CONDITIONAL LUCAS PSEUDOPRIMES

MURAT SAHIN* AND WILLIAM WEBB

ABSTRACT. Define the conditional recurrence sequence $q_n = aq_{n-1} + q_{n-2}$ if n is even, $q_n = bq_{n-1} + q_{n-2}$ if n is odd, where $q_0 = 0$, $q_1 = 1$. Then q_n satisfies a fourth order recurrence while both q_{2n} and q_{2n+1} satisfy a second order recurrence.

Analogously to a Lucas pseudoprime, we define a composite number n to be a conditional Lucas pseudoprime (clpsp) if n divides $q_{n-\left(\frac{\Delta}{n}\right)}$, where $\Delta = a^2b^2 + 4ab$ and $\left(\frac{\Delta}{n}\right)$ denotes the Jacobi symbol. We prove that if $(n, 2ab\Delta) = 1$, then there are infinitely many conditional Lucas pseudoprimes. We also address the question, given an odd composite integer n, for how many pairs (a, b) is n a conditional Lucas pseudoprime.

1. INTRODUCTION

A pseudoprime is probable prime which is not actually prime. Pseudoprimes can be classified according to which property they satisfy. Some of the classes are Fermat pseudoprimes, Euler pseudoprimes, Fibonacci pseudoprimes, Lucas pseudoprimes, Perrin pseudoprimes, strong pseudoprimes etc. In this study, after a brief recall about some classes of the pseudoprimes, we introduce a new class of pseudoprimes which are called conditional Lucas pseudoprimes.

The first pseudoprimes studied [1] were based on Fermat's little theorem which says

$$a^{p-1} \equiv 1 \pmod{p} \tag{1.1}$$

for p an odd prime. We say that a composite number n is a Fermat pseudoprime (or $psp(a)$) if (1.1) holds. Fermat pseudoprimes have been studied intensively. For a fixed base $a \geqslant 2$, pseudoprimes are sparsely distributed, but there are infinitely many. In addition to this, unfortunately, there are infinitely many Carmichael numbers which are $psp(a)$ for every integer a. The existence of such numbers provides encouragement to create other

Key words and phrases. Pseudoprimes, Fibonacci Pseudoprimes, Conditional Fibonacci Pseudoprimes, Lucas Pseudoprimes.

2000 *Mathematics Subject Classification.* 11B39, 11Y55, 11Y11, 05A15.

* Corresponding author.

pseudoprimes. Two of these are Euler and strong pseudoprimes (see[5] for detailed information).

Let D, P and Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Let $U_0 = 0,\ U_1 = 1$. The Lucas sequence $\{U_n\}$ is defined recursively for $n \geqslant 2$ by

$$U_n = PU_{n-1} - QU_{n-2}.$$

For $n \geqslant 0$, we also have

$$U_k = \frac{\left(\alpha^k - \beta^k\right)}{(\alpha - \beta)} \tag{1.2}$$

where α and β are distinct roots of $x^2 - Px + Q = 0$.

If n is prime and $\gcd(n, 2QD) = 1$, then

$$U_{n-\left(\frac{D}{n}\right)} \equiv 0 \pmod{n} \tag{1.3}$$

where $\left(\frac{D}{n}\right)$ denotes the Jacobi symbol. If n is composite, $\gcd(n, 2QD) = 1$ and (1.3) still holds, then we call n a Lucas pseudoprime with parameters P and Q (or $lpsp(P, Q)$). (See [6] for detailed information about pseudoprimes based on Fibonacci and Lucas sequences.)

Marcia Edson and Omer Yayenie [3] presented following generalized Fibonacci sequence

$$q_0 = 0,\ q_1 = 1\ q_n = \begin{cases} aq_{n-1} + q_{n-2}, & \text{if } n \text{ is even} \\ bq_{n-1} + q_{n-2}, & \text{if } n \text{ is odd} \end{cases}$$

where a and b are nonzero fixed integers. They found the generating function and Binet like formula for the conditional Fibonacci sequence. This new generalization produces a distinct sequence for each new choice of a and b. In fact, one can get many famous sequence, such as Fibonacci sequence, Pell numbers, k-Fibonacci numbers, etc., by altering the values of a and b in the sequence. For this sequence, we have the following.

The generating function $f(x)$ of the sequence $\{q_n\}$ is

$$f(x) = \frac{x(1 + ax - x^2)}{1 - (ab + 2)x^2 + x^4}.$$

Also, the Binet formula of the sequence q_n is given by

$$q_n = \frac{a^{1-\mu(n)}}{(ab)^{\lfloor \frac{n}{2} \rfloor}} \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1.4}$$

where α and β are roots of the polynomial $p(x) = x^2 - abx - ab$ and

$$\mu(m) = \begin{cases} 0, & \text{if } m \text{ is even} \\ 1, & \text{if } m \text{ is odd}\ . \end{cases}$$

In this paper, we define pseudoprimes, which are called conditional Lucas pseudoprimes, based on this sequence. We prove that there are infinitely

many composite numbers n which are conditional Lucas pseudoprimes for given pair (a, b). Also, we solve the problem, given a composite number n, for how many pairs (a, b) is n a conditional Lucas pseudoprime. Finally, we address the question of whether a pseudoprime test which depends on this sequence can be implemented efficiently or not.

2. Conditional Lucas Pseudoprimes

In this section, we define the conditional Lucas pseudoprime based on the following theorem.

Theorem 2.1. *Let the sequence (q_n) be as above and define $\Delta = a^2b^2 + 4ab$ which is not square. If p is prime with $\gcd(p, 2ab\Delta) = 1$ then*

$$q_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod{p}.$$

Proof. Define following sequence

$$K_j = K_j(a, b) = \frac{a^{1-\mu(j)}}{(ab)^{\lfloor \frac{j}{2} \rfloor}} \frac{x^j - (ab - x)^j}{x - (ab - x)} \pmod{p(x)} \tag{1}$$

where notations means that we take remainder in $\mathbb{Z}[x]$ upon division by $p(x)$. Then the sequence satisfies the following recurrence

$$K_j = \begin{cases} aK_{j-1} + K_{j-2}, & \text{if } j \text{ is even} \\ bK_{j-1} + K_{j-2}, & \text{if } j \text{ is odd} \end{cases}$$

and has initial values $K_0 = 0$ and $K_1 = 1$. That is, this sequence corresponds to generalized Lucas sequence (q_n). So, in this theorem we deal with objects in the ring $R = \mathbb{Z}_n[x]/(x^2 - abx - ab)$. That is, we deal with the set of coset representatives :

$$\{i + jx : i \text{ and } j \text{ are integers with } 0 \leqslant i, j < n\}.$$

We add coset representatives as vectors (mod n), and we multiply them via $x^2 = abx + ab$. Suppose p is prime with $(\frac{\Delta}{p}) = -1$. Then the polynomial $p(x)$ is irreducible over $\mathbb{Z}_p$. Thus R is isomorphic to the finite field $\mathbb{F}_{p^2}$. Let σ be the Frobenius automorphism in $\mathbb{F}_{p^2}$, which maps an element to its p-th power. Then

$$\begin{aligned} \sigma(u + v) &= \sigma(u) + \sigma(v), \\ \sigma(uv) &= \sigma(u)\sigma(v) \end{aligned}$$

and $\sigma(u) = u$ if and only if $u \in \mathbb{Z}_p$. The roots of $p(x)$ in the coset representatives are x and $ab - x$. Since x and $ab - x$ are not in $\mathbb{Z}_p$ and σ permutes the roots of $p(x)$, we have

$$\text{For the case } \left(\frac{\Delta}{p}\right) = -1 : \begin{cases} x^p \equiv ab - x \pmod{(p(x), p)}, \\ (ab - x)^p \equiv x \pmod{(p(x), p)}. \end{cases}$$

Then, $x^{p+1} - (ab-x)^{p+1} \equiv 0 \pmod{(p(x), p)}$ so (1) implies that $q_{p+1} \equiv 0 \pmod{p}$.

Now, suppose that $\left(\frac{\Delta}{p}\right) = 1$. So, the roots of the polynomial $p(x)$ are in $\mathbb{Z}_p$. In this case, R is not a finite field. It is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, and every element maps to the p-th power of itself. Thus,

$$\text{For the case } \left(\frac{\Delta}{p}\right) = -1 : \begin{cases} x^p \equiv x \pmod{(p(x), p)}, \\ (ab-x)^p \equiv ab - x \pmod{(p(x), p)}. \end{cases}$$

Since $\gcd(p, ab) = 1$ implies that x and $ab - x$ are invertible in R, since $x(ab-x) \equiv ab \pmod{p(x)}$. Hence $x^{p-1} = (ab-x)^{p-1} = 1$ in R. Thus (1) implies that $q_{p-1} \equiv 0 \pmod{p}$. □

Note that we say that a composite number n with $\gcd(n, 2ab\Delta) = 1$ is a conditional Lucas pseudoprime with parameters a and b (or *clpsp*(a, b)) if $q_{n-(\frac{\Delta}{n})} \equiv 0 \pmod{n}$.

Example 2.1. *For given $a = 11$ and $b = 8$, we get the following sequence*

$$\{q_n\} = \{0, 1, 11, 89, 990, 8009, \ldots\}.$$

For this sequence,

$$\begin{aligned} \Delta &= a^2b^2 + 4ab \\ &= 11^2 8^2 + 4.11.8 \\ &= 8096. \end{aligned}$$

Since

$$\gcd(9, 2ab\Delta) = \gcd(9, 1424896) = 1$$

and

$$q_{9-(\frac{9}{\Delta})} = q_8 = 8017020 \equiv 0 \pmod{9},$$

the composite number 9 is the first clpsp $(11, 8)$.

Now, we handle the following questions

Question 1: Are there infinitely many odd composite numbers n which are clpsp (a, b) for given a and b?

Question 2: Given an odd composite number n, for how many pairs (a, b) is n is a clpsp (a, b)?

In order to solve these problems, we need some Lemmas which show the relevance of conditional Lucas pseudoprimes.

Lemma 2.2. *n is a clpsp(a, b) if and only if n is a lpsp(P, Q) where $P = ab$, $Q = -ab$.*

Proof. Assume that n is clpsp (a, b) then we have

$$q_{n-(\frac{\Delta}{n})} \equiv 0 \pmod{n}$$

where $\Delta = a^2b^2 + 4ab$ and $\gcd(n, 2ab\Delta) = 1$. By the Binet formula (1.4) of the sequence $\{q_n\}$, we obtain

$$q_{n-(\frac{\Delta}{n})} = \frac{a^{1-\mu(n-(\frac{\Delta}{n}))}}{(ab)^{\left\lfloor \frac{n-(\frac{\Delta}{n})}{2} \right\rfloor}} \frac{\alpha^{n-(\frac{\Delta}{n})} - \beta^{n-(\frac{\Delta}{n})}}{\alpha - \beta} \equiv 0 \pmod{n}.$$

Since $\gcd(2ab\Delta, n) = 1$, we get

$$\frac{\alpha^{n-(\frac{\Delta}{n})} - \beta^{n-(\frac{\Delta}{n})}}{\alpha - \beta} \equiv 0 \pmod{n} \tag{2.1}$$

where α and β are the roots of the polynomial $p(x) = x^2 - abx - ab$.

For parameters $P = ab$ and $Q = -ab$ of the Lucas sequence, we have

$$D = P^2 - 4Q = (ab)^2 - 4(-ab) = a^2b^2 + 4ab = \Delta.$$

if we use the Binet formula (1.2) of the sequence $\{U_n\}$ and $D = \Delta$, we get the following

$$U_{n-(\frac{D}{n})} = U_{n-(\frac{\Delta}{n})} = \frac{\left(\alpha^{n-(\frac{\Delta}{n})} - \beta^{n-(\frac{\Delta}{n})}\right)}{(\alpha - \beta)}$$

where α and β are the roots of the polynomial $x^2 - Px + Q$ which is equal to $p(x)$. So ,we get the following

$$U_{n-(\frac{D}{n})} \equiv 0 \pmod{n} \tag{2.2}$$

by using (2.1). Since n is composite, $\gcd(2QD, n) = \gcd(2ab\Delta, n) = 1$ and (2.2) is satisfied, n is also lpsp (P, Q) where $P = ab$, $Q = -ab$. □

The converse of this theorem can be proved similarly.

Lemma 2.3. *n is a clpsp (a, b) if and only if n is a lpsp (P, Q) where $P = ab + 2, Q = 1$.*

Proof. Similar to Lemma (2.2) □

Now, we can solve the **Questions 1** and **2** by the following theorems.

Theorem 2.4. *Given pair (a, b), there are infinitely many odd composite numbers n which are clpsp(a, b).*

Proof. Given pair (P, Q) with $\gcd(P, Q) = 1$, we know that there are infinitely many odd composite numbers n which are *lpsp*(P, Q) (See Theorem 7 of [6]). So, there are infinitely many odd composite numbers n for which n is *lpsp*(P, Q) where $P = ab + 2, Q = 1$ for given a and b. By the Lemma (2.3), we get the desired result. □

Theorem 2.5. *Given an odd composite number n which has r different prime factors, the number of pairs (a,b) modulo n, for which n is a $clpsp(a,b)$ and $ab > 0$ is at most*

$$\sum_{k=0}^{r} d(ab)2^r$$

where $d(x)$ is the number of positive divisors of x.

Proof. Let p prime divisors of n. For fixed integer D, the number of distinct values of P modulo p, for which $P^2+4P \equiv D \pmod{p}$ and n is a $lpsp(P,-P)$ is $0, 1$ or 2 which depends on the number of the solutions of the quadratic equation $P^2 + 4P \equiv D \pmod{p}$ (See Theorem 2 of [6]). So, the number of distinct values of P modulo n, for which $P^2 + 4P \equiv D \pmod{n}$ and n is a $lpsp(P,-P)$ is at most 2^r. According to Lemma 2.2, for each integer P modulo n, the number of pairs (a,b) which hold $P = ab$ and $ab > 0$ is $d(P)$. So, Given an odd composite number n which has r different prime factors, the number of pairs (a,b) modulo n, for which n is a $clpsp(a,b)$ and $ab > 0$ is at most

$$\sum_{k=0}^{r} d(ab)2^r.$$

□

3. Calculation of the Conditional Lucas Sequence

We have an easy way to prove that many numbers are composite by using the ordinary pseudoprime test, since $a^{p-1} \pmod{p}$ can be rapidly computed by the technique of repeated squaring. Also, Lucas tests which determine whether the given integer is a Lucas pseudoprime can be implemented effectively in about twice the time of a (Fermat) pseudoprime test by Lucas chains. (See for detailed information [2] and [4]).

Now, we try to answer the question of whether a pseudoprime test which depends on the sequence $\{q_n\}$ can be implemented efficiently or not. the authors presented many properties of the sequence $\{q_n\}$ in [3].

The following properties

$$\left(a^{1-\mu(n+k)}b^{\mu(n+k)}\right) q_{n+k+1}^2 + \left(a^{1-\mu(n-k)}b^{\mu(n-k)}\right) q_{n-k}^2 = aq_{2n+1}q_{2k+1}$$

for any nonnegative integers n and k with $n \geqslant k$ and

$$q_{n+2}^2 - q_n^2 = a^{1-\mu(n)}b^{\mu(n)}q_{2n+2} \tag{3.1}$$

for any nonnegative integer n are hold for the sequence $\{q_n\}$ (See [3]). The first property above is also holds for $k = 0$, so we can say that

$$\left(a^{1-\mu(n)}b^{\mu(n)}\right) q_{n+1}^2 + \left(a^{1-\mu(n)}b^{\mu(n)}\right) q_n^2 = aq_{2n+1}q_1. \tag{3.2}$$

Now the question is can $q_n \pmod n$ be calculated effectively. If so we can effectively determine whether a given integer is a conditional pseudoprime or not.

If we have the residues $q_k \pmod n$ and $q_{k+1} \pmod n$ for nonnegative integer k, we can compute either the pair $q_{2k+1} \pmod n$, $q_{2k+2} \pmod n$ or the pair $q_{2k+2} \pmod n$, $q_{2k+3} \pmod n$ by using the properties (3.2), (3.1) and the definition of the sequence $\{q_n\}$ with each choice taking four multiplications modulo n and two addition modulo n. So, starting from the pair q_0, q_1 we can recursively using (3.2), (3.1) and the definition of the sequence $\{q_n\}$ to arrive any pair q_m, q_{m+1}. For example, if $m = 17$ then we can arrive 17 as follows:

$$0,1 \to 1,2 \to 2,3 \to 4,5 \to 8,9 \to 17,18.$$

There are two types of moves. One way to determine which move to choose in each step is starting from the target pair $m, m+1$ and work backwards.

4. Conclusion

In this paper, we define the conditional Lucas pseudoprimes which are the generalization of the Lucas pseudoprime. Then, we prove that there are infinitely many composite numbers n which are conditional Lucas pseudoprimes for given pair (a, b). Also, we solve the problem, given an composite numbers n, for how many pairs (a, b) is n a conditional Lucas pseudoprimes. Finally, we show that we can determine effectively given integer whether conditional Lucas pseudoprime or not.

Conditional recurrences can be defined in many different ways (for different $\{q_n\}$), having a more complex definition, would have a different set of liars yet. Ideally, the number of liars would be even less than for the other tests.

Acknowledgments: We would like to thank Professor Samuel S. Wagstaff, Jr. for his excellent comments. Also, we would like to thank the referee for their useful suggestions.

References

[1] C. Pomerance, J. L. Selfridge and S. Wagstaff, Jr. , The pseudoprimes to 25.000.000.000, Math. Comp. 35 (1980), 1003-1026.

[2] D. Bleichenbacher, Efficiency and security of cryptosystems based on number theory, Phd thesis, Swiss Federal Instute of Technology Zürich, 1996.

[3] M. Edson and O. Yayenie, A new Generalization of Fibonacci Sequence and Extended Binet's Formula, INTEGERS Electronic Journal of Combinatorial Number Theory 9 (2009), 639-654.

[4] P. Montgomery, Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains. Unpublished manuscript, 1992.

[5] R. E. Crandall and C. Pomerance, Prime numbers : A computational approach, Springer-Verlag, 2001.

[6] R. Baillie and S. Wagstaff, Jr. , Lucas pseudoprimes, Math. Comp. 35 (1980), 1390-1417.

[7] E. Lehmer, "On the infinitude of Fibonacci pseudo-primes", Fibonacci Quart., v. 2, 1964, 229-230.

DEPARTMENT OF MATHEMATICS, ANKARA UNIVERSITY, FACULTY OF SCIENCE, 06100, ANKARA, TURKEY. email: musahin@science.ankara.edu.tr

DEPARTMENT OF MATHEMATICS, WASHINGTON STATE UNIVERSITY, USA
email: webb@math.wsu.edu