BAB II
TEORI BILANGAN

Teori bilangan berhubungan dengan sifat-sifat bilangan asli 1,2,3,.... yang juga disebut bilangan bulat positif. Bilangan-bilangan ini bersama-sama dengan bilangan bulat negatif dan nol membentuk himpunan bilangan bulat. Dan diantara bilangan-bilangan asli tersebut terdapat bilangan prima yang dalam tulisan ini berperan penting dan bilangan prima ini dilambangkan dengan p. Sedangkan diantara pasangan-pasangan bilangan asli tersebut terdapat pula pasangan-pasangan yang mempunyai pembagi persekutuan tidak lebih dari satu. Pasangan-pasangan bilangan ini dikatakan saling prima relatif.

2.1. Bilangan prima, Bilangan komposit, dan sifat prima relatif

Sebelum membahas mengenai bilangan prima, bilangan komposit, dan sifat prima relatif akan dijelaskan dahulu mengenai pengertian pembagian dan pembagian persekutuan terbesar.

definisi 2.1.1

suatu bilangan bulat b habis dibagi bilangan bulat a, dengan $a \neq 0$, jika terdapat bilangan bulat x yang memenuhi $b = ax$ dan ditulis $a \mid b$. Jika b tidak habis dibagi a maka ditulis $a \nmid b$.

b habis dibagi a juga dikatakan sebagai a habis

membagi b atau a adalah pembagi dari b atau b adalah suatu kelipatan dari a. Beberapa sifat pembagian ini diterangkan pada teorema berikut :

Teorema 2.1.2

(1). $a|b \Rightarrow a|bc \quad , \quad \forall c \in Z$

(2). $a|b$ dan $b|c \Rightarrow a|c$

(3). $a|b$ dan $a|c \Rightarrow a|\ (bx + cy) \quad \forall x,y \in Z$

(4). $a|b$ dan $b|a \Rightarrow a = \pm b$

(5). $a|b, \quad a > 0, \quad b > 0 \Rightarrow a \leq b$

(6). $m \neq 0 \ , \ a|b \Leftrightarrow ma \mid mb$

Bukti :

Jika $a|b$ berarti terdapat bilangan bulat r sedemikian sehingga $b = ar$, maka :

(1). Dengan mengalikan $b = ar$ dengan sembarang bilangan bulat c diperoleh : $bc = (ar)c$

atau $bc = a(rc)$

maka $a|bc$, $\forall$ bilangan bulat c.

(2). Jika $b|c$ berarti terdapat bilangan bulat s sedemikian sehingga $c = bs$, maka $c = (ar)s$

$= a(rs)$

atau berarti $a|c$.

(3). Jika $a|c$ berarti terdapat bilangan bulat s sedemikian sehingga $c = as$, maka :

$bx + cy = (ar)x + (as)y$

$= a(rx) + a(sy)$

$= a(rx + sy)$

berarti $a|(bx + cy)$, $\vee$ bilangan bulat x dan y.

(4). Jika $b|a$ berarti terdapat bilangan bulat s sedemikian sehingga $a = bs$, maka :

$$a = (ar)s = a(rs)$$

atau $rs = 1$. Karena r dan s adalah bilangan bulat maka $r = s = 1$ atau $r = s = -1$. Jadi $a = \pm b$

(5). Jika $a > 0$ dan $b > 0$, maka $r > 0$

dengan demikian berarti $b \geq a$.

(6). Dengan mengalikan $b = ar$ dengan m diperoleh :

$mb = m(ar)$

atau $mb = (ma)r$ Jadi $ma|mb$.

Teorema 2.1.3

$a,b \in Z$ dengan $a > 0$ maka terdapat bilangan bulat q dan r yang tunggal yang memenuhi $b = aq + r$, $0 \leq r < a$ q disebut hasil bagi (yang mungkin sama dengan 0) dan r disebut sisa dari pembagian b oleh a.

Bukti :

Misalkan q bilangan bulat yang terbesar sedemikian sehingga $q \leq b/a$ berarti $q + 1 > b/a$..... (2.1)

Misalkan $r = b - aq$, berarti $b = aq + r$..... (2.2)

dan juga $r/a = b/a - q \geq 0$, tetapi $q \leq b/a$ dan $a > 0$, maka $r \geq 0$. Dari persamaan (2.1) diperoleh :

$1 > (b/a - q) = (b-aq)/a = r/a$. Dengan perkataan lain $r<a$.

Jadi $0 \leq r < a$.

Untuk membuktikan bahwa q dan r adalah bilangan yang unik, dimisalkan terdapat q' ,$r' \in Z$ sedemikian sehingga :

$b = aq' + r'$, $0 \leq r' < a$..... (2.3)

untuk q dan q' hanya terjadi 3 kasus :

(i). $q' > q$

(ii). $q' < q$

(iii). $q' = q$

Kasus (i) : $q' > q$ maka $q' \geq (q + 1)$. Sehingga diperoleh :

$r' = b - aq' \leq b - a(q + 1) = (b - aq) - a = r - a < a$.

kontradiksi dengan $r' \geq a$.

Kasus (ii) : $q' < q$ maka $q' \leq (q - 1)$.Sehingga diperoleh :

$r' = b - aq' \geq b - a(q-1) = (b - aq) + a = r + a \geq 0$.

kontradiksi dengan $r' < 0$.

Berarti yang mungkin adalah kasus (iii) yaitu $q' = q$, dari (2.2) dan (2.3) dapat disimpulkan $r' = r$.

Dengan demikian maka berlaku $r = 0$ bila $a|b$ dan $0<r<a$ bila $a \nmid b$.

Pembagi persekutuan terbesar (ppt) dari 2 bilangan bulat a dan b akan banyak dipakai dalam teorema bilangan, sehingga akan dibahas sifat-sifat dari ppt ini.

Definisi 2.1.4

Suatu bilangan bulat a adalah pembagi persekutuan dari bilangan bulat b dan c jika $a|b$ dan $a|c$. Banyaknya pembagi persekutuan dari b dan c berhingga, kecuali $b = c = 0$. Jika salah satu dari b dan c tidak sama dengan 0, maka pembagi persekutuan yang terbesar disebut pembagi persekutuan terbesar (ppt) dari b dan

c serta dinyatakan oleh (b,c).

Berarti ppt dari b dan c, yaitu (b,c) didefinisikan untuk semua bilangan bulat b,c kecuali b = 0 dan c = 0, dan berlaku (b,c) ≥ 1. Beberapa sifat ppt dijelaskan pada teorema-teorema ini :

Teorema 2.1.5

Jika g adalah ppt dari b dan c, maka terdapat bilangan bulat x_o , y_o yang memenuhi :

$g = (b,c) = bx_o + cy_o$.

Bukti

Ambil semua bentuk kombinasi linier bx + cy dengan x dan y adalah bilangan bulat. Maka himpunan bilangan-bilangan { bx +cy } memuat bilangan positif dan negatif termasuk 0. Ambil x_o dan $y_o \in Z$ sedemikian sehingga $k = bx_o + cy_o$ adalah bilangan bulat positif terkecil dalam himpunan diatas. Sekarang akan dibuktikan $k \mid b$ dan $k \mid c$ dengan menggunakan kontradiksi.

Misalkan $k \nmid b$ maka berdasarkan teorema (2.1.3) terdapat bilangan bulat q dan r sedemikian sehingga $b = kq + r$ dengan $0 < r < k$. Atau :

$$r = b - kq$$
$$= b - q (bx_o + cy_o)$$
$$= b (1 - qx_o) + c (-qy_o)$$

berarti r adalah anggota himpunan { bx + cy }. Kontradiksi dengan k sebagai bilangan bulat positif terkecil dari himpunan { bx + cy }.

Dengan cara yang sama dapat dibuktikan $k \mid c$. Jika g adalah ppt dari b dan c, maka dapat dikatakan bahwa untuk suatu bilangan $B, C \in Z$ berlaku $b = gB$, $c = gC$ dan $k = bx_o + cy_o = g (Bx_o + Cy_o)$. Berarti $g \mid k$ dengan $g > 0$ $k > 0$, berdasarkan teorema 2.1.2 (5) berlaku $g \leq k$. Jika g adalah ppt dari b dan c, maka g tidak mungkin lebih kecil dari k. Sehingga $g = bx_o + cy_o$.

Untuk mencari x_o dan y_o , akan dibahas pada teorema berikutnya yaitu teorema 2.1.10.

Teorema 2.1.6

Jika g adalah ppt dari bilangan bulat b dan c , maka g adalah :

(1). Bilangan bulat positif terkecil dari semua bilangan berbentuk bx + cy dengan x dan y adalah bilangan bulat.

(2). Pembagi persekutuan dari b dan c yang positif dan habis dibagi oleh semua pembagi persekutuan dari b dan c yang lainnya.

(3). Unik.

Bukti :

(1). Berdasarkan pembuktian teorema 2.1.5.

(2). Jika d pembagi persekutuan dari b dan c, dan g ppt dari b dan c , maka berdasarkan teorema 2.1.2 (3) dan teorema 2.1.5, $d \mid g$.

(3). Misalkan k dan g adalah ppt dari b dan c , maka berdasarkan teorema 2.1.6 (2) dan teorema 2.1.2 (4)

k|g dan g|k berarti k = ± g. Sedangkan definisi 2.1.4 mengatakan (b,c) ≥ 1 kecuali b = 0 dan c = 0. Jadi g adalah unik.

Jika k ∈ Z memenuhi k = bx + cy , maka k belum tentu merupakan ppt dari b dan c, tetapi (b,c) adalah pembagi dari k. Tetapi jika terdapat bilangan bulat x dan y sehingga bx + cy = 1 , maka (b,c) = 1.

Teorema 2.1.7

Untuk bilangan bulat positif m, maka :

(ma , mb) = m (a,b)

Bukti :

Berdasarkan teorema 2.1.6 diperoleh : (ma , mb) adalah bilangan bulat positif terkecil dari semua bilangan berbentuk max + mby . Dengan perkataan lain (ma , mb) adalah hasil kali m dengan bilangan bulat terkecil dari semua bilangan berbentuk ax + by. Sedangkan bilangan terkecil dari semua bilangan berbentuk ax + by adalah (a , b) . Jadi (ma , mb) = m (a , b).

Teorema 2.1.8

Jika d|a dan d|b dengan d > 0 , maka

(a/d , b/d) = 1/d .(a , b)

Jadi bila (a , b) = g , akan berlaku (a/g , b/g) = 1.

Bukti :

Berdasarkan teorema 2.1.7 diketahui bahwa :

(ma , mb) = m (a , b). Bila m, a, dan b masing-masing diganti oleh d, (a/d), dan (b/d), maka diperoleh :

$$(d.\ a/d\ ,\ d.\ b/d\ ) = d\ (a/d\ ,\ b/d)$$

atau

$$(a/d\ ,\ b/d\ ) = 1/d\ (\ a\ ,\ b\ )$$

Untuk mencari ppt dari dua bilangan bulat yang besar sekali tidaklah mudah. Salah satu cara mencari ppt adalah dengan menggunakan algoritma Euclidean. Algoritma ini dapat digunakan untuk mencari ppt dari 2 bilangan bulat yang berapapun besarnya.

Teorema 2.1 9

Algoritma Euclidean.

Diberikan bilangan bulat a dan b > 0 , dengan menggunakan teorema 2.1.3 berulang kali sampai diperoleh sisa pembagiannya sama dengan nol seperti berikut :

$$\left.\begin{array}{ll}
a = bq_1 + r_1 & 0 < r_1 < b \\
b = r_1q_2 + r_2 & 0 < r_2 < r_1 \\
r_1 = r_2q_3 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_{n-2} = r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n\, q_{n+1} + 0 &
\end{array}\right\} \quad \ldots.(2.4)$$

Maka ppt dari a dan b adalah r_n, yaitu pembagi terakhir yang menghasilkan sisa sama dengan 0. Persamaan (2.4) disebut persamaan pembagian dari algoritma Euclidean.

Pembuktian teorema diatas akan dibagi menjadi 2 bagian yaitu :

Pertama dibuktikan :

Pembagi terakhir r_n pada persamaan (2.4) merupakan pembagi persekutuan dari a dan b.

Bukti :

Dari persamaan (2.4) yang terakhir didapat $r_n | r_{n-1}$, sehiingga dari persamaan sebelumnya diperoleh $r_n | r_{n-2}$. Proses ini terus berlangsung sehingga $r_n | b$ dan $r_n | a$. Dari proses tersebut dapat disimpulkan bahwa r_n adalah pembagi persekutuan dari a dan b.

Kedua dibuktikan :

Semua pembagi persekutuan dari a dan b adalah pembagi dari r_n

Bukti :

Misalkan c adalah pembagi persekutuan dari a dan b dari persamaan (2.4) yang pertama $r_1 = a - bq_1$ yang merupakan kombinasi linier dari a dan b. Berdasarkan teorema 2.1.2 (3) maka $c | r_1$. Dengan cara yang sama dilakukan untuk persamaan (2.4) yang kedua $r_2 = b - r_1 q_1$. Jika $c | b$ dan $c | r_1$, maka $c | r_2$. Proses berlangsung terus sampai pada persamaan $r_n = r_{n-2} - r_{n-1} q_n$

Jika $c | r_{n-2}$ dan $c | r_{n-1}$, maka $c | r_n$

Jadi $r_n = (a , b)$.

Teorema 2.1.10

X_n dan y_n dalam persamaan $(a,b) = ax_n + by_n$ dapat

diperoleh dengan mengeliminasi r_{n-1}, r_{n-2},.....r_2, r_1 dari persamaan (2.4).

Bukti :

Dalam algoritma Euclidean terdapat persamaan :

$$a = bq_1 + r_1 \qquad \text{.....(2.4a)}$$

$$b = r_1q_2 + r_2 \qquad \text{.....(2.4b)}$$

Dari persamaan (2.4a) , diperoleh $r_1 = a - bq_1$, jika ini disubstitusikan dalam persamaan (2.4b) diperoleh :

$$b = (a - bq_1) q_2 + r_2$$

maka : $r_2 = - aq_2 + (1 + q_1q_2)\, b.$

Dengan perkataan lain r_2 adalah kombinasi linier dari a dan b , dengan masing-masing koefisien $-q_1$ dan $(1 + q_1q_2)$

Sekarang substitusikan r_1 dan r_2 ke dalam persamaan :

$r_1 = r_2q_3 + r_3$ sehingga diperoleh :

$$a - bq_1 = [\, -aq_2 + (1 + q_1q_2)b \,]\, q_3 + r_3$$

$$r_3 = a(1 + q_2q_3) + b\, [\, -q_1 - q_3 - q_1q_2q_3 \,]$$

Terlihat bahwa r_3 juga merupakan kombinasi linier dari a dan b . Dengan cara yang serupa dapat diteruskan sehingga diperoleh bentuk $r_n = ax_n + by_n$, dengan koefisien x_n dan y_n merupakan perkalian dan penjumlahan dari bilangan-bilangan bulat yang memenuhi rumus rekursif.

$$\left.\begin{aligned} x_m &= x_{m-2} - q_m\, x_{m-1} \\ y_m &= y_{m-2} - q_m\, y_{m-1} \end{aligned}\right\} \qquad \text{.....(2.5)}$$

untuk m = 1,2,3,.....,n dengan

$$x_{-1} = 1 \qquad x_0 = 0 \qquad y_{-1} = 0 \qquad y_0 = 1$$

Rumus rekursif diatas dapat dibuktikan dengan induksi

matematik sebagai berikut :

Untuk m = 1, $r_1 = a - bq_1 = ax_1 + by_1$ $x_1 = 1$ $y_1 = -q_1$

yang memenuhi rumus rekursif :

$$x_1 = x_{-1} - q_1 x_0 \quad \text{dan} \quad y_1 = y_{-1} - q_1 y_0$$

Misalkan rumus rekursif benar untuk $m \leq k$ dengan $k \geq 1$ akan dibuktikan rumus rekursif tersebut benar pula untuk $m = k + 1$. Dari persamaan

$r_{k+1} = r_{k-1} - r_k q_{k+1}$ diperoleh :

$$r_{k+1} = (ax_{k-1} + by_{k-1}) - (ax_k + by_k) q_{k+1}$$

$$= a (x_{k-1} - q_{k+1} x_k) + b (y_{k-1} - q_{k+1} y_k)$$

sehingga :

$$x_{k+1} = x_{k-1} - q_{k+1} x_k \quad \text{dan} \quad y_{k+1} = y_{k-1} - q_{k+1} y_k$$

jadi rumus rekursif tersebut berlaku untuk m = 1,2,3,....n

contoh 2.1.9

Cari ppt dari a dan b, dengan a = 2317 dan b = 1904. dengan menggunakan algoritma Euclidean diperoleh :

2317 = 1904 . 1 + 413	0 < 413 < 1904
1904 = 413 . 4 + 252	0 < 252 < 413
413 = 252 . 1 + 161	0 < 161 < 252
252 = 161 . 1 + 91	0 < 91 < 161
161 = 91 . 1 + 70	0 < 70 < 91
91 = 70 . 1 + 21	0 < 21 < 70
70 = 21 . 3 + 7	0 < 7 < 21
21 = 7 . 3 + 0	

Jadi (a , b) = 7

contoh 2.1.10 :

Cari x_o dan y_o dengan $(a,b) = ax_o + by_o$, dengan

$a = 2317$ dan $b = 1904$

Dari *contoh 2.1.9* di dapat $q_1 = 1$, $q_2 = 4$, $q_3 = 1$, $q_4 = 1$, $q_5 = 1$, $q_6 = 1$ $q_7 = 3$.

Dengan menggunakan rumus rekursif (2.5) diperoleh :

$$x_7 = x_5 - q_7x_6 = (x_3 - q_5x_4) - q_7(x_4 - q_6 x_5)$$
$$= (x_1 - q_3x_2) - (q_5 + q_7)(x_2 - q_4x_3) + q_6 q_7(x_3 - q_5x_4)$$
$$= (x_{-1} - q_1x_0) - (q_3 + q_5 + q_7)(x_0 - q_2x_1) +$$
$$[q_4(q_5+q_7)+q_6q_7](x_1 - q_3x_2) - q_5q_6q_7(x_2 - q_4x_3)$$
$$= 1 + [q_2(q_3+q_5+q_7) + q_4(q_5+q_7) + q_6q_7](x_{-1} - q_1x_0)$$
$$- [q_3q_4(q_5+q_7)+q_3q_6q_7+q_5q_6q_7](x_0 - q_2x_1)$$
$$+ q_4q_5q_6q_7(x_1 - q_3x_2)$$
$$= 1 + q_2(q_3+q_5+q_7)+q_4(q_5+q_7) + q_6q_7$$
$$+ [q_2q_3(q_4q_5 + q_4q_7 + q_6q_7) + q_2q_5q_6q_7$$
$$+ q_4q_5q_6q_7](x_{-1} - q_1x_0) - q_3q_4q_5q_6q_7(x_0 - q_2x_1)$$
$$= 1 + q_2(q_3+q_5+q_7)+q_4(q_5+q_7) + q_6q_7$$
$$+ q_2q_3(q_4q_5 + q_6q_7) + q_2q_5q_6q_7 + q_4q_5q_6q_7$$
$$+ q_2q_3q_4q_5q_6q_7(x_{-1} - q_1x_0)$$
$$= 1 + 4(1+1+3) + 1(1+3) + 1.3 + 4.1[1(1+3) + 1.3]$$
$$+ 4.1.1.3 + 1.1.1.3 + 4.1.1.1.1.3$$
$$= 1 + 20 + 4 + 3 + 4.7 + 12 + 3 + 12$$
$$= 83$$

$$y_7 = y_5 - q_7y_6 = (y_3 - q_5y_4) - q_7(y_4 - q_6y_5)$$
$$= (y_1 - q_3y_2) - (q_5 + q_7)(y_2 - q_4y_3) + q_6q_7(y_3 - q_5y_4)$$
$$= (y_{-1} - q_1y_0) - (q_3 + q_5 + q_7)(y_0 - q_2y_1)$$

$$= + [q_4(q_5+q_7)+q_6q_7](y_1+q_3y_2)-q_5q_6q_7(y_2-q_4y_3)$$

$$= - q_1-(q_3+q_5+q_7)+[q_2(q_3+q_5+q_7)+q_4(q_5+q_7)+q_6q_7] \cdot (y_{-1}-q_1y_0)-[q_3q_4(q_5+q_7)+q_3q_6q_7+q_5q_6q_7](y_0-q_2y_1) + q_4q_5q_6q_7\ (y_1-q_3y_2)$$

$$= -q_1-(q_3+q_5+q_7)-q_1[q_2(q_3+q_5+q_7)+q_4(q_5+q_7)+q_6q_7]$$

$$= - q_3q_4(q_5+q_7)-q_3q_6q_7- q_5q_6q_7 + (y_{-1}- q_1y_0) \cdot [q_2q_3q_4(q_5+q_7) + q_2q_3q_6q_7 + q_2q_5q_6q_7 + q_4q_5q_6q_7] \cdot - q_3q_4q_5q_6q_7\ (y_0 -q_2y_1)$$

$$= -q_1-(q_3+q_5+q_7)-q_1[q_2(q_3+q_5+q_7)+q_4(q_5+q_7)+q_6q_7] -q_3q_4(q_5+q_7) - q_3q_6q_7 - q_5q_6q_7 - q_1q_2q_3q_4(q_5+q_7) -q_1q_2q_3q_6q_7 - q_1q_2q_5q_6q_7 - q_1q_4q_5q_6q_7 - q_3q_4q_5q_6q_7 + q_2q_3q_4q_5q_6q_7\ (y_{-1} - q_1y_0)$$

$$= -1 - (1+1+3) - 1[4(1+1+3)+ 1(1+3)+ 1.3]- 1.1(1+3) - 1.1.3 + 1.1.3 - 1.4.1.1(1+3) - 1.4.1.1.3 - 1.4.1.1.3 - 1.1.1.1.3 - 1.1.1.1.3 - 1.4.1.1.1.1.3$$

$$= -1-5-(20+4+3)-4-3-3-16-12-12-3-3-12$$

$$= - 101$$

Definisi 2.1.11 :

Bilangan prima adalah suatu bilangan bulat p yang lebih besar dari pada 1, dan hanya mempunyai dua pembagi positif khusus, yaitu 1 dan p. Sedangkan bilangan komposit adalah suatau bilangan bulat n > 1 yang mempunyai lebih dari dua pembagi positif khusus 1 dan n.

Contoh 2.1.11 :

2 adalah bilangan prima, karena 2 hanya mempunyai dua pembagi positif khusus yaitu 1 dan bilangan itu sendiri. Demikian pula dengan bilangan 3,5,7 adalah prima karena bilangan-bilangan tersebut hanya mempunyai dua pembagi positif yaitu 1 dan bilangan itu sendiri. Sedangkan, bilangan 6 adalah bilangan komposit, karena 6 mempunyai pembagi positif : 1,2,3, dan 6. Demikian pula dengan bilangan 21 adalah bilangan komposit karena 21 mempunyai pembagi positif : 1,3,7 dan 21.

Definisi 2.1.12 :

Dua bilangan bulat a,b dikatakan saling prima relatif jika a dan b mempunyai pembagi persekutuan terbesar (a,b) = 1.

Dan dikatakan pula bahwa a prima terhadap b atau b prima terhadap a.

Contoh 2.1.12 :

2 dan 5 adalah prima relatif , karena (a,b) = 1

Demikian pula dengan 3 dan 7.

Sedangkan 3 dan 6 adalah tidak prima relatif, karena (a,b) = 3. Demikian pula dengan 4 dan 8.

Teorema 2.1.13 :

Jika (a,m) = (b,m) = 1 maka (ab,m) = 1

Bukti :

Karena (a,m) = 1, maka terdapat bilangan bulat x dan y sedemikian sehingga :

$$1 = ax + my$$

Oleh karena itu :

$$b = ab.x + m.by$$

Jadi suatu pembagi dari ab dan m harus membagi b.

Sedangkan m dan b prima relatif. Oleh karena itu

$$(ab, m) = 1$$

Teorema 2.1.14 :

Jika $0 < k < n$ dan $(k,n) = 1$ maka $(n-k,n) = 1$

Bukti :

Misalkan $(n-k,n) = m \neq 1$

Berarti terdapat r_1 dan r_2 , sehingga :

$$m \cdot r_1 = n - k$$

$$m \cdot r_2 = n$$

Jadi

$$k = mr_2 - mr_1$$

$$= m (r_2 - r_1)$$

Sedangkan

$$n = m \cdot r_2$$

Berarti

$$(k,n) = m \neq 1$$

Jadi bertentangan dengan pernyataan tersebut diatas.

Sehingga yang benar adalah (n-k,n) = 1.

Teorema 2.1.15 :

Jika a dan b prima relatif maka terdapat $s,t \in Z$ sehingga berlaku $as + bt = 1$

Bukti :

Bilangan bulat a dan b dikatakan prima relatif jika $(a,b) = 1$. Berdasarkan teorema 2.1.5 dan terdapat $s,t \in Z$ sedemikian sehingga berlaku $as + bt = 1$

Teorema 2.1.16 :

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

Bukti :

Karena $(b,c) = 1$ maka berdasarkan teorema 2.1.7 diperoleh :

$(ab, ac) = a(b,c) = a$

Diketahui $c|ab$ dan jelas bahwa $c|ac$, berarti bahwa c merupakan pembagi persekutuan dari ab dan ac, maka $c|a$.

2.2. Teorema Dasar Ilmu Hitung.

Teorema 2.2.1 :

Setiap bilangan bulat $n > 1$ adalah sebuah bilangan prima atau hasil kali dari dua atau lebih bilangan prima :

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

Dengan $p_1, p_2 \ldots, p_r$ adalah bilangan prima yang berbeda dan

$\alpha_1, \alpha_2, \ldots, \alpha_r$ adalah bilangan asli.

Bukti :

Misalkan n > 1, jika n adalah bilangan prima, maka n dapat ditulis sebagai perkalian faktor tunggal. Jika n bukan bilangan prima, maka terdapat bilangan bulat n_1, n_2 sedemikian sehingga $n = n_1 n_2$ dengan $1 < n_1 < n$ dan $1 < n_2 < n$. Jika n_1 bilangan prima, maka n_1 tidak dapat difaktorkan lagi. Akan tetapi jika n_1 bukan bilangan prima, maka akan terdapat bilangan $1 < n_{11} < n_1$ dan $1 < n_{12} < n_1$ demikian pula untuk n_2.

Jika n_2 bilangan prima, maka n_2 tidak dapat difaktorkan lagi. Akan tetapi jika n_2 bukan bilangan prima maka akan terdapat bilangan bulat n_{21}, n_{22} sedemikian sehingga $n_2 = n_{21}\, n_{22}$ dengan $1 < n_{21} < n_2$ dan $1 < n_{22} < n_2$.

Kemudian hal yang sama dikerjakan terhadap n_{11} dan n_{12} dan seterusnya, sampai setiap bilangan komposit telah dinyatakan sebagai perkalian dari bilangan-bilangan prima. Hasilnya dapat ditulis dalam bentuk :

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

Dengan p_1 , p_2 , p_3 , ... , p_r adalah bilangan prima yang berbeda dan α_1 , α_2 , α_3 , ... , α_r adalah bilangan asli.

Contoh 2.2.1 :

Misalkan n = 2

Karena 2 adalah bilangan prima maka 2 dapat ditulis sebagai faktor tunggal.

Untuk n = 6

Oleh karena 6 bukan bilangan prima maka bilangan 6 dapat dinyatakan sebagai hasil kali bilangan prima yaitu :

$$6 = 2 \cdot 3$$

dan sebagainya.

Teorema 2.2.2. :

Jika p adalah bilangan prima dan $p \mid ab$, maka $p \mid a$ atau $p \mid b$.

Bukti :

Jika $p \mid a$ maka jelas teorema benar.

Misalkan $p \nmid a$, maka akan dibuktikan bahwa p harus habis membagi b. dan jika $p \nmid a$, maka $(p,a) = 1$.

Sehingga terdapat bilangan bulat k,m yang memenuhi :

$$kp + ma = 1 \text{ berarti } kpb + mab = b.$$

Diketahui $p \mid ab$ maka terdapat bilangan bulat q sehingga

$$ab = pq \text{ berarti } kpb + mpq = b$$

atau

$$p(kb + mq) = b$$

Jadi $p \mid b$

Teorema 2.2.2 dapat diperluas menjadi :

Teorema 2.2.3 :

Jika untuk bilangan prima p berlaku $p \mid a_1 . a_2 \ \ldots \ a_n$, maka sedikitnya satu a_i $(i = 1,2,\ldots,n)$ habis dibagi p.

Bukti :

Jika p tidak habis membagi semua $a_i (i = 1,2,3, \ldots , n)$, maka berdasarkan teorema 2.2.2 p tidak habis membagi semua bentuk berikut : a_1a_2, $(a_1a_2)a_3$, $(a_1a_2 \ldots a_{n-1})a_n$

Hal ini bertentangan dengan $p \mid a_1a_2a_3 \ldots a_n$

Teorema 2.2.4 :

Teorema dasar ilmu hitung atau teorema keunikan faktorisasi,

Setiap bilangan bulat $n > 1$ dapat diuraikan dalam faktor-faktor bilangan prima secara unik, kecuali urutan faktornya.

Bukti :

Berdasarkan teorema 2.2.1 setiap bilangan bulat $n > 1$ dapat dinyatakan sebagai $n = p_1p_2p_3 \ldots p_r$ dimana setiap p_i adalah bilangan prima positif. Misalkan $n = q_1q_2 \ldots q_s$ adalah uraian lain dari n dengan setiap q_j adalah bilangan prima positif.

Akan dibuktikan bahwa kedua uraian tersebut adalah sama.

Dari $n = p_1p_2p_3 \ldots p_r$ dan $n = q_1q_2q_3 \ldots q_s$ diperoleh :

$$p_1p_2p_3 \ldots p_r = q_1q_2q_3 \ldots q_s \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Berdasarkan teorema 2.2.3, dari persamaan (1) dapat disimpulkan bahwa q_1 habis membagi salah satu faktor p_i, dengan $i = 1,2,3, \ldots, r$. Misalkan p_1. Sedangkan p_1 adalah bilangan prima, maka $p_1 = q_1$

Sekarang bagi ruas kiri dan ruas kanan persamaan (1) dengan p_1 atau q_1 sehingga diperoleh

$p_2 \ldots p_r = q_2 \ldots q_s$ ..... (2)

Berdasarkan teorema 2.2.3 lagi, dari persaman (2) dapat disimpulkan bahwa q_2 habis membagi salah satu p_i , dengan $i = 2,3,4, \ldots , r$. Misalkan P_2. Sedangkan P_2 adalah bilangan prima, maka $p_2 = q_2$. Bagi ruas kiri dan ruas kanan persamaan (2) dengan p_2 atau q_2 , akan diperoleh :

$p_3 \ldots p_r = q_3 \ldots q_s$

Proses ini dapat diteruskan sampai salah satu ruas dari persamaa (1) sama dengan 1.

Misalkan $S < r$, berarti setelah proses di atas dilakukan S kali, akan diperoleh persamaan

$$p_{S+1}\, p_{S+2} \ldots p_r = 1$$

Hal ini tidak mungkin. Begitu pula tidak mungkin terjadi $S > r$. Jadi haruslah $r = S$ dan setelah proses di atas dilakukan S kali akan diperoleh :

$p_i = q_i$, dengan $i = 1 , 2 , \ldots , S$.

Jadi uraian n dalam faktor-faktor prima adalah unik, kecuali urutan faktornya.

Contoh 2.2.4 :

12545 jika diuraikan dalam faktor-faktor prima menjadi : 5. 13. 193

21 jika diuraikan dalam faktor-faktor prima menjadi $3 \times 7 = 7 \times 3$.

2.3. Kongruensi

Teori kongruensi diperkenalkan oleh : Carl Fredrich

Gauss (1777 - 1855). Salah seorang ahli matematika terbesar. Dia menulis pada umur 24 tahun. Berikut ini akan dijelaskan mengenai sifat dasar kongruensi misalnya :

Ada 2 bilangan bulat a dan b.

Ada bilangan bulat tertentu lainnya yaitu n.

a disebut kongruen dengan b modulo n, jika

(a-b) adalah kelipatan n.

Dinotasikan dengan $a \equiv b$ (modulo n)

Jadi $a \equiv b$ (modulo n) $\Rightarrow a - b = k \cdot n$ (notasi ini dikemukakan oleh Gauss)

Definisi 2.3.1 :

Untuk bilangan bulat positif m dengan $m \neq 0$, bilangan bulat a,b dikatakan kongruen modulo m atau $a \equiv b$ (mod m), jika $m \mid (a-b)$. Jika a dan b tidak kongruen modulo m, maka ditulis $a \not\equiv b$ (mod m).

Contoh 2.3.1 :

Ambil n = 7 , maka :

$3 \equiv 24$ (mod 7) karena 3 - 24 = kelipatan 7.

$-31 \equiv 11$ (mod 7) karena -31 - 11 = kelipatan 7.

$25 \not\equiv 12$ (mod 7) karena 25 - 12 $\neq$ kelipatan 7.

$4 \not\equiv 16$ (mod 7) karena 4 - 26 $\neq$ kelipatan 7.

Berikut ini akan diberikan beberapa sifat kongruensi yang akan digunakan dalam tulisan ini.

Teorema 2.3.2. :

Kongruensi memenuhi sifat :

(1) Jika $a \equiv b \pmod m$, maka $b \equiv a \pmod m$

(2) Jika $a \equiv b \pmod m$ dan $b \equiv c \pmod m$, maka $a \equiv c \pmod m$

(3) Jika $a \equiv b \pmod m$, maka $ka \equiv kb \pmod m$ untuk $k \in Z$.

(4) Jika $a_i \equiv b_i \pmod m$ untuk $i = 1,2,3.....n$, maka

$a_1 + a_2 + ... + a_n \equiv b_1 + b_2 + ... + b_n \pmod m$..... (i)

$a_1 a_2 ... a_n \equiv b_1 b_2 ... b_n \pmod m$ .....(ii)

(5) Jika $ka \equiv kb \pmod m$, maka $a \equiv b \pmod{m/d}$ dimana $d = (k,m)$ atau $a \equiv b \pmod m$, jika k dan m prima relatif, atau $d = 1$.

Bukti :

Sifat (1), (2), (3) jelas.

Untuk pembuktian sifat (4) dipakai induksi matematik :

Untuk $n = 2$,

$a_1 \equiv b_1 \pmod m$ berarti $a_1 - b_1 = k.m$

$a_2 \equiv b_2 \pmod m$ berarti $a_2 - b_2 = r.m$

maka $(a_1 + a_2) - (b_1 + b_2) = (k + r)m$

atau $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

Untuk (ii) :

$a_1 \equiv b_1 \pmod m$ berdasarkan sifat (3) diperoleh

$a_1 a_2 \equiv b_1 a_2 \pmod m$,

$a_2 \equiv b_2 \pmod m$ berdasarkan sifat (3) diperoleh

$b_1 a_2 \equiv b_1 b_2 \pmod m$,

maka berdasarkan sifat (2) diperoleh $a_1 a_2 \equiv b_1 b_2 \pmod m$.

Jadi telah dibuktikan bahwa (i) dan (ii) benar untuk n = 2

Misalkan (i) dan (ii) benar untuk n = k , sehingga

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod m$$

$$a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod m$$

Maka untuk n = k + 1

$a_{k+1} \equiv b_{k+1} \pmod m$ berarti $a_{k+1} - b_{k+1} = t.m$

$a_1 a_2 . \; a_k \equiv b_1 b_2 \ldots b_k \pmod m$ berarti

$(a_1 + a_2 + \ldots + a_k) - (b_1 + b_2 + \ldots + b_k) = sm$,

Maka :

$$(a_1 + a_2 + \ldots + a_k + a_{k+1}) - (b_1 + b_2 + \ldots + b_k + b_{k+1}) = (t+s)m$$

Dengan perkataan lain

$$a_1 + a_2 + \ldots + a_k + a_{k+1} = b_1 + b_2 + \ldots + b_k + b_{k+1} \pmod m$$

Jadi (i) benar pula untuk n = k + 1, untuk (ii) perhatikan hal berikut :

Diketahui $a_{k+1} \equiv b_{k+1} \pmod m$, berdasarkan sifat (3) diperoleh :

$$a_{k+1} (a_1 a_2 \ldots a_k) \equiv b_{k+1} (a_1 a_2 \ldots a_k) \pmod m$$

Dari $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod m$, berdasarkan sifat (3) diperoleh :

$$b_{k+1} (a_1 a_2 \ldots a_k) \equiv b_{k+1} (b_1 b_2 \ldots b_k) \pmod m$$

Maka berdasarkan sifat (2) :

$$a_{k+1} (a_1 a_2 \ldots a_k) \equiv b_{k+1} (b_1 b_2 \ldots b_k) \pmod m$$

atau

$$a_1 a_2 \ldots a_k \, a_{k+1} \equiv b_1 b_2 \ldots b_k b_{k+1} \pmod m$$

Jadi (ii) benar juga untuk n = k + 1.

untuk pembuktian sifat (5), dimulai dari :

ka ≡ kb (mod m), hal ini berarti ka - kb = mx dengan $x \in Z$. jika d = (k,m) maka :

$$k (a-b) = mx$$

$$k/d (a-b) = m/d . x$$

berarti :

$$m/d \mid k/d . (a-b)$$

Tetapi berdasarkan teorema 2.1.8 maka (m/d, k/d) = 1

Sehingga berdasarkan teorema 2.1.16 diperoleh m/d | (a-b)

Jadi a ≡ b (mod m/d)

Definisi 2.3.4 :

Himpunan bilangan bulat S disebut sitem residu lengkap modulo m jika setiap bilangan bulat kongruen modulo m dengan tepat satu anggota dari S.

Teorema 2.3.4 :

Jika m adalah sebuah bilangan bulat positif maka S = { 0,1,2, ... , m-1} merupakan sistem residu lengkap modulo m.

Bukti :

Misalkan m adalah bilangan bulat positif dan S = { 0,1,2, ... ,m-1 }. Setiap bilangan bulat a bila dibagi oleh m akan bersisa satu dari 0, 1, 2, ..., m-1, jadi $a \equiv s_i$ (mod m) untuk $s_i \in s$. Sedangkan untuk s_i, $s_j \in S$ dengan $s_i \not\equiv s_j$ berlaku $s_i \not\equiv s_j$ (mod m), yang berarti setiap anggota S

tidak kongruen dengan anggota S yang lainnya. Maka setiap bilangan bulat akan kongruen modulo m dengan tepat satu anggota dari S. Jadi S sistem residu lengkap modulo m.

Teorema 2.3.5 :

Jika S { a_1, a_2, ..., a_m} merupakan sistem residu lengkap modulo m dan (a,m) = 1, maka :

S_1 = (aa_1, aa_2, ..., aa_m) juga merupakan sistem residu lengkap modulo m.

Bukti :

Jika S { a_1, a_2, ..., a_m} adalah sistem residu lengkap modulo m, maka (a_i,m) = 1, untuk setiap i = 1,2, ..., m. Berdasarkan teorema 2.1.13 (a_i,m) = (a,m) = 1, maka (aa_i,m) = 1, untuk setiap i = 1,2,3, ... , m.

Himpunan S_1 = (aa_1, aa_2, ..., aa_m) mempunyai jumlah anggota yang sama dengan himpunan S. Akan dibuktikan bahwa untuk setiap bilangan bulat b akan kongruen modulo m dengan tepat satu anggota S_1.

Misalkan terdapat i dan j , i ≠ j sedemikian sehingga :

$$\left.\begin{array}{l} b \equiv aa_i \pmod m \\ \text{dan } b \equiv aa_j \pmod m \end{array}\right\} \Rightarrow aa_i \equiv aa_j \pmod m ,$$

maka berdasarkan sifat teorema 2.3.2(5) dan (a,m) = 1, dapat disimpulkan $a_i \equiv a_j \pmod m$. Hal ini bertentangan dengan S yang merupakan sistem residu lengkap modulo m. Sehingga haruslah i = j. Berarti anggota S_i dapat dipasangkan tepat satu-satu dengan anggota S. Jadi S_1 merupakan sistem residu lengkap modula m.

Teorema 2.3.6 :

Jika p adalah bilangan prima dan a adalah bilangan bulat dengan (a,p) = 1 , maka :

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

Bukti :

S = { 0, 1, 2, ... , p-1} merupakan sistem residu lengkap modulo p. Berdasarkan teorema 2.3.5 S_1 = {0, a, 2a, ... , (p-1) a } Juga merupakan sistem residu lengkap modulo p. SEtiap anggota dari S_1 kongruen dengan tepat satu anggota dari S.Berdasarkan sifat teorema 2.3.2. (4) dan teorema 2.3.2. (5)

$$a \times 2a \times \ldots \times (p-1)a \equiv 1 \times 2 \times \ldots \times (p-1) \ (\text{mod } p)$$

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

Akan tetapi ((p-1)! , P) = 1 (karena p merupakan bilangan prima). Maka berdasarkan sifat 2.3.2 (5) $a^{p-1} \equiv 1 \ (\text{mod } p)$

Contoh 2.3.6 :

Ambil bilangan prima p = 5 dan a = 4, sedemikian sehingga (a,p) = 1.

Maka :

$$4^{5-1} = 256 \equiv 1 \ (\text{mod } 5)$$

Akibat Teorema 2.3.7 :

Jika p adalah bilangan prima dan a aalah bilangan bulat, maka :

Bukti :

Berdasarkan teorema 2.3.6, jika p bilangan prima dan (a,p) = 1, akan berlaku :

$$a^{p-1} \equiv 1 \pmod{p}$$

Maka berdasarkan sifat teorema 2.3.2(3) :

$$a \cdot a^{p-1} \equiv a.1 \pmod{p}$$

$$a^{p} \equiv a \pmod{p}$$

Teorema 2.3.8 :

Jika p adalah bilangan prima maka

$$(p-1)! \equiv -1 \pmod{p}$$

Bukti :

Untuk p = 2 atau p = 3 jelas.

Maka pembuktian berikut adalah untuk bilangan prima p > 3. Jika a adalah salah satu bilangan dari 1 , 2, 3, ..., p-1 akan dibuktikan bahwa persamaan $ax \equiv 1 \pmod{p}$ hanya mempunyai tepat satu solusi. Berdasarkan teorema 2.3.5 S = {0, a, 2a, 3a, ... , (p-1)a } juga merupakan suatu sistem residu lengkap modulo p. Berarti bilangan 1 kongruen modulo p dengan tepat satu anggota S berbentuk ax , dengan x adalah salah satu dari 1, 2, 3, ..., p-1. Jadi hanya ada sebuah x yang memenuhi $ax \equiv 1 \pmod{p}$.

Jika x = a , maka :

$$a^{2} \equiv 1 \pmod{p}$$

$$a^{2} - 1 \equiv 0 \pmod{p}$$

Berarti $p \mid (a-1)(a+1)$, sehingga $p \mid (a-1)$ atau $p \mid (a+1)$, akan tetapi p tidak habis membagi (a-1) dan (a+1) kedua - duanya. Maka $a \equiv 1 \pmod{p}$ atau $a \equiv -1 \pmod{p}$.

Karena $1 \leq a \leq (p-1)$ maka $a = 1$ atau $a = p - 1$.

Jadi dari $p - 3$ buah bilangan 2, 3, .., p-2 dapat dibentuk perkalian sebanyak $(p-3)/2$ pasang bilangan a dan x, dengan sifat $ax \equiv 1 \pmod p$ atau

$$2 . 3 . 4 \ldots (p-2) \equiv 1 . 1 . 1 \ldots 1 \pmod p$$

Atau :

$$1.2.3.4 \ldots (p-2)(p-1) \equiv (p-1) \pmod p, \text{ atau :}$$

$$(p-1)! \equiv (p-1) \pmod p, \text{ sedangkan}$$

$$(p-1) \equiv -1 \pmod p$$

$$\text{maka } (p-1)! \equiv -1 \pmod p$$

Akibat teorema 2.3.9 :

Jika p adalah bilangan prima dengan bentuk $4m + 1$,

Maka : $p \mid (n^2 + 1)$ dengan $n = (2m)!$.

Bukti :

Perhatikan himpunan bilangan berikut :

$A = \{ -1, -2, \ldots, -2m\}$

$B = \{ 4m, 4m - 1, \ldots, 2m + 1\}$

Terlihat bahwa masing-masing himpunan mempunyai 2m anggota dan setiap $a \in A$ ada satu $b \in B$ sedemikian sehingga berlaku :

$b - a = p$, maka $a \equiv b \pmod p$

Sehingga :

$$4m.(4m - 1) \ldots (2m + 1) \equiv (-1).(-2)\ldots(-2m) \pmod p$$

Tetapi :

$(2m)! \equiv (2m)! \pmod p$

Jadi :

$$4m.(4m-1)...(2m+1).(2m)! \equiv (-1)(-2)...(-2m)(\tau m)!(\text{mod } p)$$

$$(4m)! \equiv \{(2m)!\}^2 \pmod p$$

Berdasarkan teorema (2.3.8) :

$(4m)! = (p-1)! \equiv -1 \pmod p$

Misalkan $n = (2m)!$

Maka $n^2 \equiv -1 \pmod p$

atau :

$p \mid (n^2 + 1)$.

Teorema 2.3.10 :

Jika p adalah bilangan prima dan a,b bilangan bulat maka : $a^p + b^p \equiv (a+b)^p \pmod p$

Bukti :

Berdasarkan teorema 2.3.6 $c^p \equiv c \pmod p$, $c \in Z$.

Ambil $c = a+b$, maka $(a+b)^p \equiv (a+b) \pmod p$

Karena $a^p \equiv a \pmod p$, $b^p \equiv b \pmod p$, maka

$a^p + b^p \equiv (a+b)^p \pmod p$

2.4. Fungsi Multiplikatif

Definisi 2.4.1 :

Suatu fungsi f yang didefinisikan untuk bilangan bulat positif dikatakan multiplikatif jika

$f(m.n) = f(m) \cdot f(n)$ apabila $(m,n) = 1$

Teorema 2.4.2 :

Jika $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ merupakan uraian dalam bilangan prima berpangkat dari n dengan $\alpha_i > 0$, dan $p_i \neq p_j$ untuk $j \neq i$, maka

Banyaknya pembagi dari n adalah :

$$\tau(n) = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots(\alpha_k+1) \quad \ldots\ldots\ldots(i)$$

dan

Jumlah semua pembagi dari n adalah :

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \quad \ldots\ldots(ii)$$

Bukti :

Untuk (i) perhatikan himpunan

$$D=\{ d = p_1^{\beta_1} p_2^{\beta_1} \cdots p_k^{\beta_k} : 0 \leq \beta_i \leq \alpha_i , i = 1,2,\ldots,k\}$$

Jika $d \in D$, maka d merupakan pembagi dari n , sebab terdapat :

$$e = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \cdots p_k^{\alpha_k-\beta_k}$$

Sehingga :

$$d.e = n$$

Sebaliknya, jika d merupakan pembagi dari n, maka untuk setiap bilangan prima p,

bila p pembagi d maka akan membagi n.

Jadi terdapat $\gamma_1, \gamma_2, \ldots \gamma_k$ dengan $0 \leq \gamma_i \leq \alpha_i$

dengan i = 1,2, ..., k.

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

Ini berarti bahw d $\in$ D. Jadi D adalah himpunan dari semua pembagi dari n. Sedangkan banyaknya elemen di D adalah

$$(\alpha_1+1)\ (\alpha_2+1)\ (\alpha_3+1)\ldots(\alpha_k+1)$$

maka banyaknya pembagi dari n adalah :

$$\tau\ (n) = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots\ (\alpha_k+1)$$

Membuktikan (ii) setara dengan membuktikan

$$\sigma(n) = (1+p_1+\ldots+p_1^{\alpha_1})(1+p_2+\ldots+p_2^{\alpha_2})\ \ldots\ (1+p_k+\ldots+p_k^{\alpha_k})$$

Jika ruas kanan dari persamaan di atas dikalikan akan diperoleh suku banyak yang setiap sukunya berbentuk

$$p_1^{\beta 1}\ p_2^{\beta 2}\ \ldots p_k^{\beta k}$$

Dengan $0 < \beta_i < \alpha_i$, i = 1, 2, ..., k Dan himpunan semua suku tersebut adalah himpunan D, maka jumlah semua pembagi dari n adalah :

$$\sigma\ (n) = (1 + p_1 + \ldots\ldots+p_1^{\alpha_1})\ (\ 1 + p_2 + \ldots\ldots+p_2^{\alpha_2})$$
$$\ldots\ldots\ldots\ldots\ (\ 1 + p_k + \ldots\ldots+p_k^{\alpha_k})$$

atau

$$\sigma\ (n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\quad \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\ \ldots\ldots\ \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Teorema 2.4.3 :

$\tau\ (n)$ dan $\sigma\ (n)$ bersifat multiplikatif

Bukti :

Misal m dan n adalah bilangan yang prima relatif. Maka tidak ada pembagi m yang dapat membagi n, demikian pula sebaliknya . Jadi jika :

$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ dan $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_5^{\beta_r}$ .....(*)

masing-masing adalah uraian bilangan prima berpangkat dari m dan n , maka tidak ada q_i yang merupakan p_j dan tidak ada p_j yang merupakan q_i. Dan uraian dari mn adalah :

$$m.n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\beta_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_5^{\beta_r} \quad \dots\dots\dots \quad (**)$$

maka :

$$\tau(mn) = \{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)\}\{(\beta_1+1)(\beta_2+1)\dots(\beta_r+1)\}$$

$$= \tau(m)\,\tau(n)$$

Dan berdasarkan teorema 2.4.2 dari (*) diperoleh :

$$\gamma(m) = \frac{p_2^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}}{p_k-1}$$

$$\sigma(n) = \frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} \cdots \frac{q_r^{\beta_r+1}-1}{q_r-1}$$

Dari (**) diperoleh :

$$\sigma(mn) = \frac{p_2^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_k^{\alpha_k+1}}{p_k-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} \cdots \frac{q_r^{\beta_r+1}-1}{q_r-1}$$

Jadi $\sigma(mn) = \sigma(m) \cdot \sigma(n)$

Teorema 2.4.4 :

Jika f multipliktif dan tidak identik sama dengan nol, maka f(1) = 1

Bukti :

Jika f tidak identik sama dengan nol, maka harus ada suatu bilangan bulat n sedemikian sehingga f(n) = 0.

$$f(n) = f(1,n) = f(1).f(n)$$

Karena $f(n) \neq 0$, maka dengan membagi kedua sisi dari persamaan tersebut dengan f(n) diperoleh :

$$f(1) = 1$$

Teorema 2.4.5 :

Jika $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ adalah uraian bilangan prima berpangkat dari n, dimana n adalah bilangan bulat positif. Jika f multiplikatif maka :

$$f(n) = f(p_1^{\alpha_1}) \; f(p_2^{\alpha_2}) \; \ldots \; f(p_k^{\alpha_k})$$

Bukti :

Akan dibuktikan dengan menggunakan induksi matematik pada k untuk k = 1, jelas benar.

Anggap benar untuk k = r.

Karena :

$$(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, p_{r+1}^{\alpha_r + 1}) = 1$$

daridefinisi fungsi multiplikatif, didapat :

$$f((p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}) p_{r+1}^{\alpha_{r+1}})) = f(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}) f(p_{r+1}^{\alpha_{r+1}})$$

Dariasumsi induksi, faktor pertama adalah

$$f(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f(p_r^{\alpha_r})$$

maka:

$$f((p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}) p_{r+1}^{\alpha_{r+1}})) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f p_r^{\alpha_r}) f(p_{r+1}^{\alpha_{r+1}})$$

Jadi terbukti bahwa :

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f(p_k^{\alpha_k})$$

Berlaku untuk setiap bilangan asli k.