Proceedings

International Conference on Science and Technology (ICST)

Vol. 1, Juni 2020

Organized by Institute for Research and Community Services
University of Mataram, Indonesia

Proceedings International Conference on Science and Technology (ICST)

e-ISSN: 2722-7375 pp: 209-213, Vol. 1, Juni 2020

Some Characteristics of Prime Submodules of Gaussian Integer Modulo over Integer

Rina Juliana[1)], I Gede Adhitya Wisnu Wardhana[2)*], Irwansyah[3)]

[1), 2)*, 3)]Universitas Mataram, Jl. Majapahit No. 62 Indonesia

*Corresponding Author: adhitya.wardhana@unram.ac.id

Abstract. Prime numbers known as fundamental tools in digital security of internet, but Quantum computers might be a serious threat to most algorithm in digital security, such as the popular RSA algorithm. Recently the study of abstraction of prime numbers into a more complex mathematical system is a hot topic, and mathematicians hope that this study will deliver a new method in the future. In this article, we will give some characteristics of one abstraction of prime numbers in ring theory. This particular abstraction is in the Gaussian integer modulo over integer.

Keywords: Gaussian integer modulo, prime number, ring theory

1. Introduction

Prime numbers known as a fundamental tools in digital security of internet. Prime numbers are used to generate the decryption and encryption keys on several cryptographic algorithms. But Quantum computers might be a serious threat to most algorithm in cryptography, such as the popular RSA algorithm. As we know, classical computers that we use today can only encode information in bits that take the value of 1 or 0. Quantum computing, on the other hand, uses quantums bits or qubits. Its make quantum computers good at sorting, finding prime numbers, even quickly solve a problem that a conventional computer would take an impractically long time to solve. That's why quantum computers can be a serious threat to the data security. One of the efforts that mathematicians do in finding alternatives to create new security methods in cryptography is to study the abstraction of prime numbers.

Recently the study of abstraction of prime numbers into a more complex mathematical system is a hot topic, and mathematicians hope that this study will deliver a new method in the future. Abstraction of prime numbers into more complex mathematical system, such as ring theory has been carried out since 1871 by Dedekind, the result is the introduction of prime ideal. Then in 1978, Dauns introduced a new mathematical system called prime submodule, which was a generalization of the prime ideal. In this article, we will give some characteristics of one abstraction of prime numbers in ring theory. This particular abstraction is in the Gaussian integer modulo over integer.

2. Method

The method used in this study is Deductive Proof, this method done by making a conjecture based on the properties that already exist and then proven with rigorous proof. The first step taken is to review the definitions and theories regarding modules, prime submodules, and $\mathbb{Z}_n[i]$. Next, is to examines some examples and discusses some of the characteristics of the prime submodules in the $\mathbb{Z}_n[i]$ module over $\mathbb{Z}$.

3. Results

In this section we will discuss about prime numbers, modules, and characteristics of prime submodule of Gaussian integer modulo over integer. The results that obtained from this study denoted by (*).
First, we will give some definition about group and ring theory.

Definition 1 (Group)[2]
A group $(G,*)$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

- For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$. (associativity of $*$)
- There is an element e in G such that for all $x \in G$, $e * x = x * e = x$. (identity element e for $*$)
- Corresponding to each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$. (inverse a' of a)

Definition 2 (Ring) [2]
A ring $(R,+,.)$ is a set R together with two binary operations + and ., which we call addition and multiplication, defined on R such that the following axioms are satisfied:

- $(R, +)$ is a commutative group.
- Multiplication is associative.
- For all $a, b, c \in R$, the left distributive law, $a \times (b + c) = (a \times b) + (a \times c)$ and the right distributive law $(a + b) \times c = (a \times c) + (b \times c)$ hold.

Some examples of group are $\mathbb{Z}$ and $\mathbb{Z}_n[i]$ under the addition. We can define $\mathbb{Z}_n[i] = \{a + ib | a, b \in \mathbb{Z}_n\}$[4]. Then, we will give definition of prime number. The definition given as follow.

Definition 3 (Prime number) [2]
A non zero element p of integral domain D is prime if for all $a, b \in D$, $p|ab$ implies $p|a$ or $p|b$.

Module is a mathematical system that combines the groups and rings concept. The definition of modules and submodules given as follow.

Definition 4 (Modules) [3]
Let R be a commutative ring with identity, whose elements are called scalars. An R −module (or a module over R) is a nonempty set M, together with two operations. The first operations, called addition and denoted by $+$, assign to each pair $(u, v) \in M \, x \, M$, an element $u + v \in M$. The second operation, denoted by juxtaposition, assign to each pair $(r, v) \in R \, x \, M$, an element $rv \in M$. Furthermore, the following properties must hold:

- $(M, +)$ is commutative group.
- For all $r, s \in R$ and $m, n \in M$
  1. $(r + s)m = rm + sm$
  2. $(rs)m = r(sm)$
  3. $r(m + n) = rm + rn$
  4. $1m = m$

Definition 5 (Submodules) [3]
Is a nonempty subset N of M that is an R −module in its own right, under the operations obtained by restricting the operations of M to N.

Definition 6 (Cyclic submodules) [3]
Let M be an R −module. A submodule of the form $\langle\langle v\rangle\rangle = Rv = \{rv \mid r \in R\}$, for $v \in M$ is called the cyclic submodule generated by v.

If we have two submodules N, K of module M. We can define the fraction submodule N of K as $(N:K) = \{r \in R \mid rK \subseteq N\}$. For the example, if we have $M = \mathbb{Z}_2[i]$ module over $\mathbb{Z}$ and $N = \langle\langle 0\rangle\rangle$ submodule of M, we get $(N:M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{\bar{0}\} = 2\mathbb{Z}$. Therefore we can construct the first theorem as follow.

Theorem 1*
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with $n = {p_1}^{k_1}{p_2}^{k_2} \dots {p_j}^{k_j}$, $p_1, p_2, \dots, p_j$ are different prime numbers and $k_1, k_2, \dots, k_j$ are natural numbers. If N submodule of M, then $(N:M) = n\mathbb{Z}$.
Proof:
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with $n = {p_1}^{k_1}{p_2}^{k_2} \dots {p_j}^{k_j}$, $p_1, p_2, \dots, p_j$ are different prime numbers and $k_1, k_2, \dots, k_j$ are natural numbers. N submodule of M, let $N = \langle\langle a + ib\rangle\rangle$ with $a, b \in \mathbb{Z}_n$. We can define (N:M) as $(N:M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(c + id) \in N, \forall c, d \in \mathbb{Z}_n\}$. Therefore $rc + i\,rd = sa + i\,sb$ for some $s \in \mathbb{Z}$. Then we get $rc = sa = rd = sb = 0 = nk$ for some $k \in \mathbb{Z}$. It implies $n|rc$, because n prime number, then $n|r$ or $n|c$. We get $n|r$, so $r = nl$ for $l \in \mathbb{Z}$. Therefore, $(N:M) = n\mathbb{Z}$.
■
Then if n is a prime number, $\mathbb{Z}_n[i]$ have some special properties that defined in theorem 2, 3 and 4.

Theorem 2*
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number.if $a, b \in M$, with $a, b \neq 0$, then $a \neq \gamma b$ for $\gamma \in \mathbb{Z}$, if and only if $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$
Proof:
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number.if $a, b \in M$, with $a, b \neq 0$,
$(\rightarrow)$ Let $a \neq \gamma b$ for all $\gamma \in \mathbb{Z}$. Suppose $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$, then $a \in \langle\langle b\rangle\rangle$, such that $a = \alpha b$ for some $\alpha \in \mathbb{Z}$. Contradiction with the statement. Therefore $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$.
$(\leftarrow)$ Let $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Suppose that $a = \alpha b$ for some $\alpha \in \mathbb{Z}$, then $a \in \langle\langle b\rangle\rangle$. Such that $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$. Contradictions with the statement. Therefore $a \neq \gamma b$ for all $\gamma \in \mathbb{Z}$.
■
Theorem 3*
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number. if $a, b \in M$, with $a, b \neq 0$, then $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$ if and only if $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$.
Proof:
Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number. if $a, b \in M$, with $a, b \neq 0$.
$(\rightarrow)$ Let $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$, will be shown $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$. Suppose $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle \neq \{0\}$, then there are $0 \neq c \in \langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle$. Therefore $c = \gamma_1 a = \gamma_2 b$ for some $\gamma_1, \gamma_2 \in \mathbb{Z}$. We get $\bar{\gamma_1} \neq 0$, because n is a prime number then there are $\delta \in \mathbb{Z}$ such that $\delta\bar{\gamma_1} = \bar{1}$. Then $a = \delta\gamma_2 b = \beta b$, or $a \in \langle\langle b\rangle\rangle$. Thus $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$, contradiction with the statement. Therefore, $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$.
$(\leftarrow)$ If $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$, then clearly $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$.

■

Theorem 4*

Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number. if $a, b \in M$, with $a, b \neq 0$, $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$ then $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = M$.

Proof:

Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number. if $a, b \in M$, with $a, b \neq 0$, $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Clearly $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle \subseteq M$.

We know that the cardinality of M or $|M| = n^2$. Based on the definition, $\langle\langle a\rangle\rangle = \{ra | r \in \mathbb{Z}\} = \{0, x_1, \dots, x_{n-1}\}$ and $\langle\langle b\rangle\rangle = \{rb | r \in \mathbb{Z}\} = \{0, y_1, \dots, y_{n-1}\}$, therefore $|\langle\langle a\rangle\rangle| = |\langle\langle b\rangle\rangle| = n$.

Based on theorem 3, we get $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$, then let $A = \{x_i + y_j | i, j = 1, \dots, n-1\}$, we get $x_i + y_j \notin \langle\langle a\rangle\rangle \cup \langle\langle b\rangle\rangle$ and $|A| = (n-1)^2 = n^2 - 2n + 1$. Therefore $|\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle| = |A \cup \langle\langle a\rangle\rangle \cup \langle\langle b\rangle\rangle| = n^2 - 2n + 1 + 2n - 1 = n^2 = |M|$.Thus $M \subseteq \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle$. Then we can conclude that $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = M$.

■

As we know, prime submodule is one of the abstraction of prime numbers in ring theory. The definition of prime submodule given as follow.

Definition 7 (Prime submodule) [1]

A proper submodule N of M is said to be prime if whenever $r \in R$, $x \in M$, $rx \in N$ implies either $x \in N$ or $r \in (N:M)$.

If we have $M = \mathbb{Z}_3[i]$ module over $\mathbb{Z}$, and $\mathrm{N}_1 = \langle\langle 0\rangle\rangle$ submodule of M. we know that $(\mathrm{N}_1 : \mathrm{M}) = 3\mathbb{Z}$. N_1 is a prime submodule of M, because for $r \in \mathbb{Z}$, $m \in M$, $rm \in N_1$, can be written as $ra + rbi = 0 = 3k$, for $k \in \mathbb{Z}$. Such that $ra = rb = 3k$. Therefore $3|ra$, implies $3|r\ (r \in 3\mathbb{Z} = (N_1:M))$ or $3|a\ (a = 3k = \bar{0} \in N_1)$. And then if we have $\mathrm{N}_2 = \langle\langle 1\rangle\rangle$, $N_3 = \langle\langle 1 + i\rangle\rangle$, these submodules are prime also, with the same reason.

But if we have $\mathrm{M} = \mathbb{Z}_4[\mathrm{i}]$ module over $\mathbb{Z}$, and $\mathrm{N}_1 = \langle\langle 0\rangle\rangle$. We know that $(\mathrm{N}_1 : \mathrm{M}) = 4\mathbb{Z}$. N_1 is not prime, because for $r \in \mathbb{Z}$ and $m \in M$, $rm = \bar{0} \in N_1$, there are $r = 2 \notin (N_1:M)$ and $m = 2 \notin N_1$ such that $rm = \bar{0}$. Therefore, we can construct the last theorem as follow.

Theorem 5*

Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number, $\langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle = M$ for some $a, b \in M$. Let $N = \alpha\langle\langle a\rangle\rangle \oplus \beta\langle\langle b\rangle\rangle$ be submodule of M, N prime submodule of M if and only if $N = \langle\langle a\rangle\rangle$ or $N = \langle\langle b\rangle\rangle$, or $N = \langle\langle 0\rangle\rangle$.

Proof:

Let $M = \mathbb{Z}_n[i]$ be module over ring $\mathbb{Z}$, with n prime number, $\langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle = M$ for some $a, b \in M$. $N = \alpha\langle\langle a\rangle\rangle \oplus \beta\langle\langle b\rangle\rangle$ submodule of M.

$(\rightarrow)$ N prime submodule of M, then for each $r \in \mathbb{Z}$ and $m \in M$ such that $rm \in N$, implies $r \in (N:M)$ or $m \in N$. Based on theorem 1, $(N:M) = n\mathbb{Z}$. We have $\alpha, \beta < n$, if $\alpha = 0$ then $N = \beta\langle\langle b\rangle\rangle$. Because n is a prime number, then $(\beta, n) = 1$ or $(\beta, n) = 0$. Therefore $N = \langle\langle b\rangle\rangle$, or $N = \langle\langle 0\rangle\rangle$. Otherwise, if $\beta = 0$, we get $N = \langle\langle a\rangle\rangle$, or $N = \langle\langle 0\rangle\rangle$.

$(\leftarrow) N = \langle\langle a\rangle\rangle$ or $N = \langle\langle b\rangle\rangle$ or $N = \langle\langle 0\rangle\rangle$, its mean that $N = \langle\langle \alpha + i\beta\rangle\rangle$ for $\alpha, \beta \in \mathbb{Z}_n$. Because n is a prime number, then $(n, \alpha) = (n, \beta) = 1$, or $(n, \alpha) = (n, \beta) = n$. Let $r \in \mathbb{Z}$ and $m = m_1 + im_2 \in M$ such that $rm \in N$.

Case 1: $(n, \alpha) = n$

Its mean that $n|a$, or $a = ln$ for some $l \in \mathbb{Z}$. Because $rm \in N$, then $rm_1 = s\alpha$ for $s \in \mathbb{Z}$. Therefore, we get $rm_1 - s\alpha = kn$ such that $rm_1 - sln = kn$, then $rm_1 = tn$. Such that $n|rm_1$. Because n is a prime number, then $n|r$ $(r \in (N:M))$ or $n|m_1 (m_1 = un \in \langle\alpha\rangle)$.
Case 2: $(n, \alpha) = 1$
Because n is a prime number and $(n, \alpha) = 1$, then $\langle\alpha\rangle = \langle 1\rangle = \mathbb{Z}_n$. If we have $rm_1 = s\alpha$ for $s \in \mathbb{Z}$, for $rm_1 = 0$, its implies $r \in (N:M)$ or $m_1 = un \in \langle\alpha\rangle$. For $rm_1 \neq 0$, its impies $m_1 = l1 \in \langle\alpha\rangle$.
The same results holds for $(n, \beta) = n$ or $(n, \beta) = 1$. Thus, N is a prime submodule of M.
■

References

[1] Dauns, J., 1978, ***Prime Submodules***, J. Rine Angew Math., **1978:298**, pp. 156- 181.
[2] Fraleigh, J. B., 2014, ***A First Course in Abstract Algebra 7th ed***, Pearson Education Limited, USA.
[3] Roman, Steven. 2008. ***Advanced Linier Algebra, 3rd ed.***, Springer, New York.
[4] Rosiyanti, H., 2015, ***Wakil Unsur Pembangun Ideal dari Bilangan Bulat Gauss Modulo*** $\mathbb{Z}_m[i]$**,** Jurnal Pendidikan Matematika & Sains, 1(1), pp. 97- 100.