Songklanakarin J. Sci. Technol.
44 (5), 1179–1184, Sep. – Oct. 2022

http://www.sjst.psu.ac.th

Original Article

On (*m*, *k*) -type elements in the ring of integers modulo *n*

Phoschanun Ratanaburee, Montakarn Petapirak, and Sompong Chuysurichay*

Algebra and Applications Research Unit, Division of Computational Science, Faculty of Science, Prince of Songkla University, Hat Yai, Songkhla, 90110 Thailand

Received: 20 April 2022; Revised: 22 June 2022; Accepted: 10 July 2022

Abstract

An element a in a ring R is said to be of (m, k)-type if $a^m = a^k$ where m and k are positive integers with $m > k \geq 1$. Let $X_n(m, k)$ be the set of all (m, k)-type elements, $X^*_n(m, k)$ be the set of all nonzero (m, k)-type elements, and $S_n(m, k)$ be the set of all nonunit (m, k)-type elements in the ring of integers modulo n. In this paper, we study the algebraic structures of $X_n(m, k)$, $X^*_n(m, k)$ and $S_n(m, k)$ and characterize all values of n, m, and k for which $X_n(m, k)$ and $S_n(m, k)$ are cyclic semigroups and $X^*_n(m, k)$ is a cyclic group.

Keywords: (m, k)-type elements, ring of integers modulo n, m-potents, cyclic semigroup, cyclic group

1. Introduction

In ring theory, units, m - potents, nilpotents and unipotents are very familiar and are one of the most extensively studied elements of rings, particularly in the ring of integers modulo n. There are many studies in the literature about those elements (Breaz & Cimpean, 2018; Cheraghpour & Ghosseiri, 2019; Hou, 2021; Hummadi & Muhammad, 2010; Kanwar, Khatkar, & Sharma, 2017; MacHale, 1982; Mosic, 2015; Sibley, 2012; Zhou, 2018). In 1982, MacHale gave an upper bound value of idempotents in a finite ring (MacHale, 1982). Later, tripotents and idempotents in the ring of integers modulo n were studied by Hummadi and Muhammad (Hummadi & Muhammad, 2010) and Sibley (Sibley, 2012), respectively. In 2015, Mosic investigated several characterizations of m-potent elements in rings (Mosic, 2015).

In 2017, Kanwar, Khatkar and Sharma studied idempotents and units in a certain matrix ring over polynomial rings (Kanwar, Khatkar, & Sharma, 2017). Later, Breaz and Cimpean studied the class of rings R with the property that for any x in R at least one of the elements x and $1+x$ is tripotent (Breaz & Cimpean, 2018). In the same year, Zhou determined the rings for which every element is a sum of a nilpotent, an idempotent and a tripotent (Zhou, 2018).

*Corresponding author
Email address: sompong.c@psu.ac.th

Inspired by the work of these authors, we will introduce the (m, k)-type elements in the ring with identity and particularly investigate some of their properties in the certain ring, namely the ring $\mathbb{Z}_n$ of integers modulo n. Advantageously, such elements can be regarded as the generalization of units and m - potents. More precisely, the main purpose of this work is to study the algebraic structures of the set of all (m, k)-type elements, the set of all nonzero (m, k)-type elements, and the set of all nonunit (m, k)-type elements in $\mathbb{Z}_n$. This paper is organized as follows:

In Section 2, we provide some definitions, notations, and basic knowledge about elements in $\mathbb{Z}_n$ that will be used throughout this research.

In Section 3, the main purpose is separated into two parts. Firstly, we state general properties of the set of all (m, k)-type elements in $\mathbb{Z}_n$. In this subpart, we discover that in $\mathbb{Z}_n$ the set of all (m, k)-type elements is a subset of the set of all (r, s)-type elements if $m - k$ divides $r - s$, where r and s are positive integers with $r > s$. Moreover, for any positive integer t, the set of all (m, k)-type elements and the set of all $(m + t, k + t)$-type elements in $\mathbb{Z}_n$ coincide if n is a prime number. Secondly, we characterize all values of n, m, and k for which the set of all (m, k)-type elements and the set of all nonunit (m, k)-type elements in $\mathbb{Z}_n$ are cyclic semigroups. In this subpart, we prove that the set of all (m, k)-type elements in $\mathbb{Z}_n$ is a cyclic semigroup if and only if $n = 1$, and the set of all nonunit (m, k)-type elements in $\mathbb{Z}_n$ is a cyclic semigroup if and only if (n, m, k) is either one of the following triples:

1. (4, *m*, *k*),
2. (8, *m*, 2),
3. (*p*, *m*, *k*), where *p* is a prime,
4. (p^{α}, *m*, *1*), where *p* is a prime and $\alpha \geq 2$.

In Section 4, we determine the values of *n*, *m*, and *k* for which the set of all nonzero (*m*, *k*)-type elements in $\mathbb{Z}_n$ becomes a group and also a cyclic group. It turns out that the set of all nonzero (*m*, *k*)-type elements in $\mathbb{Z}_n$ is a group if and only if *n* is a prime number, and the set of all nonzero (*m*, 1)-type elements in $\mathbb{Z}_n$ is a group if and only if *n* is a power of prime number. In the scenario when *n* is a prime number, we get that the set of all nonzero (*m*, *k*)-type elements in $\mathbb{Z}_n$ is a cyclic group of order *r* if and only if gcd(*m*-*k*, *n*-1) = *r*. In the case that *n* is a power of 2, the set of all nonzero (*m*, 1)-type elements in $\mathbb{Z}_n$ is a cyclic group if and only if *m* is even. In the more general case that *n* is a power of an odd prime number, the set of all nonzero (*m*, 1)-type elements in $\mathbb{Z}_n$ is a cyclic group of order *r* if and only if gcd(ϕ (*n*), *m*-1) = *r*.

2. Preliminaries

Let *R* be an associative ring with identity. A nonzero element *a* of *R* is called a *zero divisor* if there is a nonzero element *b* in *R* such that either *ab* = 0 or *ba* = 0. An element *u* of *R* is called a *unit* in *R* if there is an element *v* in *R* such that *uv* = *1* = *vu*. For any positive integer $m \geq 2$, an *m-potent e* in *R* is an element satisfying $e^m = e$. A 2-potent and a 3-potent are respectively called an *idempotent* and a *tripotent*. For a pair of positive integers $m > k$, we say that an element *a* in *R* is of (*m*, *k*)-*type* if it satisfies the equation $a^m = a^k$. We can see from the definition that an idempotent is of (2,1)-type, a tripotent is of (3,1)-type and an *m*-potent is of (*m*, 1) -type.

For a fixed positive integer *n*, denote the ring $\mathbb{Z}_n$ of integers modulo *n* by

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

with the usual addition and multiplication. For convenience, we often write $a = b$ in $\mathbb{Z}_n$ or even $a = b$ instead of $a = b \pmod n$. It is well-known that $\mathbb{Z}_n$ is a commutative ring with identity. Every nonzero element in $\mathbb{Z}_n$ is either a unit or a zero divisor (Dummit & Foote, 2003).

Throughout this paper, we let *k*, *m*, *n* be positive integers such that $n \geq 2$ and $m > k$ For any ring $\mathbb{Z}_n$, the unit group of $\mathbb{Z}_n$ is denoted by $U(\mathbb{Z}_n)$ and ord(*x*) stands for the order of an element *x* in the group $U(\mathbb{Z}_n)$. The set of all (*m*, *k*)-type elements in $\mathbb{Z}_n$ and the set of all nonzero (*m*, *k*)-type elements in $\mathbb{Z}_n$ are denoted by $X_n(m, k)$ and $X^*_n(m, k)$, respectively. In other words, we have

$$X_n(m, k) = \{x \in \mathbb{Z}_n \mid x^m = x^k\}$$

and

$$X^*_n(m, k) = X_n(m, k) \backslash \{0\}.$$

We also define $S_n(m, k) = X_n(m, k) \backslash U(\mathbb{Z}_n)$.

We can easily observe that $X_n(m, k)$, $X^*_n(m, k)$ and $S_n(m, k)$ are nonempty subsets of $\mathbb{Z}_n$ as 1 is always an element of $X_n(m, k)$ and $X^*_n(m, k)$ and also $0 \in S_n(m, k)$. Moreover, $X_n(m, k)$ and $S_n(m, k)$ are semigroups under multiplication but $X^*_n(m, k)$ may or may not be a semigroup under multiplication. This leads us to explore the algebraic structures of $X_n(m, k)$, $X^*_n(m, k)$, and $S_n(m, k)$.

Suppose that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ where p_i are distinct prime numbers and $\alpha_i \geq 1$ for all $i = 1, 2, \ldots, t$. Let

$$\xi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_t^{\alpha_t}}$$

be defined by

$$\xi(x) = (x_1, x_2, \ldots, x_t)$$

for any $x \in \mathbb{Z}_n$ where $x \equiv x_i \pmod{p_i^{\alpha_i}}$ and $0 \leq x_i \leq p_i^{\alpha}-1$ for all $i = 1, 2, \ldots, t$. Then ξ is a ring isomorphism by the Chinese Remainder Theorem. For each $i = 1, 2, \ldots, t$, we define e_i in $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_t^{\alpha_t}}$ by $e_0 = (0, 0, \ldots, 0)$ and $e_i = (e_{i1}, e_{i2}, \ldots, e_{it})$ where

$$e_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

for $i = 1, 2, \ldots, t$. The following lemma will be used as our fundamental facts throughout the paper.

Lemma 1. (El-Kassar & Chehade, 2006) The group of units in $\mathbb{Z}_n$ when *n* is a power of prime number is given by

1. $U(\mathbb{Z}_2) \cong \{0\}$,
2. $U(\mathbb{Z}_4) \cong \mathbb{Z}_2$,
3. $U(\mathbb{Z}_{2^{\alpha}}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ where $\alpha \geq 3$,
4. $U(\mathbb{Z}_{p^{\alpha}}) \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\alpha-1}}$ where *p* is an odd prime.

3. The Semigroup Structures of $X_n(m, k)$, $X^*_n(m, k)$, and $S_n(m, k)$

Let *p* be a prime divisor of *n*. In this section, we will consider the semigroup structure of $X_n(m, k)$, $X^*_n(m, k)$, and $S_n(m, k)$. We begin by considering $X_n(m, k)$. As $\mathbb{Z}_n$ is a commutative ring, $(ab)^m = (ab)^k$ for all $a, b \in X_n(m, k)$. Then $X_n(m, k)$ is a semigroup.

Lemma 2. Let $x \in X_n(m, k)$. Then $x^{k+l(m-k)} = x^k$ for all positive integers *l*.

Proof. We proceed by induction on *l*. Let *x* be an element in $X_n(m, k)$. Clearly, $x^{k+(m-k)} = x^k$. Suppose that $x^{k+l(m-k)} = x^k$ for any $l \geq 1$. Then

$$x^{k+(l+1)(m-k)} = x^{k+l(m-k)} x^{m-k} = x^k x^{m-k} = x^k.$$

Hence, $x^{k+l(m-k)} = x^k$ for all positive integers *l*.

Theorem 1. Let *m*, *k*, *r*, *s* be positive integers such that $m > k \geq 1$ and $r > s \geq 1$. If $s \geq k$ and $m - k \mid r - s$, then $X_n(m, k) \subseteq X_n(r, s)$.

Proof. Suppose that $s \geq k$ and $m - k \mid r - s$. Since $m - k \mid r - s$, there exists a natural number *t* such that $r = s + t(m-k)$. Let *x* be an element in $X_n(m, k)$. By Lemma 2, we have $x^{k+t(m-k)} = x^k$, and so

$$x^r = x^{s+t(m-k)} = x^{s-k} x^{k+t(m-k)} = x^{s-k} x^k = x^s.$$

Hence, *x* is an element in $X_n(r, s)$. Therefore, $X_n(m, k) \subseteq X_n(r, s)$.

Remark 1. It follows from $s \geq k$ and $m - k \mid r - s$ that $r \geq m$. This can be seen by noticing that $r = s + l(m-k)$ for some $l \in \mathbb{Z}$. Thus $r \geq s + (m-k) = m + (s-k) \geq m$.

The following corollaries are immediate consequences of Theorem 1.

Corollary 1. For any positive integer *t*, $X_n(m, k) \subseteq X_n(m+t, k+t)$.

Corollary 2. $X_n(2, 1) \subseteq X_n(m, k)$ for all $m > k \geq 1$ and all $n \geq 2$.

The converse of Theorem 1 is not true in general because $X_5(5,2) = \{0, 1\} = X_5(7,2)$ but $(5-2) \nmid (7-2)$. Next, we give conditions for the sets $X_n(m, k)$ and $X_n(r, s)$ to be identical as sets. The following theorem shows that $X_n(m, k)$ and $X_n(m+t, k+t)$ coincide if n is a prime number.

Theorem 2. Let p be a prime number. Then $X_p(m, k) = X_p(m + t, k + t)$ for all positive integers t.

Proof. Let t be any positive integer. We already have $X_p(m, k) \subseteq X_p(m + t, k + t)$ from Corollary 1. Let x be an element in $X_p(m + t, k + t)$. For $x = 0$, we have $x \in X_p(m, k)$ Suppose that $x \neq 0$. Then $x^{m+t} = x^{k+t}$. Since $\mathbb{Z}_p$ is a field, x^{-1} exists. Then

$$x^m = x^{(m+t)-t} = x^{(k+t)-t} = x^k.$$

That is, x belongs to $X_p(m, k)$ as well. Therefore, $X_p(m, k) = X_p(m+t, k+t)$.

Next, we find an integer n with a pair (m, k) so that $X_n(m, k)$ and $S_n(m, k)$ are cyclic semigroups. A cyclic semigroup S is a semigroup generated by a single element. That is, $S = \{a, a^2, a^3, \ldots\}$ for some element a in S. If S is finite, there is the smallest positive integer m such that $a^m = a^t$ for some positive integer $t \neq m$, and there is the smallest positive integer r such that $a^m = a^{m+r}$. The positive integers m and r are called the *index* and the *period* of a cyclic semigroup S, respectively. Clearly, if S is a cyclic semigroup with index 1, then S is a cyclic group. Moreover, if $x \in S$ is a unit or an m-potent for some positive integer m, then $\langle x \rangle$ is a cyclic semigroup with index 1. The next theorem follows directly from (Toth, 2008).

Theorem 3. n is square-free if and only if every nonzero element in $\mathbb{Z}_n$ is either a unit or an m-potent for some $m \in \mathbb{Z}$. In particular,

$$x^{\phi(n)+1} \equiv x (\mathrm{mod} n) \text{ for all } x \in \mathbb{Z}_n.$$

As a consequence of Theorem 3, we have the following corollary and theorem.

Corollary 3. n is square-free if and only if $\langle x \rangle$ is a cyclic group for all $x \in \mathbb{Z}_n$.

Theorem 4. There is an element a in $\mathbb{Z}_n$ such that $\langle a \rangle$ is a cyclic semigroup with index 2 if and only if n is not square-free.

Proof. Let $n \geq 2$ be a positive integer. The necessity is obtained by Corollary 3. For the sufficiency, suppose that n is not square-free. Then $n = p^2k$ where p is prime and $k \in \mathbb{Z}$. Choose an $a = pk$. Then $a^l = 0$ for all $l \geq 2$. Thus $\langle a \rangle$ is a cyclic semigroup with index 2.

Theorem 5. $X_n(m, k)$ is not a cyclic semigroup for all positive integers $n \geq 2$.

Proof. It is clear that $0, 1, \in X_n(m, k)$. Suppose that $X_n(m, k) = \langle x \rangle$ for some $x \in X_n(m, k)$. Then there are distinct i, j such that $x^i = 0$ and $x^j = 1$. If $i < j$, then $x^t = 0$ for all $t \geq i$ and hence $0 = x^j = 1$, a contradiction. Then $i \geq j$. So there are integers r, s such that $i = js + r$ where $0 \leq r < j$. Thus $0 = x^i = x^{js+r} = x^r$. Since $j > r$, $1 = x^j = 0$, a contradiction. Hence, $X_n(m, k)$ is not a cyclic semigroup.

Theorem 6. $S_n(m, k)$ is a semigroup for all positive integers $n \geq 2$.

Proof. Let $x, y \in S_n(m, k)$. Clearly, $xy \in S_n(m, k)$ if $xy = 0$ Suppose that $xy \neq 0$. Since $x, y \in X_n(m, k)$,

$$(xy)^m = x^m y^m = x^k y^k = (xy)^k.$$

Then $xy \in X_n(m, k)$. As x is a zero divisor in $\mathbb{Z}_n$, there is $z \in \mathbb{Z}_n$ such that $xz = 0$. So $(xy)z = (xz)y = 0$. Thus xy is a zero divisor in $\mathbb{Z}_n$. Hence, $xy \in S_n(m, k)$.

It is clear that $S_4(m, k) = \{0\}$ or $\{0, 2\}$, $S_8(m, 1) = \{0\}$, $S_8(m, 2) = \{0, 4\}$, and $S_p(m, k) = \{0\}$.

Theorem 7. Let $n = p^\alpha$, where α is an integer greater than 1. Then $S_n(m, 1) = \{0\}$.

Proof. Suppose that $x \in S_n(m, 1)$ where $x \neq 0$. Then $x = p^l s$ for some positive integers l and s where $l < \alpha$ and $\gcd(p, s) = 1$. Let $q = \left\lceil \frac{\alpha}{l} \right\rceil$. Then $x, x^2, \ldots, x^q$ are distinct and $x^t = 0$ for all $t > q$. Thus $x \notin X_n(m, 1)$, a contradiction. Therefore, $S_n(m, 1) = \{0\}$, as required.

We note that $S_p(m, k)$, $S_4(m, k)$, $S_8(m, 1)$, $S_8(m, 2)$ and $S_n(m, 1)$ where $n = p^\alpha$ are cyclic semigroups. In fact, these are the only cases that $S_n(m, k)$ forms a cyclic semigroup. We prove this observation below.

First we observe that $S_8(m, k) = \{0, 2, 4, 6\}$ is not a cyclic semigroup for any $k \geq 3$.

Theorem 8. Let k and α be positive integers greater than 1. Suppose $n = p^\alpha$. If $n \geq 9$, then $S_n(m, k)$ is not a cyclic semigroup.

Proof. Let $k, \alpha \geq 2$. Suppose that $n = p^\alpha \geq 9$. Then $(p^{\alpha-1})^2 = 0$ in $\mathbb{Z}_n$ and hence $p^{\alpha-1} \in S_n(m, k)$. Choose $y = 3(p^{\lceil \alpha/2 \rceil})$ for $p = 2$ and $y = 2(p^{\lceil \alpha/2 \rceil})$ for $p \geq 3$. Then $y^2 = 0$ Since $n \geq 9$, $y \in \mathbb{Z}_n \setminus \{0\}$. This implies that $y \in S_n(m, k) \setminus \{0\}$. Suppose that $S_n(m, k) = \langle a \rangle$ for some $a \in S_n(m, k)$. Then $p^{\alpha-1} = a^i$ and $y = a^j$ for some positive integers i, j. Thus $a = p^r$ for some $1 \leq r \leq \alpha - 1$. Hence, $y = a^j = p^{rj}$, a contradiction. Therefore, $S_n(m, k)$ is not a cyclic semigroup.

Theorem 9. If n has at least two different prime divisors, then $S_n(m, k)$ is not a cyclic semigroup.

Proof. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ for some integer t such that $t \geq 2$. Let $x = \xi^{-1}(e_1)$. Clearly, e_0 and e_1 are not units in $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \mathbb{Z}_{p_t^{\alpha_t}}$. Moreover, $e^m{}_0 = e^k{}_0$ and $e^m{}_1 = e^k{}_1$. Thus there are $0, x \in \mathbb{Z}_n$ such that $\xi^{-1}(e_0) = 0$ and $\xi^{-1}(e_1) = x$. Hence, it follows that $0, x \in S_n(m, k)$.

Next, suppose that $e_0, e_1 \in \langle (x_1, x_2, \ldots, x_t) \rangle$ for some $x_i \in \mathbb{Z}_{p_i^{\alpha_i}}$. Then it is clear that $0, 1 \in \langle x_1 \rangle$. By mimicking the proof of Theorem 5, we have a contradiction. Hence, there is no element $a \in \mathbb{Z}_n$ such that $0, x \in \langle a \rangle$. This implies that $S_n(m, k)$ is not a cyclic semigroup.

In conclusion, we have the following result.

Theorem 10. $S_n(m, k)$ is a cyclic semigroup if and only if one of the following conditions holds:

1. $n = 4$.
2. $n = 8$ and $k \in \{1, 2\}$.

3. n is a prime.
4. $n = p^{\alpha}$ where $p \in$ is a prime, $\alpha \geq 1$ and $k = 1$.

4. The Group Structures of $X^*_n(m, k)$

In this section, we determine conditions on n and pairs (m, k) for which the set $X^*_n(m, k)$ is a group.

Theorem 11. Let p be a prime number. Then $X^*_p(m, k)$ is a group.

Proof. Since $X^*_n(m, k) \subseteq \mathbb{Z}_p \setminus \{0\} = U(\mathbb{Z}_p)$, which is a finite group, it is sufficient to show only that $X^*_p(m, k)$ is closed. Let a and b be elements in $X^*_p(m, k)$. Then $a^m = a^k$ and $b^m = b^k$. Since $U(\mathbb{Z}_p)$ is an abelian group,

$$(ab)^m = a^m b^m = a^k b^k = (ab)^k$$

This implies that ab belongs to $X^*_p(m, k)$. Hence, $X^*_p(m, k)$ is a subgroup of $U(\mathbb{Z}_p)$ and $X^*_p(m, k)$ is a group, as desired.

Note that if G is a group, then the identity element of G is the only idempotent element in G

Theorem 12. If n has at least two different prime divisors, then $X^*_n(m, k)$ is not a group.

Proof. Suppose that n has at least two different prime divisors. Applying Theorem 2 in (Sibley, 2012), we have $| X_n(2, 1) | \geq 2^2 = 4$. By Corollary 2, $X_n(2, 1) \subseteq X_n(m, k)$. Then $X^*_n(m, k)$ contains at least three nonzero idempotent elements. Therefore, $X^*_n(m, k)$ is not a group.

Corollary 4. If $X^*_n(m, k)$ is a group, then $n = p^{\alpha}$ where $\alpha \geq 1$.

The above corollary gives a necessary condition for $X^*_n(m, k)$ to be a group. It is clear that $X^*_n(m, k)$ is a group when n is a prime number. Now, we assume that $n = p^{\alpha}$ where $\alpha \geq 2$ in the following theorem.

Theorem 13. The following statements are equivalent.
1. $X^*_n(m, k)$ is a group.
2. $X^*_n(m, k)$ is a subset of the unit group $U(\mathbb{Z}_n)$.
3. $k = 1$

Proof. For the direction (1) $\Rightarrow$ (3), suppose that $k \geq 2$. Then $p^{\alpha-1}$ belongs to $\mathbb{Z}_n \setminus \{0\}$ and $(p^{\alpha-1})^2 = 0$ in $\mathbb{Z}_n$. It is easy to see that $p^{\alpha-1} \in X^*_n(m, k)$. Thus $X^*_n(m, k)$ is not a group as $p^{\alpha-1}$ has no inverse. As a consequence of Theorem 7, the direction (3) $\Rightarrow$ (2) is done. For the other direction, suppose $X^*_n(m, k) \subseteq U(\mathbb{Z}_n)$. Since $U(\mathbb{Z}_n)$ is a finite group, it suffices to show only that $X^*_n(m, k)$ is closed. Let $x, y \in X^*_n(m, k)$. Then $X^m = X^k$ and $y^m = y^k$. Since $U(\mathbb{Z}_n)$ is an abelian group,

$$(xy)^m = x^m y^m = x^k y^k = (xy)^k.$$

This implies $X^*_n(m, k)$ is closed. Then $X^*_n(m, k)$ is a group.

Example 1. Consider in $\mathbb{Z}_8$. Then we have $X^*_8(3, 1) = \{1, 3, 5, 7\}$ and $X^*_8(4, 1) = \{1\}$, which are groups. Observe further that $X^*_8(4, 1)$ is cyclic but $X^*_8(3, 1)$ is not cyclic.

Here is the necessary and sufficient condition of $X^*_n(m, k)$ for being a cyclic group.

Theorem 14. Let p be an odd prime. Then $X^*_p(m, k)$ is a cyclic group of order r if and only if $\gcd(m-k, p-1) = r$.

Proof. Let p be an odd prime. Assume that $X^*_p(m, k) = \langle a \rangle$ for some element a of order r in $X^*_p(m, k)$. Since $a^m = a^k$ and $X^*_p(m, k)$ is a group, a^{-1} exists and $a^{m-k} = 1$. Then r is a divisor of $m-k$. We know that $U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. Since $X^*_p(m, k)$ is a subgroup of $U(\mathbb{Z}_p)$, r is a divisor of $p-1$. Thus $r \mid \gcd(m - k, p-1)$. Suppose there exists an integer $q > r$ such that q is a divisor of both $m-k$ and $p-1$. Then $m = qs+k$ for some positive integer s. Since $U(\mathbb{Z}_p)$ is a cyclic group of order $p-1$ and $q \mid p-1$, there is an element y in $U(\mathbb{Z}_p)$ such that $\text{ord}(y) = q$. Then

$$(y^i)^m = (y^i)^{qs+k} = y^{iqs+ik} = (y^i)^k \text{ for all } 0 \leq i < q.$$

This implies that $\langle y \rangle \subseteq X^*_p(m, k)$, a contradiction.

Conversely, we assume that $\gcd(m - k, p-1) = r$. Then $m = rt + k$ for some positive integer t. Since $U(\mathbb{Z}_p)$ is a cyclic group of order $p-1$ and $r \mid p-1$, there exists an element a in $U(\mathbb{Z}_p)$ such that $\text{ord}(a) = r$. Thus

$$(a^i)^m = (a^i)^{rt+k} = a^{irt+ik} = (a^i)^k \text{ for all } 0 \leq i < r.$$

This implies $\langle a \rangle \subseteq X^*_p(m, k)$. Let x be an element in $X^*_p(m, k)$. Then $x^m = x^k$, and hence $x^{m-k} = 1$ as x^{-1} exists. Thus $\text{ord}(x) \mid m-k$. Since $X^*_p(m, k)$ is a subgroup of $U(\mathbb{Z}_p)$, $\text{ord}(x) \mid p-1$. Hence, $\text{ord}(x) \mid r$. Then $\text{ord}(x) = \frac{r}{s}$ for some positive integer S. Since $U(\mathbb{Z}_p)$ is a cyclic group, there is $y \in U(\mathbb{Z}_p)$ such that $U(\mathbb{Z}_p) = \langle y \rangle$. Let $\gamma_1 = \frac{p-1}{\text{ord}(x)}$ and $\gamma_2 = \frac{p-1}{r}$. Then $x = y^{\gamma_1}$ and $a = y^{\gamma_2}$. Hence $x = (y^{\gamma_2}) = a^s$. This implies that $x \in \langle a \rangle$. Therefore, $X^*_p(m, k) = \langle a \rangle$.

Immediate consequences of Theorem 14 are the following corollaries, assuming p is an odd prime.

Corollary 5. $X^*_p(m, k) = \{1\}$ if and only if $\gcd(m-k, p-1) = 1$.

Corollary 6. $X^*_p(m, k) = \{-1, 1\}$ if and only if $\gcd(m-k, p-1) = 2$.

Corollary 7. $X^*_p(m, k) = U(\mathbb{Z}_p)$ if and only if $p-1$ divides $m - k$.

We note that Corollary 7 gives an alternative proof of the famous Fermat's Little. Theorem as we also get $x^{pt} \equiv x \pmod{p}$ for all $x \in \mathbb{Z}_p$ and $t \in \mathbb{Z}_p$. Next, we assume that $k = 1$ and turn our attention to the case that n is a power of prime number. We start with a power of 2 by observing that $X^*_2(m, 1) = \{1\}$, $X^*_4(2s + 1, 1) = U(\mathbb{Z}_4) = \{-1, 1\}$ and $X^*_4(2s, 1) = \{1\}$ which are all cyclic groups. Let $n = 2^{\alpha}$ where $\alpha \geq 2$. Then $X^*_n(m, 1)$ is an abelian group. We consider necessary and sufficient conditions for $X^*_n(m, 1)$ to be a cyclic group.

Theorem 15. $X^*_n(m, 1) = \{1\}$ if and only if m is even.

Proof. Assume that $X^*_n(m, 1) = \{1\}$. Suppose that $m = 2s + 1$ for some positive integer s. Since $X^*_4(2s + 1, 1) = \{-1, 1\}$, we have $\alpha \geq 3$. By Lemma 1, $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$, which implies that $U(\mathbb{Z}_n)$ contains an element of order 2, say x. Then $x^m = x^{2s+1} = x$ and hence x belongs to $X^*_n(m, 1)$, a contradiction. Therefore, m is even.

Conversely, suppose that $m = 2t$ for some positive integer t. Let $x \in X^*_n(m, 1)$. By Theorem 13, $x \in U(\mathbb{Z}_n)$. Then $x^{2t-1} \equiv 1 \pmod{n}$ and hence $\text{ord}(x)$ is odd. This implies $x = 1$, a contradiction.

Theorem 16. $X^*_n(m, 1) = \{-1, 1\}$ if and only if $n = 4$ and m is odd.

Proof. Assume that $X^*_n(m, 1) = \{-1, 1\}$. Since $-1 \in X^*_n(m, 1)$, $(-1^m) = -1$. This implies that m is odd. Suppose that $\alpha \geq 3$. Then $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Since $(1, 0)$ and $(1, 2^{\alpha-3})$ are elements of order 2 in $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ there is an element x of order 2 in $U(\mathbb{Z}_n) \setminus \{-1, 1\}$. Then $x^{m-1} = 1$ as $m - 1$ is even and $\text{ord}(x) = 2$. Thus $x^m = x$ and hence $x \in X^*_n(m, 1)$, a contradiction. This concludes that $\alpha = 2$ and hence $n = 4$.

Conversely, suppose that $n = 4$ and m is odd. It is obvious that $1 \in X^*_n(m, 1)$. Since m is odd, $(-1)^m = -1$. Thus $-1 \in X^*_n(m, 1)$. Since $2^2 = 0$, $2 \notin U(\mathbb{Z}_n)$. By Theorem 13, $2 \notin X^*_n(m, 1)$. Therefore, $X^*_n(m, 1) = \{-1, 1\}$.

Next, we let $n = 2^\alpha$ where $\alpha \geq 3$.

Theorem 17. $X^*_n(m, 1) = U(\mathbb{Z}_n)$ if and only if $m \equiv 1 \pmod{2^{\alpha-2}}$.

Proof. Assume that $X^*_n(m, 1) = U(\mathbb{Z}_n)$. Since $(0, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ has order $2^{\alpha-2}$, there is an element x in $U(\mathbb{Z}_n) \setminus \{1\}$ such that x has order $2^{\alpha-2}$ Then x^{-1} exists as $U(\mathbb{Z}_n)$ is a group. Since $x^m = x$, we have $x^{m-1} = 1$. Thus $2^{\alpha-2} \mid m-1$. This means $m-1 \equiv 1 \pmod{2^{\alpha-2}}$.

Conversely, suppose that $m \equiv 1 \pmod{2^{\alpha-2}}$. Then there is a positive integer t such that $m = 2^{\alpha-2}t+1$. Let $x \in U(\mathbb{Z}_n)$. Note that $y^{2^{\alpha-2}} = 1$ for all $y \in U(\mathbb{Z}_n)$. Thus $x^{2^{\alpha-2}} = 1$ and $x^m = x^{2^{\alpha-2}t+1} = x$. Hence, $x \in X^*_n(m, 1)$ Therefore, $U(\mathbb{Z}_n) \subseteq X^*_n(m, 1)$. By Theorem 13, $X^*_n(m, 1) = U(\mathbb{Z}_n)$.

Theorem 18. $X^*_n(m, 1)$ is a cyclic group if and only if $X^*_n(m, 1) = \{1\}$.

Proof. Suppose $X^*_n(m, 1) \neq \{1\}$. By Theorem 15, m is odd. Since $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ and $H = \{(0, 2^{\alpha-3}), (1, 2^{\alpha-3}), (1, 0), (1, 0)\}$ is not a cyclic subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$, there is a noncyclic subgroup H' of $U(\mathbb{Z}_n)$ and H' is a subgroup of $X^*_n(m, 1)$. Hence, $X^*_n(m, 1)$ is not a cyclic group. The converse is obvious.

Theorem 19. Let $t \in \mathbb{Z}$, $\alpha \geq 4$ and β be an integer such that $1 \leq \beta \leq \alpha-3$. Then $X^*_n(2t, +1, 1) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^\beta}$ if and only if $t = 2^{\beta-1}s$ where s is an odd integer.

Proof. Let $t \in \mathbb{Z}$. Suppose that $X^*_n(2t, +1, 1) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^\beta}$ where $1 \leq \beta \leq \alpha-3$. Then there is an element $a \in X^*_n(2t, +1, 1)$ such that $\text{ord}(a) = 2^\beta$. Thus $a^{2t+1} = a$ and hence $a^{2t} = 1$. This implies that $2^\beta \mid 2t$. Hence, $t = 2^{\beta-1}s$ for some positive integer s. Suppose that s is even. Then there is an element $q = 2^\gamma$ with $\beta < \gamma \leq \alpha-2$ such that q is a divisor of both $2t$ and $2^{\alpha-2}$. Thus $2t = qr$ for some integer r. Note that $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. There is an element $x \in \mathbb{Z}_{2^{\alpha-2}}$ such that $\text{ord}(x) = q$. Then

$$(x^i)^{2t+1} = (x^{2t+1})^i = (x^{qr+1})^i = x^{qri+I} = x^i \text{ for all } 1 \leq i < q.$$

Hence, $(0, x^i) = (0, x^i)^{2t+1}$ and $(1, x^i) = (1, x^i)^{2t+1}$ for all $1 \leq i < q$. Thus there are at least $2q$ elements in $U(\mathbb{Z}_n)$ which belong to $X^*_n(2t, +1, 1)$. Then $|X^*_n(2t, +1, 1)| \geq 2^{\gamma+1} > 2^{\beta+1}$, a contradiction. This concludes that s is a positive odd integer.

Conversely, suppose that $t = 2^{\beta-1}s$ where s is an odd positive integer. Note that $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. There is an element $x \in \mathbb{Z}_{2^{\alpha-2}}$ such that $\text{ord}(x) = 2^\beta$. Then

$$(x^i)^{2t+1} = (x^{2t+1})^i = (x^{2(2^{\beta-1}s)+1})^i = (x^{2^\beta s+1})^i = x^{2^\beta si+i} = x^i$$

for all $1 \leq i < 2^\beta$. Thus $(0, x^i) = (0, x^i)^{2t+1}$ and $(1, x^i) = (1, x^i)^{2t+1}$ for all $1 \leq i < 2^\beta$ in $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Hence, there are at least $2^{\beta+1}$ elements in $U(\mathbb{Z}_n)$ which belong to $X^*_n(2t, +1, 1)$. Therefore, $X^*_n(2t, +1, 1) | \geq 2^{\beta+1}$. Suppose that $|X^*_n(2t, +1, 1)| > 2^{\beta+1}$. Then there is an element $a \in X^*_n(2t, +1, 1)$ such that $\text{ord}(a) = 2^\gamma$ for some γ such that $\beta < \gamma \leq \alpha-2$. Since $a^{2t+1} = a$, $2^\gamma \mid 2t$ which is a contradiction. This implies that $|X^*_n(2t, +1, 1)| = 2^{\beta+1}$. Since $X^*_n(2t, +1, 1) \subseteq U(\mathbb{Z}_n)$ and $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$, we have $X^*_n(2t, +1, 1) \cong H \times K$ for some $H \leq \mathbb{Z}_2$ and $K \leq \mathbb{Z}_{2^{\alpha-2}}$ such that $H \times K \leq \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Since $(0, x^i) = (0, x^i)^{2t+1}$ and $(1, x^i) = (1, x^i)^{2t+1}$ in $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$, $H \leq \mathbb{Z}_2$. It follows from $|X^*_n(2t, +1, 1)| = 2^{\beta+1}$ that $K = \mathbb{Z}_{2^\beta}$ Therefore, $X^*_n(2t, +1, 1)$ and $\mathbb{Z}_2 \times \mathbb{Z}_{2^\beta}$ are isomorphic as groups.

Next, we consider the case that $n = p^\alpha$ where p is an odd prime and $\alpha \geq 2$. It is known from Lemma 1 that $U(\mathbb{Z}_n)$ is isomorphic to the cyclic group $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\alpha-1}}$. By Theorem 13, $X^*_n(m, 1)$ is a cyclic group.

Theorem 20. Let r be a positive integer. Then $X^*_n(m, 1)$ is a cyclic group of order r if and only if $\gcd(\phi(n), m-1) = r$.

Proof. The proof uses the same idea as in Theorem 14.

Corollary 8. $X^*_n(m, 1) = \{1\}$ if and only if $\gcd(\phi(n), m-1) = 1$.

Corollary 9. $X^*_n(m, 1) = \{-1,1\}$ if and only if $\gcd(\phi(n), m-1) = 2$.

Corollary 10. $X^*_n(m, 1) = U(\mathbb{Z}_n)$ if and only if $\phi(n)$ divides $m-1$.

In conclusion, we obtain the following result.

Theorem 21. The following statements are equivalent:

1. $X^*_n(m, k)$ is a cyclic group.
2. $X^*_n(m, k)$ is a cyclic semigroup.
3. (n, m, k) is either one of the following triples:
   (i) $(2, m, k)$,
   (ii) $(4, m, 1)$,
   (iii) $(2^\alpha, 2t, 1)$, where $\alpha \geq 3$ and $t \geq 1$,
   (iv) (p, m, k) where p is an odd prime,
   (v) $(p^\alpha, m, 1)$, where p is an odd prime and $\alpha \geq 2$.

5. Conclusions

In this paper, we define (m, k)-type elements in a ring. This new notation can be considered as a generalization of units and m-potents. Some interesting properties of (m, k)-type elements are particularly investigated in $\mathbb{Z}_n$. The main task of this paper is to determine the algebraic structures of $X_n(m, k)$, $X^*_n(m, k)$, and $S_n(m, k)$ It turns out that $X_n(m, k)$, and $S_n(m, k)$ are semigroups for all positive integers $n \geq 2$ and $m > k \geq 1$, while $X^*_n(m, k)$ is a group if and only if (n, m, k) is either one of the following:

(i) (p, m, k) where p is prime,
(ii) $(p^\alpha, m, 1)$, where p is prime and $\alpha \geq 2$.

In addition, we characterize all values of n, m, and k for which those sets are cyclic semigroups or cyclic groups. Consequently, we also obtain an alternative proof of the Fermat Little Theorem as an extra gift.

In the general case that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, where p_i are distinct prime numbers and $\alpha_i \geq 1$ for all $i = 1, 2, \ldots, t$, the Chinese Remainder theorem may be applied via the isomorphism ξ to consider (m, k)-type elements in $X_n(m, k)$, $X^*_n(m, k)$, and $S_n(m, k)$: For any $x \in \mathbb{Z}_n$, x is an element in $X_n(m, k)$ if and only if x_i is an element in $X_{p_i^{\alpha_i}}(m, k)$ where $x \equiv x \pmod{p_i^{\alpha_i}}$ for all $i = 1, 2, \ldots, t$. Furthermore, we can replace $X_n(m, k)$ in the previous statement by $X^*_n(m, k)$ or $S_n(m, k)$ if the elements x_i in $\mathbb{Z}_{p_i^{\alpha_i}}$ are not all zeroes or not all units, respectively.

Acknowledgements

The first author is grateful to Development and Promotion of Science and Technology (DPST) for financial support. The authors would like to express their gratitude to the referees for their valuable comments and suggestions.

References

Breaz, S., & Cimpean, A. (2018). Weakly tripotent rings. *Bulletin of the Korean Mathematical Society, 55*(4), 1179–1187.

Cheraghpour, H., & Ghosseiri, N. M. (2019). On the idempotents, nilpotents, units and zero-divisors of finite rings. *Linear and Multilinear Algebra*, 67(2), 327–336.

Dummit, D. S., & Foote, R. M. (2003). *Abstract Algebra, 3rd ed*. New York, NY: John Wiley and Sons.

El-Kassar, A. N., & Chehade, H. Y. (2006). Generalized group of units. *Mathematica Balkanica, 20*, 275–286.

Hou, X. (2021). Idempotents in triangular matrix rings. *Linear and Multilinear Algebra*, *69*(2), 296–304.

Hummadi, P. A., & Muhammad, A. K. (2010). Smarandache triple tripotents in $\mathbb{Z}_n$ and in group ring $\mathbb{Z}_2$G *International Journal of Algebra, 4*(25), 1219–1229.

Kanwar, P., Khatkar, M., & Sharma, R. K. (2017). Idempotents and units of matrix rings over polynomial rings. *International Electronic Journal of Algebra*, *22*(22), 147–169.

MacHale, D. (1982). Idempotents in finite rings. *Royal Irish Academy*, *82A*(1), 9–12.

Mosic, D. (2015). Characterizations of *k*-potent elements in rings. *Annali di Mate-matica Pura ed Applicata, 194*(4), 1157–1168.

Sibley, T. Q. (2012). Idempotents ‘ala mod. *The College Mathematics Journal*, *43*(5), 401–404.

Toth, L. (2008). Regular integers modulo n. *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae Sectio Computatorica*, *29*, 263–275.

Zhou, Y. (2018). Rings in which elements are sums of nilpotents, idempotents and tripotents. *Journal of Algebra and Its Applications, 17*(01), 1850009–1-7.