Some Results on Homomorphisms of Hypergroups

W. Phanthawimol and Y. Kemprasit

Department of Mathematics, Faculty of Science
Chulalongkorn University, Bangkok 10330, Thailand
golfma35@yahoo.com, yupaporn.k@chula.ac.th

Abstract

A homomorphism of a hypergroup \((H, \circ)\) is a function \(f : H \to H\) satisfying \(f(x \circ y) \subseteq f(x) \circ f(y)\) for all \(x, y \in H\). A homomorphism of a hypergroup \((H, \circ)\) is called an epimorphism if \(f(H) = H\). Denote by \(\text{Hom}(H, \circ)\) and \(\text{Epi}(H, \circ)\) the set of all homomorphisms and the set of all epimorphisms of a hypergroup \((H, \circ)\), respectively. In this paper, the elements of \(\text{Hom}(\mathbb{Z}_n, \circ_m)\) and \(\text{Epi}(\mathbb{Z}_n, \circ_m)\) are characterized where \((\mathbb{Z}_n, \circ_m)\) is the hypergroup \(\mathbb{Z}_n\) with the hyperoperation \(\circ_m\) defined by \(x\circ_m y = x + y + m\mathbb{Z}_n\) for all \(x, y \in \mathbb{Z}\). In addition, \(|\text{Hom}(\mathbb{Z}_n, \circ_m)|\) and \(|\text{Epi}(\mathbb{Z}_n, \circ_m)|\) are determined.

Mathematics Subject Classification: 20N20

Keywords: Hypergroup, homomorphism, epimorphism

1 Introduction and Preliminaries

The cardinality of a set \(X\) is denoted by \(|X|\).

A hyperoperation on a nonempty set \(H\) is a function \(\circ : H \times H \to \mathcal{P}(H) \setminus \{\emptyset\}\) where \(\mathcal{P}(H)\) is the power set of \(H\). The value of \((x, y) \in H \times H\) under \(\circ\) is denoted by \(x \circ y\). We call the system \((H, \circ)\) a hypergroupoid. For nonempty subsets \(A, B\) of \(H\) and \(x \in H\), let

\[A \circ B = \bigcup_{a \in A} a \circ b, \quad A \circ x = A \circ \{x\}\text{ and }x \circ A = \{x\} \circ A.\]

The hypergroupoid \((H, \circ)\) is called a semihypergroup if

\[x \circ (y \circ z) = (x \circ y) \circ z\text{ for all }x, y, z \in H.\]

A hypergroup is a semihypergroup \((H, \circ)\) satisfying
\[ H \circ x = x \circ H = H \text{ for all } x \in H. \]

Then every group is a hypergroups.

By a homomorphism of a hypergroup \((H, \circ)\) we mean a function \(f : H \to H\) such that

\[ f(x \circ y) \subseteq f(x) \circ f(y) \text{ for all } x, y \in H. \]

If the equality is valid, \(f\) is called a good homomorphism of \((H, \circ)\). A homomorphism of \((H, \circ)\) is called a good homomorphism of \((H, \circ)\) satisfying \(f(H) = H\). Let \(\text{Hom}(H, \circ)\) and \(\text{Epi}(H, \circ)\) denote the set of all homomorphisms and the set of all epimorphisms of \((H, \circ)\), respectively. In particular, if \(G\) is a group, \(\text{Hom}(G)\) \([\text{Epi}(G)]\) is the set of all homomorphisms \([\text{epimorphisms}]\) of \(G\).

If \(G\) is a group, \(N\) is a normal subgroup of \(G\) and \(\circ\) \(N\) is the hyperoperation on \(G\) defined by

\[ x \circ y = xyN \text{ for all } x, y \in G, \]

then \((G, \circ_N)\) is a hypergroup ([2], p.11). Let \(\mathbb{Z}\) be the set of integers, \(\mathbb{Z}^+\) the set of positive integers and \(\mathbb{Z}_n\) the set of integers modulo \(n \in \mathbb{Z}^+\). The equivalence class of \(x\) modulo \(n\) is denoted by \(x \mod n\). For \(x, y \in \mathbb{Z}\), not both 0, let \((x, y)\) denote the g.c.d. of \(x\) and \(y\). Then

\[ \mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \{x \mod n \mid x \in \mathbb{Z}\}, |\mathbb{Z}_n| = n, \]

and for \(m \in \mathbb{Z}\),

\[ m \mathbb{Z}_n = (m, n)\mathbb{Z}_n = \{0, (m, n), \ldots, \left(\frac{n}{(m, n)} - 1\right)(m, n)\}, |m\mathbb{Z}_n| = \frac{n}{(m, n)}. \]

It can be seen that

\[ \mathbb{Z}_n = \bigcup_{i=0}^{(m,n)-1} (\overline{i} + (m, n)\mathbb{Z}_n) \]

which is a disjoint union. As mentioned above, we have that \((\mathbb{Z}, \circ_{m\mathbb{Z}})\) and \((\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})\) are hypergroups where

\[ x \circ_{m\mathbb{Z}} y = x + y + m\mathbb{Z} \text{ for all } x, y \in \mathbb{Z}, \]

\[ \overline{x} \circ_{m\mathbb{Z}_n} \overline{y} = \overline{x + y + m\mathbb{Z}_n} \text{ for all } x, y \in \mathbb{Z}. \]

In [3], the authors characterized the good homomorphisms and good epimorphisms of \((\mathbb{Z}, \circ_{m\mathbb{Z}})\). Such homomorphisms were also counted. We characterized the elements of \(\text{Hom}(\mathbb{Z}, \circ_{m\mathbb{Z}})\) and \(\text{Epi}(\mathbb{Z}, \circ_{m\mathbb{Z}})\) in [4] and also proved that \(|\text{Hom}(\mathbb{Z}, \circ_{m\mathbb{Z}})| = |\text{Epi}(\mathbb{Z}, \circ_{m\mathbb{Z}})| = 2^{\aleph_0}\).

For \(a \in \mathbb{Z}\), let \(h_\pi : \mathbb{Z}_n \to \mathbb{Z}_n\) be defined by \(h_\pi(\overline{x}) = \overline{ax}\) for all \(x \in \mathbb{Z}\). From the fact mentioned above, \(a\mathbb{Z}_n = \mathbb{Z}_n\) if and only if \((a, n) = 1\). Hence
Some results on homomorphisms of hypergroups

$\text{Hom}(\mathbb{Z}_n, +) = \{h_a | a \in \mathbb{Z}\}$ and $\text{Epi}(\mathbb{Z}_n, +) = \{h_a | a \in \mathbb{Z} \text{ and } (a, n) = 1\}$

which imply that $|\text{Hom}(\mathbb{Z}_n, +)| = n$ and $|\text{Epi}(\mathbb{Z}_n, +)| = \varphi(n)$ where $\varphi$ is the Euler phi-function.

In this paper, we aim to characterize the elements of $\text{Hom}(\mathbb{Z}_n, \circ_m \mathbb{Z}_n)$ and $\text{Epi}(\mathbb{Z}_n, \circ_m \mathbb{Z}_n)$. These sets are also counted.

We note that some results of homomorphisms and good homomorphisms of certain hypergroups can be also seen in [1].

2 Homomorphisms of the Hypergroup $(\mathbb{Z}_n, \circ_m \mathbb{Z}_n)$

To characterize the elements of $\text{Hom}(\mathbb{Z}_n, \circ_m \mathbb{Z}_n)$, the following lemma is needed.

Lemma 2.1. Let $G$ be a group, $N \lhd G$ and $f \in \text{Hom}(G, \circ_N)$. Then the following statements hold.

(i) $f(N) \subseteq N$.

(ii) For all $x \in G$, $f(xN) \subseteq f(x)N$.

(iii) For all $x, y \in G$, $f(xyN) \subseteq f(xy)N = f(x)f(y)N$.

(iv) For all $x \in G$, $f(x^{-1}N) \subseteq f(x^{-1})N = f(x)^{-1}N$.

(v) For all $x \in G$ and $k \in \mathbb{Z}$, $f(x^kN) \subseteq f(x^k)N = f(x)^kN$.

Proof. First, we recall that for all $x, y \in G$, $xN \cap yN \neq \emptyset$ implies $xN = yN$.

(i) We have that

$$f(N) = f(eeN) = f(e \circ_N e) \subseteq f(e) \circ_N f(e) = f(e)f(e)N.$$ 

Then $f(e) \in f(N) \subseteq f(e)f(e)N$. Since $G$ is cancellative, we have $e \in f(e)N$ which implies that $N = f(e)N$, so $f(N) \subseteq f(e)f(e)N = N$.

(ii) By (i), $f(e) \in N$. If $x \in G$, then

$$f(xN) = f(xeN) = f(x \circ_N e)$$
$$\subseteq f(x) \circ_N f(e)$$
$$= f(x)f(e)N$$
$$= f(x)N.$$ 

(iii) Let $x, y \in G$. Then by (ii),

$$f(xyN) \subseteq f(xy)N.$$
We also have that
\[ f(xyN) = f(x \circ_N y) \]
\[ \subseteq f(x) \circ_N f(y) \]
\[ = f(x)f(y)N. \]

These imply that \( f(xy)N = f(x)f(y)N \). Hence (iii) holds.

(iv) If \( x \in G \), then
\[ f(N) = f(xx^{-1}N) = f(x \circ_N x^{-1}) \subseteq f(x)f(x^{-1})N. \]

But \( f(N) \subseteq N \) by (i), so \( f(N) \subseteq N \cap f(x)f(x^{-1})N \). Then \( N = f(x)f(x^{-1})N \) which implies that \( f(x^{-1})N = f(x)^{-1}N \). By (ii), \( f(x^{-1})N \subseteq f(x^{-1})N \). Hence (iv) holds.

(v) Let \( x \in G \). Then by (ii), for all \( k \in \mathbb{Z} \), \( f(x^kN) \subseteq f(x^k)N \). It remains to show that \( f(x^k)N = f(x)^kN \) for all \( k \in \mathbb{Z} \). This is true for \( k = 0 \) and 1. Assume that \( k \in \mathbb{Z}^+ \) and \( f(x^k)N = f(x)^kN \). Then
\[ f(x^{k+1})N = f(x^kN) \]
\[ = f(x)f(x^kN) \]
\[ = f(x)(f(x^k)N) \]
\[ = f(x)(f(x)^kN) \]
\[ = f(x)^{k+1}N. \]

This shows that \( f(y^l)N = f(y)^lN \) for all \( y \in G \) and \( l \in \mathbb{Z}^+ \). If \( k \in \mathbb{Z}^+ \), then
\[ f(x^{-k})N = f((-x)^{-k})N \]
\[ = f(x^{-1})^kN \]
\[ = (f(x^{-1})N) \ldots (f(x^{-1})N) \quad (k \text{ brackets}) \]
\[ = (f(x)^{-1}N) \ldots (f(x)^{-1}N) \quad \text{from (iv)} \]
\[ = (f(x)^{-1})^kN \]
\[ = f(x)^{-k}N. \]

Hence (v) is proved. \( \square \)

**Theorem 2.2.** For \( f : \mathbb{Z}_n \to \mathbb{Z}_n \), the following statements are equivalent.

(i) \( f \in \text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n}) \).
(ii) \( f(\overline{x} + m\mathbb{Z}_n) \subseteq x f(\overline{1}) + m\mathbb{Z}_n \) for all \( x \in \mathbb{Z} \).
(iii) There exists an integer \( a \) such that
\[ f(\overline{x} + m\mathbb{Z}_n) \subseteq x \overline{a} + m\mathbb{Z}_n \] for all \( x \in \mathbb{Z} \).
Proof. (i)⇒(ii) follows directly from Lemma 2.1(v).

(ii)⇒(iii) is evident.

(iii)⇒(i). Let \( x, y \in \mathbb{Z} \). Then \( f(x) \equiv f(y) \pmod{m \mathbb{Z}_n} \) and \( f(x) \equiv f(y) \pmod{m \mathbb{Z}_n} \). Since \( f(x) \equiv f(y) \pmod{m \mathbb{Z}_n} \), it follows that \( f(x) + m \mathbb{Z}_n = x + m \mathbb{Z}_n \) and \( f(y) + m \mathbb{Z}_n = y + m \mathbb{Z}_n \). Consequently,

\[
\begin{align*}
  f(x + m \mathbb{Z}_n, y + m \mathbb{Z}_n) &= f(x + m \mathbb{Z}_n) + f(y + m \mathbb{Z}_n) \\
  &\subseteq (x + y) + m \mathbb{Z}_n \\
  &= x + m \mathbb{Z}_n + y + m \mathbb{Z}_n \\
  &= f(x) + m \mathbb{Z}_n + f(y) + m \mathbb{Z}_n \\
  &= f(x, y) + m \mathbb{Z}_n \\
  &= f(x) + m \mathbb{Z}_n, f(y).
\end{align*}
\]

Hence \( f \in \text{Hom}(\mathbb{Z}_n, \mathbb{Z}_n) \), as desired. \( \square \)

**Lemma 2.3.** Let \( G \) be a group and \( N \triangleleft G \). For \( f \in \text{Hom}(G) \), \( f(N) \subseteq N \) if and only if \( f \in \text{Hom}(G, \circ_N) \).

Proof. First, assume that \( f(N) \subseteq N \). Then for all \( x, y \in G \),

\[
\begin{align*}
  f(x \circ_N y) &= f(xy)N \\
  &= f(x)f(y)N \\
  &\subseteq f(x)f(y)N \\
  &= f(x) \circ_N f(y).
\end{align*}
\]

Thus \( f \in \text{Hom}(G, \circ_N) \).

For the converse, assume that \( f \in \text{Hom}(G, \circ_N) \). Since \( f \in \text{Hom}(G) \), \( f(e) = e \). Then

\[
\begin{align*}
  f(N) &= f(eeN) = f(e \circ_N e) \subseteq f(e) \circ_N f(e) = f(e)f(e)N = N.
\end{align*}
\]

\( \square \)

**Theorem 2.4.** \( \text{Hom}(\mathbb{Z}_n, +) \subseteq \text{Hom}(\mathbb{Z}_n, \circ_{m \mathbb{Z}_n}) \).

Proof. If \( a \in \mathbb{Z} \), then \( h_{\mathbb{Z}_n}(m \mathbb{Z}_n) = am\mathbb{Z}_n = m(a\mathbb{Z}_n) \subseteq m\mathbb{Z}_n \), so by Lemma 2.3, \( h_{\mathbb{Z}_n} \in \text{Hom}(\mathbb{Z}_n, \mathbb{Z}_n) \). Hence \( \text{Hom}(\mathbb{Z}_n, +) \subseteq \text{Hom}(\mathbb{Z}_n, \circ_{m \mathbb{Z}_n}) \). \( \square \)

From Theorem 2.4, we have that \( |\text{Hom}(\mathbb{Z}_n, \circ_{m \mathbb{Z}_n})| \geq n \). We show in the next theorem that \( |\text{Hom}(\mathbb{Z}_n, \circ_{m \mathbb{Z}_n})| = n \left( \frac{n}{(m,n)} \right)^{n-1} \).

**Lemma 2.5.** If \( G \) is a group, then \( \text{Hom}(G, \circ_G) = \{ f \mid f : G \to G \} \).

Proof. If \( f : G \to G \), then for all \( x, y \in G \),

\[
\begin{align*}
  f(x \circ_G y) &= f(xyG) = f(G) \subseteq G = f(x)f(y)G = f(x) \circ_G f(y),
\end{align*}
\]

so \( f \in \text{Hom}(G, \circ_G) \). Hence the result follows. \( \square \)
Theorem 2.6. \(|\text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})| = n \left(\frac{n}{(m,n)}\right)^{n-1}\).

Proof. Recall that \(m\mathbb{Z}_n = (m, n)\mathbb{Z}_n\), \(|m\mathbb{Z}_n| = \frac{n}{(m,n)}\). \(\mathbb{Z}_n = \bigcup_{i=0}^{(m,n)-1} (i + (m, n)\mathbb{Z}_n)\) which is a disjoint union and note that for nonempty sets \(A, B, |\{f | f : A \to B\}| = |B|^{|A|}\).

Case 1: \((m, n) = 1\). Then \(m\mathbb{Z}_n = \mathbb{Z}_n\) and so \((\mathbb{Z}_n, \circ_{m\mathbb{Z}_n}) = (\mathbb{Z}_n, \circ_{\mathbb{Z}_n})\). By Lemma 2.5, \(|\text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})| = n^n\). Hence \(|\text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})| = n \left(\frac{n}{(m,n)}\right)^{n-1}\).

Case 2: \((m, n) > 1\). Then \(n > 1\). By Theorem 2.2, we have that

\(\text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n}) = \{f : \mathbb{Z}_n \to \mathbb{Z}_n | f(\overline{x + m\mathbb{Z}_n}) \subseteq n f(\overline{1}) + m\mathbb{Z}_n \text{ for all } x \in \mathbb{Z}\}\).

It follows that for \(f : \mathbb{Z}_n \to \mathbb{Z}_n\),

\[f \in \text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n}) \iff f((m, n)\mathbb{Z}_n) \subseteq (m, n)\mathbb{Z}_n,\]

\[f(\overline{1} + (m, n)\mathbb{Z}_n) \subseteq f(\overline{1}) + (m, n)\mathbb{Z}_n,\]

\[f(\overline{2} + (m, n)\mathbb{Z}_n) \subseteq 2f(\overline{1}) + (m, n)\mathbb{Z}_n,\]

\[\cdots\]

\[f(\overline{(m, n) - 1} + (m, n)\mathbb{Z}_n) \subseteq ((m, n) - 1)f(\overline{1}) + (m, n)\mathbb{Z}_n.\]

For \(f : \mathbb{Z}_n \to \mathbb{Z}_n\), all the possibilities of \(f(\overline{1})\) are \(\overline{0}, \overline{1}, \ldots, \overline{n - 1}\). We have that \(f(\overline{1}) \in f(\overline{1} + (m, n)\mathbb{Z}_n)\). From these facts, we have

\[|\text{Hom}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})| = n \times \left(\frac{n}{(m,n)}\right)^{(m,n) - 1} \times \left(\frac{n}{(m,n)}\right)^{n-1} \times \cdots \times \left(\frac{n}{(m,n)}\right)^{n-1} \times \left(\frac{n}{(m,n)}\right)^{n-1} \times \cdots \times \left(\frac{n}{(m,n)}\right)^{n-1} \times \left(\frac{n}{(m,n)}\right)^{n-1} = n \times \left(\frac{n}{(m,n)}\right)^{(m,n) - 1} \times \left(\frac{n}{(m,n)}\right)^{n-1} = n \left(\frac{n}{(m,n)}\right)^{n-1} \times \left(\frac{n}{(m,n)}\right)^{n-1} = n \left(\frac{n}{(m,n)}\right)^{n-1}.\]

\[\square\]

3 Epimorphisms of the Hypergroup \((\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})\)

The following general fact is used to characterize the elements of \(\text{Epi}(\mathbb{Z}_n, \circ_{m\mathbb{Z}_n})\).
Lemma 3.1. Let $G$ be a group and $N$ a normal subgroup of $G$. If the index $[G : N]$ of $N$ in $G$ is finite and $f \in \text{Epi}(G,oc_N)$, then $f(xN) = f(x)N$ for all $x \in G$.

Proof. Let $[G : N] = n$. Then there are $x_1, \ldots, x_n \in G$ such that $G = \bigcup_{i=1}^{n} x_iN$. Then $x_1N, \ldots, x_nN$ are mutually disjoint. By Lemma 2.1(ii), $f(x_iN) \subseteq f(x_i)N$ for all $i \in \{1, \ldots, n\}$. Hence

$$G = f \left( \bigcup_{i=1}^{n} x_iN \right) = \bigcup_{i=1}^{n} f(x_iN) \subseteq \bigcup_{i=1}^{n} f(x_i)N,$$

which implies that

$$G = \bigcup_{i=1}^{n} f(x_iN) = \bigcup_{i=1}^{n} f(x_i)N.$$  

Since $[G : N] = n$, it follows that $f(x_1)N, \ldots, f(x_n)N$ are mutually disjoint. But $f(x_iN) \subseteq f(x_i)N$ for all $i \in \{1, \ldots, n\}$, thus we have

$$f(x_iN) = f(x_i)N \text{ for all } i \in \{1, \ldots, n\}.$$  

Next, let $x \in G$. Then $xN = x_jN$ for some $j \in \{1, \ldots, n\}$. By Lemma 2.1(ii), $f(xN) \subseteq f(x)N$. Hence

$$f(x_j)N = f(x_jN) = f(xN) \subseteq f(x)N$$

which implies that $f(xN) = f(x)N$. Consequently,

$$f(xN) = f(x_j)N = f(x_j)N = f(x)N.$$  

\[ \square \]

Theorem 3.2. For $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f \in \text{Epi}(\mathbb{Z}_n, oc_{m\mathbb{Z}_n})$ if and only if the following conditions hold.

(i) If $f(\overline{a}) = \overline{a}$ for $a \in \mathbb{Z}$, then $a$ and $(m, n)$ are relatively prime.

(ii) $f(\overline{x} + m\mathbb{Z}_n) = xf(\overline{1}) + m\mathbb{Z}_n$ for all $x \in \mathbb{Z}$.

Proof. Assume that $f \in \text{Epi}(\mathbb{Z}_n, oc_{m\mathbb{Z}_n})$ and $f(\overline{1}) = \overline{a}$ where $a \in \mathbb{Z}$. Since $f(\mathbb{Z}_n) = \mathbb{Z}_n$ it follows from Lemma 2.1(v) that

$$\mathbb{Z}_n = f \left( \bigcup_{x \in \mathbb{Z}} (\overline{x} + (m, n)\mathbb{Z}_n) \right) \subseteq \bigcup_{x \in \mathbb{Z}} (xf(\overline{1}) + (m, n)\mathbb{Z}_n).$$

Then $\overline{1} \in yf(\overline{1}) + (m, n)\mathbb{Z}_n$ for some $y \in \mathbb{Z}$, so $\overline{1} = y\overline{a} + (m, n)\overline{z}$ for some $z \in \mathbb{Z}$. Hence $1 = ya + (m, n)z + nw$ for some $w \in \mathbb{Z}$, so $ya + (m, n)(z + \frac{n}{(m, n)}w) = 1$. 


which implies that \( a \) and \( (m, n) \) are relatively prime. Hence (i) holds. The condition (ii) follows directly from Lemma 3.1 and Lemma 2.1(v).

For the converse, assume that (i) and (ii) hold. Then from (ii) and Theorem 2.2, \( f \in \text{Hom}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) \). From (i), we have that there are \( y, z \in \mathbb{Z} \) such that \( ay + (m, n)z = 1 \). Then
\[
\overline{1} = y\overline{a} + (m, n)\overline{z} \in yf(\overline{1}) + (m, n)\mathbb{Z}_n.
\]

Hence from (ii), we have that for \( x \in \mathbb{Z} \),
\[
\overline{x} = x\overline{1} \in x(yf(\overline{1}) + (m, n)\mathbb{Z}_n)
\subseteq xyf(\overline{1}) + (m, n)\mathbb{Z}_n = f(xy + (m, n)\mathbb{Z}_n) \subseteq f(\mathbb{Z}_n)
\]
which implies that \( f(\mathbb{Z}_n) = \mathbb{Z}_n \). Thus \( f \in \text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) \).

The following theorem clearly follows from Theorem 2.4.

**Theorem 3.3.** \( \text{Epi}(\mathbb{Z}_n, +) \subseteq \text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) \).

It follows from Theorem 2.4 that \(|\text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n)| \geq \varphi(n)\). The cardinality of \( \text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) \) is given in the next theorem.

**Theorem 3.4.** The following statements hold.

(i) If \( (m, n) = 1 \), then \(|\text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n)| = n!\).

(ii) If \( (m, n) > 1 \), then \(|\text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n)| = \varphi((m, n)) \left(\frac{n}{(m, n)} \right) - 1 \right) \left(\frac{n}{(m, n)} \right)! \left(\frac{n}{(m, n)} \right)! \right) - 1 \).

**Proof.** First we note that for finite nonempty sets \( A, B \) with \(|A| = |B|\),
\[
|\{f : A \to B \mid f(A) = B\}| = |A|!
\]
If \( a \in A \) and \( b \in B \), then
\[
|\{f : A \to B \mid f(a) = b \text{ and } f(A) = B\}| = (|A| - 1)!.
\]

(i) If \( (m, n) = 1 \), it follows from Lemma 2.5 that
\[
\text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) = \text{Epi}(\mathbb{Z}_n, \cdot \mathbb{Z}_n) = \{f : \mathbb{Z}_n \to \mathbb{Z}_n \mid f(\mathbb{Z}_n) = \mathbb{Z}_n\},
\]
so \(|\text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n)| = n!\).

(ii) Assume that \( (m, n) > 1 \). It follows from Theorem 3.2 that for \( f : \mathbb{Z}_n \to \mathbb{Z}_n \),
\[
f \in \text{Epi}(\mathbb{Z}_n, \cdot_m \mathbb{Z}_n) \iff (i) \text{ } f(\overline{1}) = \overline{a} \text{ } \text{where } a \text{ and } (m, n) \text{ are relatively prime and (ii) } f((m, n)\mathbb{Z}_n) = (m, n)\mathbb{Z}_n,
\]
\[
f(\overline{1} + (m, n)\mathbb{Z}_n) = f(\overline{1}) + (m, n)\mathbb{Z}_n,
\]
\[
f(2\overline{1} + (m, n)\mathbb{Z}_n) = 2f(\overline{1}) + (m, n)\mathbb{Z}_n,
\]
\[
\cdots
\]
\[
f((m, n)\mathbb{Z}_n) = ((m, n) - 1)f(\overline{1}) + (m, n)\mathbb{Z}_n.
\]
For $f \in \text{Epi}(\mathbb{Z}_n, o_{m\mathbb{Z}_n})$, the number of all possibilities of $f(\mathbb{T})$ is $\varphi((m, n))$. Notice that $f(\mathbb{T}) \in f(\mathbb{T} + (m, n)\mathbb{Z}_n)$. From these facts, we have that

$$|\text{Epi}(\mathbb{Z}_n, o_{m\mathbb{Z}_n})| = \varphi((m, n)) \times \left( \frac{n}{(m, n)} \right)! \times \left( \frac{n}{(m, n)} - 1 \right)!$$

$$\times \left( \frac{n}{(m, n)} \right)! \times \cdots \times \left( \frac{n}{(m, n)} \right)!$$

$$(m,n) - 2 \text{ copies}$$

$$= \varphi((m, n)) \left( \frac{n}{(m, n)} - 1 \right)! \left( \left( \frac{n}{(m, n)} \right)! \right)^{(m,n)-1} \square$$

References


Received: Received: September, 2010