BAB II

TEORI PENUNJANG

Dalam bab ini akan dibahas mengenai beberapa teori yang dapat menunjang materi pada bab III antara lain teori relasi dan fungsi, teori grup, Galois Field GFp dan teori matriks.

2.1. Relasi dan Fungsi

Definisi 2.1.1

Secara simbolis kalimat "a berada dalam relasi R dengan b" dapat disajikan dengan "a R b" atau "R(a,b)". Demikian juga "R(a,b,c)", "R(a,b,c,d)" dan seterusnya.

Definisi 2.1.2

Relasi R disebut refleksif jika dan hanya jika untuk setiap anggota dari semesta S berlaku a R a. Secara simbolis,

$$\text{R refleksif jika dan hanya jika } (\forall\, a \in \text{S})\,.\, a\,\text{R}\,a$$

Definisi 2.1.3

Relasi R disebut simetris jika dan hanya jika untuk setiap a, b dalam S berlaku jika a R b maka b R a. Secara simbolis,

$$\text{R simetris jika dan hanya jika } (\forall\, a, b \in \text{S})\,.\, a\,\text{R}\,b \Rightarrow b\,\text{R}\,a$$

Definisi 2.1.4

Relasi R disebut transitif jika dan hanya jika untuk setiap triple a, b, c dari semesta S, berlaku apabila a R b dan b R c maka a R c. Secara simbolis,

R transitif jika dan hanya jika $(\forall a, b, c \in S)$. a R b dan b R $c \Rightarrow a$ R c.

Definisi 2.1.5

Suatu relasi yang sekaligus mempunyai ketiga sifat refleksif, simetris dan transitif disebut relasi ekuivalensi.

Contoh 2.1.1

Relasi kesejajaran antara garis-garis lurus pada bidang datar adalah relasi ekuivalensi karena memenuhi ketiga sifat refleksif, simetris dan transitif.

Teorema 2.1.1

Suatu relasi ekuivalensi antara anggota-anggota dari suatu semesta S mengakibatkan adanya penggolongan (partisi) di dalam S.

Penggolongan di dalam S dimaksudkan bahwa S terbagi atas himpunan-himpunan bagian (golongan-golongan, kelas-kelas) masing-masing bukan himpunan kosong, yang saling asing sedemikian sehingga anggota dari S berada dalam salah satu (dan hanya satu) golongan dari S.

Bukti

Misalkan relasi diatas disebut R, maka R memiliki sifat-sifat refleksif, simetris dan transitif. Semua elemen-elemen yang berada dalam relasi R dengan a, dikumpulkan dalam suatu himpunan Sa. Jadi Sa = $\{ x \in S \mid x \text{ R } a \}$. Himpunan Sa tidak kosong, karena R refleksif, jadi a R a. Sehingga $a \in$ Sa dan Sa sekurang-

kurangnya mempunyai satu anggota. Dari sini disimpulkan bahwa setiap anggota pasti berada dalam sekurang-kurangnya satu kelas, yaitu kelas yang memuat dirinya sendiri.

Sekarang dibuktikan bahwa apabila dua golongan itu berserikat satu elemen saja maka kedua golongan itu berimpitan.....(1)

Andaikan Sa dan Sb berserikat elemen c. Karena $c \in$ Sa maka c R a. Karena R simetris, maka a R c. $c \in$ Sb maka c R b. Dari a R c dan c R b, dengan menggunakan sifat transitif maka a R b. Sehingga $a \in$ Sb. Selanjutnya, untuk setiap $p \in$ Sa berlaku p R a, dan karena a R b, dengan menggunakan sifat R transitif, maka p R b. Jadi, $p \in$ Sb. Maka terbukti, setiap anggota dari Sa mnjadi anggota dari Sb. Yaitu, Sa $\subseteq$ Sb.....(2)

Selanjutnya, karena $c \in$ Sb, maka c R b. Karena R simetris maka b R c. $c \in$ Sa maka c R a. Dari b R c dan c R a dengan menggunakan sifat transitif maka b R a sehingga $b \in$ Sa. Selanjutnya, untuk setiap $q \in$ Sb berlaku q R b, dan karena b R a, dengan menggunakan sifat R transitif, maka q R a. Jadi, $q \in$ Sa. Maka terbukti, setiap anggota dari Sb menjadi anggota dari Sa. Yaitu Sb $\subseteq$ Sa.....(3)

(2) dan (3) menghasilkan Sa = Sb. Dengan demikian kalimat (1) terbukti. Kontraposisi dari (1) adalah apabila kelas-kelas itu tidak berimpitan maka kedua kelas itu tidak berserikat satu elemen pun, jadi saling asing (disjoin).

Kelas-kelas atau golongan-golongan yang terbentuk karena relasi ekuivalensi disebut kelas-kelas atau golongan-golongan ekuivalensi atau equivalence classes.

Definisi 2.1.6

Misalkan g merupakan suatu integer positif. Sebarang dua integer a dan b (positif, negatif atau nol) dikatakan kongruen modulo g jika $a - b$ adalah kelipatan g ditulis

$a \equiv b \pmod{g}$ bila dan hanya bila $a - b = kg$ ($k = 0, \pm 1, \pm 2, \ldots$)

Sebaliknya, jika $a - b$ bukan kelipatan g maka a dan b dikatakan tidak kongruen modulo g dan ditulis $a \not\equiv b \pmod{g}$.

Contoh 2.1.2

$15 \equiv 1 \pmod{7}$, karena $15 - 1 = 14 = 2 \cdot 7$

$-3 \equiv 11 \pmod{7}$, karena $-3 - 11 = -14 = -2 \cdot 7$

$13 \not\equiv 2 \pmod{7}$, karena $13 - 2 = 11$, bukan kelipatan 7.

Teorema 2.1.2

Untuk setiap integer a dan g maka

$$a \equiv a \pmod{g}$$

Bukti

$a \equiv a \pmod{g}$ karena $a - a = 0 = 0 \cdot g$

Teorema 2.1.3

Jika $a \equiv b \pmod{g}$ maka $b \equiv a \pmod{g}$

Bukti

Karena $a - b = k \cdot g$ maka $b - a = -kg$ (suatu kelipatan (negatif) dari g juga). Sehingga $b \equiv a \pmod{g}$

Teorema 2.1.4

Jika $a \equiv b \pmod{g}$ dan $b \equiv c \pmod{g}$ maka

$$a \equiv c \pmod{g}$$

Bukti

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $b \equiv c \pmod{g}$ maka $b - c = k_2 g$, dengan k_1 dan k_2 adalah integer. Sehingga $a - c = (k_1 + k_2) g$ dan $a \equiv c \pmod{g}$.

Teorema 2.1.5

Jika $a \equiv b \pmod{g}$, $n > 0$, $g = k_2 n$ maka

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

Bukti

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $g = k_2 n$ maka

$$a - b = k_1 (k_2 n)$$

$$a - b = (k_1 \; k_2) n$$

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

Contoh 2.1.3

Jika $a = 15$, $b = 3$, $n = 2$, $g = 4 = 2n$ maka

$15 \equiv 3 \pmod{4}$ karena $15 - 3 = 12 = 3 \cdot 4$

$15 \equiv 3 \pmod{2}$ karena $15 - 3 = 12 = 6 \cdot 2$

Teorema 2.1.6

Jika $a \equiv b \pmod{g}$ dan $c \equiv d \pmod{g}$ maka $a + c \equiv b + d \pmod{g}$

Bukti

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $c \equiv d \pmod{g}$ maka

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

$$a + c \equiv b + d \pmod{g}$$

Berdasarkan teorema 2.1.2 , 2.1.3 dan 2.1.4, maka relasi kongruensi adalah suatu relasi ekuivalensi karena memenuhi sifat-sifat refleksif, simetris dan transitif. Sehingga berdasarkan teorema 2.1.1, maka himpunan integer dapat dibagi kedalam kelas-kelas ekuivalensi yang saling asing sedemikian sehingga sebarang dua integer yang ada dalam satu kelas yang sama adalah kongruen satu sama lain. Kelas tempat integer a berada dinotasikan dengan $(\bar{a})$ atau a. Jadi, jika a dan b ada dalam satu kelas yang sama maka $(\bar{a}) = (\bar{b})$.

Contoh 2.1.4

Jika $g = 7$, maka

$$(\bar{15}) = (\bar{1}) \text{ karena } 15 \equiv 1 \pmod{7}$$

$$(\bar{-3}) = (\bar{11}) \text{ karena } -3 \equiv 11 \pmod{7}$$

Diberikan suatu integer a, dengan mengaplikasikan algoritma pembagian maka dapat dinyatakan

$$a = a_1 + k g \text{ untuk } 0 \le a_1 < g$$

dengan k integer. a_1 disebut standar representative dari kelas $(\bar{a})$ dan $(\bar{a}) = (\bar{a_1})$

Contoh 2.1.5

Untuk $g = 7$, $15 = 1 + 2 \cdot 7$ maka 1 adalah standar representative dari kelas (15) dan (15) = (1).

Karena terdapat g integer-integer yang memenuhi $0 \leq a_1 < g$, maka terdapat tepat g kelas-kelas yang berbeda (mod g). Kelas-kelas tersebut disebut sebagai kelas-kelas residu (mod g). g kelas-kelas yang berbeda tersebut antara lain :

$$(0), (1), (2), \ldots, (g-1)$$

Contoh 2.1.6

Misal $g = 7$, maka

$0 = 0 + 0 \cdot 7$ $\quad$ $7 = 0 + 1 \cdot 7 \longrightarrow (7) = (0)$

$1 = 1 + 0 \cdot 7$ $\quad$ $8 = 1 + 1 \cdot 7 \longrightarrow (8) = (1)$

$2 = 2 + 0 \cdot 7$ $\quad$ $9 = 2 + 1 \cdot 7 \longrightarrow (9) = (2)$

$3 = 3 + 0 \cdot 7$

$4 = 4 + 0 \cdot 7$

$5 = 5 + 0 \cdot 7$

$6 = 6 + 0 \cdot 7$

Jadi, kelas-kelas residu yang terbentuk adalah (0), (1), (2),(3), (4), (5), (6)

Andaikan diberikan sistem yang terdiri atas kelas-kelas residu modulo g. Maka didefinisikan operasi-operasi penjumlahan dan perkalian dalam sistem ini dengan aturan :

$$(a)+(b)=(a+b)\,(\mathrm{mod}\,g)$$

$$(a).(b)=(a.b)\,(\mathrm{mod}\,g)$$

Contoh 2.1.7

Jika $g = 7$, maka

$$(5)+(6)=(5+6)\,(\mathrm{mod}\,7)=(11)\,(\mathrm{mod}\,7)=(4)$$

$$(5).(6)=(5.6)\,(\mathrm{mod}\,7)=(30)\,(\mathrm{mod}\,7)=(2)$$

Definisi 2.1.7

Suatu fungsi / pemetaan / mapping dari suatu himpunan S ke himpunan T (atau S sebagai daerah sumber / domain dan T sebagai daerah kawan / co-domain) adalah suatu aturan yang pada setiap anggota dari S menentukan dengan tunggal satu anggota dalam T.

Setiap fungsi dari S ke T disebut juga fungsi dari S *into* T. Jika elemen-elemen dari T juga dihabiskan, jadi jika setiap t dalam T mempunyai kawan di dalam S, atau dengan kata lain jika setiap t dalam T berasal dari suatu s dalam S, maka fungsi itu disebut fungsi dari S *onto* T. Sehingga setiap fungsi yang *onto* adalah fungsi *into*, tetapi belum tentu sebaliknya.

Untuk suatu fungsi yang onto berlaku $f(S) = T$. Yaitu daerah hasil berimpitan dengan daerah kawannya. Pemetaan yang onto disebut juga *surjektif*. Jika elemen-elemen dari T yang mempunyai kawan dalam S, hanya mempunyai kawan 1, maka pemetaannya disebut *injektif*. Dan jika setiap elemen dari S menentukan dengan tunggal satu elemen dari T dan sebaliknya, maka pemetaannya disebut *bijektif*. Dapat dikatakan juga bahwa pada fungsi bijektif,

terdapat korespondensi satu-satu bertimbal balik antara elemen-elemen dari S dengan elemen-elemen dari T.

2.2. Teori Grup

2.2.1. Grup

Definisi 2.2.1.1

Operasi biner $*$ pada himpunan A adalah suatu aturan yang menentukan suatu elemen c dalam A untuk setiap pasangan terurut (a, b) dari elemen-elemen dalam A, atau ditulis dengan $a * b = c, \forall a, b, c \in A$.

Operasi biner * pada himpunan A dikatakan :

1. komutatif jika $a * b = b * a, \forall a, b \in A$
2. assosiatif jika $(a * b) * c = a * (b * c), \forall a, b, c \in A$.

Definisi 2.2.1.2

Misalkan * merupakan operasi biner pada A dan $c \in A$ maka :

1. e disebut elemen identitas kanan untuk * jika $a * e = a, \forall a \in A$
2. e disebut elemen identitas kiri untuk * jika $e * a = a, \forall a \in A$
3. e disebut elemen identitas dua sisi untuk * jika $a * e = e * a = a, \forall a \in A$

Jika e merupakan elemen identitas dua sisi maka cukup disebut elemen identitas.

Definisi 2.2.1.3

Misalkan * merupakan operasi biner pada A dan e adalah elemen identitas untuk * dan $a, b \in A$

1. Jika $b * a = e$, maka b disebut invers kiri dari a terhadap * dan e

2. Jika $a * b = e$, maka b disebut invers kanan dari a terhadap * dan e

3. Jika $a * b = b * a = e$, maka b disebut invers dua sisi dari a terhadap * dan e

Jika b merupakan invers dua sisi dari a maka cukup disebut b invers dari a. Invers dari a dapat juga dinotasikan dengan a^{-1}.

Definisi 2.2.1.4

Suatu grup (G, *) adalah suatu himpunan G, dibawah suatu operasi biner *, sedemikian sehingga aksioma-aksioma berikut dipenuhi

A1. Operasi biner * assosiatif

A2. Terdapat elemen identitas $e \in G$ terhadap *

A3. Setiap elemen $a \in G$ mempunyai invers $a^{-1} \in G$ terhadap e dan *.

Suatu grup (G, *) dapat juga hanya ditulis dengan G.

Contoh 2.2.1.1

Misalkan G = { a , b, c } dengan operasi biner * sebagai berikut

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Maka (G, *) adalah sebuah grup, karena ketiga aksioma grup terpenuhi, yaitu :

A1. Operasi biner * assosiatif :

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

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

A2. Terdapat elemen identitas yaitu a

A3. Setiap elemen dalam G mempunyai invers, yaitu $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$.

Definisi 2.2.1.5

Suatu grup (G, *) adalah abelian jika operasi biner * bersifat komutatif, yaitu $a * b = b * a, \forall a, b \in G$.

2.2.2. Subgrup

Definisi 2.2.2.1

Jika suatu himpunan bagian H dari suatu grup G tertutup dibawah operasi biner pada G dan jika H juga merupakan suatu grup, maka H adalah subgrup dari G, dinotasikan dengan $H < G$ atau $G > H$.

Contoh 2.2.2.1

(**R**, +) adalah suatu grup, $Z \subset \mathbf{R}$ dan (Z, +) adalah grup. Maka (Z, +) adalah subgrup dari (**R**, +).

2.3. Galois Field GF*p*

Definisi 2.3.1

Field F adalah suatu struktur aljabar yang memenuhi aksioma-aksioma di bawah ini.

I. F merupakan grup abelian terhadap operasi penjumlahan, yaitu

1. Untuk semua a, b dalam F dapat ditemukan dengan tunggal elemen c dalam F juga, sedemikian sehingga $a + b = c$.
2. Untuk semua a, b, c dalam F berlaku $(a + b) + c = a + (b + c)$
3. Didalam F terdapat elemen 0 sedemikian sehingga untuk setiap a dalam F berlaku $0 + a = a + 0 = a$

4. Untuk setiap a dalam F dapat ditemukan elemen $-a$ sedemikian sehingga $-a + a = a + (-a) = 0$
5. Untuk setiap a, b dalam F berlaku $a + b = b + a$

II. Pergandaan mempunyai sifat-sifat tertutup dan assosiatif, yaitu

1. Untuk semua a, b dalam F dapat ditemukan dengan tunggal elemen c dalam F juga, sedemikian sehingga $ab = c$
2. Untuk semua a, b dalam F berlaku $(ab)\,c = a\,(bc)$
3. Adanya elemen e dalam F sedemikian sehingga $ae = ea = a$ untuk setiap a dalam F
4. Untuk setiap a, b dalam F berlaku $ab = ba$
5. Setiap a dalam F yang tidak sama dengan nol mempunyai invers a^{-1} dalam F yaitu $a^{-1}a = a\,a^{-1} = e$.

III. Kedua aturan komposisi di atas dihubungkan dengan aksioma distributivitas

1. Untuk semua a, b, c dalam F berlaku $a(b + c) = ab + ac$ dan $(b + c)\,a = ba + ca$.

Jadi F merupakan suatu field jika F adalah grup abelian terhadap operasi penjumlahan dan F-{0} adalah grup abelian terhadap operasi perkalian.

Contoh 2.3.1

Jika F adalah himpunan dari integer-integer modulo 7 dibawah operasi penjumlahan dan perkalian mod 7. Elemen-elemen dari F adalah 7 simbol $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$, $\bar{5}$, $\bar{6}$. Maka

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

F merupakan grup abelian terhadap penjumlahan dan F - { $\bar{0}$ } merupakan grup abelian terhadap perkalian. Jadi F merupakan suatu field. Karena elemen-elemennya hanya terdiri atas bilangan-bilangan terbatas maka disebut finite field.

Definisi 2.3.2

Suatu finite field yang terdiri atas p kelas-kelas residu (mod p) dengan p adalah bilangan prima disebut Galois Field berorde p dan dinotasikan dengan GFp.

Untuk menyederhanakan penulisan maka untuk selanjutnya elemen-elemen dari suatu Galois Field GFp akan dituliskan sebagai { 0, 1, 2, ..., p-1 }.

Dalam GFp terdapat suatu elemen yang disebut sebagai primitive root dari GFp.

Definisi 2.4.3

Suatu integer x disebut sebagai primitive root dari GFp jika x merupakan elemen dari GFp sedemikian sehingga semua hasil pangkat dari x yang kurang dari (p - 1) modulo p adalah semua elemen dalam GFp kecuali elemen nol yang berbeda satu sama lain dan $x^{p-1} \equiv 1 \pmod{p}$.

Contoh 2.3.2

Untuk $p = 5$, GFp mempunyai elemen-elemen { 0, 1, 2, 3, 4 }. Elemen-elemen 2 dan 3 adalah primitive root dari GF_5 karena hasil pangkat dari 2 dan 3 modulo 5 adalah semua elemen dari GF_5.

$2^0 = 1$ $\quad$ $3^0 = 1$

$2^1 = 2$ $\quad$ $3^1 = 3$

$2^2 = 4$ $\quad$ $3^2 = 4$

$2^3 = 3$ $\quad$ $3^3 = 2$

$2^4 = 1$ $\quad$ $3^4 = 1$

Berikut diberikan sebuah tabel dari primitive-primitive root untuk beberapa nilai dari p.

p	Primitive Root
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5

Untuk lebih mempermudah penentuan primitive root dari suatu GFp, terutama untuk GFp dengan nilai p besar, berikut diberikan Algoritma Program dan Program Mencari Primitive Root Dari Suatu Galois Field GFp dengan menggunakan bahasa pemrograman Turbo Pascal 7.0.

ALGORITMA PROGRAM Primitive_Root

```
[ 1 ]  Repeat
         Read ( p )
         Until p Prime
[ 2 ]  HimpA := [ 1..p-1 ] ;
[ 3 ]  For x := 2 to p-1 do
           Begin
             Rk := 1 ;
             HimpB := [ ] ;
             For j := 1 to p-1 do
                 Begin
                   Rj := ( x * Rk ) mod p ;
                   HimpB := HimpB + [ Rj ] ;
                   Rk := Rj ;
                 end ;
             If HimpB = HimpA then
                 Writeln ( ' x adalah Primitive Root ' ) ;
             Else
                  Writeln ( ' x bukan Primitive Root ' ) ;
           end.
```

```
PROGRAM Primitive_Root ;
(*-------------------------------------------------------------------------*)
(*                  Program Mencari Primitive Root                         *)
(*                  dari suatu Galois Field GFp                            *)
(*-------------------------------------------------------------------------*)
USES crt ;
LABEL
     Akhir ;
TYPE
     Digit  =  1..255 ;
     HimpDigit  =  SET OF Digit ;
VAR
      HimpA, HimpB  :  HimpDigit ;
      x , j , p          :  Byte ;
      Rj , Rk            :  Byte ;
      YN , N             :  Char ;

Function Prime ( p : Byte ) : Boolean ;
VAR
     I : Byte ;
Begin   { Function Prime }
     If p = 1 then
       Prime := False
     Else If p = 2 then
       Prime := True
     Else
       Begin
           Prime := True ;
           For I := 2 to p-1 do
               If ( p mod I = 0 ) then
                   Prime := False
        end
end ;   { Function Prime }

Begin   { PROGRAM Primitive_Root }
     Clrscr ;
     Textcolor (5) ;
     Textbackground (0) ;
     Window (10, 1, 80, 25) ;
     Writeln ( ' *=========================================* ' ) ;
     Writeln ( ' *          Primitive Root dari GFp        * ' ) ;
     Writeln ( ' *=========================================* ' ) ;
     Writeln ;
     Textcolor (4) ;
```

```
Repeat
    Write   ( ' Masukkan Nilai p ( p harus bilangan prima ) : ' ) ;
    Readln  ( p ) ;
Until Prime ( p ) ;

HimpA := [ 1..p-1 ] ;
Writeln ;

For x := 2 to p-1 do

  Begin { For x }
     Writeln ;
     Writeln ( ' Nilai x = ', x ) ;
     Rk := 1 ;
     HimpB := [ ] ;

     For j := 1 to p-1 do

        Begin { For j }
           Rj := ( x * Rk ) mod p ;
           HimpB := HimpB + [ Rj ] ;
           Rk := Rj ;
           Writeln ( ' ', x ,' pangkat ', j ,' modulo ', p ,' adalah ',Rj ) ;
        end ; { For j }

     Writeln ;
     Writeln ;

     Begin { Jawaban }
          Textcolor (2) ;
          If HimpB = HimpA then
             Writeln ( ' x = ', x ,' adalah Primitive Root dari GFp' )
          Else
             Writeln ( ' x = ', x ,' bukan Primitive Root dari GFp' ) ;
          Readln ;
     end ; { Jawaban }

     Textcolor (4) ;
     Write ( ' Mau Cari Primitive Root yang lain ( Y/N ) ? ' ) ;
     Readln (YN) ;
     Writeln ;
     If ( YN = 'N' ) or ( YN = 'n' ) then
        goto Akhir ;

end ; { For x }
```

```
        Textcolor (3) ;
        Writeln ( ' Elemen dalam GFp sudah habis !!! ' ) ;
        Readln ;

        Akhir :

        Textcolor (6+Blink) ;
        Begin { LABEL Akhir }
            Writeln ( ' Sudah dicatat semua Primitive Root-nya ? ' ) ;
            Readln ;
            Readln ;
        end ; { LABEL Akhir }

end. { PROGRAM Primitive_Root }
```

2.4. Teori Matriks

2.4.1. Definisi Umum

Definisi 2.4.1

Matriks adalah himpunan skalar (bilangan riil atau kompleks) yang disusun secara empat persegi panjang (menurut baris-baris dan kolom-kolom). Skalar-skalar itu disebut elemen matriks. Dan untuk batasnya diberikan

$$\begin{bmatrix} \quad \end{bmatrix} \text{ atau } \begin{pmatrix} \quad \end{pmatrix} \text{ atau } \begin{Vmatrix} \quad \end{Vmatrix}$$

Matriks diberi nama dengan huruf besar. Secara lengkap ditulis $A = (a_{ij})$, artinya suatu matriks A dengan elemen-elemennya a_{ij} dengan i menyatakan baris ke-i dan index j menyatakan kolom ke-j dari elemen tersebut.

Pandang suatu matriks $A = (a_{ij})$, $i = 1, 2, \ldots, m$ dan $j = 1, 2, \ldots, n$, yang berarti bahwa banyaknya baris adalah m serta banyaknya kolom adalah n. Maka

dapat dituliskan matriks $A_{(m \times n)} = (a_{ij})$. (m x n) disebut ukuran (ordo) dari matriks.

Ada beberapa jenis matriks khusus, antara lain :

1. Matriks bujur sangkar berordo n adalah suatu matriks dengan banyaknya baris sama dengan banyaknya kolom yaitu n. Barisan elemen-elemen a_{11} , a_{22} , ..., a_{nn} disebut sebagai diagonal utama dari matriks bujur sangkar tersebut.
2. Matriks identitas adalah matriks bujur sangkar yang semua elemen di luar diagonal utamanya adalah nol dan elemen-elemen pada diagonal utamanya semua = 1. Matriks identitas biasa ditulis I atau I_n dengan n menyatakan ordo matriks tersebut.
3. Matriks segitiga atas adalah matriks bujur sangkar yang semua elemen dibawah diagonal utamanya adalah nol.
4. Matriks segitiga bawah adalah matriks bujur sangkar yang semua elemen diatas diagonal utamanya adalah nol.

2.4.2. Operasi-Operasi pada Matriks

2.4.2.1. Operasi Penjumlahan pada Matriks

Jika A = (a_{ij}) dan B = (b_{ij}) adalah matriks-matriks berordo sama maka suatu matriks C = (c_{ij}) dengan $c_{ij} = a_{ij} + b_{ij}$, untuk setiap i dan j.

Mengurangi matriks A dengan matriks B, yaitu A - B, adalah menjumlahkan matriks A dengan matriks - B.

2.4.2.2. Operasi Perkalian Skalar terhadap Matriks

Jika λ adalah suatu skalar dan $A = (a_{ij})$ maka matriks $\lambda A = (\lambda a_{ij})$, dengan kata lain, matriks λA diperoleh dengan mengalikan semua elemen matriks A dengan λ.

Jika A, B, dan C adalah matriks berordo sama dan λ adalah skalar, maka terdapat beberapa hukum pada operasi penjumlahan dan perkalian skalar terhadap matriks antara lain :

1. $A + B = B + A$ (komutatif)
2. $(A + B) + C = A + (B + C)$ (asosiatif)
3. $\lambda (A + B) = \lambda A + \lambda B$ (distributif)
4. Selalu ada matriks D sedemikian sehingga $A + D = B$

2.4.2.3. Operasi Perkalian pada Matriks

Pada umumnya matriks tidak komutatif terhadap operasi perkalian. Pada perkalian matriks AB, matriks A disebut matriks pertama dan B disebut matriks kedua. Syarat perkalian matriks adalah jumlah kolom matriks pertama sama dengan jumlah baris matriks kedua.

Pandang $A = (a_{ij})$ berordo (p x q) dan $B = (b_{ij})$ berordo (q x r). Maka perkalian AB adalah suatu matriks $C = (c_{ij})$ berordo (p x r) dengan

$$c_{ij} = a_{i1}\, b_{1j} + a_{i2}\, b_{2j} + \ldots + a_{iq}\, b_{qj}$$

untuk setiap $i = 1, 2, \ldots, p$ dan $j = 1, 2, \ldots, r$.

2.4.3. Transpose dari suatu Matriks

Pandang suatu matriks A = (a_{ij}) berordo (m x n) maka transpose dari A adalah matriks A^T berordo (n x m) yang didapatkan dari A dengan menuliskan baris ke-i dari A, $i = 1, 2, \ldots, m$, sebagai kolom ke-i dari A^T. Sehingga $A^T = (a_{ji})$. Beberapa sifat matriks transpose antara lain:

1. $(A + B)^T = A^T + B^T$
2. $(A^T)^T = A$
3. $\lambda (A^T) = (\lambda A^T)$, λ skalar
4. $(AB)^T = B^T A^T$

2.4.4. Determinan

Definisi 2.4.4.1

Barisan bilangan-bilangan ($j_1 , j_2 , \ldots, j_n$) dengan $j_i \neq j_k$, untuk $i \neq k$ (i dan $k = 1, 2, \ldots, n$) serta j_i salah satu dari bilangan asli (1, 2, ... , n) disebut permutasi.

Apabila terdapat n buah bilangan asli 1, 2, ..., n, maka banyaknya permutasi yang dapat dibentuk adalah $n ! = n (n - 1) (n - 2) \ldots$ 2.1.

Definisi 2.4.4.2

Suatu inversi pada suatu permutasi ($j_1 , j_2 , \ldots, j_n$) adalah jika $j_k < j_i$ (j_k mendahului j_i) padahal $j_i < j_k$ (i dan $k = 1, 2, \ldots, n$).

Definisi 2.4.4.3

Jika banyaknya inversi dari suatu permutasi adalah bilangan ganjil maka disebut permutasi ganjil dan sebaliknya disebut permutasi genap.

Definisi 2.4.4.4

Misalkan (j_1 , j_2 , …, j_n) suatu permutasi, maka Tanda (sign) dari permutasi tersebut, ditulis $\sigma(j_1, j_2, \ldots, j_n)$ adalah $\sigma(j_1, j_2, \ldots, j_n) = +1$, bila $(j_1, j_2, \ldots, j_n)$ genap, dan $\sigma(j_1, j_2, \ldots, j_n) = -1$ bila $(j_1, j_2, \ldots, j_n)$ ganjil.

Misalkan diberikan matriks bujur sangkar A berordo n

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Pandang suatu hasil kali antara n elemen-elemen dari A yang masing-masing terletak pada baris yang berbeda dan kolom yang berbeda (suatu hasil kali yang mengandung hanya satu elemen dari setiap baris dan setiap kolom). Misalnya hasil kali n elemen diagonal utama matriks A yaitu a_{11} , a_{22} , …, a_{nn}.

Untuk memudahkan diambil satu hasil kali dari n elemen-elemen yang barisnya telah diurutkan (boleh juga kolomnya yang telah diurutkan), maka setiap hasil kali antara n elemen matriks A di atas selalu berbentuk (*) $a_1 j_1$, $a_2 j_2$, $a_3 j_3$, …, $a_n j_n$ dengan subscript j_i menunjukkan kolomnya.

Karena masing-masing faktor haruslah elemen yang datang dari kolom yang berbeda maka barisan $(j_1, j_2, \ldots, j_n)$ adalah suatu permutasi. Apabila hasil kali (*) dilengkapi dengan memberikan Tanda (sign) dari permutasi $(j_1, j_2, \ldots, j_n)$ tersebut, maka hasil kali (**)$\sigma(j_1, j_2, \ldots, j_n)$. $a_1 j_1$, $a_2 j_2$, $a_3 j_3$, …, $a_n j_n$, disebut sebagai hasil kali bertanda dari n elemen-elemen $a_1 j_1$, $a_2 j_2$, …, $a_n j_n$.

Definisi 2.4.4.5

Determinan dari suatu matriks bujur sangkar A berordo n adalah jumlah dari semua n ! hasil kali bertanda dari elemen-elemen matriks A tersebut. Dengan kata lain

$$\det(A) = |A| = \sum \sigma(j_1, j_2, \ldots, j_n).\, a_{1j_1}, a_{2j_2}, a_{3j_3}, \ldots, a_{nj_n}$$

Definisi 2.4.4.6

Suatu matriks bujur sangkar A disebut matriks singular jika det (A) = 0. Sebaliknya jika det (A) ≠ 0 maka disebut matriks nonsingular.

2.4.5. Matriks Invers

Definisi 2.4.5.1

Sebuah matriks bujur sangkar A berordo n dikatakan mempunyai invers jika ada suatu matriks B sedemikian sehingga $AB = BA = I_n$. Matriks B disebut invers matriks A, ditulis A^{-1}, merupakan matriks bujur sangkar berordo n.

Beberapa sifat matriks invers antara lain :

1. $(A^{-1})^{-1} = A$
2. $(AB)^{-1} = B^{-1} A^{-1}$

Matriks-matriks yang mempunyai invers adalah matriks-matriks yang nonsingular.

2.4.6. Sifat Matriks

Secara umum matriks mempunyai beberapa sifat antara lain :

1. Misalkan matriks B berordo n diperoleh dari matriks A dengan cara mengalikan sebuah baris / kolom dengan skalar λ maka det (B) = λ det (A).

2. Misalkan matriks B berordo *n* diperoleh dari matriks A dengan cara menukar dua baris / kolom maka det (B) = - det (A).
3. Misalkan diketahui 3 matriks A_1 , A_2 dan B mempunyai elemen sama kecuali pada baris ke-*i*, yaitu elemen baris ke-*i* dari matriks B merupakan jumlah dari elemen baris ke-*i* dari matriks A_1 dan A_2 maka det (B) = det (A_1) + det (A_2)
4. Determinan matriks identitas adalah 1.
5. Misalkan $B = A^T$ maka det (B) = det (A).
6. Jika A berordo *n* mempunyai 2 baris atau kolom yang elemennya sama maka det (A) = 0.
7. Harga determinan tidak berubah apabila baris / kolom ke-*i* ditambah dengan λ baris / kolom ke-*j*.
8. Jika semua elemen dalam suatu baris atau kolom dari suatu matriks adalah nol, maka determinan matriks tersebut sama dengan nol.