International Journal of Mathematics and
Computer Science, **14**(2019), no. 3 , 557–561

On the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n$

Sasikan Pankaew[1], **Amornrat Rattana**[1], **Ronnason Chinram**[1,2]

[1]Department of Mathematics and Statistics
Faculty of Science
Prince of Songkla University
Hat Yai, Songkhla 90110, Thailand

[2]Center of Excellence in Mathematics
CHE, Si Ayuthaya Road,
Bangkok 10400, Thailand

email: sasikan.pkaew@hotmail.com, amornrat.r@psu.ac.th,
ronnason.c@psu.ac.th

(Received February 28, 2019, Revised March 26, 2019,
Accepted April 3, 2019)

Abstract

In this paper, we describe the semigroups $\mathbb{Z}_n$ (under multiplication) having n monogenic subsemigroups.

1 Introduction and Preliminaries

In group theory, there are many articles that examine cyclic subgroups of groups, for example, [1], [2], [3], [4], [5] and [6]. Let G be a group and $C(G)$ be the poset of cyclic subgroups of G. The connections between $|C(G)|$ and $|G|$ can be seen in [1], [4], [5] and [6]. Firstly, we recall the result in group theory: A finite group G is an elementary Abelian 2-group if and only if $|C(G)| = |G|$. In [6], Tărnăuceanu described the finite groups G having $|G| - 1$ cyclic subgroups. In [1], Belshoff, Dillstrom and Reid studied the

Key words and phrases: Finite semigroups, monogenic subsemigroups, integer modulo n.
AMS (MOS) Subject Classifications: 20M10.
ISSN 1814-0432, 2019, http://ijmcs.future-in-tech.net

finite groups G having $|G| - r$ cyclic subgroups for $r = 2, 3, 4$ and 5. This is the motivation of this paper.

Let S be a semigroup and $C(S)$ be the poset of monogenic subsemigroup of S. For $a \in S$, the monogenic subsemigroup of S generated by a is denoted by $\langle a \rangle$ and $\langle a \rangle = \{a^n \mid n \in \mathbb{N}\}$. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the semigroup of integers modulo n under multiplication and $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$. It is a known fact that $\mathbb{Z}_n^\times$ is a group under multiplication. For an element a in a group $\mathbb{Z}_n^\times$, $\mathrm{o}(a)$ denotes order of a, that is, the smallest positive integer k such that $a^k = 1$. If $\mathrm{o}(a) = k$, then $\langle a \rangle = \{1, a, a^2, \ldots, a^{k-1}\}$. A generator of a group $\mathbb{Z}_n^\times$ is called a primitive root modulo n. It is well-known that there is a primitive root modulo n if and only if $n = 2, 4, p^k$ or $2p^k$, where p is prime and $p > 2$. The purpose of this paper is to describe the semigroups $\mathbb{Z}_n$ (under multiplication) having n monogenic subsemigroups. Throughout this paper, the greatest common divisor of integers a and b is denoted by (a, b).

2 Main Results

First of all, let us observe the number of the monogenic subsemigroups of semigroups $\mathbb{Z}_n$ for $n = 2, 3, 4, 5, 8$.

Example 2.1. We find the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n, n = 2, 3, 4, 5, 8$, as follows :

- $n = 2$
  Since $\langle 0 \rangle = \{0\}$ and $\langle 1 \rangle = \{1\}$ are only monogenic subsemigroups of $\mathbb{Z}_2$, $|C(\mathbb{Z}_2)| = 2$.

- $n = 3$
  We know that $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1\}$, and $\langle 2 \rangle = \{1, 2\}$ are only monogenic subsemigroups of $\mathbb{Z}_3$. Thus $|C(\mathbb{Z}_3)| = 3$.

- $n = 4$
  The monogenic subsemigroups of $\mathbb{Z}_4$ are $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{0, 2\}$, and $\langle 3 \rangle = \{1, 3\}$. Then $|C(\mathbb{Z}_4)| = 4$.

- $n = 5$
  All monogenic subsemigroups of $\mathbb{Z}_5$ are $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{1, 2, 3, 4\} = \langle 3 \rangle$ and $\langle 4 \rangle = \{1, 4\}$. Hence $|C(\mathbb{Z}_5)| = 4 \neq 5$.

- $n = 8$
  We found that $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{0, 2, 4\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 4 \rangle = \{0, 4\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 6 \rangle = \{0, 4, 6\}$, and $\langle 7 \rangle = \{1, 7\}$ are all monogenic subsemigroups of $\mathbb{Z}_8$. Thus $|C(\mathbb{Z}_8)| = 8$.

Therefore the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n$ equals n, i.e., $|C(\mathbb{Z}_n)| = n$, for $n = 2, 3, 4, 8$. However, $|C(\mathbb{Z}_n)| \neq n$ for $n = 5$. $\square$

Theorem 2.1. $|C(\mathbb{Z}_p)| = p$ *if and only if* $p = 2$ *or* $p = 3$.

Proof. Assume that $p \geq 5$. Then there is a primitive root modulo p, say a. Thus $\langle a \rangle = \{1, a, a^2, \ldots a^{p-2}\}$. So $a \neq a^{p-2}$. Since $(p-1, p-2) = 1$, $\mathrm{o}(a) = \mathrm{o}(a^{p-2})$. This implies that $\langle a \rangle = \langle a^{p-2} \rangle$. Hence $|C(\mathbb{Z}_p)| < p$. The converse is already shown in Example 2.1 ($n = 2, 3$). $\square$

Theorem 2.2. $|C(\mathbb{Z}_{2^k})| = 2^k$ *for all* $k = 1, 2, 3$.

Proof. Example 2.1 shows that the theorem is true for $k = 1, 2, 3$. Assume that $k > 3$. Then $|\mathbb{Z}_{2^k}^{\times}| = 2^{k-1}$ and $3 \in \mathbb{Z}_{2^k}^{\times}$. So $\mathrm{o}(3)|2^{k-1}$. We know that $3^2 = 9 \neq 1$, therefore $\mathrm{o}(3) \geq 4$. Thus $3 \neq 3^3$. Since $(3, 2^{k-1}) = 1$, it implies that $\mathrm{o}(3) = \mathrm{o}(3^3)$. Therefore $\langle 3 \rangle = \langle 3^3 \rangle$ which is a contradiction.

$\square$

Theorem 2.3. $|C(\mathbb{Z}_{3^k})| = 3^k$ *if and only if* $k = 1$.

Proof. The converse is already proved in Example 2.1 ($n = 3$). It remains to show that if $|C(\mathbb{Z}_{3^k})| = 3^k$, then $k = 1$. Assume, to the contrary, that $k > 1$. Note that $\phi(3^k) = 2 \cdot 3^{k-1} \geq 6$. Since there is a primitive root modulo 3^k, let a be a primitive root modulo 3^k. Thus $\mathbb{Z}_{3^k}^{\times} = \langle a \rangle = \{1, a, a^2, \ldots, a^{\phi(3^k)-1}\}$. Since $(\phi(3^k), \phi(3^k) - 1) = 1$, $\langle a^{\phi(3^k)-1} \rangle = \langle a \rangle$. Thus $|C(\mathbb{Z}_{3^k})| < 3^k$ for $k > 1$. $\square$

Theorem 2.4. $|C(\mathbb{Z}_{p^k})| < p^k$ *for all prime number* $p > 3$.

Proof. Let p be a prime number such that $p > 3$. So $\phi(p^k) \geq 4$. Then there is a primitive root modulo p^k, say a. Thus $\mathbb{Z}_{p^k}^{\times} = \langle a \rangle = \{1, a, a^2, \ldots, a^{\phi(p^k)-1}\}$. Since $a \neq a^{\phi(p^k)-1}$ and $(\phi(p^k), \phi(p^k) - 1) = 1$, this implies that $\langle a^{\phi(p^k)-1} \rangle = \langle a \rangle$. Therefore $|C(\mathbb{Z}_{p^k})| < p^k$. $\square$

The next theorem is well-known.

Theorem 2.5. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ for distinct primes $p_1, p_2, \ldots, p_k$ and $a_i > 0$, then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \ldots, \times \mathbb{Z}_{p_k^{a_k}}.$$

Theorem 2.6. *Let $S_1, S_2, \ldots, S_n$ be finite semigroups with zero. If $S = S_1 \times S_2 \times \ldots \times S_n$, then $|C(S)| = |S|$ if and only if $|C(S_i)| = |S_i|$ for all $i \in \{1, 2, \ldots, n\}$.*

Proof. Assume that $|C(S)| = |S|$ and suppose that there exists $i \in \{1, 2, \ldots, n\}$ such that $|C(S_i)| < |S_i|$. Then there exist two distinct elements a and b in S_i such that $\langle a \rangle = \langle b \rangle$. Let $a' = (a_1, a_2, \ldots, a_n) \in S$ be such that $a_i = a$ and $a_j = 0$ if $i \neq j$ and $b' = (b_1, b_2, \ldots, b_n) \in S$ be such that $b_i = b$ and $b_j = 0$ if $i \neq j$. It implies that $a' \neq b'$ and $\langle a' \rangle = \langle b' \rangle$, this is a contradiction. Conversely, assume that $|C(S_i)| = |S_i|$ for all $i \in \{1, 2, \ldots, n\}$. Suppose that $|C(S)| < |S|$. Then there exist two distinct elements $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ in S such that $\langle a \rangle = \langle b \rangle$. Thus $a_i \neq b_i$ for some $i \in \{1, 2, \ldots, n\}$. Clearly, $\langle a_i \rangle = \langle b_i \rangle$ (because $\langle a \rangle = \langle b \rangle$), which produces a contradiction. Hence $|C(S)| = |S|$. $\square$

From all the previous theorems, the next theorem holds.

Theorem 2.7. $|C(\mathbb{Z}_n)| = n$ *if and only if* $n = 2, 3, 4, 6, 8, 12, 24$.

3 Acknowledgment

This paper was supported by the Algebra and Applications Research Unit, Faculty of Science, Prince of Songkla University.

References

[1] R. Belshoff, J. Dillstrom, L. Reid, Finite groups with a prescribed number of cyclic subgroups, Commun. Algebra, article in press.

[2] M. Garonzi, I. Lima, On the number of cyclic subgroups of a finite group, Bull. Braz. Math. Soc., **49**, (2018), 515–530.

[3] M. H. Jafari, A. R. Madadi, On the number of cyclic subgroups of a finite group, Bull. Korean Math. Soc., **54**, (2017), 2141–2147.

[4] G. A. Miller, On the number of cyclic subgroups of a group, Proc. Natl. Acad. Sci. USA, **15**, (1929), 728–731.

[5] I. M. Richards, A remark on the number of cyclic subgroups of a finite group, Amer. Math. Monthly, **91**, (1984), 571–572.

[6] M. Tărnăuceanu, Finite group with a certain number of cyclic subgroups, Amer. Math. Monthly, **122**, (2015), 275–276.