JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

An integer sequence for solving the modular equation $3^x \equiv b\,[p]$, when p is prime

Omar Khadir[1], Takao Komatsu[2]

[1] Laboratory of Mathematics, Cryptography and Mechanics, Fstm
University of Hassan II Mohammedia-Casablanca, Morocco

[2] Graduate School of Science and Technology, Hirosaki University, Japan

ABSTRACT

Let p be a prime number. Consider the recurrent integer sequence $(u_n)_{n\in\mathbb{N}}$ defined by the initial term u_0 with $0 < u_0 < p$ and the relations:

$$u_{n+1} = \begin{cases} \dfrac{u_n}{3} & \text{if } u_n \equiv 0\,[3] \\ \dfrac{p \pm u_n}{3} & \text{otherwise.} \end{cases}$$

We show that this sequence is connected to the hard discrete logarithm problem. In particular, we prove that, under some favorable conditions, it is possible to solve the discrete logarithm problem modulo p in the two following situations:

1. Number 3 is a primitive root modulo p.

2. The integer p is a safe prime. Namely, it has the form $p = 2q + 1$, where q is also prime.

Keywords

Integer sequences, discrete logarithm problem, public key cryptography.

1. INTRODUCTION

Public key cryptography algorithms are based on hard issues in mathematics and particularly in number theory. One of these difficult questions is the discrete logarithm problem. Given two positive integers a, b and a large prime number p, how to find the unknown exponent x such that a^x and b are congruent modulo p.

The topic continues to be intractable when the prime p is large: some hundreds of digits. In 1972, Shanks[13] proposed an algorithm with a complexity of $O(\sqrt{p})$. In 1978, Pohlig and Hellman [11] published an efficient method if the prime p is smooth, that is, $p-1$ has only small prime divisors. In the same year, Pollard [12] constructed a remarkable probabilistic algorithm. Since then, no significant developments have been done on the subject.

In [6], trying to see what happens for particular cases, the modular equation $2^x \equiv b[p]$, with a prime p, was discussed. In this paper, following the same direction, we

address the logarithm problem $3^x \equiv b\ [p]$, where p is a large prime and element 3 is a generator modulo p. We show that, if we can solve this equation for any parameters b, p, then we can also solve the general equation $a^x \equiv b\ [p]$. On the other side, we introduce and use in the sequel, the recurrent sequence defined by the initial term u_0 such that $0 < u_0 < p$ and the relations.

$$u_{n+1} = \begin{cases} \dfrac{u_n}{3} & if\ \ u_n \equiv 0[3] \\ \dfrac{p \pm u_n}{3} & otherwise. \end{cases}$$

We take the numerator $p \pm u_n$ which is divisible by 3.

Moreover, we found that, when the modulus p is a safe prime, i.e $p = 2q+1$ and q is also prime, then $p-3$ is always a generator modulo p and then our integer sequence could be exploited to solve the general discrete logarithm problem.

The paper is organized as follows. In section 2, we present the properties of the recurrent sequence. In section 3, we describe an application to the discrete logarithm problem. In section 4, we discuss the primes for which the integer sequence is efficient. We conclude in section 5.

Classical notations will be adopted. In particular, $\mathbb{N}$ is the set of all natural integers and $\mathbb{N}^* = \mathbb{N} - \{0\}$. For every $n \in \mathbb{N}$, we denote by $\mathbb{Z}/n\mathbb{Z}$ the finite ring of modular integers. If a, b, c are three integers, we will write $a \equiv b[c]$ if c divides the difference $a-b$, and $a = b \bmod [c]$ if a is the remainder in the division of b by c, so $a < b$. The great common divisor of a and b is denoted by $\gcd(a,b)$, and the minimum of a and b by $\min(a,b)$.

Throughout this article, p denotes a fixed large odd prime integer. In the next section, we define and study the recurrent sequence $(u_n)_{n\in\mathbb{N}}$.

2. PROPERTIES OF THE RECURRENTE SEQUENCE

We define the integer sequence $(u_n)_{n\in\mathbb{N}}$ and prove some of its properties that will be exploited in section 3 of this paper. The definition is as follows. Let p be a prime number and $0 < u_0 < p$ be the initial term. We put:

$$u_{n+1} = \begin{cases} \dfrac{u_n}{3} & if\ \ u_n \equiv 0[3] \\ \dfrac{p - u_n}{3} & if\ \ p - u_n \equiv 0[3] \\ \dfrac{p + u_n}{3} & otherwise. \end{cases} \qquad (1)$$

We suppose in the sequel that number 3 is a primitive root of the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, .)$. Let $q = \dfrac{p-1}{2}$.

Next proposition is essential for the sequel. It shows that, when an integer sequence verifies the recurrence relation (1), and when it starts with value 1, then it has the maximal cycle and its general term is expressed in a simple form.

Proposition 1

Let $(w_n)_{n\in\mathbb{N}}$ be the integer sequence defined by the recurrence relation (1) with the particular initial term $w_0 = 1$. We have:

(i) $\{w_0, w_1, w_2, ..., w_{q-1}\} = \{1, 2, 3, ..., q\}$

and $\forall i \geq 0,\ \ w_{q+i} = w_i$.

(ii)

$$\forall n \in \{0, 1, 2, ...,\ q-1\},$$
$$w_n \equiv 3^{kq-n}\ [p],\ \ k \in \{1, 2\}$$

Proof. (i) Observe first that

$$\forall n \in IN,\quad 0 < w_n < \frac{p}{2}.$$

It is easy to show by induction that $w_i \equiv 3^{\alpha_i}\ [p]$ for $i \in \{0, 1, 2, ...,\ q-1\}$ and where α_i verifies $\alpha_i \equiv q - i\ [q]$. The exponent can be taken modulo q. As 3 is a primitive root modulo p, all the terms w_i are distinct. On the other hand, since $w_i \in \{1, 2, 3, ...,\ q\}$, we obtain that

$\{w_0, w_1, w_2,..., w_{q-1}\} = \{1, 2, 3,..., q\}.$

We have $w_{q-1} \equiv 3[p]$, so $w_q = 1 = w_0$

and by induction, we obtain that

$w_{q+i} = w_i$ for all i in $\mathbb{N}$.

(ii) From part (i), we have

$\forall i \in \{0, 1, 2,..., q-1\}$

$w_i \equiv 3^{\alpha_i}\ [p]$, where

$\alpha_i \equiv q - i\ [q]$. Therefore $\exists K \in \mathbb{Z}$, $\alpha_i \equiv q - i + Kq = (1+K)q - i.$ But exponents are congruent modulo $p-1$, so it suffices to take $K \in \{0, 1\}$, which gives $k \in \{1, 2\}$, hence the proof is achieved.

□

The results in the last proposition are generalized in the following theorem.

Theorem 1. Let $(u_n)_{n\in\mathbb{N}}$ be an integer sequence defined by the recurrence relation (1) with $0 < u_0 < p$. We have :

If $u_0 \leq q$, then

$\{u_0, u_1, u_2,..., u_{q-1}\} = \{1, 2, 3,..., q\}$ and

$\forall i \geq 0,\ u_{q+i} = u_i$

If $u_0 > q$, then

$\{u_2, u_3, u_4,..., u_{q+1}\} = \{1, 2, 3,..., q\}$ and

$\forall i \geq 2,\ u_{q+i} = u_i.$

Proof. Consider the sequence $(w_n)_{n\in\mathbb{N}}$ defined in Proposition 1. We know that

$\{w_0, w_1, w_2,..., w_{q-1}\} = \{1, 2, 3,..., q\}$, and

$w_q = w_0 = 1$. Therefore the set

$\{w_0, w_1, w_2,..., w_{q-1}\}$ is a cycle containing u_0 since by the hypothesis $0 < u_0 < q$. In other words, there exists

$j \in \{0, 1, 2,..., q-1\}$ such that

$u_0 = w_j = 1$ and then by induction, $\forall i \in IN$, $u_i = w_{j+i}$. We deduce that

$\{u_0, u_1, u_2,..., u_{q-1}\} = \{1, 2, 3,..., q\}$.

and $\forall i \geq 0,\ u_{q+i} = u_i$.

Suppose now that $u_0 > q$. We can check that we always have $0 < u_2 < q$, so there exists

$j \in \{0, 1, 2,..., q-1\}$ such that $u_2 = w_j$ and then by induction, $\forall i \in IN$, $u_i = w_{j+i}$. This implies

$\{u_2, u_3, u_4,..., u_{q+1}\} = \{1, 2, 3,..., q\}$ and

$\forall i \geq 2,\ u_{q+i} = u_i.$

□

Next result, in its part (ii), gives a simple expression of the general term for any integer sequence $(u_n)_{n\in\mathbb{N}}$ that verifies the recurrence relation (1).

Theorem 2. If $(u_n)_{n\in\mathbb{N}}$ is an integer sequence defined by the recurrence relation (1)

with $1 \leq u_0 \leq q$, then~:

(i) There exists an integer

$n_0 \in \{0, 1, 2,..., q-1\}$ such that $u_{n_0} = 1$

(ii) $\forall n \in \{0, 1, 2,..., q-1\}$,

$u_{n_0+n} \equiv 3^{kq-n}\ [p],\ k \in \{1, 2\}$

Proof. (i) By the first part of Theorem 1, element 1 is belonging to the set $\{0, 1, 2,..., q-1\}$,

so there exists an index

$n_0 \in \{0, 1, 2,..., q-1\}$ such that $u_{n_0} = 1$.

(i) Consider the recurrent sequence $(w_n)_{n\in\mathbb{N}}$ defined in Proposition 1. From part (i) we have $u_{n_0} = w_0$ and by induction for all integers $i \in \{0, 1, 2,..., q-1\}$, $u_{n_0+i} = w_i$.

Proposition 1 implies that

$$u_{n_0+i} \equiv 3^{kq-i}\,[p],\quad k \in \{1,2\}.$$

Hence, the proof is achieved.

As there exist fast algorithms for computing the modular exponentiation ([9, p.71], [14, p.176]), next corollary provides the means of a rapid computation of the general term u_n for any sequence defined by the recurrence relation (1). The formula is remarkable because it easily gives the term u_n by computing the minimum of two known positive integers.

Corollary 1. If $(u_n)_{n\in\mathbb{N}}$ is an integer sequence defined by the recurrence relation (1) with $1 \le u_0 \le q$ and if n_0 is a natural integer such that $u_{n_0} = 1$, then

$$\forall\, n \in \{0,1,2,\ldots,q-1\}$$

$$u_{n_0+n} = \min(3^{q-n} \bmod p,\, 3^{2q-n} \bmod p) \quad (2)$$

Proof. Consider an integer

$n \in \{0,1,2,\ldots,q-1\}$ and put

$$\alpha = 3^{q-n} \bmod p.$$

Assume first that $1 \le \alpha \le q$ (*).

We have

$$3^{q-n} \equiv \alpha\,[p] \Rightarrow 3^{2q-n} \equiv -\alpha \equiv p-\alpha\,[p],$$

with $0 < p-\alpha < p$. On the other hand:

(*) $\Rightarrow p-q \le p-\alpha < p$. But

$$p-q = \frac{p+1}{2} > q, \text{ so } 3^{2q-n} \bmod p > q,$$

which means that u_n cannot be equal to

$3^{2q-n} \bmod p$, and consequently

$$u_n = \min(3^{q-n} \bmod p,\, 3^{2q-n} \bmod p).$$

Assume now that $\alpha > q$ (**).

We have

$$3^{q-n} \equiv \alpha\,[p] \Rightarrow 3^{2q-n} \equiv -\alpha \equiv p-\alpha\,[p],$$

With $0 < p-\alpha < p$

(**) $\alpha > q \Rightarrow -p \le -\alpha < -q \Rightarrow 0 < p-\alpha$

$$< p-q = \frac{p+1}{2}.$$

As $p-q \in IN$, we obtain $p-q \le \frac{p-1}{2} = q$,

and then $p-\alpha \le q$ which implies that

$$u_n = 3^{2q-n} \bmod p = \min(3^{q-n} \bmod p,\, 3^{2q-n} \bmod p)$$

3. APPLICATION TO THE DISCRET LOGARITHM PROBLEM

In this section we show the strong relation between the sequence $(u_n)_{n\in\mathbb{N}}$ and the discrete logarithm problem. We start by recalling a well-known proposition [9, p.103]. It tells us that the difficulty of solving the discrete logarithm problem is independent of the generator.

Proposition 2. Let a be a generator of the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*,.)$. If for any integer $b \in \{1,2,3,\ldots,p-1\}$ we can efficiently solve the equation $3^x \equiv b\ [p]$, then we can also efficiently solve the equation $a^x \equiv b\ [p]$.

Proof. Consider the equation $a^x \equiv b\ [p]$. Let x_0 be a positive integer such that $3^{x_0} \equiv a\ [p]$.

Then $a^x \equiv b\ [p] \Leftrightarrow 3^{xx_0} \equiv b\ [p]$

$\Leftrightarrow xx_0 \equiv X\,[p-1]$, where X is a solution of the equation $3^X \equiv b\ [p]$. Since elements 3 and the parameter a are generators of $((\mathbb{Z}/p\mathbb{Z})^*,.)$, $\gcd(x_0, p-1)=1$ and then x_0 is invertible modulo $p-1$. Therefore $x \equiv \frac{X}{x_0}[p-1]$. Hence, the proof is achieved.

□

Let us now show the connection between our integer sequence $(u_n)_{n\in\mathbb{N}}$ and the discrete logarithm problem. But before that, we have to define the second recurrent sequence.

Fix a prime integer p and $q=\frac{p-1}{2}$. Let $(u_n)_{n\in\mathbb{N}}$ be the sequence defined by relation (1) with $1 \le u_0 \le q$. We define recursively the integer sequence $(x_n)_{n\in IN}$ as follows:

$x_0 = 0$ and

$$x_{n+1} = \begin{cases} (1+x_n+q) \bmod p-1 \ \text{if}\ u_n \bmod 3 \in \{0, p \bmod 3\} \\ (1+x_n) \bmod p-1 \ \text{otherwise} \end{cases} \quad \textbf{(3)}$$

Consider the modular equation $3^x \equiv b\ [p]$, where $1 \le b \le p$ is given and x is an unknown variable. Define two integer sequences $(u_n)_{n\in\mathbb{N}}$ and $(x_n)_{n\in IN}$ by the recurrence relations (1) and (3), respectively, with $u_0 = b$. We have the following fact:

Proposition 3. An integer α is a solution to the equation $3^x \equiv b\ [p]$ if and only if

$$\forall n \in IN,\ 3^{\alpha - x_n} \equiv u_n\ [p]. \quad (4)$$

Proof. Let us prove it by induction on n.

The relation is true for $n=0$. Suppose that

$$3^{\alpha - x_n} \equiv u_n\ [p].$$

If u_n is a multiple of 3, we have

$$u_{n+1} = \frac{u_n}{3} \text{ and } x_{n+1} = 1 + x_n \bmod (p-1)$$

So

$$3^{\alpha - x_n} \equiv u_n\ [p] \Rightarrow 3^{\alpha - x_n - 1} \equiv \frac{u_n}{3} \equiv u_{n+1}[p]$$

Finally,

$$3^{\alpha - x_{n+1}} \equiv 3^{\alpha - x_n - 1 \bmod (p-1)} \equiv 3^{\alpha - x_n - 1} \equiv u_{n+1}[p]$$

Suppose that $u_n \equiv p\,[3]$. We have $3^{\alpha - x_n} \equiv u_n\ [p]$. On another hand

$$3^{\alpha - x_{n+1}} \equiv 3^{\alpha - (1+x_n+q) \bmod (p-1)}$$

$$\equiv u_n 3^{-1-q} \equiv \frac{p-u_n}{3}[p] \equiv u_{n+1}[p]$$

Suppose that we have not $u_n \in \{0,\ p \bmod 3\}$. Then

$$3^{\alpha - x_n} \equiv u_n\ [p] \Rightarrow 3^{\alpha - x_{n+1}} \equiv 3^{\alpha - (1+x_n)}$$

$$\equiv \frac{u_n}{3} \equiv u_{n+1}[p]$$

To prove the sufficient condition is trivial.

□

Next theorem presents a theoretical characterization of the solution to the discrete logarithm problem $3^x \equiv b\ [p]$. Note that to make the equation intractable for cryptographical applications, the bit-length of the unknown variable x should be at least 160 [1, p186].

Theorem 3. Let $u_0 = b$ with $1 \le u_0 \le q$ and $(u_n)_{n\in\mathbb{N}}$ be the integer sequence defined by relation (1).

If n_0 is the least natural integer such that $u_{n_0} = 1$, then x_{n_0} is a solution of the discrete logarithm problem $3^x \equiv b\ [p]$.

Proof. If α is a solution to the modular equation $3^x \equiv b\ [p]$, Proposition 3 implies that

$3^{\alpha - x_{n_0}} \equiv u_{n_0} \ [p]$ and then $3^{x_{n_0}} \equiv b \ [p]$.

Here is one of our important results:

Corollary 2. Let $u_0 = b$ with $1 \le b \le q$ and $(u_n)_{n \in IN}$ be the integer sequence defined by relation (1).

If n_0 is the least natural integer such that $u_{n_0} = 1$, then the solution of the discrete logarithm problem

$3^x \equiv b \ [p]$ is n_0 or $n_0 + q \bmod (p-1)$.

Proof. By the last theorem, it suffices to justify that for any natural integer n, we have $x_n = n$ or

$x_n = n + q \bmod (p-1)$.

It is not difficult to show that

$x_n = P + I(q+1) \bmod (p-1)$, where P and I are respectively the number of even and odd terms, in the set $\{u_0, u_1, u_2, ..., u_{n-1}\}$. Moreover, since

$q = \dfrac{(p-1)}{2}$, we get

$x_n = P + I(q+1) \bmod (p-1)$

And $x_n \in \{n, \ (n+q) \bmod (p-1)\}$.

Remark 1. Previous corollary is significant. It transforms the hardness of finding the solution to the discrete logarithm problem into the hardness of finding the least natural integer n such that $u_n = 1$. This observation means that our recurrent sequence is not much easier than the famous Collatz sequence [8]. Given

$v_0 \in IN$, let

$$v_{n+1} = \begin{cases} \dfrac{v_n}{2} & \text{if } v_n \text{ is even,} \\ \dfrac{3v_n + 1}{2} & \text{otherwise.} \end{cases}$$

It is well-known that until today, there is no proof for the following conjecture: For any initial term v_0, there exists a natural integer n such that $v_n = 1$. For our sequence $(u_n)_{n \in IN}$, we have proved that there exists $n \in IN$ such that $u_n = 1$, but what is difficult is to show how to find this index n.

Exemple 1.

Let us apply our results to one of the examples taken by Pollard in his paper [12]. The considered modular equation is

$2^x \equiv 107 \ [99\,989]$.

Here $p = 99989$ and elements 2 and 3 are generators of the multiplicative group Z_p^*. By application of the method in the proof of Proposition 2, we need to solve the two modular equations:

$$3^{x_0} \equiv 2 \ [p] \quad \text{and} \quad 3^X \equiv 107 \ [p]$$

The solution of the equation $2^x \equiv 107 \ [99\,989]$ is then

$$\frac{X}{x_0} \bmod (p-1).$$

Consider the first equation $3^{x_0} \equiv 2 \ [p]$. With $u_0 = 2$, for $n \le 10$, terms u_n are progressively calculated and dressed in the next table.

Table 1

n	0	1	2	3	4	5
u_n	2	33329	22220	25923	8641	36210
n	6	7	8	9	10	
u_n	12070	37353	12451	37480	45823	

With the help of Maple software, we find the least natural n such that $u_n = 1$ is $n = 47449$. As $q = 49994$, the solution belongs to the pair {47449,97443}. We can check that the first possibility is the correct one.

Let us solve the second equation $3^X \equiv 107 \ [p]$. With $u_0 = 107$, the first ten terms u_n are progressively calculated and dressed in the next table.

Table 2

n	0	1	2	3	4	5
u_n	107	33294	11098	37029	12343	37444
n	6	7	8	9	10	
u_n	458111	48600	16200	5400	1800	

With the help of Maple software, we find the least natural n such that $u_n = 1$ is $n = 38183$. As $q = 49994$ the solution belongs to the pair {38183, 88177}. We can check that the second possibility is the correct one.

The solution of the equation $2^x \equiv 107 \ [99\,989]$ is then

$$\frac{X}{x_0} \bmod (p-1) = 87833.$$

Designers of cryptosystems and digital signatures should take into account the two following situations:

Corollary 3. If from the term $u_0 = b$, (respectively $u_n = 1$), we can reach the term $u_n = 1$ (respectively $u_n = b$) in an acceptable time, then we can solve the discrete logarithm problem $3^x \equiv b \ [p]$.

Proof. This is an immediate application of Corollary 2.

□

Corollary 4. If from the term $u_0 \equiv b^{\alpha} \ [p]$, where α is a known natural integer coprime to $p-1$, we can reach the term $u_n = 1$ in an acceptable time, then we can solve the discrete logarithm problem.

Proof. Indeed we have the equivalence:

$3^x \equiv b \ [p] \Leftrightarrow 3^{\alpha x} \equiv b^{\alpha} \ [p]$. We solve the equation $3^X \equiv b^{\alpha} \ [p]$. The unknown variable x is then $x \equiv \frac{X}{\alpha} [p-1]$.

□

4. PRIMES FOR WHICH OUR RECURRENT SEQUENCE CAN BE EFFICIENT

In this section we discuss the prime integers for which our recurrent sequence is efficient. In particular, we will see that even for safe primes p, our sequence can become the mean to solve the DLP modulo p. But first, we gather known facts in the following lemma.

Lemma 1. Let p be a prime number such that $p = 2^k q + 1$, where q is also prime and $k \in IN^*$.

1. An element α is a primitive root modulo p if and only if α is a quadratic non-residue modulo p and $\alpha^s \neq -1[p]$ where $s = 2^{k-1}$.

2. When $k = 3$, the number 3 is a primitive root of any p except for $p = 41$.

3. When $k = 2$, number 3 is a primitive root modulo p if and only if $q \equiv 1[3]$.

4. When $k \geq 4$ and $3^{2^{k-1}} < p-1$, element 3 is a primitive root for all p.

Proof. **1.** Recall that element α is a primitive root if and only if $\alpha^{\frac{p-1}{Q}} \neq 1[p]$ for any prime Q that divides $p-1$.

Suppose that α is a primitive root. Then α cannot be a square since its order is $p-1$. When $Q = 2$, we obtain

$$\alpha^s \neq 1[p].$$

Conversely, suppose that α is a quadratic non-residue modulo p and that $\alpha^s \neq -1[p]$ where $s = 2^{k-1}$. Let E, F and G be the three sets defined by the following:

E is the set of all primitive roots modulo p.

F is the set of all non square elements modulo p.

G is the set of all elements α such that $\alpha^s \neq -1[p]$ where $s = 2^{k-1}$.

We can prove successively that $G \subset F$, $E \subset F - G$ and $E = F - G$ by computing the cardinality of each set.

2. As $p = 8q + 1$ we have $(\frac{3}{p}) = \frac{p}{3}(-1)^{4q}$.

Therefore

$$(\frac{3}{p}) = 1 \Leftrightarrow p \equiv 1[3] \Leftrightarrow q \equiv 0[3] \Leftrightarrow q = 3,$$

which is impossible since 25 is not a prime number. Finally, $(\frac{3}{p}) = -1$. On the other hand,

$$3^{2^2} \equiv -1[p] \Leftrightarrow 41 \equiv 0[p] \Leftrightarrow p = 41$$

We conclude that when $p = 8q + 1$ and $\neq 41$, element 3 is always a primitive root.

3. Here we have $(\frac{3}{p}) = \frac{p}{3}(-1)^{2q} = \frac{p}{3}$.

Thus

$$(\frac{3}{p}) = -1 \Leftrightarrow (\frac{p}{3}) = -1 \Leftrightarrow p \equiv 2[3] \Leftrightarrow q \equiv 1.$$

As p is supposed to be large, we surely have $3^s < p - 1$, so $s = 2$.

4. Since the condition $3^{2^{k-1}} < p - 1$ implies that $3^{2^{k-1}} \neq -1[p]$, it suffices to prove that element 3 is not a square modulo p. By the Gauss reciprocity law, $(\frac{3}{p}) = (-1)^{(p-1)/2}(\frac{p}{3}) = (\frac{p}{3})$. Thus

$$(\frac{3}{p}) = 1 \Leftrightarrow p \equiv 1[3] \Leftrightarrow q \equiv 0[3] \Leftrightarrow q \equiv 3,$$

but in this case we cannot have $3^{2^{k-1}} < p - 1$. So, 3 is not a square modulo p, and consequently it is a primitive root.

□

Proposition 4. Let p be a safe prime, i.e., $p = 2q + 1$ and q is also prime. Element 3 is never a primitive root modulo p but $p - 3$ is a primitive root.

Proof. First we can prove that if $\alpha^3 \neq \alpha[p]$ then α or $p - \alpha$ is a primitive root.

Let us show that 3 is to be excluded. Indeed, it suffices to prove that 3 is a square root. The Gauss reciprocity law gives $(\frac{3}{p}) = \frac{p}{3}(-1)^k$ With $k = (p-1)/2 = q$. Thus $(\frac{3}{p}) = -1 \Leftrightarrow (\frac{p}{3}) = 1 \Leftrightarrow p \equiv 1[3]$. Since for every q, $p \equiv 3[4]$, number p verifies the modular system

$$\begin{cases} p \equiv 1[3] \\ p \equiv 3[4] \end{cases}.$$

Chinese remainder theorem implies $p \equiv -5[12]$. But

$$p = -5 + 12K, k \in IIN \Rightarrow -5 + 12K = 2q + 1$$

$$\Rightarrow q = 3 + 6K \Rightarrow q = 3 \Rightarrow p = 7,$$ which is false. Conclusion: 3 is never a primitive root modulo a safe prime.

□

We arrive to our second important result, the first one is stated in Corollary 2. Most of the cryptography designers recommend to use safe

primes when producing cryptosystems and digital signatures parameters.

Theorem 4. Let p is a safe prime. Consider the general discrete logarithm problem: $a^x \equiv b[p]$. Suppose that for $u_0 = a$ and $u_0 = b$, the first natural integer n_0 such that $u_{n_0} = 1$ is not too large, then we are able to solve the modular equation $a^x \equiv b[p]$.

Proof. As p is a safe prime, by Proposition 4, $p-3$ is always a primitive root. Consider the general equation $a^x \equiv b[p]$. We start by solving two equations:

$$(p-3)^{x_0} \equiv a \ [p] \text{ and } (p-3)^X \equiv b[p].$$

The final solution is then $x \equiv \frac{X}{x_0} \bmod (p-1)$.

A general equation $(p-3)^x \equiv b[p]$ is equivalent to $3^x \equiv b[p]$ or $3^x \equiv -b[p]$, according to the parity of the exponent x, respectively.

So, the equation $(p-3)^{x_0} \equiv a \ [p]$ can be solved by the integer sequence method studied before.

□

5. CONCLUSION

In this paper, we proposed and studied a new integer sequence that is strongly connected to the modular equation $a^x \equiv b[p]$.We also described its properties and showed how it can lead, in some cases, to an exact solution of the discrete logarithm problem. In particular, we showed that safe primes are not so safe!.

6. ACKNOWLEDGMENTS

A part of this work, was prepared, in 2013, when the first author was invited in Japan. He would like to thank the Hirosaki University and specially professor Takao Komatsu.

7. REFERENCES

[1] J.Buchmann, 2001, Introduction to cryptography, Springer-Verlag, New York.

[2] W. Diffie and M. E.Hellman, 1976, New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654.

[3] T. ElGamal,1985, A public key cryptosystem and a signature scheme based on discrete logarithm problem, IEEE Trans. Inform. Theory, vol. IT-31, pp. 469-472.

[4] P. Horster, M. Michels and H. Petersen, 1994, Generalized ElGamal signature schemes for one message block, Technical Report, TR-94-3.

[5] E. S. Ismail, N. M. F. Tahat and R. R. Ahmad, 2008, A new digital signature scheme based on factoring and discrete logarithms, J. Math. Stat., vol. 4, pp. 222-225.

[6] O. Khadir and L. Szalay, 2013, A special integer sequence strongly connected to the discrete logarithm problem, J. Theor. Phys. Cryptogr., vol. 2, pp. 1-5.

[7] N. Koblitz, 1994, A Course in number theory and cryptography}, Graduate Texts in Math., 2nd ed., vol. 114, Springer-Verlag.

[8] J. C. Lagarias, 1985, The 3x+1 problem and its generalizations, Amer. Math. Monthly, vol. 92, pp. 3-23.

[9] A. J. Menezes, P.~C. van Oorschot and S. A. Vanstone, 1997, Handbook of applied cryptography, CRC Press, Boca Raton, Florida,

Available at http://www.cacr.math.uwaterloo.ca/hac/

[10] A. Odlyzko and M. E. Hellman, 2000, Discrete logarithms, the past and the future, Des. Codes Cryptogr. vol. 19, pp. 129-145.

[11] S. C. Pohlig and M. E. Hellman, 1978, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Trans. Inform. Theory, vol. IT-24, no.1, pp. 106-110.

[12] A. Pollard, 1978, Monte Carlo method for index computation mod p, Math. Comp., vol. 32, pp. 918-924.

[13] D. Shanks, 1972, Class number, a theory of factorization and genera, Symposium Pure Mathematics.

[14] D. R. Stinson, 2006, Cryptography, theory and practice, 3rd Edition, Chapman & Hall / CRC.