Applied Mathematics, 2016, 7, 70-76
Published Online January 2016 in SciRes. http://www.scirp.org/journal/am
http://dx.doi.org/10.4236/am.2016.71006

Scholz's First Conjecture: A Brief Demonstration

José M. Sautto[1], Agustín Santiago[2], Carlos N. Bouza[3], Verónica Campos[1]

[1]Campus Costa Chica, Universidad Autónoma de Guerrero, Guerrero, México
[2]Facultad de Matemáticas, Universidad Autónoma de Guerrero, Acapulco, México
[3]Facultad de Matemática y Computación, Universidad de la Habana, Ciudad de La Habana, Cuba
Email: sautto1128@yahoo.com.mx, asantiago@uagro.mx, bouza@matcom.uh.cu

Received 5 December 2015; accepted 22 January 2016; published 25 January 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

This paper presents a brief demonstration of Schulz's first conjecture, which sets the upper and lower limits on the length of the shortest chain of addition. Two methods of the upper limit are demonstrated; the second one is based on the algorithm of one of the most popular methods for obtaining addition chains of a number, known as the binary method.

Keywords

Addition Chain, Exponentiation, Short Chain, Scholz's Conjecture, Binary Method

1. Introduction

With the development of the Internet and adding chain applications in the development of cryptography—which permits safe handling of data over the Internet—the theme began with the publication in 1937 of Arnold Scholz's paper [1], which defines a minimal addition chain, along with his three famous conjectures. In 1939 [2], Alfred Brauer gave a strong impetus to this issue, gaining importance in this area. During the last decades of the last century deterministic methods flourished. The most popular were the binary method and the window method [3]-[5]. Heuristic methods began to emerge in the 70s and toward the end of the century, began to dominate in the literature [6] [7]. This is the second paper we write on the theme [8] and in both present simple demonstrations, the third and first conjecture, we use deterministic algorithms. Our intention is to build a framework for the development of intelligent methods for generating addition chains.

2. Basic Definitions

The first conjecture presented by Scholz was: $m+1 \le l(n) \le 2m$; for the n which satisfy:

How to cite this paper: Sautto, J.M., Santiago, A., Bouza, C.N. and Campos, V. (2016) Scholz's First Conjecture: A Brief Demonstration. *Applied Mathematics*, **7**, 70-76. http://dx.doi.org/10.4236/am.2016.71006

$$2^m + 1 \le n \le 2^{m+1};\ m \ge 1. \tag{1}$$

In addition to setting maximum and lower bounds for the minimum length of addition chains, this conjecture induces a partition of our study space, in this case the natural numbers. The bounded sets defined by Schulz $2^m + 1 \le n \le 2^{m+1}$ for $m \ge 1$, exclude the numbers 1 and 2. For $m = 1$ the possible values of *n* correspond to the set $\{3, 4\}$; from there, if we increase *m* by one, the possible values of *n* are doubled. The point of this partition is that we can delimit our study space, in this case the natural numbers, to set general properties on addition chains.

We will begin our discussion with the following definitions:

Definition 2.1. Let $S_e = \{a_i\}$ be a finite sequence of natural numbers. We will call it an addition chain of a natural number if it satisfies:

I. $1 = a_0 < a_1 < \cdots < a_r = e$.

II. $a_i = a_j + a_k$, for some (j, k) and for each step *i*, $0 \le k \le j < i$, with $0 < i \le r$.

Definition 2.2. Let $S_e = \{a_i\} = \{1 = a_0, a_1 = 2, \cdots, a_r = e\}$ be an addition chain of a number *e*, the highest index of the sequence *r* is called length of the chain S_e, and it is denoted by $l(S_e)$.

Definition 2.3. The minimum length of all addition chains of a natural number *e* is denoted by $l(e)$, that is:

$$l(e) = \min\{l(S_e) \mid S_e \text{ is an addition chain of } e\}.$$

Definition 2.4. Let us consider the family G_i of natural subsets defined by:

$$G_i = \begin{cases} i = 0, G_0 = 1; \\ i \ge 1, G_i = \{n \in N \mid 2^{i-1} + 1 \le n \le 2^i\}. \end{cases}$$

The set G_i will be called *i*th generation of natural numbers.

Definition 2.5. For every *i*th generation with $i \ge 2$, we will define:

$$G_i^p = \{x \mid x = 2y; y \in G_{i-1}\} \text{ even numbers of } G_i.$$

$$G_i^m = \{x \mid x = 2y - 1; y \in G_{i-1}\} \text{ odd numbers of } G_i.$$

Definition 2.6. For every $n \in N$, we will define the *n*th dominant chain as:

$$S_{2^n}^n = \{a_i\} \text{ defined by } a_i = 2^i, 0 \le i \le n.$$

3. Important Properties

Proposition 3.1. The dominant chains are of maximum growth. That is to say, for every *x* if $S_x = \{b_i\} \ne S_{2^r}^r = \{a_i\}$ with $l(S_x) = r$; then $x < 2^r$.

Proof. As $\{b_i\} \ne \{a_i\}$ then there exists $1 < j \le r$ (since the first two values of any addition chain are the same) in such a way that $b_j \ne a_j$ as $a_j = 2 * a_{j-1} > a_{j-1} + a_k = b_j$ with $k < j - 1$, as $b_{j-1} = a_{j-1}$; $b_j = b_{j-1} + b_k$; $k < j - 1$ because if the first term of the sum had an index less than $j - 1$, at most it could be b_{j-1}, which would imply that the sequence would not be an addition chain because it does not strictly increase, and as $k < j - 1$ and the sequence strictly increases we have that: $b_j < a_j$. If it was the last term of the sequence then the inequality is true, and if it was not the last term from there $b_{j+i} \ll a_{j+i}$, for $i = 1, \cdots, r - j$ at each increment of the difference between the terms of the sequences increases. Hence $x = b_r < a_r = 2^r$.

Proposition 3.2. Dominant chains are addition chains defined on the numbers of the form $e = 2^n$, of length $l(S_{2^n}^n) = n$.

***Proof*.** By definition $S_e^n = \{a_i\}$ defined by $a_i = 2^i, 0 \le i \le n$ from where:

$$S_{2^n}^n = \{a_0 = 2^0 = 1, a_1 = 2^1 = 2, \cdots, a_n = 2^n\}.$$

From the definition of dominant chain: $a_0 = 2^0 = 1$, from where its first element is 1and the last one is $a_n = 2^n$, in addition for every *i* the following is true: $a_{i-1} = 2^{i-1} < 2^i = a_i$ from where $0 < i < n$, therefore it increases and ends in $a_n = 2^n$, which proves the first property of addition chain.

Let us have a look at the second property, that is:

$$a_i = 2^i = 2^{i-1} + 2^{i-1} = a_{j=i-1} + a_{k=i-1},$$

clearly $0 \le k \le j < i$, with $0 < i \le r$, so it satisfies the second property and therefore they are addition chains.

Finally, since $a_n = 2^n$ is an addition chain of 2^n, the Proposition (3.1) assures that any other chain of that length is of a number $x < 2^n$, which implies that it is the only chain of length *n de* 2^n. This proves that $l\left(S_{2^n}^n\right) = n = l\left(2^n\right)$.

To underline this last fact we will state the following in this corollary:

Corollary 3.3. The numbers of the form $e = 2^n$ have $S_{2^n}^n$ as minimum length chain, whose length is $l\left(S_{2^n}^n\right) = n$. This chain is unique.

Proof. The Proposition (3.2) assures that $S_{2^n}^n$ is addition chain of 2^n, and the Proposition (3.1) states that any other chain of that length different from $S_{2^n}^n$ makes $x < 2^n$ true, which guarantees the uniqueness of $S_{2^n}^n$.

Another important result:

Corollary 3.4. If $l(x) = r$ then $x \le 2^r$.

Proof. If $l(x) = r$ implies that there exists S_x in such a way that $l(S_x) = r$ if $S_x \ne S_{2^r}^r$ by the Proposition (3.1), we have that $x < 2^r$ and if $S_x = S_{2^r}^r$ by the Proposition (3.2) we know that $x = 2^r$ from where $x \le 2^r$.

Proposition 3.5. If $x \in G_i$, then $l(x) \ge i$.

Proof. If we assume that (3.5) is not true, then there exists $x \in G_i$ in such a way that $l(x) \le i - 1 < i$; from where if $l(x) = i - 1$ there exists S_x in such a way that $l(S_x) = i - 1$. The Corollary (3.4) assures that $x \le 2^{i-1}$, and this implies that $x \notin G_i$, which contradicts our hypothesis, from which we conclude that if $x \in G_i$ then $l(x) \ge i$.

Proposition 3.6. If $z \in G_i^p$, then $l(z) \le l(x) + 1$ for any $x \in G_{i-1}$.

Proof. As $z \in G_i^p$, then there exists $x \in G_{i-1}$ in such a way that $z = 2x$. Let $S_x = \{a_0 = 1, \cdots, a_r = x\}$ be a minimum length chain of *x*, from this one we will build an addition chain of *z*. $S_z = \{a_0 = 1, \cdots, a_r = x, a_{r+1} = z = 2x\}$, it is clearly an addition chain of *z*, of length $l(x) + 1$, which proves that $l(z) \le l(x) + 1$.

Proposition 3.7. If $x \in G_i^p$ and $x < 2^i$, then $z = x + 1 \in G_i^n$ and $l(z) \le l(x) + 1$.

Proof. As *x* is an even number and lower than the upper limit of G_i, that is $x < 2^i$; then $x \le 2^i - 2$ from where $z = x + 1 \le 2^i - 2 + 1 = 2^i - 1 \to z \in G_i^n$, which guarantees that $z \in G_i^n$.

Let $S_x = \{a_i\}$ be a minimum length chain $l(x)$, then its first term is 1 and its last term is *x*, from where if we add as the last term $z = x + 1$ to that sequence, now this sequence is an addition chain of *z*, that is: $S_z = \{a_i\} \cup \{x + 1 = z\}$, it is an addition chain of *Z* of length $l(x) + 1$, from where $l(z) \le l(x) + 1$.

Proposition 3.8. If $z \in G_i^n$, then $l(z) \le l(x) + 2$ for any $x \in G_{i-1}$.

Proof. By definition $G_i^n = \{x \mid x = 2y - 1; \in G_{i-1}\}$, odd numbers G_i, from where: $G_i^n = \left\{2^{i-1} + 1, 2^{i-1} + 3, \cdots, 2^{i-1}\right\}$, from these numbers only the first $z = 2^{n-1} + 1$ does not have an even numbered predecessor in G_i, an addition chain of this number is given by $S_z = S_{2^{n-1}}^{n-1} \cup \left\{2^{i-1} + 1\right\}$, whose length is $l(S_z) = n - 1 + 1 = n$, this length is minimum since if there exists another chain of *z* with a length lower than *n* according to the Corollary (3.4), we have that $z \le 2^{n-1}$ and clearly $z > 2^{n-1}$, from where we conclude that it is minimum, that is $l\left(z = 2^{i-1} + 1\right) = n$. For the rest of the elements of G_i^n, according to the Proposition (3.7), there exists a $y \in G_i^p$ in such a way that $l(z) \le l(y) + 1$. Now, the Proposition (3.6) assures $\exists x \in G_{i-1}$ in such a way that $l(y) \le l(x) + 1$, from where $l(z) \le l(y) + 1 \le l(x) + 1 + 1 = l(x) + 2$ for any $x \in G_{i-1}$.

Proposition 3.9. For every $i \ge 2$; $\wp = \left\{G_i^p, G_i^n\right\}$ is a partition of G_i.

Proof. We have to demonstrate that for every $i \ge 2$ we will always have:

a) $G_i = G_i^p \cup G_i^n$.

b) $G_i^p \cap G_i^n = \varnothing$.

For $i = 2$ we have $G_{2-1} = G_1 = \{2\}$ according to the definition of G_i from where $G_2^p = \{4\}$ and $G_i^n = \{3\}$ and $G_2 = \left\{n \in N \mid 2^{2-1} + 1 = 2^1 + 1 = 3 \le n \le 2^2 = 4\right\} = \{3, 4\}$, from where we clearly see that a) and b) are true.

Proposition 3.10. The number 3 only has an addition chain of length equal to 2.

Proof. The only addition chain of the number 3 is: $S_3 = \{a_0 = 1, a_1 = 2, a_2 = 3\}$, we will demonstrate that it is an addition chain and that it is unique.

It is an addition chain since it begins with 1, it has increasing terms and it ends with the number 3, from where it satisfies the property I of the definition of the chain addition.

Clearly $a_1 = a_0 + a_0 = 1 + 1 = 2$ and $a_2 = a_1 + a_0 = 2 + 1 = 3$, which proves part II of the definition $a_k = a_j + a_i; 0 \le i \le j < k$.

We will demonstrate now that it is unique. Let us suppose that it is not, then there exists $S_3^+ \ne S_3$, which is chain of the number 3. Let $S_3^+ = \{b_0 = 1, b_1 = 2, \cdots, b_p = 3\}$ be an addition chain different from S_3, the definition of chain forces $b_0 = 1$ and the property II when $k = 1$, and $0 \le i \le j < k = 1$, the only possible value of *i* and *j* is zero, from where $b_1 = 2$. For b_2 the possible values of (i, j) are three, which are presented in **Table 1**.

The only possible value for b_2 is 3, according to the definition of addition chain it would be the last term of the sequence. However, it is equal to S_3, which contradicts the fact that S_3^+ is different from S_3, from where we conclude that it is unique. As $b_2 = 3; l(3) = 2$.

4. Demonstration of Scholz's First Conjecture

In terms of the given definitions, Scholz's first conjecture is equivalent to:

$m + 1 \le l(n) \le 2m$; for the *n* which satisfy: $2^m + 1 \le n \le 2^{m+1}; m \ge 1$.

If we make a change of variables $i = m + 1$ we will have:

$i \le l(n) \le 2i - 2$ for the *n* which satisfy: $2^{i-1} + 1 \le n \le 2^i; i \ge 2$.

As $G_i = \{n \in N \mid 2^{i-1} + 1 \le n \le 2^i\}$ the conjecture is now:

$i \le l(n) \le 2i - 2$; for the $n \in G_i, i \ge 2$.

The new formulation would be:

Theorem 4.1. If $x \in G_i$, then $i \le l(x) \le 2i - 2$; for every $i \ge 2$.

Proof. The Proposition (3.5) guarantees the first part of the inequality, that is: if $x \in G_i$, then $i \le l(x)$.

We will now demonstrate the second part of the inequality.

The Proposition (3.6) guarantees us that if $z \in G_i^p$, then $l(z) \le l(x) + 1$, for any $x \in G_{i-1}$. The Proposition (3.8) guarantees us that if $z \in G_i^p$, then $l(z) \le l(x) + 2$, for any $x \in G_{i-1}$. The Proposition (3.9) proves that $G_i = G_i^p \cup G_i^n$, from where if k_{i-1} is another upper bound of $\{l(x) \mid x \in G_{i-1}\}$, we have that for every *i*, $k_i \le k_{i-1} + 2$ is true, it is the upper bound of $\{l(x) \mid x \in G_i\}$, that is $l(x) \le k_{i-1} + 2$; for every $x \in G_i$.

Let k_2 be the upper bound of G_2; then

$$k_i = k_2 + 2(i - 2); i \ge 2. \tag{2}$$

As $G_2 = \{3, 4\}$ and $4 = 2^2$, its minimum addition chain is $l(4 = 2^2) = 2$, according to the Corollary (3.3) and the 3 according to the Proposition (3.10) $l(3) = 2$, from where the upper bound of G_2 is 2. This is $k_2 = 2$, and substituting this value of k_2 in (2) we will have:

$$k_i = k_2 + 2(i - 2) = 2 + 2(i - 2) = 2(i - 2 + 1) = 2(i - 1) = 2i - 2,$$

which proves that if $x \in G_i$, then $l(x) \le 2i - 2$; for $i \ge 2$. This demonstrates the second part of the inequality.

An alternative way of deriving the upper bound established in Schulz's first conjecture is obtainable by using the binary analysis methods for constructing the addition chains [3]. It is expressed in the following algorithm.

Table 1. Sequence of addition chain for possible values of (i, j).

i	*j*	$b_i + b_j = b_2$	**Comment**
0	0	$b_0 + b_0 = 1 + 1 = 2$	The sequence would not be strictly increasing
0	1	$b_0 + b_1 = 1 + 2 = 3$	Possible value
1	1	$b_1 + b_1 = 2 + 2 = 4$	The last value must be 3, there can't be higher numbers

5. Binary Method

```
Input: an integer: $e=(e_0,\cdots,e_{m-2},e_m)$
Output: Addition chain $U=\{1,2,\cdots,e\}$
Start:
1: $x=1;U=\{1\}$
for $i$=1 to $m$
    $x=2*x$
    $U=U\bigcup\{x\}$
  If $e_i==1$ then: $x=x+1\wedge U=U\bigcup\{x\}$
End
```

Therefore the length of the obtained chain depends on the length of the binary expression of the number and the quantity of ones that it has, as for each one, without taking into account the first one, is added another number to the output chain; for example see **Table 2**.

Table 2. Algorithm fot the binary method.

Description	Example
Input: integer: *e*	77
Write $e=(e_0,e_1,\cdots,e_m)$	77 = 1001101
Output: Addition Chain *U*	$U=\{1,2,\cdots,e\}$
$x=1;U=\{1\};i=1$	$x=1$; $U=\{1\};i=1$
While $i<m$ $x=2*x$; $U=U\bigcup\{x\}$; $i=i+1$	While $i<7$ $e_1=0$; $x=2*1=2$; $U=\{1,2\}$; $i=1+1=2$
As $i<m$ $x=2*x$; $U=U\bigcup\{x\}$; $i=i+1$	As $i=2<7$ $e_2=0$; $x=2*2=4$; $U=\{1,2,4\}$; $i=3$
Repeat: Step $4:x=2*x$ Add *x* at the end of the list *U* As $e_i==1$ than $x=x+1$ $U=U\bigcup\{x\}$; $i=i+1$	As $i=3<7$ $x=4*2=8;U=\{1,2,4,8\}$ As e_3 is $=1$; $x=8+1=9$ $U=\{1,2,4,8,9\}$; $i=3+1=4$
As $i<m;x=2*x$ Add *x* at the end of the list *U* If $e_i==1$ then $x=x+1$ Add *x* the list of *U*; $i=i+1$	As $i=4<7$ $e_4=1$; $x=9*2=18$; $U=\{1,2,4,8,9,18\}$ As e_4 is $=1$; $x=18+1=19$ and $U=\{1,2,4,8,9,18,19\}$; $i=4+1=5$
As $i<m$; $x=2*x$ Add *x* at the end of the list *U*; $i=i+1$	As $i=5<7$; $e_5=0$; $x=19*2=38$ $U=\{1,2,4,8,9,18,19,38\};i=5+1=6$
e_i's equal to one.	As $i=6<7$ $e_6=1$; $x=38*2=76$ $U=\{1,2,4,8,9,18,19,38,76\}$ As e_6 is $=1$; $x=76+1=77$ $U=\{1,2,4,8,9,18,19,38,76,77\};i=6+1=7$
As $i=m\not<m$ stop the output is: *U*	As $i=7\not<7$ stop and the output is: $U=\{1,2,4,8,9,18,19,38,76,77\}$

The output chain has the same number of elements that the number of bytes of the expression, in base 2, of the input number *e*, plus the quantity of ones of the binary expression, minus one, which is at the beginning of the binary expression. In this case: 77 = 1001101, the length of the binary expression is of 7 bytes and the number of ones minus the first one is 3. Hence the length of the output chain is 7 + 3 = 10; *U* = {1, 2, 4, 8, 9, 18, 19, 38, 76, 77}. Therefore the length of the addition chain is 9. This fact is expressed in the next proposition, as follows:

***Proposition* 5.1.** The length of the addition chain generated by the binary method of a number *e* is equal to the last sub-index of the binary expression $e = e_0, e_1, \cdots, e_m$, plus the quantity of ones it has, minus one. That is $m + p - 1$, where *p* is the number of ones that the binary expression *e* has.

***Proof*:** Take $e \in \mathbb{N}$; and its binary expression $e = e_0, e_1, \cdots, e_m$. The algorithm starts with a one and eliminates e_0, it is equal to one, and adds it to the addition chain *U*. For each element from e_1 to e_m that is for *m* elements we have added one more to *U*. Then $U = \{u_0, u_1, \cdots, u_m, u_{m+1}, u_{m+2}, \cdots, u_{m+p-1}\}$ has *m* plus $p - 1$, where *p* is quantifies the number of e_i's equal to one. Therefore, according to Definition 2.2 the length of the addition chain is equal to the last sub-index of the chain, in this case $m + p - 1$. As *m* is the last sub-index of the binary expression, and *p* is the number of ones in the expression. Note that we have that
$U = \{u_0, u_1, \cdots, u_m, \cdots, u_{m+p-1} = e\}$. Then from Definition 2.2, we derive that the length of the chain is the last of the sub-indexes, which is $m + p - 1$.

Q.E.D.

Note that the numbers belonging to the generation G_i, for $i > 2$ have has binary expression with length equal to *n*, minus the superior limit, which has $n + 1$ elements with 1 and *n* with zeros, which corresponds to the superior limit of the generation, as it is observed in the following **Table 3**.

Note that the upper bound of the generation is given by 2^n; its minimum addition chain is *n*, because of Proposition 3.2. Then we do not take *i* into account. The maximum expected length of a chain, belonging to the generation *n*, is given by the number whose binary expression is equal to *n*, corresponding to $e = 2^n - 1$, one less than the superior limit, with binary expression: $2^n - 1 = (e_0 = 1, e_1 = 1, \cdots, e_{n-1} = 1)$. The obtained addition chain will have *n* − 1 components, as the number of ones of the expression is *n*, where the addition chain is given by $U = \{u_0 = 1, u_1 = 2, u_3 = 3, \cdots, u_{2n-2} = e\}$. Hence, the length of this chain is $2n - 2$, which is the longest generated by the method in that generation. Then is proved the following result:

***Corollary* 5.1.** The length of the longest addition chain generated by the binary method in G_i corresponds to $e = 2^i - 1$ that has as length $l(2^i - 1) = 2i - 2$.

Table 3. Example binary sequence.

Generation	Limits of the partition		Limits of the partition expressed in binary		Size of the partition
G_0	1	1	1	1	1
G_1	2	2	10	10	1
G_2	3	4	11	100	2
G_3	5	8	101	1000	4
G_4	9	16	1001	10000	8
G_5	17	32	10001	100000	16
G_6	33	64	100001	1000000	32
G_7	65	128	1000001	10000000	64
G_8	129	256	10000001	100000000	128
G_9	257	512	100000001	1000000000	256
G_{10}	513	1024	1000000001	10000000000	512
			….		
G_n	$2^{i-1}+1$	2^i	$1, 0, \cdots, 0, 1$	$1, 0, \cdots, 0$	2^{n-1}

***Theorem* 5.1.** The binary method for the generation of addition chains proofs the right hand side of the First Schulz's Conjecture that is:

If $n \in G_i$, then $l(n) \leq 2i - 2$; for every $i \geq 2$.

***Proof*.** If $n \in G_i$ then n has the binary expression $n = (e_0 = 1, e_1, e_2, \cdots, e_{i-1})$, where at least a component is different form e_0 is equal to 1, because if all are zeros, it will be the superior limit of G_{i-1}. The generation i has $i-1$ elements whose binary expression has two ones, for these elements, according to Proposition 5.1, its generated addition chain is of length equal to i, as we add only another value and the first value of the generated chain has as sub-index $i = i - 1 + 1$. The rest will have longer chains. The longest corresponding to a $n = 2^i - 1$ has length $2i - 2$ due to the results of corollary.

This fact proofs that all the chains generated with this method are not larger than $2i - 2$. Hence, the minimum chain must be smaller or equal to these values. This last result completes the proof.

References

[1] Scholz, A. (1937) Aufgabe 253. *Jahresbericht der Deutschen Mathematiker-Vereingung*, **47**, 41-42.

[2] Brauer, A.T. (1939) On Addition Chains. *Bulletin of the American Mathematical Society*, **45**, 736-739. http://dx.doi.org/10.1090/S0002-9904-1939-07068-7

[3] Knuth, D.E. (1969) The Art of Computer Programming. Vol. 1: Fundamental Algorithms. Second Printing, Addison-Wesley Publishing Co., Reading.

[4] Kunihiro, N. and Yamamoto, H. (2000) New Methods for Generating Short Addition Chains. *IEICE Transactions on Fundamentals*, **E83-A**, 60-67.

[5] Koc, C.K. (1995) Analysis of Sliding Window Techniques for Exponentiation. *Computers & Mathematics with Applications*, **30**, 17-24. http://dx.doi.org/10.1016/0898-1221(95)00153-P

[6] Cruz-Cortes, N., *et al*. (2008) An Artificial Immune System Heuristic for Generating Short Addition Chains. *IEEE Transactions on Evolutionary Computation*, **12**, 1-24. http://dx.doi.org/10.1109/TEVC.2007.906082

[7] Bos, J. and Coster, M. (1990) Addition Chain Heuristics. *Advances in Cryptology*, **435**, 400-407. http://dx.doi.org/10.1007/0-387-34805-0_37

[8] Sautto-Vallejo, J.M., Agustín, S.-M., Carlos, B.-H. and Verónica, C.-G. (2013) Scholz's Third Conjecture: A Demonstration for Star Addition Chains. *Applied Mathematics*, **4**, 1-12. http://dx.doi.org/10.4236/am.2013.410A1001