Some congruences concerning second order linear recurrences

JAMES P. JONES and PÉTER KISS*

Abstract. Let U_n and V_n (n=0,1,2,...) be sequences of integers satisfying a second order linear recurrence relation with initial terms U_0=0, U_1=1, V_0=2, V_1=A. In this paper we investigate the congruence properties of the terms U_{nk} and V_{nk}, where the moduli are powers of U_n and V_n.

Let U_n and V_n $(n = 0, 1, 2, \ldots)$ be second order linear recursive sequences of integers defined by

$$U_n = AU_{n-1} - BU_{n-2} \quad (n > 1)$$

and

$$V_n = AV_{n-1} - BV_{n-2} \quad (n > 1),$$

where A and B are nonzero rational integers and the initial terms are $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = A$. Denote by α, β the roots of the characteristic equation $x^2 - Ax + B = 0$ and suppose $D = A^2 - 4B \neq 0$ and hence that $\alpha \neq \beta$. In this case, as it is well known, the terms of the sequences can be expressed as

$$(1) \qquad U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n$$

for any $n \geq 0$.

Many identities and congruence properties are known for the sequences U_n and V_n (see, e.g. [1], [4], [5] and [6]). Some congruence properties are also known when the modulus is a power of a term of the sequences (see [2], [3], [7] and [8]). In [3] we derived some congruences where the moduli was U_n^3, V_n^2 or V_n^3. Among other congruences we proved that

$$U_{nk} \equiv kB^{n\frac{k-1}{2}} U_n \pmod{U_n^3}$$

* Research supported by the Hungarian National Research Science Foundation, Operating Grant Number OTKA T 16975 and 020295.

when k is odd and a similar congruence for even k. In this paper we extend the results of [3]. We derive congruences in which the moduli are product of higher powers of U_n and V_n.

Theorem. *Let U_n and V_n be second order linear recurrences defined above and let $D = A^2 - 4B$ be the discriminant of the characteristic equation. Then for positive integers n and k we have*

1. $U_{nk} \equiv kB^{\frac{k-1}{2}n} U_n + \frac{k(k^2-1)}{24} DB^{\frac{k-3}{2}n} U_n^3 \pmod{D^2 U_n^5}$, k odd,
2. $U_{nk} \equiv \frac{k}{2} B^{\frac{k-2}{2}n} V_n U_n + \frac{k(k^2-4)}{48} DB^{\frac{k-4}{2}n} V_n U_n^3 \pmod{D^2 V_n U_n^5}$, k even,
3. $V_{nk} \equiv k(-1)^{\frac{k-1}{2}} B^{\frac{k-1}{2}n} V_n + \frac{k(k^2-1)}{24}(-1)^{\frac{k-3}{2}} B^{\frac{k-3}{2}n} V_n^3 \pmod{V_n^5}$, k odd,
4. $V_{nk} \equiv 2(-1)^{\frac{k}{2}} B^{\frac{k}{2}n} + \frac{k^2}{4}(-1)^{\frac{k-2}{2}} B^{\frac{k-2}{2}n} V_n^2 \pmod{V_n^4}$, k even,
5. $U_{nk} \equiv U_n(-1)^{\frac{k-1}{2}} B^{\frac{k-1}{2}n} + \frac{k^2-1}{8}(-1)^{\frac{k-3}{2}} B^{\frac{k-3}{2}n} U_n V_n^2 \pmod{U_n V_n^4}$, k odd,
6. $U_{nk} \equiv \frac{k}{2}(-1)^{\frac{k-2}{2}} B^{\frac{k-2}{2}n} U_n V_n + \frac{k(k^2-4)}{48}(-1)^{\frac{k-4}{2}} B^{\frac{k-4}{2}n} U_n V_n^3 \pmod{U_n V_n^5}$, k even,
7. $V_{nk} \equiv B^{\frac{k-1}{2}n} V_n + \frac{k^2-1}{8} DB^{\frac{k-3}{2}n} V_n U_n^2 \pmod{D^2 V_n U_n^4}$, k odd,
8. $V_{nk} \equiv 2B^{\frac{k}{2}n} + \frac{k^2}{4} B^{\frac{k-2}{2}n} DU_n^2 \pmod{D^2 U_n^4}$, k even.

We note that the congruences of [3] follow as consequences of this theorem.

For the proof of the Theorem we need some auxiliary results which are known (see e.g. [6]) but we show short proofs for them. In the followings we suppose that $A > 0$ and hence that

$$\alpha = \frac{A + \sqrt{D}}{2} \quad \text{and} \quad \beta = \frac{A - \sqrt{D}}{2},$$

so that $\alpha - \beta = \sqrt{D}$, $\alpha + \beta = A$, $\alpha\beta = B$ and hence by (1)

$$U_n = \frac{\alpha^n - \beta^n}{\sqrt{D}} \tag{2}$$

Lemma 1. *For any integer $n \geq 0$ we have*

$$U_{3n} = 3U_n B^n + DU_n^3.$$

Proof. By (2), using that $\alpha\beta = B$, we have to prove that

$$\frac{\alpha^{3n} - \beta^{3n}}{\sqrt{D}} = 3 \cdot \frac{\alpha^n - \beta^n}{\sqrt{D}} (\alpha\beta)^n + D\left(\frac{\alpha^n - \beta^n}{\sqrt{D}}\right)^3,$$

which follows from $\alpha^{3n} - \beta^{3n} = 3(\alpha^n - \beta^n)\alpha^n\beta^n + (\alpha^n - \beta^n)^3$.

Lemma 2. *For any non-negative integers m and n we have*

$$U_{m+2n} = V_n U_{m+n} - B^n U_m.$$

Proof. Similarly as in the proof of Lemma 1,

$$\frac{\alpha^{m+2n} - \beta^{m+2n}}{\sqrt{D}} = (\alpha^n + \beta^n)\frac{\alpha^{m+n} - \beta^{m+n}}{\sqrt{D}} - (\alpha\beta)^n \frac{\alpha^m - \beta^m}{\sqrt{D}}$$

is an identity which by (1) and (2), implies the lemma.

Lemma 3. *For any $n \geq 0$ we have*

$$V_{2n} = 2B^n + DU_n^2 = V_n^2 - 2B^n \quad \text{and} \quad U_{2n} = U_n V_n.$$

Proof. The identities

$$\alpha^{2n} + \beta^{2n} = 2(\alpha\beta)^n + D\left(\frac{\alpha^n - \beta^n}{\sqrt{D}}\right)^2 \text{ and } \frac{\alpha^{2n} - \beta^{2n}}{\sqrt{D}} = \frac{\alpha^n - \beta^n}{\sqrt{D}}(\alpha^n + \beta^n)$$

prove the lemma.

Proof of the Theorem. We prove the first congruence of the Theorem by double induction on k. For $k = 1$ and $k = 3$, by Lemma 1, the congruence is an identity. Suppose the congruence holds for k and $k + 2$, where $k \geq 1$ is odd. Then by Lemma 2 and 3 we have

$$\begin{aligned} U_{n(k+4)} &= U_{nk+4n} = V_{2n}U_{nk+2n} - B^{2n}U_{nk} \\ &= (2B^n + DU_n^2)U_{n(k+2)} - B^{2n}U_{nk} \\ &\equiv (2B^n + DU_n^2)Q - B^{2n}R \pmod{D^2U_n^5}, \end{aligned} \tag{3}$$

where

$$Q = (k+2)B^{\frac{k+1}{2}n}U_n + \frac{(k+2)((k+2)^2 - 1)}{24}DB^{\frac{k-1}{2}n}U_n^3 \tag{4}$$

and

$$R = kB^{\frac{k-1}{2}n}U_n + \frac{k(k^2 - 1)}{24}DB^{\frac{k-3}{2}n}U_n^3. \tag{5}$$

After some calculation (3), (4) and (5) imply

$$U_{n(k+4)} \equiv U_n T + U_n^3 S \pmod{D^2 U_n^5}, \tag{6}$$

where

$$T = (2(k+2) - k)\, B^{\frac{k+3}{2}n} = (k+4) B^{\frac{(k+4)-1}{2}}$$

and

$$S = (k+2) D B^{\frac{k+1}{2}n} + 2 \frac{(k+2)\left((k+2)^2 - 1\right)}{24} D B^{\frac{k+1}{2}n} - \frac{k(k^2-1)}{24} D B^{\frac{k+1}{2}n} = \frac{(k+4)\left((k+4)^2 - 1\right)}{24} D B^{\frac{(k+4)-3}{2}n},$$

and so by (6),

$$U_{n(k+4)} \equiv (k+4) B^{\frac{(k+4)-1}{2}} U_n + \frac{(k+4)\left((k+4)^2-1\right)}{24} D B^{\frac{(k+4)-3}{2}n} U_n^3 \pmod{D^2 U_n^5}.$$

Hence the congruence holds also for $k+4$ and for any odd positive integer k.

The other congruences in the Theorem can be proved similarly using Lemma 1, 2, 3 and the identities

$$\begin{aligned}
U_{2n} &= V_n U_n, \\
V_{2n} &= V_n^2 - 2B^n = 2B^n + DU_n^2, \\
U_{3n} &= U_n V_n^2 - B^n U_n, \\
V_{3n} &= V_n^3 - 3B^n V_n = B^n V_n + DV_n U_n^2, \\
U_{4n} &= U_n V_n^3 - 2B^n U_n V_n, \\
V_{4n} &= V_n^4 - 4B^n V_n^2 + 2B^{2n}.
\end{aligned}$$

References

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

[2] J. P. Jones and P. Kiss, Some identities and congruences for a special family of second order recurrences, *Acta Acad. Paed. Agriensis, Sect. Math.* **23** (1995–96), 3–9.

[3] J. P. Jones and P. Kiss, Some new identities and congruences for Lucas sequences, *Discuss Math.*, to appear.

[4] D. H. Lehmer, On the multiple solutions of the Pell Equation, *Annals of Math.* **30** (1928), 66–72.

[5] D. H. Lehmer, An extended theory of Lucas' functions, *Annals of Math.* **31** (1930), 419–448.

[6] E. Lucas, Theorie des functions numériques simplement périodiques, *American Journal of Mathematics*, vol. **1** (1878), 184–240, 289–321. English translation: Fibonacci Association, Santa Clara Univ., 1969.

[7] S. Vajda, Fibonacci & Lucas numbers, and the golden section, *Ellis Horwood Limited Publ.*, New York-Toronto, 1989.

[8] C. R. Wall, Some congruences involving generalized Fibonacci numbers, *The Fibonacci Quarterly* **17.1** (1979), 29–33.

James P. Jones
Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta T2N 1N4
Canada

Péter Kiss
Eszterházy Károly Teachers' Training College
Department of Mathematics
Leányka u. 4.
3301 Eger, Pf. 43.
Hungary
E-mail: kissp@gemini.ektf.hu