II. TINJAUAN PUSTAKA

Pada bab ini diberikan beberapa definisi mengenai teori dalam aljabar dan teori bilangan yang mendukung proses penelitian. Dalam penyelesaian bilangan carmichael akan dibutuhkan definisi tentang konsep keterbagian sebagai berikut.

2.1 Keterbagian

Definisi 2.1.1 Sebuah bilangan bulat b dikatakan terbagi atau habis dibagi oleh bilangan bulat $a \neq 0$ jika terdapat bilangan bulat c sehingga $b = ac$, ditulis $a|b$. Notasi $a \nmid b$ digunakan untuk menyatakan b tidak habis terbagi oleh a.

Jadi 12 terbagi oleh 4 sebab $12 = 4 \cdot 3$, tetapi 10 tidak terbagi oleh 3 sebab tidak ada bilangan bulat c sehingga $10 = 3c$, atau setiap bilangan bulat c berlaku $10 \neq 3c$. Dalam kasus ini ditulis $4|12$ dan $3 \nmid 10$ (Sukirman, 1997).

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:

$a|0, 1|a,$ dan $a|a$ untuk $a \neq 0$

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

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

Teorema 2.1.1

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

1. $a|1$ jika dan hanya jika $a = 1$ atau $a = -1$.

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

3. Jika $a|b$ dan $b|c$ maka $a|c$.

4. $a|b$ dan $b|a$ jika dan hanya jika $a = b$ atau $a = -b$.

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

6. Jika $a|b$ dan $a|c$, maka $a|(bx + cy)$ untuk sebarang bilangan bulat *x* dan *y* (Sukirman, 1997).

Bukti.

1. Jika $a = 1$ atau $a = -1$,maka jelas bahwa $a|1$, sesuai penjelasan sebelumnya. Sebaliknya, diketahui $a|1$ berarti ada $k \in \mathbb{Z}$ sehinga 1 = *ka*. Persamaan ini hanya dipenuhi oleh dua kemungkinan berikut: *k* = 1, *a* = 1 atau $k = -1, a = -1$. Jadi berlaku jika $a|1$ maka $a = 1$ atau $a = -1$. Jadi terbukti $a|1$ jika hanya jika $a = 1$ atau $a = -1$,
2. Diketahui $a|b$ dan$c|d$ yaitu ada $k_1, k_2 \in \mathbb{Z}$ sehingga $b = k_1 a$ dan $d = k_2 c$. Dengan mengalikan kedua persamaan tersebut diperoleh :

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

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

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

   dan

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

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

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

4. Diketahui

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

   dan

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

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

5. Diberikan $b = ac$ untuk suatu $c \in \mathbb{Z}$. Diambil nilai mutlaknya $|b| = |ac| = |a||c|$. Karena $b \neq 0$ maka $|c| \geq 1$. Sehingga diperoleh $|b| = |a||c| \geq |a|$.
6. Diketahui $a|b$ dan $a|c$, maka terdapat $k_1, k_2 \in \mathbb{Z}$ sedemikian sehingga $b = k_1 a$ dan $c = k_2 a$. Untuk sebarang $x, y \in \mathbb{Z}$ berlaku

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

yang berarti $a|(bx + cy)$. ■

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

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

untuk setiap bilangan bulat $x_1, x_2, \cdots, x_n$. Selanjutnya, akan dibahas pengertian faktor persekutuan terbesar.

2.2 Modulo

Modulo merupakan salah satu struktur yang digunakan pada gcd**.**

Definisi 2.2.1

Misalkan *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 operator modulo :

$23\ (mod\ 5) = 3 \qquad (23 = 5\ x\ 4 + 3)$

$27\ (mod\ 3) = 0 \qquad (27 = 3\ x\ 9 + 0)$

2.3 Relasi Kongruensi

Definisi 2.3.1

Misalkan *a* dan *b* adalah bilangan bulat dan m bilangan bulat dengan $m > 0, a$ kongruen dengan b mod m, dituliskan dengan $a \equiv b$ (mod *m*) jika *m* habis membagi *a* – *b*. Jika *a* tidak kongruen dengan *b* dalam modulus *m*, maka dapat ditulis $a \not\equiv b$ (mod *m*) (Grillet, 2007).

Contoh

$17 \equiv 2\ (mod\ 3)$ (3 habis membagi $17 - 2 = 15$)

$12 \not\equiv 2\ (mod\ 7)$ (7 tidak habis membagi $12 - 2 = 10$)

Kekongruenan $a \equiv b\ (mod\ m)$ dapat pula dituliskan dalam hubungan $a = b + km$ dengan ini *k* adalah bilangan bulat..

Contoh

$17 \equiv 2(mod\ 3)$ dapat ditulis sebagai $17 = 2 + 5.3$

$-17 \equiv 15(mod\ 11)$ dapat ditulis sebagai $-7 = 15 + (-2).11$

Contoh

Beberapa hasil operasi dengan relasi kongruensi berikut:

$23(mod\ 5) = 23$ dapat ditulis sebagai $23 \equiv 3(mod\ 5)$

$27(mod\ 3) = 0$ dapat ditulis sebagai $27 \equiv 0(mod\ 3)$

Berdasarkan pengertian kongruen terdapat pada Definisi 2.3.1, maka berikut ini akan diberikan teorema tentang kongruen.

Teorema 2.3.1

Misalkan *m* adalah bilangan bulat positif.

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

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

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

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

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

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

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

Bukti

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

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

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

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

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

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

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

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

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

$(km)^p$

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

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

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

2. (i) $a \equiv b \pmod{m} \Leftrightarrow a = b + k_1m$, untuk suatu $k_1 \in \mathbb{Z}$

$c \equiv d \pmod{m} \Leftrightarrow c = d + k_2m$, untuk suatu $k_2 \in \mathbb{Z}$

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

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

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

(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 $l \in \mathbb{Z}$

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

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

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

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

2.4 Faktor Persekutuan Terbesar (FPB)

Definisi 2.4.1

Misalkan *a* atau *b* bilangan – bilangan bulat yang tidak nol, *d* adalah faktor persekutuan terbesar (FPB) atau adalah greatest common divisor dari *a* dan *b* (ditulis (*a,b*)) jika dan hanya jika *d* faktor persekutuan dari *a* dan *b*, jika *c* faktor persekutuan dari *a* dan *b* maka $c \leq d$.

Dari Definisi 2.1.1, maka dapat dinyatakan sebagai berikut :

d = (*a, b*) jika hanya jika

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

*(ii)*j ika *c* | *a* dan *c* | *b* maka $c \leq d$.

Syarat (i) menyatakan bahwa *d* adalah faktor persekutuan dari *a* dan *b*. Sedangkan syarat (ii) menyatakan bahwa *d* adalah faktor persekutuan terbesar (Burton, 1980).

2.5 Bilangan Prima

Definisi 2.5.1

Sebuah bilangan bulat $p > 1$ disebut bilangan prima, jika dan hanya jika habis dibagi dengan 1 dan bilangan itu sendiri atau p (Burton,180)

Teorema 2.5.1

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

$$n = p_1^{a_1} p_2^{\alpha 2} ... p_k^{a_k}$$

dengan $p_1, p_2, ..., p_k$ sebagai faktor-faktor prima dari n dan $a_1, a_2, ..., a_k$ merupakan eksponen positif berturut-turut $p_1, p_2, ..., p_k$.

Contoh 2.5.1

Bentuk kanonik dari bilangan bulat :

a. $360 = 2^3.3^2.5$

b. $4725 = 3^3.5^2.7$

c. $17460 = 2^3.3^2.5.7^2$

Berikut ini akan diberikan teorema terkait bilangan prima dengan relasi kongruensi.

Definisi 2.5.2

Bilangan $a, b \in \mathbb{R}$, a dan b dikatakan coprima atau relative prima jika gcd $(a, b) = 1$. Dengan kata lain a dan b tidak mempunyai faktor prima bersama (Burton, 1980).

Contoh 2.5.2

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

Penyelesaian

Untuk menunjukkan hal di atas, dengan menggunakan relasi kongruensi cukup.

ditunjukan bahwa $5^{38} \equiv 4 \pmod{11}$.

Bukti

$$5^{38} = (5^{10})^{3=8}$$

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

$$\equiv (1^3)\ x\ (3^4)\ (mod\ 11)$$

$$\equiv 81\ (mod\ 11)$$

$$\equiv 4\ (mod\ 11)\ \blacksquare$$

Definisi 2.5.3

Bentuk $n = p_1^{a_1} p_2^{\alpha 2} \ldots p_k^{a_k}$ disebut representasi *n* sebagai hasil kali bilangan-bilangan prima, sering pula bentuk itu disebut bentuk kanonik *n*.

Contoh 2.5.3

Buktikan bahwa $41 \mid 2^{20} - 1$.

Penyelesaian

Untuk menunjukkan soal di atas, cukup ditunjukkan $2^{20} - 1 \equiv 0\ (mod\ 41)$

Bukti

$$2^5 \equiv -9 (mod\ 4)$$

$\Leftrightarrow (2^5)^4 \equiv (-9)^4 (mod\ 41)$ dengan menggunakan Sifat Relasi Kongruensi

$\Leftrightarrow \quad 2^{20} \equiv 81x\ 81\ (mod\ 41)$

$\Leftrightarrow \quad 2^{20} \equiv (-1).(-1)\ (mod\ 41)$

$\Leftrightarrow \quad 2^{20} \equiv 1\ (mod\ 41)$

$\Leftrightarrow \quad 2^{20} - 1 \equiv 1 - 1\ (mod\ 41)$ dengan menggunakan Sifat Relasi Kongruensi(e)

$\Leftrightarrow \quad 2^{20} - 1 \equiv 0 \ (mod\ 41)$

Dengan kata lain $41 \mid 2^{20} - 1$. ■

Akibat 2.5.3 (Teorema Fundamental Aritmatika)

Sebarang bilangan bulat positif n > 1 dapat ditulis dengan tunggal dalam bentu kanonik

$$n = p_1^{a_1} p_2^{\ 2} ... p_k^{\ a_k}$$

dengan $a_1, a_2, ..., a_k$ bilangan bulat positif dan $p_1, p_2, ..., p_k$ bilangan prima dan $p_1 < p_2 < ... < p_k$.

Teorema 2.5.4 (Teorema Fermat)

Jika *p* adalah prima dan p tidak membagi a, maka *:*

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

Teorema 2.5.5

Jika *p* dan *q* bilangan prima berbeda sedemikian sehingga :

$$a^p \equiv a (mod\ q)$$

dan

$$a^q \equiv a (mod\ p)$$

maka

$$a^{pq} \equiv a (mod\ pq)$$

2.6 Perkongruenan Linear

2.6.1 Pengertian perkongruenan linear

Setelah dipelajari relasi kekongruenan (sifat-sifat dan kegunaan) pada bagian sebelumnya, berikut ini akan dipelajari perkongruenan linear.

Definisi 2.6.1

a. Kalimat terbuka yang menggunakan relasi kekongruenan disebut perkongruenan.
b. Jika suatu perkongruenan, pangkat tertinggi variabelnya paling tinggi satu disebut perkongruenan linear.

Teorema 2.6.1

Perkongruenan linear $ax \equiv b \pmod{m}$ mempunyai solusi jika dan hanya jika $\gcd(a,m) = d \mid b$

Contoh 2.6.1

1. Perkongruenan :

$$3x \equiv 4 \pmod{5}$$

$$x^4 + 3x - 3 \equiv 0 \pmod{31}$$

2. Perkongruenan linear :

$$3x \equiv 4 \pmod{5}$$

$$5x \equiv 2 \pmod{4}$$

Bentuk umum perkongruenan linear :

$$\boxed{ax \equiv b \pmod{m}}$$

2.6.2 Solusi Perkongruenan Linear

Perhatikan perkongruenan linear berikut :

$$3x \equiv 4 \pmod 5 \qquad (2.6.1)$$

Jika *x* pada (2.6.1) diganti dengan bilangan 3, maka akan dipeoleh $3.3 \equiv 4$ (mod 5) atau $3.3 \equiv 4 \pmod 5$ atau $9 \equiv 4 \pmod 5$, merupakan kalimat kekongruenan yang banar. 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 (2.6.1) akan mempunyai solusi (penyelesaian) jika dan hanya jika terdapat bilangan-bilangan bulat *x* dan *k* sehingga $ax = b + km$.

Misalkan *r* memenuhi perkongruenan linear (2.6.1), maka $ar \equiv b \pmod m$. Sehingga setiap bilangan bulat

(r +m), (r + 2m), (r + 3m),..., (r - m), (r – 2m), (r – 3m), . .. (2.6.2)

memenuhi perkongruenan linear (2.6.1), sebab :

$a(r + km) \equiv ar + akm \equiv b \pmod m$ untuk setiap biangan 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 $0 \le s < m$, karena setiap bilangan bulat terletak di atara dua kelipatan m yang berurutan. Jadi, jika r memenuhi perkongruenan (2.6.1) dan $km \le r \le (k+1)m$ untuk suatu bilangan bulat k maka $0 \le (r - km) < m$. Oleh karena itu, diperoleh

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

Dengan kata lain, *s* adalah **residu terkecil modulo *m*** (lihat Definisi 2.6.1) yang memenuhi perkongruenan (2.6.1). Selanjutnya s disebut **solusi (penyelesaian)** dari perkongruenan linear (2.6.1).

Contoh 2.6.2

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 $2x \equiv 4 \pmod 7$ adalah ..., -19, -12, -5, 2, 9, 16,... . Jadi solusi dari perkongruenan linear tersebut adalah 2, sebab 2 merupakan residu terkecil modulo 7 yang memenuhi $2x \equiv 4 \pmod 7$.

2. Selesaikan penyelesaian $2x \equiv 4 \pmod 6$.

   Penyelesaian :

   Gcd(2,6) = 2 dan 2 membagi 4, maka perkongruenan tersebut mempunyai penyelesaian dan mempunyai tepat 2 solusi. Nilai *x* yang memenuhi $2x \equiv 1 \pmod 6$ 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 $2x \equiv 4 \pmod 6$.

Akibat 2.6.2

Jika $\gcd(a,m) \nmid b$, maka perkongruenan linear $ax \equiv b \pmod m$ mempunyai solusi.

2.6.3 Sistem Perkongruenan Linear

Bentuk umum perkongruenan linear :

$x \equiv a_1 (mod\ m_1)$

$x \equiv a_2 (mod\ m_2)$

$x \equiv a_3 (mod\ m_3)$
. .
. .
. .
$x \equiv a_i (mod\ m_i)$

dengan m_1, m_2, ..., m_k bilangan bulat positif dan gcd(m_i, m_j) = 1 untuk $i \neq j$.

Untuk menyelesaikan sistem perkongruenan linear (2.6.3) digunakan teorema berikut.

Teorema 2.6.3

Jika gcd $(a, m) = 1$, maka perkongruenan linear $ax \equiv b (mod\ m)$

mempunyai tepat satu solusi.

Contoh 2.6.3

Tentukan penyelesaian dari sistem perkongruenan linear berikut :

$x \equiv 2 (mod\ 3)$

$x \equiv 2 (mod\ 3)$
. .
. .
. .
$x \equiv 1 (mod\ 4)$

Penyelesaian

Dari soal di atas diperoleh :

$a_1 = 2$ $m_1 = 3$ $M_1 = 20$

$a_2 = 3$ $m_2 = 5$ $M_2 = 12$

$a_3 = 1$ $m_3 = 4$ $M_3 = 15$

Selanjutnya tinggal mencari s_1, s_2, dan s_3 sebagai berikut :

$20s_1 \equiv 1\ (mod\ 3)$, maka $s_1 = 2$

$20s_2 \equiv 1\ (mod\ 5)$, maka $s_1 = 3$

$15s_2 \equiv 1\ (mod\ 4)$, maka $s_1 = 3$

Sehingga diperoleh penyelesaian

$x_0 = 2.2.20 + 3.3.12 + 1.3.15$

Teorema 2.6.4

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

Teorema 2.6.5 (Chinese Remainder Theorem)

Misalkan $m_1 , m_2 , \dots , m_k$ bilangan bulat positif sedemikian hingga $\gcd(m_i , m_j) = 1$ 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

$$x_0 = a_1 s_1 M_1 + a_2 s_2 M_2 + \dots + a_i s_i M_i$$

dengan

$M_1 \frac{m_1 m_2 \ldots m_i}{m_1} . s_i$ adalah bilangan yang memenuhi

perkongruenan linear.

$$M_1 s_1 \equiv 1 (mod\ m_1) \ ; \ i = 1,2, \ldots, k$$

2.7 Bilangan Komposit

Definisi 2.7.1

Bilangan komposit adalah bilangan asli lebih besar sama dengan 1 yang bukan merupakan bilangan prima. Bilangan komposit dapat dinyatakan sebagai faktorisasi bilangan bulat, atau hasil perkalian dua bilangan prima atau lebih.

Sepuluh bilangan komposit yang pertama adalah 4,6,8,9,10,12,14,15,16 dan 18. Atau bisa juga disebut bilangan yang mempunyai faktor lebih dari dua.

2.8 Bilangan Carmichael

Definisi 2.8.1

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

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

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).