \cdot 239)^2$. 
Nakamula and Pethö (1998) used the same method to investigate when $U_n = w □$ for $b = 1$, $w \in \{1, 2, 3, 6\}$. They showed that $n \leq 2$, except when $(a, n, w) = (1, 12, 1), (1, 3, 2), (1, 4, 3), (1, 6, 2), (2, 4, 3), 2, 7, 1), (4, 4, 2)$.

Regarding the companion $V$, they showed that if $V_n = w □$, when $w \in \{1, 2, 3, 6\}$, then $n \leq 1$, when $b = 1$ and $a$ is even; and when $b = -1$, then $n \leq 1$, except when $(a, n, w) = (1, 2, 3), (1, 3, 1), (1, 6, 2), (2, 2, 6), (3, 3, 36)$.
Stewart (1982) found an effective finiteness result for shifted perfect powers in binary recurrence sequences: if the equation $U_k = x^n + c$ has a solution in integers $x, n, c$ and $k$, with $n \geq 2$ and $|x| > 1$, then, under some conditions, $\max\{|x|, n\}$ is bounded above effectively in terms of $c$ and the recurrence.

Recall the celebrated result of Y. Bugeaud, M. Mignotte, S. Siksek (2006): The only powers in $\{F_n\}_n$ are $F_0 = 0, F_1 = F_2 = 1, F_6 = 8, F_{12} = 144$;
Making Stewart’s result more precise, Bugeaud, Luca, Mignotte, Siksek (2008) showed that $F_n \pm 1 = y^p$, $p \geq 2$, then $(n, \pm 1, y, p) = (0, 1, 1, p), (4, 1, 2, 2), (6, 1, 3, 2), (1, -1, 0, p), (3, -1, 1, p), (5, -1, 2, 2)$.

More recently, Bennett, Dahmen, Mignotte, Siksek (2014) proved a diophantine eq. result that can potentially be applied to the equations $U_k = w x^n + c$ and $V_k = w x^n + c$, as well as, $F_k \pm F_{2j} = ax^n$. 

Assume that $m$ and $n$ are coprime, so, $F_n$ and $F_m$ are coprime, thus $F_{n+1}/F_n$ is defined modulo $F_m$. They showed that the congruence class $F_{n+1}/F_n \pmod{F_m}$ has multiplicative order $s$ modulo $F_m$ and $s \notin \{1, 2, 4\}$, then

$$m < 500s^2.$$ (2)
It is possible that this order is $s = 1$. It happens precisely when $F_{n+1} \equiv F_n \pmod{F_m}$, so $F_m|F_{n+1} - F_n = F_{n-1}$, which holds when $m|n - 1$, that is, $n \equiv 1 \pmod{m}$.

It is also possible that $s = 2$, since in this case, $F_{n+1}^2 \equiv F_n^2 \pmod{F_m}$, so $F_m|F_{n+1}^2 - F_n^2 = (F_{n+1} - F_n)(F_{n+1} + F_n) = F_{n-1}F_{n+2}$.

Let $m > 12$. By Primitive Divisor Theorem (Bilu-Hanrot-Voutier, 2001) (actually, Carmichael’s Theorem from (“On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$”, Ann. Math. (2) 15 (1913), 30–70) would be sufficient, $F_m$ has a primitive prime factor $p$, that is, $p|F_m$, but $p \nmid F_{\ell}$, for $1 \leq \ell < m$.

Thus, either $p|F_{n-1}$ or $p|F_{n+2}$. When $m|n - 1$, we recover the $s = 1$ case, and so, it must be that $n \equiv -2 \pmod{m}$. 
It is also possible to have $s = 4$. In this case $F_{n+1}^4 \equiv F_n^4 \pmod{F_m}$. Thus

$$F_m \mid F_{n+2}^4 - F_n^4 = (F_{n+1} - F_n)(F_{n+1} + F_n)(F_{n+1}^2 + F_n^2)$$

$$= F_{n-1}F_{n+2}F_{2n+1}.$$

Again, if $m > 12$, $F_m$ has a primitive prime divisor $p$, and so, $p \mid n - 1, n + 2, \text{ or } 2n + 1$. The first two cases imply $s = 1, 2$, and so $p \mid 2n + 1$, which can only happen if $m$ is odd and $n \equiv (m - 1)/2 \pmod{m}$.
Our Goal

Bilu, Komatsu, Luca, Pizzaro-Madariaga, P.S. (2015): We look at the relation

\[ U_m \mid U_{n+k} - U_n^s, \]  

with positive integers \( k, m, n, s \), where \( U \) is the general Lucas sequence.
This year, the quintet (actually, a quartet) got together in Johannesburg, South Africa and looked at the general divisibility relation (3) $U_m \mid U_{n+k}^s - U_n^s$ and proved the following result.

**Theorem**

Let $a$ be a non-zero integer, $b \in \{\pm 1\}$, and $k$ a positive integer. Assume that $(a, b) \notin \{(\pm 1, -1), (\pm 2, -1)\}$. Given a positive integer $m$, let $s$ be the smallest positive integer such that the divisibility $U_m \mid U_{n+k}^s - U_n^s$ holds. Then either $s \in \{1, 2, 4\}$, or

$$m < 20000(sk)^2.$$  

(4)
Proof that we (almost) all got together
Proof method – sketch 1

- Recall the Binet formulas for $U_n$ and $V_n$:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n \quad \text{for all} \quad n \geq 0.$$ 

- We assume that $m \geq 10000k$. Since $U_{n+4m} \equiv U_n \pmod{U_m}$ ($n \geq 0$, $m \geq 2$), we may assume that $n \leq 4m$. We split $U_m$ into various factors, as follows:

$$U_{n+k}^s - U_n^s = \prod_{d|s} \Phi_d(U_{n+k}, U_n),$$

where $\Phi_d(X, Y)$ is the homogenization of the cyclotomic polynomial $\Phi_d(X)$.
We put \( s_1 := \text{lcm}[2, s] \), \( S := \{ p : p \mid 6s \} \) and

\[
D := (U_m)_S; \\
A := \gcd(U_m/D, \prod_{d \leq 6, d \neq 5} \Phi_d(U_{n+k}, U_n)); \\
E := \gcd(U_m/D, \prod_{d \mid s_1} \Phi_d(U_{n+k}, U_n)).
\]

Clearly,

\[ U_m \mid ADE. \]

We proceed on bounding \( A, D, E \).
Proof method – sketch 3

- If $k$ is even then
  \[
  \Phi_d(U_{n+k}(-\alpha, -\beta), U_n(-\alpha, -\beta)) = \pm \Phi_d(U_{n+k}(\alpha, \beta), U_n(\alpha, \beta)),
  \]
  while if $k$ is odd, then
  \[
  \Phi_d(U_{n+k}(-\alpha, -\beta), U_n(-\alpha, -\beta)) = \pm \Phi_d(U_{n+k}(\alpha, \beta), -U_n(\alpha, \beta)) = \pm \Phi_{d^*}(U_{n+k}(\alpha, \beta), U_n(\alpha, \beta)),
  \]
  where
  \[
  d^* = \begin{cases}
  d & \text{if } 4 \mid d \text{ or } \delta = 1, \\
  d/2 & \text{if } 2 \parallel d \text{ and } \delta = -1, \\
  2d & \text{if } 2 \nmid d \text{ and } \delta = -1.
  \end{cases}
  \]
Proof method – sketch 4

- Note that \( \varphi(d^*) = \varphi(d) \), \( \Phi_d^*(X) = \pm\Phi_d(\delta X) \), \( \Phi_d(X^{-1}) = \pm X^{-\varphi(d)}\Phi_d(X) \), the sign in last identity being “+” for \( d > 1 \) and the sign in the middle identity being “+” if \( \delta = 1 \) or \( \min\{d, d^*\} > 1 \).

- Note that the sets \( \{d \leq 6, \ d \neq 5\} \) and \( \{d \mid s_1, \ d = 5 \text{ or } d > 6\} \) are closed under the operation \( d \mapsto d^* \).

- Hence, \( D, \ A, \ E \) do not change if we replace \( a \) by \(-a\), so we assume that \( a > 0 \).

- Recall: for any prime number \( p \) we put \( f_p \) for the index of appearance in the Lucas sequence \( \{U_n\}_{n \geq 0} \), which is the minimal positive integer \( k \) such that \( p \mid U_k \).
Bounding $D$

First, for $a \geq 1$, if $S$ is any finite set of primes and $m$ is a positive integer, then

$$(U_m)_S \leq \alpha^2 m \ell \operatorname{lcm}[U_{f_p} : p \in S].$$

(this follows from Bilu-Hanrot-Voutier’s paper from J. Reine Angew. Math. 2001 “Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte”)

Thus, since $f_p \leq p + 1$,

$$D \leq \alpha^2 m \prod_{p \mid 6s} U_{p+1} < m\alpha^{2+\sum_{p \mid 6s}(p+1)} \leq \alpha^{6s+3+\log m/\log \alpha},$$

where we used the fact that $\sum_{p \mid t}(p + 1) \leq t + 1$, which is easily proved by induction on the number of distinct prime factors of $t$. 
Note that

\[ E \mid \prod_{\substack{\zeta: \zeta^{s_1} = 1 \\ \zeta \not\in \{\pm 1, \pm i, \pm \omega, \pm \omega^2\}}} (U_{n+k} - \zeta U_n), \tag{5} \]

where \( \omega := e^{2\pi i/3} \) is a primitive root of unity of order 3.

Let \( K = \mathbb{Q}(e^{2\pi i/s_1}, \alpha) \), which is a number field of degree \( d \leq 2\phi(s_1) = 2\phi(s) \). Assume that there are \( \ell \) roots of unity \( \zeta \) participating in the product appearing in the right–hand side of (5), say \( \zeta_1, \ldots, \zeta_\ell \). Write

\[ \mathcal{E}_i = \gcd(E, U_{n+k} - \zeta_i U_n) \quad \text{for all} \quad i = 1, \ldots, \ell, \tag{6} \]

where \( \mathcal{E}_i \) are ideals in \( \mathcal{O}_K \). Then relations (5) and (6) tell us that

\[ E\mathcal{O}_K \mid \prod_{i=1}^\ell \mathcal{E}_i. \]
We need to bound the norm $|N_{K/\mathbb{Q}}(\mathcal{E}_i)|$ of $\mathcal{E}_i$ for $i = 1, \ldots, \ell$. First of all, $U_m \in \mathcal{E}_i$. Thus, using Binet formula and $\beta = (-b)\alpha^{-1}$, we get

$$\alpha^m \equiv (-b)^m \alpha^{-m} \pmod{\mathcal{E}_i} \iff \alpha^{2m} \equiv (-b)^m \pmod{\mathcal{E}_i}.$$  

Further, by Binet and (8) (with $\zeta := \zeta_i$),

$$\alpha^{2n}(\alpha^k - \zeta) - (-b)^{n+k}(\alpha^{-k} - (-b)^k \zeta) \equiv 0 \pmod{\mathcal{E}_i}.$$  

Using a slightly sharper estimate of $\Phi_v$, we obtained that $\alpha^k - \zeta$ and $\mathcal{E}_i$ are coprime, and so, $\alpha^k - \zeta$ is invertible modulo $\mathcal{E}_i$. Now congruence (9) shows that

$$\alpha^{2n+k} \equiv (-b)^n \zeta \left( \frac{\alpha^k - (-b)^k \zeta}{\alpha^k - \zeta} \right) \pmod{\mathcal{E}_i}.$$  

(1)
We do go through quite a few cases, depending upon the value of \((-b)^n\) and use the following workhorse lemma.
Lemma (Workhorse Lemma)

Let $a$, $b$ and $k$ be as in the statement of Theorem 1, and assume in addition that $a \geq 1$. Let $v \geq 1$ be an integer and $\zeta$ a primitive $v$th root of unity. Assume that the numbers

$$\alpha \quad \text{and} \quad \frac{\alpha^k - (-b)^k \bar{\zeta}}{\alpha^k - \zeta} \quad (11)$$

are multiplicatively dependent. Then we have one of the following options:

(i) $(-b)^k = -1$, $v = 4$;

(ii) $(a, b, k) \in \{(1, 1, 1), (2, 1, 1)\}$ and $v \in \{1, 2\}$;

(iii) $(-b)^k = 1$, $v \in \{1, 2\}$;

(iv) $(a, b, k) = (4, -1, 1)$ and $v \in \{4, 6\}$. 
Bounding $E$ & $A$

- The bound we found for $E$ is
  
  \[ E \leq \alpha^{22k\phi(s)\sqrt{m}} < \alpha^{22ks\sqrt{m}}. \]

  In the above, we used that $\phi(s) \leq s$.

- A somewhat similar, but slightly more delicate argument shows that
  
  \[ A \leq \alpha^{m/2+k+2+132k\sqrt{m}}. \]
Putting these bounds together

Using $\alpha^{n-2} \leq U_n \leq \alpha^n$, $n \geq 1$, then

$$\alpha^{n-2} \leq U_n \leq \alpha^n \leq DAE \leq \alpha^{6s + 3 + \log m / \log \alpha + m / 2 + k + 2 + (132k + 22ks) \sqrt{m}}.$$  

Since $s \geq 3$, we have $132 + 22s \leq 66s$. Since also $1 / \log \alpha < 3$, we get

$$m/2 \leq (6s + 7 + 3 \log m + k) + 66sk \sqrt{m}.$$  

Since $m \geq 10000$, one checks that $6s + 7 + 3 \log m + k < ks \sqrt{m}$. Hence,

$$m \leq 134ks \sqrt{m},$$  \hspace{1cm} (12)

which leads to the desired inequality $m < 20000(sk)^2$. 
One may wonder if one can strengthen our main result in such a way as to include also the instances \( s \in \{1, 2, 4\} \) maybe at the cost of eliminating finitely many exceptions in the pairs \((a, k)\).

The fact that this is not so follows from the formulae:

(i) \( U_{n+k} - U_n = U_{n+k/2} V_{k/2} \) for all \( n \geq 0 \) when \( b = 1 \) and \( 2 \parallel k \);

(ii) \( U_{n+k} + U_n = U_{n+k/2} V_{k/2} \) for all \( n \geq 0 \) when \( b = 1 \) and \( 4 \mid k \)
or when \( b = -1 \) and \( k \) is even;

(iii) \( U_{n+k}^2 + U_n^2 = U_{2n+k} U_k \) for all \( n \geq 0 \) when \( b = 1 \) and \( k \) is odd,

which can be easily proved using the Binet formulas. Thus, taking \( m = n + k/2 \) (for \( k \) even) and \( m = 2n + k \) for \( k \) odd and \( b = 1 \), we get that divisibility \( U_m \mid U_{n+k}^s - U_n^s \) always holds with some \( s \in \{1, 2, 4\} \).

Note the “near-miss” \( U_{4n+2} \mid 4(U_{n+1}^6 - U_n^6) \) for all \( n \geq 0 \) if \((a, b, k) = (4, -1, 1)\).
Thank you for your attention!
