REPRESENTASI BILANGAN BULAT SEBAGAI JUMLAH DARI DUA BILANGAN KUADRAT DALAM RING BILANGAN BULAT MODULO n

(Skripsi)

Oleh

NEVI SETYANINGSIH

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

ABSTRAK

REPRESENTASI BILANGAN BULAT SEBAGAI JUMLAH DARI DUA BILANGAN KUADRAT DALAM RING BILANGAN BULAT MODULO n

Oleh

Nevi Setyaningsih

Ring bilangan bulat modulo n adalah salah satu ring dalam struktur aljabar yang dikembangkan dari ring Z dengan penggunaan konsep modulo n. Penelitian ini membahas tentang representasi bilangan bulat sebagai jumlah dari dua bilangan kuadrat dalam ring bilangan bulat modulo n. Metode yang digunakan pada penelitian ini adalah mencari 25 nilai pertama n yang memenuhi bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat dinyatakan sebagai jumlah dua bilangan kuadrat dengan menggunakan *software matlab* berdasarkan teorema dan konsep modulo. Pembahasan dalam penelitian ini dibagi menjadi dua kasus representasi elemen ring $\mathbb{Z}_n$ sebagai penjumlahan dari dua bilangan kuadrat yaitu: harus solusi non trivial dan boleh solusi trivial.

Kata Kunci: Ring $\mathbb{Z}_n$, modulo n, bilangan bulat, penjumlahan dua bilangan kuadrat, penjumlahan operasi biner.

ABSTRACT

REPRESENTING INTEGERS AS THE SUM OF TWO SQUARES IN THE RING OF MODULO n

By

Nevi Setyaningsih

The ring of integers modulo n is also the ring one of in algebra structure is reconstructed from ring Z by using modular concept. This paper will discuss about representation integers as the sum of two squares in the ring of modulo n. The methods of this paper are finding the first 25 values of n which holds that every element ring of integers modulo n can be represented as the sum of two squares by using *matlab software* based on the theorems and concepts associated. Solving in this paper is divided into two case are representation of element in ring $\mathbb{Z}_n$ as the sum of two squares: must have non trivial solution and may have trivial solution.

Keyword : Ring $\mathbb{Z}_n$, modulo, integer, the addition of squares number, the addition of binary operation.

REPRESENTASI BILANGAN BULAT SEBAGAI JUMLAH DARI DUA BILANGAN KUADRAT DALAM RING BILANGAN BULAT MODULO n

Oleh

NEVI SETYANINGSIH

Skripsi

Sebagai Salah Satu Syarat untuk Memperoleh Gelar

SARJANA MATEMATIKA

Pada

Jurusan Matematika

Fakultas Matematika dan Ilmu Pengetahuan Alam

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

Judul	:	**Representasi Bilangan Bulat Sebagai Jumlah dari Dua Bilangan Kuadrat dalam Ring Bilangan Bulat Modulo n**
Nama Mahasiswa	:	*Novi Setyaningsih*
NPM	:	1417031083
Jurusan	:	Matematika
Fakultas	:	Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Amanto, S.Si., M.Si.	**Drs. Suharsono S., M.S., M.Sc., Ph.D.**
NIP 19730314 200012 1 002	NIP 19620513 198803 1 003

2. Mengetahui

Ketua Jurusan Matematika

Dra. Wamiliana, M.A.,Ph.D.
NIP. 196311081989022001

MENGESAHKAN

1. Tim Penguji

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

Sekretaris : **Drs. Suharsono S., M.S., M.Sc., Ph.D.** .....

Penguji
Bukan Pembimbing : **Dr. Asmiati, S.Si., M.Si.** .....

Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

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

Tanggal Lulis Ujian Skripsi : **24 Januari 2018**

PERNYATAAN SKRIPSI MAHASISWA

Yang bertanda tangan di bawah ini :

Nama	: **Nevi Setyaningsih**
Nomor Pokok Mahasiswa	: **1417031083**
Jurusan	: **Matematika**
Judul Skripsi	: **Representasi Bilangan Bulat Sebagai Jumlah dari Dua Bilangan Kuadrat dalam Ring Bilangan Bulat Modulo *n***

Dengan ini menyatakan bahwa skripsi ini adalah hasil pekerjaan saya sendiri dan semua tulisan yang tertuang dalam skripsi ini telah mengikuti kaidah karya penulisan ilmiah Universitas Lampung.

Bandar Lampung, 24 Januari 2018
Penulis

Nevi Setyaningsih
NPM. 1417031083

RIWAYAT HIDUP

Penulis dilahirkan di Negeri Batin, Kecamatan Blambangan Umpu pada tanggal 28 Maret 1996, sebagai anak pertama dari dua bersaudara, putri dari pasangan Bapak Agus Setiyanto dan Ibu Suliyem.

Pendidikan Taman Kanak – Kanak (TK) Xaverius Metro pada tahun 2002, Pendidikan Sekolah Dasar (SD) Negeri 1 Negeri Batin pada tahun 2008, Sekolah Menengah Pertama (SMP) Negeri 1 Way Jepara pada tahun 2011, Sekolah Menengah Atas (SMA) Negeri 1 Blambangan Umpu pada tahun 2014. Kemudian penulis melanjutkan pendidikan di perguruan tinggi dan terdaftar sebagai mahasiswa Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung pada tahun 2014.

Selama menjadi mahasiswa, penulis pernah bergabung menjadi anggota di Himpunan Mahasiswa Jurusan Matematika (HIMATIKA). Selain itu penulis juga pernah bergabung di Badan Eksekutif Mahasiswa (BEM) Unila yang diamanahkan menjadi anggota Koordinator Internal 2015-2016.

Sebagai bentuk aplikasi bidang ilmu kepada masyarakat, penulis telah melaksanakan Kuliah Kerja Nyata (KKN) selama 40 hari pada awal tahun 2017 di Desa Sendang Mukti, Kecamatan Sendang Agung, Kabupaten Lampung Tengah. Dan Sebagai bentuk aplikasi bidang ilmu di dunia kerja, penulis telah melaksanakan Kerja Praktik (KP) selama 40 hari pada bulan Juli hingga Agustus 2017 di Badan Pengelola Pajak dan Retribusi Daerah Kota Bandar Lampung.

KATA INSPIRASI

"Dia memberi kekuatan kepada yang lelah dan menambah semangat kepada yang tiada berdaya."
(Yesaya 40:29)

"Ada tiga cara untuk mendapatkan kebijaksanaan. Pertama adalah refleksi, yang merupakancara tertinggi. Kedua adalah pembatasan, yang merupakan cara termudah. Ketiga adalah pengalaman, yang merupakan cara terpahit"
Confucius (Kong Hu Chu)

"Tetap sabar, semangat, dan tersenyum, karena kamu sedang menimba ilmu di Universitas kehidupan. Allah menaruhmu di tempatmu yang sekarang bukan karena kebetulan."
(Dahlan Iskan)

PERSEMBAHAN

Puji syukur kepada Tuhan Yang Maha Esa, karena atas limpahan berkah dan rahmad-Nya skripsi ini dapat diselesaikan.

Aku persembahkan karya sederhana penuh perjuangan dan kesabaran ini sebagai ungkapan rasa sayang dan bakti kepada :

Bapak, Ibu, Kakung dan Uti tercinta yang selalu mecurahkan kasih sayang, memberi semangat dan selalu memotivasi, serta dalam doa dan sujud yang selalu menantikan keberhasilanku dengan sabar dan penuh pengertian.

Almamater yang kucintai, Universitas Lampung.

SANWACANA

Penulis ucapkan puji dan syukur ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan berkat dan kasih karunia kepada penulis sehingga penulis dapat menyelesaikan skripsi ini. Skripsi dengan judul **"Representasi Bilangan Bulat sebagai Jumlah dari Dua Bilangan Kuadrat dalam Ring Bilangan Bulat Modulo n"** disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Matematika (S. Mat.) di Universitas Lampung.

Selesainya penulisan skripsi ini, adalah juga berkat motivasi dan pengarahan serta bimbingan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Amanto, S,Si., M,Si. selaku Pembimbing I, atas segala bantuan dan waktunya untuk membimbing, memberi arahan, nasehat, dan juga motivasi dalam menyelesaian skripsi ini;
2. Bapak Drs. Suharsono S., M.S., M.Sc., Ph.D. selaku Pembimbing II atas bimbingan dan saran selama penyusunan skripsi ini;
3. Ibu Dr. Asmiati, S.Si., M.Si. selaku Pembahas atas saran yang membangun dalam proses penyelesaian skripsi ini;
4. Ibu Dian Kurniasari., S.Si.,M.Sc. selaku Dosen Pembimbing Akademik;
5. Ibu Dra. Wamiliana, M.A.,Ph.D. selaku Ketua Jurusan Matematika;

6. Seluruh Dosen, staff dan karyawan Jurusan Matematika FMIPA Universitas Lampung;
7. Ibu, Bapak dan Uti, Kakung tercinta yang telah membesarkan penulis, juga atas doa, cinta, semangat, pengorbanan yang luar biasa, serta Adik tersayang yang selalu memberikan kasih sayang kepada penulis;
8. Yohan Abram Kardela yang selalu memberikan waktu, semangat dan motivasi kepada Penulis;
9. Sahabat-sahabat satu perjuangan Vindi, Fara, Shelvi, Tewe, Kurdes, Abror, Rahmad, Indri, Lucia, Darma, Nandra, Riya, Susan, Kasandra, Septi, Rere, Otin, Vivin, Ketut, Agus serta yang lainnya terima kasih banyak atas dukungan, doa, dan semangatnya, juga atas kebersamaan yang luar biasa selama ini;
10. Sahabat-sahabatku Meli, Okta, Putri, Mbak Intan, Mbak Karina, Mbak Tia, Mbak Klara, dan Siska atas kebersamaan selama ini juga atas semangat yang telah diberikan kepada penulis;
11. Teman-teman Matematika 2014 atas kebersamaan serta keceriaan yang telah diberikan kepada penulis selama menempuh pendidikan di Universitas Lampung.

Bandar Lampung, Januari 2018
Penulis

Nevi Setyaningsih

DAFTAR ISI

Halaman

DAFTAR SIMBOL

$a \mid b$	:	*a* membagi habis *b* atau *b* habis dibagi *a*
$\mathbb{Z}_n$	:	{0, 1, 2, …., n-1}
$a \nmid b$	:	*a* tidak membagi habis *b*
$\mathbb{Z}$	:	himpunan semua bilangan bulat
Mod	:	Modulo
$\equiv$	:	Kongruen
$a \equiv b \pmod{m}$	:	*a* berelasi kongruen dengan *b* modulo *m*
$\in$	:	Anggota
$\leq$	:	lebih kecil atau sama dengan
$\geq$	:	lebih besar atau sama dengan
$\ni$	:	Sedemikian sehingga
FPB	:	faktor persekutuan terbesar
$\forall$	:	untuk setiap
$\exists$	:	Terdapat
$+_n$	:	Penjumlahan terhadap modulo n
$\cdot_n$	:	Perkalian terhadap modulo n

I. PENDAHULUAN

1.1 Latar Belakang

Matematika merupakan ilmu mengenai besaran pola, struktur, ruang, dan perubahan. Matematika pada umumnya dapat dibagi menjadi matematika murni dan terapan. Matematika murni terfokus pada pembentukan teori-teori yang lebih bersifat abstrak dan tidak secara langsung dapat menggambarkan realita kehidupan, sedangkan matematika terapan merupakan pengembangan dari matematika murni sehingga dapat menjelaskan dan menginterpretasikan fenomena yang terjadi dalam kehidupan nyata.

Salah satu cabang matematika murni adalah teori bilangan. Teori bilangan lebih terfokus pada sifat-sifat dan pola bilangan bulat. Dalam teori bilangan dikenal istilah keterbagian, modulo, bilangan prima dan masih banyak lagi lainnya. Bilangan prima merupakan salah satu objek yang dipelajari teori bilangan dan memiliki sifat yang unik yaitu hanya dapat dibagi oleh satu dan bilangan itu sendiri. Bilangan prima juga merupakan faktor penyusun bilangan bulat positif. Setiap bilangan bulat positif dapat dinyatakan secara unik sebagai hasil perkalian dari satu atau beberapa bilangan bulat tanpa memperhatikan urutannya. Bilangan prima memiliki sifat yang khas dalam teori bilangan baik dalam keterbagian, modulo, ataupun materi lainnya. Sehingga konsep

bilangan prima dapat menghasilkan teorema-teorema yang penting dan mendorong berkembangnya konsep teori bilangan.

Penerapan sifat-sifat dan teorema dalam keterbagian dan modulo dapat mempermudah dalam mengkaji salah satu topik dalam teori bilangan yaitu representasi bilangan bulat positif sebagai jumlah dari dua bilangan kuadrat. Kemudian dapat dikembangkan dari objek yang semula bilangan bulat Z menjadi bilangan bulat $\mathbb{Z}_n$. Ring $\mathbb{Z}_n$ merupakan salah satu ring yang istimewa dengan operasi biner penjumlahan dan perkalian terhadap modulo n. Ring $\mathbb{Z}_n$ adalah salah satu ring dalam struktur aljabar yang dikembangkan dari ring Z dengan penggunaan konsep modulo.

Oleh karena itu, dalam penelitian ini penulis akan mengkaji tentang bilangan bulat yang dapat di representasikan sebagai penjumlahan dari dua bilangan kuadrat dalam ring $\mathbb{Z}_n$.

1.2 Tujuan Penelitian

1. Memperoleh 25 bilangan asli pertama n dimana $1 \leq n \leq 100, n \in \mathbb{Z}_n$ dari setiap elemen dalam ring $\mathbb{Z}_n$ yang dapat di representasikan sebagai jumlah dari dua bilangan kuadrat.
2. Mendapatkan representasi dari setiap elemen dalam ring $\mathbb{Z}_n$ dimana $1 \leq n \leq 100, n \in \mathbb{Z}_n$ sebagai penjumlahan dua bilangan kuadrat.

1.3 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Menambah pengetahuan dan pengalaman penulis agar dapat mengembangkan ilmu yang diperoleh selama mengikuti perkuliahan di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
2. Mempelajari lebih dalam lagi tentang konsep konsep modulo dalam penjumlahan dua bilangan kuadrat dan representasi untuk nilai khusus dari n bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat ditulis sebagai jumlah dari dua bilangan kuadrat.

II. TINJAUAN PUSTAKA

Pada bab ini akan diberikan beberapa konsep keterbagian dan modulo, Ring bilangan bulat pada modulo *n* dan aritmatika modulo yang akan digunakan dalam pembahasan hasil penelitian.

2.1 Keterbagian dan Modulo

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 $1|a$berarti bahwa 1 merupakan faktor atau pembagi dari bilangan apapun termasuk bilangan 0. Fakta $a|a$ berarti 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 dan 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:

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

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

Definisi 2.1.2

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

Definisi 2.1.3 (Relatif Prima)

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

Teorema 2.1.2

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 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 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 2.2.2, maka berikut ini akan diberikan teorema tentang relatif prima.

Teorema 2.1.3

Jika 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 $r, s \in \mathbb{Z} \exists\, c = a \cdot r = b \cdot s$. Berdasarkan hipotesis, fpb$(a, b) = 1$. Oleh karena itu dapat dituliskan $ax + by = 1$ untuk suatu bilangan bulat *x* dan *y*. Akibatnya

$$\begin{aligned} c = 1 \cdot c &= (ax + by) \cdot c \\ &= acx + bcy \\ &= a(bs)x + b(ar)y \\ &= ab(sx + ry) \end{aligned}$$

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 $a|c$ ■

Definisi 2.1.3 (Modulo)

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

Definisi 2.1.4 (Relasi Kongruensi)

Misalkan *a* dan *b* adalah bilangan bulat dan *m* > 0, *a* dinyatakan kongruen dengan *b* modulo *m* atau ditulis $a \equiv b \pmod{m}$ 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 $a \equiv b \pmod{m}$ dapat pula dituliskan dalam hubungan

$$a = b + km$$

yang dalam hal ini *k* adalah bilangan bulat.

Contoh.

$16 \equiv 4 \pmod 3$ dapat ditulis sebagai $16 = 4 + 4 \cdot 3$

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

$$a \equiv r \pmod m$$

Teorema 2.1.4

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 tidak 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

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

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

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

   $$a = b + km$$

   $$\Leftrightarrow a - b = km$$

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

$\Leftrightarrow ac = bc + Km$, dengan $K = ck$

$\Leftrightarrow ac \equiv bc \ (mod\ m)$

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

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

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

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

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

$$\Leftrightarrow a^p \equiv b^p \pmod m$$

2. (i) $a \equiv b \pmod m \quad \Leftrightarrow a = b + k_1m$

$c \equiv d \pmod m \quad \Leftrightarrow c = d + k_2m$

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

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

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

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

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

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

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

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

$\Leftrightarrow a \cdot c \equiv bd \pmod{m}$ ■

(Grillet, 2007).

Teorema 2.1.5 (Teorema Fermat)

Jika p adalah bilangan prima dan a adalah bilangan bulat positif dimana $p \nmid a$, maka $a^{p-1} \equiv 1 \pmod{p}$ (Burton, 1980).

Bukti.

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

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

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.

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

$$ra \equiv sa \pmod{p}\ ;$$

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

$$r \equiv s \pmod{p}$$

Karena *r* dan *s* harus lebih besar 1 dan harus lebih kecil dari *p*, maka hal ini berakibat

r = *s*. Pernyataan ini kontradiksi dengan asumsi awal bahwa *r* dan *s* harus berbeda. Oleh karena itu, bilangan bulat harus kongruen mod p terhadap 1,2,3,4, ... , $p-1$. Diambil semuanya , kemudian dikalikan semua kongruen, maka diperoleh sebagai berikut

$$a.\,2a.\,3a.\,\ldots(p-1).\,a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) (\text{mod } p)$$

Sehingga,

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

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

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

Contoh 2.1.5

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

Untuk menunjukkan hal di atas, dengan menggunakan relasi kongruensi cukup ditunjukan bahwa $5^{38} \equiv 4 \,(\text{mod } 11)$.

Bukti.

$5^{38} = (5^{10 \text{ x } 3 + 8})$

$= (5^{10})^3 (5^2)^4$

$\equiv 1^3 . 3^4 \,(\text{mod } 11)$

$\equiv 81 \,(\text{mod } 11) \equiv 4 \,(\text{mod } 11)$

Definisi 2.1.5 (Teori Residu Kuadrat)

Diketahui p bilangan prima ganjil dan fpb$(a,p) = 1$. Jika kongruensi kuadrat $x^2 \equiv a(\text{mod } p)$ memiliki solusi, maka a disebut sebagai residu kuadrat p. Selainnya disebut bukan residu kuadrat dari p (Burton, 1980).

Contoh 2.1.5

Selesaikan Kongruensi dari

$$x^2 \equiv 36 \text{ (mod } 45)$$

Bukti.

1. Diketahui fpb $(36,45) = 9$ dan misalkan $x = 3y$.

$$x^2 \equiv 36 \text{ (mod } 45)$$

$$(3y)^2 \equiv 36 \text{ (mod } 45)$$

$$9y^2 \equiv 36 \text{ (mod } 45)$$

Dengan menggunakan salah satu sifat modulo yaitu jika $a \equiv b$ (mod m) dan fpb$(b,m) = c$ maka $\frac{a}{c} \equiv \frac{b}{c}$ (mod $\frac{m}{c}$)

$$y^2 \equiv 4 \text{ (mod } 5)$$

$$y^2 - 4 \equiv 0 \text{ (mod } 5)$$

$$(y+2)(y-2) \equiv 0 \text{ (mod } 5)$$

$$y + 2 \equiv 0 \text{ (mod } 5) \vee y = -2 \equiv \text{(mod } 5)$$

$$y - 2 \equiv 0 \text{ (mod } 5)$$

$$y \equiv \pm 2 \pmod 5$$

$$3y \equiv \pm 6 \pmod{15}$$

$$x \equiv \pm 6 \pmod{15}$$

$$x = 6, 21, 36$$

$$x = 9, 24, 39$$

Jadi, diperoleh $6, 9, 21, 24, 36$ dan 39 adalah solusi dari $x^2 \equiv 36 \pmod{45}$.

Definisi 2.1.6 (Simbol Legendre)

Misalkan p adalah bilangan prima ganjil dan a bilangan bulat. Simbol Legendre dari a dengan memenuhi p didefinisikan oleh

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{jika } (a, p) = 1 \text{ dan } a \text{ adalah residu kuadrat modulo } p \\ -1 & \text{jika } (a, p) = 1 \text{ dan } a \text{ bukan residu kuadrat modulo } p \\ 0 & \text{jika } p \text{ membagi } a \end{cases}$$

(M. Nathanson, 2000).

Teorema 2.1.6 (Teorema Legendre)

Misalkan p adalah bilangan prima ganjil untuk setiap bilangan bulat a,

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p \qquad (2.5)$$

Bukti.

Jika p membagi a, maka kedua ruas (2.5) kongruen terhadap 0. Jika p tidak dapat membagi a, maka dengan Teorema Fermat diperoleh

$$\left(a^{(p-1)/2}\right)^2 \equiv a^{p-1} \equiv 1 \pmod p,$$

Sehingga

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Kemudian diperoleh

$$a^{(p-1)/2} \equiv 1 \pmod{p} \text{ jika dan hanya jika } \left(\frac{a}{p}\right) = 1,$$

$$a^{(p-1)/2} \equiv -1 \pmod{p} \text{ jika dan hanya jika } \left(\frac{a}{p}\right) = -1.$$

Contoh.

3 adalah residu kuadrat modulo bilangan prima 11 dan 13, dan bukan residu kuadrat modulo bilangan prima 17 dan 19, karena

$$\left(\frac{3}{11}\right) \equiv 3^5 \pmod{11} \equiv 1 \pmod{11} = 1,$$

$$\left(\frac{3}{13}\right) \equiv 3^6 \pmod{13} \equiv 1 \pmod{13} = 1,$$

$$\left(\frac{3}{17}\right) \equiv 3^8 \pmod{17} \equiv -1 \pmod{17} = -1,$$

$$\left(\frac{3}{19}\right) \equiv 3^9 \pmod{19} \equiv -1 \pmod{19} = -1.$$

(M. Nathanson, 2000).

Teorema 2.1.7

Misalkan p bilangan prima ganjil, dan misalkan a dan b bilangan bulat. Maka

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Bukti.

Jika p membagi a atau b, maka p membagi ab, dan

$$\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Jika p tidak dapat membagi ab, maka dengan Teorema 2.4.1 diperoleh

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \pmod{p}$$

$$\equiv a^{(p-1)/2} b^{(p-1)/2} \pmod{p}$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

(M. Nathanson, 2000).

Teorema 2.1.8

Misalkan p bilangan prima ganjil. Maka

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{jika } p \equiv 1 \pmod 4, \\ -1 & \text{jika } p \equiv 3 \pmod 4. \end{cases}$$

Ekuivalen dengan

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Bukti.

Diketahui bahwa

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{jika } p \equiv 1 \pmod 4, \\ -1 & \text{jika } p \equiv 3 \pmod 4. \end{cases}$$

Berdasarkan Teorema 2.4.1 dengan $a = -1$, diperoleh

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \pmod{p}$$

(M. Nathanson, 2000).

2.2 Ring Bilangan Bulat Modulo n

Sebelum membahas tentang ring bilangan bulat modulo , akan diberikan terlebih dahulu definisi tentang grup berikut.

Definisi 2.2.1

Suatu grup <G, *> adalah himpunan G yang dilengkapi 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 2.2.2

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 :

$(a * b) * c = (a + b + ab) * c$

$= (a + b + ab) + c + (a + b + ab)c$

$= a + b + ab + c + ac + bc + abc$

$= a + b + c + bc + ab + ac + abc$

$= a + (b + c + bc) + a(b + c + bc)$

$= a * (b + c + bc)$

$= a * (b * c)$. ■

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

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 ($\forall$ $a \in S$, $\exists$ $z \in S$) $a * z = z * a$ = y

Bukti :

$\Leftrightarrow z * a = 0$

$\Leftrightarrow z + a + za = 0$

$\Leftrightarrow z + za = -a$

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

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

Andaikan $z = -1$, maka

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

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

$\Leftrightarrow -a = -1 - a$

$0 = -1$, 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 :

$a * b = a + b + ab$

$= b + a + ba$

$= b * a$.

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

Selanjutnya diberikan definisi ring sebagai berikut.

Definisi 2.2.3

Himpunan R dengan dua operasi biner + (penjumlahan) dan • (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).

Definisi 2.2.4 (Ring $\mathbb{Z}_n$)

Himpunan bilangan bulat modulo n dituliskan dengan

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

Pada $\mathbb{Z}_n$ didefinisikan operasi biner penjumlahan dan perkalian yang didefinisikan sebagai berikut

$$a +_n b = (a + b) \pmod{n} \text{ dan}$$

$$a \cdot_n b = ab \pmod{n}$$

Untuk setiap $a, b \in \mathbb{Z}_n$. Himpunan $< \mathbb{Z}_n, +_n, \cdot_n >$membentuk ring (Fraleight, 2000).

Bukti:

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

Untuk sebarang $a, b \in \mathbb{Z}_n$ didefinisikan operasi biner $+_n$ (penjumlahan) dan $\cdot_n$ (perkalian) pada $\mathbb{Z}_n$

$$a +_n b = (a + b) \pmod n$$

dan

$$a \cdot_n b = ab \pmod n$$

Akan dibuktikan $< \mathbb{Z}_n, +_n, \cdot_n >$ membentuk ring.

A. Akan dibuktikan $< \mathbb{Z}_n, +_n >$ grup komutatif

(i) Tertutup

Diberikan sebarang $a, b \in \mathbb{Z}_n$ maka

$$a +_n b = (a + b) \pmod n$$

$$\equiv c \pmod n$$

Karena pasti terdapat $c < n$ yang memenuhi, maka

$$a +_n b = c \pmod n \in \mathbb{Z}_n$$

(ii) Asosiatif

Diberikan sebarang $a, b \in \mathbb{Z}_n$

$$(a +_n b) +_n c = (a + b) \pmod n +_n c$$

$$= a + b + c \pmod n$$

$$= a + (b + c) \pmod n$$

$$= a +_n (b + c) \pmod n$$

$$= a +_n (b +_n c) \pmod n$$

(iii) Terdapat elemen identitas

Akan dicari elemen identitas $e \in \mathbb{Z}_n$ sedemikian sehingga

$$e +_n a = a +_n e = a \quad \forall\, a \in \mathbb{Z}_n$$

$$e +_n a = e + a \pmod n = a$$

$$e + a \pmod n = a \pmod n$$

$$e + a = a$$

$$e = 0$$

$$a +_n n = a +_n 0 = a + 0 \pmod n = a \pmod n = a$$

Terbukti, bahwa terdapat elemen identitas $e = 0 \in \mathbb{Z}_n$ sedemikian sehingga

$$e +_n a = a +_n e = a \quad \forall\, a \in \mathbb{Z}_n$$

(iv) Invers

Untuk setiap $a \in \mathbb{Z}_n$ terdapat invers yang tunggal

$$a^{-1} \in \mathbb{Z}_n$$

Sedemikian sehingga

$$a +_n a^{-1} = a^{-1} +_n a = e$$

$$a^{-1} +_n a = e$$

$$(a + a^{-1}) \pmod n = 0 \Leftrightarrow (a + a^{-1}) \equiv 0 \pmod n$$

$$a^{-1} \equiv -\mathrm{a} \pmod n$$

$$a^{-1} \equiv (\mathrm{n} - \mathrm{a}) \pmod n \Rightarrow a^{-1} = n - a \in \mathbb{Z}_n.$$

(v) Komutatif

Diberikan sebarang $a, b \in \mathbb{Z}_n$

$$a +_n b = a + b \bmod n$$

$$b + a \bmod n = b +_n a \bmod n$$

B. $< \mathbb{Z}_n, \cdot_n >$ semigrup

(i) Tertutup

Diberikan sebarang $a, b \in \mathbb{Z}_n$ maka

$$a \cdot_n b = a\, b \bmod n \ \in \mathbb{Z}_n$$

(ii) Asosiatif

Diberikan sebarang $a, b, c \in \mathbb{Z}_n$ maka

$$\begin{aligned}(a \cdot_n b) \cdot_n \mathrm{c} &= \mathrm{a\ b} \bmod n \ \cdot_n \mathrm{c} \\ &= (\mathrm{a\ b})\ \mathrm{c} \bmod n \\ &= \mathrm{a}\ (\mathrm{b\ c}) \bmod n \\ &= a \cdot_n b\, c \bmod n \\ &= a \cdot_n (b \cdot_n \mathrm{c})\end{aligned}$$

C. Akan dibuktikan untuk sebarang $a, b, c \in \mathbb{Z}_n$ berlaku

(i) $a \cdot_n (\mathrm{b} +_n \mathrm{c}) = a \cdot_n \mathrm{b} +_n a \cdot_n \mathrm{c}$

(ii) $(a +_n b) \cdot_n \mathrm{c} = a \cdot_n \mathrm{c} +_n \mathrm{b} \cdot_n \mathrm{c}$

(i) $$\begin{aligned}a \cdot_n (\mathrm{b} +_n \mathrm{c}) &= a \cdot_n (\mathrm{b} + \mathrm{c}) \bmod n \\ &= a\ (\mathrm{b} + \mathrm{c}) \bmod n \\ &= \mathrm{a\ b} + \mathrm{a\ c} \bmod n \\ &= \mathrm{a\ b} \bmod n + \mathrm{a\ c} \bmod n \\ &= (\mathrm{a\ b} \bmod n + \mathrm{a\ c} \bmod n) \bmod n \\ &= (a \cdot_n b + a \cdot_n c) \bmod n \\ &= a \cdot_n b +_n a \cdot_n c\end{aligned}$$

(ii) $$(a +_n b) \cdot_n c = (a + b) \bmod n \cdot_n c$$
$$= (a + b)\, c \bmod n$$
$$= ac + bc \bmod n$$
$$= ac \bmod n + bc \bmod n$$
$$= (a \cdot_n c + a \cdot_n c) \bmod n$$
$$= a \cdot_n c +_n a \cdot_n c$$

Teorema 2.2.1 (Fraleight, 2000)

Anggota himpunan $\mathbb{Z}_n^*$ adalah elemen a dalam $\mathbb{Z}_n$ sehingga pembagi persekutuan terbesar dari a dan n adalah 1 atau $fpb = (a, n) = 1$.

Bukti:

Jika $d = 1$ maka orde dari a dalam $\mathbb{Z}_n$ sama dengan $n|d = n|1 = n$ sehingga semua n anggota $\mathbb{Z}_n$ termasuk dalam $1 \cdot a, 2 \cdot a, \ldots, n \cdot a = 0$. Oleh karena itu, salah satunya akan sama dengan 1, misalkan $k \cdot a = 1$ dengan $1 \leq k \leq n$. Akibatnya k dalam $\mathbb{Z}_n^*$ merupakan invers pergandaan dari a. Pada sisi lain, misalkan a sebarang anggota $\mathbb{Z}_n^*$ dengan invers pergandaan b maka untuk bilangan bulat $b \cdot a = 1$. Akibatnya grup bagian $(a) = \{1 \cdot a, 2 \cdot a, \ldots, b \cdot a, \ldots, 0\}$ dari $\mathbb{Z}_n$ memuat $b \cdot a = 1$ sehingga (a) Memuat $(1) = \mathbb{Z}_n$. Oleh karena itu a membangun $\mathbb{Z}_n$ dan mempunyai orde n dalam $\mathbb{Z}_n$ shingga $n/d = n$ dan $d = 1$ (Fraleight, 2000).

Contoh:

$\mathbb{Z}_{15}^{*}$ memuat semua anggota a dalam $\mathbb{Z}_{15}$sehingga a prima relatif dengan 15. Dalam hal ini $\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ dan $9 \notin \mathbb{Z}_{15}^{*}$ karena $(9,15) = 3$.

2.3 Teorema dalam Aritmatika Modulo

2.3.1 Teorema (*Chinese Remainder Theorem* (Teorema Sisa China))

Misalkan $m_1, m_2, \ldots, m_r$ adalah himpunan dari pasangan bilangan bulat relatif prima. Maka sistem kongruen secara simultan dituliskan $x \equiv a_1 \pmod{m_1}$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_k \pmod{r}$$

Mempunyai solusi tunggal modulo $M = m_1, m_2, \ldots, m_r$ untuk setiap bilangan bulat yang diberikan $a_1, a_2, \ldots, a_r$.

Bukti.

Misalkan $M = m_1, m_2, \ldots, m_r$ dan untuk setiap $k = 1, 2, \ldots, r$ misalkan $M_k = \frac{M}{m_k}$.

Maka fpb$(M_k, m_k) = 1$ untuk semua k. Misalkan y_k adalah invers dari M_k modulo m_k, untuk setiap k. Maka dengan definisi invers diperoleh $M_k y_k \equiv 1 \pmod{m_k}$.

Misalkan

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$

Maka x adalah solusi bersama untuk semua kongruensi.karena modulo $m_1, m_2, \dots, m_r$ adalah pasangan relatif prima, dua solusi bersama untuk sistemnya harus kongruen modulo M. Jadi solusinya adalah kongruen modulo M yang khusus dan nilai x yang memenuhi (M. Nathanson, 2000).

Contoh.

Temukan semua bilangan bulat x yang memberikan sisa $1, 2, 3,$ dan 4 bila dibagi masing-masing $5, 7, 9,$ dan 11. Selesaikanlah sistem kongruensi:

$$x \equiv 1 \pmod 5$$

$$x \equiv 2 \pmod 7$$

$$x \equiv 3 \pmod 9$$

$$x \equiv 4 \pmod{11}$$

Perhatikan bahwa modulo pasangan relatif prima, seperti yang dipersyaratkan oleh Teorema.2.7.1 diperoleh

$$M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$$

$$M_1 = M/5 = 693,$$

$$M_2 = M/7 = 495,$$

$$M_3 = M/9 = 385,$$

$$M_4 = M/11 = 315.$$

Maka dapat diperoleh

$$y_1 M_1 \equiv 1 \pmod 5$$

$$693\, y_1 \equiv 1 \pmod 5 \quad \rightarrow y_1 = 2$$

$$y_2 M_2 \equiv 1 \pmod 7$$

$$495\, y_2 \equiv 1 \pmod 7 \rightarrow y_2 = 3$$

$$y_3 M_3 \equiv 1 \pmod 9$$

$$385\, y_3 \equiv 1 \pmod 9 \rightarrow y_3 = 4$$

$$y_4 M_4 \equiv 1 \pmod{11}$$

$$315\, y_4 \equiv 1 \pmod 9 \rightarrow y_4 = 8$$

Oleh karena itu

$$x = 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8 = 19056.$$

Jadi

$$x = 19056 \pmod{\mathrm{M}} = 1731 \pmod{\mathrm{M}}.$$

Faktanya 1731 adalah solusi bilangan bulat positif terkecil. Solusi lengkap adalah $x \equiv 1731 \pmod M$ (M. Nathanson, 2000).

Teorema 2.3.2 (Teorema *Dirichlet*)

Misalkan $a, N \in \mathbb{Z}^+$ sedemikian sehingga fpb $(a, N) = 1$. Maka ada tak hingga banyaknya bilangan prima p sedemikian sehingga $p \equiv a \pmod N$

(M. Nathanson, 2000).

Teorema 2.3.3 (Hensel Lemma)

Misalkan p bilangan prima dan $f(x)$ polynomial derajat n dengan koefisien bilangan bulat dan sudah pasti koefisien tidak dapat membagi p. Jika terdapat x_1 sedemikian sehingga

$$f(x_1) \equiv 0 \pmod{p}$$

Dan

$$f'(x_1) \not\equiv 0 \pmod{p},$$

Maka untuk setiap $k \geq 2$ terdapat x_k sedemikian sehingga

$$f(x_k) \equiv 0 \pmod{p^k}$$

Dan

$$x_k \equiv x_{k-1} \pmod{p^{k-1}}.$$

(M. Nathanson, 2000).

Teorema 2.3.4 (Teorema Wilson)

Jika p adalah bilangan prima, maka $(p-1)! \equiv -1 \pmod{p}$ (Burton, 1998).

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 penelitian ini adalah:

1. Mengkaji konsep modulo yang berkaitan dengan penjumlahan dua bilangan kuadrat,
2. Mencari 25 bilangan asli pertama n yang memenuhi bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat dinyatakan sebagai jumlah dua bilangan kuadrat dengan menggunakan software Matlab berdasarkan teorema bahwa misalkan $n \geq 2$ adalah bilangan bulat. Maka, untuk setiap $z \in \mathbb{Z}_n$, pada persamaan $x^2 + y^2 \equiv z \ (mod\ n)$ memiliki solusi nontrivial jika dan hanya jika keempat syarat berikut terpenuhi: (i) $n \not\equiv 0 \pmod{q^2}$ untuk sebarang bilangan prima $q \equiv 3 \pmod 4$ jika $n \equiv 0 \pmod q$, (ii) $n \not\equiv 0 \pmod 4$, (ii) $n \equiv 0 \pmod p$ untuk suatu bilangan prima $p \equiv 1 \pmod 4$, (iv) Jika $n \equiv 1 \pmod 2$,

diperoleh syarat tambahan berikut: misalkan $n = 5^k m$, dimana $m \not\equiv 0 \pmod 5$. Maka salah satu dari pernyataan tersebut terpenuhi (a) $k \geq 3$, dengan tidak ada syarat lebih lanjut untuk m atau, (b) $k \leq 2$ dan $m \equiv 0 \pmod p$ untuk suatu bilangan prima $p \equiv 1 \pmod 4$.

Sedangkan untuk persamaan $x^2 + y^2 \equiv z \ (mod\ n)$ memiliki solusi (boleh trivial) jika dan hanya jika syarat (i) dan (ii) terpenuhi.

3. Merepresentasikan setiap elemen dalam ring $\mathbb{Z}_n$ untuk setiap n yang memenuhi.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Terdapat 25 bilangan asli pertama n yang memenuhi bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat dinyatakan sebagai jumlah dua bilangan kuadrat tak nol (solusi non trivial) yaitu $[10, 13, 17, 26, 29, 30, 34, 37, 39, 41, 50, 51, 53, 58, 61, 65, 70, 73, 74, 78, 82, 85, 87, 89, 91]$.
2. Terdapat 25 bilangan asli pertama n yang memenuhi bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat dinyatakan sebagai jumlah dua bilangan kuadrat (boleh solusi trivial) yaitu $[1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 25, 26, 29, 30, 31, 33, 34, 35, 37]$.

5.2 Saran

Pada penelitian ini hanya mencari 25 bilangan asli pertama n yang memenuhi bahwa setiap elemen dalam ring $\mathbb{Z}_n$ dapat dinyatakan sebagai jumlah dua bilangan kuadrat (nilai n kurang dari 100). Penelitian ini dapat dilanjutkan dengan mencari $\mathbb{Z}_n$ lainnya yang memenuhi syarat tersebut untuk nilai n lebih dari 100.

DAFTAR PUSTAKA

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

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

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

Grillet, P.A. 2007. *Graduate Text In Mathematics.* Second Edition. Springer. New York

J. Harrington, L. Jones, and A. Lamarche. 2014. Representing integers as the sum of two squares in the ring Zn, *Journal Integer Seq*. 17, 4-10

M. Nathanson. 2000. *Elementary Methods in Number Theory*, Springer-Verlag.

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