AIP Conference Proceedings

COUNTRY

United States

Universities and research institutions in United States

SUBJECT AREA AND CATEGORY

Physics and Astronomy
Physics and Astronomy (miscellaneous)

PUBLISHER

American Institute of Physics

H-INDEX

75

PUBLICATION TYPE

Conferences and Proceedings

ISSN

0094243X, 15517616

COVERAGE

1974-1978, 1983-1984, 1993, 2000-2001, 2003-2020

INFORMATION

Homepage

How to publish in this journal

confproc@aip.org

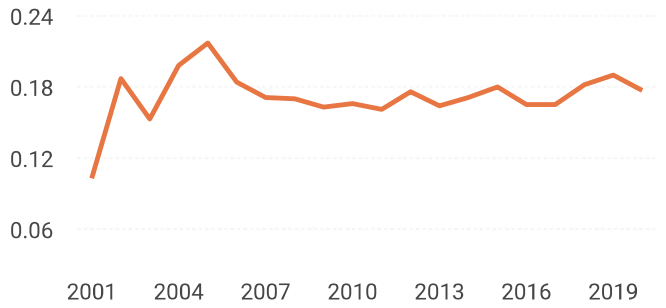
SCOPE

Today, AIP Conference Proceedings contain over 100,000 articles published in 1700+ proceedings and is growing by 100 volumes every year. This substantial body of scientific literature is testament to our 40-year history as a world-class publishing partner, recognized internationally and trusted by conference organizers worldwide. Whether you are planning a small specialist workshop or organizing

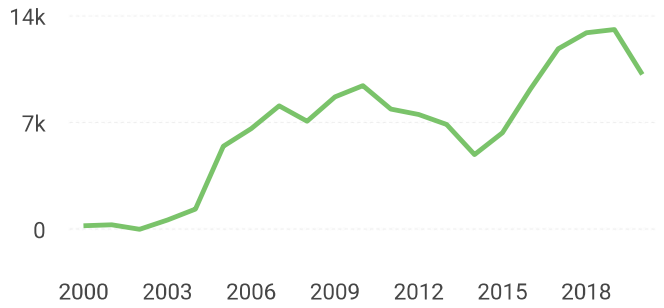
the largest international conference, contact us, or read these testimonials, to find out why so many organizers publish with AIP Conference Proceedings.

Join the conversation about this journal

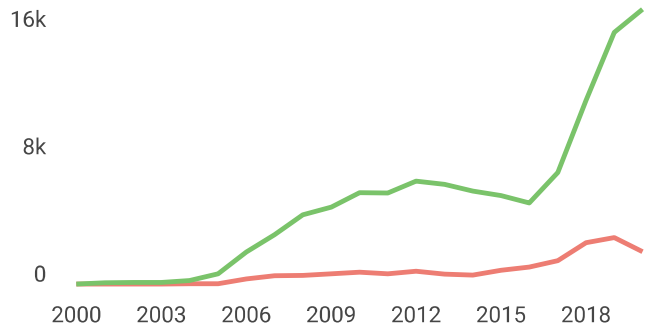
SJR



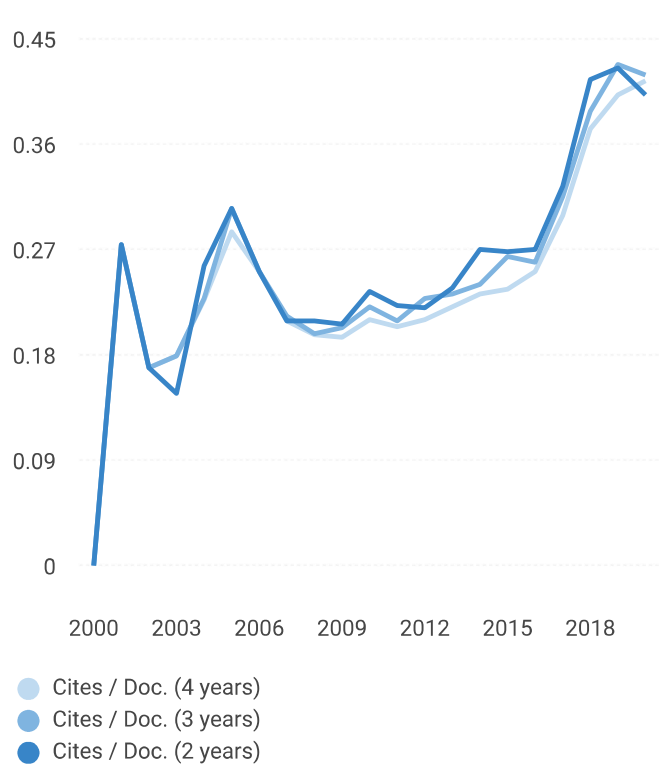
Total Documents



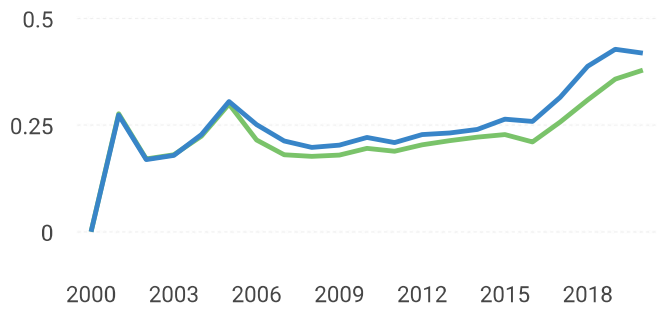
Total Cites Self-Cites



Citations per document

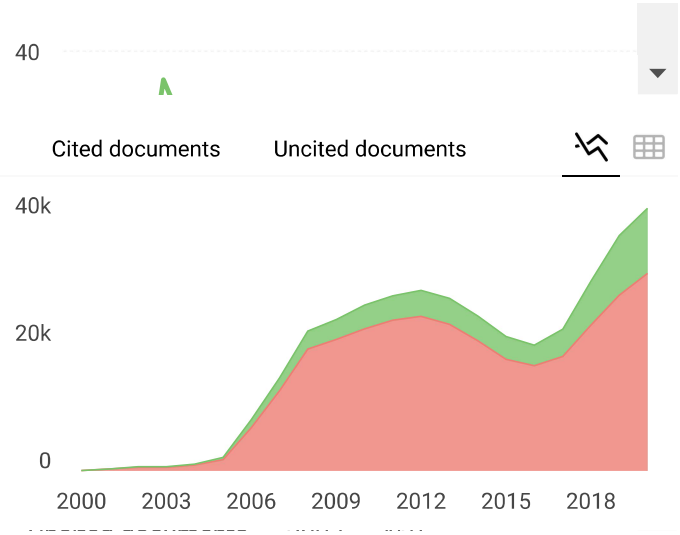


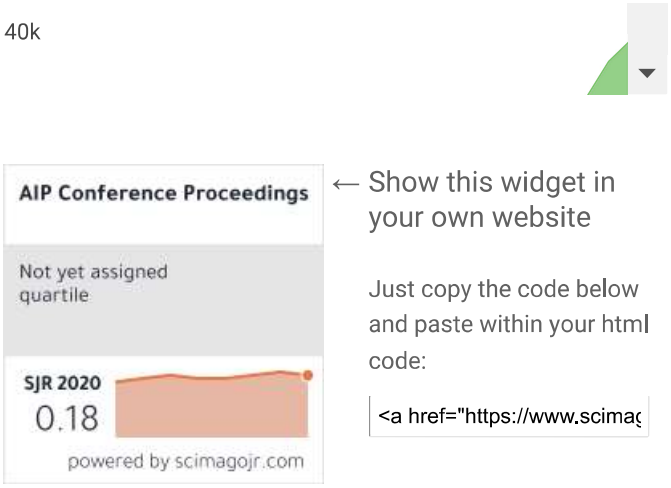
External Cites per Doc Cites per Doc



% International Collaboration

Citable documents Non-citable documents

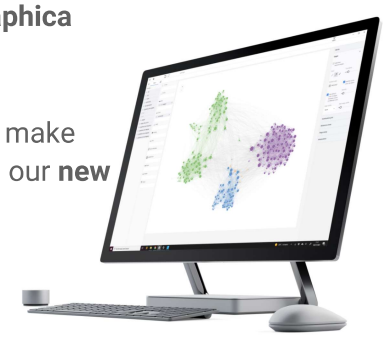




← Show this widget in your own website

Just copy the code below and paste within your html code:

<a href="https://www.scimag



Metrics based on Scopus® data as of April 2021

Loading comments...

Developed by: SCImago

Powered by: Scopus

Follow us on @ScimagoJR

Some characteristics of cyclic prime, weakly prime and almost prime submodule of Gaussian integer modulo over integer

Cite as: AIP Conference Proceedings **2329**, 020004 (2021); https://doi.org/10.1063/5.0042586
Published Online: 26 February 2021

Rina Juliana, I. Gede Adhitya Wisnu Wardhana, and Irwansyah

Some Characteristics of Cyclic Prime, Weakly Prime and Almost Prime Submodule of Gaussian Integer Modulo over Integer

Rina Juliana[a)], I Gede Adhitya Wisnu Wardhana[b)], Irwansyah[c)]

Algebra Research Group, Universitas Mataram, Jl Majapahit No.62, Mataram, 83125, Indonesia

[a)]rinajuliana@unram.ac.id
[b)]Corresponding author: adhitya.wardhana@unram.ac.id
[c)]irw@unram.ac.id

Abstract. Cryptography is a branch of mathematics used in digital security systems. Some cryptographic algorithms, such as RSA, depending on the prime factorization of integers. However, quantum computers might be a threat to some algorithms in cryptography. One of the mathematicians' efforts in finding alternatives to create new security technologies in cryptography is to study the abstraction of prime numbers. The prime submodule is one of the prime numbers abstraction, which was introduced by Dauns in 1978. Lately, the prime submodules were generalized into weakly prime submodules and almost prime submodules. This study will examine the characteristics of prime, weakly prime, and almost prime of cyclic submodules on $\mathbb{Z}-$module $\mathbb{Z}_n[i]$. The results are if n is a prime number, then the cyclic submodule is prime submodule on $\mathbb{Z}-$module $\mathbb{Z}_n[i]$ and the cyclic almost prime submodule equivalent with cyclic weakly prime submodule on $\mathbb{Z}-$module $\mathbb{Z}_n[i]$.

INTRODUCTION

Prime numbers are known as fundamental tools in the digital security of the 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 algorithms 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 quantum bits or qubits. It makes 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 data security. One of the efforts that mathematicians make 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. The abstraction of prime numbers into a more complex mathematical system, such as ring theory, has been carried out since 1871 by Dedekind, the result is the introduction of the prime ideal. Then in 1978, Dauns introduced a new mathematical system called the prime submodule, which was a generalization of the prime ideal [1]. Furthermore, in 2009, the concept of prime submodules was generalized by Hadi into weakly prime submodule [2]. Then in 2012, the concept was re-generalized into an almost prime submodule by Khashan [3].

The properties of prime numbers in the integer ring are different from the prime numbers in the Gaussian integer ring ($\mathbb{Z}[i]$), this was discussed by Maulana et al. [4]. One interesting fact is that not all prime numbers on integers are also prime numbers on Gaussian integers. Prime numbers on the integers ring are prime numbers in the Gaussian integers ring if and only if the numbers are congruent with 3 (mod 4). Wardhana and Astuti in 2014 discussed the

International Conference on Mathematics, Computational Sciences and Statistics 2020
AIP Conf. Proc. 2329, 020004-1–020004-7; https://doi.org/10.1063/5.0042586
Published by AIP Publishing. 978-0-7354-4073-9/$30.00

characteristics of weakly prime submodules and almost prime submodules on the integer modulo, namely $\mathbb{Z}-$ module $\mathbb{Z}_n$ [5].

The concepts of prime, weakly prime, and almost prime submodules in $\mathbb{Z}-$ module $\mathbb{Z}$ equivalent. But in $\mathbb{Z}-$ module $\mathbb{Z}_n$ there are many examples of almost prime submodules that are not weakly prime submodules. Therefore, in this study, we will find out the characteristics of cyclic prime, weakly prime, and almost prime submodules in the more complex structure, namely Gaussian integers modulo that generated over $\mathbb{Z}$ or can be written as $\mathbb{Z}-$ module $\mathbb{Z}_n[i]$.

SOME BASIC NOTIONS

Let R be a finitely generated integral domain, then a non-zero element of R is called prime if it satisfies this definition.

Definition 1. [6] A non-zero element p of integral domain D is prime if for all $a, b \in D$, $p|ab$ implies $p|a$ or $p|b$.

A module is a mathematical system that combines the group and ring concept. The definition of modules and submodules given as follow.

Definition 2. [6] 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, assigns to each pair $(r, v) \in R\ x\ M$, an element $rv \in M$. Furthermore, the following properties must hold:

- $(M, +)$ is a 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 3. [6] Let M be an $R-$ module. A non-zero element $v \in M$ for which $rv = 0$ for some non-zero $r \in R$ is called a torsion element of M. A module that has no non-zero torsion elements is said to be torsion-free. If all elements of M are torsion elements, then M is a torsion module.

A subset of any module over ring R that generate a module over the same ring is called submodule, the definition is given below.

Definition 4. [6] A submodule is a nonempty subset N of module M that is an $R-$module in its own right, under the operations obtained by restricting the operations of M to N.

The submodule generates by an element of module M is called the cyclic submodule, defined as follows.

Definition 5. [6] Let M be an $R-$module. A submodule of the form $\langle\langle v\rangle\rangle = Rv = \{rv\ |r \in R\}$, 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 $(N:K) = \{r \in R\ |rK \subseteq \mathrm{N}\}$. Now we will give the definition of the prime submodule, weakly prime submodule, and almost prime submodule.

Definition 6. [1] Let R be a commutative ring with identity and let M be $R-$module. 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 $r \in (N:M)$.

Definition 7. [3] Let R be a commutative ring with identity and let M be $R-$module. A proper submodule N of M is said to be weakly prime if whenever $r \in R,\ x \in M,\ rx \in N - \{0\}$ implies either $x \in N$ or $r \in (N:M)$.

Based on Definition 7, we know that every prime submodule is weakly prime, and zero submodules of any module are also weakly prime. The torsion module that is finitely generated over the integral domain, weakly prime submodule, only consists of a prime submodule and zero submodules, these properties given by Theorem 1.

Theorem 1. [7]
Let M be a torsion module that finitely generated over the principal ideal domain, and proper submodule N is weakly prime if and only if N is prime submodule or zero submodules. □

Definition 8. [3] Let R be a commutative ring with identity and let M be R −module. A proper submodule N of M is said to be almost prime if whenever $r \in R,\ x \in M,\ rx \in N - (N:M)N$ implies either $x \in N$ or $r \in (N:M)$.

MAIN RESULTS

Let $\mathbb{Z}_n[i] = \{\overline{a} + \overline{b}i \,|\overline{a}, \overline{b} \in \mathbb{Z}_n\}$ be the module over ring $\mathbb{Z}$ or can be written by $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$, with addition (mod n) operation and scalars product (mod n). Some examples of a cyclic submodule of $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ are given below.

Example 1.
The set $N_1 = \langle\langle\overline{0}\rangle\rangle, N_2 = \langle\langle\overline{1}\rangle\rangle,\ N_3 = \langle\langle i\rangle\rangle, N_4 = \langle\langle\overline{1} + i\rangle\rangle$ subset of $\mathbb{Z}$ −module $\mathbb{Z}_2[i]$ are submodules of $\mathbb{Z}$ −module $\mathbb{Z}_2[i]$. Some of the cyclic submodules of $\mathbb{Z}$ −module $\mathbb{Z}_3[i]$ are $N_1 = \langle\langle i\rangle\rangle$, $N_2 = \langle\langle\overline{1} + i\rangle\rangle$ and $N_3 = \langle\langle\overline{1} + \overline{2}i\rangle\rangle$.

We know that $(N:M) = \{r \in R \,|rM \subseteq \text{N}\}$. Now we will see some example of $(N:M)$ for $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$.

Example 2.
Let $N = \langle\langle\overline{0}\rangle\rangle$ be a submodule of $M = \mathbb{Z}_2[i]$ a module over ring $\mathbb{Z}$. We have $(N:M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 2\mathbb{Z}$. Let $N = \langle\langle\overline{1} + i\rangle\rangle$ be a submodule of $M = \mathbb{Z}_3[i]$ a module over ring $\mathbb{Z}$. We have $(N:M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 3\mathbb{Z}$.

Therefore we have a conjecture that for submodule N cyclic of $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$, $(N:M) = n\mathbb{Z}$. This conjecture will be proven in Theorem 2.

Theorem 2. Let $M = \mathbb{Z}_n[i]$ be a module over ring $\mathbb{Z}$, with $n = {p_1}^{k_1}{p_2}^{k_2} \ldots {p_j}^{k_j}$, $p_1, p_2, \ldots, p_j$ are different prime numbers and $k_1, k_2, \ldots, k_j$ are natural numbers. If N a cyclic submodule of M, then $(N:M) = n\mathbb{Z}$.

Proof. Let $N = \langle\langle\overline{a} + \overline{b}i\rangle\rangle$ with $\overline{a}, \overline{b} \in \mathbb{Z}_n$, we can choose a and b such that $a, b < n$. For $n = 2$ and $n = 3$, it's clear that $(N:M) = n\mathbb{Z}$, therefore we will prove this for $n > 3$. For each $r \in (N:M)$, we can divide a and b to four cases below.

Case 1: $a \nmid n$ and $b \nmid n$
Choose $\overline{a} \in M$, then $r\overline{a} = s\overline{a} + s\overline{b}i$ for some $s \in \mathbb{Z}$. Since $b \nmid n$ and $b < n$, we have $(b, n) = 1$. Since $s\overline{b} = \overline{0}$, then $sb = nk_1$ for some $k_1 \in \mathbb{Z}$, or $n \mid sb$. Since $\gcd(b, n) = 1$, we have $n \mid s$, or $s = nk_2$ for some $k_2 \in \mathbb{Z}$. Therefore $s\overline{a} = \overline{0} = r\overline{a}$. Since $a \nmid n$ and $a < n$ we have $\gcd(a, n) = 1$. Since $r\overline{a} = \overline{0}$, then $ra = nk_3$ for some $k_3 \in \mathbb{Z}$, or $n \mid ra$. Since $\gcd(a, n) = 1$, therefore $n \mid r$, or $r = nk_4$ for some $k_4 \in \mathbb{Z}$.

Case 2: $a \mid n$ and $b \nmid n$
Choose $\overline{b} \in M$, then $r\overline{b} = s\overline{a} + s\overline{b}i$ for some $s \in \mathbb{Z}$. Since $b \nmid n$ and $b < n$, we have $\gcd(b, n) = 1$. We have $s\overline{b} = \overline{0}$, then $sb = nk_1$ for some $k_1 \in \mathbb{Z}$, or $n \mid sb$. Since $\gcd(b, n) = 1$, we have $n \mid s$, or $s = nk_2$ for some $k_2 \in \mathbb{Z}$.

Therefore $s\bar{a} = \bar{0} = r\bar{b}$. Since $r\bar{b} = \bar{0}$, then $rb = nk_3$ for some $k_3 \in \mathbb{Z}$, or $n \mid rb$. Since $\gcd(b,n) = 1$, therefore $n \mid r$, or $r = nk_4$ for some $k_4 \in \mathbb{Z}$.

Case 3: $a \nmid n$ and $b \mid n$
Choose $\bar{a}i \in M$, then $r\bar{a}i = s\bar{a} + s\bar{b}i$ for some $s \in \mathbb{Z}$. Since $a \nmid n$ and $a < n$, we have $\gcd(a,n) = 1$. We have $s\bar{a} = \bar{0}$, then $sa = nk_1$ for some $k_1 \in \mathbb{Z}$, or $n \mid sa$. Since $\gcd(a,n) = 1$, we have $n \mid s$, or $s = nk_2$ for some $k_2 \in \mathbb{Z}$. Therefore $s\bar{b}i = \bar{0} = r\bar{a}i$. Since $r\bar{a} = \bar{0}$, then $ra = nk_3$ for some $k_3 \in \mathbb{Z}$, or $n \mid ra$. Since $\gcd(a,n) = 1$, therefore $n \mid r$, or $r = nk_4$ for some $k_4 \in \mathbb{Z}$.

Case 4: $a \mid n$ and $b \mid n$

- $\bar{a} = \bar{b}$
  Choose $\overline{n-1} \in M$, then $r\overline{(n-1)} = s\bar{a} + s\bar{b}i$ for some $s \in \mathbb{Z}$. We have $s\bar{b} = s\bar{a} = \bar{0}$, such that $r\overline{(n-1)} = \bar{0}$. Then $r(n-1) = nk$ for some $k \in \mathbb{Z}$, or $n \mid r(n-1)$. Since $\gcd(n-1,n) = 1$ for $n > 3$, therefore $n \mid r$, or $r = nl$ for some $l \in \mathbb{Z}$.
- $\bar{a} \neq \bar{b}$
  Choose $\overline{n-1} + \overline{n-1}i \in M$, then $r\overline{(n-1)} + r\overline{(n-1)}i = s\bar{a} + s\bar{b}i$ for some $s \in \mathbb{Z}$. We have $s\bar{a} = s\bar{b} = r\overline{(n-1)}$. Since $a \neq b$ and $a, b < n$, then $s\bar{a} = s\bar{b} = \bar{0}$, such that we have $r\overline{(n-1)} = \bar{0}$. We have $r(n-1) = nk$ for some $k \in \mathbb{Z}$, or $n \mid r(n-1)$. Since $\gcd(n-1,n) = 1$ for $n > 3$, therefore $n \mid r$, or $r = nl$ for some $l \in \mathbb{Z}$.

Therefore we have $r \in n\mathbb{Z}$. Conversely, for each $r \in n\mathbb{Z}$, it is clear that $r \in (N:M)$. Therefore, we conclude that $(N:M) = n\mathbb{Z}$. □

If we have two elements $a, b \in M$, then we have the properties that are given below.

Theorem 3. Let $M = \mathbb{Z}_n[i]$ be a 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 $a, b \in M$, with $a, b \neq 0$, then $a \neq kb$ or $b \neq la$ for all $k, l \in \mathbb{Z}$, if and only if $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$.

Proof. Let $a \neq kb$, $b \neq la$ for all $k, l \in \mathbb{Z}$. Suppose $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$, then $a \in \langle\langle b\rangle\rangle$ and $b \in \langle\langle a\rangle\rangle$ such that $a = \alpha b$ and $b = \beta a$ for some $\alpha, \beta \in \mathbb{Z}$. Contradiction with the statement. Therefore $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$.
Conversely, let $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Suppose that $a = kb$ and $b = la$ for some $k, l \in \mathbb{Z}$., then $a \in \langle\langle b\rangle\rangle$ and $b \in \langle\langle a\rangle\rangle$. We have $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$. Contradiction with the statement. Therefore $a \neq kb$ or $b \neq la$ for all $k, l \in \mathbb{Z}$. □

If we have two different non-zero cyclic submodules of module $M = \mathbb{Z}_n[i]$ over ring $\mathbb{Z}$ with n prime number, we can write module M as the direct sum product of the two cyclic submodules. These properties are given by Theorem 3 and Theorem 4.

Theorem 4. Let $M = \mathbb{Z}_n[i]$ be a 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 $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Suppose that $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle \neq \{\bar{0}\}$. Then there are $c \neq \bar{0}$, $c \in \langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle$ such that $c = \gamma_1 a = \gamma_2 b$ for some $\gamma_1, \gamma_2 \in \mathbb{Z}$, we can choose γ_1, γ_2 such that $\gamma_1, \gamma_2 < n$. We have $\gamma_1 \neq 0$, since $\gamma_1 < n$ and n prime, then $(\gamma_1, n) = 1$. Then there exist $p, q \in \mathbb{Z}$ such that $1 = p\gamma_1 + qn$, or $\bar{p}\gamma_1 = \bar{1}$. Let $a = \overline{a_1} + \overline{a_2}i$ and $b = \overline{b_1} + \overline{b_2}i$, then $\gamma_1(\overline{a_1} + \overline{a_2}i) = \gamma_2(\overline{b_1} + \overline{b_2}i)$. We have $\bar{p}\gamma_1(\overline{a_1} + \overline{a_2}i) = \bar{p}\gamma_2(\overline{b_1} + \overline{b_2}i)$, since $\bar{p}\gamma_1 = \bar{1}$ then $(\overline{a_1} + \overline{a_2}i) = \bar{p}\gamma_2(\overline{b_1} + \overline{b_2}i)$. We have $a = p\gamma_2 b$, or $a \in \langle\langle b\rangle\rangle$. Therefore, $\langle\langle a\rangle\rangle \subseteq \langle\langle b\rangle\rangle$. By using the same process, we have $b \in \langle\langle a\rangle\rangle$, such that $\langle\langle b\rangle\rangle \subseteq \langle\langle a\rangle\rangle$. Therefore, $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$. Contradiction with the statement $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. We conclude that $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$.

Conversely, If $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$, it is clear that $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. □

Theorem 5. Let $M = \mathbb{Z}_n[i]$ be a 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 $\langle\langle a\rangle\rangle \bigoplus \langle\langle b\rangle\rangle = M$.

Proof. 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, since n prime number, $\langle\langle a\rangle\rangle = \{ra | r \in \mathbb{Z}\} = \{0, x_1, \dots, x_{n-1}\}$ 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 have $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{0\}$, 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 $M \subseteq \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle$. Therefore we can conclude that $\langle\langle a\rangle\rangle \bigoplus \langle\langle b\rangle\rangle = M$. □

Based on Theorem 3 and Theorem 4, we know that for module $M = \mathbb{Z}_n[i]$ with n prime number, the proper submodules of M only consist of a cyclic submodule given by Theorem 5.

Theorem 6. Let $M = \mathbb{Z}_n[i]$ module over ring $\mathbb{Z}$, with n prime number, then

1. For each N proper submodule of M, N is a cyclic submodule
2. For each N proper submodule of M, then $(\mathrm{N}:\mathrm{M}) = \mathrm{n}\mathbb{Z}$.

Proof.

1. Let $N = \langle\langle a, b\rangle\rangle$ be a proper submodule of M that generates by two elements $a, b \in M$. Then by Theorem 3, we have $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$. Then by Teorema 4, we have $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = M$. Then $N = \langle\langle a, b\rangle\rangle$ is not a proper submodule of M. Therefore, submodule N must be cyclic.
2. Based on the proof of point 1, we have N is the cyclic submodule. Therefore, by Teorema 1, we have $(N:M) = n\mathbb{Z}$. □

Some examples of a cyclic prime submodule of module $M = \mathbb{Z}_n[i]$ over ring $\mathbb{Z}$ are given below.

Example 3.

Let $M = \mathbb{Z}_2[i]$ a module over ring $\mathbb{Z}$. Submodules $N_1 = \langle\langle\bar{0}\rangle\rangle, N_2 = \langle\langle\bar{1}\rangle\rangle, N_3 = \langle\langle i\rangle\rangle, N_4 = \langle\langle\bar{1} + i\rangle\rangle$ are prime submodules, since for each $r \in \mathbb{Z}$ and $m \in \mathbb{Z}_2[i]$ such that $rm \in N_i$, implies $r \in (N_i:M)$ or $m \in N_i$. Let $M = \mathbb{Z}_4[i]$ a module over ring $\mathbb{Z}$, submodule $N = \langle\langle\bar{0}\rangle\rangle$ is not prime, since there exist $r = 2 \notin (N:M)$ and $m = \bar{2} \notin N$ such that $rm = \bar{0} \in N$.

From Example 3, we have a conjecture that for $M = \mathbb{Z}_n[i]$ a module over ring $\mathbb{Z}$, with n prime number, each of the proper submodule of M is prime. This conjecture will be proven by Theorem 7.

Theorem 7. Let $M = \mathbb{Z}_n[i]$ module over ring $\mathbb{Z}$, with n prime number, then each of the proper submodules of M is prime.

Proof. Based on Theorem 5, the proper submodule of M is only the cyclic submodule. Let $N = \langle\langle\overline{n_1} + \overline{n_2}i\rangle\rangle$ for $\overline{n_1}, \overline{n_2} \in \mathbb{Z}_n$ be the proper submodule of M. We can choose n_1 and n_2 such that $n_1, n_2 < n$. By Teorema 1, we have $(N:M) = n\mathbb{Z}$. Since n prime, then $n_1, n_2 = 0$ or $n_1, n_2 \neq 0$ equivalent with $\gcd(n, n_1) = \gcd(n, n_2) = 1$.Take $r \in \mathbb{Z}$ and $m = \overline{m_1} + \overline{m_2}i \in M$ such that $rm \in N$.

Case 1: $n_1 = 0$ and $n_2 = 0$
We have $\overline{n_1} = \bar{0}$ dan $\overline{n_2} = \bar{0}$. Since $rm \in N$, then $r\overline{m_1} = \bar{0}$ and $r\overline{m_2} = \bar{0}$, we have $rm_1 = k_1 n$ and $rm_2 = k_2 n$ for some $k_1, k_2 \in \mathbb{Z}$. Then $n \mid rm_1$ dan $n \mid rm_2$. Since n prime, we have $n \mid r$ or $n \mid m_1$ and $n \mid m_2$. We have $r = k_3 n$ for some $k_3 \in \mathbb{Z}$ or $\overline{m_1} = \overline{m_2} = \bar{0}$. Therefore we have $r \in (N:M)$ or $m = \overline{m_1} + \overline{m_2}i \in N$.

Case 2: $n_1 \neq 0$ and $n_2 \neq 0$
We have $r\overline{m_1} + r\overline{m_2}i = s\overline{n_1} + s\overline{n_2}i$ for some $s \in \mathbb{Z}$. If $r\overline{m_1} = \bar{0}$ then $r \in (N:M)$ or $\overline{m_1} = \bar{0}$. If $r\overline{m_2} = \bar{0}$, then $r \in (N:M)$ or $\overline{m_2} = \bar{0}$. Therefore, if $r\overline{m_1} = \bar{0}$ or $r\overline{m_2} = \bar{0}$, then $r \in (N:M)$. Let $r\overline{m_1} \neq \bar{0}$ and $r\overline{m_2} \neq \bar{0}$, then $\bar{r} \neq \bar{0}$. Since n prime, there are $\bar{w}$ such that $\bar{r}\bar{w} = \bar{1}$. Since $r\overline{m_1} = s\overline{n_1}$ and $r\overline{m_2} = s\overline{n_2}$, we have $\overline{m_1} = sw\overline{n_1}$ dan $\overline{m_2} = sw\overline{n_2}$. Therefore we have $m = sw\overline{n_1} + sw\overline{n_2}i \in N$.

Case 3: $n_1 = 0$ and $n_2 \neq 0$
We have $r\overline{m_1} + r\overline{m_2}i = s\overline{n_2}i$, such that $r\overline{m_1} = \bar{0}$ and $r\overline{m_2} = s\overline{n_2}i$. If $r\overline{m_2} = \bar{0}$, then $r \in (N:M)$ or $\overline{m_2} = \bar{0}$. Let $r\overline{m_2} \neq \bar{0}$, then $\bar{r} \neq \bar{0}$. Since n prime, there are $\bar{w}$ such that $\bar{r}\bar{w} = \bar{1}$. Since $r\overline{m_2} = s\overline{n_2}$, then $\overline{m_2} = sw\overline{n_2}$. Therefore we have $\overline{m_1} = \bar{0}$, such that $m = sw\overline{n_2}i \in N$.

Case 4: $n_1 \neq 0$ and $n_2 = 0$
By the same process as case 3, we have the same result. If $r\overline{m_1} = \bar{0}$, then $r \in (N:M)$ or $\overline{m_1} = \bar{0}$. If $r\overline{m_1} \neq \bar{0}$ then $m = sw\overline{n_1}i \in N$.

Therefore, N is the prime submodule. □

We know that $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ is a torsion module that finitely generated over the integral domain, therefore by Theorem 1, we have Corollary 1.

Corollary 1. Let $\mathrm{M} = \mathbb{Z}_\mathrm{n}[\mathrm{i}]$ module over ring $\mathbb{Z}$, then proper submodule N is weakly prime if and only if N is prime submodule or zero submodules.

Some examples of a cyclic almost prime submodule of $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ are given below.

Example 4.
Let $M = \mathbb{Z}_2[i]$ a module over ring $\mathbb{Z}$, submodule $N_1 = \langle\langle\bar{0}\rangle\rangle$, $N_2 = \langle\langle\bar{1}\rangle\rangle, N_3 = \langle\langle i\rangle\rangle, N_4 = \langle\langle\bar{1} + i\rangle\rangle$ are almost prime, since for each $r \in \mathbb{Z}$ and $m \in \mathbb{Z}_2[i]$ such that $rm \in N_i - (N_i:M)N_i = N - \{0\}$, implies $r \in (N_i:M) = 2\mathbb{Z}$ or $m \in N_i$ for $i = 1,2,3,4$. Let $M = \mathbb{Z}_4[i]$ a module over ring $\mathbb{Z}$, submodule $N = \langle\langle\bar{0}\rangle\rangle$ is almost prime, since for each $r \in \mathbb{Z}$ and $m \in \mathbb{Z}_4[i]$ such that $rm \in N - (N:M)N = N - \{0\}$, implies $r \in (N:M) = 4\mathbb{Z}$ or $m \in N$.

We have that every prime and weakly prime submodule is almost prime, and every cyclic almost prime submodule is weakly prime on $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$. This is because cyclic weakly prime submodule and cyclic almost prime submodule on $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ are equivalent. Therefore we have Theorem 8.

Theorem 8. Let $M = \mathbb{Z}_n[i]$ 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. Submodule N of M is cyclic. Submodule N is weakly prime if and only if N is almost prime.

Proof. Let N be a weakly prime submodule of M. Then for each $r \in \mathbb{Z}$ and $m \in M$ such that $rm \in N - \{\bar{0}\}$, implies $r \in (N : M)$ or $m \in N$. By Teorema 1, we have $(N : M) = n\mathbb{Z}$. Note that $(N:M)N = n\mathbb{Z}N = \bar{0}$. Therefore by definition, submodule N is almost prime.
Conversely, if submodule N is almost prime, then for each $r \in \mathbb{Z}$ and $m \in M$ such that $rm \in N - (N:M)N$, implies $r \in (N : M)N$ or $m \in N$. We have $(N:M)N = n\mathbb{Z}N = \bar{0} = (N:M)$. Therefore by definition, submodule N is weakly prime. □

Based on Corollary 1, we know that weakly prime submodule of $\mathbb{Z} -$module $\mathbb{Z}_n[i]$ only consist of the prime submodule and zero submodules. Then by Theorem 8, we know that cyclic weakly prime submodule and cyclic almost prime submodule on $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ are equivalent. Therefore we have Corollary 2.

Corollary 2. Let $M = \mathbb{Z}_n[i]$ be a 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. Then the only almost prime cyclic submodule that is not prime is zero.

CONCLUSIONS

This study delivers some characteristics of cyclic prime, weakly prime, and almost prime submodule of $\mathbb{Z}-$ module $\mathbb{Z}_n[i]$ that given as follows:

1. Cyclic submodule N is a prime submodule on $\mathbb{Z}-$ module $\mathbb{Z}_n[i]$ if n prime number.
2. Weakly prime submodule on $\mathbb{Z}-$ module $\mathbb{Z}_n[i]$ only consist of a prime submodule and zero submodules.
3. Cyclic almost prime submodule on $\mathbb{Z}-$ module $\mathbb{Z}_n[i]$ equivalent with a cyclic weakly prime submodule.

REFERENCES

1. J. Dauns, *Prime Submodules*, J. Rine Angew Math **298,** pp. 156-181 (1978).
2. M. A. Hadi, *On Weakly Prime Submodules*, Ibn Al-Haitham Journal for Pure and Applied Science **22,** pp. 183-190 (2009).
3. H. A. Khashan, *On Almost Prime Submodules*, Acta Mathematica Scientia **32**, pp. 645-651 (2012).
4. F. Maulana, I. G. A. W. Wardhana, N. W. Switrayni, Q. Aini, *Bilangan Prima dan Bilangan Tak Tereduksi pada Bilangan Bulat Gauss*, APPPI II Conference Proceeding (2019).
5. I. G. A. W. Wardhana, P. Astuti, *Karakteristik Submodul Prima Lemah dan Hampir Prima dari* $\mathbb{Z}-$*modul* $\mathbb{Z}_n$, Jurnal Matematika & Sains **19,** pp. 16-20 (2014).
6. S. Roman, *Advanced Linear Algebra 3rd ed*, New York: Springer (2008).
7. I. G. A. W. Wardhana, P. Astuti, I. Muchtadi-Alamsyah, *On Almost Prime Submodule of A Finitely Generated Module Over Principal Ideal Domain*, JP Journal of Algebra, Number Theory and Applications, pp. 121-128 (2016).