Available online at http://scik.org
J. Math. Comput. Sci. 10 (2020), No. 6, 2544-2556
https://doi.org/10.28919/jmcs/4921
ISSN: 1927-5307

PRIMALITY TEST WITH PAIR OF LUCAS SEQUENCES

P. ANURADHA KAMESWARI*, B. RAVITHEJA

Department of Mathematics, Andhra University, Visakhapatnam-530003, India

Abstract. Lucas sequences and their applications play vital role in the study of primality tests in number theory. There are several known tests for primality of positive integer N using Lucas sequences which are based on factorization of $(N \pm 1)$ [2] [13]. In this paper we give a primality test for odd positive integer $N > 1$ by using the set $L(\Delta, N)$ where $L(\Delta, N)$ is a set of $S(N)$ distinct pair of Lucas sequences $\Big(V_n(a,1), U_n(a,1)\Big)$, where $S(N)$ for $N = p_1^{e_1}.p_2^{e_2}\dots p_s^{e_s}$ is given as $S(N) = \text{LCM}\left[\left\{p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)\right\}_{i=1}^{s}\right]$ and $\Delta = a^2 - 4$ for some fixed integer a.

Keywords: Lucas sequences; primality testing.

2010 AMS Subject Classification: 94A60, 11T71.

1. Introduction

Lucas sequences are recurrence relations. Many studies on properties of Lucas sequences, and their connections with topics like trigonometric functions, Chebyshev's functions, Dickson functions, continued fractions are known [2][7]. The primality test for a positive integer N using Lucas sequences was first initiated by Lucas and later developed further by Lehmer, was based on factorization of $(N \pm 1)$ [2][8]. In this paper we give a primality test for odd positive integer $N > 1$ by using the set $L(\Delta, N)$ where $L(\Delta, N)$ is a set of $S(N)$ distinct pair of Lucas sequences

*Corresponding author

E-mail address: panuradhakameswari@yahoo.in

Received August 8, 2020

$\Big(V_n(a,1),U_n(a,1)\Big)$, where $S(N)$ for $N = p_1^{e_1}.p_2^{e_2}\dots p_s^{e_s}$ is given as $S(N) = \mathrm{LCM}\Big[\Big\{p_i^{e_i-1}\Big(p_i - \Big(\frac{\Delta}{p_i}\Big)\Big)\Big\}_{i=1}^{s}\Big]$ and $\Delta = a^2-4$ for some fixed integer a. In the following we describe the pair of Lucas sequences and their properties.

Definition 1.1. Let a and b be two integers, α a root of the polynomial x^2-ax+b in $\mathbf{Q}(\sqrt{\Delta})$ for $\Delta = a^2-4b$ a non square, writing $\alpha = \frac{a+\sqrt{\Delta}}{2}$ and its conjugate $\beta = \frac{a-\sqrt{\Delta}}{2}$ we have $\alpha+\beta = a, \alpha\beta = b, \alpha-\beta = \sqrt{\Delta}$, and the Lucas sequences $V_n(a,b)$ and $U_n(a,b), n \geq 0$ are defined as

$$\begin{cases} V_n(a,b) = \alpha^n + \beta^n, \\ U_n(a,b) = \frac{\alpha^n-\beta^n}{\alpha-\beta}. \end{cases}$$

In particular, $V_0(a,b) = 2$, $V_1(a,b) = a$ and $U_0(a,b) = 0$, $U_1(a,b) = 1$.

$V_n(a,b)$ and $U_n(a,b)$ are given by following recurrence sequences:

$$\begin{cases} V_n(a,b) = aV_{n-1}(a,b) - bV_{n-2}(a,b), \\ U_n(a,b) = aU_{n-1}(a,b) - bU_{n-2}(a,b). \end{cases}$$

Lucas sequences satisfy the following properties [3] [4] [9]:

(1) $\Big(V_{2n}(a,b),U_{2n}(a,b)\Big) = \Big((V_n(a,b))^2 - 2b^n, U_n(a,b)V_n(a,b)\Big)$.

(2) $\Big(V_n^2(a,b),U_n^2(a,b)\Big) = \Big(\Delta(U_n(a,b))^2 + 4b^n, U_{n-1}(a,b)U_{n+1}(a,b) + b^{n-1}\Big)$.

(3) $\Big(2V_{m+n}(a,b),2U_{m+n}(a,b)\Big) = \Big(V_m(a,b)V_n(a,b) + \Delta U_m(a,b)U_n(a,b),$
$U_m(a,b)V_n(a,b) + U_n(a,b)V_m(a,b)\Big)\ \forall\ m \geq n.$

(4) $\Big(V_{m+n}(a,b),U_{m+n}(a,b)\Big) = \Big(V_m(a,b)V_n(a,b) - b^nV_{m-n}(a,b),$
$U_m(a,b)V_n(a,b) - b^nU_{m-n}(a,b)\Big),\ \forall\ m \geq n.$

In particular for $b = 1$ the above properties can be written as

(1) $\Big(V_{2n}(a,1),U_{2n}(a,1)\Big) = \Big((V_n(a,1))^2 - 2, U_n(a,1)V_n(a,1)\Big)$.

(2) $\Big(V_n^2(a,1),U_n^2(a,1)\Big) = \Big(\Delta(U_n(a,1))^2 + 4, U_{n-1}(a,1)U_{n+1}(a,1) + 1\Big)$.

(3) $\Big(2V_{m+n}(a,1),2U_{m+n}(a,1)\Big) = \Big(V_m(a,1)V_n(a,1) + \Delta U_m(a,1)U_n(a,1),$
$U_m(a,1)V_n(a,1) + U_n(a,1)V_m(a,1)\Big)\ \forall\ m \geq n.$

(4) $\Big(V_{m+n}(a,1),U_{m+n}(a,1)\Big) = \Big(V_m(a,1)V_n(a,1) - V_{m-n}(a,1),$
$U_m(a,1)V_n(a,1) - U_{m-n}(a,1)\Big),\ \forall\ m \geq n.$

Definition 1.2. If $N = p_1^{e_1}.p_2^{e_2}\dots p_s^{e_s}$ and $\Delta = a^2-4b$ for some fixed integer a such that $(N,\Delta)=1$ then we have define $S(N) = \mathrm{LCM}[n_1,n_2,\dots,n_s]$ where $n_i = p_i^{e_i-1}\left(p_i-\left(\frac{\Delta}{p_i}\right)\right)$ for all $1\le i\le s$ and $\left(\frac{\Delta}{p_i}\right)$ is the Legendre symbol [12] of Δ with respect to the prime p_i.

(1) $\left(V_{S(N)}(a,b),U_{S(N)}(a,b)\right)\equiv\left(2b^{\frac{k(1-\varepsilon)}{2}},0\right) \mod N.$

(2) $\left(V_{S(N)t}(a,b),U_{S(N)t}(a,b)\right)\equiv\left(2b^{\frac{k(1-\varepsilon)}{2}},0\right) \mod N.$

In particular for $b=1$, we have

(1) $\left(V_{S(N)}(a,1),U_{S(N)}(a,1)\right)\equiv\left(2,0\right) \mod N.$

(2) $\left(V_{S(N)t}(a,1),U_{S(N)t}(a,1)\right)\equiv\left(2,0\right) \mod N.$

In the following an algorithm is given for computation of Lucas sequences $\left(V_n(a,1),U_n(a,1)\right)$ using Lucas addition chain as in [11]. This algorithm gives Lucas addition chain [5] [11] $\{e_{-1},e_0,e_1,e_1+1,\dots e_{k-1}-1,e_{k-1},e_k\}$ and evaluates $\left\{\left(V_{e_{-1}},U_{e_{-1}}\right),\left(V_{e_0},U_{e_0}\right),\left(V_{e_1},U_{e_1}\right),\dots\left(V_{e_{t-1}},U_{e_{t-1}},\left(V_{e_t},U_{e_t}\right)\right)\right\}$ for all $t=0,1,\dots,k$ by using the formulas $V_{y+z}(a,1)$ and $U_{y+z}(a,1)$.

Algorithm 1 Evaluate $\left(V_n(a,1),U_n(a,1)\right)$

---

step 0: (Initialize) Set $N\leftarrow\frac{n}{2^{k-i}}$ where $k=\lfloor\log n\rfloor, i=0,1,2,\dots,k$ $Y\leftarrow 1, Z\leftarrow 2$

step 1: (Value N) $N\leftarrow\frac{n}{2^{k-i}}$ and determine whether N is even or odd, if N is even skip to step 4.

step 2: set $Y\leftarrow 2Y+1$ and $Z\leftarrow 2Z$

step 3: $[N=n]$, if $N=n$ the algorithm terminates with Y as the answer.

step 4: set$Y\leftarrow 2Y$, $Z\leftarrow Y+1$ and return to step 1.

step 5: [initialize $(V_n(a,1),U_n(a,1)$] set $V_0(a,1)=2, V_1(a,1)=a$ and $U_0(a,1)=0, U_1(a,1)=1$

step 6: For i from 0 *to* k set $n\leftarrow y+z$

compute $V_{y+z}(a,1)\leftarrow V_y(a,1)V_z(a,1)-V_{y-z}(a,1)$

and $U_{y+z}(a,1)\leftarrow U_y(a,1)V_z(a,1)-U_{y-z}(a,1)$

---

2. PRIMALITY OF N WITH $S(N)$

In the following we prove a theorem on primality of N with $S(N)$ [7] [9].

Theorem 2.1. If N is odd positive integer then N is prime if and only if $S(N) = N - \left(\frac{\Delta}{N}\right)$ for all Δ with $(\Delta, N) = 1$.

Proof. Let N be a prime number then by definition for $N = p$, and any Δ with $(\Delta, N) = 1$ we have $S(N) = S(p) = p - \left(\frac{\Delta}{p}\right) = N - \left(\frac{\Delta}{N}\right)$. Conversely suppose $S(N) = N - \left(\frac{\Delta}{N}\right)$, now if N is composite then for $N = \prod_{i=1}^{s} p_i^{e_i}$ we have the two cases (i) $s = 1$ with $e_1 \geq 2$ and (ii) $s \geq 2$. In case (i) for $s = 1, e_1 \geq 2$, we have $N = p_1^{e_1}, e_1 \geq 2$ and $S(N) = S(p_1^{e_1}) = p_1^{e_1 - 1}\left(p - \left(\frac{\Delta}{p}\right)\right)$, therefore as $e_1 \geq 2$ we have $p_1 | S(N)$ but note $p_1 \nmid p_1^{e_1} \pm 1$ i.e. $p_1 \nmid N - \left(\frac{\Delta}{N}\right)$ a contradiction to $S(N) = N - \left(\frac{\Delta}{N}\right)$, hence N is not in case (i). Now if N is as in case (ii) we have $N = \prod_{i=1}^{s} p_i^{e_i}$, with $s \geq 2$ and $S(N) = \mathrm{LCM}\left[\left\{p_i^{e_i - 1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)\right\}_{i=1}^{s}\right]$. Now as p_i's are odd, $(\Delta, N) = 1$ and $\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)$ are even, we note in the following that $S(N) < N - 1$:

$$
\begin{aligned}
S(N) &= \mathrm{LCM}\left[\left\{p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)\right\}_{i=1}^{s}\right] \\
&= 2\ \mathrm{LCM}\left[\left\{p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)\right\}_{i=1}^{s}\right] \\
&\leq 2\prod_{i=1}^{s}\left[\frac{1 - \frac{1}{p_i}\left(\frac{\Delta}{p_i}\right)}{2} p_i^{e_i}\right] \\
&= 2N\prod_{i=1}^{s}\frac{1}{2}\left[1 + \frac{1}{p_i}\right] \\
&\leq 2N\frac{1}{2^s}\prod_{i=1}^{s}\left[1 + \frac{1}{p_i}\right] \\
&= 2N\frac{1}{2^s}\left[1 + \sum_i \frac{1}{p_i} + \sum_{i,j}\frac{1}{p_i p_j} + \ldots + \sum_{i,j\ldots s}\frac{1}{p_i p_j \ldots p_s}\right] \\
&\leq 2N\frac{1}{2^s}\left[1 + \sum_i \frac{1}{5} + \sum_{i,j}\frac{1}{5^2} + \ldots + \sum_{i,j\ldots s}\frac{1}{5^s}\right] \text{ as } p_i \geq 5 \\
&= 2N\frac{1}{2^s}\left[1 + s_{c_1}\left(\frac{1}{5}\right) + s_{c_2}\left(\frac{1}{5^2}\right) + \ldots + s_{c_s}\left(\frac{1}{5^s}\right)\right] \\
&= 2N\frac{1}{2^s}\left(1 + \frac{1}{5}\right)^s \\
&= 2N\left(\frac{3}{5}\right)^s \\
&\leq 2N\left(\frac{3}{5}\right)^2 \text{ as } s \geq 2 \\
&< 2N\left(\frac{2}{5}\right) = \frac{4N}{5} < N - 1
\end{aligned}
$$

Therefore $S(N) < N-1$, and as $(N-1) < (N+1)$ we also have $S(N) < N+1$ in particular we have $S(N) < N - (\frac{\Delta}{N})$ which is a contradiction to $S(N) = N - (\frac{\Delta}{N})$, therefore N is not in case (ii) as well, therefore N is not composite. Hence N is prime. $\square$

3. Primality Test With Pair of Lucas Sequences

Notation 3.1. Let N be a positive integer and $\Delta = a^2 - 4$ for some positive integer a such that $(N,\Delta) = 1$, then the set of all the pairs of Lucas sequences is denoted as $L(\Delta,N)$ and is given as $L(\Delta,N) = \Big\{\Big(V_n(a,1), U_n(a,1)\Big) : 1 \le n \le S(N)\Big\}$.

The following theorem assures that all the pairs in $L(\Delta,N)$ are distinct modulo N and $|L(\Delta,N)| = S(N)$.

Theorem 3.2. $\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod N$ if and only if $r \equiv 0 \mod S(N)$ [10].

Proof. Suppose $r \equiv 0 \mod S(N)$, then we have $r = S(N)t$, for some integer t and
$\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_{S(N)t}(a,1), U_{S(N)t}(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod N$,
therefore $r \equiv 0 \mod S(N)$ implies $\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod N$.
Conversely suppose $\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod N$, then for $N = p_1^{e_1}.p_2^{e_2}\dots p_s^{e_s}$ note $\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod p_i^{e_i}$ for all $i = 1,2,\dots,s$. We now show in the following that $p_i^{e_i-1}\Big(p_i - \Big(\frac{\Delta}{p_i}\Big)\Big)$ divides r for all $i = 1,2,\dots,s$. For all Δ with $(\Delta,N) = 1$ as $(\Delta, p_i^{e_i}) = 1$ using Euler's criterion we have

$$\alpha^{p_i} \equiv \begin{cases} \alpha \mod p_i \text{ if } \Big(\frac{\Delta}{p_i}\Big) = 1, \\ \beta \mod p_i \text{ if } \Big(\frac{\Delta}{p_i}\Big) = -1 \end{cases}$$
$$\Rightarrow \alpha^{p_i} \equiv \begin{cases} \alpha + kp_i \text{ if } \Big(\frac{\Delta}{p_i}\Big) = 1, \\ \beta + kp_i \text{ if } \Big(\frac{\Delta}{p_i}\Big) = -1 \end{cases}$$

Therefore for $i = 1, 2, \ldots, s$ we have,

$$\alpha^{p_i^{e_i}} = (\alpha^{p_i})^{p_i^{e_i-1}} = (\alpha + kp_i)^{p_i^{e_i-1}}$$
$$= \alpha^{p_i^{e_i-1}} + \binom{p_i^{e_i-1}}{1}\alpha^{p_i^{e_i-1}-1}(kp_i) + \binom{p_i^{e_i-1}}{2}\alpha^{p_i^{e_i-1}-2}(kp_i)^2 + \ldots +$$
$$\binom{p_i^{e_i-1}}{p_i^{e_i-1}-1}\alpha(kp_i)^{p_i^{e_i-1}-1} + (kp_i)^{p_i^{e_i-1}}$$
$$\Rightarrow \alpha^{p_i^{e_i}} \equiv \alpha^{p_i^{e_i-1}} \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = 1.$$

Similarly,

$$\alpha^{p_i^{e_i}} = (\alpha^{p_i})^{p_i^{e_i-1}}$$
$$= (\beta + kp_i)^{p_i^{e_i-1}}$$
$$\Rightarrow \alpha^{p_i^{e_i}} \equiv \beta^{p_i^{e_i-1}} \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = 1$$

therefore,

$$\alpha^{p_i^{e_i}} \equiv \begin{cases} \alpha^{p_i^{e_i-1}} & \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = 1, \\ \beta^{p_i^{e_i-1}} & \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = -1 \end{cases}$$

now $\alpha^{p_i^{e_i}} \equiv \alpha^{p_i^{e_i-1}} \mod p_i^{e_i}$ if $\left(\frac{\Delta}{p_i}\right) = 1 \Rightarrow \alpha^{p_i^{e_i}(p-1)} \equiv 1 \mod p_i^{e_i}$ if $\left(\frac{\Delta}{p_i}\right) = 1$
and $\alpha^{p_i^{e_i}} \equiv \beta^{p_i^{e_i-1}} \mod p_i^{e_i}$ if $\left(\frac{\Delta}{p_i}\right) = -1 \Rightarrow \alpha^{p_i^{e_i}(p+1)} \equiv 1 \mod p_i^{e_i}$ if $\left(\frac{\Delta}{p_i}\right) = -1$
therefore note $p_i^{e_i}$ is smallest such that

$$\alpha^{p_i^{e_i}} \equiv \begin{cases} \alpha^{p_i^{e_i-1}} & \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = 1, \\ \beta^{p_i^{e_i-1}} & \mod p_i^{e_i} \text{ if } \left(\frac{\Delta}{p_i}\right) = -1 \end{cases}$$

$\Rightarrow p_i^{e_i}$ is smallest such that $\alpha^{p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)} \equiv 1 \mod p_i^{e_i}$.
Now note $\Big(V_r(a,1), U_r(a,1)\Big) \equiv \Big(V_0(a,1), U_0(a,1)\Big) \mod p_i^{e_i}$
$\Rightarrow V_r(a,1) \equiv V_0(a,1) \mod p_i^{e_i}$ and $U_r(a,1) \equiv U_0(a,1) \mod p_i^{e_i}$
$\Rightarrow \alpha^r + \beta^r \equiv 2 \mod p_i^{e_i}$ and $\frac{\alpha^r - \beta^r}{\alpha - \beta} \equiv 0 \mod p_i^{e_i}$
$\Rightarrow \alpha^r + \beta^r \equiv 2 \mod p_i^{e_i}$ and $\alpha^r - \equiv \beta^r \mod p_i^{e_i}$
$\Rightarrow 2\alpha^r \equiv 2 \mod p_i^{e_i}$
$\Rightarrow \alpha^r \equiv 1 \mod p_i^{e_i}$, therefore $p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)$ divides r for $i = 1, 2, \ldots, s$ therefore r is a

common multiple of $p_i^{e_i-1}\Big(p_i-\big(\frac{\Delta}{p_i}\big)\Big)$ and as $S(N)$ is the LCM$\Big[\Big\{p_i^{e_i-1}\Big(p_i-\big(\frac{\Delta}{p_i}\big)\Big)\Big\}_{i=1}^{s}\Big]$ we have $S(N)|r$ which implies $r\equiv 0 \mod S(N)$, therefore we have $\Big(V_r(a,1),U_r(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$ implies $r\equiv 0 \mod S(N)$. □

Now in the following theorem we propose a primality test for N by using the pair of Lucas sequences.

Theorem 3.3. For any odd positive integer $N>1$, N is prime if and only if $\Big(V_{N-(\frac{\Delta}{N})}(a,1),U_{N-(\frac{\Delta}{N})}(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$, for all Δ with $(\Delta,N)=1$.

Proof. Let N be prime number, then by definition $S(N)=N-\big(\frac{\Delta}{N}\big)$ for all Δ with $(\Delta,N)=1$ and as $S(N)\equiv 0 \mod S(N)$, by Theorem 3.1 we have

$\Big(V_{S(N)}(a,1),U_{S(N)}(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$

$\Rightarrow \Big(V_{N-(\frac{\Delta}{N})}(a,1),U_{N-(\frac{\Delta}{N})}(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$

$\therefore$ N is prime implies $\Big(V_{N-(\frac{\Delta}{N})}(a,1),U_{N-(\frac{\Delta}{N})}(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$, for all Δ with $(\Delta,N)=1$.

Conversely let $\Big(V_{N-(\frac{\Delta}{N})}(a,1),U_{N-(\frac{\Delta}{N})}(a,1)\Big)\equiv\Big(V_0(a,1),U_0(a,1)\Big) \mod N$, for all Δ with $(\Delta,N)=1$ then by Theorem 3.1 we have $N-\big(\frac{\Delta}{N}\big)\equiv 0 \mod S(N)$, therefore we have $S(N)\mid N-\big(\frac{\Delta}{N}\big)$, for all Δ with $(N,\Delta)=1$.

If possible suppose N is not a prime, then we have the cases that N is composite and not squarefree or N is composite and squarefree. First suppose N is composite and not squarefree then $N=p_1^{e_1}.p_2^{e_2}\dots p_s^{e_s}$, for $p_1,p_2,\dots,p_s$ are distinct primes and $s\geq 1$ with $e_i>1$ for some $1\leq i\leq s$, that is $e_i-1>0$ then for some $1\leq i\leq s$, therefore $S(N)=\mathrm{LCM}[p_1^{e_1-1}(p_1-\Big(\frac{\Delta}{p_1}\Big)),p_2^{e_2-1}(p_2-\Big(\frac{\Delta}{p_2}\Big),\dots,p_s^{e_s-1}(p_s-\Big(\frac{\Delta}{p_s}\Big))]\Rightarrow p_i^{e_i-1}\nmid S(N)$ for some $1\leq i\leq s$. Further for Δ with $(\Delta,N)=1$, we have $N-\big(\frac{\Delta}{N}\big)=N\pm 1$ and $p_i\nmid N$ for all $1\leq i\leq s$ note $p_i\nmid(N-\big(\frac{\Delta}{N}\big))$ for all $1\leq i\leq s$. Therefore as $p_i\mid S(N)$ for some $1\leq i\leq s$ and $p_i\nmid(N-\big(\frac{\Delta}{N}\big))$ for all $1\leq i\leq s$ note $S(N)\nmid N-\big(\frac{\Delta}{N}\big)$ which is contradiction to $S(N)\mid N-\big(\frac{\Delta}{N}\big)$ for all Δ with $(N,\Delta)=1$, therefore N is composite and not squarefree is not possible. Now if N is composite and squarefree then $N=p_1.p_2\dots p_s$ for $p_i's$ are distinct primes and $s>1$, therefore writing $N=p_ip_jt$ for $p_i\neq p_j$ for some $1\leq i,j\leq s$ and for $p_i>3$ we have

$P_i-\Big(\frac{\Delta}{p_i}\Big)\equiv 0 \mod p_i-\Big(\frac{\Delta}{p_i}\Big)$

$\Rightarrow p_i\equiv\Big(\frac{\Delta}{p_i}\Big) \mod p_i-\Big(\frac{\Delta}{p_i}\Big)$

$\Rightarrow N = p_i p_j t \equiv p_j t \left(\frac{\Delta}{p_i}\right) \mod p_i - \left(\frac{\Delta}{p_i}\right)$
$\Rightarrow N \equiv p_j t \left(\frac{\Delta}{p_i}\right) \mod p_i - \left(\frac{\Delta}{p_i}\right)$
$\Rightarrow N - \left(\frac{\Delta}{p_i p_j t}\right) \equiv p_j t \left(\frac{\Delta}{p_i}\right) - \left(\frac{\Delta}{p_i p_j t}\right) \mod p_i - \left(\frac{\Delta}{p_i}\right)$
$\Rightarrow N - \left(\frac{\Delta}{N}\right) \equiv p_j t \left(\frac{\Delta}{p_i}\right) - \left(\frac{\Delta}{p_i}\right)\left(\frac{\Delta}{p_j t}\right) \mod p_i - \left(\frac{\Delta}{p_i}\right)$
$\Rightarrow N - \left(\frac{\Delta}{N}\right) \equiv \left(\frac{\Delta}{p_i}\right)\left(p_j t - \left(\frac{\Delta}{p_j t}\right)\right) \mod p_i - \left(\frac{\Delta}{p_i}\right)$
$\Rightarrow p_j t - \left(\frac{\Delta}{p_j t}\right) \equiv 0 \mod p_i - \left(\frac{\Delta}{p_i}\right)$ as $p_i - \left(\frac{\Delta}{p_i}\right) \mid N - \left(\frac{\Delta}{N}\right)$

Therefore we have $p_i - \left(\frac{\Delta}{p_i}\right) \mid p_j t - \left(\frac{\Delta}{p_j t}\right)$, for all Δ with $(\Delta, N) = 1$, but note this is a contradiction as there are some Δ such that $p_i - \left(\frac{\Delta}{p_i}\right) \nmid p_j t - \left(\frac{\Delta}{p_j t}\right)$ which is seen in the following:
For a_1, a_2 with $a_1 \equiv a_2 \mod p_i$ we have for $\Delta_1 = a_1^2 - 4, \Delta_2 = a_2^2 - 4$ such that $\left(\frac{\Delta_1}{N}\right) \neq \left(\frac{\Delta_2}{N}\right)$, then $\left(\frac{\Delta_1}{p_i}\right) = \left(\frac{\Delta_2}{p_i}\right)$ and $\left(\frac{\Delta_1}{p_j t}\right) \neq \left(\frac{\Delta_2}{p_j t}\right)$ and we have the following cases;
(i) $\left(\frac{\Delta_1}{p_i}\right) = \left(\frac{\Delta_2}{p_i}\right) = 1$ and $\left(\frac{\Delta_1}{p_j t}\right) = 1, \left(\frac{\Delta_2}{p_j t}\right) = -1$.
(ii) $\left(\frac{\Delta_1}{p_i}\right) = \left(\frac{\Delta_2}{p_i}\right) = 1$ and $\left(\frac{\Delta_1}{p_j t}\right) = -1, \left(\frac{\Delta_2}{p_j t}\right) = 1$.
(iii) $\left(\frac{\Delta_1}{p_i}\right) = \left(\frac{\Delta_2}{p_i}\right) = -1$ and $\left(\frac{\Delta_1}{p_j t}\right) = 1, \left(\frac{\Delta_2}{p_j t}\right) = -1$.
(iv) $\left(\frac{\Delta_1}{p_i}\right) = \left(\frac{\Delta_2}{p_i}\right) = -1$ and $\left(\frac{\Delta_1}{p_j t}\right) = -1, \left(\frac{\Delta_2}{p_j t}\right) = 1$.
in all the cases note either $p_i - \left(\frac{\Delta_1}{p_i}\right) \nmid p_j t - \left(\frac{\Delta_1}{p_j t}\right)$ or $p_i - \left(\frac{\Delta_2}{p_i}\right) \mid p_j t - \left(\frac{\Delta_2}{p_j t}\right)$
i.e. $(p_i - 1) \nmid (p_j t - 1)$ or $(p_i - 1) \nmid (p_j t + 1)$
$(p_i - 1) \nmid (p_j t + 1)$ or $(p_i - 1) \nmid (p_j t - 1)$
$(p_i + 1) \nmid (p_j t - 1)$ or $(p_i + 1) \nmid (p_j t + 1)$
$(p_i + 1) \nmid (p_j t + 1)$ or $(p_i + 1) \nmid (p_j t - 1)$
respectively as $(p_i - 1) \mid (p_j t - 1)$ and $(p_i - 1) \nmid (p_j t + 1)$ implies $(p_i - 1) \mid \pm 2$ which implies $p_i = 1$ or 3, a contradiction which implies N is not a composite and squarefree number, therefore N is prime. □

In the following, an algorithm is given for evaluating Lucas sequences $\Big(V_n(a,1), U_n(a,1)\Big)$ and test for primality of N.

Algorithm 2 Evaluate $\Big(V_n(a,1), U_n(a,1)\Big)$ and test for primality of N

step 0: (Initialize) Set $N \leftarrow \frac{n}{2^{k-i}}$ where $k = \lfloor \log n \rfloor, i = 0,1,2,\ldots,k$

$Y \leftarrow 1, Z \leftarrow 2$

step 1: (Value N) $N \leftarrow \frac{n}{2^{k-i}}$ and determine whether N is even or odd, if N is even skip to step 4.

step 2: set $Y \leftarrow 2Y+1$ and $Z \leftarrow 2Z$

step 3: $[N = n]$, if $N = n$ the algorithm terminates with Y as the answer.

step 4: set$Y \leftarrow 2Y$, $Z \leftarrow Y+1$ and return to step 1.

step 5: [initialize $(V_n(a,1), U_n(a,1)]$ set $V_0(a,1) = 2, V_1(a,1) = a$

and $U_0(a,1) = 0, U_1(a,1) = 1$

step 6: For i from 0 *to* k set $n \leftarrow x+y$

compute $V_{y+z}(a,1) \leftarrow V_y(a,1)V_z(a,1) - V_{y-z}(a,1)$

and $U_{y+z}(a,1) \leftarrow U_y(a,1)V_z(a,1) - U_{y-z}(a,1)$

step 7: compute $\Big(V_{N\pm1}(a,1), U_{N\pm1}(a,1)\Big)$ mod N, if it is $\Big(V_0(a,1), U_0(a,1)\Big)$ mod N then N is prime otherwise N is composite.

Example 3.4. Let $N = 2883155$, $a = 41$ then $\Delta = 1677$ such that $\left(\frac{\Delta}{N}\right) = \left(\frac{1677}{2883155}\right) = -1$
Now compute $\Big(V_{N-\left(\frac{\Delta}{N}\right)}(a,1), U_{N-\left(\frac{\Delta}{N}\right)}(a,1)\Big) \mod N$
$\equiv \Big(V_{2883155+1}(41,1), U_{2883155+1}(41,1)\Big) \mod 2883155$
$\equiv \Big(V_{2883156}(41,1), U_{2883156}(41,1)\Big) \mod 2883155$
$\equiv \Big(V_{276}(41,1), U_{276}(41,1)\Big) \mod 2883155$
$\equiv (80, 192239) \mod 2883155$
so, $\Big(V_{N-\left(\frac{\Delta}{N}\right)}(a,1), U_{N-\left(\frac{\Delta}{N}\right)}(a,1)\Big) \not\equiv (V_0(a,1), U_0(a,1)) \mod N$, therefore N is not a prime.

Example 3.5. Let $N = 104701$, $a = 64$ then $\Delta = 4092$ such that $\left(\frac{\Delta}{N}\right) = \left(\frac{4092}{104701}\right) = 1$
Now compute $\Big(V_{N-\left(\frac{\Delta}{N}\right)}(a,1), U_{N-\left(\frac{\Delta}{N}\right)}(a,1)\Big) \mod N$
$\equiv \Big(V_{104701-1}(64,1), U_{104701-1}(64,1)\Big) \mod 104701$
$\equiv \Big(V_{104700}(64,1), U_{104700}(64,1)\Big) \mod 104701$
$\equiv (2,0) \mod 2883155$
so, $\Big(V_{N-\left(\frac{\Delta}{N}\right)}(64,1), U_{N-\left(\frac{\Delta}{N}\right)}(64,1)\Big) \equiv (V_0(64,1), U_0(64,1)) \mod N$, therefore N is a prime.

Note 3.6. The primality test is independent of choice of a and Δ.

Example 3.7. List of $L(\Delta,N)$ for $\left(\frac{\Delta}{N}\right)=1$ and $\left(\frac{\Delta}{N}\right)=-1$ for composite and prime N with respect to $S(N)$ is given in the following tables depicting that the primality test for $N=33$ and 37 is independent of a and Δ.

$L(\Delta,33)$			
$a=12,\Delta=8,(\frac{\Delta}{N})=1$ and $S(N)=12$		$a=18,\Delta=23,(\frac{\Delta}{N})=-1$ and $S(N)=20$	
(V_0,U_0)	(2,0)	(V_0,U_0)	(2,0)
(V_1,U_1)	(12,1)	(V_1,U_1)	(18,1)
(V_2,U_2)	(10,12)	(V_2,U_2)	(25,18)
(V_3,U_3)	(9,11)	(V_3,U_3)	(3,26)
(V_4,U_4)	(32,21)	(V_4,U_4)	(29,21)
(V_5,U_5)	(12,10)	(V_5,U_5)	(24,22)
(V_6,U_6)	(13,0)	(V_6,U_6)	(7,12)
(V_7,U_7)	(12,23)	(V_7,U_7)	(3,29)
(V_8,U_8)	(32,12)	(V_8,U_8)	(14,15)
(V_9,U_9)	(9,22)	(V_9,U_9)	(18,10)
(V_{10},U_{10})	(10,21)	(V_{10},U_{10})	(13,0)
(V_{11},U_{11})	(12,32)	(V_{11},U_{11})	(19,34)
(V_{12},U_{12})	(2,0)	(V_{12},U_{12})	(14,18)
(V_{13},U_{13})	(12,1)	(V_{13},U_{13})	(3,4)
(V_{14},U_{14})	(10,12)	(V_{14},U_{14})	(7,21)
(V_{15},U_{15})	(9,11)	(V_{15},U_{15})	(24,11)
(V_{16},U_{16})	(32,21)	(V_{16},U_{16})	(29,12)
(V_{17},U_{17})	(12,10)	(V_{17},U_{17})	(3,7)
(V_{18},U_{18})	(13,0)	(V_{18},U_{18})	(25,15)
(V_{19},U_{19})	(12,23)	(V_{19},U_{19})	(18,32)
(V_{20},U_{20})	(32,12)	(V_{20},U_{20})	(2,0)
(V_{21},U_{21})	(9,22)	(V_{21},U_{21})	(18,1)
(V_{22},U_{22})	(10,21)	(V_{22},U_{22})	(25,18)
(V_{23},U_{23})	(12,32)	(V_{23},U_{23})	(3,26)
(V_{24},U_{24})	(2,0)	(V_{24},U_{24})	(29,21)
(V_{25},U_{25})	(12,1)	(V_{25},U_{25})	(24,22)
(V_{26},U_{26})	(10,12)	(V_{26},U_{26})	(7,12)
(V_{27},U_{27})	(9,11)	(V_{27},U_{27})	(3,29)
(V_{28},U_{28})	(32,21)	(V_{28},U_{28})	(14,15)
(V_{29},U_{29})	(12,10)	(V_{29},U_{29})	(18,10)
(V_{30},U_{30})	(13,0)	(V_{30},U_{30})	(13,0)
(V_{31},U_{31})	(12,23)	(V_{31},U_{31})	(18,23)
(V_{32},U_{32})	(32,12)	(V_{32},U_{32})	(14,18)
(V_{33},U_{33})	(9,22)	(V_{33},U_{33})	(3,4)

TABLE 1. Values of $L(\Delta,33)$ for $(\frac{\Delta}{33})=1$ and $(\frac{\Delta}{33})=-1$

$L(\Delta,37)$			
$a=17,\Delta=26,(\frac{\Delta}{N})=1$ and $S(N)=36$		$a=11,\Delta=6,(\frac{\Delta}{N})=-1$ and $S(N)=38$	
(V_0,U_0)	(2,0)	(V_0,U_0)	(2,0)
(V_1,U_1)	(17,1)	(V_1,U_1)	(11,1)
(V_2,U_2)	(28,17)	(V_2,U_2)	(8,11)
(V_3,U_3)	(15,29)	(V_3,U_3)	(3,9)
(V_4,U_4)	(5,32)	(V_4,U_4)	(25,14)
(V_5,U_5)	(33,34)	(V_5,U_5)	(13,34)
(V_6,U_6)	(1,28)	(V_6,U_6)	(7,27)
(V_7,U_7)	(21,35)	(V_7,U_7)	(27,4)
(V_8,U_8)	(23,12)	(V_8,U_8)	(31,17)
(V_9,U_9)	(0,21)	(V_9,U_9)	(18,35)
(V_{10},U_{10})	(14,12)	(V_{10},U_{10})	(19,35)
(V_{11},U_{11})	(16,35)	(V_{11},U_{11})	(6,7)
(V_{12},U_{12})	(36,28)	(V_{12},U_{12})	(10,4)
(V_{13},U_{13})	(4,34)	(V_{13},U_{13})	(30,27)
(V_{14},U_{14})	(32,32)	(V_{14},U_{14})	(24,34)
(V_{15},U_{15})	(22,29)	(V_{15},U_{15})	(12,14)
(V_{16},U_{16})	(9,27)	(V_{16},U_{16})	(34,9)
(V_{17},U_{17})	(20,1)	(V_{17},U_{17})	(29,11)
(V_{18},U_{18})	(35,0)	(V_{18},U_{18})	(26,1)
(V_{19},U_{19})	(20,36)	(V_{19},U_{19})	(35,0)
(V_{20},U_{20})	(9,3)	(V_{20},U_{20})	(26,36)
(V_{21},U_{21})	(22,8)	(V_{21},U_{21})	(29,26)
(V_{22},U_{22})	(32,5)	(V_{22},U_{22})	(34,28)
(V_{23},U_{23})	(4,3)	(V_{23},U_{23})	(12,23)
(V_{24},U_{24})	(36,9)	(V_{24},U_{24})	(24,3)
(V_{25},U_{25})	(16,2)	(V_{25},U_{25})	(30,10)
(V_{26},U_{26})	(14,25)	(V_{26},U_{26})	(10,33)
(V_{27},U_{27})	(0,16)	(V_{27},U_{27})	(6,20)
(V_{28},U_{28})	(23,25)	(V_{28},U_{28})	(19,2)
(V_{29},U_{29})	(21,2)	(V_{29},U_{29})	(18,2)
(V_{30},U_{30})	(1,9)	(V_{30},U_{30})	(31,20)
(V_{31},U_{31})	(33,3)	(V_{31},U_{31})	(27,33)
(V_{32},U_{32})	(5,5)	(V_{32},U_{32})	(7,10)
(V_{33},U_{33})	(15,8)	(V_{33},U_{33})	(13,3)
(V_{34},U_{34})	(28,20)	(V_{34},U_{34})	(25,23)
(V_{35},U_{35})	(17,1)	(V_{35},U_{35})	(3,28)
(V_{36},U_{36})	(2,0)	(V_{36},U_{36})	(8,26)
(V_{37},U_{37})	(17,1)	(V_{37},U_{37})	(11,36)
(V_{38},U_{38})	(28,17)	(V_{38},U_{38})	(2,0)

TABLE 2. Values of $L(\Delta,37)$ for $(\frac{\Delta}{37})=1$ and $(\frac{\Delta}{37})=-1$

In table 1 the shaded cells are depicting that the values of $\left(V_{N-(\frac{\Delta}{N})}(a,1), U_{N-(\frac{\Delta}{N})}(a,1)\right)$ are not equal to $\left(V_0(a,1), U_0(a,1)\right)$ for composite $N = 33$, for all the choices of a and Δ and in table 2 the shaded cells are depicting that the values of $\left(V_{N-(\frac{\Delta}{N})}(a,1), U_{N-(\frac{\Delta}{N})}(a,1)\right)$ are equal to $\left(V_0(a,1), U_0(a,1)\right)$ for prime $N = 37$, for all the choices of a and Δ.

4. Conclusion

There are several studies on Lucas sequences and their applications [7] [9]. Primality tests with Lucas sequences by Lucas and Lehmer given in [9] are based on factorization of $N \pm 1$. In this paper we proposed a primality test with pair of Lucas sequences $\left(V_n(a,1), U_n(a,1)\right)$ mod N from the set $L(\Delta, N)$ of $S(N)$ distinct Lucas sequences for $S(N) = \mathrm{LCM}\left[\left\{p_i^{e_i-1}\left(p_i - \left(\frac{\Delta}{p_i}\right)\right)\right\}_{i=1}^{s}\right]$. An algorithm for primality test given, employing the addition chain as in [11] for computation of $\left(V_n(a,1), U_n(a,1)\right)$.

Acknowledgements

The financial support received for this research work under the scheme of Rajiv Gandhi National Fellowship from the University Grants Commission, India, is gratefully acknowledged by the second author.

Conflict of Interests

The author(s) declare that there is no conflict of interests.

References

[1] D.E. Knuth, The art of computer programming, Volume II: Seminumerical Algorithms, Third Edition, Addison-Wesley, Reading, 1998.

[2] D.H. Lehmer, An Extended theory of Lucas's functions, Ann. Math. 31 (1930), 419-448.

[3] L.E. Dickson, History of the theory of numbers, Textually unaltered reprint, Chelsea Publ, New York, 1966.

[4] P. Smith, M. Lennon, LUC: A new public-key system, Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security, Toronto, May 12–14, 1993, 103–117.

[5] P.L. Montgomery, Evaluating recurrences of the form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains, 1992. https://cr.yp.to/bib/1992/montgomery-lucas.pdf

[6] H.C. Williams, A $(P+1)$ Method of factoring, Math. Comput. 39 (1982), 225-234.

[7] H. Riesel, Prime numbers and computer methods for factorization, Birkhäser, Boston, 2012.

[8] J. Brillhart, D.H. Lehmer, J.L. Selfridge, New Primality Criteria and Factorization of $2^m \pm 1$, Math. Comput. 29 (1975), 620-647.

[9] P. Ribenboim, The little book of bigger primes, 2nd ed, Springer, New York, 2004.

[10] P.A. Kameswari, B. Ravitheja, Encryption Using Lucas sequences $L(\Delta, pq)$ With Arithmetic on $L(\Delta, pq)$ via $L(\Delta, p)$ and $L(\Delta, q)$, Int. J. Sci. Res. Math. Stat. Sci. 6 (2019), 178-186.

[11] P.A. Kameswari, B. Ravitheja, Addition Chain for Lucas Sequences with Fast Computation Method, Int. J. Appl. Eng. Res. 13 (2018), 9413-9419.

[12] T.M. Apostol, Introduction to analytic number theory, Springer, New York, 2011.

[13] W. More, Probable Prime Tests Using Lucas Sequences, in: G.E. Bergum, A.N. Philippou, A.F. Horadam (Eds.), Applications of Fibonacci Numbers, Springer Netherlands, Dordrecht, 1998: pp. 283–289.