Coprime (r,k)-Residue Sets In $\mathbb{Z}_n$

Vladimir Božović

Department of Science and Mathematics, University of Montenegro

Abstract. In this paper we deal with simple problem: How many elements, from the cyclic additive group $\mathbb{Z}_n$ of residues modulo n, are there such that $x \equiv r \pmod{k}$, where $\gcd(r,k) = \gcd(x,n) = 1$, where k is a divisor of n. The interest for this question arises from the problem of understanding the action of the automorphism group $\mathscr{I}(n)$ of $\mathbb{Z}_n$ on the set of $k-$sets of $\mathbb{Z}_n$ in the natural way [7]

$$(x,t) \to tx \ \ (t \in \mathscr{I}(n),\ x \in \mathbb{Z}_n).$$

Considering the aforementioned problem we introduced the notion of coprime $(r,k)-$residue sets in $\mathbb{Z}_n$, which appear to have an important role in finding number of orbits of the action of automorphism group $\mathscr{I}(n)$ on the set $\mathscr{O}_k$, that denotes the set of all subsets of $\mathbb{Z}_n$ of size k. We give the elementary analysis of coprime (r,k)-residue sets in the algebraic and number theoretical sense.

1. INTRODUCTION

Let $\mathscr{I}(n)$ be the automorphism group of cyclic additive group $\mathbb{Z}_n$. It is well known fact that the automorphism group of cyclic additive group is isomorphic to the unit group

$$\mathbb{Z}_n^* = \{t \mid 1 \le t \le n,\ \gcd(t,n) = 1\},$$

with respect to the multiplication modulo n, [3]. We consider the action of the group $\mathscr{I}(n)$ on the set of elements of $\mathbb{Z}_n$, given by

$$(x,t) \to tx \ \ (t \in \mathscr{I}(n),\ x \in \mathbb{Z}_n).$$

There is a natural way to induce this action on the set $\mathscr{O}_k$, that denotes the set of all subsets of $\mathbb{Z}_n$ of size k. In order to answer to some of the standard enumerative questions regarding this action, as a number of orbits, the cycle index ([2], [5], [6], [4]) of $\mathscr{I}(n)$ acting on $\mathbb{Z}_n$ has to be determined. Also, one might be interested in finding the stabilizer of a $k-$set $A \subseteq \mathbb{Z}_n$, since when a stabilizer is found, there is a straightforward way to determine the orbit that a set A belongs to. It turns out that the very important role in, for example, finding stablizer of a set A, play so called coprime $(r,k)-$residue sets [1]. Here, we give some algebraic description of those sets and deal with the problem of finding their cardinality.

2. THE NOTION OF COPRIME $(R,K)-$RESIDUE SET IN $\mathbb{Z}_N$

In this section, we introduce the notion of a coprime $(r,k)-$residue set in $\mathbb{Z}_n$ and give their analysis from the algebraic and number theoretical point of view. Here, by *natural* number we assume positive integer.

Definition 2.1. *Let r,k be natural numbers such that* $\gcd(r,k)=1$*, $r<k$ and let k be a divisor of natural number n. A set of integers*

$$\mathscr{I}_k^r(n)=\{x\in\mathscr{I}(n)|\, x\equiv r\ (mod\ k)\}$$

is called coprime $(r,k)-$residue set in $\mathbb{Z}_n$.

Firstly, we prove that any coprime $(r,k)-$residue set in $\mathbb{Z}_n$ is not empty.

Lemma 2.1. *Let r,k,ℓ,n be natural numbers such that* $\gcd(r,k)=1$*, $r<k$ and $n=k\ell$. Then coprime $(r,k)-$residue set $\mathscr{I}_k^r(n)$ is nonempty.*

Proof. We prove for given r,k and n and $\gcd(r,k)=1$, there exists t such that

$$\gcd(r+kt,n)=1$$

Let $p_i^{v_i}$ be a general prime power divisor of n. Then, there exists t_i such that

$$\gcd(r+kt_i,p_i^{v_i})=1$$

Namely, if $p_i\mid k$, then $p_i\nmid r$ and $t_i=0$ suffices. If $p_i\nmid k$, than any number t_i such that

$$t_i\not\equiv -r/k \pmod{p_i}$$

will work. By Chinese Reminder Theorem, there exists t such that

$$t\equiv t_i \pmod{p_i}$$

and $\gcd(r+kt,n)=1$. We need to prove that there exists $x\in\mathscr{I}(n)$ such that $x\equiv r\ (mod\ k)$. Let $x\equiv r+kt \pmod{n}$. Since $k\mid n$ then $x\equiv r \pmod{k}$. Also, it is easy to see that $\gcd(x,n)=1$ and therefore $x\in\mathscr{I}(n)$. □

Lemma 2.2. *Let r,k,ℓ be natural numbers such that $gcd(r,k)=1$ and $r<k$. It follows that*

$$|\mathscr{I}_k^r(k\ell)|=|\mathscr{I}_k^1(k\ell)|.$$

Proof. According to Lemma 2.1, both sets $\mathscr{I}_k^r(k\ell)$ and $\mathscr{I}_k^1(k\ell)$ are nonempty.
Let $x\in\mathscr{I}_k^r(k\ell)$. It follows that $x^{-1}\mathscr{I}_k^r(k\ell)\subseteq\mathscr{I}_k^1(k\ell)$. Hence, we have

$$|x^{-1}\mathscr{I}_k^r(k\ell)|=|\mathscr{I}_k^r(k\ell)|$$

and therefore

$$|\mathscr{I}_k^r(k\ell)|\le|\mathscr{I}_k^1(k\ell)| \tag{2.1}$$

Similarly, $x\mathscr{I}_k^1(k\ell) \subseteq \mathscr{I}_k^r(k\ell)$ implies

$$|\mathscr{I}_k^1(k\ell)| \leq |\mathscr{I}_k^r(k\ell)|. \tag{2.2}$$

From inequalities 2.1 and 2.2, it follows that

$$|\mathscr{I}_k^1(k\ell)| = |\mathscr{I}_k^r(k\ell)|$$

□

Lemma 2.3. *Let k,ℓ be natural numbers and $k > 1$. Then $\mathscr{I}_k^1(k\ell)$ is a subgroup of $\mathscr{I}(k\ell)$.*

Proof. According to the definition of $\mathscr{I}_k^1(k\ell)$, it is clear that $\mathscr{I}_u^1(k\ell) \subseteq \mathscr{I}(k\ell)$. Apparently the identity, 1, is in $\mathscr{I}_k^1(k\ell)$. For any $x,y \in \mathscr{I}_u^1(k\ell)$, it holds $xy^{-1} \equiv 1\ (mod\ k)$, i.e. $xy^{-1} \in \mathscr{I}_k^1(k\ell)$ that concludes the proof. □

Lemma 2.4. *Let k and ℓ be relatively prime natural numbers and $k > 1$. Then, it holds*

$$\mathscr{I}_k^1(k\ell) \cong \mathscr{I}(\ell).$$

Proof. Let $\mathscr{A}$ be a mapping from $\mathscr{I}_k^1(k\ell)$ to $\mathscr{I}(\ell)$ defined by

$$\mathscr{A}(x) = x\, mod\ \ell$$

First, we show that $Im(\mathscr{A}) \subseteq \mathscr{I}(\ell)$. Let $x \in \mathscr{I}_k^1(k\ell)$. Then,
$x = a\ell + b,\ 0 \leq b \leq \ell$. Since $x \in \mathscr{I}_k^1(k\ell)$, then by the definition of that set, it follows that $x \in \mathscr{I}(k\ell)$. Therefore $gcd(x,\ell) = 1$ and consequently $gcd(b,\ell) = 1$. Thus, $b \in \mathscr{I}(\ell)$, so we have $\mathscr{A}(x) \in \mathscr{I}(\ell)$.

$\mathscr{A}$ is evidently homomorphism, according to properties of modulo operation.
$\mathscr{A}$ is one to one. Let $x,y \in \mathscr{I}_k^1(k\ell)$ and $\mathscr{A}(x) = \mathscr{A}(y)$. From the definition of $\mathscr{I}_k^1(k\ell)$, we have $x \equiv 1 \pmod{k}$ and $y \equiv 1 \pmod{k}$, so $x \equiv y \pmod{k}$. From $\mathscr{A}(x) = \mathscr{A}(y)$ it follows $x \equiv y \pmod{\ell}$. Since k and ℓ are relatively prime numbers, then $x \equiv y \pmod{k\ell}$, so $\mathscr{A}$ is one to one.

$\mathscr{A}$ is onto. Let $z \in \mathscr{I}(\ell)$. We have to find $x \in \mathscr{I}_k^1(k\ell)$ such that $\mathscr{A}(x) = \ell$, or in other words $x \equiv z\ (mod\ \ell)$. That x must be of the form $1 + kt$, so we should find such a t for which it holds $x \equiv z\ (mod\ \ell)$. From $gcd(k,\ell) = 1$, there exist $m,n \in \mathbb{Z}$ such that $mk + n\ell = 1$. Let us define $t = (z-1)m$, i.e. $x = 1 + (z-1)mk$. Clearly, $x \equiv 1\ (mod\ k)$. Note that $x = 1 + (z-1)(1-n\ell)$, that is $x = z + n\ell(1-z)$, so $x \equiv z \pmod{\ell}$. Now, we need to prove that $gcd(x,\ell) = 1$. Let p be a prime divisor of x and l. Then, p divides z, from which we would have that $p \mid gcd(z,\ell)$ what is impossible since $z \in \mathscr{I}(\ell)$. Therefore, $gcd(x,k\ell) = 1$. At the end, we need to provide that $x < k\ell$. If $x = 1 + (z-1)mk$ is not less than $k\ell$ then we should take $x = 1 + (z-1)mk \pmod{k\ell}$ and all previously given arguments hold. □

Corollary 2.1. *Let r,k,ℓ be natural numbers such that $r < k$,* $\gcd(k,\ell) = 1$ *and* $\gcd(r,k) = 1$. *Then, it holds*

$$|\mathscr{I}_k^r(k\ell)| = \phi(\ell).$$

Proof. It follows directly from Lemma 2.2 and Lemma 2.4. $\square$

Our goal is to find the cardinality of the set $\mathscr{I}_k^r(k\ell)$ when k and ℓ are not necessarily relatively prime numbers and when $gcd(r,k) = 1$. As we sow in the proof of Lemma 2.1 it holds $gcd(x,k\ell) = 1 \Leftrightarrow gcd(x,k\ell') = 1$ where ℓ' is the largest divisor of ℓ that is relatively prime to k. This gives us idea for the following lemma.

Lemma 2.5. *Let k,ℓ be natural numbers and $k > 1$. It follows that*

$$|\mathscr{I}_k^1(k\ell)| = \phi(\ell')\frac{\ell}{\ell'}$$

where ℓ' is the largest divisor of ℓ that is relatively prime to ℓ.

Proof. According to Lemma 2.3 $\mathscr{I}_k^1(k\ell)$ is a subgroup of $\mathscr{I}(k\ell)$. Let us define a homomorphism $\mathscr{S}$ from $\mathscr{I}_k^1(k\ell)$ to $\mathscr{I}_k^1(k\ell')$ in the following way

$$\mathscr{S}(x) = x \ \ mod \ k\ell'$$

This is evidently epimorphism and $Ker(\mathscr{S}) = \{1 + tk\ell' \mid 0 \leq t < \frac{\ell}{\ell'}\}$. Therefore, we have that

$$|\mathscr{I}_k^1(k\ell)| = |\mathscr{I}_k^1(k\ell')|\frac{\ell}{\ell'}$$

By Corollary 2.1 it follows that $|\mathscr{I}_k^1(k\ell')| = \phi(\ell')$ and this concludes the proof. $\square$

Lemma 2.6. *Let k,ℓ be natural numbers and $k > 1$. Then it follows that*

$$|\mathscr{I}_k^1(k\ell)| = \frac{\phi(k\ell)}{\phi(k)}.$$

Proof. By Lemma 2.5 it holds that

$$\phi(\ell') = \frac{\ell'|\mathscr{I}_k^1(k\ell)|}{\ell}$$

where ℓ' is the largest divisor of ℓ that is relatively prime to k. Let $\ell = \ell'\ell''$. Clearly, $\ell'' \mid k$. Then $gcd(k\ell'',\ell') = 1$ and therefore $\phi(k\ell) = \phi(k\ell'')\phi(\ell')$. Since $\ell'' \mid k$ then

$$\phi(k\ell'') = k\ell''\prod_{p|k}(1-\frac{1}{p}) = \ell''\phi(k)$$

Therefore,

$$\phi(k\ell'')\phi(\ell') = \ell''\phi(k)\frac{\ell'|\mathscr{I}_k^1(k\ell)|}{\ell}$$

what implies

$$\phi(k\ell) = \frac{\phi(k)}{|\mathscr{I}_k^1(k\ell)|}$$

and

$$|\mathscr{I}_k^1(k\ell)| = \frac{\phi(k\ell)}{\phi(k)}$$

□

Corollary 2.2. *Let* k, ℓ, r *be natural numbers such that* $\gcd(r,k) = 1$ *and* $r < k$. *Then,*

$$|\mathscr{I}_k^r(k\ell)| = \frac{\phi(k\ell)}{\phi(k)}.$$

Proof. It follows directly from Lemma 2.2 and Lemma 2.6. □

REFERENCES

1. Vladimir Božović. *Factorization of finite groups*. VDM Verlag Dr. Müller, Saarbrücken, 2009.
2. N.G. De Bruijn. A survey of generalizations of pt'olyaŠs enumeration theorem. *Nieuw Archief voor Wiskunde*, 19:89–112, 1971.
3. D.S. Dummit and Foote. *Abstract Algebra*. Prentice-Hall, Upper Saddle River, NJ, 1999.
4. Harald Fripertinger. Cycle indices of linear, affine and projective groups. *Linear Algebra Appl.*, 263:133–156, 1997.
5. M.A. Harrison and R.G. High. On the cycle index of a product of permutation groups. *Journal of Combinatorial Theory*, (4):277–299, 1968.
6. Wan-Di Wei and Ju-Yong Xu. Cycle index of direct product of permutation groups and number of equivalence classes of subsets of z_v. *Discrete Mathematics*, 123:179–188, 1993.
7. Hans J. Zassenhaus. *The Theory of Groups*. Dover, 1958.