BAB II

TEORI DASAR

Algoritma Rivest-Shamir-Adleman (RSA) didasarkan pada prinsip-prinsip teori bilangan. Bab ini menjelaskan teori-teori dasar antara lain fungsi, teori bilangan, sistem bilangan biner dan file yang akan digunakan dalam pembahasan bab III.

2.1. Fungsi

Definisi 2.1.1 Himpunan

Himpunan adalah kumpulan benda atau obyek yang berbeda dengan syarat keanggotaan yang jelas. .

Obyek dari himpunan disebut dengan elemen atau anggota himpunan.

Contoh 2.1.1

Sebuah himpunan X yang terdiri atas elemen p,q,r dan s dinotasikan dengan $X = \{ p,q,r,s \}$.

Definisi 2.1.2 Fungsi

Misalkan X dan Y adalah dua buah himpunan. Fungsi f dari X dan Y adalah perkawanan dengan suatu aturan f antara setiap elemen $x \in X$ dengan tepat satu elemen $y \in Y$.

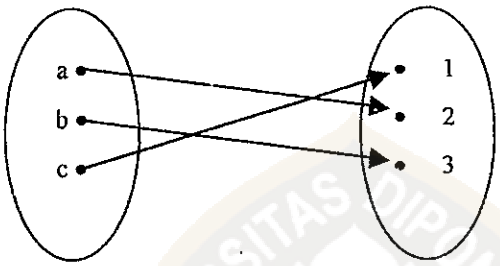
Notasi: $f: X \mapsto Y, (\forall x \in X)(\exists! y \in Y) \Rightarrow f(x) = y$.

X disebut dengan domain dan Y disebut kodomain.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2.1.2

Misalkan X = {a, b, c} dan Y = {1,2,3}, diberikan suatu fungsi f (a) = 2, f (b) = 3 dan f (c) = 1.Fungsi f di atas dapat digambarkan sebagai berikut :



Gambar 2.1 Fungsi dari himpunan X terhadap himpunan Y

Fungsi f merupakan fungsi karena $\forall x \in X$ mempunyai kawan tepat satu elemen $y \in Y$.

Definisi 2.1.3 Fungsi Injektif

Suatu fungsi $f : X \mapsto Y$ disebut fungsi satu-satu atau injektif jika hanya jika setiap $y \in Y$ mempunyai kawan tepat satu $x \in X$ sedemikian sehingga $f(x) = y$.

Notasi : $f : X \mapsto Y, (\forall y \in Y)(\exists! x \in X) \Rightarrow f(x) = y$.

Contoh 2.1.2 merupakan contoh fungsi Injektif.

Definisi 2.1.4 Fungsi Surjektif

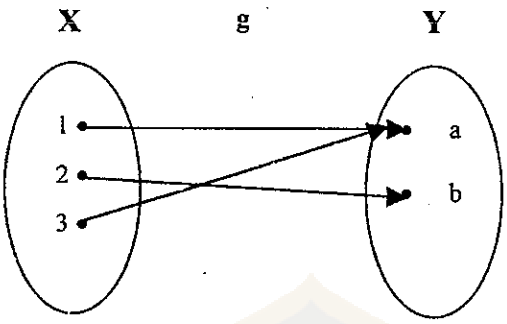
$f : X \mapsto Y$ disebut Surjektif atau Onto jika hanya jika untuk setiap $y \in Y$ dikawankan dengan satu atau lebih dari satu elemen $x \in X$ dengan $f(x) = y$.

Notasi : $f : X \mapsto Y, (\forall y \in Y)(\exists x \in X) \Rightarrow f(x) = y$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also a... the UNDIP-IR... up and preservation:
(http://...

Contoh 2.1.3

Misal X = {1, 2, 3}, Y = {a, b} diberikan fungsi g sebagai berikut:



Gambar 2.2 Fungsi Surjektif

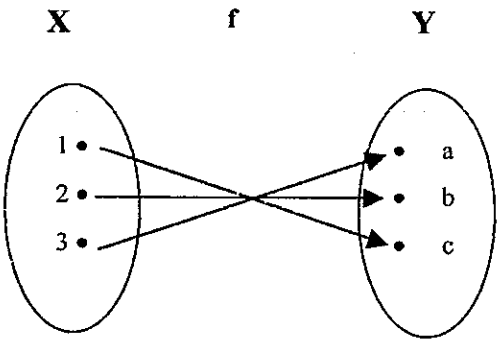
Fungsi g merupakan fungsi surjektif sebab setiap elemen $y \in Y$ dikawankan dengan satu atau lebih dari satu elemen $x \in X$.

Definisi 2.1.5 Fungsi Bijektif

Jika f adalah fungsi yang injektif dan surjektif maka f disebut bijektif (berkorespondensi satu-satu).

Contoh 2.1.4

Misal X = {1, 2, 3}, Y = {a, b, c} diberikan fungsi f (1) = c, f (2) = b, f (3) =a.



Gambar 2.3 Fungsi Bijektif

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Fungsi f merupakan fungsi yang bijektif sebab :

1. f merupakan fungsi yang injektif

   Setiap elemen $y \in Y$ mempunyai kawan tepat satu elemen $x \in X$.

2. f merupakan fungsi yang surjektif

   Setiap elemen $y \in Y$ dikawankan dengan elemen $x \in X$.

Dari contoh di atas dapat disimpulkan bahwa jika himpunan X dan Y mempunyai banyak elemen himpunan yang sama dan $f : X \mapsto Y$ fungsi Injektif maka f merupakan fungsi bijektif.

Definisi 2.1.6 Fungsi Invers

Misal f bijektif dari X dan Y. Fungsi Invers dari f adalah suatu fungsi bijektif yang mengawankan setiap elemen $y \in Y$ ke elemen $x \in X$ dengan $f^{-1}(y) = x$.

Notasi : $f : X \mapsto Y \Rightarrow f^{-1} : Y \mapsto X$, $f^{-1}(y) = x, y \in Y, x \in X$.

Definisi 2.1.7 Fungsi Komposit

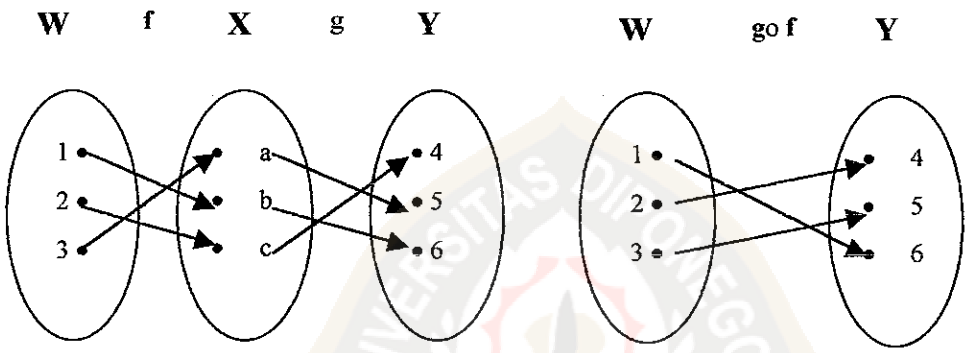
Misalkan $f : W \mapsto X$ dan $g : X \mapsto Y$ maka fungsi komposit g dengan f, dinotasikan dengan g o f , adalah suatu fungsi dari himpunan W ke himpunan Y.

Notasi : $g \circ f(w) = g(f(w)) = y, \forall w \in W, \forall y \in Y$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2.1.5

Misal W ={1,2,3}, X ={a,b,c}dan Y ={4,5,6}, f : W ↦ X dan g : X ↦ Y dengan f (1) = b, f (2) = c, f (3) = a, g (a) = 5, g (b) = 6 dan g (c) = 4 maka fungsi komposit g o f (w) dapat dinyatakan sebagai berikut :



Gambar 2.4 Fungsi Komposit

Definisi 2.1.8 Fungsi berinvers satu sama lain

Misalkan f dan g fungsi bijektif. Fungsi f dan g dikatakan berinvers satu sama lain jika f (g (x)) = x , x adalah elemen dalam domain fungsi g, dan g (f (x)) = x, x adalah elemen dalam domain fungsi f.

Contoh 2.1.6

Misalkan $f(x) = 2x + 3$ dan $g(x) = \frac{x-3}{2}$, maka

(i). $f(g(x)) = 2 \cdot \left(\frac{x-3}{2}\right) + 3 = x$.

(ii). $g(f(x)) = \frac{(2x+3)-3}{2} = x$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

dari hasil (i) dan (ii), maka dapat disimpulkan bahwa f (x) dan g (x) merupakan fungsi-fungsi yang berinvers satu sama lain.

Definisi 2.1.9 Fungsi Satu Arah

f : X↦ Y disebut fungsi satu arah, jika f (x) mudah dihitung untuk setiap x ∈ X tetapi untuk hampir seluruh y ∈ Y sangat sulit untuk menentukan nilai inversnya yaitu nilai x ∈ X sedemikian sehingga f (x) = y.

$$y = f(x) \quad \text{mudah}$$

$$x = f^{-1}(y) \quad \text{sulit}$$

Contoh 2.1.7

Misalkan X = { 1,2,3,4,5,6,7,8,9,10 } diberikan f (x) = 6x mod 13.

Hasil yang akan diperoleh adalah sebagai berikut :

x	1	2	3	4	5	6	7	8	9	10
f(x)	6	12	5	11	4	10	3	9	2	8

Tabel 2.1 Nilai Fungsi Satu Arah f (x) = 6x mod 13

Dari contoh di atas perhitungan nilai f (x) relatif mudah .Tetapi apabila diberikan nilai f (x) = 3 tanpa melihat tabel di atas maka terasa cukup sulit untuk menemukan nilai x sedemikian sehingga f (x) = 3.

Tetapi jika diberikan nilai f (x) = 6 maka dapat dengan mudah didapat nilai x = 1, akan tetapi hampir untuk semua nilai f (x) yang diberikan tidak mudah

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

menghitung nilai x yang bersesuaian tanpa menggunakan alat bantu seperti tabel di atas. Oleh sebab itulah f (x) pada contoh merupakan fungsi satu arah.

Definisi 2.1.10 Fungsi Satu Arah *Trapdoor*

Fungsi Satu Arah *Trapdoor* adalah fungsi satu arah dengan diberikan suatu tambahan informasi yang disebut *Informasi Trapdoor* untuk mempermudah pencarian invers dari fungsi.

$y = f_k(x)$ mudah

$x = f^{-1}_k(y)$ mudah jika y dan k diketahui

$x = f^{-1}_k(y)$ sulit jika y diketahui dan k tidak diketahui

Contoh 2.1.8

Diambil bilangan prima p = 43 dan q = 59 maka n = pq = 2537. Didefinisikan sebuah fungsi $f(x) = x^4 \bmod n$ dengan $x \in X = \{1,2,3,\ldots,n-1\}$. Misalkan diberikan f (x) = 2388 maka untuk mendapatkan nilai x sedemikian sehingga f (x) = 2388 terasa cukup sulit.

Tetapi jika diberikan nilai n = 2537 maka akan didapatkan nilai x dari f (x) = 2388 yaitu x = 91 karena $(91)^4 = 27029.2537 + 2388$.

Oleh sebab itulah fungsi $f(x) = x^4 \bmod n$ disebut fungsi Satu Arah *Trapdoor* dengan nilai n sebagai *informasi Trapdoor* .

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy for the purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

2.2 Teori Bilangan

2.2.1 Pembagi

Definisi 2.2.1.1 Himpunan Bilangan Bulat

Himpunan {…,-3,-2,-1,0,1,2,3,…} disebut himpunan bilangan bulat dengan notasi Z.

Himpunan {1,2,3,…}disebut himpunan bilangan bulat positif, dengan notasi Z^+.

Definisi 2.2.1.2 Pembagi

Misalkan a,b $\in$ Z, a dikatakan membagi b jika terdapat sebuah bilangan bulat c sedemikian sehingga b = a.c.

Jika a membagi b, ditulis a | b.

Definisi.2.2.1.3 Pembagi Persekutuan

Misalkan a,b $\in$ Z, a$\neq$ 0, b$\neq$ 0. Pembagi persekutuan dari a dan b adalah bilangan bulat yang membagi baik a dan b.

Teorema.2.2.1.4

Misalkan a,b,c $\in$ Z. Jika c adalah pembagi persekutuan dari a dan b, maka

(i). c | (a + b)

(ii). c | (a - b)

(iii).Jika c | a , maka c | a.b.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Bukti :

$c \mid a \Rightarrow \quad a = c.q_1 \quad$ untuk $q_1 \in Z$ (1)

$c \mid b \Rightarrow \quad b = c.q_2 \quad$ untuk $q_2 \in Z$ (2)

(i). Hasil penjumlahan persamaan (1) dan (2) adalah

$a + b = c.q_1 + c.q_2 = c.(q_1 + q_2)$,

$(q_1 \in Z)(q_2 \in Z) \Rightarrow (q_1 + q_2) \in Z$.

Maka terbukti bahwa c habis membagi (a + b) , c | (a+ b).

(ii). Hasil pengurangan persamaan (1) dan (2) adalah

$a - b = c.q_1 - c.q_2 = c.(q_1 - q_2)$,

$(q_1 \in Z)(q_2 \in Z) \Rightarrow (q_1 - q_2) \in Z$.

Maka terbukti bahwa c habis membagi (a – b), c | (a- b).

(iii). persamaan (1) : $(\exists b \in Z) \Rightarrow a.b = c.(q_1.b)$,

$(q_1 \in Z)(b \in Z) \Rightarrow (q_1.b) \in Z$.

Sehingga terbukti c | a.b.

Definisi 2.2.1.5 *Greatest Common Divisor* (Pembagi Persekutuan Terbesar)

Misalkan a,b,c dan d ∈ Z, d disebut *Greatest Common Divisor* dari a dan b jika :

(i). $d > 0$

(ii). $d \mid a$ dan $d \mid b$

(iii). Jika $c \mid a$ dan $c \mid b$ maka $c \mid d$

Notasi : d = gcd(a,b)

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

gcd(a,b) merupakan bilangan bulat positif terbesar yang dapat membagi a dan b.

Contoh 2.2.1.1

Pembagi persekutuan dari 12 dan 18 adalah { ± 1, ± 2, ± 3, ± 6 } maka gcd (12,18) = 6.

Definisi 2.2.1.6 *Least Common Multiple* (Kelipatan Persekutuan Terkecil)

Misalkan a,b,c dan d ∈ Z, d disebut *Least Common Multiple* dari a dan b jika :

(i). d > 0

(ii). a | d dan b | d

(iii). Jika a | c dan b | c maka d | c

Notasi : d = lcm (a,b).

lcm (a,b) merupakan bilangan bulat positif terkecil yang dapat dibagi a dan b.

Contoh 2.2.1.2

Misalkan a = 12 dan b = 8 maka lcm (12,8) = 24 sebab 12| 24 dan 8 | 24.

Definisi 2.2.1.7 Algoritma Pembagian

Jika a,b ∈ Z dengan a≥ 0 dan b > 0. Pembagian bilangan a oleh b menghasilkan sebuah hasil bagi q dan sisa r sedemikian sehingga

$$a = b.q + r \ , \ 0 \le r < b, q \ge 0$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Contoh 2.2.1.3

Misalkan a = 40, b = 12 maka q = 3 dan r = 4, sebab 40 = 12.(3) + (4)

Teorema 2.2.1.8

Jika $a \geq 0$, $b > 0$ dan $a = b.q + r$, $0 \leq r < b$ maka gcd(a,b) = gcd(b,r).

Bukti :

Misalkan c adalah pembagi persekutuan dari a dan b.

Teorema 2.2.1.4(iii) : $c \mid b \Rightarrow c \mid b.q, (q \in Z)$ (1)

Teorema 2.2.1.4(ii) : $c \mid a, c \mid bq \Rightarrow c \mid a - b.q \ (= r)$ (2)

Dari persamaan (1) dan (2) : $c \mid b, c \mid r \Rightarrow c = \gcd(b,r)$

Sehingga terbukti gcd(a,b) = gcd (b,r).

Contoh 2.2.1.4

Dari contoh 2.2.1.3 didapat bahwa gcd(40,12) = 4 dan gcd(12,4) = 4 sehingga gcd(40,12) = gcd(12,4) = 4.

Teorema 2.2.1.9 Algoritma Euclid

Misalkan $a \geq 0, b > 0$ dan

$$a = b.q_0 + r_1 \quad , \quad 0 \leq r_1 < b,$$

$$b = r_1.q_1 + r_2 \quad , \quad 0 \leq r_2 < r_1,$$

$$r_1 = r_2.q_2 + r_3 \quad , \quad 0 \leq r_3 < r_2,$$

$$\vdots$$

$$r_{n-1} = r_n.q_n + r_{n+1} \quad , \quad 0 \leq r_{n+1} < r_n$$

maka gcd (a,b) = r_n dengan $r_{n+1} = 0$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Bukti :

Definisi 2.2.1.7 : $b \mid a \Rightarrow a = b.q_0 + r_1 \quad , \quad 0 \leq r_1 < b,$

Teorema 2.2.1.8: $\gcd(a,b) = \gcd(b,r_1)$

$(r_1 \neq 0), (r_1 \mid b) \Rightarrow b = r_1.q_1 + r_2 \quad , \quad 0 \leq r_2 < r_1,$

Teorema 2.2.1.8: $\gcd(b,r_1) = \gcd(r_1,r_2)$

Demikian seterusnya terjadi pembagian r_i dengan r_{i+1} dengan $r_{i+1} \neq 0$.

Karena $r_1 > r_2 > r_3 > \ldots$ maka akhirnya terdapat $r_i = 0$.

Misalkan r_{n+1}merupakan sisa pertama yang nol maka berdasarkan teorema 2.2.1.8:

$$\gcd(a,b) = \gcd(b,r_1) = \ldots = \gcd(r_n,r_{n+1}) = \gcd(r_n, 0)$$

Karena $\gcd(r_n, 0) = r_n$ maka $\gcd(a,b) = \gcd(r_n, 0) = r_n$

Jadi pembagi persekutuan terbesar dari a dan b akan menjadi sisa hasil pembagian terakhir yang tidak nol.

Contoh 2.2.1.5

Pembagi persekutuan terbesar dari 1492 dan 1776 dengan menggunakan algoritma Euclid adalah sebagai berikut :

$1776 = (1) \cdot 1492 + 284 \quad (q_0 = 1, r_1 = 284)$

$1492 = (5) \cdot 284 + 72 \quad (q_1 = 5, r_2 = 72)$

$284 = (3) \cdot 72 + 68 \quad (q_2 = 3, r_3 = 68)$

$72 = (1) \cdot 68 + 4 \quad (q_3 = 1, r_4 = 4)$

$68 = (4) \cdot 17 \quad (q_4 = 17, r_5 = 0)$

Karena sisa hasil pembagian terakhir yang tidak nol adalah $r_4 = 4$ maka $\gcd(1776,1492) = 4$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Teorema 2.2.1.10

Jika a ,b$\in$ Z, a$\neq$0 dan b$\neq$0 maka terdapat c $\in$ Z pembagi persekutuan terbesar dari a dan b sedemikian sehingga c = m_0 .a + n_0.b , untuk m_0, $n_0\in$ Z.

Bukti :

Misalkan X = {m.a+n.b | m.n$\in$ Z, m.a + n.b > 0}. Dalam X terdapat bilangan bulat terkecil,sebut c, yang dapat dinyatakan dalam bentuk

$$c = m_0.a + n_0.b, (m_0 ,n_0 \in Z) \quad (1)$$

Misalkan c = gcd(a,b) maka akan dibuktikan c | a dan c | b .

Ambil x $\in$ X maka

$$x = m.a + n.b , (m,n \in Z) \quad (2)$$

Dari definisi 2.2.1.7 : $x = t.c + r$, $(t,r \in Z), 0 \leq r < c$ (3)

Dari persamaan (1),(2) dan (3) didapat :

$$m.a + n.b = t (m_0.a + n_0.b) + r \Rightarrow r = (m - t.m_0)a + (n - t.n_0.b).b \quad (4)$$

Dari persamaan (4) didapat bahwa r $\in$ X.

Persamaan (3) : $r = 0 \Rightarrow x = t.c$

$\Rightarrow c \mid x$

Persamaan (2) : $c \mid x \Rightarrow c \mid m.a + n.b$ (5)

Persamaan (5) : ambil $m = 1, n = 0 \Rightarrow c \mid 1.a + 0.b$

$\Rightarrow c \mid a$ (6)

ambil $m = 0, n = 1 \Rightarrow c \mid 0.a + 1.b$

$\Rightarrow c \mid b$ (7)

Karena c | a dan c | b maka terbukti $c = gcd(a,b) = (m_0).a + (n_0).b$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2.2.1.11

Dua bilangan bulat a dan b dikatakan relatif prima jika pembagi persekutuan terbesarnya adalah 1, gcd(a,b) = 1.

Definisi 2.2.1.12

Bilangan bulat $p \geq 2$ disebut sebagai bilangan prima jika bilangan pembagi dari p adalah 1 dan p .

Teorema 2.2.1.13

Misalkan $a,b \in Z$. Jika $n \mid ab$ dan gcd(a,n) =1 maka $n \mid b$

Bukti :

Teorema 2.2.1.2 : $n \mid ab \Rightarrow ab = nc , c \in Z$

Teorema 2.2.1.10 : gcd(a,n) =1 $\Rightarrow 1 = ax + ny, \quad (x,y \in Z)$

$\Rightarrow b = abx + nby$

$\Rightarrow b = n(cx + by)$

$\Rightarrow n \mid b$

Teorema 2.2.1.14

Misalkan p bilangan prima , a , b bilangan bulat . Jika $p \mid ab$ maka $p \mid a$ atau $p \mid b$.

Bukti :

Misalkan p tidak membagi a maka akan dibuktikan $p \mid ab \Rightarrow p \mid b$.

Misalkan p tidak membagi a $\Rightarrow$ gcd(p,a) = 1

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy for the purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Teorema 2.2.1.13 : gcd(p,a) = 1, p | ab $\Rightarrow$ p | b

Sehingga terbukti bahwa p | ab $\Rightarrow$ p | b.

Teorema 2.2.1.15 Faktorisasi Unik

Setiap bilangan bulat positif n ≥ 2 dapat dinyatakan sebagai produk bilangan prima, yaitu

$$n = p_1^{e_1} \; p_2^{e_2} \; \dots \; p_k^{e_k}$$

p_i adalah bilangan prima dari n, $p_1 < p_2 < \dots < p_k$ dan $e_i \in Z^+$.

Contoh 2.2.1.6

$720 = 2^4 \cdot 3^2 \cdot 5^1$

Teorema 2.2.1.16

Jika $\{a_1, a_2, \dots, a_n\}$ adalah himpunan dengan $a_i \in Z^+$ dengan

$$a_j = p_1^{e_{1j}} \; p_2^{e_{2j}} \; \dots \; p_k^{e_{kj}}, \; i = 1,2,\dots,n \text{ dan } j = 1,2,\dots,k$$

maka lcm $(a_1, a_2, \dots, a_n) = p_1^{g_1} \; p_2^{g_2} \; \dots \; p_k^{g_k}$ dengan $g_j = \max\{e_{j1}, e_{j2} \dots e_{jn}\}$

Bukti :

$(\forall i, j)$, $g_j = \max\{e_{j1}, e_{j2} \dots e_{jn}\} \geq e_{ji}$ maka lcm $(a_1, a_2, \dots, a_n) = p_1^{g_1} \; p_2^{g_2} \dots \; p_k^{g_k}$ dapat dibagi oleh setiap a_i.

Misalkan jika terdapat sebuah kelipatan persekutuan dari $\{a_1, a_2, \dots, a_n\}$ yang dapat dinyatakan dalam bentuk $p_1^{h_1} \; p_2^{h_2} \; \dots \; p_k^{h_k}$ dengan $(\forall i, j)$, $h_j \geq e_{ji}$ maka $h_j \geq \max\{e_{j1}, e_{j2} \dots e_{jn}\} = g_j$ dan $p_1^{h_1} \; p_2^{h_2} \; \dots \; p_k^{h_k}$ dapat dibagi oleh $p_1^{g_1} \; p_2^{g_2} \dots \; p_k^{g_k}$, sehingga $p_1^{g_1} \; p_2^{g_2} \dots \; p_k^{g_k} = \text{lcm}\,(a_1, a_2, \dots, a_n)$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2.2.1.7

Misalkan $105 = 2^0 . 3^1 . 5^1 . 7^1 . 11^0$

$360 = 2^3 . 3^2 . 5^1 . 7^0 . 11^0$

$1078 = 2^1 . 3^0 . 5^0 . 7^2 . 11^1$

maka $\text{lcm}(105,360,1078) = 2^{\max(0,3,1)} . 3^{\max(1,2,0)} . 5^{\max(1,1,0)} . 7^{\max(1,0,2)} . 11^{\max(0,0,1)}$

$= 2^3 . 3^2 . 5^1 . 7^2 . 11^1$

$= 194040$

2.2.2 Aritmatika Modulo

Misalkan $n \in Z^+$.

Definisi 2.2.2.1. Kongruensi Modulo

Jika $a,b \in Z$ maka a kongruen ke b modulo n maka n membagi (a-b), ditulis $a \equiv b \pmod n$

Contoh 2.2.2.1

$24 \equiv 9 \pmod 5$ sebab $5 \mid (24 - 9)$

Teorema. 2.2.2.2

Jika $a, b \in Z$ maka a kongruen b modulo n maka terdapat $k \in Z$ sedemikian sehingga

$$a = b + k.n$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Bukti :

Definisi 2.2.2.1 : $a \equiv b \pmod{n} \Rightarrow n \mid a-b$

Definisi 2.2.1.2 : $n \mid a-b \Rightarrow a-b = k.n \ , \ k \in Z$

$\Rightarrow a = b + k.n$

Definisi 2.2.2.3 Bilangan bulat modulo n

Bilangan modulo n ditulis Z_n adalah himpunan yang anggota-anggotanya adalah bilangan bulat {0,1,2,3,...,n-1}.

Operasi penjumlahan, pengurangan dan perkalian dalam Z_n dibentuk oleh modulo n.

Contoh 2.2.2.2

Z_{12} = { 1,2,3,...,11}. Dalam Z_{12} , $10 + 16 = 26 \bmod 12 \equiv 2$.

Definisi 2.2.2.4 Invers perkalian modulo n

Misalkan $a \in Z_n$ dan gcd(a,n) = 1. Perkalian Invers a modulo n adalah sebuah bilangan bulat tunggal $x \in Z_n$ sedemikian sehingga $ax \equiv 1 \pmod{n}$

Teorema 2.2.2.5

Jika $a \equiv b \pmod{n}$ dan $c \equiv d \pmod{n}$ maka :

(i). $a + c \equiv b + d \pmod{n}$

(ii). $a.\ c \equiv b.\ d \pmod{n}$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Bukti :

Teorema 2.2.2.2 : $a \equiv b \pmod n \Rightarrow a = b + n.k_1, k_1 \in Z$ (1)

$c \equiv d \pmod n \Rightarrow c = d + n.k_2, k_2 \in Z$ (2)

(i).Operasi penjumlahan dari persamaan (1) dan (2) didapat

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

$= b + d + n.(k_1 + k_2)$

$a + c \equiv b + d \pmod n$

(ii). Operasi perkalian dari persamaan (1) dan (2) didapat

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

$= b.d + b.n.k_2 + d.n.k_1 + n.k_1.k_2$

$= b.d + n.(b.k_2 + d.k_1 + n.k_1.k_2)$

$a.c \equiv b.d \pmod n$

Teorema 2.2.2.6

Jika $a_1 \equiv b_1 \pmod n$, $a_2 \equiv b_2 \pmod n$, ... , $a_m \equiv b_m \pmod n$ maka

$$\prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} b_i \bmod n.$$

Bukti :

Teorema dibuktikan dengan menggunakan Induksi Matematika.

1. Untuk m = 1 maka berlaku $a \equiv b \pmod n$

2. Asumsikan untuk m = k maka berlaku $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \bmod n.$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Akan dibuktikan untuk m = k+1 maka berlaku juga $\prod_{i=1}^{k+1} a_i \equiv \prod_{i=1}^{k+1} b_i \bmod n$.

$$\prod_{i=1}^{k+1} a_i = \prod_{i=1}^{k} a_i \,.\, a_{k+1} \equiv \left(\prod_{i=1}^{k} b_i \bmod n \right) . \left(b_{k+1} \bmod n \right)$$

$$\equiv \prod_{i=1}^{k} b_i \,.\, b_{k+1} \bmod n$$

$$\equiv \prod_{i=1}^{k+1} b_i \bmod n$$

Teorema 2.2.2.7 Hukum Kanselasi.

Jika $ax \equiv ay \pmod n$ dan $(a,n) = 1$ maka $x \equiv y \pmod n$

Bukti :

Definisi 2.2.2.1 : $ax \equiv ay \pmod n \Rightarrow n \mid ax - ay$

$\Rightarrow n \mid a(x-y)$

Teorema 2.2.1.13 : $\gcd(a,n) = 1 \Rightarrow n \mid x-y$

$\Rightarrow x \equiv y \pmod n$.

Definisi 2.2.2.7 Pasangan Relatif Prima

Bilangan – bilangan bulat $a_1, a_2, a_3, \ldots a_n$ disebut pasangan relatif prima jika $\gcd(a_i, a_j) = 1, i \neq j$.

Contoh 2.2.2.3

{10,17,21}merupakan pasangan relatif prima karena gcd(10,17) = 1, gcd(17,21) = 1 dan gcd(10,21) = 1 .

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Teorema 2.2.2.8

Misalkan n_1 n_2 ... n_k pasangan relatif prima dan $n = n_1.n_2. \ldots .n_k$. Jika $a \equiv b(\bmod n_1), a \equiv b(\bmod n_2) \ldots a \equiv b(\bmod n_k)$ maka $a \equiv b(\bmod n)$.

Bukti :

Menurut teorema 2.2.2.1:

$$a \equiv b(\bmod n_1), a \equiv b(\bmod n_2) \ldots a \equiv b(\bmod n_k) \Rightarrow n_1 \mid (a-b), n_2 \mid (a-b) \ldots n_k \mid (a-b) \quad (1)$$

Teorema 2.2.1.16 :

Terdapat lcm(n_1 n_2 ... n_k) yang dapat membagi (a-b). Karena n_1 n_2 ... n_k merupakan pasangan relatif prima maka lcm($n_1, n_2, \ldots, n_k$) = n yang dapat membagi (a-b), $n \mid (a-b)$. (2)

Dari persamaan(1)dan (2) diperoleh :

$$a \equiv b(\bmod n_1), a \equiv b(\bmod n_2) \ldots a \equiv b(\bmod n_k) \Rightarrow n_1 \mid (a-b), n_2 \mid (a-b) \ldots n_k \mid (a-b)$$

$$\Rightarrow n \mid (a-b)$$

$$\Rightarrow a \equiv b(\bmod n)$$

2.2.3 Fungsi Euler

Definisi 2.2.3.1. Fungsi Euler (φ)

(i). Jika $n \in Z^+$, $\varphi(n) = |Z_n^*|$, $Z_n^* = \{a \in Z_n \mid \gcd(a,n) = 1\}$, Z_n^* disebut himpunan grup multikatif dari Z_n.

(ii). Jika p bilangan prima maka $\varphi(p) = p - 1$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

(iii). Jika p,q adalah bilangan prima, n = p.q maka φ (n) = (p –1) (q –1).

Contoh 2.2.3.1

Berikut ini adalah nilai fungsi Euler untuk Z_{11}.

n	1	2	3	4	5	6	7	8	9	10
φ(n)	0	1	2	2	4	2	6	4	6	4

Tabel 2.2 Nilai Fungsi Euler Z_{11}

(i). φ (8) = 4 yaitu diperoleh dari Z_8^*={ 1,3,5,7 } sehingga φ (8) = $|Z_8^*|$ = 4.

(ii). φ (5) = 5-1 = 4.

(iii). φ (6) = φ (3.2) = (3-1) (2-1) = 2.

Teorema 2.2.3.2 Teorema Euler

Misalkan x ∈ Z, jika (x,n) = 1 maka $x^{\varphi(n)} \equiv 1 \pmod n$,

Bukti :

Ambil W = { a_i | $1 \le a_i \le n$, gcd(a_i,n) =1} = { $a_1, a_2, \ldots a_{\varphi(n)}$ } , $1 \le i \le \varphi(n)$.

Teorema 2.2.1.14 : Terdapat bilangan prima, p, pembagi $x.a_i$ maka p membagi x atau p membagi a_i.

gcd(x,n) = 1, gcd (a_i,n) = 1 ⇒ gcd($x.a_i$,n) = 1 (1)

Teorema 2.2.1.7 : $x.a_i = nq + r$ ⇒ $x.a_i \equiv r \pmod n$, $0 \le r < n$ (2)

Teorema 2.2.1.8 : gcd($x.a_i$,n)= 1 ⇒ gcd(r,n) = 1 (3)

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Dari persamaan (2) dan (3) : $r \in W$ maka terdapat $r = a_j$, $1 \le j \le \varphi(n)$ (4)

Karena gcd(a_i,n)=1 maka $a_{i_1} \not\equiv a_{i_2} \pmod n$, $i_1 \neq i_2$.

Teorema 2.2.2.7 : $1 \le i_1, i_2 \le \varphi(n), i_1 \neq i_2$, gcd(x,n) =1 $\Rightarrow x.a_{i_1} \not\equiv x.a_{i_2} \pmod n$ (5)

Dari persamaan (5) didapat bahwa setiap $x.a_1, x.a_2, \ldots x.a_{\varphi(n)}$ kongruen terhadap elemen yang berbeda dalam W .

Dari persamaan (2) dan (4) maka dalam W terdapat :

$$x.a_1 \equiv a_{j_1} \pmod n$$

$$x.a_2 \equiv a_{j_2} \pmod n$$

.

.

$$x.a_{\varphi(n)} \equiv a_{\varphi(n)} \pmod n$$

dengan menggunakan teorema 2.2.2.6, kongruensi-kongruensi di atas dapat dinyatakan dalam bentuk $x^{\varphi(n)} \prod_{i=1}^{\varphi(n)} a_i \equiv \prod_{i=1}^{\varphi(n)} a_i \bmod n$.

Karena gcd(a_i,n)=1 maka gcd($\prod_{i=1}^{\varphi(n)} a_i$,n)=1.

Hukum Kanselasi : gcd($\prod_{i=1}^{\varphi(n)} a_i$, n) = 1 $\Rightarrow$ $x^{\varphi(n)} \prod_{i=1}^{\varphi(n)} a_i \equiv \prod_{i=1}^{\varphi(n)} a_i \bmod n$

$$\Rightarrow \quad x^{\varphi(n)} \equiv 1 \bmod n.$$

Contoh 2.2.3.2

Misalkan n = 14 dan x = -5 maka $W = \{ a_i \mid 1 \le a_i \le n , \gcd(a_i,n) = 1\}$ = {1,3,5,9,11,13} maka $\{x.a_i\}$ = {-5,-15,-25,-45,-55,-65 }dengan gcd($x.a_i$,n) = 1.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

Dengan menggunakan teorema 2.2.1.7 maka setiap $\{xa_i\}$ dapat dinyatakan sebagai berikut :

$-5 = (-1).\ 14 + 9 \equiv 9 \mod 14$ $\quad -45 = (-4).\ 14 + 11 \equiv 11 \mod 14$

$-15 = (-2).\ 14 + 13 \equiv 13 \mod 14$ $\quad -55 = (-4).\ 14 + 1 \equiv 1 \mod 14$

$-25 = (-2).\ 14 + 3 \equiv 3 \mod 14$ $\quad -65 = (-5).\ 14 + 5 \equiv 5 \mod 14$

sehingga didapat$\{r_j\} = \{1,3,5,9,11,13\}$ dengan setiap r_j berelatif prima dengan n.

Dengan menggunakan teorema 2.2.2.6 , maka

$[(-5).1]\ [(-5).3]\ [(-5).5]\ [(-5).9]\ [(-5).11]\ [(-5).13] = [1.3.5.9.11.13] \mod 14$

$(-5)^6 \quad [1.3.5.9.11.13] = [1.3.5.9.11.13] \mod 14$

Dengan menggunakan hukum kanselasi, maka :

$(-5)^6\ [1.3.5.9.11.13] = [1.3.5.9.11.13] \mod 14$

$(-5)^6 = 1 \mod 14$

Teorema 2.2.3.3 Teorema Fermat

Jika p bilangan prima dan $(x,p) = 1$ maka $x^{p-1} \equiv 1 \pmod p$.

Bukti :

Definisi 2.2.3.1(ii) : p adalah bilangan prima $\Rightarrow \varphi(p) = p-1$

Teorema 2.2.3.2 : $\varphi(p) = p-1 \Rightarrow x^{p-1} \equiv 1 \pmod p$

Teorema Fermat merupakan kasus khusus teorema Euler dengan p berupa bilangan prima.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation: (http://eprints.undip.ac.id)

2.3 Sistem Bilangan Biner

Sistem bilangan biner adalah sistem bilangan yang hanya menggunakan dua simbol yaitu 0 dan 1. Pembacaan bilangan biner dimulai dari kanan, simbol pertama mewakili bilangan satuan atau 2^0, bilangan kedua mewakili bilangan dua-an atau 2^1 , bilangan ketiga mewakili bilangan empat-an atau 2^2 dan seterusnya. Secara umum, simbol dengan posisi n, dengan simbol paling kanan pada posisi 0, menyatakan 2^n – an.

Bilangan biner dinyatakan dalam bentuk $(j_n\ j_{n-1}\ j_{n-2} \ldots j_2\ j_1\ j_0)_2$ dengan j_i adalah bilangan 0 atau 1.

$$\sum_{i=0}^{n} j_i \cdot 2^i = j_0 .2^0 + j_1 .2^1 + j_2 .2^2 + j_3 .2^3 + \ \ldots \ + j_n .2^n$$

Contoh 2.3.1

Bilangan biner $(11101)_2$ dalam basis 10 adalah :

$(11101)_2 = (1.2^4) + (1.2^3) + (1.2^2) + (0.2^1) + (1.2^0)$

$= 16 + 8 + 4 + 0 + 1$

$= 29$

Contoh di atas merupakan konversi bilangan biner ke bilangan desimal.

Konversi bilangan desimal ke biner dapat dilakukan dengan pembagian yang bersifat rekursif.

Algoritma pembagian dapat dinyatakan sebagai berikut :

1. Masukkan bilangan desimal n

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy for the purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

2. Jika n>0 maka lakukan proses :

   a. Lakukan pembagian n dengan sisa adalah sisa pembagian (n mod 2).

   b. Nilai n akan berubah menjadi hasil pembagian (n div 2).

Contoh 2.3.1

Bilangan $(29)_{10}$ dalam basis dua atau biner adalah :

Perhitungan	Hasil
n ←29	
	29 mod 2→ 1
n ←29 div 2 = 14	
	14 mod 2→ 0
n ←14 div 2 = 7	
	7 mod 2→ 1
n ←7 div 2 = 3	
	3 mod 2→ 1
n ←3 div 2 = 1	
	1 mod 2→ 1
n ←1 div 2 = 0	

Tabel 2.3 Perhitungan Biner $(29)_{10}$

Hasil yang didapat adalah $(11101)_2$ yaitu dengan penulisan dari hasil paling bawah ke hasil paling atas.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, backup and preservation:
(http://eprints.undip.ac.id)

2.4 File

Definisi 2.4.1

File adalah kumpulan sejumlah komponen yang bertipe data sama dengan jumlah tidak terbatas. Komponen file disebut dengan rekaman atau record.

Seringkali pada program aplikasi, data perlu disimpan untuk pengolahan lebih lanjut. Bila data yang perlu disimpan mempunyai volume yang cukup besar maka penyimpanan data dalam memori internal komputer bukanlah langkah yang tepat. Memori internal komputer mempunyai daya tampung yang terbatas dan data akan disimpan dalam sementara waktu saja sehingga tidak dapat diakses lagi pada waktu yang akan datang.

Untuk menyimpan data dengan volume besar harus menggunakan cara lain yaitu dengan menyimpannya dalam memori eksternal komputer. Memori eksternal komputer mempunyai daya tampung yang besar dan data disimpan secara permanen sehingga dapat diakses kembali . Data dalam memori eksternal disimpan dalam bentuk file. Media penyimpanan dalam memori eksternal dapat berupa disk yang akan menyimpan file dengan jumlah tidak terbatas. Komponen file dapat ditambah atau dikurangi sesuai dengan kebutuhan. Data dalam file dapat digunakan oleh sembarang program yang tipe datanya sama.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)