Volume 2 No 1 Juni (2019)

e-ISSN: **2615-3270**

p-ISSN: **2615-3599**

Eigen Mathematics Journal

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

# Ekivalensi Ideal Hampir Prima dan Ideal Prima pada Bilangan Bulat Gauss

***Fariz Maulana*[a,*]*, I Gede Adhitya Wisnu Wardhana*[b]*, Ni Wayan Switrayni*[c]**

[a,*] Program Studi Matematika FMIPA Universitas Mataram, Jalan Majapahit no. 62, Mataram 83125, Indonesia. Email: farizholmes@gmail.com

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

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

A B S T R A C T

Cryptography is one branch of mathematics that is widely used in digital security systems. Cryptography itself is related to integers and their properties, especially prime numbers. More specifically, some important algorithms such as RSA, are very dependent on prime factorization of integers. Prime number abstraction was introduced by Dedekind in 1871, known as the prime ideal name. Bhatwadekar in 2009 generalize prime ideal and called almost prime ideal. This paper will prove that almost prime ideal and prime ideal in Gaussian integer are equivalent.

Keywords: almost prime ideals; Gaussian integers; prime ideals

A B S T R A K

Kriptografi adalah salah satu cabang ilmu matematika yang banyak digunakan pada sistem keamanan digital. Kriptografi itu sendiri berkaitan dengan bilangan bulat dan sifat-sifatnya, terutama bilangan prima. Lebih spesifik, beberapa algoritma penting seperti RSA, sangat bergantung pada faktorisasi prima dari bilangan bulat. Abstraksi bilangan prima diperkenalkan oleh Dedekind pada tahun 1871, dikenal dengan nama ideal prima. Ideal prima diperumum oleh Bhatwadekar pada tahun 2009 dan dinamakan ideal hampir prima. Paper ini akan membuktikan bahwa ideal hampir prima dan ideal prima di bilangan bulat Gasuss adalah ekivalen.

Kata kunci: bilangan bulat Gauss; ideal hampir prima; ideal prima

Diserahkan: 24-05-2019; Diterima: 27-06-2019; Doi: https://doi.org/10.29303/emj.v1i1.29

## 1. Pendahuluan

Bilangan prima adalah topik yang menarik dibahas pada teori kriptografi dan teori kode. Kriptografi itu

* Corresponding author.
Alamat e-mail: *farizholmes@gmail.com*

sendiri berkaitan dengan bilangan bulat dan sifat-sifatnya, terutama bilangan prima. Beberapa sifat bilangan prima di Bilangan Bulat Gauss telah dibahas oleh Maulana, dkk. (2018). Bilangan bulat Gauss merupakan bilangan kompleks yang bagian real dan imajinernya berupa bilangan bulat. Salah satu fakta menarik yang ditemukan adalah tidak semua bilangan prima pada himpunan bilangan bulat juga merupakan bilangan prima pada bilangan bulat Gauss. Bilangan prima pada bilangan bulat yang bersisa 3 saat dibagi dibagi 4 merupakan bilangan prima pada bilangan bulat Gauss.

Abstraksi bilangan prima diperkenalkan oleh Dedekind pada tahun 1871, dikenal dengan nama ideal prima. Bhatwadekar dan Sharma memperkenalkan perumuman ideal prima yang dinamakan ideal hampir prima. Abstraksi lain dari bilangan prima juga dilakukan di teori modul yang dan dengan istilah submodul prima dan submodul hampir prima (Wardhana dkk, 2012).

## 2. Bilangan Prima Gauss

Seperti halnya bilangan kompleks yang merupakan perluasan dari bilangan real, bilangan bulat Gauss juga meupakan perluasan dari bilangan bulat.

**Definisi 2.1**

Bilangan bulat Gauss adalah suatu bilangan kompleks $a+ib$ dengan $a,b \in \mathbb{Z}$. Untuk bilangan bulat Gauss $\alpha = a+ib$, norma dari $\alpha$ ialah

$$N(\alpha) = a^2 + b^2$$

Dalam daerah integral, bilangan prima dan bilangan tak tereduksi dapat didefinisikan.

**Definisi 2.2**

Suatu elemen taknol dan bukan unit $p$ dari suatu daerah integral $D$ disebut bilangan tak tereduksi di $D$ jika setiap pemfaktoran $p = ab$ di $D$ hanya terpenuhi bila $a$ atau $b$ adalah unit (Fraleigh, 2014).

**Definisi 2.3**

Suatu elemen taknol dan bukan unit $p$ dari suatu daerah integral $D$ disebut prima jika untuk setiap $a,b \in D$ dengan $p \mid ab$ mengakibatkan $p|a$ atau $p|b$ (Fraleigh, 2014).

Himpunan bilangan prima dan himpunan bilangan tak tereduksi adalah dua hal yang sama pada daerah ideal utama.

**Teorema 2.1**

Misalkan $D$ daerah ideal utama, bilangan $p \in D$ prima jika hanya jika $p$ tak tereduksi (Roman, 2008).

**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 $< p >$ ideal maksimal. Akibatnya $< p, a > = < p >$ atau $< p, a > = D = < 1 >$. Untuk $< p, a > = < p >$ diperoleh $p|a$. Untuk $< p, a > = D = < 1 >$ 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. ■

Himpunan bilangan bulat Gauss merupakan daerah ideal utama, sehingga himpunan bilangan prima Gauss dan himpunan bilangan tak tereduksi adalah dua hal yang sama

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

**Teorema 2.2 (Teorema Fermat $p = a^2 + b^2$)**

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

**Bukti.** Misalkan $p$ prima ganjil dan $p = a^2 + b^2$, $a,b \in \mathbb{Z}$. 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 $p - 1$, kita dapatkan $\mathbb{Z}_p - \{0\}$ mengandung suatu elemen $n$ berorde 4. Itu berakibat $n^2$ berorde 2, sehingga $n^2 = -1 = p - 1$ di $\mathbb{Z}_p$. Selanjutnya di $\mathbb{Z}$ kita dapatkan $n^2 \equiv -1\ mod\ p$, jadi $p$ membagi $n^2 + 1$ di $\mathbb{Z}$.

Pandang $p$ dan $n^2 + 1$ di $\mathbb{Z}[i]$, kita dapatkan $p$ 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 $a, b \in \mathbb{Z}$. Kita dapatkan $pb = 1$, tidak dapat terjadi karena $p$ bilangan prima ganjil. Begitu pula jika $p$ membagi $(n - i)$ maka $(n - i) = p\,(c + id)$ untuk suatu $c, d \in \mathbb{Z}$ Kita dapatkan $pd = -1$, 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 kita dapatkan $p = (a^2 + b^2) = (a + ib)(a - ib)$ dengan $(a - ib) = (c + id)$.■

Teorema di atas digunakan untuk menentukan bilangan prima yang merupakan bilangan prima Gauss. Hal tersebut diberikan oleh teorema berikut.

**Teorema 2.3**

Diberikan $p$ suatu bilangan prima ganjil di $\mathbb{Z}$, $p$ merupakan bilangan prima Gauss jika dan hanya jika $p \equiv 3\ (mod\ 4)$ (Maulana dkk, 2018).

**Bukti.** Dari Teorema Fermat, didapatkan fakta bahwa Suatu bilangan prima ganjil $p \neq a^2 + b^2$ untuk setiap $a, b \in \mathbb{Z}$ 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 $p \equiv 3(mod\ 4)$.

Sebaliknya, karena $p$ tidak dapat ditulis dalam bentuk $(a + ib)(a - ib) = a^2 + b^2$, maka $p$ hanya dapat ditulis dalam bentuk $p = p.1$ atau $p = (-p)(-1)$ atau $p = ip(-i)$ atau $p = (-ip)i$. Karena$1, -1, i, -i$ merupakan unit di $\mathbb{Z}[i]$, berimplikasi $p$ bilangan prima Gauss■

**Contoh 1.**

1. Contoh bilangan prima 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 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 2.4**

Jika $p$ sebarang bilangan prima Gauss, maka $-p, ip$ dan $-ip$ juga bilangan prima Gauss (Maulana, 2018).

**Bukti**. Karena $p$ prima Gauss, maka setiap faktor $p = ab$ hanya terpenuhi bila $a$ unit atau $b$ unit. Tanpa mengurangi keumuman, misalkan $a$ 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. ■

Teorema 2.3 memberikan cara untuk melihat apakah bilangan prima merupakan bilangan prima Gauss, Teorema 2.4 memberikan variasi bilangan prima Gauss lain. Teorema berikut memberikan

kemudahan untuk mengenali bilangan prima Gauss yang lebih komplek

**Teorema 2.5**

Misalkan $\alpha = a + ib \in \mathbb{Z}[i], a, b \neq 0$, jika $N(\alpha)$ merupakan bilangan prima di $\mathbb{Z}$, maka $\alpha$ merupakan bilangan prima Gauss (Fraleigh, 2014).

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

**Contoh 2.2**

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

Bentuk umum bilangan prima Gauss diberikan dalam teorema berikut.

**Teorema 2.6**

Misalkan $\alpha = a + ib \in \mathbb{Z}[i]$ memenuhi salah satu sifat berikut

1. Untuk $a \neq 0, b = 0$, Bilangan $\alpha$ merupakan bilangan prima Gauss jika dan hanya jika $a$ bilangan prima di $\mathbb{Z}$ dan $|a| \equiv 3\ (mod\ 4)$.
2. Untuk $a = 0, b \neq 0$, Bilangan $\alpha$ merupakan bilangan prima Gauss jika dan hanya jika $b$ bilangan prima di $\mathbb{Z}$ dan $|b| \equiv 3\ (mod\ 4)$.
3. Untuk $a, b \neq 0$, Bilangan $\alpha$ merupakan bilangan prima Gauss jika dan hanya jika $a^2 + b^2$ merupakan bilangan prima di $\mathbb{Z}$.

Maka $\alpha$ bilangan prima Gauss.

**Bukti.** Berdasarkan teorema 2.1 dan 2.3 jelas sifat (1) dan (2) terbukti. Sedangkan berdasarkan teorema 2.4 jelas sifat (3) terbukti. ■

## 3. Ideal Prima dan Ideal Hampir Prima

Abstraksi bilangan prima pada gelanggang diperkenalkan oleh Dedekind pada tahun 1871, yakni ideal prima yang definisinya diberikan sebagai berikut.

**Definisi 3.1**

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

**Contoh 2.**

Ideal $I =< (1 + i) >$ dan $J =< 3i >$ merupakan ideal prima dari gelanggang bilangan bulat Gauss.

1. Ideal $I =< 2 >$ bukan merupakan ideal prima dari gelanggang bilangan bulat Gauss.
   Penyangkal. Terdapat $3 + 3i, 5 + 5i \in \mathbb{Z}[i]$ dimana $(3 + 3i)(5 + 5i) = 30i \in < 2 >$, tetapi $3 + 3i \notin < 2 >$ dan $5 + 5i \notin < 2 >$.
2. Ideal $I =< 5i >$ bukan merupakan ideal prima dari gelanggang bilangan bulat Gauss.
   Penyangkal. Terdapat $1 + 2i, 2 + i \in \mathbb{Z}[i]$ dimana $(1 + 2i)(2 + i) = 5i \in < 5i >$, tetapi $1 + 2i \notin < 5i >$ dan $2 + i \notin < 5 >$.

Ideal yang dibangun oleh 0 merupakan ideal prima sekaligus ideal hampir prima. Untuk ideal yang tak nol, karakteristik ideal prima diberikan pada Teorema berikut.

**Teorema 3.1**

Misalkan ideal tak nol $I =< p >$, Ideal $I$ merupakan ideal prima pada gelanggang bilangan bulat Gauss jika dan hanya jika $p$ merupakan bilangan prima Gauss.

**Bukti.** Misalkan $\alpha, \beta \in \mathbb{Z}[i]$ dimana $p|\alpha\beta$, maka diperoleh $\alpha\beta \in < p >$. Karena $< p >$ ideal prima maka diperoleh $\alpha \in < p >$ atau $\beta \in < p >$. Akibatnya $p|\alpha$ atau $p|\beta$. Jadi $p$ bilangan prima Gauss.
Sebaliknya, ambil $\alpha, \beta \in \mathbb{Z}[i]$ dimana $\alpha\beta \in < p >$ artinya $p|\alpha\beta$. Karena $p$ bilangan prima Gauss maka diperoleh $p|\alpha$ atau $p|\beta$, diperoleh $\alpha \in < p >$ atau $\beta \in < p >$. Jadi $I$ merupakan ideal prima pada ring bilangan bulat Gauss. ■

**Teorema 3.2**

Misalkan ideal tak nol $I =< p >$, Ideal $I$ merupakan ideal hampir prima pada gelanggang bilangan bulat Gauss jika dan hanya jika $p$ merupakan bilangan prima Gauss.

**Bukti.** Diberikan $< p >$ ideal hampir prima, andaikan $p$ bukan prima. Karena $p \neq 0$ bukan unit dan $\mathbb{Z}[i]$ merupakan daerah faktorisasi tunggal, maka $p$ dapat ditulis sebagai perkalian hingga bilangan-bilangan prima Gauss.

Misalkan $p = p_1 p_2 p_3 \dots p_n$ dimana $p_1, p_2, p_3, \dots, p_n$ merupakan bilangan prima Gauss.

Pilih $a = p_1 p_2$ dan $b = p_3 \dots p_n$, diperoleh $ab = p_1 p_2 p_3 \dots p_n \in < p > - < p^2 >$, tetapi $p_1 p_2 \notin < p >$ dan $p_3 \dots p_n \notin < p >$. Akibatnya $< p >$ bukan ideal hampir prima, kontradiksi dengan $< p >$ merupakan ideal hampir prima. Jadi haruslah $p$ merupakan bilangan prima Gauss.

Sebaliknya, diberikan $p$ bilangan prima Gauss. Berdasarkan teorema 3.1 maka $< p >$ merupakan ideal prima. Berdasarkan definisi ideal prima, maka jelas $< p >$ merupakan ideal hampir prima pada gelanggang bilangan bulat Gauss.■

Berdasarkan teorema-teorema di atas, diperoleh ideal prima dan ideal hampir prima adalah dua hal yang sama pada gelanggang bilangan bulat Gauss

**Teorema 3.3**

Misalkan $I$ ideal pada gelanggang bilangan bulat Gauss, Ideal $I$ merupakan ideal prima jika dan hanya jika $I$ merupakan ideal hampir prima.

**Bukti.** Untuk $I = 0$, jelas $I$ merupakan ideal prima dan juga ideal hampir prima.

Untuk $I \neq 0$, berdasarkan Teorema 3.1 dan 3.2 jelas $I$ ideal prima jika dan hanya jika $I$ ideal hampir prima

**Teorema 3.4**

Misalkan ideal tak nol $I =< a + ib >$ merupakan ideal pada gelanggang bilangan bulat Gauss. Jika $a + ib$ memenuhi salah satu sifat di bawah

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

Maka $I =< a + ib >$ merupakan ideal hampir prima.

**Bukti.** Berdasarkan Teorema 2.6 dan Teorema 3.2, jelas teorema ini terbukti. ■

## DAFTAR PUSTAKA


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

Fraleigh, John. (2014). *A First Course In Abstract Algebra, Seventh Edition.* United States of America : Pearson Education Limited.

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.

Roman, S. (2008). *Advanced Linier Algebra, Third Edition*. Newyork : Springer.

Wardhana, I.G.A.W., Astuti, P. Muchtadi-Alamsyah, I. *On Almost Prime Submodules of a Finitely Generated Free Module Over a Principal Ideal Domain*, AJP Journal of Algebra, Number Theory and Application, 38(2), 121–128.