Annales Mathematicae et Informaticae
49 (2018) pp. 101–107
DOI: 10.33039/ami.2018.05.002
http://ami.uni-eszterhazy.hu

On sunlet graphs connected to a specific map on $\{1, 2, \dots, p-1\}$

Omar Khadir[a], **László Németh**[b], **László Szalay**[c]

[a]Laboratory of Mathematics, Cryptography and Mechanics, University of Hassan II
Mohammedia-Casablanca, Morocco
khadir@hotmail.com

[b]Institute of Mathematics, University of Sopron, Hungary
nemeth.laszlo@uni-sopron.hu

[c]J. Selye University, Department of Mathematics and Informatics, Slovakia
Institute of Mathematics, University of Sopron, Hungary
szalay.laszlo@uni-sopron.hu

Submitted September 12, 2017 — Accepted May 29, 2018

Abstract

In this article, we study the structure of the graph implied by a given map on the set $S_p = \{1, 2, \dots, p-1\}$, where p is an odd prime. The consecutive applications of the map generate an integer sequence, or in graph theoretical context a walk, that is linked to the discrete logarithm problem.

Keywords: directed sunlet graph, recurrence sequence, discrete logarithm problem.

MSC: 11T71, 05C20, 11B37.

1. Introduction

Public key cryptography began in 1976 with a publication of Diffie and Hellman [1], their fundamental work is *New direction in cryptography.*

In the most cases, the security of a protocol is based on known hard questions in mathematics, and particularly in number theory. One of them is the discrete logarithm problem (in short, DLP). Let p denote a large prime integer, say having more than a hundred of digits. If a is a primitive root modulo p, and b is a fixed integer not divisible by p, then it is difficult to compute the unknown x such that

$$a^x \equiv b \pmod{p}. \tag{1.1}$$

For example, the Diffie and Hellman method [1] and ElGamal signature [2] are based on the supposition that this modular equation is intractable. It is easy to see that if 2 is also a primitive root modulo p, and $2^y \equiv a \pmod{p}$ can be efficiently solved, then (1.1) can be also efficiently solved. Hence it is sufficient to investigate the DLP with base 2. The present paper is also associated with this specification.

The first significant algorithm for solving the discrete logarithm problem was proposed by Shanks [8] in 1971. Pohlig and Hellman [5] published an improved algorithm in 1978. In the same year, other methods were suggested by Pollard [6]. But until now, no polynomial time algorithm is known. This fact justifies the efforts made by researchers to obtain advances in this mathematical field.

In 2013 two of the authors [4] studied a special recurrent integer sequence $(u_n)_{n\in\mathbb{N}}$ which can be used in solving the discrete logarithm problem when some favorable conditions are satisfied. More precisely, let p and q be odd primes such that $p = 2q + 1$, and 2 is a primitive root modulo p. Further let $u_0 = b$, $1 \leq b \leq q$, and

$$u_{n+1} = \begin{cases} u_n/2, & \text{if } u_n \text{ is even,} \\ (p - u_n)/2, & \text{if } u_n \text{ is odd.} \end{cases} \tag{1.2}$$

They proved that if n_0 is the smallest positive integer such that $u_{n_0} = 1$, then x_{n_0} is a solution of the discrete logarithm problem $2^x \equiv b \pmod{p}$. Here $x_0 = 0$, further

$$x_{n+1} = \begin{cases} x_n + 1 \pmod{p}, & \text{if } u_n \text{ is even,} \\ x_n + 1 + q \pmod{p}, & \text{if } u_n \text{ is odd.} \end{cases} \tag{1.3}$$

Consequently, the designers of cryptosystems must avoid the situation of small n_0.

The connection between DLP and the sequences (1.2), (1.3) motivated us to investigate the graph generated by (1.2) if one considers it as a map on the set $S_p = \{1, 2, \ldots, p - 1\}$. In this work, we principally concentrated on the structure of the aforementioned graph. Here we assume only the primality of p, and we do not suppose the primality of q in $p = 2q + 1$. It turned out that our graphs are so-called sunlet graphs (see, for example [3]), and we discovered and described many properties of them.

Our paper is organized as follows. In Section 2 we define the map which induces the graph denoted by $\mathcal{G}_p$. Then we investigate the properties of the graph. Section 3 is devoted to provide some examples and remarks.

2. The map and its properties

Fix an odd prime p, and then the set $S_p = \{1, 2, \ldots, p-1\}$. Consider the map

$$u(n+1) = \begin{cases} u(n)/2, & \text{if } u(n) \text{ is even,} \\ (p - u(n))/2, & \text{if } u(n) \text{ is odd} \end{cases} \tag{2.1}$$

on S_p. The map u induces a digraph $\mathcal{G}_p$, such that there is an edge from x to y exactly when $u(x) = y$. In this paper, we describe the structure and some properties of the graph induced by (2.1). As an illustration, the graph belonging to $p = 17$ is drawn in Fig. 1.

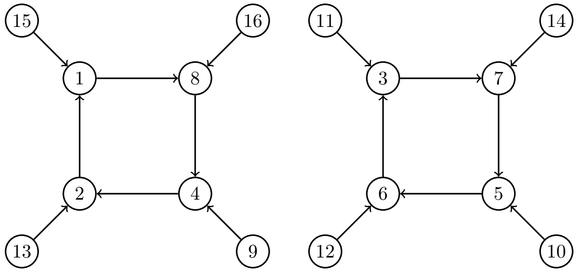

Figure 1: Sunlet subgraphs in case $p = 17$

Define

$$c_p = \frac{p-1}{2\,\mathrm{ord}_p(4)},$$

that is clearly integer. We prove the following theorem.

Theorem 2.1. *The graph* $\mathcal{G}_p$ *splits into* c_p *connected isomorphic subgraphs. Each subgraph contains a cycle with length* $L_p = \mathrm{ord}_p(4)$*, and each vertex of the cycle possesses two incoming edges.*

First we justify a lemma which has an important corollary.

Lemma 2.2. *Suppose that* $u(x) = a$ *and* $u(y) = b$ *hold for some* $x, y, a, b \in S_p$*. Then*

$$ay \equiv (-1)^{y-x} bx \pmod{p}. \tag{2.2}$$

Proof. If x and y have the same parity, then either $a = x/2$ and $b = y/2$, or $a = (p-x)/2$ and $b = (p-y)/2$. Hence either $ay = a \cdot 2b = 2a \cdot b = bx$, or $ay = a(p-2b) \equiv b(p-2a) = bx \pmod{p}$, respectively.

Assume now that $x \not\equiv y \pmod{2}$. It leads either $a = x/2$ and $b = (p-y)/2$, or $a = (p-x)/2$ and $b = y/2$. In the first case we see $ay = a(p-2b) = ap - bx \equiv -bx \pmod{p}$, while in the second case we have $ay = a \cdot 2b \equiv -b(p-2a) = -bx \pmod{p}$.

Then the statement is clearly comes from the previous arguments. □

Now we give a direct consequence of Lemma 2.2.

Corollary 2.3. *Under the same conditions*

$$a \equiv (-1)^{y-x} bxy^{-1} \pmod{p} \tag{2.3}$$

holds.

Now we give the proof of Theorem 2.1, which is split into a few parts called observations. Put $q = (p-1)/2$. Note that the map u does not possess fixed points.

Observation 2.4. *If $u(x) = u(y)$ holds for some $x \neq y$, then $x + y = p$.*

Proof. Since $x \neq y$, we see that the parity of x differs the parity of y. Thus either

$$\frac{x}{2} = \frac{p-y}{2} \qquad \text{or} \qquad \frac{p-x}{2} = \frac{y}{2}$$

follows, both options admit $x + y = p$. □

Observation 2.5. *The equation $u(x) = a$ is soluble if and only if $a \leq q$, and in this case there exist exactly two solutions.*

Proof. Assume that x and a satisfy $u(x) = a$. If $x \in S_p$ is even, then $u(x) = x/2 \leq (p-1)/2 = q$. Contrary, if x is odd, then $u(x) = (p-x)/2 \leq (p-1)/2 = q$. On the other hand, $u(2a) = a$ and $u(p-2a) = a$ hold. By Observation 2.4 no third solution to the equation. □

Note that exactly one of $2a$ and $p - 2a$ is larger than q. Let $S_p^\ell = \{1, 2, \ldots, q\}$ and $S_p^u = \{q+1, q+2, \ldots, p-1\}$. Clearly $S_p^\ell \cup S_p^u = S_p$, and $|S_p^\ell| = |S_p^\ell|$. Hence, using graph theoretical terminology, we obtain the following information about the structure of $\mathcal{G}_p$: *the elements of S_p^ℓ form cycle(s), further each element of S_p^u goes to an appropriate element of S_p^ℓ such that different elements of S_p^u go different elements of S_p^ℓ. In other words, $\mathcal{G}_p$ consists of sunlet graph(s) (or sun graph(s)).*

In the next step we show that the sunlet graphs included in $\mathcal{G}_p$ are isomorphic.

Observation 2.6. *If $\mathcal{G}_p$ consists of at least two connected sunlet graphs, then all the sunlet graphs are isomorphic.*

Proof. Obviously it is sufficient to prove that two cycles have the same length. Take two cycles, saying $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_k$, where $n \geq 2$ and $k \geq 2$. Without loss of generality we may assume that $k \leq n$. By Corollary 2.3 the following congruences hold modulo p.

$$\begin{aligned}
y_2 &\equiv (-1)^{x_1-y_1} y_1 x_2 x_1^{-1}, \\
y_3 &\equiv (-1)^{x_2-y_2} y_2 x_3 x_2^{-1}, \\
&\vdots \\
y_k &\equiv (-1)^{x_{k-1}-y_{k-1}} y_{k-1} x_k x_{k-1}^{-1},
\end{aligned}$$

$$y_{k+1} = y_1 \equiv (-1)^{x_k - y_k} y_k x_{k+1} x_k^{-1}.$$

The product of all the congruences above returns with

$$1 \equiv (-1)^{x_\sigma - y_\sigma} x_{k+1} x_1^{-1} \pmod{p},$$

where $x_\sigma = \sum_{i=1}^{k} x_i$ and $y_\sigma = \sum_{i=1}^{k} y_i$. Thus

$$x_1 \equiv (-1)^{x_\sigma - y_\sigma} x_{k+1} \pmod{p}.$$

In accordance with the parity of exponent $x_\sigma - y_\sigma$, we have either $x_{k+1} = x_1$ or $x_{k+1} = p - x_1$. But the second case cannot be occurred because it leads to a contradiction by $q \geq x_{k+1} = p - x_1 > q$. Subsequently, $x_{k+1} = x_1$, and then $n = k$. □

A direct consequence is the following statement.

Corollary 2.7. $L_p \mid p - 1$.

Observation 2.8. $L_p = \operatorname{ord}_p(4)$.

Proof. The formula (2.1) of map u implies

$$u(x) \equiv \pm\frac{x}{2} \pmod{p}, \tag{2.4}$$

where the minus sign is occurring exactly if x is odd. Applying (2.4) consecutively for the cycle $x_1, x_2, \ldots, x_{L_p}$ it leads to

$$x_1 \equiv (-1)^t \frac{x_1}{2^{L_p}} \pmod{p},$$

where t is a suitable non-negative integer, showing the number of odd entries of map u. Equivalently we have

$$2^{L_p} \equiv (-1)^t \pmod{p},$$

and then

$$4^{L_p} \equiv 1 \pmod{p}.$$

Thus $\operatorname{ord}_p(4) \mid L_p$. To show the reverse relation $L_p \mid \operatorname{ord}_p(4)$ we assume $\operatorname{ord}_p(4) > L_p$. Let $s \geq 1$ and $0 \leq r < L_p$ two non-negative integers such that $\operatorname{ord}_p(4) = sL_p + r$, where $r \neq 0$ holds if $s = 1$. Consider now the sequence

$$x_1, x_2, \ldots, x_{L_p}; x_1, x_2, \ldots, x_{L_p}; \ldots; x_1, x_2, \ldots, x_{L_p}; x_1, x_2, \ldots, x_r,$$

assuming that here the cycle $x_1, x_2, \ldots, x_{L_p}$ occurs s times. For a suitable τ we see

$$x_r \equiv (-1)^\tau \frac{x_1}{2^{\operatorname{ord}_p(4)}} \pmod{p},$$

and then squaring both sides it follows that

$$x_r^2 \equiv x_1^2 \pmod{p}.$$

It provides either $x_r + x_1 = p$ which contradicts the facts that neither x_1 nor x_r exceeds q, or $x_r = x_1$ which leads to $qL_p = \operatorname{ord}_p(4)$, that is $L_p \mid \operatorname{ord}_p(4)$. Together with $\operatorname{ord}_p(4) \mid L_p$ we conclude $L_p = \operatorname{ord}_p(4)$, and the proof is complete. □

3. Examples and remarks

1. Let $p = 31$. Now $L_{31} = \mathrm{ord}_{31}(4) = 5$ is the length of the cycles. The number of connected subgraphs is $c_{31} = 30/(2 \cdot 5) = 3$. The corresponding graph is drawn here.

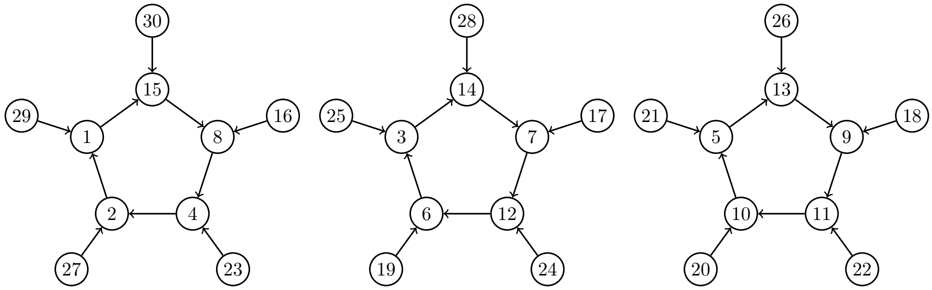

Figure 2: Sunlet subgraphs in case of $p = 31$

2. Let $p = 5419$. Now $L_{5419} = \mathrm{ord}_{5419}(4) = 21$ is relatively a very small value for the length of the cycles, and primes having such a property are unavailable for cryptographic purposes. The number of connected subgraphs is $c_{5419} = 129$.

Acknowledgments. This paper was written when the first author visited the Institute of Mathematics, University of Sopron, and the Department of Mathematics and Informatics, J. Selye University. He expresses his gratitude both departments for their hospitality.

References

[1] Diffie, W., Hellman, M. E., New directions in cryptography, *IEEE Trans. Info. Theory*, Vol. 22 (1976), 644–654.
`https://doi.org/10.1109/tit.1976.1055638`

[2] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithm problem, *IEEE Trans. Info. Theory*, Vol. 31 (1985), 469–472.
`https://doi.org/10.1109/tit.1985.1057074`

[3] Fu, C. M., Jhuang, N. H., Lin, Y. L., Sung, H. M., On the existence of k-sun systems, *Discrete Mathematics*, Vol. 312 (2012), 1931–1939.
`https://doi.org/10.1016/j.disc.2012.03.007`

[4] Khadir, O., Szalay, L., A special integer sequence strongly connected to the discrete logarithm problem, *J. Theor. Phys. Cryptogr.*, Vol. 2 (2013), 1–5.

[5] Pohlig, S. C., Hellman, M. E., An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Info. Theory*, Vol. 24 (1978), 106–110.
`https://doi.org/10.1109/tit.1978.1055817`

[6] Pollard, A., Monte Carlo method for index computation (mod p), *Math. Comp.*, Vol. 32 (1978), 918–924.
https://doi.org/10.1090/s0025-5718-1978-0491431-9

[7] Rivest, R. L., Shamir, A., Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, Vol. 21 (1978), 120–126.
https://doi.org/10.1145/359340.359342

[8] Shanks, D., Class number, a theory of factorization and genera, in: *Proc. Symp. Pure Math.*, AMS, Providence, R. I. Vol. 20 (1971), 415–440.
https://doi.org/10.1090/pspum/020/0316385