J. Ris. & Ap. Mat. Vol. 08 No. 02 (2024) pp. 136-141
Jurnal Riset dan Aplikasi Matematika
e-ISSN: 2581-0154
URL: journal.unesa.ac.id/index.php/jram

SUBMODUL PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA DARI MODUL MATRIKS BILANGAN BULAT MODULO

I GEDE ADHITYA WISNU WARDHANA[1], ABDURAHIM[2,] *

[1,2] Program Studi Matematika, Fakultas MIPA, Universitas Mataram, Jl Majapahit no 62, Mataram, Indonesia ,

*abdurahim@staff.unram.ac.id

ABSTRAK

Bilangan prima berperan kunci dalam keamanan digital dan kriptografi, terutama dalam algoritma seperti RSA yang bergantung pada faktor bilangan prima besar untuk kunci enkripsi. Tantangan utama yang dihadapi adalah kemampuan komputer kuantum untuk mengancam keamanan dengan mempercepat faktorisasi bilangan prima besar. Oleh karena itu, diperlukan perkembangan sistem kriptografi post-kuantum yang tidak bergantung pada faktorisasi bilangan prima, untuk menjaga keamanan data di era komputasi kuantum. Submodul prima, prima lemah, dan hampir prima adalah konsep-konsep yang merupakan abstraksi bilangan prima, diharapkan abstraksi ini dapat menjadi alternatif baru dalam sistem keamanan. Pada artikel ini diberikan karakteristik dari submodul prima, submodul prima lemah dan submodul hampir prima pada modul matriks bilangan bulat modulo atas gelanggnag bilangan bulat, salah satu hasilnya adalah dekomposisi modul menjadi submodul-submodul siklik yang dapat dipandang sebagai abstraksi Teorema Fundamental Aritmatika dari bilangan bulat.
Kata Kunci: submodul prima, submodul prima lemah, submodul hampir prima

ABSTRACT

Prime numbers play a pivotal role in digital security and cryptography, especially in algorithms like RSA that rely on large prime numbers for encryption keys. The primary challenge lies in the ability of quantum computers to threaten security by accelerating the factorization of large prime numbers. Therefore, the development of post-quantum cryptographic systems that do not rely on prime factorization is essential to maintain data security in the era of quantum computing. Concepts such as submodules of primes, weak primes, and nearly primes serve as abstractions of prime numbers, offering potential alternatives in security systems. This article explores the characteristics of submodules of primes, weak primes, and nearly primes within the module of integer matrices modulo a given integer ring, with one of the results being the decomposition of the module into cyclic submodules, which can be viewed as an abstraction of the Fundamental Theorem of Arithmetic for integers.
Keywords: *prime submodule, weakly prime submodule, almost prime submodule*

1 Pendahuluan

Bilangan prima memainkan peran sentral dalam keamanan digital dan kriptografi modern. Mereka digunakan sebagai dasar untuk algoritma seperti RSA, di mana bilangan prima besar digunakan untuk membuat kunci yang mengamankan data dengan cara yang sangat sulit untuk

2010 *Mathematics Subject Classification*: 16P70
Tanggal Masuk: 05-10-24; diterima: 27-10-24

dipecahkan oleh pihak yang tidak berwenang. Kesulitan faktorisasi bilangan prima besar menjadi faktor-faktor prima yang lebih kecil membentuk dasar keamanan yang kuat dalam sistem-sistem ini, memastikan kerahasiaan dan integritas data dalam komunikasi dan penyimpanan digital [1].

Tantangan utama komputer kuantum dalam kriptografi bilangan prima adalah kemampuannya untuk secara drastis mempercepat proses faktorisasi bilangan besar, mengancam keamanan sistem kriptografi seperti RSA yang bergantung pada faktorisasi. Dalam menghadapinya, diperlukan pengembangan sistem kriptografi post-kuantum yang tidak terpengaruh oleh komputer kuantum, menggunakan masalah matematis yang sulit dipecahkan oleh komputer kuantum sebagai dasar keamanan, sehingga memastikan keamanan data dalam era komputasi kuantum [2].

Salah satu sifat fundamental dari bilangan bulat adalah, setiap bilangan bulat dapat ditulis dalam perkalian bilangan prima secara unik, hal ini lebih dikenal sebagai Teorema Fundamental Aritmetika (TFA). Dalam teori modul, mendapatkan sifat fundamental seperti TFA adalah tantangan besar. Salah satu usaha untuk mendapatkan sifat ini adalah mengkonstruksi dekomposisi modul, salah satunya adalah dekomposisi siklik [3]. Oleh karena itu pada studi ini diberikan dekomposisi siklik dari submodul prima, submodul prima lemah, dan submodul hampir prima dalam modul matriks bilangan bulat modulo berukuran 2×2 atas gelanggang bilangan bulat.

2 Hasil

Submodul prima, submodul prima lemah dan submodul hampir prima didefinisikan sebagai berikut

Definisi 1 [4] Misalkan N submodul sejati dari R-modul M dan $(N:M) = \{r \in R | rM \subseteq N\}$.

1. Submodul N disebut submodul prima jika untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N$ berakibat $r \in (N:M)$ atau $m \in N$.
2. Submodul N disebut submodul prima lemah jika untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N - \{0\}$ berakibat $r \in (N:M)$ atau $m \in N$.
3. Submodul N disebut submodul hampir prima jika untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N - (N:M)N$ berakibat $r \in (N:M)$ atau $m \in N$.

Dari definisi diatas mudah dilihat bahwa submodul prima pasti merupakan submodul prima lemah, dan submodul prima lemah pasti merupakan submodul hampir prima. Akan tetapi tidak berlaku sebaliknya. Dalam $\mathbb{Z}$-modul $\mathbb{Z}_{12}$, submodul $\langle \bar{4} \rangle$ adalah submodul hampir prima tetapi bukan submodul prima lemah, dan $\{\bar{0}\}$ adalah contoh submodul prima lemah tapi bukan submodul prima. Notasi $(N:M)$ dinamakan fraksi submodul N dari modul M.

Sebelumnya karakteristasi submodul prima, submodul prima lemah dan hampir prima dari $\mathbb{Z}$-modul $M_{2x2}(\mathbb{Z}_9)$ telah didapatkan dengan melakukan dekomposisi siklik modulnya terlebih dahulu [5]. Metode yang sama dilakukan pada studi ini. Karakterisasi diberikan dalam dua kasus, kasus pertama saat order modul adalah perpangkatan prima, dan kasus kedua saat ordernya bukan perpangkatan prima.

Modul $M_{2x2}(\mathbb{Z}_n)$ dapat didekomposisi menjadi submodul-submodul siklik. Dekomposisi siklik modul $M_{2x2}(\mathbb{Z}_n)$ adalah $\bigoplus_{i=1}^{2}\bigoplus_{j=1}^{2} \langle E_{ij} \rangle$ dengan E_{ij} adalah matriks unit, yakni matriks dengan $\bar{1}$ sebagai elemen pada baris ke-i dan kolom ke-j, dan $\bar{0}$ untuk elemen lainnya.

Teorema 1 Jika modul $M_{2x2}(\mathbb{Z}_n)$ memiliki dekomposisi siklik $\langle E_{11} \rangle \oplus \langle E_{12} \rangle \oplus \langle E_{21} \rangle \oplus \langle E_{22} \rangle$, maka $\langle E_{ij} \rangle \approx \mathbb{Z}_n$ untuk semua $i, j \in \{1,2\}$.

Bukti: Misalkan $M_{2x2}(\mathbb{Z}_n) = \bigoplus_{i=1}^{2}\bigoplus_{j=1}^{2}\langle E_{ij}\rangle$. Ambil $i,j \in \{1,2\}$ sebarang. Tanpa mengurangi perumuman, misalkan $i = 1, j = 1$. Buat pengaitan $\partial: \langle E_{11}\rangle \to \mathbb{Z}_n$ dengan $\partial\left(\begin{bmatrix}\bar{k} & 0\\ 0 & 0\end{bmatrix}\right) = \bar{k}$, dengan $\bar{k} \in \mathbb{Z}_n$. Apabila $\begin{bmatrix}\overline{k_1} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}, \begin{bmatrix}\overline{k_2} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix} \in \langle E_{11}\rangle$ dengan $\begin{bmatrix}\overline{k_1} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix} = \begin{bmatrix}\overline{k_2} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}$, kita peroleh $\overline{k_1} = \overline{k_2}$. Akibatnya $\partial\left(\begin{bmatrix}\overline{k_1} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}\right) = \partial\left(\begin{bmatrix}\overline{k_2} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}\right)$, sehingga ∂ adalah suatu pemetaan. Kemudian apabila $\bar{x} \in \mathbb{Z}_n$, mudah dilihat bahwa $\partial\left(\begin{bmatrix}\bar{x} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}\right) = \bar{x}$, akibatnya ∂ suatu pemetaan yang bersifat pada. Terakhir, jika diberikan $\begin{bmatrix}\bar{x} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}, \begin{bmatrix}\bar{y} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix} \in \langle E_{11}\rangle$ dengan $\partial\left(\begin{bmatrix}\bar{x} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}\right) = \partial\left(\begin{bmatrix}\bar{y} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}\right)$, diperoleh $\bar{x} = \bar{y}$. Akibatnya $\begin{bmatrix}\bar{x} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix} = \begin{bmatrix}\bar{y} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}$, sehingga ∂ suatu pemetaan yang bersifat satu-satu. Jadi ∂ suatu isomorfisme, akibatnya $\langle E_{ij}\rangle \approx \mathbb{Z}_n$. ■

Berdasarkan Teorema 1, karakterisasi submodul prima, submodul prima lemah dan submodul hampir prima dari $M_{2x2}(\mathbb{Z}_n)$ cukup diperoleh dari karakterisasi tiap suku-suku langsungnya. Teorema 1 mengakibatkan:

Akibat 1 $M_{2x2}(\mathbb{Z}_n) \approx \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Karakterisasi dari submodul prima, submodul prima lemah dan submodul hampir prima dari $\mathbb{Z}$-modul $\mathbb{Z}_n$ diberikan pada Teorema 2.

Teorema 2 [6] Misalkan N submodul dari $\mathbb{Z}$-modul $\mathbb{Z}_n$ dan $n = p_1^{k_1}.p_2^{k_2}...p_m^{k_m}$ dengan p_i bilangan prima berbeda dan $k_i \in \mathbb{N}$.

1. Submodul tak nol N adalah submodul prima jika dan hanya jika $N =< \overline{p_i} >$ untuk suatu $i \in \{1,2,...,m\}$.
2. Submodul N adalah submodul prima lemah jika dan hanya jika $N =< \overline{p_i} >$ untuk suatu $i \in \{1,2,...,m\}$ atau $N = \{\bar{0}\}$.
3. Submodul N adalah submodul hampir prima $\mathbb{Z}_n$ jika dan hanya jika $N = \{\bar{0}\}$ atau $N =< \overline{p_i} >$ untuk suatu $i \in \{1,2,...,m\}$ atau $N =< \overline{p_i^{k_i}} >$ untuk $i \in \{1,2,...,m\}$.

Bukti: Cek [6] ■

Untuk memanfaatkan Teorema 2 pada artikel ini, akan digunakan sifat yang telah diperoleh pada artikel sebelumnya [7].

Teorema 3 [7] Misalkan diberikan $\mathbb{Z}$-modul M dengan S adalah submodulnya. Apabila

$$M = M_1 \oplus M_2 \oplus ... \oplus M_n$$

dan

$$S = S_1 \oplus S_2 \oplus ... S_n$$

dengan $S_i \subseteq M_i$ untuk $i = 1,2,...,n$, maka

$$(S: M) = \bigcap_{i=1}^{n}(S_i: M_i).$$

Bukti: Lihat [7]. ■

Teorema 3 mengatakan bahwa fraksi submodul dari suatu modul sama dengan irisan semua fraksi suku langsung dari dekomposisinya.

Apabila K, L adalah submodul dari $\mathbb{Z}$-modul M dengan $M = K \oplus L$. Apabila K_S dan L_S berturut-turut adalah submodul hampir prima dari K dan L, submodul $K_S \oplus L_s$ belum tentu merupakan submodul hampir prima. Sebagai contoh, pada $\mathbb{Z}$-modul $M = \mathbb{Z}_6 \oplus \mathbb{Z}_4$, $\langle\bar{3}\rangle$ dan $\langle\bar{2}\rangle$ berturut-turut adalah submodul hampir prima dari $\mathbb{Z}_6$ dan $\mathbb{Z}_4$ dan $(\langle\bar{3}\rangle \oplus \langle\bar{2}\rangle : M) = 6\mathbb{Z}$. Dengan memilih $r = 3 \notin 6\mathbb{Z}$ dan $m = \bar{1} \oplus \bar{2} \notin \langle\bar{3}\rangle \oplus \langle\bar{2}\rangle$ diperoleh $rm \in \langle\bar{3}\rangle \oplus \langle\bar{2}\rangle - (\langle\bar{3}\rangle \oplus \langle\bar{2}\rangle : M)(\langle\bar{3}\rangle \oplus \langle\bar{2}\rangle)$ yang menunjukkan $\langle\bar{3}\rangle \oplus \langle\bar{2}\rangle$ bukan submodul hampir prima.

Submodul $K_S \oplus L_s$ pada contoh sebelumnya merupakan submodul hampir prima apabila memenuhi suatu kondisi berikut.

Teorema 4 [8] Misalkan K, L submodul hampir prima dari $\mathbb{Z}$-modul M dengan $M = K \oplus L$. Misalkan K_S dan L_S berturut-turut adalah submodul hampir prima tak nol dari K dan L. Maka $K_S \oplus L_s$ adalah submodul hampir prima jika dan hanya jika $(K_S : M) = (L_s : \mathrm{M})$.
Bukti: Lihat [8]. ■

Berdasarkan Teorema 4 diperoleh karakterisasi submodul hampir prima sebagai berikut pada Teorema 5.

Teorema 5 Misalkan $M_{2x2}(\mathbb{Z}_n) = \langle E_{11}\rangle \oplus \langle E_{12}\rangle \oplus \langle E_{21}\rangle \oplus \langle E_{22}\rangle$ dengan E_{ij} adalah matriks unit. Submodul N dari $M_{2x2}(\mathbb{Z}_n)$ adalah submodul hampir prima jika dan hanya jika submodul N berbentuk

1. $N = N_{kl} \oplus (\bigoplus_{i=1,i\neq k}^{2} \bigoplus_{j=1,j\neq l}^{2} N_{ij})$ dengan N_{kl} adalah submodul hampir prima dari $\langle E_{kl}\rangle$ dan $N_{ij} = \{\bar{0}\}$ atau $N_{ij} = \langle E_{ij}\rangle$.
2. $N = N_{kl} \oplus N_{cd} \oplus (\bigoplus_{i=1,i\neq k,c}^{2} \bigoplus_{j=1,j\neq l,d}^{2} N_{ij})$ atau $N = N_{kl} \oplus N_{cd} \oplus N_{ef} \oplus (\bigoplus_{i=1,i\neq k,c,e}^{2} \bigoplus_{j=1,j\neq l,d,f}^{2} N_{ij})$ dengan N_{kl},N_{cd} dan N_{ef} adalah submodul hampir prima dari $\langle E_{kl}\rangle$,$\langle E_{cd}\rangle$ dan $\langle E_{ef}\rangle$, dan untuk lainnya, $N_{ij} = \{\bar{0}\}$ atau $N_{ij} = \langle E_{ij}\rangle$, dengan $(N_{kl} : \langle E_{kl}\rangle) = (N_{cd} : \langle E_{cd}\rangle) = (N_{ef} : \langle E_{ef}\rangle)$.

Bukti: Bukti bagian (1) akan dibagi menjadi dua kasus, yang mana kasus pertama apabila N_{ij} bukan submodul nol semua, dan kasus kedua dimana salah satu N_{ij} merupakan submodul nol.

- Misalkan $N = N_{kl} \oplus (\bigoplus_{i=1,i\neq k}^{2} \bigoplus_{j=1,j\neq l}^{2} \langle E_{ij}\rangle)$ dengan N_{kl} adalah submodul hampir prima dari $\langle E_{ij}\rangle$, maka berdasarkan Teorema 3 didapatkan $(N : M) = \bigcap_{i,j=1}^{2}(N_{ij} : \langle E_{ij}\rangle)$. Karena untuk semua $i \neq k$ dan $k \neq l$ didapatkan $(\langle N_{ij}\rangle : \langle E_{ij}\rangle) = \mathbb{Z}$, akibatnya $(N : M) = (N_{kl} : \langle E_{kl}\rangle)$. Misalkan $r \in \mathbb{Z}$ dan $m = m_{11} + m_{12} + m_{21} + m_{22} \in M_{2x2}(\mathbb{Z}_n)$ sebarang dengan $rm \in N - (N : M)N = N - (N_{kl} : \langle E_{kl}\rangle)N$, dengan $m_{ij} \in \langle E_{ij}\rangle$. Akibatnya $rm = r(m_{11} + m_{12} + m_{21} + m_{22}) = rm_{11} + rm_{12} + rm_{21} + rm_{22} \in N - (N_{kl} : \langle E_{kl}\rangle)N$, sehingga diperoleh $rm_{ij} \in N_{ij} - (N_{kl} : \langle E_{ij}\rangle)N_{ij}$ untuk semua $i, j \in \{1,2\}$. Secara khusus $rm_{kl} \in N_{kl} - (N_{kl} : \langle E_{kl}\rangle)N_{kl}$, karena N_{kl} submodul hampir prima, didapatkan $r \in (N_{kl} : \langle E_{kl}\rangle) = (N : M)$ atau $m_{kl} \in N_{kl}$. Karena $m = m_{11} + m_{12} + m_{21} + m_{22}$, dengan $N_{ij} = \{\bar{0}\}$ atau $N_{ij} = \langle E_{ij}\rangle$ untuk $i \neq k$ dan $j \neq l$, diperoleh $m_{kl} \in N_{kl}$ mengakibatkan $m \in N$. Sehingga dapat dismpulkan $r \in (N : M)$ atau $m \in N$, sehingga N adalah submodul hampir prima.
- Misalkan $N_{kl} \oplus (\bigoplus_{i=1,i\neq k}^{2} \bigoplus_{j=1,j\neq l}^{2} \langle N_{ij}\rangle)$ dengan N_{kl} adalah submodul hampir prima dari $\langle E_{ij}\rangle$ dan salah satu $N_{ij} = \{\bar{0}\}$. Berdasarkan Teorema 3 didapatkan $(N : M) = \bigcap_{i,j=1}^{2}(N_{ij} : \langle E_{ij}\rangle)$, karena untuk $N_{ij} = \{\bar{0}\}$ didapatkan $(\langle N_{ij}\rangle : \langle E_{ij}\rangle) = \{0\}$, akibatnya $(N : M) = \bigcap_{i,j=1}^{2}(N_{ij} : \langle E_{ij}\rangle) = \{0\}$. Misalkan $r \in \mathbb{Z}$ dan $m = m_{11} + m_{12} + m_{21} +$

$m_{22} \in \mathrm{M}_{2x2}(\mathbb{Z}_n)$ sebarang dengan $rm \in N - (N:M)N = N - \{\bar{0}\}$, dengan $m_{ij} \in \langle E_{ij} \rangle$. Dengan cara yang sama seperti kasus pertama, didapatkan $rm_{kl} \in N_{kl} - \{\bar{0}\}$. Karena N_{kl} submodul hampir prima, maka $r \in \{\bar{0}\} = (N:M)$ atau $m_{kl} \in N_{kl}$. Akibatnya $r \in (N:M)$ atau $m \in N$, sehingga N adalah submodul hampir prima.

Bukti bagian (2) akan dibagi menjadi dua kasus. Kasus pertama apabila N_{ij} semuanya bukan submodul nol, dan kasus kedua apabila N_{ij} salah satunya adalah submodul nol

- Misalkan $N = N_{kl} \oplus N_{cd} \oplus (\bigoplus_{i=1,i\neq k,c}^{2} \bigoplus_{j=1,j\neq l,d}^{2} N_{ij})$ atau $N = N_{kl} \oplus N_{cd} \oplus N_{ef} \oplus (\bigoplus_{i=1,i\neq k,c,e}^{2} \bigoplus_{j=1,j\neq l,d,f}^{2} N_{ij})$ dengan N_{kl}, N_{cd} dan N_{ef} adalah submodul hampir prima dari $\langle E_{kl} \rangle, \langle E_{cd} \rangle$ dan $\langle E_{ef} \rangle$, dan $N_{ij} = \langle E_{ij} \rangle$ untuk indeks lainnya, dengan $(N_{kl}: \langle E_{kl} \rangle) = (N_{cd}: \langle E_{cd} \rangle) = \big(N_{ef}: \langle E_{ef} \rangle\big) = \langle p \rangle$. Berdasarkan Teorema 3 didapatkan $(N:M) = \langle p \rangle$. Misalkan $r \in \mathbb{Z}$ dan $m = m_{11} + m_{12} + m_{21} + m_{22} \in M_{2x2}(\mathbb{Z}_n)$ sebarang dengan $rm \in N - (N:M)N = N - \langle \bar{p} \rangle$, dimana $m_{ij} \in \langle E_{ij} \rangle$. Dengan metode serupa dengan bukti bagian pertama, didapatkan $rm_{ij} \in N_{ij} - \langle \bar{p} \rangle$ untuk $i = k, c, e$ dan $j = l, d, f$. Karena N_{ij} submodul hampir prima untuk $i = k, c, e$ dan $j = l, d, f$, maka $r \in \langle p \rangle = (N:M)$ atau $m_{ij} \in N_{ij}$ untuk $i = k, c, e$ dan $j = l, d, f$. Akibatnya $r \in (N:M)$ atau $m \in N$, sehingga N adalah submodul hampir prima.
- Misalkan $N = N_{kl} \oplus N_{cd} \oplus (\bigoplus_{i=1,i\neq k,c}^{2} \bigoplus_{j=1,j\neq l,d}^{2} N_{ij})$ atau $N = N_{kl} \oplus N_{cd} \oplus N_{ef} \oplus (\bigoplus_{i=1,i\neq k,c,e}^{2} \bigoplus_{j=1,j\neq l,d,f}^{2} N_{ij})$ dengan N_{kl}, N_{cd} dan N_{ef} adalah submodul hampir prima dari $\langle E_{kl} \rangle, \langle E_{cd} \rangle$ dan $\langle E_{ef} \rangle$, dan $N_{ij} = \langle E_{ij} \rangle$ untuk indeks lainnya, dengan $(N_{kl}: \langle E_{kl} \rangle) = (N_{cd}: \langle E_{cd} \rangle) = \big(N_{ef}: \langle E_{ef} \rangle\big) = \langle p \rangle$. Berdasarkan Teorema 3 didapatkan $(N:M) = \{0\}$ karena terdapat $N_{ij} = \{\bar{0}\}$. Misalkan $r \in \mathbb{Z}$ dan $m = m_{11} + m_{12} + m_{21} + m_{22} \in M_{2x2}(\mathbb{Z}_n)$ sebarang dengan $rm \in N - (N:M)N = N - \langle \bar{0} \rangle$, dimana $m_{ij} \in \langle E_{ij} \rangle$. Dengan metode serupa dengan bukti bagian pertama, didapatkan $rm_{ij} \in N_{ij} - \langle \bar{0} \rangle$ untuk $i = k, c, e$ dan $j = l, d, f$. Karena N_{ij} submodul hampir prima untuk $i = k, c, e$ dan $j = l, d, f$, maka $r \in \langle 0 \rangle = (N:M)$ atau $m_{ij} \in N_{ij}$ untuk $i = k, c, e$ dan $j = l, d, f$. Akibatnya $r \in (N:M)$ atau $m \in N$, sehingga N adalah submodul hampir prima.

Sebaliknya, misalkan N submodul hampir prima, dan $N \neq N_{kl} \oplus (\bigoplus_{i=1,i\neq k}^{2} \bigoplus_{j=1,j\neq l}^{2} N_{ij})$ dengan N_{kl} adalah submodul hampir prima dari $\langle E_{kl} \rangle$ dan $N_{ij} = \{\bar{0}\}$ atau $N_{ij} = \langle E_{ij} \rangle$. Akan ditunjukkan $N = N_{kl} \oplus N_{cd} \oplus (\bigoplus_{i=1,i\neq k,c}^{2} \bigoplus_{j=1,j\neq l,d}^{2} N_{ij})$ atau $N = N_{kl} \oplus N_{cd} \oplus N_{ef} \oplus (\bigoplus_{i=1,i\neq k,c,e}^{2} \bigoplus_{j=1,j\neq l,d,f}^{2} N_{ij})$ dengan N_{kl}, N_{cd} dan N_{ef} berturut-turut adalah submodul hampir prima dari $\langle E_{kl} \rangle, \langle E_{cd} \rangle$ dan $\langle E_{ef} \rangle$, dan $N_{ij} = \{\bar{0}\}$ atau $N_{ij} = \langle E_{ij} \rangle$ dengan $(N_{kl}: \langle E_{kl} \rangle) = (N_{cd}: \langle E_{cd} \rangle) = (N_{ef}: \langle E_{ef} \rangle)$. Jadi pembuktian cukup menunjukkan apabila ada lebih dari satu suku langsung yang tak trivial, maka farksi submodulnya harus sama. Karena N submodul hampir prima dari $M_{2x2}(\mathbb{Z}_n)$, didapatkan $N = N_{11} \oplus N_{12} \oplus N_{21} \oplus N_{22}$ dengan N_{ij} submodul dari $\langle E_{ij} \rangle$. Andaikan ada lebih dari 1 suku langsung N yang bukan submodul trivial, tanpa mengurangi perumuman, misalkan N_{11}dan N_{12} adalah suku langsung yang bukan submodul trivial, berdasarkan Teorema 4 maka $(N_{11}: \langle E_{11} \rangle) = (N_{12}: \langle E_{12} \rangle)$. Jadi apabila ada dua submodul tak trivial, maka fraksi submodulnya haruslah sama. ■

Daftar Pustaka

[1] N. Al-Juaid and A. Gutub, "Combining RSA and audio steganography on personal computers for enhancing security," *SN Appl Sci*, vol. 1, no. 8, pp. 1–11, Aug. 2019, doi: 10.1007/s42452-019-0875-8.

[2] T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, "Quantum Computers' threat on Current Cryptographic Measures and Possible Solutions," *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 5, pp. 10–20, Oct. 2022, doi: 10.5815/ijwmt.2022.05.02.

[3] I. G. A. W. Wardhana, "The Decomposition of a Finitely Generated Module over Some Special Ring," *JTAM (Jurnal Teori dan Aplikasi Matematika)*, vol. 6, no. 2, pp. 261–267, 2022, doi: 10.31764/jtam.v6i2.6769.

[4] H. A. Khashan, "On almost prime submodules," *Acta Mathematica Scientia*, vol. 32, no. 2, pp. 645–651, Mar. 2012, doi: 10.1016/S0252-9602(12)60045-9.

[5] I. G. A. W. Wardhana, N. W. Switrayni, and Q. Aini, "Eigen Mathematics Journal Submodul Prima Lemah dan Submodul Hampir Prima Pada Z-modul M2(Zn)," *Eigen Mathematics Journal*, vol. 1, no. 1, pp. 28–30, 2018, Accessed: Dec. 20, 2021. [Online]. Available: https://doi.org/10.29303/emj.v1i1.6

[6] I. G. A. W. Wardhana and P. Astuti, "Karakteristik Submodul Prima Lemah dan Submodul Hampir Prima pada Z-Modul Zn," *Jurnal Matematika & Sains*, vol. 19, no. 1, pp. 16–20, 2014.

[7] I. G. A. W. Wardhana, P. Astuti, and I. Muchtadi-Alamsyah, "On almost prime submodules of a module over a principal ideal domain," *JP Journal of Algebra, Number Theory and Applications*, vol. 38, no. 2, pp. 121–128, Apr. 2016, doi: 10.17654/NT038020121.

[8] I. G. A. W. Wardhana, P. Astuti, and I. Muchtadi-Alamsyah, "The Characterization of Almost Prime Submodule on the Finitely Generated Module over Principal Ideal Domain," *Journal of the Indonesian Mathematical Society*, vol. 30, no. 01, pp. 63–76, 2024.