International Journal of Mathematics and
Computer Science, **17**(2022), no. 1, 99–105

On semigroups $\mathbb{Z}_n$ having $n-1$ and $n-2$ monogenic subsemigroups

Ronnason Chinram[1], **Napaporn Sarasit**[2]

[1]Division of Computation Science
Faculty of Science
Prince of Songkla University
Hat Yai, Songkhla 90110, Thailand

[2]Division of Mathematics
Faculty of Engineering
Rajamangala University of Technology Isan Khon Kaen Campus
Khon Kaen 40000, Thailand

email: ronnason.c@psu.ac.th, napaporn.sr@rmuti.ac.th

(Received June 11, 2021, Accepted July 12, 2021)

Abstract

In this paper, we describe the semigroups $\mathbb{Z}_n$ (under multiplication modulo n) having $n-1$ and $n-2$ monogenic subsemigroups.

1 Introduction and Preliminaries

Let G be a group and let $C(G)$ be the poset of cyclic subgroup of G. First, we recall the well-known result in group theory: A finite group G is an elementary Abelian 2-group if and only if $|C(G)| = |G|$. In 2015, Tărnăuceanu [3] described the finite groups G having $|G|-1$ cyclic subgroups. In 2019, Belshoff, Dillstrom and Reid [1] investigated the finite groups G having $|G|-r$ cyclic subgroups for $r = 2, 3, 4$ and 5. In this paper, we will focus on semigroups. Let S be a semigroup and let $C(S)$ be the poset of monogenic subsemigroup of S. For $a \in S$, the monogenic subsemigroup of S generated

Key words and phrases: Finite semigroups, monogenic subsemigroups, integers modulo n, primitive roots modulo n.
AMS (MOS) Subject Classifications: 20M10.
Corresponding author: Napaporn Sarasit (napaporn.sr@rmuti.ac.th).
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

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 modulo n) 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 modulo n). For any element a in a group $\mathbb{Z}_n^\times$, $\mathrm{o}(a)$ denotes the 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 a prime number. In [2], the semigroups $\mathbb{Z}_n$ such that $|C(\mathbb{Z}_n)| = n$ were characterized as follows:

Theorem 1.1. ([2]) *$|C(\mathbb{Z}_n)| = n$ if and only if $n = 2, 3, 4, 6, 8, 12, 24$.*

The purpose of this paper is to describe the semigroups $\mathbb{Z}_n$ (under multiplication modulo n) having $n-1$ and $n-2$ monogenic subsemigroups. Now, we will recall some results from [2] which we will use in this paper.

Theorem 1.2. ([2]) *$|C(\mathbb{Z}_p)| = p$ if and only if $p = 2$ or $p = 3$.*

Theorem 1.3. ([2]) *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 $i \in \{1, 2, \ldots, n\}$.*

Theorem 1.4. ([2]) *$|C(\mathbb{Z}_{2^k})| = 2^k$ for $k = 1, 2, 3$.*

Theorem 1.5. ([2]) *$|C(\mathbb{Z}_{3^k})| = 3^k$ if and only if $k = 1$.*

Theorem 1.6. ([2]) *$|C(\mathbb{Z}_{p^k})| < p^k$ for all prime numbers $p > 3$.*

2 Main Results

First of all, let us find the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n$ for $n = 5, 7, 9, 10, 11, 14, 15, 16$.

Example 2.1. We find the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n$, where $n = 5, 7, 9, 10, 11, 14, 15, 16$, as follows:

- $n = 5$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 3 >= \{1, 2, 3, 4\}$, $< 4 >= \{1, 4\}$.
  So $C(\mathbb{Z}_5) = 4$. In this case, $C(\mathbb{Z}_n) = n - 1$.

- $n = 7$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 4 >= \{1, 2, 4\}$,
  $< 3 >=< 5 >= \{1, 2, 3, 4, 5, 6\}$, $< 6 >= \{1, 6\}$.
  Thus $|C(\mathbb{Z}_7)| = 5$. In this case, $|C(\mathbb{Z}_n)| = n - 2$.

- $n = 9$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 5 >= \{1, 2, 4, 5, 7, 8\}$,
  $< 3 >= \{0, 3\}$, $< 4 >=< 7 >= \{1, 4, 7\}$,
  $< 6 >= \{0, 6\}$, $< 8 >= \{1, 8\}$.
  So $|C(\mathbb{Z}_9)| = 7$. In this case, $|C(\mathbb{Z}_n)| = n - 2$.

- $n = 10$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 8 >= \{2, 4, 6, 8\}$,
  $< 3 >=< 7 >= \{1, 3, 7, 9\}$, $< 4 >= \{4, 6\}$, $< 5 >= \{5\}$,
  $< 6 >= \{6\}$, $< 9 >= \{1, 9\}$.
  Therefore $|C(\mathbb{Z}_{10})| = 8$. In this case, $|C(\mathbb{Z}_n)| = n - 2$.

- $n = 11$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$,
  $< 2 >=< 6 >=< 7 >=< 8 >= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$,
  $< 3 >=< 4 >=< 5 >=< 9 >= \{1, 3, 4, 5, 9\}$, $< 10 >= \{1, 10\}$.
  Therefore $|C(\mathbb{Z}_{11})| = 5$. In this case, $|C(\mathbb{Z}_n)| = n - 6$.

- $n = 14$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 4 >= \{2, 4, 8\}$,
  $< 3 >=< 5 >= \{1, 3, 5, 9, 11, 13\}$, $< 6 >= \{6, 8\}$, $< 7 >= \{7\}$,
  $< 8 >= \{8\}$, $< 9 >=< 11 >= \{1, 9, 11\}$,
  $< 10 >=< 12 >= \{2, 4, 6, 8, 10, 12\}$, $< 13 >= \{1, 13\}$.
  Therefore $|C(\mathbb{Z}_{14})| = 10$. In this case, $|C(\mathbb{Z}_n)| = n - 4$.

- $n = 15$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >=< 8 >= \{1, 2, 4, 8\}$,
  $< 3 >=< 12 >= \{3, 6, 9, 12\}$, $< 4 >= \{1, 4\}$, $< 5 >= \{5, 10\}$,
  $< 6 >= \{6\}$, $< 7 >=< 13 >= \{1, 4, 7, 13\}$, $< 9 >= \{6, 9\}$,
  $< 10 >= \{10\}$, $< 11 >= \{1, 11\}$, $< 14 >= \{1, 14\}$.
  Therefore $|C(\mathbb{Z}_{15})| = 12$. In this case, $|C(\mathbb{Z}_n)| = n - 3$.

- $n = 16$
  $< 0 >= \{0\}$, $< 1 >= \{1\}$, $< 2 >= \{0, 2, 4, 8\}$,
  $< 3 >=< 11 >= \{1, 3, 9, 11\}$, $< 4 >= \{0, 4\}$,
  $< 5 >=< 13 >= \{1, 5, 9, 13\}$, $< 6 >= \{0, 4, 6, 8\}$,
  $< 7 >= \{1, 7\}$, $< 8 >= \{0, 8\}$, $< 9 >= \{1, 9\}$,
  $< 10 >= \{0, 4, 8, 10\}$, $< 12 >= \{0, 12\}$,
  $< 14 >= \{0, 4, 8, 14\}$, $< 15 >= \{1, 15\}$.
  Therefore $|C(\mathbb{Z}_{16})| = 14$. In this case, $|C(\mathbb{Z}_n)| = n - 2$.

Lemma 2.1. *Let $a \in \mathbb{Z}_n^{\times}$. If $1 \in < a >$, then $1 \in < b >$ for all $b \in < a >$.*

Proof. Let k be the order of a. Then $a^k = 1$. Let $b \in < a >$. So $b = a^m$ for some $m \in \{1, 2, \ldots, k\}$. Thus $1 = 1^m = (a^k)^m = (a^m)^k = b^k \in < b >$. This implies that $1 \in < b >$. $\square$

Lemma 2.2. *Let $a \in \mathbb{Z}_n^\times$ and let $b, c \in < a >$. If $bc = 1$, then $< b > = < c >$.*

Proof. Let $b, c \in < a >$. Assume that $bc = 1$. Then $1 \in < a >$. By Lemma 2.1, $1 \in < c >$. Let $b^m \in < b >$ where $m \in \{1, 2, ..., o(b)\}$ and let n be the order of c. We have $(b^m)(c^m) = (bc)^m = (1)^m = 1 = c^n$; that is, $b^m = c^{n-m} = c^t \in < c >$ for some $t \in \{1, 2, \ldots, o(c)\}$. Hence $< b > \subseteq < c >$. In a similar way, $< c > \subseteq < b >$. Therefore, $< b > = < c >$. $\square$

The following corollary follows from Lemma 2.2.

Corollary 2.3. *Let a be a primitive root modulo p of a group $\mathbb{Z}_p^\times$ and let $b, c \in < a >$. If $bc = 1$, then $o(b) = o(c)$.*

Theorem 2.4. *Let p be a prime number. Then $|C(\mathbb{Z}_p)| = p - 1$ if and only if $p = 5$.*

Proof. Assume that $|C(\mathbb{Z}_p)| = p - 1$. Suppose that $p \neq 5$. If $p \leq 3$, then $|C(\mathbb{Z}_p)| = p$ by Theorem 1.2, a contradiction. If $p \geq 7$, then there is a primitive root modulo p, say a. Thus $< a > = \{1, a, a^2, \ldots, a^{p-2}\} = \mathbb{Z}_p^\times$; that is, $a^{p-1} = 1$ and $a^i \neq a^j$ for all $i, j \in \{1, 2, p-3, p-2\}$. We know that $(a)(a^{p-2}) = a^{p-1} = 1$ and $(a^2)(a^{p-3}) = a^{p-1} = 1$. By Lemma 2.2, we have $< a > = < a^{p-2} >$ and $< a^2 > = < a^{p-3} >$. Hence $|C(\mathbb{Z}_p)| < p - 1$, a contradiction. This implies that $p = 5$. The converse was already proved in Example 2.1. $\square$

Theorem 2.5. *Let p be a prime number. Then $|C(\mathbb{Z}_{2p})| = 2p - 2$ if and only if $p = 5$.*

Proof. By Example 2.1, the converse is clear. Assume that $|C(\mathbb{Z}_{2p})| = 2p-2$. Suppose that $p \neq 5$. If $p \leq 3$, then, by Theorem 1.1, $|C(\mathbb{Z}_{2p})| = 2p$, a contradiction. If $p = 7$, then by Example 2.1, which is a contradiction. If $p \geq 11$, then, by Euler phi function, $\phi(2p) = \phi(2)\phi(p) = (1)(p-1) = p-1$. So $|\mathbb{Z}_{2p}^\times| = p - 1 \geq 10$. Then there is a primitive root of modulo $2p$, say a. So $< a > = \{1, a, a^2, ..., a^{\phi(2p)-1}\}$ and $a^i \neq a^{\phi(2p)-i}$ for all $i \in \{1, 2, 3\}$. Since $(a^i)(a^{\phi(2p)-i}) = a^{\phi(2p)} = 1$, by Lemma 2.2 we have, $< a^i > = < a^{\phi(2p)-i} >$ for all $i \in \{1, 2, 3\}$. Thus $|C(\mathbb{Z}_{2p})| \leq 2p - 3$ which is a contradiction. Therefore $p = 5$. $\square$

Theorem 2.6. *Let p be a prime number. Then $|C(\mathbb{Z}_p)| = p-2$ if and only if $p = 7$.*

Proof. By Example 2.1, the converse is clear. Assume that $|C(\mathbb{Z}_p)| = p-2$. Suppose that $p \neq 7$. If $p \leq 5$, then by Theorems 1.1 and 2.4, $|C(\mathbb{Z}_p)| \neq p-2$, which is a contradiction. If $p \geq 11$, then there is a primitive root of modulo p, say a. So $< a >= \{1, a, a^2, a^3, \ldots, a^{\phi(p)-1}\}$ and $a^i \neq a^{\phi(p)-i}$ for all $i \in \{1, 2, 3\}$. Since $(a^i)(a^{\phi(p)-i}) = a^{\phi(p)} = 1$, by Lemma 2.2 we have, $< a^i >=< a^{\phi(p)-i} >$. Thus $|C(\mathbb{Z}_{2p})| \leq p-3$, which is a contradiction. Hence $p = 7$. $\square$

Theorem 2.7. $|C(\mathbb{Z}_p)| \leq p - \frac{p-3}{2}$ *for all prime numbers $p \geq 5$.*

Proof. Let p be a prime number such that $p \geq 5$. Then $\phi(p) = p-1$ and there exists a primitive root modulo p, say a. Thus, for all $i \in \{1, 2, \ldots, \frac{p-3}{2}\}$, $a^i \neq a^{(p-1)-i}$ and $< a^i >=< a^{(p-1)-i} >$. So $|C(\mathbb{Z}_p)| \leq p - \frac{p-3}{2}$. $\square$

Theorem 2.8. $|C(\mathbb{Z}_{2^k})| \leq 2^k - 3$ *for all integers $k \geq 5$.*

Proof. Assume $k \geq 5$. Then $\phi(2^k) = 2^{k-1} \geq 16$. Let $a \in \{3, 5, 7\} \subset \mathbb{Z}_{2^k}^{\times}$. So $o(a) | 2^{k-1}$ and $a^2 \neq 1$, which implies $4 \leq o(a) \leq 2^{k-1}$. By Euler's theorem, $a^{\phi(2^k)} \equiv 1 \pmod{2^k}$; that is, $a^{2^{k-1}} = 1$. This implies that $(a)(a^{(2^{k-1})-1}) = 1 \in < a >$. By Lemma 2.2, $< a >=< a^{(2^{k-1})-1} >$ and $a \neq a^{(2^{k-1})-1}$. Thus $|C(\mathbb{Z}_{2^k})| \leq 2^k - 3$. $\square$

Theorem 2.9. $|C(\mathbb{Z}_{p^k})| \leq p^k - \frac{p^{k-1}(p-1)-2}{2}$ *for all prime numbers $p \geq 3$ and integers $k \geq 2$.*

Proof. Let k be an integer such that $k \geq 2$. Since there is a primitive root modulo p^k, say a, and $o(a) \geq 6$, we have $\mathbb{Z}_{p^k}^{\times} =< a >= \{1, a, a^2, ..., a^{\phi(p^k)-1}\}$ and $a^i \neq a^j$ for all $i, j \in \{1, 2, \ldots, \phi(p^k) - 1\}$. Thus $(a^i)(a^{\phi(p^k)-i}) = 1$, by Lemma 2.2, $< a^i >=< a^{\phi(p^k)-i} >$ for all $i \in \{1, 2, \ldots, \frac{\phi(p^k)-2}{2}\}$. Therefore $|C(\mathbb{Z}_{p^k})| \leq p^k - \frac{\phi(p^k)-2}{2} = p^k - \frac{p^{k-1}(p-1)-2}{2}$. $\square$

Lemma 2.10. *Let $S_1, S_2, \ldots, S_n$ be finite semigroups with zero 0 and identity 1 and assume that $S = S_1 \times S_2 \times \ldots \times S_n$. If $|C(S_i)| < |S_i|$ for some $i \in \{1, 2, \ldots, n\}$, then $|C(S)| \leq |S| - 2$.*

Proof. Assume $|C(S_i)| < |S_i|$ for some $i \in \{1, 2, \ldots, n\}$. Then there exist $a, b \in S_i$ such that $a \neq b$ and $< a >=< b >$. So there are four distinct elements $a' = (a_1, a_2, \ldots, a_n), b' = (b_1, b_2, \ldots, b_n), c' = (c_1, c_2, \ldots, c_n), d' = (d_1, d_2, \ldots, d_n) \in S$ such that $a_i = a$, $a_j = 0$ if $i \neq j$, $b_i = b$, $b_j = 0$ if $i \neq j$, $c_i = a$, $c_j = 1$ if $i \neq j$ and $d_i = b$, $d_j = 1$ if $i \neq j$. This implies that $a' \neq b'$, $< a' >=< b' >$ and $c' \neq d', < c' >=< d' >$. Thus $|C(S)| \leq |S| - 2$. $\square$

Lemma 2.11. *Let $S_1, S_2, \ldots, S_n$ be finite semigroups with zero* 0 *and identity* 1 *and assume that $S = S_1 \times S_2 \times \ldots \times S_n$. If $|C(S_i)| < |S_i| - 1$ for some $i \in \{1, 2, \ldots, n\}$, then $|C(S)| \leq |S| - 4$.*

Proof. Assume $|C(S_i)| < |S_i| - 1$ for some $i \in \{1, 2, \ldots, n\}$. Then there exist 3 distinct elements $a, b, c \in S_i$ such that and $< a >=< b >=< c >$ or $< a >=< b >, < c >=< d >$ for some $d \in S_i$. Let $x \in S_i$ and let $x' = (a'_1, a'_2, \ldots, a'_n), x'' = (a''_1, a''_2, \ldots, a''_n) \in S$ be such that $a'_i = x, a'_j = 0$ and $a''_i = x, a''_j = 1$ for all $j \neq i$. By assumption there exist $a', b', c', a'', b'', c'' \in S$ such that $< a' >=< b' >=< c' >$ or $< a' >=< b' >, < c' >=< d' >$ and $< a'' >=< b'' >=< c'' >$ or $< a'' >=< b'' >, < c'' >=< d'' >$ for some $d', d'' \in S$. Thus $|C(S)| \leq |S| - 4$. $\square$

From all the previous theorems, the next theorems hold.

Theorem 2.12. $|C(\mathbb{Z}_n)| = n - 1$ *if and only if* $n = 5$.

Proof. Assume that $|C(\mathbb{Z}_n)| = n - 1$. Suppose that $n \neq 5$. If $n < 5$, then by Example 2.1 in [2], $|C(\mathbb{Z}_n)| = n$, a contradiction. If $n > 5$ and n is a prime number, by Theorem 2.4, $|C(\mathbb{Z}_n)| \neq n-1$, which is a contradiction. If $n > 5$ and n is not a prime number, we let $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes and $k_i > 0$. By Theorems 1.5, 1.6 and Lemma 2.10, this is only possible if $n = 2^k 3, k = 1, 2, 3$. This implies that $|C(\mathbb{Z}_n)| = n$ by Theorems 1.3, 1.4 and 1.5, a contradiction. Thus $n = 5$. The converse is clear by Theorem 2.4. $\square$

Theorem 2.13. $|C(\mathbb{Z}_n)| = n - 2$ *if and only if* $n = 7, 9, 10, 16$.

Proof. Assume that $|C(\mathbb{Z}_n)| = n - 2$. By Example 2.1 and Theorems 1.1, 1.4 and 2.8, this is only possible if $n = 7, 9, 10, 16$ or $n > 16$. If $n > 16$ and n is a prime number, then, by Lemma 2.4, $|C(\mathbb{Z}_n)| \leq n - \frac{n-3}{2}$, this implies that $|C(\mathbb{Z}_n)| \leq n - 7 < n - 2$. This is a contradiction. Suppose that $n > 16$ and n is not prime. Then $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ for distinct primes $p_1, p_2, \ldots, p_m$ and $k_i > 0$. So $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$. Consider the case of $p_i \geq 3, k_i \geq 2$ or $p_i > 5, k_i = 1$ for some $i \in \{1, 2, \ldots, m\}$. Then by Theorems 2.7 and 2.9, $|C(\mathbb{Z}_{p_i^{k_i}})| < p_i^{k_i} - 1$. Thus, by Lemma 2.11, $|C(\mathbb{Z}_n)| < n - 2$, a contradiction. This implies that it is only possible if (i) $n = (2^k)(3)(5)$ for all $k > 0$, (ii) $n = (2^k)(3)$ for all $k > 3$ by Theorem 1.1, (iii) $n = 2^k$ for all $k > 4$. Consider the case of (i) $n = (2^k)(3)(5)$ for all $k > 0$. It is clear that there exist $(0, 0, 2), (0, 0, 3), (0, 1, 2), (0, 1, 3), (1, 0, 2), (1, 0, 3) \in \mathbb{Z}_{2^k} \times \mathbb{Z}_3 \times \mathbb{Z}_5$ such that $< (0, 0, 2) >=< (0, 0, 3) >, < (0, 1, 2) >=< (0, 1, 3) >$ and

$< (1,0,2) >=< (1,0,3) >$. This means that $|C(\mathbb{Z}_n)| \leq n-3 < n-2$, a contradiction. Finally, consider the cases of (ii) $n = (2^k)(3)$ for all $k > 3$ and (iii) $n = 2^k$ for all $k > 4$. By Theorem 2.8, Lemma 2.11 and $|C(\mathbb{Z}_{16})| = 14$, we have $|C(\mathbb{Z}_n)| < n-2$. This is a contradiction. Therefore $n = 7, 9, 10, 16$. The converse is clear by Example 2.1. $\square$

Acknowledgments: This paper was supported by the Faculty of Engineering, Rajamangala University of Technology Isan, Khon Kean Campus, Thailand.

References

[1] R. Belshoff, J. Dillstrom, L. Reid, Finite groups with a prescribed number of cyclic subgroups, Commun. Algebra, **47**, no. 3, (2019), 1043–1056.

[2] S. Pankaew, A. Rattana, R. Chinram, On the number of monogenic subsemigroups of semigroups $\mathbb{Z}_n$, Int. J. Math. Comput. Sci., **14**, no. 3, (2019), 557–561.

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