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 $n = 1$: $1 ! = 1 \le 1^1 = 1$

Jadi pernyataan benar untuk $n = 1$

Langkah induktif

Sekarang andaikan pernyataan benar untuk n

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

Untuk melengkapi bukti, dengan menggunakan hipotesis induktif akan dibuktikan :

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

Pandang $(n + 1) !$

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

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 $\leq$ n termuat di T.

Maka 1 $\in$ S dan menurut hipotesis,

Jika n $\in$ S maka n + 1 $\in$ 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 $\subseteq$ 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, ... , fn terdefinisi secara rekursif oleh :

$f_1 = 1,\ f_2 = 1$ dan $f_n = f_{n-1} + f_{n-2}$ 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 $f_n > \left[\dfrac{(1 + \sqrt{5})}{2}\right]^{n-2}$

Bukti :

Untuk membuktikan soal diatas dapat digunakan PRINSIP INDUKSI MATEMATIKA KEDUA SEBAGAI BERIKUT :

Untuk $n = 3$, $F_3 = 2 > \left(\dfrac{1 + \sqrt{5}/2}{2}\right)^{3-1} = \dfrac{1 + \sqrt{5}}{2}$

Untuk $n = 4$, $f_4 = 3 > \dfrac{3 + \sqrt{5}}{2} = \left(\dfrac{1 + \sqrt{5}}{2}\right)^{4-2}$

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 $k \leq n$

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

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

$13 \mid 182$ karena $182 = 13.\ 14$ dan

$-5 \mid 30$ 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 $c \mid (ma + nb)$

Bukti :

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

$a = ce$ dan $b = cf$

Dan $ma + nb = mce + ncf$

$= c (me + nf)$

Akibatnya $c \mid (ma + nb)$

Contoh 1.2.2

Karena $11 \mid 66$ dan $66 \mid 198$ maka $11 \mid 198$

Contoh 1.2.3

Karena $3 \mid 21$ dan $3 \mid 33$ maka $3 \mid 5.21 - 3.33 = 6$

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 $0 \le r < b$

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 $T \ne \emptyset$, karena $a\text{-}bk > 0$ 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 $0 \le r < b$ akan

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

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

(b). $2 >^n + 3. 5^n - 5$ 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 $|b| \le |a|$

(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 $cd \leq d$

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 , $c \mid a + cb$

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

Disini $c = (a,b) \leq (a + cb, b)$ ... (1)

Sekarang misalkan $f = (a + cb, b)$

Kembali menurut teorema 1.2.2, $f \mid a = (a+cb- cb)$

Jadi f adalah pembagi persekutuan dari a dan b

Jadi $f = (a + cb, b) \leq (a,b)$ ... (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 $d \mid a$ dan $d \mid b$.

Dengan algoritma pembagian diperoleh :

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

Atau

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

$\quad = (\ 1 - qm\ )\ a - qnb$

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 ... , 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, ... , a_n).

Contoh 2.1.2

(12 , 18 , 30) = 6

(10 , 15 , 25) = 5

Lemma 2.1.3

Jika a_1 , a_2 , ... , 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

$$\begin{aligned}(105 , 140 , 350) &= (105 , (140 , 350)) \\ &= (105 , 70) \\ &= 35.\end{aligned}$$

Definisi

Bilangan-bilangan bulat a_1 , a_2 , ... , a_n dikatakan saling relatif prima jika (a_1 , a_2 , ... , 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 $e \mid d$ da $e \mid r$, maka karenna $c = dq + r$, $e \mid c$

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 :

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

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

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

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

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

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

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

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 $(a, b) \mid 0$

Sekarang andaikan $n \neq 0$

$(\Rightarrow)$ Andaikan $(a, b) \nmid ax + by$

Maka $ax + by = n$ tidak akan punya solusi

Kecuali bila $(a, b) \mid n$

$(\Leftarrow)$ Andaikan $(a, b) \mid n$

Andaikan $n = (a, b) \mid n_0$

Maka terdapat bilangan-bilangan bulat x_0 dan y_0 sedemikian sehingga

$(a, b) = a x_0 + b y_0$

Dengan demikian :

$n = (ax_0 + by_0) n_0 = ax_0 n_0 + b y_0 n_0$

Disini $x = x_0 n_0$ dan $y = y_0 n_0$

adalah sebuah solusi.

Contoh 2.2.2

Tentukan sebuah solusi dari persamaan

$533x + 117y = 65$

Penyelesaian

Dengan menggunakan Algoritma Euclid diperoleh :

$533 = 117 \cdot 4 + 65$

$$117 = 65 \cdot 1 + 52$$
$$65 = 52 \cdot 1 + 13$$
$$52 = 13 \cdot 4$$

Jadi $(533, 117) = 13$ dan $13 \mid 65$

Maka menurut teorema 2.2.3, persamaan

$533x + 117y = 65$ mempunyai sebuah solusi.

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

$$\begin{aligned} 13 &= 65 - 52 \\ &= 65 - (117 - 65) \\ &= 65 \cdot 2 - 117 \\ &= (533 - 117 \cdot 4) \cdot 2 - 117 \\ &= 533 \cdot 2 - 117 \cdot 9 \end{aligned}$$

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 $533x + 117y = 65$.

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

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_n, q_n adalah bilangan prima

Untuk setiap m , $1 \leq m \leq k$, 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 :

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

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 : $n = p_1^{l_1}\ p_2^{l_2}\ \ldots\ p_k^{l_k}$

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

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

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

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

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

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

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

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

Contoh 2.3.2

$24 = 2^3 . 3$

$180 = 2^2 . 3^2 . 5$

Maka $(24 , 180) = 2^2 . 3$

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 $24 | 360$ dan $180 | 360$

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

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

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

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

Teorema 2.4.1. (Teorema Euclid)

Terdapat tak terhingga banyaknya bilangan prima.

Bukti :

Andaikan bilangan prima terhingga banyaknya.

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

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

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

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

hal ini tidak mungkin karena apabila m dibagi oleh p_1 atau $p_2 \dots$ 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 $a \not\equiv$ mod 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 $a \equiv b$ $(\bmod m)$ jika dan hanya jika terdapat suatu bilangan bulat k sedemikian sehingga $a = b + km$.

Bukti :

$(\Rightarrow)$ Jika $a \equiv b \ (\bmod m)$ maka $m|a - b$ 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 $a \equiv b \ (\bmod m)$

Contoh 3.1.2

$$19 \equiv -2 \ (\bmod 7) \iff 19 = -2 + 3 \cdot 7$$

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 $a \equiv a \pmod{m}$

(ii) Sifat symetri

Jika a dan b bilangan bulat dengan $a \equiv b \pmod{m}$ *maka* $b \equiv a \pmod{m}$

(iii) Sifat transitif

Jika a , b , dan c bilangan-bilangan bulat dengan $a \equiv b \pmod{m}$ *dan* $b \equiv c \pmod{m}$

Maka $a \equiv c \pmod{m}$

Bukti :

(i) Jika $a \equiv a \pmod{m}$ karena $m \mid a - a = 0$

(ii) Jika $a \equiv b \pmod{m}$ maka $m \mid a - b$

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

Jadi terdapat bilangan bulat $(-k)$ sedemikian sehingga $b - a = -k \cdot m$. Yaitu $m \mid b - a$

jadi $b \equiv a \pmod{m}$

(iii) Jika $a \equiv b \pmod{m}$ maka $m \mid a - b$

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

Dan jika $b \equiv c \pmod{m}$ maka $m \mid b - c$

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 $0 \le r \le m - 1$. 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

$17 \bmod 5 = 2$

$-8 \bmod 7 = 6$

Jadi dari persamaan $a = bm + r$, diperoleh $a \equiv r (\bmod m)$ 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 $\{ 0,1,2, \ldots, m-1 \}$ 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 $ac \equiv bc \pmod{m}$ maka $a \equiv b \pmod{m}$

Contoh 3.1.10

Karena $42 \equiv 7 \pmod{5}$ dan (5 , 7) = 1

maka $6 \equiv 1 \pmod{5}$

Teorema 3.1.6

Jika a, b, c, d dan m adalah bilangan-bilangan bulat dengan m > 0 dan $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ 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 $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka berarti bahwa $m \mid a - b$ dan $m \mid c - d$ 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

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= km + lm \\ &= (k + l) m\end{aligned}$$

Jadi disini $m \mid (a + c) - (b + d)$

atau $a + c \equiv b + d \pmod{m}$

(ii) Dan (iii) dapat dibuktikan dengan cara yang sama dengan menggunakan kesamaan-kesamaan :

$(a - c) - (b - d) = (a - b) - (c - d)$ dan

$ac - bd = ac - bc + bc - bd$

Teorema 3.1.7

Jika a, b, k dan m adalah bilangan-bilangan bulat dimana $k > o$, $m > o$ dan $a \equiv b \pmod{m}$ maka $a^k \equiv b^k \pmod{m}$

Bukti :

Untuk pembuktian teorema ini dapat digunakan prinsip induksi matematika dan teorema 3.1.6.

Dan diserahkan pada pembaca sebagai latihan.

Teorema 3.1.8 (TEOREMA KECIL FERMAT)

Jika a adalah bilangan asli dan p bilangan prima maka $ap \equiv a \pmod{p}$

Bukti :

Untuk pembuktian teorema ini dapat digunakan prinsip induksi matematika pada a.

Untuk $a = 1$, $a^P \equiv 1 \pmod{P}$

Andaikan $a^P \equiv a \pmod{p}$ untuk $a \leq n$

Pandang $a = n + 1$

Maka menurut teorema binomial

$$a^p = (n + 1)^p = n^p + \binom{p}{1} n^{p-1} + \ldots + \binom{p}{p-1} n + 1$$

Dan setiap koefisien binomial $\binom{p}{r}$ habis dibagi oleh p .

$$\begin{aligned} \text{Jadi } (n + 1)^p &\equiv n^p + 1 \pmod{p} \\ &\equiv n + 1 \pmod{p} \\ &(\text{karena } n^p \equiv n \pmod{p}) \end{aligned}$$

dan bukti selesai .

Kasus-kasus dari teorema ini adalah :

$a^{p-1} \equiv 1 \pmod{p}$ jika $(a , p) = 1$, akibat langsung dari teorema 3.1.5.

Contoh 3.1.11

Tentukan $3^{201} \pmod{11}$

Penyelesaian :

Menurut fermat teorema :

$$3^{10} \equiv 1 \pmod{11}$$

$$\begin{aligned} 3^{201} = (3^{10})^{20} &\equiv 1^{20} \pmod{11} \\ &\equiv 1 \pmod{11} \end{aligned}$$

Jadi $3^{201} = 3 \pmod{11}$

Definisi :

Misalkan n bilangan asli dan misalkan $\emptyset (n)$ melambangkan banyaknya bilangan bulat t sedemikian sehingga :

(i) $1 \leq t \leq n$

(ii) $(t , n) = 1$

Maka fungsi $\emptyset : \mathbb{N} \longrightarrow \mathbb{N}$ disebut fungsi Euler atau fungsi $\emptyset$.

Misalnya $\emptyset(1) = 1$; $(1 , 1) = 1$

$\emptyset(2) = 1$; $(1 , 2) = 1$

$\emptyset(10) = 4$ karena $(1 , 10) = 1$, $(3 , 10) = 1$, $(7 , 10) = 1$ $(9 , 10) = 1$

dan $\emptyset(p) = p - 1$, p bilangan prima

Teorema 3.1.9 (teorema Euler)

Jika $(a , m) = 1$ maka $a^{\emptyset(m)} \equiv 1 \pmod m$

Kasus khusus dari teorema Euler

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

Ini juga merupakan kasus khusus dari teorema kecil fermat.

Pada tahun 1770, Wilson mengemukakan bahwa jika p bilangan prima, maka

$$\frac{(p - 1)! + 1}{p}$$ adalah sebuah bilangan bulat

atau $(p - 1)! + 1$ habis dibagi oleh p atau juga

$(p - 1)! = 2 \equiv -1 \pmod p$.

Teorema 3.1.10 (Teorema Wilson)

Jika p bilangan prima, maka $(p - 1)! \equiv -1 \pmod{p}$

Bukti :

Mudah untuk melihat untuk p = 2 dan 3

$p = 2$, $(2 - 1)! = 1 \equiv -1 \pmod{2}$

$p = 3$, $(3 - 1)! = 2 \equiv -1 \pmod{3}$

Andaikan $p \geq 5$ adalah bilangan prima jika $2 \leq a \leq p - 2$

Maka terdapat a^1 secara tunggal dengan $0 \leq a^1 < p$ sedemikian sehingga $aa^1 \equiv 1 \pmod{p}$

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

(kasus khusus teorema fermat)

Maka a^{p-2} akan menempati posisi a^1 atau mewakili kelas kongruensinya yaitu antara 0 dan $p - 1$.

Lebih khusus lagi, $a^1 \not\equiv 0 \pmod{p}$

karena $aa^1 \equiv 0 \pmod{p}$

Juga $a^1 \not\equiv p - 1 \pmod{p}$ karena jika $a \equiv 1 \pmod{p}$

Juga $a^1 \not\equiv p - 1 \pmod{p}$ karena $(p - 1)^2 \equiv 1 \pmod{p}$

Tetapi $a \leq p - 2$

Juga $a^1 \not\equiv a \pmod{p}$ karena jika $a^1 \equiv a \pmod{p}$

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

Jadi $p \mid a^2 - 1$ atau $p \mid (a + 1)(a - 1)$

Jadi $p \mid a + 1$ atau $p \mid a - 1$

tetapi $1 \leq a - 1 \leq p - 3$

Jadi $p \nmid a - 1$

Dan $3 \leq a + 1 \leq p - 1$

jadi $p \nmid a + 1$

Sehingga $p - 3$ adalah bilangan genap antara 2 dan $p - 2$ yang apabila di pasangkan adalah $\frac{1}{2}$ (p - 3) pasangan, yang masing-masingnya adalah 1 (mod p)

$$\text{Jadi}(p-1)! = (p-1)(p-2)3.2.1$$
$$\equiv (p-1)\,1^{\frac{p-3}{2}}\,.\,1 \pmod p$$
$$= (p-1) \pmod p$$
$$= -1 \pmod p$$

Akibat (Corollary) 3.1.12

$(p-1)! \equiv (p-1) \bmod p$

$(p-2)! \equiv 1 \pmod p$ (karena $(p-1, p) = 1$)

Teorema 3.1.12

jika $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m}$ dimana a, b, m_1, m_2, ..., mk adalah bilangan-bilangan bulat dengan m_1, m_2, ..., mk bilangan bulat positif maka $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$ dimana $[m_1, m_2, \ldots, m_k]$ adalah pengali persekutuan terkecil dari m_1, m_2, ..., m_k .

3.2. KONGRUENSI LINIER

Sebuah kongruensi yang berbentuk $ax \equiv b \pmod m$ dimana x adalah peubah bilangan bulat, disebut kongruensi linier dengan satu variabel. Pada bagian ini kita akan melihat bahwa mencari solusi dari kongruensi linier, sama halnya dengan mencari solusi dari persamaan linier atau disebut juga persamaan Diophantine $ax + my = b$.

Dari teorema 2.2.3 kita tahu bahwa persamaan $ax = my = b$ mempunyai solusi apabila $(a , m) \mid b$

Sekarang, yang menjadi pertanyaan adalah, ada berapa banyak solusi dari kongruensi linier $ax \equiv b \pmod{m}$

Teorema berikut ini menyatakan kapan sebuah kongruensi linier punya solusi dan ada berapa banyaknya solusi tersebut.

Teorema 3.2.1

Misalkan a, b dan m adalah bilangan-bilangan bulat dimana $m > 0$ dan $(a , m) = d$

Jika $d \nmid b$, maka $ax \equiv b \pmod{m}$ tidak punya solusi.

Jika $d \mid b$ maka $ax \equiv b \pmod{m}$ mempunyai d solusi tak kongruen modulo m.

Bukti :

Kongruensi linier $ax \equiv b \pmod{m}$ ekivalen dengan persamaan diophantine $ax - my = b$

Bilangan bulat x adalah solusi dari $ax \equiv b \pmod{m}$ jika dan hanya terdapat sebuah bilangan bulat y dengan $ax-my = b$

Menurut teorema 2.2.3, jika $d \nmid b$, maka persamaan $ax - my = b$ tidak punya solusi

Dan jika $d \mid b$, terdapat tak hingga banyaknya solusi yang diberikan oleh :

$$x = xo + ({}^{m}/d) t \ , \ y = yo + ({}^{a}/d) t$$

dimana $x = xo$ dan $y = yo$ adalah solusi khusus dari persamaan.

Nilai x yang diberikan oleh $x = xo + ({}^{m}/d)\,t$ adalah solusi dari kongruensi linier dan terdapat tak terhingga banyaknya. Untuk menentukan berapa banyak solusi yang tak kongruen. Maka pandang dua buah solusi yaitu :

$$X_1 = Xo + ({}^{m}/d)\,t_1 \text{ dan } X_2 = Xo + ({}^{m}/d)\,t_2$$

Jika kedua solusi ini kongruen maka

$$Xo + ({}^{m}/d)\,t_1 \equiv Xo + ({}^{m}/d)\,t_2 \pmod{m}$$

Atau :

$$({}^{m}/d)\,t_2 \equiv ({}^{m}/d)\,t_2 \pmod{m}$$

Sekarang $({}^{m}/d\,,\,m) = {}^{m}/d$ karena ${}^{m}/d \mid m$

Jadi banyaknya solusi tak kongruen adalah d yaitu dimana nilai t terletak antara $0, 1, \ldots, d - 1$

Contoh 3.2.1

Untuk menentukan solusi dari $9x \equiv 12 \pmod{15}$

Pertama perlu dilihat bahwa $(9, 15) = 3$ dan $3 \mid 15$

Jadi persamaan $9x \equiv 12 \pmod{15}$ punya 3 solusi.

Untuk menentukan solusi-solusi ini, pertama dicari dulu solusi khusus dari persamaan

$$9x - 15y = 12$$

Dengan algoritma Euclid diperoleh :

$$15 = 9 \cdot 1 + 6$$
$$9 = 6 \cdot 1 + 3$$
$$6 = 3 \cdot 2$$

Jadi $3 = 9 - 6 = 9 - (15 - 9) = 9 . 2 - 15$

Jadi $12 = 9 . 8 - 15 . 4$

dan $x_o = 8$ dan $y_o = 4$ adalah sebuah solusi khusus dari persamaan $9x - 15y = 12$

Ketiga solusi tak kongruen dari $9x \equiv 12 \pmod{15}$ adalah :

$$x = x_o = 8 \pmod{15}$$

$$x = x_o + 5 \equiv 13 \pmod{15}$$

$$x = x_o + 10 \equiv 18 \pmod{15}$$

Selanjutnya akan kita tinjau bentuk khusus dari kongruensi yaitu $ax \equiv 1 \pmod{m}$. Dari teorema 3.2.1 kita tahu bahwa kongruensi ini punya solusi jika dan hanya jika $(a,m) = 1$, dan semua solusi dari kongruensi ini adalah kongruen modulo m.

Definisi :

Diberikan sebuah bilangan bulat a dengan $(a, m) = 1$ Sebuah solusi dari $ax \equiv 1 \pmod{m}$ disebut inversi dari $a \pmod{m}$

Contoh 3.2.2

Karena solusi dari $7x \equiv 1 \pmod{31}$ memenuhi $x \equiv 9 \pmod{31}$, maka 9 dan semua bilangan bulat yang kongruen dengan $9 \pmod{31}$ adalah invers dari $7 \pmod{31}$

Apabila diketahui sebuah invers dari a (mod m) , kita dapat menggunakannya untuk menyelesaikan sebarang kongruensi $ax \equiv b \pmod m$.

Caranya adalah sebagai berikut . Misalkan $\bar{a}$ adalah invers dari a (mod m) . jadi $a\bar{a} \equiv 1 \pmod m$

Maka jika $ax \equiv b \pmod m$, kita dapat mengalikan kedua ruas dengan $\bar{a}$ untuk memperoleh $X \equiv \bar{a}b \pmod m$

Contoh 3.2.3

Untuk menentukan solusi dari $7x \equiv 22 \pmod{31}$ kalikan kedua ruas dengan 9 yaitu invers dari 7 (mod 31) untuk memperoleh

$$X \equiv 198 \equiv 12 \pmod{31}$$

Jadi disini, jika (a , m) = 1, maka kongruensi linier $ax = b \pmod m$ mempunyai solusi tunggal modulo m

Contoh 3.2.4

Untuk menentukan semua solusi dari $7x \equiv 4 \pmod{12}$, diketahui bahwa (7 , 12) = 1, maka hanya terdapat satu solusi.

Untuk menentukan solusinya, kita hanya perlu mencari sebuah solusi dari persamaan diophantine $7x - 12y = 4$.

Algoritma Euclid memberikan :

$$12 = 7 . 1 + 5$$

$$7 = 5 . 1 + 2$$

$$5 = 2 . 2 + 1$$

$2 = 2 \, . \, 1$

Jadi $1 = 5 - 2 \, . \, 2$

$= 5 - 2 (7 - 5) = 5 \, . \, 3 - 7 \, . \, 2$

$= (12 - 7) 3 - 7 \, . \, 2 = 12 . \, 3 - 7 \, . \, 5$

Jadi $1 = 12 - 3 - 75$

Dan $4 = 12 \, . \, 12 - 7 \, . \, 20$

Jadi $X = - 20$ dan $y = - 12$ adalah solusi dari persamaan diophantine $7x - 12y = 4$

Dan dengan demikian $X = - 20 \equiv 4 \pmod{12}$ adalah solusi dari $7x \equiv 4 \pmod{12}$

Selanjutnya kita ingin mengetahui, bilangan-bilangan bulat mana saja yang inversnya adalah bilangan tersebut (mod p) dimana p adalah bilangan prima.

Teorema 3.2.2

Misalkan p bilangan prima. Bilangan bulat positif a adalah invers dari a (mod p) jika dan hanya jika $a \equiv 1 \pmod{p}$ atau $a \equiv - 1 \pmod{p}$

Bukti :

Jika $a \equiv 1 \pmod{p}$ atau $a \equiv - 1 \pmod{p}$

Maka $a.a = a^2 \equiv 1 \pmod{p}$

Jadi a adalah invers dari a (mod p)

Sebaliknya, jika a adalah invers dari a (mod p) maka $a^2 \equiv 1 \pmod{p}$

Yaitu $p \mid a^2 - 1 = (a - 1) (a + 1)$

Disini $p \mid a - 1$ atau $p \mid a + 1$

Yaitu $a \equiv 1 \pmod p$ atau $a \equiv -1 \pmod p$

3.3. SISTEM KONGRUENSI LINIER SIMULTAN

Pada bagian ini dan bahagian selanjutnya akan didiskusikan sistem kongruensi linier simultan.
Akan dipelajari sistem kongruensi dengan satu variabel dan modulo yang berbeda. Sistem ini muncul di Cina untuk menjawab pertanyaan : Tentukan sebuah bilangan yang apabila dibagi tiga memberikan sisa 1, dan memberikan sisa 2 bila dibagi dengan 5, dan bila dibagi 7 memberikan sisa 3.
Bentuk pertanyaan ini, apabila dibuat dalam bentuk kongruensi adalah sebagai berikut :

$$X \equiv 1 \pmod 2$$
$$X \equiv 2 \pmod 5$$
$$X \equiv 3 \pmod 7$$

Berikut ini, diberikan suatu metoda untuk mencari solusi dari sistem kongruensi linier simultan diatas.
Teori untuk mencari solusi dari sitem ini diberikan dalam bentuk teorema berikut.

Teorema 3.3.1 (Teorema Sisa Cina)

Misalkan $m_1, m_2, \ldots, m_r$ adalah bilangan-bilangan bulat positif yang relatif prima berpasangan.

Maka sistem kongruensi

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

/

$x \equiv a_r \ (\mathrm{mod}\ m_r)$

Mempunyai solusi tunggal modulo $M = m_1\ m_2\ \ldots\ m_r$

Bukti :

Misalkan $n_i = \dfrac{M}{mi} = m_1\ m_2\ \ldots\ m_{i-1}\ m_{i+1}\ \ldots\ M_r$

Sehingga $mj \mid ni$ bila $j \neq i$ & $(mi\ , ni) = 1$

Karena $(mj\ , nj) = 1$ untuk setiap j , maka terdapat xj sedemikian. Sehingga $nj\ xj \equiv aj\ (\mathrm{mod}\ mj)$.

Selanjutnya pandang $x = n_1\ x_1 + n_2\ x_2 + \ldots + n_r\ x_r$

Karena $mj \mid ni\ xi$. Untuk $j \neq i$, maka

$$\begin{aligned} x &\equiv nj\ xj \ (\mathrm{mod}\ mj) \\ &\equiv aj\ (\mathrm{mod}\ mj) \text{ untuk } j = 1,2,\ \ldots,\ r \end{aligned}$$

Disini x adalah solusi simultan dari sistem r kongruensi untuk membuktikan ketunggalan solusi, misalkan x dan y adalah dua solusi dari sistem r kongruensi, maka

$$x \equiv y\ (\mathrm{mod}\ mj) \text{ untuk } j = 1,2,\ \ldots,\ r$$

Dan karena $(mi, mj) = 1$ Untuk $i \neq j$

maka $x \equiv y\ (\mathrm{mod}\ m)$

Jadi solusi dari sistem kongruensi linier simultan adalah tunggal.

Contoh 3.3.1

Selesaikan sistem kongruensi linier simultan :

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

Penyelesaian :

$M = 3 \,.\, 5 \,.\, 7 = 105$

$n_1 = {}^{m}/_{m_1} = {}^{105}/_{3} = 35$

$n_2 = {}^{m}/_{m_2} = {}^{105}/_{5} = 21$

$n_3 = {}^{m}/_{m_3} = {}^{105}/_{7} = 15$

Solusi dari $35 \; x_1 \equiv 1 \pmod 3$ adalah

$x_1 \equiv 2 \pmod 3$

Solusi dari $21 \; x_2 \equiv 2 \pmod 5$ adalah

$x_2 \equiv 2 \pmod 5$

Solusi dari $15 \; x_3 \equiv 3 \pmod 7$ adalah

$x_3 \equiv 3 \pmod 7$

Jadi
$$\begin{aligned} x &= n_1 x_1 + n_2 x_2 + n_3 x_3 \\ &= 35 \,.\, 2 + 21 \,.\, 2 + 15 \,.\, 3 \\ &= 157 \\ &\equiv 52 \pmod{105} \end{aligned}$$

Jadi $x = 52$ adalah solusi dari kongruensi linier simultan
$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

Karena $52 \equiv 1 \pmod 3$

$$52 \equiv 2 \pmod 5$$

$$52 \equiv 3 \pmod 7$$

Akibat (Corollary) 3.3.2

Jika $m_1, m_2, \ldots, m_k$ adalah bilangan-bilangan bulat yang relatif prima berpasangan maka sistem kongruensi linier

$$a_j x \equiv b_j \pmod{m_j} \text{ untuk } j = 1, 2, \ldots, r$$

dapat diselesaikan secara simultan mod $M = m_1 m_2 \ldots m_r$ Jika dan hanya jika $(a_j, m_j) \mid b_j$ untuk setiap j.

Contoh 3.3.2

Sistem kongruensi linier : $7x \equiv 22 \pmod{31}$

$2x \equiv 1 \pmod 3$

mempunyai solusi simultan karena

$(7, 31) \mid 22$ dan $(2, 3) \mid 1$

Dan sistem diatas ekivalen dengan :

$$x \equiv 12 \pmod{31}$$

$$x \equiv 2 \pmod 3$$

Dengan menggunakan teorema sisa Cina diperoleh solusi

$x \equiv 74$ (mod 93

Soal-soal

1. Buktikan bahwa jika a bilangan genap, maka

   $a^2 \equiv 0 \pmod 4$

   dan jika a bilangan ganjil maka $a^2 \equiv 1 \pmod 8$

2. Buktikan bahwa hasil kali dari 3 bilangan bulat berurutan $\equiv 0 \pmod 6$

3. Buktikan bahwa :

   a. Jika $n > 0$ dan $n \mid m$ dan $a \equiv b \pmod m$ maka $a \equiv b \pmod n$

   b. Jika $c > o$ dan $a \equiv b \pmod m$ maka $ac \equiv bc \pmod{mc}$

4. Buktikan bahwa jika $a \equiv b \pmod c$ maka $(a,c) = (b,c)$

5. Buktikan bahwa untuk setiap bilangan ganjil a,

   $a^{2^n} \equiv 1 \pmod{2^{n+1}}$

6. Tentukan semua solusi tak kongruen dari kongruensi berikut :

   a. $5x \equiv 6 \pmod 7$

   b. $6x \equiv 7 \pmod 8$

   c. $7x \equiv 8 \pmod 9$

   d. $2x \equiv 0 \pmod 4$

7. Buktikan bahwa jika $(a,m) = 1$, maka kongruensi $ax \equiv b \pmod m$ mempunyai solusi

   $X = a^{\varnothing(m)-1} b$ dimana $\varnothing(m)$ adalah fungsi Euler

8. Tentukan solusi simultan dari sistem kongruensi berikut :

   a. $x \equiv 11 \pmod{17}$
      $x \equiv 17 \pmod{11}$

   b. $x \equiv 2 \pmod 3$
      $2x \equiv 3 \pmod 5$
      $3x \equiv 4 \pmod 7$

9. Tentukan bilangan positif terkecil sedemikian sehingga apabila bilangan tersebut dibagi oleh 10, 13, dan 17 memeberikan sisa 3, 11, 15 masing-masingnya.

10. Selesaikan sistem kongruensi :

$$7x \equiv 47 \pmod{55}$$

$$13x \equiv 97 \pmod{128}$$

$$-17x \equiv 49 \pmod{73}$$

$$-16x \equiv 8 \pmod{237}$$

BAB IV

FUNGSI MULTIPLIKATIF

4.1. Fungsi Phi - Euler

Fungsi Phi - Euler mempunyai sifat bahwa nilai fungsinya yaitu $\emptyset$ (n) adalah hasil kali nilai-nilai fungsi tersebut pada $pi^{\alpha i}$ dimana pi adalah bilangan prima dan $n = \Pi\ pi^{\alpha i}$.

Fungsi-fungsi dengan sifat seperti diatas disebut fungsi multiplikatif. Pada bab ini akan ditunjukkan bahwa fungsi phi - Euler adalah fungsi multiplikatif. Dari fakta ini akan diturunkan sebuah formula untuk nilai fungsi ini berdasarkan pada faktor-faktor primanya. Dan selanjutnya akan dipelajari fungsi-fungsi multiplikatif lainnya, termasuk fungsi banyaknya pembagi dan fungsi jumlah pembagi. Berikut ini diberikan sebuah definisi.

Definisi :

Sebuah fungsi aritmatika adalah sebuah fungsi yang terdefinisi untuk semua bilangan bulat positif.

Fungsi multiplikatif adalah fungsi aritmatika yang mempunyai sifat tertentu.

Definisi :

Sebuah fungsi aritmatika disebut fungsi multiplikatif jika $f(mn) = f(m) f(n)$ dimana m dan n bilangan-bilangan bulat dan m,n relatif prima. Dan sebuah fungsi aritmatika disebut fungsi multiplikatif lengkap jika $f(mn) = f(m) f(n)$ untuk setiap bilangan-bilangan bulat m dan n.

Contoh 4.1.1

a. Fungsi $f(n) = 1 \ \forall n$ adalah fungsi multiplikatif lengkap karena $f(mn) = 1 = 1.1 = f(m) \ f(n)$; $\forall m, n$

b. Fungsi $f(n) = n$ adalah fungsi multiplikatif lengkap karena $f(mn) = mn \ f(m) \ f(n) \ \forall \ m, n$

Jika f adalah sebuah fungsi multiplikatif, maka kita dapat mencari sebuah formula sederhana untuk $f(n)$ dalam faktor-faktor prima dari n.

Teorema 4.1.1

Jika f adalah fungsi multiplikatif dan $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_r^{\alpha r}$ adalah faktor-faktor prima dari n, maka

$f(n) = f(p_1^{\alpha 1}) \ f(p_2^{\alpha 2}) \ldots f(p_r^{\alpha r})$

Bukti (Dengan menggunakan Prinsip Induksi matematika)

Jika n mempunyai satu faktor prima maka $n = p_1^{\alpha 1}$ untuk p_1 suatu bilangan prima

Dan $f(n) = f \;(p_1^{\alpha 1})$

Andaikan n mempunyai k faktor prima yang berbeda yaitu

$n = p_1^{\alpha 1}\; p_2^{\alpha 2} \; \ldots \; p_k^{\alpha k}$ dan

$f(n) = f\;(p_1^{\alpha 1})\;\; f\;\;(p_2^{\alpha 2}) \;\ldots\; (p_k^{\alpha k})$

Sekarang andaikan $n = p_1^{\alpha 1}\; p_2^{\alpha 2} \;\ldots\; p_k^{\alpha k}\; p_{k+1}^{\alpha k+1}$

Karena f multiplikatif dan $(\; p_1^{\alpha 1}\;\; p_2^{\alpha 2} \;\;\ldots\;\; p_k^{\alpha k},$
$p_{k+1}^{\alpha k+1}) = 1$

Maka $f(n) = f\;(p_1^{\alpha 1}\; p_2^{\alpha 2} \;\ldots\; p_k^{\alpha k})\; f\;(\; p_{k+1}^{\alpha k+1})$

Dan dengan menggunakan hipotesis induktif, diperoleh

$f(n) = f\;(p_1^{\alpha 1})\; f\;(p_2^{\alpha 2}) \;\ldots\; f\;(p_k^{\alpha k})\; f\;(p_{k+1}^{\alpha k+1})$

Teorema 4.1.2

Jika p bilangan prima, maka $\emptyset\,(p) = p-1$.
Sebaliknya, jika p bilangan bulat positif dengan $\emptyset\,(p) = p-1$ maka p adalah bilangan prima.

Bukti :

Jika p bilangan prima, maka setiap bilangan bulat positif yang lebih kecil dari p relatif prima dengan p

Karena terdapat p-1 bilangan bulat positif yang akan lebih kecil dari p maka $\emptyset\,(p) = p-1$.

Sebaliknya, Andaikan p bilangan komposit, maka 7 d , $1 < d < p$ dan $d \mid p$. Jadi sekurang-kurangnya terdapat satu diantara p-1 bilangan bulat 1,2, ... , p-1 yaitu d yang tidak relatif prima dengan p.

Jadi $\emptyset\,(p) \leq p-2$ (kontradiksi). Jadi pengandaian p komposit salah. Jadi haruslah p bilangan prima.

Teorema 4.1.3

Misalkan p adalah bilangan prima dan a sebuah bilangan bulat positif. Maka $\varnothing(p^a) = p^a - p^{a-1}$

Bukti :

Bilangan bulat positif $< p^a$ yang tidak relatif prima dengan p^a adalah bilangan-bilangan yang habis dibagi oleh p. Bilangan-bilangan tersebut adalah kp dimana $1 \le k \le p^{a-1}$. Dan terdapat sebanyak p^{a-1} bilangan-bilangan tersebut.

Jadi terdapat $p^a - p^{a-1}$ bilangan yang lebih kecil dari p^a yang relatif prima dengan p^a.

Jadi $\varnothing(p^a) = p^a - p^{a-1}$.

Contoh : 4.1.2

Dengan menggunakan teorema 6.3 , diperoleh bahwa

$$\varnothing(5^3) = 5^3 - 5^2 = 100$$

$$\varnothing(2^{10}) = 2^{10} - 2^9 = 512$$

$$\varnothing 9(11^2) = 11^2 - 11 = 110$$

Untuk menentukan formula $\varnothing(n)$, bila diberikan faktor-faktor primanya, cukup ditunjukkan bahwa $\varnothing$ adalah multiplikatif.

Contoh 4.1.3

Misalkan m = 4 dan n = 9 sehingga mn = 30.

Berikut ini kita tuliskan bilangan-bilangan dari 1 sampai 36 :

1	5	9	13	17	21	25	29	33
2	6	10	14	18	22	26	30	34
3	7	11	15	19	23	23	31	35
4	8	12	16	20	24	28	32	36

Dari daftar bilangan-bilangan diatas, tidak ada bilangan-bilangan yang terdapat pada baris kedua dan ke empat yang relatif prima dengan 36.

Sekarang perhatikan bilangan-bilangan pada baris pertama dan ke tiga. Semua bilangan tersebut relatif prima dengan 4. Dan 6 bilangan pada baris pertama, Juga 6 bilangan pada baris ketiga relatif prima dengan 36. Jadi ada 12 bilangan yang relatif prima dengan 36 yaitu 2.6. Jadi disini $\emptyset$ (36) = 2 . 6 = $\emptyset$ (4) $\emptyset$ (9).

Teorema 4.1.4

Misalkan m dan n adalah bilangan bulat positif dan m, n relatif prima yaitu (m , n) = 1

Maka $\emptyset(mn) = \emptyset(m)\,\emptyset(n)$

Bukti :

Tuliskan semua bilangan-bilangan bulat positif $\leq$ mn sebagai berikut :

$$
\begin{array}{lllll}
1 & m + 1 & 2m + 1 & \ldots & (n-1) \\
2 & m + 2 & 2m + 2 & & (n-1)\, m + 2 \\
3 & m + 3 & 2m + 3 & & (n-1)\, m + 3 \\
\vdots & \vdots & \vdots & & \vdots \\
r & m + r & 2m + r & & (n-1)\, m + r \\
\vdots & \vdots & \vdots & & \vdots \\
m & 2m & 3m & & mn
\end{array}
$$

Sekarang andaikan r bilangan bulat positif dengan $r < m$ dan $(r,m) = d > 1$. Maka tidak ada bilangan yang terletak pada baris ke r yang relatif prima dengan mn, karena setiap elemen pada baris ini dapat dituliskan dalam bentuk $km + r$, $0 \leq k \leq n-1$.
dan $d \mid km + r$ karena $d \mid m$ dan $d \mid r$.
Jadi untuk mencari bilangan yang relatif prima dengan mn dari bilangan-bilangan pada daftar di atas, kita hanya perlu memperhatikan baris ke r dimana $(m,r) = 1$. Jika $(m,r) = 1$ dan $1 \leq r \leq m$, harus ditentukan berapa banyaknya bilangan bulat pada baris ini yang relatif prima dengan mn.
Elemen-elemen pada baris ini adalah :
r , $m + r$, $2m + r$, ..., $(n - 1)m + r$
Karena $(m , r) = 1$ maka setiap bilangan ini adalah relatif prima dengan m. Dan terdapat $\emptyset (n)$ bilangan pada baris ke r ini yang relatif prima dengan n .
Karena ke $\emptyset (n)$ bilangan ini juga relatif prima dengan

m, maka bilangan-bilangan ini relatif prima dengan mn. Karena ada Ø (m) baris yang memuat Ø (n) bilangan bulat yang relatif prima dengan mn maka Ø (mn) = Ø (m) Ø (n).

Teorema 4.1.5

Misalkan $n = p_1^{a1} \; p_2^{a2} \; \ldots \; p_k^{ak}$ *adalah faktor-faktor prima dari bilangan bulat positif n*

Maka $\text{Ø}(n) = n\left(1 - \frac{1}{p1}\right)\left(1 - \frac{1}{p2}\right)\ldots\left(1 - \frac{1}{pk}\right)$

Bukti :

Karena Ø multiplikatif, maka

$\text{Ø}\,(n) = \text{Ø}\,(p_1^{a1})\,\text{Ø}\,(p_2^{a2}) \ldots \text{Ø}\,(p_k^{ak})$

Dan menurut teorema 4.1.3,

$$\begin{aligned}\text{Ø}\,(p_i^{ai}) &= p_i^{ai} - p_i^{ai-1} \text{ untuk } i = 1,2, \ldots, k.\\ &= p_i^{ai}\left(1 - \frac{1}{pi}\right)\end{aligned}$$

$$\begin{aligned}\text{Jadi } \text{Ø}\,(n) &= p_1^{a1}\left(1 - \frac{1}{p1}\right) p_2^{a2}\left(1 - \frac{1}{p2}\right) \ldots p_k^{ak}\left(1 - \frac{1}{pk}\right)\\ &= p_1^{a1}\; p_2^{a2} \ldots p_k^{ak}\left(1 - \frac{1}{p1}\right)\left(1 - \frac{1}{p2}\right)\\ &\quad \ldots \left(1 - \frac{1}{pk}\right)\\ &= n\left(1 - \frac{1}{p1}\right)\left(1 - \frac{1}{p2}\right) \ldots \left(1 - \frac{1}{pk}\right)\end{aligned}$$

Contoh 4.1.4

Dengan menggunakan teorema 4.1.5, diperoleh bahwa

$$\varnothing\ (100) = \varnothing\ (\ 2^2\ .\ 5^2\ ) = 100 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$
$$= 40$$

dan

$$\varnothing\ (720) = \varnothing\ (\ 2^4\ 3^2\ 5\ ) = 720 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 750\ .\frac{1}{2}\ .\frac{2}{3}\ .\frac{4}{5}$$
$$= 192$$

Teorema 4.1.6

Misalkan n bilangan bulat positif dan n > 2

Maka $\varnothing$ (n) adalah bilangan genap.

Bukti :

Andaikan $n = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$ adalah faktor-faktor prima dari n.

Karena $\varnothing$ multiplikatif, maka $\varnothing\ (n) = \prod_{i=1}^{k} \varnothing\ (pi^{ai})$

Dan menurut teorema 4.1.3, diperoleh bahwa

$$\varnothing \left(p_i^{ai}\right) = p_i^{ai-1}\left(p_i - 1\right)$$

Disini $\varnothing \left(p_i^{ai}\right)$ adalah genap apabila pi bilangan prima yang ganjil karena pi-1 genap atau jika

$p_i = 2$ dan $a_i > 1$ maka $p_i^{a_i-1}$ adalah genap.

Karena $n > 2$, maka salah satu dari kondisi di atas dipenuhi oleh n. Dengan demikian, $\emptyset\left(p_i^{a_i}\right)$ genap untuk sekurang-kurangnya satu dari salah satu bilangan i , $1 \leq i \leq k$

Jadi $\emptyset$ (n) adalah genap.

Misalkan f adalah fungsi aritmatika

Maka $\sum_{d|n} f$ (n) adalah jumlah nilai-nilai f pada

Semua pembagi positif dari n.

Contoh 4.1.5

Jika f adalah sebuah fungsi aritmatika, maka

$\sum f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$

$$\text{Dan } \sum_{d|12} d^2 = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2$$
$$= 1 + 4 + 9 + 16 + 36 + 144 + = 240$$

Teorema berikut menyatakan bahwa n adalah jumlah dari nilai-nilai fungsi phi - Euler pada semua pembagi dari n.

Teorema 4.1.7

Misalkan n bilangan bulat positif

Maka $\sum_{d|n} \emptyset(d) = n$

Bukti :

Disini kita membagi bilangan-bilangan 1,2,5 ..., n kedalam kelompok-kelompok.

Masukkan bilangan m ke dalam kelompok Cd apabila $(m,n) = d$

yaitu $m \in Cd$ apabila $(m,n) = d$

atau $(^m/d , ^n/d) = 1$

Jadi disini banyaknya elemen di Cd addalah $\emptyset$ (n/d), karena bilangan-bilangan 1 sampai n, dikelompokkan kedalam kelompok- kelompok yang disjoin, dan setiap bilangan berada dalam hanya satu kelompok, maka

n = jumlah banyaknya elemen dalam kelompok-kelompok yang berbeda.

$$\text{Jadi } n = \sum_{d|n} \emptyset (n/d)$$

Dan karena d adalah bilangan bulat positif yang membagi n, maka $^n/d$ juga merupakan pembagi dari n.

$$\text{Jadi } n = \sum_{d|n} \emptyset (n/d) = \sum_{d|n} \emptyset (d)$$

Contoh 4.1.6

Misalkan n = 18. Maka bilangan-bilangan dari 1 sampai 18 dapat dikelompokan kedalam kelompok cd, d | 18 sedemikian sehingga kelompok cd memuat bilangan-bilangan bulat m dimana (m,18) = d

Diperoleh :

$C_1 = \{ 1,5,7,11,13,17 \}$

$C_2 = \{ 2,4,8,10,14,16 \}$

$C_3 = \{ 3,15 \}$

$C_6 = \{ 6,12 \}$

$C_9 = \{9\}$

$C_{18} = \{18\}$

Kita lihat bahwa setiap Cd memuat ϕ ($^{18}/d$) bilangan bulat yaitu :

C_1 memuat ϕ ($^{18}/1$) = ϕ (18) = 6

C_2 memuat ϕ ($^{18}/2$) = ϕ (9) = 6

C_3 memuat ϕ ($^{18}/3$) = ϕ (6) = 2

C_6 memuat ϕ ($^{18}/6$) = ϕ (3) = 2

C_9 memuat ϕ ($^{18}/9$) = ϕ (2) = 1

C_{18} memuat ϕ ($^{18}/18$) = ϕ (1) = 1

Jadi $18 = \phi\ (18) + \phi\ (9) + \phi\ (6) + \phi\ (3) + \phi\ (2) + \phi\ (1)$

$$= \sum_{d|18} \phi\ (d)$$

4.2. JUMLAH PEMBAGI DAN BANYAKNYA PEMBAGI SUATU BILANGAN BULAT POSITIF

Seperti telah dikatakan pada bagian 4.1.1, bahwa fungsi jumlah pembagi dan fungsi banyaknya pembagi dari suatu bilangan bulat positif adalah fungsi-fungsi multiplikatif. Berikut ini akan kita perlihatkan bahwa fungsi-fungsi ini adalah fungsi multiplikatif dan akan diberikan formula untuk nilai fungsi-fungsi ini pada suatu bilangan bulat positif n berdasarkan faktor-faktor prima dari n.

Definisi :

Fungsi jumlah pembagi dari n, dinotasikan dengan σ (n), dan didefinisikan sebagai jumlah dari semua pembagi positif dari n.

Definisi :

Fungsi banyaknya pembagi dari n, dinotasikan dengan τ (n) dan didefinisikan sebagai banyaknya pembagi positif dari n.

Contoh 4.2.1

Misalkan n = 6

Maka $\sigma(6) = 1 + 2 + 3 + 6 = 12$

$\tau(6) = 4$

Karena 1,2,3,6 adalah pembagi-pembagi dari 6

Misalkan n = 12

Maka $\sigma(12) = 1 + 2 + 3 + 4\ 6 + 12 = 28$

$\tau(12) = 6$

Disini juga dapat dituliskan bahwa :

$$\sigma(n) = \sum_{d|n} d$$

$$\tau(n) = \sum_{d|n} 1$$

Teorema 4.2.1

Jika f adalah fungsi multiplikatif, maka fungsi aritmatika $F(n) = \sum_{d|n} f(d)$ juga fungsi multiplikatif.

Sebelum diberikan bukti dari teorema diatas, lebih baik di tuliskan terlebih dahulu ide yang ada pada teorema dengan contoh berikut.

Contoh 4.2.2

Misalkan f adalah fungsi multiplikatif dan

$$F(n) = \sum_{d|n} f(d)$$

Maka $F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$

Karena 1,2,3,4,6 dan 12 adalah pembagi-pembagi dari 12.

Dan karena

$1 = 1 \cdot 1$	$4 = 1 \cdot 4$
$2 = 1 \cdot 2$	$6 = 2 \cdot 3$
$3 = 1 \cdot 3$	$12 = 3 \cdot 4$

$$\begin{aligned} \text{Maka } F(12) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\ &= f(1)\,f(1) + f(1) \cdot f(2) + f(1)\,f(3) + \\ &\quad f(1)\,f(4) + f(2)\,f(3) + f(3)\,f(4) \\ &= f(1)\left\{ f(1) + f(2) + f(4) \right\} + f(3)\left\{ f(1) \right. \\ &\quad \left. + f(2) + f(4) \right\} \\ &= \left\{ f(1) + f(3) \right\} \left\{ f(1) + f(2) + f(4) \right\} \\ &= F(3)\ F(4) \end{aligned}$$

Selanjutnya kita buktikan teorema 4.2.1

Bukti :

Untuk membuktikan f multiplikatif, harus dibuktikan bahwa jika (m,n) = 1 maka f (mn) = f (m) f (n)

Sekarang andaikan (m,n) = 1

Jadi kita punya.

$$F\,(mn) = \sum_{d \mid mn} f(d)$$

Karena (m,n) = 1 maka setiap pembagi d dari mn dapat dituliskan sebagai $d = d_1\, d_2$ dimana $(d_1\, d_2) = 1$, $d_1 \mid m$ dan $d_2 \mid n$.

Sehingga sekarang

$$F\,(mn) = \sum_{\substack{d \mid m \\ d \mid n}} f\,(d_1 d_2)$$

Dan karena f fungsi multiplikatif, maka

$$F\,(mn) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f\,(d_1)\, f\,(d_2)$$

$$= \sum_{d_1 \mid m} f\,(d_1) \sum_{d_2 \mid n} f\,(d_2)$$

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

Selanjutnya teorema 4.2.1 ini dapat digunakan untuk membuktikan bahwa σ (n) dan τ (n) adalah fungsi-fungsi multiplikatif.

Akibat (Corollary) 4.4.2

Fungsi jumlah pembagi, σ (n) dan fungsi banyaknya pembagi τ (n) adalah fungsi-fungsi multiplikatif.

Bukti :

Misalkan f(n) = n dan g(n) = 1.

Disini f(n) dan g(n) adalah fungsi-fungsi multiplikatif.

Maka menurut teorema 4.2.1, fungsi-fungsi

$$\sigma(n) = \sum_{d|n} f(d) \quad \text{dan} \quad \tau(n) = \sum_{d|n} g(d)$$

adalah fungsi-fungsi multiplikatif.

Lemma 4.2.3

Misalkan p bilangan prima dan a bilangan bulat positif. Maka :

$$\sigma(p^a) = (1 + p + p^2 + \ldots + p^a) = \frac{p^{a+1} - 1}{p - 1}$$

dan

$$\tau(p^a) = a + 1$$

Bukti :

Pembagi-pembagi dari p^a adalah 1, p, p^2, ..., p^a

Akibatnya p^a mempunyai a + 1 pembagi

Jadi $\tau(p^a) = a + 1$

Juga $\sigma(p^a) = 1 + p + p^2 + \ldots + p^a$

Ruas kanan merupakan deret geometri dengan rasio p , p bilangan prima (yaitu p > 1)

$$\text{Maka } \sigma(p^{a}) = \frac{p^{a+1}-1}{p-1} \quad (\text{ rumus jumlah deret geometri })$$

Teorema 4.2.4

Misalkan n bilangan bulat positif dengan faktor-faktor prima : $n = p_a^{a1}\ p_2^{a2} \ldots p_k^{ak}$

Maka

$$\sigma(n) = \frac{p_1^{a1+1}-1}{p_1-1} \cdot \frac{p_2^{a2+1}-1}{p_2-1} \cdot \ldots \frac{p_k^{ak+1}-1}{p_k-1}$$

dan

$$\tau(n) = (a_1+1)(a_2+1)\ldots(a_k+1)$$

Bukti :

Untuk $n = p_a^{a1}\ p_2^{a2} \ldots p_k^{ak}$

Karena σ dan τ fungsi-fungsi multiplikatif

maka :

$$\begin{aligned}\sigma(n) &= \sigma(p_1^{a1}\ p_2^{a2} \ldots p_k^{ak}) \\ &= \sigma(p_1^{a1})\ \sigma(p_2^{a2}) \ldots \sigma(p_k^{ak}) \\ &= \left(\frac{p_1^{a1+1}-1}{p_1-1}\right)\left(\frac{p_2^{a2+1}-1}{p_2-1}\right)\ldots\left(\frac{p_k^{ak+1}-1}{p_k-1}\right)\end{aligned}$$

Dan

$$\begin{aligned}\tau(n) &= \tau(p_1^{a1}\ p_2^{a2} \ldots p_k^{ak}) \\ &= \tau(p_a^{a1})\ \tau(p_2^{a2}) \ldots \tau(p_k^{ak}) \\ &= (a_1+1)(a_2+1)\ldots(a_k+1)\end{aligned}$$

Contoh 4.2.3

Dengan menggunakan teorema 4.2.3 diperoleh

$$\sigma\ (200) = \sigma\ (2^3 . 5^2)$$

$$= \sigma\ (2^3)\ \sigma\ (5^2)$$

$$= \left(\frac{2^4 - 1}{2 - 1}\right) \left(\frac{5^3 - 1}{5 - 1}\right) =$$

$$= 15 . 31 = 465$$

$$\tau\ (200) = \tau\ (2^3\ 5^2)$$

$$= \tau\ (2^3)\ \tau\ (5^2)$$

$$= (4)(3)$$

$$= 12$$

Sama halnya

$$\sigma\ (750) = \sigma\ (2^4 . 3^2 . 5)$$

$$= \sigma\ (2^4)\ \sigma\ (3^2)\ \sigma\ (5)$$

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

$$= (31)(13)(6)$$

$$= 2418$$

$$\tau\ (720) = \tau\ (2^4\ 3^2\ 5)$$

$$= \tau\ (2^4)\ \tau\ (3^2)\ \tau\ (5)$$

$$= (4 + 1)(2 + 1)(1 + 1)$$

$$= 5 . 3 . 2$$

$$= 30$$

4.3. BILANGAN-BILANGAN SEMPURNA DAN BILANGAN PRIMA MARSENNE

Ahli matematika Mesir juga tertarik pada bilangan-bilangan bulat yang sama dengan jumlah pembagi-pembagi positifnya. Bilangan-bilangan bulat ini disebut bilangan sempurna.

Definisi

Jika n adalah sebuah bilangan bulat positif dan $\sigma(n) = 2n$, maka n disebut bilangan sempurna

Contoh 4.3.1

Karena $\sigma(6) = 1 + 2 + 3 + 6 = 12$ maka 6 adalah bilangan sempurna.

Juga 28 adalah bilangan sempurna karena

$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28$

$= 56 = 2 \cdot 28$

Teorema 4.3.1

Bilangan bulat positif n adalah bilangan sempurna genap jika dan hanya jika $n = 2^{m-1}(2^m - 1)$ dimana m adalah sebuah bilangan bulat sedemikian sehingga $m > 2$ dan $2^m - 1$ bilangan prima.

Bukti :

($\Leftarrow$) Misalkan $n = 2^{m-1}(2^m - 1)$ untuk $m \geq 2$ dan $(2^m - 1)$ bilangan prima.

Karena $2^m - 1$ prima maka $(2^{m-1}, 2^m - 1) = 1$

Dan karena σ adalah fungsi multiplikatif,

maka :

$\sigma \ (n) = \sigma \ (2^{m-1}) \ \sigma \ (2^m - 1)$

Dan menurut lemma 4.2.2,

$$\sigma \ (2^{m-1}) = \frac{2^{m-1+1} - 1}{2 - 1} = 2^m - 1$$

Dan karena $2^m - 1$ bilangan prima, maka

$\sigma \ (2^m - 1) = 1 + 2^m - 1 = 2^m$

$$\begin{aligned} \text{Jadi } \sigma \ (n) &= (2^m - 1)\ (2^m) \\ &= 2\ (2^{m-1})\ (2^m - 1) \\ &= 2\ n \end{aligned}$$

Jadi n adalah bilangan sempurna.

($\Leftarrow$) Sebaliknya , misalkan n adalah sebuah bilangan sempurna yang genap, tuliskan sebagai $n = 2^5\ t$ dimana 5 dan t adalah bilangan-bilangan bulat positif dan t bilangan ganjil.

Karena $(2^5, t) = 1$, maka berdasarkan lemma 2.4.2 :

$$\begin{aligned} \sigma \ (n) &= \sigma \ (2^5)\ \sigma \ (t) \\ &= (2^{5+1} - 1)\ \sigma \ (t) \ \ldots \ (4.3.1) \end{aligned}$$

Dan karena n adalah bilangan sempurna, maka $\sigma \ (n) = 2n = (2^{5+1} - 1)\ \sigma \ (t)$

Atau

$$2^{5+1}\ t = (2^{5+1} - 1)\ \sigma \ (t) \ \ldots \ (4.3.2)$$

Karena $(2^{5+1}\ ,\ 2^{5+1} - 1) = 1$ maka $2^{5+1} \mid \sigma \ (t)$

Dengan demikian $\exists$ sebuah bilangan bulat q sedemikian sehingga $\sigma \ (t) = q\ 2^{2+1}$

Jadi

$$2^{5+1}\ t = (2^{5+1} - 1)\ (q\ 2^{5+1})\ \ldots\ (4.3.3)$$

Atau

$$t = (2^{5+1} - 1)\ q = \ldots.\ (4.3.4)$$

Disini $q|t$ dan $q \neq t$

Substitusikan $t = (2^{5+1} - 1)\ q$ diperoleh

$t + q = (2^{5+1})\ q + q = 2^{5+1}\ q = \sigma\ (t)\ \ldots\ (4.3.5)$

Selanjutnya akan ditunjukkan bahwa $q = 1$

Jika $\neq 1$, maka terdapat sekurang-kurangnya tiga pembagi positif dari t yaitu 1 , q dan t.

Akibatnya $\sigma\ (t) \geq 1 + q + t$

Ini kontradiksi dengan persamaan (4.3.5)

Jadi haruslah $q = 1$.

Dan dari persamaan (4.3.4) di peroleh

$t = (2^{5+1} - 1)$

Dan persamaan (4.3.5) memberikan :

$$\sigma\ (t) = t + 1$$

Yang berarti bahwa t adalah bilangan prima.

Dengan demikian

$n = 2^5\ (2^{5+1} - 11)$ dimana $2^{5+1} - 1$ adalah bilangan prima.

Teorema 4.3.2

Jika m bilangan bulat positif dan $2^m - 1$ adalah bilangan prima maka m haruslah bilangan prima

Bukti :

Andaikan m bukan bilangan prima

Jadi m dapat dituliskan sebagai a.b dimana $1 < a,b < m$

Maka $2^m - 1 = 2^{ab} - 1$

$= (2^a - 1)(2^{a(b-1)}) + 2^{a(b-2)} + \ldots$

$+ 2^a + 1)$

Karena kedua faktor pada ruas kanan > 1

maka $2^m - 1$ adalah komposit.

Kontradiksi dengan hipotesis bahwa $2^m - 1$ prima jadi haruslah m bilangan prima.

Definisi :

Jika m bilangan bulat positif maka $Mm = 2^m - 1$ disebut bilangan Marsenne ke m, dan jika p bilangan prima dan $Mp = 2^p - 1$ juga bilangan prima maka Mp disebut bilangan prima Marsenne.

Teorema 4.3.3

Jika p adalah bilangan prima ganjil, maka sebarang pembagi dari bilangan Marsenne $Mp = 2^p - 1$ berbentuk $2kp + 1$ dimana k bilangan bulat positif.

Bukti :

Misalkan q sebuah bilangan prima yang membagi $Mp = 2^p - 1$. Makamenurut teorema kecil Fermat,

$q \mid (2^{q-1} - 1)$

Dan $(2^p - 1, 2^{q-1}) = 2^{(p,q-1)} - 1$

Karena q adalah pembagi persekutuan dari $2^p - 1$ dan $2^{q-1} - 1$, maka $(2^{p-1}, 2^{q-1} - 1) > 1$

Disini (p , q - 1) = p

Sehingga $p \mid q - 1$

Dengan demikian , terdapat bilangan bulat positif m dengan q - 1 = mp. Karena q ganjil maka m haruslah bilangan genap, sebut m = 2k dimana k bilangan bulat positif.

Jadi q = mp + 1 = 2kp + 1.

Contoh 4.3.2

Untuk menentukan apakah $M_{13} = 2^{13} - 1 = 8191$ adalah bilangan prima, hanya perlu dilihat untuk sebuah faktor prima $\leq \sqrt{8191} = 90,504 \ldots$

Dan menurut teorema 4.3.3 , pembagi prima tersebut mempunyai bentuk 26k + 1.

Kemungkinan untuk bilangan prima yang membagi M_{13} yang lebih kecil atau sama dengan $\sqrt{M_{13}}$ adalah 53 dan 79. Dengan mencobakan pembagian M_{13} dengan ke dua bilangan diatas menunjukkan bahwa M_{13} adalah bilangan prima.

Contoh 4.3.3

Untuk menentukan apakah $M_{23} = 2^{23} - 1 = 8388607$ adalah bilangan prima, kita hanya perlu menentukan apakah M_{23} habis dibagi oleh sebuah bilangan prima $\leq$ $\sqrt{M_{23}} = 2896,309 \ldots$ yang berbentuk 46 k + 1.

Bilangan prima yang pertama adalah 47

Dan 83886077 = 47 . 17 8481

Jadi M_{23} bukanlah bilangan prima

Atau M_{23} adalah bilangan komposit.

Soal-soal

1. Tentukan apakah setiap fungsi-fungsi aritmatika berikut adalah fungsi multiplikatif lengkap.

   (a) $f(n) = 0$ (d) $f(n) = \log n$

   (b) $f(n) = 2$ (e) $f(n) = n^2$

   (c) $f(n) = {}^{n}/2$ (f) $f(n) = n!$

2. Tentukan jumlah pembagi positif dari setiap bilangan berukut (Yaitu tentukan σ (n)).

   a. 35 d. 2^{100}

   b. 196 e. $2^5 . 3^4 . 5^3 . 7^2 . 11$

   c. 1000 f. 20 !

3. Tentukan banyaknya pembagi positif dari setiap bilangan berikut (yaitu tentukan τ (n)).

   a. 36 d. 2 . 3 . 5 . 7 . 11 . 13 . 17 . 19

   b. 99 e. $2 . 3^2 . 5^3 . 7^4$

   c. 14 f. 20 !

4. Bilangan bulat positif yang mempunyai sebuah pembagi positif ganjil

5. Untuk bilangan bulat positif n yang manakah sehingga jumlah pembagi dari n adalah bilangan ganjil

6. Tentukan semua bilangan bulat positif n dengan σ (n) sama dengan :

   (a) 12 (b) 24 (e) 52

   (b) 18 (d) 48 ((f) 84

7. Tentukan bilangan bulat terkecil n, dimana τ (n) sama dengan :

(a) 1 (c) 3 (e) 14

(b) 2 (d) 6 (f) 100

8. Tentukan semua bilangan bulat positif yang hanya punya dua pembagi positif

9. Tentukan semua bilangan bulat positif yang hanya punya tiga pembagi positif

10. Buktikan bahwa sebuah bilangan positif n adalah bilangan komposit jika dan hanya jika

$$\sigma(n) > n + \sqrt{n}$$

11. Misalkan n adalah sebuah bilangan bulat positif. Buktikan bahwa $\tau(2^n - 1) \geq \tau(n)$

12. Buktikan bahwa jika σ (n) ganjil, maka n adalah sebuah kuadrat atau dua kali sebuah kuadrat dari satu bilangan

13. Tentukan :

(a) $\emptyset$ (100) (c) $\emptyset$ (100!)

(b) $\emptyset$ (256) (d) $\emptyset$ (10!)

14. Tentukan semua bilangan bulat positif n sedemikian sehingga $\emptyset$ (n) sama dengan :

(a) 1 (c) 3 (e) 14

(b) 2 (d) 6 (f) 24

15. Untuk n manakah $\emptyset$ (n) ganjil ?

16. Buktikan bahwa $\emptyset(2n) = \begin{cases} \emptyset(n) \text{ Jika n ganjil} \\ 2\,\emptyset(n) \text{ Jika n genap} \end{cases}$

17. Buktikan $m \mid n$ maka $\emptyset(m) \mid \emptyset(n)$

18. Buktikan bahwa n komposit jika dan hanya jika $\emptyset(n) \le n - \sqrt{n}$

DAFTAR PUSTAKA

Adam , Wlliam W, and Larry Joel Goldstein, (1986). Introduction to Number Theory, Prentice Hall Inc. Englewood Cliffs, New Jersey

Andrews, George E, (1971). Number Theory. W. B Saunders Company, Phidelphia

Burton, David M, (1980). Elementary Number Theory, Allyn and Bacon Inc., Boston

Grosswald, Emil, 91984). Topics from the Theory of Numbers, 2nd edition, Birkhauser, Boston

Rosen, Kenneth H, (1993). Elementary Number Theory and Its Aplication , Addison-Wisley Publishing Company, New York