Bull. Math. Soc. Sci. Math. Roumanie
Tome 55(103) No. 1, 2012, 79–93

A generalization of the Lucas addition chains

by
Amadou Tall

Abstract

In this paper, a generalization of Lucas addition chains, where subtraction is allowed, is given. It is called "Lucas addition-subtraction chain" (LASC). LASC gives minimal addition-subtraction chains for infinitely many integers and will also be used to prove the optimality of Lucas addition chains for many cases. One of the main result in the theory of addition-subtraction chains is due to Vogler [2] and this paper gives a way of getting addition-subtraction chains that satisfy his conditions. Moreover, this paper will prove that Lucas addition chains give minimal addition chains for all even integers of Hamming weight 3, like the *binary method*. Finally, we give a theorem to get short (and many times minimal) Lucas addition-subtraction chains.

Key Words: Addition chain, Lucas chain, addition-subtraction chain, Hamming weight.
2010 Mathematics Subject Classification: Primary 11Y55; Secondary 11Y16.

1 Introduction

Lucas addition chains are very used in cryptography and more generally in number theory.
A great interest is given to algorithms over the elliptic curves using Lucas chains. That gives us the idea to *create new addition-subtraction chains* based on Lucas chains to decrease the cost of these algorithms. We notice that subtraction and addition have the same cost in the case of the elliptic curves.

We will remind the problem 3 given by Peter L. Montgomery in [1] that also motivated this work.
Problem The sequence $\{0,\ 1,\ 2,\ 3,\ 4,\ 7,\ 10,\ 11,\ 9\}$ is not a Lucas chain for 9, since it is not ascending. It cannot be rearranged to form a Lucas chain for 9

(although $9 = 7 + 2$, the difference $7 - 2$ is missing). It doesn't represent a way to compute $X_9 = f(X_{10}, X_{-1}(X_1), X_{11})$.
Does there exist a positive integer n such that X_n can be computed using fewer than $\ell_L(n)$ times?

Definition 1. *A sequence* $\{1 = a_0,\ a_1,\ \cdots,\ a_l = n\}$ *is called an addition chain for an integer* n *if and only if: For every integer* $i \in [1..l]$*, there exist* j *and* k *with* $0 \leq j, k < i$ *such that:*

$$a_i = a_j + a_k.$$

Example 2. *The sequence* $\{1,\ 2,\ 3,\ 5,\ 7,\ 9,\ 14,\ 19\}$ *is an addition chain for* 19*.*

This is motivated by the problem of computing x^n knowing x and n. Later comes the notion of addition-subtraction chain motivated by the problem of computing $n * P$ where n is a known integer and P is a known point on an elliptic curve (or any other group where addition and subtraction have the same cost).

Definition 3. *A sequence* $\{1 = a_0,\ a_1,\ \ldots,\ a_l = n\}$ *is called an addition-subtraction chain for an integer* n *if and only if:*

For every integer $i \in [1..l]$*, there exist* j *and* k *with* $0 \leq j, k < i$ *such that*

$$a_i > 0 \ \text{ and } a_i = a_j + a_k \ \text{ or } a_i = a_j - a_k.$$

Example 4. *The sequence* $\{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 31\}$ *is an addition-subtraction chain for* 31*.*

Lucas addition chains are special addition chains introduced by Peter L. Montgomery [1]. They are chains for which the difference $|a_j - a_k|$ is also part of the chain or $a_j = a_k$.

Definition 5. *An addition chain* $c = \{a_0,\ a_1,\ \ldots,\ a_r\}$ *is a Lucas addition chain if and only if:*

$$\text{if } a_i = a_j + a_k \ \text{ for some } i,\ j,\ k \in [1..r], \ \text{ then } a_j = a_k \ \text{ or } |a_j - a_k| \in c.$$

Example 6. *The sequence* $\{1,\ 2,\ 3,\ 5,\ 7,\ 9,\ 14,\ 19\}$ *is a Lucas addition chain for* 19*.*

Notice that, in this example, 14 is obtained by $7 + 7$ and not $9 + 5$.

2 Main results

Here is the definition of the *new* kind of addition-subtraction chains called "Lucas addition-subtraction chains".

Definition 7. *A Lucas addition-subtraction chain for an integer n is a list $c = \{a_0 = 1,\ a_1,\ \ldots,\ a_r = n\}$ such that:*

$$\text{For all } k \in [1..r],\ \exists i,\ j \in \mathbb{N} \mid 0 \leq j, i < k \text{ such that:}$$

$$a_k = \begin{cases} a_i + a_j & \text{and } |a_i - a_j| \in c \cup \{0\}, \\ & \text{or} \\ a_i + 1, & \\ & \text{or} \\ a_i - a_j. & \end{cases} \tag{1}$$

The Lucas addition-subtraction chains are optimal for all integers of Hamming weight 2 thanks to the condition $a_i + 1$. There are other reasons and some of them will be seen with the main theorems of this paper.

Example 8. *1) Let (F_n) be the n^{th} number of Fibonacci, then $\{F_1,\ F_2,\ \ldots,\ F_r\}$ is a Lucas addition-subtraction chain for F_r. Here*

$$F_k = \begin{cases} 1, & \text{for } k = 0, 1, \\ F_{k-1} + F_{k-2}, & \text{for } k \geq 2. \end{cases} \tag{2}$$

We can see that $F_n - F_{n-1} = F_{n-2}$ for all $n > 2$

2) $\{1,\ 2,\ 3,\ 5,\ 10,\ 20,\ 19\}$ is a Lucas addition-subtraction chain for 19.

3) $\{1,\ 2,\ 3,\ 4,\ 7,\ 10,\ 11,\ 9\}$ is a Lucas addition-subtraction chain for 9 and it corresponds to the chain given in Montgomery's problem.
We have:

$$10 = 7 + 3 \text{ where } 4 = 7 - 3,\ 11 = 7 + 4 \text{ where } 3 = 7 - 4,\ 9 = 11 - 2.$$

Lucas addition chains are also Lucas addition-subtraction chains. That give us this *first result.*

Theorem 9. *Let ${\ell_L}^-(n)$ be the minimal length of all Lucas addition-subtraction chains for n and $\ell_L(n)$ the minimal length of all Lucas addition chains for n. We have:*

$${\ell_L}^-(n) \leq \ell_L(n). \tag{3}$$

As we know, a Lucas addition-subtraction chain is an addition-subtraction chain and for that, the factor method must hold for it too.
In this paper, we will also show that there are integers for which the inequality above is strict.

Theorem 10. *Let c_1 and c_2 be Lucas addition-subtraction chains respectively for n_1 and n_2. Then $c_1 \otimes c_2$ is a Lucas addition-subtraction chain for $n_1 \times n_2$ where $\otimes$ is* defined *as follows:*
if $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ and $c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\}$, then

$$c_1 \otimes c_2 = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r \times b_1,\ a_r \times b_2,\ \ldots,\ a_r \times b_l\}.$$

Proof: Let $c = c_1 \otimes c_2 = \{d_0, d_1, \ldots, d_{r+l}\}$. Let $d_i \in c$.
if $i \leq r$, then $d_i = d_j + d_k$ and $d_j - d_k \in c$ because $d_i,\ d_j,\ d_k \in c_1$,
if $r < i \leq r + l$, then

$$d_i = a_r \times b_{i-r} = a_r \times (b_{j-r} + b_{k-r})$$

and we can deduce then that $a_r \times (b_{j-r} - b_{k-r}) \in c$ because

$$b_{j-r} - b_{k-r} \in c_2.$$

□

This important result gives us a corollary that will be used very often in this paper.

Corollary 11. *We have:*

$$\ell_L{}^-(n_1 \times n_2) \leq \ell_L{}^-(n_1) + \ell_L{}^-(n_2). \tag{4}$$

A very important theorem due to Vogler in [2] shows that the Lucas addition-subtraction chain are optimal for infinitely many integers. Following is a theorem introduced by Ching-Te Wang, Chu-Hsing Lin and Chin-Chen Chang [4] that gives an easy way to compute short Lucas addition chains.

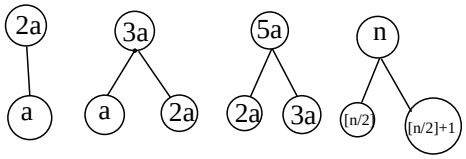
Theorem 12. *Let n be an integer, a Lucas subtree for n is defined as follows:*

(1) *if $n = 2a$, then a Lucas subtree for n is $\{a\}$,*

(2) *if $n = 3a$, then a Lucas subtree for n is $\{a,\ 2a\}$,*

(3) *if $n = 5a$, then a Lucas subtree for n is $\{2a, 3a\}$,*

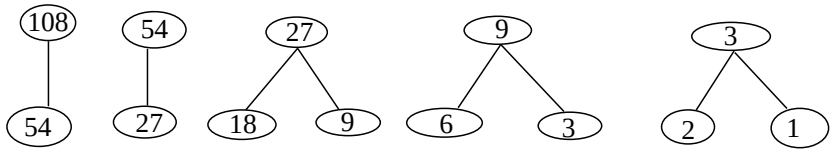
(4) *if n is in none of the three cases below, then a Lucas subtree for n is* $\left\{ \lfloor \frac{n}{2} \rfloor ,\ \lfloor \frac{n}{2} \rfloor + 1 \right\}$.



This method gives sometimes minimal Lucas chains. IT will be used in the proof of the main results of this paper to show the interest of introducing the new kind of "addition-subtraction chains".

This gives us an easy way of computing short (not necesseraly optimal) Lucas addition chain.

Example 13. *For $n = 108$,*



The corresponding Lucas chain for 108 *is then:*

$$\{1,\ 2,\ 3,\ 6,\ 9,\ 18,\ 27,\ 54,\ 108\}.$$

Now, here is a list of results which appears in a theorem of Vogler [2] which is a key tool for this paper:

Theorem 14. *Let $\ell^-(n)$ be the minimal length of all addition-subtraction chains for n, then:*

- $\ell^-(2^k - 2^i) = k + 1$, *for all* $i \leq k - 3$,
- $\ell^-(2^k + 2^i + 2^j) = k + 2$, *for all* $i,\ j,\ k$ *such that* $j < i \leq k - 2$,
- $\ell^-(2^k + 2^{k-1} + 2^j) = k + 2$, *for all* $j \leq k - 4$,
- $\ell^-(2^k - 2^i - 2^j) = k + 2$, *for all* $i,\ j,\ k$ *such that* $j < i \leq k - 4$,

- $\ell^-(2^k - 2^{k-3} - 2^j) = k + 2, \qquad$ *for all* $\; j \leq k - 6,$
- $\ell^-(2^k - 2^{k-3} - 2^j) = k + 1, \qquad$ *where* $\; j = k - 4 \quad$ *or* $\quad j = k - 5.$

This theorem allows us to get the following result which motivated our introduction of the present new kind of addition-subtraction chains.

Main Theorem 1. *Lucas addition-subtraction chains give minimal addition-subtraction chain in the following cases:*

1. $2^k - 2^i, \qquad$ *for all* $\; i \leq k - 3,$
2. $2^k + 2^i + 2^j, \qquad$ *for all* $\; i,\ j,\ k \quad$ *such that* $\; 0 \leq j < i \leq k - 2,$
3. $2^k + 2^{k-1} + 2^j, \qquad$ *for all* $\; 0 \leq j \leq k - 4,$
4. $2^k - 2^i - 2^j, \qquad$ *for all* $\; i,\ j,\ k \;$ *such that* $\; j < i \leq k - 4,$
5. $2^k - 2^{k-3} - 2^j, \qquad$ *for all* $\; j \leq k - 6,$
6. $2^k - 2^{k-3} - 2^j, \qquad$ *where* $\; j = k - 4 \quad$ *or* $\quad j = k - 5.$

Proof: The proof is simple, for the cases 1, 4, 5 and 6 we will give a Lucas addition-subtraction chain for n which is minimal. The cases 2 and 3 will be proved by induction.

1. $n = 2^k - 2^i$ with $i \leq k - 3$. — Let's take
$$c = \{1,\ 2,\ 2^2,\ \ldots,\ 2^i,\ \ldots,\ 2^k,\ 2^k - 2^i\},$$
then we have $\ell^-(n) = {\ell_L}^-(n) = k + 1$.
2. $2^k + 2^i + 2^j$ with $0 < j < i \leq k - 2$.
Let
$$P_k = \{\exists \text{ a Lucas a/s chain for } 2^k + 2^i + 2^j \text{ with } 0 < j < i \leq k - 2 \text{ of length } k + 2\}.$$
Notice that $\{1,\ 2,\ 3,\ 5,\ 6,\ 11,\ 22\}$ is a Lucas addition-subtraction chain for 22, then P_4 is true.
Suppose that P_k is true for any $k < k_0$. Then
$$P_{k_0} = \{\exists \text{ a Lucas a/s chain for } 2^{k_0} + 2^i + 2^j$$

$$\text{with } j < i \leq k_0 - 2 \text{ of length } k_0 + 2\}.$$

or

$$2^{k_0} + 2^i + 2^j = 2(2^{k_0-1} + 2^{i-1} + 2^{j-1}).$$

But, we do know that P_{k_0-1} is true, then using the factor method, we have:

$$\begin{aligned}\ell_L{}^-(2^{k_0} + 2^i + 2^j) &\leq \ell_L{}^-(2(2^{k_0-1} + 2^{i-1} + 2^{j-1})) \\ &\leq ((k_0 - 1) + 2) + 1 \\ &\leq k_0 + 2 = \ell^-(2^{k_0} + 2^i + 2^j),\end{aligned}$$

hence the result.

Second case: $j = 0$

$n = 2^k + 2^i + 1$,

$$c = \{1,\ 2,\ 2^2,\ \ldots,\ 2^{k-i},\ 2^{k-i} + 1,\ \ldots,,\ (2^{k-i} + 1) \cdot 2^i,\ 2^k + 2^i + 1\},$$

we can see that c is a Lucas addition-subtraction chain for n of length $k+2$.

3. $2^k + 2^{k-1} + 2^j$ with $0 < j \leq k - 4$.

Consider the property

$$P_k = \{\exists \text{ a Lucas a/s chain for } 2^k + 2^{k-1} + 2^j$$
$$\text{with } 0 < j \leq k - 4 \text{ of length } k + 2\}.$$

Notice that $\{1,\ 2,\ 3,\ 5,\ 10,\ 15,\ 25,\ 50\}$ is a Lucas addition-subtraction chain for 50, then P_5 is true.

Suppose that P_k is true for any $k < k_0$. We now want to prove

$$P_{k_0} = \{\exists \text{ a Lucas a/s chain for } 2^{k_0} + 2^{k-1} + 2^j$$
$$\text{with } 0 < j \leq k_0 - 4 \text{ of length } k_0 + 2\}$$

or

$$2^{k_0} + 2^i + 2^j = 2(2^{k_0-1} + 2^{k_0-2} + 2^{j-1}).$$

But, we do know that P_{k_0-1} is true, then using the factor method, we have:

$$\begin{aligned}\ell_L{}^-(2^{k_0} + 2^{k_0-1} + 2^j) &\leq \ell_L{}^-(2(2^{k_0-1} + 2^{k_0-2} + 2^{j-1})) \\ &\leq ((k_0 - 1) + 2) + 1 \\ &\leq k_0 + 2 = \ell^-(2^{k_0} + 2^{k_0-1} + 2^j),\end{aligned}$$

hence the result.

Second case: $j = 0$

$n = 2^k + 2^{k-1} + 1$,

$$c = \{1,\ 2,\ 2^2,\ \ldots,\ 2^{k-2},\ 2^{k-1},\ 2^k,\ 2^k + 2^{k-1},\ n\},$$

we can see that c is a Lucas addition-subtraction chain for n of length $k+2$.

4. $n = 2^k - 2^i - 2^j$ with $j < i \leq k-4$. Let's take

$$c = \{1,\ 2,\ 2^2,\ \ldots,\ 2^j,\ \ldots,\ 2^i,\ \ldots,\ 2^k,\ 2^k - 2^i,\ 2^k - 2^i - 2^j\},$$

we have $\ell_L{}^-(n) = k + 2 = \ell^-(n)$.

5. $n = 2^k - 2^{k-3} - 2^j$, with $j \leq k-6$. Let's take

$$c = \{1,\ 2,\ 2^2,\ \ldots,\ 2^j,\ \ldots,\ 2^{k-3},\ \ldots,\ 2^k,\ 2^k - 2^{k-3},\ 2^k - 2^{k-3} - 2^j\},$$

we have $\ell_L{}^-(n) = k + 2 = \ell^-(n)$.

6. $2^k - 2^{k-3} - 2^j$, where $j = k-4$ or $j = k-5$.

(i) $j = k-4$. Then

$$n = 2^k - 2^{k-3} - 2^{k-4} = 2^{k-4}(2^4 - 2 - 1) = 13(2^{k-4}).$$

A chain for 13 of length 5 is $\{1,\ 2,\ 3,\ 6,\ 7,\ 13\}$. Using the factor method, we have:

$$\begin{aligned}\ell_L{}^-(2^k - 2^{k-3} - 2^{k-4}) &= \ell^-(13 \cdot 2^{k-4}) \\ &\leq \ell^-(13) + \ell^-(2^{k-4}) \\ &\leq 5 + (k-4) = k + 1 = \ell^-(2^k - 2^{k-3} - 2^{k-4}).\end{aligned}$$

(ii) the same for $j = k-5$.

□

The proof of this theorem leads to the following *corollary*:

Corollary 15. *We have:*

$$\ell_L(n) = \ell(n) \tag{5}$$

for all n satisfying one of the following conditions:

1. $n = 2^k + 2^i + 2^j$, *with* $i,\ j,\ k$ *such that* $0 < j < i \leq k-2$,

2. $n = 2^k + 2^{k-1} + 2^j$, *with* $j,\ k$ *such that* $0 < j \leq k-4$,

3. $2^k - 2^{k-3} - 2^j$, *where* $j = k-4$ *or* $j = k-5$.

We will give a very important result that shows that Lucas addition chains give minimal addition chains for all even integers of Hamming weight 3.

Main Theorem 2. *For all even n such that $s_2(n) = 3$,*

$$\ell_L(n) = \ell(n).$$

Thanks to the corollary above, we only need to prove that this theorem is true for all integers n such that $n = 2^k + 2^{k-1} + 2^{k-2}$ or $n = 2^k + 2^{k-1} + 2^{k-3}$.

Proof: 1. $n = 2^k + 2^{k-1} + 2^{k-2}$:

$$\begin{aligned} n &= 2^k + 2^{k-1} + 2^{k-2} \\ &= 2^{k-2}(2^2 + 2 + 1) \\ &= 7 * (2^{k-2}). \end{aligned}$$

A Lucas addition chain for 7 is $(1,\ 2,\ 3,\ 4,\ 7)$, then we have a Lucas addition chain for n of
lenght $k + 2$.

2. $n = 2^k + 2^{k-1} + 2^{k-3}$:

$$\begin{aligned} n &= 2^k + 2^{k-1} + 2^{k-3} \\ &= 2^{k-3}(2^3 + 2^2 + 1) \\ &= 13 * (2^{k-3}). \end{aligned}$$

A Lucas addition chain for 13 is $(1,\ 2,\ 3,\ 6,\ 7,\ 13)$, then we have a Lucas addition chain for n of lenght $k + 2$.

□

Remark 16. *The previous theorem may be false when $s_2(n) = 2$. For example, let's take $n = 33 = 2^5 + 1$ then, $\ell(33) = 6$ and $\ell_L(33) = 7$.*

Thanks to the theorem above:

Main Theorem 3. *For all n such that $s_2(n) \leq 3$,*

$$\ell_L{}^-(n) = \ell(n) = \ell^-(n).$$

This theorem means that the Lucas addition-subtraction chains are minimal for all integers of Hamming weight $1,\ 2$, or 3.

3 Conjecture

After testing and taking the minimal addition-subtraction chains for some integers and comparing their length to their minimal addition chain length, we have conjectured that:

Conjecture 17. *There are infinitely many integers n such that:*

$$\ell_L{}^-(n) < \ell(n) \leq \ell_L(n).$$

Here is a list of some integers verifying the conjecture.

1. **Integers satisfying the first part of the theorem**

n	$\ell(n)$	$\ell_L{}^-(n)$
254	11	9
496	11	10
504	11	10
510	11	10
508	12	10
511	12	10
992	12	11
1008	12	11
1020	12	11
1016	13	11
1022	13	11
1023	13	11
1984	13	12
2016	13	12
2040	13	12
2032	14	12
2044	14	12
2046	14	12

2. **Integers n satisfying the second, third and the sixth part of the theorem**
   Thanks to the corollary, we can see that for all these integers:

$$\ell(n) = \ell_L{}^-(n) = \ell_L(n).$$

3. **Integers satisfying the fourth part of the theorem**

n	$\ell(n)$	$\ell_L{}^-(n)$
239	11	10
247	11	10
251	11	10
253	11	10
509	12	11
507	12	11
506	12	11
478	12	11
479	12	11
494	12	11
502	12	11
503	12	11

4. **Integers satisfying the fifth part of the theorem**

n	$\ell(n)$	$\ell_L{}^-(n)$
223	11	10
446	12	11
892	13	12
895	13	12
1784	14	13
1790	14	13
1791	14	13
3568	15	14
3580	15	14
3582	15	14
3583	16	14

4 Algorithms

4.1 Montgomery algorithm for Lucas addition chains

Here is the corresponding algorithm which gives Lucas addition chains of length $2\lfloor \log_2(n) \rfloor + 1$ for any integer n.

Algorithm 1 MontgomeryChains(n)

Require: n : integer
Ensure: a sequence of integers that is a Lucas addition chain for n
1: Let $(d_0 d_1 \cdots d_k)_2$ be the binary expansion of n
2: $a_0 = d_0 = 1$ and $a_1 = a_0 + 1 = 2$
3: **for** i from 2 to $k-1$ **do**
4: $a_i = 2a_{i-1} + d_i$ and add it to the chain
5: add $a_i + 1$ to the chain
6: **end for**
7: add $a_k = 2a_{k-1} + d_k$

We notice that Lucas chains given theorem 12 are shorter.

4.2 New algorithms for Lucas addition-subtraction chains

Here is an algorithm giving Lucas addition-subtraction chain for any integer n .

Algorithm 2 LucasASChains(n)

Require: n : integer
Ensure: a sequence of integers that is a Lucas addition-subtraction chain for n
1: Let $(d_0 d_1 \cdots d_k)_2$ be the non-ajacent form of n
2: $a_0 = d_0 = 1$ and $a_1 = a_0 + 1 = 2$
3: **for** i from 2 to $k-1$ **do**
4: $a_i = 2a_{i-1} + d_i$ and add it to the chain
5: add $a_i + 1$ to the chain
6: **end for**
7: add $a_k = 2a_{k-1} + d_k$

We can see that this is just the Montgomery algorithm using the non adjacent form, and that we do not gain in the length of the chains.
This leads to this *very important question:*
Question 2: Can we have a good algorithm that gives minimal chains for at least all integers of the theorem?

The answer is *yes*. We give an algorithm that satisfy these criteria with the following theorem.

Theorem 18. *Let n be an integer. A Lucas addition-subtraction subtree for n is obtained this way:*

1. *if $n = 2a$ for some a then n is obtained by doubling $\{a\}$,*
2. *if $n = 2^k - 1$ for some k then n is obtained by $\{2^k\}$,*
3. *if not, then n is obtained by $\{\lfloor n/2 \rfloor,\ \lfloor n/2 \rfloor + 1\}$.*

Here is a source code, implemented in Pari-GP that gives short (minimal for at least all the integers of the theorem) Lucas addition-subtraction chains.

```
LASC(n)=
{
local(chaine);
chaine=n;

while(n>=2,
if(n==(2^#binary(n)-1)&& n>3,
n=n+1;
chaine=concat(chaine,n);
,
if(n%2==0,
chaine=concat(chaine,n/2);n=n/2;
,

a=floor(n/2);
b=a+1;
if(a%2==0||b==2,
n=a;
                chaine=concat(chaine,b);
    chaine=concat(chaine,a);
,
n=b;
                chaine=concat(chaine,a);
    chaine=concat(chaine,b);
);

);
);
);
print("The length of the chain is  "(#chaine-1));
print(chaine);
```

```
return(chaine);
}
```

And here are the chains obtained for some of the integers that are in the list below.

```
? LASC(254)
The length of the chain is  9
[254, 127, 128, 64, 32, 16, 8, 4, 2, 1]

? LASC(1984)
The length of the chain is  12
[1984, 992, 496, 248, 124, 62, 31, 32, 16, 8, 4, 2, 1]

? LASC(2046)
The length of the chain is  12
[2046, 1023, 1024, 512, 256, 128, 64, 32, 16, 8, 4, 2, 1]

? LASC(247)
The length of the chain is  10
[247, 123, 124, 62, 31, 32, 16, 8, 4, 2, 1]

? LASC(507)
The length of the chain is  11
[507, 253, 254, 127, 128, 64, 32, 16, 8, 4, 2, 1]


? LASC(1790)
The length of the chain is  13
[1790, 895, 447, 448, 224, 112, 56, 28, 14, 7, 8, 4, 2, 1]


? LASC(3583)
The length of the chain is  14
[3583, 1791, 1792, 896, 448, 224, 112, 56, 28, 14, 7, 8, 4, 2, 1]
```

5 Conclusion

Lucas addition-subtraction chains give shorter chains than the Lucas chains for so many integers that one can think about using them for the elliptic curve cryptosystem (or based algorithms) that uses the Lucas chains. Also, it can be used in any algorithms based on elliptic curve. One can think about redoing the work of [3] done using the binary method with the Lucas chains and see what it

will imply.
One can also think about using the Lucas addition-subtraction chains on the ECM and see if it help reducing the computational cost of the "step 1".

6 Acknowledgements

This work is done under the supervision of Professor Maurice Mignotte. This work was finalize during my visit to IRMA Strasbourg, thanks to the Ibni Prize. The author would like to thank Dustin Moody for his precious help.

References

[1] Peter L. Montgomer, Evaluating recurrences of form $X_{m+n} = f(X_m,\ X_n,\ X_{m-n})$ via Lucas Chains, January 1992.

[2] Hugo Volger, Some results on addition-subtraction chains, Information Processing Letters Volume 20, Issue 3, 8 April 1985, Pages 155-160.

[3] Franqis Morrain, Jorge Olivos, Speeding up the computation on an elliptic curve using addition-subtaction chains, Informatique théorique et applications, tome 24, no. 6 (1990), p. 531, 543.

[4] Ching-Te Wang, Chu-Hsing Lin and Chin-Chen Chang, A method for computing Lucas sequences, Computers and Mathematics with Applications 38 (1999) 187-196.

[5] Maurice MIGNOTTE,Amadou TALL, A note on addition chains, International Journal of Algebra, Vol. 5, 2011, no. 6, 269 - 274.

[6] D.M. Gordon, A survey of fast exponentiation methods Journal of Algorithms, **27** (1) (1998) 129-146.

Received: 03.08.2011,
Accepted: 04.12.2011.

African Institute for Mathematical Sciences
Senegal
E-mail: amadou.tall@aims-senegal.org