Some identities and congruences for a special family of second order recurrences

JAMES P. JONES* and PÉTER KISS**

Abstract. For a fixed integer a with $|a|>2$ let $Y(n)$ and $X(n)$ be second order linear recursive sequences defined by

$$Y(n)=aY(n-1)-Y(n-2) \quad \text{and} \quad X(n)=aX(n-1)-X(n-2)$$

respectively, where the initial terms are $Y(0)=0$, $Y(1)=1$, $X(0)=2$ and $X(1)=a$. In this paper we prove identities for these sequences which yield some congruences for the terms $Y(kn)$ and $X(kn)$, where the modulus are a power of the n^{th} terms.

Let $Y(n)$, $n = 0, 1, 2, \ldots$, be a second order linear recursive sequence defined by

$$Y(n) = aY(n-1) - Y(n-2),$$

where a is a given integer with $|a| > 2$ and the initial terms are $Y(0) = 0$ and $Y(1) = 1$. Its associated sequence will be denoted by $X(n)$ which is defined by

$$X(n) = aX(n-1) - X(n-2)$$

and by initial terms $X(0) = 2$, $X(1) = a$. It is well known that the terms of these sequences can be expressed as

$$(1) \qquad Y(n) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad X(n) = \alpha^n + \beta^n,$$

where

$$\alpha = \frac{a + \sqrt{a^2 - 4}}{2} \qquad \text{and} \qquad \beta = \frac{a - \sqrt{a^2 - 4}}{2}$$

are the roots of the polynomial $x^2 - ax + 1$.

---

* Research supported by National Science and Research Council of Canada, Grant N° OGP 0004525.

** Research supported by Foundation for Hungarian Higher Education and Research and Hungarian OTKA Foundation, Grant N° 016975 and 020295.

The sequences $X(n)$ and $Y(n)$ have important applications to Diophantine equations and Hilbert's tenth problem since they give all solutions to the polynomial identity

$$X^2 - (a^2 - 4)\, y^2 = 4$$

(see [4]). These sequences are special cases $P = a$ and $Q = 1$ of more general linear recurrent sequences V_n and U_n of Lucas which was defined by the recursion $U_n = PU_{n-1} - QU_{n-2}$. Consequently many identities and congruence properties are know for our sequences X, Y and also for more general sequences (see, e.g. [1], [2], [3] and [5]). For example it is well known that

$$Y(kn) \equiv 0 \pmod{Y(n)}$$

for any natural numbers k and n. Lucas [3] also showed many properties of these sequences, e.g. he showed that $Y(2n) = X(n)Y(n)$ and $X(2n) = X(n)^2 - 2$ and so

$$X(2n) \equiv -2 \pmod{X(n)^2}.$$

The purpose of this paper is to prove some congruences involving $Y(kn)$ and $X(kn)$, where the modulus is a power of the nth term. In the proofs we use formulas of (1) but sometimes we give other methods not using the Binet formula. Specifically we prove the following congruences:

Theorem 1. Let k be an even positive integer. Then

$$Y(kn) \equiv \frac{k}{2} Y(2n) \pmod{Y(n)^3}$$

for any integer $n > 0$.

Theorem 2. Let k be an odd positive integer. Then

$$Y(kn) = kY(n) \pmod{Y(n)^3}$$

for any integer $n > 0$.

Theorem 3. Let k be an odd positive integer. Then

$$X(kn) \equiv k(-1)^{\frac{k-1}{2}} X(n) \pmod{X(n)^2}$$

for any integer $n > 0$.

Theorem 4. Let k be an even positive integer. Then

$$X(kn) \equiv 2(-1)^{k/2} \pmod{X(n)^2}$$

for any integer $n > 0$.

We prove some summation identities for the sequences which will be used for the proofs of the above theorems.

Lemma 1. If k is an even positive integer, then

$$Y(kn) - \frac{k}{2}Y(2n) = (a^2-4)Y(2n) \sum_{1\le i\le [\frac{k}{4}]} Y\left(n\left(\frac{k}{2}-2i+1\right)\right)^2$$

for any natural number n.

Proof. Since k is even, we can write $k = 2t$.

Let first t be an odd integer. By (1), using $\alpha-\beta = \sqrt{a^2-4}$ and $\alpha\beta = 1$, we have

$$\begin{aligned} Y(kn) &= \frac{\alpha^{2tn} - \beta^{2tn}}{\alpha-\beta} \\ &= \frac{\alpha^{2n} - \beta^{2n}}{\alpha-\beta}\left(\alpha^{2n(t-1)} + \alpha^{2n(t-2)}\beta^{2n} + \cdots + \beta^{2n(t-1)}\right) \\ &= Y(2n)\left(1 + \sum_{i=1}^{\frac{t-1}{2}}\left(\alpha^{2n(t-2i+1)} + \beta^{2n(t-2i+1)}\right)\right), \\ &= Y(2n)\left(1 + 2\frac{t-1}{2} + \sum_{i=1}^{\frac{t-1}{2}}\left(\alpha^{n(t-2i+1)} - \beta^{n(t-2i+1)}\right)^2\right) \\ &= Y(2n)\left(t + \sum_{i=1}^{\frac{t-1}{2}}(a^2-4)Y\left(n(t-2i+1)\right)^2\right). \end{aligned}$$

From this the lemma follows in the case t is odd.

Now let t be even, i.e. $t = 2j$ for some j. Then

$$\begin{aligned} &\left(\alpha^{2n(t-1)} + \alpha^{2n(t-2)}\beta^{2n} + \cdots + \beta^{2n(t-1)}\right) \\ &= \sum_{i=1}^{t/2}\left(\alpha^{2n(t-2i+1)} + \beta^{2n(t-2i+1)}\right) \\ &= 2\frac{t}{2} + \sum_{i=1}^{t/2}\left(\alpha^{n(t-2i+1)} - \beta^{n(t-2i+1)}\right)^2 \\ &= t + \sum_{i=1}^{t/2}(a^2-4)Y\left(n(t-2i+1)\right)^2, \end{aligned}$$

and so, similarly as above

$$Y(kn)=Y(2n)\left(t+(a^2-4)\sum_{i=1}^{t/2}Y\left(n(t-2i+1)\right)^2\right)$$

follows which implies the lemma.

Lemma 2. If k is an even positive integer, then

$$Y(kn)-\frac{k}{2}Y(2n)=(a^2-4)Y(n)\sum_{i=1}^{\frac{k-2}{2}}Y(ni)Y(ni+n)$$

for any natural number n.

Proof. The identity will be proved by induction on k. The lemma holds for $k=2$ since both sides of the identity are 0 in this case. Now let us suppose that the identity holds for an even positive integer k. We prove that then it holds also for $k+2$. To this and by the induction hypothesis, it is enough to prove that

$$\begin{aligned}\left(Y((k+2)n)\right.&\left.-\frac{k+2}{2}Y(2n)\right)-\left(Y(kn)-\frac{k}{2}Y(2n)\right)\\&=(a^2-4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n+n\right),\end{aligned}$$

or equivalently

$$\begin{aligned}&2Y(kn+2n)-2Y(kn)-2Y(2n)\\&=2(a^2-4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n+n\right).\end{aligned}\tag{2}$$

To prove this we need the equations

$$Y(2n)=X(n)Y(n),\tag{3}$$

$$X(2n)=(a^2-4)Y(n)^2+2=X(n)^2-2,\tag{4}$$

$$2Y(n+m)=Y(n)X(m)+X(n)Y(m)\tag{5}$$

and

$$2X(n+m)=X(n)X(m)+(a^2-4)Y(n)Y(m).\tag{6}$$

These are old identities known to Lucas [3], which can be proved easily using (1) and the fact that $(\alpha-\beta)^2 = a^2-4$.

To verify (2), by (3), (4) and (5) we get

$$\begin{aligned}
2Y(kn+2n) &- 2Y(kn) - 2Y(2n)\\
&= Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 2Y(2n)\\
&= Y(2n)\left(X(kn)-2\right) + Y(kn)\left(X(2n)-2\right)\\
&= Y(n)X(n)\left(X(kn)-2\right) + Y(kn)(a^2-4)Y(n)^2\\
&= Y(n)X(n)(a^2-4)Y\left(\frac{k}{2}n\right)^2 + Y\left(\frac{k}{2}n\right)X\left(\frac{k}{2}n\right)\left(a^2-4\right)Y(n)^2\\
&= \left(a^2-4\right)Y(n)Y\left(\frac{k}{2}n\right)\left(Y\left(\frac{k}{2}n\right)X(n) + X\left(\frac{k}{2}n\right)Y(n)\right)\\
&= 2(a^2-4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n+n\right).
\end{aligned}$$

So (2) holds and the lemma is proved.

Lemma 3. If k is an even positive integer, then

$$(7)\qquad Y(n)\sum_{i=0}^{\frac{k-2}{2}} Y(ni)Y(ni+n) = Y(2n)\sum_{1\le i\le\left[\frac{k}{4}\right]} Y\left(n\left(\frac{k}{2}-2i+1\right)\right)^2$$

and

$$(8)\qquad \sum_{i=0}^{k-2} Y(ni)Y(ni+n) = X(n)\sum_{1\le i\le\left[\frac{k}{4}\right]} Y\left(n\left(\frac{k}{2}-2i+1\right)\right)^2$$

for any natural number n.

Proof. (7) follows from Lemma 1 and 2 and (8) follows from (7) using (3).

Lemma 4. If k is an odd positive integer, then

$$Y(kn) - kY(n) = (a^2-4)Y(n)\sum_{i=0}^{\frac{k-1}{2}} Y(ni)^2$$

for any natural number n.

Proof. The proof could be carried out by using the Binet formula (1), but we follow another way similar to the proof of Lemma 2.

The lemma holds for $k = 1$, because then both sides are 0. Assume that the identity holds for an odd k. We have to show that then it holds also for $k + 2$. By the induction hypothesis we have to prove that

$$\left(Y\left((k+2)n\right)-(k+2)Y(n)\right) - \left(Y(kn) - kY(n)\right) = (a^2-4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2$$

or equivalently

$$2Y(kn+2n) - 2Y(kn) - 4Y(n) = 2(a^2-4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2. \tag{9}$$

By (3), (4), (5) and (6) we have

$$\begin{aligned}
&2Y(kn+2n) - 2Y(kn) - 4Y(n) \\
&\quad= Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 4Y(n) \\
&\quad= X(kn)Y(n)X(n) + \left(X(2n)-2\right)Y(kn) - 4Y(n) \\
&\quad= Y(n)X(kn)X(n) + (a^2-4)Y(n)^2Y(kn) - 4Y(n) \\
&\quad= Y(n)\left(X(kn)X(n) + (a^2-4)Y(kn)Y(n)\right) - 4Y(n) \\
&\quad= 2Y(n)X(kn+n) - 4Y(n) = 2Y(n)\left(X(kn+n)-2\right) \\
&\quad= 2Y(n)(a^2-4)Y\left(\frac{kn+n}{2}\right)^2 = 2(a^2-4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2.
\end{aligned}$$

Thus (9) holds which proves the lemma.

Now we can prove the theorems.

Proof of Theorem 1. The theorem follows from Lemma 1 or Lemma 2 since $Y(tn)$ is divisible by $Y(n)$ for any positive integers t and n.

Proof of Theorem 2. Similarly as above, the theorem follows from Lemma 4 since $Y(n) \mid Y(ni)$.

Proof of Theorem 3. Let $k = 2q + 1$ $(q \geq 0)$. We prove the theorem by induction on q. For $q = 0$ and $q = 1$ the theorem can be seen directly. Suppose that $q > 1$ and that the theorem is true for numbers less than q.

Then using $\alpha\beta = 1$ we have

$$\begin{aligned} X(kn) &= X\big(n(2q+1)\big) = \alpha^{n(2q+1)} + \beta^{n(2q+1)} \\ &= \left(\alpha^{n(2q-1)} + \beta^{n(2q-1)}\right)\left(\alpha^{2n} + \beta^{2n}\right) - \left(\alpha^{n(2q-3)} + \beta^{n(2q-3)}\right) \\ &\equiv (-1)^{q-1}(2q-1)(\alpha^n + \beta^n)(\alpha^{2n} + \beta^{2n}) \\ &\quad - (-1)^{q-2}(2q-3)(\alpha^n + \beta^n) \pmod{(\alpha^n + \beta^n)^2}. \end{aligned}$$

But $\alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2 \equiv -2 \pmod{X(n)^2}$ and so

$$\begin{aligned} X(kn) &\equiv (\alpha^n + \beta^n)\left(-2(-1)^{q-1}(2q-1) - (-1)^{q-2}(2q-3)\right) \\ &\equiv (\alpha^n + \beta^n)(-1)^q\left(2(2q-1) - (2q-3)\right) \\ &\equiv (-1)^q(2q+1)(\alpha^n + \beta^n) \pmod{(\alpha^n + \beta^n)^2}. \end{aligned}$$

From this the theorem follows since $k = 2q + 1$.

Proof of Theorem 4. Let $k = 2q \quad (q > 0)$. We prove Theorem 4 also by induction on q. By (4) the theorem can be easily verified for $q = 1$ and $q = 2$. Assume that $q > 2$ and that the theorem holds for $q - 1$ and $q - 2$. Then by the hiphothesis, using (1) and (4), we have

$$\begin{aligned} X(kn) &= X(2nq) = \alpha^{2nq} + \beta^{2nq} \\ &= \left(\alpha^{2n(q-1)} + \beta^{2n(q-1)}\right)\left(\alpha^{2n} + \beta^{2n}\right) - \left(\alpha^{2n(q-2)} + \beta^{2n(q-2)}\right) \\ &\equiv -4(-1)^{q-1} - 2(-1)^{q-2} \equiv 2(-1)^q \pmod{X(n)^2} \end{aligned}$$

which proves the theorem.

References

[1] D. JARDEN, Recurring sequences. *Riveon Lematematika*, Jerusalem (Israel), 1973.

[2] J. P. JONES and P. KISS, Generalized Lucas sequences, to appear.

[3] E. LUCAS, Theorie des fonctions numériques simplement périodiques. *Amer. Jour. of Math.*, **1** (1878), 184–240, 289–321.

[4] J. ROBINSON and Y. V. MATIJASEVIC, Reduction of an arbitraty diophantine equatin to one in 13 unknowns. *Acta Arithmetica*, **27** (1975), 521–553.

[5] C. R. WALL., Some congruence involving generalized. Fibonacci numbers, *Fibonacci Quart.*, **17** (1979), 29–33.