BAB II
KONSEP DASAR

2.1 PRIME

Definisi 2.1

Bilangan bulat p>1 disebut bilangan prime atau prime Islam suatu kasus jika tidak ada pembagi d dari p sedemikian hungga 1< d <p. Jika bilangan bulat a>1 bukan prime disebut bilangan komposit.

Jadi sebagai contoh 2,3,5,7 dan 11 adalah prime sedangkan 4,6,8,9 dan 10 adalah bilangan komposit.

Teorema 2.1

Setiap bilangan bulat n > 1 dapat dinyatakan sebagai hasil kali dari prime.

Bukti :

Jika bilangan bulat n adalah prime, maka bilangan bulat tersebut berdiri sebagai hasil kali dengan faktor tunggal. Sebaliknya, bila n dapat difaktorkan ke dalam yang disebut $n_1 n_2$. dengan $1<n_1<n$ dan $1<n_2<n$. Jika n_1 adalah prime maka n_1 adalah berdiri sendiri. Sebaliknya bila dapat difaktorkan ke dalam bentuk $n_3 n_4$ dengan $1<n_3<n_1$ dan $1<n_4<n_1$,dengan cara yang sama dilakukan juga untuk n_2. Proses ini dilakukan berulang - ulang terhadap bilangan yang dibangun sebagai hasilkali dari faktor - faktor. Sampai dengan yang terakhir karena faktor - faktor ini

lebih kecil daripada gabungan bilangannya dan tiap - tiap faktor masih merupakan bilangan bulat yang lebih besar daripada satu. Jadi n dapat dituliskan sebagai hasilkali dari prime dan faktor prime tidak perlu berbeda, sebagai akibatnya dapat dituliskan dalam bentuk :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$$

dengan $p_1, p_2, \ldots p_r$ adalah bilangan prime yang berbeda dan $\alpha_1, \alpha_2, \ldots, \alpha_r$ positif.

Teorema 2.2

Jika $p|ab$, dengan p adalah prime, maka $p|a$ atau $p|b$. Lebih bersifat umum jika $p|a_1 a_2 \ldots a_n$ maka p membagi pada sedikit - dikitnya satu faktor a_i dari hasil kali a_i, $i = 1,2,\ldots,n$.

Bukti :

Jika $p \nmid a$, maka $(a,b) = 1$ dan karena $p|ab$. Ini adalah langkah awal pada pembuktian dari pernyataan umum dengan induksi matematik. Kemudian diasumsikan bahwa dalil tersebut berlaku pada p yang membagi hasil kali a dengan n faktor. Jika $p|a_1 a_2 \ldots a_n$ sehingga $p|a_1 c$ denga $c = a_2 a_3 \ldots a_n$ maka $p|a_1$ atau $p|c$ dengan menerapkan hipotesa induksi disimpulkan bahwa $p|a_i$ untuk beberapa selang i dari 2 sampai n.

Definisi 2.2 (Daerah Faktorisasi Tunggal)

Daerah integral komutatif R dengan elemen satuan disebut daerah faktorisasi tunggal jika memenuhi syarat - syarat berikut :

(1). setiap non unit dari R adalah hasil kali finite dari faktor irreducible.

(2). jika elemen irreducible p dalam R membagi ab, b∈R maka p membagi a atau p membagi b

contoh dari daerah faktorisasi tunggal adalah ring dari bilangan bulat.

Teorema 2.3 (teorema fundamental pada aritmatik).

Faktor dari sembarang bilangan bulat n >1 kedalam ptime adalah terpisah kedalam order pada faktor - faktor prime.

Bukti :

Bukti pertama :

Diandaikan bahwa terdapat bilangan bulat n dengan 2 faktor yang berbeda dan membaginya atas 2 representasi prime biasa, sehingga didapatkan persamaan dalam bentuk :

$$p_1 p_2 = q_1 q_2 \ldots q_s$$

dengan faktor - faktor p_j dan q_j adalah prime pada kedua sisi. Hal ini adalah tidak mungkin karena $p_1 | q_1 q_2 \ldots q_s$ dari teorema 2.2, p_1 adalah membagi pada sedikit - dikitnya satu dari q_j. Sehingga p_1 harus sama dengan sedikit - dikitnya satu elemen dari pada q_j.

Bukti kedua

Diandaikan bahwa teorema ini salah dan ambil n sebagai bilangan bulat positif terkecil yang mempunyai lebih dari satu representasi sebagai hasil kali dari prime.

$$n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_s$$

dari sini jelas bahwa r dan s adalah lebih besar dari pada satu. Prime $p_1, p_2, \ldots p_s$ tidak mempunyai anggota yang bersamaan dengan $q_1, q_2, \ldots q_s$, karena sebagai contoh , jika p_1 bilangan prime maka dapat membagi kedua sisi pada persamaan (2.2) menjadi 2 faktor yang berbeda dari n/p_1. Tetapi ini akan kontradiksi dengan asumsi bahwa semua bilangan bulat yang lebih kecil dari pada n dapat difaktorkan secara tunggal. Selanjutnya, tanpa menghilangkan anggapan bahwa $p_1 < q_1$ dan didefinisikan bilangan bulat positip n sebagai berikut:

$$N = (q_1 - p_1) q_2 q_3 \ldots q_s = p_1 (p_2 p_3 \ldots p_i - q_2 q_3 \ldots q_s)$$

hal ini jelas bahwa N <n , sehingga N adalah faktor tunggal; dalam prime. Tetapi $p_1 \nmid (q_1 - p_1)$, maka (2.3) memberikan 2 faktor pada N, satu yang mnenyangkut p_1 dan yang lainnya tidak menyangkut p_1 jadi kontradiksi.

Dalam pengguanaan pada teorema fundamental kadang ditulis beberapa bilangan bulat a > 1 dalam bentuk :

$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, dengan prime p_i yang berbeda dengan exponent α_i positif. Meskipun kadang -kadang dilakukan perjanjian untuk menggunakan sedikit variasi pada bentuk kanonik dan memperbolehkan beberapa exponentnya sama dengan 0. Untuk contoh, jika ingin menggambarkan pembagi terbesar g pada a dan b pada hubungannya dengan faktor prime pada a dan b dapat dituliskan :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$$

dengan $\alpha_i \geq 0$ dan $\beta_i \geq 0$. maka pembagi persekutuan terbesarnya

adalah :

$g = (a,b) = p_1^{\min(\alpha_1,\beta_1)} \quad p_2^{\min(\alpha_2,\beta_2)} \ldots\ldots p_r^{\min(\alpha_r,\beta_r)}$

dengan $\min(\alpha,\beta)$ menyatakan minimum dari α dan β. Dalam kasus a = 108 dan b = 225 akan diperoleh :

$a = 2^2 3^3 5^0 \qquad b = 2^0 3^2 5^2 \qquad g = 2^0 3^2 5^0 = 9$

dengan cara sama kelipatan persekutuan terkecil dari a dan b adalah sebagai berikut :

$[a,b] = p_1^{\max(\alpha_1,\beta_1)} \; p_2^{\max(\alpha_2,\beta_2)} \ldots p_r^{\max(\alpha_r,\beta_r)}$

dengan $\max(\alpha,\beta)$ menyatakan maximum dari α dan β. Jika tidak ada α_i yang lebih besar daripada 1 maka dikatakan bahwa adalah hasil perkalian bebas.

Teorema 2.4

Bilangan-bilangan prime adalah infinite. sehingga tidak ada akhir dari barisan bilangan - bilangan prime.

2, 3, 5, 7, 11, 13, ...

Bukti :

Diandaikan bahwa bilangan prime hanya finite $p_1 p_2 .. p_r$ Maka bentuk dari bilangan tersebut adalah $n = 1 + p_1 p_2 \ldots p_r$ dengan catatan bahwa n tidak dapat dibagi dengan p_1 atau p_2 ...atau p_r. Dari sini terdapat beberapa pembagi p dari n adalah prime yang berbeda dari $p_1, p_2 \ldots p_r$. Dengan n adalah salah satu prime yang membagi faktor prime p, ini menyatakan bahwa bilangan prime adalahinfinite.

Teorema 2.5

Terdapat suatu selang dalam barisan prime. Selanjutnya, ditetapkan, diberikan bilangan bulat positif k, terdapat k bilangan bulat yang berurutan.

Bukti :

Dinyatakan bilangan -bilangan bulat:
$(k+1)!+2, (k+1)!+3, \ldots,(k+1)!+k, (k+1)!+k+1.$
setiap unsurnya adalah kombinasi karena j membagi $(k+1)!+j$ jika $2 \leq j \leq k+1$.

Teorema 2.6

Hasil kali dari k bilangan bulat berurutan dapat dibagi dengan k!.

Bukti :

Diasumsikan bahwa koefisien dari $x^k y^{n-k}$ dalam expansi pada $(x+y)^n$ adalah bilangan bulat dengan bentuk :

$$\frac{n!}{k!(n-k)!}$$

dengan n dan k adalah bilangan bulat positif dan $k \leq n$. Sehingga dapat dituliskan dalam bentuk sebagai berikut:

$$\frac{n(n-1)(n-2)\ldots(n-k+1)}{k!}$$

dengan menghilangkan (n-k)! dengan beberapa faktor yang terdapat dalam n!. Hal ini membuktikan untuk bilangan bulat

positif yang berurutan. Tetapi teorema ini mengatakan lebih dari itu, karena disini tidak dibatasi untuk bilangan bulat positif. Mengenai kasus pada bilangan bulat negatifnya dapat dibuktikan sebagai berikut :

pertama - tama terdapat k bilangan bulat negatif yang berurutan , sebagian tanda sama dengan hasil kali dari bilangan bulat yang tidak semuanya positif dan tidak semuanya negatif harus memuat nol diantara hasil kalinya. Dalam kasus ini, hasilnya diperoleh dari definisi pada pembagian.

2.2 RELATIF PRIME.

Perlu dicatat bahwa (a,b) adalah himpunan dari setiap 2 elemen yang assosiate. Jika ditulis (a,b) = c artinya bahwa (a,b) termuat dalam semua unit pergandaan dari c

Definisi 2.3(Relatif prime)

Dalam faktorisasi tunggal domain, 2 elemen a,b disebut relatif prime jika dipenuhi kondisi bahwa (a,b) = 1.

Definisi 2.4 (Pembagian persekutuan terbesar)

Elemen d dari faktorisasi tunggal domain R disebut pembagian persekutuan terbesar dari elemen - elemen a,b jika :

(1). d|a dan d|b .

(2). jika c|a dan c|b maka c|d

Sifat - sifat dari bilangan bulat relatif prime untuk

setiap bilangan bulat a,b,c,d,r dan s adalah sebagai berikut :

(1). Jika terdapat bilangan bulat r dan s sedemikian hingga ra + sb = 1, maka a dan b saling relatif prime.

(2). Jika (a,b) = 1 dan c|ab maka c|b

(3). Jika a|d dan c|d dan (a,c) = 1 maka ac|d

(4). Jika d|ab dan d|cb dengan (a,c)=1 maka d|b

(5). Jika (a,b) = d dengan a=dr dan b=ds maka (r,s) = 1

(6). Jika (a,c) = 1 dan (b,c) = 1 maka (ab,c) = 1

Selanjutnya sifat - sifat dari pembagi persekutuan terbesar dan bilangan bulat relatif prime untuk semua bilangan bulat a,b,c,d,r dan s adalah sebagai berikut :

(1). Andaikan a|b dan c|b dan (a,c) = d maka ac|bd

(2). Jika ac|b dan ad|b dan (c,d) = 1 maka acd|b

(3). Andaikan (a,b) = d maka untuk beberapa bilangan bulat x , d|x jika x adalah kombinasi linier dari a dan b

(4). Andaikan untuk setiap bilangan bulat x,x|a dan x|b jika x|c maka (a,b)=c

(5). Untuk semua n > 0 , jika (a,b) = 1 maka $(a,b^n) = 1$

(6). Andaikan (a,b) = 1 dan c|ab maka terdapat bilangan bulat r dan s sedemikian hingga c = rs , r|a, s|b dan (r,s) = 1

2.3 POLINOMIAL

Polinomial yang terdiri dari bilangan - bilangan

rasional pada koefisien - koefisiennya disebut polinomial atas φ, dengan φ menyatakan field dari bilangan - bilangan rasional. Kumpulan dari polinomial - polinomial dengan variabel x ini dinotasikan sebagai φ [x]. Jadi φ[x] didefinisikan sebagai :

$\varphi[x] = \{f(x) \mid f(x)=a_o x^n + a_1 x^{n-1} + \ldots + a_n , a_o , a_1, \ldots, a_n \in \varphi, \varphi$ = himpunan bilangan rasional $\}$.

Demikian pula polinomial dengan koefisien bilangan bulat dinotasikan sebagai Z[x], dengan Z[x] didefinisikan sebagai :

$Z[x] = \{f(x) \mid f(x)=a_o x^n + a_1 x^{n-1} + \ldots + a_n , a_o , a_1, \ldots, a_n \in Z$, Z = himpunan bilangan bulat rasional $\}$.

Didalam polinomial berikut $f(x)=a_o x^n + a_1 x^{n-1} + \ldots + a_n , a_o \neq 0$. Bilangan bulat non negatif n disebut derajad dari polinomial itu dan a_o disebut koefisien utama. Polinomial f(x) disebut dapat dibagi dengan g(x) yang tidak nol, jika terdapat polinomial g(x) sedemikian hingga f(x) = g(x) dan dituliskan sebagai g(x)|f(x). Sehingga g(x) disebut sebagai pembagi atau faktor dari f(x).

Teorema 2.7

Terdapat polinomial f(x) dan g(x) atas φ dengan g(x) $\neq$ 0, sehingga terdapat korespondensi polinomial q(x) dan r(x) sedemikian hingga f(x) = g(x)q(x) + r(x) dengan r(x) = 0 atau r(x) berderajad lebih rendah dari pada g(x).

Bukti :

dalam kasus $f(x) = 0$ atau $f(x)$ berderajad lebih rendah dari pada $g(x)$, didefinisikan $g(x) = 0$ dan $r(x) = f(x)$.Sebaliknya bila dilakukan pembagian dengan $g(x)$ terhadap $f(x)$ menghasilkan quotient $q(x)$ dengan sisa $r(x)$. Jelas bahwa $g(x)$ dan $r(x)$ polinomial atas φ, dan $r(x) = 0$ atau derajad $r(x)$ lebih kecil daripada derajad dari $g(x)$ jika sifat pembagian berlaku. Jika terdapat pasangan $q_1(x)$ dan $r_1(x)$ maka akan berlaku :

$f(x) = g(x)q_1(x) + r_1(x)$

$r(x) - r_1(x) = g(x) \{q_1(x) - q(x)\}$

Jadi $g(x)$ akan merupakan pembagi dari polinomial $r(x) - r_1(x)$ kecuali kalau sama dengan nol, mempunyai derajad yang lebih rendah dari pada $g(x)$. Dari sini $r(x) - r_1(x) = 0$ dan berakibat $q(x) = q_1(x)$.

Teorema 2.8

Terdapat polinomial $f(x)$ dan $g(x)$, yang keduanya tidak sama dengan nol yang mempunyai pembagi $h(x)$ ynag merupakan kombinasi linear dari $f(x)$ dan $g(x)$. Jadi terdapat hubungan $h(x) | f(x)$, $h(x) | g(x)$ dan

$$h(x) = f(x)F(x) + g(x)G(x) \qquad (2.5)$$

Bukti :

Dari semua polinomial persamaan (2.5) yang tidak nol dipilih satu yang derajadnya terkecil dan menandainya dengan $h(x)$. Jika bukan pembagi dari $f(x)$, menurut teorema

2.7 akan memberikan persamaan $f(x)=h(x)q(x)+r(x)$ dengan $r(x)$ tidak sama dengan nol dan $r(x)$ mempunyai derajad yang lebih rendah daripada $h(x)$. Tetapi $r(x)=f(x)-h(x)q(x)=f(x)\{1-F(x)q(x)\}-g(x)\{G(x)q(x)\}$. Yang dari persamaan 2.5 akan kontradiksi pada pilihan $h(x)$, jadi $h(x)|f(x)$ dan dengan cara yang sama $h(x)|g(x)$.

Definisi 2.5

Apabila diketahui dua polinomial yaitu $f(x)$ dan $g(x)$, maka apabila $f(x)$ dan $g(x)$ dapat difaktorkan atas faktor-faktor dengan koefisien bilangan bulat maka faktor yang merupakan pembagi persekutuan terbesar tersebut disebut polinomial monic *d(x)*. Dan ditulis sebagai :
$(f(x),g(x))=d(x)$.

Contoh :

$f(x)=x^2+6x-7=(x+7)(x-1)$

$g(x)=x^3+7x^2-x-7=(x^2-1)(x+7)$

$d(x)=x+7$

Teorema 2.9

Terdapat polinomial $f(x)$ dan $g(x)$, keduanya tidak nol maka terdapat korespondensi dengan polinomial monic $d(x)$ yang mempunyai sifat-sifat :

(1) $d(x)|f(x)$, $d(x)|g(x)$.

(2) $d(x)$ adalah kombinasi linear dari $f(x)$ dan $g(x)$ seperti dalam persamaan (2.5).

(3) Setiap pembagi persekutuan dari f(x) dan g(x) adalah pembagi dari d(x), jadi tidak ada pembagi persekutuan lain yang mempunyai derajad yang lebih tinggi daripada d(x).

Bukti :

Didefinisikan $d(x)=c^{-1}h(x)$, dengan c adalah koefisien utama dari h(x), sehingga d(x) adalah monic. Sifat-sifat (1) dan (2) diturunkan dari h(x) dan d(x). Persamaan (2.5) menyatakan bahwa $d(x)=c^{-1}f(x)F(x)+c^{-1}g(x)G(x)$ dan persamaan ini menunjukkan bahwa jika m(x) adalah pembagi pada f(x) dan g(x) maka $m(x)|d(x)$. Akhirnya terbukti bahwa d(x) adalah tunggal, diandaikan bahwa d(x) dan $d_1(x)$ keduanya mempunyai sifat-sifat (1),(2) dan (3). Maka terdapat $d(x)|d_1(x)$ dan $d_1(x)|d(x)$, jadi $d_1(x)=q(x)d(x)$ dan terdapat $d(x)=q_1(x)d_1(x)$ untuk polinomial-polinomial q(x) dan $q_1(x)$. Ini menyatakan $q(x)q_1(x)=1$, dari yang diketahui bahwa $q(x)q_1(x)$ berderajad nol. Sehingga d(x) dan $d_1(x)$ adalah monic, maka didapatkan q(x)=1, $d_1(x)=d(x)$.

Contoh :

$f(x)=x^2+6x+5=(x+1)(x+5)$

$g(x)=x^2+4x+3=(x+1)(x+3)$

$d(x)=x+1$

$x+1=\frac{1}{2}\ f(x)\ -\ \frac{1}{2}\ g(x).$

Definisi 2.6

Polinomial f(x) tidak sama dengan nol adalah irreducible atau prime atas φ, jika tidak terdapat faktor-faktor g(x) dan h(x) dari f(x) yang berderajad positis atas φ.

Contoh :

x^2-2 adalah irreducible atas φ. Polinomial tersebut mempunyai faktor-faktor $(x-\sqrt{2}),(x+\sqrt{2})$ atas bilangan real, tetapi tidak mempunyai faktor atas φ.

Teorema 2.10

Jika polinomial irreducible p(x) membagi hasil kali f(x) dan g(x), maka p(x) membagi pada sedikit-dikitnya satu dari polinomial f(x) dan g(x) atau :

$p(x)|f(x)g(x) \Rightarrow p(x)|f(x)$ atau $p(x)|g(x)$

Bukti :

Diandaikan $p(x)=f(x)g(x)$ dengan $p(x)\nmid f(x)$ dan $p(x)\nmid g(x)$. Maka ini berarti $(p(x),f(x))=1$ dan $(p(x),g(x))=1$. Apabila dilakukan operasi pergandaan antara f(x) dengan g(x) maka seharusnya $(p(x),f(x)g(x))=1$ tetapi ini tidak mungkin karena $f(x)g(x)=p(x)$ sehingga :

$(p(x),f(x)g(x))=(p(x),p(x))=p(x)$ maka yang benar adalah $p(x)|f(x)$ atau $p(x)|g(x)$.

Teorema 2.11

Polinomial atas φ berderajad positif dapat difaktorkan atas hasil kali $f(x)=cp_1(x)p_2(x)p_3(x)...p_k(x)$ dengan $p_j(x)$ irreducible polinomial monic atas φ. Dengan faktor-faktornya adalah tunggal atas φ.

Bukti :

f(x) dapat difaktorkan secara berulang-ulang sampai menjadi hasil kali dari polinomial irreducible dan c konstan dapat disesuaikan untuk membuat semua faktor monic. Sekarang harus dibuktikan ketunggalannya. Dinyatakan faktor-faktor yang lain, $f(x)=cq_1(x)q_2(x)q_3(x)...q_j(x)$ dalam irreducible polinomial monic. Menurut teorema 2.10, $p_1(x)$ membagi beberapa $q_i(x)$ dan dapat membagi q(x) yang membuat $p_1(x)|q_1(x)$. Dengan $p_1(x)$ dan $q_1(x)$ adalah irreducible dan monic, diperoleh bahwa $p_1(x)=q_1(x)$. Dengan pengulangan yang sama maka didapatkan hasil $p_2(x)=q_2(x), p_3(x)=q_3(x),...,k=j$. Jadi terbukti bahwa faktor-faktornya adalah tunggal atas φ.

Definisi 2.7

Polinomial $f(x)=a_0x^n+a_1x^{n-1}+...+a_n$ dengan koefisien bilangan bulat a_j disebut primitif jika pembagi

persekutuan dari setiap koefisiennya sama dengan satu.

Teorema 2.12

Hasil kali dari dua polinomial primitif adalah primitif.

Bukti :

Pandang $a_0x^n+a_1x^{n-1}+\ldots+a_n$ dan $b_0x^n+b_1x^{n-1}+\ldots+b_m$ adalah polinomial primitif dan dinyatakan bahwa hasil kali polinomial ini adalah tidak primitif. Maka terdapat prime p yang membagi setiap koefisien c_k dengan k=0,1,2,...,m+n. Dengan $a_0x^n+a_1x^{n-1}+\ldots+a_n$ adalah primitif, sedikit-dikitnya satu koefisien tidak dapat dibagi dengan p. Sehingga terdapat hubungan bahwa p=prime $p|c_k$, $p\nmid a_i$, $p\nmid b_j$ akibatnya $c_k\equiv 0 \pmod p$, $a_i\not\equiv 0 \pmod p$, $b_j\not\equiv 0 \pmod p$, k=0,1,2,...,m+n, $0\le i\le n$, $0\le j\le m$. Tetapi ini tidak mungkin, karena hasil perkalian antara a_i dengan b_j termuat dalam c_k, misal c_{i+j}. Sehingga :

$p\nmid a_i \Rightarrow a_i\not\equiv 0 \pmod p$

$p\nmid b_j \Rightarrow b_j\not\equiv 0 \pmod p$

$a_ib_j=c_{i+j}$, $c_{i+j}\in c_k$

$a_ib_j\equiv c_{i+j}\not\equiv 0 \pmod p$ berarti ada $c_k\not\equiv 0 \pmod p$ atau $p\nmid c_k$.

Jadi $c_0x^{m+n}+c_1x^{m+n-1}+\ldots+c_{m+n}$ adalah polinomial primitif.

Teorema 2.13

Jika polinomial monic f(x) dapat difaktorkan menjadi dua polinomial monic dengan koefisien rasional, dinyatakan f(x)=g(x)h(x) maka g(x)h(x) mempunyai koefisien bilangan bulat.

Bukti :

Diambil c sebagai bilangan bulat positif terkecil sedemikian hingga cg(x) mempunyai koefisien bilangan bulat. Jika g(x) mempunyai koefisien bilangan bulat maka c=1. Jadi cg(x) adalah polinomial primitif, karena jika p adalah pembagi koefisien, maka p|c dan (c/p)g(x) mempunyai koefisien bilangan bulat. Hal ini berlawanan dengan sifat minimal dari c.

Dengan cara yang sama diambil c_1 sebagai bilangan bulat positif terkecil sedemikisn hingga $c_1h(x)$ mempunyai koefisien bilangan bulat, dari sini $c_1h(x)$ adalah juga primitif. Maka dengan menggunakan teorema 2.11 hasilkali dari $\{cq(x)\}\{c_1h(x)\}=cc_1f(x)$ adalah juga primitif. Tetapi dengan f(x) mempunyai koefisien bilangan bulat, sehingga g(x) dan h(x) juga mempunyai koefisien bilangan bulat.

2.4 TEORI BILANGAN DILIHAT DARI SUDUT PANDANG SECARA ALJABAR

Definisi 2.8

Sebauh grup G adalah himpunan yang terdiri atas elemen-elemen yang tidak didefinisikan (undefined elements) beserta suatu hukum komposisi, yang dapat disajikan dengan tanda penjumlahan (+) yang memenuhi aksioma-aksioma berikut :

(1) tertutup pada G, yaitu $(\forall a,b \in G)\ a+b \in G$.

(2) memenuhi hukum assosiatif $(\forall a,b,c \in G)$ berlaku :

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

(3) himpunan ini mempunyai elemen identitas

$(\exists e \in G)\ (\forall a \in G)\ e+a=a+e=a$

(4) tiap elemen dalam G mempunyai invers juga dalam G.

$(\forall a \in G)\ (\exists (-a) \in G)\ a+(-a)=(-a)+(a)=e$.

Contoh lain yang termasuk grup mengingat kongruensi modulo m. Misal dalam kasus m=6 diberikan contoh nyata dengan kongruensi sederhana berikut :

$3+4 \equiv 1 \pmod 6$ adalah tertutup.

$(2+5)+4 \equiv 2+(5+4) \equiv 5 \pmod 6$ adalah assosiatif.

$3+0 \equiv 0+3 \equiv 3 \pmod 6$ elemen identitasnya adalah $0 \pmod 6$

$4+(-4) \equiv (-4)+4 \equiv 0 \pmod 6$ sehingga elemen invers dari $a \pmod m$ adalah $-a \pmod m$.

dengan sistem residu lengkapnya 0,1,2,3,4,5.

Jalan lain untuk memikirkan dari penjumlahan grup modulo 6 dalam hubungannya dengan klas residu. Diambil dua bilangan bulat a dan b dalam klas residu yang sama modulo 6 jika $a \equiv b \pmod 6$, dan hasil pemisahan semua bilangan bulat dimasukkan kedalam 6 klas residu :

C_0:...,-18,-12,-6,0,6,12,18,...

C_1:...,-17,-11,-5,1,7,13,19,...

C_2:...,-16,-10,-4,2,8,14,20,...

C_3:...,-15,-9,-3,3,9,15,21,...

C_4:...,-14,-8,-2,4,10,16,22,...

C_5:...,-13,-7,-1,5,11,17,23,...

jika elemen-elemen dalam klas C_2 dijumlah dengan elemen-elemen dalam klas C_3 jumlahnya adalah elemen dalam klas C_5, maka dapat ditulis $C_2+C_3=C_5$. Sehingga untuk yang lain $C_3+C_4=C_1$, $C_3+C_5=C_2$ dan seterusnya.

Teorema 2.14

Bentuk sistem residu lengkap modulo m dari grup penjumlahan 2 sistem residu lengkap modulo m menyatakan grup isomorphis terhadap penjumlahan dan disebut grup penjumlahan modulo m

Bukti :

Diambil sistem residu lengkap 0,1,2,3,...,m-1 modulo m, sistem tertutup terhadap penjumlahan modulo m dan sifat assosiatif pada penjumlahan diturunkan dari sifat korespondensi untuk semua bilangan bulat, bahwa a + (b+c) = (a+b)+c yang menyatakan a+(b+c)≡(a+b)+c(mod m). Elemen identitasnya adalah nol. Akhirnya invers pada penjumlahan dari 0 adalah 0(mod m) dan invers penjumlahan dari elemen a adalah m-a.

2.5 GRUP CYCLIC

Definisi 2.9

Apabila suatu sistem itu terdiri atas satu elemen saja, maka elemen yang dihasilkan olehnya disebut grup cyclic dengan notasi [a]. Ada 2 macam grup cyclic yaitu berhingga dan tak berhingga.

Contoh :

Grup cyclic [e].

Teorema 2.15

Grup cyclic [a] yang dihasilkan oleh a adalah tak berhingga jika dan hanya jika $a^p=a^q \Rightarrow p=q$ yaitu jika dan hanya jika a^p sama dengan a^q hanya jika p sama dengan q

Bukti :

Bukti pertama $a^p=a^q \Rightarrow p=q \Rightarrow$ [a] tak berhingga.

Memang jika diketahui bahwa $a^p=a^q$ berlaku hanya jika $p=q$, ini berarti bahwa semua anggota dari :

$\ldots,a^{-3},a^{-2},a^{-1},a^0,a^1,a^2,a^3,\ldots$adalah berlainan. Sehingga [a] tak berhingga.

Bukti kedua [a] tak berhingga $\Rightarrow a^p=a^q \Rightarrow p=q$

Dibuktikan kontraposisinya. Diandaikan bahwa $a^p=a^q$ dengan $p\neq q$. Lalu dibuktikan [a] berhingga.

Apabila $a^p=a^q$ dengan pemisalan $p>q$, maka dari satu pihak $a^p.a^{-q}=a^q.a^{-q}=a^0=e$.

Pada lain pihak $a^p.a^{-q}=a^{q-q}$ sehingga $a^{q-q}=e$. Misal a adalah bilangan bulat positif terkecil, dengan sifat bahwa $a^n=e$. Pandang $a^0,a^1,a^2,a^3,\ldots,a^{n-1}$.

Pertama-tama akan diperlihatkan bahwa n elemen diatas semuanya berlainan. Sebab andaikan $a^s=a^r$ dengan $0\leq r<s<n$. Maka karena $a^s=a^r$ dengan menggandakan dengan a^{-r} akan didapatkan bahwa :

$a^{s-r}=a^{r-r}=a^0=e$ sehingga $s-r<n$. Ini bertentangan dengan pengandaian bahwa n adalah bilangan bulat positif terkecil sedemikian hingga $a^n=e$. Selanjutnya setiap bilangan bulat m dapat ditulis dalam bentuk $m=kn+l$ dengan $0\leq l<n$. Maka :

$a^m=a^{kn+l}=a^{kn}.a^l=(a^n)^k.a^l=e.a^l=a^l$ sehingga setiap exponen dapat direduksi menjadi satu diantara $0,1,\ldots,n-1$. Dengan

demikian terbukti bahwa [a] adalah berhingga dan terdiri atas n elemen. Untuk grup cyclic atas n elemen, berlaku $e=a^n=a^{2n}$ dan seterusnya. Semua grup cyclic adalah abelian sebab :

$a^m.a^n=a^{m+n}=a^{n+m}=a^m.a^n$

2.6 PERGANDAAN GRUP, RING DAN FIELD

Teorema 2.16

Diambil $m>1$ sebagai bilangan bulat positif. Reduksi sistem residu modulo m adalah grup pergandaan modulo m. Grup ini berorde $\phi(m)$. Kedua grup disebut isomorphis dan disebut grup modulo m.

Bukti :

Dinyatakan reduksi sistem residu $r_1,r_2,r_3,\ldots,r_n$ dengan $n=\phi(m)$. Himpunan tertutup terhadap pergandaan modulo m. Sifat assosiatif pergandaan diturunkan dari sifat korespondensi pada bilangan bulat, karena $a(bc)=(ab)c$ menyatakan bahwa $a(bc)\equiv(ab)c \pmod m$. Reduksi sistem residu memuat satu elemen, disebut r_j, sedemikian hingga $r_j\equiv1 \pmod m$ dan ini jelas merupakan elemen identitas yang khas dari grup. Akhirnya untuk tiap r_i, kongruensi $xr_i\equiv r_j \pmod m$ mempunyai solusi dan solusi ini khas dalam reduksi sistem residu $r_1,r_2,r_3,\ldots,r_n$. Dua reduksi sistem residu modulo m yangberbeda adalah kongruen

elemen demi elemen modulo m dan didapatkan kedua grup adalah isomorphis.

Definisi 2.10

Diambil grup G finite atau infinite dan a elemen dari G. Jika $a^s=e$ untuk bilangan bulat positif s, maka a disebut berorde finite. Jika a berorde finite, orde dari a adalah bilangan bulat positif terkecil r sedemikian hingga $a^r=e$. Jika tiada bilangan bulat positif s sehingga $a^s=e$, maka a disebut berorde infinite. Grup G disebut cyclic jika memuat elemen a sedemikian hingga pangkat dari a,

$\ldots,a^{-3},a^{-2},a^{-1},a^0,a^1,a^2,a^3,\ldots$

terdiri dari keseluruhan elemen sehingga elemen a disebut penghasil grup dan disebut sebagai generator.

Jika grup cyclic adalah berhingga dan mempunyai generator a, maka grup ini terdiri dari $e,a,a^2,a^3,\ldots,a^{r-1}$ dengan r adalah orde dari elemen a.

Definisi 2.11

Ring adalah himpunan dengan sedikit-dikitnya dua operasi (+) dan (x) sedemikian hingga merupakan grup komutatif terhadap (+), tertutup terhadap pergandaan dan sedemikian hingga assosiatif terhadap (x) dan distributif terhadap operasi (+). Jika semua elemen dari ring selain zero maka ini adalah bentuk grup komutatif

terhadap (x) dan ini yang disebut field.

Teorema 2.17

Himpunan Z_m yang elemen-elemennya 0,1,2,...,m-1 dengan didefinisikan penjumlahan dan pergandaan modulo m, adalah ring untuk bilangan bulat m>1 sehingga ring ini adalah field jika dan hanya jika m adalah prime.

Bukti :

Telah dijelaskan bahwa sistem residu lengkap modulo m adalah grup penjumlahan modulo m. Grup ini adalah komutatif, assosiatif dan bersifat distributif terhadap pergandaan modulo m yang diturnkan dari sifat-sifat pada pergandaan biasa. Oleh karenanya Z_m adalah ring. Selanjutnya juga telah diketahui bahwa reduksi sistem residu modulo m adalah grup terhadap pergandaan modulo m. Jika m adalah prime, reduksi sistem residu dari Z_p adalah 1,2,...,p-1 maka semua elemen dari Z_p selain daripada nol. Karena 0 adalah zero dari ring, Z_p adalah field. Pada bagian lain jika m adalah bukan prime maka m adalah berbentuk ab dengan $0<a\leq b<m$. Kemudian elemen-elemen dari Z_m selain 0 bukan merupakan grup pergandaan modulo m karena tidak ada invers untuk elemen a, tidak ada solusi dari $ax\equiv b \pmod m$. Jadi Z_m bukan merupakan field.

2.7 PERGANDAAN GRUP MODULO M

Dalam teorema 2.17 telah ditetapkan bahwa untuk bilangan bulat m>1, himpunan bilangan bulat positif yang lebih kecil daripada m dan m prime adalah membentuk grup pergandaan modulo m.

Teorema 2.18

Jika m dan n adalah bilangan bulat relatif prime positif, maka G(mn) adalah isomorphis terhadap perkalian langsung G(m)xG(n). G(n) adalah grup dengan n elemen.

Bukti :

Jika r adalah beberapa elemen dalam G(m) dan jika s adalah beberapa elemen dalam G(n) maka terdapat bilangan bulat x modulo mn yang memenuhi kongruensi :

$x \equiv r \pmod m \quad x \equiv s \pmod n$ (2.10)

dari (r,m)=1 dan (s,n)=1 dapat dinyatakan bahwa (x,mn)=1, sehingga x adalah elemen dari G(mn), terdapat elemen satuan r dalam G(m) dan s dalam G(n) yang memenuhi kongruensi (2.10). Selanjutnya terdapat korespondensi 1-1 antara elemen x dalam G(mn) dan pasangan (r,s) dengan r dalam G(m) dan s dalam G(n).

Bukti secara lengkap harus membuktikan sifat dasar pada perkalian langsung grup bahwa jika x_1 dalam G(m)

berkorespondensi dengan pasangan (r_1,s_1) dan x_2 dengan pasangan (r_2,s_2) maka x_1x_2 berkorespondensi dengan (r_1r_2, s_1s_2) sehingga dapat diperoleh bahwa :

$x_1 \equiv r_1 \pmod m$ $\qquad$ $x_2 \equiv r_2 \pmod m$

$x_1 \equiv s_1 \pmod n$ $\qquad$ $x_2 \equiv s_2 \pmod n$

sehingga dapat dibuktikan bahwa :

$x_1x_2 \equiv r_1r_2 \pmod m$

$x_1x_2 \equiv s_1s_2 \pmod n$