SOME CONGRUENCE PROPERTIES OF GENERALIZED SECOND-ORDER INTEGER SEQUENCES

R. S. Melham

University of Technology, Sydney, 2007, Australia

A. G. Shannon

University of Technology, Sydney, 2007, Australia

(*Submitted April 1993*)

1. INTRODUCTION

Hoggatt and Bicknell [3] proved that for a prime p

$$L_{kp} \equiv L_k \pmod{p} \tag{1.1}$$

where $\{L_n\}$ is the Lucas sequence. Robbins [8] proved more general results for a broader class of integer sequences $\{U_n\}$ and $\{V_n\}$ which we soon define.

In the notation of Horadam [4] write

$$W_n = W_n(a, b; \mathrm{P}, \mathrm{Q}) \tag{1.2}$$

so that

$$W_n = \mathrm{P}W_{n-1} - \mathrm{Q}W_{n-2}, \quad W_0 = a,\ W_1 = b,\ n \geq 2. \tag{1.3}$$

Then

$$\begin{cases} U_n = W_n(0, 1; \mathrm{P}, \mathrm{Q}) \\ V_n = W_n(2, \mathrm{P}; \mathrm{P}, \mathrm{Q}) \end{cases}. \tag{1.4}$$

Indeed, $\{U_n\}$ and $\{V_n\}$ are the fundamental and primordial sequences generated by (1.3). They have been studied extensively, particularly by Lucas [7]. Further information can be found, for example, in [1], [4], and [6].

All sequences generated by (1.3) can be extended to negative subscripts using either the Binet form [4] or the recurrence relation (1.3). In all that follows, a, b, P, and Q are assumed to be integers. Robbins proved the following theorem.

Theorem 1: Let p be prime. If $\Delta = \mathrm{P}^2 - 4\mathrm{Q}$, then

$$V_{kp^n} \equiv V_{kp^{n-1}} \pmod{p^n}, \quad \text{all } p, \tag{1.5}$$

$$U_{kp^n} \equiv \left(\frac{\Delta}{p}\right) U_{kp^{n-1}} \pmod{p^n}, \quad \text{for } p \text{ odd and } p \nmid \Delta, \tag{1.6}$$

$$U_{k2^n} \equiv (-1)^{\mathrm{Q}} U_{k2^{n-1}} \pmod{2^n}, \tag{1.7}$$

where $\left(\frac{\Delta}{p}\right)$ is the Legendre symbol.

Remark 1: Robbins proved Theorem 1 under two strong assumptions. Firstly he assumed that $(P, Q) = 1$ and secondly that $\Delta > 0$. The first of these assumptions was used by Lucas [7] in his study of the sequences (1.4) and need not be adhered to in all contexts. Indeed, Robbins' arguments do not make explicit use of it and so it may be dropped. The assumption that $\Delta > 0$ was apparently made to ensure that $\sqrt{\Delta}$, which appears in a key proof involving Binet forms (Lemma 2.12), is real. However, this proof remains valid for $\Delta < 0$. In work on second-order recurrences the assumption $\Delta \neq 0$ is usually made so that the Binet form does not degenerate. However, in this context, following convention and putting $\left(\frac{0}{p}\right) = 0$, the proofs of certain key results (Lemmas 2.3 and 2.13) are greatly simplified when $\Delta = 0$. This is because the Binet forms become

$$\begin{cases} U_n = nA^{n-1} \\ V_n = 2A^n \end{cases}$$

where A is an integer. Likewise, putting $\left(\frac{\Delta}{p}\right) = 0$ when $p|\Delta$, the proof of Robbins' Lemma 2.14, another key result, becomes trivial.

With these observations, and following Robbins' arguments, Theorem 1 remains valid for all integers P and Q. Indeed, for p odd and $p|\Delta$, (1.6) becomes

$$U_{kp^n} \equiv 0 \pmod{p^n}. \tag{1.8}$$

The object of this paper is to generalize (1.5)-(1.8) to the sequence $W_n = W_n(a, b; \mathrm{P}, \mathrm{Q})$.

2. PRELIMINARY RESULTS

We now state some identities which are used subsequently.

$$V_n = U_{n+1} - \mathrm{Q}U_{n-1}, \tag{2.1}$$

$$2U_{n+1} = V_n + \mathrm{P}U_n, \tag{2.2}$$

$$-2\mathrm{Q}U_{n-1} = V_n - \mathrm{P}U_n, \tag{2.3}$$

$$W_n = W_0U_{n+1} + (W_1 - \mathrm{P}W_0)U_n, \tag{2.4}$$

$$W_n = -\mathrm{Q}W_0U_{n-1} + W_1U_n, \tag{2.5}$$

$$2W_n = W_0V_n + (2W_1 - \mathrm{P}W_0)U_n, \tag{2.6}$$

$$2W_{m+n} = W_mV_n + (2W_{m+1} - \mathrm{P}W_m)U_n, \tag{2.7}$$

$$W_mU_{n+1} - W_{m+1}U_n = \mathrm{Q}^nW_{m-n}, \tag{2.8}$$

$$\mathrm{Q}^nU_{-n} = -U_n, \tag{2.9}$$

$$\mathrm{Q}^nV_{-n} = V_n. \tag{2.10}$$

Identity (2.1) is easily proved using Binet forms and (2.2) and (2.3) can be obtained from (2.1) by simple substitution using (1.3). However, we state (2.2) and (2.3) for easy reference subsequently. Identity (2.4) is essentially (2.14) in [4] where the initial terms of $\{U_n\}$ are shifted. Identity (2.5) is obtained from (2.4) using (1.3) and (2.6) is obtained by adding (2.4) and (2.5).

Identity (2.7) is obtained from (2.6) by shifting the initial terms of $\{W_n\}$ to W_m, W_{m+1}. Finally, (2.8)-(2.10) are easily obtained using Binet forms.

3. A RESULT FOR ODD PRIMES

We now state and prove a result which generalizes (1.5) and (1.6) for odd primes p to the sequence $\{W_n\}$. Throughout, Δ is as in Theorem 1.

Theorem 2: Let p be an odd prime and k and m be nonnegative integers. Then

$$W_{m+kp^n} \equiv \begin{cases} W_{m+kp^{n-1}} & \pmod{p^n} \text{ if } \left(\frac{\Delta}{p}\right)=1, \\ Q^{kp^{n-1}} W_{m-kp^{n-1}} & \pmod{p^n} \text{ if } \left(\frac{\Delta}{p}\right)=-1. \end{cases} \tag{3.1}$$

Proof: Suppose $\left(\frac{\Delta}{p}\right) = 1$. Then in (2.7), if we replace n by kp^n and use (1.5) and (1.6), we obtain

$$2W_{m+kp^n} \equiv W_m V_{kp^{n-1}} + (2W_{m+1} - \mathrm{P}W_m)U_{kp^{n-1}} \pmod{p^n}. \tag{3.2}$$

Using (2.7) to substitute for the right side gives

$$2W_{m+kp^n} \equiv 2W_{m+kp^{n-1}} \pmod{p^n}, \tag{3.3}$$

and since 2 has a multiplicative inverse modulo p^n, the first half of Theorem 2 follows.

If $\left(\frac{\Delta}{p}\right) = -1$, then in (2.7) we replace n by kp^n and use (1.5) and (1.6) to obtain

$$2W_{m+kp^n} \equiv W_m V_{kp^{n-1}} - (2W_{m+1} - \mathrm{P}W_m)U_{kp^{n-1}} \pmod{p^n}, \tag{3.4}$$

and rearranging terms gives

$$2W_{m+kp^n} \equiv W_m(V_{kp^{n-1}} + \mathrm{P}U_{kp^{n-1}}) - 2W_{m+1}U_{kp^{n-1}} \pmod{p^n}. \tag{3.5}$$

Now (2.2) reduces (3.5) to

$$2W_{m+kp^n} \equiv 2W_m U_{kp^{n-1}+1} - 2W_{m+1}U_{kp^{n-1}} \pmod{p^n}, \tag{3.6}$$

and making use of (2.8) completes the proof. □

Using a similar argument, we see that if $p|\Delta$ then (1.8) generalizes to

$$W_{m+kp^n} \equiv ((p^n+1)/2)W_m V_{kp^{n-1}} \pmod{p^n}. \tag{3.7}$$

Remark 2: If we take the case $m=0$ and $\{W_n\} = \{U_n\}$, then (2.9) shows that Theorem 2 reduces to (1.6). If we take the case $m=0$ and $\{W_n\} = \{V_n\}$, then (2.10) shows that Theorem 2 reduces to (1.5). Thus, for p odd Theorem 2 both unifies and generalizes Robbins' results.

4. A RESULT FOR THE PRIME $p = 2$

We now prove the following theorem.

Theorem 3: If k and m are nonnegative integers and W_m is even, then

$$W_{m+k2^n} \equiv \begin{cases} W_{m+k2^{n-1}} & (\bmod 2^n) \text{ if Q is even,} \\ \mathrm{Q}^{k2^{n-1}} W_{m-k2^{n-1}} & (\bmod 2^n) \text{ if Q is odd.} \end{cases} \tag{4.1}$$

Proof: Putting $W_m = 2Q_m$, Q_m an integer, we use (2.7) to write

$$W_{m+n} = Q_m V_n + (W_{m+1} - \mathrm{P}Q_m)U_n. \tag{4.2}$$

Now with $k2^n$ in place of n, (1.5) and (1.7) imply

$$W_{m+k2^n} \equiv Q_m V_{k2^{n-1}} + (-1)^{\mathrm{Q}}(W_{m+1} - \mathrm{P}Q_m)U_{k2^{n-1}} \pmod{2^n}. \tag{4.3}$$

If Q is even, (4.3) becomes

$$W_{m+k2^n} \equiv Q_m V_{k2^{n-1}} + (W_{m+1} - \mathrm{P}Q_m)U_{k2^{n-1}} \pmod{2^n} \tag{4.4}$$

and the right side of (4.4) simplifies using (4.2) to prove the theorem for Q even.

If Q is odd, (4.3) becomes

$$W_{m+k2^n} \equiv Q_m V_{k2^{n-1}} - (W_{m+1} - \mathrm{P}Q_m)U_{k2^{n-1}} \pmod{2^n}, \tag{4.5}$$

and rearranging terms gives

$$W_{m+k2^n} \equiv Q_m(V_{k2^{n-1}} + \mathrm{P}U_{k2^{n-1}}) - W_{m+1}U_{k2^{n-1}} \pmod{2^n}. \tag{4.6}$$

Now using (2.2) and recalling that $W_m = 2Q_m$, (4.6) becomes

$$W_{m+k2^n} \equiv W_m U_{k2^{n-1}+1} - W_{m+1}U_{k2^{n-1}} \pmod{2^n}. \tag{4.7}$$

We now use (2.8) to simplify the right side of (4.7) and this completes the proof. □

Remark 3: If we take $\{W_n\} = \{U_n\}$ and $m = 0$, then $U_0 = 0$ is even and we see with the aid of (2.9) that Theorem 3 reduces to (1.7). If we take $\{W_n\} = \{V_n\}$ and $m = 0$, then $V_0 = 2$ is even and we see with the aid of (2.10) that Theorem 3 reduces to (1.5) for the case $p = 2$.

Remark 4: Bisht [2] proved that (1.5) carries over to higher-order analogues of $\{V_n\}$. However, we have seen no results similar to (1.6) and (1.7) for higher-order analogues of $\{U_n\}$.

ACKNOWLEDGMENT

We wish to record our gratitude to an anonymous referee whose suggestions have greatly improved this paper.

REFERENCES

1. G. E. Bergum & V. E. Hoggatt, Jr. "Sums and Products for Recurring Sequences." *The Fibonacci Quarterly* **13.2** (1975):115-20.
2. C. S. Bisht. "Some Congruence Properties of Generalized Lucas Integral Sequences." *The Fibonacci Quarterly* **22.3** (1984):290-95.
3. V. E. Hoggatt, Jr., & M. Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime *p*." *Mathematics Magazine* **47** (1974):210-14.
4. A. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *The Fibonacci Quarterly* **3.2** (1965):161-76.
5. A. F. Horadam. "Generating Functions for Powers of a Certain Generalized Sequence of Numbers." *Duke Mathematical Journal* **32** (1965):437-46.
6. D. Jarden. *Recurring Sequences.* Jerusalem: Riveon Lematematika, 1966.
7. E. Lucas. *Théorie des nombres.* Paris: Albert Blanchard, 1961.
8. N. Robbins. "Some Congruence Properties of Binomial Coefficients and Linear Second Order Recurrences." *International Journal of Mathematics and Mathematical Sciences* **11** (1988):743-50.
9. C. W. Wall. ."Some Congruences Involving Generalized Fibonacci Numbers." *The Fibonacci Quarterly* **17.1** (1979):29-33.

AMS Classification Numbers: 11B37, 11B39

Applications of Fibonacci Numbers

Volume 5

New Publication

Proceedings of 'The Fifth International Conference on Fibonacci Numbers and Their Applications, University of St. Andrews, Scotland, July 20-24, 1992'

Edited by **G.E. Bergum, A.N. Philippou** *and* **A.F. Horadam**

This volume contains a selection of papers presented at the Fifth International Conference on Fibonacci Numbers and Their Applications. The topics covered include number patterns, linear recurrences and the application of the Fibonacci Numbers to probability, statistics, differential equations, cryptography, computer science and elementary number theory. Many of the papers included contain suggestions for other avenues of research.

For those interested in applications of number theory, statistics and probability, and numerical analysis in science and engineering.

1993, 625 pp. ISBN 0-7923-2491-9
Hardbound Dfl. 320.00/£123.00/US $180.00

A.M.S. members are eligible for a 25% discount on this volume providing they order directly from the publisher. However, the bill must be prepaid by credit card, registered money order or check. A letter must also be enclosed saying "I am a member of the American Mathematical Society and am ordering the book for personal use."

KLUWER ACADEMIC PUBLISHERS

P.O. Box 322, 3300 AH Dordrecht
The Netherlands

P.O. Box 358, Accord Station
Hingham, MA 02018-0358, U.S.A.

Volumes 1-4 can also be purchased by writing to the same address.