TEORI BILANGAN

Oleh

DRA. ISNA MAIZURNA
DRA. SRI ELNIATI

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
INSTITUT KEGURUAN DAN ILMU PENDIDIKAN
PADANG
1995

KATA PENGANTAR

Puji dan syukur penulis panjatkan pada Yang Maha Kuasa karena atas rahmatNya jualah penulis dapat menyelesaikan buku ini yang berjudul "TEORI BILANGAN".

Buku ini dapat di pergunakan sebagai buku terks pada mata kuliah Teori Bilangan. Tetapi buku ini juga mudah dimengerti bagi pembaca yang berminat mengetahui tentang bilangan. Sebetulnya tidak ada prasyarat untuk mempelajari buku ini, tentu saja minat dalam matematika akan sangat menunjang dalam mempelajarinya.

Pada buku ini disajikan definisi-definisi dari teori yang dibicarakan dan juga teorema-teorema serta beberapa akibat dari teorema beserta buktinya. Beberpa contoh soal juga dihadirkan untuk memperjelas teori. Pada akhir setiap bab diberikan soal-soal yang pemecahannya berdasarkan pada teorema, definisi dan akibat yang telah diuraikan sebelumnya.

Akhirnya kami berharap, semoga saja buku ini ada manfaatnya bagi pembaca sekalian dan juga berguna bagi pengembangan ilmu terutama matematika.

Penulis

April 1995

DAFTAR ISI

BAB I

BILANGAN BULAT

I.1. PRINSIP INDUKSI MATEMATIKA

Prinsip induksi matematika sangat penting peranannya untuk membuktikan hasil-hasil yang berkenaan dengan bilangan bulat. Pada bagian ini akan kita perkenalkan prinsip induksi matematika dan cara penggunaannya. Kemudian, dengan menggunakan prinsip terurut rapi dari bilangan bulat akan ditunjukkan bahwa teknik-teknik pada prinsip induksi matematika adalah valid. Dalam mempelajari teori bilangan, akan digunakan kedua prinsip diatas yaitu prinsip induksi matematika dan prinsip terurut rapi secara berulang-ulang.

Teorema 1.1. (Prinsip Induksi Matematika)

Jika sebuah himpunan bilangan bulat positif memuat 1, dan untuk setiap bilangan bulat positif n, himpunan tersebut juga memuat n + 1 jika memuat n, maka himpunan tersebut adalah himpunan bilangan bulat positif.

Bukti

Misalkan S himpunan semua bilangan bulat positif yang memuat 1 dan memuat n + 1 bila S memuat n.

Andaikan S bukan himpunan semua bilangan bulat positif

Maka terdapat beberapa bilangan bulat positif yang tidak termuat di S.

Menurut sifat terurut rapi, karena himpunan semua bilangan bulat positif tidak termuat di S, maka terdapat bilangan bulat positif dan lebih kecil dari n dan $n - 1 \in S$.
Sekarang karena $n > 1$, maka bilangan $n - 1$ adalah bulat positif dan lebih kecil dari n dan $n - 1 \in S$.
Karena S memuat $n - 1$, maka S harus memuat $(n - 1) + 1 = n$ yang mengakibatkan kontradiksi dengan pengandaian bahwa n bilangan bulat positif terkecil yang tidak di S.
Jadi S haruslah himpunan semua bilangan bulat positif

Jadi untuk membuktikan dengan menggunakan prinsip induksi matematika, ada dua langkah yang perlu dilakukan yaitu :

1. Pernyataan adalah benar untuk bilangan bulat 1
   langkah ini disebut langkah dasar
2. Untuk setiap bilangan bulat positif n, harus ditunjukkan bahwa pernyataan benar untuk bilangan bulat positif $n + 1$, jika pernyataan benar untuk bilangan bulat positif n.

   Langkah ini disebut langkah induktif.

Setelah kedua langkah diatas dilengkapi maka menurut prinsip induksi matematika dapat disimpulkan bahwa pernyataan benar untuk semua bilangan bulat positif.

Contoh 1.1.1.

Akan dibuktikan bahwa $n ! \leq n^n$ untuk setiap bilangan bulat positif n.

Dengan menggunakan prinsip induksi matematika.

Langkah dasar :

Kasus $n = 1 : 1 ! = 1 \leq 1^1 = 1$

Jadi pernyataan benar untuk $n = 1$

Langkah induktif

Sekarang andaikan pernyataan benar untuk n

Yaitu $n ! \leq n^n$. Ini disebut hipotesis induktif.

Untuk melengkapi bukti, dengan menggunakan hipotesis induktif akan dibuktikan :

$$(n + 1) 1 \leq (n + 1)^{n+1}$$

Pandang $(n + 1) !$

$$\begin{aligned} (n + 1) ! &= (n + 1) n ! \\ &\leq (n + 1) n^n \\ &< (n + 1) (n + 1)^n \\ &\leq (n + 1)^{n+1} \end{aligned}$$

Dan bukti selesai.

Teorema 1.2. PRINSIP INDUKSI MATEMATIKA KEDUA

Sebuah himpunan bilangan bulat positif yang memuat 1, dan yang mempunyai sifat bahwa untuk setiap bilangan positif n, jika himpunan tersebut memuat semua bilangan bulat positif 1,2 . . . , n, maka himpunan itu memuat n + 1, maka himpunan tersebut adalah himpunan semua bilangan bulat positif.

Bukti :

Misalkan T adalah himpunan bilangan bulat positif yang memuat 1, dan untuk setiap bilangan bulat positif n,

Jika T memuat 1,2, ... , n maka T memuat n + 1.

Misalkan S adalah himpunan semua bilangan bulat positif n sedemikian sehingga semua bilangan bulat positif ≤ n termuat di T.

Maka 1 ϵ S dan menurut hipotesis,

Jika n ϵ S maka n + 1 ϵ S

Menurut prinsip induksi matematika, S haruslah himpunan semua bilangan bulat positif.

Dan juga jelas bahwa T adalah himpunan semua bilangan bulat positif karena S ⊆ T.

Prinsip induksi matematika mengembangkan sebuah metoda untuk mendefinisikan nilai-nilai dari sebuah fungsi pada bilangan bulat positif. Sebagai ganti pendefinisian nilai fungsi secara eksplisit di n, diberikan nilai fungsi pada 1 dan diberikan aturan untuk menentukan nilai fungsi di n + 1, dari nilai fungsi di n untuk setiap bilangan bulat positif n.

Definisi :

Dikatakan fungsi f terdefinisi secara rekursif jika nilai f di 1 tertentu dan jika untuk setiap n, terdapat aturan untuk menentukan f(n+1) dari f(n).

Contoh 1.1.2.

Akan didefinisikan secara rekursif fungsi faktorial f(n)= n!

Pertama, tentukan f (1) yaitu f (1) = 1

Kemudian buat aturan untuk menentukan f (n + 1) dan f (n),

yaitu :

$f(n+1) = (n+1)\, f(n)$

Kedua pernyataan ini secara tunggal mendefinisikan n !

Contoh 1.1.3

Barisan Fibonacci $f_1, f_2, \ldots, fn$ terdefinisi secara rekursif oleh :

$f_1 = 1$, $f_2 = 1$ dan $fn = f_{n-1} + f_{n-2}$ untuk $n \geq 3$

Dari definisi dapat dilihat :

$f_3 = f_1 + f_2 = 1 + 1 = 2$

$f_4 = f_3 + f_2 = 2 + 1 = 3$

$f_5 = f_4 + f_3 = 3 + 2 = 5$

$f_6 = f_5 + f_4 = 5 + 3 = 8$ dst.

Contoh 1.1.4.

Buktikan bahwa $fn > \left[\frac{(1 + \sqrt{5})}{2} \right]^{n-2}$

Bukti :

Untuk membuktikan soal diatas dapat digunakan

PRINSIP INDUKSI MATEMATIKA KEDUA SEBAGAI BERIKUT :

Untuk $n = 3$, $F_3 = 2 > \left[\frac{1 + \sqrt{5}/2}{2} \right]^{3-1} = \frac{1 + \sqrt{5}}{2}$

Untuk $n = 4$, $f_4 = 3 > \frac{3 + \sqrt{5}}{2} = \left[\frac{1 + \sqrt{5}}{2} \right]^{4-2}$

Jadi pernyataan benar untuk n = 3 dan n = 4

Andaikan $f_k > \left(\frac{1 + \sqrt{5}}{2} \right)^{k-2}$ untuk semua k dengan $k \leq n$

Maka $f_{k+1} = f_k + f_{k-1} > \left(\frac{1 + \sqrt{5}}{2} \right)^{k-2} + \left(\frac{1 + \sqrt{5}}{2} \right)^{k-3}$

$$= \left(\frac{1 + \sqrt{5}}{2} \right)^{k-3} \left\{ 1 + \frac{1+\sqrt{5}}{2} \right\}$$

$$= \left(\frac{1 + \sqrt{5}}{2} \right)^{k-3} \left(\frac{3 + \sqrt{5}}{2} \right)$$

$$= \left(\frac{1 + \sqrt{5}}{2} \right)^{k-3} \left(\frac{1 + \sqrt{5}}{2} \right)^{2}$$

$$= \left(\frac{1 + \sqrt{5}}{2} \right)^{k-1}$$

Juga pernyataan benar untuk n = k+1

Jadi $f_n > \left(\frac{1 + \sqrt{5}}{2} \right)^{n-2}$ untuk $n \geq 3$

1.2. KETERBAGIAN

Apabila sebuah bilangan bulat dibagi oleh bilangan bulat tak nol lainnya, maka hasil bagi bisa bilangan bulat, bisa juga tidak merupakan bilangan bulat.

Misalnya 24/8 = 3 adalah bilangan bulat, sedangkan 17/5 = 3.4 bukan bilangan bulat. Untuk itu dipunyai definisi berikut.

DEFINISI :

Jika a dan b adalah bilangan-bilangan bulat dengan a $\neq$ 0, kita katakan a membagi b jika terdapat sebuah bilangan c sedemikian sehingga b = ac.

Jika a membagi b, dikatakan juga bahwa a pembagi dari b atau a sebuah faktor dari b.

Jika a membagi b, maka dituliskan a|b dan jika a tidak membagi b maka dituliskan a $\nmid$ b.

Contoh 1.2.1

13 | 182 karena 182 = 13. 14 dan

- 5 | 30 karena 30 = -5. 6.

Tetapi 6 $\nmid$ 44 karena tidak ada bilangan bulat c yang memenuhi 44 = 6. c.

Juga 7 $\nmid$ 50.

Teorema 1.2.1

Jika a, b dan C adalah bilangan-bilangan bulat dengan a|b dan b|c, maka a|c.

Bukti :

Jika a|b dan b|c maka ada bilangan-bilangan bulat e dan f dengan ae = b dan bf = c

Jadi c = bf

= a (ef) untuk ef bilangan bulat

Jadi a|c.

Teorema 1.2.2

Jika a, b, m dan n adalah bilangan-bilangan bulat dan jika c|a dan c|b maka c |(ma + nb)

Bukti :

Karena c|a dan c|b maka terdapat bilangan-bilangan bulat e dan f sehingga

a = cc dan b = cf

Dan ma + nb = mce + ncf

= c (me + nf)

Akibatnya c | (ma + nb)

Contoh 1.2.2

Karena 11 | 66 dan 66 | 198 maka 11 | 198

Contoh 1.2.3

Karena 3 | 21 dan 3 | 33 maka 3 | 5.21 - 3.33 = 6

Teorema 1.2.3 (Algoritma Pembagian)

Jika a dan b bilangan-bilangan bulat sedemikian sehingga b > 0, maka terdapat secara tunggal bilangan-bilangan bulat q dan r sehingga a = bq + r dimana 0 ≤ r < b

Bukti :

Pandang S = Himpunan semua bilangan bulat yang berbentuk a - bk dimana k bilangan bulat

Yaitu S = $\{ a - bk \ / \ ke \ Z \}$

Misalkan T adalah semua himpunan bilangan bulat tak negatif di S. Disini T ≠ Ø, karena a-bk > 0 untuk k X a/b.

Menurut sifat terurut rapi, T mempunyai elemen terkecil sebut $r = a - bq$

Kita tahu bahwa $r \geq 0$ dan $r < b$

Karena jika $r > b$ maka $r > r - b = a - bq - b$

$= a - b(q + 1) \geq 0$

Yang kontradiksi dengan pemilihan $r = a - bq$ adalah bilangan bulat tak negatif terkecil yang berbentuk $a - bk$ jadi

$0 \leq r < b$

Untuk menunjukkan bahwa q dan r tunggal,

andaikan ada q_1, q_2 dan r_1, r_2 yang memenuhi

$a = bq_1 + r_1$ dan $a = bq_2 + r_2$dimana $0 \leq r_1 < b$ dan

$0 \leq r_2 < b$

Dengan memperkurangkan kedua persamaan diatas diperoleh

$0 = b(q_1 - q_2) + r_1 - r_2$ atau $r_2 - r_1 = b(q_1 - q_2)$

yang berarti $b \mid r_2 - r_1$

Karena $0 \leq r_1 < b$ dan $0 \leq r_2 < b$

diperoleh $-b < r_2 - r_2 < b$

Disini $b \mid r_2 - r_1$ jika dan hanya jika $r_2 - r_1 = 0$

atau $r_2 = r_1$

Dan karena $bq_1 + r_1 = bq_2 + r_2$ dan $r_1 = r_2$

maka diperoleh $q_1 = q_2$

Ini menunjukkan bahwa hasil bagi q dan sisa r adalah tunggal.

Definisi :

Jika sisa dari n bila dibagi dengan 2 adalah 0, maka n = 2 k untuk suatu bilangan bulat positif k dan dikatakan n genap.

Dan jika sisa dari n bila dibagi dengan dua adalah 1, maka n = 2k + 1 untuk suatu bilangan bulat positif k dan dikatakan n ganjil.

Contoh 1.2.4

Jika a = 133 dan b = 21 maka q = 6 dan r = 7

karena 133 = 21. 6 + 7

Contoh 1.2.5

Misalkan a = 1028 dan b = 34

Maka a = bq + r dengan $0 \leq r < b$ akan

memberikan $b = \left\lfloor \frac{1028}{34} \right\rfloor = 30$

dan r = 1028 - 30 . 34 = 8

Soal-soal

1. Buktikan bahwa : jika n adalah bilangan bulat positif $\geq$ 10 maka $(2n)! < \frac{2^{2n}}{5} (n!)^2$

2. Misalkan H_n adalah jumlah partial ke n dari deret harmonik

$$\sum_{j=1}^{n} \frac{1}{j}$$

Gunakan induksi untuk membuktikan bahwa :

(a) $H_{2^n} \geq 1 + \frac{n}{2}$, $n \geq 1$

(b) $H_{2^n} \leq 1 + n$, $n \geq 1$

3. Buktikan : $\sum_{j=1}^{n} f_j^2 = f_n f_{n+1}$, $n \geq 1$

dimana f_n adalah suku ke n dari barisan Fibonacci.

4. Dengan menggunakan induksi matematika, buktikan :

(a). $10^n + 3 \cdot 4^{n+2} + 5$ dapat dibagi oleh 9, $n \geq 0$

(b). $2^{5n} + 3 \cdot 5^n - 5$ dapat dibagi oleh 24, $n \geq 0$

5. Gunakan induksi matematika untuk membuktikan :

(a). $f_1 + f_2 \ldots + f_n = f_{n+2} - 1$ untuk $n \geq 1$

(b). $f_n^2 + f_{n-1} f_{n+1} = (-1)^{n-1}$ untuk $n \geq 2$

6. Gunakan induksi matematika atau cara lain untuk membuktikan :

(a). $a^n - b^n$ habis dibagi oleh a - b jika n bilangan bulat positif.

(b). $a^n - b^n$ habis dibagi oleh a + b jika n bilangan positif ganjil.

(c). $a^n - b^n$ habis dibagi oleh a - b jika n bilangan positif genap.

7. Buktikan :

(a). Jika $b \mid a$ maka $|b| \leq |a|$

(b). Jika $a \mid b$ maka $a^k \mid b^k$ dimana k adalah bilangan asli

(c). Jika $ab \mid bc$ dan $b \neq 0$ maka $a \mid c$.

8. Andaikan $a \mid b$ dan $c \mid d$. Buktikan atau beri contoh penyangkalan untuk setiap pernyataan berikut.

(a). $(a + c) \mid (b + d)$

(b). $ac \mid bd$

(c). Jika $a \mid bc$ maka $a \mid b$ atau $a \mid c$.

BAB II

PEMBAGI PERSEKUTUAN TERBESAR DAN FAKTOR PRIMA

2.1. PEMBAGI PERSEKUTUAN TERBESAR.

Jika a dan b adalah bilangan-bilangan bulat, yang tidak keduanya 0, maka himpunan pembagi persekutuan dari a dan b adalah sebuah himpunan hingga dari bilangan-bilangan bulat yang selalu memuat 1 dan -1. Berikut ini akan dipelajari bilangan bulat terbesar dari pembagi persekutuan dua bilangan bulat.

Defenisi :

Pembagi persekutuan terbesar dari dua bilangan bulat a dan b, yang tidak keduanya nol adalah bilangan bulat terbesar yang membagi a dan b.

Pembagi persekutuan terbesar dari a dan b dituliskan dengan (a,b). Dan juga didefinisikan (0,0) = 0.

Contoh 2.1.1

(24,84) = 12

(15,81) = 3

(100,5) = 5

(17,25) = 1

(0,44) = 44

(-6,15) = 3

(-17,289) = 17

Definisi :

Bilangan-bilangan bulat a dan b dikatakan relatif prima jika pembagi persekutuan terbesar dari a dan b adalah 1 yakni (a,b) = 1

Contoh 2.1.2

Karena (25 , 42) = 1 maka 25 dan 42 adalah relatif prima.

Teorema 2.1.1

Misalkan a , b dan c adalah bilangan-bilangan bulat dengan (a,b) = d. Maka

(i) (a|d , b|d) = 1

(ii) (a + cb , b) = (a,b)

Bukti :

(i) Misalkan (a,b) = d

Dan andaikan (a|d , b|d) = c

Maka terdapat bilangan-bilangan bulat k dan l sedemikian sehingga :

a|d = k.c dan b|d = l c

Atau a = k. cd dan b = l. cd

Disini cd adalah pembagi persekutuan dari a dan b.Dan karena d adalah pembagi persekutuan terbesar maka haruslah cd ≤ d

jadi haruslah c = 1

(a|d , b|d) = 1

(ii) Akan dibuktikan (a + cb , b) = (a,b)

Misalkan (a,b) = c

Maka menurut teorema 1.2.2 , c | a + cb

Jadi c adalah pembagi persekutuan dari a + cb dan b.

Disini c = (a,b) ≤ (a + cb , b) ... (1)

Sekarang misalkan f = (a + cb , b)

Kembali menurut teorema 1.2.2, f | a = (a+cb- cb)

Jadi f adalah pembagi persekutuan dari a dan b

Jadi f = (a + cb , b) ≤ (a,b) ... (2)

Dari (1) dan (2) di peroleh :

(a,b) = (a + cb , b).

Selanjutnya akan dibuktikan bahwa pembagi persekutuan terbesar dari bilangan-bilangan bulat a dan b, tidak keduanya nol, dapat dituliskan sebagai jumlah dari perkalian a dan b.

Definisi :

Jika a dan b adalah bilangan-bilangan bulat, maka sebuah kombinasi linier dari a dan b adalah sebuah penjumlahan yang berbentuk ma + nb dimana m dan n adalah bilangan-bilangan bulat.

Teorema 2.1.2

Pembagi persekutuan terbesar dari bilangan-bilangan bulat a dan b, tidak keduanya nol adalah bilangan bulat positif terkecil dari kombinasi linier a dan b.

Bukti :

Misalkan d adalah bilangan bulat positif terkecil dari kombinasi linier a dan b.

Kita tulis d = ma + nb dimana m dan n adalah bilangan-bilangan bulat.

Akan ditunjukkan bahwa d|a dan d|b.

Dengan algoritma pembagian diperoleh :

$a = dq + r , 0 \leq r < d$

Atau

$r = a - dq = a - q (ma + nb)$

$= (1 - qm) a - qnb$

Disini r adalah kombinasi linier dari a dan b

Karena $0 \leq r < d$ dan d adalah bilangan bulat positif terkecil yang merupakan kombinasi linier dari a dan b maka haruslah r = 0.

Jadi $d \mid a$

Dan dengan cara yang sama dapat ditunjukkan bahwa $d \mid b$.

Dan d merupakan pembagi persekutuan dari a dan b.

Selanjutnya akan ditunjukkan bahwa d adalah pembagi persekutuan terbesar dari a dan b.

Misalkan $c \mid a$ dan $c \mid b$

Maka menurut teorema 1.2.2,

$c \mid ma + nb = d$

Jadi d adalah pembagi persekutuan terbesar dari a dan b

Definisi :

Misalkan $a_1, a_2 \ldots , a_n$ adalah bilangan-bilangan bulat yang tidak semuanya nol. Pembagi persekutuan terbesar dari bilagan-bilangan bulat ini adalah bilanngan bulat terbesar yang merupakan pembagi dari ke semua bilangan bulat tersebut, dan dilambangkan dengan $(a_1, a_2, \ldots , a_n)$.

Contoh 2.1.2

$(12 , 18 , 30) = 6$

$(10 , 15 , 25) = 5$

Lemma 2.1.3

Jika $a_1 , a_2 , \ldots , a_n$ adalah bilangan-bilangan bulat yang tidak semuanya nol maka

$(a_1 , a_2 , \ldots , a_n) = (a_1 , a_2 , \ldots , a_{n-2} , (a_{n-1} , a_n))$

Contoh 2.1.3

$(105 , 140 , 350) = (105 , (140 , 350))$

$= (105 , 70)$

$= 35.$

Definisi

Bilangan-bilangan bulat $a_1 , a_2 , \ldots , a_n$ dikatakan saling relatif prima jika $(a_1 , a_2 , \ldots , a_n) = 1$.

Dan dikatakan relatif prima berpasangan jika untuk

setiap sepasang bilangan bulat a_i dan a_j , dari himpunan diatas, $(a_i , a_j) = 1$, yaitu setiap pasangan bilangan bulat adalah relatif prima.

Contoh 2.1.4

Bilangan-bilangan bulat 15 , 21 , 35 adalah saling relatif prima karena $(15 , 21, 35) = (15 , (21,35))$

$= (15 , 7)$

$= 1$

Tetapi tidak relatif prima berpasangan karena

$(15 , 21) = 3$, $(15 , 35) = 5$ dan $(21 , 35) = 7$

2.2. ALGORITMA EUCLID

Selanjutnya akan dikembangkan sebuah metoda yang sistematik untuk mencari pembagi persekutuan terbesar dari dua bilangan bulat. Metoda ini disebut Algoritma Euclid, yang dinamakan sesuai dengan nama penemunya yaitu Euclid seorang matematikawan Yunani.

Teorema 2.2.1. Algoritma Euclid

Misalkan $r_0 = a$ *dan* $r_1 = b$ *adalah bilangan-bilangan bulat sedemikian sehingga* $a \geq b > 0$. *Jika algoritma pembagi dapat digunakan untuk memperoleh* $r_j = r_{j+1} q_{j+1} + r_{j+2}$ *dimana* $0 < r_{j+2} < r_{j+1}$

untuk $j = 0, 1, 2, \ldots, n-2$ *dan* $r_{n+1} = 0$, *maka*

$(a,b) = r_n$ *yaitu sisa terakhir yang tak nol.*

Dari teorema diatas dapat dilihat bahwa pembagi persekutuan terbesar, dari a dan b adalah sisa terakhir yang tak nol dari barisan persamaan yang diperoleh dengan menggunakan algoritma pembagi secara terus menerus sampai diperoleh sisa 0. Untuk membuktikan Algoritma Euclid, diperlukan Lemma berikut.

Lemma 2.2.2

Jika c dan d adalah bilangan-bilangan bulat dan

c = dq + r dimana q dan r bilangan-bilangan bulat.

Maka (c,d) = (d,r)

Bukti :

Jika sebuah bilangan bulat e membagi c dan d, maka karena r = c - dq , e membagi r (menurut teorema 1.2.2)

Jika e | d da e | r, maka karenna c = dq + r , e | c

Karena pembagi persekutuan dari c dan d sama dengan pembagi persekutuan dari d dan r, maka (c,d) = (d,r).

Selanjutnya kita buktikan Algoritma Euclid

Bukti : (Algoritma Auclid)

Misalkan r_0 = a dan r_1 = b adalah bilangan-bilangan bulat positif dengan a $\geq$ b

Dengan menggunakan algoritma pembagian diperoleh :

$r_0 = r_1 q_1 + r_2 \quad , \quad 0 \leq r_2 < r_1$

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

$r_{j-2} = r_{j-1} r_{j-1} + r_j \quad , \quad 0 \leq r_j < r_{j-1}$

$r_{n-4} = r_{n-3} q_{n-3} + r_{n-2} \quad , \quad 0 \leq r_{n-2} < r_{n-3}$

$$r_{n-3} = r_{n-2}\, q_{n-2} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}\, q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n\, q_n.$$

Dapat di asumsikan bahwa akhirnya diperoleh sisa nol karena barisan $a = r_0 > r_1 > r_2 > \ldots \geq 0$ tidak akan memuat lebih dari a suku.

Dari lemma 2.2.2, diperoleh :

$(a,b) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$.

Jadi disini $(a, b) = r_n$ yaitu sisa yang terakhir yang tidak nol.

Contoh 2.2.1

Untuk menentukan (252 , 198) dapat digunakan algoritma pembagian sebagai berikut :

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18$$

Jadi $(252, 198) = 18$

Pembagi persekutuan terbesar juga dapat digunakan untuk menentukan eksistensi solusi bilanga bulat dari persamaan $ax + by = n$ seperti dinyatakan pada teorema berikut ini.

Teorema 2.2.3

Persamaan $ax + by = n$ mempunyai solusi bilangan bulat jika dan hanya jika $(a , b) \mid n$

Bukti :

Jika n = 0 , maka ax + by = 0 dan

(0,0) adalah sebuah solusi trivial dan (a , b) | 0

Sekarang andaikan $n \neq 0$

(=>) Andaikan (a , b) | ax + by

Maka ax + by = n tidak akan punya solusi

Kecuali bila (a , b) | n

(<=) Andaikan (a , b) | n

Andaikan $n = (a , b) \mid n_o$

Maka terdapat bilangan-bilangan bulat x_o dan y_o sedemikian sehingga

$(a , b) = a x_o + b y_o$

Dengan demikian :

$n = (ax_o + by_o) n_o = ax_o n_o + b y_o n_o$

Disini $x = x_o n_o$ dan $y = y_o n_o$

adalah sebuah solusi.

Contoh 2.2.2

Tentukan sebuah solusi dari persamaan

533 x + 117 y = 65

Penyelesaian

Dengan menggunakan Algoritma Euclid diperoleh :

533 = 117 . 4 + 65

$$117 = 65 \cdot 1 + 52$$

$$65 = 52 \cdot 1 + 13$$

$$52 = 13 \cdot 4$$

Jadi (533 , 117) = 13 dan 13 | 65

Maka menurut teorema 2.2.3, persamaan

533 x + 117 y = 65 mempunyai sebuah solusi.

Untuk menentukan solusi dari persamaan tersebut, gunakan substitusi mundur dari algoritma Euclid sebagai berikut :

$$13 = 65 - 52$$

$$= 65 - (117 - 65)$$

$$= 65 \cdot 2 - 117$$

$$= (533 - 117 \cdot 4) \cdot 2 - 117$$

$$= 533 \cdot 2 - 117 \cdot 9$$

Jadi : $533 \cdot 2 - 117 \cdot 9 = 13$

Kalikan persamaan diatas dengan 5 di peroleh :

$533 \cdot 10 - 117 \cdot 45 = 65$

Disini x = 10 dan y = - 45 adalah

Sebuah solusi dari 533 x + 117 y = 65.

SOLUSI UMUM DARI PERSAMAAN ax + by = n, $n \neq 0$

Jika (x_0 , y_0) adalah sebuah solusi dari persamaan ax + by = n dan (x , y) adalah solusi lainnya, maka jelas bahwa

$$\frac{y - y_0}{x - x_0} = \frac{-a}{b} = \frac{-a / (a,b)}{b / (a,b)}$$

Atau $x - x_0 = \frac{bt}{(a,b)}$ dan $y - y_0 = \frac{-at}{(a,b)}$

Untuk suatu bilangan bulat t. Disini, sebarang bilangan bulat t memberikan suatu solusi.

2.3. FAKTORISASI TUNGGAL

Definisi :

Sebuah bilangan asli kecuali 1 disebut bilangan prima apabila bilangan tersebut hanya dapat dibagi oleh bilangan itu sendiri dan 1.

Bilangan-bilangan prima yang terkecil adalah 2,3,5,7,11,13, ... 2 adalah satu-satunya bilangan prima yang genap.

Definisi :

Sebuah bilangan asli yang bukan merupakan bilangan prima disebut bilangan komposit.

Misalkan n adalah sebarang bilangan asli selain dari 1. Maka pembagi terkecil dari n (selain 1) haruslah sebuah bilangan prima, sebut p_1. Jika $n \neq p_1$ maka n / p_1 adalah sebuah bilangan bulat > 1.

Dengan demikian terdapat bilangan prima yang lebih kecil yang membagi n / p_1 (boleh saja $p_2 = p_1$).

Jika $n \neq p_1 p_2$, maka terdapat bilangan prima terkecil yang membagi bilangan bulat $n / p_1 p_2$ dan sterusnya.

Setelah sejumlah hingga langkah, diperoleh :

$$n / p_1 p_2 \ldots p_m = 1$$

Atau $n = p_1 p_2 \ldots p_m$

Dengan mengelompokkan bilangan prima - bilangan prima yang sama diperoleh :

$$n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$$

dimana p_1 , p_2 , .. p_k adalah bilangan prima - bilangan prima yang berbeda dan i_1 , i_2 , ... $i_k \in N$.

$p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ disebut dekomposisi kanonik dari n.

Teorema 2.3.1 (TEOREMA DASAR ARITMETIKA)

Dekomposisi kanonik dari sebuah bilangan asli n ada dan tunggal (terhadap urutan faktornya) dalam arti sebuah bilangan asli tidak dapat difaktorkan dalam lebih dari satu bentuk yang benar-benar berbeda.

Bukti :

Eksistensi dari dekomposisi kanonik telah dilengkapi oleh definisi sebelumnya.

Bukti ketunggalan :

Andaikan ada dua dekomposisi kanonik untuk n yaitu :

$$n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$$
$$= q_1^{j_1} q_2^{j_2} \dots q_e^{j_e}$$

dimana p_m, q_n adalah bilangan prima

Untuk setiap m , $1 \le m \le k$, diperoleh

$$p_m \mid q_1^{j_1} q_2^{j_2} \dots q_e^{j_e}$$

Dan karena (p_m-q) = 1 untuk semua prima kecuali p_m maka :

$$p_m \mid q_t^{i_t} \text{ untuk suatu } t , 1 \le t \le l$$

Karena p_m dan q_t keduanya adalah bilangan prima maka $p_m = q_t$

Disini setiap bilangan prima yang ada pada $p_1^{i_1}$ $p_2^{i_2}$ ... $p_k^{i_k}$ juga ada pada $q_1^{j_1}$ $q_2^{j_2}$ ... $q_l^{j_l}$.

Dengan demikian k = l dan dekomposisi kanonik yang kedua dapat dituliskan sebagai : $n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$

Sehingga $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$

Sekarang andaikan $\alpha_t > i_t \; \forall \; t = 1,2, \dots , k$

maka bilangan bulat $\dfrac{n}{p_t^{\,i_t}}$ mempunyai dua komposisi yaitu

$n = p_1^{i_1} p_2^{i_2} \dots p_{t-2}^{i_{t-1}} p_{t+1}^{i_{t+1}} \dots p_k^{i_k}$

$= p_1^{\alpha_1} \dots p_t^{(\alpha_t - i_t)} \dots p_k^{i_k}$

Dekomposisi kedua memuat bilangan prima p_t, tetapi dekomposisi yang pertama tidak. Hal ini kontradiksi dengan penyataan sebelumnya.

Jadi $\alpha_t = i_t$ untuk setiap t.

Dengan menggunakan teorema diatas, dapat diturunkan suatu formula untuk pembagi persekutuan terbesar dalam bentuk faktor prima.

Definisi :

Misalkan $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha i}$

$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta i}$

Maka $(a , b) = \prod_{i=1}^{k} p_i^{\min(\alpha i, \beta i)}$

Contoh 2.3.2

$24 = 2^3 \cdot 3$

$180 = 2^2 \cdot 3^2 \cdot 5$

Maka $(24, 180) = 2^2 \cdot 3$

2.4. HASIL KALI PERSEKUTUAN TERKECIL

Definisi :

Hasil kali persekutuan terkecil dari a dan b, dilambangkan dengan hpt (a,b) atau [a,b], adalah bilangan bulat positif terkecil yang habis dibagi oleh a dan b.

Contoh : 2.4.1

(2 4 , 180) = 360 karena $24 \mid 360$ dan $180 \mid 360$

Definisi :

Jika $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$ dan

$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i}$

(dimana α_i, B_i dapat juga nol)

Maka $[a,b] = \prod_{i=1}^{k} p_i^{\text{maks}\,(\alpha_i,\beta_i)}$

Sifat-sifat dari hasil kali persekutuan terkecil

(i) $[a,b] = \frac{|ab|}{(a,b)}$

(ii) jika $a \mid m$ dan $b \mid m$ maka $[a,b] \mid m$

(iii) $[a, b, c] = [a, [b,c]]$

(iv) $[a_1\ a_2 \ldots a_n] = [a_1, [a_2, \ldots, a_{n-1}, a_n]]$

Teorema 2.4.1. (Teorema Euclid)

Terdapat tak terhingga banyaknya bilangan prima.

Bukti :

Andaikan bilangan prima terhingga banyaknya.

Andaikan terdapat n bilangan prima sebut $p_2, p_2, \ldots, p_n$.

Pandang bilangan $m = p_1 p_2 \ldots p_n + 1$

Sekarang , m bisa merupakan bilangan prima atau m bilangan komposit.

Jika m bilangan komposit, maka m harus dapat dibagi oleh salah satu bilangan prima $p_1, p_2, \ldots, p_n$

hal ini tidak mungkin karena apabila m dibagi oleh p_1 atau $p_2 \ldots$ atau p_n akan menghasilkan sisa satu.

Jadi m adalah bilangan prima

Jadi terdapat tak terhingga banyaknya bilangan prima.

Lemma 2.4.2

Misalkan $a > 1$ dan $c > 0$

Maka $a^c - 1$ adalah bilangan komposit jika

$a > 2$ atau c adalah bilangan komposit.

Bukti :

$a^c - 1$ habis dinagi oleh $a - 1$

jadi jika $a > 2$ maka $a^c - 1$ adalah bilangan komposit.

Juga, jika c adalah komposit, maka dapat dituliskan $c = d\ e$ dimana $d > 1$, $e > 1$

Sehingga :

$$a^c - 1 = a^{de} - 1$$
$$= (a^e)^d - 1$$

Yang habis dibagi oleh $a^e - 1$ dan $a^e - 1 \neq 1$

Karena $a > 1$ dan $e > 1$.

Definisi :

Bilangan $M_n = 2^n - 1$ disebut bilangan Marsenne.

Menurut lemma 2.4.2, bilangan Marsenne M_n adalah bilangan kompisit apabila n adalah bilangan komposit. Dan jika p bilangan prima maka M_p kadang-kadang juga bilangan prima dan disebut bilangan prima Marsenne seperti :

$M_2 = 2^2 - 1 = 3$ adalah bilangan prima

$M_3 = 2^3 - 1 = 7$ adalah bilangan prima

Juga M_5 , M_7 , M_{11} , M_{17}, M_{19} semuanya adalah bilangan prima.

Lemma 2.4.3

Misalkan $a > 1$ dan $c > 1$

maka $a^c + 1$ adalah bilangan komposit jika a adalah bilangan ganjil atau jika c mempunyai faktor ganjil.

Bukti :

Misalkan a bilangan ganjil, katakan $a = 2_k + 1$

Untuk k suatu bilangan bulat

Maka $a^c + 1 = (2k + 1)^c + 1$

$$= (2k)^c + \binom{c}{1} 2k^{c-1} + \binom{c}{2} 2k^{c-2} + \ldots + 2_k + 1 + 1$$

$$= \left[2k \right]^c + \binom{c}{1} 2k^{c-1} + \ldots + 2k + 2$$

Yang habis dibagi oleh 2

Jadi $a^c + 1$ adalah bilangan kompisit.

Sekarang misalkan c mempunyai faktor ganjil

Misalkan $c = (2k + 1)\, d$

Maka $a^c + 1 = (a^d)^{2k+1} + 1$ habis dibagi oleh $a^d + 1$

Jadi disini $a^c + 1$ juga bilangan komposit.

Definisi :

Bilangan $F_n = 2^{2n-1} + 1$ disebut bilangan Fermat.

Teorema 2.4.3. (Teorema Dirichlet)

Sebarang ungkapan aritmatika ($a + n_b$) dimana (a,b) = 1, memuat tak terhingga banyaknya bilangan prima.

Kasus khusus dari teorema Dirichlet ini dapat dituliskan sebagai teorema berikut ini.

Soal-soal

1. Tentukan pembagi persekutuan terbesar dari setiap pasangan bulat berikut :

   (a) (15 , 35) (b) (0 , 111)

   (c) (99 , 100) (d) (100 . 102)

2. Buktikan bahwa (a,b) = (a , b + ka) untuk setiap bilangan bulat k

3. Misalkan n adalah bilangan bulat positif

   (a) Apakah (n , 2n) ?

   (b) Apakah (n , n^2) ?

   (c) Apakah (n , n + 1) ?

   (d) apakah (n , n + 2) ?

4. Buktikan : Jika a dan b adalah bilangan-bilangan bulat yang tidak keduanya nol dan c adalah bilangan bulat yang tak nol maka (ca , cb) = $|c|$(a,b)

5. Buktikan bahwa jika a dan b adalah dua bilangan bulat sedemikian sehingga (a,b) = 1 maka (a + b , a - b) = 1 atau 2

6. Buktikan bahwa jika a,b dan c adalah bilangan-bilangan bulat sedemikian sehingga (a,b) = 1 dan c | a + b maka (c,a) = (c,b) = 1

7. Buktikan bahwa jika a, b dan c saling relatif prima maka (a, bc) = (a,b) (a,c)

8. Gunakan Algoritma Euclid untuk menentukan :

   (a) (666 , 1414)

   (b) (20785 . 44350)

   (c) (981 , 1234)

(d) (34709 . 100313)

9. Gunakan Algoritma Euclid untuk membuktikan :

   (f_n , $f_n + 1$) = 1 , dimana f_n adalah suku ke n dari barisan Fibonacci

10. (a) Tentukan bilangan-bilangan bulat x dan y sedemikian sehingga 95 x + 432 y = 1

    (b) Tentukan bilangan-bilangan bulat x , y dan z sedemikian sehingga 35 x + 55 y + 77 z = 1

11. Tentukan solusi umum dari persamaan-persamaan berikut :

    (a) 2072 x + 1813 y = 2849

    (b) 117 x + 54 y = 203

12. Tentukan semua solusi dari persamaan :

    19 x + 20 y = 1909 , $x \geq 0$, $y \geq 0$

BAB III

KONGRUENSI

3.1. PENDAHULUAN

Istilah kongruensi yang akan dibicarakan pada bab ini, banyak kegunaannya dalam teori bilangan. Istilah ini diperkenalkan pada awal abad ke 19 oleh Karl Friedrich Qauss, seorang matematikawan yang terkenal pada zamannya. Berikut ini diberikan definisi dari kongruensi itu sendiri.

Definisi :

Misalkan m adalah sebuah bilangan bulat. Dan jika a dan b adalah bilangan-bilangan bulat, dikatakan a kongruen dengan b modulo m jika $m \mid a - b$.

Jika a kongruen modulo m dengan b, maka dituliskan $a \equiv b \pmod{m}$. Jika $m \nmid (a - b)$, maka dituliskan $a \not\equiv \pmod{m}$ dan dikatakan a dan b tidak kongruen modulo m.

Contoh 3.1.1

$22 \equiv 4 \pmod{9}$ karena $9 \mid 22 - 4 = 18$

$3 \equiv -6 \pmod{9}$ karena $9 \mid 3 - (-6) = 9$

$200 \equiv 2 \pmod{9}$ karena $9 \mid 200 - 2 = 198$

$13 \not\equiv 5 \pmod{9}$ karena $9 \nmid 13 - 5 = 8$

Kongruensi sering kali muncul dalam kehidupan sehari-hari. Misalnya pada kerja jam, digunakan modulo 12 dan 24 untuk jam, dan modulo 6 untuk menit dan detik. Pada

kalender, kita memakai modulo 7 untuk hari-hari dalam seminggu, modulo 12 untuk bulan.

Dalam bekerja dengan kongruensi, kita sering kali perlu menterjemahkannya ke dalam persamaan. Untuk itu, diperlukan teorema berikut :

Teorema 3.1.1

Jika a dan b adalah bilangan-bilangan bulat, maka $a \equiv b \pmod m$ *jika dan hanya jika terdapat suatu bilangan bulat k sedemikian sehingga* $a = b + km$.

Bukti :

($\Rightarrow$) Jika $a \equiv b \pmod m$ maka $m \mid a - b$ yang berarti terdapat sebuah bilangan bulat k sedemikian sehingga $a - b = km$ atau $a = b + km$

($\Leftarrow$) Sebaliknya, jika terdapat sebuah bilangan bulat k dengan $a = b + km$.

Maka $a - b = km$

Yaitu $m \mid a - b$ atau $a \equiv b \pmod m$

Contoh 3.1.2

$19 \equiv -2 \pmod 7$ < > $19 = -2 + 3 \cdot 7$

Teorema 3.1.2

Misalkan m bilangan bulat positif

Maka kongruensi modulo m adalah suatu relasi

ekivalensi yaitu suatu relasi yang memenuhi :

(i) Sifat refleksif :

Jika a bilangan bulat, maka a ≡ a (mod m)

(ii) Sifat symetri

Jika a dan b bilangan bulat dengan a ≡ b (mod m) maka b ≡ a (mod m)

(iii) Sifat transitif

Jika a , b , dan c bilangan-bilangan bulat dengan a ≡ b (mod m) dan b ≡ c (mod m)

Maka a ≡ c (mod m)

Bukti :

(i) Jika a ≡ a (mod m) karena m | a - a = 0

(ii) Jika a ≡ b (mod m) maka m | a - b

Jadi terdapat bilangan bulat k sehingga a - b = km atau b -a = (-k) m

Jadi terdapat bilangan bulat (-k) sedemikian sehingga b - a = -k . m. Yaitu m | b - a

jadi b ≡ a (mod m)

(iii) Jika a ≡ b (mod m) maka m | a - b

Yaitu terdapat k_1 sedemikian sehingga a - b = k_1 m atau a = b + k_1 m.

Dan jika b ≡ c (mod m) maka m | b - c

Yaitu terdapat k_2 sedemikian sehingga b - c = k_2 m atau b = c + k_2 m.

Jadi $a = b + k_1 m$

$= c + k_2 m + k_1 m$

$= c + (k_2 + k_1) m$

Atau $a - c = (k_2 + k_1) m$

Atau $m \mid a - c$

Jadi $a \equiv c \pmod m$

Dari teorema 3.1.2 dapat dilihat bahwa himpunan bilangan dibagi menjadi m himpunan yang berbeda yang disebut dengan kelas kongruensi modulo m, masing-masing himpunan memuat bilangan-bilangan bulat yang saling kongruen modulo m.

Contoh 3.1.3

4 kelas kongruensi modulo 4 adalah sebagai berikut :

$\ldots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \ldots \pmod 4$

$\ldots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \ldots \pmod 4$

$\ldots \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots \pmod 4$

$\ldots \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv \ldots \pmod 4$

Andaikan m sebuah bilangan bulat positif, dan diberikan sebuah bilangan bulat a , dengan menggunakan algoritma pembagian diperoleh $a = bm + r$ dimana $0 \leq r \leq m - 1$. Kita katakan r adalah sisa tak negatif terkecil dari a mod m dan dinotasikan dengan $r = a \bmod m$ yang menyatakan bahwa r adalah sisa yang diperoleh bila a dibagi dengan m.

Contoh 3.1.4

17 mod 5 = 2

-8 mod 7 = 6

Jadi dari persamaan $a = bm + r$, diperoleh $a \equiv r \pmod{m}$ Disini setiap bilangan bulat adalah kongruen modulo m dengan salah satu bilangan-bilangan bulat 0, 1, .., m-1 yaitu sisa dari bilangan tersebut apabila dibagikan dengan m.

Definisi :

Sebuah sistem lengkap dari residu modulo m adalah sebuah himpunan bilangan bulat sedemikian sehingga setiap bilangan bulat kongruen modulo m dengan salah satu bilangan bulat pada himpunan tersebut.

Contoh 3.1.5

Himpunan bilangan-bilangan bulat { 0,1,2, ..., m-1 } adalah sebuah sistem lengkap residu modulo m dan disebut residu tak negatif terkecil modulo m.

Contoh 3.1.6

Misalkan m bilangan positif ganjil

Maka himpunan bilangan-bilangan bulat

$$-\frac{m-1}{2}, \frac{-m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$$

disebut himpunan mutlak terkecil residu modulo m, dan adalah sebuah sistem lengkap residu modulo m.

Teorema 3.1.3

jika a, b, c dan m adalah bilangan-bilangan bulat dengan

$m > 0$ sedemikian sehingga $a \equiv b \pmod m$

Maka : (i) $a + c \equiv b + c \pmod m$

(ii) $a - c \equiv b - c \pmod m$

(iii) $ac \equiv bc \pmod m$

Bukti :

(i) Karena $a \equiv b \pmod m$ maka $m \mid a - b$

Dan kita tahu bahwa $a - b = (a + c) - (b + c)$

jadi $m \mid a - b = (a + c) - (b + c)$

Jadi $a + c \equiv (b + c) \pmod m$

(ii) Juga $a - b = (a - c) - (b - c)$

Sehingga bila $m \mid a - b$ maka $m \mid (a - c) - (b - c)$

Jadi $a - c \equiv bc \pmod m$

(iii) Diketahui bahwa $ac - bc = (a - b)c$

Karena $m \mid a - b$ maka $m \mid (a - b)c$

Jadi $ac \equiv bc \pmod m$

Contoh 3.1.7

Karena $19 \equiv 3 \pmod 8$, maka menurut teorema 3.1.3

$26 = 19 + 7 \equiv 3 + 7 \equiv 10 \pmod 8$

$15 = 19 - 4 \equiv 3 - 4 \equiv -1 \pmod 8$

$38 = 19 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod 8$

Contoh 3.1.8

Diketahui bahwa $14 = 7 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \pmod 6$

tetapi $7 \equiv 4 \pmod 6$

Contoh diatas menunjukkan bahwa kongruensi mempertahankan operasi pembagian dengan bilangan bulat. Walaupun demikian, teorema berikut menyatakan kongruensi bila kedua ruas dibagi oleh bilangan bulat yang sama.

Teorema 3.1.4.

Jika a, b, c dan m adalah bilangan-bilangan bulat dimana $m > 0$, $d = (c , m)$ dan $ac \equiv bc \pmod m$ maka $a \equiv b \pmod{m/d}$

Bukti :

Jika $ac \equiv bc \pmod m$ maka $m \mid ac - bc = (a - b)c$

Yaitu terdapat sebuah bilangan bulat k sedemikian sehingga $(a - b)c = km$

Dengan membagi kedua ruas dengan d diperoleh $c/d\,(a - b) = k\,(m/d)$

Karena $(c/d , m/d) = 1$ maka $m/d \mid a - b$

Jadi $a \equiv b \pmod{m/d}$

Contoh 3.1.9

Karena $50 \equiv 20 \pmod{15}$ dan $(10 , 15) = 5$

maka $5 \equiv 2 \pmod{15/5}$

$\equiv 2 \pmod 3$

Akibat 3.1.5

Jika a, b, c dan m adalah bilangan-bilangan bulat dengan m > 0 dan (c , m) = 1 dan ac ≡ bc (mod m) maka a ≡ b (mod m)

Contoh 3.1.10

Karena 42 ≡ 7 (mod 5) dan (5 , 7) = 1

maka 6 ≡ 1 (mod 5)

Teorema 3.1.6

Jika a, b, c, d dan m adalah bilangan-bilangan bulat dengan m > 0 dan a ≡ b (mod m) , c ≡ d (mod m) maka :

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

(ii) $a - c \equiv b - d \pmod{m}$

(iii) $ac \equiv bd \pmod{m}$

Bukti :

Karena a ≡ b (mod m) dan c ≡ d (mod m) maka berarti bahwa m | a - b dan m | c - d yaitu terdapat bilangan-bilangan bulat k dan l yang memenuhi a - b = km dan c - d = lm.

(i) Untuk membuktikan (i) diturunkan langsung dari kesamaan

(a + c) - (b + d) = (a - b) + (c - d)

= km + lm

= (k + l) m