PENGUJIAN BILANGAN CARMICHAEL

(Skripsi)

Oleh

SELMA CHYNTIA SULAIMAN

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
2016

ABSTRAK

PENGUJIAN BILANGAN CARMICHAEL

Oleh

SELMA CHYNTIA SULAIMAN

Untuk bilangan bulat $a > 1$ dan bilangan bulat positif n, didefinisikan F(a) himpunan bilangan bulat positif n yang memenuhi $a^{n-1} \equiv 1(mod\ n)$. Bilangan a-pseudoprima adalah bilangan komposit n yang termuat dalam F(a). Bilangan Carmichael n adalah bilangan a-pseudoprima untuk semua a yang *coprima* (relatif prima) dengan n.

Dalam mencari bilangan Carmichael dapat dengan cara perkalian faktor-faktor prima (teori faktorisasi prima) dan bentuk $(6m + 1)(12m + 1)(18m + 1)$ dimana $(m \equiv 0(mod\ 5)$ atau $m \equiv 1(mod\ 5))$ yang membentuk perkalian 3 komponen bilangan prima didalamnya. Himpunan bilangan Carmichael dalam bentuk $(6m + 1)(12m + 1)(18m + 1)$ merupakan bagian dari himpunan bilangan Carmichael dengan faktorisasi prima.

Untuk menentukan bilangan Carmichael lebih baik menggunakan teori faktorisasi prima karena dengan cara ini akan didapatkan bilangan Carmichael pertama dari yang terkecil sampai tak berhingga.

Kata Kunci : Bilangan Carmichael, bilangan bulat positif, bilangan prima, bilangan komposit, relatif prima, pseudoprima.

ABSTRACT

TESTING OF CARMICHAEL NUMBER

By

SELMA CHYNTIA SULAIMAN

For *a* fixed $a > 1$ and positive integers *n*, we write $F(a)$ for the set of positive integers *n* satisfying $a^{n-1} \equiv 1(mod\ n)$. *A*-pseudoprima number is a composite number *n* and contained in $F(a)$. Carmichael number *n* is the number of *a*-pseudoprima for all the coprima a (relatively prime) with *n*.

In search of Carmichael numbers can be by way of multiplication factors of prime (prime factorization theory) and form $(6m + 1)\ (12m + 1)\ (18m + 1)$ where $(n \equiv 0\ (mod\ 5)$ or $m \equiv 1\ (mod\ 5))$ that form a component of prime number multiplication 3 therein. Carmichael set of numbers in the form $(6\mathrm{m} + 1)(12\mathrm{m} + 1)(18\mathrm{m} + 1)$ is part of a set Carmichael numbers with prime factorization.

To determine the Carmichael number better use prime factorization theory because in this way we will get the first Carmichael numbers from the smallest to infinity.

Keywords **:** Carmichael number, positive integer, prime number, composite number, coprime, pseudoprima.

PENGUJIAN BILANGAN CARMICHAEL

Oleh

Selma Chyntia Sulaiman

Skripsi

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA SAINS

Pada

Jurusan Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Lampung

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2016

Judul Skripsi	: **PENGUJIAN BILANGAN CARMICHAEL**
Nama Mahasiswa	: Selma Chyntia Sulaiman
Nomor Pokok Mahasiswa	: 1317031075
Jurusan	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

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

Subian Saidi, S.Si., M.Si.
NIP 19800821 200812 1 001

2. Ketua Jurusan Matematika

Drs. Tiryono Ruby, M.Sc., Ph.D.
NIP 19620704 198803 1 002

MENGESAHKAN

1. Tim Penguji

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

Sekretaris : **Subian Saidi, S.Si., M.Si.** .....

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

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 : **09 Desember 2016**

PERNYATAAN SKRIPSI MAHASISWA

Saya yang bertanda tangan di bawah ini:

Nama : **Selma Chyntia Sulaiman**

Nomor Pokok Mahasiswa : **1317031075**

Judul : **PENGUJIAN BILANGAN CARMICHAEL**

Jurusan : **Matematika**

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, Desember 2016

Penulis,

SELMA CHYNTIA SULAIMAN
NPM. 1317031075

RIWAYAT HIDUP

Penulis bernama lengkap Selma Chyntia Sulaiman, anak kedua dari empat bersaudara yang dilahirkan di Malang pada tanggal 11 Juli 1995 oleh pasangan Bapak Sulaiman dan Ibu Puspasari.

Menempuh pendidikan di Taman Kanak-Kanak (TK) Kartika X-1 Malang pada tahun 1999 - 2001, Sekolah Dasar (SD) diselesaikan di SD Kartika II-5 Bandar Lampung pada tahun 2001-2007, kemudian bersekolah di SMP N 22 Bandar Lampung pada tahun 2007-2010, dan bersekolah di SMA N 7 Bandar Lampung pada tahun 2010-2013.

Pada tahun 2013 penulis terdaftar sebagai mahasiswi S1 Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung melalui Jalur SNMPTN undangan.

Pada tahun 2016 penulis melakukan Kerja Praktik (KP) di Kejaksaan Negeri Bandar Lampung dan pada tahun yang sama penulis melaksanakan Kuliah Kerja Nyata (KKN) di Desa Kediri Kecamatan Gading Rejo, Kabupaten Pringsewu, Provinsi Lampung.

PERSEMBAHAN

Dengan mengucap puji dan syukur kehadirat Allah SWT kupersembahkan karya kecil dan sederhana ini untuk :

Ayah dan Ibu tercinta yang selalu mendoakan, memberi semangat, dan telah menjadi motivasi terbesar selama ini.

Kakak dan Adik tercinta Ahmad Nurhuda A., M. Rizki Ramdhani dan M. Hidayatullah yang selalu berbagi canda, tawa serta menjadi penyemangat penulis agar bisa menjadi seseorang yang bisa dibanggakan.

Dosen Pembimbing dan Penguji yang sangat berjasa dan selalu memberikan motivasi kepada penulis.

Sahabat-sahabat tersayang. Terimakasih atas kebersamaan, keceriaan, canda dan tawa serta doa dan semangat yang telah diberikan.

Almamater Universitas Lampung

KATA INSPIRASI

"Cinta yang kita berikan, adalah cinta yang akan kita terima, karena selalu ada balasan yang baik ketika kita berbuat baik."

"Masa Depan adalah misteri. Tapi kalau Anda mau mempersiapkannya hari ini, maka 50% dari Masa Depan itu sudah bisa diprediksi."

"Tidak ada jaminan kesuksesan, namun tidak mencobanya adalah jaminan kegagalan."

SANWACANA

Dengan mengucapkan *Alhamdulillah* penulis panjatkan puji syukur kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "PENGUJIAN BILANGAN CARMICHAEL". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains (S.Si.) di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.

Dengan ketulusan hati penulis ingin mengucapkan terima kasih banyak kepada :

1. Bapak Amanto, S.Si., M.Si. selaku Dosen Pembimbing I, terima kasih untuk bimbingan dan kesedian waktunya selama penyusunan skripsi ini.
2. Bapak Subian Saidi, S.Si., M.Si. selaku Dosen Pembimbing II, terima kasih untuk bantuan dan masukannya selama penyusunan skripsi.
3. Ibu Dr. Asmiati, S.Si., M.Si. selaku Dosen Penguji, terima kasih atas kesediannya untuk menguji, memberikan saran dan kritik yang membangun dalam penyelesaian skripsi ini.
4. Bapak Drs. Suharsono S., M.S., M.Sc., Ph.D. selaku Pembimbing Akademik, terima kasih atas bimbingan dan pembelajarannya dalam menjalani perkuliahan.

5. Bapak Drs. Tiryono Ruby, M.Sc., P.hD. selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
6. Bapak Prof. Warsito, S.Si., D.E.A., Ph.D., selaku Dekan FMIPA Universitas Lampung.
7. Seluruh Dosen dan Karyawan Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
8. Ayah dan Ibu tercinta yang tak pernah berhenti memberi semangat, doa, dorongan, nasehat dan kasih sayang serta pengorbanan yang tak tergantikan hingga penulis selalu kuat menjalani setiap rintangan yang ada di depan.
9. Kakak dan adik Ahmad Nurhuda, M. Rizki Ramdhani , dan M. Hidayatullah yang selalu berbagi canda dan tawa serta selalu menyemangati hingga terselesaikannya skripsi ini.
10. Sahabat-sahabat seperjuangan menuju wisuda Tina, Haris, Karina, Ali, Luluk, Risa, Heni, Olivia, Matematika 2013 yang banyak membantu dan sabar menghadapi penulis, serta Zahra, Wulan, Sella, Nisrima, Gina yang selalu memberikan dukungan dan juga semangat hingga terselesaikannya skripsi ini.
11. Almamater tercinta Universitas Lampung.
12. Seluruh pihak yang telah membantu yang tidak dapat disebutkan satu persatu.

Bandar Lampung, Desember 2016
Penulis,

Selma Chyntia Sulaiman

DAFTAR ISI

Halaman

DAFTAR GAMBAR……..…..……..…….....i

DAFTAR TABEL……...……..…… .....…ii

I. PENDAHULUAN

1.1 Latar Belakang…….....……...1

1.2 Rumusan Masalah.....…….....…...2

1.3 Tujuan Penelitian.....…….....……...3

1.4 Manfaat Penilitian.....…….....3

II. TINJAUAN PUSTAKA

2.1 Keterbagian.....…….....4

2.2 Modulo.....…….….....7

2.3 Relasi Kongruensi.....…….....…...8

2.4 Faktor Persekutuan Besar (FPB).....….....…12

2.5 Perkongruenan Linear.....14

2.5.1 Pengertian Perkongruenan Linear.....…….....….14

2.5.2 Solusi Perkongruenan Linear.....15

2.6 Bilangan Prima.....18

2.7 Bilangan Komposit.....23

2.8 Bilangan Carmichael.....23

III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian.…….....…….....….25

3.2 Metode Penelitian.....…….....25

IV. HASIL DAN PEMBAHASAN

4.1 Karakteristik Bilangan Carmichael…….…….....…..27

4.2 Menentukan Bilangan Carmichael…….....…….....….30

4.2.1 Bilangan Carmichael sampai 3000…….....……30
4.2.2 Bilangan Carmichael dan Teorema Fermat.....31
4.2.3 Bilangan Carmichael bentuk $(6m + 1)(12m + 1)(18m + 1)$.....35
4.3 Bilangan Carmichael dengan software Matlab.....38
4.3.1 Himpunan Bilangan Carmichael 3 Bilangan Prima.....39
4.3.2 Himpunan Bilangan Carmichael $(6m + 1)(12m + 1)(18m + 1)$....45
V. KESIMPULAN
5.1 Kesimpulan.....49
5.2 Saran.....49
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR GAMBAR

Halaman

Gambar 4.2.1 Pengujian Bilangan Carmichael dengan faktorisasi prima menggunakan *software* Matlab R2013b.....37

Gambar 4.2.2 Pengujian Bilangan Carmichael bentuk $(6m + 1)(12m + 1)(18m + 1)$ menggunakan *software* Matlab R2013b.....37

Gambar 4.3.1 Penggunaan *software* Matlab R2013b perkalian 3 faktor prima....44

Gambar 4.3.2 Penggunaan *software* Matlab R2013b dengan bentuk $(6m + 1)(12m + 1)(18m + 1)$.....47

DAFTAR TABEL

Halaman

Tabel 4.2.1 Bilangan Carmichael *pqr* sampai 3000.....31

Tabel 4.3.1 Bilangan Carmichael *pqr* sampai 1000000.....38

DAFTAR SIMBOL DAN SINGKATAN

$(a\|b)$	: *a* membagi habis *b* atau *b* habis dibagi *a*
$a \nmid b$	: *a* tidak habis membagi *b*
$\mathbb{Z}$	: Himpunan semua bilangan bulat
mod	: Modulo
$\|a\|$	: Harga multak *b*
$a \equiv b(mod\ m)$	: *a* berelasi kongruen dengan *b* modulo *m*
$\in$	: Anggota atau elemen
$\leq$	: Lebih kecil atau sama dengan
$\geq$	: Lebih besar atau sama dengan
gcd	: $Greatest\ common\ divisor$ (FPB)
FPB	: Faktor Persekutuan Besar
$\forall$	: Untuk setiap
$\exists$	: Terdapat

I. PENDAHULUAN

1.1 Latar Belakang

Matematika adalah pola berpikir, mengorganisasikan, pembuktian yang logik. Matematika itu adalah bahasa yang menggunakan istilah yang didefinisikan dengan cermat, jelas, dan akurat, representasinya dengan simbol. Didalam matematika terdapat banyak cabang pembagian ilmu matematika salah satunya adalah teori bilangan. Teori bilangan adalah cabang dari matematika murni yang mempelajari sifat-sifat bilangan bulat dan mempunyai berbagai masalah terbuka yang dapat dengan mudah dimengerti sekalipun bukan oleh ahli matematika.

Awal kebangkitan teori bilangan modern dipelopori oleh Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), J.L Lagrange (1736-1813), A.M. Legendre (1752-1833), Dirichlet (1805-1859), Dedekind (1831-1916), Riemann (1826-1866), Giussepe Peano (1858-1932), Poisson (1866-1962), dan Hadamard (1865-1963). Sebagai seorang pangeran matematika, Gauss begitu terpesona terhadap keindahan dan kecantikan teori bilangan, dan untuk melukiskannya, ia menyebut teori bilangan sebagai *the queen of mathematics*. Pada masa ini, teori bilangan tidak hanya berkembang sebatas konsep, tapi juga banyak diaplikasikan dalam berbagai bidang ilmu pengetahuan dan teknologi. Hal ini dapat dilihat pada

pemanfaatan konsep bilangan dalam metode kode baris, kriptografi, komputer, dan lain sebagainya (Burton, 1980).

Pada tahun 1910, Carmichael memulai penelitiannya dengan sifat bilangan komposit, bilangan komposit adalah bilangan asli lebih besar sama dengan 1 yang bukan merupakan bilangan prima. Kemudian munculah bilangan Carmichael, pada penelitiannya Carmichael menunjukkan bahwa algoritma dibangun oleh bilangan-bilangan. Teorema Fermat menyatakan bahwa bilangan Carmichael mirip dengan bilangan prima. Pada tahun 1993, berdasarkan penelitian Carmichael sebelumnya, Chernick memperlihatkan bahwa jika p= 6m+1, q= 12m+1 dan r= 18m+1 untuk semua bilangan prima, maka pqr adalah bilangan Carmichael (Dubner, 2002).

Dalam penelitian ini akan dibahas mengenai pengujian bilangan Carmichael yang ditinjau berdasarkan pada karakterisiktiknya. Oleh karena itu, penulis memilih judul "**Pengujian Bilangan Carmichael."**

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah bagaimana cara menemukan bilangan Carmichael pada suatu bilangan yang ditinjau dari karakteristiknya.

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Mengkaji karakteristik bilangan Carmichael.
2. Menguji bilangan Carmichael berdasarkan karakteristiknya.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Memberikan pemikiran dalam ilmu matematika khususnya mengenai bilangan Carmichael.
2. Menambah pengetahuan tentang bilangan Carmichael.
3. Mengetahui karakteristik bilangan Carmichael.

II. TINJAUAN PUSTAKA

2.1 Keterbagian

Keterbagian atau *divisibility* artinya, sudut pandang matematika yang mempelajari suatu bilangan yang habis dibagi oleh bilangan lain. Misalkan suatu bilangan bulat b dikatakan terbagi oleh bilangan bulat $a \neq 0$ jika terdapat bilangan bulat c sehingga $b = ac$, dapat ditulis $a \mid b$. Notasi $a \nmid b$ digunakan untuk menyatakan tidak habis terbagi oleh a. Istilah lain untuk $a \mid b$ adalah a faktor dari b, dengan 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 :

$$a \mid 0 \; ; \; 1 \mid a \text{ dan } a \mid a \text{ untuk } a \neq 0$$

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

Jadi 15 terbagi oleh 3 sebab 15 = 3×5 , tetapi 14 tidak terbagi oleh 5 sebab tidak ada bilangan bulat *c* sehingga 14 = 5*c*, atau setiap bilangan bulat *c* berlaku 14 ≠ 5*c*. Dalam kasus ini ditulis $3 \mid 15$ dan $5 \nmid 14$ (Sukirman, 1997).

Teorema 2.1.1

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

1. $a \mid 1$ jika dan hanya jika $a = 1$ atau $a = -1$.

Bukti :

Jika $a = 1$ atau $a = -1$, maka jelas bahwa $a \mid 1$, sesuai penjelasan sebelumnya. Sebaliknya, diketahui $a \mid 1$ 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 $a \mid 1$ maka $a = 1$ atau $a = -1$.

Sehingga terbukti $a \mid 1$ jika dan hanya jika $a = 1$ atau $a = -1$. ■

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

Bukti :

Diketahui $a \mid b$ dan $c \mid d$ yaitu $k_1, k_2 \in \mathbb{Z}$

Sehingga $b = k_1 a$ dan $d = k_2 c$

Dengan mengkalikan kedua persamaan tersebut diperoleh :

$bd = (k_1 a)(k_2 c)$

$= (k_1 k_2)\, ac$

Maka terbukti bahwa $ac \mid bd$. ■

3. Jika $a \mid b$ dan $b \mid c$ maka $a \mid c$.

Bukti :

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

$$b = k_1 a \qquad (2.1)$$

dan

$$c = k_2 b \qquad (2.2)$$

Substitusikan pesamaan (2.1) ke persamaan (2.2)

$c = k_2 b = k_2 (k_1 a) = (k_1 k_2)\, a$

maka terbukti bahwa $a \mid c$. ■

4. Jika $a \mid b$ dan $b \mid a$ jika dan hanya jika $a = b$ atau $a = -b$

Bukti :

Diketahui

$$a = k_1 b \qquad (2.3)$$

dan

$$b = k_2 a \qquad (2.4)$$

Persamaan (2.3) dikalikan dengan persamaan (2.4) sehingga diperoleh

$ab = (k_1 b)\,(k_2 a) = (k_1 k_2)\,(ab)$

Dengan $k_1 k_2 = 1$, yakni $k_1 = k_2 = 1$ atau $k_1 = k_2 = -1$

Jadi terbukti $a = b$ atau $a = -b$ ■

5. Jika $a \mid b$ dan $b \neq 0$, maka $|a| < |b|$

Bukti :

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. Jika $a \mid b$ dan $a \mid c$, maka $a \mid (bx + cy)$ untuk sebarang bilangan bulat x dan y.

Bukti :

Diketahui $a \mid b$ dan $a \mid c$, 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 $bx + cy = (k_1 a)\, x + (k_2 a)\, y = (k_1 x + k_2 y)\, a$

Jadi terbukti bahwa $a \mid (bx + cy)$. ■

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 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 mod $m = r$ 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, …, *m* – 1} (Grillet, 2007).

Contoh beberapa hasil operasi dengan modulo :

- 27 mod 3 = 0 (27 = 3 × 9 + 0)
- 6 mod 8 = 6 (6 = 8 × 0 + 6)
- – 41 mod 9 = 4 (–41 = 9 (–5) + 4)

Catatan : Karena *a* negatif, bagi |*a*| dengan *m* mendapatkan sisa *r'* ,
maka *a* mod = *m* – *r'* bila *r'* ≠ 0.
Jadi |– 41| mod 9 = 5, sehingga –41 mod 9 = 9 – 5 = 4.

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 :

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

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

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

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

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

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

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

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

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

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

(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 $l \in \mathbb{Z}$

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

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

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

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

2.4 Faktor Persekutuan Besar (FPB)

Definisi 2.4.1

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, kondisi 1 menyatakan bahwa *d* adalah faktor persekutuan dan kondisi 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 2.4.1 (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 2.4.2

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 $d = \gcd(a, b)$. ■

2.5 Perkongruenan Linear

2.5.1 Pengertian perkongruenan linear

Definisi 2.5.1

a. Kalimat terbuka yang menggunakan relasi kekongruenan disebut perkongruenan.

b. Jika suatu perkongruenan, pangkat tertinggi variabelnya paling tinggi satu disebut perkonguruenan linear (Grillet, 2007).

Teorema 2.5.1

Perkongruenan linear $ax \equiv b$ (mod m) mempunyai solusi jika dan hanya jika gcd$(a, m) =$ d | b.

Contoh 2.5.1

1. Perkongruenan :

   $3x \equiv 4\ (mod\ 5)$

   $x^4 + 3x - 3 \equiv 0\ (mod\ 31)$

2. Perkongruenan linear :

   $3x \equiv 4\ (mod\ 5)$

   $5x \equiv 2\ (mod\ 4)$

Bentuk umum pengkongruenan linear :

$$ax \equiv b(\text{mod } m)$$

Nilai-nilai *x* dicari sebagai berikut:

ax = *b* + *km* yang dapat disusun menjadi $x = \frac{b+km}{a}$, dengan *k* adalah sembarang bilangan bulat. Untuk *k* = 0, 1, 2, … dan *k* = –1, –2, … yang menghasilkan *x* sebagai bilangan bulat.

2.5.2 Solusi Perkongruenan Linear

Perhatikan perkongruenan berikut

$$3x \equiv 4 \text{ (mod } 5)$$

Jika x pada diganti dengan bilangan 3, maka akan diperoleh 3 ò 3 ≡ 4 (mod 5) atau 3 ò 3 ≡ 4 atau 9 ≡ 4 (mod 5), merupakan kalimat kekongruenan yang

benar. Begitu pula jika x diganti berturut-turut oleh ..., -7, -2, 8, 13, ... akan memberikan kalimat-kalimat kekongruenan yang benar.

Diketahui bahwa $ax \equiv b \pmod{m}$ berarti $ax - b = km$ atau $ax = b + km$. Dengan kata lain, perkongruenan linear akan mempunyai solusi (penyelesaian) jika dan hanya jika terdapat bilangan-bilangan bulat *x* dan *k* sehingga *ax* = *b* + *km*. Misalkan *r* memenuhi pekongruenan linear, maka $ar \equiv b \pmod{m}$. Sehingga setiap bilangan bulat

$(r + m), (r + 2m), (r + 3m),..., (r - m), (r - 2m), (r - 3m),...$

Memenuhi perkongruenan linear sebab :

$a(r + km) \equiv ar + akm \equiv b \pmod{m}$ untuk setiap bilangan bulat *k*.

Diantara bilangan –bilangan bulat (*r* + *km*), dengan *k* = 1, 2, 3, ..., -1, -2, -3, ... ada tepat satu dan hanya satu, katakan bilangan itu *s*, sehingga $0 \leq s < m$, karena setiap bilangan bulat terletak di antara dua kelipatan *m* yang berurutan. Jadi, jika *r* memenuhi perkongruenan dan $km \leq r \leq (k + 1)m$ untuk suatu bilangan bulat k maka $0 \leq (r - km) < m$. Oleh karena itu, di peroleh

$s = r - km$, untuk suatu bilangan bulat *k*.

Dengan kata lain, *s* adalah residu terkecil modulo *m* yang memenuhi perkongruenan. Selanjutnya *s* disebut solusi (penyelesaian) dari perkongruenan linear. Jika $\gcd(a, m) \neq db$, maka perkongruenan linear $ax \equiv b \pmod{m}$ mempunyai solusi.

Contoh 2.5.2

1. Tentukan solusi dari $2x \equiv 4 \pmod{7}$

   Penyelesaian :

Karena gcd (2,7) = 1 dan $1 \mid 4$, maka perkongruenan linear di atas mempunyai penyelesaian. Nilai-nilai *x* yang memenuhi perkongruenan linear $2x \equiv 4\ (mod\ 7)$ adalah ..., -19, -12, -5, 2, 9, 16, ... jadi solusi dari perkongruenan linear tersebut adalah 2, sebab 2 merupakan residu terkecil modulo 7 yang memenuhi $2x \equiv 4\ (mod\ 7)$

2. Selesaikan penyelesaian $2x \equiv 4\ (mod\ 7)$

   Penyelesaian :

   Gcd (2,6) = 2 dan 2 membagi 4, maka perkongruenan tersebut mempunyai penyelesaian dan mempunyai tepat 2 solusi. Nilai *x* yang memenuhi $2x \equiv 1\ (mod\ 6)$ adalah ..., -7, -4, -2, ..., 2, 5, 8, 11, 14, ... Bilangan 2 dan 5 merupakan residu terkecil modulo 6, sehingga 2 dan 5 merupakan solusi dari $2x \equiv 1\ (mod\ 6)$.

Akibat 2.5.2

Jika $\gcd(a,m) \neq d \mid b$, maka perkongruenan linear $ax \equiv b\ (mod\ m)$ mempunyai solusi (Grillet, 2007).

Teorema 2.5.2

Jika $\gcd(a,m) = 1$, maka perkongruenan linear $ax \equiv b\ (mod\ m)$ mempunyai tepat satu solusi.

Teorema 2.5.3

Jika $\gcd(a,m) = d$ dan $d \mid b$, maka perkongruenan linear $ax \equiv b \ (mod\ m)$ mempunyai tepat sebanyak *d* solusi.

Teorema 2.5.4 (Chinese Remainder Theorm)

Misalkan $m_1, m_2, \dots, m_k$ bilangan bulat positif sedemikian sehingga $\gcd(m_i, m_j) = 1$ untuk $i \neq j$, maka sistem perkongruenan linear

$x \equiv a_1 (mod\ m_1)$

$x \equiv a_2 (mod\ m_2)$

$x \equiv a_3 (mod\ m_3)$

. .
. .
. .
. .

$x \equiv a_i (mod\ m_i)$

Mempunyai solusi bersama modulo $(m_1, m_2, \dots, m_i)$ yang tunggal dan solusi tersebut adalah $x_0 = a_1 s_1 M_1 + a_2 s_2 M_2 + \cdots + a_i s_i M_i$

Dengan $M_i \frac{m_1, m_2, \dots, m_i}{m_1}$. s_i adalah bilangan yang memenuhi perkongruenan linear.

$M_1 s_1 \equiv 1 \ (mod\ m_1)$; $i = 1,2, \dots, k$ (Grillet, 2007).

2.6 Bilangan Prima

Definisi 2.6.1

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

Teorema 2.6.1

Setiap bilangan bulat *n*, *n* > 1 dapat dinyatakan sebagai hasil kali bilangan-bilangan prima (mungkin hanya memiliki satu faktor) (Sukirman, 1997).

Lebih lanjut dari teorema di atas, karena faktor-faktor prima itu mungkin tidak saling berbeda, maka hasil kali bilangan-bilangan prima dari bilangan bulat *n* dapat ditulis sebagai $n = {p_1}^{a_1}{p_2}^{a_2} \dots {p_k}^{a_k}$ dengan $p_1, p_2, \dots, p_k$ sebagai faktor-faktor prima dari *n* dan $a_1, a_2, \dots, a_k$ merupakan eksponen positif berturut-turut $p_1, p_2, \dots, p_k$.

Definisi 2.6.2 (Relatif Prima)

Bilangan bulat *a* dan *b* dikatakan *coprima* atau relatif prima jika $\gcd(a, b) = 1$. Dengan kata lain *a* dan *b* tidak mempunyai faktor prima bersama (Dudley, 1969).

Teorema 2.6.2

Bilangan *a* dan *b* relatif prima bila 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 Benzout 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. ■

Teorema 2.6.3

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 :

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

   Karena terdapat bilangan bulat $sx + ry$ sedemikian sehingga $ab|c$.

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

2. Diketahui $a|bc$, $\gcd(a,b) = 1$. Oleh karena itu dapat dituliskan $ax + by = 1$ untuk suatu bilangan bulat *x, y*. Akibatnya :

$$\begin{aligned} c = 1 \cdot c &= (ax + by) \cdot c \\ &= acx + bcy \end{aligned}$$

   Karena diketahui $a|bc$ dan faktanya $a|ac$ maka $a|(acx + bcy)$ karena $c = acx + bcy$ jadi terbukti $a|c$ ■

Definisi 2.6.4

Bentuk $n = {p_1}^{a_1}{p_2}^{a_2} \ldots {p_k}^{a_k}$ disebut *representasi n* sebagai hasil kali bilangan-bilangan prima, sering pula bentuk itu disebut bentuk kanonik *n* (Dudley, 1969).

Akibat 2.6.4 (Teorema Fundamental Aritmatika)

Sebarang bilangan bulat positif $n > 1$ dapat ditulis dengan tunggal dalam bentuk kanonik $n = {p_1}^{a_1}{p_2}^{a_2} \dots {p_k}^{a_k}$ dengan $a_1, a_2, \dots, a_k$ bilangan bulat positif dan $p_1, p_2, \dots, p_k$ bilangan prima dan $p_1 < p_2 < \cdots < p_k$ (Dudley, 1969).

Berikut ini akan diberikan Teorema Fermat yang diambil dari (Burton, 1980) :

Teorema 2.6.4 (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 :

Pertama, perhatikan $(p-1)$ bilangan positif pertama kelipatan dari a, yaitu bilangan bulat.

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

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.

Diasumsikan 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, himpunan bilangan bulat diatas harus kongruen $(mod\ p)$ dengan $1, 2, 3, 4, \dots, p-1$. Diambil semua himpunan bilangan bulat tersebut, selanjutnya kalikan semua kongruen diperoleh

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

Sehingga,

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

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

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

Akibat Teorema 2.6.4 (Teorema Fermat)

Jika *p* prima, maka $a^p \equiv a\ (mod\ p)$ untuk sebarang bilangan bulat *a*.

Teorema 2.6.5

Jika p dan q bilangan prima berbeda sedemikian hingga $a^p \equiv a\ (mod\ p)$ dan $a^q \equiv a\ (mod\ q)$, maka $a^{pq} \equiv a\ (mod\ pq)$ (Sukirman, 1997).

Teorema 2.6.6 (Teorema Euler (Generalisasi Teorema Fermat))

Jika gcd (*a*,*m*) = 1, maka $a^{\phi(m)} \equiv 1\ (mod\ m)$, $\phi(m)$ adalah banyaknya bilangan bulat positif yang kurang dari atau sama dengan *m* dan relatif prima dengan *m*.

Sifat :

1. Jika $m = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$, p_i berbeda untuk setiap *i*, maka

$$\phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$$

2. $\phi(p) = p - 1$, p prima

3. $\phi(m,n) = \phi(m).\phi(n)$

2.7 Bilangan Komposit

Bilangan komposit adalah bilangan asli yang lebih besar dari satu yang bukan termasuk bilangan prima. Bilangan komposit juga dapat didefinisikan sebagai faktorisasi dari bilangan bulat. Dapat juga diartikan bahwa bilangan komposit adalah hasil perkalian antara dua bilangan prima atau lebih. Setiap bilangan prima adalah ganjil kecuali 2. Sehingga dengan konsep penjumlahan pada bilangan ganjil dan genap berlaku hal seperti ini:

Bilangan prima ganjil + Bilangan prima ganjil = Bilangan komposit (Sukirman, 1997).

2.8 Bilangan Carmichael

Definisi 2.8.1

Untuk bilangan bulat $a > 1$ dan bilangan bulat positif n, didefinisikan himpunan

$$F(a) = \{n | a^{n-1} \equiv 1 (mod\ n)\}$$

Bilangan a-pseudoprima adalah bilangan komposit n yang termuat dalam $F(a)$ (Dubner, 2002).

Definisi 2.8.2

Bilangan Carmichael *n* adalah bilangan *a-pseudoprima* untuk semua *a* yang *coprima* (relatif prima) dengan *n* (Dubner, 2002).

Dengan kata lain, jika $(a,n) = 1$ maka kongruensi dari $a^n \equiv a(mod\ n)$ adalah ekuivalen dengan $a^{n-1} \equiv 1(mod\ n)$ disebut bilangan Carmichael atau *pseudoprima absolute.*

III. METODOLOGI 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 2016/2017.

3.2 Metode Penelitian

Langkah-langkah yang digunakan dalam menyelesaikan penelitian ini adalah sebagai berikut:

1. Mengkaji karakteristik bilangan Carmichael yang dituliskan dalam bentuk teorema, lemma, dan proposisi.
2. Menentukan bilangan Carmichael sampai 3000 dengan menggunakan teori-teori berikut : Faktorisasi prima (3 bilangan prima), relasi kongruensi (teorema Fermat), dan dengan bentuk $(6m + 1)(12m + 1)(18m + 1)$.
3. Menemukan bilangan Carmichael sampai 1000000 dengan menggunakan sistem komputasi (*software* Matlab R2013b).
4. Menguji contoh himpunan bilangan Carmichael 3 faktor prima dan himpunan bilangan Carmichael dalam bentuk $(6m + 1)(12m + 1)(18m + 1)$ yang telah diketahui dengan dibantu *software* Matlab R2013b.

5. Membandingkan 2 himpunan bilangan Carmichael pada langkah (4).
6. Menarik kesimpulan terhadap bilangan Carmichael yang telah diuji melalui langkah (2), (3) dan (4).

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil dan pembahasan pada bab sebelumnya dapat disimpulkan bahwa :

Himpunan bilangan Carmichael dalam bentuk $(6m + 1)(12m + 1)(18m + 1)$ merupakan bagian dari himpunan bilangan Carmichael dengan menggunakan faktorisasi prima. Secara umum untuk menentukan bilangan Carmichael dapat menerapkan teori faktorisasi prima dan teorema Fermat karena dengan kedua langkah tersebut dapat ditemukan bilangan Carmichael yang pertama dan terkecil secara berurut.

5.2 Saran

Pada penelitian selanjutnya dapat diteliti untuk karakteristik bilangan Carmichael yang lain dan dapat dilakukan pengujian pada bilangan Carmichael dengan diberikan empat faktor prima.

DAFTAR PUSTAKA

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

Dubner, Harvey. 2002. Carmichael Number of the Form (6m+1)(12m+1)(18m+1). *Journal of Integer Sequences,* Vol. 5 (2002). Article 02.2.1.

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

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

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

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