Advances in Social Science, Education and Humanities Research, volume 550
Proceedings of the 1st International Conference on Mathematics
and Mathematics Education (ICMMED 2020)

Ideal Generated by The Coefficient of a Polynomial Over $\mathbb{Z}_k$, k > 1

Larasati Onna Roufista[1], Indriati Nurul Hidayah[1]

[1]*Department of Mathematics, Universitas Negeri Malang*
Email: indriati.nurul.fmipa@um.ac.id

ABSTRACT
Let $\mathbb{Z}_k, k > 1$, $k \in \mathbb{N}$ be a commutative ring with unity, polynomial $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}_k[x], a_i \in \mathbb{Z}_k$. We can construct $c(f)$= $\langle a_0, \dots, a_n\rangle$ be an ideal of $\mathbb{Z}_k$ generated by $a_0, \dots, a_n$. If $(a_0, \dots, a_n) = 1$ or a_i *unit* of $\mathbb{Z}_k$ for $i = 0, \dots, n$, then $c(f) = \mathbb{Z}_k$, for k composite.. For k is prime, because all of the elements in $\mathbb{Z}_k$ is unit, then $c(f) = \mathbb{Z}_k$, for every $f \in \mathbb{Z}_k[x]$.

Keywords: *polynomial ring* $\mathbb{Z}_k, k > 1$, *Ideal* $c(f)$, *unit, relative prime.*

1. INTRODUCTION

A ring R is a set with two binary operations and satisfies some properties. A subset A of ring R, which itself a ring, is a subring of ring R. If every element $r \in R$ and $a \in A$, both ra and ar are in A, then A is an ideal of R [1].

A set of integers modulo k, $\mathbb{Z}_k$, $k > 1, k \in \mathbb{N}$ is an example of a ring with two binary operations, that is, addition and multiplication modulo k . If k is prime, that is $\mathbb{Z}_p$, then every element of $\mathbb{Z}_p$ has an inverse over multiplication modulo n. A set of integers modulo p, $\mathbb{Z}_p$, is a field [1].

A polynomial ring over $\mathbb{Z}_k$, is denoted $\mathbb{Z}_k[x]$, is $\mathbb{Z}_k[x] = \{a_0 + a_1x + \cdots + a_nx^n | a_i \in \mathbb{Z}_k, \quad n$ is nonnegative integer$\}$. An element of $\mathbb{Z}_k[x]$ is denoted f, with $a_0, a_1, \dots, a_n$ is the coefficient of f. Coefficients of the polynomial f in $\mathbb{Z}_k[x]$ can form an ideal, is denoted $c(f) = \langle a_0, a_1, \dots, a_n\rangle$ [2]. In this paper, we will discuss a characteristic of the coefficient of a polynomial f over $\mathbb{Z}_k$, $k > 1$, $k \in \mathbb{N}$.

2. PRELIMINARIES

An ideal is formed from a subring. Therefore, we introduce a discussion about ring and subring of ring. The definition of ring and subring refer to [1].

Definition 2.1. A ring R is a set with two binary operations, that is an addition (denoted by $a + b$) and multiplication (denoted by ab), such that for every $a, b, c \in R$:

(i) Commutative over addition that is $a + b = b + a$

(ii) Associative over addition that is $(a + b) + c = a + (b + c)$

(iii) There is an additive identity 0. That is, there is an element 0 in R, such that $a + 0 = a$, for all a in R

(iv) There is the additive inverse $-a$ in R, such that $a + (-a) = 0$

(v) Associative over multiplication that is $a(bc) = (ab)c$

(vi) Distributive over addition that is $a(b + c) = ab + ac$ dan $(b + c)a = ba + ca$

A ring R is commutative if and only if for every $a, b \in R$, $ab = ba$. If a ring R has a multiplicative identity, then ring R is called a ring with unity. A nonzero element a of a commutative ring with unity need not have a multiplicative inverse. When it does, then a is called unit if there is a^{-1} such that $aa^{-1} = 1, 1$ is a notation of unity. If every nonzero element of ring R is a unit, then ring R is a field, as the definition 2.2 below.

Definition 2.2 ([3]**)** Field is a commutative ring with unity, in which every nonzero element of the field is a unit.

Corollary 2.3 ([3]) For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p is a field.

In the main result, we discuss an ideal formed from the coefficient of a polynomial over R. So, the definition of an ideal of a ring, polynomial over ring, and an ideal generated by coefficients f will be explained.

Definition 2.4. A subring A of ring R is called an ideal of R if and only if for every $r \in R, a \in A, ra, ar \in A$. An ideal A of R is called a proper ideal of R if $A \subset R$.

For example, let R be a commutative ring with unity and $c \in R$. Let I be the set of all multiples of c, that is, $I = \{rc | r \in R\}$. Then I is called principal ideal generated by c, also denoted by $\langle c \rangle$ [4].

Definition 2.5. [1] Let R be a commutative ring. A set

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n | a_i \in R, n \text{ is nonnegative integer}\}$$

is called a ring of polynomials over R.

Let $f, g \in R[x]$, that is

$$f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i$$

and

$$g = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + b_m x^m = \sum_{i=0}^{m} b_i x^i$$

Two polynomials over R are equal, that is, $f = g$, if and only if $a_i = b_i$, for all nonnegative integers i (defined $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$).

Let $f = a_0 + \cdots + a_n x^n$, with $a_n \neq 0$, then we say that f has degree n, denoted by $\deg(f) = n$, the term a_n is called the leading coefficient of f [5]. If $f = a_n x^n$, $a_n \neq 0$, then f is called a monomial.

For example, Let $f = x^2 - 5x + 4 \in \mathbb{Z}[x]$, then f is called monic polynomial since the leading coefficient, a_2, is unity in $Z[x]$.

Theorem 2.6. [2] Let $f \in R[x]$, and $a_0, a_1, \dots, a_n$ are coefficients of f. An ideal generated by coefficients f denoted by $c(f)$, that is

$$c(f) = \langle a_0, a_1, \dots, a_n \rangle = \left\{ \sum_{i=0}^{n} r_i a_i, r_i \in R \right\}$$

For example, let $f = x^2 - 5x + 4 \in \mathbb{Z}[x]$, then

$$\begin{aligned} c(f) &= \langle 4, -5, 1 \rangle \\ &= \{4r_0 + (-5r_1) + r_2, r_i \in \mathbb{Z}\} \\ &= \mathbb{Z} \end{aligned}$$

is an ideal in $\mathbb{Z}$.

A set of integers modulo k, $\mathbb{Z}_k$, $k > 1, k \in \mathbb{N}$ is a ring, so we can form polynomial over ring $\mathbb{Z}_k$, $k > 1, k \in \mathbb{N}$, denoted $\mathbb{Z}_k[x]$. The main result will discuss the characteristic of a polynomial f over $\mathbb{Z}_k$, $k > 1$, $k \in \mathbb{N}$ such that $c(f) = \mathbb{Z}_k$. To analyze it, we need to discuss the greatest common divisor (gcd) of two nonzero integers that refers to [1].

Definition 2.7. The greatest common divisor (gcd) of two nonzero integers a and b is the largest of all common divisors of a and b, denoted by $\gcd(a, b)$.

If $\gcd(a, b) = 1$, then a and b are relatively prime.

Theorem 2.8. For every nonzero integer a and b, there is $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Theorem 2.9. If a and b are relatively prime, then there is $s, t \in \mathbb{Z}$ such that $as + bt = 1$

3. MAIN RESULT

In this section, we will discuss the characteristic of polynomials over a ring of integers modulo k, $\mathbb{Z}_k$, $k > 1, k \in \mathbb{N}$, such that $c(f) = \mathbb{Z}_k$. The discussion is divided into k is even, k is odd, and k is prime. The result are

Theorem 3.1 Let $\mathbb{Z}_k$, k composite, is a commutative ring with unity, and $f = a_0 + a_1 + \cdots + a_n x^n \in \mathbb{Z}_k[x]$, $a_i \in \mathbb{Z}_k$, $c(f)$ is an ideal of $\mathbb{Z}_k$.

If $gcd\ (a_0, \dots, a_n) = 1$ or a_i is $unit$ in $\mathbb{Z}_k$ for some $i = 0, \dots, n$, then $c(f) = \mathbb{Z}_k$

Proof:

- Suppose $gcd(a_0, \dots, a_n) = 1$. We will prove that $c(f) = \mathbb{Z}_k$

Let $f = a_0 + \cdots + a_n x^n \in \mathbb{Z}_k[x]$.

Since $c(f)$ is ideal of $\mathbb{Z}_k$, it is clear that $c(f) \subseteq \mathbb{Z}_k$.

Now, we will prove that $\mathbb{Z}_k \subseteq c(f)$

If $gcd(a_0, \dots, a_n) = 1$ then by theorem 2.9, $\exists r_0, \dots, r_n \in \mathbb{Z}_k$ such that $(r_0 a_0 + \cdots + r_n a_n)(mod\ k) = 1$, (it means $\exists q \in \mathbb{Z}$ such that $r_0 a_0 + \cdots + r_n a_n = qk + 1$).

Therefore $1 \in c(f)$

For any $r \in \mathbb{Z}_k$, since $\mathbb{Z}_k$ have unity, and $1 \in c(f)$, then

$$r = r.1 = r(r_0 a_0 + \cdots + r_n a_n) = \big((rr_0)a_0 + \cdots + (rr_n)a_n\big)$$

If $rr_i = t_i \in \mathbb{Z}_k$, for $0 \le i \le n$, then

$$r = t_0 a_0 + \cdots + t_n a_n \in c(f)$$

So $\exists t_i = rr_i \in \mathbb{Z}_k$ such that $r = t_0 a_0 + \cdots + t_n a_n \in c(f)$

So $c(f) = \mathbb{Z}_k$

- Suppose a_i is $unit$ in $\mathbb{Z}_k$. We will prove $c(f) = \mathbb{Z}_k$

Let $f = a_0 + \cdots + a_n x^n \in \mathbb{Z}_k[x]$

Since $c(f)$ is ideal in $\mathbb{Z}_k$, it's clear that $c(f) \subseteq \mathbb{Z}_k$

Now, we will prove that $\mathbb{Z}_k \subseteq c(f)$

If a_i is $unit$ in $\mathbb{Z}_k$ for some $i = 0, \dots, n$ then $\exists r_i = {a_i}^{-1} \to r_i a_i = {a_i}^{-1} a_i = 1$

We obtain

(1) For $i = 0$, then $1 = r_i a_i = r_0 a_0$, choose $r_j = 0, j = 1, \dots, n$, such that

$$r_0 a_0 + \cdots + r_n a_n = r_0 a_0 + 0.a_1 + \cdots + 0.a_n = r_0 a_0 + 0 = 1 \in c(f)$$

(2) For $0 < i < n$, then $1 = r_i a_i$, choose $r_j = 0, j = 0, \dots, n, i \neq j$, such that

$$r_0 a_0 + \cdots + r_n a_n = 0.a_0 + \cdots + r_i a_i + \cdots + 0.a_n = 0 + r_i a_i + 0 = 1 \in c(f)$$

(3) For $i = n$, then $1 = r_n a_n$, Therefore,

$$r_0 a_0 + \cdots + r_n a_n = 0.a_0 + \cdots + 0.a_{n-1} + r_n a_n = 0 + r_n a_n = 1 \in c(f)$$

Hence $1 \in c(f)$

For any $r \in \mathbb{Z}_k$, since $\mathbb{Z}_k$ have unity, and $1 \in c(f)$, then

$$r = r.1 = r(r_0 a_0 + \cdots + r_n a_n) = \big((rr_0)a_0 + \cdots + (rr_n)a_n\big)$$

if $rr_i = t_i \in \mathbb{Z}_k$, for $0 \le i \le n$, then

$$r = t_0 a_0 + \cdots + t_n a_n \in c(f)$$

So $\exists t_i = rr_i \in \mathbb{Z}_k$ such that $r = t_0 a_0 + \cdots + t_n a_n \in c(f)$

So $c(f) = \mathbb{Z}_k$

Note that, if $a_i = 1$, which is 1 is unity in $\mathbb{Z}_k$, clearly $c(f) = \mathbb{Z}_k$.

The following is the example of theorem 3.1

Example 3.2 Let $f = 3 + 2x \in \mathbb{Z}_6[x]$ then $gcd(2,3) = 1$ but 3 and 2 are not $\mathbb{Z}_6$. We have

$$c(f) = \langle 3,2 \rangle = \{3r_0 + 2r_1 | r_i \in \mathbb{Z}_6\}$$

and $0 \in c(f)$ because $\exists r_0 = 0, r_1 = 0 \to 3r_0 + 2r_1 = 0$

$1 \in c(f)$ because $\exists r_0 = 1, r_1 = 2 \to 3r_0 + 2r_1 = 1$

$2 \in c(f)$ because $\exists r_0 = 0, r_1 = 1 \to 3r_0 + 2r_1 = 2$

$3 \in c(f)$ because $\exists r_0 = 1, r_1 = 0 \to 3r_0 + 2r_1 = 3$

$4 \in c(f)$ because $\exists r_0 = 0, r_1 = 2 \to 3r_0 + 2r_1 = 4$

$5 \in c(f)$ because $\exists r_0 = 1, r_1 = 1 \to 3r_0 + 2r_1 = 5$

So, $c(f) = \mathbb{Z}_6$.

But, if $gcd\ (a_0, \ldots, a_n) \neq 1$ and a_i is not $unit$ in $\mathbb{Z}_k$ k composite then is not necessarily $c(f) = \mathbb{Z}_k$ as the example

Example 3.3 Let $f = 2 + 4x \in \mathbb{Z}_6[x]$. We know that $gcd(2,4) = 2 \neq 1$ and 2 and 4 is not unit in $\mathbb{Z}_6$. Then $c(f) = \langle 2,4 \rangle = \{2r_0 + 4r_1 | r_i \in \mathbb{Z}_6\} = \{0,2,4\} \neq \mathbb{Z}_6$

For k is a prime, that is $\mathbb{Z}_p$, because every element of $\mathbb{Z}_p$ is unit then $c(f) = \mathbb{Z}_p$, as follow:

Corollary 3.2 Let $\mathbb{Z}_p, p$ prime is a commutative ring with unity and $f = a_0 + \cdots + a_n x^n \in \mathbb{Z}_p[x]$, $a_i \in \mathbb{Z}_p$, $c(f)$ is ideal in $\mathbb{Z}_p$, then $c(f) = \mathbb{Z}_p$.

Proof:

Suppose $\mathbb{Z}_p, p$ prime is a commutative ring with unity, then $\forall r \in \mathbb{Z}_p, r$ is $unit$ since $\mathbb{Z}_p$ is field.

Let $f = a_0 + \cdots + a_n x^n \in \mathbb{Z}_p[x]$, $a_i \in \mathbb{Z}_p$ for some $i = 0, \ldots, n$

Since $a_i \in \mathbb{Z}_p$, then a_i is $unit$, therefore, by theorem 3.1, $c(f) = \mathbb{Z}_p$.

4. CONCLUSION

Based on the discussion above, we can conclude that if $gcd(a_0, \ldots, a_n) = 1$ or a_i is $unit$ in $\mathbb{Z}_k$ for some $i = 0, \ldots, n$, then $c(f) = \mathbb{Z}_k, k$ composite. Especially for p is a prime, if $\mathbb{Z}_p$, p prime, then $c(f) = \mathbb{Z}_p$.

ACKNOWLEDGMENTS

This research was supported by PNBP Universitas Negeri Malang. The authors would like to express sincere appreciation for all the support given.

REFERENCES

[1] J.A. Gallian, Contemporary Abstract Algebra. Ninth edit. Boston, MA: Brooks/Cole Cengage Learning, 2016.

[2] H.A. Khashan, W. Burhan, Cleanness of overrings of polynomial rings. J Egypt Math Soc 2016, pp. 1–4. DOI: https://doi.org/10.1016/j.joems.2014.08.003.

[3] L. Gilbert, J. Gilbert, Elements of Modern Algebra. seventh ed. Belmont, USA: Brooks/Cole, Cengage Learning, 2009.

[4] T. Hungerford, Algebra. New York: Springer-Verlag New; 2000. DOI: https://doi.org/10.1007/978-1-4612-6101-8 e-ISBN-13:

[5] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul. Basic Abstract Algebra. Second Edi. New York, 1994.