East Asian Math. J.
Vol. 33 (2017), No. 3, pp. 257–263
http://dx.doi.org/10.7858/eamj.2017.018

REGULAR ACTION IN $\mathbb{Z}_n$

Jinsun Jeong and Sangwon Park

Abstract. Let n be any positive integer and $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the ring of integers modulo n. Let X_n be the set of all nonzero, nonunits of $\mathbb{Z}_n$, and G_n be the group of all units of $\mathbb{Z}_n$. In this paper, by investigating the regular action on X_n by G_n, the following are proved : (1) The number of orbits under the regular action (resp. the number of annihilators in X_n) is equal to the number of all divisors ($\neq 1, n$) of n; (2) For any positive integer n, $\sum_{g\in G_n} g \equiv 0 \pmod{n}$; (3) For any orbit $o(x)$ ($x \in X_n$) with $|o(x)| \geq 2$, $\sum_{y\in o(x)} y \equiv 0 \pmod{n}$.

1. Introduction and basic definitions

Let n be any positive integer and $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the ring of integers modulo n. Let X_n be the set of all nonzero, nonunits of $\mathbb{Z}_n$ and G_n be the group of all units of $\mathbb{Z}_n$. In this paper, we will consider a group action on X_n by G_n given by $((g, x) \longrightarrow gx)$ from $G_n \times X_n$ to X_n, called the regular action on X_n by G_n. Under the regular action on X_n by G_n, we define the *orbit* of x by $o(x) = \{gx : \forall g \in G_n\}$ and the *stabilizer* of x by $stab(x) = \{g \in G_n : gx = x\}$ (refer [1], [2], [3]).

Recall that the annihilator of $x \in X_n$ (denoted by $ann(x)$) is defined by $\{a \in \mathbb{Z}_n : ax = 0\}$. Throughout this paper, we will denote the greatest common divisor of any two positive integers s and t by $gcd(s, t)$ (or simply (s, t)) and $s|t$ means that s is a divisor of t. In section 2, we will show that all orbits under the regular action on X_n by G_n consists of $o(x)$ for all divisors $x(\neq 1, n)$ of n by investigating that for all $x, y \in X_n$, $o(x) = o(y)$ if and only if $(x, n) = (y, n)$. We can also show that for all $x, y \in X_n$, $ann(x) = ann(y)$ if and only if $(x, n) = (y, n)$.

In section 3, we will show that for any positive integer n, (1) $\sum_{g\in G_n} g \equiv 0 \pmod{n}$; (2) for any orbit $o(x)$ ($x \in X_n$) with $|o(x)| \geq 2$, $\sum_{y\in o(x)} y \equiv 0$ (mod n). As a corollary of the result (2), we obtain $\sum_{d|n} \phi(d) = n$ where $\phi(d)$ is the Euler-phi number of d.

Received December 12, 2016; Accepted February 13, 2017.
2010 *Mathematics Subject Classification.* 16W22, 11A07.
Key words and phrases. regular group action, orbit, stabilizer.
This study was supported by research funds from Dong-A University.

(pISSN 1226-6973, eISSN 2287-2833)

2. Orbits and annihilators under the regular action

We begin this section with some lemmas.

Lemma 2.1. *Let n be any positive integer and $x, y \in X_n$ be divisors of n such that $x < y$ and $x \neq y$. Then $o(x) \neq o(y)$ under the regular action on X_n by G_n.*

Proof. Assume that $o(x) = o(y)$. Then $y = gx$ for some $g \in G_n$. Since x, y are divisors of n such that $x < y$ and $x \neq y$, we can choose an element $a \in X_n$ so that $ax \neq 0, ay = 0$. On the other hand, since $0 = ay = a(gx)$ and $g \in G_n$, we have $ax = 0$, which is a contradiction. Hence $o(x) \neq o(y)$. □

Lemma 2.2. *Let n be any positive integer and $y \in X_n$ be arbitrary. Then there exists $x \in X$ such that $x|n$ and $(x, n) = (y, n)$.*

Proof. Let $x = (y, n)$. Then clearly, $x|n$ and $(x, n) = ((y, n), n) = (y, n)$. □

Lemma 2.3. *Let k and n be any positive integers such that $k|n$. If $\bar{g} \in G_k$, then there exists $g \in G_n$ such that $g \equiv \bar{g}$ (mod k).*

Proof. Note that since $k|n$, $\mathbb{Z}_n/ < k >$ is isomorphic to $\mathbb{Z}_k$ where $< k >$ is an ideal of $\mathbb{Z}_n$ generated by k. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ be the prime factorization of n where $p_1, p_2, \cdots, p_t$ are distinct primes for some positive integer t. Then $k = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$ with $\alpha_i \geq \beta_i \geq 0$ for all $i = 1, \cdots, t$. Without loss of generality, we can assume that $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$ (resp. $\mathbb{Z}_k = \mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \cdots \times \mathbb{Z}_{p_t^{\beta_t}}$). Then we can consider a ring epimorphism $\pi : \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \cdots \times \mathbb{Z}_{p_t^{\alpha_t}} \to \mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \cdots \times \mathbb{Z}_{p_t^{\beta_t}}$ given by $\pi(a_1, \cdots, a_t) = (\bar{a}_1, \cdots, \bar{a}_t)$ for all $(a_1, \cdots, a_t) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$ where $\bar{a}_i$ is the remainder obtained from dividing a_i by $p_i^{\beta_i}$ for all i.

Case 1. Suppose that $\beta_i \geq 1$ for all $i = 1, \cdots, t$.

Let $\bar{g} = (\bar{g}_1, \cdots, \bar{g}_t) \in \mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \cdots \times \mathbb{Z}_{p_t^{\beta_t}}$ be an arbitrary unit. Then there exists an element $g = (g_1, \cdots, g_t) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$ such that $\pi(g) = \bar{g}$ i.e., $g_i \equiv \bar{g}_i$ (mod $p_i^{\beta_i}$) for all i. Since $\bar{g}$ is a unit in $\mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \cdots \times \mathbb{Z}_{p_t^{\beta_t}}$, we have $(\bar{g}_i, p_i^{\beta_i}) = 1$ and so $(g_i, p_i^{\alpha_i}) = 1$ for all $i = 1, \cdots, t$, which implies that $g \in \mathbb{Z}_n$ is a unit.

Case 2. Suppose that $\beta_i = 0$ for some i.

Let $I_1 = \{i \in \{1, \cdots, t\} : \beta_i \geq 1\}$ and $I_2 = \{i \in \{1, \cdots, t\} : \beta_i = 0\}$. Consider $R = R_1 \times R_2$ where $R_1 = \prod_{i \in I_1} \mathbb{Z}_{p_i^{\beta_i}}$ and $R_2 = \prod_{i \in I_2} \{1_i\}$ where 1_i is the unity of $\mathbb{Z}_{p_i^{\beta_i}}$. By changing the order of the $\mathbb{Z}_{p_i^{\beta_i}}$ if necessary we can assume that $R = \mathbb{Z}_k = \mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \cdots \times \mathbb{Z}_{p_t^{\beta_t}}$. Let $G(R)$ be the group of all units in R. Let $\bar{g} = (\bar{g}_1, \cdots, \bar{g}_{|I_1|}, 1_1, \cdots, 1_{|I_2|}) \in G(R)$ be arbitrary. Then by the similar argument given in Case 1, there exists a unit $g_i \in \mathbb{Z}_{p_1^{\alpha_1}}$ such that $g_i \equiv \bar{g}_i$ (mod $p_i^{\beta_i}$) for all $i = 1, \cdots, |I_1|$. Let $g = (g_1, \cdots, g_{|I_1|}, 1_1, \cdots, 1_{|I_2|}) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$. Then g is a unit in $\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$ such that $\pi(g) = \bar{g}$. □

Theorem 2.4. *Let n be any positive integer. Then for all $x, y \in X_n$, $o(x) = o(y)$ if and only if $(x, n) = (y, n)$.*

Proof. ($\Rightarrow$) Suppose that for all $x, y \in X_n$, $o(x) = o(y)$. Then $y = gx$ for some $g \in G_n$. Since $(g, n) = 1$, we have $(y, n) = (gx, n) = (x, n)$.

($\Leftarrow$) Suppose that for all $x, y \in X_n$, $(x, n) = (y, n)$. It is enough to consider $x|n$, i.e., $x = (x, n)$ by Lemma 2.2. Since $x|y$, $y = ax$ for some integer a. Since $x = (y, n)$, $x = by + cn$ for some integers b and c. Hence $x \equiv by \equiv bax \pmod{n}$, and then $1 \equiv ba \pmod{\frac{n}{x}}$. Let $\bar{a}$ be an element of $\mathbb{Z}_{\frac{n}{x}}$ so that $a \equiv \bar{a} \pmod{\frac{n}{x}}$. Then $1 \equiv b\bar{a} \pmod{\frac{n}{x}}$, which implies that $\bar{a} \in G_{\frac{n}{x}}$. By Lemma 2.3, there exists $a_0 \in G_n$ such that $a_0 \equiv \bar{a} \pmod{\frac{n}{x}}$. Since $a_0 = \bar{a} + k(\frac{n}{x})$ for some integer k, we have $a_0 x \equiv (\bar{a} + k(\frac{n}{x}))x \equiv \bar{a}x \equiv ax \equiv y \pmod{n}$, which implies that $o(x) = o(y)$. $\square$

Remark 1. (1) Let n be any positive integer. Then the number of orbits under the regular action on X_n by G_n is equal to the number of divisors ($\neq 1, n$) of n by Lemma 2.1 and Theorem 2.4.
(2) The regular action on X_n by G_n is transitive, i.e., $X_n = o(x)$ for some $x \in X_n$ if and only if $n = p^2$ for some prime p.

Corollary 2.5. *Let n be a positive integer and $x(\neq 1, n)$ be a divisor of n. Then $o(x) = \{gx : \forall g \in G_{\frac{n}{x}}\}$, and so $|o(x)| = |G_{\frac{n}{x}}|$.*

Proof. Let $y \in o(x)$ be arbitrary. By Theorem 2.4, $(x, n) = (y, n)$. Since x is a divisor of n, $x = (x, n) = (y, n)$, and so $1 = (\frac{y}{x}, \frac{n}{x})$. Thus $\frac{y}{x} \in G_{\frac{n}{x}}$, and then $y = gx$ for some $g \in G_{\frac{n}{x}}$. Assume that there exist $g_1, g_2 \in G_{\frac{n}{x}}$ ($g_1 \neq g_2$) such that $g_1 x = g_2 x$. Then $(g_1 - g_2)x \equiv 0 \pmod{n}$, which implies that $g_1 - g_2 \equiv 0 \pmod{\frac{n}{x}}$. Since $g_1 - g_2 \in \mathbb{Z}_{\frac{n}{x}}$, $g_1 - g_2 = 0$, a contradiction. Hence $o(x) = \{gx : g \in G_{\frac{n}{x}}\}$, and so $|o(x)| = |G_{\frac{n}{x}}|$. $\square$

Example 1. Consider $\mathbb{Z}_{36}$. Then $G_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$, $X_{36} = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34\}$. Thus all the distinct orbits under the regular action on X_{36} by G_{36} are obtained as follows:

$o(2) = \{y \in X_{36} : (2, 36) = (y, 36)\} = \{2, 10, 14, 22, 26, 34\}$,

$o(3) = \{y \in X_{36} : (3, 36) = (y, 36)\} = \{3, 15, 21, 33\}$,

$o(4) = \{y \in X_{36} : (4, 36) = (y, 36)\} = \{4, 8, 16, 20, 28, 32\}$,

$o(6) = \{y \in X_{36} : (6, 36) = (y, 36)\} = \{6, 30\}$,

$o(9) = \{y \in X_{36} : (9, 36) = (y, 36)\} = \{9, 27\}$,

$o(12) = \{y \in X_{36} : (12, 36) = (y, 36)\} = \{12, 24\}$,

$o(18) = \{y \in X_{36} : (18, 36) = (y, 36)\} = \{18\}$.

Also we can have

$|o(2)| = |G_{18}| = 6$, $|o(3)| = |G_{12}| = 4$, $|o(4)| = |G_9| = 6$, $|o(6)| = |G_6| = 2$,

$|o(9)| = |G_4| = 2$, $|o(12)| = |G_3| = 2$, $|o(18)| = |G_2| = 1$.

Corollary 2.6. *Let n be a positive integer. Then $n = \sum_{x|n} \phi(x)(\forall x, x|n)$ where $\phi(x)$ is the Euler-phi number of x, i.e., $\phi(x) = |G_x|$.*

Proof. By Remark 1 and Corollary 2.5, $|X_n| = \sum_{x|n} |o(x)| = \sum_{x|n} \phi(\frac{n}{x}) = \sum_{x|n} \phi(x)(x \neq 1, n)$ - (1). On the other hand, since $\mathbb{Z}_n \setminus \{0\} = X_n \cup G_n$, $|X_n| = n - 1 - |G_n| = n - \phi(1) - \phi(n)$ - (2). By equalities (1) and (2), we have $n = \phi(1) + \phi(n) + \sum_{x|n} \phi(x)(x \neq 1, n) = \sum_{x|n} \phi(x)(\forall x, x|n)$. □

Remark 2. (1) Let n be any positive integer. Then for all divisors $x(\neq 1, n)$ of n, we have that $|stab(x)| = \frac{|G_n|}{|o(x)|} = \frac{\phi(n)}{\phi(\frac{n}{x})}$ - (*) by Corollary 2.5.
(2) Let p be any prime and t be any positive integer. Then by the equality (*) we have that $|stab(p^{t-1})| = \frac{\phi(p^t)}{\phi(p)} = p^{t-1}$, and so $stab(p^{t-1}) = \{1 + kp : k = 0, 1, \cdots, p^{t-1} - 1\}$ is the Sylow p-subgroup of G_{p^t}.
(3) Let n be any even integer. Then by the equality (*) we also have that $\phi(n) = \phi(2)|stab(\frac{n}{2})| = |stab(\frac{n}{2})|$, and so $G_n = stab(\frac{n}{2})$.
We will denote $ann(x) \setminus \{0\}$ by $ann(x)^*$.

Lemma 2.7. *Let n be any positive integer and $x, y \in X_n$ be divisors of n such that $x < y$. Then $ann(x)^* \neq ann(y)^*$.*

Proof. Assume that $ann(x)^* = ann(y)^*$. Since x, y are divisors of n such that $x < y$ and $x \neq y$, we can choose an element $a \in X_n$ so that $ax \neq 0, ay = 0$, and so $a \notin ann(x)^*, a \in ann(y)^*$, which is a contradiction. Hence $ann(x)^* \neq ann(y)^*$. □

Theorem 2.8. *Let n be any positive integer. Then for all $x, y \in X_n$, $(x, n) = (y, n)$ if and only if $ann(x)^* = ann(y)^*$.*

Proof. ($\Rightarrow$) Suppose that for all $x, y \in X_n$, $(x, n) = (y, n)$. Then $o(x) = o(y)$ by Theorem 2.4. Let $a \in ann(x)^*$ be arbitrary. Then $ax = 0$. Since $o(x) = o(y)$, $y = gx$ for some $g \in G_n$. Thus $ay = a(gx) = g(ax) = 0$, and so $ay = 0$, which implies that $a \in ann(y)^*$, and so $ann(x)^* \subseteq ann(y)^*$. Similarly, we can also show that $ann(y)^* \subseteq ann(x)^*$.

($\Leftarrow$) Suppose that for all $x, y \in X_n$, $ann(x)^* = ann(y)^*$. We can take x_0, y_0 such that divisors of n, $x_0, y_0 \in X_n$ such that $x_0 = (x_0, n) = (x, n), y_0 = (y_0, n) = (y, n)$ by Lemma 2.2. By the similar argument given in the proof of ($\Rightarrow$), we have $ann(x_0)^* = ann(x)^*, ann(y_0)^* = ann(y)^*$. Assume that $(x, n) \neq (y, n)$. Then $x_0 \neq y_0$, and so $ann(x)^* \neq ann(y)^*$ by Lemma 2.7, a contradiction. Hence we have $(x, n) = (y, n)$. □

Remark 3. Let n be any positive integer. Then the number of the $ann(x)^*$'s in X_n is equal to the number of divisors ($\neq 1, n$) of n by Lemma 2.1 and Theorem

2.8. We observe that $ann(x)^*$ in X_n is the union of some orbits under the regular action on X_n by G_n.

Example 2. Consider $\mathbb{Z}_{36}$. Then $\{2, 3, 4, 6, 9, 12, 18\}$ is the set of all divisors $(\neq 1, 36)$ of 36 given in Example 1. Thus we obtained all the $ann(x)^*$'s in X_{36} as follows:

$ann(2)^* = \{18\} = o(18)$,

$ann(3)^* = \{12, 24\} = o(12)$,

$ann(4)^* = \{9, 18, 27\} = o(9) \cup o(18)$,

$ann(6)^* = \{6, 12, 18, 24, 30\} = o(6) \cup o(12) \cup o(18)$,

$ann(9)^* = \{4, 8, 12, 16, 20, 24, 28, 32\} = o(4) \cup o(12)$,

$ann(12)^* = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$

$= o(3) \cup o(6) \cup o(9) \cup o(18)$,

$ann(18)^* = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34\}$

$= o(2) \cup o(4) \cup o(6) \cup o(12) \cup o(18)$.

3. Some properties of orbits under the regular action

Consider $\mathbb{Z}_{36}$. Then there are 7 distinct orbits under the regular action on X_{36} by G_{36} as in the Example 1.

$o(2) = \{y \in X_{36} : (2, 36) = (y, 36)\} = \{2, 10, 14, 22, 26, 34\}$,

$o(3) = \{y \in X_{36} : (3, 36) = (y, 36)\} = \{3, 15, 21, 33\}$,

$o(4) = \{y \in X_{36} : (4, 36) = (y, 36)\} = \{4, 8, 16, 20, 28, 32\}$,

$o(6) = \{y \in X_{36} : (6, 36) = (y, 36)\} = \{6, 30\}$,

$o(9) = \{y \in X_{36} : (9, 36) = (y, 36)\} = \{9, 27\}$,

$o(12) = \{y \in X_{36} : (12, 36) = (y, 36)\} = \{12, 24\}$,

$o(18) = \{y \in X_{36} : (18, 36) = (y, 36)\} = \{18\}$.

On the other hand, we have the following:

$\sum_{g \in G_{36}} y \equiv 1 + 5 + 7 + 11 + 13 + 17 + 19 + 23 + 25 + 29 + 31 + 35 \equiv 0 \pmod{36}$,

$\sum_{y \in o(2)} y \equiv 2 + 10 + 14 + 22 + 26 + 34 \equiv 0 \pmod{36}$,

$\sum_{y \in o(3)} y \equiv 3 + 15 + 21 + 33 \equiv 0 \pmod{36}$,

$\sum_{y \in o(4)} y \equiv 4 + 8 + 16 + 20 + 28 + 32 \equiv 0 \pmod{36}$,

$\sum_{y \in o(6)} y \equiv 6 + 30 \equiv 0 \pmod{36}$,

$\sum_{y\in o(9)} y \equiv 9+27 \equiv 0 \pmod{36}$,

$\sum_{y\in o(12)} y \equiv 12+24 \equiv 0 \pmod{36}$,

$\sum_{y\in o(18)} y \equiv 18 \pmod{36}$.

In this section, we will show that for all positive integers n, $\sum_{g\in G_n} g \equiv 0 \pmod{n}$ and $\sum_{y\in o(x)} y \equiv 0 \pmod{n}$ for any orbit $o(x)$ ($|o(x)| \geq 2$) under the regular action on X_n by G_n.

Lemma 3.1. *Let p be any prime and t ($t \geq 2$) be any positive integer. Then $\sum_{g\in G_{p^t}} g \equiv 0$ (mod p^t).*

Proof. Since $X_{p^t} = \{p, 2p, \cdots, (p^{t-1}-1)p\} = \mathbb{Z}_{p^t} \setminus (G_{p^t} \cup \{0\})$, we have

$\sum_{g\in G_{p^t}} g = \sum_{a\in\mathbb{Z}_{p^t}} a - \sum_{x\in X_{p^t}} x$

$= (1+2+\cdots+(p^t-1)) - (p+2p+\cdots+(p^{t-1}-1)p)$

$= \frac{p^t(p^t-1)}{2} - \frac{p^t(p^{t-1}-1)}{2}$

$= p^t(\frac{p^{t-1}(p-1)}{2})$, and so $\sum_{g\in G_{p^t}} g \equiv 0 \pmod{p^t}$ because $\frac{p^{t-1}(p-1)}{2}$ is an integer for any prime p. □

Theorem 3.2. *Let n be any positive integer. Then $\sum_{g\in G_n} g \equiv 0$ (mod n).*

Proof. Let $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ be the prime factorization of n where p_i are all distinct primes and $\alpha_i \geq 1$ for all $i = 1, \cdots, s$. Since $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$, G_n is also isomorphic to $G_{p_1^{\alpha_1}} \times G_{p_2^{\alpha_2}} \times \cdots \times G_{p_s^{\alpha_s}}$. Without loss of generality, we can assume that $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ (resp. $G_n = G_{p_1^{\alpha_1}} \times G_{p_2^{\alpha_2}} \times \cdots \times G_{p_s^{\alpha_s}}$). Since $\sum_{g\in G_n} g = \sum_{(g_1,\cdots,g_s)\in G_{p_1^{\alpha_1}}\times\cdots\times G_{p_s^{\alpha_s}}} (g_1, \cdots, g_s) = (\sum_{g_1\in G_{p_1^{\alpha_1}}} g_1, \cdots, \sum_{g_s\in G_{p_s^{\alpha_s}}} g_s)$ and
$\sum_{g_i\in G_{p_i^{\alpha_i}}} g_i \equiv 0_i$ (Mod $p_i^{\alpha_i}$) by Lemma 3.1 where 0_i is the zero identity of $G_{p_i^{\alpha_i}}$ for all $i = 1, \cdots, s$, we have $\sum_{g\in G_n} g \equiv 0 \pmod{n}$. □

Corollary 3.3. *Let n be any positive integer. If n is odd (resp. even), then $\sum_{x\in X_n} x \equiv 0$ (mod n) (resp. $\sum_{x\in X_n} x \equiv \frac{n}{2}$ (mod n)).*

Proof. Note that $\sum_{x\in X_n} x = \sum_{a\in\mathbb{Z}_n} a - \sum_{g\in G_n} g = \frac{n(n-1)}{2} - \sum_{g\in G_n} g \equiv \frac{n(n-1)}{2}$ (mod n) - (*) by Theorem 3.2. If n is odd, then $\frac{n(n-1)}{2} \equiv 0 \pmod{n}$, and so $\sum_{x\in X_n} x \equiv 0 \pmod{n}$ from the equality (*). If n is even, then $\frac{n(n-1)}{2} + \frac{n}{2} = n(\frac{n}{2})$. Since $\frac{n}{2}$ is integer, $\frac{n(n-1)}{2} \equiv \frac{-n}{2} \equiv \frac{n}{2} \pmod{n}$, and so $\sum_{x\in X_n} x \equiv \frac{n}{2}$ (mod n) from the equality (*). □

Lemma 3.4. *Let $n = p^t$ for any prime p and positive integer t ($t \geq 2$). Then $\sum_{y\in o(x)} y \equiv 0$ (mod n) for any orbit $o(x)$ ($|o(x)| \geq 2$), under the regular action on X_n by G_n.*

Proof. Let $x \in X_n$ be an arbitrary divisor of n. Then $x = p^k$ for some k $(t-1 \geq k \geq 2)$. Since $o(p^i) = \{y \in X_n : p^k = (n, y)\}$ by Theorem 2.4, $o(p^k) = \{ax \in X_n : a \in G_n\} = \{p^k, 2p^k, \cdots, (p^t-1)p^k\} \setminus \{pp^k, 2pp^k, \cdots, (p^t-1)p)p^k\}$. Hence we have

$$\begin{aligned}
&\textstyle\sum_{y \in o(p^i)} y \\
&\equiv (1 + 2 + \cdots + (p^t-1))p^k - (p + 2p + \cdots + (p^t-1)p)p^k \\
&\equiv \tfrac{(p^t-1)p^t}{2} p^k - \tfrac{(p^{t-1}-1)p^{t-1}}{2} p^{k+1} \\
&\equiv (p^k \tfrac{(p^t - p^{t-1})}{2}) p^t \equiv 0 \pmod{p^t}.
\end{aligned}$$

□

Theorem 3.5. *Let n be a positive integer. Then $\sum_{y \in o(x)} y \equiv 0$ (mod n) for any orbit $o(x)$ ($|o(x)| \geq 2$) under the regular action on X_n by G_n.*

Proof. Let $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ be the prime factorization of n where $p_i^{\alpha_i}$ are all distinct primes and $\alpha_i \geq 1$ for all $i = 1, \cdots, s$. Since $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$, G_n is also isomorphic to $G_{p_1^{\alpha_1}} \times G_{p_2^{\alpha_2}} \times \cdots \times G_{p_s^{\alpha_s}}$. Without loss of generality, we can assume that $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ (resp. $G_n = G_{p_1^{\alpha_1}} \times G_{p_2^{\alpha_2}} \times \cdots \times G_{p_s^{\alpha_s}}$). Let $x = (x_1, x_2, \cdots, x_s) \in X_n$ be arbitrary and 0_i be the additive identity of $\mathbb{Z}_{p_i^{\alpha_i}}$ for all $i = 1, \cdots, s$. By assumption, it is enough to show that for all $x_i \in \mathbb{Z}_{p_i^{\alpha_i}}$, $\sum_{y_i \in o(x_i)} y_i \equiv 0_i$ (mod $p_i^{\alpha_i}$). Observe that if $x_i \in X_{p_i^{\alpha_i}}$, then $\sum_{y_i \in o(x_i)} y_i \equiv 0$ (mod $p_i^{\alpha_i}$) by Lemma 3.4; if $x_i \in G_{p_i^{\alpha_i}}$, then $\sum_{g \in G_{p_i^{\alpha_i}}} gx_i \equiv \sum_{g \in G_{p_i^{\alpha_i}}} g \equiv 0$ (mod $p_i^{\alpha_i}$) by Lemma 3.1; if $x_i = 0_i$, then clearly, $\sum_{g \in G_{p_i^{\alpha_i}}} g0_i \equiv 0_i$ (mod $p_i^{\alpha_i}$). Hence we have the result. □

References

[1] J. A. Cohen and K. Koh, *Half-transitive group actions in a compact ring*, J. Pure and Appl. Algebra **60** (1989), 139-153.

[2] J. Han, *Regular action in a ring with a finite number of orbits*, Comm. Algebra **25** (1997), no.7, 2227-2236.

[3] J. Han, *Group actions in a unit-regular ring*, Comm. Algebra **27** (1999), no.7, 3353-3361.

Jinsun Jeong
Department of Mathematics
Dong-A University
Pusan, 49315, Korea
E-mail address: jsjeong@donga.ac.kr

Sangwon Park
Department of Mathematics
Dong-A University
Pusan, 49315, Korea
E-mail address: swpark@donga.ac.kr