KYUNGPOOK Math. J. 49(2009), 41-46

Ideals of the Multiplicative Semigroups $\mathbb{Z}_n$ and their Products

Wattapong Puninagool
Department of Mathematics, Udon Thani Rajabhat University, Udon Thani, 41000, Thailand
e-mail : wattapong1p@yahoo.com

Jintana Sanwong*
Department of Mathematics, Chiang Mai University, Chiang Mai, 50200, Thailand
e-mail : scmti004@chiangmai.ac.th

Abstract. The multiplicative semigroups $\mathbb{Z}_n$ have been widely studied. But, the ideals of $\mathbb{Z}_n$ seem to be unknown. In this paper, we provide a complete descriptions of ideals of the semigroups $\mathbb{Z}_n$ and their product semigroups $\mathbb{Z}_m \times \mathbb{Z}_n$. We also study the numbers of ideals in such semigroups.

1. Introduction

Many authors have studied the multiplicative semigroups $\mathbb{Z}_n$ in various aspects. For examples, Vandiver and Weaver [9] studied the cyclic subsemigroups generated by nonunit elements in $\mathbb{Z}_n$. In [2], Hewitt and Zuckerman followed [3] to study the semicharacters of $\mathbb{Z}_n$. Later, Ehrlich proved that $(\mathbb{Z}_n, +, \cdot)$ is regular if and only if n is square-free. In 1980, Livingstons solved the problem: compute H and D for the semigroup $\mathbb{Z}_n$ where $H = max\ \{h_a |\ a \in \mathbb{Z}_n\},\ D = lcm\ \{d_a |\ a \in \mathbb{Z}_n\}$ and h_a, d_a are the least positive integers such that $a^{h_a} = a^{h_a + d_a}$. Recently, Kemprasit and Buapradist showed that: in the multiplicative semigroups $\mathbb{Z}_n$, the set of bi-ideals and the set of quasi-ideals coincide if and only if either $n = 4$ or n is square-free.

In this papers, we determine all the ideals of these semigroups and their products. The study also show that they are a lot more ideals of $\mathbb{Z}_n$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ as semigroups than those of $\mathbb{Z}_n$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ as rings. As usual, if a and b are integers not both zero, then (a, b) denotes the *greatest common divisor* of a and b in $\mathbb{Z}$, and $a \mid b$ means *a divides b* in $\mathbb{Z}$. For each positive integer n, we write $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and regard this, in the usual way, as a semigroup under multiplication modulo n. That is, for each $a, b \in \mathbb{Z}_n$, we write $a.b$ (or simply ab) for the remainder $r \in \mathbb{Z}_n$ when the usual product of a and b in $\mathbb{Z}$ is divided by n. It will be clear from the context whether $a.b$ means this product in $\mathbb{Z}_n$ or the usual

* Corresponding author.
Received November 14, 2007; accepted 9 June 2008.
2000 Mathematics Subject Classification: 20M12.
Key words and phrases: ideals, integers modulo n, product semigroups.

product in $\mathbb{Z}$.

2. Ideals of $\mathbb{Z}_n$

We begin by describing the elements of each principal ideal in $\mathbb{Z}_n$.

Lemma 1. *If $a \in \mathbb{Z}_n$ and $d = n/(a,n)$ then $a\mathbb{Z}_n = \{0, a, 2a, \cdots, (d-1)a\}$ and $|a\mathbb{Z}_n| = d$.*

Proof. If $a = 0$ then $(0,n) = n$, so $d = 1$ and $a\mathbb{Z}_n = \{0\}$ as required. Suppose $a \neq 0$ and $x \in \mathbb{Z}_n$. By the Division Algorithm for $\mathbb{Z}$, we know $x = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r \le d-1$. Therefore, since $a/(a,n)$ is an integer, we have:

$$xa = qda + ra = qn \cdot \frac{a}{(a,n)} + ra \equiv ra \bmod n.$$

That is, $xa = ra$ in $\mathbb{Z}_n$, and it follows that $a\mathbb{Z}_n = \{0, a, 2a, \cdots, (d-1)a\}$. Moreover, if $xa = ya$ for some x, y such that $0 \le x < y \le d-1$ then $(x-y)a = kn$ for some $k \in \mathbb{Z}$. Hence

$$(x-y) \cdot \frac{a}{(a,n)} = kd,$$

where $a/(a,n)$ and d are coprime, and $0 < x - y < d$. Since this is impossible, we deduce that the elements of $\{0, a, 2a, \cdots, (d-1)a\}$ are distinct and hence $|a\mathbb{Z}_n| = d$. $\square$

The next result provides more information about the principal ideals of $\mathbb{Z}_n$.

Lemma 2. *For each non-zero $a \in \mathbb{Z}_n$, $a\mathbb{Z}_n = (a,n)\mathbb{Z}_n$.*

Proof. Since $a = (a,n).k$ for some $k \in \mathbb{Z}^+$ and $(a,n) \in \mathbb{Z}_n$, we have $a\mathbb{Z}_n \subseteq (a,n)\mathbb{Z}_n$. Conversely, by the Euclidean Algorithm, $(a,n) = ra + sn$ for some $r, s \in \mathbb{Z}$, hence $(a,n) \equiv ra \bmod n$. That is, $(a,n) = a.\ell$ for some $\ell \in \mathbb{Z}_n$ and so $(a,n)\mathbb{Z}_n \subseteq a\mathbb{Z}_n$. $\square$

Theorem 1. *Every ideal of $\mathbb{Z}_n$ is principal if and only if $n = p^k$ for some prime p and some integer $k \ge 0$. Moreover, in this event, the ideals of $\mathbb{Z}_n$ are precisely the set $p^t\mathbb{Z}_n$ where $0 \le t \le k$, and hence they form a chain under $\subseteq$.*

Proof. Suppose that every ideal of $\mathbb{Z}_n$ is principal, and assume that there are distinct prime divisors p, q of n. Then $p\mathbb{Z}_n \cup q\mathbb{Z}_n = x\mathbb{Z}_n$ for some $x \in \mathbb{Z}_n$ and, without loss of generality, we assume that $x \in p\mathbb{Z}_n$. This implies $x\mathbb{Z}_n \subseteq p\mathbb{Z}_n$, hence $q\mathbb{Z}_n \subseteq p\mathbb{Z}_n$ and so $q = pa$ for some $a \in \mathbb{Z}_n$. In other words, $q = pa + kn$ for some $k \in \mathbb{Z}$, and hence $p|q$, a contradiction. Therefore, $n = p^k$ for some integer $k \ge 0$, as required.

Conversely, suppose that $n = p^k$ for some integer $k \ge 0$, and let I be an ideal of $\mathbb{Z}_n$. Since $\{0\} = 0\mathbb{Z}_n$ and $\mathbb{Z}_n = 1\mathbb{Z}_n$, we can assume that I is non-trivial. Let $a \in I\backslash\{0\}$. If $p \nmid a$ then $(a, p^k) = 1$, hence $a \in U_n$, the group of units in $\mathbb{Z}_n$, and so $1 = a^{-1}a \in I$, contradicting our assumption. That is, each non-zero element of I is divisible by some (positive) power of p. Let t be the least positive s such that $p^s|a$ for some non-zero $a \in I$. Then I contains a non-zero element $a = p^t x$ where $p \nmid x$ (otherwise we contradict the choice of t). In fact, since $0 < a < n$, we have $0 < x < n$

and so $x \in U_n$. Consequently, $p^t = p^t x x^{-1} \in I$ and so $p^t\mathbb{Z}_n \subseteq I$. Moreover, if $b \in I$ and $b = p^r y$ then $r \geq t$ (by the choice of t) and $b = p^t.p^{r-t}y \in p^t\mathbb{Z}_n$, so $I \subseteq p^t\mathbb{Z}_n$ and equality follows. □

We have already known that $\mathbb{Z}_n$ as a ring is a principal ideal ring [5] p 133, Exercise 10(c). But, as a semigroup, $\mathbb{Z}_n$ is not principal (i.e., some ideals are not principal) if $n \neq p^k$ for some prime number p and $k \geq 1$ (see Theorem 2 for detail).

Recall that, if I is an ideal of a commutative semigroup S with identity, then $I = \cup\{aS : a \in I\}$; and conversely, the union of any family of principal ideals of S is an ideal of S. In fact, $aS \subseteq bS$ if and only if $b|a$. From this observation, we deduce the following result.

Theorem 2. *If I is a non-zero ideal of $\mathbb{Z}_n$, then $I = \cup\{m_i\mathbb{Z}_n : i = 1, \cdots, k\}$, where $m_1, \cdots, m_k$ are divisors of n such that $m_i \nmid m_j$ if $i \neq j$.*

Proof. By the above remarks, there exists $m_1, \cdots, m_k$ such that $I = \cup\{m_i\mathbb{Z}_n : i = 1, \cdots, k\}$. Clearly, we can assume $m_i \nmid m_j$ if $i \neq j$: otherwise, if $m_i | m_j$ then $m_j\mathbb{Z}_n \subseteq m_i\mathbb{Z}_n$ and so $m_j\mathbb{Z}_n$ can be omitted from the union. Also, by Lemma 2, $m_i\mathbb{Z}_n = (m_i, n)\mathbb{Z}_n$ for each $i = 1, \cdots, k$, so we can assume that each m_i is a divisor of n. □

As an application of Theorem 2, we get a characterization of ideals in the ring $\mathbb{Z}_n$.

Corollary 1. *As a ring, the ideals of $\mathbb{Z}_n$ are precisely the sets*

$$I = m\mathbb{Z}_n,$$

where m is a divisor of n.

Proof. Let I be an ideal of $\mathbb{Z}_n$. If $I = \{0\}$, then $I = n\mathbb{Z}_n$. But, if I is non-zero, then since $\mathbb{Z}_n$ is a principal ideal ring it follows from Theorem 2 that $I = m\mathbb{Z}_n$, where m is a divisor of n. □

Here, if we denote the number of the divisors of $n = p_1^{r_1} \cdots p_k^{r_k}$ where p_i are distinct primes and $r_i > 0$ for all i by $d(n)$ then we see that the number of ideals of $\mathbb{Z}_n$ (as ring) is

$$d(n) = (r_1 + 1) \cdots (r_k + 1)$$

(see [8] p167, Theorem 2 for detail). But, for the semigroup $\mathbb{Z}_n$ the number of its ideals is different except when $n = p^k$ for some prime p and $k > 0$.

Theorem 3. *The number of non-zero ideals in $\mathbb{Z}_n$ equals the number of sets $\{z_1, \cdots, z_k\}$ where $k \geq 1$, $z_i | n$ for each $i = 1, \cdots, k$ and, $z_i \nmid z_j$ if $i \neq j$.*

Proof. It suffices to show that, if I is a non-zero ideals of $\mathbb{Z}_n$ and $I = \cup\{x_i\mathbb{Z}_n : i = 1, \cdots, r\} = \cup\{y_j\mathbb{Z}_n : j = 1, \cdots, s\}$ where $\{x_1, \cdots, x_r\}$ and $\{y_1, \cdots, y_s\}$ satisfy the stated condition, then $r = s$ and $\{x_1, \cdots, x_r\} = \{y_1, \cdots, y_s\}$. To see this, first note that $x_1 \in y_j\mathbb{Z}_n$ for some $j \in \{1, \cdots, s\}$ and $y_j \in x_k\mathbb{Z}_n$ for some $k \in \{1, \cdots, r\}$, hence $x_1 = y_j u$ and $y_j = x_k v$ for some $u, v \in \mathbb{Z}_n$, so $x_1 = x_k vu$. Since $x_k | n$, this implies $x_k | x_1$, a contradiction unless $k = 1$. That is, $x_1\mathbb{Z}_n \subseteq y_j\mathbb{Z}_n \subseteq x_k\mathbb{Z}_n$, and thus

$x_1\mathbb{Z}_n = y_j\mathbb{Z}_n$. Consequently, $x_1 = y_ju$ and $y_j = x_1v$ and, since $y_j|n$ and $x_1|n$, we deduce that $y_j|x_1$ and $x_1|y_j$ in $\mathbb{Z}$, so $x_1 = y_j$. Similarly, $\{x_2, \cdots, x_r\} \subseteq \{y_1, \cdots, y_s\}$ and hence $r \leq s$. Using the same argument, but starting with y_1, we find that $\{y_1, \cdots, y_s\} \subseteq \{x_1, \cdots, x_r\}$, hence $s \leq r$ and so the two sets are equal. $\square$

3. Ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$

The Chinese Remainder Theorem states that, if m, n are coprime, then $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ as rings, hence they are isomorphic as semigroups in this event (for a proof, see [5]). However, if $(m, n) \neq 1$ then, as semigroups, $\mathbb{Z}_{mn}$ may not be isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$. To illustrate this, we first remark that, if p is prime and $k \geq 1$, then the only idempotents in $\mathbb{Z}_{p^k}$ are 0 and 1.

Example 1. By the last remark, the only non-trivial idempotents in $\mathbb{Z}_3 \times \mathbb{Z}_4$ are $(1, 0)$ and $(0, 1)$, and we know $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$, so $\mathbb{Z}_{12}$ contains exactly two non-trivial idempotents. Now, if $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_6$ is an idempotent then $a = 0, 1$ and $b = 0, 1, 3, 4$ so $\mathbb{Z}_2 \times \mathbb{Z}_6$ contains more than two non-trivial idempotents. Hence, $\mathbb{Z}_{12} \ncong \mathbb{Z}_2 \times \mathbb{Z}_6$ as semigroups.

More generally, Suppose $p \neq q$ are primes. Then the Chinese Remainder Theorem implies $\mathbb{Z}_{pq^2} \cong \mathbb{Z}_p \times \mathbb{Z}_{q^2}$, hence $\mathbb{Z}_{pq^2}$ contains exactly two non-trivial idempotents. Likewise, $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$, so $\mathbb{Z}_{pq}$ contains exactly two non-trivial idempotents. Therefore, $\mathbb{Z}_{pq^2} \ncong \mathbb{Z}_q \times \mathbb{Z}_{pq}$, since $\mathbb{Z}_q \times \mathbb{Z}_{pq}$ contains at least four non-trivial idempotents.

In view of these remarks, we now determine all ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$. Like before, since $\mathbb{Z}_m \times \mathbb{Z}_n$ contains an identity, every non-zero ideal I of $\mathbb{Z}_m \times \mathbb{Z}_n$ can be written as

$$I = \bigcup\{(a_i, b_i) \cdot \mathbb{Z}_m \times \mathbb{Z}_n : i = 1, \cdots, k\} = \bigcup\{a_i\mathbb{Z}_m \times b_i\mathbb{Z}_n : i = 1, \cdots, k\}$$

for some $k \geq 1$ and some a_i, b_i in $\mathbb{Z}_m, \mathbb{Z}_n$ respectively. In fact, by Lemma 2, we can assume that

(A1) each $a_i = 0$ or $a_i|m$ and, each $b_i = 0$ or $b_i|n$.

We can also assume that $(a_i, b_i) \neq (0, 0)$ for each $i = 1, \cdots, k$ and that $a_i \nmid a_j$ or $b_i \nmid b_j$ if $i \neq j$ (for the same reason as before). Clearly, this means

(A2) if $i \neq j$ and $a_i = 0$, $b_i \neq 0$, then $b_j \nmid b_i$,
(A3) if $i \neq j$ and $a_i \neq 0$, $b_i = 0$, then $a_j \nmid a_i$,
(A4) if $i \neq j$ and $a_i \neq 0$, $b_i \neq 0$, then $a_i \nmid a_j$ or $b_i \nmid b_j$.

In other words, we have the following result.

Theorem 4. *If I is a non-zero ideal of $\mathbb{Z}_m \times \mathbb{Z}_n$, then $I = \bigcup\{a_i\mathbb{Z}_m \times b_i\mathbb{Z}_n : i = 1, \cdots, k\}$ for some $k \geq 1$ and some $(a_i, b_i) \in \mathbb{Z}_m \times \mathbb{Z}_n$ which satisfy* (A1) - (A4).

In general, if R_1, R_2 are rings with identities, then all ideals of $R_1 \times R_2$ have the form $I \times J$ for some ideals I, J of R_1, R_2 respectively [5] p135, Exercise 22(a).

But, this is not true for semigroup $\mathbb{Z}_m \times \mathbb{Z}_n$. For example, $K = (1,0)\mathbb{Z}_m \bigcup (0,1)\mathbb{Z}_n$ is an ideal of $\mathbb{Z}_m \times \mathbb{Z}_n$ by Theorem 4, but K does not equal $A \times B$ for any ideals A, B of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively. However, as an application of Theorem 4, we get a characterization of ideals in the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ as follows:

Corollary 2. *As a ring, the ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$ are precisely the sets*

$$J = u\mathbb{Z}_m \times v\mathbb{Z}_n,$$

where u and v are divisors of m and n respectively.

Proof. Let J be an ideal of $\mathbb{Z}_n$. If $J = \{(0,0)\}$, then $J = m\mathbb{Z}_m \times n\mathbb{Z}_n$. But, if J is non-zero, then since $\mathbb{Z}_m \times \mathbb{Z}_n$ is a principal ideal rings we have $J = (u,v)\mathbb{Z}_m \times \mathbb{Z}_n = u\mathbb{Z}_m \times v\mathbb{Z}_n$ where $u = 0$ or $u \mid m$; and $v = 0$ or $v \mid n$ by Theorem 4. Since $0\mathbb{Z}_t = t\mathbb{Z}_t$, so $J = u\mathbb{Z}_m \times v\mathbb{Z}_n$ where u, v are divisors of m, n respectively. □

In view of Corollary 2 and Corollary 1, we have the number of ideals of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ where the prime decompositions of $m = p_1^{r_1} \cdots p_k^{r_k}$ and $n = q_1^{s_1} \cdots q_t^{s_t}$ is

$$d(m)d(n) = (r_1 + 1) \cdots (r_k + 1)(s_1 + 1) \cdots (s_t + 1).$$

But, for the semigroup $\mathbb{Z}_m \times \mathbb{Z}_n$ the result is completely different:

Theorem 5. *The number of non-zero ideals in $\mathbb{Z}_m \times \mathbb{Z}_n$ equals the number of the sets $\{(a_1, b_1), \cdots, (a_k, b_k)\}$ where $k \geq 1$ and $(a_i, b_i) \in \mathbb{Z}_m \times \mathbb{Z}_n$ which satisfy* (A1) - (A4).

Proof. Let I be a non-zero ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$ and $I = \bigcup\{a_i\mathbb{Z}_m \times b_i\mathbb{Z}_n : i = 1, \cdots, r\}$ $= \bigcup\{c_j\mathbb{Z}_m \times d_j\mathbb{Z}_n : j = 1, \cdots, s\}$ where (a_i, b_i) and (c_j, d_j) satisfy (A1) - (A4). We aim to prove that $r = s$ and $\{(a_1, b_1), \cdots, (a_r, b_r)\} = \{(c_1, d_1), \cdots, (c_s, d_s)\}$. For convenience, let $B = \{(a_1, b_1), \cdots, (a_r, b_r)\}$ and $C = \{(c_1, d_1), \cdots, (c_s, d_s)\}$. First, we note that $(a_1, b_1) \in c_\ell\mathbb{Z}_m \times d_\ell\mathbb{Z}_n$ for some $\ell \in \{1, \cdots, s\}$ and $(c_\ell, d_\ell) \in a_k\mathbb{Z}_m \times b_k\mathbb{Z}_n$ for some $k \in \{1, \cdots, r\}$, hence $a_1 = c_\ell u, b_1 = d_\ell v$ and $c_\ell = a_k x, d_\ell = b_k y$ for some $u, x \in \mathbb{Z}_m$ and $v, y \in \mathbb{Z}_n$, so $a_1 = a_k xu$ and $b_1 = b_k yv$. We claim that $(a_1, b_1) = (c_\ell, d_\ell)$. And, consider the ordered pairs $(a_k, b_k) \in B$ and $(c_\ell, d_\ell) \in C$ in the following cases:

Case 1. $a_k = 0$. Then $c_\ell = a_k x = 0 \cdot x = 0 = c_\ell u = a_1$ which implies $b_1 \neq 0 \neq d_\ell$. From $a_k = 0$, we must have $0 \neq b_k \mid n$ and thus $b_k \mid b_1$ (since $b_1 = b_k yv$), so $b_k = b_1$ otherwise it will contradict to that B satisfies (A1) - A(4). Since $b_1 = d_\ell v, d_\ell = b_k y$ and $d_\ell \mid n, b_k \mid n$, it follows that $d_\ell \mid b_1$ and $b_1 = b_k \mid d_\ell$ and hence $b_1 = d_\ell$.

Case 2. $b_k = 0$. By using the same arguments as given in case 1, but starting with $d_\ell = b_k y = 0 \cdot y = 0 = d_\ell v = b_1$ and $a_1 = a_k xu$ we get $a_1 = c_\ell$.

Case 3. $c_\ell = 0$. Then $a_1 = c_\ell u = 0 \cdot u = 0 = c_\ell$ which implies $b_1 \neq 0 \neq d_\ell$. If $b_k = 0$, then $d_\ell = b_k y = 0 \cdot y = 0 = 0 \cdot v = b_1$ which is a contradiction. So $b_k \mid n$, and since $d_\ell = b_k y$ we get $b_k \mid d_\ell$. Since $b_1 = d_\ell v$ and $d_\ell \mid n$, so $d_\ell \mid b_1$. Thus $b_k \mid b_1$ and $0 \neq a_k \mid a_1$ and B satisfies (A4) imply $k = 1$, hence $a_k = a_1$ and $b_k = b_1$. From $b_1 = b_k \mid d_\ell$ and $d_\ell \mid b_1$, we get $b_1 = d_\ell$.

Case 4. $d_\ell = 0$. By using the same arguments as given in case 3, but starting with $b_1 = d_\ell v = 0 \cdot v = 0 = d_\ell$ and consider a_k instead of b_k we find that $a_1 = c_\ell$.

Case 5. $a_k, b_k, c_\ell, d_\ell \notin \{0\}$. Then $a_k \mid m$, $c_\ell \mid m$ and $b_k \mid n, d_\ell \mid n$. From $a_1 = a_k xu, b_1 = b_k yv$ and $a_k \mid m$, $b_k \mid n$, we get $a_k \mid a_1$ and $b_k \mid b_1$. Since (a_k, b_k) and (a_1, b_1) satisfy (A4), so $k = 1$, this means $a_k = a_1$ and $b_k = b_1$. Since $c_\ell = a_k x, a_1 = c_\ell u$ and $a_k \mid m, c_\ell \mid m$, it follows that $a_1 = a_k \mid c_\ell$ and $c_\ell \mid a_1$ which implies $a_1 = c_\ell$. From $b_1 = d_\ell v, d_\ell = b_k y$ and $d_\ell \mid n, b_k \mid n$, we get $d_\ell \mid b_1$ and $b_1 = b_k \mid d_\ell$, so $b_1 = d_\ell$.

Therefore, in each cases we get $(a_1, b_1) = (c_\ell, d_\ell)$. Similarly, we can prove that $\{(a_2, b_2), \cdots, (a_r, b_r)\} \subseteq \{(c_1, d_1), \cdots, (c_s, d_s)\}$ and hence $r \leq s$. Using the same arguments, but beginning with (c_1, d_1) we find that $\{(c_1, d_1), \cdots, (c_s, d_s)\} \subseteq \{(a_1, b_1), \cdots, (a_r, b_r)\}$, hence $s \leq r$ and so $s = r$ and the two sets are equal. □

Acknowledgment. The authors would like to thank Professor R. P. Sullivan at University of Western Australia for his help in writing this paper.

References

[1] G. Ehrlich, *Unit-regular ring*, Portugaliae Math., **27**(1968), 209-212.

[2] E. Hewitt and H. S. Zuckerman, *The multiplicative semigroup of integers modulo m*, Pacific J. Math., **10**(1960), 1291-1308.

[3] E. Hewitt and H. S. Zuckerman, *Finitely dimensional convolution algebras*, Acta Math. **93**(1955), 67-119.

[4] J. M. Howie, An Introduction to Semigroup Theory, Academic Press, London, 1976.

[5] T. M. Hungerford, Algebra, Spring-Verlag, Newyork, 2003.

[6] Y. Kemprasit and S. Buapradist, *A note on the multiplicative semigroup $\mathbb{Z}_n$ whose bi-ideals are quasi-ideals*, Southeast Asian Bull. Math., Springer-Verlag **25**(2001), 269-271.

[7] A. E. Livingston and M. L. Livingston, *The congruence $a^{r+s} \equiv a^r (mod\ m)$*, Amer. Math. Monthly, **85**(1980), 811-814.

[8] W. Sierpinski, Elementary Theory of Numbers, PWN-Polish Scientific Publisher, Warszawa, 1988.

[9] H. S. Vandiver and M. W. Weaver, *Introduction to arithmetic factorization and congruences from the standpoint of abstract algebra*, Amer. Math. Monthly, **65**(1958), 48-51.