II. TINJAUAN PUSTAKA

Pada bab ini akan diberikan beberapa definisi teori pendukung dalam proses penelitian untuk penyelesaian persamaan Diophantine dengan relasi kongruensi modulo *m* mengenai aljabar dan teori bilangan, yaitu tentang konsep keterbagian yang erat kaitannya dengan konsep modulo berikut merupakan penjelasan tentang konsep keterbagian.

2.1 Keterbagian

Definisi 2.1.1

Bilangan bulat *a* membagi habis bilangan bulat *b* (ditulis $a|b$) jika dan hanya jika ada bilangan bulat *k* sehingga $b = a \cdot k$. Jika *a* tidak membagi habis *b* maka ditulis $a \nmid b$ (Dudley, 1969).

Istilah lain untuk $a|b$ adalah *a* faktor dari b, a pembagi *b* atau *b* kelipatan dari *a*. Bila *a* pembagi *b* maka $-a$ juga pembagi *b*, sehingga pembagi suatu bilangan selalu terjadi berpasangan. Jadi dalam menentukan semua faktor dari suatu bilangan bulat cukup ditentukan faktor-faktor positifnya saja, kemudian tinggal menggabungkan faktor negatifnya. Fakta sederhana yang diturunkan langsung dari definisi adalah sebagai berikut:

$$a|0, 1|a, \text{dan } a|a \text{ untuk } a \neq 0$$

Fakta $a|0$ dapat dijelaskan bahwa bilangan 0 selalu habis dibagi oleh bilangan apapun yang tidak nol. Fakta $1|a$ mengatakan bahwa 1 merupakan faktor atau pembagi dari bilangan apapun termasuk bilangan 0. Fakta $a|a$ menyatakan bahwa bilangan tidak nol selalu habis membagi dirinya sendiri dengan hasil baginya adalah 1.

Berdasarkan pengertian keterbagian bilangan terdapat pada definisi 2.1.1, maka berikut ini akan diberikan teorema tentang keterbagian.

Teorema 2.1.1

Untuk setiap $a, b, c \in \mathbb{Z}$ berlaku pernyataan berikut :

1. $a|1$ jika dan hanya jika $a = 1$ atau $a = -1$.
2. Jika $a|b$ dan $c|d$ maka $ac|bd$.
3. Jika $a|b$ dan $b|c$ maka $a|c$.
4. $a|b$ dan $b|a$ jika dan hanya jika $a = b$ atau $a = -b$.
5. Jika $a|b$ dan $b \neq 0$, maka $|a| < |b|$.
6. Jika $a|b$ dan $a|c$, maka $a|(bx + cy)$ untuk sebarang bilangan bulat *x* dan *y*.

(Sukirman, 1997)

Bukti.

1. Jika $a = 1$ atau $a = -1$, maka jelas bahwa $a|1$, sesuai penjelasan sebelumnya. Sebaliknya, diketahui $a|1$ berarti ada $k \in \mathbb{Z}$ sehinga 1 = *ka*. Persamaan ini hanya dipenuhi oleh dua kemungkinan berikut: *k* = 1, *a* = 1 atau $k = -1, a = -1$. Jadi berlaku jika $a|1$ maka $a = 1$ atau $a = -1$. Jadi terbukti $a|1$ jika hanya jika $a = 1$ atau $a = -1$,

2. Diketahui $a|b$ dan $c|d$ yaitu ada $k_1, k_2 \in \mathbb{Z}$ sehingga $b = k_1 a$ dan $d = k_2 c$. Dengan mengalikan kedua persamaan tersebut diperoleh :

$$bd = (k_1 k_2)ac,$$

yaitu $ac|bd$.

3. Diketahui $a|b$ dan $b|c$, maka terdapat $k_1, k_2 \in \mathbb{Z}$ sehingga

$$b = k_1 a \tag{2.1}$$

dan

$$c = k_2 b \tag{2.2}$$

Substitusi persamaan (2.1) ke persamaan (2.2), diperoleh

$$c = k_2 b = k_2(k_1 a) = (k_1 k_2 a).$$

4. Diketahui

$$a = k_1 b \tag{2.3}$$

dan

$$b = k_2 a \tag{2.4}$$

Persamaan (2.3) dikalikan dengan persamaan (2.4), diperoleh $ab = (k_1 k_2)(ab)$. Diperoleh $k_1 k_2 = 1$, yakni $k_1 = k_2 = 1$ atau $k_1 = k_2 = -1$, jadi terbukti $a = b$ atau $a = -b$.

5. Diberikan $b = ac$ untuk suatu $c \in \mathbb{Z}$. Diambil nilai mutlaknya $|b| = |ac| = |a||c|$. Karena $b \neq 0$ maka $|c| \geq 1$. Sehingga diperoleh $|b| = |a||c| \geq |a|$.

6. Diketahui $a|b$ dan $a|c$, maka terdapat $k_1, k_2 \in \mathbb{Z}$ sedemikian sehingga $b = k_1 a$ dan $c = k_2 a$. Untuk sebarang $x, y \in \mathbb{Z}$ berlaku

$$bx + cy = k_1 ax + k_2 ay = (k_1 x + k_2 y)a$$

yang berarti $a|(bx + cy)$. ■

Pernyataan terakhir teorema ini berlaku juga untuk berhingga banyak bilangan yang dibagi oleh *a*, yaitu $a|b_k, k = 1, \cdots, n$ yaitu:

$$a|(b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

untuk setiap bilangan bulat $x_1, x_2, \cdots, x_n$.

2.2 Faktor Persekutuan Terbesar (FPB)

Definisi 2.2.1

Misalkan *a* atau *b* dua bilangan bulat dengan minimal salah satunya tidak nol. Faktor persekutuan terbesar (FPB) atau *greatest common divisor* (GCD) dari *a* dan *b* adalah bilangan bulat *d* yang memenuhi

(i) $d|a$ dan $d|b$, dan

(ii) jika $c|a$ dan $c|b$ maka $c \leq d$.

Dari definisi 2.2.1, kondisi (i) menyatakan bahwa *d* adalah faktor persekutuan dari *a* dan *b*. Sedangkan kondisi (ii) menyatakan bahwa *d* adalah faktor persekutuan terbesar. Selanjutnya, jika *d* faktor persekutuan terbesar dari *a* dan *b* akan ditulis $d = \gcd(a, b)$ (Sukirman,1997).

Berdasarkan definisi 2.2.1 maka berikut ini akan diberikan teorema sebagai berikut.

Teorema 2.2.1

Jika *a* dan *b* dua bilangan bulat yang keduanya tak nol maka terdapat bilangan bulat *x* dan *y* sehingga

$$\gcd(a, b) = ax + by \qquad (2.5)$$

Persamaan (2.5) disebut dengan identitas Benzout (Sukirman, 1997).

Sebelum dibuktikan, perhatikan ilustrasi berikut,

$$\gcd(-12,30) = 6 = (-12)2 + 30(-1)$$

$$\gcd(-8,-36) = 4 = (-8)4 + (-36)(-1)$$

identitas Benzout menyatakan bahwa $d = \gcd(a,b)$ dapat disajikan dalam bentuk kombinasi linear atas *a* dan *b*. Ekspresi ruas kanan pada (2.5) disebut kombinasi linear dari *a* dan *b*. Pada teorema ini keberadaan *x* dan *y* tidak harus tunggal.

Bukti.

Bentuk *S* himpunan semua kombinasi linear positif dari *a* dan *b* sebagai berikut

$$S = \{au + bv | au + bv \geq 1, u, v \in \mathbb{Z}\}$$

Perhatikan bahwa, jika $a \neq 0$ maka $|a| = au + b \cdot 0 \in S$, yaitu dengan mengambil *u* = 1 bila *a* positif atau *u* = -1 bila *a* negatif. Jadi, himpunan *S* tak kosong. Menurut sifat urutan, *S* terjamin memiliki anggota terkecil, katakan saja *d*. Selanjutnya, dibuktikan $d = \gcd(a,b)$. Karena $d \in S$ maka terdapat $x, y \in \mathbb{Z}$ sehingga $d = ax + by$. Dengan menerapkan algoritma pembagian pada *a* dan *d* maka terdapat *q* dan *r* sehingga $a = qd + r$, dengan $0 \leq r < d$. Selanjutnya ditunjukkan *r* = 0, sehingga diperoleh $d|a$. Jika $r > 0$ maka dapat ditulis

$$0 < r = a - qd = a - q(ax + by) = a(1 - qx)b(-qy) \in S$$

Faktanya $r \in S$ sedangkan syaratnya $r < d$ ini bertentangan dengan pernyataan bahwa *d* elemen terkecil *S* sehingga disimpulkan *r* = 0 atau $d|a$. Argumen yang sama dapat dipakai dengan menerapkan algoritma pembagian pada *b* dan *d* untuk menunjukkan $d|b$. Jadi, terbukti bahwa *d* adalah faktor persekutuan dari *a* dan *b*. Selanjutnya ditunjukkan faktor persekutuan ini adalah yang terbesar. Misalkan *c* adalah bilangan bulat positif dengan $c|a$ dan $c|b$ maka $c|ax + b$ yaitu $c|d$. Jadi

$c \leq d$, karena tidak mungkin pembagi lebih besar dari bilangan yang dibagi.

Terbukti bahwa $d = \gcd(a, b)$ ■

Teorema 2.2.2 Algoritma Pembagian

Diberikan dua bilangan bulat *a* dan *b* dengan *a*,*b* > 0, $a \neq 0$ maka ada tepat satu pasang bilangan-bilangan *q* dan *r* sehingga:

$$b = qa + r \quad \text{dengan} \, 0 \leq r < a$$

Algoritma pembagian adalah suatu cara atau prosedur yang dapat dipakai untuk mendapatkan faktor persekutuan terbesar. Ilustrasinya adalah :

Diberikan dua bilangan bulat *a* dan *b* dengan *a* > 0, *b* > 0, maka gcd (*a*,*b*) dapat dicari dengan mengulang algoritma pembagian.

$a = q_1 b + r_1 \qquad 0 < r_1 < b$

$b = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2$

……

$r_{n-1} = q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n + 0 \qquad 0 < r_1 < b$

maka r_n, sisa terakhir dari pembagian diatas yang bukan nol merupakan gcd (*a*,*b*) (Graham, 1957).

2.3 Bilangan Prima

Definisi 2.3.1

Sebuah bilangan bulat $p > 1$ disebut bilangan prima, jika dan hanya jika habis dibagi dengan 1 dan bilangan itu sendiri atau p (Burton,1976).

Definisi 2.3.2 (Relatif Prima)

Bilangan bulat *a* dan *b* dikatakan *coprima* atau *relatif prima* jika $\gcd(a, b) = 1$ (Dudley, 1969).

Berdasarkan definisi 2.3.2, maka akan diberikan teorema sebagai berikut

Teorema 2.3.2

Bilangan *a* dan *b* relatif prima hanya bila terdapat bilangan bulat *x*, *y* sehingga $ax + by = 1$ (Sukirman, 1997).

Bukti.

Karena *a* dan *b* relatif prima maka $\gcd(a, b) = 1$. Identitas Bezout menjamin adanya bilangan bulat *x*, *y* sehingga $1 = ax + by$. Sebaliknya, misalkan ada bilangan bulat $ax + by = 1$. Dibuktikan $\gcd(a, b) = d = 1$. Karena $d|a$ dan $d|b$ maka $d|(ax + by = 1)$, jadi $d|1$. Karena itu disimpulkan *d* =1

Berdasarkan pengertian relatif prima yang terdapat pada definisi 2.3.2, maka berikut ini akan diberikan teorema tentang relatif prima.

Teorema 2.3.3

Jika $\gcd(a, b) = 1$, maka berlaku pernyataan berikut

1. Jika $a|c$ dan $b|c$ maka $ab|c$
2. Jika $a|bc$ maka $a|c$

(Sukirman, 1997).

Bukti.

1. Diketahui $a|c$ dan $b|c$. Artinya terdapat $r, s \in \mathbb{Z} \exists\ c = a \cdot r = b \cdot s$.

   Berdasarka hipotesis, $\gcd(a, b) = 1$. Oleh karena itu dapat dituliskan

   $ax + by = 1$ untuk suatu bilangan bulat *x*, *y*. Akibatnya

   $$c = 1 \cdot c = (ax + by) \cdot c$$
   $$= acx + bcy$$
   $$= a(bs)x + b(ar)y$$
   $$= ab(sx + ry)$$

   Karena terdapat bilangan bulat $sx + ry$ sedemikian sehingga

   $ab|c$. Terbukti bahwa, jika $a|c$ dan $b|c$ maka $ab|c$.

2. Diketahui $a|bc$, $\gcd(a, b) = 1$. Oleh karena itu dapat dituliskan $ax + by = 1$

   untuk suatu bilangan bulat *x*, *y*. Akibatnya

   $$c = 1 \cdot c = (ax + by) \cdot c$$
   $$= acx + bcy$$

   Karena diketahui $a|bc$ dan faktanya $a|ac$ maka $a|(acx + bcy)$ karena

   $c = acx + bcy$ jadi terbukti $a|c$ ■

Karena penyelesaian persamaan Diophantine yang digunakan adalah dengan relasi rekuensi modulo *m*, maka diberikan definisi modulo sebagai berikut.

2.4 Modulo

Definisi 2.4.1

Misalkan a , $m > 0$ bilangan bulat. Operasi a mod m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Notasi: $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$. Bilangan m disebut modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m - 1\}$ (Grillet, 2007).

Definisi 2.4.2 (Relasi Kongruensi)

Misalkan a dan b adalah bilangan bulat dan $m > 0$, a dikatakan kongruen dengan b modulo m atau ditulis $a \equiv b \ (mod\ m)$ jika m habis membagi $a - b$. Jika a tidak kongruen dengan b dalam modulo m, maka ditulis $a \not\equiv b \pmod m$ (Grillet, 2007).

Kekongruenan $a \equiv b \ (mod\ m)$ dapat pula dituliskan dalam hubungan

$$a = b + km$$

yang dalam hal ini k adalah bilangan bulat.

Contoh.

$16 \equiv 4 \ (mod\ 3)$ dapat ditulis sebagai $16 = 4 + 4 \cdot 3$

Sehingga , dapat dituliskan $a \bmod m = r$ sebagai :

$$a \equiv r \ (mod\ m)$$

Teorema 2.4.2

Misalkan *m* adalah bilangan bulat positif

1. Jika $a \equiv b \pmod m$ dan *c* adalah sebarang bilangan bulat maka

   (i) $(a + c) \equiv (b + c) \pmod m$

   (ii) $ac \equiv bc \pmod m$

   (iii) $a^p \equiv b^p \pmod m$ untuk suatu bilangan bulat tak negatif *p*.

2. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$, maka

   (i) $(a + c) \equiv (b + d) \pmod m$

   (ii) $ac \equiv bd \pmod m$ (Grillet, 2007).

Bukti .

1. (i) $a \equiv b \pmod m$ berarti $a = b + km$ untuk suatu $k \in \mathbb{Z}$

   untuk sebarang $c \in \mathbb{Z}$, diperoleh

   $$a + c = b + c + km$$

   $$\Leftrightarrow a + c = (b + c)(mod\ m)$$

   (ii) $a \equiv b \pmod m$ berarti:

   $$a = b + km$$

   $$\Leftrightarrow a - b = km$$

   $$\Leftrightarrow (a - b)c = ckm$$

   $$\Leftrightarrow ac = bc + km, \text{ dengan } k = ck$$

   $$\Leftrightarrow ac \equiv bc \pmod m$$

   (iii) $a \equiv b \pmod m$ berarti $a = b + km$ dengan $k \in \mathbb{Z}$

   $$p \in \mathbb{Z}^+ \cup \{0\}$$

   $$a^p = (b + km)^p$$

$$\Leftrightarrow a^p = b^p + \binom{p}{1}b^{p-1}km + \binom{p}{2}b^{p-2}(km)^2 + \cdots + \binom{p}{p-1}b(km)^{p-1} + (km)^p$$

$$= b^p + \{\binom{p}{1}b^{p-1}k + \binom{p}{2}b^{p-2}k^2m + \cdots + \binom{p}{p-1}bk^{p-1}m^{p-2} + k^pm^{p-1}\}m$$

$$\Leftrightarrow a^p \equiv b^p (mod\ m)$$

2 (i) $a \equiv b\ (mod\ m) \Leftrightarrow a = b + k_1m$

$c \equiv d\ (mod\ m) \Leftrightarrow c = d + k_2m$

Jadi, $(a + c) = (b + d) + (k_1 + k_2)m$

$\Leftrightarrow (a + c) = (b + d) + km \qquad (k = k_1 + k_2)$

$\Leftrightarrow (a + c) = (b + d)(mod\ m)$

(ii) $a \equiv b\ (mod\ m) \Leftrightarrow a = b + mk$, untuk suatu $k \in \mathbb{Z}$

$c \equiv d\ (mod\ m) \Leftrightarrow c = d + ml$, untuk suatu $l \in \mathbb{Z}$

$\Leftrightarrow a \cdot c = (b + mk)(d + ml)$

$\Leftrightarrow a \cdot c = bd + blm + kdm + klm^2$

$\Leftrightarrow a \cdot c = bd + (bl + kd + klm)m$

$\Leftrightarrow a \cdot c \equiv bd(mod\ m)$ ■

(Grillet, 2007).

Teorema 2.4.3 (Teorema Fermat)

Jika p adalah bilangan prima dan a adalah bilangan bulat positif dimana $p \nmid a$, maka $a^{p-1} \equiv 1\ (mod\ p)$.

Bukti.

Asumsikan $(p-1)$ bilangan positif pertama kelipatan dari a, yaitu bilangan bulat. Sehingga terdapat barisan sebagai berikut:

$$a, 2a, 3a, \dots, (p-1)a$$

Tidak ada satu pun suatu bilangan dari barisan diatas yang habis dibagi *p*, karena barisan tersebut terbentuk dengan pola *ka* dimana $1 \leq k \leq p-1$. Oleh karena $p \nmid a$ dan $p \nmid k$, maka $p \nmid ka$. Kemudian, dari barisan tersebut tidak ada dua bilangan yang kongruen $mod\ p$. Atau dengan kata lain, jika bilangan-bilangan tersebut dibagi dengan *p*, maka sisa pembagiannya akan selalu berbeda satu sama lain.

Asumsikan bahwa ada dua bilangan kongruen $mod\ p$, yaitu *ra* dan *sa* dimana $1 \leq r < s \leq p-1$

$$ra \equiv sa(mod\ p)$$

Karena gcd (*a*,*p*) = 1, maka

$$r \equiv s\ (mod\ p)$$

Karena *r* dan *s* harus lebih besar 1 dan harus lebih kecil dari *p*, maka ini menyatakan *r* = *s*. Pernyataan ini kontradiksi dengan asumsi awal bahwa *r* dan *s* harus berbeda. Oleh karena itu, sebelumnya, bilangan bulat harus kongruen $mod\ p$ ke 1,2,3,4, $\dots, p-1$. Ambil semuanya , kemudian kalikan semua kongruen, maka diperoleh sebagai berikut

$$a, 2a, 3a, \dots, (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)(mod\ p)$$

Sehingga,

$$a^{p-1}(p-1)! \equiv (p-1)!\,(mod\ p)$$

Karena gcd $\big((p-1)!, p\big) = 1$, maka

$$a^{p-1} \equiv 1\ (mod\ p)$$ ■

(Burton, 1980).

Contoh 2.4.1

Tunjukkan bahwa sisa pembagian 5^{38} oleh 11 adalah 4.

Untuk menunjukkan hal di atas, dengan menggunakan relasi kongruensi cukup ditunjukkan bahwa $5^{38} \equiv (mod\ 11)$.

Bukti.

$$\begin{aligned} 5^{38} &= (5^{10})^{3+8} \\ &= (5^{10})^{3}(5^{2})^{4} \\ &= 1^{3} \cdot 3^{4}(mod\ 11) \\ &= 81(mod\ 11) \\ &= 4(mod\ 11) \end{aligned}$$ ■

2.5 Persamaan Diophantine

Definisi 2.5.1

Persamaan Diophantine adalah persamaan polinomial atas $\mathbb{Z}$ dalam *n* variabel dengan solusi bilangan bulat. Adapun persamaannya sebagai berikut:

$$f(x_1, \dots\dots, x_n) = 0$$

(Sembiring, 2010).

Berdasarkan definisi persamaan Diophantine linear di atas dapat dibentuk teorema berikut ini.

Teorema 2.5.1

Persamaan linear Diophantine $ax + by = c$ mempunyai penyelesaian jika dan hanya jika faktor persekutuan terbesar dari a dan b habis membagi c .

Bukti .

Misalkan $d = \gcd(a,b)$ dan $d \mid c$

$d \mid c \Leftrightarrow$ ada k bulat sehingga $c = kd$.

$d \mid \gcd(a,b) \Leftrightarrow$ ada bilangan bulat m dan n sehingga : $am + bn = d$

$$a(km) + b(kn) = kd$$

$$a(km) + b(kn) = c$$

berarti $x = mk$ dan $y = nk$ (Sembiring, 2010).

Berikut ini merupakan teorema tentang solusi umum persamaan Diophantine.

Teorema 2.5.2

Jika $d = \gcd(a,b)$ dan x_0, y_0 penyelesaian persamaan Diophantine $ax + by = c$, maka penyelesaian umum persamaan tersebut adalah $x = x_0 + \frac{b}{d}k$ dan $y = y_0 - \frac{a}{d}k$ dengan k parameter bilangan bulat (Sembiring, 2010).

Karena ring yang akan dibahas adalah $\mathbb{Z}[i]$ dimana ruang lingkupnya sangat erat dengan sistem bilangan kompleks sehingga akan dijelaskan sistem bilangan kompleks sebagai berikut.

2.6 Sistem Bilangan Kompleks

Definisi 2.6.1

Sistem bilangan kompleks $\mathbb{C}$ adalah bilangan kompleks $\mathbb{C}$ yang dilengkapi oleh operasi penjumlahan (+) dan perkalian (•) yang memenuhi aksioma atas lapangan $\mathbb{C}$ (Spiegel, M.R, 1981).

Berikut ini adalah sifat – sifat operasi penjumlahan dalam sistem bilangan kompleks.

Teorema 2.6.1

Untuk semua bilangan kompleks berlaku sifat additif dan assosiatif terhadap penjumlahan.

$$z_1 + z_2 = z_2 + z_1 \qquad (2.6)$$

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3 \qquad (2.7)$$

(Spiegel, M.R, 1981).

Bukti .

Misal $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$ dan $z_3 = a_3 + ib_3$ maka :

$$\begin{aligned} z_1 + z_2 &= (a_1 + ib_1) + (a_2 + ib_2) \\ &= (a_1 + a_2) + i(b_1 + b_2) \\ &= (a_2 + ib_2) + (a_1 + ib_1) \\ &= z_2 + z_1 \end{aligned}$$

■

$$z_1 + (z_2 + z_3) = (a_1 + ib_1) + [(a_2 + ib_2) + (a_3 + ib_3)]$$
$$= (a_1 + ib_1) + [(a_2 + a_3) + i(b_2 + b_3)]$$
$$= [a_1 + (a_2 + a_3)] + i[b_1 + (b_2 + b_3)]$$
$$= [(a_1 + a_2) + a_3] + i[(b_1 + b_2) + b_3]$$
$$= [(a_1 + a_2) + i(b_1 + b_2)] + (a_3 + ib_3)$$
$$= (z_1 + z_2) + z_3 \quad \blacksquare$$

Berikut ini adalah sifat – sifat operasi perkalian dalam sistem bilangan kompleks.

Teorema 2.6.2

1. Perkalian bilangan-bilangan kompleks bersifat komutatif.

$$z_1 \bullet z_2 = z_2 \bullet z_1 \qquad (2.8)$$

2. Perkalian bilangan-bilangan kompleks bersifat assosiatif.

$$z_1 \bullet (z_2 \bullet z_3) = (z_1 \bullet z_2) \bullet z_3 \qquad (2.9)$$

3. Perkalian bilangan-bilangan kompleks bersifat distributif terhadap penjumlahan.

$$z_1 \bullet (z_2 + z_3) = z_1 \bullet z_2 + z_1 \bullet z_3 \qquad (2.10)$$

(Spiegel, M.R, 1981).

Bukti .

Misal $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$ dan $z_3 = a_3 + ib_3$ maka :

1. $z_1 \bullet z_2 = (a_1 + ib_1) \bullet (a_2 + ib_2)$
$$= a_1 + a_2 + i(a_1 + b_2) + i^2 b_1 b_2$$
$$= a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)$$
$$= a_2 a_1 - b_2 b_1 + i(b_2 a_1 + a_2 b_1)$$

$= (a_2 + ib_2)\,(a_1 + ib_1)$

$= z_2 \bullet z_1$

2. $z_1 \bullet (z_2 \bullet z_3) = (a_1 + ib_1) \bullet [(a_2 + ib_2) \bullet (a_3 + ib_3)]$

$= (a_1 + ib_1) \bullet [(a_2a_3 - b_2b_3) + i\,(b_2a_3 + a_2b_3)]$

$= a_1\,(a_2a_3 - b_2b_3) - b_1\,(b_2a_3 + a_2b_3) +$

$i\,[(b_1(a_2a_3 - b_2b_3) + a_1(b_2a_3 + a_2b_3)$

$=(a_1a_2 - b_1b_2)a_3 - (a_1b_2 + a_2b_1)b_3 + i\,[(a_1 + a_2b_1)\,a_3$

$+ (a_1a_2 - b_1b_2)\,b_3]$

$= [(a_1 + ib_1) \bullet (a_2 + ib_2)] \bullet (a_3 + ib_3)$

$= ((z_1 \bullet z_2) \bullet z_3)$

3. $z_1 \bullet (z_2 + z_3) = (a_1 + ib_1) \bullet [(a_2 + ib_2) + (a_3 + ib_3)]$

$= (a_1 + ib_1) \bullet [(a_2 + a_3) + i(b_2 + b_3)]$

$= a_1\,(a_2 + a_3) - b_1(b_2 + b_3) + ib_1(a_2 + a_3) + ia_1(b_2 + b_3)$

$= (a_1a_2 - b_1b_2) + i\,(b_1a_2 + a_1b_2) + (a_1a_3 - b_1b_3) +$

$i\,(a_1b_3 + b_1a_3)$

$= z_1 \bullet z_2 + z_1 \bullet z_3$ ■

Metode ring yang digunakan pada penelitian ini adalah Ring $\mathbb{Z}[i]$**,** sehingga didefinisikan bilangan Gaussian sebagai berikut.

2.7 Bilangan Gaussian

Definisi 2.7.1

Bilangan bulat Gaussian adalah bilangan kompleks yang bagian reall dan bagian imajinernya adalah bilangan bulat. Dengan penjumlahan biasa dan perkalian

bilangan kompleks, membentuk daerah integral dinotasikan dengan $\mathbb{Z}[i]$**.** Domain ini tidak bisa dinyatakan dalam ring berurut, selama memuat suatu akar kuadrat dari -1 Secara umum himpunan bilangan bulat Gaussian adalah :

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

(Andreescu dkk, 2010).

Dalam penyelesaian persamaan Diophantine akan menggunakan metode ring $\mathbb{Z}[i]$**,** sehingga, dibutuhkan definisi tentang ring sebagai berikut.

2.8 Ring $\mathbb{Z}[i]$

Sebelum membahas tentang ring $\mathbb{Z}[i]$, akan diberikan terlebih dahulu definisi tentang ring berikut.

Definisi 2.8.1

Himpunan *R* dengan dua operasi biner + (penjumlahan) dan • (perkalian) merupakan ring jika memenuhi aksioma berikut:

1. $\langle R, + \rangle$ merupakan grup Abel;
2. Opersi perkaliannya bersifat asosoatif, yaitu $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ untuk setiap $a, b, c \in R$;
3. Hukum distributif terpenuhi di *R*, yaitu untuk setiap $a, b, c \in R$ $(a + b) \bullet c = (a \bullet c) + (b \bullet c)$ dan $a \bullet (b + c) = (a \bullet b) + (a \bullet c)$

(Dummit and Foote, 2004).

Berikut ini akan dibuktikan bahwa himpunan semua bilangan bulat Gaussian $\mathbb{Z}[i]$ dengan operasi penjumlahan dan perkalian membentuk ring.

Teorema 2.8.1

Jika diberikan himpunan semua bilangan bulat Gaussian :

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

Pada $\mathbb{Z}[i]$ didefinisikan dua operasi :

(i) Operasi penjumlahan ($+'$), yaitu :

$$(a + bi) +' (c + di) = (a + c) +' (bi + di)$$

(ii) Operasi perkalian ($\bullet'$), yaitu :

$$(a + bi) \bullet' (c + di) = (ac + bd) + (ad + bc)i$$

maka, $< \mathbb{Z}[i], +', \bullet' >$ membentuk ring.

Bukti.

a. Harus dibuktikan $< \mathbb{Z}[i], +' >$ grup abel / grup komutatif.

(i) Diberikan sebarang $(a + bi), (c + di) \in \mathbb{Z}[i]$, maka dipeeroleh:

$$(a + bi) +' (c + di) = (a + c) + (bi + di)$$

Karena $a + c \in \mathbb{Z}$ dan $(b + d) \in \mathbb{Z}[i]$, maka $(a + c), (bi + di) \in \mathbb{Z}[i]$.

Jadi operasi $+'$ tertutup pada $\mathbb{Z}[i]$.

(ii) Diberikan sebarang $(a + bi), (c + di), (e + fi) \in \mathbb{Z}[i]$ maka diperoleh:

$$\begin{aligned}[(a + bi) + (c + di)] + (e + fi) &= [(a + c) +' (b + d)i\,] + (e + fi) \\ &= (a + c) +' (b + d)i + (e + fi) \\ &= (a + c) +' (e(b + d + f)i) \\ &= a + c + e + (b + d + f)i \\ &= (a + bi) +' [(c + e) +' (d + f)i] \\ &= (a + bi) +' [(c + di) +' (d + fi)]\end{aligned}$$

Jadi operasi $+'$ bersifat assosiatif pada $\mathbb{Z}[i]$.

(iii) Diberikan sebarang $(a + bi) \in \mathbb{Z}[i]$, maka terdapat $(c + di)$ $\in \mathbb{Z}[i]$ sehingga,

$$(a + bi) +' (c + di) = (c + di) +' (a + bi) = (a + bi)$$

Dari persamaan

$$(a + bi) +' (c + di) = (a + bi)$$

$$\Leftrightarrow (a + c) + (b + di) = (a + bi)$$

$$\Leftrightarrow a + c = a \text{ dan } b + d = b$$

$$\Rightarrow c = 0 \text{ dan } d = 0$$

Jadi $c + di = 0 + 0i$ merupakan elemen netral pada $\mathbb{Z}[i]$.

(iv) Untuk setiap $(a + bi) \in \mathbb{Z}[i]$, terdapat $(e + fi) \in \mathbb{Z}[i]$ sehingga,

$$(a + bi) +' (c + di) = (c + di) +' (a + bi) = 0 + 0i$$

Dari persamaan

$$(a + bi) +' (c + di) = 0 + 0i$$

$$\Leftrightarrow (a + c) + (b + di) = 0 + 0i$$

$$\Leftrightarrow a + c = 0 \text{ dan } b + d = 0$$

$$\Rightarrow c = -a \text{ dan } d = -b$$

Jadi $-(a + bi)$ merupakan invers pada $-\mathbb{Z}[i] \; \forall \; (a + bi) \in \mathbb{Z}[i]$.

(v) Diberikan sebarang $(a + bi), (c + di) \in \mathbb{Z}[i]$, maka diperoleh :

$$\begin{aligned}(a + bi) +' (c + di) &= (a + c) + (b + d)i \\ &= (a + c) + bi + di \\ &= (a + bi) + (c + di)\end{aligned}$$

Jadi operasi $+'$ komutatif.

Dari (i), (ii), (iii), (iv), dan (v) disimpulkan $< \mathbb{Z}[i] , +' >$ grup komutatif.

b. Terdapat operasi perkalian (•) harus dibuktikan:

(i) Diberikan sebarang $(a + bi), (c + di) \in \mathbb{Z}[i]$, maka

$$(a + bi) \bullet (c + di) = (ac - bd) + (ad + bc)i$$

karena $(ac - bd) \in \mathbb{Z}$ dan $(ad + bc)i \in \mathbb{Z}$, maka

$$(ac - bd) + (ad + bc)i \in \mathbb{Z}[i].$$

Jadi operasi • tertutup pada $\mathbb{Z}[i]$.

(ii) Assosiatif

Diberikan sebarang $(a + bi), (c + di), (e + fi) \in \mathbb{Z}[i]$, maka diperoleh:

$$[(a + bi) \bullet (c + di)] \bullet (e + fi)$$

$$= [(ac - bd) + (ad + bc)i] \bullet (e + fi)$$

$$= [(ac - bd)e - (ad + bc)f] + [(ac + bd)f + (ad + bc)e]i$$

$$= ace - bde - adf - bcf + acfi + bdfi + adei + bcei$$

$$= ace - adf + bcei - bdfi + acfi + adei - bcf - bde$$

$$= a + bi\left((ce - df)\right) + (cf + de)i)$$

$$= a + bi(ce - df + cfi + dei)$$

$$= a + bi((c + di)(e + fi)$$

c. Terhadap operasi $+'$ dan • harus dipenuhi

(i) Distributif kiri

Diberikan sebarang $(a + bi), (c + di), (e + fi) \in \mathbb{Z}[i]$, maka diperoleh:

$$(a + bi) \bullet [(c + di) +' (e + fi)]$$

$$= (a + bi) \bullet [(c + e) +' (d + f)i]$$

$$= [a(c+e) - b(d+f)] +' [a(d+f) + b(c+e)]i$$

$$= ac + ae - bd - bf + (ad + af)i + (bc + be)i$$

$$= ac + adi + bci - bd + ae + afi + bei - bf$$

$$= (a + bi) \bullet' (c + di) +' (a + bi) \bullet' (e + fi)$$

(ii) Distributif kanan

Diberikan sebarang $(a + bi), (c + di), (e + fi) \in \mathbb{Z}[i]$, maka diperoleh:

$$[(a + bi) +' (c + di)] \bullet (e + fi)$$

$$= [(a + c) +' (b + d)i] \bullet (e + fi)$$

$$= [(a + c)e - (b + d)f] +' [(a + c)f - (b + d)e)]i$$

$$= ae + ce - bf - df + afi + cfi - bei - dei$$

$$= (ae + af)i + (be - bf)i + ce + cfi + dei - dfi$$

$$= (a + bi) \bullet' (e + fi) +' (c + di) \bullet' (e + fi)$$ ■

Selanjutnya ring $\mathbb{Z}[i]$ merupakan daerah integral, yang dituliskan dalam teorema berikut :

Teorema 2.8.2

Ring $\mathbb{Z}[i]$ merupakan daerah integral.

Bukti.

Untuk membuktikan ring $\mathbb{Z}[i]$ daerah integral cukup dibuktikan.

(i) Ring $\mathbb{Z}[i]$ komutatif

Diberikan sebarang $(a + b), (c + di) \in \mathbb{Z}[i]$**,** maka diperoleh:

$$(a + bi) \bullet (c + di) = (ac - bd) + (ad + bc)i = (ca - db) + (da + cb)i$$

$$= (c + di) \bullet (a + bi)$$

(ii) Ring $\mathbb{Z}[i]$ tidak memuat pembagi nol

Ring $\mathbb{Z}[i]$ tidak memuat pembagi nol, sebab jika diambil sebarang $(a+bi) \neq 0, (c+di) \neq 0$, maka $(a+bi) \bullet (c+di) \neq 0$.

Selanjutnya akan didefinisikan pengertian norm atau jarak pada vektor pada $\mathbb{Z}[i]$.

Definisi 2.8.3

Norm pada $\mathbb{Z}[i]$ merupakan fungsi :

$$N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$$

dengan rumus $N(a + bi) = a^2 + b^2, \forall (a+bi) \in \mathbb{Z}[i]$.

Norm di atas menyatakan ukuran besaran dari elemen $\mathbb{Z}[i]$**.** Norm juga digunakan untuk pembuktian eksistansi (keberadaan) unit dalan ring $\mathbb{Z}[i]$**.** Selain itu, norm juga digunakan untuk mengukur sisa keterbagian pada ring $\mathbb{Z}[i]$.

Berikut ini diberikan sifat multiplikatif dari norm pada $\mathbb{Z}[i]$.

Teorema 2.8.3

Fungsi norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$ bersifat multiplikatif, yaitu :

$$(N(\alpha\beta)) = N(\alpha)\, N(\beta), \forall\, \alpha, \beta \in \mathbb{Z}[i]$$

Bukti.

Diberikan sebarang $\alpha, \beta \in \mathbb{Z}[i]$ dengan $\alpha = a + bi$ dan $\beta = c + di$, maka diperoleh :

$$\alpha\beta = (a+bi)(c+di) = (ac - bd) + (ad + bc)i$$

Sehingga diperoleh,

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \end{aligned}$$

$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2)$$

$$= (a^2 + b^2)(c^2 + d^2)$$

$$= N(\alpha)\, N(\beta)$$

Sifat multiplikatif norm N pada $\mathbb{Z}[i]$ ini juga dapat digunakan untuk menghubungkan struktur multiplikatif pada $\mathbb{Z}$ dengan struktur multiplikatif pada $\mathbb{Z}[i]$, dan juga dapat untuk menghubungkan keterbagian, keprimaan pada $\mathbb{Z}$ dengan keterbagian serta keprimaan dalam ring $\mathbb{Z}[i]$. ■

Dengan definisi norm pada $\mathbb{Z}[i]$ pada definisi 2.8.2 dapat digunakan untuk mengembangkan pengertian unit pada ring $\mathbb{Z}[i]$ berikut ini :

Definisi 2.8.3

Misalkan $\alpha \in \mathbb{Z}[i]$**.** Bilangan bulat Gaussian α dikatakan unit dari $\mathbb{Z}[i]$ jika $\mathrm{N}(\alpha) = 1$.

Sehingga unit dari $\mathbb{Z}[i]$ adalah 1, -1, *i*, *-i.* Unit-unit tersebut dapat dicari dengan cara berikut:

Diberikan sebarang $u + vi \in \mathbb{Z}[i]$**,** sebagai unit. Maka terdapat elemen lain $x + yi \in \mathbb{Z}[i]$ sedemikian sehingga,

$$(u + vi)(x + yi) = 1$$

$$\Leftrightarrow \mathrm{N}\big((u + vi)(x + yi)\big) = N(1)$$

$$\Leftrightarrow \mathrm{N}\,(u + vi) \bullet N(x + yi) = 1$$

$$\Leftrightarrow (u^2 + v^2)(x^2 + y^2 = 1$$

Karena u, v, x, y bilangan bulat, maka

$$u^2 + v^2 = 1$$

Maka diperoleh solusi $(u, v) = (1,0), (0,1), (-1,0)$ dan $(0, -1)$. Dalam ring $\mathbb{Z}[i]$, maka solusi tersebut menjadi $1, i, -1$ dan $-i$.

Selanjutnya akan didefinisikan konsep keterbagian pada $\mathbb{Z}[i]$ dengan mengacu keterbagian pada $\mathbb{Z}$.

Definisi 2.8.4

Misalkan $\alpha, \beta \in \mathbb{Z}[i]$. Bilangan α dikatakan membagi β atau ditulis $\alpha \mid \beta$ jika dan hanya jika terdapat bilangan $\gamma \in \mathbb{Z}[i]$ sedemikian sehingga $\beta = \alpha\gamma$.

Teorema 2.8.4

Jika norm dari bilangan bulat Gaussian prima dalam $\mathbb{Z}$, maka bilangan bulat Gaussian tersebut prima dalam $\mathbb{Z}[i]$.

Bukti.

Misalkan $\alpha \in \mathbb{Z}[i]$ mempunyai norm prima, katakan $N(\alpha) = p$, akan ditunjukkan α hanya mempunyai faktor trivial (faktornya mempunyai norm 1 atau hanya $N(\alpha)$).

Perhatikan faktorisasi dari $\alpha \in \mathbb{Z}[i]$, katakan $\alpha = \beta\gamma$.

Dari $N(\alpha) = p$, diperoleh:

$$N(\beta\gamma) = p$$

Maka,

$$N(\beta)N(\gamma) = p$$

Sehingga, $N(\beta)$ atau $N(\gamma)$ sama dengan 1. Jadi β atau γ adalah unit, sehingga α prima dalam $\mathbb{Z}[i]$.

Contoh 2.8.1

$N(4+5i) = 41$, maka $4+5i$ prima dalam $\mathbb{Z}[i]$.

$N(4-5i) = 41$, maka $4-5i$ prima dalam $\mathbb{Z}[i]$.

$N(1+2i) = 5$, maka $1+2i$ prima dalam $\mathbb{Z}[i]$.

2.9 Unit

Definisi 2.9.1

Misalkan D daerah integral dan 1 adalah elemen satuan di D. Unsur $u \in$ D merupakan unit jika dan hanya jika *u* membagi 1 sedemikian sehingga $1 = u.u^{-1}$ untuk suatu $u^{-1} \in$ D, dengan kata lain *u* mempunyai invers terhadap perkalian di dalam D. Misalkan $a,b \in$ D . Elemen *a* dan *b associate* di D jika $a = bu$, untuk *u* unit di D (Dummit and Foote, 2004).

Contoh 2.9.1

(i) Elemen unit di $\mathbb{Z}$ adalah 1 dari -1.

karena 1 | 1 (1 = 1 . 1)

dan karena -1 | 1 (1 = (-1) (-1)) $\Longrightarrow 1 = u.u^{-1}$

(ii) Elemen assosiasi dari 25 di $\mathbb{Z}$ adalah 25 dan -25.

karena 25 = 25 . 1

25 = -25 (-1)

(Dummit and Foote, 2004).