PRIMITIVE PRIME FACTORS IN SECOND-ORDER LINEAR RECURRENCE SEQUENCES

ANDREW GRANVILLE AND H. W. LENSTRA JR

ABSTRACT. For a class of Lucas sequences \( \{x_n\} \), we show that if \( n \) is a positive integer then \( x_n \) has a primitive prime factor which divides \( x_n \) to an odd power, except perhaps when \( n = 1, 2 \) or \( 6 \). This has several desirable consequences.

1. Introduction

1a. Repunits and primitive prime factors.

The numbers 11, 111 and 1111111111 are known as repunits, that is all of their digits are 1 (in base 10). Repunits cannot be squares (since they are \( \equiv 3 \pmod{4} \)), so one might ask whether a product of distinct repunits can ever be a square? We will prove that this cannot happen. A more interesting example is the set of repunits in base 2, the integers of the form \( 2^n - 1 \). In this case there is one easily found product of distinct repunits that is a square, namely \((2^3 - 1)(2^6 - 1) = 21^2 \) (which is 111 · 111111 = 10101 · 10101 in base 2); this turns out to be the only example.

For a given sequence of integers \( \{x_n\}_{n \geq 0} \), we define a primitive prime factor of \( x_n \) to be a prime \( p \) which divides \( x_n \) but \( p \nmid x_m \) for \( 1 \leq m \leq n - 1 \). The Bang-Zsigmondy theorem (1892) states that if \( r > s \geq 1 \) and \((r, s) = 1\) then the numbers

\[
x_n = \frac{r^n - s^n}{r - s}
\]

have a primitive prime factor for each \( n > 1 \) except for the case \( \frac{2^6 - 1}{2 - 1} \).

For various Diophantine applications it would be of interest to determine whether there is a primitive prime factor \( p \) of \( x_n \) for which \( p^2 \) does not divide \( x_n \). As an example of such an application, note that if \( x_{n_1} \ldots x_{n_k} \) is a square where \( 1 < n_1 < n_2 < \cdots < n_k \) and \( k \geq 1 \) then a primitive prime factor \( p \) of \( x_{n_k} \) divides only \( x_{n_k} \) in this product and hence must divide \( x_{n_k} \) to an even power. Thus if \( p \) divides \( x_{n_k} \) to only the first power then \( x_{n_1} \ldots x_{n_k} \) cannot be a square. Unfortunately we are unable to prove anything about primitive prime factors dividing \( x_n \) only to the first power, but we are able to show that there is a primitive prime factor which divides \( x_n \) to an odd power, which is just as good for this particular application.
Theorem 1. If $r$ and $s$ are pairwise coprime integers for which $2$ divides $rs$ but not $4$, then $(r^n - s^n)/(r - s)$ has a primitive prime factor which divides it to an odd power, for each $n > 1$ except perhaps for $n = 2$ and $n = 6$. The case $n = 2$ is exceptional if and only if $r + s$ is a square. The case $n = 6$ is exceptional if and only if $r^2 - rs + s^2$ is $3$ times a square.

In particular $2^n - 1$ has a primitive prime factor which divides it to an odd power, for all $n > 1$ except $n = 6$. Also $(10^n - 1)/9$ has a primitive prime factor which divides it to an odd power for all $n > 1$.

Corollary 1. Let $x_n = (r^n - s^n)/(r - s)$ where $r$ and $s$ are pairwise coprime integers for which $2$ divides $rs$ but not $4$. If $x_{n_1}x_{n_2} \cdots x_{n_k}$ is a square where $1 < n_1 < n_2 < \cdots < n_k$ and $k \geq 1$, then either $x_2 = r + s$ is a square, or $x_3x_6 = x_3^2(r^3 + s^3)$ is a square.

The infinitely many examples of this last case include $2^3 + 1 = 3^2$, leading to the solution $(2^3 - 1)(2^6 - 1) = 21^2$, and $7^3 - 47^3 = 549^2$ leading to $74^3 - (-47)^3 = 121 \cdot 74^3 - (-47)^3 = 2309643^2$. Since $2^3 + 1 = 3^2$ is the only non-trivial solution in integers to $r^3 + 1 = t^2$, we have proved that the only example of a product of repunits which equals a square, in any base $b$ with $b \equiv 2 \pmod{4}$, is the one base 2 example $(2^3 - 1)(2^6 - 1) = 21^2$ given already.

1b. Certain Lucas sequences.

The numbers $x_n = (r^n - s^n)/(r - s)$ satisfy $x_0 = 0, x_1 = 1$ and the second order linear recurrence $x_{n+2} = (r + s)x_{n+1} - rsx_n$ for each $n \geq 0$. There are examples of a Lucas sequence, where $\{x_n\}_{n \geq 0}$ is a Lucas sequence if $x_0 = 0, x_1 = 1$ and

$$x_{n+2} = bx_{n+1} + cx_n \quad \text{for all } n \geq 0,$$

for given non-zero, coprime integers $b, c$. The discriminant of the Lucas sequence is

$$\Delta := b^2 + 4c.$$

Carmichael showed in 1913 that if $\Delta > 0$ then $x_n$ has a primitive prime factor for each $n \neq 1, 2$ or $6$ except for $F_{12} = 144$ where $F_n$ is the Fibonacci sequence ($b = c = 1$), and for $F'_n$ where $F'_n = (-1)^{n-1}F_n$ ($b = -1, c = 1$). We have been able to show the analogy to Theorem 1 for a class of Lucas sequences:

Theorem 2. Let $b$ and $c$ be pairwise coprime integers with $c \equiv 2 \pmod{4}$ and $\Delta = b^2 + 4c > 0$. Let $\{x_n\}_{n \geq 0}$ be the Lucas sequence satisfying (1). If $n \neq 1, 2$ or $6$ then $x_n$ has a primitive prime factor which (exactly) divides $x_n$ to an odd power.

In fact $x_2$ does not have such a prime factor if and only if $x_2 = b$ is a square; and $x_6$ does not have such a prime factor if and only if $x_6/(x_3x_2) = b^2 + 3c$ equals $3$ times a square.

Theorem 1 is a special case of Theorem 2 since there we have $c = -rs \equiv 2 \pmod{4}$, $(b, c) = (r + s, rs) = 1$ and $\Delta = (r - s)^2 > 0$. 
Corollary 2. Let the Lucas sequence \( \{x_n\}_{n \geq 0} \) be as in Theorem 2. If \( x_{n_1}x_{n_2} \ldots x_{n_k} \) is a square where \( 1 < n_1 < n_2 < \cdots < n_k \) and \( k \geq 1 \) then the product is either \( x_2 = b \) or \( x_3x_6 \).

In fact \( x_3x_6 \) is a square if and only if \( b \) and \( b^2 + 3c \) are both 3 times a square; that is, there exist odd integers \( B \) and \( C \) with \( (C, 3B) = 1 \) and \( 4C^2 > 3B^4 \), for which \( b = 3B^2 \) and \( c = C^2 - 3B^4 \).

1c. Fermat’s last theorem and Catalan’s conjecture; and a new observation.

Before Wiles’ work, one studied Fermat’s last theorem by considering the equation \( x^p + y^p = z^p \) for prime exponent \( p \) where \( (x, y, z) = 1 \), and split into two cases depending on whether \( p \) divides \( xyz \). In the “first case”, in which \( p \nmid xyz \), one can factor \( z^p - y^p \) into two coprime factors \( (z - y) \) and \( (z^p - y^p)/(z - y) \) which must both equal the \( p \)th power of an integer. Thus if the \( p \)th term of the Lucas sequence \( x_p = (z^p - y^p)/(z - y) \) is never a \( p \)th power the odd primes \( p \) then the first case of Fermat’s last theorem follows, an approach that has not yet succeeded. However Terjanian [Te] did develop these ideas to prove the first case of Fermat’s last theorem is true for even exponents, showing that if \( x^{2p} + y^{2p} = z^{2p} \) in coprime integers \( x, y, z \) where \( p \) is an odd prime then \( 2p \) divides either \( x \) or \( y \).

In any solution, \( x \) or \( y \) is even, else 2 divides \( (x^p)^2 + (y^p)^2 = z^{2p} \) but not 4, which is impossible. So we may assume that \( x \) is even, but not divisible by \( p \), and \( y \) and \( z \) are odd so that we have a solution \( r = z^2, s = y^2, t = x^p \) to \( r^p - s^p = t^2 \) with \( r \equiv s \equiv 1 \) (mod 4) and \( (t, 2p) = 2 \). Let \( x_n = (r^n - s^n)/(r - s) \) for all \( n \geq 1 \), so that \( x_p(r - s) = t^2 \) and \( (x_p, r - s) = (p, r - s)(p, t) = 1 \), which implies that \( x_p \) is a square. Terjanian’s key observation is that the Jacobi symbols

\[
\left( \frac{x_m}{x_n} \right) = \left( \frac{m}{n} \right)
\]

for all odd, positive integers \( m \) and \( n \).

Thus by selecting \( m \) to be an odd quadratic non-residue mod \( p \), we have \( (x_m/x_p) = -1 \) and therefore \( x_p \) cannot be a square. This contradiction implies that \( p \) must divide \( t \), and hence Terjanian’s result.

A similar method was used earlier by Chao Ko [Ko] in his proof that \( x^2 - 1 = y^p \) with \( p > 3 \) prime has no non-trivial solutions (a first step on the route to proving Catalan’s conjecture). Rotkiewicz [Ro] showed, by these means, that if \( x^p + y^p = z^2 \) with \( (x, y) = 1 \) then either \( 2p \) divides \( z \) or \( (2p, z) = 1 \), which implies both Terjanian’s and Chao Ko’s results. Rotkiewicz’s key lemma in [Ro], and then his Theorem 2 in [Ro2], extend (2):

Assume that \( \Delta \) and \( b \) are positive with \( (b, c) = 1 \). If \( b \) is even and \( c \equiv -1 \) (mod 4) then (2) holds. If 4 divides \( c \), or if \( b \) is even and \( c \equiv 1 \) (mod 4) then \( (x_m/x_n) = 1 \) for all odd, positive integers \( m, n \). In the most interesting case, when 2, but not 4, divides \( c \), we have

\[
\left( \frac{x_m}{x_n} \right) = (-1)^{\Lambda(m/n)}
\]

for all odd, coprime, positive integers \( m \) and \( n > 1 \),

where \( \Lambda(m/n) \) is the length of the continued fraction for \( m/n \); more precisely, we have a unique representation \( m/n = [a_0, a_1, \ldots, a_{\Lambda(m/n)-1}] \) where each \( a_i \) is an integer, with \( a_0 \geq 0, \ a_i \geq 1 \) for each \( i \geq 1 \), and \( a_{\Lambda(m/n)-1} \geq 2 \).
Note that we have not given an explicit evaluation of \((x_m/x_n)\) when \(b\) and \(c\) are both odd, the most interesting case being \(b = c = 1\) which yields the Fibonacci numbers. Rotkiewicz [Ro3] does give a complicated formula for determining \((F_m/F_n)\) in terms of a special continued fraction type expansion for \(m/n\); it remains to find a simple way to evaluate this formula.

To apply (3) we show that one can replace \(\Lambda(m/n) \pmod{2}\) by the much simpler \([2u/n] \pmod{2}\), where \(u\) is any integer \(\equiv 1/m \pmod{n}\) (and that this formula holds for all coprime positive integers \(m, n\)). Our proof of this, and the more general (4), is direct (see Theorem 3 and Corollary 6 below), though Vardi explained, in email correspondence, how to use the theory of continued fractions to show that \((m/n)\) (both odd, the most interesting case being the end of section 5). The observation that \(\Lambda(m/n) \equiv [2u/n] \pmod{2}\) (see the end of section 5). The observation that \(\Lambda(m/n) \equiv [2u/n] \pmod{2}\) is really the starting point for the proofs of our main results.

It is much more difficult to prove that Lucas sequences with negative discriminant have primitive prime factors. Nonetheless, in 1974 Schinzel succeeded in showing that \(x_n\) has a primitive prime factor once \(n > n_0\), for some sufficiently large \(n_0\), if \(\Delta \neq 0\), other than in the periodic case \(b = \pm 1, c = -1\). Determining the smallest possible value of \(n_0\) has required great efforts culminating in the beautiful work of Bilu, Hanrot and Voutier [BHV] who proved that \(n_0 = 30\) is best possible. One can easily deduce from Siegel’s theorem that if \(\phi(n) > 2\) then there are only finitely many Lucas sequences for which \(x_n\) does not have a primitive prime factor, and these exceptional cases are all explicitly given in [BHV]. They show that such examples occur only for \(n = 5, 7, 8, 10, 12, 13, 18, 30\): if \(b = 1, c = -2\) then \(x_5, x_8, x_{12}, x_{13}, x_{18}, x_{30}\) have no primitive prime factors; if \(b = 1, c = -5\) then \(x_7 = 1\); if \(b = 2, c = -3\) then \(x_{10}\) has no primitive prime factors; there are a handful of other examples besides, all with \(n \leq 12\).

1d. Sketches of some proofs.

In this subsection we sketch the proof of a special case of Theorem 2 (the details being completed in the next four sections). The reason we focus now on a special case is that this is already sufficiently complicated, and extending the proof to all cases involves some additional (and uninteresting) technicalities, which will be given in section 6.

**Theorem 2’**. Let \(b\) and \(c\) be integers for which \(b \equiv 3 \pmod{4}\), \(c \equiv 2 \pmod{4}\), the Jacobi symbol \((c/b) = 1\) and \(\Delta = b^2 + 4c > 0\). If \(\{x_n\}_{n \geq 0}\) is the Lucas sequence satisfying (1) then \(x_n\) has a primitive prime factor which (exactly) divides \(x_n\) to an odd power for all \(n > 1\) except perhaps when \(n = 6\). This last case occurs if and only if \(x_6/(3x_2x_3)\) is a square.

**Sketch of the proof of Theorem 2’**. Let \(x_n = y_nz_n\) where \(y_n\) is divisible only by primitive prime factors of \(x_n\), and \(z_n\) is divisible only by imprimitive prime factors of \(x_n\). If every primitive prime factor divides \(x_n\) to an even power then \(y_n\) is a square: it is our goal to show that this is impossible.

Complex number \(\xi\) is a primitive \(nth\) root of unity if \(\xi^n = 1\) but \(\xi^m \neq 1\) for all \(1 < m < n\). Let \(\phi_n(t) \in \mathbb{Z}[t]\) be the \(nth\) cyclotomic polynomial, that is the monic polynomial whose roots are the primitive \(nth\) roots of unity. Evidently \(x^n - 1 = \prod_{d|n} \phi_d(x)\)
so, by Mobius inversion, we have
\[ \phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \]

Homogenizing, we have \( \phi_n(r, s) := s^{\phi(n)} \phi_n(r/s) \in \mathbb{Z}[r, s] \) and \( x_n = (r^n - s^n)/(r - s) = \prod_{d|n, d>1} \phi_d(r, s) \). Indeed for any Lucas sequence \( x_n \) the number
\[ n := \sum_{d|n} x_d^{\mu(n/d)} \]
is an integer. Most importantly, this definition yields that \( p \) is a primitive prime factor of \( n \) if and only if \( p \) is a primitive prime factor of \( x_n \); moreover \( p \) divides both \( \phi_n \) and \( x_n \) to the same power. Therefore \( y_n \) divides \( \phi_n \), which divides \( x_n \). In fact \( y_n \) and \( \phi_n \) are very close to each other multiplicatively (as we show in Corollaries 3 and 4 below): either \( \phi_n = y_n \), or \( \phi_n = py_n \) where \( p \) is some prime dividing \( n \), in fact \( n = p^e m \) where \( p \) is a primitive prime factor of \( \phi_m \). So if we can show that

(i) \( \phi_n \) is not a square, and
(ii) \( p\phi_n \) is not a square when \( n \) is of the form \( n = p^e m \) where \( p \) is an odd prime, \( e \geq 0 \), \( m > 1 \) and \( m \) divides \( p - 1 \), \( p \) or \( p + 1 \)
then we can deduce that \( y_n \) is not a square. To prove this we modify the approach of Terjanian described above: We will show that there exist integers \( k \) and \( \ell \) for which
\[ \left( \frac{x_k}{\phi_n} \right) = \left( \frac{x_\ell}{p^{\phi_n}} \right) = -1, \]where \( (\cdot) \) is the Jacobi symbol.

Our first step then is to evaluate the Jacobi symbol \( (x_k/x_m) \) for all positive integers \( m \) and \( k \). In fact this equals 0 if and only if \( (k, m) > 1 \). Otherwise, we will show that for any coprime positive integers \( k \) and \( m > 2 \) we have
\[ \left( \frac{x_k}{x_m} \right) = (-1)^{\lfloor 2u/m \rfloor} \]
for any integer \( u \) which is \( \equiv 1/k \pmod{m} \) (as discussed above). From this we deduce that
\[ \left( \frac{x_k}{\phi_m} \right) = (-1)^{N(m, u)} \]
for all \( m \geq 1 \), where, for \( r(m) = \prod_{p|m} p \) and the Mobius function \( \mu(m) \), we have
\[ N(m, u) := \mu^2(m) + \# \{ i : 1 \leq i < 2ur(m)/m \text{ and } (i, m) = 1 \}. \]

Now if \( \phi_m \) is a square then by (5), we have that \( N(m, u) \) is even whenever \( (u, m) = 1 \). In Proposition 4.1 we show that this is false unless \( m = 1, 2 \) or 6: our proof of this elementary fact is more complicated than one might wish.

In Lemma 5.1 we show, using (5), that if \( p\phi_m \) is a square where \( m = p^e n \), \( n > 1 \) and \( n \) divides \( p - 1 \), \( p \) or \( p + 1 \) then \( N(m, u') - N(m, u) \) is even whenever \( u \equiv u' \pmod{n} \) with
(uu’, m) = 1. In Propositions 5.2 and 5.4 we show that this is false unless m = 6: again our proof of this elementary fact is more complicated than one might wish.

Since \( x_d \equiv 3 \pmod{4} \) for all \( d \geq 2 \) (as may be proved by induction), and since any squarefree integer \( m \) has exactly \( 2^\ell - 1 \) divisors \( d > 1 \), where \( \ell \) is the number of prime factors of \( m \), therefore \( \phi_m \equiv \prod_{d|m} x_d \equiv x_1 3 \equiv 3 \pmod{4} \), and so cannot be a square. Hence neither \( \phi_2 \) nor \( \phi_6 \) is a square (despite the fact that \( (x_k/\phi_6) = 1 \) for all \( k \) coprime to 6, since \( N(6, u) \) is even whenever \( (u, 6) = 1 \). Therefore the only possibility left is that 3\( \phi_6 \) is a square, as claimed.

**Proof of Corollary 2.** If \( p \) is a primitive prime factor of \( x_{n_k} \), which divides \( x_{n_k} \) to an odd power then \( p \) does not divide \( x_{n_i} \) for any \( i < k \) and so divides \( \prod_{1 \leq i < k} x_{n_i} \) to an odd power, contradicting the fact that this is a square. Therefore \( n_k = 2 \) or 6 by Theorem 2. Since a similar argument may be made for any \( x_{n_i} \), where \( n_i \) does not divide \( n_j \) with \( j > i \) we deduce, from Theorem 1, that every \( n_i \) must divide 6.

Therefore either \( k = 1 \) and \( x_2 = b \) is a square, or we can rewrite \( \prod_{1 \leq i < k} x_{n_i} \) as a product of \( \prod_{1 \leq j \leq \ell} \phi_{m_j} \) times a square, where \( 1 < m_1 < \cdots < m_\ell = 6 \) and \( \{m_1, \ldots, m_{\ell-1}\} \subset \{2, 3\} \). However \( \phi_3 \) is divisible by some primitive odd prime factor \( p \) to an odd power, which does not divide \( \phi_6 \) (as all \( x_n \), \( n \geq 1 \) are odd), and so \( \phi_3 \) cannot be in our product. Now \( \phi_6 \) is not a square since \( \phi_6 = b^2 + 3c \equiv 3 \pmod{4} \). Therefore both \( \phi_2 \) and \( \phi_6 \) are 3 times a square, which is equivalent to \( x_3x_6 \) being a square.

Theorem 1 follows from Theorem 2, and Corollary 1 follows from Corollary 2.

## 2. Elementary properties of Lucas sequences

### 2a. Lucas sequences in general.

If \( y_{n+2} = -by_{n+1} + cy_n \) for all \( n \geq 0 \) with \( y_0 = 0, \ y_1 = 1 \) then \( y_n = (-1)^{n-1} x_n \) for all \( n \geq 0 \). Therefore the prime factors, and primitive prime factors, of \( x_n \) and \( y_n \) are the same and divide each to the same power, and so we may assume, without loss of generality, that \( b > 0 \).

Let \( \alpha \) and \( \beta \) be the roots of \( T^2 - bT - c \). Then

\[
x_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for all } n \geq 0
\]

(as may be proved by induction). We note that \( \alpha + \beta = b \) and \( \alpha \beta = -c \), so that \( (\alpha, \beta)|(b, c) = 1 \) and \( \Delta = (\alpha - \beta)^2 = b^2 + 4c \).

**Lemma 1.** We establish various properties of the sequence \( \{x_n\} \):

(i) We have \( (x_n, c) = 1 \) for all \( n \geq 1 \).

(ii) We have \( (x_n, x_{n+1}) = 1 \) for all \( n \geq 0 \).

(iii) We have \( x_{d+j} \equiv x_{d+j} x_j \pmod{x_d} \) for all \( d \geq 1 \) and \( j \geq 0 \). Therefore if \( k - \ell = jd \) then \( x_k \equiv x_{\ell} x_{d+1}^j \pmod{x_d} \).

(iv) Suppose \( d \) is the minimum integer \( \geq 1 \) for which \( x_d \) is divisible by given integer \( r \). Then \( r|x_k \) if and only if \( d|k \).

(v) For any two positive integers \( k \) and \( m \) we have \( (x_k, x_m) = x_{(k,m)} \).
Proof. (i) If not let select $n$ minimal so that there exists a prime $p$ with $p|(x_n, c)$. Then $bx_{n-1} = x_n - cx_{n-2} \equiv 0 \pmod{p}$ and so $p|x_{n-1}$ since $(p, b)|(c, b) = 1$, contradicting minimality.

(ii) If not we again proceed by minimality using that $(x_{n+1}, x_{n+2})|x_{n+2} - bx_{n+1} = cx_n$, and thus divides $x_n$, since $(x_{n+1}, c) = 1$ by (i). Therefore $(x_{n+1}, x_{n+2})(x_n, x_{n+1}) = 1.$

(iii) We proceed by induction on $j$: it is trivially true for $j = 0$ and $j = 1$. For larger $j$ we have $x_{d+j} = bx_{d+j-1} + cx_{d+j-2} \equiv x_{d+1}(bx_j - 1 + cx_{j-2}) = x_{d+1}x_j \pmod{x_d}$.

(iv) Since $(x_{d+1}, x_d) = 1$ we see that $(x_d, x_{d+j}) = (x_d, x_j)$ by (iii). So if $j$ is the least positive residue of $k \pmod{d}$ we find that $(r, x_k) = (r, x_j)$ and the result follows from the definition of $d$.

(v) Let $g = (k, m)$ so (iv) implies that $x_g|(x_k, x_m) = r$, say. Let $d$ be the minimum integer $\geq 1$ for which $x_d$ is divisible by $r$. Then $d|(k, m) = g$ by (iv), and thus $r|x_g$ by (iv), and the result is proved.

Proposition 1. For given prime $p$ let $q = p$ if $p$ is odd, and $q = 4$ if $p = 2$. Select $r_p$ to be the minimal integer $\geq 1$ for which $q|\alpha^r - \beta^r$ (such an $r_p$ exists if and only if $p \nmid c$). Define $e_p \geq 1$ so that $p^{e_p}|\alpha^r - \beta^r$ but $p^{e_p+1}$ does not. Then $m = m_k = p^kr_p$ is the smallest integer for which $p^{e_p+k}|\alpha^m - \beta^m$ for each integer $k \geq 0$.

Proof. Since $p|x_n$ for some $n \geq 1$ we have $(p, \alpha\beta)|(x_n, c) = 1$ by Lemma 1(i) so that $p$ is coprime to both $\alpha$ and $\beta$. On the other hand if $(p, \alpha\beta) = 1$ then $\alpha, \beta$ are in the group of units mod $p$, and therefore there exists an integer $n$ for which $\alpha^n \equiv 1 \equiv \beta^n \pmod{p}$ so that $p|\alpha^n - \beta^n$.

The result is true by definition for $k = 0$. Let us suppose it is true for $k$ and write $\alpha^{mk} = \beta^{mk} + p^{e_p+k}\gamma$ where $p \nmid \gamma$. If $p^{e_p+k+1}|\alpha^m - \beta^m$ then $p^{e_p+k}|\alpha^m - \beta^m$ and so $m|p$ by Lemma 1(iv). Now $p^{e_p+k} > 2$ so that $\alpha^{jm_k} = (\beta^{mk} + p^{e_p+k}\gamma)^j \equiv \beta^{jm_k} + jp^{e_p+k}\gamma(\beta^{-1})m_k + j^p^{e_p+k+1}\gamma$ (mod $p^{e_p+k+2}$) for some algebraic integer $\delta$. Therefore we have $(p^2, (\alpha^{jm_k} - \beta^{jm_k})/p^{e_p+k}) = (p^2, j)$ as $(p, \gamma) = 1$, which implies that $m_{k+1} = pm_k$.

Corollary 3. We have that each $\phi_n$ is an integer. When $p$ is a primitive prime factor of $\phi_n$ define $n_p = n$. Then $p$ divides both $x_n$ and $\phi_n$ to the same power. Otherwise if prime $p|\phi_n$ where $n \neq n_p$ then $n/n_p$ is a power of $p$, and $p^2 \nmid \phi_n$ with one possible exception: if $p = 2$ with $b$ odd and $c \equiv 1 \pmod{4}$ then $n_2 = 3$ and $2^2|\phi_6$. If $p$ is an odd prime for which $p^2|\Delta$ then $p|\phi_p$ but $p^2 \nmid \phi_p$.

Proof. We need to establish that $\phi_n$ is an integer. By using the fact that $\phi_n = \prod_{d|n} x_d^{\mu(n/d)}$ we note that if prime $p$ divides the numerator or denominator of $\phi_n$ then it divides $x_d$ for some $d|n$, and so $p|x_n$ by Lemma 1(iv). If $c$ is odd then let $s$ be the minimal integer $\geq 1$ for which $2(\alpha^s - \beta^s)$. In the notation of Proposition 1 suppose that $s = r_2$, and note that if $p|x_d$ for some $d|n$ then $r_p|d$. Writing $n = r_mp^km$ where $p|m$ and $d = r_p\ell q$ with $0 \leq \ell \leq k$ and $q|m$, we find that the power of $p$ dividing $x_d$ is $e_p + \ell$. Therefore, if $n > 1$ then the
power of \( p \) dividing \( \phi_n \) is

\[
\sum_{0 \leq \ell \leq k} \mu(p^{k-\ell})(e_p + \ell) \sum_{q | m} \mu(m/q) = \begin{cases} 
1 & \text{if } m = 1 \text{ and } k \geq 1 \\
e_p & \text{if } m = 1 \text{ and } k = 0 \\
0 & \text{if } m \geq 2.
\end{cases}
\]

If \( s \neq r \) then \( r_2 = 2s \), which can be proved in the manner of Proposition 1. Proceeding as above we find that the power of \( p \) dividing \( \phi_n \), where \( n = s2^km \), is 0 if \( m \geq 2 \), equals \( e_2 - 1 \) if \( n = r_2 = 2s \), and equals 1 if \( n = 2^k \) with \( k \neq 1 \).

Evidently this implies that \( \phi_n \) is an integer and that if \( p | \phi_n \) then \( n/p \) is a power of \( p \).

By Proposition 1 we have that \( n_p = r_p \) if \( p \not| 2(\alpha - \beta) \), that is \( p \not| 2\Delta \). On the other hand if odd prime \( p | \alpha - \beta \) then \( r_p = 1 \) and \( n_p = p \) by Proposition 1; and, by the above \( p | \phi_p \) but \( p^2 \nmid \phi_p \). These remarks also hold if \( r_2 = s \). Otherwise \( n_2 = s = r_2/2 \). In this case if \( b \) is even then \( s = 2 \) and \( b \equiv 2 \pmod{4} \) so that \( e_2 = 2 \), and the result holds; if \( b \) is odd then \( s = 3 \) and \( c \equiv 1 \pmod{4} \), so that \( e_2 \geq 3 \). The result follows.

Since \( \phi_n \) is usually significantly smaller than \( x_n \) and since we have a very precise description of the imprimitive prime factors of \( \phi_n \), it is easier to study primitive prime factors of \( x_n \) by studying the factors of \( \phi_n \).

**Lemma 3.** We have that \( n_p \) divides \( p - (\Delta/p) \); so that \( n_p \leq p + 1 \).

**Proof.** We have \( \alpha = (b + \sqrt{\Delta})/2 \) and \( \beta = (b - \sqrt{\Delta})/2 \), which implies that

\[
\alpha^p \equiv \frac{b^p + \sqrt{\Delta}^p}{2^p} = \frac{b + \Delta(p-1)/2}{2} \equiv \frac{b + (\Delta/p)\sqrt{\Delta}}{2} \pmod{p},
\]

and thus \( \beta^p \equiv (b - (\Delta/p)\sqrt{\Delta})/2 \). If \( p | \Delta \) then \( \alpha^p \equiv \beta^p \equiv b/2 \pmod{p} \) so that \( p | (\alpha - \beta)x_p \) and thus, by Corollary 3, \( n_p | p \). If \( (\Delta/p) = -1 \) then \( \alpha^{p+1} = \alpha \beta = -c \pmod{p} \) and similarly \( \beta^{p+1} \) and so \( p | x_{p+1} \). Finally if \( (\Delta/p) = 1 \) then \( \alpha^{p-1} = \alpha^{-1} \alpha^p \equiv \alpha^{-1} \alpha = 1 \pmod{p} \) and similarly \( \beta^{p+1} \) and so \( p | x_{p-1} \).

**Corollary 4.** Each \( \phi_n \) has at most one imprimitive prime factor, except \( \phi_6 \) is divisible by 6 if \( b \equiv 3 \pmod{6} \) and \( c \equiv 1 \pmod{2} \), and \( \phi_{12} \) is divisible by 6 if \( b \equiv \pm 1 \pmod{6} \) and \( c \equiv 1 \pmod{6} \).

**Proof.** Suppose \( \phi_n \) has two imprimitive prime factors \( p < q \). By Corollary 3 we have that \( q | n_p \) and so \( q \leq n_p \leq p + 1 \) by Lemma 3. Therefore \( p = 2 \) and \( q = 3 \), in which case \( n_2 = 3 \), so that \( n = 2^e3 \) for some \( e \geq 1 \), and this equals \( 3^f \) for some \( f \geq 1 \) by Corollary 3. Thus \( f = 1 \) and \( n_3 = 2 \) or 4. The result follows by working through the possibilities mod 2 and mod 3.

**Corollary 5.** Suppose that \( x_n \) does not contain a primitive prime factor to an odd power and \( n \neq 6 \) or 12. Then either \( \phi_n = \Box \) (where \( \Box \) represents the square of an integer), or \( \phi_n = p^2 \) where \( p \) is a prime for which \( p^e | n \) with \( e \geq 1 \) and \( n/p^e \leq p + 1 \).

**Proof.** Follows from Corollaries 3 and 4 and Lemma 3.
2b. Lucas sequences with \( b, \Delta > 0 \) and \( b \equiv 3 \pmod{4}, \ c \equiv 2 \pmod{4} \).

As \( b, \Delta > 0 \) this implies that \( x_n > 0 \) for all \( n \geq 1 \) since \( \alpha > |\beta| \).

We also have \( x_n \equiv 3 \pmod{4} \) for all \( n \geq 2 \), by induction. In fact \( x_{n+2} \equiv x_n \pmod{8} \) for all \( n \geq 3 \), which we can prove by induction: We have \( x_5 = b^4 + 3cb^2 + c^2 \equiv 1 + 3c + 4 \equiv 1 + c \equiv b^2 + c = x_3 \) \( \pmod{8} \), and \( x_6 = b(b^4 + 4cb^2 + 3c^2) \equiv b(1 + 0 + 4) = b(1 + 4) \equiv b(b^2 + 2c) = x_4 \) \( \pmod{8} \). For larger \( n \), we then have \( x_{n+2} = bx_{n+1} + cx_n \equiv bx_n + cx_{n-2} = x_n \pmod{8} \) by the induction hypothesis.

**Proposition 2.** We have \( (x_{d+1}/x_d) = 1 \) for all \( d \geq 1 \).

**Proof.** For \( d = 1 \) this follows as \( x_1 = 1 \); for \( d = 2 \) we have \( (x_3/x_2) = ((b^2 + c)/b) = (c/b) = 1 \). The result then follows from proving that \( \theta_d := (x_{d+1}/x_d)(x_d/x_{d-1}) = 1 \) for all \( d \geq 3 \). Since \( x_{d+1} \equiv cx_{d-1} \pmod{x_d} \) and as \( x_d \equiv x_{d-1} \equiv 3 \) \( \pmod{4} \) for \( d \geq 3 \), we have \( \theta_d = (cx_{d-1}/x_d)(x_d/x_{d-1}) = (-c/x_d) = (-c/x_d) \). Since \( c \equiv 2 \pmod{4} \) we may write \( c = 2\delta C \) where \( \delta = \pm 1 \) and \( C \) is an odd positive integer, so that \( (-c/x_d) = (-2\delta C/x_d) = (-2\delta/x_d)(-x_d/C) \). Thus \( \theta_3 = (-2\delta/(b^2 + c))(-1/C) = (-2\delta/(1 + 2\delta C))(-1/C) = 1 \) if \( b^2 + c \equiv 1 + 2\delta C \pmod{8} \). For larger \( d \) and as \( C \equiv \pm 1 \pmod{4} \) and \( \delta = \pm 1 \). Also \( \theta_4 = (-2\delta/(b^2 + 2cb))(-1/C) \equiv (-2\delta/5b)(C/b) = (-2\delta/5)(-c/b) = (2/5)(-1) = 1 \) as \( b^3 + 2cb \equiv 5b \pmod{8} \) and \( (c/b) = 1 \). Since \( x_{j+1} \equiv bx_j \pmod{c} \) for \( j \geq 1 \), therefore \( x_d \equiv b^{d-1} \pmod{c} \). Thus \( (x_d/C) = (b/C)^{d-1} \) and so \( \theta_d = (-2\delta/x_d)(-1/C)(b/C)^{d-1} \). But then \( \theta_d = \theta_{d-2} \) for \( d \geq 5 \) by Lemma 1(vi), which equals 1 by the induction hypothesis.

3. Evaluation of Jacobi symbols

3a. The reciprocity law.

Suppose that \( k \) and \( m > 1 \) are coprime positive integers. Let \( u_{k,m} \) be the least residue, in absolute value, of \( 1/k \pmod{m} \) (that is \( u \equiv k \pmod{m} \) with \(-m/2 < u \leq m/2 \)).

**Lemma 4.** If \( m, k \geq 2 \) with \( (m, k) = 1 \) then \( ku_{k,m} + mu_{m,k} = 1 \).

**Proof.** Now \( v := (1 - ku_{k,m})/m \) is an integer \( \equiv 1/m \pmod{k} \) with \(-k/2 + 1/m \leq v < k/2 + 1/m \). Thus implies that \(-k/2 < v \leq k/2 \), and so \( v = u_{m,k} \).

**Theorem 3.** If \( k \) and \( m > 1 \) are coprime positive integers then the value of the Jacobi symbol \((x_k/x_m)\) equals the sign of \( u_{k,m} \).

**Proof.** By induction on \( k + 2m \geq 5 \). Note that when \( k = 1 \) we have \( u = 1 \) and the result follows as \((x_1/x_m) = (1/x_m) = 1 \). For larger \( k \), we have two cases. If \( k > m \) then let \( \ell \) be the least positive residue of \( k \pmod{m} \), say \( k - \ell = jm \). By Lemma 1(iii) we have \((x_k/x_m) = (x_\ell/x_m)(x_{\ell+1}/x_m)^j = (x_\ell/x_m) \) by Proposition 2. Moreover \( 1 = ku_{k,m} + mu_{m,k} = \ell u_{k,m} + m(u_{m,k} + ju_{k,m}) \) and so \( u_{m,k} = u_{k,m} \) so that the result follows from the induction hypothesis. If \( 2 \leq k < m \) then \((x_k/x_m) = -(x_m/x_k) \) since \( x_m \equiv x_k \equiv 3 \pmod{4} \). Moreover \( u_{k,m} \) and \( u_{m,k} \) must have opposite signs, else \( 1 = k|u_{k,m}| + m|u_{m,k}| \geq 1 + 1 \) by Lemma 4 which is impossible. The result follows from the induction hypothesis.

Define \((t)_m\) to be the least (positive) residue of \( t \pmod{m} \), so that \((t)_m = t - m[t/m]\).

Note that \( 0 \leq (t)_m \leq m/2 \) if and only if \( [(t)_m/(m/2)] = 0 \). Also that \([[t]/(m/2)] = \)
\[ [2t/m] - 2[t/m] \equiv [2t/m] \pmod{2} \] Now, if \( m \geq 3 \) and \( (t, m) = 1 \) then \( (t)_m \) is not equal to 0 or \( m/2 \); therefore if \( u \) is any integer \( \equiv 1/k \pmod{m} \) then the sign of \( u_{k,m} \) is given by \( (-1)^{[2u/m]} \). We deduce the following from this and Theorem 3:

**Corollary 6.** Suppose that \( k \) and \( m \neq 2 \) are coprime positive integers. If \( u \) is any integer \( \equiv 1/k \pmod{m} \) then

\[ \left( \frac{x_k}{x_m} \right) = (-1)^{[2u/m]}. \]

Note that if \( k \) is odd then \( \left( \frac{x_k}{x_2} \right) = 1 \), whereas (4) would always give \(-1\).

**Remark.** In email correspondence with Ilan Vardi we understood how (4) can be deduced directly from (3) and known facts about continued fractions. Write \( p_n/q_n = [a_0, a_1, \ldots, a_n] \) for each \( n \), and recall that

\[ \left( \begin{array}{cc} p_n & p_{n-1} \\ q_n & q_{n-1} \end{array} \right) = \left( \begin{array}{cc} a_0 & 1 \\ 1 & 0 \end{array} \right) \left( \begin{array}{cc} a_1 & 1 \\ 1 & 0 \end{array} \right) \cdots \left( \begin{array}{cc} a_n & 1 \\ 1 & 0 \end{array} \right) \]

as may easily be established by induction on \( n \geq 1 \). By taking determinants we see that \( p_nq_{n-1} = p_{n-1}q_n + (-1)^{n+1} \equiv (-1)^{n+1} \pmod{q_n} \). Taking \( p_{n-1}/q_{n-1} = k/m \) with \( n = \Lambda(k/m) \) and \( u \) to be the least residue of \( 1/k \pmod{m} \) we see that \( q_{n-1} \equiv (-1)^{n+1}u \pmod{m} \) and \( q_{n-1} < q_n \), so \( q_{n-1} = u \) if \( n \) is odd, \( q_{n-1} = m - u \) if \( n \) is even. Now \( m = q_n = a_nq_{n-1} + q_{n-2} \geq 2q_{n-1} + 1 \), and so \( q_{n-1} < m/2 \). Therefore if \( u < m/2 \) then \( q_{n-1} = u \), so \( n \) is odd and the values given in (4) and (3) are equal. A similar argument works if \( u > m/2 \).

**3b. The primitive part.**

If \( (m, k) = 1 \) and \( u \equiv 1/k \pmod{m} \) then

\[ \left( \frac{x_k}{\phi_m} \right) = \prod_{d|\phi_m} \left( \frac{x_k}{x_d} \right)^{\mu(m/d)} = (-1)^{N(m,u)} \]

by (4) since \( (x_k/x_d) = 1 \) if \( d = 1 \) or \( 2 \), where

\[ N(m,u) \equiv \sum_{d|m} \mu \left( \frac{m}{d} \right) \left[ \frac{2u}{d} \right] = \sum_{d|m} \mu \left( \frac{m}{d} \right) \sum_{1 \leq j \leq 2u-1} \frac{1}{d \mid j} \]

\[ = \sum_{1 \leq j \leq 2u-1} \sum_{d|\phi_m} \mu \left( \frac{m}{d} \right) + \mu(m)(2u - 1) + E_2 \pmod{2} \]

where \( E_2 \), the contribution when \( d = 2 \), occurs only when \( m \) is even, and is then \( \mu(m/2)(u-1) \). However \( u \) is then odd since \( (u, m) = 1 \) and so \( E_2 \equiv \mu(m/2)(u-1) \equiv 0 \pmod{2} \).
Now let \( r(n) = \prod_{p|n} p \) for any integer \( n \). We see that \( \mu(m/d) = 0 \) unless \( m/d \) divides \( r(m) \), that is \( d \) is divisible by \( m/r(m) \), in which case \( j \) must be also. Write \( j = i(m/r(m)) \), and each \( d = D(m/r(m)) \) and so

\[
N(m, u) \equiv \mu(m) + \sum_{1 \leq i < 2ur(m)/m} \sum_{D|(r(m),i)} \mu(r(m)/D) \equiv \mu(m) + \sum_{1 \leq i < 2ur(m)/m} 1 \quad (\text{mod } 2),
\]

as claimed above.

4. When \( \phi_m = \Box \) with \( m > 1 \).

**Proposition 4.1.** If \( m \neq 1, 2, 6 \) then \( N(m, u') - N(m, u) \) is odd for some \( u, u' \) with \((uu', m) = 1\).

**Proof.** If \( m \) is squarefree then \( N(m, u') - N(m, u) \equiv \#\{i : 2u \leq i < 2u' \text{ and } (i, m) = 1\} \). So, if \( m \) is odd and \( > 1 \) let \( u = (m - 1)/2 \) and \( u' = u + 1 \). If \( m \) is even then there exists a prime \( q|m \) with \( q \geq 5 \) (as \( m \neq 2 \) or 6), so we can write \( m = qs \) where \( q \nmid s > 1 \): Then select \( u \equiv -1 \pmod{2s} \) and \( u' \equiv -3/2 \pmod{q} \) with \( u' = u + 2 \) to get a contradiction.

For \( m \) not squarefree let \( m_2 \) be the largest powerful number dividing \( m \) and \( m = m_1 m_2 \) so that \( m_1 \) is squarefree, \((m_1, m_2) = 1\), and \( r(m_2)^2|m_2 \). Note that \( m/r(m) = m_2/r(m_2) \).

When \( m_2 = 4 \) then \( N(m, u) = \#\{i : 1 \leq i < u\} \), so if \( u \) is the smallest integer \( > 1 \) that is coprime with \( m \) then \( N(m, u) - N(m, 1) = 1 \).

So we may assume that \( m_2 > 4 \), in particular that \( 2r(m)/m \leq 2/3 \). Consider

\[
N(m, \frac{m}{r(m)}(\ell + 1) + 1) - N(m, \frac{m}{r(m)}(\ell + 1)) = \#\{i : 2\ell + 1 \leq i \leq 2\ell + 2 \text{ : } (i, m) = 1\}.
\]

Select \( \ell \equiv -1 \pmod{m_2} \) so that \( (2\ell + 2, m) \geq m_2 \). Then we need to select \( \ell \pmod{p} \) for each prime \( p \) dividing \( m_1 \) so that each of \( \frac{m}{r(m)}(\ell + 1) + 1 \), \( \frac{m}{r(m)}\ell + 1 \), \( 2\ell + 1 \) are coprime to \( p \). Since there are just three linear forms, such congruence classes exist modulo primes \( p > 3 \) by the pigeonhole principle; and also for \( p = 3 \) as may be verified by a case-by-case analysis. Thus the result follows when \( m_1 \) is odd.

So we may assume that \( m_1 \) is even and now consider

\[
N(m, \frac{2m}{r(m)}(\ell + 1) + 1) - N(m, \frac{2m}{r(m)}(\ell + 1)) = \#\{i : 4\ell + 1 \leq i \leq 4\ell + 4 \text{ : } (i, m) = 1\}.
\]

Select \( \ell \equiv -3/4 \pmod{m_2} \) so that \( (4\ell + 3, m) \geq m_2 \). We can again select \( \ell \pmod{p} \) for each prime \( p \) dividing \( m_1 \) so that each of \( \frac{2m}{r(m)}(\ell + 1) + 1 \), \( \frac{2m}{r(m)}\ell + 1 \), \( 4\ell + 1 \) are coprime to \( p \) by the pigeonhole principle, and therefore the result follows if \( 3 \) does not divide \( m_1 \).

So we may assume that \( 6|m_1 \). Select integer \( \ell \) so that \( \ell \equiv 1 \pmod{m_2} \), \( \ell \equiv m/r(m) \pmod{4} \) and, for each prime \( p \) dividing \( m_2/2 \), \( p \) does not divide \( \ell, \frac{m}{r(m)}\ell - 1 \) or \( \frac{m}{r(m)}\ell + 3 \). Therefore, since \( 3r(m)/m \leq 3/5 \), we have

\[
N(m, \frac{1}{2}((\frac{m}{r(m)}(\ell + 3)) - N(m, \frac{1}{2}((\frac{m}{r(m)}\ell - 1))) = \#\{i : \ell \leq i < \ell + 1 \pmod{1} \} = 1.
\]

5. When \( \phi_m = p\Box \).

**Lemma 5.1.** Suppose that \( \phi_m = p\Box \), where \( p \) is an odd prime, \( m = p^e n \), \( 1 < n \leq p + 1 \) and \( p|\phi_n \). If \( u \equiv u' \pmod{n} \) with \((uu', m) = 1 \) then \( N(m, u') - N(m, u) \) is even. If \( e = 1 \) and \( n \neq p \) then this implies that \( N(n, u'/p) - N(n, u/p) \) is even.
Proof. Let \( k, k^* \) be integers for which \( k \equiv 1/u \pmod{m} \) and \( k^* \equiv 1/u' \pmod{m} \). Evidently \( k \equiv 1/u \equiv 1/u' \equiv k^* \pmod{n} \). If \( k \equiv k^* \pmod{2n} \) then let \( k' = k^* \), otherwise take \( k' = k + m \), so \( k' \equiv k \pmod{2n} \) (since \( m/n = p^e \) is odd). Therefore writing \( k' = k + 2nj \) we have \( x_{k'} = x_kx_{n+1}^{2j} \pmod{x_n} \), by Lemma 1(iii); and so \( (x_k/p) = (x_{k'}/p) \) since \( p|x_n \). Therefore since \( \phi_m = p \) we have \( (x_k/\phi_m) = (x_k/p) = (x_{k'}/\phi_m) \) and the first result follows from (5).

If \( e = 1 \) then \( m = pn \) so that \( r(m)/m = r(n)/n \). Therefore \( N(m, u') - N(m, u) \) equals, for \( U = 2ur(n)/n \) and \( U' = 2ur(n)/n \),

\[
\sum_{1 \leq i < U'} \frac{1}{(i, r(n)) = 1} - \sum_{1 \leq i < U'} \frac{1}{(i, r(n)) = 1} \equiv \sum_{1 \leq i < U'} \frac{1}{(i, r(n)) = 1} \quad \pmod{2},
\]

since \( U' \equiv U \pmod{2r(n)} \) (as \( u \equiv u' \pmod{n} \)), so that the first term counts each residue class coprime with \( r(n) \) an even number of times, and by writing \( i = jp \) in the second sum. The result follows.

Proposition 5.2. Suppose \( n \geq 2 \) and \( n \) divides \( p - 1 \) or \( p + 1 \) for some odd prime \( p \). Let \( m = p^en \) for some \( e \geq 1 \). There exists an integer \( u \) such that \( (u(u + n), m) = 1 \) for which \( N(m, u + n) - N(m, u) = 1 \) if \( e \geq 2 \), for which \( N(n, (u + n)/p) - N(n, u/p) = 1 \) if \( e = 1 \), except when \( p = 3, n = 2 \). In that case we have \( N(2 \cdot 3^e, \frac{3^{e-1} + 4 + 3(-1)^e}{2}) - N(2 \cdot 3^e, 1) = 1 \), for \( e \geq 2 \).

Lemma 5.3. If \( n \geq 3 \) and odd prime \( p = n - 1 \) or \( p \geq n + 1 \) (except for the cases \( n = 3 \) or \( 6 \) with \( p = 5 \); and \( n = 4, p = 3 \)) then in any non-closed interval of length \( n \), containing exactly \( n \) integers, there exists an integer \( u \) for which \( u \) and \( u + n \) are both prime to \( np \).

Proof. Since \( p \geq n - 1 \) there are no more than three integers, in our two consecutive intervals of length \( n \), that are divisible by \( p \) so the result follows when \( \phi(n) \geq 4 \). Otherwise \( n = 3, 4 \) or \( 6 \), and if the reduced residues are \( 1 < a < b < n \) then \( p \) divides \( b - a, (n + b) - a, (n + a) - b \) or \( (2n + a) - b \). Therefore \( p|4, 10, 2 \) or \( 8 \) for \( n = 6; p|2 \) or \( 6 \) for \( n = 4; p|1, 4, 2 \) or \( 5 \) for \( n = 3 \). The result follows.

Proof of Proposition 5.2. Let \( f := \max\{1, e - 1\} \). The result holds for

\[
(m, u) = \left(3 \cdot 5^e, \frac{5f - 3}{2}\right), \left(6 \cdot 5^e, \frac{5f - 3}{2}\right), \left(4 \cdot 3^e, 3f - 2\right), \left(2 \cdot p^e, \frac{p^f - j}{2}\right)
\]

for each \( e \geq 1 \) and, in the last case, any prime \( p > 3 \), where \( j \) is either 1 or 3, chosen so that \( u \) is odd.

Otherwise we can assume the hypotheses of Lemma 5.3. Now suppose that \( e \geq 2 \). Given an integer \( \ell \) we can select \( u \) in the range \( \ell \frac{m}{2\ell} - n < u \leq \ell \frac{m}{2\ell} \) (which is an interval of length \( n \)) such that \( u \) and \( u' := u + n \) are both prime to \( np \), by Lemma 5.3. Therefore \( N(m, u') - N(m, u) \) counts the number of integers, coprime with \( m \), in an interval of length \( \lambda := 2nr(m)/m = 2r(n)/p^{e-1} \). Note that \( \lambda \leq 2n/p \leq 2(p + 1)/p < 3 \) so our...
interval contains no more than \( |\lambda| + 1 \leq 3 \) integers, one of which is \( \ell \). If \( \lambda < 2 \) we select \( \ell \equiv 1 \pmod{p} \) and \( \ell \equiv -1 \pmod{n} \) so that \( N(m, u') - N(m, u) = 1 \). Otherwise \( \lambda \geq 2 \) so that \( n \geq r(n) \geq p^{e-1} \geq p \), and thus \( n = p + 1 \), \( e = 2 \) and \( r(n) = n \), that is \( n \) is squarefree, and \( 2(p + 1)|n \). So select \( \ell \) to be an odd integer for which \( \ell \equiv 2 \pmod{p} \) and \( \ell \equiv -2 \pmod{n/2} \) so that \( \ell \pm 2, \ell \pm 1 \) all have common factors with \( m \), and therefore \( N(m, u') - N(m, u) = 1 \).

For \( e = 1 \) and given integer \( \ell \) we now select \( u \) in the range \( \ell \frac{p^m}{2r(n)} - n < u \leq \ell \frac{p^m}{2r(n)} \), and \( N(n, u'/p) - N(n, u/p) \) counts the number of integers, coprime with \( n \), in an interval of length \( \lambda := 2r(n)/p \). If \( \lambda < 1 \) we select \( \ell \) so that it is coprime with \( n \) then we have that \( N(n, u'/p) - N(n, u/p) = 1 \) is odd. If \( \lambda \geq 1 \) we have \( r(n) \geq p/2 \), and we know that \( r(n)|n|p \pm 1 \), so that \( r(n) \) and \( n \) equal \( \frac{p+1}{2} \), \( p - 1 \) or \( p + 1 \). If \( n = r(n) = p - 1 \) then \( n \) is squarefree and divisible by 2, and \( [\lambda] = 1 \); so we select \( \ell \equiv 1 \pmod{2} \) and \( \ell \equiv -1 \pmod{n/2} \) so that \( N(n, u'/p) - N(n, u/p) = 1 \). In all the remaining cases, one may check that \( N(n, (n + 1)/p) - N(n, 1/p) = 1 \).

**Proposition 5.4.** If \( m = p^{e+1} \) where \( p \) is an odd prime then \( N\left(m, \frac{p^{e+1}}{2}\right) - N(m, 1) = 1 \).

### 6. Other Lucas sequences

**Proposition 6.1.** Assume that \( \Delta \) and \( b \) are positive with \( (b, c) = 1 \). For \( n > 1 \) odd with \( (m, n) = 1 \) we have the following:

\[
\left(\frac{x_m}{x_n}\right) = \begin{cases} 
\left(\frac{\varepsilon}{b}\right)^{\frac{(m-1)(n-1)}{2}} & \text{if } 4 | c \\
(-1)^{(m/n) + \frac{b+1}{2}(m-1)} \left(\frac{\varepsilon}{b}\right)^{\frac{(m-1)(n-1)}{2}} & \text{if } c \equiv 2 \pmod{4} \\
\left(\frac{m}{n}\right)^{\frac{m-1}{2}} \left(\frac{2}{n}\right)^{(m-1)(b+\varepsilon)} \left(\frac{b}{c}\right)^{\frac{(m-1)(n-1)}{2}} & \text{if } 2 | b 
\end{cases}
\]

**Proof.** For \( m \) odd this is the result of Rotkiewicz [Ro2], discussed in section 1c. Note that if \( c \) is even then \( b \) is odd and \( x_n \) is odd for all \( n \geq 1 \); and if \( b \) is even then \( c \) is odd and \( x_n \equiv n \pmod{2} \) is odd for all \( n \geq 1 \). Thus \( x_n \) is odd if and only if \( n \) is odd.

For \( m \) even and \( n \) odd we have that \( m + n \) is odd and so

\[
\left(\frac{x_m}{x_n}\right) = \left(\frac{x_{m+n}}{x_n}\right) \left(\frac{x_{n+1}}{x_n}\right);
\]

and therefore

\[
\left(\frac{x_{n+1}}{x_n}\right) = \left(\frac{x_2}{x_n}\right) \left(\frac{x_{n+2}}{x_n}\right);
\]

note that \( n, n + 2 \) are both odd, so we have yet to determine only \( (x_2/x_n) = (b/x_n) \).

Suppose that \( c \) is even so that \( b \) is odd. If \( 4 | c \) then \( x_n \equiv 1 \pmod{4} \) if \( n \) is odd so that \( (b/x_n) = (x_n/b) \). If \( c \equiv 2 \pmod{4} \) and \( b \equiv 1 \pmod{4} \) then \( (b/x_n) = (x_n/b) \). Now \( x_n \equiv cx_{n-2} \pmod{b} \) and so \( x_n \equiv c^{(n-1)/2} \pmod{b} \) for every odd \( n \). Therefore

\[
\left(\frac{x_m}{x_n}\right) = \left(\frac{x_{m+n}}{x_n}\right) \left(\frac{x_{n+2}}{x_n}\right) \left(\frac{c}{b}\right)^{(n-1)/2}.
\]
The results follow in these cases since \( \Lambda((m+n)/n) = \Lambda(m/n) \) as \((m+n)/n = 1 + m/n, \) and \( \Lambda((n+2)/n) = 3 \) as \((n+2)/n = [1, \frac{n-1}{2}, 2]. \)

If \( c \equiv 2 \pmod{4} \) and \( b \equiv 3 \pmod{4} \) then \( x_n \equiv 3 \pmod{4} \) for all \( n \geq 2. \) Therefore \( b/x_n = -(x_n/b) \) for all odd \( n > 1, \) and the result follows.

Now assume that \( b \) is even so that \( c \) is odd. As \( x_n \equiv c^{(n-1)/2} \pmod{[b,4]} \) for each odd \( n \) we have, writing \( b = 2^e B \) with \( B \) odd,

\[
\left( \frac{b}{x_n c^{(n-1)/2}} \right) = \left( \frac{2}{x_n c^{(n-1)/2}} \right)^e \left( \frac{x_n c^{(n-1)/2}}{B} \right) = \left( \frac{2}{x_n c^{(n-1)/2}} \right)^e.
\]

Now if \( 8 | b \) then \( x_n \equiv c^{(n-1)/2} \pmod{8}; \) if \( e = 2 \) this last term is also 1. Finally, if \( e = 1 \) then \( x_n c^{(n-1)/2} \equiv 1 \pmod{8} \) if \( n \equiv \pm 1 \pmod{8}, \) and \( \equiv 5 \pmod{8} \) if \( n \equiv \pm 3 \pmod{8}. \) Therefore \( \left( \frac{2}{x_n c^{(n-1)/2}} \right) = \left( \frac{2}{n} \right). \) The result follows.

**Corollary 6.2.** Suppose that \( c \equiv 2 \pmod{4} \) and \( b \equiv 1 \pmod{2}, \) with \( n \) odd, \( m > 1 \) and \((m,n) = 1. \) If \( n \) is a power of prime \( p \) then

\[
\left( \frac{x_m}{\phi_n} \right) = (-1)^{N(n,u)} \left( \frac{c}{b} \right)^{m-1(p-1)/2}.
\]

If \( n \) has at least two distinct prime factors then

\[
\left( \frac{x_m}{\phi_n} \right) = (-1)^{N(n,u)}.
\]

If \( m \) is even and > 2 then

\[
\left( \frac{\phi_m}{x_n} \right) = (-1)^{N(m,u)+\mu^2(m)}.
\]

**Proof.** Follows immediately from Proposition 6.1 and the easily verified fact that

\[
\prod_{d|n} \left( \frac{A}{d} \right)^{\mu(n/d)} = 1,
\]

except that it is \( \left( \frac{A}{p} \right) \) where \( n \) is a power of prime \( p. \)

**Proof of Theorem 2.** If \( m \) is odd and has at least two prime factors, or if \( m \) is even \( \neq 2,6, \) or if \( m = p^e \) where \( p \) is an odd prime and \( (c/b)^{(p-1)/2} = 1, \) then we can deduce that \( y_m \) is not a square, just as we did in the proof of Theorem 2', by using Corollary 6.2, and then Propositions 4.1 and 5.2 (with Lemma 5.1). Now suppose that \( m = p^e \) where \( p \) is an odd prime and \( (c/b)^{(p-1)/2} = -1: \) If \( \phi_m \) is a square then Corollary 6.2 yields

\[
1 = (x_{m-1}/\phi_m)(x_{2m-1}/\phi_m) = -1, \quad \text{a contradiction.}
\]

If \( p\phi_m \) is a square and \( e \geq 2 \) then Lemma 5.1 remains valid (since \( k \equiv k' \pmod{2} \) in the proof there, and by Corollary 6.2) and the result follows from Proposition 5.4.

We note that in the other cases with \( bc \) even, our argument will not yield such a general result about primitive prime factors:
Corollary 6.3. Suppose that $4|c$ and $b \equiv 1 \pmod{2}$, with $n$ odd and $(m, n) = 1$. If $n$ is a power of prime $p$ then
$$\left(\frac{x_m}{\phi_n}\right) = \left(\frac{c}{b}\right)^{(m-1)(p-1)/2}.$$Otherwise $(x_m/\phi_n) = 1$ if $n$ has at least two distinct prime factors; and $(\phi_m/x_n) = 1$ if $m$ is even and $> 2$.

Corollary 6.4. Suppose that $b$ is even and $c$ is odd, with $n$ odd and $(m, n) = 1$. If $n$ is a power of prime $p$ then
$$\left(\frac{x_m}{\phi_n}\right) = \left(\frac{m}{p}\right)^{\frac{c-1}{2}} \left(\frac{2}{p}\right)^{(m-1)(b+c-1)} \left(\frac{b}{c}\right)^{(m-1)(p-1)/2}.$$Otherwise $(x_m/\phi_n) = 1$ if $n$ has at least two distinct prime factors; and $(\phi_m/x_n) = 1$ if $m$ is even and $> 2$, except when $c \equiv -1 \pmod{4}$, $m$ is a power of 2, and $n \equiv \pm 3 \pmod{8}$.

References
2. Chao Ko, On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica (Notes) 14 (1965), 457-460.