International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

ADDITION CHAIN FOR LUCAS SEQUENCES WITH FAST COMPUTATION METHOD[1]

P. Anuradha Kameswari[2] and B. Ravitheja
Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India.

Abstract: In this paper using the fast computation method for Lucas sequences proposed by Smith and Lennon [9], we generate a Lucas addition chain for any integer n that yield Lucas sequence $V_n(a,1)$ and show that the algorithm for computation of $V_n(a,1)$ using this Lucas addition chain is based on the formula $V_{x+y}(a,1)$ for $x, y, x-y$ in the Lucas addition chain.

AMS subject classification: 94A60, 11T71.
Keywords: Lucas sequences, addition chain, Lucas addition chain.

INTRODUCTION

LUC public key cryptosystem is a public key cryptosystem based on trapdoor function defined by Lucas sequences. It is proposed by Smith and Lennon as analogue to RSA Cryptosystem. Lucas sequences are recurring relations $V_n(a,1)$, that need numerous computations. There is a need for fast computation methods to reduce the time of computation of Lucas sequences. The algorithm for computation of $V_n(a,1)$ using the existing computation methods are based on three formulas $V_{2n}(a,1)$, $V_{2n-1}(a,1)$, $V_{2n+1}(a,1)$. An addition chain for a positive integer n is a sequence $(n_0, n_1, n_2, ..., n_s)$ with $n_s = n$ and $n_i = n_j + n_k$ for all $1 \leq i \leq s$, for some j, k less than i. An addition chain [7] for an integer n is useful in developing a scheme for the computation methods of $V_n(a,1)$. Knuth in [5] describes an addition chain of n by right-to-left binary method of n for exponentiation with n, in computing x^n.

In this paper we investigate methods to compute Lucas sequences and it is observed that the right-to-left binary method by Knuth gives an addition chain that may not yield the Lucas sequences. We show that the left-to-right binary method generate addition chains that yield the Lucas sequences always. The left-to-right binary method generate addition chain of length $3\lfloor \log n \rfloor - 1$ that yield the Lucas sequences V_n, using the formulas $V_{2n}(a,1)$, $V_{2n+1}(a,1)$ and $V_{2n-1}(a,1)$ and gives an addition chain of length $2\lfloor \log n \rfloor$ that yield the Lucas sequences V_n, using the formulas $V_{2n}(a,1)$, $V_{2n+1}(a,1)$ and $V_{2n-1}(a,1)$. Also generate an addition chain of length $2\lfloor \log n \rfloor - 1$ that yield the Lucas sequences V_n, using only one formula $V_{x+y}(a,1)$. We also give algorithms for generating the above three addition chains.

PRELIMINARIES

Addition Chains [5], [3], [7], [2]

Definition 1. An addition chain for n is a sequence of positive integers $\{1 = a_0, a_1, \ldots, a_r = n\}$ with the property that $a_i = a_j + a_k$, for some $k \leq j < i$ for all $i = 1, 2, 3, \ldots, r$.

Note: If $\{1 = a_0, a_1, \ldots, a_r = n\}$ is an addition chain for n, r is called the length of the addition chain and shortest length is denoted as $l(n)$.

[1] The second author thanks the University Grants Commission, India, for research support under the scheme of Rajiv Ghandi National Fellowship.
[2] corresponding author

International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

Remark 2. $l(n) \leq \lambda(n) + \nu(n) - 1$, where $\lambda(n)$ is the exponent of highest power of 2 and $\nu(n)$ is the number of 1's in the binary representation.

Example 3. The binary representation of $23 = (10111)_2$. An addition chain for 23 is $\{1, 2, 3, 5, 10, 20, 23\}$ and length of the chain is $l(n) = 6. \lambda = 4, \nu = 4$ then $\lambda(n)+\nu(n)-1 = 7$. Therefore $l(n) \leq \lambda(n) + \nu(n) - 1$.

There are several classification of addition chains like star addition chain, Lucas addition chain, differential addition chain, addition-subtraction chain etc.

Remark 4. Not all the addition chains yields the computation of Lucas sequences.

Example 5. For $n = 314$ the addition chain $\{1, 2, 4, 8, 9, 10, 19, 38, 39, 78, 156, 157, 314\}$ cannot yield V_{314} as V_9 computation requires V_3 and V_3 computation is not included as 3 is not in the chain.

Definition 6. A Lucas addition chain for a positive integer n is a sequence $\{0 = a_{-1}, 1 = a_0, a_1, \ldots, a_r = n\}$ such that

1. $a_{-1} = 0, a_0 = 1$ and $a_r = n$
2. $a_i = a_j + a_k$, for some $k \leq j < i$ for all $i = 1, 2, \ldots, r$
3. $a_j - a_k \in a_{-1}, a_0, a_1, \ldots, a_r$.

The length of the chain is r and minimal length of Lucas addition chain is denoted by $L(n)$ [10].

Example 7. A Lucas addition chain for 5096 is $\{0, 1, 2, 3, 4, 7, 8, 14, 28, 56, 112, 168, 224, 392, 616, 1008, 1624, 2240, 2856, 5096\}$ and length of this chain is 19.

When a_{-1} is removed in the Lucas addition chain it becomes an addition chain. So many properties of addition chains are apply to Lucas addition chains. Lucas addition chain is an addition chain, but addition chain is not Lucas addition chain.

Special classes of Lucas addition chains [8]

Definition 8. Let $C = \{0, 1, a_1, a_2, \ldots, a_r\}$ be Lucas addition chain. A doubling step denotes $a_{i+1} = 2a_i$, two consecutive elements.

Definition 9. A Lucas addition chain without doubling step $a_{i+1} = 2a_i$ for $i \geq 1$ is called simple.

Definition 10. A Lucas addition chain is called composite if it is of the form $\{0, 1, a_1, a_2, \ldots, a_r, b_1.a_r, b_2.a_r, \ldots, b_s.a_r\}$ where $\{0, 1, a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_s\}$ are two Lucas addition chains.

Definition 11. A Lucas addition chain $C = \{0, 1, a_1, a_2, \ldots, a_r = n\}$ is called degenerate if one element in the chain is not necessary.

Lucas Sequences and their Properties

In this section we introduce the basic concepts of Lucas Sequences and some properties of Lucas sequences [9], [4], [6], [1], [11].

Definition 12. Let a and b be two integers and 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 $\{V_k(a, b)\}$ *and* $\{U_k(a, b)\}, n \geq 0$ are defined as

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

In Particular, $V_0 = 2$, $V_1 = a$, and $U_0 = 0$ $U_1 = 1$ $V_k(a, b)$ and $U_k(a, b)$ are given by following recurrence sequences

1. $V_k(a, b) = aV_{k-1}(a, b) - bV_{k-2}(a, b)$
2. $U_k(a, b) = aU_{k-1}(a, b) - bU_{k-2}(a, b)$

Lucas sequences Properties: Lucas sequences satisfying the following properties for $V_n(a, b)$.

1. $V_{2n}(a, b) = (V_n(a, b))^2 - 2b^n$
2. $V_{2n-1}(a, b) = V_n(a, b)V_{n-1}(a, b) - ab^{n-1}$
3. $V_{2n+1}(a, b) = aV_n^2(a, b) - bV_n(a, b)V_{n-1}(a, b) - ab^n$.
4. $V_{x+y}(a, b) = V_x(a, b)V_y(a, b) - V_{x-y}(a, b)$
5. $U_n^2(a, 1) = \frac{V_n^2(a,1)-4}{\Delta}$
6. If $m = p_1^{e_1}, p_2^{e_2} \ldots p_r^{e_r}$, such that $(m, \Delta) = 1$ then for $S(m) = lcm \left\{ p_i^{e_i - 1} \left(p_i - (\frac{\Delta}{p_i}) \right) \right\}_{i=1}^{r}$, where $(\frac{\Delta}{p_i})$ is the Legendre's symbol of Δ with respect to the prime p_i,
   $V_{s(m)}(a, b) \equiv 2b^{\frac{k(1-\epsilon)}{2}} \mod m$
   $U_{s(m)}(a, b) \equiv 0 \mod m$

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

International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

1. $V_{2n}(a,1) = (V_n(a,1))^2 - 2$
2. $V_{2n-1}(a,1) = V_n(a,1)V_{n-1}(a,1) - a$
3. $V_{2n+1}(a,1) = aV_n^2(a,1) - V_n(a,1)V_{n-1}(a,1) - a.$
4. $V_{x+y}(a,1) = V_x(a,1)V_y(a,1) - V_{x-y}(a,1)$
5. $U_n^2(a,1) = \frac{V_n^2(a,1)-4}{\Delta}$
6. If $m = p_1^{e_1}, p_2^{e_2} \dots p_r^{e_r}$, such that $(m,\Delta) = 1$ then for $S(m) = lcm\left\{p_i^{e_i-1}\left(p_i - (\frac{\Delta}{p_i})\right)\right\}_{i=1}^{r}$, where $(\frac{\Delta}{p_i})$ is the Legendre's symbol of Δ with respect to the prime p_i,
   $V_{s(m)}(a,1) \equiv V_0(a,1) \mod m$
   $U_{s(m)}(a,1) \equiv U_0(a,1) \mod m$

Notation: For a fixed a, $V_n(a,1)$ and $U_n(a,1)$ are written as just V_n and U_n.

In the study of, cryptosystems with Lucas sequences $(V_n,\ U_n)$, the values of V_n and U_n are considered modulo m where m is such that $(m,\Delta) = 1$ and in view of property(5) we concentrate only on the computations of V_n. In the calculations of values of V_n, it needs enormous computations. The computation of V_n needs two previous values. The initial values are $V_0 = 2$ and $V_1 = a$. The computation starts with V_2 and V_2 requires V_0, V_1, then the computation of V_3 needs V_1 and V_2. This continues and finally computes V_n. The computation of $V_n(a,1)$ is based on three formulas $V_{2n}(a,1)$, $V_{2n-1}(a,1)$, $V_{2n+1}(a,1)$ and $V_{x+y}(a,1)$. There is need of fast computation methods that can reduce the steps involved. An addition chain for n is useful in developing a scheme for computation of V_n and it is also important to trace out the addition chain for n that yield the Lucas sequences V_n.

ADDITION CHAINS FOR LUCAS SEQUENCES WITH FAST COMPUTATION METHOD

There are different methods like Binary method, Factor method etc. and for generating addition chains for any positive integer. If the binary representation of n is $(x_k, x_{k-1} \dots, x_o)_2$ then $n = x_k 2^k + x_{k-1}2^{k-1} + \dots + x_1^2 + x_o$, The right-to-left binary method for n is $n = (2(\dots 2(2x_k + x_{k-1}) + \dots + x_0))$ and the chain for n is given as $(a_1, a_2 \dots, a_r)$ with $a_r = n$, and

$$a_{i-1} = \begin{cases} a_i - 1, \text{ if } a_i \text{ is odd} \\ \frac{a_i}{2}, \text{if } a_i \text{ is even} \end{cases}$$

Remark 13. An addition chain generated by the right-to-left binary method may not yield Lucas sequences using the formulas V_{2n}, V_{2n+1} and V_{2n-1} from V_n, V_{n-1} or V_{x+y} form V_x, V_y and V_{x-y}.

Example 14. For $n = 1103$, the binary representation of 1103 is $(10001001111)_2$ The addition chain $\{1, 2, 4, 8, 16, 17, 34, 68, 136, 137,\ 274, 275, 550, 551,\ 1102, 1103\}$ for 1103 cannot yield V_{1103} as V_{17} computation requires V_7 is not computed as 7 is not in the addition chain. Hence the computation of V_{1103} is not possible from the above addition chain

Therefore the addition chain for 1103 obtained by right-to-left binary method does not yield required Lucas sequence V_{1103}.

Now in the following we prove that addition chains for n generated by left-to-right binary method always yield Lucas sequences V_n. P.J. Smith proposed the computation of Lucas sequences with left-to-right binary method known as fast computation method for Lucas sequences.
For any positive integer n if the binary representation for n is given as $n = x_k 2^k + x_{k-1}2^{k-1} + \dots + x_1^2 + x_o$ for $x_i = 0$ or 1 and $e_t = \sum_{i=0}^{t} x_i 2^{t-i}$, The left-to-right method for n is $n = (2(\dots 2(2e_o + x_o) + \dots + x_k))$. To generate the addition chain we first note the following theorems:

Theorem 15. For any integer $t \geq 0$, if $e_t = \sum_{i=0}^{t} x_i 2^{t-i}$ for $x_i = 0$ or 1 then

$$e_t = \begin{cases} 2e_{t-1} \text{ and if } x_t = 0 \\ 2e_{t-1} + 1 \text{ and if } x_t = 1 \end{cases}$$

Proof.

$$\begin{aligned} Let\ e_t &= \sum_{i=0}^{t} x_i 2^{t-i} \\ &= 2\sum_{i=0}^{t-1} x_i 2^{(t-1)-i} + x_t 2^{t-(t-1)-1} \\ &= 2\sum_{i=0}^{t-1} x_i 2^{(t-1)-i} + x_t \\ &= 2e_{t-1} + x_t \end{aligned}$$

Therefore

$$e_t = \begin{cases} 2e_{t-1} \text{ and if } x_t = 0 \\ 2e_{t-1} + 1 \text{ and if } x_t = 1 \end{cases}$$

International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

■

Remark 16. For any integer $t \geq 0$, if $e_t = \sum_{i=0}^{t} x_i 2^{t-i}$ for $x_i = 0$ or 1 then

$$e_t - 1 = \begin{cases} 2e_{t-1} - 1 \text{ and if } x_t = 0 \\ 2e_{t-1} \text{ and if } x_t = 1 \end{cases}$$

and

$$e_t + 1 = \begin{cases} 2e_{t-1} + 1 \text{ and if } x_t = 0 \\ 2(e_{t-1} + 1) + 1 \text{ and if } x_t = 1 \end{cases}$$

Proof. We have $e_t = 2e_{t-1} + x_t$
$\Rightarrow e_t - 1 = 2e_{t-1} - 1 + x_t$

$$\text{Therefore } e_t - 1 = \begin{cases} 2e_{t-1} - 1 \text{ and if } x_t = 0 \\ 2e_{t-1} \text{ and if } x_t = 1 \end{cases}$$

similarly as $e_t + 1 = 2e_{t-1} + 1 + x_t$, we have

$$e_t + 1 = \begin{cases} 2e_{t-1} + 1 \text{ and if } x_t = 0 \\ 2(e_{t-1} + 1) + 1 \text{ and if } x_t = 1 \end{cases}$$

■

Theorem 17. For any t such that $1 \leq t \leq k, e_t$ is the sum of two of its previous values $e_t - 1$ and e_{t-1}.

Proof. we have $e_0 = 1$ and for any t such that $1 \leq t \leq k$

$$e_t = \begin{cases} 2e_{t-1} \text{ and if } x_t = 0 \\ 2e_{t-1} + 1 \text{ and if } x_t = 1 \end{cases}$$

$$= \begin{cases} e_{t-1} + e_{t-1} \text{ and if } x_t = 0 \\ (e_t - 1) + 1 \text{ and if } x_t = 1 \end{cases}$$

and note $e_t - 1$ is a previous value for e_t and is given as

$$e_t - 1 = \begin{cases} 2e_{t-1} - 1 \text{ and if, } x_t = 0 \\ 2e_{t-1} \text{ and if } x_t = 1 \end{cases}$$

$$= \begin{cases} e_{t-1} + e_{t-1} - 1 \text{ and if, } x_t = 0 \\ e_{t-1} + e_{t-1} \text{ and if } x_t = 1 \end{cases}.$$

Therefore e_t is the sum of two previous values e_{t-1} and $e_t - 1$. ■

Theorem 18. For any t such that $1 \leq t \leq k, e_t$ is the sum of two of its previous values $e_{t-1} + 1$ and $e_{t-2} + 1$.

Proof. we have $e_{-1} = 0$, $e_0 = 1$ and for any t such that $1 \leq t \leq k$

$$e_t = \begin{cases} 2e_{t-1} \text{ and if } x_t = 0 \\ 2e_{t-1} + 1 \text{ and if } x_t = 1 \end{cases}$$

$$= \begin{cases} e_{t-1} + e_{t-1} \text{ and if } x_t = 0 \\ e_{t-1} + (e_{t-1} + 1) \text{ and if } x_t = 1 \end{cases}$$

and for $t \geq 2$ note $e_{t-1} + 1$ is a previous value for e_t and is given as

$$e_{t-1} + 1 = \begin{cases} 2e_{t-2} + 1 \text{ and if } x_t = 0 \\ 2(e_{t-2} + 1) \text{ and if } x_t = 1 \end{cases}$$

$$= \begin{cases} e_{t-2} + e_{t-2} + 1 \text{ and if } x_t = 0 \\ e_{t-2} + (e_{t-2} + 1) + 1 \text{ and if } x_t = 1 \end{cases}$$

Therefore e_t is the sum of two previous values $e_{t-1} + 1$ and $e_{t-2} + 1$. ■

Theorem 19. All the addition chains generated by left-to-right binary method for any positive integer n yield the Lucas sequence $V_n(a, 1)$.

Proof. Let $n = x_k 2^k + x_{k-1} 2^{k-1} + \ldots + x_1^2 + x_o$ for $x_i = 0$ or 1 and $e_t = \sum_{i=0}^{t} x_i 2^{t-i}$ then we have $e_k = n$ and in the left-to-right binary method for $e_k = n = (2(\ldots 2(2x_k + x_{k-1}) + \ldots + x_0))$ we reach e_k only after computing $e_0, e_1, \ldots, e_{k-1}$, therefore any chain for e_k includes e_t for all $t = 0, 1, \ldots, k$. Now note by above theorems as each e_t is sum of two of its previous values $e_t - 1$ and e_{t-1} or e_{t-1} and $e_{t-1} + 1$, any chain that includes $\{e_t, e_t - 1\}$for all t = 1, 2, . . . , k or $\{e_t, e_t + 1\}$for all t = 1, 2, . . . , k yields V_{e_k} as V_{e_t} can be computed from $V_{e_{t-1}}, V_{e_t-1}$ by using the formulas $V_{2n}(a, 1)$, $V_{2n+1}(a, 1)$ and V_{2n-1} or V_{e_t} can be computed from $V_{e_{t-1}}, V_{e_{t-1}+1}$ by using the formula V_{x+y} for x + y = e_t Hence all the addition chains generated by left-to-right binary method for any positive integer n yield the Lucas sequences V_n. ■

Note: The left-to-right binary method for $e_t = n$, generates the addition chains

1. $\{e_0, e_1 - 1, e_1, e_1 + 1, e_2 - 1, e_2, e_2 + 1 \ldots, e_{t-1} - 1, e_{t-1}, e_{t-1} + 1, e_t - 1, e_t\}$ of length $3\lfloor \log n \rfloor - 1$ and this yields the Lucas sequences V_n by using the formulas $V_{2n}(a, 1)$,
$V_{2n+1}(a, 1)$ or V_{2n-1}. This chain is a degenerate

addition chain and we have the two non-degenerate addition chains as follows:

2. The chain $\{e_0, e_1 - 1, e_1, e_2 - 1, e_2, \ldots, e_{t-1} - 1, e_{t-1}, e_t - 1, e_t\}$ is a non-degenerate addition chain from the above addition chain of length $2\lfloor \log n \rfloor$.
3. The chain $\{e_{-1}, e_0, e_1, e_1+1, e_2, e_2+1, \ldots, e_{t-1}, e_{t-1}+1, e_t\}$ is a non-degenerate addition chain from the above addition chain of length $2\lfloor \log n \rfloor - 1$ and note this is a Lucas addition chain.

The non degenerate addition chain given in (1) yield Lucas sequences by using the formulas $V_{2n}(a, 1)$, and $\mathrm{V}_{2n+1}(a, 1)$ and the non degenerate addition chain given in (2) yield the Lucas sequences by using the formula $V_{x+y}(a, 1)$.

Algorithms: The addition chains generated by left-to-right binary method
for $n = x_k 2^k + x_{k-1}2^{k-1} + \ldots + x_1^2 + x_o$ for $x_i = 0$ or 1 and $e_t = \sum_{i=0}^{t} x_i 2^{t-i}$ are given as:

1. $\{e_0, e_1 - 1, e_1, e_1 + 1, \ldots e_{k-1} - 1, e_{k-1}, e_{k-1} + 1, e_k\}$
2. $\{e_0, e_1 - 1, e_1, \ldots e_{k-1} - 1, e_{k-1}, e_k\}$
3. $\{e_{-1}, e_0, e_1, e_1 + 1, \ldots e_{k-1} - 1, e_{k-1}, e_k\}$.

In the following the algorithms for evaluating V_n using the above three addition chains for n are given:

Algorithm 1:
This algorithm evaluates $V_n(a, 1)$ for n is any positive integer.
step 0:(Initialize) Set$N \leftarrow \frac{n}{2^{k-i}}$ where $k = \lfloor \log n \rfloor, i = 0, 1, 2, \ldots, k$
$X \leftarrow 0, Y \leftarrow 1, Z \leftarrow Y + 1$
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 $X \leftarrow 2Y, Y \leftarrow X + 1$ and $Z \leftarrow 2z$
step 3: $[N = n]$, if $N = n$ the algorithm terminates with Y as the answer.
step 4: set$X \leftarrow X + Y, Y \leftarrow 2Y, Z \leftarrow Y + 1$ and return to step 1.
step 5: [initialize $V_n(a, 1)$] set $V_0(a, 1) = 2, V_1(a, 1) = a$
step 6: For i from 0 to k set $V_n \leftarrow V_X, V_Y$ and $\mathrm{V_Z}$
set $n \leftarrow 2n$ and compute $V_{2n}(a, 1) \leftarrow V_n^2(a, 1) - 2$
set $n \leftarrow 2n + 1$ and compute $V_{2n+1}(a, 1) \leftarrow aV_n^2(a, 1) - V_n(a, 1)V_{n-1}(a, 1) - a$
set $n \leftarrow 2n - 1$ and compute $V_{2n-1}(a, 1) \leftarrow V_n(a, 1)V_{n-1}(a, 1) - a$

This algorithm gives an addition chain $\{e_t - 1, e_t, e_{t+1}\}_{t=0}^{k}$ and evaluates V_{e_t} for all $t = 0, 1, \ldots, k$, $\{V_{e_0}, V_{e_1-1}, V_{e_1}, V_{e_1+1} \ldots V_{e_{t-1}-1}, V_{e_{t-1}, V_{e_{t-1}+1}, V_{e_t}}\}$ by using the formulas $V_{2n}(a, 1)$, $V_{2n+1}(a, 1)$ and $\mathrm{V_{2n-1}(a, 1)}$.

Example 20. In the evaluation of $V_n(a, 1)$ for $n = 171, a = 12$ the above algorithm proceeds according to the steps in the following table:

N	X	Y	Z
O	0	1	2
E	1	2	3
O	4	5	6
E	9	10	11
O	20	21	22
E	41	42	43
O	84	85	86
O	170	171	-

This algorithm may be used in the cryptosystem with Lucas sequences, where the computations are performed modulo m for $(m, \Delta) = 1$. The values of Lucas sequences $V_n(a, 1)$ and Lucas sequences $V_n(a, 1) \mod m$ are given in the following table for$m = 209$.

S.No.	$n = 171$	V_n	Values of V_n	$V_n \mod 209$
1	0	V_0	2	2
2	1	V_1	12	12
3	2	V_2	142	142
4	3	V_3	1692	20
5	4	V_4	20162	98
6	5	V_5	240252	111
7	6	V_6	2862862	189
8	9	V_9	4843960812	207
9	10	V_{10}	57721023502	197
10	11	V_{11}	687808321212	67
11	20	V_{20}	3331716554118436344002	142
12	21	V_{21}	39701000273549017124412	20
13	22	V_{22}	473080286728469769148942	98
14	41	V_{41}	1322724798264438300094544854098038484639768 12	111
15	42	V_{42}	1576166422720339132541626393731849621486345742	189
16	43	V_{43}	1878176059281762576049006223937239160937217 2092	67
17	84	V_{84}	2484310049118567112883121793767370478729645 44 26995765222320852424504447471518595744761530562	189
18	85	V_{85}	2960323675125297167935868306901063618201612941 53629122801885683893815757610516603222354322 62	111

International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

S.No.	$n = 171$	V_n	Values of V_n	$V_n \mod 209$
19	86	V_{86}	352754530965917093039421075034360263705463907541655370840030735430128464385468064122063656462	98
20	170	V_{170}	876351626150734597031770304149551820824222055718927446154922251477708095113513590942818516038687157906278451331626728632673293462203885424876421175271581197966671460983645077990436644	197
21	171	V_{171}	1044267589526124132318350887674334654756837362967832717987987511255799414302060427286343040669733793766699639270335720270856195583080053388291486419515957049859644342791512839577032	207

The second column gives the degenerate addition chain of length 21 that is used in the computation of V_{171}.

Algorithm2: This algorithm evaluates $V_n(a,1)$ for n is any positive integer.
step 0:(Initialize) Set$N \leftarrow \frac{n}{2^{k-i}}$ where $k = \lfloor \log n \rfloor, i = 0,1,2,\ldots,k$
$X \leftarrow 0, Y \leftarrow 1$
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 $X \leftarrow 2Y$ and $Y \leftarrow X+1$
step 3: $[N = n]$, if $N = n$ the algorithm terminates with Z as the answer.
step 4: set$X \leftarrow Y + X$, $Y \leftarrow 2Y$ and return to step 1.
step 5: [initialize $V_n(a,1)$] set $V_0(a,1) = 2, V_1(a,1) = a$
step 6: For i from 0 to k set $V_n \leftarrow V_X \; and \; V_Y$
set $n \leftarrow 2n$ and compute $V_{2n}(a,1) \leftarrow V_n^2 - 2$
set $n \leftarrow 2n+1$ and compute $V_{2n+1}(a,1) \leftarrow aV_n^2(a,1) - V_n(a,1)V_{n-1}(a,1) - a$
set $n \leftarrow 2n-1$ and compute $V_{2n-1}(a,1) \leftarrow V_n(a,1)V_{n-1}(a,1) - a$

This algorithm gives non degenerate addition chain $\{e_t - 1, e_t\}_{t=0}^{k}$ and evaluates V_{e_t} for all $t = 0,1,\ldots,k$, $\{V_{e_0}, V_{e_1-1}, V_{e_1}, \ldots V_{e_{t-1}-1}, V_{e_{t-1}}, V_{e_t}\}$ by using the formulas $V_{2n}(a,1), V_{2n-1}(a,1), V_{2n+1}(a,1)$.

Example 21. In the evaluation of $V_n(a,1)$ for $n = 171, a = 12$ with the above algorithm is proceeds according to the steps in the following table:

N	X	Y
O	0	1
E	1	2
O	4	5
E	9	10
O	20	21
E	41	42
O	84	85
O	170	171

This algorithm may be used in the cryptosystem with Lucas sequences where the computations are performed modulo m for $(m, \Delta) = 1$. The values of Lucas sequences$V_n(a,1)$ and Lucas sequences $V_n(a,1) \mod m$ are given in the following table for $m = 209$.

S.No.	$n = 171$	V_n	Values of V_n	$V_n \mod 209$
1	0	V_0	2	2
2	1	V_1	12	12
3	2	V_2	142	142
4	3	V_3	1692	20
5	4	V_4	20162	98
6	5	V_5	240252	111
7	9	V_9	4843960812	207
8	10	V_{10}	57721023502	197
9	20	V_{20}	3331716554118436344002	142
10	21	V_{21}	39701000273549017124412	20
11	41	V_{41}	1322724798264438300094544854098038484639768 12	111
12	42	V_{42}	1576166422720339132541626393731849621486345742	189
13	84	V_{84}	2484310049118567112883121793767370478729645442699576522232085242450444747151859744761530562	189
14	85	V_{85}	2960323675125297167935868306901063618201612941536291228018856838938157576105166032225432262	111
15	170	V_{170}	8763516261507345970317703041495518208242220557189274461549222514777080951135135909428185160386871579062784513316267286326732934622038854248764211752715811979666714609836450779904366 44	197
16	171	V_{171}	1044267589526124132318350887674334654756837362936783271798798751125579941430206042728634304066973379376669963927033572027085619558308005033882914864195159570498596443427915128395770320	207

The second column gives the non degenerate addition chain of length 16 that is used in the computation of V_{171}.

Algorithm 3: This algorithm evaluates $V_n(a,1)$ for n is any positive integer.
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 $V_n(a,1)$] set $V_0(a,1) = 2, V_1(a,1) = a$

International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419

step 6: For i from 0 *to* k set $V_n \leftarrow V_Y$ *and* V_Z
set $n \leftarrow x + y$ and compute $V_{y+z}(a,1) \leftarrow V_y(a,1)V_z(a,1) - V_{y-z}(a,1)$

This algorithm gives Lucas addition chain $\{e_t, e_{t+1}\}_{t=0}^{k}$ and evaluates V_{e_t} for all $t = 0, 1, \ldots, k$, $\{V_{e_0}, V_{e_1}, V_{e_1+1} \ldots V_{e_{t-1}, V_{e_{t-1}+1}, V_{e_t}}\}$ by using the formula $V_{x+y}(a,1)$.

Example 22. In the evaluation of $V_n(a,1)$ for $n = 171, a = 12$ with the above algorithm is proceeds according to the steps in the following table:

N	Y	Z
O	2	2
E	2	3
O	5	6
E	10	11
O	21	22
E	42	43
O	85	86
O	171	-

This algorithm may be used in the cryptosystem with Lucas sequences where the computations are performed modulo m for $(m, \Delta) = 1$. The values of Lucas sequences $V_n(a,1)$ and Lucas sequences $V_n(a,1) \mod m$ are given in the following table for $m = 209$.

S.No.	$n = 171$	V_n	Values of V_n	$V_n \mod 209$
1	0	V_0	2	2
2	1	V_1	12	12
3	2	V_2	142	142
4	3	V_3	1692	20
5	5	V_5	240252	111
6	6	V_6	2862862	189
7	10	V_{10}	57721023502	197
8	11	V_{11}	687808321212	67
9	21	V_{21}	39701000273549017124412	20
10	22	V_{22}	473080286728469769148942	98
11	42	V_{42}	157616642272033913254162639373184962148634 5742	189
12	43	V_{43}	187817605928176257604900622393723916093721 72092	67
13	85	V_{85}	296032367512529716793586830690106361820161 29 415362912280188568389381575761051660322235432262	111
14	86	V_{86}	352754530965917093039421075034360263705463 9 075416553708400307354301284643854680641220636564 62	98
15	171	V_{171}	104426758952612413231835088767433465475683 73 629367832717987987511255799414302060427286343040 669733793766699639270335720270856195583 0860500 533882914864195159570498596443427915128395770 32	207

The second column gives the non degenerate addition chain of length 15 that is used in the computation of V_{171}.

CONCLUSION

An addition chain for a positive integer n is a sequence $\{n_0, n_1, n_2, \ldots, n_s\}$ with $n_s = n$ and $n_i = n_j + n_k$ for all $1 \leq i \leq s$, for some j, k less than i. An addition chain for an integer n is useful in developing a scheme for the computation methods of $V_n(a,1)$. The left-to-right binary method generates addition chains that always yield the Lucas sequences with fast computation method. In this paper we generated addition chain of length $3\lfloor \log n \rfloor - 1$ that yield the Lucas sequences V_n by using the formulas $V_{2n}(a,1)$, $V_{2n+1}(a,1)$ and V_{2n-1}, an addition chain of length $2\lfloor \log n \rfloor$ that yield the Lucas sequences V_n by using the formulas $V_{2n}(a,1)$ and $V_{2n+1}(a,1)$. Also generated Lucas addition chain of length $2\lfloor \log n \rfloor - 1$ that yield the Lucas sequences V_n by using only one formula $V_{x+y}(a,1)$, for x, y such that $x, y, x-y$ are in the Lucas addition chain. This study on addition chains for Lucas sequences gives a cross sectional view in understanding and evaluating similar computations like the point addition on elliptic curves.

REFERENCES

[1] P. Anuradha Kameswari, T. Surendra and B.Ravitheja, *Shank's Baby-step Gaint-step Attack extended to discrete log with Lucas sequences*, IOSR Journal of Mathematics,Vol 12, Issue 1,pp 09-16, 2016.

[2] A. Brauer, *on addition chains*, Bull. Amer. Math. Soc. 45(1939), 736–739.

[3] Zulkarnian Md Ali, M. Othman, M.R.M. Said, M.N. Sulaiman, *Computation of cryptosystem based on Lucas functions using addition chain*, IEEE, (2010), 1082–1086.

[4] L.E. Dickson, *History of the Theory of Numbers*, Chelsea Publishing Company, New York.

[5] D.E. Knuth, LU-*The art of computer programming*, Volume II: Seminumerical Algorithms, Third Edition, Addison-Wesley (1998).

[6] D.H. Lehmer, *An Extendeds theory of Lucas functions*, Annals of Math., 31(1930), pp. 419–448.

[7] P. Downey, B. Loney, and R. Sethi, *Computing sequences with addition chains*, SIAM Journal of Computing 10(3), 638–646(1981).

[8] Daniel Bleinchenbacher, *Efficiency and security of cryptosystems based on Number Theory*, Ph.D thesis, (1964).

[9] P.J. Smith, G.J.J. Lennon, *VLUC: a new public key cryptosystem*, Ninth IFIP Sympoiusm on Computer Science Security, Elsevier Science Publications (1993), 103–117.

[10] Peter L. Montgomery, *evaluating recurrences of the form* $X_{m+n} = f(X_m, X_n, X_{m-n})$ *via Lucas chains*, January, (1992).

[11] Ravitheja. B, *RSA-like cryptosystem based on Lucas sequences*, Dissertation, Andhra University, (2015).