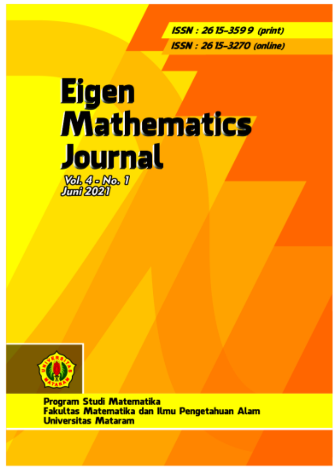
B33

by Adhitya Wisnu

Eigen Mathematics Journal



Eigen Mathematics Journal publishes articles which contribute to new information or knowledge related to:

- **Mathematical Analysis**,
- **Algebra**,
- **Applied Mathematics**,
- **Statistics**, and
- **Computational Mathematics**.

Moreover, this journal also publishes surveys in the aforementioned areas in order to introduce recent development and to stimulate further research. All articles published in this journal are available for **FREE**.

Do you want to submit an article?

Register Login Template

Announcements

Eigen Mathematics Journal

Vol. 5 No. 1 Juni 2022

Published: 2022-06-21

DOI: *https://doi.org/10.29303/emj.v5i1*

Articles

PDF

Classification of Poverty Status using the Random Forest Algorithm

Syaidatussalihah, Abdurahim

37-44

PDF

Eigen Mathematics Journal

Volume 5 No 1 Juni (2022)

e-ISSN: **2615-3270**

p-ISSN: **2615-3599**

Eigen Mathematics Journal

Homepage jurnal: http://eigen.unram.ac.id

The Prime Submodule Of The Integer Module Over Itself

***Muhammad Rijal Alfian** [a]**, Fariz Maulana** [b]**, Ni Wayan Switrayni** [c]**, Qurratul Aini** [d]**, Dwi Noorma Putri** [e] **I Gede Adhitya Wisnu Wardhana** [f*]*

[a] Program Studi Matematika FMIPA Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia. Email: rijal_alfian@unram.ac.id

[b]Department of Mathematics Institut Teknologi Bandung, Jl. Ganesha 10, Bandung 40132, Indonesia. Email: 20120008@mahasiswa.itb.ac.id

[c] Program Studi Matematika FMIPA Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia.. Email: niwayan.switrayni@unram.ac.id

[d] Program Studi Matematika FMIPA Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia. Email: qurratulaini.ami@unram.ac.id

[e] Fakultas Pertanian Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia. Email: dwinoormaputri@unram.ac.id

[f*] Program Studi Matematika FMIPA Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia.. Email: adhitya.wardhana@unram.ac.id

A B S T R A C T

One of the sciences used in digital security systems is cryptography. Cryptography is closely related to the integer system, especially prime numbers. Prime numbers themselves have been abstracted a lot. One form of abstraction of prime numbers is the prime ideal. Previous studies have proven that an Ideal I is said to be a prime ideal on $\mathbb{Z}$ if and only if I is constructed by a prime element. Other studies have also shown how the prime ideal develops. One of them is the research result of Dauns, where the prime ideal form is developed in the form of a prime submodule. A prime submodule is one of the objects in the module, which is an abstraction of prime numbers. Based on these things, it is exciting if the properties of the prime submodule are applied to other module forms, one of which is the integer module.

Keywords: Ideal, Prime Submodule, Integer Module.

Diserahkan: 23-05-2022; Diterima: 30-06-2022; Doi: https://doi.org/10.29303/emj.v5i1.132

* Corresponding author.
Alamat e-mail: *adhitya.wardhana@unrama.c.id*

Volume 5 No 1 Juni (2022)

e-ISSN: 2615-3270

p-ISSN: 2615-3599

Eigen Mathematics Journal

Homepage jurnal: http://eigen.unram.ac.id

1. Pendahuluan

Kriptografi adalah salah satu cabang ilmu matematika yang digunakan pada sistem keamanan digital. Kriptografi berkaitan dengan bilangan bulat dan sifat-sifatnya, khususnya bilangan prima. Beberapa algoritma penting seperti RSA (Rivest-Shamir-Adleman), sangat erat kaitannya dengan faktorisasi prima. Bilangan prima pertama kali diabstraksikan oleh Dedekind, menjadi ideal prima. Ideal I merupakan ideal prima dari $\mathbb{Z}$ jika dan hanya jika I dibangun oleh suatu unsur prima (Maulana dkk, 2019).

Teori modul adalah salah satu topik dalam aljabar yang membahas perumumam dari ruang vektor dimana skalar dari ruang vektor diperlemah dari suatu lapangan menjadi suatu gelanggang (Wardhana & Maulana, 2021). Salah satu objek dalam modul yang sangat menarik untuk ditelaah adalah submodul prima, yang merupakan bentuk abstrak dari bilangan prima. Bilangan prima merupakan dasar yang sangat penting pada ilmu kriptografi maupun teori koding (Maulana dkk., 2018).

Submodul prima diperkenalkan oleh Dauns yang merupakan perumuman dari ideal prima. Beberapa penelitian terkait submodul prima yang telah dikerjakan, antara lain pada modul bilangan bulat modulo (Wardhana & Astuti, 2014), modul siklik (Juliana dkk., 2020), modul CSM (Wardhana dkk., 2021) dan modul bebas (Wardhana dkk., 2016).

Pada artikel ini akan membahas sifat-sifat submodul prima pada modul bilangan bulat yang mana pembahasan sebelumnya berkisar pada karakteristik submodul hamper prima pada modul bilangan bulat modulo (Wardhana & Astuti, 2014). Pada artikel ini, gelanggang R senantiasa suatu gelanggang komutatif dengan unsur kesatuan.

2. Hasil dan Pembahasan

Dalam matematika, modul adalah perumuman dari ruang vektor dengan definisi

Seperti halnya ruang vektor, modul juga memiliki sub-struktur yang dinamakan submodul, yakni subhimpunan tak hampa dari suatu modul yang membentuk modul dengan skalar dan operasi yang sama dengan modulnya. Layaknya ruang vektor, submodul ini memiliki ekivalensi definisi sebagai berikut

Definisi 1 Misalkan M suatu modul atas gelanggang R. Subhimpunan tak hampa $S \subseteq M$ dikatakan submodul M apabila memenuhi

1. Untuk setiap $x, y \in S$, berlaku $x + y \in S$
2. Untuk setiap $x \in S, \alpha \in R$, berlaku $\alpha x \in S$

Terdapat beberapa jenis submodul, diantaranya adalah submodul minimal, submodul siklik, submodul prima, dan submodul hampir prima (Juliana dkk., 2021). Dalam artikel ini pembahasan akan difokuskan pada submodul hampir prima yang didefinisikan

Definisi 2 (Wardhana dkk., 2016) Misalkan M suatu modul atas gelanggang R. Submodul N dari M dikatakan submodul prima apabila untuk setiap $x \in M$ dan untuk setiap $\alpha \in R$ dengan $\alpha x \in P$ berakibat $\alpha \in \{r \in R | rM \subseteq N\}$ atau $x \in N$.

Himpunan $\{r \in R | rM \subseteq N\}$ merupakan ideal dari R dan dinotasikan dengan $(N: M) = \{r \in R | rM \subseteq N\}$. Sebagai contoh untuk $\mathbb{Z}$ −modul $\mathbb{Z}$, submodul $N = \langle 2 \rangle = \{2r | r \in \mathbb{Z}\}$ adalah submodul prima dengan $(N: M) = \langle 2 \rangle$.

Apabila R adalah suatu gelanggang, maka R juga merupakan suatu modul atas dirinya sendiri, atau R suatu R −modul.

* Corresponding author.

Alamat e-mail: *adhitya.wardhana@unrama.c.id*

Teorema 1 (Facchini, 1998) Misalkan R suatu gelanggang, maka didapatkan R suatu R −modul.

Bukti: Karena R suatu gelanggang, maka $(R, +)$ suatu grup komutatif. Sifat-sifat pada Definisi 1 otomatis terpenuhi karena skalar adalah gelanggang R itu sendiri ∎.

Pada artikel ini, untuk selanjutnya pembahasan akan dibatasi pada modul $\mathbb{Z}$ atas dirinya sendiri. Pertama-tama akan ditunjukkan bahwa setiap submodul dari $\mathbb{Z}$ dibangun oleh satu unsur.

Teorema 2 (Facchini, 1998) Misalkan $\mathbb{Z}$ suatu $\mathbb{Z}$ −modul. Jika N suatu submodul dari $\mathbb{Z}$ maka $N = \langle a \rangle$, untuk suatu $a \in \mathbb{Z}$.

Bukti: Misalkan diberikan N submodul dari $\mathbb{Z}$, Jika $N = \{0\}$ maka pilih $a = 0$. Asumsikan N bukan submodul nol, bentuk X subhimpunan dari N, dengan $X = \{r \in N | r > 0\}$. Himpunan X tak hampa karena N adalah submodul tak nol, yang mana punya unsur tak nol $x \in N$. Jika $x > 0$ maka $x \in X$ dan jika $x < 0$ maka $(-1)x = -x \in X$.

Jelas X adalah subhimpunan dari bilangan asli, akibatnya X punya unsur terkecil, namakan a, akan ditunjukkan setiap unsur di N merupakan kelipatan dari a. Apabila $r \in N$ sebarang, maka didapatkan $r = pa + q$ untuk suatu $p, q \in \mathbb{N}$ dengan $0 \leq q < a$. Andaikan $q \neq 0$ maka didapatkan $q = r - pa \in X$, hal ini kontradiksi dengan a adalah unsur terkecil dari X. Jadi haruslah $q = 0$, sehingga $r = pa \in \langle a \rangle$. Karena r diambil sebarang, maka $N = \langle a \rangle$∎.

Untuk memahami suatu submodul prima N, terlebih dahulu akan dicari karakteristik dari himpunan $(N: M)$. Sifat berikut menyatakan struktur dari $(N: M)$.

Teorema 3 (Facchini, 1998) Misalkan N suatu submodul dari modul M atas gelanggang R. Himpunan $(N: M)$ adalah ideal dari R.

Bukti: Jelas $0 \in R$, akibatnya diperoleh $(N: M) \neq \emptyset$. Misalkan $x \in (N: M)$ dan $r \in R$ sebarang, sehingga $xM \subset N$. Akibatnya $xrM = rxM \subset rN \subset N$. Diperoleh $xr \in (N: M)$ dan $rx \in (N: M)$. Jadi $(N: M)$ adalah suatu ideal ∎.

Catat bahwa sifat pada Teorema 3 di atas berlaku secara umum untuk M suatu modul atas gelanggang komutatif R.

Untuk lebih jelasnya, berikut diberikan contoh.

Contoh 1 Himpunan $\langle \bar{2} \rangle$ merupakan submodul dari modul $\mathbb{Z}_6$ atas $\mathbb{Z}$. Diperoleh $(\langle \bar{2} \rangle: \mathbb{Z}_6) = \{r \in \mathbb{Z} : r\mathbb{Z}_6 \subseteq \langle \bar{2} \rangle\} = \langle 2 \rangle$, dan $\langle 2 \rangle$ merupakan ideal dari $\mathbb{Z}$.

Berikutnya akan ditunjukkan bahwa apabila M suatu gelanggang, yang mana M suatu modul atas dirinya sendiri, maka $(N: M) = N$.

Teorema 4 Misalkan M suatu gelanggang dengan M dipandang sebagai modul atas dirinya. Jika N suatu submodul dari M, maka $(N: M) = N$ untuk setiap N submodul dari M.

Bukti: Misalkan $r \in N$, karena N suatu submodul dari M, maka N juga merupakan suatu ideal dari M. Akibatnya didapatkan $rM \subset N$, sehingga diperoleh $r \in (N: M)$. Sebaliknya apabila $r \in (N: M)$ maka $rM \subset N$, akibatnya $r1 = r \in N$. Jadi telah ditunjukkan bahwa $(N: M) = N$∎.

Contoh 2 Himpunan $\langle 5 \rangle$ merupakan submodul dari modul $\mathbb{Z}$ atas $\mathbb{Z}$. Diperoleh $(\langle 5 \rangle: \mathbb{Z}) = \{r \in \mathbb{Z} : r\mathbb{Z} \subseteq \langle 5 \rangle\} = \langle 5 \rangle$.

Seperti halnya Teorema 3, Teorema 4 di atas juga berlaku secara umum. Kemudian berdasarkan Teorema 2, Teorema 3 dan Teorema 4 diperoleh sifat berikut.

Akibat 5 Misalkan N submodul dari $\mathbb{Z}$ modul atas $\mathbb{Z}$. Jika $N = \langle a \rangle$ suatu submodul dari $\mathbb{Z}$ maka $(N: \mathbb{Z}) = \langle a \rangle$.

Berdasarkan hasil-hasil yang diperoleh di atas, maka didapatkan suatu karakterisasi submodul prima.

Teorema 6 Misalkan N submodul dari modul $\mathbb{Z}$ atas gelanggang $\mathbb{Z}$. Submodul N adalah submodul prima jika dan hanya jika $N = \langle p \rangle$ untuk suatu p bilangan prima.

Bukti: Misalkan $N = \langle p \rangle$ untuk suatu p bilangan prima, menurut Akibat 5 diperoleh $(N: \mathbb{Z}) = \langle p \rangle$. Misalkan $rm \in N = \langle p \rangle$, ini berakibat $p | rm$. Karena p bilangan prima, maka diperoleh $p | r$ atau $p | m$. Dengan kata lain $r \in (N: \mathbb{Z})$ atau $m \in N$, sehingga N suatu submodul prima.

Sebagai contoh, $N = \langle 2 \rangle$ adalah submodul prima dari modul $\mathbb{Z}$. Berdasarkan Akibat 5 diperoleh $(N: M) =$

$\langle 2\rangle$, dan untuk $rm \in N$ diperoleh $2|rn$. Ini berakibat $2|r$ atau $2|m$, dengan perkataan lain $r \in \langle 2\rangle = (N:M)$ atau $m \in \langle 2\rangle$, sehingga N adalah submodul prima.

Sebaliknya, misalkan N suatu submodul prima, menurut Teorema 2 didapatkan $N = \langle q\rangle$ untuk suatu $q \in \mathbb{Z}$. Akan ditunjukkan q suatu bilangan prima. Misalkan $q|ab$, akibatnya $ab \in N$, karena N submodul prima maka $a \in (N:M)$ atau $b \in N$. Akibatnya $a \in \langle q\rangle$ atau $b \in \langle q\rangle$, dengan kata lain $q|a$ atau $q|b$, sehingga q adalah suatu bilangan prima ■.

3. Kesimpulan

Berdasarkan hasil pembahasan pada bagian sebelumnya, diperoleh sifat bahwa sebarang submodul N dari modul $\mathbb{Z}$ atas $\mathbb{Z}$ merupakan submodul prima jika dan hanya N dibangun oleh suatu bilangan prima.

DAFTAR PUSTAKA

Facchini, A. (1998). *Module Theory: Endomorphism Rings and Direct Sum Decompositions in Some Classes of Modules* (1st ed., Vol. 1). Birkhauser.

Juliana, R., Wardhana, I. G. A. W., & Irwansyah. (2021). Some Characteristics of Cyclic Prime, Weakly Prime and Almost Prime Submodule of Gaussian Integer Modulo over Integer. *AIP Conference Proceedings*, *2329*(February). https://doi.org/10.1063/5.0042586

Juliana, R., Wardhana, I. G. W. W., & Irwansyah, I. (2020). Some Characteristics of Prime Submodules of Gaussian Integer Modulo over Integer. *Proceeding International Conference on Science (ICST)*, 209–213.

Maulana, F., Wardhana, I. G. A. W., & Switrayni, N. W. (2019). Ekivalensi Ideal Hampir Prima dan Ideal Prima pada Bilangan Bulat Gauss. *EIGEN MATHEMATICS JOURNAL*, *1*(1), 1. https://doi.org/10.29303/emj.v1i1.29

Maulana, F., Wardhana, I. G. A. W., Switrayni, N. W., & Aini, Q. (2018). Bilangan Prima dan Bilangan tak Tereduksi pada Bilangan bulat Gauss. *Prosiding Seminar Nasional APPPI II*, 383–387.

Wardhana, I. G. A. W., & Astuti, P. (2014). Karakteristik Submodul Prima Lemah dan Submodul Hampir Prima pada Z-Modul Zn. *Jurnal Matematika & Sains*, *19*(1), 16–20.

Wardhana, I. G. A. W., Astuti, P., & Muchtadi-Alamsyah, I. (2016). On almost prime submodules of a module over a principal ideal domain. *JP Journal of Algebra, Number Theory and Applications*, *38*(2), 121–128. https://doi.org/10.17654/NT038020121

Wardhana, I. G. A. W., & Maulana, F. (2021). *Sebuah Karakteristik dari Modul Uniserial dan Gelanggang Uniserial*. *7*, 9–17.

Wardhana, I. G. A. W., Nghiem, N. D. H., Switrayni, N. W., & Aini, Q. (2021). A note on almost prime submodule of CSM module over principal ideal domain. *Journal of Physics: Conference Series*, *2106*(1), 012011. https://doi.org/10.1088/1742-6596/2106/1/012011

B33

ORIGINALITY REPORT

11%	11%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	123dok.com Internet Source	8%
2	journalseeker.researchbib.com Internet Source	3%

Exclude quotes	On	Exclude matches	< 3%
Exclude bibliography	On		