II. TINJAUAN PUSTAKA

2.1 Keterbagian

Secara umum apabila *a* bilangan bulat dan *b* bilangan bulat positif, maka ada tepat satu bilangan bulat *q* dan *r* sedemikian sehingga :

$$b = q + r, \ 0 \leq r < b$$

dalam hal ini *b* disebut hasil bagi dan *r* adalah sisa pada pembagian " *b* dibagi dengan *a*". jika *r* = 0 maka dikatakan b habis dibagi *a* dan ditulis $a|b$. untuk *b* tidak habis dibagi *a* ditulis $a \nmid b$.

Ada bahasa lain untuk menyatakan relasi pembagian $a|b$, mungkin dikatakan bahwa a membagi b, a adalah pembagi dari *b*, bahwa *a* adalah faktor dari *b* atau bahwa *b* adalah multiple dari *a*.

Definisi 2.1.1

Bilangan bulat *a* membagi habis bilangan bulat $b \neq 0$, ditulis $a|b$, jika dan hanya jika ada bilangan bulat k sehingga $b = a$. Jika *a* tidak membagi *b* maka $a \nmid b$.

(Sukirman,1997)

Contoh:

1. $2|14$, sebab $14 = 2k$ dengan $k = 7$
2. $3 \nmid 10$, sebab tidak ada bilangan bulat k sehingga $10 = 3k$.

Teorema 2.1.1

Untuk bilangan bulat $a, b,$ dan c berlaku sebagai berikut:

1. $a|0, 1 \mid a, a|a$
2. $a|1$ jika dan hanya jika $a = \pm 1$
3. Jika $a|b$ dan $b|c$, maka $a|c$
4. Jika $a|b$ dan $a|c$ maka $a|(b + c)$
5. Jika $a \ |c$, maka $a|c$ dan $b|c$
6. Jika $d|b$ maka $d| - b$
7. Jika $a|b$ dan $c|d$, maka $a \ |b$
8. $a|b$ maka $a|c$, untuk sebarang bilangan bulat c
9. Jika $a|b$ dan $a|c$, maka $a|(b \ + c)$ untuk setiap bilangan bulat m dan n.

(Burton,1994)

Bukti.

(1). Untuk $a|0$, ada suatu bilangan bulat m sehingga $a = 0$ karena $a \neq 0$ maka haruslah $m = 0$ sehingga $a|0$. Untuk $1|a, 1.m = a,$ maka haruslah $m = a$ sehingga $1|a$. Untuk $a|a, a.m = a,$ maka haruslah $m = 1$ sehingga $a|a$.

(2). Misalkan $a \neq 1$ atau $a \neq -1$, maka $a = 1$, karena a dan m bilangan bulat, maka haruslah a dan m sama dengan 1 atau -1.

(3). Jika $a|b$ maka ada suatu bilangan m sehingga $a = b$, dan jika $b|c$ maka ada suatu bilangan bulat n sehingga $b = c$. Jika $a|b$ dan $b|c$ maka berlaku:

$a \ .b \ = b$

$a \ .m \ = b$ ($m \ = k$, untuk setiap k bilangan bulat)

$a \ = c$

dengan demikian dapat ditulis $a|c$

(4). Dengan mengikuti sifat (3), maka $a|b$ dapat ditulis dengan $a \ = c$

$a \ + a \ = b + c$

$a \, (m + n) \ = b \ + \ c$ ($m \ + \ n \ = \ k$, untuk setiap k bilangan bulat)

$a \ = b \ + \ c$

dengan demikian benar bahwa $a|(b \ + c)$

(5). Jika $a \ |c$, ada suatu bilangan bulat m sehingga dapat ditulis dengan

$a \ .m \ = \ c$

$a \, . b \ = \ c$ ($b \ = k$, untuk setiap k bilangan bulat)

$a \ = \ c$, dapat ditulis dengan $a|c$

$b \, . a \ = \ c$ ($a \ = \ l$, untuk setiap l bilangan bulat)

$b \, . l \ = \ c$, dapat ditulis dengan $b|c$

(6). Dengan mengikuti sifat (2) jelas bahwa jika $d|b$ maka $d| - b$.

(7). Jika $a|b$, maka terdapat bilangan bulat m sehinga $a \ = \ b$, dan jika $c|d$ maka terdapat bilangan bulat n sehingga $c \ = \ d$. Jika $a|b$ dan $c|d$, maka:

$a \ .c \ = b.d$

$a \ .m \ = \ b$ ($m \ = k$, untuk setiap k bilangan bulat)

$a \ .k \ = \ b$

dengan demikian, jika $a|b$ dan $c|d$ maka $a \ |b$

(8). Jika $a|b$, maka terdapat bilangan bulat m sehinga $a \ = \ b$.

$a \ = \ b$

$a \ .c \ = \ c$ (c adalah bilangan bulat)

$a.m = c$ ($m = k$, untuk setiap k bilangan bulat)

$a = c$

dengan demikian jika $a|b$ maka $a|c$ untuk setiap c sebarang bilangan bulat.

(9). Jika $a|b$, maka terdapat bilangan bulat k sehinga $a = b$. Jika $a|c$, maka terdapat bilangan bulat l sehinga $a = c$. maka berlaku:

$b + c = al + a\ n = a(k + ln) = a(k + ln)$

$= b + c$

dengan demikian jika $a|b$ dan $a|c$ maka $a|(b + c)$

2.2 Bilangan Prima

Definisi 2.2.1

Suatu bilangan bulat $p > 1$ yang tidak memiliki faktor positif kecuali 1 dan p, maka p disebut bilangan prima. Bilangan buat lebih dari 1 dan bukan prima disebut bilangan komposit (tersusun).

(Sukirman,1977)

Contoh:

$2, 3, 5, 7, 11, 13, 17$ adalah bilangan prima. $4, 6, 8, 9, 10, 12$ adalah contoh dari bilangan-bilangan komposit. Menurut definisi 2.2.1 tersebut, 1 bukan bilangan prima maupun komposit, 1 disebut unit. Jadi himpunan bilangan bulat positif (bilangan asli) terbagi dalam 3 himpunan yang saling lepas, yaitu himpunan semua bilangan prima, himpunan semua bilangan komposit dan himpunan unit. Ambil sebarang bilangan bulat, misalnya 84, maka 84 dapat ditulis sebagai hasil kali bilangan prima,

$84 = 2.2.3.7$ atau

$84 = 2.3.2.7$ atau

$84 = 3.7.2.2$ atau lainnya.

Teorema 2.2.1

Setiap bilangan bulat $n, n > 1$ dapat dibagi oleh suatu bilangan prima.

(Sukirman, 1997)

Bukti:

Jika n bilangan prima maka $n|n$, teorema terbukti. Misalnya diambil bilangan komposit n, maka n mempunyai faktor selain 1 dan n. Misalnya d_1, $d_1|n$ maka n_1 sehingga $n = d_1 n_1$ karena $d_1 \neq 1$ dan $d_1 \neq n_1$, maka $1 < n_1 < n$. Jika n_1 bilangan prima maka $n_1 |n$, jika n_1 bilangan komposit, misalkan $d_2|n_1$, maka ada n_1 sehingga $n_1 = d_2 n_2$ dengan $1 < n_2 < n_1$. Jika n_2 bilangan prima maka $n_2|n_1$ dan n_1 |n, maka $n_2|n$. tetapi jika n_2 bilangan komposit dan misalkan $d_3|n_2$, maka ada n_3 sehingga $n_2 = d_3 n_3$ dengan $1 < n_3 < n_2$. Demikian seterusnya sehingga terdapat barisan $n, n_1, n_2, n_3, \ldots$ dengan $n > n_1 > n_2 > n_3 >$ ... dan setiap $n_i > 1$ dengan $i = 1, 2, 3, \ldots$, misalkan n_k adalah bilangan prima, maka n $|n$ karena $n_k| n_{k-1}$, $n_{k-1}| n_{k-2}, \ldots, n_1 |n$, dengan menggunakan pernyataan di atas dapat disimpulkan bahwa setiap bilangan bulat positif lebih besar dari 1 dapat dinyatakan sebagai hasil kali bilangan-bilangan prima.

Teorema 2.2.2

Setiap bilangan bulat $n > 1$ dapat dinyatakan sebagai hasil kali bilangan prima (mungkin hanya memiliki 1 faktor).

(Sukirman, 1997)

Bukti:

Dari teorema 2.2.1 diketahui bahwa ada n_i sehingga $n = p_1 n_1$ dengan $1 \leq n_1 < n$. jika $n_1 = 1$ maka $n = p$, berarti n bilangan prima. Sehingga $n_1 = p_2 n_2$dengan $1 \leq n_2 < n_1$. Jika $n_2 = 1$ maka $n_1 = p_2$ sehingga $n = p_1 p_2$, berarti n dapat dinyatakan sebagai hasil kali faktor-faktor bilangan prima. Tetapi jika $n_2 > 1$ proses seperti di atas dilanjutkan sehingga diperoleh $ni = 1$. Penguraian atas faktor-faktor prima itu pasti berakhir, karena $n > n_1 > n_2 >$ ... dan setiap $n_i \geq 1$. Misalkan untuk suatu $k, n_k = 1$, maka $n = p_1 p_2 \ldots p_k$ adalah hasil kali faktor-faktor prima yang sama dengan n jadi setiap bilangan bulat positif yang lebih besar dari 1 dapat dinyatakan sebagai hasil kali bilangan-bilangan prima.

2.3 Kekongruenan

Definisi 2.3.1

Misal n ditetapkan sebagai bilangan bulat positif, bilangan bulat *a* dan *b* dikatakan sebagai kongruen modulo n dituliskan dengan:

$$a \equiv b \pmod{n}$$

jika n adalah pembagi selisih $a - b$, berarti bahwa $a - b = k$, untuk setiap bilangan bulat k. Untuk membenarkan gagasan tersebut misal $n = 7$. Dan sebagai contoh sebagai berikut:

$3 \equiv 24 \pmod{7}$ $\quad -31 \equiv 11 \pmod{7}$ $\quad -15 \equiv -64 \pmod{7}$

Karena $3 - 24 = (-3)\,7, -31 - 11 = (-6)\,7$, dan $-15 - (-64) = (7)\,7$.

Pada sisi lain, jika $n \nmid (a - b)$, kemudian dikatakan bahwa *a* adalah bukan kongruen untuk *b* modulo n dan ditulis $a \not\equiv b \pmod{n}$. Sebagai contoh,

$25 \not\equiv 12 \pmod 7$, karena 7 tidak bisa untuk membagi $25 - 12 = 13$.

(Burton, 1999)

Teorema 2.3.1

Setiap bilangan bulat kongruen modulo n tepat satu diantara $0, 1, 2, \ldots, n-1$.

(Sukirman, 1997)

Definisi 2.3.2

Pada $a \equiv r \pmod n$ dengan $0 \leq r < n$, maka r disebut *residu* terkecil moduloi n. Untuk kongruen ini disebut himpunan *residu* terkecil modulo n.

(Sukirman, 1997)

Contoh:

1. *Residu* terkecil dari 71 modulo 2 adalah 1
2. *Residu* terkecil dari 71 modulo 3 adalah 2
3. Walaupun $34 \equiv 9 \pmod 5$ tetapi 9 bukan *residu* terkecil dari $34 \equiv 9 \pmod 5$ karena $9 > 5$.
4. Himpunan *residu* terkecil modulo 5 adalah { 0,1,2,3,4}.

Teorema 2.3.2

$a \equiv b \pmod n$ jika dan hanya jika a dan b memiliki sisa-sisa yang sama jika dibagi n.

(Sukirman,1997)

Bukti:

Pertama dibuktikan jika $a \equiv b \pmod n$ maka ada a dan b yang memiliki sisa yang sama jika dibagi m. $a \equiv b \pmod n$ maka $a \equiv r \pmod n$ dan

$b \equiv r \pmod n$ dengan r adalah *residu* terkecil modulo n atau $0 \leq r < n$.

$a \equiv r \pmod{n}$ berarti $a = n + r$ untuk suatu bilangan bulat q

$b \equiv r \pmod{n}$ berarti $b = n + r$ untuk suatu bilangan bulat t

ini berarti a dan b memiliki sisa yang sama yaitu r jika dibagi n. Kedua, dibuktikan jika a dan b memiliki sisa yang sama jika dibagi n maka $a \equiv b \pmod{n}$.Misalkan a memiliki sisa r jika dibagi n, berarti $a = n + r$ dan a memiliki sisa r jika dibagi n, berarti $a = n + r$ dari kedua persamaan itu diperoleh bahwa:

$a - b = n(q - t)$ berarti $n|(q - b)$ atau $a \equiv a \pmod{n}$

Contoh:

$47 \equiv 12 \pmod{5}$

$47 = (6)\ 7 + 5$

$12 = (1)\ 7 + 5$

Dengan sisa yang sama yaitu 5.

Teorema 2.3.3

Misal $n > 0$ dan a, b, c, d sebarang bilangan bulat. Maka mengikuti sifat-sifat sebagai berikut:

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$, maka $b \equiv a \pmod{n}$
3. Jika $a \equiv b \pmod{n}$ dan $b \equiv c \pmod{n}$, maka $a \equiv c \pmod{n}$
4. Jika $a \equiv b \pmod{n}$ dan $c \equiv d \pmod{n}$ maka $a + c \equiv b + d \pmod{n}$ dan $a \equiv b \pmod{n}$
5. Jika $a \equiv b \pmod{n}$ maka $a + c \equiv b + c \pmod{n}$ dan $a \equiv b \pmod{n}$

6. Jika $a \equiv b \pmod{n}$ maka $a \equiv b \pmod{n}$ untuk setiap bilangan bulat k

(Burton, 1999)

Bukti:

1. Untuk setiap bilangan bulat a diketahui bahwa $a - a = 0.n$, sedemikian sehingga $a \equiv a \pmod{n}$.
2. Jika $a \equiv b \pmod{n}$ maka, $a - b = k$, untuk setiap bilangan bulat *k*, karena itu $b - a = -k = (-k)n$, dan $-k$ adalah bilangan bulat.
3. Andaikan bahwa $a \equiv b \pmod{n}$ dan juga $b \equiv c \pmod{n}$ dan ada bilangan bulat h dan k memenuhi $a - b = hn$ dan $b - c = k$. Hal itu Menunjukkan bahwa $a - c = (a - b) + (b - c) = hn + k = (h + k)n$, ini berakibat dimana $a \equiv c \pmod{n}$.
4. Jika $a \equiv b \pmod{n}$ dan $c \equiv d \pmod{n}$, maka diketahui bahwa $a - b = k_1 n$ dan $c - d = k_2 n$ untuk pilihan yang sama dari $k_1$dan k_2

   Penjumlahan persamaan tersebut, diperoleh

   $(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n = (k_1 + k_2)n$

   Atau seperti suatu pernyataan kongruen, $a + c \equiv b + d \pmod{n}$

   $$a = (b + k_2 n)(d + k_2 n) = b + (bk_2 + dk_2 + k_1 k_2 n)n$$

   karena $bk_2 + dk_2 + k_1 k_2 n$ adalah suatu bilangan bulat, ini bisa dikatakan bahwa $a - b$ dapat dibagi dengan n, dimana

   $a \equiv b \pmod{n}$.
5. Bukti dari sifat 5 mencakup 4 dan kenyataan bahwa $c \equiv c \pmod{n}$.
6. Untuk $k = 1$ diasumsikan bahwa hal ini benar untuk semua k, dari sifat 4 ditahui bahwa $a \equiv b \pmod{n}$ dan $a^k \equiv b^k \pmod{n}$,secara tidak

langsung dapat dinyatakan $aa^k \equiv bb^k \pmod{n}$, atau *equivalent* dengan $a^{k+1} \equiv b^{k+1}$ ($m \quad n$) hal ini menyatakan bahwa $k+1$ merupakan akhir dari pembuktian. Dengan demikian terbukti bahwa jika $a \equiv b \pmod{n}$ maka $a^k \equiv b^k \pmod{n}$, untuk sebarang bilangan positif k.

2.4 Barisan

Sebuah barisan dapat di bayangkan sebagai suatu daftar bilangan yang dituliskan dalam suatu daftar urutan tertentu:

$$a_1, a_2, a_3, \dots, a_n, \dots$$

Bilangan $a_1$disebut suku pertama, a_2, suku kedua dan secara umum a_n suku ke n, akan dibahas barisan tak hingga saja dan karenanya setiap suku berikutnya a_{n+1}. Perhatikan bahwa untuk setiap bilangan bulat positif n terdapat satu bilangan $a_n$yang terkait dan karenanya sebuah barisan dapat didefinisikan sebagai sebuah fungsi yang daerah asalnya adalah himpunan bilangan bulat positif. Tetapi biasanya ditulis $a_n$dan bukan notasi fungsinya $f(n)$ untuk menyatakan notasi fungsi tersebut ada di bilangan *n*. Notasi barisan {a_1, a_2, a_3, …} juga dinyatakan sebagai $\{a_n\}$ atau $\{a_n\}_{n-1}^{\infty}$.

Contoh:

Sejumlah barisan dapat didefinisikan dengan memberikan rumus untuk suku ke *n*-nya. Pada contoh berikut diberikan tiga penyajian barisan: pertama dengan menggunakan notasi di atas, kedua dengan menggunakan rumus suku ke-n dan ketiga dengan menuliskan suku-suku barisan tersebut. Perhatikan bahwa n tidak harus dimulai dari satu.

a. $\left\{\frac{n}{n+1}\right\}_{n=1}^{\infty}$ $a_n = \frac{n}{n+1}$ $\left\{\frac{1}{2},\frac{2}{3},\frac{3}{4},\frac{4}{5},\ldots,\frac{n}{n+1},\ldots\right\}$

b. $\left\{\frac{(-1)^n(n+1)}{3^n}\right\}$ $a_n = \frac{(-1)^n(n+1)}{3^n}$ $\left\{-\frac{2}{3},\frac{3}{9},-\frac{4}{27},\frac{5}{81},\ldots,\frac{(-1)^n(n+1)}{3^n},\ldots\right\}$

c. $\left\{\sqrt{n-3}\right\}_{n=3}^{\infty}$ $a_n = \sqrt{n-3}, n \geq 3$ $\left\{0,1,\sqrt{2},\sqrt{3},\sqrt{n-3},\ldots\right\}$

(James Stewart, 2003)

2.5 Norma Euler (Euler's Criterion)

Corollary 2.5.1

Misal p adalah bilangan prima dan misal gcd $(a,p) = 1$ maka a adalah

q r m p jika

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

Dan a adalah q n nr m p jika

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

(Bach and Eric, 1996)

2.6 Simbol Jacobi

Definisi 2.6.1

Untuk setiap bilangan bulat a dan untuk setiap bilangan bulat positif , simbol Jacobi didefinisikan sebagai hasil dari simbol Legendre bersamaan dengan faktor-faktor prima dari n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^{\alpha_1}\left(\frac{a}{p}\right)^{\alpha_2}\ldots\left(\frac{a}{p}\right)^{\alpha_k}$$ dimana $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$

$\left(\frac{a}{p}\right)$ merupakan simbol Legendre, yang didefinisikan untuk semua

bilangan bulat a dan semua bilangan prima p dengan

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ jika } a \equiv 0 (\text{mod } p) \\ 1 \text{ jika } a \not\equiv 0 (\text{mod } p) \text{dan untuk bilangan bulat } x, a \equiv x^2 (\text{mod } p) \\ -1 \text{ jika tidak ada } x \end{cases}$$

Mengikuti ketentuan umum untuk hasil kosong, $\left(\frac{a}{1}\right) = 1$.

(Wikipedia,2011)

Theorema 2.6.1

1. jika n adalah bilangan prima, maka simbol Jacobi $\left(\frac{a}{n}\right)$ juga merupakan simbol Legendre.
2. Jika $a \equiv b (\text{mod } n)$ maka $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ jika } \gcd(a, n) \neq 1 \\ \pm 1 \text{ jika } \gcd\ (a, n) = 1 \end{cases}$
4. $\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ jadi $\left(\frac{a^2}{p}\right) = 1$ (atau 0)
5. $\left(\frac{a}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{n}\right)$ jadi $\left(\frac{a}{n^2}\right) = 1$ (atau 0)

Hukum dari *quadratic reciprocity*: jika m dan n adalah bilangan bulat prima positif , maka

6. $\left(\frac{m}{n}\right) =$

$$\left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}} = \begin{cases} \left(\frac{n}{m}\right) \text{ jika } n \equiv 1 (\text{mod } 4) \text{atau } m \equiv 1 (\text{mod } 4) \\ -\left(\frac{n}{m}\right) \text{ jika } n \equiv m \equiv 3 (\text{mod } 4) \end{cases}$$

Dan berikut ini sebagai tambahan.

7. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 \text{ jika } n \equiv 1 \pmod 4 \\ -1 \text{ jika } n \equiv 3 \pmod 4 \end{cases}$

8. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 \text{ jika } n \equiv 1,7 \pmod 8 \\ -1 \text{ jika } n \equiv 3,5 \pmod 8 \end{cases}$

(Wikipedia,2011)

2.7 Lapangan berhingga (*Finite Field*)

Jika suatu lapangan (*field*) memuat elemen yang banyaknya berhingga, maka lapangan ini disebut dengan lapangan berhingga (*finite field*).

Teorema 2.7.1

Himpunan $\mathbb{Z}_n$ merupakan lapangan berhingga jika dan hanya jika n adalah bilangan prima.

(Fraleigh, 2000)

Teorema 2.7.2

Misal p adalah bilangan prima dan misal n adalah bilangan bulat positif, maka terdapat suatu lapangan berhingga dengan anggota p^n.

(Erich Bach dan Jeffrey Shallit, 1997

2.8 *Frobenius Automorphism*

Misal $\mathbb{F}$ adalah suatu lapangan dari karekteristik lapangan p. Maka Frobenius automorphism pada $\mathbb{F}$ adalah pemetaan $\emptyset : \mathbb{F} \to \mathbb{F}$ yang memetakan dari α ke α^puntuk setiap anggota α dari $\mathbb{F}$

(Wikipedia, 2011)

2.9 Teorema *Lucas-Lehmer test*

Teorema 2.9.1

Misal *p* sebuah bilangan prima > 2, dan $n = 2^p - 1$. juga didefinisikan $S_1 = 4$ dan $S_{k+1} = S_k^2 - 2$ untuk $k \geq 1$, maka n adalah prima jika $S_{p-1} \equiv 0 (\mathrm{mod}\ n)$.

(Eric Bach dan Jeffrey Shallit,1997

Contoh:

Diberikan suatu test yang praktis untuk keprimaan dari bilangan prima *Mersenne*. Sebagai contoh, misal sebagai test M_7 =127. menghitung modulo 127, ditemukan $S_1 \equiv 4$, $S_2 \equiv 14$, $S_3 \equiv 67$, $S_4 \equiv 42$, $S_5 \equiv 111$, $S_6 \equiv 0$, karenanya 127 adalah prima.

2.10 Test kemungkinan prima Melham untuk N_p

Teorema 2.10.1

Misal p adalah suatu bilangan prima. Didefinisikan suatu barisan $\{Sn\} n \geq 0$ dengan

$S_0 = 6$,

$S_{k+1} = S^2_k - 2$, $k \geq 0$.

Jika N_p adalah prima, maka $S_{p-1} \equiv -34 \pmod{N_p}$.

(Pedro Berrizbeitia, Florian Luca and Ray Melham, 2010)