JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY
www.IJTPC.org/Publications

A Special Integer Sequence Strongly Connected to the Discrete Logarithm Problem

Omar Khadir [1], Laszlo Szalay [2]
[1] Laboratory of Mathematics, Cryptography and Mechanics, Fstm University of Hassan II Mohammedia-Casablanca, Morocco
[2] Institute of Mathematics, University of West Hungary, Sopron, Hungary

ABSTRACT

Let p be a large prime integer. In this work, we study the recurrent sequence defined by $u_0 \in \mathbb{N}$, $0 < u_0 < p$, and

$$\begin{cases} u_{n+1} = \dfrac{u_n}{2} \ if \ u_n \ is \ even \\ u_{n+1} = \dfrac{p - u_n}{2} \ if \ not \end{cases}$$

This integer sequence has connection with the discrete logarithm problem, and under certain assumptions, we obtain an exact solution.

Keywords

Integer sequences, discrete logarithm problem, public key cryptography.

1. INTRODUCTION

Numerous public key cryptosystems, digital signatures protocols and identification schemes are based on the discrete logarithm problem [1, p.130]. Given a large prime integer p and two elements a, b in the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, .)$, it is computationally hard to find a natural exponent x such that $a^x = b$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

In 1976 Diffie and Hellman [2] exploited this fact to show how two people can product and share the same common key even if they never met each other before. They actually signed the beginning of the public key cryptography era. A few years before, Shanks [3] presented a practical algorithm that solves the problem with a complexity of $O(\sqrt{p})$. In 1978, Pollard [4] described a Monte Carlo method based on Floyd algorithm for graph cycles. In the same year, Pohlig and Hellman [5] proposed a fast algorithm for solving the discrete logarithm problem in the particular case where the integer $p - 1$ has only short prime divisors. However, in practice, the index calculs seems to be the most powerful method.

In 1985 ElGamal [6] constructed a cryptosystem and an ingenious digital signature scheme both based on the discrete logarithm problem. Since then, many variants of his signature algorithm were published. See [7, 8, 9] or Table 11.5, page 457 in [1].

Let p be a fixed odd prime integer. In this work, we study the recurrent integer sequence $(u_n)_{n\in\mathbb{N}}$ defined by $u_0 \in \mathbb{N}$, such that $0 < u_0 < p$, and

$$\begin{cases} u_{n+1} = \dfrac{u_n}{2} \ if \ u_n \ is \ even, \\ u_{n+1} = \dfrac{p - u_n}{2} \ if \ not. \end{cases}$$

We present some properties of this sequence whose behavior seems to be difficult to predict. We also show how its terms u_n are connected to the solution of the discrete logarithm problem. To our best knowledge, this sequence has not been previously studied or even mentioned in mathematics or computer science literature.

The paper is organized as follows. In section 2, we give the definition of the sequence and prove some of its mathematical properties. In section 3, relation between this integer sequence and public key cryptography is described. More precisely, we explain how the sequence is efficient for solving the discrete logarithm problem. Conclusion is given in section 4.

Classical notations will be adopted. In particular, $\mathbb{N}$ is the set of all natural integers and $\mathbb{N}^* = \mathbb{N} - \{0\}$. If a, b, c are three integers, we will write $a \equiv b\ [c]$ if c divides the difference $a - b$, and $a = b \ mod \ c$ 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 $\min(a, b)$ means the minimum of a and b.

Throughout this article, p designs a fixed large odd prime integer such that element 2 is a generator of the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, .)$. Notice that there exist only

algorithms for generating large probable primes [1 p.126, 1 p. 135, 11 p.178, 12].

In the next section, we define and study the recurrent sequence $(u_n)_{n\in\mathbb{N}}$.

2. THE RECCURENT SEQUENCE AND ITS PROPERTIES

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 u_0 be a natural integer less than $p-1$. We put:

$$\begin{cases} u_{n+1} = \dfrac{u_n}{2} \ if\ u_n\ is\ even, \\ \\ u_{n+1} = \dfrac{p-u_n}{2} \ if\ not. \end{cases} \qquad (1)$$

Let $p = 2q+1$, $q \in \mathbb{N}^*$ be an odd prime integer such that number 2 is a primitive root of the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, .)$. 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 a 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 $w_0 = 1$. We have:

(i) $\{w_0, w_1, w_2, \dots, w_{q-1}\} = \{1,2,3,\dots,q\}$ and $\forall\, i \geq 0, w_{q+i} = w_i$.

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

Proof. (i) By Fermat theorem we have $2^{p-1} \equiv 1 \equiv w_0\ [p]$. As 2 is a primitive root, $2^q \equiv -1\ [p]$ and then $w_1 = \frac{p-w_0}{2} \equiv 2^{q-1}\ [p]$.

If w_1 is even, $w_2 = \frac{w_1}{2} \equiv 2^{q-2}$ [p].

If not, $w_2 = \frac{p-w_1}{2} \equiv 2^{2q-2}\ [p]$. In both cases the exponent of base 2 is equivalent to $(q-2)$ modulo q.

Suppose that $w_2 \equiv 2^{q-2}\ [p]$. If w_2 is even,

$w_3 = \frac{w_2}{2} \equiv 2^{q-3}\ [p]$, if not
$w_3 = \frac{p-w_2}{2} \equiv 2^{2q-3}\ [p]$. In both cases the exponent of base 2 is $(q-3)$ modulo q.

Suppose that $w_2 \equiv 2^{2q-2}\ [p]$. If w_2 is even,

$w_3 = \frac{w_2}{2} \equiv 2^{2q-3}\ [p]$, if not
$w_3 = \frac{p-w_2}{2} \equiv 2^{2q-3}\ [p]$. In both cases the exponent of base 2 is $(q-3)$ modulo q.

Finally the exponent of base 2 associated to w_3 is $q-3$ modulo q.

Continuing in this fashion, we obtain that for every $i \in \{0,1,2,\dots,q-1\}$, $w_i \equiv 2^{\alpha_i}\ [p]$ with $\alpha_i \equiv q-i\ [p]$ and $w_q = w_0 = 1$. We deduce, by induction, that $\forall i \geq 0$, $w_{q+i} = w_i$.

Therefore, as number 2 is a primitive root, all the terms w_i are distinct when $i \in \{0,1,2,\dots,q-1\}$. On the other hand,

$w_i \in \{1,2,3,\dots,q\}$, so $\{w_0, w_1, \dots, w_{q-1}\} = \{1,2,3,\dots,q\}$.

(ii) We saw in part (i) that $w_i \equiv 2^{\alpha_i}\ [p]$, with

$\alpha_i \equiv q-i\ [p]$, so $\alpha_i = q-i+Kq = (1+K)q-i$, where $K \in \mathbb{Z}$. Since exponents are equivalent modulo $(p-1)$, it suffices to take $K \in \{0,1\}$ or $k = 1+K \in \{1,2\}$ which ends the proof.

□

The last proposition results 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 $\{u_0, u_1, \dots, u_{q-1}\} = \{1,2,3,\dots,q\}$ and $\forall i \geq 0$, $u_{q+i} = u_i$.

If $u_0 > q$ then $\{u_1, u_2, \dots, u_q\} = \{1,2,3,\dots,q\}$ and $\forall i \geq 1$, $u_{q+i} = u_i$.

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

$\{w_0, w_1, w_2, \dots, w_{q-1}\} = \{1,2,3,\dots,q\}$ and $w_q = w_0 = 1$ so the set $\{w_0, w_1, w_2, \dots, w_{q-1}\}$ is a cycle containing u_0 since by hypothesis $0 \leq u_0 \leq q$. In other words, there exists

$j \in \{0,1,2,\dots,q-1\}$ such that $u_0 = w_j = 1$ and then by induction, for all $i \in \mathbb{N}$ $u_i = w_{j+i}$. We deduce that $\{u_0, u_1, \dots, u_{q-1}\} = \{1,2,3,\dots,q\}$ and $\forall i \geq 0$, $u_{q+i} = u_i$.

Suppose now that $u_0 > q$. We have $0 \leq u_1 \leq q$, so there

exists $j \in \{0,1,2,\dots,q-1\}$ such that $u_1 = w_j$ and then

by induction, for all $i \in \mathbb{N}$, $u_i = w_{j+i}$. This implies

$\{u_1, u_2, \dots, u_q\} = \{1,2,3,\dots,q\}$ and $\forall i \geq 1$, $u_{q+i} = u_i$.

□

Now we give two other results. In particular, statement (ii) below is an interesting modular equivalence. It provides 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 $n_0 \in \{0,1,2,\dots,q-1\}$ such that $u_{n_0} = 1$.

(ii) $\forall\, n \in \{0,1,2,\dots,q-1\}, u_{n_0+n} \equiv 2^{kq-n}\ [p]$, $k \in \{1,2\}$.

Proof. By the first part of theorem 1, element 1 is belonging to the set $\{u_0, u_1, \dots, u_{q-1}\}$, so there exists an index $n_0 \in \{0,1,2,\dots,q-1\}$ such that $u_{n_0} = 1$.

(ii) 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 $i \in \{0,1,2,\dots,q-1\}$, $u_{n_0+i} = w_i$. Proposition 1 implies that $u_{n_0+i} \equiv 2^{kq-i}\ [p]$, $k \in \{1,2\}$ which achieves the proof.

□

As there exist fast algorithms for computing the modular exponentiation [1 p.71, 11 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 gives easily 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

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

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

Proof. Consider an integer $n \in \{0,1,2,\dots,q-1\}$ and put $\alpha = 2^{q-n} \bmod p$. By Theorem 1, $1 \le \alpha \le q$. Assume first that $1 \le \alpha \le q$ (*).

We have $2^{q-n} \equiv \alpha\ [p] \Rightarrow 2^{2q-n} \equiv -\alpha \equiv p-\alpha\ [p]$, with $0 < p-\alpha$<p. In another hand: (*)⇒-q≤ $\alpha < 0 \Rightarrow p - q \le p - \alpha < p$. But $p - q = \frac{p+1}{2} > q$, so $2^{2q-n} \bmod p > q$, which means that u_n cannot be equal to $2^{2q-n} \bmod p$, and consequently
$u_n = 2^{q-n} \bmod p = \min\{2^{q-n} \bmod p, 2^{2q-n} \bmod p\}$.

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

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

$0 < p - \alpha < p$

(**)⇒ $-p \le -\alpha < -q \Rightarrow 0 < p-\alpha < p-q = \frac{p+1}{2}$. As

$p - q \in \mathbb{N}$, we obtain $p - q \le \frac{p-1}{2} = q$ and then

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

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

□

We move to the next section where we show the strong relation between the sequence $(u_n)_{n\in\mathbb{N}}$ and the discrete logarithm problem.

3. CONNECTION WITH THE DISCRETE LOGARITHMPROBLEM

We start by recalling a well-known proposition [1, p.103]. It tells that the difficulty of solving the discrete logarithm problem is independent of the generator.

Proposition 2. [1] Let a be a generator of the multiplicative group $((\mathbb{Z}/p\mathbb{Z})^*, .)$. If for any integer $b \in \{1,2,3,\dots,p-1\}$ we can efficiently solve the equation $2^x \equiv b\ [p]$ 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 $2^{x_0} \equiv a\ [p]$. Then $a^x \equiv b\ [p] \Leftrightarrow 2^{xx_0} \equiv b\ [p] \Leftrightarrow xx_0 \equiv X(p-1]$, where X is a solution of the equation $2^X \equiv b\ [p]$. Since elements 2 and 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 $x \equiv \frac{X}{x_0}\ [p-1]$, which achieves the proof.

□

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

$$x_0 = 0 \quad \text{and}$$
$$\begin{cases} x_{n+1} = (1 + x_n) \bmod (p-1) \text{ if } u_n \text{ is even}, \\ x_{n+1} = (1 + x_n + q) \bmod (p-1) \text{ if not}. \end{cases} \qquad (3)$$

In other words $x_{n+1} = (1 + x\_n + q\varepsilon_n) \bmod (p-1)$ where $\varepsilon_n = u_n \bmod 2$.

Consider the modular equation $2^x \equiv b\ [p]$ where $1 \le b \le q$ is given and x is an unknown variable. Define two integer sequences $(u_n)_{n\in\mathbb{N}}$ and $(x_n)_{n\in\mathbb{N}}$ respectively by the recurrence relations (1) and (3) with $u_0 = b$. We have the equivalence:

Proposition 3. An integer α is a solution to the equation $2^x \equiv b\ [p]$ if and only if

$$\forall\, n \in \mathbb{N}, \quad 2^{\alpha - x_n} \equiv u_n\ [p] \qquad (4)$$

Proof. Let us prove it by induction on n. The relation is true for $n = 0$. Suppose that $2^{\alpha - x_n} \equiv u_n\ [p]$. If u_n is even, we have

$u_{n+1} = \frac{u_n}{2}$ and $x_{n+1} = (1 + x_n) \bmod (p-1)$, so

So $2^{\alpha - x_n} \equiv u_n\ [p] \Rightarrow 2^{\alpha - x_n - 1} \equiv \frac{u_n}{2} \equiv u_{n+1}\ [p]$. Finally

$$2^{\alpha-x_{n+1}} \equiv 2^{(\alpha-x_n-1)\,mod\,(p-1)} \equiv 2^{\alpha-x_n-1} \equiv u_{n+1}\ [p]$$

If u_n is odd, we have

$u_{n+1} = \frac{p-u_n}{2}$ and $x_{n+1} = (1 + x_n + q)\ mod\ (p-1)$.

In another hand, as 2 is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$:

$2^q \equiv -1\ [p]$. So

$$2^{\alpha-x_n} \equiv u_n\ [p] \Rightarrow 2^{\alpha-x_{n+1}} \equiv 2^{\alpha-x_n-1-q} \equiv \frac{p-u_n}{2} \equiv u_{n+1}\ [p]$$

□

Next theorem presents a theoretical characterization of the solution to the discrete logarithm problem $2^x \equiv b\ [p]$. Note that to make the equation intractable for cryptographic applications, the bit-length of the unknown variable x should be at least 160 [13, p.186].

Theorem 3. Let $u_0 = b$, $1 \le b \le q$ and $(u_n)_{n\in\mathbb{N}}$ is 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 $2^x \equiv b\ [p]$.
Proof By induction on the natural index n.

□

Next corollary is more precise. 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 [14].

Corollary 2. Let Let $u_0 = b$, $1 \le b \le q$ and $(u_n)_{n\in\mathbb{N}}$ is the integer sequence defined by relation (1).
If n_0 is the least natural integer such that $u_{n_0} = 1$, then solution of the discrete logarithm problem $2^x \equiv b\ [p]$ is n_0 or $n_0 + q\ mod\ (p-1)$.
Proof By last theorem, it suffices to justify that for any natural integer n, we have $x_n = n$. Or $x_n = (n + q)\ mod\ (p-1)$. It is not difficult to show that $x_n = (P + I(q+1))\ mod\ (p-1)$, where P and I are respectively the number of even terms and odd terms in the set $\{u_0, u_1, \dots, u_{n-1}\}$. Moreover since $q = \frac{p-1}{2}$,
$x_n = (P + I + Iq)\ mod\ (p-1) \in \{n, (n+q)mod\ (p-1)\}$

□

Example 1. Let us apply our method to one of the examples taken by Pollard in his paper [5]. The considered modular equation is $2^x \equiv 107\ [99\,989]$. Here $p = 99\,989$ and element 2 is a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. The first ten terms are u_n progressively calculated and dressed in the next table.

n	0	1	2	3	4	5
u_n	107	44941	25024	49799	25095	37447

n	6	7	8	9	10
u_n	31271	34359	32815	33587	33201

Table 1

With the help of Maple software, we find the least natural n such that $u_n = 1$ is $n = 37\,839$. As $p = 49\,994$, the solution belongs to the pair $\{37\,839,\ 87\,833\}$.
We can check that the second possibility is the correct one.
Designers of cryptosystems and digital signatures should take in account the two following situations:

Corollary 3. If from the term $u_0 = b$ (respectively $u_0 = 1$) we can reach the term $u_n = 1$ (respectively $u_n = b$) in an acceptable time, then we can solve the discrete logarithm problem $2^x \equiv b\ [p]$.
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 $2^x \equiv b\ [p]$.
Proof. Indeed : $a^x \equiv b^\alpha\ [p] \Leftrightarrow a^{\frac{x}{\alpha}} \equiv b\ [p]$.

□

4. 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.

ACKNOWLEDGMENTS
A part of this work was prepared, in 2012, when the first author was invited to the Institute of Mathematics in Sopron. He thanks the University of West Hungary and specially professor Laszlo Szalay.

5. REFERENCES

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

[2] Diffie W., Hellman M.E., 1976. New directions in cryptography, IT-22 644–654.

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

[4] Pollard A., 1978, Monte Carlo method for index computation (mod p), Mathematics of computation, 32 918-924.

[5] Pohlig S.C., Hellman M.E, 1978. An improved algorithm for computing over GFp and its cryptographic significance, IEEE Trans. Information Theory IT-24 1 106-110.

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

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

[8] Ismail E.S, Tahat N.M.F, Ahmad R.R, 2008. A new digital signature scheme based on factoring and discrete logarithms, J. of Mathematics and Statistics (4) 222-225.

[9] Khadir O., 2010. New variant of ElGamal signature scheme, Int. J. Contemp. Math. Sciences, 5 34 1653-1662.

[10] N. Koblitz, 1994, A Course in number theory and cryptography, GraduateTexts in Mathematics, 2nd ed., Vol. 114, Springer-Verlag.

[11] D. R. Stinson, 2006, Cryptography, theory and practice, Third Edition, Chapman & Hall /CRC.

[12] Khadir O., Szalay L., 2009. Experimental results on probable primality, Acta Univ. Sapientiae, Math. 1 2 161-168

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

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