TEORI BILANGAN

Dr. H. Edy Waluyo, M.Pd.

Dr. Sri Supiyati, M.Pd.Si.

Rody Satriawan, M.Pd.

Neny Endriana, M.Pd.

PROGRAM STUDI PENDIDIKAN MATEMATIKA
FAKULTAS MATEMATIKA DAN IPA
UNIVERSITAS HAMZANWADI PRESS

Teori Bilangan

Penulis : 1. Dr. H. Edy Waluyo, M.Pd.

2. Dr. Sri Supiyati, M.Pd.Si.

3. Rody Satriawan, M.Pd.

4. Neny Endriana, M.Pd.

Editor : 1. Dr. Sri Supiyati, M.Pd.Si.

2. Rody Satriawan, M.Pd.

3. Ahmad Rasidi, M.Pd.

Desain Cover : Rody Satriawan, M.Pd.

Lay Out : Rody Satriawan, M.Pd.

KATA PENGANTAR

Modul Teori Bilangan ini merupakan modul yang dirancang untuk membantu mahasiswa dalam mengikuti program Rekognisi Pembelajaran Lampau yang diselenggarakan oleh KEMENRISTEK DIKTI Republik Indonesia dan dilaksanakan di dua Perguruan Tinggi yaitu Universitas Hamzanwadi sebagai PT Mitra dan Universitas Katolik Widya Mandira sebagai PTDT Mitra.

Dalam modul ini, terdiri dari 12 kegiatan belajar. Setiap awal kegiatan belajar diawali oleh pendahuluan dimana pendahuluan berisikan bahan kajian, capaian pembelajaran, indikator pembelajaran,dan materi prasyarat. Bagian pendahuluan akan sangat membantu mahasiswa dalam mengetahui apa yang perlu dipersiapkan dan juga apa yang akan dicapai dalam setiap kegiatan belajar. Selain itu, materi yang telah disajikan pada setiap kegiatan belajar telah disajikan dalam bahasa yang sederhana sehingga mudah untuk dipahami. Pada setiap akhir kegiatan belajar juga terdapat latihan sebagai wadah bagi mahasiswa untuk lebih mengasah dan menguji pemahaman yang telah diperolehnya.

Akhir kata, semoga modul yang telah disusun ini dapat bermanfaat bagi mahasiswa peserta program Rekognisi Pembelajaran Lampau pada khususnya, dan kita semua pada umumnya.

Selong, 12 Oktober 2020

Tim Penyusun

DAFTAR ISI

HALAMAN JUDUL i

KATALOG ii

KATA PENGANTAR iii

DAFTAR ISI iv

SINOPSIS v

Kegiatan Belajar 1. Induksi Matematik dan Teorema Bilangan 1

Kegiatan Belajar 2. Relasi Keterbagian 15

Kegiatan Belajar 3. FPB dan KPK 18

Kegiatan Belajar 4. Basis Bilangan Bulat 29

Kegiatan Belajar 5. Bilangan Prima 35

Kegiatan Belajar 6. Faktorisasi Tunggal 42

Kegiatan Belajar 7. Definisi dan sifat Kekongruenan 48

Kegiatan Belajar 8. Perkongruenan Linear 61

Kegiatan Belajar 9. Teorema Fermat 74

Kegiatan Belajar 10. Teorema Wilson 83

Kegiatan Belajar 11. Fungsi Tu dan Sigma 89

Kegiatan Belajar 12. Fungsi Mobius Dan Fungsi Bilangan Bulat Diperbesar 94

Daftar Pustaka 95

SINOPSIS

Teori bilangan merupakan cabang matematika yang berkaitan dengan sifat bilangan bulat positif. Kadang-kadang disebut juga sebagai aritmatika yang lebih tinggi. Teori bilagan merupakan salah satu pengajaran matematika tertua dan paling alami. Hingga sekarang ini, teori bilangan dianggap sebagai cabang matematika paling murni, tanpa penerapan langsung ke dunia nyata.Munculnya komputer digital dan komunikasi digital mengungkapkan bahwa teori bilangan dapat memberikan jawaban tak terduga untuk masalah dunia nyata. Pada saat yang sama, peningkatan teknologi komputer memungkinkan para ahli teori bilangan membuat kemajuan luar biasa dalam memfaktorkan bilangan besar, menentukan bilangan prima, menguji dugaan, dan memecahkan masalah numerik yang pernah dianggap tidak terjangkau. Mata kuliah teori bilangan dirancang untuk mahasiswa agar setelah mengikuti mata kuliah ini; mahasiswa menguasaikonsep teori bilangan, yang ditunjukkan dengan kemampuan bekerja secara individu maupun tim dalam menerapkan konsep konsep Induksi matematika, teorema bilangan, relasi keterbagian, FPB dan KPK, basis bilangan bulat, bilangan prima, faktorisasi tunggal, definisi dan sidat kekongruenan, perkongruenan linear, teorema wilson, fungsi tu, teorema sigma, fungsi mobius, dan fungsi bilangan bulat diperbesar dalam menyelesaikan masalah matematika dengan baik.

A. KEGIATAN BELAJAR 1

A.1. Pendahuluan Kegiatan Belajar 1

Bahan kajian : induksi matematik dan teorema bilangan

Capaian pembelajaran : mahasiswa menguasai pemahaman tentang induksi matematik dan teorema binomial.

Indikator pembelajaran :

- mahasiswa mampu membuktikan pernyataan matematika dengan induksi matematik.
- mahasiswa mampu mengimplemnetasikan konsep dan prinsip induksi matematik untuk menyelesaikan masalah.
- mahasiswa mampu mengimplemnetasikan konsep dan prinsip teorema binomial untuk menyelesaikan masalah.

Materi prasyarat : teori himpunan, sistem bilangan bulat, dan notasi sigma.

A.2. Bahan Pembelajaran Kegiatan Belajar 1

A. Induksi Matematik

Induksi matematik merupakan salah satu metode pembuktian dari banyak teorema dalam Teori Bilangan maupun dalam matematika lainnya. Sedangkan Teorema Binomial, selain sebagai dasar, banyak digunakan dalam penuruan beberapa teorema dan pemecahan masalah dalam matematika. Oleh karena itu, pengusaan kemampuan-kemampuan tersebut sangat penting bagi mereka yang akan mempelajari matematika, karena banyak bahasan dalam matematika yang menggunakan prinsip-prinsip tersebut untuk meurunkan teorema atau untuk pemecahan masala. Hampir setiap bahasan berikutnya nanti menggunakan dua prinsip tersebut, baik untuk membuktikan teorema maupun untuk memecahkan soal-soal yang ada.

Induksi matematik meruakan slah satu argumentasi pembuktian suatu teorema atau ernyataan matematika yang semesta pembicaraannya himpunan bilangan bulat atau lebih khusus himpunan bilangan asli. Perhatikan contoh penrnyataan-pernyataan matematik berikut.

Contoh 1.1:

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1) \text{ untuk setiap bilangan asli } n.$$

Benarkah pernyataan ini? Untuk menjawab pertanyaan ini, kita dapat mencoba dengan mensubstitusikan n dalam pernyataan itu sembarang bilangan asli.

Jika $n = 1$, maka pernyataan itu menjadi $1 = \frac{1}{2} \cdot 1(1 + 1)$, atau $1 = 1$ yaitu diperoleh suatu pernyataan yang benar.

Jika $n = 2$ maka pernyataan itu menjadi $1 + 2 = \frac{1}{2} \cdot 2(2 + 1)$, atau $3 = 3$, yaitu diperoleh suatu pernyataan yang benar.

Jika $n = 3$ maka pernyataan itu menjadi $1 + 2 + 3 = \frac{1}{2} \cdot 3(3 + 1)$, atau $6 = 6$, yaitu suatu pernyataan benar pula.

Pembaca dapat melanjutkannya untuk $n = 4$; 5; atau bilangan asli lainnya dan akan selalu memperoleh pernyataan yang bernilai benar. Apakah dengan memberikan beberapa contoh dengan mensubstitusi beberapa bilangan asli pada n dari pernyataan semula dan diperoleh pernyataan-pernyataan yang benar, sudah memberikan bukti tentang kebenaran pernyataan tersebut.

Dalam matematika, pemberian beberapa contoh seperti itu bukan merupakan bukti dari kebenaran suatu pernyataan yang berlaku dalam himpuanan semestanya. Pernyataan pada contoh di atas, himpunan semestanya ialah himpunan semua bilangan asli. Jika kita dapat memberikan contoh untuk tiap bilangan asli n pada pernyataan yang benar, maka hal tersebut dapat merupakan bukti kebenaran dari pernyataan itu, tetapi hal ini tidak efisien dan tidak mungkin kita lakukan, karena banyaknya anggota himpunan bilangan asli ada tak berhingga.

Lalu bagiamana cara membuktikan pernyataan tersebut? Salah satu caranya ialah memandang ruas pertama dari pernyataan itu sebagai deret aritmatika dengan suku pertama $a = 1$; bedanya $b = 1$, suku terakhirnya ialah $U_n = n$ dan memiliki n buah suku, maka jumlah deret itu adalah

$$S_n = \frac{1}{2} n(a + U_n)$$

$$= \frac{1}{2} n(1 + n) = \frac{1}{2} n(n + 1),$$ yaitu ruas kedua dari pernyataan yang dibuktikan.

Cara lain untuk membuktikan pernyataan itu adalah dengan induksi matematik. Langkah-langkah pembuktian dengan induksi matematik adalah sebagai berikut.

Misalkan $p(n)$ adalah suatu proposisi yang akan dibuktikan benar untuk setiap bilangan asli n. Langkah-langkah pembuktiaannya dengan induksi matematik sebagai berikut:

Langkah (1) : Ditunjukkan bahwa $p(1)$ benar

Langkah (2) : Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k dan ditunjukkan bahwa $p(k + 1)$ benar.

Jika langkah-langkah (1) dan (2) berhasil ditunjukkan kebenarannya, maka selanjutnya disimpulkan bahwa $p(n)$ benar untuk setiap bilangan asli n. Mengapa demikian? Karena langkah (1) yaitu $p(1)$ benar, dan karena langkah (2), maka $p(2)$ benar pula. Selanjutnya, karena $p(2)$ benar, menurut langkah (2), maka $p(3)$ benar pula. Dan menurut langkah (2) lagi, $p(4)$ benar pula, dan seterusnya sehingga $p(n)$ benar untuk setiap bilangan asli n. Langkah (1) di atas sering disebut *basis (dasar) induksi*, dan langkah (2) disebut *langkah induksi*.

Kita sekarang akan menerapkan langkah-langkah pembuktian dengan induksi matematik itu untuk mmbuktikan pernyataan pada contoh 1.1 di atas.

Contoh 1.2:

Buktikan bahwa $1+2+3+\cdots+n=\frac{1}{2}n(n+1)$ untuk setiap bilangan asli n.

Bukti :

Misalkan $p(n)$ menyatakan $1+2+3+\cdots+n=\frac{1}{2}n(n+1)$

(1) $p(1)$ adalah $1=\frac{1}{2}1(1+1)$ yaitu $1=1$ jelas benar.

(2) Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k, yaitu $1+2+3+\ldots+k=\frac{1}{2}k(k+1)$ benar

Selanjutnya harus ditunjukkan bahwa $p(k+1)$ benar, yaitu :

$$1+2+3+\cdots.+k+(k+1)=\frac{1}{2}(k+1)(k+2)$$

Hal ini ditunjukkan sebagai berikut:

$$\begin{aligned}1+2+3+\cdots+k+(k+1) &= (1+2+3+\cdots+k)+(k+1)\\ &= \tfrac{1}{2}k(k+1)+(k+1)\text{(karena diasumsikan)}\\ &= (k+1)\left(\frac{1}{2}k+1\right)\\ &= \frac{1}{2}(k+1)(k+2)\end{aligned}$$

Jadi, $1+2+3+\cdots+k+(k+1)=\frac{1}{2}(k+1)(k+2)$ berarti $p(k+1)$ benar.

Contoh 1.3:

Hitunglah $1+3+5+\cdots+(2n-1)$!!

Jawab :

$1+3+5+\cdots+(2n-1)$ sebagai deret aritmatika dengan suku pertama $a=1$, beda $b=2$ dan banyaknya suku adalah n serta suku terakhirnya $U_n=(2n-1)$. Maka jumlahan tersebut dapat dihitung denga rumus jumlahan deret aritmatika yaitu

$$S_n = \frac{1}{2}n(a + U_n)$$

$$S_n = \frac{1}{2}n(1 + 2n - 1) = n^2$$

Jadi, $1 + 3 + 5 + \ldots + (2n - 1) = n^2$

Tetapi jika kita lupa atau belum mngerti rumus deret aritmatika tersebut, maka hal tersebut tidak dapat kita lakukan. Kita dapat membuat dugaan dengan mencoba jumlah beberapa suku berikut:

$$1 = 1$$
$$1 + 3 = 4$$
$$1 + 3 + 5 = 9$$
$$1 + 3 + 5 + 7 = 16$$

Dan seterusnya

$$1 + 3 + 5 + \cdots + 99 = \cdots$$

Tampak bahwa jumlahan-jumlahan ini merupakan bilangan kuadrat sempurna, sehingga kita bisa menduga bahwa:

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2$$

Tetapi dugaan ini baru merupakan jawabn sementara, sehingga harus dibuktikan kebenarannya. Pembuktiannya dapat dilakukan dengan induksi matematik sebagai berikut:

Misalkan $p(n)$ menyatakan $1 + 3 + 5 + \ldots + (2n - 1) = n^2$

(1) $p(1)$ adalah $1 = 1^2$, jelas benar.

(2) Dimisalkan $p(k)$ benar untuk suatu bilangan asli k yaitu $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ dan ditunjukkan bahwa $p(k + 1)$ benar, yaitu $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$.

Hal ini ditunjukkan sebagai berikut:

$$1 + 3 + 5 + \cdots + (2k - 1) + (2 + 1) = k^2 + 2k + 1 = (k + 1)^2$$

Sehingga $p(k + 1)$ benar.

Jadi, $p(n)$ benar untuk setiap bilangan asli n.

Contoh 1.4:

Buktikan bahwa $3 + 7 + 11 + \cdots + (4n - 1) = 2n^2 + n$ untuk setiap bilangan asli n.

Bukti :

Misalkan $p(n)$ menyatakan $3 + 7 + 11 + \cdots + (4n - 1) = 2n^2 + n$

(1) $p(1)$ adalah $3 = 2(1^2) + 1$ yaitu $3 = 3$ (benar).

(2) Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k, yaitu $3 + 7 + 11 + \cdots + (4k - 1) = 2k^2 + k$.

Selanjutnya harus ditunjukkan bahwa $p(k + 1)$ benar, yaitu :

$$3 + 7 + 11 + \cdots + (4k - 1) + [4(k + 1) - 1] = 2(k + 1)^2 + (k + 1)$$

Hal ini ditunjukkan sebagai berikut:

$3 + 7 + 11 + \cdots + (4k - 1) + [4(k + 1) - 1] = 2(k + 1)^2 + (k + 1)$

$= (2k^2 + k) + [4(k + 1) - 1]$karena diasumsikan

$= 2k^2 + k + 4k + 4 - 1$

$= 2k^2 + 5k + 3$

$= 2k^2 + 5k + 3$

$= 2k^2 + 4k + 2 + k + 1$

$= 2(k^2 + 2k + 1) + k + 1$

$= 2(k^2 + 1) + (k + 1)$

Jadi, $3 + 7 + 11 + \cdots + (4k - 1) = 2k^2 + k$ berarti $p(k + 1)$ benar.

Contoh 1.5:

Buktikan bahwa $2 + 4 + 6 + 8 + \cdots + 2n = n^2 + n$ untuk setiap bilangan asli n.

Bukti :

Misalkan $p(n)$ menyatakan $2 + 4 + 6 + 8 + \cdots + 2n = n^2 + n$.

(1) $p(1)$ adalah $2 = 1^2 + 1$ yaitu $2 = 2$ (benar).

(2) Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k, yaitu $2 + 4 + 6 + 8 + \cdots + 2k = k^2 + k$.

Selanjutnya harus ditunjukkan bahwa $p(k + 1)$ benar, yaitu :

$$2 + 4 + 6 + 8 + \cdots + 2k + 2(k + 1) = (k + 1)^2 + (k + 1)$$

$= k^2 + 2k + 1 + k + 1$

$= k^2 + k + 2k + 2$

Hal ini ditunjukkan sebagai berikut:

$2 + 4 + 6 + 8 + \cdots + 2k + 2(k + 1) = (k + 1)^2 + (k + 1)$

$= (k^2 + k) + 2(k + 1)$ (Karena diasumsikan)

$= k^2 + k + 2k + 2$

$= k^2 + 3k + 2$

Jadi, $2 + 4 + 6 + 8 + \cdots + 2k + 2(k+1) = (k+1)^2 + (k+1)$ berarti $p(k+1)$ benar.

Contoh 1.6:

Buktikanlah bahwa untuk setiap bilangan asli n berlaku:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Bukti:

Misalkan $p(n)$ adalah $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

(1) $p(1)$ adalah $1^2 = \frac{1}{6} \cdot 2 \cdot 3$ yaitu $1 = 1$ (benar)

Jadi, $p(1)$ benar.

(2) Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k yaitu $1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1)$. Dan harus ditunjukkan bahwa $p(k+1)$ benar, yaitu ditunjukkan bahwa $1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{1}{6}(k+1)(k+2)(2k+3)$.

Hal ini ditunjukkan sebagai berikut:

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{1}{6}k(k+1)(2k+1)(k+1)^2 \\ &= (k+1)\left[\frac{1}{6}k(2k+1)\right] + (k+1) \\ &= (k+1)\left[\frac{1}{6}(2k^2 + k + 6k + 6)\right] \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3) \end{aligned}$$

Jadi, $p(k+1)$ benar.

Selanjutnya dari langkah-langkah (1) dan (2) disimpulkan bahwa $p(n)$ benar untuk setiap bilangan asli n.

B. Teorema Binomial

Kita akan mengingat kembali pengertian kombinasi sejumlah r proyek yang diambil dari n obyek. Banyaknya kombinasi dari r obyek yang diambil dari n obyek $(r \leq n)$ adalah:

$$C(n,r) = \binom{n}{r} = \frac{n!}{(n-r)!\,r!}$$

Contoh 1.7:

1. Misalkan ada 5 obyek yaitu a, b, c, d, dan e. Jika dari 5 obyek ini diambil 3 obyek, maka banyaknya cara pengambilan 3 obyek tersebut adalah

2. Misalkan dalam sutau kotak terdapat 3 kelereng merah dan 4 kelereng putih. Jika kita mengambil 3 kelereng merah dari dalam kotak tersebut, maka banyaknya cara pengambilan ada

$$\binom{3}{3} = \frac{3!}{0!\,3!} = \frac{1\cdot 2\cdot 3}{1\cdot 1\cdot 2\cdot 3\cdot} = 1 \text{ cara}$$

Tetapi jika kita mengambil 3 kelereng dari dalam kotak itu, maka banyaknya cara pengambilan ada

$$\binom{7}{3} = \frac{7!}{4!\,3!} = \frac{7\cdot 6\cdot 5}{1\cdot 2\cdot 3\cdot} = 35 \text{ cara}$$

Jika kita mengambil 4 kelereng dari dalam kotak tersebut, maka banyaknya cara pengambilan ada

$$\binom{7}{4} = \frac{7!}{3!\,4!} = \frac{7\cdot 6\cdot 5}{1\cdot 2\cdot 3\cdot} = 35 \text{ cara}$$

3. Misalkan ada tiga kotak yang terambil masing-masing berisi satu bola merah dan satu bola putih. Dari tiap-tiap kotak diambil satu bola, sehingga terambil tiga bola.

   Banyaknya cara pengambilan 3 bola tersebut, agar terambil bola merah semua ada $\binom{3}{3} = 1$ cara. Banyaknya cara pengambilan 3 bola tersebut, agar terambil dua bola merah ada $\binom{3}{2} = 3$ cara. Banyaknya cara pengambilan 3 bola itu, agar terambil satu bola merah ada $\binom{3}{1} = 3$ cara. Banyaknya cara pengambilan 3 bola itu, agar tak terambi bola merah ada $\binom{3}{0} = 1$ cara.

Contoh terakhir ini akan digunakan untuk menyatakan suku banyak yang merupakan penjabaran dari $(m+p)^3$. Perpangkatan ini dapat dinyatakan sebagai perkalian berulang dengan 3 faktor sama yaitu: 3

$$(m+p)(m+p)(m+p) = mmm + mmp + mpm + pmm + ppm + pmp + mpp + ppp$$

Tiap suku dari ruas kanan kesamaan ini terdiri dari 3 faktordan masing-masing berturut-turut diambil dari faktor pertama, faktor kedua dan faktor ketiga dari ruas pertama. Memperhatikan contoh 1.7 nomor 3 di atas, maka

Banyaknya suku dengan tiga m adalah $\binom{3}{3} = 1$,

Banyaknya suku dengan dua m ada $\binom{3}{2} = 1$,

Banyaknya suku dengan satu m ada $\binom{3}{1} = 1$, dan

Banyaknya suku tanpa m ada $\binom{3}{0} = 1$,

Pada kesamaan terakhir itu, jika suku-suku sejenisnya dijumlahkan, maka akan diperoleh:

$$(m+p)^3 = m^3 + 3mp^2 + 3p^2m + p^3$$

Koefisien-koefisien suku-suku dari ruas kanan dari kesamaan terakhir ini dapat dinyatakan dengan kombinasi-kombinasi banyaknya m dalam tiap sukunya, sehingga kesamaan itu dapat ditulis sebagai berikut.

$$(p+m)^3 = \binom{3}{0} p^3 + \binom{3}{1} mp^2 + \binom{3}{2} m^2p + \binom{3}{3} m^3$$

Dengan argumentasi yang mirip dengan ilustrasi di atas, kita dapat menuliskan kesamaan-kesamaan berikut ini. Coba periksalah kebenaran !

$(a+x)^1 = \binom{1}{0} a + \binom{1}{1} x$

$(a+x)^2 = \binom{2}{0} a^2 + \binom{2}{1} ax + \binom{2}{2} x^2$

$(a+x)^3 = \binom{3}{0} a^3 + \binom{3}{1} a^2x + \binom{3}{2} ax^2 + \binom{3}{3} x^3$

$(a+x)^4 = \binom{4}{0} a^4 + \binom{4}{1} a^3x + \binom{4}{2} a^2x^2 + \binom{4}{3} ax^3 + \binom{4}{4} x^4$

… … … …

$(a+x)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}x + \binom{n}{2} a^{n-2}x^2 + \cdots + \binom{n}{k} x^{n-k}x^k + \cdots + \binom{n}{n} x^n$

Kesamaan terakhir ini baru merupakan dugaan, karena kesamaan terakhir diperoleh dengan penalaran induktif. Oleh karena itu, kesamaan itu perlu dibuktikan kebenarannya. Kita perlu beberapa persiapan berikut ini:

Dari rumus kombinasi di atas, yaitu:

$$C(n,r) = \binom{n}{r} = \frac{n!}{(n-r)!\,r!}$$

Kita dapat memahami bahwa:

$$\binom{n}{n-r} = \frac{n!}{r!\,(n-r)!}$$

Jadi,

$$\binom{n}{r} = \binom{n}{n-r}$$

Teorema 1.1:

Jika $r \leq n$, maka $\binom{n}{r} = \binom{n}{n-r}$

Teorema ini sering disebut sifat simetrik dari koefisien binomial. Sifat ini membantu kita untuk menghitung lebih mudah nilai suatu kombinasi.

Contoh 1.8:

1) $\binom{20}{18} = \binom{20}{2} = \frac{20 \cdot 19}{1 \cdot 2} = 190$

2) $\binom{30}{27} = \binom{30}{3} = \frac{30 \cdot 29 \cdot 28}{1 \cdot 2 \cdot 3} = 4060$

Perhatikan contoh berikut ini:

Contoh 1.9:

Misalkan dalam suatu perkumpulan terdiri dari 10 orang dan akan dipilih 3 orang sebagai utusan yang mewakilinya, maka banyaknya pilihan 3 orang dari 10 orang tersebut ada $\binom{10}{3}$ pilihan. Sekarang, jika pemilihan 3 orang tersebut tidak menyertakan seorang tertentu dari 10 orang tersebut, berarti 3 orang itu dipilih dari 9 orang, maka banyaknya pilihan 3 orang dari 9 orang itu ada $\binom{9}{3}$ pilihan. Selanjutnya, jika seorang tertentu yang tidak diikutkan dalam pemilihan tadi harus ikut pada setiap pemilihan, berarti untuk memilih 3 orang tu, kita tinggal memilih 2 orang dari 9 orang, maka banyaknya pilihan 3 orang tersebut ada $\binom{9}{2}$ pilihan. Dari argumentasi ini, kita memperoleh hubungan bahwa

$$\binom{10}{3} = \binom{9}{3} + \binom{9}{2}$$

Periksalah bahwa kesamaan tersebut benar! Secara umum hubungan itu dinyatakan sebagai teorema berikut ini.

Teorema 1.2.

Jika k dan r bilangan-bilangan asli dengan $k > r$, maka

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}$$

Bukti:

$$\binom{k}{r-1} + \binom{k}{r} = \frac{k!}{(k-r+1)!\,(r-1)!} + \frac{k!}{(k-r)!\,r!}$$

$$= \frac{k!\,r + k!\,(k-r+1)}{(k+1-r)!\,r!}$$

$$= \frac{k!\,(r+k-r+1)}{(k+1-r)!\,r!}$$

$$= \frac{k!\,(k+1)}{(k+1-r)!\,r!}$$

$$= \frac{(k+1)!}{(k+1-r)!\,r!}$$

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}$$

Sekarang kita siap untuk membuktikan kebenaran penjabaran suku dua berpangkat n di atas dengan mengambil $a = 1$ dan $x = a$, yang selanjutnya disebut teorema binomial.

Teorema 1.3 (Teorema Binomial):

$$(1+a)^n = \binom{n}{0} + \binom{n}{1} a + \binom{n}{2} a^2 + \binom{n}{3} a^3 + \cdots + \binom{n}{k} a^k + \cdots + \binom{n}{n} a^n$$

Untuk setiap bilangan asli-n.

Bukti:

Kita buktikan dengan induksi matematik:

(1) Untuk $n = 1$, maka $(1+a)^1 = \binom{1}{0} + \binom{1}{1} a = 1 + a$, benar.

(2) Diasumsikan bahwa pernyataan benar untuk $n = k$, yaitu:

$$(1+\mathrm{a})^{\mathrm{k}} = \binom{\mathrm{k}}{0} + \binom{\mathrm{k}}{1}\mathrm{a} + \binom{\mathrm{k}}{2}\mathrm{a}^2 + \binom{\mathrm{k}}{\mathrm{r}}\mathrm{a}^{\mathrm{r}} + \cdots + \binom{\mathrm{k}}{\mathrm{r}}\mathrm{a}^{\mathrm{r}} + \cdots + \binom{\mathrm{k}}{\mathrm{k}}\mathrm{a}^{\mathrm{k}}$$

Selanjutnya akan ditunjukkan benar untuk $n = k + 1$.

$$(1+a)^{k+1} = (1+a)^k (1+a)$$

$$= \left[\binom{k}{0} + \binom{k}{1} a + \binom{k}{2} a^2 + \cdots + \binom{k}{k} a^k\right](1+a)$$

$$= \binom{k}{0} + \left[\binom{k}{0} + \binom{k}{1}\right] a + \left[\binom{k}{1} + \binom{k}{2}\right] a^2 + \cdots + \left[\binom{k}{k-1} + \binom{k}{k}\right] a^k + \binom{k}{k} a^{k+1}$$

$$= \binom{k+1}{0} + \binom{k+1}{1} a + \binom{k+1}{2} a^2 + \cdots + \binom{k+1}{k} a^k + \binom{k+1}{k+1} a^{k+1}$$

Dari langkah-langkah (1) dan (2) dapat disimpulkan bahwa teorema terbukti benar untuk setiap bilangan asli n.

Koefisien-koefisien a pada ruas kanan pada teorema 1.3 di atas disebut koefisien binomial.

Contoh :

1) Koefisien x^9 dari penjabaran $(1+x)^{12}$ adalah $\binom{12}{9} = \frac{12\cdot 11\cdot 10}{1\cdot 2\cdot 3} = 660$.

2) Koefisien x^8 dari penjabaran $(1+1)^{11}$ adalah $\binom{11}{9} = \frac{11\cdot 10\cdot 9}{1\cdot 2\cdot 3} = 165$.

Jika pada teorema binomial tersebut $a = 1$, maka diperoleh kesamaan:

$$(1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n}$$

$$\Leftrightarrow 2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n}$$

Kesamaan terakhir ini dinyatakan sebagai teoema berikut ini.

Teorema 1.4:

Jika n suatu bilangan asli, maka:

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n}=2n$$

Selanjutnya perhatikan penurunan rumus berikut ini:

$$\begin{aligned}\binom{n}{k}\binom{k}{m} &= \frac{n!}{(n-k)!\,k!}\cdot\frac{k!}{(k-m)!\,m!}\\ &= \frac{n!}{(n-k)!\,k!}\cdot\frac{(n-m)!}{(n-m-k+m)!\,(k-m)!}\\ &= \binom{n}{m}\binom{n-m}{k-m}\end{aligned}$$

Rumus yang diperoleh ini dinyatakan sebagai teorema berikut ini.

Teorema 1.5:

Jika n, m, dan k bilangan-bilangan asli dengan $n>k>m$, maka

$$\binom{n}{k}\binom{k}{m}=\binom{n}{m}\binom{n-m}{k-m}$$

Untuk memperjelas makna dari teorema ini, perhatikan contoh berikut!

Contoh:

Suatu perkumpulan terdiri dari 15 orang. Akan dibentuk suatu pengurus dari perkumpulan tersebut yang terdiri 5 orang dan 2 orang diantaranya sebagai inti.

Maka banyaknya pilihan pengurus itu adalah

$$\binom{15}{5}\binom{5}{2}=\frac{15\cdot 14\cdot 13\cdot 12\cdot 11}{1\cdot 2\cdot 3\cdot 4\cdot 5}\cdot\frac{5\cdot 4}{1\cdot 2}=30.030$$

Pemilihan tersebut dapat pula dilakukan dengan memilih 2 orang pengurus inti dari 15 orang dan selanjutnya untuk melengkapi pengurus inti dari 15 orang dan selanjutnya untuk melengkapi pengurus itu dipilih 3 orang dari 13 orang (yang 2 orang telah telah terpilih sebagai pengurus inti).

Maka banyaknya pilihan pengurus ini adalah

$$\binom{15}{2}\binom{13}{3}=\frac{15\cdot 14}{1\cdot 2}\cdot\frac{13\cdot 12\cdot 11}{1\cdot 2\cdot 3}=30.030$$

Tampak di sini bahwa $\binom{15}{5}\binom{5}{2}=\binom{15}{5}\binom{13}{3}$

Pada teorema 1.5 tersebut, jika $m=1$, maka diperoleh :

$$k\binom{n}{k}=n\binom{n-1}{k-1}$$

Hubungan ini dinyatakan sebagai teorema berikut ini.

Teorema 1.6:

Jika n dan k bilangan-bilangan asli dengan $n \geq k$, maka

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Koefesien-koefisien binomial pada teorema binomial di atas dapat kita susun secara rekursif, seprti tampak pada gambar 1. dan sering disebut juga dengan segitiga Pascal sebagai berikut:

1					1						
1			6				1				
2				1		2		1			
3			1		3		3		1		
4		1		4		6		4		1	
5	1		5		10		10		5		1

Gambar 1

Bilangan-bilangan segtiga Pascal tersebut dapa dibangun tanpa proses rekursif dengan notasi kombinatorik seperti tampak pada gambar 2.

$$\binom{0}{0}$$

$$\binom{1}{0} \qquad \binom{1}{1}$$

$$\binom{2}{0} \qquad \binom{2}{1} \qquad \binom{2}{2}$$

$$\binom{3}{0} \qquad \binom{3}{1} \qquad \binom{3}{2} \qquad \binom{3}{3}$$

$$\binom{4}{0} \qquad \binom{2}{1} \qquad \binom{2}{2} \qquad \binom{2}{3} \qquad \binom{2}{4}$$

$$\binom{2}{0} \qquad \binom{2}{1} \qquad \binom{2}{2} \qquad \binom{2}{3} \qquad \binom{2}{4} \qquad \binom{2}{5}$$

$$\binom{6}{3}$$

Gambar 3

Perhatikan anak panah 5 pada gambar 1 dan gambar 2

Anak panah 6 itu menunjukkan bahwa $1 + 3 + 6 + 10 = 20$ atau $\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \binom{6}{3}$

Fakta ini secara umum dapat dituliskan sebagai berikut:

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} = \binom{k+r+1}{k+r}$$

Anak panah 6 pada gambar 1 dan gambar 2 berturut-turut menunjukkan bahwa

$$1 + 3 + 6 + 10 = 20 \text{ atau } \binom{2}{0} + \binom{3}{1} + \binom{4}{2} + \binom{5}{3} = \binom{6}{3}$$

Fakta ini secara umum dapat dinyatakan sebagai berikut:

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} = \binom{k+r+1}{k+r}$$

Selanjutnya dua fakta ini dinyatakan sebagai teorem berikut ini.

Teorema 1.7:

Jika k dan r bilangan-biangan asli dengan $k \geq r$ maka:

a. $\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+r}{r} = \binom{k+r+1}{r}$

b. $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} = \binom{k+r+1}{k+1}$

Buktikan teorema 1.7 tersebut sebagai latihan! (Gunakan induksi matematik).

Contoh:

Buktikanlah bahwa $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdots + (n-2)(n-1) = 3!\binom{n+3}{4}$

Jawab:

$$(k-2)(k-1)k = \frac{k!}{(k-3)!} = \frac{3!\,k!}{(k-1)!\,3!} = 3!\binom{k}{3}$$

Maka jumlahan pada ruas kiri dalam soal cerita tersebut dapat dinyatakan sebagai berikut:

$$3!\binom{3}{3} + 3!\binom{4}{3} + 3!\binom{5}{3} + \cdots + 3!\binom{n}{3} = 3!\left[\binom{3}{3} + \binom{4}{3} + \binom{5}{3} + \cdots + \binom{n}{3}\right]$$

$= 3!\binom{n+1}{4}$ (*Sesuai* teorema 1.7b di atas).

Contoh 1.16:

Buktikan bahwa

$$1^2 + 2^2 + 3^2 + 4^2 + \cdots + n^2 = 2\binom{n+1}{4} + \binom{n+1}{4}$$

Jawab:

Perhatikan bahwa k^2 dapat ditulis sebagai $k^2 = k(k-1) + k$

Sehingga ruas kiri dari soal tersebut dapat ditulis sebagai:

Contoh 1.17:

Buktikan bahwa $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$!

Jawab:

Pada teorema binomial di atas, jika $a = -1$ maka diperoleh:

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^k\binom{n}{k}+\cdots+(-1)^n\binom{n}{n}=(1-1)^n$$

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^k\binom{n}{k}+\cdots+(-1)^n\binom{n}{n}=0$$

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots$$

Selanjutnya, *mengingat* teorema 1.4 diperoleh:

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots=2^{n-1}$$

A.4. Latihan Kegiatan Belajar 1

Selesaikan soal-soal berikut ini dengan benar!

1. Buktikan bahwa $4+10+16+\ldots+(6n-2)=n(3n-1)$ untuk setiap bilangan asli!
2. Buktikan bahwa $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)=\frac{1}{3}n(n+1)(n+2)$ untuk setiap bilangan asli!
3. Buktikan $1^3+2^3+3^3+\ldots+n^3=\frac{1}{3}n(4n^2-1)$ untuk setiap bilangan asli!
4. Buktikan bahwa $\sum_{i=1}^{n}(2i+5)=n(n+6)$ untuk setiap bilangan asli!
5. Tunjukkan $1+2+3+4+\ldots+n=\binom{n+1}{2}$!
6. Buktkan bahwa untuk $n\geq 1$, berlaku $\binom{n}{k}=\binom{n}{k+1}$ jika dan hanya jika n suatu bilangan gasal dan $k=\frac{1}{2}(n-1)$!
7. Bukitkan bahwa $\binom{n-1}{k}=(k+1)\binom{n}{k+1}$!
8. Jika $0\leq k\leq r\leq n$, buktikan bahwa $\binom{n}{r}\binom{r}{k}=\binom{n}{k}\binom{n-k}{k+1}$!
9. Tentukan $\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\ldots$!
10. Tentukan $\sum_{k=1}^{n}12(k-1)k(k+1)$!

B. KEGIATAN BELAJAR 2

B.1. Pendahuluan Kegiatan Belajar 2

Bahan kajian : relasi keterbagian

Capaian pembelajaran : mahasiswa menguasai pemahaman tentang relasi keterbagian.

Indikator pembelajaran :

- mahasiswa mampu merumuskan konsep relasi keterbagian.
- mahasiswa mampu mengimplemnetasikan konsep dan prinsip dari relasi keterbagian untuk menyelesaikan masalah.

Materi prasyarat : teori himpunan dan sistem bilangan bulat.

B.2. Bahan Pembelajaran Kegiatan Belajar 2

A. Relasi Keterbagian

Semesta pembicaraan dalam teori bilangan adalah himpunan semua bilangan bulat. Bilangan-bilangan bulat dinyatakan dengan huruf-huruf latin kecil $a, b, c, \ldots, m, n$ dan sebagainya yang dapat bernilai positif, negatif, atau nol. Namun, banyak pembahasan dalam teori bilangan yang semesta pembicaraannya terbatas pada himpunan semua bilangan asli.

Definisi 2.1:

Bilangan bulat a membagi (habis) bilangan bulat b ditulis $a|b$, jika dan hanya jika ada bilangan bulat k sedemikian hingga $b = ka$. Jika a tidak membagi (habis) b, maka ditulis $a \nmid b$.

Contoh 2.1:

1) $5|30$, karena ada bilangan bulat, yaitu 6, sedemikian hingga $5 \cdot 6 = 30$.
2) $7|-21$, karena ada bilangan bulat, yaitu -3, sedemikian hingga $7(-3) = -21$.
3) $-6|24$, karena ada bilangan bulat, yaitu -4, sedemikian hingga $-6(-4) = 24$.
4) $8 \nmid 27$, karena tidak ada biangan bulat k, sedemikian hingga $8k = 27$.

Bilangan bulat k pada definisi 2.1 tersebut adalah tunggal, karena jika ada bilangan bulat m selain k sedemikian hingga

$$b = ma \text{ dan } b = ka$$

$$\text{maka } ma = ka$$

$$\text{sehingga } m = k$$

Jika $a = 0$ dan $b \neq 0$, maka tidak ada bilangan k yang memenuhi $b = ka$. Tetapi jika $a = 0$ dan $b = 0$, maka terdapat tak hingga bilangan bulat k yang memenuhi $b = ka$.

Istilah:

Untuk seterusnya istilah "membagi habis" dan "terbagi habis" berturut-turut disingkat menjadi "membagi" dan "terbagi", "a membagi b" dan "b terbagi a" keduanya simbolkan dengan "$a|b$," adalh "a faktor dari b", "a adalah pembagi dari b" atau "b adalah kelipatan dari a".

Jika a, b, dan k adalah bilangan-bilangan bulat dengan $a \neq 0$ dan $b = ka$, maka k disebut hasil bagi (*quotient*) dari b oleh a. Disebut pula bahwa k adalah faktor dari b yang menjadi komplemen (sekawan) dari a, atau dengan singkat dikatakan bahwa a dan k adalah pembagi-pembagi sekawan (komplementer) dari b.

Jika $a|b$, menurut definisi 2.1, maka ada bilangan bulat m sehingga $c = mb$. Karena $b = ka$, maka $c = mka$, sehingga menurut definisi 2.1 diperoleh $a|c$. Hal ini berarti relasi keterbagian pada himpunan bilangan bulat mempunyai sifat transitif. Sifat ini dinyatakan sebagai teorema berikut:

Teorema 2.1:

Jika $a|b$ dan $b|c$, maka $a|c$.

Jika $a|b$ yaitu a membagi habis b, maka a membagi habis setiap kelipatan b, yaitu $a|mb$, untuk setiap bilangan bulat m. Hal ini dinyatakan sebagai teorema berikut ini:

Teorema 2.2:

Jika $a|b$ maka $a|mb$ untuk setiap bilangan bulat m.

Jika $a|b$ dan $a|c$, menurut definisi 2.1 , maka diperoleh $b = ka$ dan $c = ma$ untuk bilangan-bilangan bulat k dan m.

Dari dua kesamaan ini dapat diperoleh bahwa:

(i) $b + c = (k + m)a$ berarti $a|(b + c)$

(ii) $b - c = (k - m)a$ berarti $a|(b - c)$ dan

(iii) $bc = (kma)a$ berarti $a|bc$.

Ketiga kesimpulan ini dinyatakan sebagai ini:

Teorema 2.3:

Jika $a|b$ dan $a|c$, maka $a|(b + c)$, $a|(b - c)$, dan $a|bc$.

Teorema terakhir ini dapat diperluas dalam sebuah pernyataan yang dinyatakan dalam teorema berikut ini ini yang biasa disebut sifat linearitas.

Teorema 2.4: (Sifat Linieritas)

Jika $a|b$ dan $a|c$, maka $a(mb + nc)$ untuk setiap bilangan bulat m dan n.

Bukti:

Karena $a|b$ dan $a|c$, menurut teorema 2.2, maka $a|mb$ dan $a|nc$ untuk setiap bilangan-bilangan m dan n. Selanjutnya, menurut teorema 2.3, maka $a|(mb + nc)$.

Teorema 2.5:

(i) $a|a$ untuk setiap bilangan bulat a (sifat reflektif).

(ii) Jika $a|b$ maka $ma|mb$ untuk setiap bilangan bulat m.

(iii) Jika $ma|mb$ dengan $m \neq 0$, maka $a|b$.

(iv) $1|a$ dan $a|0$.

(v) Jika $0|a$ maka $a = 0$.

(vi) Jika $a|b$ dengan $b \neq 0$, maka $|a| \leq |b|$.

(vii)Jika $a|b$ dengan $b|a$, maka $|a| \leq |b|$.

B.4. Latihan Kegiatan Belajar 2

Selesaikan soal-soal berikut ini dengan benar!

1. Buktikan bahwa jika $a|b$ untuk setiap bilangan bulat m!
2. Jika $a|b$, tunjukkan bahwa $(-a)|b$, $a|(-b)$, dan $(-a)|(-b)$!
3. Buktikan bahwa jika $a|b$ dan $c|d$, maka $ac|bd$!
4. Jika $a|b$ dan $a|c$, buktikan bahwa $a^2|bc$!
5. Buktikan bahwa jika $a|(b-1)$, maka $a|(b^4-1)$!
6. Benarkah pernyataan : jika $a|(b-c)$, maka $a|b$ atau $a|c$. Berilah alasan!
7. Buktikan bahwa hasilkali dua bilangan bulat berurutan selalu terbagi oleh dua !
8. Buktikan bahwa hasilkali tiga bilangan bulat berturutan selalu terbagi oleh 6!
9. Buktikan bahwa hasilkali tiga bilangan bulat berturutan selalu terbagi oleh 3!
10. Buktikan bahwa $4 \nmid (a^2 + 2)$, untuk setiap bilangan bulat a!

C. KEGIATAN BELAJAR 3

C.1. Pendahuluan Kegiatan Belajar 3

Bahan kajian : induksi matematik dan teorema bilangan

Capaian pembelajaran : mahasiswa menguasai pemahaman tentang faktor persekutuan terbesar dan kelipakatan persekutuan terkecil.

Indikator pembelajaran :

- mahasiswa mampu merumuskan konsep dan mengimplementasikan faktor persekutuan terbesar untuk menyelesaikan masalah.
- mahasiswa mampu merumuskan konsep dan mengimplementasikan kelipatan persekutuan terkecil untuk menyelesaikan masalah.

Materi prasyarat : teori himpunan, sistem bilangan bulat, dan relasi keterbagian.

C.2. Bahan Pembelajaran Kegiatan Belajar 3

A. Faktor Persekutuan Terbesar (FPB)

Kita telah mengetahui bahwa semua faktor bulat positif dari 30 adalah $1, 2, 3, 5, 6, 10, 15$, dan 30.

Sedangkan semua faktor-faktor persekutuan (pembagi-pembagi bersama) dari 30 dan 45 adalah $1, 3, 5$, dan 15.

Dan faktor persekutuan terbesar dari 30 dan 45 adalah 15.

Secara umum, pengertian tentang faktor pesekutuan dari dua bilangan bulat dituliskan sebagai definis berikut ini.

Definisi 3.1:

Jika a dan b adalah bilangan-bilangan bulat, maka bilangan bulat d disebut faktor persekutuan dari a dan b jika dan $d|a$ dan $d|b$.

Karena 1 adalah pembagi (faktor) dari setiap bilangan bulat, maka 1 adalah faktor persekutuan dari dua bilangan bulat merupakan faktor persekutuan dari a dan b. Jadi, himpunan semua persekutuan dari a dan b tidak pernah kosong.

Setiap bilangan bulat kecuali nol selalu membagi nol, sehingga jika $a = b = 0$, maka setap bilangan bulat merupakan faktor persekutuan dari a dan b. Dalam hal ini, himpunan semua faktor persekutuan bulat positif dari a dan b merupakan himpunan tak hingga.

Jika sekurang-kurangnya satu dari a dan b tidak sama dengan nol, maka himpunan semua faktor persekutuan bulat positif dari a dan b merupakan himpunan berhingga, sehingga mesti ada anggota dari himpunan tersebut yang terbesar dan disebut faktor persekutuan terbesar (FPB) dari a dan b. Secara formal, hal tersebut dinyatakan sebagai definisi berikut ini.

Definisi 3.2:

Jika a dan b bilangan-bilangan bulat yang sekurang-kurangnya satu diantaranya tidak sama dengan nol, maka faktor persekutuan terbesar (FPB) dari a dan b diberi simbol "(a, b) adalah suatu bilangan positif, misalnya d, yang memenuhi

a. $d|a$ dan $d|b$ serta

b. Jika $e|a$ dan $e|b$, maka $e \leq d$.

Dari definisi tersebut dapat dimengerti bahwa jika $(a, b) = d$, maka $d \geq 1$. Dan jika ada faktor persekutuan lain, misalnya e, maka $e \geq d$.

Contoh 3.1:

Faktor-faktor bulat positif dari -12 adalah 1, 2, 3, 4, 6, dan 12.

Faktor-faktor bulat positif dari 30 adalah 1, 2, 3, 5, 6,10,15, dan 30.

Maka faktor-faktor persekutuan yang positif dari -12 dan 30 adalah 1,2,3,dan 6.

Jadi, faktor persekutuan terbesar dari -12 dan 30 adalah 6, atau dapat ditulis secara singkat sebagai $(-12, 30) = 6$.

Selanjutnya, dengan mudah dapat ditunjukkan bahwa $(-5,5) = 5$, $(8,15) = 1$; $(8, -36) = 4$; $(-6, -42) = 6$.

Perhatikan bahwa $(30,105) = 15$ dan $(30{:}15, 105{:}15) = (2,7) = 1$. Jika $(a, b) = d$, apakah $(a{:}d, b{:}d) = 1$?

Misalkan $(a{:}d, b{:}d) = c$, maka $c \geq 1$ dan $c|(a{:}d)$ dan $c|(b{:}d)$.

$c|(a{:}d)$ maka ada bilangan bulat m, sehingga $a{:}d = mc$ atau $c = mcd$.

$c|(b{:}d)$ maka ada bilangan bulat n, sehingga $b{:}d = ncd$.

Karena $a = mcd$ dan $b = ncd$, maka cd adalah faktor persekutuan dari a dan b. Karena $(a, b) = d$, maka $cd \leq d$, yaitu $c \leq 1$, sebab d suatu bilangan bulat positif. Karena $c \geq 1$ dan $c \leq 1$,maka $c = 1$.

Uraian tersebut merupakan bukti dari teorema berikut ini.

Teorema 3.1:

Jika $(a, b) = d$, maka $(a{:}d, b{:}d) = 1$.

Jika a dan b dua bilangan bulat positifi dengan $(a, b) = 1$, maka dikatakan bahwa a dan b saling prima atau a prima relatif terhadap b.

Misalkan a dan b dua bilangan bulat dengan $a > 0$, maka b dibagi oleh a akan memberikan hasil bagi dan sisa pembagian. Hal ini dinyataan sebagai teorema berikut ini dan terkenal dengan nama Algoritma Pembagian.

Teorema 3.1.

Jika a dan b bilangan-bilangan bulat dengan $a > 0$, maka ada dengan tunggal pasangan bilangan-bilangan bulat q dan r yang memenuhi $b = qa + r$, dengan $0 \leq r \leq a$.

Bukti:

Dibentuk himpunan $S = \{b - xax\ bilangan\ bulat\ dan\ b - xa > 0\}$. S bukan merupakan himpunan kosong sebab jika $x = -|b|$ dan karena $a > 0$, maka $(b - xa) \in S$. Karena S beranggotakan bilangan-bilangan bulat tak negatif berbentuk $(b - xa)$, maka S pasti memiliki anggota terkecil, misalkan r.

Sesuai dengan bentuk anggota dari S, maka $r = b - qa$, untuk suatu bilangan bulat q dan $r \geq 0$, Selanjutnya akan ditunjukkan bahwa $r < a$.

Andaikan $r \geq a$, maka $r = a + k$ dengan $k \geq 0$. Jadi, $k = r - a$, karena $r = b - qa$, maka $k = b - qa - a = b - (q + 1)a$. Ini berarti bahwa k adalah suatu anggota dari S.

Tetapi $0 \leq k = r - a < r$. Hal ini tidak mungkin, karena r adalah bilangan bulat tak negatif yang terkecil dalam S. Oleh karena itu, pengandaian tersebut harus diingkari. Jadi, $r < a$, sehingga ada q dan r sedemikian sehingga $b = qa + r$ dengan $0 \leq r < a$.

Selanjutnya kita akan menunjukkan ketunggalan dari q dan r.

Misalkan bahwa b mempunyai dua representasi, yaitu:

$b = aq + r = aq + r$ dengan $0 \leq r < a$ dan $0 \leq r < a$.

Maka $r - r = a(q - q)$.

$|r' - r| = a|q' - q|$ karena $a > 0$

Dari $-a < -r \leq 0$ dan $0 \leq r' < a$ diperoleh $-a < r' - r < a$ atau $|r' - r| < a$.

Jadi, $a|q' - q| < a$, yang menghasilkan $0 \leq |q' - q| < 1$.

Karena $|q' - q|$ adalah bilangan bulat tak negatif, maka hanya mungkin jika $|q' - q| = 0$, yaitu $q = q'$, sehingga $r' = r$ juga.

Berdasarkan pembuktian tersebut, maka teorema tersebut diperluas untuk $a < 0$, sehingga diperoleh akibat sebagai berikut:

Akibat 3.1

Jika a dan b bilangan-bilangan bulat dengan $b \neq 0$, maka ada dengan tunggal pasangan bilangan-bilangan bulat q dan r sedemikian hingga

$b = aq + r$ dengan $0 \leq r < |a|$

Untuk membuktikan akibat ini, kita cukup memperhatikan untuk a yang negatif maka $|a| > 0$, sehingga dengan teorema 2.7 tersbebut menghasilkan pasangan bilangan-bilangan bulat tunggal q' dan r yang memenuhi:

$b = aq' + r$ dengan $0 \leq r < |a|$

Perhatikan bahwa $|a| = -a$ dan mengambil $q = q'$ untuk mendapatkan $b = aq + r$ dengan $0 \leq r < |a|$

Sebagai ilustrasi, jika $a = 21$ dan $b = 75$, maka $q = 3$ dan $r = 12$, yaitu: $375 = 3 \cdot 21 + 12$

Di sini tampak bahwa $(75,21) = (21,12) = 3$

Apakah benar, jika $b = aq + r$, maka $(b, a) = (a, r)$?

Misalkan $(b, a) = d$ dan $(a, r) = c$, maka kita akan menunjukkan bahwa $c = d$, karena $(b, a) = d$, maka $d|b$ dan $d|a$, karena $b = aq + r$, maka $d|r$.

Dari $d|a$ dan $d|r$, maka d adalah faktor persekutuan dari a dan r, tetapi karena $(a, r) = c$, maka $d \leq c$.

Selanjutnya, karena $(a, r) = c$, maka $c|a$ dan $c|r$ dan karena $b = aq + r$, maka $d|r$.

Dari $d|a$ dan $d|r$, maka d adalah faktor persekutuan dari a dan r. Tetapi karena $(a, r) = c$, maka $d \leq c$.

Selanjutnya, karena $(a, r) = c$, maka $c|a$ dan $c|r$ dan karena $b = aq + r$, maka $c|b$. Dari $c|a$ dan $c|b$, maka c adalah faktor persekutuan a dan b.

Tetapi karena dari $(a, b) = d$, maka $d \geq c$.

Dari $d \leq c$ dan $d \geq c$, maka c=d, yaitu $(b, a) = (a, r)$.

Uraian tersebut merupakan bukti dari teorema berikut ini.

Teorema 3.2:

Jika $b = aq + r$, maka (b, a), maka $(b - a) = (a, r)$.

Dengan menggunakan teorema ini, memudahkan kita untuk menghitung faktor persekutuan terbesar dari sembarang bilangant bulat, meskipun bilangan-bilangan bulat tersebut cukup besar.

Contoh 3.2:

Carilah (5767, 4457)

Penyelesaian :

Kita gunakan algoritma pembagian (teorema 2.8)

$5767 = 1 \cdot 4453 + 1314$, maka $(5767,4453) = (4453,1314)$

$5767 = 3 \cdot 1314 + 511$, maka $(4453,1314) = (1314,511)$

$1314 = 2 \cdot 511 + 292$, maka $(1314{,}511) = (511{,}292)$

$511 = 1 \cdot 292 + 73$, maka $(511{,}292) = (219{,}73)$

$219 = 3 \cdot 73 + 0$, maka $(219{,}73) = (73{,}0) = 73$

Faktor persekutuan terbesar dari a dan b dapat dinyatakan sebagai kombinasi linear dari a dan b yaitu berbentuk $ac + by$ dengan x dan y bilangan-bilangan bulat tertentu.

Misalnya :

$(-12{,}30) = 6 = (-12) \cdot 2 + 30 \cdot 1$

$(8{,}15) = 1 = 8 \cdot 2 + 15 \cdot (-1)$

$(8, -36) = 4 = 8 \cdot 5 + (-36) \cdot 1$

$(-6, -42) = 6 = (-6) \cdot (-8) + (-42) \cdot 1$

Uraian ini memberikan contoh untuk teorema berikut ini:

Teorema 3.2:

Jika a dan b bilangan bulat tidak nol, maka ada bilangan-bilangan bulat x dan y, sedemikian hingga $ax + by = (a, b)$.

Bukti:

Dibentuk himpunan S yaitu himpunan semua kombinasi linear dari a dan b yang bernilai positif.

$$S = \{au + bv | au + bv > 0 \text{ dan u, v bilangan bulat}\}$$

S bukan himpunan kosong, sebab jika $a > 0$ dan $u = 1$ dengan $v = 0$, maka $a < 0$, dengan $u = -1$ dan $v = 0$, maka $|a| \in S$.

Karena S memuat bilangan-bilangan bulat positif, maka S memuat anggota yang terkecil, misalnya d, karena $d \in S$, maka ada bilangan-bilangan bulat x dan y sehingga $ax + by = d$. Selanjutnya, kita akan mnunjukkan bahwa $(a, b) = d$.

Perhatikan a dan d, menurut algoritma pembagian, maka ada bilangan-bilangan bulat q dan r sedemikian hingga :

$a = qd + r$ dengan $0 \leq r < d$

$r = a - qd = a - q(ax + by)$

$r = a(1 - qx) + b(-qy)$

Karena $r > 0$ dan r merupakan kombinasi linear dari a dan b, maka $r \in S$.

Hal ini bertentangan dengan fakta bahwa d adalah anggota terkecil dari S (ingat bahwa $0 \leq r < d$).

Jadi, $r = 0$, sehingga $a = qd$ atau $d|a$.

Dengan penalaran yang sama diperoleh $d|b$, sehingga d adalah faktor persekuuan dari a dan b.

Selanjutnya, jika c adalah sembarang faktor persekutuan dari a dan b, yaitu $c|a$ dan $c|b$, maka $c|ax + by$ atau $c|d$, sehingga $c \leq d$. Ini berarti bahwa $d = (a, b)$.

Bukti teorema 2.9 tersebut hanya merupakan bukti eksistensi dan tidak memberikan cara mencari nilai-nilai x dan y. Hal ini akan dibahas kemudian.

Sesuai dengan teorema 3.2 tersebut, jika $(a, b) = 1$, maka ada bilangan-bilangan bulat x dan y sedemikian hingga $ax + by = 1$.

Sebaliknya jika $ax + by = 1$ untuk bilangan-bilangan bulat x dan y tertentu, apakah $(a, b) = 1$?

Misalkan bahwa $(a, b) = d$, maka $d|a$ dan $d|b$, sehingga menurut teorema 2.2 didapat $d|(ax + by)$ atau $d \geq 1$, maka $d = 1$.

Teorema 3.3:

Jika a dan b dua bilangan bulat tidak nol, maka a dan b saling prima jika dan hanya jika ada bilangan-bilangan bulat x dan y yang memenuhi $ax + by = 1$.

Contoh 3.3:

Hitunglah $(247, 299)$ dan ditenttukan bilangan-bilangan bulat m dan n yang memenuhi $247m + 299n = (247{,}299)$.

Jawab:

$$299 = 247 \cdot 1 + 52$$
$$247 = 52 \cdot 4 + 39$$
$$52 = 39 \cdot 1 + 13$$
$$39 = 13 \cdot 3$$

Jadi, $(247{,}299) = 13$.

Selanjutnya,

$$13 = 52 - 39 \cdot 1$$
$$= 52 - (247 - 52 \cdot 4)$$
$$= 52 \cdot 5 - 247$$
$$13 = 299 \cdot 5 + 247(-6)$$

Jadi, $m = -6$ dan $n = 5$

Tetapi nilai m dan n yang memenuhi $247m + 299n = 13$ tidak tunggal, sebab $247(-6 + 299) + 299(5 - 247t) = 13$, untuk setiap bilangan bulat t.

Jadi, $m = -6 + 299t$ dan $n = 5 - 247t$, untuk setiap bilangan bulat t.

Misalkan $a|c$ dan $b|c$ dapatkah kita menyimpulkan bahwa $ab|c$?

Diambil contoh sebagai berikut: $8|24$ dan $6|24$ maka tidak benar bahwa $8 \cdot 6|24$, tetapi jika diberi tambahan ketentuan bahwa (a,b)=1, maka kita dapat menyimpulkan bahwa $ab|c$.

Hal ini ditunjukkan sebagai berikut:

Karena $(a, b) = 1$, menurut teorema 2.10 tersebut, maka ada bilangan-bilangan bulat x dan y sedemikian hingga:

$$ax + by = 1$$

Jika kedua ruas dikalikan c, maka diperoleh persamaan:

$$acx + bcy = c$$

Karena $a|c$ dan $b|c$, maka ada bilangan-bilangan bulat r dan t sedemikian hingga $c = ar$ dan $c = bt$. Sehingga persamaan (1) menjadi:

$$Abtx + abry = c$$

$$Ab(tx + ry) = c$$

Ini berarti bahwa $ab|c$

Uraian tentang akibat dari teorema 2.10 tersebut dinyatakan sebagai berikut:

Akibat 3.2:

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

Jika diketahui bahwa $ab|c$, apakah kita dapat meyimpulkan bahwa $a|b$ atau $a|c$?

Diambil sebagai contoh: $3|(3,4)$ maka tidak benar jika kita mengambil kesimpulan bahwa $6|3$ ataupun $6|4$.

Tetapi jika $a|bc$ ditambah ketentuan $(a, b) = 1$, maka kita dapat menyimpulkan bahwa $a|c$.

Hal itu ditunjukkan sebagai berikut:

Karena $(a, b) = 1$, maka ada bilangan-bilangan bulat x dan y sedemikian hingga:

$$ax + by = 1$$

Jika kedua ruas dari persamaan ini dikalikan dengan c, maka diperoleh :

$$acx + bcy = c$$

Karena $a|bc$ dan $a|ac$, maka $a|(acx + bcy)$ atau $a|c$.

Uraian yang tampak sederhana ini, tetapi pernyataan itu merupakan hal yang fundamental (mendasar) dan biasa disebut dengan “lemma Euclid”.

Teroema 3.4 (Lemma Euclid)

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

B. Kelipatan Persekutuan Terkecil (KPK)

Di Sekolah Dasar dan Sekolah Lanjutan, kita telah mempelajari kelipatan persekutuan terkecil (KPK).

Misalnya, kelipatan bulat positif dari 3 adalah $3, 6, 9, 12,15,18,. . .$

Kelipatan bulat positif dari 4 adalah $4, 8, 12, 16, 20, 24, 28, \ldots$

Maka kelipatan persekutuan dari 3 dan 4 adalah $12, 24, 36, 48, \ldots$

Selanjutnya istilah "kelipatan bulat positif" hanya dikatakan lebih singkat menjadi "kelipatan" saja.

Selanjutnya secara umum pengertian kelipatan persekutuan dari dua bilangan bulat dinyatakan dalam definisi berikut ini.

Definisi 3.2:

Misalkan a dan b adalah bilangan-bilangan bulat, m adalah kelipatan persekutuan dari a dan b jika $a|m$ dan $b|m$.

Nol (0) adalah suatu kelipatan persekutuan dari a dan b. Ab dan $-ab$ masing-masing juga merupakan suatu kelipatan persekutuan dari a dan b. Jadi, himpunan semua kelipatan persekutuan bulat positif a dan b tidak pernah sama dengan himpunan kosong.

Himpunan semua kelipatan bulat positif dari 6 adalah $\{6,12,18,24, \ldots\}$

Himpunan semua kelipatan bulat positif dari -9 adalah $\{6,12,18,24, \ldots\}$

Jadi, himpunan semua kelipatan persekutuan dari 6 dan -9 adalah $\{18,36,54,72, \ldots\}$, sehingga kelipatan persekutuan dari 6 dan -9 adalah 18.

Ingat bahwa dalam himpunan bagian dari himpunan bilangan-bilangan bulat positif selalu mempunyai anggota terkecil, sehingga KPK dari sebab dua biangan bulat selalu ada.

Secara formal, KPK dari dua bilangan bulat didefinisikan sebagai berikut:

Kelipatan persekutuan terkecil (KPK) dari dua bilangan bulat tidak nol a dan b adalah suatu bilangan bulat positif m ditulis $[a, b] = m$, jika memenuhi: (i) $a|m$ dan $b|m$, (ii) jika $a|c$ dan $b|c$, maka $m \leq c$.

Dalam definisi ini dapat dimengerti bahwa kelipatan dari setiap dua bilangan bulat yang tidak nol selalu merupakan suatu bilangan bulat positif. Dalam (i) pada definisi itu mengatakan bahwa masing-masing dari dua bilangan itu membagi kelipatan persektutuan terkecilnya, sedangkan (ii) mengatakan bahwa kelipatan persekutuan lainnya tidak lebih kecil dari KPK dari dua bilangan itu.

Contoh 3.5:

$[6,8] = 24$, maka $6|24$ dan $8|24$.

Perhatikan pada contoh di atas, yaitu himpunan semua kelipatan persekutuan bulat positif dari 6 dan -9 adalah $\{18,36,54,72,\ldots\}$ dan KPK dari 6 dan -9 adalah 18 atau ditulis $[6,-9]=18$. Tampak di sini tHal ini dapat dikar

Hal ini dapat dikatakan bahwa setiap kelipatan persekutuan dari dua bilangan bulat selalu terbagi oleh KPK dari dua bilangan tersebut. Hal ini dinyatakan sebagai teorema berikut ini:

Teorema 3.5:

Jika c adalah suatu kelipatan persekutuan dari dua bilangan bulat tidak nol a dan b, maka KPK a dan b membagi c, yaitu $[a,b]|c$.

Bukti:

Misalkan [a,b]=m, maka harus ditunjukkan bahwa $m|c$. Andaikan $m \nmid c$, maka algoritma pembagian, ada bilangan bulat q dan r sedemikian hingga

$c=qm+r$ dengan $0<r<m$

Karena c adalah kelipatan persekutuan dari a dan b, maka $a|c$ dan $b|c$.

Karena $[a,b]=m$, maka $a|m$ dan $b|m$.

$a|m$ maka $a|qm$ dan $a|c$, maka $a|c$.

Demikian pula $b|m$, maka $b|qm$ dan karena $b|c$, maka $b|(c-qm)$. Berarti $b|r$.

Karena $a|r$ dan $b|r$ maka r adalah kelipatan persekutuan dari a dan b.

Tetapi karena $[a,b]=m$ dan $0<r<m$, maka hal tersebut tidak mungkin (kontradiksi). Jadi, pengandaian di atas tidak benar, berarti $m|c$ atau $[a,b\}|c$.

Perhatikan bahwa $[6,9]=18$ dan $[2\cdot 6,2\cdot 9]=[12,18]=36$.

Tampak bahwa $[2\cdot 6,2\cdot 9]=2[6,9]$.

Hal ini memberikan ilustrasi dari teorema berikut ini:

Teorema 3.6:

Jika $c>0$, maka $[ca,cb]=c[a,b]$.

Bukti :

Misalkan $[a,b]=d$, maka $a|d$ dan $b|d$, sehingga $ac|dc$ dan $bc|dc$. Hal ini berarti dc adalah kelipatan persekutuan dari ac dan bc. Dan menurut teorema 2.10, maka $[ac,bc]|dc$.

Karena $[ac,bc]$ adalah suatu kelipatan dari ac, maka $[ac,bc]$ adalah suatu kelipatan dari c. Misalkan $[ac,bc]=mc$, maka $mc|dc$, sehingga $m|d$.

Teorema 3.7:

Jika $c>0$, maka $[ca,cb]=c[a,b]$

Bukti:

Misalkan $[a, b] = d$, maka $a|d$ dan $b|d$, sehingga $ac|dc$. Hal ini berarti dc adalah kelipatan persekutuan dari aca dan bc. Dan menurut teorea 2.10, maka $[ac, bc]|dc$.

Karena $[ac, bc]$ adalah suaut kelipatan dari ac, maka $[ac, bc]$, sehingga $m|d$.

Karena $[ac, bc] = mc$, maka $ac|mc$ dan $bc|mc$, sehingga $a|m$ dan $b|m$, dan menurut teorema 2.12, maka $[a, b]|m$, yaitu $d|m$ dan karena $m|d$, maka $d = m$.

Sehingga $dc = mc$, yaitu $c[a, b] = [ac, bc]$.

Contoh 3.7:

(1) $[105,45] = [15 \cdot 7,15 \cdot 3]$

$= 15[7,3]$

$= 15 \cdot 21$

$= 315$

(2) $[18,30] = [6 \cdot 3,6 \cdot 5]$

$= 6[3 \cdot 5]$

$= 6 \cdot 15$

$= 90$

Mengingat teroema tersebut, maka dengan mengeluarkan faktor persekutuannya akan mempermudah dalam mencari KPK-nya.

Jika $(a, b) = 1$, berapakah [a,b]? Apakah $[a, b] = ab$? Akan ditunjukkan sebagai berikut:

Jelas bahwa ab adalah suatu kelipatan persekutuan dari a dan b, menurut teorema 2.12, maka $[a, b]|a \cdot b$. Di lain pihak, menurut akibat dari teorema 2.10, karena $ab|[a, b]$ dan $b|[a, b]$ dengan $(a, b) = 1$, maka $ab|[a, b]$ dan karena $[a, b]|ab$, maka disimpulkan $[a, b] = ab$.

Selanjutnya, jika $(a, b) = d$, maka $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Berdasarkan pada kesimpulan di atas, maka $\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{ab}{d^2}$.

Jika kedua ruas dikalikan d^2, maka diperoleh bahwa

$$d^2\left[\frac{a}{d}, \frac{b}{d}\right] = ab \Leftrightarrow d[a, b] = ab$$

$$\Leftrightarrow (a, b)[a, b] = ab$$

Uraian di atas merupakan bukti teorema berikut ini:

Teorema 3.7:

Jika a dan b bilangan-bilangan bulat yang keduanya positif, maka $(a, b)[a, b] = ab$

Contoh 3.8:

(1) Karena $(16,20) = 4$ dan $[16,20] = 80$, terdapat hubungan $(16,20)[16,20] = 4 \cdot 80 = 320 = 16 \cdot 20$.

(2) $(25{,}18) = 1$ dan $[25{,}18] = 450$, terdapat hubungan $(25{,}18)[25{,}18] = 1 \cdot 450$ =25·18n

B.4. Latihan Kegiatan Belajar 3

Selesaikan soal-soal berikut ini dengan benar!

1. Jika $(a, b) = d$ buktikan bahwa $d|(ax + by)$ untuk setiap bilangan-bilangan bulat x da y !
2. Jika $a|b$ dan $a > 0$ buktikan bahwa $(a, b) = a$!
3. Jika a dan b bilangan-bilangan bulat tidak nol, tunjukkan bahwa $(a, b) = (-a, b) = (a, -b) = (-a, -b)$!
4. Jika n suatu bilangan bulat positif dan a sembarang bilangan bulat, buktikan bahwa $(a, a + n)|n$!
5. Jika $(a, b) = 1$ dan $c|a$, buktikan bahwa $(c, b) = 1$!
6. Buktikan bahwa $\big((a, b), b\big) = (a, b)$!
7. Buktikan bahwa $(a + b, a) = (a, b)$!
8. Buktikan jika c suatu kelipatan persekutuan dari a dan b, maka $(a, b)|c$!
9. Buktikan jika $[a, b] = b$, maka $a|b$!
10. Jika $a|b$, maka $[a, b] = b$!

D. KEGIATAN BELAJAR 4

D.1. Pendahuluan Kegiatan Belajar 4

Bahan kajian	:	basis bilangan bulat.
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang basis bilangan bulat.
Indikator pembelajaran	:	mahasiswa mampu merepresentasikan suatu bilangan dalam berbagia basis.
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, relasi keterbagian, faktor persekutuan terbesar, dan kelipatan persekutuan terkecil.

D.2. Bahan Pembelajaran Kegiatan Belajar 4

A. BASIS BILANGAN BULAT

Cara yang telah kita kenal untuk menuliskan lambang bilangan bulat adalah dengan notasi desimal (basis sepuluh). Lambang dasar yang digunakan dalam basis sepuluh adalah 0, 1, 2, 3, 4, 5, 6, 7, 8, dan 9. Lambang bilangan-bilangan bulat lainnya dituliskan dengan menerapkan nilai tempat dengan menggunakan lambang dasar tersebut, seperti yang telah kita kenal sejak di sekolah dasar.

Contoh 4.1:

$$4275 = 4 \cdot 10^3 + 2 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0$$

Penggunaan basis sepuluh yang biasa kita lakukan, bukan satu-satunya basis untuk menuliskan lambang bilangan, kemungkinan hanya karena banyaknya jari tangan kita berjumlah sepuluh. Tak ada alasan khusus lainnya dari penggunaan basis sepuluh yang telah biasa kita lakukan. Bangsa babilonia kuno menggunakan basis enam puluh, bangsa maya menggunakan basis dua, delapan atau enam belas untuk menyatakan lambang bilangan bulat.

Teorema 4.1:

Misalkan *b* suatu bilangan bulat positif yang lebih besar dari 1, maka setiap bilangan bulat positif n dapat ditulis secara tunggal dalam bentuk

$$n = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0$$

dengan k suatu bilangan bulat taknegatif, a_j suatu bilangan bulat dengan

$$0 \leq a_j \leq b - 1 \text{ untuk } j = 0, 1, 2, \ldots, k \text{ dengan } a_k \neq 0$$

Bukti:

Untuk memperoleh reprentasi dari n seperti yang diinginkan, kita menerapkan algoritma pembagian sebagai berikut.

Pertama, kita membagi n dengan b untuk mendapatkan

$$n = \mathrm{b}\mathrm{q}_0 + \mathrm{a}_0,\ 0 \le \mathrm{a}_0 \le \mathrm{b} - 1$$

Jika $\mathrm{q}_0 \neq 0$, kita membagi q_0 dengan b dan mendapatkan bahwa

$$\mathrm{q}_0 = \mathrm{b}\mathrm{q}_1 + \mathrm{a}_1, 0 \le \mathrm{a}_1 \le \mathrm{b} - 1$$

Kita melanjutkan proses ini untuk memperoleh

$$\mathrm{q}_1 = \mathrm{b}\mathrm{q}_2 + \mathrm{a}_2, 0 \le \mathrm{a}_2 \le \mathrm{b} - 1$$
$$\mathrm{q}_2 = \mathrm{b}\mathrm{q}_3 + \mathrm{a}_3, 0 \le \mathrm{a}_3 \le \mathrm{b} - 1$$

.

.

.

$$\mathrm{q}_{\mathrm{k}-2} = \mathrm{b}\mathrm{q}_{\mathrm{k}-1} + \mathrm{a}_{\mathrm{k}-1}, 0 \le \mathrm{a}_{\mathrm{k}-1} \le \mathrm{b} - 1$$
$$\mathrm{q}_{\mathrm{k}-1} = \mathrm{b} \cdot 0 + \mathrm{a}_{\mathrm{k}}, \qquad 0 \le \mathrm{a}_{\mathrm{k}} \le \mathrm{b} - 1$$

Langkah terakhir dari proses ini terjadi apabila kita memperoleh hasilbagi 0. Perhatikan bahwa dalam penerapan algoritma-algoritma pembagian tersebut, kita memperoleh hasilbagi-hasilbagi yang memenuhi

$$n > \mathrm{q}_0 > \mathrm{q}_1 > \mathrm{q}_2 > \cdots \ \ge 0$$

Karena barisan $\mathrm{q}_0, \mathrm{q}_1, \mathrm{q}_{2,}, \ldots..$ adalah suatu barisan turun dari bilangan-bilangan bulat tak negatif, maka barisan ini akan berakhir pada suku 0. Selanjutnya dari persamaan pertama q_0 disubtitusi dalam persamaan kedua diperoleh

$$n = \mathrm{b}^3\mathrm{q}_2 + \mathrm{b}^2\mathrm{a}_2 + \mathrm{b}\mathrm{a}_1 + \mathrm{a}_0$$
$$n = \mathrm{b}^4\mathrm{q}_3 + \mathrm{b}^3\mathrm{a}_3 + \mathrm{b}^2\mathrm{a}_2 + \mathrm{b}\mathrm{a}_1 + \mathrm{a}_0$$

.

.

.

$$n = \mathrm{b}^{\mathrm{k}-1}\mathrm{q}_{\mathrm{k}-2} + \mathrm{b}^{\mathrm{k}-2}\mathrm{a}_{\mathrm{k}-2} + \cdots \mathrm{b}^2\mathrm{a}_2 + \mathrm{b}\mathrm{a}_1 + \mathrm{a}_0$$
$$n = \mathrm{b}^{\mathrm{k}}\mathrm{a}_{\mathrm{k}} + \mathrm{b}^{\mathrm{k}-1}\mathrm{a}_{\mathrm{k}-1} + \cdots + \mathrm{b}^2\mathrm{a}_2 + \mathrm{b}\mathrm{a}_1 + \mathrm{a}_0$$
$$= \mathrm{a}_{\mathrm{k}}\mathrm{b}^{\mathrm{k}} + \mathrm{a}_{\mathrm{k}-1}\mathrm{b}^{\mathrm{k}-1} + \ \ldots. + \mathrm{a}_2\mathrm{b}^2 + \mathrm{a}_1\mathrm{b} + \mathrm{a}_0$$

Dimana $0 \le \mathrm{a}_{\mathrm{j}} \le \mathrm{b} - 1$ untuk $\mathrm{j} = 0, 1, 2, \ldots., \mathrm{k}$ dan $\mathrm{a}_{\mathrm{k}} \neq 0$,

karena $\mathrm{a}_{\mathrm{k}} = \mathrm{q}_{\mathrm{k}-1}$ adalah hasilbagi terakhir yang tidak sama dengan 0.

Kita telah mendapatkan representasi dari n seperti yang diinginkan. Untuk memperlihatkan bahwa representasi n tersebut tunggal, misalkan kita mempunyai dua representasi dari n, yaitu:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ \ldots . + a_1 b + a_0 \ , 0 \le a_j \le b - 1$$

dan $$n = c_k b^k + c_{k-1} b^{k-1} + \ \ldots . + c_1 b + c_0 \ , 0 \le c_j \le b - 1$$

Jika kedua persamaan tersebut dikurangkan, maka diperoleh

$$(a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \ \ldots . + (a_1 - c_1) b + (a_0 - c_0) = 0$$

Jika kedua represetasi dari n tersebut berbeda, maka ada bilangan bulat terkecil j, $0 \le j \le k$, sedemikian hingga $a_j \ne c_j$. jadi

$$b^j \{ (a_k - c_k) b^{k-j} + (a_{k-1} - c_{k-1}) b^{k-j-1} + \ \ldots . + (a_{j+1} - c_{j+1}) b + (a_j - c_j) \} = 0$$

sehingga

$$(a_k - c_k) b^{k-j} + (a_{k-1} - c_{k-1}) b^{k-j-1} + \ \ldots . + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0$$

$$a_j - c_j = (c_k - a_k) b^{k-j} + (c_{k-1} - a_{k-1}) b^{k-j-1} + \ \ldots . + (c_{j+1} - a_{j+1}) b$$

$$a_j - c_j = b \{ (c_k - a_k) b^{k-j-1} + (c_{k-1} - a_{k-1}) b^{k-j-2} + \ \ldots . + (c_{j+1} - a_{j+1}) \}$$

Ini berarti bahwa $b \big| (a_j - c_j)$

Tetapi karena $0 \le a_j < b$ dan $0 \le c_j < b$, yaitu $-b < a_j - c_j < b$,

sehingga $a_j - c_j = 0$, yaitu $a_j = c_j$

Jadi, representasi dari n adalah tunggal.

Selanjutnya, jika $n = a_k b^k + a_{k-1} b^{k-1} + \ a_{k-2} b^{k-2} + \ \ldots . + a_1 b + a_0$ yaitu n dinyatakan sebagai jumlahan dari perpangkatan bulat dari b, maka n dapat dituliskan sebagai $n = (a_k a_{k-1} a_{k-2} \cdots a_1 a_0) b$

Contoh 4.2:

1) $100110_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$

2) $100110_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$

$= 32 + 0 + 0 + 4 + 2 + 0$

$= 38$

Jadi $100110_2 = 38$ (dalam basis 10)

Seperti telah dikatakan di atas basis 10 disebut pula basis *desimal*. Basis 2 disebut *biner*, basis 4 disebut *quarter*, basis 8 disebut *oktal* dan basis 16 disebut *heksadesimal* atau secara singkat heks. Koefisisen a_j dalam ekspansi jumlahan itu disebut angka (digits). Angka biner biasa disebut dengan bits, yang merupakan singkatan dari *binary digits* yang merupakan istilah dalam computer.

Untuk mengubah penulisan bilangan dari basis decimal ke basis nondesimal, kita menggunakan proses algoritma pembagian berulang-uang seperti pada proses pada pembuktian teorema diatas.

Contoh 4.4:

Tulislah 116 dalam lambang bilangan dengan basis 2.

Jawab:

Penerapan algoritma pembagian berulang-ulang, yaitu:

$$\begin{aligned}
116 &= 2\,.\,58 + 0 \\
58 &= 2\,.\,29 + 0 \\
29 &= 2\,.\,14 + 1 \\
14 &= 2\,.\,7 + 0 \\
7 &= 2\,.\,3 + 1 \\
3 &= 2\,.\,1 + 1 \\
1 &= 2\,.\,0 + 1
\end{aligned} \quad \Big\uparrow$$

Penulisan bilangan bulat n seperti ini dikatakan bahwa n dituliskan dalam basis b.

Contoh 4.5:

Misalnya b = 5 sebagai basis penulisan, maka lambang dasarnya adalah $0, 1, 2, 3,$ dan 4. Misalkan suatu bilangn bulat n dinyatakan sebagai:

$$n = 3 \cdot 5^4 + 2 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 4$$

Maka dalam basis 5, n tersebut ditulis sebagai n = 32014_5. Jika n ingin ditulis dalam basis decimal (sepuluh), maka kita tinggal menghitung jumlahan dari perpangkatan lima tersebut, yaitu:

$$\begin{aligned}
n &= 3 \cdot 5^4 + 2 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 4 \\
&= 3 \cdot 625 + 2 \cdot 125 + 5 + 4 \\
&= 1875 + 250 + 9 \\
&= 2134_{10}
\end{aligned}$$

Jika kita ingin menuliskan lambang bilangan n tersebut dalam basis lainnya, misalnya basis 8, maka kita mengerjakannya seperti dalam proses pembuktian teorema di atas, yaitu:

$$\begin{aligned}
2134 &= 8\,.266 + 6 \\
&= 8 \cdot 266 + 6 \\
&= 8(8 \cdot 33 + 2) + 6 \\
&= 8^2 \cdot 33 + 8 \cdot 2 + 6 \\
&= 8^2(8 \cdot 4 + 1) + 8 \cdot 2 + 6 \\
&= 8^3 \cdot 4 + 8^2 \cdot 1 + 8 \cdot 2 + 6
\end{aligned}$$

Ini berarti $2134_{10} = 4126_8$

Untuk selanjutnya penulisan lambang bilangan dengan basis 10, indeks 10 yang menyatakan basis yng digunakan tidak perlu dituliskan.

Sehingga 2134_{10} cukup ditulis 2134

Berdasarkan teorema di atas, setiap bulat positif dapat ditulis dalam basis 2, yaitu:

$n = \mathrm{a_k}2^{\mathrm{k}} + \mathrm{a_{k-1}}2^{\mathrm{k-1}} + \mathrm{a_{k-2}}2^{\mathrm{k-2}} + \cdots\cdots + \mathrm{a_1}2 + \mathrm{a_0}$ dengan $\mathrm{a_i}$ adalah 0 atau 1.

Jadi $116 = 1110100_2$, yaitu menuliskan sisa-sisa pembagian itu dengan urutan dari bawah ke atas, seperti ditunjukkan anak panah.

Untuk mengubah penulisan lambang bilangan dari basis non desimal ke decimal, kita tuliskan lambang bilangan dengan basis non decimal itu dalam bentuk panjang (bentuk jumlahan dari perpangkatan basis tersebut).

Contoh 4.5:

Tuliskan 3201_4 dalam basis desimal !

Jawab:

$$\begin{aligned} 3201_4 &= 3 \cdot 4^3 + 2 \cdot 4^2 + 0 \cdot 4 + 1 \\ &= 3 \cdot 64 + 2 \cdot 16 + 0 + 1 \\ &= 192 + 32 + 1 \\ &= 225 \end{aligned}$$

Jadi $3201_4 = 225$

Komputer, selain menggunakan basis 2, juga menggunakan basis 8 atau 16. Dalam heksadesimal (basis 16) mempunyai 16 lambang dasar, yaitu:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Huruf-huruf A, B, C, D, E, dan F digunakan untuk menyatakan angka-angka yang bersesuaian dengan 10, 11, 12, 13, 14, dan 15 (dalam basis desimal).

Contoh berikut ini menunjukkan cara mengubah lambang bilangan dari heksadesimal ke desimal

Contoh 4.6:

(1) $$\begin{aligned} \mathrm{2AC3_{16}} &= 2 \cdot 16^3 + 10 \cdot 16^2 + 12 \cdot 16 + 3 \\ &= 2 \cdot 4096 + 10 \cdot 256 + 192 + 3 \\ &= 10947 \end{aligned}$$

(2) $\mathrm{FA0_{16}} = 15 \cdot 16^2 + 10 \cdot 16 + 0 = 4000$

B.4. Latihan Kegiatan Belajar 2

Selesaikan soal-soal berikut ini dengan benar!

1. Buktikan bahwa jika $a|b$ untuk setiap bilangan bulat m!
2. Jika $a|b$, tunjukkan bahwa $(-a)|b, a|(-b)$, dan $(-a)|(-b)$!
3. Buktikan bahwa jika $a|b$ dan $c|d$, maka $ac|bd$!
4. Jika $a|b$ dan $a|c$, buktikan bahwa $a^2|bc$!
5. Buktikan bahwa jika $a|(b-1)$, maka $a|(b^4-1)$!
6. Benarkah pernyataan : jika $a|(b-c)$, maka $a|b$ atau $a|c$. Berilah alasan!
7. Buktikan bahwa hasilkali dua bilangan bulat berurutan selalu terbagi oleh dua !
8. Buktikan bahwa hasilkali tiga bilangan bulat berturutan selalu terbagi oleh 6!
9. Buktikan bahwa hasilkali tiga bilangan bulat berturutan selalu terbagi oleh 3!
10. Buktikan bahwa $4 \nmid (a^2+2)$, untuk setiap bilangan bulat a!

E. KEGIATAN BELAJAR 5

E.1. Pendahuluan Kegiatan Belajar 5

Bahan kajian : bilangan prima

Capaian pembelajaran : mahasiswa menguasai pemahaman tentang konsep bilangan prima dan faktorisasi bilangan bulat.

Indikator pembelajaran :

- mahasiswa merumuskan konsep bilangan prima.
- mahasiswa memfaktorkan bilangan sebagai hasil kali faktor-faktor primamahasiswa mampu merepresentasikan suatu bilangan dalam berbagia basis.

Materi prasyarat : teori himpunan, sistem bilangan bulat, relasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat.

E.2. Bahan Pembelajaran Kegiatan Belajar 5

A. Bilangan Prima

Kita telah mengenal dua bilangan bulat positif saling prima (*prima relatif atau koprima*), yaitu faktor persekutuan terbesar dari dua bilangan itu sama dengan 1.

Jika $a_1, a_2,\ a_3, \ldots, a_n$ adalah bilangan-bilangan bulat positif sedemikian hingga $(a_1, a_2, a_3, \ldots, a_n) = 1$, maka dikatakan bahwa $a_1, a_2,\ a_3, \ldots, a_n$ saling prima pula, tetapi, jika $(a_i, a_j)\ =\ 1$, untuk setiap i, j = 1, 2, 3, ..., n dengan $i \neq j$, maka dikatakan bahwa bilangan-bilangan bulat positif $a_1, a_2,\ a_3, \ldots, a_n$ saling *prima* dua-dua atau saling prima sepasang demi sepasang.

Contoh 5.1:

(1) Karena $(5, 8, 9) = 1$, maka $5, 8$ dan 9 dikatakan tiga bilangan yang saling prima dan sekaligus saling prima sepasang-demi sepasang, karena $(5, 8) =\ (5, 9) = (8,9) = 1$.

(2) Karena $(3, 9, 4, 8)\ =\ 1$, maka $3, 4, 8$, dan 9 adalah empat bilangan yang saling prima, tetapi bukan merupakan empat bilangan yang saling prima sepasang-demi sepasang, sebab $(3, 9)\ =\ 3$ dan $(4, 8)\ =\ 4$, meskipun $(3, 4)\ =\ (3, 8)\ =\ (9, 4)\ =\ (9, 8)\ =\ 1.$

Misalkan a dan b bilangan-bilangan bulat positif, maka menurut algoritma pembagian ada bilangan-bilangan bulat q dan r sedemikian hingga

$$\mathrm{b = qa + r\ dengan\ 0 \leq r < a}$$

Jika diketahui $(a, r) = 1$, maka menurut Teorema 2.8 kita dapat menyimpulkan bahwa $(a, b) = 1$. Hal ini dapat dikatakan bahwa jika sisa pembagian b oleh a saling prima dengan a, maka b saling prima dengan a pula.

Definisi 4.1:

Bilangan bulat positif yang lebih besar dari 1 dan tidak mempunyai faktor bulat positif kecuali 1 dan bilangan bulat itu sendiri disebut *bilangan prima*. Bilangan buat positif yang lebih besar dari 1 dan bukan bilangan prima disebut *bilangan komposit* (tersusun).

Barisan bilangan prima: $2, 3, 5, 7, 11, 13, 17, \ldots$.

Barisan bilangan komposit: $4, 6, 8, 9, 10, 12, 14, 15, \ldots$.

Perhatikan bahwa 1 bukan bilangan prima dan bukan bilangan komposit pula. Satu (1) disebut *unit*. Jadi himpunan semua bilangan bulat positif (bilangan asli) terbagi dalam tiga himpunan bagian yang saling lepas, yaitu (1) himpunan semua bilangan prima; (2) himpunan semua bilangan komposit; dan (3) himpunan unit.

Perhatikan suatu bilangan bulat positif, misalnya 210, maka 210 dapat diuraikan atas faktor-faktor prima, yaitu:

$210 = 2.3.5.7$ atau

$210 = 3.7.2.5$ atau

$210 = 7.3.5.2$ atau lainnya

Perbedaan penguraian dari 210 atas faktor-faktor prima tersebut hanya berbeda pada urutan faktor-faktornya saja. Hal ini merupakan suatu contoh bahwa suatu bilangan bulat positif yang lebih besar dari 1 dapat dinyatakan sebagai perkalian bilangan-bilangan prima tertentu. Bentuk perkalian bilangan-bilangan prima itu adalah tunggal, kecuali urutan dari bilangan-bilangan prima tersebut. Hal ini sering disebut dengan *Teorema Faktorisasi Tunggal*. Teorema-teorema nerikut merupakan persiapan untuk membuktikan teorema faktorisasi tunggal.

Teorema 4.2:

Setiap bilangan bulat positif yang lebih besar dari 1 dapat dibagi oleh suatu bilangan prima.

Bukti:

Ambil sembarang bilangan bulat positif $n > 1$. Apabila n suatu bilangan prima, maka $n|n$, berarti teorema telah terbukti.

Jika n suatu bilangan komposit, maka n mempunyai faktor bulat positif selain 1 dan n_1, misalnya d_2, yaitu $d_2 \mid n_1$. Sehingga ada bilangan bulat positif n_2 sedemikian hingga

$$n = d_1 n_1 \; dengan \; 1 < n_1 < n$$

Jika n_1 suatu bilangan prima, maka $n_1 \mid n$. Sehingga teorma terbukti. Tetapi jika n_1 suatu bilangan komposit, maka n_1 mempunyai faktor bulat positif selain 1 dan n_1, misalnya d_2, yaitu $d_2 \mid n_1$. Sehingga ada bilangan bulat positif n_2 sedemikian hingga

$$n_1 = d_2 n_2 \; dengan \; 1 < n_2 < n$$

Jika n_2 suatu bilangan prima, maka $n_2 \mid n_1$ maka $n_2 \mid n$. Dan karena $n_1 \mid n$, maka $n_2 \mid n$. Jadi n terbagi oleh bilangan prima n_2, berarti teorema terbukti. Tetapi jika n_2 suatu bilangan komposit, maka n_2 mempunyai faktor bulat positif selain 1 dan n_2, misalnya d_3, yaitu $d_3 \mid n_2$. Ini berarti ada bilangan bulat positif n_3 sedemikian hingga

$$n_2 = d_3 n_3 \text{ dengan } 1 < n_3 < n_2$$

Jika n_3 suatu bilangan prima, maka $n_3 \mid n_2$. Karena $n_2 \mid n_1$ dan $n_1 \mid n$, maka $n_3 \mid n$. Jadi n terbagi oleh bilangan prima n_3, berarti teorema terbukti. Tetapi jika n_3 suatu bilangan komposit, maka proses seperti di atas dapat dilanjutkan sedemikian hingga diperoleh suatu barisan:

$$n, n_1, n_3, \ldots dengan \; n > n_1 > n_2 > n_3 > \cdots > 1$$

Penguraian di atas faktor-faktor komposit ini tentu berakhir pada suatu faktor prima, karena faktor-faktir tersebut selalu lebih kecil dari bilangan yang difaktorkan dan selalu lebih besae dari 1. Misalkan pemfaktoran tersebut berakhir pada faktor prima n_k, maka

$$n_k \mid n_{k-1}, n_{k-1} \mid n_{k-2}, \ldots \;, n_2 \mid n_1 \text{ dan } n_1 \mid n$$

Bukti alternatif lain:

Karena n suatu bilangan bulat positif yang lebih besar dari 1, maka n mempunyai sekurang-kurangnya satu faktor bulat positif katakan n sendiri. Sehingga n mesti mempunya faktor bulat positif terkecil, misalnya 1, maka 1 adalah suatu bilangan prima. Sebab jika q bukan bilangan prima, maka $q = q_1 q_2$ dengan $1 < q_1 < q$ sehingga q_1 adalah fator bulat positif dari n, tetapi karena q adalah faktor bulat positif terkecil dari n, maka terdapat kontradiksi.

Memperhatikan teorema di atas, suatu bilangan bulat positif yang lebih besar 1 selalu terbagi oleh suatu bilangan prima, maka hasilbaginyapun akan terbagi oleh suatu bilangan prima pula. Dan hasilbagi berikutnyapun demikian pula. Sehingga suatu bilangan buat positif yang lebih besar dari 1 dapat dinyatakan sebagai perkalian dan bilangan-bilangan prima tertentu. Hal ini dinyatakan sebagai teorema berikut ini.

Teorema 5.3:

Setiap bilangan bulat positif yang lebih besar dari 1 adalah suatu bilangan prima atau bilangan itu dapat dinyaakan sebagai perkalian bilangan-bilabnan prima.

Bukti**:**

Ambil sebarang bilangan bulat positif $n > 1$. Menurut teorema 4.1, maka ada suatu bilangan prima p_1 sedemikian hingga $p_1 \mid n$. Sehingga ada suatu bilangan positif n_1, sehingga

$$n = p_1 n_1 \text{ dengan } 1 \leq n_1 < n$$

Jika $n_1 = 1$, maka $n = p_1$ sehingga n suatu bilangan prima. Tetapi jika $n_1 > 1$, maka menurut Teorema 4.1 lagi, ada suatu bilangan prima p_2 sedemikian hingga $p_2 \mid n_1$. Sehingga ada suatu bilangan bulat positif n_2, sehingga

$$n_1 = p_2 n_2 \text{ dengan } 1 \leq n_3 < n_2$$

Jika $n_2 = 1$, maka $n_2 = p_3$ sehingga $n = p_1 p_2 p_3$. Berarti teorema terbukti. Tetapi jika $n_2 > 1$, maka ada suatu bilangan prima p_3 sedemikian hingga

$$n_2 = p_3 n_3 \ dengan 1 \leq n_3 < n_2$$

Jika $n_3 = 1$, maka $n_2 = p_3$ sehingga $n = p_1 p_2 p_3$ berarti teoriema terbukti. Tetapi jika $n_2 > 1$, maka proses seperti di atas dapat dilanjutkan sehingga akan berakhir pada $n_k = 1$, maka diperoleh $n = p_1 p_2 p_3 \dots p_k$, yaitu bilangan bulat positif $n > 1$ dapat dinyatakan sebagai perkalian bilangan prima.

Suatu bilangan bulat positif yang lebih besar dari 1 dapat dinyatakan sebagai perkalian bilangan-bilangan prima. Mungkin saja di antara faktor-faktor prima tersebut ada yang sama, maka faktor-faktor yang sama dapat ditulis sebagai bilangan berpangkat.

Contoh 5.2:

$5544 = 2.2.2.3.3.7.11$ dapat ditulis $5544 = 2^3.3^2.7.11$

Hal ini secra umum, jika n suatu bilangan bulat positif yang lebih besar dari 1 dapat dinyatakan sebagai

$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ dengan $p_1, p_2, p_3, \dots, p_k$ adalah faktor-faktor prima dari n dan $a_1, a_2, a_3, \dots, a_k$ adalah eksponen-eksponen bulat tak negatif.

Selanjutnya bentuk (1) disebut *representasi* dari n sebagai perkalian bilangan-bilangan prima atau sering pula disebut *bentuk kanonik* dari n.

Teorema 5.2 tersebut sangat memudahkan untuk menentukan FPB dan KPK dari dua bilangan bulat atau lebih, yaitu dengan menyatakan masing-masing bilangan bulat itu dalam bentuk kanoniknya. Tetapi sebelum itu, kita perlu mengenal lebih dulu notasi-notasi berikut ini.

"$min(a, b)$" menyatakan nilai minimum dari a dan b.

"$maks(a, b)$" menyatakan nilai maksimum dari a dan b.

Misalnya : $min\ (7,5) = 5, maks\ (8,3) = 8$

$min\ (5,0,3) = 0, maks\ (7,4,5,0) = 7$

Misalkan m, n dan t adalah bilangan-bilangan bulat positif yang lebih besar dari 1 yang bentuk-bentuk kanoniknya berturut-turut sebagai berikut:

$$m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$

$$n = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$$

$$t = p_1^{c_1} p_2^{c_2} p_3^{c_3} \dots p_k^{c_k}$$

Maka FPB dan KPK dari m, n, dan t berturut-turut

$(m,n,t) = p_1^{d_1} p_2^{d_2} p_3^{d_3} \dots p_k^{d_k}$ dengan $d_i = \min(a_i, b_i, c_i)$ untuk $i = 1,2,3, \dots, k$

$(m,n,t) = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$ dengan $e_i = \min(a_i, b_i, c_i)$ untuk $i = 1,2,3, \dots, k$

Contoh 5.3:

Tentukan FPB dan KPK dari 198, 216, dan 252!

Penyelesaian:

Jika tiga bilangan tersebut diuraikan atas faktor-faktor prima, maka diperoleh :

$$198 = 2 \cdot 3^2 \cdot 11$$

$$216 = 2^3 \cdot 3^3$$

$$252 = 2^2 \cdot 3^2 \cdot 7$$

Uraian atas faktor-faktor prima tersebut dapat ditulis sebagai berikut:

$$198 = 2 \cdot 3^2 \cdot 7^0 \cdot 11$$

$$216 = 2^3 \cdot 3^3 7^0 \cdot 11^0$$

$$252 = 2^2 \cdot 3^2 \cdot 7 \cdot 11^0$$

$$(198,216,252) = 2^{\min(1,2,3)} 3^{\min(2,3,2)} 7^{\min(0,0,1)} 11^{\min(1,0,0)}$$

$$= 2^1 \cdot 3^2 \cdot 7^0 \cdot 11^0$$

$$= 18$$

$$(198,216,252) = 2^{\text{maks}(1,2,3)} 3^{\text{maks}(2,3,2)} 7^{\text{maks}(0,0,1)} 11^{\text{maks}(1,0,0)}$$

$$= 2^3 \cdot 3^3 \cdot 7^1 \cdot 11^1$$

$$= 16.632$$

Jika diberikan suatu bilangan bulat positif, misalnya 2167, apakah bilannngan ini suatu bilangan prima? Untuk menjawab pertanyaan ini, kita akan mencoba-coba membagi bilangan tersebut dengan 2,3,4,5, dan seterusnya, sampai sautu bilangan yang tidak lebih dari bilangan tersebut. Jika bilangan tersebut tak terbagi oleh salah satu dari pembagi-pembagi itu, maka bilangan tersebut adalah suatu bilangan prima. Cara ini jelas tidak efesien. Berikut ini suaut teorema yang memberikan batas sampai bilangan bulat positif mana jita berhenti membagi dan segera menyimpulkan bawa bilangan terebut adalah bilangan prima.

Teorema 5.3:

Jika n suatu bilangan komposit, maka n memiliki faktor dengan $1 < k \leq \sqrt{n}$.

Bukti:

Karena n suatu bilangan komposit, maka ada bilangan-bilangan positif k dan m sedemikian hingga

$km = n\ dengan$ $1 < k < n$ dan $1 < m < n$

Jika k dan m kedua-duanya lebih besar dari $\sqrt{n}$, yaitu $k > \sqrt{n}$ dan $m > \sqrt{n}$, maka

$$n = km > \sqrt{n} \cdot \sqrt{n} = n$$

Terdapat $n > n$, hal ini tidak mungkin. Oleh karena itu, salah satu dari k atau m harus tidak lebih kecil dari $\sqrt{n}$, misalnya k yaitu $1 < k \leq \sqrt{n}$.

Jadi, n memiliki faktor k dengan $1 < k \leq \sqrt{n}$.

Teorema 4.3 tersebut sama benarnya dengan kontraposisinya, yaitu:

Jika bilangan bulat positif n tidak memiliki faktor k dengan $1 < k \leq \sqrt{n}$, maka n adalah suatu bilangan prima.

Dengan kontraposisi Teorema 4.3 tersebut, maka untuk menentukan apakah 2.167 merupakan suatu bilangan prima atau bukan, kita harus mencoba membagi bilangan itu dengan $2,3,4,5, \dots ,46, \sqrt{2167}$. Tetapi ingat bahwa 2167 tak terbagi oleh 2, maka 2167 tak terbagi oleh semua kelipatan 2. Demikian pula 2167 tak terbagi olh 3, maka 2167 tak terbagi oleh kelipatan 3. Demikian seterusnya, sehingga kita cukup mencoba-coba membagi bilangan tersebut dengan bilangan-bilangan prima yang kurang dari 46.

Dari contoh tersebut, kita dapat memperketat syarat perlu dari teorema 4.3, sehingga diperoleh teorema sebagai berikut:

Teorema 5.4:

Jika bilangan bulat positif n tidak memiliki faktor prima p dengan $1 < p \leq \sqrt{n}$, maka n suatu bilangan prima.

E.4. Latihan Kegiatan Belajar 5

Selesaikan soal-soal berikut ini dengan benar!

F. KEGIATAN BELAJAR 6

F.1. Pendahuluan Kegiatan Belajar 6

Bahan kajian	:	faktorisasi tunggal
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep faktorisasi tungal.
Indikator pembelajaran	:	mahasiswa mampu mengimplementasikan konsep dan prinsip faktorisasi tunggal dalam menyelesaikan masalah
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, relasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, dan faktorisasi bilangan tunggal.

F.2. Bahan Pembelajaran Kegiatan Belajar 6

A. Faktorisasi Tunggal

Pada sub bab sebelumnya telah dibicarakan bahwa setiap bilangan bulat positif yang lebih besar dari 1 terbagi oleh suatu bilangan prima, sehingga setiap bilangan bulat positifyang lebih besar dari 1 adalah suaut bilangan prima atau bilangan itu dapat dinyatakan sebagai perkalian dari bilangan-bilangan prima tertentu. Pada sesi ini akan dipelajari bahwa pembfaktoran suatu bilangan bulat positif atas faktor-faktor prima tunggal, tetapi sebelum membicarakan faktorisasi tunggal, kita akan mempelajari beberapa teorema sebagai persiaan untuk mempelajari faktorisasi tunggal.

Teorema 6.1:

Jika p suatu bilangan prima dan $p|ab$, maka $p|a$ atau $p|b$.

Bukti:

Karena p suatu bilangan prima, maka untuk sebarang bilangat bulat a berlaku $(a,p) = 1$ atau $(a,p) = p$. Jika $(a,p) = 1$ dan $p|ab$, kita pernah membuktikan bahwa $p|b$. Buktikanlah kembali! Dan jika $(a,p) = p$ maka $p|a$. Jadi, terbukti bahwa $p|a$ atau $p|b$.

Teorema 4.5 ini dapat diperluas untuk bilangan-bilangan $a_1, a_2, a_3, \dots, a_n$, yaitu:

Jika p suatu bilangan prima dan $p|a_1a_2a_3 \dots a_n$, maka $p|a_1$ untuk suatu $i = 1,2,3,4, \dots, n$.

Bukti:

Kita akan membuktikan dengan induksi matematik pada n, yaitu banyaknya faktor.

Untuk $n = 1$, yaitu $p|a_1$, jelas benar.

Untuk $n = 2$, yaitu $p|a_1a_2$, karena p suatu bilangan prima, maka menurut Teorema 4.5 $p|a_1$ atau $p|a_2$.

Diambil sebagai hipotesis induksi untuk t dengan $2 < t < n$, yaitu p bilangan prima dan $p|a_1a_2a_3 \dots a_t$ maka $p|a_k$ untuk $2 < k < t$.

Pandang $p|a_1a_2a_3 \dots a_n$ atau dapat ditulis sebagai $p|(a_1a_2a_3 \dots a_{n-1})(a_n)$, maka menurut Teorema 4.5 diperoleh $p|a_1a_2a_3 \dots a_{n-1}$ atau $p|a_n$.

Jika $p|a_n$, maka teorema telah terbukti.

Jika $p|a_1a_2a_3 \dots a_{n-2}a_{n-1}$, maka menurut Teorema 4.5 lagi diperoleh $p|a_1a_2a_3 \dots a_{n-2}$ atau $p|a_{n-1}$.

Jika $p|a_{n-1}$, maka teorema terbukti.

Jika $p|a_1a_2a_3 \dots a_{n-2}$ maka proses seperti di atas dapat diteruskan. Berdasarkan hipotesis yang diambil, maka dapat diteruskan mesti akan berakhir. Berarti bilangan prima p membagi salah satu dari $a_1a_2a_3, \dots, a_n$.

Jika pada teorema 4.5 diambil kasus bahwa p,q, dan r masing-masing bilangan prima dan $p|qr$ maka $p|q$ atau $p|r$, yaitu $p = q$ atau $p = r$. Karena p, q, dan r masing-masing bilangan prima kasus tersbut dapat diperluas sebagai berikut:

Jika p, q_1, q_2, q_3,....,q_n semuanya bilangan prima dan $p|q_1q_2q_3 \dots q_n$, maka $p = q_k$ untuk suatu k dengan $1 \leq k \leq n$.

Selanjutnya kita akan membuktikan ketunggalan dari faktorisasi prima dari suatu bilangan bulat positif. Teorema ini sering disebut faktorisasi tunggal yng merupakan teorema dasar dalam aritmetika.

Teorema 6.2:

Pemfaktoran suatu bilangan bulat positif yang lebih besar dari 1 atas faktor-faktor prima adalah tunggal, kecuali urutan dari faktor-faktornya.

Bukti:

Pada teorema 4.2 kita telah membuktikan bahwa bilangan bulat positif yang lebih besar dari 1 adalah suatu bilangan prima atau bilangan itu dapat dinyatakan sebagai perkalian dari bilangan-bilangan prima tertentu. Sekarang, kita akan membuktikan bahwa faktor-faktor prima tersebut adalah tunggal.

Ambil sembarang bilangan bulat positif $n > 1$.

Jika n suatu bilangan prima, maka n adalah faktornya sendiri.

Jika n suatu bilangan komposit dan diandalkan bahwa pemfaktoran n atas faktor-faktor prima adalah tidak tinggal, misalnya:

$n = p_1p_2 \dots p_t$ dan $n = q_1q_2 \dots q_r$

dengan p_i dan q_j masing-masing adalah bilangan-bilangan prima untuk $i = 1,2,3, \dots, t$ dan $j = 1,2,3, \dots, r$ serta $p_1 \geq p_2 \geq p_3 \geq \dots \geq q_r$ dan $t \leq r$.

Karena $n = p_1p_2 \dots p_t$ maka $p_1|n$ sehingga $p_1|q_1q_2q_3 \dots q_r$. Dan selanjutnya menurut perluasan teorema 4.5, maka $p_1 = q_k$ untuk suatu k dengan $1 \leq k \leq r$. Dan mengingat $q_1 \geq q_2 \geq q_3 \geq \dots \geq q_r$, maka $p_1 \leq q_1$.

Karena $n = q_1q_2 \dots q_r$ maka $q_1|n$ sehingga $q_1|p_1p_2 \dots p_t$. Dan menurut perluasan teorema 4.5, maka $q_1 = p_m$ untuk suatu m dengan $1 \leq m \leq t$. Dan mengingat $p_1 \geq p_2 \geq p_3 \geq \dots \geq p_r$, maka $q_1 \leq p_1$.

Karena $p_1 \leq q_1$ dan $q_1 \leq p_1$, maka $p_1 = q_1$ sehingga dari pemisalan n diatas kita memperoleh bahwa $p_2p_3 \dots p_t = q_2q_3 \dots q_r$. Jika proses seperti di atas diteruskan, maka kita akan memperoleh bahwa

$p_2 = q_2$ sehingga $p_3p_4 \dots p_t = q_3q_4 \dots q_r$.

$p_3 = q_3$ sehingga $p_4p_5 \dots p_t = q_4q_5 \dots q_r$.

Dan seterusnya.

Jika $t = r$ maka proses tersebut akan berakhir pada $p_t = q_r$ dan teorema terbukti.

Tetapi jika $t < r$, maka akan diperoleh bahwa

$$1 = q_{t+1}q_{t+2}q_{t+3} \dots . q_r$$

Hal ini mustahil, karena $q_{t+1}q_{t+2}q_{t+3} \dots . q_r$ adalah bilangan-bilangan prima, maka haruslah $t = r$, sehingga

$$p_1 = q_1, p_2 = q_2, p_3 = q_3, \dots, p_t = q_t$$

Ini berarti bahwa bilangan bulat positif n tersebut hanya dapat dinyatakan sebagi hasil kali faktor-faktor prima secara tunggal.

Pembuktian yang lebih singkat dari teorema faktorisasi tunggal tersebut menggunakan induksi matematik. Coba lakukan pembuktian dengan induksi matematik ini dengan memperhatikan petunjuk berikut ini.

Apakah teorema benar untuk $\mathrm{n} = 2$?

Sebagai hipotesis, misalkan teorema benar-benar untuk bilangan bulat positif $n \leq k$ dan harus ditunjukkan bahwa benar untuk $n = k + 1$.

Misalkan $k + 1 = p_1p_2 \dots p_t = q_1q_2q_3 \dots q_r$ denan p_i atau q_i masing-masing adalah bilangan-bilangan prima .... dan seterusnya seperti bagian pembuktian di atas, sehingga diperoleh $p_1 = q_1$ dan $p_2 \dots p_t = q_2q_3 \dots q_r$. Bilangan ini lebih kecil atau sama dengan k, mengingat hipotesis, maka teorema benar untuk $n = k + 1$.

Dengan demikian terbuktilah teorema tersebut.

Kita mengetahui bahwa banyaknya bilangan asli adalah tak berhingga dan setiap bilangan bulat positif dapat difaktorkan atas faktor-faktor prima. Apakah banyaknya bilangan prima itu tak berhingga pula?

Euclides membuktikan dengan bukti tak langsung (bukti dengan kontradiksi) bahwa benyaknya bilangna prima adalah tak berhingga.

Misalkan $p_1 = 2$, $p_1 = 2$, $p_1 = 2$, $p_1 = 2$, ... adalah urutan bilangan-bilangan prima dan andaikan ada bilangan prima terbesar, misalkan p_n, sekarang dibentuk suatu bilangan bulat positif:

$$N = p_1 p_2 \dots p_n + 1$$

Karena $N > 1$, menurut Teorema 4.1, maka N dapat dibagi oleh suatu bilangan prima, sehingga N dapat dibagi oleh sekurang-kurangnya satu bilangan prima dari

$$p_1, p_2, p_3, \dots, p_n.$$

Misalnya bilangan prima p_k dengan $1 \leq k \leq n$ yang membagi N, yaitu $p_k | N$.

$N = p_1 p_2 p_3 \dots p_1 + 1$, dengan $p_k | N$ dan $p_k | p_1 p_2 p_3 \dots p_n$, maka $p_k | 1$.

Hal ini tidak mungkin, karena p_k adalah suatu bilangan prima. Oleh karena itu pengandaian bahwa ada bilangan prima terbesar adalah tidak benar; sehingga pengandaian tersebut harus diingkari, dan diperoleh bahwa tak ada bilangan primer terbesar. Atau dengan kata lain bahwa banyaknya bilangan prima adalah tak berhingga. Hal ini terkenal sebagai teorema Euclides.

Teorema 5.7 (Teorema Euclides)

Banyaknya bilangan prima adalah tak berhingga.

Pada pembuktian teorema Euclides tersebut yang menarik adalah pembentukan bilangan bulat positif N sebagai hasilkali semua bilangan prima ditambah 1.

Apakah N tersebut suatu bilangan prima?

Misalkan kita memulai untuk bilangan prima pertama yaitu 2, maka kita memperoleh:

$$N_1 = 2 + 1 = 3$$

$$N_2 = 2 \cdot 3 + 1 = 7$$

$$N_3 = 2 \cdot 3 \cdot 5 + 1 = 31$$

$$N_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$N_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

Coba tunjukkan bahwa N_1, N_2, N_3, N_4, dan N_5 tersebut masing-masing adalah prima. Selanjutnya tentukanlah N_6, N_7, dan N_8. Tunjukkan bahwa bilangan-bilangan ini bukan bilangan prima!

$$N_6 = 59 \cdot 509$$

$$N_7 = 19 \cdot 97 \cdot 277$$

$$N_8 = 347 \cdot 27953$$

Suatu pertanyaan yang jawabannya belum diketahui, apakah ada tak berhingga k sedemikian N_k suatu bilangan prima pula. Demikian pula, apakah tak berhingga bilangan komposit N_k?

Perhatikan barisan bilangan prima 2,3,5,7,...,p_n. p_n adalah bilangan prima ke-n. Sekarang kita ingin menentukan suatu batas atas dari barisan bilangan prima p_n tersebut. Pada pembuktian Teorema Euclides di atas dapat diambil kesimpulan bahwa:

$$p_{n+1} \leq p_1 p_2 p_3 \ldots p_n + 1 < p_n^n + 1$$

Sebagai contoh, jika $n = 3$, maka ketidaksamaan itu menjdai

$$7 = p_4 < p_3^3 + 1 = 5^3 + 1 = 126$$

Ketidaksamaan ini menujukkan bahwa bilangan prima ke-4 kurang dari 126.

Tampak bahwa pendekatan ini masih sangat kasar. Pendekatan yang lebih halus diberikan pada teorema berikut ini.

Teorema 5.8:

Dalam suatu barisan bilangan prima, jika p_n menyatakan bilangan prima ke-n. maka :

$$p_n \leq 2^{2^{n-1}}$$

Bukti:

Pembuktian menggunakan induksi matematik pada n.

Untuk $n = 1$ diperoleh $p_1 \leq 2^{2^0}$ yaitu $p_1 \leq 2$. Hal ini memang benar, sebab bilangan prima pertama adalah 2.

Selanjutnya sebagai hipotesis, teorema diasumsikan benar untuk $n = k,$ yaitu:

$$p_k \leq 2^{2^{k-1}}$$

Harus dibuktikan bahwa teorema benar untuk $n = k + 1$, yaitu $p_{k+1} \leq 2^{2^k}$.

Perhatikan bahwa:

Mudah ditunjukkan bahwa $1 + 2 + 3$ .... dengan suatu deret geometri dengan rasio 2, sehingga diperoleh:

Yaitu sudah deret geometri dengan rasio 2, sehingga diperoleh:

$$p_{k+1} \leq \left(2^{2^k-1} + 1\right)$$

Karena $2^{2^k-1} > 1$ untuk setiap bilangan asli k, maka ketidaksamaan itu menjadi

$$p_{k+1} \leq 2^{2^2-1} + 2^{2^k-1}$$

$$p_{k+1} \leq 2^{2^k}$$

Karena teorema benar untuk $n = 1$ dan benar untuk $n = k$ dan telah ditunjukkan benar untuk $n = k + 1$, maka teorema benar untuk setiap bilangan asli n.

Memperhatikan teorema ini, maka bilangan rima ke $(n + 1)$, yaitu $p_n \leq 2^{2^n}$, sehingga benyaknya bilangan prima yang lebih kecil dari 2^{2^n} tidak kurang dari $(n + 1)$ buah. Jadi, untuk $n \geq 1$, maka ada paling sedikiti n+1 buah bilangan prima yang lebih kecil dari 2^{2^n}.

G. KEGIATAN BELAJAR 7

G.1. Pendahuluan Kegiatan Belajar 7

Bahan kajian	:	definisi dan sifat kekongruenan
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep definisi dan sifat kekongruenan.
Indikator pembelajaran	:	

- mahasiswa mampu merumuskan definisi dan sifat kekongruenan.
- mahasiswa mampu mengaplikasikan definisi dan sifat kekongruenan untuk menyelesaikan masalah.

Materi prasyarat	:	teori himpunan, sistem bilangan bulat, relasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, dan faktorisasi bilangan tunggal.

G.2. Bahan Pembelajaran Kegiatan Belajar 8

A. Definisi dan Sifat Kekongruenan

Pada bab sebelumnya kita telah membahas konsep keterbagian beserta sifat-sifatnya. Konsep dan sifat-sifat keterbagian itu dapat dipelajari lebih mendalam lagi dengan menggunakan konsep kekongruenan. Memang kekongruenan merupakan cara lain untuk menelaah keterbagian dalam himpunan bilangan bulat.

Definisi 8.1:

Jika m suatu bilangan bulat positif, maka a kongruen dengan b modulo m (ditulis $a \equiv b$ (mod m)) bila m membagi $(a - b)$. Jika m tidak membagi $(a - b)$ maka dikatakan bahwa a tidak kongruen dengan b modulo m (ditulis $a \not\equiv b$ (mod m)).

Contoh 8.1:

$25 \equiv 1$ (mod 4), sebab 4 membagi (habis) $25 - 1$.

$31 \not\equiv 5$ (mod 6), sebab 4 membagi (habis) $31 - 5$.

Definisi 8.1 tersebut dapat ditulis bahwa jika $m > 0$ maka $m \mid (a - b)$ bila dan haya bila $a \equiv b$ (mod m). Jika $m \mid (a - b)$, maka ada bilangan bulat k sehingga $(a - b) = m$. Sehingga $a \equiv b$ (mod m) bila dan hanya bila $a - b = m$ untuk suatu bilangan bulat k.

Tetapi karena $-b = m$ sama artinya dengan $a = m \quad + b$, maka $a \equiv b$ (mod m) bila dan hanya bila $a = \quad m \quad + b$.

Contoh 8.2:

$26 \equiv 4$ (mod 11) sama artinya dengan $26 = 11 \,.\, 2 + 4$.

$38 = 3$ (mod 5) sama artinya dengan $38 = 5 \,.\, 7 + 3$.

Uraian tersebut merupakan bukti dari teorema berikut ini:

Teorema 8.1:

$a \equiv b$ (mod m) bila dan hanya bila ada bilangan bulat k sehingga $a = m \quad + b$.

Kita telah mempelajari bahwa jika a dan m bilangan-bilangan bulat dan $m > 0$, menurut algoritma pembagian, maka a dapat dinyatakan sebagai:

$$a = m \quad + \text{r dengan } 0 \le r < m.$$

Ini berarti bahwa $a - r = m$, yaitu $a \equiv r$ (mod m). Karena $0 \le r < m$, maka ada m buah pilihan untuk r, yaitu $0, 1, 2, 3, \ldots, (m - 1)$. Jadi setiap bilangan bulat akan kongruen modulo m dengan tepat satu diantara $0, 1, 2, 3, \ldots, (m - 1)$. Hal ini dinyatakan sebagai teorema berikut ini.

Teorema 8.2:

Setiap bilangan bulat kongruen modulo m dengan tepat satu diantara $0, 1, 2, 3, \ldots, (m - 1)$.

Definisi 8.2:

Jika $a \equiv r$ (mod m) dengan $0 \le r < m$, maka r disebut *residu terkecil* dari a m m.

Untuk kekongruenan modulo m ini, $\{0, 1, 2, 3, \ldots, (m - 1)\}$ disebut himpunan residu terkecil modulo m.

Contoh 8.3:

Residu terkecil dari 71 modulo 2 adalah 1, karena sisa 71 : 2 adalah 1.

Residu terkecil dari 71 modulo 3 adalah 2, karena sisa 71 : 3 adalah 2.

Residu terkecil dari – 53 modulo 10 adalah 7, sebab sisa -53 : 10 adalah 7. (ingat bahwa residu terkecil dari suatu bilangan diambil bilangan bulat positif).

Residu terkecil dari 34 modulo 5 adalah 4, sebab sisa 34 : 5 adalah 4.

Walupun $34 \equiv 9$ (mod 5), tetapi 9 bukan residu terkecil dari 34 (mod 5), sebab 9 bukan sisa dari 34 : 5.

Contoh 8.4:

Himpunan residu terkecil modulo 5 adalah $\{0, 1, 2, 3, 4\}$.

Himpunan residu terkecil modulo 9 adalah $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

Himpunan residu terkecil modulo 25 adalah $\{0, 1, 2, 3, \ldots, 24\}$.

Kita dapat melihat relasi kekongruenan itu dengan cara lain, seperti pada teorema berikut ini.

Teorema 8.3:

$a \equiv b$ (mod m) bila dan hanya bila a dan b memiliki sisa yang sama jika dibagi m.

Bukti:

Pertama dibuktikan jika $a \equiv b$ (mod m) maka a dan b memiliki sisa yang sama jika dibagi m. Karena $a \equiv b$ (mod m) maka $a \equiv r$ (mod m) dan $b \equiv r$ (mod m) dengan r adalah residu terkecil modulo m atau $0 \leq r < m$.

Selanjutnya, $a \equiv r$ (mod m) berarti $a = m \quad + r$ untuk suatu bilangan bulat q, dan $b \equiv r$ (mod m) berarti $b = \quad m \quad + r$ untuk suatu bilangan bulat t.

Jadi, a dan b memiliki sisa yang sama jika dibagi m.

Kedua, buktikan jika a dan b memiliki sisa yang sama jika dibagi m, maka $a \equiv b$ (mod m). Misalkan a memiliki sisa r jika dibagi m, berarti $a = m \quad + r$ dan b memiliki sisa r jika dibagi m, berarti $b = m \quad + r$.

Dari kedua persamaan itu diperoleh bahwa:

$a - b = m(q - t)$ berarti $m|(a - b)$ atau $a \equiv b$ (mod m)

Menurut *teorema*-teorema terdahulu, ungkapan-ungkapan berikut mempunyai arti yang sama yaitu:

“ n ≡ 7 (mod 8)”

“n = 7 + 8k untuk suatu bilangan bulat k”, dan

“n dibagi 8 bersisa 7”

Definisi 8.3:

Himpunan bilangan bulat $\{r1, r2, r3, \ldots, rm\}$ disebut sistem residu lengkap modulo m, bia setiap elemennya kongruen modulo m dengan satu dan hanya satu dari 0, 1, 2, ..., (m – 1).

Contoh 8.5:

(i) Himpunan {45, -9, 12, -22, 24} adalah suatu sistem residu lenngkap modulo 5. Dapat diperiksa bahwa

$$45 \equiv 0 \pmod 5$$
$$-9 \equiv 1 \pmod 5$$
$$12 \equiv 2 \pmod 5$$
$$-22 \equiv 3 \pmod 5$$
$$24 \equiv 4 \pmod 5$$

(ii) Himpunan $\{0, 1, 2, 3, 4\}$ juga merupakan suatu sistem residu lengkap modulo 5, sekaligus sebagai himpunan residu terkecil modulo 5.

(iii) Himpunan $\{4, 3, 1, 2, 0\}$ pun merupakan suatu sistem residu lengkap modulo 5.

(iv) Himpunan $\{5, 11, 6, 1, 8, 15\}$ bukan merupakan sistem residu lengkap modulo 6, sebab $5 \equiv 11$ (mod 6) yang dua-duanya berada dalam himpunan tersebut.

Kekongruenan modulo suatu bilangan bulat positif adalah suatu relasi antara bilangan-bilangan bulat. Dapat ditunjukkan bahwa relasi kekongruenan itu merupakan relasi ekuivlensi. Kita ingat bahwa suatu relasi disebut relasi ekuivalensi jika relasi itu memiliki sifat refleksi, sifat simetris dan sifat transitif.

Jika m, a, b, dan c adalah bilangan-bilangan bulat dengan m positif, maka:

(i) Jika $a \equiv a$ (mod m), sifat refleksi.

(ii) Jika $a \equiv b$ (mod m) maka $b \equiv a$ (mod m), sifat simetris.

(iii) Jika $a \equiv b$ (mod m) dan $b \equiv c$ (mod m) maka $a \equiv c$ (mod m) sifat transitif.

Kita buktikan tiap-tiap sifat itu!

(i) Karena $a - a = 0 = 0m$, maka $a \equiv a$ (mod m).

(ii) Karena $a \equiv b$ (mod m) maka $a - b = k$ untuk suatu bilangan bulat k, sehingga $b - a = -k$ yang berarti bahwa $b \equiv a$ (mod m).

(iii) $a \equiv b$ (mod m) berarti $a - b = k$ untuk suatu bilangan bulat $k \cdot b \equiv c$ (mod m) berarti $b - c = hm$ untuk suatu bilangan bulat h. Ruas-ruas kedua persamaan dijumlahkan, sehingga diperoleh $a - c = (k - h)m$ yang berarti bahwa $a \equiv c$ mod m.

Karena relasi "≡" (kekongruenan) pada himpunan bilangan bulat memenuhi tiga sifat tersebut, maka relasi kekongruenan pada himpunan tersebut merupakan relasi ekivalen. Akibatnya himpunan bilangan bulat terpartisi dalam himpunn-himpunan bagian yang setiap himpunan bagian disebut kelas.

Contoh 8.6:

Misalnya kita memperhatikan himpunan bilangan bulat dengan relasi kekongruenan modulo 5, maka dengan relasi ini himpunan bilangan bulat terpartisi (terbagi menjadi himpunan bagian – himpunan bagian yang saling asing dan gabungannya sama dengan himpunan bilangan bulat) menjadi 5 kelas, yaitu:

$\bar{0}$ = [0] = { . . . , -10, -5, 0, 5, 10, . . .}

$\bar{1}$ = [1] = { . . . , -9, -4, 1, 6, 11, . . . }

$\bar{2}$ = [2] = { . . . , -8, -3, 2, 7, 12, . . . }

$\bar{3}$ = [3] = { . . . , -7, -2, 3, 8, 13, . . . }

$\overline{4}$ = [4] = { . . . , -6, -1, 4, 9, 14, . . . }

Pemberian nama untuk suatu kelas menggunakan nama salah satu anggota dari kelas tersebut yang dibubuhi tanda garis diatasnya atau dikurung persegi. Misalnya:

[3] = [-2] = [8] atau $\overline{3} = \overline{2} = \overline{8}$

Relasi kekongruenan mempunyai kemiripan sifat dengan sifat persamaan, sebab relasi kekongruenan dapat dinyatakan sebagai persamaan, yaitu $a \equiv b(m \quad m)$ sama artinya dengan $a = b + k \quad$, untuk suatu bilangan k.

Misalnya:

(1) jika $a \equiv b$ (mod m) maka $a + c \equiv b + c$ (mod m) untuk setiap bilangan bulat c.

(2) Jika $a \equiv b$ (mod m) maka $a \quad \equiv b \quad$ (mod m) untuk setiap bilangan bulat c.

Coba buktikan kedua sifat tersebut!

Kemiripan itu akan tampak pula pada teorema berikut ini.

Teorema 8.4:

Jika $a \equiv b$ (mod m) dan $c \equiv d$ (mod m) maka $a + c = b + d$.

Bukti:

$a \equiv b$ (mod m) berarti $a = m \quad + b$ untuk suatu bilangan bulat s.

$c \equiv d$ (mod m) berarti $c = \quad m \quad + d$ untuk suatu bilangan bulat t.

Dua pasangan ini akan *memberikan* bahwa:

$$a + c = (m \quad + b) + (m \quad + d)$$

$$a + \ c = m(s + t) + (b + d)$$

$$(a + c) - (b + d) \ = m\ (s\ +\ t)$$

Ini berarti $a + c \equiv b + \ d$ (mod m).

Lebih umum teorema 8.4 dinyatakan sebagai teorema berikut ini.

Teorema 8.5:

Jika $a \equiv b$ (mod m) dan $c \equiv d$ (mod m) maka $a \quad + c \quad \equiv b \quad + d \quad$ (mod m), untuk setiap bilangan bulat x dan y.

Bukti:

$a \equiv b$ (mod m) berarti $a = m \quad + b$ untuk suatu bilangan bulat s.

$c \equiv d$ (mod m) berarti $c = m \quad + d$ untuk suatu bilangan bulat t.

Jika kedua ruas persamaan pertama dikalikan x dan kedua ruas persamaan kedua dikalikan y diperoleh:

$a \quad = m \quad + b$ dan

$c \quad = m \quad + d$

Dengan menjumlahkan ruas persamaan ini diperoleh

$a \quad + c \quad = (m \quad + b \quad) + (m \quad + d \quad)$

$a \quad + c \quad = m\,(s \quad + t \quad) + (bx + d \quad)$

$(a \quad + c \quad) - (b \quad + d \quad) = m(s \quad t \quad)$

Persamaan terakhir ini berarti bahwa:

$m \mid [(a \quad + \ c \quad) - (b \quad + \ d \quad)]$ atau $a \quad + \ c \quad \equiv \ b \quad + \ d \quad (m \quad m)$

Pada persamaan/kesamaan bilangan-bilangan bulat berlaku sifat kanselasi (penghapusan) sebagai berikut: jika $a \quad = a \quad$ dengan $a \neq \ 0$ maka $b = c$. Apakah dalam kekongruenan berlaku sifat yang mirip dengan sifat kanselasi tersebut? Misalkan, jika $a \quad \equiv a \quad$ (mod m) dengan $a \not\equiv 0$ (mod m), apakah $b \equiv c$ (mod m)?

Ambil sebuah contoh:

$24 \equiv 12$ (mod 4) adalah suatu pernyataan yang benar (mengapa?).

2.12 ≡ 2.6 (mod 4) dan jels bahwa 2 ≢0 (mod 4).

Apakah 12 ≡ 6 (mod 4)? Jelas tidak! (mengapa?)

Tetapi jika 3.8 ≡ 3.4 (mod 4) maka 8 ≡ 4 (mod 4) adalah suatu pernyataan yang benar.Walaupun sifat kaselasi tidak berlaku sepenuhnya pada relasi kekongruenan, tetapi akan berlaku dengan suatu syarat seperti dinyatakan dalam teorema berikut ini.

Teorema 8.6

Jika $a \quad \equiv b \quad$ (mod m) dengan $(c, m) \ = \ 1$, maka $a \equiv b$ (mod m).

Bukti:

$a \quad \equiv b \quad$ (mod m) berarti $m|(c - b \quad)$ atau $m|(c - b)$.

$m|c(a - b)$ dengan $(c, m) = 1$, maka $m|(a - b)$ berarti $a \equiv b$ (mod m).

Contoh 8.7:

Tentukanlah bilangan-bilangan bulat y yang memenuhi perkongruenan $3y \equiv 1$ (mod 7).

Jawab:

Karena $1 \equiv 15$ (mod 7), maka kita dapat mengganti 1 pada perkongruenan tersebut dengan 15, sehingga diperoleh $3y \equiv 15$ (mod 7). Selanjutnya, karena $(3, 7) = 1$, maka kita dapat membagi 3 pada ruas-ruas perkongruenan itu, sehingga diperoleh $y \equiv 5$ (mod 7). Perkongruenan terakhir ini berarti $y = 5 + 7k$ untuk setiap bilangan bulat k. atau dapat dikatakan bahwa himpunan penyelesaian dari perkongruenan tersebut adalah $\{5 \ + \ 7k \mid k$ bilangan bulat$\}$.

Kita dapat menghapus (melenyapkan) suatu faktor dari suatu kekongruenan, jika faktor tersebut dan bilangan modulonya saling prima. Tetapi, jika faktor adan modulonya tidak saling prima, maka kita harus mengganti bilangan modulonya seperti tampak dalam teorema berikut ini.

Teorema 8.7:

Jika $a \equiv b \pmod{m}$ dengan $(c, m) = d$, maka $a \equiv b$ (mod $\frac{m}{d}$).

Bukti:

$a \equiv b \pmod{m}$ berarti $m|(a - b)$ atau $m|c(a-b)$ maka $\frac{m}{d}\Big|\frac{c}{d}$ (a – b).

Karena d adalah FPB dari c dan m, maka $\frac{m}{d}$ dan $\frac{c}{d}$ adalah bilangan-bilangan bulat. Karena $(c, m) = d$ maka $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$.

Karena $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ dan $\frac{m}{d} \mid \frac{c}{d}$ (a – b) berarti $a \equiv b$ (mod $\frac{m}{d}$).

Contoh 8.8:

Tentukan x yang memenuhi $2x \equiv 4 \pmod{6}$.

Jawab:

$2x \equiv 2.2$ (modulo 6) karena (2, 6) = 2, maka $x \equiv 2 \pmod{3}$.

Jadi nilai-nilai x adalah $(3k + 2)$ untuk setiap bilangan bulat k. atau dapat dikatakan bahwa himpunan penyelesaian dari perkongruenan itu adalah $\{3k + 2 | k$ bilangan bulat$\}$.

B. Aplikasi Kekongruenan

Pada sub bab sebelum ini telah kita pelajari pengertian relasi kekongruenan beserta sifat-sifatnya. Pada sub bab ini kita akan mempelajari penggunaan pengertian dan sifat-sifat kekongruenan itu.

Kekongruenan modulo 9 dapat digunakan untuk memeriksa kebenaran perkalian dan penjumlahan bilangan-bilangan bulat. Kita mengetahui bahwa:

$10.000 - 1 = 9.999 = 9k_1$ sehingga $10.000 \equiv 1$ (m 9)

$1.000 - 1 = 999 = 9k_2$ sehingga $1.000 \equiv 1$ (m 9)

$100 - 1 = 99 = 9k_3$ sehingga $100 \equiv 1$ (m 9)

$10 - 1 = 9 = 9k_4$ sehingga $10 \equiv 1$ (m 9)

Selanjutnya akan di tunjukkan bahwa setiap bilangan bulat kongruen modulo 9 dengan jumlah angka-angkanya.

Contoh 8.9

$8.234 \equiv 8000 + 200 + 30 + 4 \pmod{9}$

$\equiv 8(1000) + 2(100) + 3(10) + 4 \pmod{9}$

$\equiv 8(1) + 2(1) + 3(1) + 4 \pmod{9}$

$8.234 \equiv 17 \pmod 9$

Selanjutnya dengan cara yang sama:

$17 \equiv 10 + 7 \pmod 9$

$\equiv 1 + 7 \pmod 9$

$17 \equiv 8 \pmod 9$

Jadi $8.234 \equiv 8 \pmod 9$

Uraian dan contoh di atas secara umum dinyatakan sebagai teorema-teorema berikut ini.

Teorema 8.8:

$10^n \equiv 1 \pmod 9$ untuk $n = 0, 1, 2, 3, \ldots$

Bukti :

$10^n \equiv 1 = 999\ldots9$ (n angka semuannya 9) terbagi oleh 9

Jadi $10^n \equiv 1 \pmod 9$

Teorema 8.9

Setiap bilangan bulat kongruen modulo 9 dengan jumlah angka-angkanya.

Bukti :

Ambil sembarangan bilangan bulat n yang angka-angkanya secara berturut-turut adalah:

$n = d_k\, d_{k-1} d_{k-2} \ldots d_2\, d_1\, d_0$ atau

$n = d_k\, 10^k + d_{k-1}\, 10^{k-1} + d_{k-2}\, 10^{k-2} + \ldots + d_2\, 10^2 + d_1\, 10 + d_0$

dengan $0 \leq d_i \leq 9$ untuk $i = 0, 1, 2, \ldots, k$ dan $d_k \neq 0$.

Menurut Teorema 5.8 $10^n \equiv 1 \pmod 9$ untuk $n = 0, 1, 2, 3, \ldots$ sehingga

$n \equiv d_k (1) + d_{k-1} (1) + d_{k-2} (1) + \ldots + d_2 (1)\, d_1 (1) + d_0 \pmod 9$

$n \equiv d_k + d_{k-1} + d_{k-2} + \ldots + d_2 + d_1 + d_0 \pmod 9$

Jadi bilangan bulat n kongruen modulo 9 dengan jumlah angka-angkanya.

Perhatikan sekarang, misalkan $a + b = c$ maka tentulah $a + b \equiv c \pmod 9$. Jika $a \equiv m \pmod 9$, $b \equiv n \pmod 9$, dan $c \equiv p \pmod 9$, maka dari $a + b \equiv c \pmod 9$ dapat disimulkan bahwa $m + n \equiv p \pmod 9$.

Prinsip tersebut dapat digunakan untuk memriksa kebenaran suatu penjumlahan maupun pengurangan bilangan-bilangan bulat.

Contoh 8.10

Periksalah kebenaran penjumlahan berikut ini dengan prinsip di atas: $248 + 324 + 672 = 1.244$

Jawab:

$248 \equiv 2 + 4 + 8 \pmod 9$

$\equiv 14 \pmod 9$

$\equiv 10+4 \pmod 9$

$\equiv 1 + 4 \pmod 9$

$\equiv 5 \pmod 9$

$324 \equiv 3 + 2 + 4 \pmod 9$

$\equiv 9 \pmod 9$

$\equiv 0 \pmod 9$

$672 \equiv 6 + 7 + 2 \pmod 9$

$\equiv 15 \pmod 9$

$\equiv 6 \pmod 9$

Jadi $248 + 324 + 672 \equiv 5 + 0 + 6 \pmod 9$

$\equiv 11 \pmod 9$

$\equiv 10+1 \pmod 9$

$\equiv 1 + 1 \pmod 9$

$\equiv 2 \pmod 9$ . . . .(i)

Sedangkan $1.244 \equiv 1 + 2 + 4 + 4 \pmod 9$

$\equiv 11 \pmod 9$

$\equiv 2 \pmod 9$ . . . .(ii)

Dari kekongruenan (i) dan (ii) berarti :

$$248 + 324 + 672 = 1244 \text{ ((benar)}$$

Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$, maka $ac \equiv bd \pmod m$ prinsip ini dapat digunakan untuk memeriksan kebenaran suatu perkalian.

Contoh 5.11

Berikut $84 \times 428 = 35.952$?

Jawab :

$84 \equiv 8 + 4 \pmod 9$ $\Leftrightarrow 8 + 4 \pmod 9 \equiv 12 \pmod 9$

$\Leftrightarrow 12 \pmod 9 \equiv 3 \pmod 9$

$428 \equiv 4 + 2 + 8 \pmod 9$

$\equiv 14 \pmod 9$

$\equiv 5 \pmod 9$

Maka $84 \times 428 \equiv 3 \times 5 \pmod 9$

$\equiv 15 \pmod 9$

$\equiv 6 \pmod 9$ . . . .(i)

Sedangkan $35.952 \equiv 3 + 5 + 9 + 5 + 2 \pmod 9 \Leftrightarrow 3 + 5 + 9 + 5 + 2 \equiv 24 \pmod 9$

$$\Leftrightarrow 24 \equiv 20 + 4 \pmod 9$$

$$\Leftrightarrow 24 \equiv 2(10) + 4 \pmod 9$$

$$\Leftrightarrow 2(10) + 4 \equiv 2(1) + 4 \pmod 9$$

$$\Leftrightarrow 2(1) + 4 \equiv 2 + 4 \pmod 9$$

$$\Leftrightarrow 2 + 4 \equiv 6 \pmod 9$$

$$\Leftrightarrow 24 \equiv 6 \pmod 9 \ldots\ldots \text{(ii)}$$

Dari (i) dan (ii) *disimpulkan* bahwa 84 x 428 = 35.952 (benar)

Coba buatlah contoh-contoh *untuk* pengurangan dan pembagian bilangan-bilangan bulat dan periksalah kebenaranya dengan kekongruenan modulo 9.

Perlu dicatat bahwa pemeriksaan kebenaran penjumlahan, pembagian, pengurangan, perkalian dan pembagian dengan kekongruenan modulo 9 ini belum menjamin bahwa operasi yang kita lakukan itu benar atau salah. Tetapi cara ini kita lakukan, setelah kita mengerjakan operasi hitung tersebut *mungkin* dalam mengoperasikan kita keliru menjumlah puluhannya, ratusannya atau lainnya. Dengan kata lain koreksi 9 tersebut bukan merupakan syarat cukup, tetapi hanya merupakan syarat perlu untuk kebenaran hasil operasi.

Contoh 8.12:

10 + 11 = 30

Kita mengetahui bahwa $10 + 11 \equiv 3 \pmod 9$

dan $30 \equiv 3 \pmod 9$

Menurut cara pemeriksaan di atas 10 + 11 = 30, benar.

Tetapi kita mengetahui bahwa 10 + 11 = 30, salah

Selain itu, kekongruenan modulo 9 dapat digunakan untuk menguji keterbagian suatu bilangan bulat oleh 9.

Suatu bilangan terbagi oleh 9 bila dan hanya bila sisa pembagian itu nol.

$n \equiv a(m$ 9) jika dan hanya jika n dan a masing-masing mempunyai sisa yang sama jika dibagi 9.

Jadi, jika $n \equiv a \pmod 9$ maka n terbagi oleh 9, bila dan hanya bila a terbagi oleh 9. Padahal n kongruen modulo 9 dengan jumlah angka-angkanya.

Jadi suatu bilangan terbagi *oleh 9 bila dan hanya bila jumlah angka-angkanya terbagi oleh 9.*

Contoh 8.13

(i) $7.587 \equiv 7 + 5 + 8 + 7 \equiv 27 \equiv 9 \pmod 9$

$7.587 \equiv 9 \pmod 9$

Karena 9 | 9 maka 9 | 7587

(ii) 47.623 ≡ 4 + 7 + 6 + 2 + 3 ≡ 22 ≡ 4 (mod 9)

Karena 9 ∤ 4 maka 9 ∤ 47.623

Apakah suatu bilangan yang terbagi oleh 9 akan terbagi pula oleh 3?

Misalkan 9 | n dan 3 | 9 dengan sifat transitif diperoleh jumlah angka-angkanya terbagi oleh oleh 9, maka n terbagi oleh 3 bila dan hanya bila jumlah angka-angkanya terbagi oleh 3.

Suatu bilangan terbagi oleh 3 jika dan hanya jika jumlah angka-angkanya terbagi oleh 3.

Contoh 8.14

(1) 12.456 ≡ 1 + 2 + 4 + 5 + 6 ≡ 18 ≡ 9 (mod 9)

Karena 3 | 9 maka 3 | 12.456.

(2) 42.641 ≡ 4 + 2 + 6 + 4 + 1 ≡ 17 ≡ 8 (mod 9)

Karena 3 ∤ 8 maka 3 ∤ 42.641.

Bagaimana menguji suatu bilangan terbagi oleh 2, dan 4 dan oleh 8?. Anda pasti setuju, bahwa suatu bilangan terbagi oleh 2, bilangan-bilangan itu genap. Coba buktikan pernyataan itu dengan menggunakan kekongruenan mod 2?

Ambil n, yaitu bilangan yang dinyatakan oleh

$n = a_k\, a_{k-1}\, a_{k-2} \ldots a_1\, a_0$ dengan $0 \le a_i \le 9$ untuk $i = 0, 1, 2, \ldots.$

$n = a_k\, 10^k + a_{k-1}\, 10^{k-1}\, a_{k-1}\, 10^{k-2} + \ldots + a_1\, 10 + a_0$

Terlihat bahwa suku-suku ruas kanan pada persamaan ini terbagi oleh 2, kecuali a_0. Apabila n terbagi oleh 2, maka a_0 pun terbagi oleh 2. $a_0$adalah angka terahir dari bilangan n.

Jadi suatu bilangan terbagi oleh 2 bila dan hanya bila angka terahirnya terbagi oleh 2.

Apakah 10^2. 10^3, 10^4,. . .masing-masing terbagi oleh 4? Jelas terbagi oleh 4 bukan! (mengapa?) nah, bagaimana menguji suatu bilangan terbagi oleh 4.

Misalkan $n = a_k\, a_{k-1}\, a_{k-2} \ldots a_1\, a_0$ atau

$$n = a_k\, 10^k + a_{k-1}\, 10^{k-1}\, a_{k-2}\, 10^{k-2} + \ldots + a_2\, 100 + (a_1\, 10 + a_0)$$

Setiap suku pada ruas kanan pada persamaan itu, kecuali dua suku terahir, yaitu a_1 10 dan a_0, terbagi oleh 4. Jadi, n terbagi oleh 4 bila dan hanya bila (a1 10 + a0) terbagi oleh 4.

Uraian itu dapat disimpulkan sebagai berikut:

Suatu bilangan terbagi oleh 4 bila dan hanya bila bilangan yang *dinyatakan oleh dua angka terahir dari bilangan itu terbagi oleh 4.*

Contoh 8.15:

5.134.216 terbagi oleh 4, sebab 16 (dua angka terahir) terbagi oleh 4.

Dengan cara yang mirip dengan keterbagian oleh 4, turunkanlah suatu aturan keterbagian suatu bilangan oleh 8.

Suatu bilangan terbagi oleh 8 bila dan hanya bila bilangan yang dinyatakan oleh tiga angka terair dari bilangan itu terbagi oleh 8.

Contoh 8.16:

17.256 terbagi oleh 8, sebab 256 (tiga angka terahir) terbagi oleh 8.

Nah, sekarang, bagaimana menguji suatu bilangan terbagi oleh 6?

Apabila 2 | n dan 3 | n dan karena (2, 3) = 1, maka 6 | n. Buktikanlah pernyataan itu! Pernyataan itu dapat dikatakan sebagai berikut.

Suatu bilangan terbagi oleh 6 bila dan hanya *bila bilangan itu terbagi oleh 2 dan terbagi pula oleh 3.*

Selanjutnya dengan mudah pembaca membuktikan bahwa suatu bilangan terbagi oleh 5 bila dan hanya bila angka terahir itu adalah 5 atu 0.

Begitu juga pembaca mudah membuktikan bahwa suatu bilangan terbagi oleh 10 bila dan hanya bila angka terahir itu adalah 0.

Berikut ini dipelajari keterbagian suatu bilangan oleh 11.

$10 \equiv -1 \pmod{11}$

$100 \equiv 10.10 = (-1)(-1) \equiv 1 \pmod{11}$

$1000 \equiv 10.10.10 \equiv (-1)(-1)(-1) \equiv -1 \pmod{11}$ dan seterusnya.

Sehingga pada umumnya $10^n \equiv (-1)^n \pmod{11}$

Apabila $n = a_k\, a_{k-1}\, a_{k-2} \ldots a_1\, a_0$, dengan $0 \le a_i \le 9$ dan $a_k \neq 0$, maka

$$n \equiv a_k\, 10^k + a_{k-1}\, 10^{k-1} + a_{k-2}\, 10^{k-2} + \ldots + a_2\, 100 + a_1\, 10 + a_0 \pmod{11}$$

$$\equiv a_k\, (-1)^k + a_{k-1}(-1)^{k-1} + a_{k-2}\, (-1)^{k-2} + \ldots + a_2\, (-1)^2 + a_1\, (-1) + a_0 \pmod{11}$$

$$\equiv a_k\, (-1)^k + a_{k-1}(-1)^{k-1} + a_{k-2}\, (-1)^{k-2} + \ldots + a_2 - a_1 + a_0 \pmod{11}$$

$$\equiv ((a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)) \pmod{11}$$

a_1, a_3, a_5, . . . berturut-turut adalah ke 2, ke 4, ke 6,. . . pada bilangan n dari belakang dan a_0, a_2, a_4, . . . berturut-turut adalah angka ke 1, ke 3, ke 5, . . . pada bilangan n dari belakang.

Jadi *jika $n = a_k\, a_{k-1}\, a_{k-2} \ldots a_1\, a_0$, maka n terbagi oleh 11 bila dan hanya bila $((a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots))$ terbagi oleh 11.*

Contoh 8.17 :

(1) 180.829 terbagi oleh 11, karena (9 + 8 + 8) – (2 + 0 + 1) = 22 terbagi oleh 11.

(2) 29.183 terbagi oleh 11, karena (3 + 1 + 2) – (8 + 9) = -11 terbagi oleh 11.

Selain penggunaan di atas, kekongruenan dapat digunakan untuk masalah-masalah seperti berikut ini.

(1) Tentukan sisa, jika 20^{50} dibagi 7?

$$20 \equiv -1 \pmod{7}$$

$20^{50} \equiv (-1)^{50}$ (mod 7)

$20^{50} \equiv 1$ (mod 7)

Jadi 20^{50} : 7 bersisa 1

(2) Misalkan satu tahun 360, sekarang hari selasa, seribu hari lagi jatuh pada hari apa? Coba selesaikan dengan kekongruenan modulo 7.

G.4. Latihan Kegiatan Belajar 8

Selesaikan soal-soal berikut ini dengan benar!

1. Tunjukkan bahwa jika a ada sebuah bilangan bulat genap, maka $a^2 \equiv 0(m \quad 4)$, dan jika a adalah sebuah bilangan bulat ganjil, maka $a^2 \equiv 1(m \quad 4)$!
2. Tunjukkan bahwa jika a adalah sebuah bilangan bulat ganjil, maka $a^2 \equiv 1(m \quad 8)$!
3. Tunjukkan bahwa jika a, b, dan m adalah bilangan bulat dengan 90 dan $a \equiv b(m \quad m)$, maka $a\ m \quad m = b\ m \quad m$!
4. Tunjukkan bahwa jika a, b, m dan n adalah bilangan bulat sedemikian sehingga $m > 0$, $n > 0$, $n|m$, dan $a \equiv b(m \quad m)$, maka $a \equiv b(mo \quad n)$!
5. Tunjukkan bahwa jika a, b, c, dan m adalah bilangan bulat sedemikian sehingga $c > 0$, $m > 0$, dan $a \equiv b(m \quad m)$, maka $a \quad \equiv b \quad (m \quad m \quad)$!
6. Show that jika a, b, dan c adalah bilangan bulat dengan $c > 0$ sedemikian sehingga $a \equiv b(m \quad c)$, maka $(a, c) = (b, c)$!

I. KEGIATAN BELAJAR 8

I.1. Pendahuluan Kegiatan Belajar 8

Bahan kajian : perkongruenan linier

Capaian pembelajaran : mahasiswa menguasai pemahaman tentang konsep perkongruenan linier dan sistem perkongruenan linier.

Indikator pembelajaran :

- mahasiswa mampu merumuskan dan mengamplikasikn konsep perkongreunan linier untuk menyelesaikan masalah.
- mahasiswa mampu merumuskan dan mengamplikasikan konsep sism teperkongreunan linier untuk menyelesaikan masalah.

Materi prasyarat : teori himpunan, sistem bilangan bulat, relasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, dan faktorisasi bilangan tunggal.

I.2. Bahan Pembelajaran Kegiatan Belajar 9

A. Perkongruenan Linier

Setelah kita mempelajari pengertian relasi kekongruenan, sifat-sifat dan kegunaannya. Berikut ini akan di pelajari pengkongruenan linier. Kalimat terbuka yang menggunakan relasi kekongruenan disebut *perkongruenan.*

Misalnya:

$$3x \equiv 4(m \quad 5)$$

$$x^4 + 3x - 3 \equiv 0(m \quad 31)$$

Jika suatu pengkongruenan, variabelnya berpangkat paling tinggi satu disebut *pengkongruenan linier*. Bentuk umum perkongruenan linier adalah :

$$a \quad \equiv b\ (m \quad m), \text{ dengan } a \not\equiv 0 \text{ (mod m)}.$$

Perhatikan perkongruenan linier $3x \equiv 4(m \quad 5)$. Apabila x diganti 3 memberikan $3 \cdot 3 \equiv 4\ (m \quad 5)$ atau $9 \equiv 4\ (m \quad 5)$. Yaitu suatu kalimat kekongruenan yang benar. Begitu pula jika x diganti berturut-turut oleh $\ldots -7, -2, 8, 13, \ldots$ akan memberikan kalimat-kalimat kekongruenan yang benar. (coba periksalah!)

Kita telah mengerti bahwa $a \quad \equiv b(m \quad m)$ berarti $ax - b = k \quad$ atau $a \quad = b + k \quad$, untuk suatu bilangan bulat k. Jadi perkongruenan linier $a \quad \equiv b(m \quad m)$ akan mempunyai solusi (penyelesaian) bila dan hanya bila ada bilangan-bilangan bulat x dan k yang memenuhi persamaan.

$$\mathrm{ax} - b = k \quad .$$

Misalkan r memenuhi perkongruenan linier $a \quad \equiv b(m \quad m)$, berarti $a \quad \equiv b(m \quad m)$. Maka setiap bilangan bulat

$(r + m), (r + 2m), (r + 3m), \ldots (r - m), (r - 2m), (r - 3m),. . .$ memenuhi perkongruenan itu, sebab $a(r + k \quad) \equiv a \quad \equiv b(m \quad m)$, untuk setiap bilangan bulat k.

Diantara bilangan-bilangan bulat $(\mathrm{r} + \mathrm{km})$, dengan $\mathrm{k} = 1, 2, 3, 4, \ldots -1, -2, -3, \ldots$. ada tepat satu dan hanya satu, katakan s dengan $0 \leq s \leq m$, sebab suatu bilangan bulat mesti terletak di antara dua kelipatan m yang berurutan.

Jadi, jika r memenuhi perkongruenan $a \quad \equiv b\ (m \quad m)$ dan $k \quad \leq r \leq (k+1)m$ untuk suatu bilangan bulat k, maka $0 \leq (r - k \quad) < m$. Jadi $s = r - k$ untuk suatu bilangan bulat k.

Dengan kata lain, s adalah residu terkecil modulo m yang memenuhi perkongruenan $a \quad \equiv b(m \quad m)$. Selanjutannya s disebut solusi (penyelesaian) dari perkongruenan itu.

Contoh 9.1:

Nilai-nilai x yang memenuhi perkongruenan $2x \equiv 4\ (m \quad 7)$ adalah

. . . -19, -12, -5, 2, 9, 16, . . .

Solusi dari perkongruenan itu adalah 2, yaitu residu terkecil modulo 7 yang memenuhi perkongruenan linier $2x \equiv 4\ (m \quad 7)$.

Pada persamaan $a \quad \equiv b$, dengan $a \neq 0$ hanya mempunyai satu solusi, tetapi pada perkongruenan linier $a \quad \equiv b\ (m \quad m)$ dapat mempunyai tepat satu solusi, banyak solusi, bahkan bisa tidak mempunyai solusi. Pada contoh di atas $2x \equiv 4\ (m \quad 7)$ mempunyai tepat satu solusi, yaitu 2. Perkongruenan linier $2x \equiv 1\ (m \quad 4)$ tidak mempunyai solusi, sebab $4 \nmid (2x + 1)$, yaitu tak ada bilangan bulat x sedemikian $2x - 1$ terbagi oleh 4 (mengapa?). Sedangkan perkongruenan linier $2x \equiv 4\ (m \quad 6)$ mempunyai dua solusi, yaitu 2 dan 5. (coba periksa kebenaranya!). selanjutnya, akan kita pelajari cara menguji suatu perkongruenan linier mempunyai solusi atau tidak.

Teorema 9.1:

Jika $(a, m)\ b$ maka perkongruenan linier $a \quad \equiv b\ (m \quad m)$ tidak memiliki solusi.

Bukti **:**

Kita buktikan kontraposisi dari teorema itu, yaitu jika $a \quad \equiv b(m \quad m)$ memiliki solusi maka $(u, m) \,|b$. Misalkan r adalah solusi dari $a \quad \equiv b\ (m \quad m)$ maka $a \quad \equiv b(m \quad m)$ sehingga $a \ - b = k$ untuk suatu bilangan bulat k.

Perhatikan $a \ - b = k$, karena $(u, m)|\ u$ dan $(u, m)|k$, maka $(u, m)|b$.

Terbuktilah kontraposisi dari teorema itu, sehingga terbukti pula teorema itu.

Contoh 9.2:

$6x \equiv 7(m \quad 8)$, karena $(6, 2) = 2$ dan $2 \nmid 7$ maka perkongruenan linier $6x \equiv\ 7\ (m \quad 8)$ tidak mempunyai solusi.

Teorema 9.2:

Jika $(u, m) = 1$, maka perkongruenan linier $a \quad \equiv b\ (m \quad m)$ memiliki tepat satu solusi.

Bukti **:**

Karena $(u, m) = 1$ maka ada bilangan bulat r dan s sehingga $a \quad + m \quad = 1$.

Jika kedua ruas dari persamaan ini dikaitkan b, diperoleh :

$$(a \quad)b + (m \quad)b\ b$$

$$a(r \quad) \ + \ m\ (s \quad) = b$$

$$u(r \quad) - b = -\ (s \quad)m$$

Persamaan terahir ini berarti bahwa $u(r \quad) - b$ adalah kelipatan m.

Jadi $u(r \quad) \equiv b(m \quad m)$

Maka residu terkecil dari rb modulo m adalah solusi dari perkogruenan linier itu.

Selanjutnya tinggal menunjukkan bahwa solusi itu tunggal andalkan solusi perkongruenan linier itu tidak tunggal, misalkan r dan s masing-masing solusi dari $a \quad \equiv b(m \quad m)$, maka $a \quad \equiv b\ (m \quad m)$ dan $a \quad \equiv b(m \quad m)$,

dengan sifat transituf di peroleh : $a \quad = a\ \ (m \quad m)$.

Karena $(u, m) = 1$, maka $r \equiv s(m \quad m)$. Ini berarti $m|(r - s\ )$.

Tetapi karena r dan s adalah solusi dari perkongruenan itu, maka r dan s masing-masing residu terkecil modulo m, sehingga $0 \leq r < m$ dan $0 \leq s < m$.

Dari kedua ketidaksamaan ini diperoleh bahwa $-m < r - s < m$, tetapi karena $m|(r - s)$ maka

$$r - s = 0 \text{ atau } r = s$$

Ini berarti bahwa solusi dari perkoruenan linier tunggal (terbukti).

Salah satu cara menyelesaikan perkongruenan linier adalah memanipulasi koefisienatau konstanta pada perkongruenan itu, sehingga memungkinkan kita untuk melakukan kanselasi (penghapusan).

Contoh 9.3:

(1) Selesaikan $4x \equiv 1\ (m\quad 15)$

Jawab :

$$4x \equiv 1\ (m\quad 15)$$
$$4x \equiv 16\ (m\quad 15)$$
$$x \equiv 4\ (m\quad 15)$$

Karena $(4,15) = 1$ maka memungkinkan kita melakukan kanselasi 4 pada perkongruenan $4x \equiv 16(m\quad 15)$ sehingga di peroleh $x \equiv 4\ (m\quad 15)$. Solusi dari perkongruenan $4x \equiv 1\ (m\quad 15)$ adalah 4.

(2) Selesaikan $14x \equiv 27(m\quad 31)$

Jawab :

$$14x \equiv 27\ (m\quad 31) \Leftrightarrow 14x \equiv 58\ (m\quad 31)$$
$$\Leftrightarrow 7x \equiv 29\ (m\quad 31)$$
$$\Leftrightarrow 7x \equiv 91\ (m\quad 31)$$
$$\Leftrightarrow x \equiv 13\ (m\quad 31)$$

Karena $27 \equiv 58\ (m\quad 31)$ maka $14x \equiv 58\ (m\quad 31)$.

Karena $(2,31) = 1$, kita dapat menghapus 2 pada perkongruenan $14x \equiv 58(m\quad 31)$ dan di peroleh $7x \equiv 29(m\quad 31)$.

Selanjutnya $7x \equiv 91(m\quad 31)$, sebab $29 \equiv 91(m\quad 31)$

$x \equiv 13(m\quad 31)$, sebab $(7,31) = 1$

Jadi, 13 adalah solusi $4x \equiv 24(m\quad 31)$.

Sesuai teorema 5.11 di atas, jika $(a,m) = 1$, maka perkongruenan $a\quad \equiv 1(m\quad m)$ mempunyai tepat satu solusi pula. Solusi perkongruenan itu disebut *invers dari a modulo m* yang diberi simbol a^{-1}.

Contoh 9.4:

Carilah $2^{-1}(m\quad 31)$.

Jawab :

Untuk mencari $2^{-1}(m\quad 31)$, kita perlu menyelesaikan perkongruenan $2x \equiv 1\ (m\quad 31)$.

$2x \equiv 1\ (m\quad 31)$

$2x \equiv 14\ (m\quad 31)$

$x \equiv 7\ (m\quad 31)$

Jadi $2^{-1}(m\quad 31)$ adalah 7.

Periksalah bahwa 3^{-1} (mod 31) adalah 9, 4^{-1}(mod 31) adalah 10, 5^{-1}(mod 31) adalah 8, 6^{-1}(mod 31) adalah 11, dan 12^{-1}(mod 31) adalah 12.

Berikut ini akan dipelajari banyaknya solusi dari ax ≡ b (mod m), apabila (a, m) = d dan d | b dengan d > 1.

Teorema 9.3:

Jika $(a, m) = d$ dan $d|b$ maka perkongruenan linier $a \quad = b(m \quad m)$ memiliki tepat d solusi.

Bukti :

Kita harus membuktikan bahwa perkongruenan linier $a \quad \equiv b(m \quad m)$ memiliki d solusi. Dan seterusnya harus ditunjukkan bahwa tak ada solusi lain kecuali d solusi itu.

Sekarang akan dibuktikan bahwa perkongruenan linier itu memiliki d solusi. $(a, m) = d$ berarti ada a' dan m'' sehingga $a = d \quad '$ dan $m = d \quad '$. $d \mid b$ berarti ada b' sehingga $b = \; d \quad '$. Sehingga dari $a \quad \equiv b(m \quad m)$ memberikan

$$d \quad 'x \equiv d \quad '(m \quad d \quad ') \text{ atau}$$

$$a'x \equiv b'(m \quad m').$$

Dari $(a, m) = d$ memberikan $(d \quad ', d \quad ') = d$ atau $(a', m') = 1$

Menurut Teorema 9.1, jika $(a', m') = 1$, maka $a' x \equiv b'(m \quad m')$ memiliki satu solusi. Misalkan solusi itu r, maka d buah bilangan, yaitu

$$r, r \; + \; m', r \; + \; 2\, m', \ldots r \; + \; (d-1)\, m'$$

atau $r + k \quad '$ untuk $k = 0, 1, 2, \ldots, (d-1)$ memenuhi perkongruenan $a \quad \equiv b(m \quad m)$.

Hal ini ditunjukkan sebagai berikut.

Pertama, setiap $r + k \quad '$ dengan $k = 0, 1, 2, \ldots, (d-1)$ memenuhi perkongruenan

$$a \quad \equiv b(m \quad m)$$

$$a \quad = a(r + k \quad) = d \quad '(r + k \quad ') = d \quad 'r + \; d \quad 'k \quad '$$

Karena $a' r \equiv b' (m \quad m')$ dan $m'd = m$, maka

$$a \quad \equiv a' r \quad + a' k \quad ' (m \quad m)$$

$$\equiv \; b' d \; + \; a' k \quad ' d\, (m \quad m)$$

$$\equiv b' d\, (m \quad m) \text{ (mengapa?)}$$

$$a \quad \equiv \; b\, (m \quad m)\, k \qquad b \; = \; b' d$$

Jadi $r \; + \; k \quad '$ untuk $k \; = \; 0, 1, 2, \ldots (d \; - \; 1)$ memenuhi perkongruenan $a \quad \equiv \; b\, (m \quad m)$.

Kedua, setiap $r + k\ \ '$ dengan $k = 0, 1, 2, .. (d - 1)$ adalah residu terkecil modulo m. Ditunjukkan sebagai berikut :

r adalah solusi dari $a'x \equiv b' (m \quad m')$ berarti $r \geq 0$ sehingga $0 \leq r + k\ \ '$

$r + k\ \ ' \leq r + (d - 1)\, m'$ untuk setiap $k = 0, 1, 2, \ldots (d - 1)$.

$r + (d - 1)\, m' < m' + (d - 1)\, m' = d\ \ ' = m'$.

Jadi, $0 \leq r + k\ \ ' < m$

Hal ini menunjukkan bahwa $r + k\ \ '$ untuk $k = 0, 1, 2, \ldots (d - 1)$ adalah residu-residu terkecil modulo m.

Ketiga, tak ada dua bilangan dari $r + k\ \ '$ untuk $k = 0, 1, 2, \ldots (d - 1)$ yang kongruen modulo m, sebab $r + k\ \ '$ untuk $k = 0, 1, 2, \ldots (d - 1)$ adalah residu-residu terkecil modulo m yang berbeda.

Sampai disini telah ditunjukkan bahwa perkongruenan linier $a \quad \equiv b(m \quad m)$ memiliki d buah solusi.

Nah, sekarang tinggal menunjukkan bahwa tak ada solusi lain, kecuali d buah solusi itu. Tadi diambil bahwa r adalah solusi dari perkongruenan linier $a \quad \equiv b(m \quad m)$. Misalkan s adalah solusi lain, maka $a \quad \equiv b(m \quad m)$ dan $a \quad \equiv b(m \quad m)$.

Jadi, $a \quad \equiv a \quad \equiv b(m \quad m)$.

Karena $(a, m) = d$ dan $a \quad \equiv a \quad (m \quad m)$ di peroleh bahwa

$$s \equiv r \left(m \quad \frac{m}{d}\right)$$

$s \equiv r\ (m \quad m')$ karena $m = d\ \ '$

Ini berarti s – r = tm’ atau s = r + tm’ untuk suatu bilangan bulat t.

Karena s adalah residu terkecil modulo m, sedangkan semua residu terkecil modulo m berbentuk r + km’ dengan $k = 0, 1, 2, \ldots (d - 1)$.

Maka $s = r + k\ \ '$ adalah salah satu di antara $r + k\ \ '$.

Jadi tak ada solusi lain, kecuali d buah solusi, yaitu $r + k\ \ '$ dengan $k = 0, 1, 2, .. (d - 1)$. Lengkaplah bukti teorema itu.

Contoh 9.5:

Selesaikan $6x \equiv 15\ (m \quad 33)$

Jawab :

Karena (6, 33) = 3, maka perkongruenan ini memiliki 3 solusi.

$6x \equiv 15$ (mod 33)

$2x \equiv 5\ (m \quad 11)$

$2x \equiv 16\ (m \quad 11)$ mengapa ?

$$x \equiv 8\ (m \quad 11)$$

Maka bilangan-bilangan bulat positif yang memenuhi $x \equiv 8(m \quad 11)$ dan merupakan residu terkecil modulo 33 adalah 8, 19 dan 30. Jadi solusi-solusi dari $6x \equiv 15\ (m \quad 33)$ adalah 8, 19 dan 30.

Kita telah mengenal fungsi linier $a \quad + b \quad = c$ dengan x dan y menyatakan bilangan-bilangan rill. Dengan kata lain, fungsi linier itu diselesaikan dalam domain (himpunan semesta) himpunan bilangan rill. Apabila domainnya di persempit, yaitu himpunan bilangan bulat, maka persamaan $a \quad + b \quad = c$ dengan $a, b,$ dan c bilangan-blangan bulat disebut *Persamaan Linier Diophantus.*

Persamaan $a \quad + b \quad = c$ berarti $a \quad \equiv c\ (m \quad a)$.

Dapat pula bahwa $a \quad + b \quad = c$ berarti $b \quad \equiv c(m \quad a)$.

Oleh karena itu, untuk menyelesaikan persamaan $a \quad + b \quad = c$ dengan a, b, c, x dan y bilangan-bilangan bulat, kita dapat menyelesaikan salah satu perkongruenan.

$$\text{ax} \equiv c\ (m \quad b)\ a \quad b \quad \equiv c\ (m \quad a).$$

Selanjutnya solusi dari salah satu perkongruenan itu disubstitusikan pada persamaan semula untuk memperoleh penyelesaian dari persamaan linier tersebut.

Contoh 9.6:

Misalkan kita harus menyelesaikan $9x + 16y = 35$.

$$9x + 16y = 35\ b \qquad 16y \equiv 35\ (m \quad 9)$$

$$7y \equiv 35\ (m \quad 9)$$

$$y \equiv 5\ (m \quad 9)$$

Berarti $y = 5 + 9t$ untuk suatu bilangan bulat t.

Nilai y ini disubtitusikan pada $9x + 16y = 35$ memberikan

$$9x + 16\,(5 + 9t) = 35 \Leftrightarrow 9x + 144t = -45$$

$$\Leftrightarrow x + 16t = -5$$

$$\Leftrightarrow x = -5 - 16t$$

Sehingga himpunan penyelesaian dari $9x + 16y = 35$ adalah

$\{(x, y) | x = -5 - 16t, y = 5 + 9t$ dan t bilangan bulat$\}$

Jika $t = 0$, maka $x = -5, y = 5$, sehingga $(-5, 5)$ adalah salah satu penyelesaian dari persamaan $9x + 16y = 35$.

Penyelesaian itu, secara umum dapat dikatakan bahwa apabila (x_0, y_0) adalah salah satu solusi dari persamaan linier Diophantus $a \quad + b \quad = c$, maka solusi-solusi lainnya adalah $(x_0 + b \quad, y_0 - a \quad)$ untuk setiap bilangan bulat t. Coba buktikanlah pernyataan itu!

Apakah setiap persamaan linier Diophantus $a\quad + b\quad = c$ mesti memiliki solusi? Ingat bahwa $a\quad + b\quad = c$ sama artinya dengan $a\quad \equiv c(m\quad b)$ atau $b\quad \equiv c(m\quad a)$.

Kedua pengkongruenan ini akan mempunyai solusi, jika $(a, b)|c$, dan perkongruenan itu tidak mempunyai solusi apabila $(a, b) \nmid c$.

Jadi, dapat disimpulkan bahwa:

(1) Persamaan Linier Diophantus $a\quad + b\quad = c$ dengan $a\quad \neq 0$ tidak mempunyai penyelesaian, jika $(a, b) \nmid c$.

(2)Persamaan Linier Diophantus $a\quad + b\quad = c$ dengan $a\quad 0$ mempunyai penyelesaian, jika $(a, b)|c$.

Coba buktikan kedua kesimpulan tersebut!

Contoh 9.7:

Persamaan Linier Diophantus $2x + 4y = 5$ tidak mempunyai solusi, karena $(2, 4)\nmid 5$. Mudah pula diperiksa bahwa jika $y = t$, maka

$$x = \frac{5 - 4t}{2}$$

Untuk setiap bilangan bulat t maka $(5 - 4t)$ adalah suatu bilangan ganjil (Mengapa?).

Sehingga $x = \frac{5-4}{2}$ tidak akan menyatakan bilangan bulat untuk setiap bilangan bulat t.

Contoh 9.8:

Jika x dan y menyatakan bilangan-bilangan bulat positif, selesaikanlah $7x + 15y = 51$.

Jawab:

$7x + 15y = 51$ berarti $15y \equiv 51\ (m\quad 7)$

$$5y \equiv 17\ (m\quad 7)$$
$$5y \equiv 10\ (m\quad 7)$$
$$y \equiv 2\ (m\quad 7)$$

Jadi $y = 2 + 7t$ dengan t bilangan cacah (Mengapa bilangan cacah?)

Subtitusikan nilai y pada persamaan semula, sehingga diperoleh

$$7x + 15(2 + 7t) = 51$$
$$7x + 105t = 21$$
$$x = 3 - 15t$$

Karena x bilangan bulat positif dan t bilangan cacah, maka $x = 3$, yaitu untuk $t = 0$, sehingga $y = 2$. Jadi bilangan-bilangan bulat positif x dan y yang memenuhi $7x + 15y = 51$ berturut-turut adalah 3 dan 2.

Contoh 9.9:

Selesaikan persamaan linier Diophantus $2x + 6y = 20$!

Jawab:

$2x + 6y = 20$ berarti $2x \equiv 20(m\quad 6)$

$x \equiv 10(m\quad 3)$

$x \equiv 1(m\quad 3)$

Berarti $x = 1 + 3t$ dengan t bilangan bulat.

Subtitusi $1 + 3t$ pada x dalam $2x + 6y = 20$.

$$2(1 + 3t)6y = 20$$

$$6y = 18 - 6t$$

$$y = 6 - t.$$

Himpunan penyelesaian dari $2x + 6y = 20$ adalah

$\{(x, y)|x = -1 + 3t, y = 6 - t$, bilangan bulat$\}$

Apakah $x = 10 + 3t$ dan $y = -t$, dengan t suatu bilangan bulat juga merupakan penyelesaian dari persamaan itu? Bandingkan hasil penyelesaian persamaan $x + 3y = 10$ dengan himpunan penyelesaian dari $2x + 6y = 20$,. Contoh ini secara umum dinyatakan dalam teorema berikut ini.

Teorema 9.4:

Persamaan Linier Diophantus a’ x + b’ y = c’ yang diperoleh dari ax + by = c dengan a’ = a : (a, b), dengan b’ = b : (a, b) dan c’ = c : (a, b) mempunyai suatu penyelesaian (solusi) x = r dan y = s, maka himpunan semua penyelesaian dari ax + by = c adalah {(x, y) | x = r + b’t, y = s + a’t, t bilangan bulat}.

Coba buktikan Teorema 9.4 ini sebagai latihan.

Hal lain yang berhubungan dengan perkongruenan linier, salah satu diantaranya adalah sistem perkongruenan linier. Masalah yang penyelesaiannya menggunakan sistem perkongruenan ini telah muncul dalam suatu tulisan bangsa Cina kuno sebagai berikut:

Tentukan suatu bilangan bulat yang bersisa 2 jika dibagi 3, bersisa 4 jika dibagi 5, dan bersisa 6 jika dibagi 7.

Jika bilangan bulat yang dicari dimisalkan x, maka kalimat dalam masalah itu dapat dinyatakan sebagai berikut:

$$x \equiv 2(m\quad 3),$$

$$x \equiv 4(m\quad 5),$$

$$x \equiv 6(m\quad 7).$$

Apakah bilangan bulatyang dicar itu adalah 104? Adakah bilangan lain yang masih memenuhi?

Untuk menjawab pertanyaan ini, ikutilah uraian berikut ini:

Dari perkongruenan pertama $x \equiv 2(m \quad 3)$ berarti $x = 2 + 3k_1$, untuk suatu bilangan bukat k_1.

Subtitusikan nilai x itu dalam perkongruenan keduan dan diperoleh

$2 + 3k_1 \equiv 4 \pmod 5$

$3k_1 \equiv 2 \pmod 5$

$K_1 \equiv 4 \pmod 5$ Mengapa?

Ini berarti $k_1 = 4 + 5k_2$ untuk suatu bilangan bulat k_2.

Subtitusikan nilai k_1 ini dalam persamaan $x = 2 + 3k_1$ sehingga diperoleh:

$$x = 2 + 3\,(4 + 5k2)$$

$$x = 14 + 15k2.$$

Subtitusikan nilai x ini dalam perkongruenan ketiga dan diperoleh:

$$14 + 15k2 \equiv 6\,(m \quad 7)$$

$$15k2 \equiv -8\,(m \quad 7)$$

$$k2 \equiv -1\,(m \quad 7)$$

$$k2 \equiv 6\,(m \quad 7)$$

Hal ini berarti $k_2 = 6 + 7t$ untuk suatu bilangan bulat t.

Subtitusikan nilai k_2 ini dalam persamaan $x = 14 + 15k_2$ dan diperoleh:

$x = 14 + 15(6 + 7t)$

$x = 104 + 105t$ untuk suatu bilangan bulat t

Persamaan terakhir ini dapat dinyatakan sebagai $x \equiv 104 \pmod{105}$ yang memenuhi ketiga perkongruenan diatas. Solusi perkongruenan $x \equiv 104 \pmod{105}$ adalah 104, yang merupakan solusi bersama dari tiga pengkongruenan (sistem perkongruenan) diatas. Cara menyelesaikan sistem perkongruenan linier di atas merupakan langkah-langkah pembuktian dari teorema berikut:

Teorema 9.5 (Teorema Sisa):

Sistem perkongruenan linier $x \equiv a_i \pmod{m_i}$, $i = 1, 2, 3, \ldots, k$ dengan $(m_i, m_j) = 1$ untuk setiap $i \neq j$ memiliki solusi bersama modulo m dan solusi bersama itu tunggal dengan $m = m_1 , m_2, m_3, \ldots m_k$.

Bukti:

Pembuktian dengan induksi matematik untuk bilangan asli k.

Untuk $k = 1$ berarti $x \equiv a_1 \pmod{m_1}$ jelas mempunyai solusi.

Untuk $k = 2$ berarti $x \equiv a_1 \pmod{m_1}$ dan $x \equiv a_2 \pmod{m_2}$ dengan $(m_1 , m_2) = 1$, apakah mempunyai solusi bersama.

$x \equiv a_1 \pmod{m_1}$ berarti $x = a_1 + k_1m_1$ untuk suatu bilangan bulat k_1.

Sehingga $a_1 + k_1m_1 \equiv a_2 \pmod{m_2}$

$$k_1m_1 \equiv a_2 - a_1 \pmod{m_2}$$ dengan k_1 suatu variabel.

Karena $(m_1 , m_2) = 1$ maka kekongruenan terakhir mempunyai solusi untuk k_1 modulo m_2, katakanlah t, maka $k_1 = t + k_2m_2$ untuk suatu bilangan bulat k_2 yang memenuhi perkongruenan terakhir itu.

Jadi $x = a_1 + k_1m_1 = a_1 + (t + k_2m_2)m_1$

$$x = (a_1 + t\, m_1) + k_2m_2m_1$$

ini berarti $x \equiv (a_1 + t\, m_1) \pmod{m_1\, m_2}$.

Perkongruenan ini memenuhi untuk 2 perkongruenan (untuk $k = 2$).

Selanjutnya, sebagai hipotesis diambil bahwa sistem perkongruenan linier $x \equiv a_i \pmod{m_i}$ mempunyai satu solusi bersama untuk $i = 1, 2, 3, \ldots, (r - 1)$.

Misalkan solusi bersama itu s, maka $x \equiv a_i \pmod{m_i}$, $i = 1, 2, 3, \ldots, (r - 1)$ dapat dinyatakan sebagai suatu perkongruenan, yaitu:

$x \equiv s \pmod{m_1\, m_2\, m_3 \ldots .\, m_{r-1}}$

$x \equiv a_r \pmod{m_r}$.

Sistem perkongruenan dari dua perkongruenan ini mempunyai solusi bersama mod $(m_1\, m_2\, m_3 \ldots .\, m_{r-1})$ karena $(m_r , m_1\, m_2\, m_3 \ldots .\, m_{r-1}) = 1$ sebab m_i dan m_j saling prima untuk $i \neq j$.

Nah! Terbuktilah bahwa sistem perkongruenan $x \equiv a_i \pmod{m_i}$ untuk $i = 1, 2, 3, \ldots, k$ mempunyai solusi bersama modulo $(m_1\, m_2\, m_3 \ldots .\, m_r)$.

Selanjutnya tinggal membuktikan bahwa solusi itu tunggal. Misalkan r dan s adalah solusi-solusi bersama dari sitem tersebut, maka:

$r \equiv a_i \pmod{m_i}$ dan $s \equiv a_i \pmod{m_i}$

sehingga $(r - s) \equiv 0 \pmod{m_i}$.

Ini berarti bahwa $m_i \mid (r - s)$ untuk setiap $i = 1, 2, 3, \ldots, k$.

Jadi $(r - s)$ suatu bilangan kelipatan persekutuan dari $m_1\, m_2\, m_3 \ldots .\, m_k$. karena $(m_i , m_j) = 1$ untuk setiap $i \neq j$, maka $(m_1\, m_2\, m_3 \ldots .\, m_k) \mid (r - s)$.

Tetapi ingat bahwa r maupun s adalah solusi-solusi perkongruenan, berarti r dan s adalah residu-residu terkecil modulo $(m_1\, m_2\, m_3 \ldots .\, m_k)$ sehingga

$-(m_1\, m_2\, m_3 \ldots .\, m_k) < r - s < (m_1\, m_2\, m_3 \ldots .\, m_k)$.

Mengingat r – s adalah kelipatan persekutuan dari $m_1\ m_2\ m_3\ .\ .\ .\ .\ m_k$ dan $(m_i\ ,\ m_j\ ) = 1$ untuk setiap $i \neq j$.

Dapat disimpulkan bahwa: r – s = 0 atau r = s.

Jadi solusi bersama dari sitem $x \equiv a_i \pmod{m_i}$ untuk i = 1, 2, 3, . . . , k adalah tunggal.

Catatan:

$(m_i\ ,\ m_j\ ) = 1$ untuk setiap $i \neq j$ dengan i ; j = 1, 2, 4, . . ., k, ddikatakan $m_1\ m_2\ m_3\ .\ .\ .\ .\ m_k$ saling prima dua-dua.

Contoh 5.27:

Tentukan solusi sistem perkongruenan

$$(i)\quad \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 4 \end{cases}$$

Sebelum menyelesaikan contoh tersebut, ditulis suatu teorema yang memudahkan kita dalam menyelesaikan sistem perkongruenan, yaitu:

misalkan sistem (i) $x \equiv a_i \pmod{m_i}$ untuk i = 1, 2, 3, . . . , k dengan $(m_i\ ,\ m_j\ ) = 1$, j = 1, 2, 3, . . ., k ; i = 1, 2, 3, . . ., k dan $M_i = (m_1\ m_2\ m_3\ .\ .\ .\ .\ m_k) : m_i$, untuk i = 1, 2, 3, . . ., k dan s_i adalah solusi $M_i\ x \equiv 1 \pmod{m_i}$, i = 1, 2, 3, . . ., k.

Maka $s = a_1\ s_1\ M_1 + a_2\ s_2\ M_2 + . . . + a_k\ s_k\ M_k$ memenuhi sistem (i).

Sehingga solusi bersama dari sistem (i) adalah solusi dari

$x \equiv s \pmod{m_1\ m_2\ m_3\ .\ .\ .\ .\ m_k}$.

Pada contoh soal diatas	$a_1 = 2$	$m_1 = 3$
	$a_2 = 3$	$m_2 = 5$
	$a_3 = 1$	$m_3 = 4$

$M_1 = 5.4 = 20$,	sehingga	$20x \equiv 1 \pmod 3$	ata	$x \equiv 2 \pmod 3$

			u	
$M_2 = 3.4 =$ 12,	sehi ngg a	$12x \equiv 1$ (mod 5)	A t a u	$x \equiv 3$ (mod 5)
$M_3 = 3.5 =$ 15,	sehi ngg a	$15x \equiv 1$ (mod 4)	a t a u	$x \equiv 3$ (mod 4)

Maka $s = a_1 s_1 M_1 + a_2 s_2 M_2 + a_3 s_3 M_3$

$= 2.2.20 + 3.3.12 + 1.3.15$

$= 197$

Maka sistem perkongruenan diatas dapat dinyatakan sebagai

$$x \equiv 197 \pmod{3.5.4}$$

$$x \equiv 197 \pmod{60}$$

$$x \equiv 17 \pmod{60}$$

H.4. Latihan Kegiatan Belajar 8

Selesaikan soal-soal berikut ini dengan benar!

1. Tentukan semua solusi dari setiap kekongruenan linear berikut!
   a. $2x \equiv 5(m \quad 7)$
   b. $3x \equiv 6(m \quad 9)$
2. Tentukan semua solusi dari setiap kekongruenan linear berikut!
   a. $17x \equiv 14(m \quad 21)$
   b. $15x \equiv 9(m \quad 25)$

J. KEGIATAN BELAJAR 9

J.1. Pendahuluan Kegiatan Belajar 9

Bahan kajian	:	teorema Fermat.
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep dari teorema Fermat.
Indikator pembelajaran	:	mahasiswa mampu merumuskan dan mengamplikasikan konsep dari teoerma Fermat untuk menyelesaikan masalah.
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, elerelasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, faktorisasi bilangan tunggal, dan kekongruenan.

J.2. Bahan Pembelajaran Kegiatan Belajar 9

A. Teorema Fermat

Perhatikan barisan bilangan $4, 8, 12, 16, 20, 24$

Bilangan-bilangan dalam barisan ini kongruen modulo 7 berturut-turut dengan $4, 1, 5, 2, 6, 3$.

Tampak pada barisan bilangan terakhir ini, suku-sukunya adalah bilangan-bilangan asli kurang dari 7, yaitu aitu unsur-unsur dari himpunan residu terkecil modulo 7.

Coba, tentukan residu-residu terkecil modulo 8 dari bilangan–bilangan dalam barisan:

$$3, 6, 9, 12, 15, 18, 21.$$

Residu-residu terkecil modulo 8 dari bilangan-bilangan dalam barisan itu berturut-turut adalah

$$3, 6, 1, 4, 7, 2, 5.$$

Tampak pula bahwa residu-residu terkecil dari bilangan-bilangan dalam barisan tadi adalah semua bilangan asli kurang dari 8.

Residu-residu terkecil mod 9 dari bilangan-bilangan dalam barisan:

$$3, 6, 9, 12, 15, 18, 21, 24$$

Berturut-turut adalah

$$3, 6, 0, 3, 6, 0, 3, 6.$$

Tampak di sini bahwa residu-residu terkecilnya ternyata tidak memuat semua bilangan asli yang kurang dari 9.

Contoh-contoh tersebut merupakan suatu ilustrasi dari teorema berikut ini:

Teorema 10.1:

Jika $(u, m) = 1$, maka residu-residu terkecil modulo m dari barisan: $u, 2u, 3u, \dots, (m-1)u$ adalah suatu permutasi dari $1, 2, 3, \dots, (m-1)$.

Dengan perkataan lain, teorema 6.1 dapat dikatakan bahwa jika $(u, m) = 1$, maka setiap bilangan bulat kongruen modulo m dengan tepat satu dari $0, u, 2u, 3u, \dots, (m-1)u$.

Ingat bahwa setiap bilangan bulat akan kongruen modulo m dengan tepat satu dari $0, 1, 2, 3, 4, \dots, (m-1)$.

Bukti teorema 6.1:

Perhatikan barisan bilangan: $u, 2u, 3u, \dots, (m-1)a \dots\dots (1)$

Bilangan-bilangan pada barisan ini tidak ada satupun yang kongruen modulo m dengan 0 (nol). Mengapa? Selanjutnya, kita harus membuktikan bahwa bilangan-bilangan (suku-suku) dalam barisan (1) masing-masing kongruen modulo m dengan tepat satu dari $1{,}2{,}3, \dots, (m-1)$.

Andaikan ada dua suku dari barisan (1) yang kongruen modulo m, misalnya:

$r \;=\; s$ (mod m) dengan $1 \le r < s < m$.

Karena $(u, m) = 1$, maka kita dapat melenyapkan u dari kekongruenan itu, sehingga diperoleh

$$r = s\,(m \quad m)$$

Tetapi, karena ra dan sa adalah suku-suku dari barisan (1), maka r dan s adalah residu-residu terkecil modulo m, sehingga $r = s$. Hal ini kontradiksi dengan pengandaian bahwa $1 \le r < s < m$, maka pengandaian tersebut tidak benar.

Jadi tidak ada dua suku dari barisan (1) yang kongruen modulo m. Ini berarti bahwa suku-suku dalam barisan (1) masing-asing kongruen modulo m dengan tepat satu dari $1{,}2{,}3, \dots, (m-1)$.

Perhatikan barisan bilangan: $4, 8, 12, 16, 20, 24$.

Residu-residu terkecil mod 7 dari masing-mmasing suku dari barisan ini adalah:

$$4 \equiv 4\ (m \quad 7)$$
$$8 \equiv 1 (m \quad 7)$$
$$12 \equiv 5 (m \quad 7)$$
$$16 \equiv 2 (m \quad 7)$$
$$20 \equiv 6 (m \quad 7)$$
$$24 \equiv 3 (m \quad 7)$$

Tampak pada enam kekongruenan tersebut bahwa residu-residu terkecil modulo 7 dari suku-suku pada barisan: $4, 8, 12, 16, 20, 24$ adalah suatu perutasi dari $1, 2, 3, 4, 5, 6$.

Jika semua bilangan pada ruas kiri dari 6 kekongruenan ini dikalikan, maka hasilnya akan kongruen mod 7 dengan hasil kali semua bilangan pada ruas kanannya, yaitu:

$$4.8.12.16.20.24 \equiv 3.1.5.2.6.3 \ (m \quad 7)$$

$$4^6(1.2.3.4.5.6) \equiv 1.2.3.4.5.6(\text{mod } 7) \Leftrightarrow 4^6.\,6! \equiv 6!\,(\text{mod } 7)$$

$$\Leftrightarrow 4^6 \equiv 1(\text{mod } 7)$$

Dengan cara seperti itu, cobalah tunjukkan bahwa:

a) $5^6 \equiv 1(\text{mod } 7)$

b) $3^{1} \equiv 1(\text{mod } 11)$

c) $4^{1} \equiv 1(\text{mod } 13)$

d) $8^4 \equiv 1(\text{mod } 5)$

e) $13^{1} \equiv 1(\text{mod } 17)$

Contoh-contoh tersebut merupakan penerapan dari teorema fermat berikut ini:

Teorema 10.2: (Teorema Fermat)

Jika p suatu bilangan prima dan $(a, p) = 1$, maka $a^{p-1} \equiv 1(\text{mod p})$

Bukti:

Ambil sembarang bilangan prima p dan bilangan bulat a sedemikian $(a, p) = 1$, maka menurut Teorema 6.1, residu-residu terkecil mod p dari a, $a, 2a, 3a, \dots, (p-1)a$ adalah suatu permutasi dari $1, 2, 3, \dots, (p-1)$, sehingga hasil kali-hasil kalinya akan kongruen mod p juga, yaitu:

$$a, 2a, 3a, \dots, (p-1)a \equiv 1 \cdot 2 \cdot 3 \dots, (p-1)(m \quad p)$$

$$a^{p-1}\,(1 \cdot 2 \cdot 3 \dots, (p-1)) \equiv (p-1)!\,(m \quad p)$$

$$a^{p-1}\,(p-1)! \equiv (p-1)!\,(m \quad p)$$

Karena p dan $(p-1)!$ Saling rima (mengapa?), maka kita dapat melenyapkan (p-1)! Dari kekongruenan terakhir ini, sehingga diperoleh $a^{p-1} \equiv 1(m \quad p)$.

Contoh 10.1:

Tunjukkan bahwa jika $(3,7) = 1$, maka $3^{7-1} \equiv 1(m \quad 7)$!

Jawab:

Menurut teorema Fermat, Diketahui $p = 7$ and $a = 3$. Sehingga, $1 \cdot 3 \equiv 3(m \quad 7)$, $2 \cdot 3 \equiv 3(m \quad 7)$, $3 \cdot 3 \equiv 3(m \quad 7)$, $4 \cdot 3 \equiv 3(m \quad 7)$, $5 \cdot 3 \equiv 3(m \quad 7)$, dan $6 \cdot 3 \equiv 4(m \quad 7)$. Akibatnya

$$(1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot 3) \cdot (6 \cdot 3) \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4(m \quad 7)$$

$$3^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4(m \quad 7)$$

$$3^6 \cdot 6! \equiv 6!\,(m \quad 7) \Leftrightarrow 3^6 \equiv 1(m \quad 7)$$

$$\Leftrightarrow 3^{7-1} \equiv 1(m \quad 7) \text{ (terbukti)}$$

Teorema Fermat tersebut dapat dinyatakan lebih umum dengan meniadakan ketentuan $(a, p) = 1$ sebagai berikut:

Teorema 10.3:

Jika p suatu bilangan prima, maka $a^p \equiv a(m \quad p)$, untuk setiap bilangan bulat a.

Bukti:

Ambil sembarang bilangan prima p dan sembarang bilat a, maka $(a, p) = 1$ atau $(a, p) = p$. Apakah ada kemungkinan lain antara FPB dari a dan p? Jika $(a, p) = 1$, maka menurut teorema 10.2 diperoleh bahwa $a^{p-1} \equiv 1(m \quad p)$. Selanjutnya, jika kedua ruas dikalikan a, maka diperoleh $a^p \equiv a(m \quad p)$.

Jika $(a, p) = p$, maka $p|a$, sehingga $a \equiv 0(m \quad p)$ dan $a^p \equiv a(m \quad p)$ pula.

Jadi, $a^p \equiv a(m \quad p)$

Bukti lain dari teorema 6.3 dengan menggunakan induksi matematiak pada a.

Jika $a = 1$, maka pernyataan $1^p \equiv 1(m \quad p)$ jelas benar. Demikian pula, jika diambil $a = 0$.

Selanjutnya diasumsikan $a^p \equiv a(m \quad p)$ benar untuk suatu bilangan bulat positif a, dan harus ditunjukkan benar untuk $(a + 1)$, yaitu $(a + 1)^p = a + 1(m \quad p)$.

Hal ini ditunjukkan sebagai berikut:

Menurut teorema binomial, maka :

$$(a + 1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{k} a^{p-k} + \cdots + \binom{p}{p-1} a + 1$$

Ingat bahwa $\binom{p}{k} = \frac{p!}{k!(p-k)} = \frac{p(p-1)(p-1)\ldots(p-1)}{1\cdot 2\cdot 3\ldots k}$, karena p suatu bilangan prima, maka $p|\binom{p}{k}$ berarti $\binom{p}{k} \equiv 0(m \quad p)$ untuk $1 \leq k \leq p - 1$.

Jadi kita memperoleh bahwa:

$$(a + 1)^p = a^p + 0 + 0 + \cdots + 0 + 1(m \quad p)$$

$$(a + 1)^p = a^p + 1(m \quad p)$$

Karena $a^p \equiv a(m \quad p)$, maka $(a + 1)^p = a + 1(m \quad p)$

Dengan induksi matematik pada a kita telah membuktikan bahwa $a^p \equiv a(m \quad p)$ untuk setia bilangan asli a. Selanjutnya jika a suatu bilangan bulat negatif, bukan lagi menjadi persoalan, sebab untuk setiap bilangan bulat negatif a berlaku bahwa $a \equiv r(m \quad p)$ dengan $0 \leq r < p - 1$. Jadi, $a^p \equiv r^p \equiv r \equiv a(m \quad p)$.

Teorema Fermat mempunyai banyak kegunaan, khususnya dalam mengembangkan Teori Bilangan.

Contoh 10.2:

Berapakah sisa pembagaian 5^3 oleh 11?

Jawab:

Menurut teorema Fermat $5^1 \equiv 1(m \quad 11)$, maka $5^3 \equiv 5^{1 \cdot 3+8} \equiv (5^1)^3(5^2)^4 \equiv 81 \equiv 4(m \quad 11)$.

Jadi, 5^3 : 11 bersisa 4.

Bacalah lagi dengan seksama teorema 6.3 tersebut. Kontraposisi dari teorema itu benar pula, yaitu:

Jika untuk suatu bilangan bulat a, $a^p \not\equiv a(m \quad p)m \quad p\, b \quad b \quad p$.

Hal ini menunjukkan bahwa teorema fermat dapat digunakan untuk menguji apakah suatu bilangan bulat n merupakan bilangan komposit atau bukan.

Contoh 10.3:

Apakah 117 suatu bilangan prima?

Jawab:

Untuk memeriksa ini dipilih bilangan bulat positif yang cukup kecil, misalnya 2. Selanjutnya diperiksa apakah $2^1 \equiv 2(m \quad 117)$?

$$2^1 = 2^{7.1 \; +5} = (2^7)^1 \, .2$$

$$2^7 = 128 \equiv 11(m \quad 117), m$$

$$\begin{aligned} 2^1 &\equiv (11)^1 \, .2^5(m \quad 117) \\ &\equiv (121)^8 . 2^5(m \quad 117) \\ &\equiv 4^8 . 2^5(m \quad 117) \\ &\equiv 2^2 \; (m \quad 117) \\ &\equiv (2^7)^3(m \quad 117) \\ &\equiv 11^3(m \quad 117) \\ &\equiv 121.11(m \quad 117) \\ &\equiv 4.11(m \quad 117) \\ &\equiv 44(m \quad 117) \end{aligned}$$

Sehingga diperoleh bahwa $2^1 \equiv 44 \neq 2 \; (m \quad 117)$

Hal ini berarti bahwa 117 adalah bilangan komposit dan kenyataan bahwa 117 = 13. 9

Contoh 10.4:

Tanpa menggunakan teorema fermat, tunjukkan bahwa $3^{1} \equiv 1(m \quad 17)$.

Jawab: $3^{3} \equiv 27 \equiv 10(m \quad 17)$ dikuadratkan

$$3^{6} \equiv 100 \equiv (m \quad 17)$$

$$3^{6} \equiv 100 \equiv (m \quad 17)$$

$$3^{6} \equiv -2 \equiv (m \quad 17) \text{ dikuadratkan}$$

$$3^{1} \equiv 4(m \quad 17)$$

Sehingga $3^{1} \equiv 3^{1} . 3^{3} . 3 \equiv 4.10.3(m \quad 17)$

$$120 \equiv 1(m \quad 17)$$

Jadi, $3^{1} \equiv 1(m \quad 17)$

Perhatikan kembali teorema fermat di atas. Perlu ditekankan di sini bahwa konvers dari teorema tersebut tidak benar, yaitu:

Jika $a^{n-1} \equiv 1(m \quad n)$ untuk suatu bilangan bulat a, maka n tidak perlu suatu bilangan prima.

Untuk menunjukkan contohnya, terlebih dahulu kita bicarakan teorema berikut ini yang merupakan akibat dari teorema fermat.

Teorema 10.4

Jika p dan q adalah bilangan-bilangan prima yang berlainan sedemikian hingga $a^{p} \equiv a\,(m \quad q)$dan $a^{q} \equiv a\,(m \quad p)$, maka $a^{p} \equiv a\,(m \quad p\ )$.

Bukti:

Menurut teorema 6.3, karena p suatu bilangan prima maka ini berarti bahwa p $(a^{q})^{p} \equiv a^{q}(\text{mod } p)$. selanjutnya, karena diketahui bahwa $a^{q} \equiv a\,(m \quad p)$. Ini berarti bahwa $p|(a^{p} \quad - a)$.................. (1).

Menurut Teorema 6.3 lagi, karena q suatu bilangan prima maka $(a^{p})^{q} \equiv a^{p}(m \quad q)$. Selanjutnya, karena diketahui bahwa $a^{p} \equiv a\,(m \quad q)$. Ini berarti bahwa $q|(a^{p} \quad - a)$......................... (2)

Dari (1) dan (2) disimpulkan bahwa $p \quad |(a^{p} \quad - 1)$ dan dapat dinyatakan sebagai $a^{p} \equiv a(m \quad p\ )$

Contoh 10.5:

Tunjukkan bahwa $2^{3} \equiv 1(m \quad 341)$

Jawab:

$341 = 11 \cdot 31 \Leftrightarrow 2^{1} = 1.024 = 31 \cdot 33 + 1$, sehingga

$2^{1} = 1(m \quad 31)$

$2^{1} \equiv 2(m \quad 31)$

$2^{1} = 1.024 = 31 \cdot 33 + 1$, sehingga

$2^{1} \equiv 1(m \quad 11)$, jika kedua ruas dibagi dua, maka diperoleh $2^{3} \equiv 2(m \quad 11)$, maka $2^{11 \cdot 3} \equiv 2(m \quad 11 \cdot 31)$, yaitu :

$2^{3} \equiv 2(m \quad 341)$

Jika kedua ruas dibagi dua, maka diperoleh $2^{3} \equiv 2(m \quad 341)$ dan tidak dapat disimpulkan bahwa 341 sutu bilangan prima.

Contoh 10.6:

Tentukan solusi dari $7x \equiv 12(m \quad 17)$ dengan menggunakan teorema Fermat!

Jawab:

Dengan menggunakan teorema fermat, $a = 7; p = 17$

Karena terdapat modulo 17 maka kita dapat memanfaatkan bentuk a^{p-1} sehingga kita dapat mengalikan kedua sisi dengan 17^{1} untuk memperoleh :

$$17^{1} \cdot 7x \equiv 17^{1} \cdot 12(m \quad 7) \Leftrightarrow 17^{1}\ x \equiv 17^{1} \cdot 12(m \quad 7)$$

Karena $17^{1} \equiv 1(m \quad 17)$ memberikan $17^{1}\ x \equiv 17^{1} \cdot 12(m \quad 7) \Leftrightarrow x \equiv 17^{1} \cdot 12(m \quad 17)$

$$\begin{aligned} x &\equiv 17^{1} \cdot 12(m \quad 17) \\ &\equiv (17^{3})^{5} \cdot 12(m \quad 17) \\ &\equiv (343)^{5} \cdot 12(m \quad 17) \\ &\equiv (3)^{5} \cdot 12(m \quad 17) \\ &\equiv 243 \cdot 12(m \quad 17) \\ &\equiv 5 \cdot 12(m \quad 17) \\ &\equiv 60(m \quad 17) \\ &\equiv 9(m \quad 17) \end{aligned}$$

Sehingga diperoleh $x \equiv 9(m \quad 17)$

$x \equiv 9(m \quad 7) \Leftrightarrow x = 17n + 9\ \{n \in \mathbb{N}\}$

Nilai-nilai x yang memenuhi :

$n = \cdots$

$n = -3 : x = 17n + 9 = 17(-3) + 9 = -51 + 9 = -42$

$n = -2 : x = 17n + 9 = 17(-2) + 9 = -34 + 9 = -25$

$n = -1 : x = 17n + 9 = 17(-1) + 9 = -17 + 9 = -8$

$n = 0 : x = 17n + 9 = 17(0) + 9 = 9$

$n = 1 : x = 17n + 9 = 17(1) + 9 = 1 + 9 = 26$

$n = 2 : x = 17n + 9 = 17(2) + 9 = 34 + 9 = -43$

$n = 3 : x = 17n + 9 = 17(3) + 9 = 51 + 9 = 60$

$n = \cdots$

Jadi, solusi dari $7x \equiv 12(m\quad 17)$ adalah 9, yaitu residu terkecil modulo 7.

Dalam sejarahnya, bilangan berbentuk $2^n - 2$ ditemukan oleh matematikawan Cina pada 25 abad yang lalu dana menyatakan bahwa

n suatu bilangan prima jika dan hanya jika $n|2^n - 2$

Dalam kenyataan, kriteria ini benar untuk semua bilangan prima $n < 340$. Dan pada contoh di atas, kita memperoleh fakta bahwa $341|2^3\quad - 2$, walaupun 341 bukan bulangan prima. Selanjutnya bilangan komposit n sedemikian hingga $n|2^n - 2$ disebut bilangan prima semu *(pseudoprima)*. Ada tak terhingga banyaknya bilangan prima semu. Emat bilangan prima semu pertama $341, 561, 645,$ dan 1.105.

J.4. Latihan Kegiatan Belajar 9

Selesaikan soal-soal berikut ini dengan benar!

1. Hitunglah $6^4\quad (m\quad 11)$!
2. Hitunglah $5^2\quad (m\quad 41)$!
3. Tentukan sisa 2019^2 dibagi 7 !
4. Tunjukkan bahwa 31 membagi $8^3\quad - 1$!
5. Tentukan sisa dari 7^2 sehingga 5 membagi 7^2 !
6. Tentukan sisa dari 18! Sehingga 437 membagi 18! !
7. Tentukan bilangan prima terbesar yang dapat dinyatakan dalam bentuk $a^4 + b^4 + 3$ untuk suatu bilangan prima a dan b !
8. Tentukan sisa pembagian dari $(6^2\quad + 7^2\quad + 8^2\quad + 9^2\quad)$ oleh 2017 !
9. Tunjukkan bahwa jika p dan q adalah dua bilangan prima berbeda, maka $p^{q-1} + q^{p-1} \equiv 1(m\quad p\ )$!
10. Tunjukkan bahwa jika p adalah bilangan prima dan a adalah bilangan bulat, maka $p|(a^p + (p-1)!\,a)$!

K. KEGIATAN BELAJAR 10

K.1. Pendahuluan Kegiatan Belajar 10

Bahan kajian	:	teroema Wilson
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep dari teorema limit.
Indikator pembelajaran	:	mahasiswa mampu merumuskan dan mengamplikasikan konsep perkongreunan linier untuk menyelesaikan masalah
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, elerelasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, faktorisasi bilangan tunggal, kekongruenan, dan teroema Fermat.

K.2. Bahan Pembelajaran 10

A. Teorema Wilson

Teorema Fermat dikemukakan oleh Pierre de Fermat (bangsa Prancis) pada tahun 1640 yang merupakan teorema fundamental dalam mengembangkan Teori Bilangan pada saat itu. Teorema yang terkenal pula adalah Teorema Wilson, yang pertama kali dipublikasikan Edward Waring (1770) tanpa mencantumkan buktinya. Sebenarnya Wilson bukanlah orang pertama kali mengemukakan teoremanya, sebab pada tahun 1682 Leibniz juga telah membicarakannya. Bukti teorema Wilson pertama kali diberikan oleh Lagrange pada tahun 1771 dan menamakan teoremanya dengan sebutan “Teorema Wilson”.

Sebelum membicarakan Teorema Wilson akan kita pelajari lebih dahulu teorema-teorema berikut ini yang akan membantu untuk membuktikan Teorema Wilson.

Teorema 11.1:

Jika p suatu bilangan prima, maka kekongruenan $x^2 \equiv 1 (m \quad p)$ mempunyai tepat dua solusi, yaitu 1 dan $p - 1$.

Bukti:

Misalkan r adalah suatu solusi dari perkongruenan $x^2 \equiv 1 \ (m \quad p)$, maka

$$r^2 - 1 \equiv 0 \ (m \quad p) \Leftrightarrow (r + 1)(r - 1) \equiv 0 \ (m \quad p)$$

Perkongruenan terakhir ini berarti $p \mid (r + 1)(r - 1)$, karena p suatu bilangan prima, maka:

$$p|(r+1) \qquad \text{atau} \qquad p|(r-1)$$

$$r + 1 \equiv 0 \ (m \quad p) \qquad \text{atau} \qquad r - 1 \equiv 0(m \quad p)$$

$$r \equiv -1(m \quad p) \qquad \text{atau} \qquad r \equiv 1(m \quad p)$$

$$r \equiv (p-1)(m \quad p) \qquad \text{atau} \qquad r \equiv 1(m \quad p)$$

Karena r suatu solusi dari perkongruenan $x^2 \equiv 1(m \quad p)$, maka r adalah residu terkecil $m \quad p$. Jadi 1 dan $p-$ 1 adalah solusi dari $x^2 \equiv 1(m \quad p)$.

Bukti lain yang lebih mudah, apabila $(p-1)$ dan 1 masing-masing disubtitusi pada x dalam perkongruenan $x^2 \equiv 1(m \quad p)$. Coba lakukanlah!

Selesaikan perkongruenan-perkongruenan berikut ini:

(1) $x^2 \equiv 1(m \quad 7)$

(2) $x^2 \equiv 24(m \quad 23)$

Perhatikan himpunan residu-residu terkecil modulo 7 selain nol, yaitu $T = \{1, 2, 3, 4, 5, 6\}$. Mudah anda peroleh solusi-solusi berikut ini:

Solusi dari $x \equiv 1 \ (m \quad 7)$ adalah 1

Solusi dari $2x \equiv 1 \ (m \quad 7)$ adalah 4

Solusi dari $3x \equiv 1 \ (m \quad 7)$ adalah 5

Solusi dari $4x \equiv 1 \ (m \quad 7)$ adalah 2

Solusi dari $5x \equiv 1 \ (m \quad 7)$ adalah 3

Solusi dari $6x \equiv 1 \ (m \quad 7)$ adalah 6

Tampak dari perkongruenan-perkongruenan tersebut bahwa jika $a \in T$, maka solusi dari $a \quad \equiv 1(m \quad 7)$ adalah $a' \in T$ pula. Dapat diperiksa pula bahwa apabila $a, b \in T$ dengan $a \not\equiv b(m \quad 7)$ maka $a' \not\equiv b'(m \quad 7)$ dengan $a', b' \in T$ yang merupakan solusi berturut-turut dari $a \quad \equiv 1(m \quad 7)$ dan $b \quad \equiv 1 \ (m \quad 7)$. Jika $a = 1$ dan $b = 6$ maka solusi-solusinya berturut-turut adalah $a' = 1$ dan $b' = 6$.

Hal ini merupakan penerapan dari teorema berikut:

Teorema 11.2:

Misalkan p suatu bilangan prima selain 2 dan a' adalah solusi dari $a \quad \equiv 1 \ (m \quad p)$ dengan $a = 1, 2, 3, \ldots, p-$ 1 yaitu ($a \quad ' \equiv 1(m \quad p)$, dengan $0 < a' < p$), maka:

(i) jika $a \not\equiv b(m \quad p)$ maka $a' \not\equiv b'(m \quad p)$

(ii) jika $a = 1$ atau $a = p-$ 1 maka $a' \equiv \ a \ (m \quad p)$

Bukti:

Jika $a = 1, 2, 3, \ldots$, atau $p-1$, maka $(a, p) = 1$, sehingga $a \quad \equiv 1(m \quad p)$ mempunyai tepat satu solusi. Ini berarti a' ada, sedemikian hingga $a \quad ' \equiv 1(m \quad p)$.

Bagian (i) dibuktikan kontraposisinya, yaitu:

Jika $a' \equiv b'(m \quad p)$, maka $a \equiv b(m \quad p)$.

Misalkan $a' \equiv b'(m \quad p)$, maka

aa' $\equiv a \quad ' \equiv 1(m \quad p)$. Ingat bahwa a' dan b' adalah solusi dari $a \quad \equiv 1(m \quad p)$.

$a \quad 'b \equiv a \quad 'b \equiv b\ (m \quad p)$ dengan $b = 1, 2, \ldots, p - 1$.

$a\, b\ (m \quad m)$, sebab $b'b \equiv 1(m \quad p)$.

Jadi (i) terbukti.

Bagian (ii) dibuktikan sebagai berikut:

Jika $a = 1$, yaitu $x \equiv 1(m \quad p)$, maka solusinya adalah $a' = 1$, sehingga $a' \equiv a(m \quad p)$.

Jika $a = p - 1$. Yaitu $(p - 1)x \equiv 1(m \quad p)$

$$-x \equiv 1(m \quad p)$$

$$x \equiv -1\ (m \quad p)$$

$$x \equiv p - 1\ (m \quad p)$$

Jadi $a' = p - 1$, sehingga $a' \equiv a\ (m \quad p)$.

Contoh 11.1:

Pandang perkongruenan $a \quad \equiv 1\ (m \quad 11)$ dan a' adalah solusinya, sehingga $a \quad ' \equiv 1(m \quad p)$. Maka hubungan a, a' dan $a \quad$' tampak pada tabel berikut ini.

a	1	2	3	4	5	6	7	8	9	10
a'	1	6	4	3	9	2	8	7	5	10
$a \quad '$	1	1	1	1	1	1	1	1	1	1

Hasil kali- hasilkali pasangan yang kongruen modulo 11 dapat dituliskan sebagai berikut:

$$2 \cdot 6 \equiv 1\ (m \quad 11)$$

$$3 \cdot 4 \equiv 1\ (m \quad 11)$$

$$5 \cdot 9 \equiv 1\ (m \quad 11)$$

$$7 \cdot 8 \equiv 1\ (m \quad 11)$$

Hasil kali semua bilangan pada ruas-ruas kiri akan kongruen mod 11 dengan 1 pula, yaitu:

$2 \cdot 6 \cdot 3 \cdot 4 \cdot 5 \cdot 9 \cdot 7 \cdot 8 \equiv 1(m \quad 11)$. Jika kedua ruas dikalikan 10, diperoleh:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 10(m \quad 11) \Leftrightarrow 10! \equiv 10(m \quad 11)$$

$$\Leftrightarrow 10! \equiv -1(m \quad 11)$$

Coba tunjukkan bahwa $6! \equiv 6(m \quad 7)$,

$$12! \equiv 12(m \quad 13), d$$

$$18! \equiv 18(m \quad 19).$$

Contoh tersebut merupakan suatu cara membuktikan Teorema Wilson berikut ini.

Teorema 11.3 (Teorema Wilson):

Jika p suatu bilangan prima, maka $(p-1)! \equiv -1\ (m\quad p)!$

Bukti:

Menurut Teorema 5.6, kita dapat memasangkan a dan a' dari $2, 3, 4, \ldots, (p-1)$ demikian sehingga $a\ ' \equiv 1(m\quad p)$. Dan terdapat $\frac{1}{2}(p-3)$ pasangan bilangan-bilangan tersebut yang kongruen mod p dengan 1 jika ruas-ruas kiri dari $\frac{1}{2}(p-3)$ kekongruenan mod p tersebut dikalikan, maka hasil kalinya akan kongruen mod p dengan 1 pula, yaitu:

$$2 \cdot 3 \cdot 4 \cdot 5 \ldots (p-2) \equiv 1\ (m\quad p) \Leftrightarrow 1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv\ p-1\ (m\quad p)$$

$$\Leftrightarrow (p-1)! \equiv -1(m\quad p).$$

Sebagai contoh diambil $p = 13$, maka kita dapat memasangkan a dan a' dari $2, 3, 4, \ldots, 11$, sehingga terdapat 5 pasang bilangan-bilangan itu yang hasil kalinya kongruen mod 13 dengan 1, yaitu:

$$2 \cdot 7\ \equiv 1(m\quad 13)$$

$$3 \cdot 9 \equiv 1(m\quad 13)$$

$$4 \cdot 10\ \equiv 1(m\quad 13)$$

$$5 \cdot 8 \equiv\ 1(m\quad 13)$$

$$6 \cdot 1 \equiv 1(m\quad 13)$$

Hasil kali ruas-ruas dari 5 kekongruenan ini adalah

$$(2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6.11) \equiv 1(m\quad 13) \Leftrightarrow 1.2.3.4.5. \ldots 11.12\ \equiv\ 12\ (m\quad 13)$$

$$\Leftrightarrow 12! \equiv -1(m\quad 13)$$

Konvers dan Teorema Wilson juga benar, yaitu:

Jika $(p-1) \equiv -1(m\quad p)$, *maka p suatu bilangan prima.*

Hal ini dibuktikan sebagai berikut:

Andaikan p bukan bilangan prima, maka $p = a \cdot b$ dengan a, b bilangan-bilangan bulat positif dan $a \neq 1$ atau $a \neq p$, sehingga $a|p$ dan $a \leq p-1$.

Karena $(p-1)! \equiv -1(m\quad p)$ maka $p|(p-1)! + 1$. Dan karena $a|p$, maka $a|(p-1)! + 1$. Karena $a \leq p-1$, maka a merupakan salah satu faktor dari $(p-1)!$, sehingga $a|(p-1)!$.

Mengingat $a|(p-1)! + 1$ dan $a|(p-1)!$, maka $a|1$. Diperoleh suatu kontradiksi, karena $a \neq 1$, sehingga pengandaian tersebut tidak benar.

Jadi p adalah suatu bilangan prima.

Jika Teorema Wilson dan konversnya dituliskan bersama-sama, kita memperoleh bahwa:

Syarat *perlu dan cukup agar p suatu bilangan prima adalah* $(p-1)! \equiv -1(m \quad p)$.

Atau dapat ditulis :

p suatu bilangan prima bila dan hanya bila adalah $(p-1)! \equiv -1\ (m \quad p)$.

Berikut ini sebuah contoh penggunaan Teorema Wilson untuk menyelesaikan perkongruenan kuadrat seperti dalam teorema berikut ini.

Teorma 11.4:

Jika p suatu bilangan prima ganjil, maka perkongruenan $x^2 + 1 \equiv 0(m \quad p)$ mempunyai solusi bila dan hanya bila $p \equiv 1(m \quad 4)$.

Bukti:

Misalkan a adalah suatu solusi dari $x^2 + 1 \equiv 0\ (m \quad p)$ maka $a^2 \equiv -1(m \quad p)$ dan $(a, p) = 1$. Karena $(a, p) = 1$, menurut Teorema Fermat, maka

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

$$(a^2)^{\frac{1}{2}(p-1)} \equiv 1(m \quad p)$$

$$(-1)^{\frac{1}{2}(p-1)} \equiv 1(m \quad p)$$

$$(-1)^{\frac{1}{2}} \equiv 1\ (m \quad p)$$

Bilangan prima berbentuk $4k\ +\ 3$ tampak tidak memenuhi, sebab akan didapat

$$(-1)2k + 1 \equiv 1(m \quad p)$$

$-1 \equiv 1(m \quad p)$, yaitu $p|2$ yang jelas salah.

Jadi bilangan prima p berbentuk $4k + 1$, yaitu $p \equiv 1(m \quad 4)$.

Untuk sebaliknya dibuktikan sebagai berikut:

Perhatikan bahwa $p - 1 \equiv -1(m \quad p)$

$p - 2 \equiv -2(m \quad p)$

. . .

. . .

. . .

$\frac{p+1}{2} = -\frac{p-1}{2}$ (mod p) dan

$(p-1)!\ \equiv 1 \cdot 2 \cdot\ 3 \ldots . \frac{p-1}{2}\ . \frac{p+1}{2} \ldots (p - 2)(p - 1)$, maka

(p – 1)! $\equiv 1 \cdot 2 \cdot 3\ \ldots \frac{(p-1)}{2}\ . (\frac{(-p+1)}{2}) \ldots (-2)(-1)(m \quad p)$

(p – 1)! $\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \ldots . \frac{p-1}{2}\right)^2\ (m \quad p)$

$(p-1)! \equiv \left(1.2.3 \ldots . \frac{p-1}{2}\right)^2$ $(m \quad p)$, sebab $p = 4k+1$, untuk suatu bilangan bulat positif k, sehingga $(-1)^{\frac{p-1}{2}} = 1$

$(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2$ $(m \quad p)$

Mengingat Teorema Wilson bahwa $(p-1) \equiv -1$ $(m \quad p)$, maka:

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \ (m \quad p)$$

Hal ini berarti $\left[\left(\frac{p-1}{2}\right)!\right]^2$ memenuhi perkongruenan $x^2+1 \equiv 0(m \quad p)$.

Jadi, perkongruenan itu mempunyai solusi.

Contoh 11.3:

Selesaikan perkongruenan $x^2+1 \equiv 0(m \quad 13)$!

Jawab:

Karena 13 adalah bilangan prima berbentuk $4x+1$, maka perkongruenan tersebut mempunyai solusi, yaitu:

$$\left(\frac{1 \ -1}{2}\right)! = 6! = 720 \equiv (\text{mod } 13)$$

Dapat diperiksa kebenarannya dengan subtitusi 5 pada x dari perkongruenan tersebut, yaitu

$$5^2 + 1 = 26 \equiv 0 \ (m \quad 13)$$

K.4. Latihan Kegiatan Belajar 10

Selesaikan soal-soal berikut ini dengan benar!

1. Buktikan bahwa untuk setiap bilangan asli n berlaku $4 + 10 + 16 + \cdots + (6n-2) = n(3n+1)$!
2. Terkalah rumus umum untuk jumlahan dari n bilangan genap positif pertama. Berikanlah hasil terkaan itu dengan induksi matematik!
3. Buktikanah $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$ untuk setiap bilangan asli n.
4. Terkalah rumus untuk A^n, jika $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Buktikanlah hasil terkaan itu dengan menggunakan induksi matematik!
5. Buktikan $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 + \frac{1}{3}n(4n^2-1)$ untuk setiap bilangan asli n
6. Buktikan bahwa $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1+2+3+\cdots+n)^2$ untuk setiap bilangan n.
7. Buktikan bahwa
   a) $n^2 > n+1$, untuk setiap bilangan bulat $n \geq 2$.
   b) $2^n > n^3$, untuk setiap bilangan bulat $n > 9$.
8. Buktikan bahwa $n^5 - n$ terbagi habis oleh 5 untuk setiap bilangan asli n berlaku !

K. KEGIATAN BELAJAR 11

K.1. Pendahuluan Kegiatan Belajar 11

Bahan kajian	:	fungsi Tu
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep fungsi Tu.
Indikator pembelajaran	:	mahasiswa mampu merumuskan dan mengamplikasikan konsep fungsi Tu.
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, elerelasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, faktorisasi bilangan tunggal, kekongruenan, teorema fermat, dan teorema wilson.

K.2. Pendahuluan Kegiatan Belajar 11

A. Fungsi τ (tau)

Berdasarkan sifat-sifat yang dimiliki bilangan-bilangan bulat dapat didefinisikan fungsi-fungsi khusus yang mepunyai peranan penting dalam Teori Bilangan. Fungsi-fungsi khusus tersebut sering diseut fungsi artimatik didefinisikan/mempunyai daerah asal pada himpunan bilangan bulat positif seprti berikut ini.

Jika f suatu fungsi, maka $f: B^+ \rightarrow B$ dengan B adalah himpunan semua bilangan bulat dan B^+ adalah himpuanan semua bilangan bulat positif.

Definisi 11.1:

Misalkan n suatu bilangan bulat positif, $\tau(n)$ menyatakan banyaknya pembagi bulat positif dari n.

Contoh 11.1:

1) Semua pembagi bulat positif dari 12 adalah 1,2,3,4,5,6, dan 12, maka $\tau(12) = 6$.
2) Semua pembagi bulat positif dari 15 adalah 1,3,5, dan 15, maka $\tau(15) = 4$.
3) Semua pembagi bulat positif dari 13 adalah 1 dan 13, maka $\tau(13) = 2$.
4) Periksalah bahwa $\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$, $\tau(5) = 2$, $\tau(6) = 4$, $\tau(8) = 4$,
5) Jika p suatu bilangan prima, maka $\tau(p) = 2$.

$\tau(n)$ yaitu banyaknya pembagi bulat positif dari n, sering dinyatakan dengan rumus yang menggunakan notasi Σ (sigma). Berikut ini beberapa contoh ketentuan penggunaan notasi Σ.

$$\sum_{n=1}^{5} u_n = u_1 + u_2 + u_3 + u_4 + u_5$$

$$\sum_{n=2}^{6} n = 2 + 3 + 4 + 5 + 6$$

$$\sum_{n=1}^{5} 3 = 3 + 3 + 3 + 3 + 3$$

$\sum_{d|1} \; d = 1 + 2 + 3 + 4 + 6 + 12$, yaitu banyaknya pembagi bulat positif dari 12.

$\sum_{d|1} \; 1 = 1 + 1 + 1 + 1 + 1$ yaitu banyaknya pembagi bulat positif dari 12.

Memperhatikan contoh-contoh pemakaian notasi Σ tersebut, $\tau(n) = 2$ dapat dirumuskan sebagai berikut:

$\tau(n) = \sum_{d|n} 1$ untuk bilangan bulat $n \geq 1$.

Jadi, $\tau(n)$ merupakan penjumlahan dari 1 sebanyak pembagi bulat positif dari n.

Contoh 11.2:

1) Semua pembagi bulat positif dari 32 adalah 1,2,4,8,16, dan 32, maka $\sum_{d|3} \; 1 = 1 + 1 + 1 + 1 + 1 + 1 = 6$.
2) Semua pembagi bulat positif dari 48 adalah 1,2,3,4,6,8,12,16,24, dan 48, maka $\sum_{d|4} \; 1 = 1 + 1 + 1 + 1 + 1 + 1 + 1 = 10$
3) Perksalah bahwa $\sum_{d|1} 1 = 1$, $\sum_{d|2} 1 + 1 = 2$, $\sum_{d|4} 1 = 1 + 1 + 1 = 3$, $\sum_{d|6} 1 = 1 + 1 + 1 + +4$
4) Jika p suatu bilangan prima, maka $\sum_{d|p} 1 = 1 + 1 = 2$

Dari uraian dan contoh-contoh di atas dapat dipahami bahwa jika p suatu bilangan prima, maka pembagi-pembagi bulat positifnya hanyalah 1 dan p saja, sehingga $\tau(p) = 2$.

Pembagi-pembagi bulat positif dari p^2 adalah 1, p, dan p^2 sehingga $\tau(p^2) = \sum_{d|p^2} 1 = 1 + 1 + 1 = 3$.

Periksalah bahwa $\tau(p^k) = k + 1$

Contoh 11.3:

1) $64 = 2^6$, maka $\tau(2^6) = 6 + 1 = 7$

   Periksalah dengan mencacah semua pembagi bulat positif dari 64.
2) $\tau(3^5) = 5 + 1 = 6$
3) Periksalah bahwa $\tau(32) = 6$, $\tau(16) = 5$, $\tau(125) = 4$, dan $\tau(2401) = 5$.

Sekarang, jika p_1 dan p_2 adalah bilangan-bilangan prima yang berlainan dan $n = p_1p_2$, maka pembagi-pembagi bulat positif dari n adalah 1, p_1, p_2, dan $n = p_1p_1$ sehingga $\tau(n) = 4$.
Jika $m = p_1^2p_2^3$ maka pembagi-pembagi bulat positif m dapat disusun sebagai berikut:

1	p_2	p_2^2	p_2^3
p_2	p_2p_2	$p_2p_2^2$	$p_2p_2^3$
p_1^2	$p_1^2p_2$	$p_1^2p_2^2$	$p_1^2p_2^3 = m$

Tampak pada daftar ini bahwa $\tau(m) = \tau(p_1^2p_2^3) = 3 \times 4 = 12$.
Contoh 11.4:
1) $\tau(144) = \tau(2^4, 3^2) = 5 \times 3 = 15$
2) $\tau(144) = \tau(2^4, 3^2) = 5 \times 3 = 15$
3) Periksalah bahwa $\tau(675) = 12$, $\tau(784) = 15$.

Dapatkah anda membuktikan bahwa jika $n = p^kq^t$ dengan p dan q bilangan-bilangan prima yang berlainan dan k, t adalah bilangan-bilangan bulat positif, maka:

$$\tau(n) = \tau(p^kq^t) = (k+1)(t+1)$$

Bukti:
Semua pembagi bulat positif dari $n = p^kq^t$ dapat disusun daftar sebagai berikut:
1, p, p^2, p^3, ..., p^k
q, p , p^2q, p^3q, ..., p^kq
q^2, pq^2, p^2q^2, p^3q^2, ..., p^kq^2
..., ..., ..., ..., ..., ...
..., ..., ..., ..., ..., ...
..., ..., ..., ..., ..., ...
q^t, pq^t, p^2q^t, p^3q^t, ..., $p^kq^t = n$
Tampak daftar tersebut bahwa:

$$\tau(n) = \tau(p^kq^t) = (k+1)(t+1)$$

Kita telah mengetahui teorema dasar artimatika, yaitu bahwa setiap bilangan bulat positif yang lebih besar dari 1 dapat difaktorkan secara tunggal adat faktor-faktor prima.
Misalnya: $72 = 2^2 \cdot 3^2$

$$300 = 2^2 \cdot 3 \cdot 5^2$$

Setiap bilangan bulat positif $n \geq 1$, maka n dapat ditulis dalam bentuk kanonik sebagai:
$n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_k^{a_k}$ dengan p_i untuk $i = 1, 2, \dots, k$ adalah bilangan-bilangan prima yang berlainan dan $a_i \geq 1$ untuk setiap $i = 1, 2, \dots, k$.

Teorema 10.1:

Jika bentuk kanonik dari bilangan positif n adalah $p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_k^{a_k}$, maka

$$\tau(n) = (a_1 + 1)(a_2 + 1)(a_3 + 1) \dots (a_k + 1)$$

Bukti:

Jika d suatu pembagi bulat positif dari n, maka d berbentuk:

$d = p_1^{t_1}p_2^{a_2}p_3^{a_3}\dots p_k^{a_k}$ dengan $0 \leq t_1 \leq a_1$

Maka banyaknya pembagi bulat positif dari n merupakan hasilkali banyaknya piliha yang mungkin untuk t_i dari $(a_i + 1)$ pilihan. Sehingga diperoleh

$$\tau(n) = (a_1 + 1)(a_2 + 1)(a_3 + 1) \dots (a_k + 1)$$

Rumus $\tau(n)$ tersebut sering dinyatakan dengan notasi $\prod$ (pi).

Berikut ini diberikan contoh pemakaian notasi $\prod$.

Contoh 10.6:

1) $\prod_{i=1}^{5} d_i = d_1 \cdot d_4 \cdot d_3 \cdot d_4 \cdot d_5$
2) $\prod_{n=1}^{4} f(n) = f(1) \cdot f(2) \cdot f(3) \cdot f(4)$
3) $\prod_{i=1}^{n} (d_i + 1) = (d_1 + 1)(d_2 + 1)(d_3 + 1) \dots\ (d_n + 1)$

Teorema 7. 1 di atas dapat dituliskan dengan notasi Π sebagai berikut:

Jika $n = p_1^{a_1}p_2^{a_2}p_3^{a_3} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$, maka $\tau(n) = \prod_{i=1}^{k}(a_i + 1)$

Contoh 10. 7:

1) $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$, maka $\tau(1260) = \tau(2^2 \cdot 3^2 \cdot 5 \cdot 7) = (2 + 1)(2 + 1)(1 + 1)(1 + 1) = 36$
2) $33.075 = 3^3 \cdot 5^2 \cdot 7^2$, maka $\tau(33.075) = \tau(3^3 \cdot 5^2 \cdot 7^2) = (3 + 1)(2 + 1)(2 + 1) = 36$
3) Periksalah bahwa $\tau(2310) = 10$, $\tau(210) = 8$, $\tau(1.156) = 9$

Sekarang kita akan memperhatikan hasilkali pembagi-pembagi bulat positif dari suatu bilangan bulat positif n.

Contoh 10. 8:

1) Pembagi-pembagi bulat positif dari 12 adalah 1, 2, 3, 4, 6 dan 12, $\tau(12) = 6$

   Hasilkali semua pembagi bulat positif dari 12 ditulis dengan notasi K(12) maka:

$$\begin{aligned} K(12) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12 \\ &= (1 \cdot 12)(2 \cdot 6)(3 \cdot 4) \\ &= 12 \cdot 12 \cdot 12 \\ &= (12)^3 \end{aligned}$$

2) Semua pembagi bulat positif dari 28 adalah 1, 2, 4, 7, 14, dan 28. $\tau(28) = 6$

   Hasilkali semua pembagi bulat positif dari 28 adalah :

$$\begin{aligned}K(28) &= 1 \cdot 2 \cdot 4 \cdot 7 \cdot 14 \cdot 28\\ &= (1 \cdot 28)(2 \cdot 14)(4 \cdot 7)\\ &= 28 \cdot 28 \cdot 28\\ &= (28)^3\end{aligned}$$

3) Periksalah bahwa $K(2) = 2$, $K(5) = 5$, $K(9) = 27$, $K(18) = 18^3$, $K(24) = 24^3$, $K(32) = 32^3$.

4) Jika p suatu bilangan prima, maka $K(p) = p$, $K(p^2) = p^3$, $K(p^3) = p^6$, $K(p^4) = p^1$, dan $K(p^t) = p^{\frac{t(t+1)}{2}}$

Teorema 10. 2:

Jika n suatu bilangan bulat positif, maka hasilkali semua pembagi bulat positif dari n adalah:

$$K(n) = n^{\frac{1}{2}\tau(n)}$$

Bukti:

Misalkan d adalah suatu pembagi bulat positif dari n, maka ada d' (yaitu pembagi komplemen dari n) sedemikian hingga $dd' = n$. Hal ini mungkin saja terjadi bahwa $d = d'$, yaitu jika n suatu kuadrat sempurna.

Karena banyaknya pembagi bulat positif dari n adalah $\tau(n)$, dengan mengalikan setiap pembagi dari n (misalnya d) dengan pembagi komplemennya (misalkan d') sedemikian hingga $dd' = n$, maka akan diperoleh bahwa hasilkali semua pembagi bulat positif dari n adalah:

$$K(n) = n^{\frac{1}{2}\tau(n)}$$

Notasi lain dari $K(n)$ adalah $\prod_{d|n} d$

K. KEGIATAN BELAJAR 12

K.1. Pendahuluan Kegiatan Belajar 12

Bahan kajian	:	fungsi mobius dan fungsi bilangan bulat diperbesar
Capaian pembelajaran	:	mahasiswa menguasai pemahaman tentang konsep dari fungsi Mobius dan fungsi bilangan bulat diperbesar.
Indikator pembelajaran	:	mahasiswa mampu merumuskan dan mengamplikasikan konsep fungsi Mobius dan fungsi bilangan bulat diperbesar untuk menyelesaikan masalah.
Materi prasyarat	:	teori himpunan, sistem bilangan bulat, lerelasi keterbagian, faktor persekutuan terbesar, kelipatan persekutuan terkecil, basis bilangan bulat, bilangan prima, faktorisasi bilangan tunggal, teorema Fermat, dan teorema Wilson.

K.1. Pendahuluan Kegiatan Belajar 12

A. Fungsi Mobius

Sebelum mendefinisikan fungsi Mobius, terlebih dahulu didefinisikan bilangan bulat bebas kuadrat, yaitu bilangan bulat yang tidak mempunyai faktor suatu bilangan bulat sempurna yang lebih dari 1.

Contoh 13.1:

1) $2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21$ dan sebagainya adalah bilangan-bilangan bebas kuadrat.
2) $4, 8, 12, 16, 18, 20, 24, 27$ dan sebagainya adalah bilangan-bilangan bulat tak bebas kuadrat.

Definisi 13:

Jika n suatu bilangan bulat positif, maka:

$$\mu(n) = \begin{cases} 1, \text{jika } n = 1. \\ 0, \text{jika } n \text{ takbebas kuadrat.} \\ (-1)^k, \quad \text{jika } n \text{ bebas kuadrat} \end{cases}$$

Contoh 13.2:

1) $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-3)^3 = -1$
2) $\mu(500) = \mu(2^2 \cdot 5^3) = 0$
3) $\mu(2) = -1, \mu(3) = -1, \mu(5) = -1, \mu(6) = 1$

4) Jika p suatu bilangan prima, maka $\mu(30) = -1$ dan $\mu(p^k) = 0$, untuk $k \geq 2$.

Fungsi μ Mobius ini merupakan fungsi ganda seperti yang dinyatakan dalam teorema berikut ini:

Teorema 13.1:

Fungsi μ adalah suatu fungsi ganda

Bukti:

Kita akan memperlihatkan bahwa jika $(\mathrm{m}, \mathrm{n}) = 1$, maka $\mu(\mathrm{mn}) = \mu(\mathrm{m})\mu(\mathrm{n})$.

Jika p suatu bilangan prima dan $p^2|m$ atau $p^2|n$, maka $p^2|m$, sehingga $\mu(m\ \ ) = 0 = \mu(m)\mu(n)$.

Jika m dan n adalah bilangan-bilangan bebas kuadrat, misalnya $m = p_1p_2 \ldots p_r$ dan $n = p_1p_2 \ldots q_t$ dengan p_i dan q_j adalah bilangan-bilangan prima.

Maka $\mu(m\ \ ) = \mu(p_1p_2 \ldots p_r q_1q_2 \ldots q_t) = (-1)^{r+t}$

Jadi, μ adalah fungsi ganda.

Perhatikan contoh berikut ini!

Contoh 13.3:

Semua faktor bulat positif dari 12 adalah $1, 2, 3, 4, 5, 6, 12$. Kita akan menghitung jumlah semua nilai fungsi μ untuk smua faktor dari 12, yaitu:

$$\sum_{d|1} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(6) + \mu(12)$$

$$= (1) + (-1) + (-1) + 1 + 0 + 1$$

$$= 0$$

Misalkan suatu bilangan bulat $n > 1$, dan didefinisikan bahwa:

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

Jika $n = p^k$ dengan p suatu bilangan prima dan k suatu bilangan bulat positif, maka semua faktor bulat positif dari n adalah 1, p, p^2,. . . , p^k, sehingga :

$$F(n) = \sum_{d|n} \mu(d) = \ \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k)$$

$$= 1 + (-1) + 0 + \ldots + 0$$

$$= 0$$

Mengingat bahwa μ suatu fungsi ganda dan memperlihatkan Teorema 13.1, maka F merupakan fungsi ganda pula. Selanjutnya, jika bentuk kanonik dari n adalah:

$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k}$, maka

$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F\,(p_r^{k_r})$

$= 0$

Uraian tersebut merupakan bukti dari teorema berikut ini:

Teorema 13.2:

Untuk setiap bilangan bulat bilangan bulat positif n, berlaku :

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \text{jika } n = 1 \\ 0, \text{jika } n > 1 \end{cases}$$

dengan d suatu bilangan bulat positif.

Pada teorema 13.1, telah dijelaskan bahwa jika f suatu fungsi ganda dan fungsi F didefinisikan oleh :

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

maka F suatu fungsi ganda pula. Dari hubungan ini, kita akan mencari rumus f yang dinyatakan dalam fungsi F. Untu ini, kita akan menggunakan fungsi μ Mobius dan mendapatkan teorema berikut ini yang biasa disebut dengan rmus interval Mobius.

Teorema 13.3:

Misalkan F dan f adalah dua fungsi aritmatik yang dihubungkan oleh rumus :

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

Maka $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) F(d)$

Bukti:

Mudah ditunjukkan bahwa $d|n$ dan $c|\frac{n}{d}$, jika dan hanya jika $c|n$ dan $d|\frac{n}{c}$, sehingga

$$\sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c) \right) = \sum_{c|n} \left(\sum_{d|\frac{n}{c}} f(c) \mu(d) \right)$$

$$= \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) \text{ .... (1)}$$

Menurut Teorema 7.7, $\sum_{c|n} = \begin{cases} 1, \text{jika } \frac{n}{c} = 1 \\ 0, \text{jika } \frac{n}{c} > 1 \end{cases}$

Sehingga persamaan (1) menjadi:

$$\sum_{c|n}\left(f(c)\sum_{d|\frac{n}{c}}\mu(d)\right)=\sum_{c=n}f(c)\cdot 1$$

$$= f(n)$$

Sebagai ilustrasi untuk menjelaskan penggunaan jumlahan rangkap tersbut, misalkan diambil $n = 10$.

$$\sum_{d,1}\left(\sum_{c|\frac{1}{d}}\mu(d)f(c)\right)=\mu(1)[f(1)+f(2)+f(5)+f(10)]+\mu(2)[f(1)+f(5)]$$

$$+\mu(5)[f(1)+f(2)]+\mu(10)f(1)$$

$$= f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]+f(2)[\mu(1)+\mu(5)]+f(5)[\mu(1)+\mu(2)]$$

$$+f(1)\mu(1)$$

$$=\sum_{c|1}\left(\sum_{d|\frac{1}{c}}f(c)\mu(d)\right)$$

Untuk melihat bagaiaman peranan rumus inversi Mobius ini, kita perlihatkan kembali fungsi τ dan σ yang dinyatakan sebagai

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

maka dengan menggunakan rumus inversi Mobius (teorema 7.8), maka rumus-rumus τ dan σ tersebut dapat ditentukan inversinya, yaitu $\tau(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\tau(d)=1$ dan $\sigma(n)=\sum_{d|n}\sigma(d)$, untuk setiap bilangan asli n.

Konvers dari Teorema 13.1 juga benar jika dinyatakan sebagai teorema beriku ini:

Teorema 13.4:

Jika F suatu fungsi ganda dan $F(n)=\sum_{d|n}f(d)$, untuk semua bilangan asli n, maka f adalah ganda pula.

Bukti:

Ambil dua bilangan bulat positif m dan n dengan $(m,n)=1$. Jika $d|m$ dan $d=d_1d_2$, karena $(m,n)=1$, maka $d_1|d$ dan $d_2|d$ dan $(d_1,d_2)=1$. Dengan menerapkan rumus inversi Mobius, maka:

$$f(m\ )=\sum_{d|m}\mu(d)F\left(\frac{m}{d}\right)$$

$$=\sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1,d_2)F\left(\frac{m}{d_1d_2}\right)$$

$$=\sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1)F\left(\frac{m}{d_1}\right)\sum_{d_2|n} \mu(d_2)F\left(\frac{n}{d_2}\right)$$

Jadi, f adalah fungsi ganda.

B. Fungsi Bilangan Bulat Terbesar

Fungsi bilangan bulat terbesar atau fungsi kurung persegi [ ] bukan merupakan fungsi aritmatik (fungsi teori bilangan), sebab daerah asal/domainnya adalah himpunan semua bilangan real, tetapi daerah hasil/rangenya adalah himpunan bilangan bulat.

Definisi 13.2:

Untuk suatu bilangan real x, $[x]$ adalah suaut bilangan bulat terbesar yang kurang dari atau sama dengan x, yaitu $[x]$ adalah bilangan bulat tunggal yang memenuhi $x - 1 < [x] \leq x$.

Contoh 13.5:

$\left[-1\frac{1}{2}\right] = -2$; $\left[\sqrt{3}\right] = 1$; $\left[\frac{1}{5}\right] = 0$; $[\pi] = 3$; $[-\pi] = -4$.

Jadi, $[x] = x$ jika dan hanya jika x suatu bilangan bulat sehingga untuk suatu bilangan real x dapat ditulis sebagai:

$x = [x] + \theta$ dengan $0 \leq \theta \leq 1$

Salah satu penggunaan konsep fungsi bilangan bulat terbesar ini adalah menentukan banyaknya faktor prima p yang muncul membagi $n!$. Sebagai contoh, berapa kalikah bilangan 3 muncul sebagai pembagi dari 9!.

$$9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9$$
$$= 2^7 \cdot 3^4 \cdot 5 \cdot 7$$

Ini berarti bilangan 3 muncul sebagai pembagi 9! Sebanyak 4 kali, yang ditunjukkan oleh eksponen dari 3 dalam bentuk kanonik dari 9!.

Sekarang kita menginginkan suatu rumus untuk menghitungnya tanpa menyatakan dalam bentuk kanonik. Rumus itu dinyatakan dalam teorema berikut ini:

Teorema 13.5:

Jika n suatu bilangan bulat positif dan p suatu bilangan prima, maka eksponen tertinggi dari p yang membagi $n!$ adalah

$$\sum_{k=1}^{\infty} \frac{n}{p^k}$$

(deret ini bukan deret tak hingga, karena $\left[\frac{n}{p^k}\right] = 0$, untuk $p^k > n$).

Bukti:

Pertama, bilangan-bilangan bulat positif n yang dapat dibagi oleh p adalah

$$p, 2p, 3p, \ldots, tp$$

Dengan t adalah bilangan bilangan bulat terbesar sedemikian hingga $tp \le n < (t+1)p$. Atau dengan kata lain, t adalah bilangan bulat terbesar yang kurang dari atau sama dengan $\frac{n}{p}$, yaitu $t = \left[\frac{n}{p}\right]$. Jadi, terdapat $\left[\frac{n}{p}\right]$ faktor dari n! yang faktor lainnya adalah p, yaitu:

$$p, 2p, 3p, \ldots, \left[\frac{n}{p}\right] p$$

Selanjutnya dicacah banyaknya bilangan-bilangan bulat positif $1,2,3,\ldots,n$ yang tepat terbagi oleh p^2, seperti paragraph pertama, maka benyaknya factor dari n! yang tepat terbagi oleh p^2 adalah $\left[\frac{n}{p^2}\right]$, yaitu:

$$p^2, 2p^2, 3p^2, \ldots, \left[\frac{n}{p^2}\right] p^2$$

Demikian seterusnya dicacah banyaknya bilangan-bilangan bulat positif $1,2,3,4,\ldots,n$ yang tepat dibagi oleh $p^3, 2p^4, 3p^2, \ldots, \left[\frac{n}{p^k}\right]$.

Proses ini hanya berhingga banyaknya karena mesti ada p^k dengan $p^k > n$, sehingga banyaknya faktor p dari n! adalah

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

Hasil ini dapat dinyatakan sebagi persamaan berikut ini, yang biasanya disebut dengan rumus *Legendre*:

$$n! = \prod_{p \le n} p^{\sum_{k=1}^{x} \frac{n}{p^k}}$$

Contoh13.6:

Berapakah banyaknya angka nol dari repsesntasi desimal 50!?

Jawab:

Untuk menjawab soal tersebut menghitung banyaknya faktor 10 dari hasil kali 50!. Hal ini cukup menghitung eksponen tertinggi dari 2 dan 5 dalam faktorisai prima dari 50! dan memilih eksponennya yang terkecil.

Eksponen tertinggi dari 2 dalam 50! adalah $\sum_{k=1}^{x} \left[\frac{5}{2^k}\right]$, yaitu

$$= \left[\frac{5}{2}\right] + \left[\frac{5}{2^2}\right] + \left[\frac{5}{2^3}\right] + \left[\frac{5}{2^4}\right] + \left[\frac{5}{2^5}\right]$$

$$= 25 + 12 + 6 + 3 + 1 = 47$$

Ini berarti bahwa 2^{47} merupakan faktor dari 50!, sedangkan 2^{48} bukan faktor dari 50!. Eksponen tertinggi dari 5 yang menjadi faktor dari 50! adalah $\sum_{k=1}^{x}\left[\frac{5}{5^k}\right] = \left[\frac{5}{5}\right] + \left[\frac{5}{5^2}\right]$ = 10 + 2 = 12

Jadi, pangkat tertinggi dari 5 yang membagi 50! adalah 12. Sehingga banyaknya angka nol dalam representasi desimal dari 50! adalah 12.

Teorema berikut ini mengkaitkan fungsi bilangan bulat terbesar dengan fungsi-fungsi aritmatik.

Teorema 13.6:

Misalkan *f* dan *F* adalah fungsi-fungsi aritmatik sedemikian hingga:

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

Maka untuk sebarang bilangan bulat positif *N*, berlaku

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Bukti**:**

Dari ketentuan diperoleh bahwa

$$\sum_{n=1}^{N} F(N) = \sum_{n=1}^{N}\sum_{d|n} f(d) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Kita akan mengumpulkan suku-suku yang nilainya sama dari *f*(*d*) dalam jumlahan rangkap tersebut. Untuk suatu bilangan bulat positif tertentu $k \leq N$, suku *f(k)* muncul dalam $\sum_{d|n} f(d)$ jika dan hanya jika k sebagai pembagi dari *n*. (karena setiap bilangan bulat mempunyai pembagi dirinya sendiri, maka ruas kanan dari (1) memuat *f(k)* sekurang-kurangnya sebuah suku). Selanjutnya untuk menghitung jumlahan $\sum_{d|n} f(d)$ dimana *f(k)* hanya sebuah suku, cukup menentukan banyknya bilangan-bilangan bulat diantara 1, 2, 3, . . . , *N* yang dibagi oleh *k*. terdapat tepat $\left[\frac{N}{k}\right]$, yaitu:

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k$$

Jadi, untuk setiap *k* dengan $1 \leq k \leq N$, adalah suatu suku dari jumlahan $\sum_{d|n} f(d)$ untuk $\left[\frac{N}{k}\right]$ bilangan-bilangan bulat berbeda yang lebih kecil atau sama dengan *N*. hal ini dapat ditulis jumlahan rangkap dalam (1) sebagai:

$$\sum_{n=1}^{N}\sum_{d|n} f(d) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Sebagai penerapan teori ini, kita ambil fungsi aritmatik τ dan σ, yaitu:

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

Jika *N* suatu bilangan bulat positif, maka

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right] \text{ dan} \sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$$

Contoh 13.7:

Hitunglah (a) $\sum_{n=1}^{6} \tau(n)$ dan (b) $\sum_{n=1}^{6} \sigma(n)$

Jawab:

(a) $\sum_{n=1}^{6} \tau(n) = \sum_{n=1}^{6} \left[\frac{N}{n}\right] = [6] + [3] + [2] + \left[\frac{6}{4}\right] + \left[\frac{6}{5}\right] + [1]$

$= 6 + 3 + 2 + 1 + 1 + 1 = 14$

(b) $\sum_{n=1}^{6} \sigma(n) = \sum_{n=1}^{6} n \left[\frac{N}{n}\right] = 1. [6] + 2.[3] + 3. [2] + 4. \left[\frac{6}{4}\right] + 5. \left[\frac{6}{5}\right] + 6 [1]$

$= 1.6 + 2.3 + 3.2 + 4.1 + 5.1 + 6.1 = 33$

DAFTAR PUSTAKA

Rosen, K. H. (2011). *Elementary number theory*. London: Pearson Education.

Sukirman. (2006). *Pengantar teori bilangan.* Yogyakarta: UNY Press.

Wahyu Henky (2014). *Pengantar teori bilangan.* Malang: UIN-Maliki Press.

ISBN 978-623-94860-8-2

9 786239 486082