BEBERAPA SIFAT IDEAL SIKLIK PRIMA PADA RING BILANGAN BULAT GAUSS MODULO

SKRIPSI

Oleh

WAHYU ULYAFANDHIE MISUKI
NIM : G1D 016 049
(Program Studi : Matematika)

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS MATARAM
2020

BEBERAPA SIFAT IDEAL SIKLIK PRIMA PADA RING BILANGAN BULAT GAUSS MODULO

SKRIPSI

Karya tulis sebagai salah satu syarat untuk mendapatkan gelar Sarjana dari Universitas Mataram

Oleh

WAHYU ULYAFANDHIE MISUKI
NIM : G1D 016 049
(Program Studi : Matematika)

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS MATARAM
2020

ABSTRAK

BEBERAPA SIFAT IDEAL SIKLIK PRIMA PADA RING BILANGAN BULAT GAUSS MODULO

Oleh

WAHYU ULYAFANDHIE MISUKI
NIM. G1D 016 049

Saat ini salah satu algoritma penting dalam sistem keamanan digital adalah algoritma RSA (Rivest – Shamir – Adleman) yang sangat bergantung pada faktorisasi prima dari bilangan bulat. Ancaman terhadap RSA yaitu teknologi komputer kuantum yang akan mudah memecahkan metode RSA menyebabkan keamanan dunia digital yang banyak memanfaatkan RSA menjadi tidak aman lagi. Salah satu usaha matematikawan dalam mencari alternatif untuk menciptakan teknologi keamanan baru dalam kriptografi adalah dengan mempelajari abstraksi bilangan prima. Dedekind (1871) memberikan abstraksi bilangan prima menjadi ideal prima dan ideal prima kembali diabstraksi menjadi ideal hampir prima oleh bhatwadekar (2009). Maulana (2019) menemukan sifat-sifat ideal prima dan ideal hampir prima pada ring bilangan bulat Gauss. Dalam penelitian ini telah dikaji sifat-sifat yang yang berkaitan dengan ideal siklik prima pada ring bilangan bulat Gauss modulo, diantaranya yaitu ideal tak nol $I = \langle \bar{a} \rangle$ pada $\mathbb{Z}_n[i]$ merupakan ideal prima jika $(a,n) = p$ merupakan prima Gauss.

Kata Kunci : *bilangan bulat Gauss modulo, ideal prima, prima Gauss*

ABSTRACT

SOME CHARACTERISTICS OF PRIME CYCLIC IDEAL ON MODULO GAUSSIAN INTEGER RING

By

WAHYU ULYAFANDHIE MISUKI
NIM. G1D 016 049

One of the important algorithms in digital security systems is the RSA (Rivest - Shamir - Adleman) algorithm which is very dependent on the prime factorization of integers. The threat to RSA is quantum computer technology that will easily solve the RSA method causing the security of the digital world which mostly use RSA to be no longer secure. One of the efforts of mathematicians to find alternatives to create new security technologies in cryptography is to study the abstraction of prime numbers. Dedekind (1871) provides an abstraction of prime numbers to be prime ideal and ideal prime is again abstracted into almost prime ideal by Bhatwadekar (2009). Maulana (2019) found the properties of prime ideals and almost prime ideals on Gaussian integer ring. In this research, the properties associated with the prime cyclic ideals in modulo Gaussian integer ring, including the non-zero ideal $I = \langle \bar{a} \rangle$ on $\mathbb{Z}_n[i]$ is prime ideal if $(a,n) = p$ is Gaussian prime.

Keywords : *modulo Gaussian integer, prime ideal, Gaussian prime*

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi ini murni karya saya sendiri dan di dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan disuatu perguruan tinggi serta tidak terdapat karya atau pendapat yang pernah dituliskan atau dipublikasikan oleh orang lain, kecuali yang tertulis pada situasi dalam naskah ini dan disebutkan di dalam daftar pustakanya.

Mataram, November 2020

Yang menyatakan,

WAHYU ULYAFANDHIE MISUKI

NIM. G1D 016 049

HALAMAN PERSETUJUAN

BEBERAPA SIFAT IDEAL SIKLIK PRIMA PADA RING BILANGAN BULAT GAUSS MODULO

WAHYU ULYAFANDHIE MISUKI
NIM G1D 016 049

Menyetujui

Tim Pembimbing

Tanggal : November 2020

Pembimbing I,	Pembimbing II,
Dr. I Gede Adhitya Wisnu Wardhana, M.Si.	Ni Wayan Switrayni, M.Si.
NIP. 19800429 200801 1 010	NIP. 19890517 201504 2 002

HALAMAN PENGESAHAN

Skripsi yang berjudul :

BEBERAPA SIFAT IDEAL SIKLIK PRIMA PADA RING BILANGAN BULAT GAUSS MODULO

WAHYU ULYAFANDHIE MISUKI
NIM. G1D 016 049

Telah dipertahankan di depan Tim Penguji Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Mataram

Pada tanggal : 30 November 2020

Tim Penguji :

Dr. Irwansyah, M.Si. NIP. 19890707 201504 1 004	(Ketua)	……
Qurratul Aini, M.Sc NIP. 19870830 201404 2 002	(Sekretaris)	……
Dr. I Gede Adhitya Wisnu Wardhana, M.Si. NIP. 19800429 200801 1 010	(Anggota I)	……
Ni Wayan Switrayni, M.Si. NIP. 19890517 201504 2 002	(Anggota II)	……

Mengetahui,

Dekan FMIPA Universitas Mataram,	Ketua Program Studi Matematika,
Drs. Dedy Suhendra, M.Si., Ph.D. NIP. 1971207 199603 1 002	Dr. Marwan, S.Si, M.Si. NIP. 1971005 200003 1 001

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat merampungkan skripsi dengan judul : "Beberapa Sifat Ideal Siklik Prima Pada Ring Bilangan Bulat Gauss Modulo". Skripsi ini untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar Sarjana Matematika pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.

Penghargaan dan terima kasih yang setulus-tulusnya kepada Ibunda tercinta Baiq Nuratun Aini yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil serta kepada Almarhum Ayahanda Ahmad Misuki yang telah membentuk karakter sehingga menjadi pribadi saat ini. Semoga Allah SWT selalu melimpahkan rahmat, kesehatan, karunia, dan keberkahan di dunia dan di akhirat atas budi baik yang telah diberikan kepada penulis.

Penghargan dan terima kasih juga penulis berikan kepada Bapak Dr. I Gede Adhitya Wisnu Wardhana, M.Si. selaku Pembimbing I dan Ibu Ni Wayan Switrayni, M.Si. selaku Pembimbing II atas bimbingannya selama penulisan skripsi ini. Serta ucapan terima kasih kepada :

1. Bapak Prof. Dr. Lalu Husni, SH., M.Hum., selaku Rektor Universitas Mataram, atas kesempatan yang diberikan kepada penulis untuk mengikuti dan menyelesaikan pendidikan Strata Satu (S1) di Universitas Mataram.
2. Bapak Prof. Drs. Dedy Suhendra, M.Si., Ph.D., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.
3. Bapak Dr. Marwan, S.Si, M.Si., selaku Ketua Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.
4. Bapak/ Ibu Dosen pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram, atas ilmu dan pengetahuan yang diberikan kepada penulis.
5. Keluarga Mahasiswa Matematika (GAMATIKA), atas pengalaman luar biasa yang diberikan kepada penulis.

6. Kawan-kawan seperjuangan Program Studi Matematika Angkatan 2016 (*COS 16),* atas dukungan dan kebersamaannya.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaannya dan semoga bermanfaat bagi kita semua. Aamiin.

Mataram, November 2020

Penulis,

Wahyu Ulyafandhie Misuki

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR NOTASI

$a \in G$	: a anggota dari G
$a \notin G$	: a bukan anggota dari G
a^{-1}	: Invers dari a
R	: Ring
mod	: Modulo
$\mathbb{Z}_n$	: Himpunan semua bilangan bulat modulo n
$\mathbb{Z}_n - \{0\}$	: Himpunan semua bilangan bulat modulo n tanpa 0
$\mathbb{Z}[\mathbb{x}]$	: Himpunan semua polinomial dengan koefisien bilangan bulat
$\mathbb{Z}_n[i]$	: Himpunan semua bilangan bulat Gauss modulo n
$a\|b$	: a habis membagi b
$N(\alpha)$	: Norma dari α
■	: Akhir pembuktian (terbukti)

BAB I

PENDAHULUAN

1.1. Latar Belakang

Bilangan prima adalah bilangan asli yang lebih besar dari 1 yang faktornya adalah 1 dan bilangan itu sendiri. Bilangan prima banyak digunakan dalam kriptografi untuk keperluan keamanan, terutama dalam proses enkripsi dan dekripsi untuk algoritma asimetris (Rahim dkk, 2017). Kriptografi banyak digunakan dalam kehidupan modern saat ini antara lain ketika mengisi kata rahasia (*password*) saat mengambil uang di ATM (memakai nomor PIN) hingga untuk mengecek surel (*email*). Dapat dikatakan bahwa bilangan prima sebagai pembangun sistem kriptografi sehingga pesan atau *password* aman.

RSA (Rivest – Shamir – Adleman) MIT dikembangkan pada tahun 1978 oleh Rivest, Adi Shamir dan Leonard Adleman dan menjadi salah satu algoritma penting dalam sistem keamanan digital (Ivy dkk, 2012). RSA ini sangat bergantung pada faktorisasi prima dari bilangan bulat sehingga salah satu ancaman terhadap RSA yaitu teknologi komputer kuantum, yang mana jika teknologi komputer kuantum ditemukan maka metode RSA ini akan mudah dipecahkan. Akibatnya keamanan dunia digital yang banyak memanfaatkan RSA menjadi tidak berguna lagi. Oleh karena itu diperlukan metode kriptografi yang baru untuk keamanan dunia digital. Salah satu usaha matematikawan dalam mencari alternatif untuk menciptakan teknologi keamanan baru dalam kriptografi adalah dengan mempelajari abstraksi bilangan prima.

Abstraksi bilangan prima diperkenalkan oleh Dedekind pada tahun 1871, dikenal dengan istilah ideal prima. Pada tahun 2009, ideal prima diabstraksi menjadi ideal hampir prima oleh Bhatwadekar. Abstraksi lain dari bilangan prima juga dilakukan di teori modul yang diketahui dengan istilah submodul prima dan submodul hampir prima.

Maulana *dkk* (2018) telah menemukan beberapa sifat bilangan prima pada bilangan bulat Gauss. Bilangan bulat Gauss merupakan bilangan kompleks yang bagian *real* dan imajinernya berupa bilangan bulat. Salah satu fakta yang menarik

yang ditemukan adalah tidak semua bilangan prima pada bilangan bulat juga merupakan bilangan prima pada bilangan bulat Gauss. Bilangan prima pada bilangan bulat merupakan bilangan prima pada bilangan bulat Gauss jika dan hanya jika bilangan tersebut dibagi 4 bersisa 3.

Maulana (2019) menemukan sifat-sifat ideal prima dan ideal hampir prima pada ring bilangan bulat Gauss. Dalam hal ini, penulis ingin melihat lebih jauh lagi karakteristik ideal prima pada ring bilangan bulat Gauss modulo khusunya pada ideal-ideal sikliknya. Hal tersebut melandasi penulis untuk mengangkat judul "Beberapa Sifat Ideal Siklik Prima Pada Ring Bilangan Bulat Gauss Modulo".

1.2. Rumusan Masalah

Dari latar belakang yang telah dipaparkan sebelumnya, maka diperoleh rumusan masalah yaitu, bagaimana sifat ideal siklik prima pada ring bilangan bulat Gauss modulo?

1.3 Tujuan

Adapun tujuan yang ingin dicapai dari penelitian ini yaitu untuk mengetahui sifat ideal siklik prima pada ring bilangan bulat Gauss modulo.

1.4 Manfaat

Adapun manfaat penelitian ini adalah:

1. Sebagai tambahan ilmu pengetahuan dalam bidang teori ring dan teori kriptografi.
2. Abstraksi bilangan prima sebagai alternatif keamanan baru dalam kriptografi di masa depan.

BAB II

LANDASAN TEORI

Pada bagian ini akan dijabarkan beberapa teori yang menjadi dasar dalam penelitian ini yaitu grup, ring, daerah integral, daerah ideal utama, daerah euclid, daerah faktorisasi tunggal, ideal prima, ideal hampir prima, bilangan bulat Gauss, dan bilangan bulat Gauss modulo.

2.1 Grup

Dalam matematika banyak dijumpai objek yang berupa grup, contohnya sistem-sistem bilangan yaitu sistem bilangan bulat, sistem bilangan rasional, sistem bilangan *real*, sistem bilangan kompleks terhadap penjumlahan atau sistem bilangan *real* dan kompleks tanpa nol terhadap perkalian.

Definisi 2.1.1 (Fraleigh, 2014)

Operasi biner $*$ *pada himpunan S adalah fungsi pemetaan* $S \times S$ *ke* S. *Untuk setiap* $(a,b) \in S \times S$, *elemen* $*((a,b))$ *di S dituliskan menjadi* $a * b$.

Dengan definisi operasi biner di atas, berikut diberikan definisi dari grup.

Definisi 2.1.2 (Fraleigh, 2014)

Suatu grup $(G, *)$ *merupakan himpunan* G *dengan operasi biner* $*$ *yang memenuhi aksioma berikut :*

1. *Untuk setiap* $a,b,c \in G$ *berlaku* $(a * b) * c = a * (b * c)$. *(sifat asosiatif)*
2. *Terdapat suatu elemen* $e \in G$ *sehingga berlaku* $a * e = e * a$, *untuk setiap* $a \in G$. *(elemen identitas operasi* $*$*)*
3. *Untuk setiap* $a \in G$, *terdapat* $a^{-1} \in G$ *sehingga berlaku* $a * a^{-1} = a^{-1} * a = e$. *(*$a^{-1}$ *invers dari* a*)*

Contoh 2.1.1

1. Himpunan bilangan bulat $\mathbb{Z}$ merupakan grup terhadap operasi penjumlahan biasa dengan $e = 0$ dan $a^{-1} = -a$ untuk setiap $a \in Z$.
2. Himpunan bilangan bulat modulo $\mathbb{Z}_n$ merupakan grup terhadap operasi penjumlahan biasa dengan $e = 0$ dan $\bar{a}^{-1} = -\bar{a}$ untuk setiap $\bar{a} \in \mathbb{Z}_n$.
3. Himpunan bilangan asli $\mathbb{N}$ terhadap operasi penjumlahan biasa bukan grup terhadap operasi penjumlahan karena $3 \in N$ tidak memiliki invers.

Suatu grup G dikatakan grup Abelian atau komutatif jika operasi binernya bersifat komutatif, berikut diberikan definisinya.

Definisi 2.1.3 (Romdhini, Irwansyah & Switrayni, 2016)

Jika $(G, *)$ *suatu grup yang memenuhi sifat komutatif, yaitu untuk setiap* $a,b \in G$, $a * b = b * a$, *maka* $(G, *)$ *disebut grup komutatif atau grup Abelian.*

Contoh 2.1.1

Himpunan bilangan bulat, bilangan bulat modulo, bilangan *real*, dan bilangan kompleks terhadap operasi penjumlahan biasa merupakan grup Abelian.

Suatu subhimpunan H dari grup G membentuk suatu subgrup dari G bila subhimpunan H juga membentuk grup dengan operasi yang sama pada G berikut definisinya.

Definisi 2.1.4 (Fraleigh, 2014)

Jika suatu subhimpunan H *dari grup* G *tertutup di bawah operasi biner yang sama dengan* G *dan merupakan grup di bawah operasi yang sama dengan* G, *maka* H *merupakan subgrup dari* G.

Untuk mempermudah identifikasi suatu subgrup, berikut teorema yang diberikan.

Teorema 2.1.1 (Romdhini, Irwansyah & Switrayni, 2016)

Suatu subhimpunan H yang tak kosong dari grup $(G, *)$ merupakan subgrup dari G jika dan hanya jika untuk setiap $a,b \in H$ berlaku $a * b^{-1} \in H$.

Bukti. Misalkan H subgrup dari G jelas berlaku $a * b^{-1} \in H$ untuk setiap $a,b \in H$. Sebaliknya, jelas operasi $*$ juga bersifat asosiatif di H. Ambil sebarang $a \in H$, berlaku $a * a^{-1} = e \in H$. Akibatnya, untuk stiap $a \in H$ diperoleh $e * a^{-1} = a^{-1} \in H$ sehingga H tertutup pada operasi invers. Kemudian untuk sebarang $a,b \in H$, diperoleh $b^{-1} \in H$ sehingga $a * (b^{-1})^{-1} = a * b \in H$. Artinya operasi $*$ tertutup juga di H. ■

Contoh 2.1.3

1. Himpunan bilangan bulat dengan bentuk nZ untuk suatu $n \in N$ merupakan subgrup dari $\mathbb{Z}$, dan $\mathbb{H} = \{0, 2, 4, 6\}$ merupakan subgroup dari $\mathbb{Z}_8$.
2. Himpunan bilangan tak negatif bukan merupakan subgrup dari $\mathbb{Z}$, karena setiap unsur positifnya tak memiliki invers.

2.2 Ring

Suatu ring adalah grup dengan operasi penjumlahan dan perkalian yang memenuhi beberapa kondisi. Definisi berikut akan mendeskripsikan hal tersebut lebih jauh.

Definisi 2.2.1 (Dummit dan Foote, 2004)

1. *Suatu himpunan tak kosong R dengan dua operasi biner yaitu penjumlahan $(+)$ dan perkalian $(\times)$ yang didefinisikan pada R dinamakan ring jika memenuhi beberapa aksioma berikut.*
   a. $(R, +)$ *merupakan grup komutatif.*
   b. *Operasi* $(\times)$ *bersifat asosiatif, yakni* $(a \times b) \times c = a \times (b \times c)$ *untuk setiap* $a,b,c \in R$.
   c. *Hukum distributif berlaku pada R, yakni : untuk setiap* $a,b,c \in R$ $a \times (b + c) = (a \times b) + (a \times c)$ *dan* $(a + b) \times c = (a \times c) + (b \times c)$.

2. *Ring R dikatakan komutatif jika operasi $(\times)$ bersifat komutatif, yakni $a \times b = b \times a$, untuk setiap $a,b \in R$.*
3. *Ring R dikatakan memiliki elemen satuan terhadap operasi perkalian jika terdapat elemen $1 \in R$ sehingga $a \times 1 = 1 \times a = a$, untuk setiap $a \in R$.*

Contoh 2.2.1

Himpunan bilangan bulat modulo $\mathbb{Z}_n$ dengan operasi penjumlahan dan perkalian biasa merupakan salah satu contoh ring komutatif dengan unsur satuan.

Definisi 2.2.2 (Dummit dan Foote, 2004)

Misalkan R ring komutatif dan $a,b \in R$ dimana $b \neq 0$.

1. *a dikatakan kelipatan dari b jika terdapat $x \in R$ dimana $a = bx$. Dalam kasus ini b dikatakan membagi a atau pembagi dari a. ditulis $b|a$.*
2. *Faktor persekutuan terbesar dari a dan b adalah elemen tak nol d sedemikian hingga*
   i. *$d|a$ dan $d|b$*
   ii. *Jika $d'|a$ dan $d'|b$ maka $d'|d$*

Faktor persekutuan terbesar dari a dan b dinotasikan gcd(a,b) atau secara sederhana (a,b).

Pada ring yang memiliki unsur satuan, semua unsurnya tidak harus memiliki invers terhadap perkalian. Contohnya adalah ring $\mathbb{Z}$, hanya 1 dan -1 yang memiliki invers terhadap perkalian. Unsur yang memiliki invers terhadap perkalian disebut unit.

Definisi 2.2.3 (Fraleigh, 2014)

Suatu elemen u dari ring komutatif R dengan unsur satuan disebut unit jika u habis membagi 1 atau dengan kata lain u memiliki invers perkalian. Dua elemen $a,b \in R$ berasosiasi di R jika $a = bu$ dimana u adalah suatu unit di R.

Ideal merupakan sub-struktur yang penting dari suatu ring, konsep ideal dari suatu ring analog dengan konsep subgrup normal dari suatu grup.

Definisi 2.2.4 (Roman, 2008)

Misalkan R adalah ring, suatu subhimpunan tak kosong I dari R dinamakan ideal jika

1. *Himpunan I merupakan subgrup dari R, yakni* $a,b \in I$ *berlaku* $a - b \in I$
2. *Himpunan* I *tertutup terhadap perkalian oleh setiap unsur di ring* R*, yakni jika* $a \in I$*,* $r \in R$ *maka berlaku* $ar \in I$ *dan* $ra \in I$*.*

Pada suatu ring R dengan elemen satuan, untuk ideal I dari R yang mengandung unit maka ideal I akan sama dengan ring R sifat tersebut disajikan pada teorema berikut.

Teorema 2.2.1 (Fraleigh, 2014)

Misalkan R *suatu ring dengan elemen satuan dan* I *adalah ideal dari* R *yang mengandung unit, maka* $I = R$*.*

Bukti. Akan ditunjukkan $I \subseteq R$ dan $R \subseteq I$. Karena I merupakan ideal dari R, jelas $I \subseteq R$. Misalkan $u \in I$ merupakan unit, maka terdapat $u^{-1} \in R$ sehingga $uu^{-1} = 1 \in I$. Akibatnya untuk sebarang $a \in R$, diperoleh $a1 = 1a = a \in I$. Artinya $R \subseteq I$. Karena $I \subseteq R$ dan $R \subseteq I$ maka haruslah $I = R$. ■

Tidak semua ideal dibangun oleh satu unsur, ideal yang memiliki satu pembangun disebut ideal utama, berikut definisinya.

Definisi 2.2.5 (Roman, 2008)

Misalkan R *suatu ring, ideal yang dibangun oleh suatu unsur* $a \in R$ *dinamakan ideal utama, yakni* $\langle a \rangle = \{ra | r \in R\}$*.*

Contoh 2.2.2

1. Himpunan bilangan bulat genap yaitu $2Z$ merupakan ideal utama yang dibangun oleh 2.
2. Ideal $\langle 2, x \rangle$ dari ring $\mathbb{Z}[\mathbb{x}]$ bukan merupakan ideal utama karena dibangun oleh 2 dan x.

Semua unsur dalam suatu ring R belum tentu memiliki invers perkalian atau merupakan unit. Ring komutatif dengan elemen satuan dimana setiap unsurnya kecuali 0 memiliki invers perkalian disebut lapangan. Berikut definisinya

Definisi 2.2.6 (Romdhini, Irwansyah & Switrayni, 2016)

Suatu ring komutatif R dengan unsur satuan dinamakan lapangan jika setiap unsur tak nolnya memiliki invers terhadap operasi perkalian di R.

Contoh 2.2.3

1. Himpunan bilangan Real merupakan lapangan.
2. Ring $\mathbb{Z}_n$ dimana n bilangan prima merupakan lapangan.

Teorema 2.2.2 (Romdhini, Irwansyah & Switrayni, 2016)

Misalkan R adalah ring komutatif dengan unsur satuan. R adalah lapangan jika dan hanya jika ideal-ideal dari R hanya 0 *dan R.*

Bukti. Misalkan R adalah lapangan dan I ideal tak nol dari R. Maka terdapat $0 \neq x \in I$. Karena R lapangan, maka terdapat $x^{-1} \in R$ sehingga $1 = xx^{-1} \in I$. Berdasarkan Teorema 2.2.1 maka $I = R$. Hal ini berarti berarti R tidak memiliki ideal sejati tak nol. Dengan kata lain, ideal-ideal dari R hanya 0 dan R. Sebaliknya misalkan ideal-ideal dari R hanya 0 dan R. Ambil sebarang unsur tak nol a di R. Maka $\langle a \rangle$ merupakan ideal tak nol dan haruslah $\langle a \rangle = R$. Hal ini menunjukkan $1 \in \langle a \rangle$. Artinya terdapat $r \in R$ sehingga $ra = 1$. Jadi, setiap unsur tak nol a di R merupakan unit. Dengan demikian, R adalah lapangan. ■

Suatu ideal I dari ring R dikatakan ideal maksimal bila I berbeda dengan R dan tidak ada ideal lain selain R yang mengandung I. Berikut definisinya.

Definisi 2.2.7 (Roman, 2008)

Suatu ideal I dari R dinamakan ideal maksimal jika $I \neq R$ dan apabila ada ideal J dari R dimana $I \subseteq J \subseteq R$ maka $I = J$ atau $J = R$.

Contoh 2.2.3

1. Ideal $I = \langle 2 \rangle$ merupakan ideal maksimal dari $\mathbb{Z}$, karena tidak ada ideal lain yang mengandung *I* kecuali $\mathbb{Z}$ itu sendiri.
2. Ideal $I = \langle 4 \rangle$ bukan merupakan ideal maksimal dari $\mathbb{Z}$ karena ada $J = \langle 2 \rangle \neq \mathbb{Z}$ dimana $I \subset J$.

Bila I dan J merupakan ideal maka perkalian I dan J dapat didefinisikan sebagai berikut.

Definisi 2.2.8 (Dummit dan Foote, 2004)

Diberikan I dan J merupakan ideal dari ring R. Perkalian ideal I dan J didefinisikan sebagai $IJ = \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in N\right\}$.

Perkalian dua ideal juga membentuk ideal, berikut teorema yang diberikan.

Teorema 2.2.3 (Romdhini, Irwansyah & Switrayni, 2016)

Jika I dan J merupakan ideal dari ring R, maka IJ merupakan ideal dari ring R.

Bukti. Ambil sebarang $\alpha = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$ dan $= p_1 q_1 + p_2 q_2 + \cdots + p_n q_n \in IJ$, jelas $\alpha - \beta \in IJ$.
Perhatikan bahwa $r\alpha = ra_1 b_1 + ra_2 b_2 + \cdots + ra_n b_n$. Karena $a_i \in I$ dan I ideal, maka jelas $ra_i \in I$, $i = 1, 2, \ldots, n$. Jadi diperoleh $r\alpha \in IJ$.
Perhatikan bahwa $\alpha r = a_1 b_1 r + a_2 b_2 r + \cdots + a_n b_n r$. Karena $b_i \in J$ dan J ideal, maka jelas $b_i r \in J$, $i = 1, 2, \ldots, n$. Jadi diperoleh $\alpha r \in IJ$.■

2.3 Daerah Integral

Misalkan R adalah ring dan $a \in R$ maka $a0 = 0a = 0$. Hal ini menunjukkan bahwa jika terdapat faktor yang 0 dalam perkalian unsur-unsur dari R, maka hasil kalinya adalah 0. Akan tetapi konvers dari pernyataan itu tidak selalu benar. Contohnya pada ring $\mathbb{Z}_{10}$ diperoleh $\overline{2} \times \overline{5} = 0$, akan tetapi tidak ada satupun dari faktor-faktor tersebut merupakan $\overline{0}$. Dari contoh tersebut, $\overline{2}$ dan $\overline{5}$

dikatakan pembagi nol di $\mathbb{Z}_{10}$. Definisi berikut akan mendeskripsikan lebih lanjut mengenai hal tersebut.

Definisi 2.3.1 (Romdhini, Irwansyah & Switrayni, 2016)

Misalkan R adalah ring. Suatu unsur tak nol $a \in R$ disebut pembagi nol jika terdapat suatu unsur tak nol $b \in R$ sehingga $ab = 0$ atau $ba = 0$.

Definisi 2.3.2 (Romdhini, Irwansyah & Switrayni, 2016)

Suatu ring komutatif R dengan unsur satuan dinamakan daerah integral jika R tidak memuat unsur pembagi nol.

Contoh 2.3.1

1. Himpuan bilangan bulat dengan operasi penjumlahan dan perkalian biasa merupakan salah satu contoh daerah integral.
2. $\mathbb{Z}_n$ merupakan daerah integral saat n prima.
3. $\mathbb{Z}_6$ bukan daerah integral karena terdapat pembagi nol yaitu $\overline{2}$ dan $\overline{3}$.

Teorema 2.3.1 (Dummit dan Foote, 2004)

Misalkan R daerah integral. Jika dua elemen d dan d' di R membangun ideal utama yang sama yaitu $\langle d \rangle = \langle d' \rangle$, maka $d' = ud$ untuk suatu unit $u \in R$. Khususnya jika d dan d' keduanya faktor persekutuan terbesar dari a dan b, maka $d' = ud$ untuk suatu unit u.

Bukti. Jelas untuk d atau d' yang bernilai nol, jadi asumsikan d atau d' elemen tak nol di R. Karena $d \in \langle d' \rangle$ artinya terdapat $x \in R$ sehingga $d = xd$. Karena $d' \in \langle d \rangle$ artinya terdapat $d' \in \langle d \rangle$ sehingga $d' = yd$. Maka $d = xyd$ dan $d(1 - xy) = 0$. Karena $d \neq 0$ maka haruslah $xy = 1$ sehingga keduanya x dan y merupakan unit. Ini membuktikan pernyataan pertama. Untuk pernyataan kedua merupakan akibat dari pernyataan pertama karena dua faktor persekutuan terbesar dari a dan b membangun ideal utama yang sama (membagi satu sama lain).

Dalam daerah integral, bilangan tak tereduksi bisa didefinisikan, berikut definisinya.

Definisi 2.3.3 (Fraleigh, 2014)

Suatu elemen taknol dan bukan unit p dari suatu daerah integral D dikatakan tak tereduksi di D jika setiap pemfaktoran $p = ab$ di D hanya terpenuhi bila a atau b adalah unit.

Kemudian berikut ini bilangan prima yang didefinisikan pada daerah integral.

Definisi 2.3.4 (Fraleigh, 2014)

Suatu elemen taknol dan bukan unit p dari suatu daerah integral D disebut prima jika untuk setiap $a,b \in D$, $p|ab$ berimplikasi $p|a$ atau $p|b$.

Contoh 2.3.2

1. Pada bilangan bulat, 5 merupakan salah satu bilangan tak tereduksi karena semua faktornya berbentuk $5 = 5 \cdot 1$ atau $5 = (-5) \cdot (-1)$ dimana 1 dan -1 merupakan unit.
2. Pada bilangan bulat, 6 bukan merupakan bilangan tak tereduksi karena ada faktornya yang berbentuk $2 \cdot 3 = 6$ dimana 2 dan 3 bukan unit.

2.4 Daerah Ideal Utama, Daerah Euclid dan Daerah Faktorisasi Tunggal

Pada daerah integral D dimana setiap idealnya merupakan ideal utama maka D merupakan daerah ideal utama. Berikut definisinya.

Definisi 2.4.1 (Romdhini, Irwansyah & Switrayni, 2016)

Suatu daerah integral D merupakan suatu daerah ideal utama jika setiap idealnya merupakan ideal utama.

Dalam daerah ideal utama, ideal maksimal dan bilangan tak tereduksi saling berkaitan. Berikut teoremanya.

Teorema 2.4.1 (Fraleigh, 2014)

Suatu ideal $\langle p \rangle$ pada daerah ideal utama merupakan ideal maksimal jika dan hanya jika p tak tereduksi.

Bukti. Diberikan p ideal maksimal dari suatu daerah ideal utama D. Misalkan $p = ab$ di D, maka $\langle p\rangle \subseteq \langle a\rangle$. Jika $\langle p\rangle = \langle a\rangle$ maka a dan p berasosiasi, sehingga b merupakan unit. Jika $\langle p\rangle \neq \langle a\rangle$ maka haruslah $\langle a\rangle = \langle 1\rangle = D$. Karena $\langle p\rangle$ ideal maksimal, sehingga a dan 1 berasosiasi. Akibatnya a unit. Dari dua kasus tersebut diperoleh a atau b unit. Jadi p tak tereduksi.
Sebaliknya, misalkan p tak tereduksi di D. Jika $\langle p\rangle \subseteq \langle a\rangle$ didapatkan $p = ab$. Jika a unit, maka $\langle a\rangle = \langle 1\rangle = D$. Jika a bukan unit, maka b harus unit, sehingga terdapat $u \in D$ sehingga $bu = 1$. Akibatnya $pu = abu = a1 = a$, jadi $\langle a\rangle \subseteq \langle p\rangle$ dan didapatkan $\langle p\rangle = \langle a\rangle$. Dari dua kasus tersebut diperoleh $\langle a\rangle = D$ atau $\langle a\rangle = \langle p\rangle$. Jadi $\langle p\rangle$ ideal maksimal.■

Dalam daerah ideal utama, unsur tak tereduksi dan unsur prima ekivalen. Lebih jelasnya berikut teorema yang diberikan.

Teorema 2.4.2 (Roman, 2008)

Misalkan D daerah ideal utama, $p \in D$ *prima jika hanya jika* p *tak tereduksi.*

Bukti. Misalkan p prima dan $p = ab$, artinya $p|ab$. Karena p prima berlaku $p|a$ atau $p|b$. Tanpa mengurangi keumuman, misalkan hanya berlaku $p|a$ artinya $a = pk$ untuk suatu $k \in D$. Selanjutnya $p = ab = pkb$ diperoleh $p(1 - kb) = 0$.
Karena daerah ideal utama merupakan daerah integral dan $p \neq 0$ maka haruslah $1 - kb = 0$ diperoleh $kb = 1$, akibatnya b suatu unit di D. Jadi p tak tereduksi.
Sebaliknya, misalkan p tak tereduksi dan $p|ab$. Berdasarkan teorema 2.4.1 diperoleh $\langle p\rangle$ ideal maksimal. Akibatnya $\langle p,a\rangle = \langle p\rangle$ atau $\langle p,a\rangle = D = \langle 1\rangle$. Untuk $\langle p,a\rangle = \langle p\rangle$ diperoleh $p|a$. Untuk $\langle p,a\rangle = D = \langle 1\rangle$ diperoleh $1 = xp + ya$ untuk suatu $x,y \in D$. Dengan mengalikan kedua ruas dengan b diperoleh $b = bxp + bya$. Karena $p|bxp$ dan $p|bya$ maka $p|b$. Dari kedua kasus tersebut maka $p|a$ atau $p|b$. Jadi p prima. ■

Setiap bilangan bulat yang lebih dari 1, dapat ditulis sebagai perkalian hingga bilangan-bilangan prima. Secara umum, pada daerah integral yang setiap elemennya dapat ditulis sebagai perkalian hingga bilangan-bilangan tak tereduksi dikatakan daerah faktorisasi tunggal. Berikut definisi yang diberikan.

Definisi 2.4.2 (Roman, 2008)

Suatu daerah integral D disebut daerah faktorisasi tunggal bila memenuhi kondisi berikut:

a. *Setiap elemen D yang bukan nol ataupun unit bisa difaktorkan menjadi perkalian hingga bilangan tak tereduksi.*
b. *Jika $p_1p_2...p_r$ dan $q_1q_2...q_s$ adalah dua faktorisasi berbeda dari suatu unsur di D maka $r = s$ dan faktorisasi q_j dapat diurutkan kembali sehingga p_i dan q_i berasosiasi.*

Daerah ideal utama merupakan daerah faktorisasi tunggal, berikut lemma dan teorema yang diberikan.

Lemma 2.4.1 (Kondisi rantai naik) (Fraleigh, 2014)

Diberikan D suatu daerah ideal utama. Jika $N_1 \subseteq N_2 \subseteq \cdots$ merupakan suatu rantai naik dari ideal-ideal N_i di D, maka terdapat suatu bilangan bulat positif r sehingga $N_r = N_s$ untuk setiap $s \geq r$.

Bukti. Misalkan $a,b \in N$, artinya $a \in N_i$ dan $b \in N_j$ untuk suatu $i,j \in \mathbb{Z}^+$. Untuk $i = j$ maka jelas N ideal. Untuk $i \neq j$, diperoleh $i < j$ atau $j < i$. Tanpa mengurangi perumuman misalkan $i < j$, artinya $N_i \subseteq N_j$. Karena $a \in N_i$ maka haruslah $a \in N_j$. Diperoleh $a - b \in N_j$ dan $N_j \subseteq N$ maka $a - b \in N$. Selanjutnya untuk sebarang $r \in D$ dan $a \in N$ dimana $a \in N_i$ untuk suatu $i \in \mathbb{Z}^+$, diperoleh $ra = ar \in N_i$. Karena $N_j \subseteq N$ maka $ra = ar \in N$. Dengan demikian $N = \bigcup_{i=1}^{\infty} N_i$ merupakan ideal di D. Karena D merupakan daerah ideal utama maka $N = \langle c \rangle$ untuk suatu $c \in D$. Karena $N = \bigcup_{i=1}^{\infty} N_i$, maka $c \in N_r$, untuk suatu $r \in \mathbb{Z}^+$. Untuk $s \geq r$, diperoleh $\langle c \rangle \subseteq N_r \subseteq N_s \subseteq \langle c \rangle$. Diperoleh $N_r = N_s$ untuk $s \geq r$. ■

Selanjutnya diberikan teorema yang menunjukkan bahwa setiap daerah ideal utama merupakan daerah faktorisasi tunggal.

Teorema 2.4.3 (Roman, 2008)

Setiap daerah ideal utama D merupakan daerah faktorisasi tunggal.

Bukti. Diberikan $r \in D$ dimana r tak nol dan bukan unit, jika r tak tereduksi maka bukti selesai. Jika r tereduksi maka $r = r_1 r_2$ dimana faktor-faktonya bukan unit. Jika r_1 dan r_2 tak tereduksi maka bukti selesai. Jika tidak, misalkan r_2 tereduksi, sehingga $r_2 = r_3 r_4$ dimana faktor-faktonya bukan unit. Dengan cara yang sama, didapatkan

$$r = r_1 r_2 = r_1(r_3 r_4) = r_1 r_3(r_5 r_6) = r_1 r_3 r_5(r_7 r_8) = \cdots$$

Setiap langkah, memfaktorkan r menjadi perkalian faktor-faktor yang bukan unit. Bagaimanapun proses itu akan berhenti setelah berhingga langkah. Dalam keadaan lain, itu akan menghasilkan tak berhingga barisan $s_1, s_2, \cdots$ elemen elemen bukan unit dari R, dimana s_{i+1} membagi s_i, sehingga diperoleh rantai naik

$$\langle s_1 \rangle \subset \langle s_2 \rangle \subset \langle s_3 \rangle \subset \cdots$$

Tetapi kontradiksi dengan kondisi rantai naik ideal utama. Jadi haruslah r dapat difaktorkan menjadi berhingga elemen-elemen tak tereduksi. Untuk menunjukkan ketunggalan, misalkan $r = p_1 p_2 \cdots p_s$ dan $r = q_1 q_2 \cdots q_s$ merupakan faktor-faktor lain tak tereduksi. Kemudian didapatkan $p_1 | (q_1 q_2 \cdots q_s)$ berimplikasi $p_1 | q_j$. Tanpa mengurangi perumuman, asumsikan $j = 1$ atau $p_1 | q_1$ maka $q_1 = p_1 u_1$ dan karena q_1 tak tereduksi maka u_1 unit. Jadi r_1 dan q_1 berasosiasi. diperoleh

$$p_1 p_2 \cdots p_r = p_1 u_1 q_2 \cdots q_s$$

Berdasarkan hukum pembatalan diperoleh

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s$$

Dengan cara yang sama, diperoleh

$$1 = u_1 u_2 \cdots q_{r+1} \cdots q_s$$

Karena q_j tak tereduksi, maka haruslah $r = s$. ■

Dalam daerah integral, norma Euclid bisa didefinisikan. Norma Euclid merupakan fungsi yang memetakan elemen tak nol ke bilangan bulat tak negatif dengan beberapa kondisi. Untuk lebih jelasnya berikut definisi norma Euclid.

Definisi 2.4.3 (Fraleigh, 2014)

Suatu norma Euclid pada suatu daerah integral D adalah suatu fungsi v yang memetakan elemen tak nol ke bilangan bulat tak negatif yang memenuhi kondisi berikut :

a. *Untuk setiap $a,b \in D, b \neq 0$ terdapat $q,r \in D$ sehingga $a = bq + r$ dimana $r = 0$ atau $v(r) < v(b)$.*
b. *Untuk setiap $a,b \neq 0 \in D$ berlaku $v(a) < v(ab)$.*

Suatu daerah integral D merupakan daerah Euclid bila terdapat norma Euclid pada D.

Teorema 2.4.4 (Fraleigh, 2014)

Setiap daerah Euclid merupakan daerah ideal utama.

Bukti. Diberikan D suatu daerah Euclid dengan norma Euclid v, dan diberikan I suatu ideal di D. Jika $I = \{0\}$ maka $I = \langle 0 \rangle$ dan I ideal utama. Untuk $I \neq 0$, maka ada $b \neq 0$ di I. Pilih b sehingga $v(b)$ merupakan minimal dari $v(n)$ untuk semua $n \in I$. Jelas $\langle b \rangle \subseteq I$, karena $b \in I$ dan I ideal. Sebaliknya, ambil sebarang $a \in I$ sehingga berdasarkan kondisi 1 definisi norma Euclid, terdapat q dan r sehingga $a = bq + r$, dimana $r = 0$ atau $v(r) < v(b)$. Perhatikan bahwa $r = a - bq$ dimana $a,b \in I$, karena I ideal berakibat $r \in I$. Karena keminimalan dari $v(b)$, maka $v(r) < v(b)$ tidak mungkin. Jadi haruslah $r = 0$ sehingga $a = bq \in \langle b \rangle$, diperoleh $I \subseteq \langle b \rangle$. Jadi $I = \langle b \rangle$. ■

Dengan menggunakan norma Euclid, dapat ditentukan unit dari dari daerah Euclid itu sendiri, untuk lebih jelasnya berikut teorema yang diberikan.

Teorema 2.4.5 (Fraleigh, 2014)

Untuk suatu daerah Euclid D dengan norma Euclid v, $v(1)$ adalah minimal dari semua $v(a)$ untuk elemen tak nol $a \in D$, dan $u \in D$ adalah unit jika dan hanya jika $v(u) = v(1)$.

Bukti. Perhatikan bahwa untuk $0 \neq a \in D$ berlaku $v(1) \leq v(1a) = v(a)$. Misalkan u sebarang unit di D, maka berlaku juga $v(u) \leq v(uu^{-1}) = v(1)$. Tetapi $v(1)$ minimal, jadi haruslah $v(u) = v(1)$.

Sebaliknya, andaikan ada elemen tak nol $u \in D$ dimana $v(u) = v(1)$. Dengan menggunakan algoritma pembagian, terdapat $q,r \in D$ sehingga berlaku

$$1 = uq + r,$$

Dimana $r = 0$ atau $v(r) < v(u)$. Karena $v(u) = v(1)$ adalah minimal dari semua $v(d)$ untuk elemen tak nol $d \in D$, maka $v(r) < v(u)$ tidak mungkin terjadi, jadi haruslah r= 0. Diperoleh $1 = uq$. Jadi u adalah unit di D. ■

2.5 Ideal Prima dan Ideal Hampir Prima

Abstraksi bilangan prima pada ring diperkenalkan oleh Dedekind pada Tahun 1871, dinamakan ideal prima, berikut definisinya.

Definisi 2.5.1 (Fraleigh, 2014)

Suatu ideal $I \neq R$ dalam ring komutatif R merupakan ideal prima jika $ab \in I$ berimplikasi $a \in I$ atau $b \in I$ untuk $a,b \in R$.

Selanjutnya pada Tahun 2009, ideal prima diperumum lagi menjadi ideal hampir prima oleh Bhatwadekar-Sharma. Definisnya sebagai berikut.

Definisi 2.5.2 (Bhatwadekar dan Sharma, 2009)

Suatu ideal $I \neq R$ dalam ring komutatif R merupakan ideal hampir prima jika $ab \in I - I^2$ berimplikasi $a \in I$ atau $b \in I$ untuk $a,b \in R$.

Untuk lebih jelasnya, berikut diberikan beberapa contoh :

Contoh 2.5.1

1. Ideal $I = \langle 2 \rangle$ merupakan ideal prima dari ring $\mathbb{Z}$.
2. Ideal $I = \langle 6 \rangle$ bukan merupakan ideal prima dari ring $\mathbb{Z}$ karena ada $2,3 \in Z$ dimana $2 \cdot 3 \in \langle 6 \rangle$ tetapi $2 \notin \langle 6 \rangle$ dan $3 \notin \langle 6 \rangle$.

3. Ideal $I = \langle \overline{0} \rangle = \{\overline{0}\}$ merupakan ideal hampir prima dari ring $\mathbb{Z}_6$, tetapi bukan merupakan ideal prima karena ada $\overline{2},\overline{3} \in \mathbb{Z}_6$ dimana $\overline{2} \cdot \overline{3} \in \langle \overline{0} \rangle$ tetapi $\overline{2} \notin \langle \overline{0} \rangle$ dan $\overline{3} \notin \langle \overline{0} \rangle$.
4. Ideal $I = \langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\}$ merupakan ideal hampir prima dari ring $\mathbb{Z}_{12}$, tetapi bukan merupakan ideal prima karena ada $\overline{2} \in \mathbb{Z}_{12}$ dimana $\overline{2} \cdot \overline{2} \in \langle \overline{4} \rangle$ tetapi $\overline{2} \notin \langle \overline{4} \rangle$.

2.6 Bilangan Bulat Gauss

Bilangan kompleks merupakan perumumam dari bilangan *real*, begitu juga dengan bilangan bulat Gauss yang meupakan perumuman dari bilangan bulat.

Definisi 2.6.1 (Fraleigh, 2014)

Ring bilangan bulat Gauss modulo $\mathbb{Z}_n = \{a + ib | a,b \in \mathbb{Z}_n\}$. *Untuk bilangan bulat Gauss* $\alpha = a + ib$, *norma dari* α *ialah* $N(\alpha) = a^2 + b^2$.

Norma pada bilangan bulat Gauss memiliki beberapa sifat, lebih jelasnya berikut lemma yang diberikan.

Lemma 2.6.1 (Fraleigh, 2014)

Dalam $\mathbb{Z}[\mathbb{i}]$, *fungsi norma* N *untuk setiap* $\alpha,\beta \in Z[i]$ *berlaku beberapa sifat sebagai berikut :*

a. $N(\alpha) \geq 0$.

b. $N(\alpha) = 0$ *jika dan hanya jika* $\alpha = 0$

c. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Bukti.

Misalkan $\alpha = a_1 + ia_2$ dan $\beta = b_1 + ib_2$

a. $N(\alpha) = a_1^2 + a_2^2$, jelas $N(\alpha) \geq 0$.
b. $N(\alpha) = a_1^2 + a_2^2 = 0$ terpenuhi jika dan hanya jika $a = b = 0$ $(\alpha = 0)$
c. $N(\alpha\beta) = N((a_1 + ia_2)(b_1 + ib_2))$

$$\Leftrightarrow N(\alpha\beta) = N(a_1b_1 + ia_1b_2 + ia_2b_1 - a_2b_2)$$
$$\Leftrightarrow N(\alpha\beta) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2$$
$$\Leftrightarrow N(\alpha\beta) = (a_1^2b_1^2 - 2a_1a_2b_1b_2 + a_2^2b_2^2) + (a_1^2b_2^2 + 2a_1a_2b_1b_2 + a_2^2b_1^2)$$
$$\Leftrightarrow N(\alpha\beta) = a_1^2\left(b_1^2 + b_2^2\right) + a_2^2(b_2^2 + b_1^2)$$
$$\Leftrightarrow N(\alpha\beta) = \left(a_1^2 + a_2^2\right)\left(b_1^2 + b_2^2\right) = N(\alpha)N(\beta) \quad \blacksquare$$

Berikut lemma yang menunjukkan bahwa bilangan bulat Gauss merupakan daerah integral.

Lemma 2.6.2 (Fraleigh, 2014)

Himpunan bilangan bulat Gauss adalah daerah integral.

Bukti. Jelas bahwa $\mathbb{Z}[\mathbb{i}]$ merupakan ring komutatif dengan unsur satuan. Akan ditunjukkan bahwa $\mathbb{Z}[\mathbb{i}]$ tidak memiliki pembagi 0. Jika $\alpha\beta = 0$ maka $N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0$. Berimplikasi $N(\alpha) = 0$ atau $N(\beta) = 0$ sehingga berimplikasi $\alpha = 0$ atau $\beta = 0$. Jadi $\mathbb{Z}[\mathbb{i}]$ tidak memiliki pembagi nol sehingga $\mathbb{Z}[\mathbb{i}]$ merupakan daerah integral. ■

Telah dibuktikan di atas bahwa bilangan bulat Gauss merupakan daerah integral, sehingga dapat ditunjukkan bahwa bilangan bulat Gauss merupakan daerah Euclid.

Teorema 2.6.1 (Fraleigh, 2014)

Fungsi v diberikan oleh $v(\alpha) = N(\alpha)$ untuk $\alpha \neq 0 \in Z[i]$ adalah norma Euclid pada $\mathbb{Z}[i]$, sehingga $\mathbb{Z}[i]$ merupakan daerah Euclid.

Bukti. Perhatikan bahwa untuk $\beta = b_1 + ib_2 \neq 0$, $N(\beta) = b_1^2 + b_2^2$, jelas $N(\beta) \geq 1$. Sehingga untuk setiap $\alpha,\beta \neq 0$ di $\mathbb{Z}[i]$, $N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta)$.

Ini membuktikan kondisi 2 pada definisi norma Euclid. Selanjutnya akan dibuktikan kondisi 1 pada definisi norma Euclid. Diberikan $\alpha,\beta \in Z[i]$ dengan $\alpha = a_1 + ia_2$ dan $\beta = b_1 + ib_2$, dimana $\beta \neq 0$. Akan dikonstruksi $\sigma,\rho \in Z[i]$ sehingga $\alpha = \beta\sigma + \rho$ dimana $\rho = 0$ atau $N(\rho) < N(\beta) = b_1^2 + b_2^2$.

Diberikan $\frac{\alpha}{\beta} = r + is$ untuk $r,s \in Q$. Diberikan q_1,q_2 bilangan bulat di $\mathbb{Z}$ yang mendekati r dan s yaitu $q_1 = \lfloor r \rfloor$ untuk $r - \lfloor r \rfloor \leq r - \lceil r \rceil$ atau $q_1 = \lceil r \rceil$ untuk $r - \lceil r \rceil < r - \lfloor r \rfloor$ dan $q_2 = \lfloor s \rfloor$ untuk $s - \lfloor s \rfloor \leq s - \lceil s \rceil$ atau $q_2 = \lceil s \rceil$ untuk s$- \lceil s \rceil < s - \lfloor s \rfloor$. Diberikan $\sigma = q_1 + iq_2$ dan $\rho = \alpha - \beta\sigma$. Jika $\rho = 0$ bukti selesai. Jika tidak, dari kontruksi σ diketahui bahwa $|r - q_1| \leq \frac{1}{2}$ dan $|s - q_2| \leq \frac{1}{2}$. Sehingga $N\left(\frac{\alpha}{\beta} - \sigma\right) = N((r + is) - (q_1 + iq_2)) = N((r - q_1) + i(s - q_2)) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$. Didapatkan $N(\rho) = N(\alpha - \beta\sigma) = N\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \sigma\right) \leq N(\beta)\frac{1}{2} < N(\beta)$**.** Jadi fungsi N merupakan norma Euclid sehingga $\mathbb{Z}[i]$ merupakan daerah Euclid. ■

Tidak semua unsur di bilangan bulat Gauss merupakan unit, berikut lemma yang diberikan.

Lemma 2.6.3 (Fraleigh, 2014)

Unit di $\mathbb{Z}[i]$ *hanya* $1, -1, i$ *dan* $-i$.

Bukti. Karena $v(1) = 1$ merupakan minimal dari $v(\alpha)$ untuk setiap elemen tak nol $\alpha \in Z[i]$ dengan $\alpha = a + ib$ dan $v(\alpha) = a^2 + b^2$. Berdasarkan Teorema 2.4.5, maka semua $u = c + id$ yang memenuhi $v(u) = v(1) = 1$ merupakan unit. Karena $v(u) = c^2 + d^2 = 1$, maka haruslah $c^2 = 1$ dan $d = 0$ atau $c = 0$ dan $d^2 = 1$. Jadi unit di $\mathbb{Z}[i]$ hanya $1, -1, i$ dan $-i$. ■

Bilangan tak tereduksi dan bilangan prima merupakan ekivalen pada bilangan bulat Gauss, untuk lebih jelasnya berikut teorema yang diberikan.

Teorema 2.6.2 (Roman, 2008)

Misal $p \in Z[i]$, p *tak tereduksi jika dan hanya jika* p *prima.*

Bukti. Karena $\mathbb{Z}[i]$ merupakan daerah Euclid, maka berakibat $\mathbb{Z}[i]$ merupakan daerah ideal utama. Berdasarkan teorema 2.4.2 maka jelas teorema ini terbukti.

2.7 Bilangan Prima Gauss

Pada bagian sebelumnya telah dijabarkan definisi bilangan prima dan bilangan tak tereduksi dimana keduanya merupakan dua hal yang ekivalen pada bilangan bulat Gauss. Selanjutnya bilangan prima pada bilangan bulat disebut bilangan prima biasa dan bilangan prima pada bilangan bulat Gauss disebut bilangan prima Gauss.

Tidak semua bilangan prima biasa ganjil dapat ditulis sebagai penjumlahan dua bilangan kuadrat. Kondisi dimana bilangan prima biasa ganjil dapat ditulis sebagai penjumlahan dua bilangan kuadrat diberikan oleh teorema berikut.

Teorema 2.7.1 (Teorema Fermat $p = a^2 + b^2$) (Fraleigh, 2014)
Diberikan p *suatu bilangan prima ganjil di* $\mathbb{Z}$*, maka* $p = a^2 + b^2$ *untuk* $a,b \in Z$ *jika dan hanya jika* $p \equiv 1 \ (mod\ 4)$.

Bukti. Misalkan p prima ganjil dan $p = a^2 + b^2$, $a,b \in Z$. Karena p ganjil maka a dan b tidak boleh keduanya ganjil atau keduanya genap, sehingga haruslah yang satu genap dan lainnya ganjil. Misalkan $a = 2r$ dan $b = 2s + 1$ diperoleh $p = a^2 + b^2 = (2r)^2 + (2s + 1)^2 = 4r^2 + 4(s^2 + s) + 1$. Jadi $p \equiv 1(mod\ 4)$.

Sebaliknya, misalkan $p \equiv 1 \ (mod\ 4)$. Perhatikan bahwa $\mathbb{Z}_p - \{0\}$ adalah grup perkalian dan memiliki order $p - 1$. Karena 4 merupakan pembagi $p - 1$, didapatkan $\mathbb{Z}_p - \{0\}$ mengandung suatu elemen n berorde 4. Itu berakibat n^2 berorde 2, sehingga $n^2 = -1 = p - 1$ di $\mathbb{Z}_p$. Selanjutnya di $\mathbb{Z}$ didapatkan $n^2 \equiv -1 \ mod\ p$, jadi p membagi $n^2 + 1$ di $\mathbb{Z}$.

Pandang p dan $n^2 + 1$ di $\mathbb{Z}[\mathbb{i}]$, didapatkan p membagi $n^2 + 1 = (n + i)(n - i)$.

Andaikan p tak tereduksi di $\mathbb{Z}[i]$, maka p harus membagi $(n + i)$ atau $(n - i)$. Jika p membagi $(n + i)$ maka $(n + i) = p(a + ib)$ untuk suatu $a,b \in Z$. Didapatkan $pb = 1$, tidak dapat terjadi karena p bilangan prima ganjil. Begitu pula jika p membagi $(n - i)$ maka $(n - i) = p\ (c + id)$ untuk suatu $c,d \in Z$ didapatkan $pd = -1$, tidak dapat terjadi karena p bilangan prima

ganjil. Pengandaian bahwa p tak tereduksi pada $\mathbb{Z}[i]$ salah, jadi haruslah p tereduksi pada $\mathbb{Z}[i]$.

Karena p tereduksi pada $\mathbb{Z}[i]$, maka $p = (a+ib)(c+id)$ dimana $(a+ib)$ dan $(c+id)$ bukan unit.

Dengan mengambil normanya, $p^2 = (a^2+b^2)(c^2+d^2)$ dimana tidak ada satupun $(a^2+b^2) = 1$ atau $(c^2+d^2) = 1$. Akibatnya $p = (a^2+b^2) = (c^2+d^2)$ Sehingga didapatkan $p = (a^2+b^2) = (a+ib)(a-ib)$ dengan $(a-ib) = (c+id)$.■

Lemma 2.7.1 (Fraleigh, 2014)

Diberikan p suatu bilangan prima di $\mathbb{Z}$, $p = (a+ib)(a-ib) = a^2+b^2$ untuk $a,b \in Z$ jika dan hanya jika p tereduksi di $\mathbb{Z}[\mathbb{i}]$.

Bukti. Misalkan $p = (a+ib)(a-ib)$. Untuk $a = 0$ berakibat $p = b^2$, untuk $b = 0$ berakibat $p = a^2$. Kedua kasus tersebut tidak mungkin terjadi karena p merupakan bilangan prima. Jadi haruslah $a,b \neq 0$, akibatnya $(a+ib)$ dan $(a-ib)$ bukan unit di $\mathbb{Z}[\mathbb{i}]$. Jadi p tereduksi di $\mathbb{Z}[\mathbb{i}]$.

Sebaliknya, diberikan p tereduksi di $\mathbb{Z}[i]$, artinya ada $(a+ib), (c+id) \in \mathbb{Z}[\mathbb{i}]$ sehingga $p = (a+ib)(c+id)$ dimana $(a+ib)$ dan $(c+id)$ bukan unit. Dengan mengambil normanya, diperoleh $p^2 = (a^2+b^2)(c^2+d^2)$ dimana tidak ada satupun $(a^2+b^2) = 1$ atau $(c^2+d^2) = 1$. Akibatnya $p = (a^2+b^2) = (c^2+d^2)$ Sehingga didapatkan $p = (a^2+b^2) = (a+ib)(a-ib)$ dengan $(a-ib) = (c+id)$.■

Teorema dan lemma sebelumnya digunakan untuk menentukan bilangan prima biasa yang merupakan bilangan prima Gauss. Hal tersebut diberikan oleh teorema berikut.

Teorema 2.7.2 (Maulana, Wardhana, Switrayni dan Aini, 2018)

Diberikan p suatu bilangan prima di $\mathbb{Z}$, p merupakan bilangan prima Gauss jika dan hanya jika $p \equiv 3 \ (mod\ 4)$.

Bukti. Untuk bilangan prima genap yakni $p = 2$, jelas tidak bertentangan dengan teorema.

Untuk p prima ganjil di $\mathbb{Z}$, berdasarkan teorema Fermat dan lemma 2.7.1, didapatkan fakta bahwa, p tereduksi di $\mathbb{Z}[\mathbb{i}]$ jika dan hanya jika $p \equiv 1\ (mod\ 4)$.

Ekivalen dengan, p tak tereduksi di $\mathbb{Z}[\mathbb{i}]$ jika dan hanya jika $p \not\equiv 1\ (mod\ 4)$.

Perhatikan bahwa $p \not\equiv 1\ (mod\ 4)$, artinya $p \equiv 0\ (mod\ 4)$ atau $p \equiv 2\ (mod\ 4)$ atau $p \equiv 3(mod\ 4)$.

Untuk $p \equiv 0\ (mod\ 4)$ atau $p \equiv 2\ (mod\ 4)$, tidak mungkin karena p merupakan bilangan prima ganjil, maka haruslah $p \equiv 3\ (mod\ 4)$.

Karena tak tereduksi dan prima ekivalen di $\mathbb{Z}[\mathbb{i}]$, jadi didapatkan p bilangan prima Gauss jika dan hanya jika $p \equiv 3\ (mod\ 4)$. ■

Contoh 2.7.1

1. Contoh bilangan prima biasa yang merupakan bilangan prima Gauss adalah 3, 7, dan 11 karena bilangan-bilangan tersebut tidak dapat ditulis menjadi perkalian dua bilangan yang bukan unit.
2. Contoh bilangan prima biasa yang bukan bilangan prima Gauss adalah 2 dan 5 karena $2 = (1 + i)(1 - i)$ dan $5 = (1 + 2i)(1 - 2i)$.

Bila p merupakan bilangan prima Gauss, maka $-p,\ ip$ dan $-ip$ juga merupakan bilangan prima Gauss. Hal tersebut akan dituangkan pada teorema berikut.

Teorema 2.7.3 (Maulana, Wardhana, Switrayni dan Aini, 2018)
Jika p sebarang bilangan prima Gauss, maka $-p, ip$ dan $-ip$ juga bilangan prima Gauss.

Bukti. Karena p prima Gauss, maka setiap faktor $p = ab$ hanya terpenuhi bila a unit atau b unit. Tanpa mengurangi keumuman, misalkan hanya a merupakan unit. Perhatikan bahwa $-p = (-1)ab = (-a)b,\ ip = iab = (ia)b$ dan $-ip = (-i)ab = (-ia)b$. Karena himpunan unit di $\mathbb{Z}[i]$ tertutup terhadap perkalian, maka $-a, ia$ dan $-ia$ juga unit di $\mathbb{Z}[i]$. Jadi $-p, ip$ dan $-ip$ juga merupakan bilangan prima Gauss. ■

Bila p merupakan bilangan prima Gauss, maka konjugat dari p juga merupakan bilangan prima Gauss. Hal tersebut akan dituangkan pada teorema berikut.

Teorema 2.7.4 (Maulana, Wardhana, Switrayni, 2019)

Jika $p = a + ib$ sebarang bilangan prima Gauss, maka $\overline{p} = a - ib$ juga bilangan prima Gauss.

Bukti. Misalkan $\overline{p} = \alpha\beta$. Perhatikan bahwa $p = \overline{\overline{p}} = \overline{\alpha}\,\overline{\beta}$, karena p prima Gauss maka $\overline{\alpha}$ atau $\overline{\beta}$ unit di $\mathbb{Z}[i]$. Karena unit di $\mathbb{Z}[i]$ hanya $1, -1, i$ dan $-i$, berakibat α atau β juga unit di $\mathbb{Z}[i]$. Jadi $\overline{p}$ merupakan bilangan prima Gauss.

Dari contoh 2.7.1, diketahui bahwa 5 bukan merupakan bilangan prima Gauss karena $5 = (1 + 2i)(1 - 2i)$ dimana keduanya bukan unit, tetapi $(1 + 2i)$ dan $(1 - 2i)$ merupakan bilangan prima Gauss karena normanya merupakan bilangan prima biasa. Hal tersebut akan dijelaskan dalam teorema berikut.

Teorema 2.7.5 (Maulana, Wardhana, Switrayni, 2019)

Misalkan $\alpha = a + ib \in Z[i]$, jika $N(\alpha)$ merupakan bilangan prima di $\mathbb{Z}$ maka α merupakan bilangan prima Gauss.

Bukti. Misalkan $\alpha = \beta\,\gamma$, dimana $\beta, \gamma \in Z[i]$. Dengan mencari normanya, diperoleh $N(\alpha) = N(\beta)N(\gamma)$, karena $N(\alpha)$ merupakan bilangan prima maka haruslah $N(\beta)$ atau $N(\gamma)$ unit. Diketahui bahwa normanya merupakan suatu bilangan bulat tak negatif dan unit pada bilangan bulat hanya 1 dan -1, sehingga diperoleh $N(\beta) = 1$ atau $N(\gamma) = 1$ berakibat β atau γ merupakan unit di $\mathbb{Z}[i]$. Jadi α merupakan bilangan prima Gauss. ■

Teorema 2.7.6 (Maulana, Wardhana, Switrayni, 2019)
Misalkan $\alpha = a + ib \in Z[i], a,b \neq 0$, jika α merupakan bilangan prima Gauss, maka $N(\alpha)$ merupakan bilangan prima di $\mathbb{Z}$.

Bukti. Misalkan α prima Gauss, diperoleh juga $\overline{\alpha}$ prima Gauss. Andaikan $N(\alpha)$ bukan prima di $\mathbb{Z}$, maka $N(\alpha) = p_1 p_2 ... p_n$ dimana $p_1, p_2, ..., p_n$ prima di $\mathbb{Z}$. Bila $p_1, p_2, ..., p_n$ dibagi 4, maka akan bersisa 1, 2 atau 3.

Untuk $p_i \equiv 1 \ (mod\ 4)$, suatu $i \in \{1,2,...,n\}$ berdasarkan teorema Fermat maka $p_i = (c^2 + d^2) = (c + id)(c - id)$, karena normanya prima di $\mathbb{Z}$ diperoleh juga $(c + id)$ prima Gauss. Perhatikan bahwa $p_i | N(\alpha)$ dan $(c + id) | p_i$ berakibat $(c + id) | N(\alpha)$. Karena $c + id$ prima Gauss dan $N(\alpha) = \alpha\overline{\alpha}$, maka $(c + id) | \alpha$ atau $(c + id) | \overline{\alpha}$, dimana α dan $\overline{\alpha}$ tidak berasosiasi dengan $c + id$ karena $N(\alpha) = N(\overline{\alpha}) \neq p_i = N(c + id)$.

Untuk $p_j \equiv 2 \ (mod\ 4)$, suatu $j \in \{1,2,...,n\}$, diperoleh $p_j = 2 = (1 + i)(1 - i)$. Perhatikan bahwa $p_j | N(\alpha)$ dan $(1 + i) | p_j$ berakibat $(1 + i) | N(\alpha)$. Karena $1 + i$ prima Gauss dan $N(\alpha) = \alpha\overline{\alpha}$, maka $(1 + i) | \alpha$ atau $(1 + i) | \overline{\alpha}$, dimana α dan $\overline{\alpha}$ tidak berasosiasi dengan $1 + i$ karena $N(\alpha) = N(\overline{\alpha}) \neq p_j = N(1 + i)$.

Untuk $p_k \equiv 3 \ (mod\ 4)$, suatu $k \in \{1,2,...,n\}$, berdasarkan teorema 2.7.2 maka p_k merupakan prima Gauss. Karena $p_k | N(\alpha)$ dan $(\alpha) = \alpha\overline{\alpha}$ maka $p_k | \alpha$ atau $p_k | \overline{\alpha}$, dimana α dan $\overline{\alpha}$ tidak berasosiasi dengan p_k karena α maupun $\overline{\alpha}$ bagian *real*, imajinernya tak nol dan p_k bilangan prima Gauss yang bulat.

Berdasarkan ketiga kasus tersebut, akan selalu bisa ditemukan bilangan prima Gauss yang tidak berasosiasi dengan α dan $\overline{\alpha}$, dimana bilangan prima Gauss tersebut merupakan faktor dari α atau $\overline{\alpha}$. Akibatnya α bukan bilangan prima Gauss atau $\overline{\alpha}$ bukan prima Gauss. Kontradiksi dengan α dan $\overline{\alpha}$ prima Gauss. Pengandaian salah, jadi haruslah $N(\alpha)$ merupakan prima di $\mathbb{Z}$. ■

Contoh 2.7.2

Bilangan $(1 + i)$, $(1 - i)$ merupakan bilangan prima Gauss karena $N(1 + i) = N(1 - i) = 2$ merupakan bilangan prima biasa.

Bentuk umum bilangan prima Gauss diberikan dalam teorema berikut.

Teorema 2.7.7 (Maulana, Wardhana, Switrayni, 2019)

Misalkan $\alpha = a + ib \in Z[i]$, α memenuhi salah satu sifat berikut

1. *Untuk $a \neq 0, b = 0$, a bilangan prima di $\mathbb{Z}$ dan $|a| \equiv 3 \ (mod\ 4)$.*

2. *Untuk* $a = 0, b \neq 0$, *b bilangan prima di* $\mathbb{Z}$ *dan* $|b| \equiv 3 \ (mod\ 4)$.

3. *Untuk* $a, b \neq 0$, $a^2 + b^2$ *merupakan bilangan prima di* $\mathbb{Z}$.

Jika dan hanya jika α *merupakan bilangan prima Gauss.*

Bukti. Untuk sifat (1) dan (2), merupakan akbiat dari teorema 2.7.2 dan 2.7.3. Sifat (3), merupakan akibat dari teorema 2.7.5 dan 2.7.6 ■

2.8 Bilangan Bulat Gauss Modulo

Pada ring bilangan bulat terdapat bilangan bulat modulo, hal ini berlaku juga pada bilangan bulat Gauss terdapat bilangan bulat Gauss modulo. Berikut definisinya.

Definisi 2.8.1 (Wardhana, Astuti, Muchtadi-Alamsyah 2016)

Ring bilangan bulat Gauss modulo $\mathbb{Z}_n = \{a + ib | a,b \in \mathbb{Z}_n\}$.

Untuk lebih jelasnya berikut diberikan beberapa contoh ring bilangan bulat Gauss modulo

Contoh 2.8.1

- $\mathbb{Z}_2[i] = \{\overline{0},\overline{1},\overline{i},\overline{1+i}\}$
- $\mathbb{Z}_3[i] = \{\overline{0}, \overline{1},\overline{2},\overline{i},\overline{1+i},\overline{2+i},\overline{2i},\overline{1+2i},\overline{2+2i}\}$
- $\mathbb{Z}_4[i] =$
  $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{i}, \overline{1+i}, \overline{2+i},\overline{3+i},\overline{2i},\overline{1+2i},\overline{2+2i},\overline{3+2i},\overline{3i}, \overline{1+3i}, \overline{2+3i}, \overline{3+3i}\}$

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

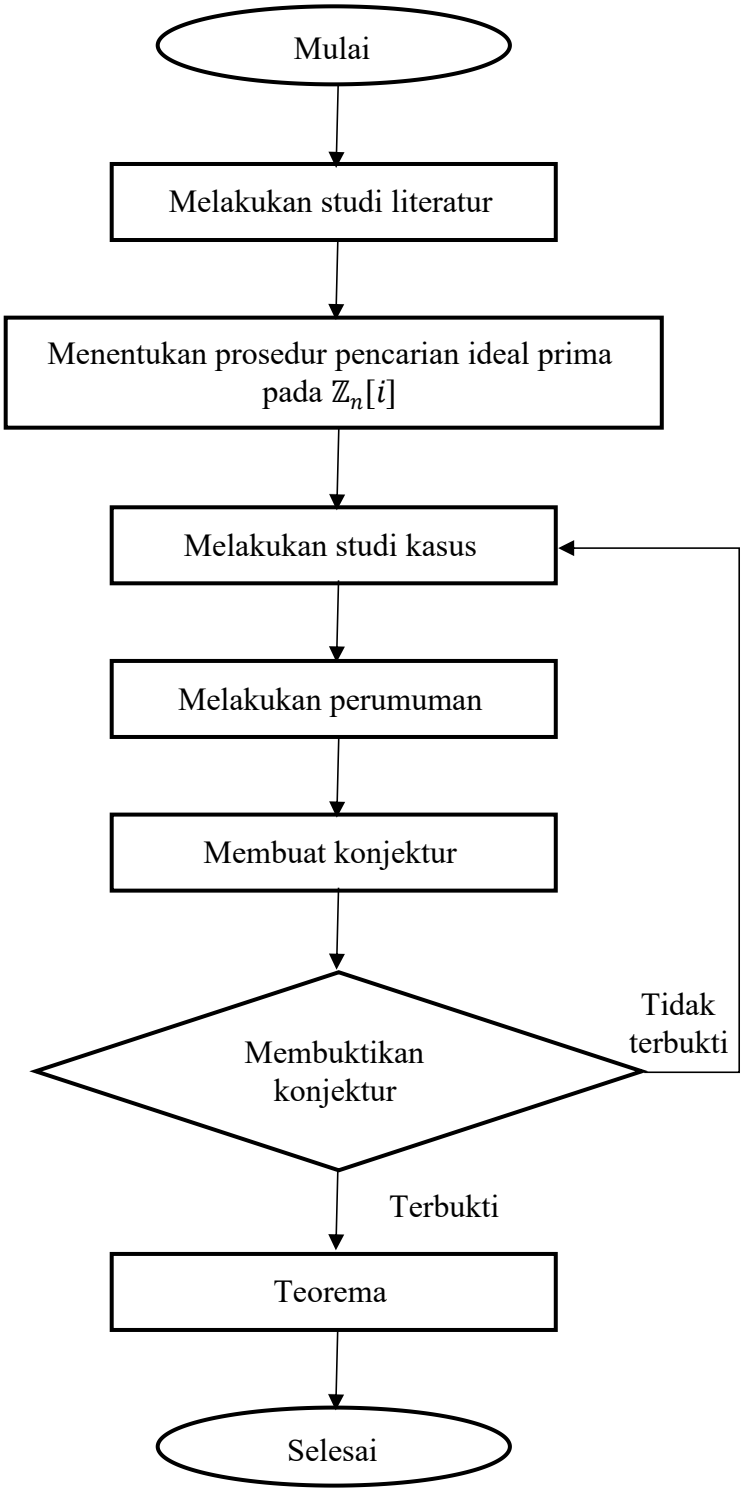
Jenis penelitian dalam tulisan ini adalah kajian pustaka (studi literatur), yaitu dilakukan dengan mempelajari buku-buku, maupun sumber bacaan lain yang berkaitan dengan judul yang diangkat oleh penulis. Penelitian dilakukan dengan membaca, mengkaji dan memahami referensi yang berasal dari buku maupun sumber bacaan yang lain seperti majalah, jurnal, dan makalah-makalah yang memuat topik ataupun materi yang berkaitan dengan grup, ring, bilangan prima, ideal prima, serta beberapa teori yang dibutuhkan untuk menunjang skripsi ini.

3.2 Langkah-Langkah Penelitian

Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah :

1. Melakukan studi literatur, yaitu mencari dan mempelajari sumber literatur yang berhubungan dengan grup, ring, bilangan prima, ideal prima, dan serta beberapa teori yang dibutuhkan untuk menunjang penelitian ini.
2. Menentukan prosedur pencarian ideal prima pada $\mathbb{Z}_n[i]$ untuk mendapatkan gambaran secara umum.
3. Melakukan studi kasus, yaitu mencari contoh dan mengelompokkan ideal prima pada $\mathbb{Z}_n[i]$, mempelajari bentuk-bentuknya, sehingga dapat diperumum.
4. Membuat perumuman, yaitu merumuskan ideal prima pada $\mathbb{Z}_n[i]$ secara umum.
5. Membuat konjektur, yakni menduga karakteristik ideal prima pada $\mathbb{Z}_n[i]$.
6. Membuktikan konjektur, yakni membuktikan dugaan sehingga didapatkan karakteristik ideal prima pada $\mathbb{Z}_n[i]$.

Adapun langkah-langkah yang akan dilakukan dalam penelitian ini bisa diamati dalam bagan berikut :



Gambar 3.2.1 Bagan langkah-langkah

BAB IV

PEMBAHASAN

Pada bagian ini akan dibahas beberapa contoh ideal prima pada bilangan bulat Gauss modulo kemudian menemukan sifat-sifat yang dimiliki.

Setiap ring tak nol R memiliki paling sedikit dua ideal, ideal tidak sejati R dan ideal trivial $\{0\}$. Ideal yang dibangun oleh 0 pada ring bilangan bulat Gauss merupakan ideal prima. Namun hal ini belum tentu berlaku pada bilangan bulat Gauss modulo.

Contoh 4.2

1. Ideal $\langle\bar{0}\rangle$ bukan merupakan ideal prima pada $\mathbb{Z}_2[i]$ karena $\overline{(1+i)}\overline{(1+i)} = \bar{0} \in \langle\bar{0}\rangle$ tetapi $\overline{(1+i)} \notin \langle\bar{0}\rangle$.
2. Ideal $\langle\bar{0}\rangle$ merupakan ideal prima pada $\mathbb{Z}_3[i]$.
3. Ideal $\langle\bar{0}\rangle$ bukan merupakan ideal prima pada $\mathbb{Z}_4[i]$ karena $\bar{2} \cdot \bar{2} = \bar{0} \in \langle\bar{0}\rangle$ tetapi $\bar{2} \notin \langle\bar{0}\rangle$.

Pada ring bilangan bulat Gauss modulo dimana setiap anggotanya dipandang pada ring bilangan bulat Gauss dan saling prima dengan modulonya, maka ideal yang dibangun akan sama dengan ring bilangan bulat Guass modulo itu sendiri. Berikut teorema yang diberikan.

Teorema 4.1

Misalkan $I = \langle\bar{a}\rangle$ *ideal dari* $\mathbb{Z}_n[i]$. $(a,n) = 1$ *maka* $I = \mathbb{Z}_n[i]$.

Bukti. Karena $(a,n) = 1$ maka terdapat $p,q \in Z[i]$ sehingga $pa + qn = 1$ atau $pa = 1 - qn$. Dengan membagi kedua ruas dengan n, diperoleh $\overline{pa} = \bar{1} - \overline{qn}$ atau $\overline{pa} = \bar{1} - \bar{0}$. Artinya $\bar{1} = \overline{pa}$, sehingga $\bar{1} = \bar{p}(\bar{a}) \in \langle\bar{a}\rangle$. Karena $\bar{1}$ merupakan unit di $\mathbb{Z}_n[i]$ maka berdasarkan Teorema 2.2.1 diperoleh $I = \mathbb{Z}_n[i]$. ■

Akibat dari Teorema 4.1, pada ring bilangan bulat Gauss modulo dengan n merupakan prima Gauss, maka $\langle\bar{a}\rangle = \mathbb{Z}_n[i]$ untuk setiap $\bar{a} \in \mathbb{Z}_n[i]$ tak nol. Lebih

jauh untuk $\mathbb{Z}_n[i]$ dengan n prima Gauss, ideal-ideal dari $\mathbb{Z}_n[i]$ hanya 0 dan $\mathbb{Z}_n[i]$ atau berdasarkan Teorema 2.2.2 $\mathbb{Z}_n[i]$ merupakan lapangan. Disisi lain ideal yang dibangun oleh $\bar{0}$ merupakan ideal maksimal dan satu-satunya ideal prima pada $\mathbb{Z}_n[i]$ dengan n prima Gauss.

Pada ring bulat Gauss modulo, dua atau lebih ideal memiliki anggota yang sama. Sebagai contoh berikut diberikan ideal-ideal sejati pada $\mathbb{Z}_4[i]$.

Tabel 4.1 Ideal-ideal sejati $\mathbb{Z}_4[i]$.

Ideal sejati pada $\mathbb{Z}_4[i]$	Anggota
$\langle\bar{2}\rangle$	$\bar{0}, \bar{2}, \bar{2}i, \overline{2+2i}$
$\langle\bar{2}i\rangle$	$\bar{0}, \bar{2}, \bar{2}i, \overline{2+2i}$
$\langle\overline{1+i}\rangle$	$\bar{0}, \bar{2}, \overline{1+i}, \overline{3+i}, \bar{2}i, \overline{2+2i}, \overline{1+3i}, \overline{3+3i}$
$\langle\overline{3+i}\rangle$	$\bar{0}, \bar{2}, \overline{1+i}, \overline{3+i}, \bar{2}i, \overline{2+2i}, \overline{1+3i}, \overline{3+3i}$
$\langle\overline{2+2i}\rangle$	$\bar{0}, \overline{2+2i}$
$\langle\overline{1+3i}\rangle$	$\bar{0}, \bar{2}, \overline{1+i}, \overline{3+i}, \bar{2}i, \overline{2+2i}, \overline{1+3i}, \overline{3+3i}$
$\langle\overline{3+3i}\rangle$	$\bar{0}, \bar{2}, \overline{1+i}, \overline{3+i}, \bar{2}i, \overline{2+2i}, \overline{1+3i}, \overline{3+3i}$

Berdasarkan Tabel 4.1, pada $\mathbb{Z}_4[i]$ diperoleh $\langle\bar{2}\rangle = \langle\bar{2}i\rangle$ dan $\langle\overline{1+i}\rangle = \langle\overline{3+i}\rangle = \langle\overline{1+3i}\rangle = \langle\overline{3+3i}\rangle$. Secara umum untuk ideal $I = \langle\bar{a}\rangle$ pada $\mathbb{Z}_n[i]$, maka $\langle\bar{a}\rangle = \langle\bar{b}\rangle$ jika $(a,n) = (b,n)$ yang diberikan oleh teorema berikut.

Teorema 4.2

Diberikan $I = \langle\bar{a}\rangle$ *ideal dari* $\mathbb{Z}_n[i]$. *Jika* $(a,n) = p$ *maka* $\langle\bar{a}\rangle = \langle\bar{p}\rangle$.

Bukti. Misalkan $(a,n) = p$ maka $p|a$ dan $p|n$. Untuk $\bar{x} \in \langle\bar{a}\rangle$ diperoleh $\bar{x} = \overline{ka}$ atau $\bar{x} - \overline{ka} = \bar{0}$ untuk suatu $k \in \mathbb{Z}_n[i]$. Akibatnya diperoleh $x - ka = ln$ atau

$x = ka + ln$ sehingga $x = krp + lsp = (kr + ls)p$ untuk suatu $r,s \in \mathbb{Z}_n[i]$. Dengan demikian $\bar{x} = (\overline{kr + ls})\bar{p} \in \langle \bar{p} \rangle$. Sebaliknya untuk $\bar{x} \in \langle \bar{p} \rangle$, maka $\bar{x} = \overline{kp}$ atau $\bar{x} - \overline{kp} = \bar{0}$. Akibatnya $x - kp = ln$ atau $x = ln + kp$. Karena $(a,n) = p$ diperoleh $ra + sn = p$ untuk suatu $r,s \in Z[i]$ sehingga $x = ln + k(ra + sn) = ln + kra + ksn$. Dengan demikian $\bar{x} = \overline{kra}$ atau $\bar{x} = \overline{kr}(\bar{a}) \in \langle \bar{a} \rangle$. Jadi $\langle \bar{a} \rangle = \langle \bar{p} \rangle$. ■

Akibatnya untuk $(a,n) = (b,n) = p$ maka $\langle \bar{a} \rangle = \langle \bar{b} \rangle$. Contohnya $(4,10) = (6,10) = (8,10) = 2$ sehingga $\langle \bar{4} \rangle = \langle \bar{6} \rangle = \langle \bar{8} \rangle$ pada $\mathbb{Z}_{10}[i]$.

Ideal-ideal pada ring bilangan bulat Gauss modulo tidak hanya dibangun oleh satu unsur seperti contoh pada Tabel 4.1. Ideal lain pada $\mathbb{Z}_4[i]$ yang dibangun oleh 2 unsur yaitu $I = \langle \bar{2},\bar{i} \rangle = \{2\alpha + i\beta | \alpha,\beta \in \mathbb{Z}_4\} = \{\bar{0},\bar{2},\bar{i},\overline{2 + i},\overline{2i},\overline{2 + 2i},\overline{3i},\overline{2 + 3i}\}$.

Di bawah ini beberapa contoh ideal tak nol yang merupakan ideal prima dan bukan ideal prima pada ring bilangan bulat Gauss modulo.

Contoh 4.2

1. Ideal $I = \langle \bar{3} \rangle$ merupakan ideal prima pada $\mathbb{Z}_6[i]$.
2. Ideal $I = \langle \bar{3} \rangle$ bukan merupakan ideal prima pada $\mathbb{Z}_5[i]$ karena $\langle \bar{3} \rangle = \mathbb{Z}_5[i]$.
3. Ideal $I = \langle \bar{2} \rangle$ bukan merupakan ideal prima pada $\mathbb{Z}_4[i]$ karena $(\overline{1 + i})(\overline{1 + i}) = 2i \in \langle 2 \rangle$ tetapi $(1 + i) \notin \langle 2 \rangle$.
4. Ideal $I = \langle \overline{1 + i} \rangle$ merupakan ideal prima pada $\mathbb{Z}_2[i]$.
5. Ideal $I = \langle \overline{3 + 3i} \rangle$ bukan merupakan ideal prima pada $\mathbb{Z}_6[i]$ karena $\bar{3}(\overline{1 + i}) = \overline{3 + 3i} \in \langle \overline{3 + 3i} \rangle$ tetapi $\bar{3},\overline{1 + i} \notin \langle \overline{3 + 3i} \rangle$.

Dari beberapa contoh tersebut, ideal prima pada ring bilangan bulat Gauss modulo ditentukan oleh faktor-faktor prima pada ring bilangan bulat Gauss. Berikut ini tabel faktor beberapa n pada ring bilangan bulat Gauss.

n	$faktor\ prima\ di\ Z$	$faktor\ prima\ di\ Z[i]$
2	2	$(1 + i)(1 - i)$
3	3	3
4	2^2	$(1 + i)^2(1 - i)^2$

5	5	$(1+2i)(1-2i)$
6	2.3	$(1+i)(1-i)3$
7	7	7
8	2^3	$(1+i)^3(1-i)^3$
9	3^2	3^2
10	2.5	$(1+i)(1-i)\,(1+2i)(1-2i)$
11	11	11
12	$2^2.3$	$(1+i)^2(1-i)^2 3$
Dst.	…	…

Tabel 4.2 Faktorisasi n pada $\mathbb{Z}[i]$.

Dari contoh dan tabel di atas, dapat dibuat konjektur/dugaan bahwa suatu ideal yang dibangun oleh suatu anggota ring bilangan bulat Gauss modulo n yang memiliki faktor persekutuan terbesar dengan n berupa bilangan prima Gauss merupakan ideal prima. Konjektur ini telah dibuktikan menjadi suatu teorema sebagai berikut.

Teorema 4.3

Misalkan $I = \langle \bar{a} \rangle$ ideal tak nol pada $\mathbb{Z}_n[i]$. Jika $(a,n) = p$ merupakan prima Gauss maka $I = \langle \bar{a} \rangle$ merupakan ideal prima.

Bukti. Jelas $\langle \bar{a} \rangle \neq \mathbb{Z}_n[i]$. **Kasus 1**. Misalkan a prima Gauss maka haruslah $a = p$ prima Gauss sehingga $a|n$ atau $n = aq$. Artinya untuk sebarang $\overline{xy} \in \langle \bar{a} \rangle$ maka $\overline{xy} = \overline{ka}$. Akibatnya $xy - ka = ln$ atau $xy = ka + ln$. Karena $n = aq$ maka $xy = ka + laq = (k + lq)(a)$. Karena a prima Gauss haruslah $a|x$ atau $a|y$, diperoleh $\bar{x} \in \langle \bar{a} \rangle$ atau $\bar{y} \in \langle \bar{a} \rangle$ dengan demikian I merupakan ideal prima. **Kasus 2**. Misalkan a bukan prima Gauss dan karena $(a,n) = p$ maka menurut Teorema 4.2 diperoleh $\langle \bar{a} \rangle = \langle \bar{p} \rangle$. Berdasarkan kasus 1, $\langle \bar{p} \rangle$ merupakan ideal prima. Dengan demikian $\langle \bar{a} \rangle$ juga merupakan ideal prima. ■

Berdasarkan definisi ideal hampir prima, jika I ideal prima maka I juga ideal hampir prima. Berikut teorema yang diberikan.

Teorema 4.4

Misalkan $I = \langle \bar{a} \rangle$ *ideal tak nol pada* $\mathbb{Z}_n[i]$. *Jika* I *ideal prima maka* I *juga ideal hampir prima.*

Bukti. Misalkan $\overline{xy} \in I - I^2$ sebarang. Karena $I - I^2 \subset I$ dan I ideal prima maka jelas $\bar{x} \in I$ atau $\bar{y} \in I$. ■

Pada ring bilangan bulat Gauss berlaku I ideal prima jika dan hanya jika I ideal hampir prima. Namun hal ini tidak berlaku pada ring bilangan bulat Gauss modulo, sebagai contoh pada $\mathbb{Z}_{12}[i]$, $I = \langle \bar{4} \rangle$ merupakan ideal hampir prima karena $I - I^2 = \langle \bar{4} \rangle - \langle \bar{4} \rangle = \{\emptyset\}$, namun I bukan ideal prima.

BAB V

PENUTUP

Pada bab ini akan diberikan kesimpulan dan saran yang dapat diambil berdasarkan materi-materi yang telah dibahas sebelumnya.

5.1 Kesimpulan

Penelitian ini menghasilkan karakteristik ideal prima pada ring bilangan bulat Gauss modulo yaitu :

1. Misalkan $I = \langle \bar{a} \rangle$ ideal tak nol pada $\mathbb{Z}_n[i]$. Jika $(a,n) = p$ merupakan prima Gauss maka $I = \langle \bar{a} \rangle$ merupakan ideal prima.
2. Misalkan $I = \langle \bar{a} \rangle$ ideal tak nol pada $\mathbb{Z}_n[i]$. Jika I ideal prima maka I juga ideal hampir prima.

5.2 Saran

Setelah membahas ideal siklik prima pada ring bilangan bulat Gauss modulo, penulis berharap pembaca atau peneliti selanjutnya dapat mengembangkan dalam hal karakteristik ideal non siklik prima pada ring bilangan bulat Gauss modulo.

DAFTAR PUSTAKA

Bhatwadekar, S. M., Sharma, S.K., 2009, *Unique Factorization and Birth of Almost Prime*, Communication in Algebra, 33(1) :43-49.

Dummit, S. D., Foote, M. R., 2004, *Abstract Algebra Third Edition.* New York : John Wiley & Sons, Inc.

Fraleigh, J. B., 2014, *A First Course in Abstract Algebra Seventh Edition*, United States of America : Pearson Education Limited.

Ivy, B.P.U., Mandiwa, P., Kumar, M., 2012, A Modified RSA Cryptosystem Based On 'n' Prime Numbers, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66

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.

Maulana, F., Wardhana, I. G. A. W., Switrayni, N. W., 2019, *Ekivalensi Ideal Prima dan Ideal Hampir Prima pada Bilangan Bulat Gauss,* Eigen Mathematics Journal Volume 2 No. 1 : 1-5.

Rahim, R., Winata, H., Zulkarnain, I., Jaya, H., 2017, *Prime Number: an Experiment Rabin-Miller and Fast Exponentiation*, Journal of Physics: Conf. Series **930** (2017) 012032

Roman, S., 2008, *Advanced Linier Algebra Third Edition,* New York : Springer.

Romdhini, M. U., Irwansyah., Switrayni, N. W., 2016, *Struktur Aljabar,* Mataram : Universitas Mataram.

Wardhana, I. G. A. W., Astuti, P., Muchtadi-Alamsyah, I., 2016, *On Almost Prime Submodule of a finetly Generated Module Over Principal Ideal Domain*, JP Journal of Algebra, Number Theory and Aplications: 121-128.