SOME CONGRUENCE PROPERTIES OF GENERALIZED LUCAS INTEGRAL SEQUENCES

C. S. BISHT
D.S.B.C. College, K.U. Naini Tal, 263002, India
(Submitted December 1982)

1. INTRODUCTION

Let $\{L_n\}$ be a sequence on integers defined as

$$L_0 = 2,\ L_1 = 1, \text{ and } L_n = L_{n-1} + L_{n-2}, \text{ for } n \geqslant 2.$$

This is the famous Lucas sequence. In [1], Hoggatt and Bicknell proved that $L_p \equiv L_1 \pmod{p}$ if p is a prime, together with its generalization $L_{kp} \equiv L_k \pmod{p}$. It is interesting to note that these properties are not lost in generalization of the sequence. The purpose of this paper is to prove these results for generalized Lucas integral sequences defined in §2 below. One more generalization of $L_p \equiv L_1 \pmod{p}$ has also been proved. In light of these results, the sequences given in [2] have been discussed.

2. DEFINITIONS

A generalized Lucas integral sequence of order m is defined as

$$L_n = \alpha_1^n + \alpha_2^n + \cdots + \alpha_m^n, \tag{2.1}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_m$ are the roots of the equation

$$x^m = a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m \tag{2.2}$$

with integral coefficients and $a_m \neq 0$.

These L_n's are easily obtained in terms of the a_i's by Newton's well-known formula:

$$L_0 = m,\ L_n = a_1 L_{n-1} + a_2 L_{n-2} + \cdots + a_{n-1} L_1 + n a_n, \text{ if } n = 1, 2, \ldots, m-1,$$
$$L_n = a_1 L_{n-1} + a_2 L_{n-2} + \cdots + a_m L_{n-m}, \text{ for } n \geqslant m. \tag{2.3}$$

Equation (2.2) is called the characteristic equation of (2.3).

3. MAIN RESULTS

First, we shall prove a lemma for each theorem. The monomial symmetric functions

$$\sum \alpha_1^{t_1} \alpha_2^{t_2} \cdots \alpha_n^{t_n},$$

where $t_1, t_2, \ldots, t_n$ are integers as defined in [3]. Equation (3.1), used in the proofs of the lemmas, is given in [3].

Lemma 3.1

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of (2.2). Then $\sum \alpha_1^{t_1} \alpha_2^{t_2} \cdots \alpha_n^{t_n}$, with different indices for α's, is an integer.

Proof: We prove the lemma by mathematical induction on n. Since

$$\sum \alpha_1^{t_1} = \alpha_1^{t_1} + \alpha_2^{t_1} + \cdots + \alpha_m^{t_1} = L_{t_1},$$

an integer, therefore, the lemma is true for $n = 1$. Suppose the lemma is true for $n = s - 1$. As all the indices for α's are different, we have:

$$\begin{aligned}\Big(\sum \alpha_1^{t_1}\Big)\Big(\sum \alpha_1^{t_2}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s}\Big) &= \sum \alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_s^{t_s} + \sum \alpha_1^{t_2+t_1}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s} \\ &\quad + \sum \alpha_1^{t_2}\alpha_2^{t_3+t_1} \cdots \alpha_{s-1}^{t_s} + \cdots + \sum \alpha_1^{t_2}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s+t_1}\end{aligned} \tag{3.1}$$

Using the induction hypothesis and the fact that $\sum \alpha_1^{t_1}$ is an integer, we find that

$$\sum \alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_s^{t_s}$$

is an integer; i.e., the lemma is true for $n = s$. So, by induction, the lemma is completely proved.

Theorem 3.1

Let $\{L_n\}$ be a generalized Lucas integral sequence and p be a prime number. Then

$$L_p \equiv L_1 \pmod{p}.$$

Proof: By using the multinomial theorem, we have

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_m)^p = \sum \frac{p!}{t_1!t_2! \cdots t_m!}\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_m^{t_m}, \tag{3.2}$$

where $t_1, t_2, \ldots, t_m$ are nonnegative integers such that $t_1 + t_2 + \cdots + t_m = p$ and all indices of α's are different.

From (3.2), we have

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_m)^p = \alpha_1^p + \alpha_2^p + \cdots + \alpha_m^p + \sum \frac{p!}{t_1! \cdots t_m!}\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_m^{t_m}, \tag{3.3}$$

with the above conditions on t_i's and no $t_i = p$. With these conditions on the t_i's, we have that

$$\frac{p!}{t_1! \cdots t_m!}$$

is an integral multiple of p. Since for each set of possible values of $t_1, t_2, \ldots, t_m$ all $\sum \alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_m^{t_m}$'s are integers, by our Lemma 3.1 we have, from (3.3) and (2.1),

$$(L_1)^p = L_p + p\lambda, \text{ where } \lambda \text{ is an integer.}$$

Using Fermat's little theorem, we get

$$L_p \equiv L_1 \pmod{p}.$$

This completes the proof of Theorem 3.1.

Lemma 3.2

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of (2.2). Then, for different indices of α's, $\sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_n^{t_n})^k$ is an integer for every positive integer k.

Proof: Simply write kt_i for t_i everywhere in the proof of Lemma 3.1.

Theorem 3.2

Let $\{L_n\}$ be a generalized Lucas integral sequence and p be a prime number. Then, for every positive integer k,

$$L_{pk} \equiv L_k \pmod{p}.$$

Proof: $(\alpha_1^k + \alpha_2^k + \cdots + \alpha_m^k)^p$

$$= \alpha_1^{pk} + \alpha_2^{pk} + \cdots + \alpha_m^{pk} + \sum \frac{p!}{t_1!t_2! \ldots t_m!}(\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_m^{t_m})^k.$$

$\frac{p!}{t_1! \ldots t_m!}$ is a multiple of p and $\sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_m^{t_m})$ is an integer for every given set of values of $t_1, \ldots, t_m$ by Lemma 3.2. Therefore,

$$(L_k)^p = L_{pk} + p\lambda_1, \text{ where } \lambda_1 \text{ is an integer}$$

or $L_{pk} \equiv L_k \pmod{p}$, by Fermat's little theorem,

$$L_k^p \equiv L_k \pmod{p}.$$

Lemma 3.3

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of (2.2). Then, for different indices of α's,

$$\sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_n^{t_n})^{kp^r} \equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_n^{t_n})^{kp^{r-1}} \pmod{p^r}.$$

Proof: We shall prove the lemma by induction on r. In order to prove the lemma for $r = 1$, we have to prove

$$\sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_n^{t_n})^{kp} \equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_n^{t_n})^k \pmod{p}. \tag{3.4}$$

The congruence (3.4) may be proved by induction on n. Since

$$\sum (\alpha_1^{t_1})^{kp} - \sum (\alpha_1^{t_1})^k = L_{t_1kp} - L_{t_1k}$$

$$\equiv 0 \pmod{p} \quad \text{(by Theorem 3.2)},$$

or

$$\sum (\alpha_1^{t_1})^{kp} \equiv \sum (\alpha_1^{t_1})^k \pmod{p}. \tag{3.5}$$

Therefore, (3.4) is true for $n = 1$. Consider the equation

$$\Big(\sum \alpha_1^{t_1kp}\Big)\Big(\sum (\alpha_1^{t_2}\alpha_2^{t_3} \ldots \alpha_{s-1}^{t_s})^{kp}\Big)$$

$$= \sum (\alpha_1^{t_1}\alpha_2^{t_2} \ldots \alpha_s^{t_s})^{kp} + \sum (\alpha_1^{t_2+t_1}\alpha_2^{t_3} \ldots \alpha_{s-1}^{t_s})^{kp}$$

$$+ \sum (\alpha_1^{t_2}\alpha_2^{t_3+t_1} \ldots \alpha_{s-1}^{t_s})^{kp} + \cdots + \sum (\alpha_1^{t_2}\alpha_2^{t_3} \ldots \alpha_{s-1}^{t_s+t_1})^{kp}.$$

Using the induction hypothesis and (3.5), we have

$$\Big(\sum \alpha_1^{t_1 k}\Big)\Big(\sum (\alpha_1^{t_2}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s})^k\Big)$$

$$\equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_s^{t_s})^{kp} + \sum (\alpha_1^{(t_2+t_1)}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s})^k$$

$$+ \sum (\alpha_1^{t_2}\alpha_2^{t_3+t_1} \cdots \alpha_{s-1}^{t_s})^k + \cdots + \sum (\alpha_1^{t_2}\alpha_2^{t_3} \cdots \alpha_{s-1}^{t_s+t_1})^k \pmod p$$

or

$$\sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_s^{t_s})^{kp} \equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_s^{t_s})^k \pmod p.$$

This proves that (3.4) is true for $n = s$. Thus, induction completes the proof of (3.4).

Next, we suppose that our lemma is true for $r = s$. That is,

$$\sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_n^{t_n})^{kp^s} \equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_n^{t_n})^{kp^{s-1}} \pmod{p^s}$$

or

$$\lambda_1^{kp^s} + \cdots + \lambda_q^{kp^s} \equiv \lambda_1^{kp^{s-1}} + \cdots + \lambda_q^{kp^{s-1}} \pmod{p^s},$$

where q is the number of terms in the expansion of

$$\sum \alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_n^{t_n}$$

and each λ is the product of powers of the α's. Therefore,

$$(\lambda_1^{kp^s} + \cdots + \lambda_q^{kp^s})^p \equiv (\lambda_1^{kp^{s-1}} + \cdots + \lambda_q^{kp^{s-1}})^p \pmod{p^{s+1}}$$

or

$$\lambda_1^{kp^{s+1}} + \cdots + \lambda_q^{kp^{s+1}} + \sum \frac{p!}{\mu_1! \cdots \mu_q!}(\lambda_1^{\mu_1}\lambda_2^{\mu_2} \cdots \lambda_q^{\mu_q})^{kp^s}$$

$$\equiv \lambda_1^{kp^s} + \cdots + \lambda_q^{kp^s} + \sum \frac{p!}{\mu_1! \cdots \mu_q!}(\lambda_1^{\mu_1}\lambda_2^{\mu_2} \cdots \lambda_q^{\mu_q})^{kp^{s-1}}.$$

Since $\dfrac{p!}{\mu_1! \cdots \mu_q!}$ is a multiple of p and

$$\sum (\lambda_1^{\mu_1}\lambda_2^{\mu_2} \cdots \lambda_q^{\mu_q})^{kp^s} \equiv \sum (\lambda_1^{\mu_1}\lambda_2^{\mu_2} \cdots \lambda_q^{\mu_q})^{kp^{s-1}} \pmod{p^s}$$

by the induction hypothesis, we have

$$\lambda_1^{kp^{s+1}} + \cdots + \lambda_q^{kp^{s+1}} \equiv \lambda_1^{kp^s} + \cdots + \lambda_q^{kp^s} \pmod{p^{s+1}}$$

or

$$\sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_n^{t_n})^{kp^{s+1}} \equiv \sum (\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_n^{t_n})^{kp^s} \pmod{p^{s+1}},$$

which shows that the lemma is true for $r = s + 1$. Thus, the lemma is proved completely by induction.

Theorem 3.3

Let $\{L_n\}$ be a generalized Lucas integral sequence and p be a prime number. Then, for positive integers k and r,

$$L_{kp^r} \equiv L_{kp^{r-1}} \pmod{p^r}.$$

Proof: The proof will be given by induction on r. By Theorem 3.2,

$$L_{kp} \equiv L_k \pmod{p}.$$

This proves the theorem for $r = 1$.

Suppose that the theorem is true for $r = s - 1$, i.e.,

$$L_{kp^{s-1}} \equiv L_{kp^{s-2}} \pmod{p^{s-1}},$$

which implies

$$L^p_{kp^{s-1}} \equiv L^p_{kp^{s-2}} \pmod{p^s}. \tag{3.6}$$

Now,

$$(\alpha_1^{kp^{s-1}} + \cdots + \alpha_m^{kp^{s-1}})^p = \alpha_1^{kp^s} + \cdots + \alpha_m^{kp^s} + \sum \frac{p!}{t_1! \cdots t_m!}(\alpha_1^{t_1} \cdots \alpha_m^{t_m})^{kp^{s-1}}$$

or

$$L^p_{kp^{s-1}} = L_{kp^s} + \sum \frac{p!}{t_1! \cdots t_m!}(\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_m^{t_m})^{kp^{s-1}}.$$

Similarly,

$$L^p_{kp^{s-2}} = L_{kp^{s-1}} + \sum \frac{p!}{t_1! \cdots t_m!}(\alpha_1^{t_1}\alpha_2^{t_2} \cdots \alpha_m^{t_m})^{kp^{s-2}}.$$

On subtracting, we get

$$L^p_{kp^{s-1}} - L^p_{kp^{s-2}}$$

$$= L_{kp^s} - L_{kp^{s-1}} + \sum \frac{p!}{t_1! \cdots t_m!}[(\alpha_1^{t_1} \cdots \alpha_m^{t_m})^{kp^{s-1}} - (\alpha_1^{t_1} \cdots \alpha_m^{t_m})^{kp^{s-2}}].$$

Using (3.6), $\frac{p!}{t_1! \cdots t_m!}$ is a multiple of p, and Lemma 3.3, we have

$$L_{kp^s} \equiv L_{kp^{s-1}} \pmod{p^s},$$

which shows that the theorem is true for $r = s$. Therefore, the theorem is completely proved by induction.

Note: Theorem 3.3 is a generalization of our previous theorems. The beauty of this theorem is that multiplying the index of each term of the difference

$$L_{kp^r} - L_{kp^{r-1}}$$

by p produces one more factor p to the new difference. It is observed that

$$L_{kp^s} \not\equiv L_{kp^{s-1}} \pmod{p^{s+1}}$$

in most of the cases. In some cases, there exist primes where this incongruence relation fails. For example, we take the sequence

$$L_0 = 3,\ L_1 = 1,\ L_2 = 5, \text{ and } L_n = L_{n-1} + 2L_{n-2} + L_{n-3}, \text{ for } n \geq 3.$$

Writing a few initial terms of the sequence,

$$3, 1, 5, 10, 21, 46, \ldots,$$

we find that there exist primes 2 and 3 such that

$$L_2 \equiv L_1 \pmod{4} \quad \text{and} \quad L_3 \equiv L_1 \pmod{9}.$$

4. SEQUENCES WHERE $p \mid L_p$ FOR EVERY PRIME p

Sequences of this type have been considered in [2]. First, let us prove the following simple theorem.

Theorem 4.1

Let $\{L_n\}$ be a generalized Lucas integral sequence. Then, for every prime p, $p|L_p \iff L_1 = 0$.

Proof: Suppose $L_1 = 0$. Therefore, by Theorem 3.1,

$$L_p \equiv 0 \pmod{p}, \text{ i.e., } p|L_p \text{ for every prime } p.$$

Conversely, suppose $p|L_p$ for every prime p. We find, again from Theorem 3.1,

$$L_1 \equiv 0 \pmod{p} \text{ for every prime } p.$$

This implies that $L_1 = 0$. Hence, the theorem is proved.

Note: In light of this theorem, we conclude that for making such sequences we need $L_1 = 0$. Ensuring the right start as pointed out in [2] is not needed. As a matter of fact, this right start is a consequence of $L_1 = 0$. Moreover, it will be an appropriate place to point out a shortcoming in Lehmer's proof presented in [2]. He first takes integers x, y, z, and t, and then allows $x = \alpha$, $y = \beta$, $z = \gamma$, and $t = \delta$, which are not integers because α, β, γ, and δ are the roots of the characteristic equation $x^4 = 2x^2 + 2x + 1$. Consequently, one cannot argue that $F_p(x, y, z, t)$ is an integer implies $F_p(\alpha, \beta, \gamma, \delta)$ is also an integer. In fact, $F_p(\alpha, \beta, \gamma, \delta)$ is an integer, as we see in our Theorem 3.1, with the help of Lemma 3.1.

REFERENCES

1. V. E. Hoggatt, Jr., and Marjorie Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime p." *Math. Mag.* 47 (1974):210-14.
2. B. H. Neuman & L. G. Wilson. "Some Sequences Like Fibonacci's." *The Fibonacci Quarterly* 17, no. 1 (1979):80-83.
3. D. E. Littlewood. *A University Algebra.* London: William Heinemann, Ltd., 1958, p. 86.

◆◇◆◇◆