Discussion on the Structure of the Reduced Residue Class Additive Group in Cyclic Group

Lijiang ZENG
Northern Guizhou Institute of Culture and Economy, Zunyi Normal College, Zunyi 563000, China

Keywords: additive group; residue class ring; abelian groups; generating element; cyclic group

Abstract. Additive group in the group theory is an important tool to research group. Studying of different kinds of additive group is helpful to the study group. The method itself can be applied to earech the other in the natural sciences. In this paper, a class of additive group of the residue class ring mod \( m \) has been studied. The properties of the residue class ring and the formula for Euler’s function were used. Finally, the order of group and its prime factor of the corresponding cyclic group were used to depict the structure of this kind of group.

1. Introduction

The additive group [1-3] of the residue class ring [4-5] mod \( m \) is, up to isomorphism, the cyclic group of order \( m \) generate, say, by the residue class 1 mod \( m \). For finite group, the direct sum decomposition [6] with respect to the prime power appearing in \( m \) is simply a special case of the basis theorem for finite abelian groups, according to the sum of cyclic subgroups of prime power order. Here, however, the direct sum of each cyclic subgroup belongs to the same prime number, rather than the direct sums of the cyclic subgroups themselves, which are uniquely determined. Let us go somewhat deeper into the additive group mod \( m \).

2. Reduced Residue Class

According to the division theorem of natural numbers, generating elements of the additive group mod \( m \) are exactly the reduced residue class \( k \) mod \( m \). Therefore, the automorphisms are described by means of the substitutions \( 1 \mapsto k \) mod \( m \) or, more generally, \( a \mapsto ka \) mod \( m \). Successive application of these substitutions corresponds to multiplication of the reduced residue class \( k \) mod \( m \). Hence, the group of automorphisms is isomorphic to the reduced residue class group mod \( m \).

Since the additive group mod \( m \) is isomorphism, we switch the cyclic group \( \mathbb{Z}_m \) of order \( m \) over to multiplicative notation and obtain the following frequently used group-theoretic theorems:

For every natural number \( m' \mid m \) (and only for such numbers) there exists in exactly subgroup of order \( m' \) and that one is isomorphic to \( \mathbb{Z}_{m'} \). It consists of the \( d \)th powers of the elements of \( \mathbb{Z}_m \), where \( m = dm' \).

The group of automorphisms of \( \mathbb{Z}_m \) is isomorphic to the reduced residue class group mod \( m \) by virtue of the mapping \( (a \mapsto a^k) \mapsto k \) mod \( m \) (with \( k \) relatively prime to \( m \)).

Let us now turn to the task the general case of describing the structure of the residue class ring mod \( p^\mu \), and that of the reduced residue class group mod \( p^\mu \) for a prime power \( p^\mu \) (where \( \mu \geq 1 \)).

3. Structure of Reduced Residue Class Ring

Regarding the structure of the residue class ring mod \( p^\mu \), we shall now prove the assertion in the following. The residue classes mod \( p^\mu \) have a unique representation of the form:

\[
a \equiv a_0 + a_1 p + \cdots + a_{\mu-1} p^{\mu-1} \mod p^\mu \quad (a_i \in R)
\]

(1)
Where $R$ is any complete residue system mod $p$.

**Proof.** For $\mu=1$, the assertion is obvious. Suppose that $\mu>1$, and that the assertion holds for $\mu-1$. Then, we have a unique representation:

$$a \equiv a_0 + a_1 p + \cdots + a_{\mu-2} p^{\mu-2} \mod p^{\mu-1} \quad (a_i \in R)$$

(2)

So that:

$$a = a_0 + a_1 p + \cdots + a_{\mu-2} p^{\mu-2} + gp^{\mu-1}$$

(3)

With some $p$-integral $g$. Then, $a_{\mu-1}$ is uniquely determined from:

$$g \equiv a_{\mu-1} \mod p \quad (a_{\mu-1} \in R)$$

(4)

This completes the proof by induction.

For $\mu=1$, the residue class ring mod $p$ is a field, namely, the prime field of characteristic $p$.

For $\mu>1$, the unique representation derived above does not yet give a satisfactory view into the structure of the residue class ring mod $p^{\mu}$ since it does not immediately show how to carry out the ring operations. To describe these operations, our problem is essentially to indicate how these unique representations rend for the sum and product of two representatives $a_0$ and $b_0$ in $R$. If we take for $R$ the least (non-negative) residue system mod $p$, we obtain for the sum $a_0 + b_0 = c_0 + \varepsilon p$

with $c_0 \in R$ and $\varepsilon = \begin{cases} 0 & \text{for } a_0 + b_0 < p \\ 1 & \text{for } a_0 + b_0 \geq p \end{cases}$, since in the latter case, we have $a_0 + b_0 < 2p$.

The representation itself can then be regarded as the digit representation in the system with base $p$ (with only the $\mu$ lowest digits considered), and the $\varepsilon = 0$ or 1 that appear may be regarded as the numbers that one has to “carry” in digit-wise addition. For the product, however, we have no such simple rule, from a more advanced point of view we shall find another distinguishable residue system $R$ and use it to describe calculations in the residue class rings mod $p^{\mu}$ (even for all $\mu \geq 1$ simultaneously) in a transparent form: more precisely, we shall reduce these calculations to those in the residue class field mod $p$.

### 4. The Structure of the Reduced Residue Class Group

Finally we shall describe the structure of the reduced residue classes group mod $p^{\mu}$. Instead of the systematic notation $\Theta_{p^{\mu}}$, in what follows, we shall use the shorter notation $B_{\mu}$.

The unique representation derived above for all the residue classes mod $p^{\mu}$ enable us to recognize the reduced residue classes mod $p^{\mu}$ in a simple manner. Naturally, a residue class a mod $p^{\mu}$ is reduced if and only if $a$ is relatively prime to $p$, which in turn will be the casa if and only if $a \not\equiv 0 \mod p$. Since here $a \equiv 0 \mod p$, it follows that the reduced residue classes mod $p^{\mu}$ are characterized in that representation by $a \not\equiv 0 \mod p$, $a_1, \ldots, a_{\mu-1}$ arbitrary mod $p$. Hence the number of them is give by:

$$\varphi(p^{\mu}) = (p-1)p^{\mu-1} = p^{\mu}\left(1 - \frac{1}{p}\right)$$

(5)

If one combines this with the reduction of $\varphi(m)$ to the $\varphi(p^{\mu})$ obtained the formula for Euler's function $\varphi(m)$ that was proved in many books is now proved conceptually.

For $\mu=1$, the group $B_1$ being the multiplicative group of a finite field, is cyclic. Therefore, there is a form of unique representation

$$a \equiv w^\alpha \mod p \quad (\alpha \mod p - 1)$$

(6)
$B_1$ is hereby mapped isomorphically onto the additive group mod $p$-1. A representative $w$ of a basis class (generating class) $w$ mod $p$ of $B_1$ is called a primitive root mod $p$. A number $w' \equiv w^k$ mod $p$ is also a primitive root mod $p$ if and only if $k$ is a basis element (generator) of the additive group mod $p$-1, that is, if and only if $(k, p - 1) = 1$. Consequently there are $\phi(p - 1)$ incongruent primitive roots mod $p$. For $p = 2$, all these assertions are trivial, since in that case $B_1 = 1$. Suppose henceforth that $\mu > 1$. Then the order $\phi(p^\mu) = (p - 1)p^{\mu - 1}$ of $B_\mu$ is decomposed into the two co-prime factors $p - 1$ and $p^{\mu - 1}$. Therefore, it flowers from the basis theorem for finite abelian groups that $B_\mu = M \times B_\mu$ is the direct product of the two subgroups $M$ and $B_\mu$ of orders $p$-1 and $p^{\mu - 1}$ respectively.

By virtue of the uniqueness part of the basis theorem, these are the only subgroups with the orders mentioned, and they consist of all elements whose orders divide $p$-1 and $p^{\mu - 1}$ respectively. They can be determined explicitly from the homomorphisms of $B_\mu$ given by raising to the powers $p$-1 and $p^{\mu - 1}$ respectively. On the one hand, in view of the orders, we have $M^{p - 1} = 1$ and $B_\mu^{p^{\mu - 1}} = 1$. On the other hand, raising to the powers $p^{\mu - 1}$ and $p$-1 yields, according to the theorem in Mohsen Aliabadi’s study “A Note on the Fundamental Theorem of Algebra” [2], an automorphism of each direct factor of $M$ and $B_\mu$ respectively, and consequently of these groups themselves. Hence, we have the main conclusions of this paper: $M^{p - 1} = M$ and $B_\mu^{p^{\mu - 1}} = B_\mu$.

From all this, one obtains the explicit representations: $M = B_\mu^{p - 1}$ and $B_\mu = B_\mu^{p^{\mu - 1}}$.

5. Conclusion

As we have seen above, for every natural divisor $d$ of $m$, the residue class $a$ mod $m$ such that $a \equiv 0 \mod d$ form a subgroup. This subgroup is cyclic of order $m' = \frac{m}{d}$ since upon division by $d$ it is mapped isomorphically onto the additive group of all residue classes $a'$ mod $m'$. Conversely, for every subgroup of the additive group mod $m$, the numbers $a$ lying in it constitute an additive group which contains $m$ since the subgroup contains the residue class $0$ mod $m$ and which thus consists of all multiples of a natural divisor $d$ of $m$. Therefore, there exist only the subgroups mentioned.

References


