BILANGAN ISTIMEWA DI RING $\mathbb{Z}_n$

(Skripsi)

Oleh

Ecy Ratna Sari

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

ABSTRACT

SPECIAL NUMBER IN THE RING $\mathbb{Z}_n$

by

Ecy Ratna Sari

Number theory will introduced several kinds of number, one of it is special number. It have been know a special number concept is $a^2 + b^2 - dc^2$. Whereas positive integers d is special if every integers m declared as $m = a^2 + b^2 - dc^2$ for integers a, b, and c non zero. Because for every integer m there has pairs a, b, c infinitely many solutions. In this research a, b, c will be limited in Ring $\mathbb{Z}_n$ satisfying $a^2 + b^2 - dc^2 \equiv m (\text{mod } n)$. Referring to the exist theorem and lemma, n is a prime less than 50, so $n = 7,11,19,29,31,37,41,43,47$. So the result is $d = 1,2,5,10,13,17,25,26,29,34,37,41$ as special number in Ring $\mathbb{Z}_n$.

Key Words : *Integers, Special number, Ring* $\mathbb{Z}_n$

ABSTRAK

BILANGAN ISTIMEWA DI RING $\mathbb{Z}_n$

oleh

Ecy Ratna Sari

Di teori bilangan akan di perkenalkan berbagai macam bilangan, salah satunya bilangan istimewa. Telah diketahui konsep bilangan istimewa yaitu $a^2 + b^2 - dc^2$. Dimana bilangan bulat positif d adalah istimewa jika setiap bilangan bulat m dinyatakan sebagai $m = a^2 + b^2 - dc^2$ untuk bilangan bulat a, b, dan c tidak nol. Karena untuk setiap bilangan bulat m terdapat pasangan a, b, c tak berhingga banyaknya. Pada penelitian ini a, b, c akan dibatasi di Ring $\mathbb{Z}_n$ yang memenuhi $a^2 + b^2 - dc^2 \equiv m(\text{mod } n)$. Merujuk pada teorema dan lemma yang ada, n adalah bilangan prima lebih kecil dari 50, maka $n = 7,11,19,29,31,37,41,43,47$. Sehingga didapatkan $d = 1,2,5,10,13,17,25,26,29,34,37,41$ yang merupakan bilangan istimewa di Ring $\mathbb{Z}_n$.

Kata Kunci : *Bilangan Bulat, Bilangan Istimewa, Ring* $\mathbb{Z}_n$

BILANGAN ISTIMEWA DI RING $\mathbb{Z}_n$

Oleh

Ecy Ratna Sari

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA MATEMATIKA

pada

Jurusan Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

Judul Skripsi : **BILANGAN ISTIMEWA DI RING $\mathbb{Z}_n$**

Nama Mahasiswa : Ecy Ratna Sari

Nomor Pokok Mahasiswa : 1417031045

Program Studi : Matematika

Fakultas : Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Amanto, S.Si., M.Si.
NIP. 19730314 200012 1 002

Dorrah

Dra. Dorrah Aziz, M.Si.
NIP. 19610128 198811 2 001

2. Ketua Jurusan Matematika

Dra. Wamiliana, M.A., Ph.D.
NIP. 19631108 198902 2 001

MENGESAHKAN

1. Tim Penguji

   Ketua : **Amanto, S.Si., M.Si.** ....

   Sekretaris : **Dra. Dorrah Aziz, M.Si.** ....

   Penguji
   Bukan Pembimbing : **Drs. Tiryono Ruby, M.Sc., Ph.D.** ....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

   Prof. Warsito, S.Si., D.E.A., Ph.D.
   NIP. 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : **25 Januari 2018**

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **"BILANGAN ISTIMEWA DI RING $\mathbb{Z}_n$"** merupakan hasil karya saya sendiri dan bukan hasil karya orang lain. Semua hasil tulisan yang tertuang dalam skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila kemudian hari terbukti bahwa skripsi ini merupakan hasil salinan atau dibuat oleh orang lain, maka saya bersedia menerima sanksi sesuai dengan ketentuan akademik yang berlaku.

Bandar Lampung, Januari 2018

Penulis,

Ecy Ratna Sari
NPM. 1417031045

RIWAYAT HIDUP

Penulis dilahirkan di Bandar Lampung pada tanggal 27 Februari 1996 dengan nama lengkap Ecy Ratna Sari dan merupakan anak ketiga dari 3 bersaudara, dari pasangan Bapak Firdaus dan Ibu Paula Sari.

Penulis mengawali pendidikan Taman Kanak-kanak di TK Kartika Jaya II-26 Bandar Lampung pada tahun 2001-2002, Sekolah Dasar di SD Kartika Jaya II- 5 Bandar Lampung pada tahun 2002-2008, kemudian pendidikan menengah di SMP Kartika Jaya II-2 Bandar Lampung pada tahun 2008-2011, dan pendidikan lanjutan di SMA Negeri 9 Bandar Lampung pada tahun 2011-2014.

Pada tahun 2014 penulis melanjutkan pendidikan Strata Satu (S1) Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung melalui jalur SNMPTN. Penulis aktif dalam beberapa organisasi, yaitu menjadi anggota Generasi Muda Matematika, serta menjabat sebagai anggota Kementrian Komunikasi dan Infomasi BEM U KBM Universitas Lampung periode 2017-2018.

Penulis melaksanaan kerja praktik pada tanggal 1 Februari 2017 sampai dengan 27 Februari 2017 di Kantor Perwakilan Bank Indonesia (KPw BI) Provinsi

Lampung bertempat di Jalan Hasanuddin No. 38 Bandar Lampung. Dan mengikuti kuliah kerja nyata (KKN) periode II tahun 2017 pada tanggal 24 Juli sampai 31 Agustus 2017, ditempatkan selama 40 hari di Desa Sidomulyo, Kecamatan Sidomulyo, Kabupaten Lampung Selatan, Lampung.

PERSEMBAHAN

Kupersembahkan karya kecilku ini dengan ketulusan cinta dan segala kerendahan hati kepada :

Ayah dan Umi tercinta yang dengan segala cinta, doa, dorongan semangat, dan pengorbanan untukku dalam menyelesaikan skripsi ini, serta kakakku Alan Suparnanda dan Ardila Yanti tersayang yang selalu memberi doa, dan semangat, serta setia menunggu atas keberhasilanku

Keluarga Besarku tercinta yang selalu memberikan semangat untuk menyelesaikan skripsi ini

Dosen Pembimbing dan Penguji yang sangat berjasa, seluruh sahabat-sahabatku dan Almamaterku Universitas Lampung

MOTTO

"Sesungguhnya di balik setiap kesulitan ada kemudahan"

(Al-Insyirah:6)

Berusahalah jangan sampai terlengah walau sedetik saja,karena atas kelengahan kita tak akan bisa dikembalikan seperti semula.

SANWACANA

Puji syukur penulis panjatkan atas kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah serta nikmat yang tak kurang-kurangnya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Bilangan Istimewa di Ring $\mathbb{Z}_n$”**. Terselesaikannya skripsi ini tidak terlepas dari bantuan dan kerja sama berbagai pihak yang telah membantu dan memberikan bimbingan, saran maupun motivasi sehingga skripsi dapat diselesaikan. Oleh karena itu, dalam kesempatan ini penulis ingin mengucapkan terimakasih kepada :

1. Bapak Amanto, S.Si., M.Si., selaku dosen pembimbing I yang tidak hanya memberikan bimbingan serta motivasi, tetapi juga telah banyak membantu mempermudah penulis selama proses penulisan skripsi.
2. Ibu Dra. Dorrah Aziz, S.Si., M.Si., selaku dosen pembimbing II dan dosen pembimbing akademik yang telah memberikan bimbingan dan arahan selama proses penulisan skripsi.
3. Bapak Drs. Tiryono Rubby, Ph.D., selaku dosen penguji yang telah memberikan ide, kritik dan saran yang membangun serta membimbing penulis sehingga terselesainya skripsi ini.
4. Ibu Dra. Wamiliana, M.A., Ph.D., selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
5. Bapak Prof. Warsito, S.Si., D.E.A., Ph.D., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam.

6. Ayah dan Umi yang selalu mendukung, menemani, mendoakan serta memberikan semangat dengan penuh kasih sayang sehingga menguatkan penulis dalam menjalani setiap proses meraih gelar sarjana.
7. Wika, Syafa, Magdalena, Dea yang menemani suka duka penulis selama di Lampung serta memberikan masukan, semangat, saran dan mendengarkan keluhan penulis.
8. Amoy, Olin, Yola, Ananda, Maget, Pule, Tika, Hage, Arif, Zulfi, Widi, Kiki, Fajar dan keluarga besar Matematika 2014 yang telah membuat "Matematika" menjadi tidak suram.
9. Seluruh serta seluruh pihak yang telah banyak membantu.

Penulis menyadari bahwa skripsi ini masih banyak kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran. Terimakasih.

Bandar Lampung,   Januari 2018

Penulis

Ecy Ratna Sari

DAFTAR ISI

Halaman

DAFTAR SIMBOL DAN SINGKATAN

$a \mid b$	:	*a* membagi habis *b* atau *b* habis dibagi *a*
$\mathbb{Z}_n$	:	Himpunan semua bilangan bulat
$a \nmid b$	:	*a* tidak membagi habis *b*
$\mathbb{Z}$	:	himpunan semua bilangan bulat
mod	:	modulo
$a \equiv b \pmod{m}$	:	*a* berelasi kongruen dengan *b* modulo *m*
$\in$	:	anggota
$\leq$	:	lebih kecil atau sama dengan
$\geq$	:	lebih besar atau sama dengan
gcd	:	*greatest common divisor*
FPB	:	factor persekutuan terbesar
$\forall$	:	untuk setiap
$\exists$	:	terdapat

I. PENDAHULUAN

1.1 Latar Belakang dan Masalah

Dalam kehidupan sehari- hari, manusia tidak lepas dari berbagai masalah yang menyangkut berbagai aspek penyelesaiannya perlu pemahaman melalui sesuatu metode dan ilmu bantu tertentu. Matematika merupakan salah satu cabang ilmu yang mendasari berbagai macam ilmu lain. Seiring dengan perkembangan zaman, keilmuan matematika juga berkembang dalam konsep dan penerapannya. Salah satu dari cabang - cabang ilmu tersebut adalah struktur aljabar . Dalam struktur aljabar dikenal istilah grup, subgrup, ring, subring, homomorfisma, grup faktor, ring faktor, ideal, ideal prima, ideal maksimal, dan masih banyak lagi. Ring merupakan suatu himpunan dan dua operasi yang biasa. Sebagai contoh himpunan bilangan bulat ($\mathbb{Z}$) dengan operasi penjumlahan aritmatika yang biasa berlaku pada himpunan bilangan-bilangan bulat.

Di teori bilangan akan di perkenalkan berbagai macam bilangan, salah satunya bilangan istimewa. Sementara itu, pada artikel yang berjudul bilangan $a^2 + b^2 - dc^2$. Nowcki memperkenalkan konsep bilangan istimewa. Dimana bilangan bulat positif d adalah istimewa jika setiap bilangan bulat m dinyatakan sebagai $m = a^2 +$

$b^2 - dc^2$ untuk bilangan bulat $a, b,$ dan c tidak nol. Oleh karena itu akan dilakukan pengujian dari bilangan bulat (n, d) dengan n ≥ 2, maka setiap bilangan bulat m terdapat $a, b,$ dan c di ring $\mathbb{Z}_n$ yang memenuhi $a^2 + b^2 - dc^2 \equiv m(\text{mod } n)$. Sehingga dalam penelitian ini penulis akan mengkaji karakteristik bilangan istimewa di ring $\mathbb{Z}_n$.

1.2 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah mengkaji karakteristik bilangan istimewa di ring $\mathbb{Z}_n$.

1.3 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut :

1. Menambah pengetahuan agar dapat mengembangkan ilmu yang diperoleh selama mengikuti perkuliahan di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
2. Menambah wawasan tentang materi struktur aljabar, khususnya pada bilangan istimewa di ring $\mathbb{Z}_n$.

II. TINJAUAN PUSTAKA

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 $a \nmid b$. (Burton, 1980).

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. Fakta sederhana yang diturunkan langsung dari definisi 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 yang terdapat pada Definisi 2.1.1, maka berikut ini akan diberikan teorema tentang keterbagian.

Teorema 2.1.1 (Sukirman, 1997)

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*.

Bukti.

1. Jika $a = 1$ atau $a = -1$, maka jelas bahwa $a|1$, sesuai penjelasan sebelumnya. Sebaliknya, diketahui $a|1$ berarti ada $k \in \mathbb{Z}$ sehingga 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 :

$$bd = (k_1 k_2)ac \text{ yaitu } ac|bd.$$

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

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

Persamaan (2.1) disubstitusikan ke persamaan (2.2), sehingga diperoleh

$$c = k_2 b = k_2(k_1 a) = (k_1 k_2)a = ka. \qquad \blacksquare$$

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 $a = -b$. $\blacksquare$

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 $a|(bx + cy)$. $\blacksquare$

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

$$a|(b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$$

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

2.2 Modulo

Modulo adalah suatu metode dalam ilmu matematika yang menyatakan suatu sisa bilangan bulat jika dibagi dengan bilangan bulat yang lain.

Definisi 2.2.1 :

Misalkan didefinisikan a adalah bilangan bulat dan m adalah bilangan bulat > 0. 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 modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m - 1\}$ (Grillet, 2007).

2.3 Relasi Kongruensi

Misalkan a dan b adalah bilangan bulat dan m bilangan bulat m [0, a kongruen dengan b mod m, dituliskan dengan $a \equiv b \pmod{m}$ jika m habis membagi $a - b$. Kekongruenan $a \equiv b \pmod{m}$ dapat pula dituliskan dalam hubungan $a = b + km$ yang dalam hal ini k adalah bilangan bulat.

Sifat-sifat dasar kongruensi :

Misalkan m adalah bilangan bulat positif

1. $a \equiv a \pmod{m}$ (Refleksif)

Bukti :

$a \equiv a \pmod{m}$, sebab $m \mid a - a$ ■

2. $a \equiv b \pmod{m}$ jika dan hanya jika $b \equiv a \pmod{m}$ (Simetris)

Bukti :

$a \equiv b \pmod{m}$ dengan didefinisikan $m \mid a - b$

$m \mid a - b$, $\exists\, k \in \mathbb{Z}$

$a - b = km$

$-a + b = -km$

$b - a = (-k)m$ dengan $k \in \mathbb{Z}$ dan $k \in \mathbb{Z}$

$m \mid b - a \rightarrow b \equiv a \pmod{m}$ ■

3. Jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$ maka $a = c \pmod{m}$ (Transitif)

Bukti :

$a \equiv b \pmod{m}$ dengan didefinisikan $m \mid a - b$

$m \mid a - b$, berarti $\ni k_1 \in \mathbb{Z}$ $dengan\ a - b = k_1 m$

$$a = b + k_1 m \tag{2.5}$$

$b \equiv c \pmod{m}$ dengan didefinisikan $m \mid b - c$

$m \mid b - c$, berarti $\ni k_2 \in \mathbb{Z}$ $dengan\ b - c = k_2 m$

$$b = c + k_2 m \tag{2.6}$$

$a = (c + k_2 m) + k_1 m$

$a = c + (k_2 m + k_1 m)$

$a = c + m(k_2 + k_1)$

$a - c = m(k_2 + k_1)$

Karena $\exists\ (k_1 + k_2) \in \mathbb{Z}$ dengan $a - c = m(k_2 + k_1)$ berarti ini $m \mid a - c$

Jadi $a \equiv c \pmod{m}$ ■

Teorema 2.3.1

Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \pmod{m}$ dan c adalah sembarang 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

$a + c = b + c + km$

$\Leftrightarrow a + c = (b + c) \pmod{m}$ ■

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

$\Leftrightarrow a = b + km$, untuk suatu $k \in \mathbb{Z}$

$\Leftrightarrow a - b = km$

$\Leftrightarrow (a - b)\, c = c(km)$

$\Leftrightarrow ac - bc = c(km)$

$\Leftrightarrow ac = bc + c(km)$

$\Leftrightarrow ac = bc + lm$, dengan $l = ck$

$\Leftrightarrow ac \equiv bc \pmod{m}$ ■

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

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

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

Dengan Koefisien Binomial yaitu :

$a^p = \sum_{j=0}^{p} \binom{p}{j} b^{p-j}(km)^j$

$= \binom{p}{0} b^{p-0}(km)^0 + \binom{p}{1} b^{p-1}(km)^1 + \binom{p}{2} b^{p-2}(km)^2 + \cdots +$

$\binom{p}{p-1} b^{p-(p-1)}(km)^{(p-1)} + \binom{p}{p} b^{p-p}(km)^p$

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

$(km)^p$

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

$\left. k^p m^{p-1}\right\}$

$\Leftrightarrow a^p \equiv b^p (\bmod)\ m$ ■

2. (i) $a \equiv b(\bmod m) \Leftrightarrow a = b + k_1 m$, untuk suatu $k_1 \in \mathbb{Z}$

$c \equiv d(\bmod m) \Leftrightarrow c = d + k_2 m$, untuk suatu $k_2 \in \mathbb{Z}$

$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$

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

$$\Leftrightarrow (a+c) = (b+d)(\text{mod } m) \qquad \blacksquare$$

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

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

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

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

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

$$\Leftrightarrow a \cdot c \equiv bd(\text{mod } m) \qquad \blacksquare$$

2.4 Bilangan Prima

Definisi 2.4.1

Sebuah bilangan bulat $p > 1$ disebut bilangan prima, jika dan hanya jika *p* habis dibagi dengan 1 dan bilangan p sendiri (Burton,1980).

Definisi 2.4.2 (Relatif Prima)

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

Teorema 2.4.1

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

Bukti:

Karena *a* dan *b* relatif prima maka $\text{fpb}(a, b) = 1$. Identitas Bezout menjamin adanya bilangan bulat *x, y* sehingga $1 = ax + by$. Sebaliknya, misalkan ada bilangan bulat $ax + by = 1$. Dibuktikan $\text{fpb}(a, b) = d = 1$. 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 2.4.2, maka berikut ini akan diberikan teorema tentang relatif prima.

Teorema 2.4.2

Jika $\text{fpb}(a, b) = 1$, maka berlaku pernyataan berikut

1. Jika $a|c$ dan $b|c$ maka $ab|c$
2. Jika $a|bc$ maka $a|c$ (Lemma Euclid)

(Sukirman, 1997).

Bukti:

1. Diketahui $a|c$ dan $b|c$. Artinya terdapat $r, s \in \mathbb{Z} \ni c = a \cdot r = b \cdot s$. Berdasarkan hipotesis, $\text{fpb}(a, b) = 1$. Oleh karena itu dapat dituliskan $ax + by = 1$ untuk suatu bilangan bulat *x* dan *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 $a|bc$, $\text{fpb}(a,b) = 1$. 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 $a|c$ ■

2.5 Faktor Persekutuan Besar (FPB)

Definisi 2.5.1

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

1. $d \mid a$ dan $d \mid b$

2. Jika $c \mid a$ dan $c \mid b$ maka $c \leq d$

Pada definisi ini, syarat 1 menyatakan bahwa *d* adalah faktor persekutuan dan syarat 2 menyatakan bahwa *d* adalah faktor persekutuan terkecil diantara semua faktor persekutuan yang ada. Selanjutnya jika d faktor persekutuan terbesar dari a dan b akan ditulis d = gcd (a,b) (Sukirman,1997).

Teorema 2.5.1 (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.

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

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

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

……

$r_{n-2} = q_n r_{n-1} + r_n$ $\quad 0 < r_n < r_{n-1}$

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

maka r_n, sisa terakhir dari pembagian di atas yang bukan nol merupakan gcd (a,b) (Graham, 1975).

Teorema 2.5.2

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

$$\gcd(a,b) = ax + by \tag{2.7}$$

Persamaan (2.7) 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 (2.7) 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 $d = \gcd(a, b)$.

2.6 Ring

Sebelum membahas tentang ring , akan diberikan terlebih dahulu definisi tentang grup berikut:

Definisi 2.6.1

Suatu grup <G, *> adalah himpunan G yang diperlengkapi dengan operasi biner * pada G yang memenuhi aksioma-aksioma berikut:

1. Operasi biner * asosiatif, yaitu $\forall$ a, *b*, c $\in$ G berlaku : (a*b)*c = a*(b*c)
2. Terdapat elemen identitas e untuk * pada G, yaitu terdapat e $\in$ G sedemikian sehingga

   e*a = a*e = a, $\forall$ a $\in$ G

3. Untuk setiap a $\in$ G mempunyai invers a^{-1}, yaitu terdapat $a^{-1} \in$ G sedemikian hingga

$$a*a^{-1} = a^{-1} * a = e$$

(Dummit and Foote, 2004).

Definisi 2.6.2

Suatu grup G disebut abelian (komutatif) jika operasi biner * pada G adalah komutatif, yaitu $\forall$ a,b $\in$ G maka a * b = b*a.

Contoh :

Didefinisikan himpunan $S = \{x \in R \mid x \neq -1\}$. Selanjutnya didefinisikan * pada S, dengan

$$a * b = a + b + ab$$

Tunjukkan $< S,*,>$ grup komutatif.

Bukti:

Harus dipenuhi aksioma grup berikut:

1. Tertutup, yaitu ($\forall$ a, b $\in$ S) ($a * b$) $\in S$

Bukti :

Diketahui $a * b = a + b + ab$. Akan dibuktikan dengan kontradiksi.

Andaikan $a * b = -1$

$$\Leftrightarrow a + b + ab = -1$$

$$\Leftrightarrow a + ab = -1 - b$$

$\Leftrightarrow a\,(1 + b) = -(1 + b),\ b \neq -1$

$\Leftrightarrow a = -1$, kontradiksi.

Jadi pengandaian salah, yang benar $a + b + ab \neq -1$ Dengan kata lain $a * b \in S$. ■

2. Asosiatif, yaitu ($\forall$ a, b, c $\in$ S) (a $*$ b) $*$ c = a $*$ (b $*$ c)

   Bukti :

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a + b + c + bc + ab + ac + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c)\ .\end{aligned}$$ ■

3. Terdapat elemen netral / identitas, yaitu ($\forall$ a $\in$ S, $\exists$ y $\in$ S) y $*$ a = a $*$ y = a

   Bukti :

Misal y elemen netral untuk $*$ dari S, maka :

$\Leftrightarrow y * a = a$

$\Leftrightarrow y + a + ya = a$

$\Leftrightarrow y + ya = 0$

$\Leftrightarrow y(1 + a) = 0$

$y = 0$ atau $(1 + a) = 0$

$(1 + a) = 0$ tidak mungkin, sebab $a \neq -1$.

Oleh karena itu, satu – satunya penyelesaian persamaan di atas adalah y = 0 yang merupakan elemen netral $*$ pada S. ■

4. Terdapat invers, yaitu ($\forall\ a \in S, \exists\ z \in S$) $z * a = a * z = 0$

Bukti :

$\Leftrightarrow z * a = 0$

$\Leftrightarrow z + a + za = 0$

$\Leftrightarrow z + za = -a$

$\Leftrightarrow z(1 + a) = -a$

$\Leftrightarrow z = \dfrac{-a}{1+a}$, apakah z $\in$ S ? atau z $\neq -1$?

Andaikan z = –1, maka

$\Leftrightarrow \dfrac{-a}{1+a} = -1$

$\Leftrightarrow -a = -(1 + a)$

$\Leftrightarrow -a = -1 - a$

0 = –1, Kontradiksi.

Jadi yang benar z $\neq -1$, dengan kata lain $z \in S$. ■

5. Komutatif, yaitu ($\forall$ a, b $\in$ S) a $*$ b = b $*$ a

Bukti :

$$\begin{aligned} a * b &= a + b + ab \\ &= b + a + ba \\ &= b * a\ . \end{aligned}$$

Berdasarkan (1) sd (5), maka disimpulkan $< S, * >$ grup komutatif . ■

Selanjutnya diberikan definisi ring sebagai berikut.

Definisi 2.6.3

Himpunan R dengan dua operasi biner + (penjumlahan) dan $\bullet$ (perkalian) atau ditulis $\langle R, +, \bullet \rangle$ merupakan ring jika memenuhi aksioma berikut:

1. $\langle R, + \rangle$ merupakan grup komutatif;
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 $a \bullet (b + c) = (a \bullet b) + (a \bullet c)$

Contoh :

Didefinisikan himpunan $S = \{x \in R \mid x \neq -1\}$. Selanjutnya didefinisikan dua operasi pada S, yaitu $*$ dan $\bullet$ dengan definisi :

i. $a * b = a + b + ab$

ii. $a \bullet b = 0, \forall\, a, b \in S$

Pasangan $\langle R, +, \bullet \rangle$ membentuk ring.

(Dummit and Foote, 2004).

2.7 Ring $\mathbb{Z}_n$

Himpunan bilangan bulat modulo n

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

Dengan operasi biner penjumlahan dan perkalian yang didefinisikan sebagai berikut

$$a + b \equiv (a+b) \bmod n \text{ dan } a \cdot b \equiv ab \bmod n$$

Untuk setiap $a, b \in \mathbb{Z}_n$ (Fraleight, 2000).

III. METODE PENELITIAN

3.1 Waktu dan Tempat

Penelitian ini dilakukan di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung pada semester ganjil tahun ajaran 2017/2018.

3.2 Metode Penelitian

Langkah-langkah yang digunakan dalam menyelesaikan tugas akhir ini adalah:

1. Mengkaji konsep bilangan berbentuk $a^2 + b^2 - dc^2$
2. Mengkaji karakteristik unit-bilangan istimewa di ring $\mathbb{Z}_n$
3. Menemukan bilangan istimewa d yang memenuhi persamaan $a^2 + b^2 - dc^2 \equiv m (mod\ n)$

V. KESIMPULAN

Dari hasil dan pembahasan pada bab sebelumnya dapat disimpulkan bahwa :

1. Bilangan Istimewa d adalah persamaan yang memenuhi $a^2 + b^2 - dc^2 \equiv m(\text{mod } n)$.
2. Pada Ring $\mathbb{Z}_n$, n yang digunakan yaitu 7,11,19,29,31,37,41,43,47 dimana n merupakan bilangan prima dan tidak dibagi dengan 2,3,4,5.

DAFTAR PUSTAKA

Burton, D.M. 1980. *Elementary Number Theory.* University Of New Hampshire.United State of Afrika.

Dudley, Underwood. 1969. *Elementary Number Theory*. W.H. Ferman and Company, San Fransisco.

Dummit, D.S., Foote, R.M. 2004. *Abstract Algebra* . Third Edition. Y&Y. United states of America.

Fraleigh, J.B. 2000. *A First Course In Abstract Algebra.* Sixth Edition. Addison Wesley Publishing Company, Inc. Philippines

Graham, M. 1975. *Modern Elementary Mathematics*. Harcort Brace Jonanovich, inc. New York.

Sukirman, M. P. 1997. *Ilmu Bilangan.* Universitas Terbuka. Jakarta.