Lucas $(a_1, a_2, \ldots, a_k = 1)$ Sequences and Pseudoprimes

Curtis Cooper
University of Central Missouri
Lawrence Somer
The Catholic University of America

July 10, 2008

Outline

Definition - Generalized Lucas Integral Sequence of Order $k \geq 1$ - Bisht (1984)

Let n be a nonnegative integer and

$$G_n = x_1^n + x_2^n + \cdots + x_k^n,$$

where x_1, x_2, ..., x_k are the roots of the equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k$$

with integral coefficients and $a_k \neq 0$.

The generalized Lucas integral sequence of order 2 with equation $x^2 = x + 1$ is the Lucas sequence.

The generalized Lucas integral sequence of order 2 with equation $x^2 = x + 1$ is the Lucas sequence.

Perrin's sequence is the generalized Lucas integral sequence of order 3 with $a_1 = 0$, $a_2 = 1$, and $a_3 = 1$. Perrin's sequence (Sloane - A001608) is defined as $G_0 = 3$, $G_1 = 0$, $G_2 = 2$, and

$$G_n = G_{n-2} + G_{n-3} \text{ for } n \geq 3.$$

G_n's in terms of the a_i's (Newton's Formulas) - Bisht (1984)

$$\begin{aligned} G_0 &= k, & \\ G_n &= \sum_{j=1}^{n-1} a_j G_{n-j} + n a_n, & \text{if } n = 1, 2, \ldots, k-1, \\ G_n &= \sum_{j=1}^{k} a_j G_{n-j}, & \text{if } n \geq k. \end{aligned}$$

Using the Girard-Waring formula we have the following closed form.

Using the Girard-Waring formula we have the following closed form.

Closed Form

Let $\{G_n\}$ be a generalized Lucas integral sequence and n be a positive integer. Then

$$G_n = n \cdot \sum_{\substack{i_1+2i_2+\cdots+ki_k=n \\ i_1,i_2,\ldots,i_k\geq 0}} \frac{(i_1+i_2+\cdots+i_k-1)!}{i_1!i_2!\cdots i_k!} a_1^{i_1} a_2^{i_2} \cdots a_k^{i_k}.$$

Outline

Theorem 1 - Bisht

Let $\{G_n\}$ be a generalized Lucas integral sequence of order $k \geq 1$ and p be a prime number. Then

$$G_p \equiv G_1 \pmod{p}.$$

Theorem 1 - Bisht

Let $\{G_n\}$ be a generalized Lucas integral sequence of order $k \geq 1$ and p be a prime number. Then

$$G_p \equiv G_1 \pmod{p}.$$

Theorem 2 - Bisht

Let $\{G_n\}$ be a generalized Lucas integral sequence of order $k \geq 1$ and p be a prime number. Then, for positive integers m and r,

$$G_{mp^r} \equiv G_{mp^{r-1}} \pmod{p^r}.$$

Hoggatt and Bicknell (1974) proved that if p is prime, then $L_p \equiv L_1 \pmod{p}$.

Hoggatt and Bicknell (1974) proved that if p is prime, then $L_p \equiv L_1 \pmod{p}$.

Lucas (1878) studied Perrin's sequence and proved that if p is prime, then $G_p \equiv G_1 \pmod{p}$.

Outline

During their study of Perrin's sequence, Adams and Shanks (1982) extended Perrin's sequence to negative indices and proved that $G_{-p} \equiv G_{-1} \pmod{p}$ when p is prime.

During their study of Perrin's sequence, Adams and Shanks (1982) extended Perrin's sequence to negative indices and proved that $G_{-p} \equiv G_{-1} \pmod{p}$ when p is prime.

We wish to extend the definition of a generalized Lucas integral sequence of order $k \geq 1$ to negative indices so that

$$G_n = x_1^n + x_2^n + \cdots + x_k^n$$

is true for negative integers n.

During their study of Perrin's sequence, Adams and Shanks (1982) extended Perrin's sequence to negative indices and proved that $G_{-p} \equiv G_{-1} \pmod{p}$ when p is prime.

We wish to extend the definition of a generalized Lucas integral sequence of order $k \geq 1$ to negative indices so that

$$G_n = x_1^n + x_2^n + \cdots + x_k^n$$

is true for negative integers n.

In the meantime, we want these G_n's to be integers. One way to do this is to let $a_k = 1$.

Therefore, we define G for negative indices as follows:

$$\begin{array}{lcll} G_0 & = & k, & \\ G_{-n} & = & -\sum_{j=1}^{n-1} a_{k-j} G_{-n+j} - n a_{k-n}, & \text{if } n = 1, 2, \ldots, k-1, \\ G_{-n} & = & -\sum_{j=1}^{k-1} a_{k-j} G_{-n+j} + G_{-n+k}, & \text{if } n \geq k. \end{array}$$

Therefore, we define G for negative indices as follows:

$$
\begin{aligned}
G_0 &= k, \\
G_{-n} &= -\sum_{j=1}^{n-1} a_{k-j} G_{-n+j} - n a_{k-n}, \quad \text{if } n = 1, 2, \ldots, k-1, \\
G_{-n} &= -\sum_{j=1}^{k-1} a_{k-j} G_{-n+j} + G_{-n+k}, \quad \text{if } n \geq k.
\end{aligned}
$$

We call these generalized Lucas integral sequences of order $k \geq 1$ with $a_k = 1$ that are defined for negative indices Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequences.

Outline

Lucas $(1, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	2	1	3	4	7	11	18	29	47	76	123	199
G_{-n}	2	-1	3	-4	7	-11	18	-29	47	-76	123	-199

Lucas $(1, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	2	1	3	4	7	11	18	29	47	76	123	199
G_{-n}	2	-1	3	-4	7	-11	18	-29	47	-76	123	-199

This is the Lucas sequence.

Lucas $(2, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9
G_n	2	2	6	14	34	82	198	478	1154	2786
G_{-n}	2	-2	6	-14	34	-82	198	-478	1154	-2786

Lucas $(2, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9
G_n	2	2	6	14	34	82	198	478	1154	2786
G_{-n}	2	-2	6	-14	34	-82	198	-478	1154	-2786

This is the Pell-Lucas sequence.

Lucas $(0,1,1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
G_n	3	0	2	3	2	5	5	7	10	12	17	22	29	39
G_{-n}	3	-1	1	2	-3	4	-2	-1	5	-7	6	-1	-6	12

Lucas $(0, 1, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
G_n	3	0	2	3	2	5	5	7	10	12	17	22	29	39
G_{-n}	3	-1	1	2	-3	4	-2	-1	5	-7	6	-1	-6	12

This is Perrin's sequence.

Lucas $(0, 2, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	3	0	4	3	8	10	19	28	48	75	124	198
G_{-n}	3	-2	4	-5	8	-12	19	-30	48	-77	124	-200

Lucas $(0, 2, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	3	0	4	3	8	10	19	28	48	75	124	198
G_{-n}	3	-2	4	-5	8	-12	19	-30	48	-77	124	-200

Lucas $(1, 0, 1, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	4	1	1	4	9	11	16	29	49	76	121	199
G_{-n}	4	-1	1	-4	9	-11	16	-29	49	-76	121	-199

Lucas $(0, 2, 0, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11	12
G_n	4	0	4	0	12	0	28	0	68	0	164	0	396
G_{-n}	4	0	-4	0	12	0	-28	0	68	0	-164	0	396

Lucas $(0, 2, 0, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11	12
G_n	4	0	4	0	12	0	28	0	68	0	164	0	396
G_{-n}	4	0	-4	0	12	0	-28	0	68	0	-164	0	396

Lucas $(0, 4, 0, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9	10	11
G_n	4	0	8	0	36	0	152	0	644	0	2728	0
G_{-n}	4	0	-8	0	36	0	-152	0	644	0	-2728	0

Lucas $(1, 3, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9
G_n	3	1	7	13	35	81	199	477	1155	2785
G_{-n}	3	-3	7	-15	35	-83	199	-479	1155	-2787

Lucas $(1, 3, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9
G_n	3	1	7	13	35	81	199	477	1155	2785
G_{-n}	3	-3	7	-15	35	-83	199	-479	1155	-2787

Lucas $(2, 0, 2, 1)$ Sequence

n	0	1	2	3	4	5	6	7	8	9
G_n	4	2	4	14	36	82	196	478	1156	2786
G_{-n}	4	-2	4	-14	36	-82	196	-478	1156	-2786

Outline

Theorem 3

Let $\{G_n\}$ be a Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence. Then

$$G_{-p} \equiv G_{-1} \pmod{p}$$

when p is prime and for positive integers m and r and for p a prime

$$G_{-mp^r} \equiv G_{-mp^{r-1}} \pmod{p^r}.$$

Outline

Definition

Let $\{G_n\}$ be a Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence. A composite n such that

$$G_n \equiv G_1 \pmod{n}$$

and

$$G_{-n} \equiv G_{-1} \pmod{n}$$

is called a Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprime.

k	$(a_1, a_2, \ldots, a_k = 1)$	pseudoprimes $\leq N$
2	$(1, 1)$	$705, 2465, 2737, 3745, 4181, 5777 \leq 6000$
2	$(2, 1)$	$4, 169, 385, 961, 1105, 1121, 3827 \leq 4000$
3	$(1, 0, 1)$	≤ 1000000
3	$(0, 1, 1)$	≤ 1000000
3	$(2, 0, 1)$	≤ 1000000
3	$(1, 1, 1)$	≤ 1000000
3	$(0, 2, 1)$	$705, 2465, 2737, 3745, 4181, 5777 \leq 6000$
3	$(3, 0, 1)$	≤ 100000
3	$(2, 1, 1)$	≤ 100000
3	$(1, 2, 1)$	$4 \leq 100000$
3	$(0, 3, 1)$	≤ 100000
3	$(4, 0, 1)$	$4 \leq 100000$

k	$(a_1, a_2, \ldots, a_k = 1)$	pseudoprimes $\leq N$
3	$(3, 1, 1)$	$4, 66, 33153, 79003 \leq 100000$
3	$(2, 2, 1)$	$79003 \leq 100000$
3	$(1, 3, 1)$	$169, 385, 961, 1105, 1121, 3827 \leq 4000$
3	$(0, 4, 1)$	$4 \leq 100000$
4	$(1, 0, 0, 1)$	$4, 34, 38, 46, 62, 94, 106, 122, 158 \leq 160$
4	$(0, 1, 0, 1)$	$9, 12, 15, 21, 25, 27, 33, 35, 36, 39 \leq 40$
4	$(0, 0, 1, 1)$	≤ 100000
4	$(2, 0, 0, 1)$	≤ 100000
4	$(0, 2, 0, 1)$	$4, 9, 12, 15, 21, 25, 27, 33, 35, 36 \leq 38$
4	$(0, 0, 2, 1)$	$6 \leq 100000$
4	$(1, 1, 0, 1)$	≤ 100000
4	$(1, 0, 1, 1)$	$705, 2465, 2737, 3745, 4181, 5777 \leq 6000$

k	$(a_1, a_2, \dots, a_k)$	pseudoprimes $\leq N$
4	$(0, 1, 1, 1)$	≤ 100000
4	$(3, 0, 0, 1)$	≤ 100000
4	$(0, 3, 0, 1)$	$6, 9, 15, 18, 21, 25, 27, 33, 35, 39, 45 \leq 48$
4	$(0, 0, 3, 1)$	$4 \leq 100000$
4	$(2, 1, 0, 1)$	≤ 100000
4	$(2, 0, 1, 1)$	≤ 100000
4	$(1, 2, 0, 1)$	$4 \leq 100000$
4	$(1, 0, 2, 1)$	≤ 100000
4	$(0, 1, 2, 1)$	$2465, 2737, 3745, 4181, 5777, 6721 \leq 10000$
4	$(0, 2, 1, 1)$	≤ 100000
4	$(1, 1, 1, 1)$	$49 \leq 100000$
4	$(4, 0, 0, 1)$	$4, 6 \leq 100000$

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
4	$(0, 4, 0, 1)$	$4, 9, 12, 15, 21, 25, 27, 33, 35, 36, 39 \leq 40$
4	$(0, 0, 4, 1)$	$4, 10, \leq 100000$
4	$(3, 1, 0, 1)$	≤ 100000
4	$(3, 0, 1, 1)$	$9 \leq 100000$
4	$(1, 3, 0, 1)$	≤ 100000
4	$(1, 0, 3, 1)$	$4, 9 \leq 100000$
4	$(0, 3, 1, 1)$	≤ 100000
4	$(0, 1, 3, 1)$	≤ 100000
4	$(2, 2, 0, 1)$	≤ 100000
4	$(2, 0, 2, 1)$	$169, 385, 961, 1105, 1121, 3827, 4901 \leq 4000$
4	$(0, 2, 2, 1)$	≤ 100000
4	$(2, 1, 1, 1)$	$4 \leq 100000$
4	$(1, 2, 1, 1)$	≤ 100000
4	$(1, 1, 2, 1)$	≤ 100000

Outline

Question 1

Is the set of Lucas $(0, 2, 1)$ pseudoprimes equal to the set of Lucas $(1, 0, 1, 1)$ pseudoprimes?

Question 1

Is the set of Lucas $(0, 2, 1)$ pseudoprimes equal to the set of Lucas $(1, 0, 1, 1)$ pseudoprimes?

The key to looking at this question is the characteristic polynomials of these sequences.

Characteristic Polynomials

Lucas $(1,1)$ sequence: $x^2 - x - 1$.

Characteristic Polynomials

Lucas $(1, 1)$ sequence: $x^2 - x - 1$.
Lucas $(0, 2, 1)$ sequence: $x^3 - 2x - 1 = (x^2 - x - 1)(x + 1)$.

Characteristic Polynomials

Lucas $(1, 1)$ sequence: $x^2 - x - 1$.
Lucas $(0, 2, 1)$ sequence: $x^3 - 2x - 1 = (x^2 - x - 1)(x + 1)$.
Lucas $(1, 0, 1, 1)$ sequence:
$x^4 - x^3 - x - 1 = (x^2 - x - 1)(x^2 + 1)$.

Characteristic Polynomials

Lucas $(1, 1)$ sequence: $x^2 - x - 1$.
Lucas $(0, 2, 1)$ sequence: $x^3 - 2x - 1 = (x^2 - x - 1)(x + 1)$.
Lucas $(1, 0, 1, 1)$ sequence:
$x^4 - x^3 - x - 1 = (x^2 - x - 1)(x^2 + 1)$.
Lucas $(0, 1, 2, 1)$ sequence:
$x^4 - x^2 - 2x - 1 = (x^2 - x - 1)(x^2 + x + 1)$.

Characteristic Polynomials

Lucas $(1, 1)$ sequence: $x^2 - x - 1$.
Lucas $(0, 2, 1)$ sequence: $x^3 - 2x - 1 = (x^2 - x - 1)(x + 1)$.
Lucas $(1, 0, 1, 1)$ sequence:
$x^4 - x^3 - x - 1 = (x^2 - x - 1)(x^2 + 1)$.
Lucas $(0, 1, 2, 1)$ sequence:
$x^4 - x^2 - 2x - 1 = (x^2 - x - 1)(x^2 + x + 1)$.

Observe that in each case, the characteristic polynomial of the Lucas $(0, 2, 1)$, $(1, 0, 1, 1)$, or $(0, 1, 2, 1)$ sequence is equal to the characteristic polynomial of the Lucas $(1, 1)$ sequence multiplied by a cyclotomic polynomial.

Theorem 5

Suppose that the characteristic polynomial of a Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence is equal to the characteristic polynomial of a Lucas $(b_1, b_2, \ldots, b_r = 1)$ sequence multiplied by j polynomials, each of which is a cyclotomic polynomial of order m_1, m_2, ..., m_j, respectively. Assume that the characteristic polynomial of the Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence has no repeated roots. Let $m = lcm(m_1, m_2, \ldots, m_j)$. Then each Lucas $(b_1, b_2, \ldots, b_r = 1)$ pseudoprime which is relatively prime to m is a Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprime.

Theorem 5

Suppose that the characteristic polynomial of a Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence is equal to the characteristic polynomial of a Lucas $(b_1, b_2, \ldots, b_r = 1)$ sequence multiplied by j polynomials, each of which is a cyclotomic polynomial of order m_1, m_2, ..., m_j, respectively. Assume that the characteristic polynomial of the Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence has no repeated roots. Let $m = lcm(m_1, m_2, \ldots, m_j)$. Then each Lucas $(b_1, b_2, \ldots, b_r = 1)$ pseudoprime which is relatively prime to m is a Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprime.

Since there are no even Lucas $(1, 1)$ pseudoprimes and since $x + 1$ and $x^2 + 1$ are cyclotomic polynomials of orders 2 and 4, respectively, all Lucas $(1, 1)$ pseudoprimes are both Lucas $(0, 2, 1)$ pseudoprimes and Lucas $(1, 0, 1, 1)$ pseudoprimes.

Question 2

Is the set of Lucas $(0, 2, 0, 1)$ pseudoprimes equal to the set of Lucas $(0, 4, 0, 1)$ sequences?

Question 2

Is the set of Lucas $(0, 2, 0, 1)$ pseudoprimes equal to the set of Lucas $(0, 4, 0, 1)$ sequences?

Theorem 6

The Lucas $(0, a_2, 0, 1)$ pseudoprimes are precisely the odd composite natural numbers and the even integers $2m \geq 4$ for which $m | G_m(a_2, 1)$.

Question 2

Is the set of Lucas $(0, 2, 0, 1)$ pseudoprimes equal to the set of Lucas $(0, 4, 0, 1)$ sequences?

Theorem 6

The Lucas $(0, a_2, 0, 1)$ pseudoprimes are precisely the odd composite natural numbers and the even integers $2m \geq 4$ for which $m | G_m(a_2, 1)$.

Lawrence Somer gives comprehensive criteria for determining when $n | G_n(a_1, 1)$, which relates to Theorem 6.

The answer to Question 2 is no.

The answer to Question 2 is no.

The first composite even integers which are Lucas $(0, 2, 0, 1)$ pseudoprimes and not Lucas $(0, 4, 0, 1)$ pseudoprimes are 132, 396, and 1188.

The answer to Question 2 is no.

The first composite even integers which are Lucas $(0, 2, 0, 1)$ pseudoprimes and not Lucas $(0, 4, 0, 1)$ pseudoprimes are 132, 396, and 1188.

The first composite even integer which is a Lucas $(0, 4, 0, 1)$ pseudoprime and not a Lucas $(0, 2, 0, 1)$ pseudoprime is 1284.

Question 3

For every $k \geq 2$, is there a k-tuple $(a_1, a_2, \ldots, a_k = 1)$ such that there are an infinite number of Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprimes?

Question 3

For every $k \geq 2$, is there a k-tuple $(a_1, a_2, \ldots, a_k = 1)$ such that there are an infinite number of Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprimes?

The answer is yes.

Question 4

Is there a Lucas $(0, 1, 1)$ pseudoprime?

Question 4

Is there a Lucas $(0, 1, 1)$ pseudoprime?

The answer to this question is unknown. Composite n up to 10^7 have been checked and so far, no Lucas $(0, 1, 1)$ pseudoprimes have been found. If such an example exists, we suspect it will be very large.

References

1. W. W. Adams and D. Shanks, "Strong primality tests that are not sufficient," *Math. Comp.*, 39 (1982), 255–300.
2. R. André-Jeannin, "On the Existence of Even Fibonacci Pseudoprimes with Parameters *P* and *Q*," *The Fibonacci Quarterly*, 34 (1996), 75–78.
3. C. S. Bisht, "Some Congruence Properties of Generalized Lucas Integral Sequences," *The Fibonacci Quarterly*, 22 (1984), 290–295.
4. P. S. Bruckman, "Lucas Pseudoprimes are Odd," *The Fibonacci Quarterly*, 32 (1994), 155–157.
5. A. Di Porto, "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind," *The Fibonacci Quarterly*, 31 (1993), 173–177.

References

6. H. W. Gould, “The Girard-Waring Power Sum Formulas for Symmmetric Functions and Fibonacci Sequences,” *The Fibonacci Quarterly*, 37 (1999), 135–140.
7. V. E. Hoggatt, Jr. and Marjorie Bicknell, “Some Congruences of the Fibonacci Numbers Modulo a Prime *p*,” *Mathematics Magazine*, 47 (1974), 210–214.
8. D. E. Littlewood, *A University Algebra*, William Heinemann, Ltd., London, 1958, p. 86.
9. E. Lucas, “Théorie des fonctions numériques simplement périodiques,” *Amer. J. of Math.*, 1 (1878), 197–240.
10. R. Perrin, “Query 1484,” *L'Intermédiaire des Mathématiciens*, 6 (1899), 76.
11. P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, 2nd edition, New York, 1996.

References

12. A. Rotkiewicz, “On the Pseudoprimes with Respect to the Lucas Sequence,” *Bull. Acad. Polon. Sci. Ser. Math. Astronom. Phys.*, 21 (1973), 703–797.
13. N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, World-Wide Web URL www.research.att.com/∼njas/sequences/.
14. L. Somer, “Divisibility of Terms in Lucas Sequences of the Second Kind by Their Subscripts,” *Applications of Fibonacci Numbers*, Vol. 6 (Eds. G. E. Bergum et al.), Kluwer Academic Publishers, Dordrecht, 473–486.
15. J. V. Uspensky, *Theory of Equations,* McGraw-Hill, New York, 1948.
16. J. White, J. N. Hunt, and L. A. G. Dresel, “Uniform Huffman Sequences Do Not Exist,” *Bull. London Math. Soc.*, 9