

Mode: Similarity Report

paper text:

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**

95

PRESS Teori Bilangan Penulis : 1.

**Dr. H. Edy Waluyo, M.Pd . 2. Dr. Sri Supiyati, M.Pd.Si**

74

. 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. ii 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**

92

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 iii DAFTAR ISI HALAMAN JUDUL ..... i KATALOG**

66

**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 iv SINOPSIS Teori bilangan merupakan  
cabang matematika yang berkaitan dengan sifat bilangan bulat positif. Kadang-kadang disebut juga sebagai aritmatika yang lebih tinggi. Teori bilangan  
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 menguasai konsep 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

38

sidat kekongruenan, perkongruenan linear, teorema Wilson, fungsi tu, teorema sigma, fungsi mobius, dan fungsi bilangan bulat diperbesar dalam menyelesaikan masalah matematika dengan baik. v 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 penurunan **beberapa teorema dan pemecahan masalah dalam matematika**

42

. Oleh karena itu, penguasaan 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 salah

**satu argumentasi pembuktian suatu teorema atau** pernyataan **matematika yang semesta pembicaraannya himpunan bilangan bulat atau lebih khusus himpunan bilangan asli**

64

. Perhatikan contoh pernyataan-pernyataan matematik berikut. Contoh 1.1: ( ) untuk setiap bilangan asli . Benarkah pernyataan ini? Untuk menjawab pertanyaan ini, kita dapat mencoba dengan mensubstitusikan n dalam pernyataan itu sembarang bilangan asli. Jika , maka pernyataan itu menjadi ( ), atau yaitu diperoleh suatu pernyataan yang benar. Jika maka pernyataan itu menjadi ( ), atau , yaitu diperoleh suatu pernyataan yang benar. Jika maka pernyataan itu menjadi ( ), atau , yaitu suatu pernyataan benar pula. Pembaca dapat melanjutkannya untuk ; ;

**atau bilangan asli lainnya dan akan selalu memperoleh pernyataan yang bernilai benar. Apakah** dengan **memberikan beberapa contoh dengan**

65

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**

48

himpunan semestanya. Pernyataan

pada contoh di atas, himpunan semestanya ialah himpunan semua bilangan asli

48

. Jika kita dapat memberikan contoh untuk tiap bilangan asli 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 bagaimana cara membuktikan pernyataan tersebut? Salah satu caranya ialah memandang ruas pertama dari pernyataan itu sebagai deret aritmatika dengan suku pertama ; bedanya , suku terakhirnya ialah dan memiliki buah suku, maka jumlah deret itu adalah  $(n+1) \cdot n / 2$ , 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 pembuktiannya dengan induksi matematik sebagai berikut : Langkah (1) : **Ditunjukkan bahwa  $P(1)$  benar** Langkah (2) : **Diasumsikan bahwa  $P(k)$  benar untuk suatu bilangan asli 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)****

25

yaitu  $P(1)$  benar, dan karena langkah (2), maka  $P(k+1)$  benar pula. Selanjutnya, karena  $P(k+1)$  benar, menurut langkah (2), maka  $P(k+2)$  benar pula. Dan menurut langkah (2) lagi,  $P(k+2)$  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**

25

. Kita sekarang akan menerapkan langkah-langkah pembuktian dengan induksi matematik itu untuk membuktikan pernyataan pada contoh 1.1 di atas. Contoh 1.2: Buktikan bahwa  $n^2 > n$  untuk setiap bilangan asli  $n$ . **Bukti :** Misalkan  $P(n)$  menyatakan  $n^2 > n$  ( $n > 1$ ) adalah benar. (2) Diasumsikan bahwa  $P(k)$  benar untuk suatu bilangan asli  $k$ , yaitu  $k^2 > k$

**benar Selanjutnya harus ditunjukkan bahwa  $P(k+1)$  benar, yaitu :  $(k+1)^2 > k+1$  Hal ini ditunjukkan sebagai berikut :  $(k+1)^2 = k^2 + 2k + 1 > k + 1$  (karena diasumsikan  $k^2 > k$ ) Jadi,  $P(k+1)$  berarti  $P(k+1)$  benar. Contoh**

7

1.3: Hitunglah  $1 + 2 + 3 + \dots + n$  !! Jawab :  $n(n+1)/2$  sebagai deret aritmatika dengan suku pertama  $1$ , beda  $1$  dan banyaknya suku adalah  $n$  serta suku terakhirnya  $n$ . Maka jumlahan tersebut dapat dihitung dengan rumus jumlahan deret aritmatika yaitu  $(n+1) \cdot n / 2$  Jadi,  $n(n+1)/2$  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:

**Dan seterusnya Tampak bahwa jumlahan-jumlahan ini merupakan bilangan kuadrat sempurna**

88

, sehingga kita bisa menduga bahwa:  $n(n+1)/2$  Tetapi dugaan ini baru merupakan jawabn sementara, sehingga harus dibuktikan kebenarannya. Pembuktiannya dapat dilakukan dengan induksi matematik sebagai berikut: Misalkan  $P(n)$  menyatakan  $n(n+1)/2$  adalah benar, jelas benar. (2) Dimisalkan  $P(k)$

**benar untuk suatu bilangan asli yaitu  $n$  dan ditunjukkan bahwa  $P(k+1)$  benar, yaitu  $(k+1)(k+2)/2$ . Hal ini ditunjukkan**

46

sebagai berikut:  $(k+1)(k+2)/2 = (k^2 + 3k + 2)/2 = (k^2 + 2k + 2k + 2)/2 = (k(k+2) + 2(k+1))/2 = (k(k+1) + (k+1) + 2(k+1))/2 = (k+1)(k+2)/2$  Sehingga  $P(k+1)$  benar. Jadi,  $P(k+1)$  benar untuk setiap bilangan asli  $k$ . Contoh 1.4: Buktikan bahwa  $n^2 > n$  untuk setiap bilangan asli  $n$ . **Bukti :** Misalkan  $P(n)$  menyatakan  $n^2 > n$  ( $n > 1$ ) adalah benar yaitu ( $n^2 > n$ ) benar. (2) Diasumsikan bahwa  $P(k)$  benar untuk suatu bilangan asli  $k$ , yaitu  $k^2 > k$ .

**Selanjutnya harus ditunjukkan bahwa  $P(k+1)$  benar, yaitu :  $(k+1)^2 > k+1$  Hal ini ditunjukkan sebagai berikut :  $(k+1)^2 = k^2 + 2k + 1 > k + 1$  karena**

7







Disebut pula bahwa adalah faktor dari yang menjadi komplemen (sekawan) dari , atau dengan singkat dikatakan bahwa dan adalah pembagi-pembagi sekawan (komplementer) dari 55

. Jika  $|$  , menurut definisi 2.1, maka ada bilangan bulat  $m$  sehingga . Karena , maka , sehingga menurut definisi 2.1 diperoleh  $|$  . Hal ini berarti

relasi keterbagian pada himpunan bilangan bulat mempunyai sifat transitif. Sifat ini dinyatakan sebagai teorema berikut: **Teorema 2. 1: Jika  $|$  dan  $|$  , maka** 69

$|$  . Jika  $|$  yaitu membagi habis , maka  $|$  membagi habis setiap kelipatan , yaitu  $|$  , untuk setiap

bilangan bulat . Hal ini dinyatakan sebagai teorema berikut ini: **Teorema 2 .2: Jika  $|$  maka** 81

$|$  untuk setiap bilangan bulat . Jika  $|$  dan  $|$  , menurut definisi 2.1 , maka diperoleh dan untuk bilangan- bilangan bulat dan . Dari dua kesamaan ini dapat diperoleh bahwa: (i)  $|$  berarti  $|$  (ii)  $|$  berarti  $|$  dan (iii)  $|$  berarti  $|$  . Ketiga kesimpulan ini dinyatakan sebagai ini: **Teorema 2.3: Jika  $|$  dan  $|$  , maka  $|$  ,  $|$  , dan  $|$  .** 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  $|$  dan  $|$  , maka  $|$  untuk setiap bilangan bulat dan .** Bukti: Karena  $|$  dan  $|$  , menurut teorema 2.2, maka  $|$  dan  $|$  untuk setiap bilangan- bilangan  $m$  dan  $n$ . Selanjutnya, menurut teorema 2.3, maka  $|$  . **Teorema 2.5: (i)  $|$  untuk setiap bilangan bulat  $a$  (sifat reflektif). (ii)**

**Jika  $|$  maka  $|$  untuk setiap bilangan bulat . (iii) Jika  $|$  dengan , maka  $|$  . (iv)  $|$  dan  $|$  . (v) Jika  $|$  maka** 15

. (vi) Jika  $|$  dengan , maka  $|$  . (vii) Jika  $|$  dengan  $|$  , maka  $|$  . B.4. Latihan Kegiatan Belajar 2 Selesaikan soal-soal berikut ini dengan benar! 1. Buktikan bahwa jika  $|$  untuk setiap bilangan bulat ! 2. Jika  $|$  , tunjukkan bahwa  $|$  ,  $|$  , dan  $|$  ! 3. Buktikan bahwa

**jika  $|$  dan  $|$  , maka  $|$  ! 4. Jika  $|$  dan  $|$  , buktikan bahwa  $|$  ! 5 . Buktikan bahwa **jika  $|$  , maka  $|$  ! 6 .** Benarkah pernyataan : **jika  $|$  ,** 5  
maka**

$|$  atau  $|$  . 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  $|$  , untuk setiap bilangan bulat ! 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 adalah dan Sedangkan semua faktor-faktor persekutuan (pembagi-pembagi bersama) dari dan 45 adalah dan Dan faktor persekutuan terbesar dari dan adalah

Secara umum, pengertian tentang faktor pesekutuan dari dua bilangan bulat dituliskan sebagai definis berikut ini. **Definisi** 7

3.1: Jika dan adalah bilangan-bilangan bulat, maka

bilangan bulat disebut faktor persekutuan dari  $a$  dan  $b$  jika dan  $|$  dan  $|$  . Karena 1 adalah pembagi ( faktor ) dari setiap bilangan bulat , maka 1 adalah faktor 31

persekutuan dari dua bilangan bulat merupakan faktor persekutuan dari dan . Jadi, himpunan semua persekutuan dari dan tidak pernah

**kosong. Setiap bilangan bulat** kecuali **nol** selalu **membagi nol, sehingga** jika, **maka** setiap **bilangan bulat merupakan faktor** persekutuan dari **dan**. **Dalam hal ini**, himpunan semua **faktor**

31

persekutuan bulat positif dari dan b merupakan himpunan tak hingga. Jika sekurang-kurangnya satu dari dan

**tidak sama dengan nol, maka** himpunan semua **faktor persekutuan** bulat positif **dari a dan b**

21

merupakan himpunan berhingga, sehingga mesti

**ada anggota dari himpunan tersebut yang terbesar** dan **disebut** faktor persekutuan **terbesar (FPB)** dari dan

47

. Secara formal, hal tersebut dinyatakan sebagai definisi berikut ini. Definisi 3.2: Jika dan bilangan-

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

21

. Dari definisi tersebut dapat dimengerti

**bahwa jika, maka**. Dan jika **ada faktor persekutuan lain, misalnya e, maka**. Contoh

7

3.1: Faktor-faktor bulat positif dari

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

39

-12 dan 30 adalah 6, atau dapat ditulis secara singkat sebagai . Selanjutnya, dengan mudah dapat ditunjukkan bahwa, ; . Perhatikan bahwa apakah Misalkan ? , maka dan dan | dan | . . Jika, | | maka ada bilangan bulat, sehingga maka ada bilangan bulat, sehingga atau . . Karena dan, maka, maka dan, maka adalah faktor persekutuan dari dan . Karena, yaitu, sebab suatu bilangan bulat positif. Karena Uraian tersebut merupakan bukti dari teorema berikut ini. Teorema 3.1: Jika, maka . Jika dan

**dua bilangan bulat** positif **dengan, maka dikatakan bahwa dan saling prima atau prima relatif terhadap**

7

. Misalkan dan dua bilangan bulat dengan, maka b dibagi oleh akan memberikan hasil bagi dan sisa pembagian. Hal ini dinyatakan sebagai teorema berikut ini dan terkenal dengan nama Algoritma Pembagian. Teorema 3.1. Jika

**dan b bilangan-bilangan bulat dengan, maka ada dengan tunggal pasangan bilangan-bilangan bulat dan yang memenuhi, dengan**

12

. Bukti: Dibentuk himpunan { }. S bukan merupakan himpunan kosong sebab jika | | dan karena, maka . Karena S beranggotakan bilangan-



**bilangan bulat tak negatif** berbentuk , maka  $S$  pasti memiliki anggota terkecil , misalkan . Sesuai dengan bentuk anggota dari  $S$  , maka , untuk suatu bilangan bulat dan , Selanjutnya akan ditunjukkan bahwa

12

. Andaikan , maka dengan . Jadi , karena , maka . Ini berarti bahwa adalah suatu anggota dari  $S$ . Tetapi .

**Hal ini tidak mungkin, karena adalah bilangan bulat tak negatif yang terkecil dalam  $S$ . Oleh karena itu, pengandaian tersebut harus diingkari. Jadi , sehingga ada dan sedemikian sehingga dengan . Selanjutnya kita akan menunjukkan ketunggalan dari dan .** Misalkan bahwa  $b$  mempunyai dua representasi, yaitu

12

: dengan dan . Maka . ||| karena Dari – dan diperoleh atau || . Jadi, || , yang menghasilkan || . Karena ||

**adalah bilangan bulat tak negatif, maka hanya mungkin jika || , yaitu , sehingga juga**

12

. Berdasarkan pembuktian tersebut, maka teorema tersebut diperluas untuk , sehingga diperoleh akibat sebagai berikut: Akibat 3.1 Jika dan

**bilangan-bilangan bulat dengan , maka ada dengan tunggal pasangan bilangan-bilangan bulat dan**

12

sedemikian hingga dengan || Untuk membuktikan akibat ini, kita cukup memperhatikan untuk yang negatif maka || , sehingga dengan teorema 2.7 tersebut menghasilkan pasangan bilangan-bilangan bulat tunggal dan yang memenuhi: dengan || Perhatikan bahwa || dan mengambil untuk mendapatkan dengan || Sebagai ilustrasi, jika dan , maka dan , yaitu: 3 Di sini tampak bahwa Apakah benar, jika , maka ? Misalkan dan , maka kita akan menunjukkan bahwa , karena , maka | dan | , karena , maka | . Dari | dan | , maka  $d$  adalah faktor persekutuan dari dan , tetapi karena maka . Selanjutnya, karena , maka | dan | dan karena , maka | . Dari | dan | , maka  $d$  adalah faktor persekutuan dari dan . Tetapi karena maka . , Selanjutnya, karena , maka | dan | dan karena , maka | . Dari | dan | , maka adalah faktor persekutuan dan . Tetapi karena dari , maka . Dari dan , maka  $c=d$ , yaitu . Uraian tersebut merupakan bukti dari teorema berikut ini. Teorema 3.2: Jika , maka , maka . Dengan menggunakan teorema ini, memudahkan kita untuk menghitung faktor persekutuan terbesar

**dari sembarang bilangan bulat, meskipun bilangan-bilangan bulat tersebut cukup besar**

14

. Contoh 3.2: Carilah (5767, 4457) Penyelesaian : Kita gunakan algoritma pembagian (teorema 2.8) , maka , maka , maka , maka , maka Faktor persekutuan terbesar dari

**$a$  dan  $b$  dapat dinyatakan sebagai kombinasi linear dari dan yaitu berbentuk dengan**

96

dan bilangan-bilangan bulat tertentu. Misalnya : Uraian ini memberikan contoh untuk teorema berikut ini: Teorema 3.2: Jika dan

**bilangan bulat tidak nol, maka ada bilangan-bilangan bulat dan , sedemikian**

83

hingga . Bukti: Dibentuk himpunan  $S$  yaitu himpunan semua kombinasi linear dari dan yang bernilai positif.  $\{ \}$   $S$  bukan himpunan kosong, sebab jika dan dengan , maka , dengan dan , maka || . Karena  $S$  memuat bilangan-bilangan bulat positif, maka  $S$  memuat anggota yang terkecil, misalnya  $d$ , karena , maka ada bilangan-bilangan bulat dan sehingga . Selanjutnya, kita akan menunjukkan bahwa . Perhatikan dan , menurut algoritma pembagian, maka ada bilangan-bilangan bulat dan sedemikian hingga : dengan Karena dan  $r$  merupakan kombinasi linear dari dan , maka . Hal ini bertentangan dengan fakta bahwa  $d$  adalah anggota terkecil dari  $S$  (ingat bahwa ). Jadi , sehingga atau | . Dengan penalaran yang sama diperoleh | , sehingga adalah faktor persekutuan dari dan .

Selanjutnya, jika adalah sembarang faktor persekutuan dari dan , yaitu | dan | , maka | atau | , sehingga . Ini berarti bahwa . Bukti teorema 2.9 tersebut hanya merupakan bukti eksistensi dan tidak memberikan cara mencari nilai-nilai dan . Hal ini akan dibahas kemudian. Sesuai dengan teorema 3.2 tersebut, jika ,

maka ada bilangan -bilangan bulat dan sedemikian hingga . Sebaliknya jika untuk bilangan -bilangan bulat dan

7

tertentu, apakah ? Misalkan bahwa , maka | dan | , sehingga menurut teorema 2.2 didapat | atau , maka . Teorema 3.3: Jika dan dua

bilangan bulat tidak nol , maka dan saling prima jika dan hanya jika ada bilangan -bilangan bulat dan

31

yang memenuhi . Contoh 3.3: Hitunglah dan ditentukan bilangan-bilangan bulat dan yang memenuhi . Jawab: Jadi, . Selanjutnya, Jadi, dan Tetapi nilai dan yang memenuhi tidak tunggal, sebab , untuk setiap bilangan bulat . Jadi, dan , untuk setiap bilangan bulat . Misalkan | dan | dapatkah kita menyimpulkan bahwa | ? Diambil contoh sebagai berikut: | dan | maka tidak benar bahwa | , tetapi jika diberi tambahan ketentuan bahwa  $(a,b)=1$ , maka kita dapat menyimpulkan bahwa | . Hal ini ditunjukkan sebagai berikut: Karena , menurut teorema 2.10 tersebut, maka ada bilangan-bilangan bulat dan sedemikian hingga: Jika kedua ruas dikalikan , maka diperoleh persamaan: Karena | dan | , maka ada bilangan-bilangan bulat dan sedemikian hingga dan . Sehingga persamaan (1) menjadi: Ini berarti bahwa | Uraian tentang akibat dari teorema 2.10 tersebut dinyatakan sebagai berikut: Akibat 3.2: Jika | dan | dengan , maka | . Jika diketahui bahwa | , apakah kita dapat menyimpulkan bahwa | atau | ? Diambil sebagai contoh: | maka tidak benar jika kita mengambil kesimpulan bahwa | ataupun | . Tetapi jika | ditambah ketentuan , maka kita dapat menyimpulkan bahwa | . Hal itu ditunjukkan sebagai berikut:

Karena , maka ada bilangan -bilangan bulat dan sedemikian hingga: Jika kedua ruas dari persamaan ini dikalikan dengan c, maka diperoleh

5

: Karena | dan | , maka | atau | . 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 | dan , maka | . 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 Kelipatan bulat positif dari 4 adalah Maka kelipatan persekutuan dari 3 dan 4 adalah 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

7

3.2: Misalkan dan

adalah bilangan-bilangan bulat, adalah kelipatan persekutuan dari dan jika | dan

35

| . Nol (0) adalah suatu kelipatan persekutuan dari dan . dan - masing-masing juga merupakan suatu kelipatan persekutuan dari dan . Jadi, himpunan semua kelipatan persekutuan bulat positif a dan b tidak pernah sama dengan himpunan kosong. Himpunan semua kelipatan bulat positif dari 6 adalah { Himpunan semua kelipatan bulat positif dari -9 adalah { } } Jadi, himpunan semua kelipatan persekutuan dari

6 dan -9 adalah { }, sehingga kelipatan persekutuan dari 6 dan -9 adalah 18

34

Ingat bahwa dalam himpunan bagian dari himpunan bilangan-bilangan bulat positif selalu mempunyai anggota terkecil , sehingga KPK

34

dari sebab dua bilangan 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

84

m ditulis  $[ ]$ , jika memenuhi: (i)  $|$  dan  $|$ , (ii) jika  $|$  dan  $|$ , maka  $|$ . 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 persekutuan terkecilnya, sedangkan (ii) mengatakan bahwa kelipatan persekutuan lainnya tidak lebih kecil dari KPK dari dua bilangan itu. Contoh 3.5:  $[ ]$ , maka  $|$  dan  $|$ . Perhatikan pada

contoh di atas, yaitu himpunan semua kelipatan persekutuan bulat positif dari 6 dan -9 adalah

34

$\{ \}$  dan KPK dari 6 dan -9 adalah 18 atau ditulis  $[ ]$ . Tampak di sini bahwa 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

adalah suatu kelipatan persekutuan dari dua bilangan bulat tidak nol dan  $m$ , maka KPK dan membagi  $m$ , yaitu  $[ ]$ . Bukti: Misalkan  $[ a, b ]$

35

$m$ , maka harus ditunjukkan bahwa  $|$ . Andaikan maka algoritma pembagian, ada bilangan bulat  $q$  dan  $r$  sedemikian hingga dengan  $m = aq + r$ . Karena  $a$  adalah kelipatan persekutuan

dari  $a$  dan  $b$ , maka  $|$  dan  $|$ . Karena  $[ ]$ , maka  $|$  dan  $|$ . Maka  $|$  dan  $|$ , maka

17

$|$ . Demikian pula  $|$ , maka  $|$  dan karena  $|$ , maka  $|$ . Berarti  $|$ . Karena  $|$  dan  $|$  maka  $r$  adalah kelipatan persekutuan dari  $a$  dan  $b$ . Tetapi karena  $[ ]$  dan  $|$ , maka hal tersebut tidak mungkin (kontradiksi). Jadi, pengandaian di atas tidak benar, berarti  $|$  atau  $|$ . Perhatikan bahwa  $[ ]$  dan  $[ ]$ . Tampak bahwa  $[ ]$ . Hal ini memberikan ilustrasi dari teorema berikut ini: Teorema 3.6: Jika  $[ ]$ , maka  $[ ]$ . Bukti: Misalkan  $[ ]$ , maka  $|$  dan  $|$ , sehingga  $|$  dan  $|$ . Hal ini berarti  $dc$  adalah kelipatan persekutuan dari  $ac$  dan  $bc$ . Dan menurut teorema 2.10, maka  $[ ]$ . Karena  $[ ]$  Misalkan  $[ ]$  adalah suatu kelipatan dari  $a$ , maka  $[ ]$ , maka  $|$ , sehingga  $|$ . ] adalah suatu kelipatan dari  $a$ . Teorema 3.7: Jika  $[ ]$ , maka  $[ ]$  Bukti: Misalkan  $[ ]$ , maka  $|$  dan  $|$ , sehingga  $|$ . Hal ini berarti  $dc$  adalah kelipatan persekutuan dari  $aca$  dan  $bc$ . Dan menurut teorema 2.10, maka  $[ ]$ . Karena  $[ ]$  adalah suatu kelipatan dari  $ac$ , maka  $[ ]$ , sehingga  $|$ . Karena  $[ ]$ , maka  $|$  dan  $|$ , sehingga  $|$  dan  $|$ , dan menurut teorema 2.12, maka  $[ ]$ , yaitu  $|$  dan karena  $|$ , maka Sehingga, yaitu  $[ ]$ . Contoh 3.7: (1)  $[ ]$  (2)  $[ ]$  Mengingat teorema tersebut, maka

dengan mengeluarkan faktor persekutuannya akan mempermudah dalam mencari KPK-nya. Jika  $[ ]$ , berapakah  $[ a, b ]$

35

? Apakah  $[ ]$ ? Akan ditunjukkan sebagai berikut: Jelas bahwa  $ab$  adalah suatu kelipatan persekutuan dari  $a$  dan  $b$ , menurut teorema 2.12, maka  $[ ]$ . Di lain pihak, menurut akibat dari teorema 2.10, karena  $[ ]$  dan  $[ ]$  dengan  $[ ]$ , maka  $[ ]$  dan karena  $[ ]$ , maka disimpulkan  $[ ]$ . Selanjutnya, jika  $[ ]$ , maka  $( )$ . Berdasarkan pada kesimpulan di atas, maka  $* +$ . Jika kedua ruas dikalikan  $[ ]$ , maka diperoleh bahwa  $[ ]$  Uraian di atas merupakan bukti teorema berikut ini: Teorema 3.7: Jika  $a$  dan  $b$  bilangan-bilangan bulat yang keduanya positif, maka Contoh 3.8: (1) Karena  $a$  dan  $b$ , terdapat hubungan  $[ ]$  (2) dan  $[ ]$ , terdapat hubungan  $[ ]$  25-18n B.4. Latihan Kegiatan Belajar 3 Selesaikan soal-soal berikut ini dengan benar! 1. Jika buktikan bahwa  $|$  untuk setiap bilangan-bilangan bulat  $a$  dan  $b$ . 2. Jika  $a$  dan  $b$  buktikan bahwa!

3. Jika  $a$  dan  $b$  bilangan-bilangan bulat tidak nol

11

, tunjukkan bahwa! 4. Jika  $n$  suatu bilangan bulat positif dan  $a$  sembarang bilangan bulat, buktikan bahwa  $|$ ! 5. 6. 7. Jika  $a$  dan  $b$ , buktikan bahwa Buktikan bahwa  $( )$ ! Buktikan bahwa  $|$ ! 8. 9. Buktikan jika suatu kelipatan persekutuan dari  $a$  dan  $b$ , maka Buktikan jika  $[ ]$ , maka  $|$ ! 10. Jika  $|$ , maka  $[ ]$ ! 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 berbagai 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: 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 suatu bilangan bulat positif yang lebih besar dari 1, maka setiap bilangan bulat positif  $n$  dapat ditulis secara tunggal dalam bentuk dengan  $k$  suatu bilangan bulat taknegatif, suatu bilangan bulat dengan  $r$  untuk dengan

**Bukti: Untuk memperoleh** representasi **dari seperti yang diinginkan, kita menerapkan algoritma pembagian** sebagai **berikut.** 28  
**Pertama, kita membagi dengan  $a$  untuk mendapatkan**

Jika  $a > b$ , kita membagi dengan  $b$  dan mendapatkan bahwa  $a = qb + r$ , Kita melanjutkan proses ini untuk memperoleh  $r = q_1b + r_1$ , . . . . , Langkah terakhir dari proses ini terjadi apabila kita memperoleh hasilbagi

**0. Perhatikan bahwa dalam penerapan algoritma** -algoritma pembagian **tersebut, kita** memperoleh hasilbagi-hasilbagi **yang** 28  
**memenuhi**

Karena barisan adalah suatu barisan turun dari bilangan-bilangan bulat tak negatif, maka barisan ini akan berakhir pada suku 0. Selanjutnya dari persamaan pertama disubstitusi dalam persamaan kedua diperoleh  $r = q_1b + r_1$ . . . Dimana karena  $a > b$  untuk dan 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:  $n = aq + r$  dan  $n = aq_1 + r_1$ , Jika kedua persamaan tersebut dikurangkan, maka diperoleh  $a(q - q_1) = r_1 - r$ . Jika kedua representasi dari  $n$  tersebut berbeda, maka ada bilangan bulat terkecil  $j$ , sedemikian hingga  $\{0, 1, \dots, j-1\}$  jadi  $\{0, 1, \dots, j-1\}$  sehingga  $r_1 - r = a(q - q_1) + a(j - 1)$   $\{0, 1, \dots, j-1\}$  Ini berarti bahwa  $|a(j - 1)| < a$  Tetapi karena  $a > b$ , yaitu  $a > r_1 - r$ , sehingga  $r_1 - r = a(j - 1)$  Jadi, representasi dari  $n$  adalah tunggal. Selanjutnya, jika yaitu

**dinyatakan sebagai jumlahan dari perpangkatan bulat dari  $a$ , maka dapat dituliskan sebagai** 28

( ) Contoh 4.2: 1) 2) Jadi (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** 28

atau secara singkat heks. Koefisien 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-ulang seperti pada proses pada pembuktian teorema diatas. Contoh 4.4: Tulislah dalam lambang bilangan dengan basis  $b$ . Jawab: Penerapan algoritma pembagian berulang-ulang, yaitu:

**Penulisan bilangan bulat  $n$  seperti ini dikatakan bahwa** dituliskan **dalam basis** 28

. Contoh 4.5: Misalnya  $b = 5$  sebagai basis penulisan, maka lambang dasarnya adalah  $\{0, 1, 2, 3, 4\}$  dan  $\{0, 1, 2, 3, 4\}$ . Misalkan suatu bilangan bulat  $n$  dinyatakan sebagai: Maka dalam basis 5,  $n$  tersebut ditulis sebagai  $n = 320145_5$ . Jika  $n$  ingin ditulis dalam basis decimal (sepuluh), maka kita tinggal menghitung jumlahan dari perpangkatan lima tersebut, yaitu: Jika kita ingin menuliskan lambang bilangan tersebut dalam basis lainnya, misalnya basis  $b$ , maka kita mengerjakannya seperti dalam proses pembuktian teorema di atas, yaitu:  $n = aq + r$  Ini berarti



(tersusun). Barisan bilangan prima: Barisan bilangan komposit: 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  $n$ , maka dapat diuraikan atas faktor-faktor prima, yaitu: atau atau atau lainnya Perbedaan penguraian dari 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 berikut 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  $n$ .

68

suatu bilangan prima, maka  $n$ , berarti teorema telah terbukti.

**Jika suatu bilangan komposit, maka mempunyai faktor bulat positif selain 1 dan  $n$ , misalnya  $p$ , yaitu  $n = p \cdot m$ . Sehingga ada bilangan bulat positif sedemikian  $m$  hingga  $m < n$ . Jika suatu bilangan prima, maka  $n$  adalah bilangan prima.**

27

. Sehingga teorema terbukti.

**Tetapi jika suatu bilangan komposit, maka mempunyai faktor bulat positif selain 1 dan  $n$ , misalnya  $p$ , yaitu  $n = p \cdot m$ . Sehingga ada bilangan bulat positif sedemikian  $m$  hingga  $m < n$ . Jika suatu bilangan prima, maka  $n$  adalah bilangan prima. Dan karena  $m < n$ , maka  $m$  terbagi oleh bilangan prima.**

27

, berarti teorema terbukti.

**Tetapi jika suatu bilangan komposit, maka mempunyai faktor bulat positif selain 1 dan  $n$ , misalnya  $p$ , yaitu  $n = p \cdot m$ . Ini berarti ada bilangan bulat positif sedemikian  $m$  hingga  $m < n$  dengan  $m$  terbagi oleh bilangan prima. Karena  $m < n$ , maka  $m$  terbagi oleh bilangan prima.**

27

, berarti teorema terbukti. Tetapi jika suatu bilangan komposit, maka proses seperti di atas dapat dilanjutkan sedemikian hingga diperoleh suatu barisan: Penguraian di atas faktor-faktor komposit ini tentu berakhir pada suatu faktor prima, karena faktor-faktor tersebut selalu lebih kecil dari bilangan yang difaktorkan dan selalu lebih besar dari 1. Misalkan pemfaktoran tersebut berakhir pada faktor prima  $p$ , maka  $n = p \cdot m$  dan Bukti alternatif lain: Karena

**suatu bilangan bulat positif yang lebih besar dari 1, maka**

28

$n$  mempunyai sekurang-kurangnya satu faktor bulat positif katakan  $p$  sendiri. Sehingga  $n$  mesti mempunyai faktor bulat positif terkecil, misalnya  $p$ , maka  $n = p \cdot m$  adalah suatu bilangan prima. Sebab jika  $m$  bukan bilangan prima, maka dengan demikian  $m$  adalah faktor bulat positif dari  $n$ , tetapi karena  $p$  adalah faktor bulat positif terkecil dari  $n$ , maka terdapat kontradiksi. Memperhatikan teorema di atas, suatu bilangan bulat positif yang lebih besar dari 1 selalu terbagi oleh suatu bilangan prima, maka hasilbagi apapun akan terbagi oleh suatu bilangan prima pula. Dan hasilbagi berikutnya pun demikian pula. Sehingga suatu bilangan bulat positif yang lebih besar dari 1 dapat dinyatakan sebagai perkalian dari bilangan-bilangan prima tertentu.

**Hal ini dinyatakan sebagai teorema berikut ini. Teorema 4.3: Setiap bilangan bulat**

8

positif yang lebih besar dari 1 adalah suatu bilangan prima atau bilangan itu dapat dinyatakan sebagai perkalian bilangan-bilangan prima. Bukti: Ambil sembarang bilangan bulat positif  $n$ . Menurut teorema 4.1, maka ada suatu bilangan prima sedemikian hingga  $n = p \cdot m$ . Sehingga ada suatu bilangan positif,

dengan Jika , maka sehingga n suatu bilangan prima. Tetapi jika , maka menurut Teorema 4.1 lagi, ada suatu bilangan prima sedemikian hingga . Sehingga ada suatu bilangan bulat positif , sehingga dengan Jika , maka sehingga . Berarti teorema terbukti. Tetapi jika , maka ada suatu bilangan prima sedemikian hingga dengan Jika , maka sehingga berarti teorema terbukti. Tetapi jika , maka proses seperti di atas dapat dilanjutkan sehingga akan berakhir pada , maka diperoleh , yaitu

**bilangan bulat positif dapat dinyatakan sebagai perkalian bilangan prima . Suatu bilangan bulat**

16

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: dapat ditulis Hal ini secara umum,

**jika n suatu bilangan bulat positif yang lebih besar dari**

60

1 dapat dinyatakan sebagai dengan adalah faktor-faktor prima dari n dan 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 . 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. menyatakan nilai minimum dari dan . menyatakan nilai maksimum

**dari a dan b . Misalnya : Misalkan , dan adalah bilangan -bilangan bulat positif yang lebih besar dari 1**

91

yang bentuk-bentuk kanoniknya berturut-turut sebagai berikut: Maka FPB dan KPK dari , dan berturut-turut dengan untuk dengan untuk Contoh 5.3: Tentukan FPB dan KPK dari 198, 216, dan 252! Penyelesaian: Jika tiga bilangan tersebut diuraikan atas faktor-faktor prima, maka diperoleh : Uraian atas faktor-faktor prima tersebut dapat ditulis sebagai berikut: Jika diberikan suatu bilangan bulat positif, misalnya 2167, apakah bilangan ini suatu bilangan prima? Untuk menjawab pertanyaan ini, kita akan mencoba-coba membagi bilangan tersebut dengan 2,3,4,5, dan seterusnya, sampai suatu 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 efisien. Berikut ini suatu teorema yang memberikan batas sampai bilangan bulat positif mana kita berhenti membagi dan segera menyimpulkan bahwa bilangan tersebut adalah bilangan prima. Teorema 5.3: Jika suatu bilangan komposit, maka memiliki faktor dengan  $\sqrt{n}$ . Bukti: Karena suatu bilangan komposit, maka ada bilangan-bilangan positif dan sedemikian hingga dan Jika k dan m kedua-duanya lebih besar dari  $\sqrt{n}$ , yaitu  $\sqrt{n}$  dan  $\sqrt{n}$ , maka  $\sqrt{n}\sqrt{n}$  Terdapat, hal ini tidak mungkin. Oleh karena itu, salah satu dari k atau m harus tidak lebih kecil dari  $\sqrt{n}$ , misalnya k yaitu Jadi, memiliki faktor k dengan  $\sqrt{n}$ . Teorema 4.3 tersebut sama benarnya dengan kontraposisinya, yaitu: Jika bilangan bulat positif n tidak memiliki faktor dengan  $\sqrt{n}$ , 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  $\sqrt{2167}$  Tetapi ingat bahwa 2167 tak terbagi oleh 2, maka 2167 tak terbagi oleh semua kelipatan 2. Demikian pula 2167 tak terbagi oleh 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 tidak memiliki faktor prima dengan  $\sqrt{n}$ , maka 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 tunggal. 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 positif yang lebih besar dari 1 adalah suatu bilangan prima atau bilangan itu dapat dinyatakan sebagai perkalian dari bilangan-bilangan prima tertentu. Pada sesi ini akan dipelajari bahwa pembuktian suatu bilangan bulat positif atas faktor-faktor prima tunggal, tetapi sebelum membicarakan faktorisasi tunggal, kita akan mempelajari beberapa teorema sebagai persiapan untuk mempelajari faktorisasi tunggal. Teorema 6.1: Jika suatu bilangan prima dan | , maka | atau | . Bukti: Karena p suatu bilangan prima, maka untuk sebarang bilangan bulat a berlaku ( ) atau ( ) . Jika ( ) dan | , kita pernah membuktikan bahwa | . Buktikanlah kembali! Dan jika ( ) maka | . Jadi, terbukti bahwa | atau | . Teorema 4.5 ini dapat diperluas untuk bilangan-bilangan Jika suatu bilangan prima dan | , maka | untuk suatu yaitu: . Bukti: Kita akan membuktikan dengan induksi matematik pada , yaitu banyaknya faktor. Untuk Untuk atau | . , yaitu | , jelas benar. , yaitu | , karena p suatu bilangan prima, maka menurut Teorema 4.5 | Diambil sebagai hipotesis induksi untuk dengan | maka | untuk . , yaitu p bilangan prima dan Pandang | atau dapat ditulis sebagai |( Teorema 4.5 diperoleh | atau | . )( ), maka menurut Jika | , maka teorema telah

terbukti. Jika  $|$ , maka menurut Teorema 4.5 lagi diperoleh  $|$  atau  $|$ . Jika  $|$ , maka teorema terbukti. Jika  $|$  maka proses seperti di atas dapat diteruskan.

Berdasarkan hipotesis yang diambil, maka dapat diteruskan mesti akan berakhir. Berarti bilangan prima membagi salah satu dari  $|$ . Jika pada teorema 4.5 diambil kasus bahwa  $p, q$ , dan  $r$  masing-masing bilangan prima dan  $|$  maka  $|$  atau  $|$ , yaitu atau  $|$ . Karena  $p, q$ , dan  $r$  masing-masing bilangan prima kasus tersebut dapat diperluas sebagai berikut: Jika  $p, q, r, \dots$ , semuanya bilangan prima dan  $|$ , maka untuk suatu dengan  $|$ . Selanjutnya kita akan membuktikan ketunggalan dari faktorisasi prima dari suatu bilangan bulat positif. Teorema ini sering disebut faktorisasi tunggal yang merupakan teorema dasar dalam aritmetika.

**Teorema 6.2:** Pemfaktoran suatu bilangan bulat positif yang lebih besar dari 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** 78  
-bilangan **prima**

tertentu. Sekarang, kita akan membuktikan bahwa faktor-faktor prima tersebut adalah tunggal. Ambil sembarang bilangan bulat positif  $n$ . Jika suatu bilangan prima, maka adalah faktornya sendiri. Jika suatu bilangan komposit dan diandaikan bahwa pemfaktoran  $n$  atas faktor-faktor prima adalah tidak tunggal, misalnya:  $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m$  dan dengan  $p_i$  dan  $q_j$  masing-masing adalah bilangan-bilangan prima untuk  $i = 1, 2, \dots, k$  dan  $j = 1, 2, \dots, m$ . Karena maka perluasan teorema 4.5, maka  $p_1 | q_1 q_2 \dots q_m$ . Dan selanjutnya menurut untuk suatu  $k$  dengan  $|$ . Dan mengingat  $p_1$  prima, maka  $p_1 | q_1$ . Karena 4.5, maka  $p_1 = q_1$ . Karena  $p_1$  dan  $q_1$  untuk suatu  $m$  dengan  $|$ , maka  $p_1 | q_2 \dots q_m$ . Dan menurut perluasan teorema 4.5,  $p_1 | q_2$ . Dan mengingat  $p_1$  prima, maka  $p_1 = q_2$ . Demikian seterusnya. Dan mengingat  $p_1 | q_1 q_2 \dots q_m$  dari pemisalan diatas kita maka  $p_1 | q_1 q_2 \dots q_m$  memperoleh bahwa  $p_1 | q_1$ . Jika proses seperti di atas diteruskan, maka kita akan memperoleh bahwa  $p_1 | q_1$ . Dan seterusnya. Jika  $p_1 = q_1$  maka proses tersebut akan berakhir pada  $p_1 = q_1$ . Tetapi jika  $p_1 \neq q_1$ , maka akan diperoleh bahwa  $p_1 | q_1$  dan teorema terbukti. Hal ini mustahil, karena  $p_1$  dan  $q_1$  adalah bilangan-bilangan prima, maka haruslah  $p_1 = q_1$ . Ini berarti bahwa bilangan bulat positif  $n$  tersebut hanya dapat dinyatakan sebagai 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  $n = 1$ ? Sebagai hipotesis, misalkan teorema benar-benar untuk bilangan bulat positif  $n$  dan harus ditunjukkan bahwa benar untuk  $n+1$ . Misalkan  $n+1 = p_1 p_2 \dots p_k$  dan  $n = q_1 q_2 \dots q_m$  adalah bilangan-bilangan prima .... dan seterusnya seperti bagian pembuktian di atas, sehingga diperoleh  $p_1 | q_1 q_2 \dots q_m$ . Bilangan ini lebih kecil atau sama dengan  $n$ , mengingat hipotesis, maka teorema benar untuk  $n$ . Dengan demikian terbukti bahwa 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 banyaknya bilangan prima adalah tak berhingga. Misalkan  $p_1, p_2, \dots, p_k$  adalah urutan bilangan-bilangan prima dan andaikan ada bilangan prima terbesar, misalkan  $p_k$ , sekarang dibentuk suatu bilangan bulat positif:  $N = p_1 p_2 \dots p_k + 1$ . Karena  $N$ , menurut Teorema 4.1, maka dapat dibagi oleh suatu bilangan prima, sehingga dapat dibagi oleh sekurang-kurangnya satu bilangan prima dari  $p_1, p_2, \dots, p_k$ . Misalkan  $N = p_i m$  bilangan prima dengan  $p_i$  yang membagi  $N$ , yaitu  $N = p_i |$ , dengan  $|$  dan  $|$ , maka  $|$ . Hal ini tidak mungkin, karena  $N$  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 sebagai hasil kali semua bilangan prima ditambah 1. Apakah tersebut suatu bilangan prima? Misalkan kita memulai untuk bilangan prima pertama yaitu 2, maka kita memperoleh:  $2 + 1 = 3$ . Coba tunjukkan bahwa Selanjutnya tentukanlah bilangan prima!  $3 + 1 = 4$ ,  $4 + 1 = 5$ , dan tersebut masing-masing adalah prima.  $5 + 1 = 6$ , dan  $6 + 1 = 7$ . Tunjukkan bahwa bilangan-bilangan ini bukan Suatu pertanyaan yang jawabannya belum diketahui, apakah ada tak berhingga sedemikian suatu bilangan prima pula. Demikian pula, apakah tak berhingga bilangan komposit? Perhatikan barisan bilangan prima  $2, 3, 5, 7, \dots$ . adalah bilangan prima ke- $n$ . Sekarang kita ingin menentukan suatu batas atas dari barisan bilangan prima tersebut. Pada pembuktian Teorema Euclides di atas dapat diambil kesimpulan bahwa: Sebagai contoh, jika  $n = 4$ , maka ketidaksamaan itu menjadi Ketidaksamaan ini menunjukkan 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 menyatakan bilangan prima ke- $n$ . maka  $p_n < 2^n$ . **Bukti:** Pembuktian menggunakan induksi matematik pada  $n$ . Untuk diperoleh yaitu  $p_1 = 2$ . Hal ini memang benar, sebab bilangan prima pertama adalah 2. Selanjutnya sebagai hipotesis, teorema diasumsikan benar untuk  $n$ , yaitu: Harus dibuktikan bahwa teorema benar untuk  $n+1$ , yaitu  $p_{n+1} < 2^{n+1}$ . Perhatikan bahwa: Mudah ditunjukkan bahwa  $p_{n+1} < 2^{n+1}$  dengan suatu deret geometri dengan rasio 2, sehingga diperoleh:  $p_{n+1} < 2^{n+1}$ . Yaitu sudah deret geometri dengan rasio 2, sehingga diperoleh:  $(2^n - 1) < p_{n+1}$ . Karena untuk setiap bilangan asli  $n$ , maka ketidaksamaan itu menjadi  $(2^n - 1) < p_{n+1}$ . Karena teorema benar untuk  $n$  dan benar untuk  $n+1$  dan telah ditunjukkan benar untuk  $n$ , maka teorema benar untuk setiap bilangan asli  $n$ . Memperhatikan teorema ini, maka bilangan rima ke  $(n)$ , yaitu  $p_n$ , sehingga banyaknya bilangan prima yang lebih kecil dari tidak kurang dari  $(n)$  buah. Jadi, untuk  $n$ , maka ada paling sedikit  $n+1$  buah bilangan prima yang lebih kecil dari  $2^n$ .

**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 suatu bilangan bulat positif, maka kongruen dengan modulo  $m$  (ditulis  $\equiv (\text{mod } m)$ ) bila membagi  $(-)$ . Jika  $m$  tidak membagi  $(-)$  maka dikatakan bahwa tidak kongruen dengan modulo (ditulis  $\not\equiv (\text{mod } m)$ ). Contoh 8.1 :  $25 \equiv 1 (\text{mod } 4)$ , sebab**

4

4 membagi (habis)  $25 - 1$ .  $31 \not\equiv 5 (\text{mod } 6)$ , sebab 4 membagi (habis)  $31 - 5$ . Definisi 8.1 tersebut dapat ditulis bahwa jika  $a > 0$  maka  $a \equiv b (\text{mod } m)$  bila dan hanya bila  $a - b \equiv 0 (\text{mod } m)$ . Jika  $a \equiv b (\text{mod } m)$ , maka ada bilangan bulat sehingga  $a - b = km$ . Sehingga  $a \equiv b (\text{mod } m)$  bila dan hanya bila  $a - b = km$

untuk suatu bilangan bulat  $k$ . Tetapi karena  $-k = (-1)k$  sama artinya dengan  $k = (-1)(-k)$ , maka  $a \equiv b (\text{mod } m)$

54

) bila dan hanya bila  $a - b = km$ . Contoh 8.2:

$26 \equiv 4 (\text{mod } 11)$  sama artinya dengan  $26 = 11 \cdot 2 + 4$ .  $38 \equiv 3 (\text{mod } 5)$  sama artinya dengan  $38 = 5 \cdot 7 + 3$

29

. Uraian tersebut merupakan bukti dari teorema berikut ini: Teorema 8.1:  $a \equiv b (\text{mod } m)$  bila dan hanya bila ada bilangan bulat sehingga  $a - b = km$ .

**$a \equiv b (\text{mod } m)$  bila dan hanya bila ada bilangan bulat sehingga  $a - b = km$ . Kita telah mempelajari bahwa jika  $a$  dan  $m$  bilangan-bilangan bulat dan  $m > 0$ , menurut algoritma pembagian, maka dapat dinyatakan sebagai  $a = qm + r$  dengan  $0 \leq r < m$ . Ini berarti bahwa  $a \equiv r (\text{mod } m)$ . Karena**

3

$0 \leq r < m$ ,

**maka ada buah pilihan untuk  $r$ , yaitu  $0, 1, 2, 3, \dots, (m - 1)$ . Jadi setiap bilangan bulat akan kongruen modulo dengan tepat satu diantara  $0, 1, 2, 3, \dots, (m - 1)$ . Hal ini dinyatakan sebagai teorema berikut ini. Teorema 8.2: Setiap bilangan bulat kongruen modulo dengan tepat satu diantara  $0, 1, 2, 3, \dots, (m - 1)$ . Definisi 8.2: Jika  $a \equiv r (\text{mod } m)$  dengan  $0 \leq r < m$ , maka disebut residu terkecil dari  $a$  modulo  $m$ . Untuk kekongruenan modulo**

2

ini,  $\{0, 1, 2, 3, \dots, (m - 1)\}$  disebut himpunan residu

**terkecil modulo. 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**

2

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**

4

**$34 : 5$  adalah 4. Walaupun  $34 \equiv 9 (\text{mod } 5)$ , 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  $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$**

4

4, 5, 6, 7, 8}. Himpunan residu terkecil modulo 25 adalah  $\{0, 1, 2, 3, \dots, 24\}$

2

Kita dapat melihat relasi kekongruenan itu dengan cara lain, seperti pada teorema berikut ini. **Teorema 8.3**  $a \equiv b \pmod{m}$  bila dan hanya bila  $a$  dan  $b$  memiliki sisa yang sama jika dibagi  $m$ . **Bukti:** Pertama dibuktikan jika  $a \equiv b \pmod{m}$  maka  $a$  dan  $b$  memiliki sisa yang sama jika dibagi  $m$ . Karena  $a \equiv b \pmod{m}$  maka  $a - b \equiv 0 \pmod{m}$  dan  $a - b = km$  dengan  $k$  adalah residu terkecil modulo  $m$  atau  $0 \leq k < m$ . Selanjutnya,  $a = b + km$  berarti  $a$  dan  $b$  memiliki sisa yang sama jika dibagi  $m$ . Kedua, buktikan jika  $a$  dan  $b$  memiliki sisa yang sama jika dibagi  $m$ , maka  $a \equiv b \pmod{m}$ . Misalkan  $a$  memiliki sisa  $r$  jika dibagi  $m$ , berarti  $a = km + r$  dan  $b = lm + r$  dan memiliki sisa  $r$  jika dibagi  $m$ . Dari kedua persamaan itu diperoleh bahwa  $a - b = (k - l)m$  berarti  $a - b \equiv 0 \pmod{m}$  atau  $a \equiv b \pmod{m}$ .

8

Menurut teorema terdahulu, ungkapan-ungkapan berikut mempunyai arti yang sama

4

Teorema "  $n \equiv 7 \pmod{8}$ " "  $n = 7 + 8k$  untuk suatu bilangan bulat  $k$ ", dan "  $n$  dibagi 8 bersisa 7" Definisi 8.3: Himpunan bilangan bulat  $\{1, 2, 3, \dots\}$  disebut sistem

residu lengkap modulo  $m$ , bila setiap elemennya kongruen modulo  $m$  dengan satu dan hanya satu dari  $0, 1, 2, \dots, (m - 1)$ . Contoh 8.5: (i) Himpunan  $\{45, -9, 12, -22, 24\}$  adalah suatu sistem residu lengkap 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  $5 \equiv 11 \pmod{6}$  yang dua-duanya berada dalam himpunan tersebut

4

Kekongruenan modulo suatu bilangan bulat positif adalah suatu relasi antara bilangan-bilangan bulat

54

Dapat ditunjukkan bahwa relasi kekongruenan itu merupakan relasi ekuivalensi. Kita ingat bahwa suatu relasi disebut relasi ekuivalensi jika relasi itu memiliki sifat refleksi, sifat simetris dan sifat transitif. Jika  $a, b, c$  dan  $m$  adalah bilangan-bilangan bulat dengan positif, maka: (i) Jika  $a \equiv a \pmod{m}$ , sifat refleksi. (ii) Jika  $a \equiv b \pmod{m}$  maka  $b \equiv a \pmod{m}$ , sifat simetris. (iii) Jika  $a \equiv b \pmod{m}$  dan  $b \equiv c \pmod{m}$  maka  $a \equiv c \pmod{m}$  sifat transitif

3

Kita buktikan tiap-tiap sifat itu! (i) Karena  $a - a = 0 = 0$ ,

maka  $a \equiv a \pmod{m}$ . (ii) Karena  $a \equiv b \pmod{m}$  maka  $a - b = km$  untuk suatu bilangan bulat  $k$ , sehingga  $b - a = -km$  yang berarti bahwa  $b \equiv a \pmod{m}$ . (iii)  $a \equiv b \pmod{m}$  berarti  $a - b = km$  dan  $b \equiv c \pmod{m}$  berarti  $b - c = lm$  maka  $a - c = (k - l)m$  berarti  $a \equiv c \pmod{m}$ .

3

untuk suatu bilangan bulat  $a \equiv b \pmod{m}$  berarti  $a - b = hm$  untuk suatu bilangan bulat  $h$ . Ruas-ruas kedua persamaan dijumlahkan, sehingga diperoleh  $a - b = (-h)m$  yang berarti bahwa  $a \equiv b \pmod{m}$ . Karena relasi " $\equiv$ " (kekongruenan) pada himpunan bilangan bulat memenuhi tiga sifat tersebut, maka relasi kekongruenan pada himpunan tersebut merupakan relasi

29

ekivalen. Akibatnya himpunan bilangan bulat terpartisi dalam himpunan-himpunan bagian yang setiap himpunan bagian disebut kelas. Contoh

87

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

8

$0 = [0] = \{\dots, -10, -5, 0, 5, 10, \dots\}$   $1 = [1] = \{\dots, -9, -4, 1, 6, 11, \dots\}$   $2 = [2] = \{\dots, -8, -3, 2, 7, 12, \dots\}$   $3 = [3] = \{\dots, -7, -2, 3, 8, 13, \dots\}$   $4 = [4] = \{\dots, -6, -1, 4, 9, 14, \dots\}$  Pemberian nama untuk suatu kelas menggunakan nama salah satu anggota dari kelas tersebut yang dibubuhi tanda garis di atasnya atau dikurung persegi. Misalnya:  $[3] = [-2] = [8]$  atau  $3 \equiv -2 \equiv 8 \pmod{5}$  Relasi kekongruenan mempunyai kemiripan sifat dengan sifat persamaan, sebab relasi kekongruenan dapat dinyatakan sebagai persamaan, yaitu  $a \equiv b \pmod{m}$  sama artinya dengan  $a = b + km$  untuk suatu bilangan  $k$ . Misalnya: (

1) jika  $a \equiv b \pmod{m}$  maka  $a + c \equiv b + c \pmod{m}$  untuk setiap bilangan bulat  $c$ . (2) Jika  $a \equiv b \pmod{m}$  maka

15

$a \equiv b \pmod{m}$  untuk setiap bilangan bulat  $c$ . Coba buktikan kedua sifat tersebut! Kemiripan itu akan tampak pula pada teorema berikut ini. Teorema 8.4: Jika  $a \equiv b \pmod{m}$  dan  $c \equiv d \pmod{m}$  maka  $a + c \equiv b + d \pmod{m}$ . Bukti:  $a \equiv b \pmod{m}$  berarti  $a = b + km$  dan  $c \equiv d \pmod{m}$  berarti  $c = d + lm$  untuk suatu bilangan bulat  $k, l$ . Maka  $a + c = b + d + (k + l)m$  sehingga  $a + c \equiv b + d \pmod{m}$ .

$a \equiv b \pmod{m}$  berarti  $a = b + km$  untuk suatu bilangan bulat  $k$ .  $a \equiv b \pmod{m}$  berarti  $a = b + km$  untuk suatu bilangan bulat  $k$ .

3

Dua pasangan ini akan membuktikan bahwa:  $(a + c) + (d + e) = (a + d) + (c + e)$   $(a) - (b) = (a - b)$  Ini berarti  $a \equiv b \pmod{m}$ . Lebih umum teorema 8.4 dinyatakan sebagai teorema berikut ini. Teorema 8.5: Jika  $a \equiv b \pmod{m}$  dan  $c \equiv d \pmod{m}$  maka  $a + c \equiv b + d \pmod{m}$ , untuk setiap bilangan bulat  $a, b, c, d, m$ . Bukti:  $a \equiv b \pmod{m}$  berarti  $a = b + km$  dan  $c \equiv d \pmod{m}$  berarti  $c = d + lm$  untuk suatu bilangan bulat  $k, l$ . Maka  $a + c = b + d + (k + l)m$  sehingga  $a + c \equiv b + d \pmod{m}$ .

untuk suatu bilangan bulat  $a, b, c, d, m$ . Jika kedua ruas persamaan pertama dikalikan dan kedua ruas persamaan kedua dikalikan diperoleh:  $a + c \equiv b + d \pmod{m}$  dan  $a + c \equiv b + d \pmod{m}$  Dengan menjumlahkan ruas persamaan ini diperoleh

30

$a + c \equiv b + d \pmod{m}$   $(a + c) + (d + e) = (a + d) + (c + e)$   $(a) - (b) = (a - b)$  Persamaan terakhir ini berarti bahwa:  $|[(a + c) - (b + d)]|$  atau  $a + c \equiv b + d \pmod{m}$  Pada persamaan/kesamaan bilangan-bilangan bulat berlaku sifat kanselasi (penghapusan) sebagai berikut: jika  $a = b$  dengan  $c \neq 0$  maka  $ac = bc$ .

Apakah dalam kekongruenan berlaku sifat yang mirip dengan sifat kanselasi tersebut? Misalkan, jika  $a \equiv b \pmod{m}$  dengan

23

$a \equiv b \pmod{m}$ , apakah  $a \equiv b \pmod{m}$ ? Ambil sebuah contoh:  $24 \equiv 12 \pmod{4}$  adalah suatu pernyataan yang benar (mengapa?).  $2 \cdot 12 \equiv 2 \cdot 6 \pmod{4}$  dan jelas bahwa  $2 \not\equiv 6 \pmod{4}$  (mod 4). Apakah  $12 \equiv 6 \pmod{4}$ ? Jelas tidak! (mengapa?) Tetapi jika  $3 \cdot 8 \equiv 3 \cdot 4 \pmod{4}$  maka  $8 \equiv 4 \pmod{4}$  adalah suatu pernyataan yang benar. Walaupun sifat kanselasi tidak berlaku sepenuhnya pada relasi kekongruenan, tetapi akan berlaku dengan suatu syarat seperti dinyatakan dalam teorema berikut ini.

Teorema 8.6 Jika  $a \equiv (mod) dengan (, ) = 1$ , maka  $a \equiv (mod)$ . Bukti:  $a \equiv (mod)$  berarti  $a = k(-) atau a = k(-)$ .  $a = k(-)$  dengan  $(, ) = 1$ , maka  $a \equiv (mod)$ . Contoh 8.7:

Tentukanlah bilangan-bilangan bulat yang memenuhi perkongruenan  $3 \equiv$

**1 (mod 7). Jawab** : Karena  $1 \equiv 15 (mod 7)$ , maka kita dapat mengganti 1 pada perkongruenan tersebut dengan 15, sehingga diperoleh

13

$3 \equiv$

**15 (mod 7)** . Selanjutnya, karena  $(3, 7) = 1$  , maka kita dapat **membagi 3 pada ruas-ruas perkongruenan** itu, **sehingga diperoleh**  $5 \equiv (mod 7)$  . Perkongruenan terakhir ini **berarti**

13

$= 5 + 7$  untuk setiap bilangan bulat . atau dapat dikatakan bahwa himpunan penyelesaian dari perkongruenan tersebut adalah  $\{5 + 7 | \text{bilangan bulat}\}$ . Kita dapat menghapus (melenyapkan) suatu faktor dari suatu kekongruenan, jika faktor tersebut dan bilangan modulonya saling prima. Tetapi, jika faktor dan modulonya tidak saling prima, maka kita harus mengganti bilangan modulonya seperti tampak dalam teorema berikut ini. Teorema 8.7: Jika  $a \equiv (mod)$  dengan  $(, ) =$  , maka  $a \equiv (mod)$  . Bukti:  $a \equiv (mod)$  berarti  $a = k(-) atau a = k(-)$

**maka  $(a - b)$ . Karena adalah FPB dari dan , maka dan adalah bilangan-bilangan bulat. Karena  $(, ) =$  maka  $, = 1$ . Karena  $, = 1$  dan  $| (a - b)$  berarti  $\equiv (mod$**

30

Contoh 8.8: Tentukan yang memenuhi  $2 \equiv 4 (mod 6)$ . Jawab:  $2 \equiv 2 \cdot 2 (mod 6)$  karena  $(2, 6) = 2$ , maka  $2 \equiv 2 (mod 3)$ . Jadi nilai-nilai adalah  $(3 + 2)$  untuk setiap bilangan bulat . atau dapat dikatakan bahwa himpunan penyelesaian dari perkongruenan itu adalah  $\{3 + 2 | \text{bilangan bulat}\}$ . 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:  $10.000 - 1 = 9.999 = 9$  sehingga  $10.000 \equiv 1 (1.000 - 1 = 999 = 9$  sehingga  $1.000 \equiv 1 (9)$   $100 - 1 = 99 = 9$  sehingga  $100 \equiv 1 (10 - 1 = 9 = 9$  sehingga  $10 \equiv 1 (9)$  Selanjutnya akan di tunjukkan bahwa

**setiap bilangan bulat kongruen modulo 9 dengan jumlah angka-angkanya. Contoh**

59

8.9  $8.234 \equiv 8000 + 200 + 30 + 4 (mod 9) \equiv 8(1000) + 2(100) + 3(10) + 4($

**$mod 9) \equiv 8 (1) + 2 (1) + 3(1) + 4 (mod 9)$**   $8.234 \equiv 17 (mod 9)$  Selanjutnya **dengan cara yang sama:  $17 \equiv 10 + 7 (mod 9) \equiv 1 + 7$**   $(mod 9)$   $17 \equiv 8 (mod 9)$  Jadi  **$8.234 \equiv 8 (mod 9$**

43

Uraian dan contoh di atas secara umum dinyatakan sebagai teorema-teorema berikut ini. Teorema 8.8:  $10^n \equiv 1 (mod 9)$  untuk  $n = 0, 1, 2, 3, \dots$  Bukti :  $10^n \equiv 1 = 999 \dots 9$  ( $n$  angka semuanya 9) terbagi oleh 9 Jadi  $10^n \equiv 1 (mod 9)$  Teorema 8.9

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

59

Bukti : Ambil sembarang bilangan bulat  $n$  yang angka-angkanya secara berturut-turut adalah:  $n = dk dk-1 dk-2 \dots d_2 d_1 d_0$  atau  $n = dk 10^k + dk-1 10^{k-1} + dk-2 10^{k-2} + \dots + d_2 10^2 + d_1 10 + d_0$  dengan  $0 \leq d_i \leq 9$  untuk  $i = 0, 1, 2, \dots, k$  dan  $dk \neq 0$ . Menurut Teorema 5.8  $10^n \equiv 1 (mod 9)$  untuk  $n = 0, 1, 2, 3, \dots$  sehingga  $n \equiv dk (1) + dk-1 (1) + dk-2 (1) + \dots + d_2 (1) d_1 (1) + d_0 (mod 9)$   $n \equiv dk + dk-1 + dk-2 + \dots + d_2 + d_1 + d_0 (mod 9)$  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  $a \equiv m \pmod{9}$ ,  $b$

61

$\equiv n \pmod{9}$ , dan  $c \equiv p \pmod{9}$ , maka dari  $a + b \equiv c \pmod{9}$  dapat disimpulkan bahwa  $m + n \equiv p \pmod{9}$ . Prinsip tersebut dapat digunakan untuk memeriksa 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:  $248 \equiv$

$$2 + 4 + 8 \pmod{9} \equiv 14 \pmod{9} \equiv 10 + 4 \pmod{9} \equiv 1 + 4 \pmod{9} \equiv 5 \pmod{9}$$

40

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

$$\pmod{9} \equiv 9 \pmod{9} \equiv 0 \pmod{9} \quad 672 \equiv 6 + 7 + 2 \pmod{9} \equiv 15 \pmod{9} \equiv 6 \pmod{9}$$

40

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

$$\pmod{9} \equiv 11 \pmod{9} \equiv 10 + 1 \pmod{9} \equiv 1 + 1 \pmod{9}$$

85

$\equiv 2 \pmod{9}$  .....(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 :  $248 + 324 + 672 = 1244$  ((benar)

**Jika  $a \equiv b \pmod{m}$  dan  $c \equiv d \pmod{m}$ , maka  $ac \equiv bd \pmod{m}$**  ) prinsip ini **dapat**

67

digunakan untuk memeriksa kebenaran suatu perkalian. Contoh 5.11 Berikut  $84 \times 428 = 35.952$ ? Jawab :  $84 \equiv 8 +$

$$4 \pmod{9} \Leftrightarrow 8 + 4 \pmod{9} \equiv 12 \pmod{9} \Leftrightarrow 12 \pmod{9} \equiv 3 \pmod{9}$$

73

$428 \equiv 4 + 2 + 8 \pmod{9} \equiv 14 \pmod{9} \equiv 5 \pmod{9}$  Maka  $84 \times 428 \equiv 3 \times 5 \pmod{9} \equiv 15 \pmod{9} \equiv 6 \pmod{9}$  .....(i) Sedangkan  $35.952 \equiv 3 + 5 + 9 + 5 + 2 \pmod{9} \Leftrightarrow 3 + 5 + 9 + 5 + 2 \equiv 24 \pmod{9} \Leftrightarrow 24 \equiv 20 + 4 \pmod{9} \Leftrightarrow 24 \equiv 2(10) + 4 \pmod{9} \Leftrightarrow 2(10) + 4 \equiv 2(1) + 4 \pmod{9}$

$$\pmod{9} \Leftrightarrow 2(1) + 4 \equiv 2 + 4 \equiv 6 \pmod{9} \Leftrightarrow 24 \equiv 6 \pmod{9}$$

40

..... (ii) Dari (i) dan (ii) bahwa  $84 \times 428 = 35.952$  (benar) Coba buatlah cek dengan pengurangan dan pembagian bilangan-bilangan bulat dan periksalah kebenarannya 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 dalam mengoperasikan kita keliru menjumlah puluhannya, ratusannya atau lainnya. Maka 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**

22

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

22

$\equiv (9)$

jika dan hanya jika dan masing-masing mempunyai sisa yang sama jika dibagi

30

9. Jadi, jika  $n \equiv a \pmod{9}$  maka  $n$

terbagi oleh 9, bila dan hanya bila  $a$  terbagi oleh 9

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

22

. Contoh 8.13 (i)  $7.587 \equiv 7 + 5 + 8 + 7 \equiv 27 \equiv 9 \pmod{9}$   $7.587 \equiv 9 \pmod{9}$  Karena  $9 \mid 9$  maka  $9 \mid 7587$  (ii)  $47.623 \equiv 4 + 7 + 6 + 2 + 3 \equiv 22 \equiv 4 \pmod{9}$  Karena  $9 \nmid 4$  maka  $9 \nmid 47.623$  Apakah suatu bilangan yang terbagi oleh 9 akan terbagi pula

oleh 3? Misalkan  $9 \mid n$  dan  $3 \mid 9$  dengan sifat transitif diperoleh

22

jumlah angka-angkanya terbagi 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

32

. Contoh 8.14 (1)  $12.456 \equiv 1 + 2 + 4 + 5 + 6 \equiv 18 \equiv 9 \pmod{9}$  Karena  $3 \mid 9$  maka  $3 \mid 12.456$ . (2)  $42.641 \equiv 4 + 2 + 6 + 4 + 1 \equiv 17 \equiv 8 \pmod{9}$  Karena  $3 \nmid 8$  maka  $3 \nmid 42.641$ . 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  $n = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$  dengan  $0 \leq a_i \leq 9$  untuk  $i = 0, 1, 2, \dots$

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

36

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 terakhir dari bilangan  $n$ .

Jadi suatu bilangan terbagi oleh 2 bila dan hanya bila angka terakhirnya terbagi oleh 2

22

. Apakah 102, 103, 104, ... masing-masing terbagi oleh 4? Jelas terbagi oleh 4 bukan! (mengapa?) nah, bagaimana menguji suatu bilangan terbagi oleh 4. Misalkan  $n = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$  atau

$$n = a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \dots + a_2 10^2 + a_1 10 + a_0$$

36

Setiap suku pada ruas kanan pada persamaan itu, kecuali dua suku terakhir, yaitu  $a_1 10$  dan  $a_0$ , terbagi oleh 4. Jadi,  $n$  terbagi oleh 4 bila dan hanya bila  $(a_1 10 + a_0)$  terbagi oleh 4. Uraian itu dapat disimpulkan sebagai berikut:

Suatu bilangan terbagi oleh 4 bila dan hanya bila bilangan yang dinyatakan oleh dua angka terakhir dari bilangan itu terbagi oleh 4

9

Contoh 8.15: 5.134.216 terbagi oleh 4, sebab 16 (dua angka terakhir) 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 terakhir dari bilangan itu terbagi oleh 8

9

Contoh 8.16: 17.256 terbagi oleh 8, sebab 256 (tiga angka terakhir) terbagi oleh 8. Nah, sekarang, bagaimana menguji suatu bilangan terbagi oleh 6? Apabila  $2 \mid n$  dan  $3 \mid n$  dan karena  $(2, 3) = 1$ , maka  $6 \mid n$ . 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

9

Selanjutnya dengan mudah pembaca membuktikan bahwa

suatu bilangan terbagi oleh 5 bila dan hanya bila angka terakhir itu adalah 5 atau 0

9

Begitu juga pembaca mudah membuktikan bahwa

suatu bilangan terbagi oleh 10 bila dan hanya bila angka terakhir itu adalah 0

9

Berikut ini dipelajari keterbagian suatu bilangan oleh 11.

$$10 \equiv -1 \pmod{11} \quad 100 \equiv 10 \cdot 10 \equiv (-1)(-1) \equiv 1 \pmod{11} \quad 1000 \equiv 10 \cdot 100 \equiv (-1)(-1)(-1) \equiv -1 \pmod{11}$$

41

dan seterusnya. Sehingga pada umumnya  $10^n \equiv (-1)^n \pmod{11}$  Apabila  $n = a_k a_{k-1} a_{k-2} \dots a_1 a_0$ , dengan  $0 \leq a_i \leq 9$  dan  $a_k \neq 0$ , maka  $\equiv$

$$a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \dots + a_2 10^2 + a_1 10 + a_0 \pmod{11} \equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + a_{k-2} (-1)^{k-2} + \dots + a_2 (-1)^2 + a_1 (-1) + a_0 \pmod{11}$$

45

)  $\equiv$

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

36

$11) \equiv ((a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots)) \pmod{11}$   $a_1, a_3, a_5, \dots$  berturut-turut adalah ke 2, ke 4, ke 6, ... pada bilangan  $n$  dari belakang dan  $a_0, a_2, a_4, \dots$  berturut-turut adalah angka ke 1, ke 3, ke 5, ... pada bilangan  $n$  dari belakang. Jadi

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

9

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 2050 dibagi 7?  $20 \equiv -1 \pmod{7}$   $2050 \equiv (-1)50 \pmod{7}$   $2050 \equiv 1 \pmod{7}$  Jadi 2050 : 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  $\equiv 0 \pmod{4}$ , dan jika adalah sebuah bilangan bulat ganjil, maka**

50

$\equiv 1 \pmod{4}$  ! 2. Tunjukkan bahwa jika adalah sebuah bilangan bulat ganjil, maka  $\equiv 1 \pmod{8}$  ! 3. Tunjukkan bahwa jika  $m = a$ , dan adalah bilangan bulat dengan  $90$  dan  $\equiv 1 \pmod{9}$ , 4. Tunjukkan bahwa jika  $a > 0$ ,  $b$ , dan  $\equiv c \pmod{m}$ , dan adalah bilangan bulat sedemikian sehingga  $am \equiv b \pmod{m}$ , maka  $\equiv c \pmod{m}$  !  $> 0$ , 5. Tunjukkan bahwa jika  $a, b$ , dan adalah bilangan bulat sedemikian sehingga  $a > 0$ , dan  $\equiv b \pmod{m}$ , maka  $\equiv c \pmod{m}$  !  $> 0$ , 6. Show that jika  $a, b$ , dan adalah bilangan bulat dengan  $a > 0$  sedemikian sehingga  $\equiv b \pmod{m}$ , maka  $\equiv c \pmod{m}$  ! 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:  $3 \equiv 4 \pmod{5} + 3 - 3 \equiv 0 \pmod{31}$  Jika suatu pengkongruenan,

**variabelnya berpangkat paling tinggi satu** disebut perkongruenan linier. **Bentuk umum perkongruenan linier adalah  $ax \equiv b \pmod{m}$** , dengan

13

$\equiv 0 \pmod{m}$

). Perhatikan perkongruenan linier  $3x \equiv 4 \pmod{5}$

**5). Apabila diganti 3 memberikan  $3 \cdot 3 \equiv 4 \pmod{5}$  atau  $9 \equiv 4 \pmod{5}$ . Yaitu suatu kalimat kekongruenan yang benar. Begitu pula jika diganti berturut-turut oleh  $\dots -7, -2, 8, 13, \dots$  akan memberikan kalimat -kalimat kekongruenan yang benar**

10

. (coba periksalah!) Kita telah mengerti bahwa  $\equiv c \pmod{m}$  berarti  $- =$  atau  $= +$ , untuk suatu bilangan bulat  $m$ . Jadi perkongruenan linier  $\equiv c \pmod{m}$

**akan mempunyai solusi (penyelesaian) bila dan hanya bila ada bilangan -bilangan bulat dan yang memenuhi persamaan.  $ax - =$**

11

**Misalkan memenuhi perkongruenan linier**

$\equiv c \pmod{m}$ , berarti  $\equiv c \pmod{m}$ . Maka setiap bilangan bulat  $(+), (+2), (+3), \dots (-), (-2), (-3), \dots$  memenuhi perkongruenan itu, sebab  $(+) \equiv c \pmod{m}$ ,

**untuk setiap bilangan bulat. Diantara bilangan-bilangan bulat  $(r + km)$ , dengan  $k = 1, 2, 3, 4, \dots -1, -2, -3, \dots$  ada tepat satu dan hanya satu, katakan dengan  $0 \leq s < m$ , sebab suatu bilangan bulat mesti terletak di antara dua kelipatan yang berurutan. Jadi, jika memenuhi perkongruenan**

10

$\equiv c \pmod{m}$  dan  $0 \leq s < m$  untuk suatu bilangan bulat  $m$ , maka  $0 \leq (-) < m$ . Jadi  $= -$



untuk suatu bilangan bulat . Dengan kata lain, adalah residu terkecil modulo m yang memenuhi perkongruenan

11

$\equiv ()$ . Selanjutnya s disebut solusi (penyelesaian) dari perkongruenan itu. Contoh 9.1: Nilai-nilai yang memenuhi perkongruenan  $2 \equiv 4 ()$

7) adalah ... -19, -12, -5, 2, 9, 16, ... Solusi dari perkongruenan itu adalah 2, yaitu residu terkecil modulo 7 yang memenuhi perkongruenan linier

10

$2 \equiv 4 (7)$ . Pada persamaan  $\equiv$ , dengan  $\neq 0$  hanya mempunyai satu solusi, tetapi pada perkongruenan linier  $\equiv ()$  dapat mempunyai tepat satu solusi, banyak solusi, bahkan bisa tidak mempunyai solusi. Pada contoh di atas  $2 \equiv 4 (7)$  mempunyai tepat satu solusi, yaitu 2. Perkongruenan linier  $2 \equiv 1 (4)$  tidak mempunyai solusi, sebab  $4 \nmid (2 + 1)$ , yaitu tak ada bilangan bulat sedemikian  $2 - 1$  terbagi oleh 4 (mengapa?). Sedangkan perkongruenan linier  $2 \equiv 4 (6)$  mempunyai dua solusi, yaitu 2 dan 5. (coba periksa kebenarannya!). selanjutnya, akan kita pelajari cara menguji suatu perkongruenan linier mempunyai solusi atau tidak. Teorema 9.1: Jika  $(, )$  maka perkongruenan linier  $\equiv ()$  tidak memiliki solusi. Bukti : Kita buktikan kontraposisi dari teorema itu,

yaitu jika  $\equiv ()$  memiliki solusi maka  $(, ) \mid$ . Misalkan adalah solusi dari  $\equiv ()$  maka  $\equiv ()$  sehingga  $- =$  untuk suatu bilangan bulat . Perhatikan  $- =$ , karena  $(, ) \mid$  dan  $(, ) \mid$ , maka  $(, ) \mid$ . Terbuktilah kontraposisi dari teorema itu, sehingga terbukti pula teorema itu.

Contoh

5

9.2:  $6 \equiv 7 (8)$ ,

karena  $(6, 2) = 2$  dan  $2 \nmid 7$  maka perkongruenan linier

10

$6 \equiv 7 (8)$  tidak mempunyai solusi. Teorema 9.2: Jika  $(, ) = 1$ , maka perkongruenan linier  $\equiv ()$  memiliki tepat satu solusi.

Bukti : Karena  $(, ) = 1$  maka ada bilangan bulat dan sehingga  $+ = 1$ . Jika kedua ruas dari persamaan ini dikaitkan, diperoleh :  $( ) + ( ) ( ) + ( ) = ( ) - = - ( )$  Persamaan terakhir ini berarti bahwa  $( ) -$  Jadi  $( ) \equiv ( )$  adalah kelipatan . Maka residu terkecil dari  $rb$  modulo  $m$  adalah solusi dari perkongruenan linier itu. Selanjutnya tinggal menunjukkan bahwa solusi itu tunggal

5

andalkan solusi perkongruenan

linier itu tidak tunggal, misalkan dan masing-masing solusi dari  $\equiv ()$ , maka  $\equiv ()$  dan  $\equiv ()$  (dengan sifat transitif di peroleh : Karena  $(, ) = 1$ , maka  $\equiv () =$ ). Ini berarti  $(- )$ . Tetapi karena dan adalah solusi dari perkongruenan itu, maka dan masing-masing residu terkecil modulo  $m$ , sehingga  $0 \leq < dan  $0 \leq <$ . Dari kedua ketidaksamaan ini diperoleh bahwa  $- < - <$ , tetapi karena  $(- )$  maka  $- = 0$  atau  $=$  Ini berarti bahwa solusi dari perkongruenan linier tunggal (terbukti). Salah satu cara menyelesaikan perkongruenan linier adalah memanipulasi koefisien atau konstanta pada perkongruenan itu, sehingga memungkinkan kita untuk melakukan kanselasi (penghapusan). Contoh 9.3: (1) Selesaikan  $4 \equiv 1 (15)$  Jawab$

5

$4 \equiv 1 (15)$   $4 \equiv 16 (15) \equiv 4 (15)$  Karena  $(4, 15) = 1$  maka memungkinkan kita melakukan kanselasi 4 pada perkongruenan  $4 \equiv 16 (4 \equiv 1 (15))$  sehingga di peroleh  $\equiv 4 (15)$  adalah 4. 15). Solusi dari perkongruenan (2) Selesaikan  $14 \equiv 27 (31)$  Jawab :  $14 \equiv 27 (31) \Leftrightarrow 14 \equiv 58 (31) \Leftrightarrow 7 \equiv 29 (31) \Leftrightarrow 7 \equiv 91 (31) \Leftrightarrow \equiv 13 (31)$  Karena  $27 \equiv 58 (31)$  maka  $14 \equiv 58 (31)$ . Karena  $(2, 31) = 1$ , kita dapat menghapus 2 pada perkongruenan  $14 \equiv 58 (31)$  dan di peroleh  $7 \equiv 29 (31)$ . Selanjutnya  $7 \equiv 91 (31)$ , sebab  $29 \equiv 91 (31) \equiv 13 (31)$ , sebab  $(7, 31) = 1$  Jadi, 13 adalah solusi  $4 \equiv 24 (31)$ . Sesuai teorema 5.11 di atas, jika  $(, ) = 1$ , maka perkongruenan  $\equiv 1()$  mempunyai tepat satu solusi pula. Solusi perkongruenan itu disebut invers dari a modulo m yang diberi simbol . Contoh 9.4: Carilah 2 (31). Jawab : Untuk mencari 2 (31), kita perlu menyelesaikan perkongruenan  $2 \equiv 1 (31)$ .  $2 \equiv 1 (31)$   $2 \equiv 14 (31) \equiv 7 (31)$  Jadi 2 (31) adalah 7. Periksalah bahwa  $3 \cdot 1 \pmod{31}$  adalah 9,  $4 \cdot 1 \pmod{31}$  adalah 10,  $5 \cdot 1 \pmod{31}$  adalah 8,  $6 \cdot 1 \pmod{31}$  adalah 11, dan  $12 \cdot 1 \pmod{31}$  adalah 12. Berikut ini akan dipelajari

banyaknya solusi dari  $ax \equiv b \pmod{m}$ , apabila  $(a, m) = d$  dan  $d \mid b$  dengan  $d > 1$ . Teorema 9.3: Jika  $(a, m) = d$  dan  $d \mid b$  maka perkongruenan linier  $ax \equiv b \pmod{m}$  memiliki tepat solusi. Bukti : Kita harus membuktikan bahwa perkongruenan linier  $ax \equiv b \pmod{m}$  memiliki solusi. Dan seterusnya harus ditunjukkan bahwa tak ada solusi lain kecuali solusi itu. Sekarang akan dibuktikan bahwa perkongruenan linier itu memiliki solusi.  $(a, m) = d$  berarti ada  $a'$  dan  $m'$  sehingga  $a = a'd$  dan  $m = m'd$ .  $b = b'$  berarti ada  $b'$  sehingga  $b = b'd$ . Sehingga dari  $ax \equiv b \pmod{m}$  memberikan  $a'x \equiv b' \pmod{m'}$  atau Dari  $(a', m') = 1$  Menurut Teorema 9.1, jika  $(a', m') = 1$ , maka  $a'x \equiv b' \pmod{m'}$  memiliki satu solusi. Misalkan solusi itu  $x_0$ , maka buah bilangan, yaitu  $x_0 + m', x_0 + 2m', \dots, x_0 + (m')m'$  atau  $x_0 + km'$  untuk  $k = 0, 1, 2, \dots, (m') - 1$  memenuhi perkongruenan  $ax \equiv b \pmod{m}$ . Hal ini ditunjukkan sebagai berikut. Pertama, setiap  $x_0 + km'$  dengan  $k = 0, 1, 2, \dots, (m') - 1$  memenuhi perkongruenan Karena  $a'x_0 \equiv b' \pmod{m'}$  ( $= a'(x_0 + km') \equiv a'x_0 + a'km' \equiv b' + km'a'd \equiv b' + km'b' \equiv b' \pmod{m'}$ ) (mengapa?)  $= b'$  Jadi  $x_0 + km'$  untuk  $k = 0, 1, 2, \dots, (m') - 1$  memenuhi perkongruenan  $ax \equiv b \pmod{m}$ . Kedua, setiap  $x_0 + km'$  dengan  $k = 0, 1, 2, \dots, (m') - 1$  adalah residu terkecil modulo  $m$ . Ditunjukkan sebagai berikut : adalah solusi dari  $x_0 + km' \leq x_0 + (k+1)m' < x_0 + (k+2)m'$  berarti  $(k+1)m' \leq x_0 + (k+1)m' < x_0 + (k+2)m'$  untuk setiap  $x_0 + (k+1)m' \geq 0$  sehingga  $0 \leq km' < m$ ,  $2, \dots, (m') - 1$ .  $x_0 + km'$  Jadi,  $0 \leq x_0 + km' < m$  Hal ini menunjukkan bahwa terkecil modulo  $m$ .  $x_0 + km'$  untuk  $k = 0, 1, 2, \dots, (m') - 1$  adalah residu-residu Ketiga, tak ada dua bilangan dari  $x_0 + km'$  untuk  $k = 0, 1, 2, \dots, (m') - 1$  yang kongruen modulo  $m$  yang berbeda. Sampai disini telah ditunjukkan bahwa perkongruenan linier  $ax \equiv b \pmod{m}$  memiliki buah solusi. Nah, sekarang tinggal menunjukkan bahwa tak ada solusi lain, kecuali  $d$  buah solusi itu. Tadi diambil bahwa adalah solusi dari perkongruenan linier  $ax \equiv b \pmod{m}$ . Misalkan adalah solusi lain, maka  $ax_1 \equiv b \pmod{m}$  (Jadi,  $ax_1 \equiv b \pmod{m}$  Karena  $(a, m) = d$  dan  $d \mid b$ ).  $ax_1 \equiv b \pmod{m}$  dan  $ax_0 \equiv b \pmod{m}$  di peroleh bahwa  $d(x_1 - x_0) \equiv 0 \pmod{m}$  karena  $a = a'd$  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  $k = 0, 1, 2, \dots, (m') - 1$ . Maka  $s = r + km'$  adalah salah satu di antara  $r + km'$ . Jadi tak ada solusi lain, kecuali buah solusi, yaitu  $x_0 + km'$  dengan  $k = 0, 1, 2, \dots, (m') - 1$ . Lengkaplah bukti teorema itu.

Contoh 9.5: Selesaikan  $6x \equiv 15 \pmod{33}$  Jawab : Karena  $(6, 33) = 3$ , maka perkongruenan ini memiliki 3 solusi.  $6x \equiv 15 \pmod{33} \iff 2x \equiv 5 \pmod{11}$   $2x \equiv 16 \pmod{11}$  mengapa ?  $\iff 8 \pmod{11}$  Maka bilangan-bilangan bulat positif yang memenuhi  $2x \equiv 8 \pmod{11}$  dan merupakan residu terkecil modulo 33 adalah 8, 19 dan 30. Jadi solusi-solusi dari  $6x \equiv 15 \pmod{33}$  adalah 8, 19 dan 30. Kita telah mengenal fungsi linier  $ax + by = c$  dengan  $a, b, c$  menyatakan bilangan-bilangan riil. Dengan kata lain, fungsi linier itu diselesaikan dalam domain (himpunan semesta) himpunan bilangan riil. Apabila domainnya di persempit, yaitu himpunan bilangan bulat, maka persamaan  $ax + by = c$  dengan  $a, b, c$  dan bilangan-bilangan bulat disebut Persamaan Linier Diophantus. Persamaan  $ax + by = c$  berarti  $ax \equiv c - by \pmod{m}$ . Dapat pula bahwa  $ax + by = c$  berarti  $ax \equiv c - by \pmod{m}$ . Oleh karena itu, untuk menyelesaikan persamaan  $ax + by = c$  dengan  $a, b, c$  dan bilangan-bilangan bulat, kita dapat menyelesaikan salah satu perkongruenan.  $ax \equiv c - by \pmod{m}$ . 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  $9x + 16y = 35$ .  $9x + 16y = 35 \iff 9x \equiv 35 - 16y \pmod{9}$   $9x \equiv 5 \pmod{9}$  Berarti  $5 + 9$  untuk suatu bilangan bulat. Nilai ini disubstitusikan pada  $9x + 16y = 35$  memberikan  $9x + 16(5 + 9) = 35 \iff 9x + 144 = -45 \iff 9x + 16 = -5 \iff -5 - 16$  Sehingga himpunan penyelesaian dari  $9x + 16y = 35$  adalah  $\{(x, y) \mid x = -5 - 16t, y = 5 + 9t \text{ dan bilangan bulat}\}$  Jika  $t = 0$ , maka  $(-5, 5)$  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  $ax + by = c$ , maka solusi-solusi lainnya adalah  $(x_0 + bt, y_0 - at)$  untuk setiap bilangan bulat  $t$ . Coba buktikanlah pernyataan itu! Apakah setiap persamaan linier Diophantus  $ax + by = c$  mesti memiliki solusi? Ingat bahwa  $ax + by = c$  sama artinya dengan  $ax \equiv c - by \pmod{m}$  atau  $ax \equiv c - by \pmod{m}$ . Kedua perkongruenan ini akan mempunyai solusi, jika  $(a, m) \mid c - by$ , dan perkongruenan itu tidak mempunyai solusi apabila  $(a, m) \nmid c - by$ . Jadi, dapat disimpulkan bahwa: (1) Persamaan Linier Diophantus  $ax + by = c$  dengan  $c \neq 0$  tidak mempunyai penyelesaian, jika  $(a, m) \nmid c - by$ . (2) Persamaan Linier Diophantus  $ax + by = c$  dengan  $c = 0$  mempunyai penyelesaian, jika  $(a, m) \mid c - by$ . 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  $x = 5 - 4t$  untuk setiap bilangan bulat maka  $(5 - 4t) + 4t = 5$  adalah suatu bilangan ganjil (Mengapa?). Sehingga  $2x + 4y = 5$  tidak akan menyatakan bilangan bulat untuk setiap bilangan bulat  $t$ . Contoh 9.8: Jika  $7x + 15y = 51$  dan menyatakan bilangan-bilangan bulat positif, selesaikanlah  $7x + 15y = 51$ . Jawab:  $7x + 15y = 51$  berarti  $7x \equiv 51 - 15y \pmod{7}$   $7x \equiv 17 - 15y \pmod{7}$   $7x \equiv 10 - 15y \pmod{7}$   $7x \equiv 2 - 15y \pmod{7}$  Jadi  $2 - 15y$  dengan bilangan cacah (Mengapa bilangan cacah?) Subtitusikan nilai pada persamaan semula, sehingga diperoleh  $7x + 15(2 - 15y) = 51$   $7x + 105 - 225y = 51$   $7x - 225y = -54$  Karena bilangan bulat positif dan bilangan cacah, maka  $y = 3$ , yaitu untuk  $y = 0$ , sehingga  $x = 2$ . Jadi bilangan-bilangan bulat positif dan 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  $2x \equiv 20 - 6y \pmod{2}$   $2x \equiv 10 - 6y \pmod{2}$   $2x \equiv 1 - 6y \pmod{2}$  Berarti  $1 - 6y$  dengan bilangan bulat. Subtitusi  $1 - 6y$  pada dalam  $2x + 6y = 20$ .  $2(1 - 6y) + 6y = 20$   $2 - 12y + 6y = 20$   $2 - 6y = 18$   $-6y = 16$   $y = -\frac{8}{3}$ . Himpunan penyelesaian dari  $2x + 6y = 20$  adalah  $\{(x, y) \mid x = -1 + 3t, y = -\frac{8}{3} - 2t, \text{ bilangan bulat}\}$  Apakah  $x = -1 + 3t$  dan  $y = -\frac{8}{3} - 2t$ , dengan suatu bilangan bulat juga merupakan penyelesaian dari persamaan itu? Bandingkan hasil penyelesaian persamaan  $2x + 6y = 20$  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  $a' = a/d$  :  $(a, b)$ , dengan  $b' = b/d$  :  $(a, b)$  dan  $c' = c/d$

49

$(a, b)$  mempunyai suatu penyelesaian (solusi)  $x = r$  dan  $y = s$ , maka himpunan semua penyelesaian dari  $ax + by = c$  adalah  $\{(x, y) \mid x = r + b't, y = s + a't, t \text{ bilangan bulat}\}$ . 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**

32

7. Jika bilangan bulat yang dicari dimisalkan  $x$ , maka kalimat dalam masalah itu dapat dinyatakan sebagai berikut:  $\equiv 2(3), \equiv 4(5), \equiv 6(7)$ . Apakah bilangan bulat yang dicari itu adalah 104? Adakah bilangan lain yang masih memenuhi? Untuk menjawab pertanyaan ini, ikutilah uraian berikut ini: Dari perkongruenan pertama  $\equiv 2(3)$  berarti  $x = 2 + 3k_1$ , untuk suatu bilangan bulat  $k_1$ . Substitusikan nilai  $x$  itu dalam perkongruenan kedua 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  $k_2$ . Substitusikan nilai  $k_1$  ini dalam persamaan  $x = 2 + 3k_1$  sehingga diperoleh:  $= 2 + 3(4 + 5k_2) = 14 + 15k_2$ . Substitusikan nilai ini dalam perkongruenan ketiga dan diperoleh:  $14 + 15k_2 \equiv 6 \pmod{7}$   $15k_2 \equiv -8 \pmod{7}$   $2k_2 \equiv -1 \pmod{7}$   $2k_2 \equiv 6 \pmod{7}$  Hal ini berarti  $k_2 = 6 + 7t$  untuk suatu bilangan bulat  $t$ . Substitusikan nilai 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 perkongruenan (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

$$x \equiv a_i \pmod{m_i}, i = 1, 2, 3, \dots, k \text{ dengan } (m_i, m_j) = 1 \text{ untuk setiap } i \neq j$$

44

memiliki solusi bersama modulo  $m$  dan solusi bersama itu tunggal dengan  $m = m_1, m_2, m_3, \dots, m_k$ . Bukti: Pembuktian dengan induksi matematik untuk bilangan asli. Untuk  $k = 1$  berarti  $x \equiv a_1 \pmod{m_1}$  jelas mempunyai solusi. Untuk  $k = 2$  berarti

$$x \equiv a_1 \pmod{m_1} \text{ dan } x \equiv a_2 \pmod{m_2} \text{ dengan } (m_1, m_2) = 1$$

56

, 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  $x = a_1 + k_1m_1 = a_1 + (t + k_2m_2)m_1$   $x = (a_1 + tm_1) + k_2m_2m_1$  ini berarti  $x \equiv (a_1 + tm_1) \pmod{m_1m_2}$ . 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  $i = 1, 2, 3, \dots, (r - 1)$ . Misalkan solusi bersama itu  $s$ , maka  $x \equiv a_i \pmod{m_i}, i = 1, 2, 3, \dots, (r - 1)$  dapat dinyatakan sebagai suatu perkongruenan, yaitu:  $x \equiv s \pmod{m_1m_2m_3 \dots m_{r-1}}$   $x \equiv a_r \pmod{m_r}$ . Sistem perkongruenan dari dua perkongruenan ini mempunyai solusi bersama mod  $(m_1m_2m_3 \dots m_{r-1})$  karena  $(m_r, m_1m_2m_3 \dots m_{r-1}) = 1$  sebab  $m_i$  dan  $m_j$  saling prima untuk  $i \neq j$ . Nah! Terbuktilah bahwa

$$\text{sistem perkongruenan } x \equiv a_i \pmod{m_i} \text{ untuk } i = 1, 2, 3, \dots, k \text{ mempunyai solusi bersama modulo } (m_1m_2m_3 \dots m_r)$$

26

$\dots m_r$ ). Selanjutnya tinggal membuktikan

$$\text{bahwa solusi itu tunggal. Misalkan } r \text{ dan } s \text{ adalah solusi -solusi bersama dari sistem tersebut, maka: } r \equiv a_i \pmod{m_i} \text{ dan } s \equiv a_i \pmod{m_i}$$

11

$s \equiv a_i \pmod{m_i}$  sehingga  $(r - s) \equiv 0 \pmod{m_i}$ . Ini berarti bahwa  $m_i \mid (r - s)$  untuk setiap  $i = 1, 2, 3, \dots, k$ . Jadi  $(r - s)$  suatu bilangan kelipatan persekutuan dari  $m_1, m_2, m_3, \dots, m_k$ . karena  $(m_i, m_j) = 1$  untuk setiap  $i \neq j$ , maka  $(m_1m_2m_3 \dots m_k) \mid (r - s)$ . Tetapi ingat bahwa  $r$  maupun  $s$

$$r - s \text{ untuk setiap } i = 1, 2, 3, \dots, k. \text{ Jadi } (r - s) \text{ suatu bilangan kelipatan persekutuan dari } m_1, m_2, m_3, \dots, m_k.$$

11

$$m_1m_2m_3 \dots m_k. \text{ karena } (m_i, m_j) = 1 \text{ untuk setiap } i \neq j, \text{ maka } (m_1m_2m_3 \dots m_k) \mid (r - s).$$

26

$(m_1m_2m_3 \dots m_k) \mid (r - s)$ . Tetapi ingat bahwa  $r$  maupun  $s$

$$\text{adalah solusi-solusi perkongruenan, berarti } r \text{ dan } s \text{ adalah residu -residu terkecil modulo } (m_1m_2m_3 \dots m_k) \text{ sehingga } (m_1m_2m_3 \dots m_k) < r - s < (m_1m_2m_3 \dots m_k). \text{ Mengingat } r - s \text{ adalah kelipatan persekutuan dari } m_1m_2m_3 \dots m_k$$

26

dan  $(m_i, m_j) = 1$  untuk setiap  $i \neq j$ . Dapat disimpulkan bahwa:  $r - s = 0$  atau  $r = s$ . Jadi solusi bersama dari sistem  $x \equiv a_i \pmod{m_i}$  untuk  $i = 1, 2, 3, \dots, k$  adalah tunggal. Catatan:  $(m_i, m_j) = 1$

untuk setiap  $i \neq j$  dengan  $i, j = 1, 2, 4, \dots, k$ , dikatakan  $m_1, m_2, m_3, \dots, m_k$  saling prima dua-dua. Contoh 5.27: Tentukan solusi sistem perkongruenan

$$x \equiv 2 \pmod{3} \quad (i) \quad x \equiv 3 \pmod{5} \quad x \equiv 1 \pmod{4}$$

77

) Sebelum menyelesaikan contoh tersebut, ditulis suatu teorema yang memudahkan kita dalam menyelesaikan sistem perkongruenan, yaitu: misalkan sistem (i)

$$x \equiv a_i \pmod{m_i} \quad \text{untuk} \quad i = 1, 2, 3, \dots, k \quad \text{dengan} \quad (m_i, m_j) = 1, j$$

44

$= 1, 2, 3, \dots, k$ ;

$i = 1, 2, 3, \dots, k$  dan  $M_i = (m_1, m_2, m_3, \dots, m_k) : m_i$ , untuk  $i = 1, 2, 3, \dots, k$  dan  $s_i$  adalah solusi  $M_i x \equiv 1 \pmod{m_i}$ ,  $i = 1, 2, 3, \dots, k$ . Maka  $s = a_1 s_1 M_1 + a_2 s_2 M_2 + \dots + a_k s_k M_k$  memenuhi sistem (i). Sehingga solusi bersama dari sistem (i) adalah solusi dari  $x \equiv s \pmod{m_1, m_2, m_3, \dots, m_k}$ . Pada contoh soal  $a_1 = m_1$  diatas  $2 = 3, a_2 = m_2, 3 = 5, a_3 = m_3, 1 = 4, M_1 = 5 \cdot 4 = 20$ , sehi  $20x \equiv 1 \pmod{3}$  a ngg  $(\text{mod } 3)$  t a a  $x \equiv 2 \pmod{3}$   $M_2 = 3 \cdot 4 = 12$ , sehi ngg a  $12x \equiv 1 \pmod{5}$   $M_3 = 3 \cdot 5 = 15$ , sehi  $15x \equiv 1 \pmod{4}$  a u A t a u a t a u  $x \equiv 3 \pmod{5}$   $x \equiv 3 \pmod{4}$  Maka  $s = a_1 s_1 M_1 + a_2 s_2 M_2 + a_3 s_3 M_3 = 2 \cdot 2 \cdot 20 + 3 \cdot 3 \cdot 12 + 1 \cdot 3 \cdot 15 = 197$  Maka sistem perkongruenan diatas dapat dinyatakan sebagai  $x \equiv 197 \pmod{3 \cdot 5 \cdot 4} \equiv 197 \pmod{60} \equiv 17 \pmod{60}$  H.4. Latihan Kegiatan Belajar 8 Selesaikan soal-soal berikut ini dengan benar! 1. Tentukan semua solusi dari setiap kekongruenan linear berikut! a.  $2 \equiv 5 \pmod{7}$  b.  $3 \equiv 6 \pmod{9}$  2. Tentukan semua solusi dari setiap kekongruenan linear berikut! a.  $17 \equiv 14 \pmod{21}$  b.  $15 \equiv 9 \pmod{25}$  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 mengamplifikasikan 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  $(a, m) = 1$ , maka residu-residu terkecil modulo  $m$  dari barisan:  $a, 2a, 3a, \dots, (m-1)a$

adalah suatu permutasi dari  $1, 2, 3, \dots, (m-1)$ . Dengan perkataan lain, teorema 6.1 dapat dikatakan bahwa jika

1

$(a, m) =$

1, maka setiap bilangan bulat kongruen modulo  $m$  dengan tepat satu dari 0

1

$a, 2a, 3a, \dots, (m-1)a$ . Ingat bahwa

setiap bilangan bulat akan kongruen modulo  $m$  dengan tepat satu dari  $0, 1, 2, 3$

2

$4, \dots, (-1)$ . Bukti teorema 6.1: Perhatikan barisan bilangan:  $1, 2, 3, \dots, (-1)$  . . . . . (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** . . . . .  $(-1)$ . **Andaikan ada dua suku dari barisan** (1) **yang kongruen modulo  $m$ , misalnya:  $a \equiv b \pmod{m}$  dengan**  $1 \leq r < s < m$  . Karena  $(a - b) = 1$ , **maka kita dapat**

1

melenyapkan dari kekongruenan itu, sehingga diperoleh  $a - b = 1$

**Tetapi, karena  $a$  dan  $b$  adalah suku-suku dari barisan** (1), **maka  $r$  dan  $s$  adalah** residu-residu **terkecil modulo  $m$ , sehingga  $a - b = 1$ . Hal ini** **kontradiksi dengan pengandaian bahwa**  $1 \leq r < s < m$ , 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-masing** **kongruen modulo  $m$  dengan tepat satu dari** **1,2,3**

1

$1, 2, 3, \dots, (-1)$ . Perhatikan barisan bilangan: 4, 8, 12, 16, 20, 24. Residu-residu terkecil mod 7 dari masing-masing suku dari barisan ini adalah:  $4 \equiv 4 \pmod{7}$   $8 \equiv 1 \pmod{7}$   $12 \equiv 5 \pmod{7}$   $16 \equiv 2 \pmod{7}$   $20 \equiv 6 \pmod{7}$   $24 \equiv 3 \pmod{7}$  Tampak pada enam kekongruenan tersebut bahwa residu-residu terkecil modulo 7 dari suku-suku pada barisan: 4, 8, 12, 16, 20, 24 adalah suatu permutasi 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:  $4 \cdot 8 \cdot 12 \cdot 16 \cdot 20 \cdot 24 \equiv 3 \cdot 1 \cdot 5 \cdot 2 \cdot 6 \cdot 3 \pmod{7}$   $4(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7} \Leftrightarrow 4 \cdot 6! \equiv 6! \pmod{7} \Leftrightarrow 4 \equiv 1 \pmod{7}$  Dengan cara seperti itu, cobalah tunjukkan bahwa: a)  $5 \equiv 1 \pmod{7}$  b)  $3 \equiv 1 \pmod{11}$  c)  $4 \equiv 1 \pmod{13}$  d)  $8 \equiv 1 \pmod{5}$  e)  $13 \equiv 1 \pmod{17}$  Contoh-contoh tersebut merupakan penerapan dari teorema Fermat berikut ini: Teorema 10.2: (Teorema Fermat) Jika suatu bilangan prima dan  $(a, p) = 1$ , maka  $a^{p-1} \equiv 1 \pmod{p}$

**1(mod p) Bukti: Ambil sembarang bilangan prima  $p$  dan bilangan bulat  $a$  sedemikian**

13

$(a, p) = 1$ , maka menurut Teorema 6.1, residu-residu terkecil mod  $p$  dari  $a, 2a, 3a, \dots, (p-1)a$

**adalah suatu permutasi dari  $1, 2, 3, \dots, (p-1)$ , sehingga hasil kali-hasil kalinya akan kongruen mod  $p$  juga, yaitu**

13

$a, 2a, 3a, \dots, (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$   $(1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)) \equiv (p-1)! \pmod{p}$  Karena dan  $(p-1)!$  Saling rima (mengapa?), maka kita dapat melenyapkan  $(p-1)!$  Dari kekongruenan terakhir ini, sehingga diperoleh  $a^{p-1} \equiv 1 \pmod{p}$ . Contoh 10.1: Tunjukkan bahwa jika  $(3,7) = 1$ , maka  $3^6 \equiv 1 \pmod{7}$  ! Jawab: Menurut teorema Fermat, Diketahui  $p = 7$  and  $a = 3$ . Sehingga,  $1 \cdot 3 \equiv 3 \pmod{7}$ ,  $2 \cdot 3 \equiv 6 \pmod{7}$ ,  $3 \cdot 3 \equiv 2 \pmod{7}$ ,  $4 \cdot 3 \equiv 5 \pmod{7}$ ,  $5 \cdot 3 \equiv 4 \pmod{7}$ , dan  $6 \cdot 3 \equiv 1 \pmod{7}$ . Akibatnya  $(1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot 3) \cdot (6 \cdot 3) \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod{7}$   $3 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod{7}$   $3 \cdot 6! \equiv 6! \pmod{7} \Leftrightarrow 3 \equiv 1 \pmod{7} \Leftrightarrow 3^6 \equiv 1 \pmod{7}$  (terbukti) Teorema Fermat tersebut dapat dinyatakan lebih umum dengan meniadakan ketentuan  $(a, p) = 1$  sebagai berikut: Teorema 10.3: Jika suatu bilangan prima, maka  $a^p \equiv a \pmod{p}$ , untuk setiap

**bilangan bulat . Bukti: Ambil sembarang bilangan prima dan sembarang bilat  $a$ , maka**

1

$(a, p) = 1$  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  $a^{p-1} \equiv 1 \pmod{p}$ . Selanjutnya, jika kedua ruas dikalikan  $a$ , maka  $a^p \equiv a \pmod{p}$ , sehingga  $a^p - a \equiv 0 \pmod{p}$  (Jadi,  $a^p \equiv a \pmod{p}$ ) dan  $a^p \equiv a \pmod{p}$  pula. Bukti lain dari teorema 6.3 dengan menggunakan induksi matematika pada  $a$ . Jika  $a = 1$ , maka pernyataan  $1^p \equiv 1 \pmod{p}$  jelas benar. Demikian pula, jika diambil  $a = 0$ . Selanjutnya diasumsikan  $a \equiv b \pmod{p}$

benar untuk suatu bilangan bulat positif  $a$ , dan harus ditunjukkan benar untuk  $(+1)$ , yaitu  $(+1)$

1

$\equiv +1$ . Hal ini ditunjukkan sebagai berikut: Menurut teorema binomial, maka: Ingat bahwa  $(+1) = \sum_{k=0}^n \binom{n}{k} (+1)^k = \sum_{k=0}^n \binom{n}{k} = 2^n$ , karena suatu bilangan prima, maka  $n$  berarti  $\equiv 0$  untuk  $1 \leq k < n$ . Jadi kita memperoleh bahwa:  $(+1) = \sum_{k=0}^n \binom{n}{k} = 1 + \sum_{k=1}^{n-1} \binom{n}{k} + 1$ . Karena  $\binom{n}{k} \equiv \binom{n}{n-k}$ , maka  $(+1) = 1 + \sum_{k=1}^{n-1} \binom{n}{k} + 1$ . Dengan induksi matematik pada kita telah membuktikan bahwa  $\equiv$  untuk setia bilangan asli.

Selanjutnya jika  $a$  suatu bilangan bulat negatif, bukan lagi menjadi persoalan, sebab untuk setiap bilangan bulat negatif  $a$  berlaku bahwa

1

$\equiv$  dengan  $0 < -1$ . Jadi,  $\equiv \equiv$ .

**Teorema Fermat mempunyai banyak kegunaan, khususnya dalam mengembangkan Teori Bilangan**

1

Contoh 10.2: Berapakah sisa pembagian 5 oleh 11? Jawab: Menurut teorema Fermat  $5 \equiv 1 \pmod{11}$ , maka  $5^5 \equiv 5 \cdot 5^4 \equiv 5 \cdot 1 \equiv 5 \pmod{11}$ . Jadi,  $5 : 11$  bersisa 4. Bacalah lagi dengan seksama teorema 6.3 tersebut.

Kontraposisi dari teorema itu benar pula, yaitu: Jika untuk suatu bilangan bulat  $a$

1

,  $\equiv$ . Hal ini menunjukkan bahwa teorema

fermat dapat digunakan untuk menguji apakah suatu bilangan bulat merupakan bilangan komposit atau bukan. Contoh 10.3: Apakah 117 suatu bilangan prima

1

Jawab: Untuk memeriksa ini dipilih bilangan bulat positif yang cukup kecil, misalnya 2. Selanjutnya diperiksa apakah  $2 \equiv 2 \pmod{117}$ ?  $2 = 2 \cdot 1 = 2$ .  $2^2 = 4 \equiv 4 \pmod{117}$ .  $2^3 = 8 \equiv 8 \pmod{117}$ .  $2^4 = 16 \equiv 16 \pmod{117}$ .  $2^5 = 32 \equiv 32 \pmod{117}$ .  $2^6 = 64 \equiv 64 \pmod{117}$ .  $2^7 = 128 \equiv 11 \pmod{117}$ .  $2^8 = 256 \equiv 121 \pmod{117}$ .  $2^9 = 512 \equiv 117 \pmod{117}$ .  $2^{10} = 1024 \equiv 4 \pmod{117}$ .  $2^{11} = 2048 \equiv 2 \pmod{117}$ .  $2^{12} = 4096 \equiv 2 \pmod{117}$ . Sehingga diperoleh bahwa  $2 \equiv 44 \pmod{117}$ . Hal ini berarti bahwa 117 adalah bilangan komposit dan kenyataan bahwa  $117 = 13 \cdot 9$ . Contoh 10.4: Tanpa menggunakan teorema Fermat, tunjukkan bahwa  $3 \equiv 1 \pmod{17}$ . Jawab:  $3 \equiv 27 \pmod{17}$  dikuadratkan  $3 \equiv 100 \pmod{17}$ .  $3 \equiv 100 \pmod{17}$  dikuadratkan  $3 \equiv 4 \pmod{17}$ . Sehingga  $3 \equiv 3 \cdot 3 \cdot 3 \equiv 4 \cdot 10 \cdot 3 \pmod{17}$ . Jadi,  $3 \equiv 1 \pmod{17}$ . Perhatikan kembali teorema Fermat di atas. Perlu ditekankan di sini bahwa konvers dari teorema tersebut tidak benar, yaitu: Jika  $\equiv 1$ .

untuk suatu bilangan bulat, maka tidak perlu suatu bilangan prima

1

Untuk menunjukkan contohnya, terlebih dahulu kita bicarakan teorema berikut ini yang merupakan akibat dari teorema Fermat. Teorema 10.4 Jika  $p$  dan  $a$  adalah bilangan-bilangan prima yang berlainan sedemikian hingga  $a \equiv 1 \pmod{p}$  dan  $a \equiv 1 \pmod{p}$ , maka  $a \equiv 1 \pmod{p}$ . Bukti: Menurut teorema 6.3, karena suatu bilangan prima maka ini berarti bahwa  $a \equiv 1 \pmod{p}$ . selanjutnya, karena diketahui bahwa  $a \equiv 1 \pmod{p}$ . Ini berarti bahwa  $a \equiv 1 \pmod{p}$ . Menurut Teorema 6.3 lagi, karena suatu bilangan prima maka  $a \equiv 1 \pmod{p}$ . Selanjutnya, karena diketahui bahwa  $a \equiv 1 \pmod{p}$ . Ini berarti bahwa  $a \equiv 1 \pmod{p}$ . (2) Dari (1) dan (2) disimpulkan bahwa  $a \equiv 1 \pmod{p}$  dan dapat dinyatakan sebagai  $a \equiv 1 \pmod{p}$ . Contoh 10.5: Tunjukkan bahwa  $2 \equiv 1 \pmod{341}$ . Jawab:  $341 = 11 \cdot 31 \Leftrightarrow 2 = 1.024 = 31 \cdot 33 + 1$ , sehingga  $2 \equiv 1 \pmod{31}$ .  $2 \equiv 2 \pmod{31}$ .  $2 = 1.024 = 31 \cdot 33 + 1$ , sehingga  $2 \equiv 1 \pmod{11}$ , jika kedua ruas dibagi dua, maka diperoleh  $2 \equiv 2 \pmod{11}$ , maka  $2 \cdot 2 \equiv 2 \pmod{11 \cdot 31}$ , yaitu:  $2 \equiv 2 \pmod{341}$ . Jika kedua ruas dibagi dua, maka diperoleh  $2 \equiv 2 \pmod{341}$  dan tidak dapat disimpulkan bahwa 341 suatu bilangan prima. Contoh 10.6: Tentukan solusi dari  $7 \equiv 12 \pmod{17}$  dengan menggunakan teorema Fermat! Jawab: Dengan menggunakan teorema Fermat,  $7 = 7 \pmod{17}$ . Karena terdapat modulo 17 maka kita dapat memanfaatkan bentuk sehingga kita dapat mengalikan kedua sisi dengan 17 untuk memperoleh:  $17 \cdot 7x \equiv 17 \cdot 12 \pmod{17} \Leftrightarrow 17 \equiv 17 \cdot 12 \pmod{17}$ . Karena  $17 \equiv 1 \pmod{17}$  memberikan  $17 \equiv 17 \cdot 12 \pmod{17} \Leftrightarrow 17 \cdot 12 \pmod{17} \equiv 17 \cdot 12 \pmod{17} \equiv (17) \cdot 12 \pmod{17} \equiv (343) \cdot 12 \pmod{17} \equiv (3) \cdot 12 \pmod{17} \equiv 243 \cdot 12 \pmod{17} \equiv 5 \cdot 12 \pmod{17} \equiv 60 \pmod{17} \equiv 9 \pmod{17}$ . Sehingga diperoleh  $9 \pmod{17} \equiv 9 \pmod{17} \Leftrightarrow 17 + 9 \in \mathbb{N}$ . Nilai-nilai yang memenuhi:  $\dots = -3 : = 17 + 9 = 17(-3) + 9 = -51 + 9 = -42 = -2 : = 17 + 9 = 17(-2) + 9 = -34 + 9 = -25 = -1 : = 17 + 9 = 17(-1) + 9 =$

$$-17 + 9 = -8 = 0 : = 17 + 9 = 17(0) + 9 = 9 = 1 : = 17 + 9 = 17(1) + 9 = 1 + 9 = 26 = 2 : = 17 + 9 = 17(2) + 9 = 34 + 9 = -43 = 3 : = 17 + 9 = 17(3) + 9 = 51 + 9 = 60 = \dots$$

Jadi, solusi dari  $7 \equiv 12 \pmod{17}$  adalah 9, yaitu residu terkecil modulo 7. Dalam sejarahnya, bilangan berbentuk  $2 - 2$  ditemukan oleh matematikawan Cina pada 25 abad yang lalu dan menyatakan bahwa suatu bilangan prima jika dan hanya jika  $|2 - 2|$ . Dalam kenyataan, kriteria ini benar untuk semua bilangan prima < 340. Dan pada contoh di atas,

**kita memperoleh fakta bahwa 341**  $|2 - 2$ , **walaupun 341 bukan** bilangan **prima**. Selanjutnya **bilangan komposit** 1

sedemikian hingga  $|2 - 2|$  disebut bilangan prima semu (pseudoprime). Ada tak terhingga banyaknya

**bilangan prima semu**. Empat **bilangan prima semu** pertama **341, 561, 645, dan** 1

1.105. J.4. Latihan Kegiatan Belajar 9

**Selesaikan soal-soal berikut** ini **dengan benar! 1. 2. 3. 4. 5. 6. 7** 72

. Hitunglah  $6 \pmod{11}$ ! Hitunglah  $5 \pmod{41}$ ! Tentukan sisa 2019 dibagi 7! Tunjukkan bahwa 31 membagi  $8 - 1$ ! Tentukan sisa dari 7 sehingga 5 membagi 7! Tentukan sisa dari 18! Sehingga 437 membagi 18! Tentukan bilangan prima terbesar yang dapat dinyatakan dalam bentuk  $+ \text{suatu bilangan prima}$  dan  $+ 3$  untuk 8. Tentukan sisa pembagian dari  $(6 + 7 + 8 + 9)$  oleh 2017! 9. Tunjukkan bahwa jika  $p$  dan  $q$  adalah dua bilangan prima berbeda, maka  $a + b \equiv$

**10. Tunjukkan** bahwa **jika  $p$  adalah bilangan prima dan  $a$  adalah bilangan bulat, maka** 52

$((-1)!) + 1(1)!$  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 mengamplifikasikan konsep perkongruenan 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 suatu bilangan prima, maka** kekongruenan  $\equiv 1 \pmod{p}$  **mempunyai tepat dua** solusi, **yaitu 1 dan  $-1$ .** **Bukti: Misalkan adalah** 19  
**suatu** solusi **dari** perkongruenan  $\equiv 1 \pmod{p}$ , **maka**

$$-1 \equiv 0 \pmod{p} \Leftrightarrow (+1)(-1) \equiv 0 \pmod{p}$$

Perkongruenan terakhir ini berarti  $p \mid (+1)(-1)$

**1)(-1), karena  $p$  suatu bilangan prima, maka**  $p \mid (+1)$  atau  $p \mid (-1)$  **atau** 53

$-1 \equiv 0 \pmod{p} \Leftrightarrow -1 \pmod{p}$  atau  $\equiv 1 \pmod{p} \Leftrightarrow (-1) \pmod{p}$  atau  $\equiv 1 \pmod{p}$  Karena suatu solusi dari perkongruenan  $\equiv 1 \pmod{p}$ , maka adalah residu terkecil. Jadi 1 dan  $-1$  adalah solusi dari  $\equiv 1 \pmod{p}$ . Bukti lain yang lebih mudah, apabila  $(-1)$  dan 1 masing-masing disubstitusi pada dalam perkongruenan  $\equiv 1 \pmod{p}$ . Coba lakukanlah! Selesaikan perkongruenan-perkongruenan berikut ini:  $(1) \equiv 1 \pmod{7}$   $(2) \equiv 24 \pmod{23}$  Perhatikan himpunan residu-residu terkecil modulo 7 selain nol, yaitu  $= \{1, 2, 3, 4, 5, 6\}$ . Mudah anda peroleh solusi-solusi berikut ini: Solusi dari  $\equiv 1 \pmod{7}$  adalah 1 Solusi dari  $2 \equiv 1 \pmod{7}$  adalah 4 Solusi dari  $3 \equiv 1 \pmod{7}$  adalah 5 Solusi dari  $4 \equiv 1 \pmod{7}$  adalah 2 Solusi dari  $5 \equiv 1 \pmod{7}$  adalah 3 Solusi dari  $6 \equiv 1 \pmod{7}$  adalah 6 Tampak dari perkongruenan-perkongruenan tersebut bahwa jika  $a \in \{1, 2, 3, 4, 5, 6\}$ , maka solusi dari  $\equiv 1 \pmod{7}$

7) adalah  $a \in \mathbb{Z}$ . Dapat diperiksa pula bahwa apabila  $a \in \mathbb{Z}$  dengan  $a \equiv 1 \pmod{7}$  maka  $a \equiv 1 \pmod{7}$  dengan  $a \in \mathbb{Z}$  yang merupakan solusi berturut-turut dari  $a \equiv 1 \pmod{7}$  dan  $a \equiv 1 \pmod{7}$ . Jika  $a = 1$  dan  $a = 6$  maka solusi- solusinya berturut-turut adalah  $a = 1$  dan  $a = 6$ . Hal ini merupakan penerapan dari teorema berikut: Teorema 11.2: Misalkan suatu bilangan prima selain 2 dan  $a$  adalah solusi dari  $a \equiv 1 \pmod{p}$  dengan  $a = 1, 2, 3, \dots, -1$  yaitu ( $a \equiv 1 \pmod{p}$ ), dengan  $0 < a < p$ , maka: (i) jika  $a \equiv 1 \pmod{p}$  maka  $a \equiv 1 \pmod{p}$  (ii) jika  $a = 1$  atau  $a = -1$  maka  $a \equiv 1 \pmod{p}$  Bukti: Jika  $a = 1, 2, 3, \dots, -1$ , maka  $(a, p) = 1$ , sehingga  $a \equiv 1 \pmod{p}$  mempunyai tepat satu solusi. Ini berarti  $a$  ada, sedemikian hingga  $a \equiv 1 \pmod{p}$ . Bagian (i) dibuktikan kontraposisinya, yaitu: Jika  $a \not\equiv 1 \pmod{p}$ , maka  $a \equiv 1 \pmod{p}$ . Misalkan  $a \equiv 1 \pmod{p}$ , maka  $aa \equiv 1 \pmod{p}$ . Ingat bahwa  $a$  dan  $a$  adalah solusi dari  $a \equiv 1 \pmod{p}$ .  $a \equiv 1 \pmod{p}$  dengan  $a = 1, 2, \dots, -1$ . ( $a$ ), sebab  $a \equiv 1 \pmod{p}$ . Jadi (i) terbukti. Bagian (ii) dibuktikan sebagai berikut: Jika  $a = 1$ , yaitu  $a \equiv 1 \pmod{p}$ , maka solusinya adalah  $a = 1$ , sehingga  $a \equiv 1 \pmod{p}$ . Jika  $a = -1$ . Yaitu  $(-1) \equiv 1 \pmod{p}$  Jadi  $a = -1$ , sehingga  $a \equiv (-1) \equiv 1 \pmod{p}$  ( $a \equiv -1 \pmod{p}$ )) Contoh 11.1: 1( Pandang perkongruenan  $a \equiv 1 \pmod{11}$  dan  $a$  adalah solusinya, sehingga  $a \equiv 1$ ). Maka hubungan  $a$  dan  $a$  tampak pada tabel berikut ini.  $a \equiv 1 \pmod{11}$  2 6 3 4 4 3 5 9 6 2 7 8 8 7 9 5 10 10 1 1 1 1 1 1 1 1 1 Hasil kali- hasilkali pasangan yang kongruen modulo 11 dapat dituliskan sebagai berikut:  $2 \cdot 6 \equiv 1 \pmod{11}$   $3 \cdot 4 \equiv 1 \pmod{11}$   $5 \cdot 9 \equiv 1 \pmod{11}$   $7 \cdot 8 \equiv 1 \pmod{11}$

**Hasil kali semua bilangan pada ruas-ruas kiri akan kongruen mod 11 dengan 1 pula, yaitu** 19

$2 \cdot 6 \cdot 3 \cdot 4 \cdot 5 \cdot 9 \cdot 7 \cdot 8 \equiv 1 \pmod{11}$ . Jika kedua ruas dikalikan 10, diperoleh:  $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 10 \pmod{11} \Leftrightarrow 10! \equiv 10 \pmod{11} \Leftrightarrow 10! \equiv -1 \pmod{11}$  Coba tunjukkan bahwa  $6! \equiv 6 \pmod{7}$ ,  $12! \equiv 12 \pmod{13}$ ,  $18! \equiv 18 \pmod{19}$ . Contoh tersebut merupakan suatu cara membuktikan Teorema Wilson berikut ini. Teorema 11.3 (Teorema Wilson): Jika suatu bilangan prima, maka  $(-1)! \equiv -1 \pmod{p}$  Bukti:

**Menurut Teorema 5.6, kita dapat memasang dan dari 2, 3, 4** 24

$\dots, (-1)$  demikian sehingga  $a \equiv 1 \pmod{p}$ . Dan terdapat  $(-3)$  pasangan bilangan-bilangan tersebut yang kongruen mod dengan 1 jika ruas-ruas kiri dari  $(-3)$  kekongruenan mod tersebut dikalikan, maka hasil kalinya akan kongruen mod dengan 1 pula, yaitu:  $2 \cdot 3 \cdot 4 \cdot 5 \dots (-2) \equiv 1 \pmod{p} \Leftrightarrow 1 \cdot 2 \cdot 3 \cdot 4 \dots (-2)(-1) \equiv -1 \pmod{p} \Leftrightarrow (-1)! \equiv -1 \pmod{p}$ . Sebagai contoh diambil  $p = 13$ , maka kita dapat memasang dan dari 2, 3, 4,  $\dots, 11$ , sehingga terdapat 5 pasang bilangan-bilangan itu yang hasil kalinya kongruen mod 13 dengan 1, yaitu:  $2 \cdot 7 \equiv 1 \pmod{13}$   $3 \cdot 9 \equiv 1 \pmod{13}$   $4 \cdot 10 \equiv 1 \pmod{13}$   $5 \cdot 8 \equiv 1 \pmod{13}$   $6 \cdot 11 \equiv 1 \pmod{13}$  Hasil kali ruas-ruas dari 5 kekongruenan ini adalah  $(2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13} \Leftrightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \dots 11 \cdot 12 \equiv 12 \pmod{13} \Leftrightarrow 12! \equiv -1 \pmod{13}$  Konvers dan Teorema Wilson juga benar, yaitu: Jika  $(-1) \equiv -1 \pmod{p}$ , maka

**suatu bilangan prima. Hal ini dibuktikan sebagai berikut: Andaikan positif dan bukan bilangan prima, maka** 19

$a \neq 1$  atau  $a \neq -1$ , sehingga  $a$  dan  $a$  dengan  $a = 1, 2, 3, \dots, -1$ , bilangan-bilangan bulat Karena  $(-1)! \equiv -1 \pmod{p}$  maka  $|(-1)!| = 1$ . Dan karena  $a$ , maka  $|(-1)!| = 1$ . Karena  $a \leq -1$ , maka merupakan salah satu faktor dari  $(-1)!$ , sehingga  $|(-1)!| = 1$ . Mengingat  $|(-1)!| = 1$  dan  $|(-1)!| = 1$ , maka  $a = 1$ . Diperoleh suatu kontradiksi, karena  $a \neq 1$

**1, sehingga pengandaian tersebut tidak benar. Jadi adalah suatu bilangan prima. Jika Teorema Wilson dan konversnya dituliskan bersama-sama, kita memperoleh bahwa** 19

**Syarat perlu dan cukup agar p suatu bilangan prima adalah** 19

$(-1)! \equiv -1 \pmod{p}$ . Atau dapat ditulis:  $p$  suatu bilangan prima bila dan hanya bila adalah  $(-1)! \equiv -1 \pmod{p}$ . Berikut ini sebuah contoh penggunaan Teorema Wilson untuk menyelesaikan perkongruenan kuadrat seperti dalam teorema berikut ini. Teorema 11.4: Jika suatu bilangan prima ganjil, maka perkongruenan  $x^2 + 1 \equiv 0 \pmod{p}$  mempunyai solusi bila dan hanya bila  $p \equiv 1 \pmod{4}$ . Bukti: Misalkan adalah suatu solusi dari  $x^2 + 1 \equiv 0 \pmod{p}$  maka  $x^2 \equiv -1 \pmod{p}$  dan  $(x, p) = 1$ . Karena  $(x, p) = 1$ , menurut Teorema Fermat, maka  $x^{p-1} \equiv 1 \pmod{p}$  ( $x^{p-1} \equiv 1 \pmod{p}$ ) ( $x^{p-1} \equiv 1 \pmod{p}$ ) ( $x^{p-1} \equiv 1 \pmod{p}$ ) Bilangan prima berbentuk  $4k + 3$  tampak tidak memenuhi, sebab akan didapat  $(-1)^{2k+1} \equiv 1 \pmod{p}$   $-1 \equiv 1 \pmod{p}$ , yaitu  $12$  yang jelas salah. Jadi bilangan prima berbentuk  $4k + 1$ , yaitu  $p \equiv 1 \pmod{4}$ . Untuk sebaliknya dibuktikan sebagai berikut: Perhatikan bahwa  $-1 \equiv (-1) \equiv -2 \equiv -2 \pmod{p} \dots \dots \dots = -1 \pmod{p}$  dan  $(-1)! \equiv 1 \cdot 2 \cdot 3 \dots \dots \dots (-2)(-1)$ , maka ( $-1)! \equiv -1 \pmod{p}$ )



$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \pmod{p} \quad (p-1)! \equiv (-1)^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p} \quad (p-1)! \equiv -1 \pmod{p}$$

71

... ( ), sebab  $4 + 1$ , untuk suatu bilangan bulat positif, sehingga  $(-1) = 1 \pmod{p}$  (ingat Teorema Wilson bahwa  $(-1) \equiv -1 \pmod{p}$ ), maka: Hal ini berarti  $!$  memenuhi perkongruenan  $+ 1 \equiv 0 \pmod{p}$ . Jadi, perkongruenan itu mempunyai solusi. Contoh 11.3: Selesaikan perkongruenan  $+ 1 \equiv 0 \pmod{13}$ ! Jawab: Karena 13 adalah bilangan prima berbentuk  $4 +$

1, maka perkongruenan tersebut mempunyai solusi, yaitu:  $! = 6! = 720 \equiv 6 \pmod{13}$  Dapat diperiksa kebenarannya dengan substitusi 5 pada dari perkongruenan tersebut, yaitu  $52 + 1 = 53 \equiv 0 \pmod{13}$

19

(13) K.4. Latihan Kegiatan Belajar 10 Selesaikan soal-soal berikut ini dengan benar! 1.

Buktikan bahwa untuk setiap bilangan asli  $n$  berlaku  $4 + 10 + 16 + \dots + (6n - 2) = (3n + 1)^2$ . Terkalah rumus umum untuk jumlahan dari  $n$  bilangan genap positif pertama. Berikanlah hasil terkaan itu dengan induksi matematik! 3. Buktikanlah  $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + (n-1)n = \frac{1}{3}n(n+1)(n+2)$  untuk setiap bilangan asli  $n$ . 4. Terkalah rumus untuk  $\sum_{k=1}^n k^2$ , jika  $n = 1, 2, 3, \dots$ . Buktikanlah hasil terkaan itu dengan menggunakan induksi matematik! 5. Buktikan  $1 + 3 + 5 + \dots + (2n-1) = n^2$  untuk setiap bilangan asli  $n$ . 6. Buktikan bahwa  $1 + 2 + 3 + \dots + n = \frac{1}{2}n(n+1)$  untuk setiap bilangan  $n$ . 7. Buktikan bahwa  $a) > + 1$ , untuk setiap bilangan bulat  $\geq 2$ . b)  $2 > \frac{1}{n}$ , untuk setiap bilangan bulat  $n > 9$ .

86

Buktikan bahwa  $n^2 - 1$  terbagi habis oleh 5 untuk setiap bilangan asli  $n$

7

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 mengamplifikasikan 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 (tau)

Berdasarkan sifat-sifat yang dimiliki bilangan-bilangan bulat dapat didefinisikan fungsi-fungsi khusus yang mempunyai peranan penting dalam Teori Bilangan. Fungsi-fungsi khusus tersebut sering disebut fungsi

37

artimatik didefinisikan/mempunyai daerah asal pada himpunan bilangan bulat positif seperti berikut ini. Jika  $f$  suatu fungsi, maka:  $\rightarrow$

dengan  $B$  adalah himpunan semua bilangan bulat dan  $A$  adalah himpunan semua bilangan bulat positif

37

. Definisi 11.1: Misalkan suatu bilangan bulat positif,  $(n)$  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

32

(12) = 6. 2) Semua pembagi bulat positif dari 15 adalah 1,3,5, dan 15, maka (15) = 4. 3) Semua pembagi bulat positif dari 13 adalah 1 dan 13, maka (13) = 2. 4) Periksalah bahwa (1) = 1, (2) = 2, (3) = 2, (4) = 3, (5) = 2, (6) = 4, (8) = 4, (9) = 3. Jika suatu bilangan prima, maka  $(p) = 2$ .  $(n)$  yaitu banyaknya pembagi bulat positif dari  $n$ , sering dinyatakan dengan rumus yang menggunakan notasi  $\Sigma$  (sigma). Berikut ini beberapa contoh ketentuan penggunaan notasi  $\Sigma$ .  $\Sigma_{i=1}^n 1 = 1 + 1 + \dots + 1 = n$ .  $\Sigma_{i=1}^n i = 1 + 2 + 3 + \dots + n = \frac{1}{2}n(n+1)$ , yaitu banyaknya pembagi bulat positif dari 12.  $\Sigma_{i=1}^n \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$  yaitu banyaknya pembagi bulat positif dari 12. Memperhatikan contoh-contoh pemakaian notasi  $\Sigma$  tersebut,  $(n) = 2$  dapat dirumuskan sebagai berikut:  $(n) = \sum_{d|n} 1$  untuk bilangan bulat  $n \geq 1$ . Jadi,  $(n)$  merupakan penjumlahan dari 1 sebanyak pembagi bulat positif dari  $n$ . Contoh 11.2: 1) Semua pembagi bulat positif



suatu bilangan bulat positif, maka hasil kali semua pembagi bulat positif dari adalah:  $K(n) = n$

79

( ) Bukti: Misalkan  $d$  adalah suatu pembagi bulat positif dari  $n$ , maka ada  $d'$  (yaitu pembagi komplement 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 komplementnya (misalkan  $d'$ ) sedemikian hingga  $dd' = n$ , maka akan diperoleh bahwa hasil kali semua pembagi bulat positif dari  $n$  adalah:  $K(n) = n^{(\tau(n)/2)}$  Notasi lain dari  $K(n)$  adalah  $\prod_{d|n} d$ . 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 mengamplifikasikan konsep fungsi Mobius dan fungsi bilangan bulat diperbesar untuk menyelesaikan masalah. Materi prasyarat : teori himpunan, sistem bilangan bulat, relasi 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 suatu bilangan bulat positif, maka: 1, jika  $n = 1$ .  $\mu(n) = 0$ , jika  $n$  tak bebas kuadrat.  $(-1)^k$ , jika  $n$  bebas kuadrat Contoh 13.2: 1)  $\mu(30) = (2 \cdot 3 \cdot 5) = (-3) = -1$  2)  $\mu(500) = (2 \cdot 5)^3 = 0$  3)  $\mu(2) = -1$ ,  $\mu(3) = -1$ ,  $\mu(5) = -1$ ,  $\mu(6) = 1$  4) Jika suatu bilangan prima, maka  $\mu(30) = -1$  dan  $\mu(n) = 0$ , untuk  $n \geq 2$ . Fungsi Mobius ini merupakan fungsi ganda seperti yang dinyatakan dalam teorema berikut ini: Teorema 13.1: Fungsi adalah suatu fungsi ganda Bukti: Kita akan memperlihatkan bahwa jika  $(m, n) = 1$ , maka  $\mu(mn) = \mu(m)\mu(n)$ . Jika suatu bilangan prima dan  $n$  atau  $n$  bukan, maka  $\mu(n) = 0$ , sehingga  $\mu(mn) = 0 = \mu(m)\mu(n)$ . Jika  $n$  dan  $m$  adalah bilangan-bilangan bebas kuadrat, misalnya  $m = \dots$  dan  $n = \dots$  dengan  $n$  dan  $m$  adalah bilangan-bilangan prima. Maka  $\mu(mn) = (\dots) = (-1)^{k+l}$  Jadi, 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

57

menghitung jumlah semua nilai fungsi untuk semua faktor dari 12, yaitu:  $\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 + (-1) + (-1) + 1 + 0 + 1 = 0$  Misalkan suatu bilangan bulat  $n > 1$ , dan didefinisikan bahwa:  $\mu(n) = 0$  | Jika  $n$  dengan

$\mu$  suatu bilangan prima dan  $k$  suatu bilangan bulat positif, maka

13

semua faktor bulat positif dari  $n$  adalah  $1, p_1, p_2, \dots, p_k$ , sehingga:  $\mu(n) = \mu(1) + \mu(p_1) + \mu(p_2) + \dots + \mu(n) = 1 + (-1) + 0 + \dots + 0 = 0$  Mengingat bahwa suatu fungsi ganda dan memperlihatkan Teorema 13.1, maka merupakan fungsi ganda pula. Selanjutnya, jika bentuk kanonik dari  $n$  adalah:  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ , maka  $\mu(n) = (-1)^k$  Uraian tersebut merupakan bukti dari teorema berikut ini: Teorema 13.2: Untuk setiap bilangan bulat bilangan bulat positif  $n$ , berlaku: 1, jika  $n$  bilangan bulat positif. Pada teorema 13.1, telah dijelaskan bahwa jika didefinisikan oleh:  $\mu(n) = 1$   $n > 1$  suatu fungsi ganda dan fungsi  $\mu(n) = 0$  | maka suatu fungsi ganda pula. Dari hubungan ini, kita akan mencari rumus yang dinyatakan dalam fungsi. Untu ini, kita akan menggunakan fungsi Mobius dan mendapatkan teorema berikut ini yang biasa disebut dengan rumus interval Mobius. Teorema 13.3: Misalkan  $f$  dan  $g$  adalah dua fungsi aritmatik yang dihubungkan oleh rumus:  $f(n) = \sum_{d|n} g(d)$  | Mudah ditunjukkan bahwa  $\mu$  dan  $\mu$ , jika  $n$  dan hanya jika  $n$  dan  $n$ , sehingga Maka  $f(n) = \sum_{d|n} g(d)$  Bukti:  $\mu(d)f(c) = f(c)\mu(d)$  |  $\sum_{d|n} \mu(d) \sum_{d|n} g(d) = \dots$  (1) Menurut Teorema 7.7,  $\sum_{d|n} \mu(d) = 1$ , jika  $n = 1$ ,  $0$ , jika  $n > 1$  Sehingga persamaan (1) menjadi:  $f(n) = \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \sum_{d'|n/d} g(d')$  Sebagai ilustrasi untuk menjelaskan penggunaan jumlahan rangkap tersebut, misalkan diambil  $n = 10$ .  $f(10) = (1)[(1) + (2) + (5) + (10)] + (2)[(1) + (5)] + (-1)[(1) + (2)] + (10)(1) = (1)[(1) + (2) + (5) + (10)] + (2)[(1) + (5)] + (5)[(1) + (2)] + (1)(1) = \sum_{d|10} \mu(d) f(10/d)$  Untuk melihat bagaimana peranan rumus inversi Mobius ini, kita perhatikan kembali fungsi  $f$  dan yang dinyatakan sebagai  $f(n) = \sum_{d|n} g(d)$  1 dan  $g(n) = \sum_{d|n} \mu(d) f(n/d)$  maka dengan menggunakan rumus inversi Mobius (teorema 7.8), maka rumus-rumus dan tersebut dapat ditentukan inversinya, yaitu  $f(n) = \sum_{d|n} g(d)$  = 1 dan  $g(n) = \sum_{d|n} \mu(d) f(n/d)$ , untuk setiap bilangan asli  $n$ . Konvers dari Teorema 13.1 juga benar jika dinyatakan sebagai teorema beriku ini: Teorema 13.4: Jika suatu fungsi ganda dan  $f(n) = \sum_{d|n} g(d)$ , untuk semua bilangan asli  $n$ , maka adalah ganda pula. Bukti: Ambil

dua bilangan bulat positif  $m$  dan  $n$  dengan  $(m, n) = 1$ . Jika  $f$  dan  $g$ , karena  $(m, n) = 1$ , maka

90

| dan | dan  $(m, n) = 1$ . Dengan menerapkan rumus inversi Mobius, maka:  $f(n) = \sum_{d|n} g(d) = \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \sum_{d'|n/d} g(d')$  Jadi, adalah fungsi ganda.  $(f(n)) = \sum_{d|n} \mu(d) f(n/d)$  B. Fungsi Bilangan Bulat Terbesar Fungsi bilangan bulat terbesar atau fungsi kurung persegi  $[n]$  bukan merupakan fungsi aritmatik (fungsi teori bilangan), sebab daerah asal/domainnya adalah himpunan semua bilangan real, tetapi daerah hasil/rangennya adalah himpunan bilangan bulat. Definisi 13.2: Untuk

suatu bilangan real,  $[x]$  adalah suatu bilangan bulat terbesar yang kurang dari atau sama dengan  $x$ , yaitu  $[x]$  adalah bilangan bulat tunggal yang memenuhi  $-1 < [x] \leq x$ . Contoh

13.5:  $-1 = -2; \sqrt{3} = 1; 0 = 0; [3] = 3; [-4] = -4$ . Jadi,  $[x] = k$  jika dan hanya jika  $x$  suatu bilangan bulat sehingga untuk suatu bilangan real  $x$  dapat ditulis sebagai:  $x = [x] + \{x\}$  dengan  $0 \leq \{x\} < 1$  Salah satu penggunaan konsep fungsi bilangan bulat terbesar ini adalah menentukan banyaknya faktor prima yang muncul membagi  $n!$ . Sebagai contoh, berapa kalikah bilangan 3 muncul sebagai pembagi dari  $9!$ .  $9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 2 \cdot 3 \cdot 5 \cdot 7$  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 suatu bilangan bulat positif  $n$  dan suatu bilangan prima, maka eksponen tertinggi dari  $p$  yang membagi  $n!$  adalah  $\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$  (deret ini bukan deret tak hingga, karena  $\frac{n}{p^k} < 1$  untuk  $k > \log_p n$ ). Bukti: Pertama, bilangan-bilangan bulat positif yang dapat dibagi oleh  $p$  adalah  $p, 2p, 3p, \dots$ . Dengan  $\lfloor \frac{n}{p} \rfloor$  adalah bilangan bilangan bulat terbesar sedemikian hingga  $kp \leq n$ . Atau dengan kata lain,

adalah bilangan bulat terbesar yang kurang dari atau sama dengan  $\frac{n}{p}$ , yaitu

$\lfloor \frac{n}{p} \rfloor$ . Jadi, terdapat faktor  $p$  dari  $n!$  yang faktor lainnya adalah, yaitu:  $2, 3, \dots$ . Selanjutnya dicacah banyaknya bilangan-bilangan bulat positif  $1, 2, 3, \dots$ , yang tepat terbagi oleh  $p$ , seperti paragraph pertama, maka banyaknya factor dari  $n!$  yang tepat terbagi oleh  $p^2$  adalah, yaitu:  $2, 3, \dots$ . Demikian seterusnya dicacah banyaknya bilangan-bilangan bulat positif  $1, 2, 3, 4, \dots$ , yang tepat dibagi oleh  $p^3, \dots$ . Proses ini hanya berhingga banyaknya karena mesti ada  $p^k > n$ , sehingga banyaknya faktor  $p$  dari  $n!$  adalah  $\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$  Hasil ini dapat dinyatakan sebagai persamaan berikut ini, yang biasanya disebut dengan rumus Legendre:  $\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$  Contoh 13.6: Berapakah banyaknya angka nol dari representasi 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 faktorisasi prima dari  $50!$  dan memilih eksponennya yang terkecil. Eksponen tertinggi dari 2 dalam  $50!$  adalah  $\sum_{k=1}^{\infty} \lfloor \frac{50}{2^k} \rfloor = 25 + 12 + 6 + 3 + 1 = 47$  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  $\sum_{k=1}^{\infty} \lfloor \frac{50}{5^k} \rfloor = 10 + 2 = 12$  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:  $(f * F)(n) = \sum_{d|n} f(d)F(\frac{n}{d})$  Maka untuk sebarang bilangan bulat positif  $N$ , berlaku  $F(n) = \sum_{k|n} f(k)$  Bukti: Dari ketentuan diperoleh bahwa  $F(N) = \sum_{d|N} f(d) \dots (1)$  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 banyaknya bilangan-bilangan bulat diantara  $1, 2, 3, \dots, N$  yang dibagi oleh  $k$ . terdapat tepat  $\lfloor \frac{N}{k} \rfloor$  yaitu:  $k, 2k, 3k, \dots, k \lfloor \frac{N}{k} \rfloor$  Jadi, untuk setiap  $k$  dengan  $1 \leq k \leq N$ , adalah suatu suku dari jumlahan  $\sum_{d|N} f(d)$  untuk bilangan-bilangan bulat berbeda yang lebih kecil atau sama dengan  $N$ . hal ini dapat ditulis jumlahan rangkap dalam (1) sebagai:  $f(d) = \sum_{k|d} f(k) \lfloor \frac{N}{k} \rfloor$  Sebagai penerapan teori ini, kita ambil fungsi aritmatik dan  $\tau$ , yaitu:  $(\tau * \sigma)(n) = 1$  dan  $\sigma(n) = d | n$

Jika  $N$  suatu bilangan bulat positif, maka  $\tau * \sigma(n) = N$  dan  $\sigma(n) = \sum_{d|n} d$

Contoh 13.7: Hitunglah (a)  $\sum_{n=1}^N \tau(n)$  dan (b)  $\sum_{n=1}^N \sigma(n)$  Jawab: (a)  $\sum_{n=1}^N \tau(n) = \sum_{d=1}^N \lfloor \frac{N}{d} \rfloor = [6] + [3] + [2] + \dots + [1] = 6+3+2+1+1+1=14$  (b)  $\sum_{n=1}^N \sigma(n) = \sum_{d=1}^N d \lfloor \frac{N}{d} \rfloor = 1 \cdot [6] + 2 \cdot [3] + 3 \cdot [2] + 4 \cdot [1] + 5 \cdot [1] + 6 \cdot [1] = 1 \cdot 6 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 1 = 33$  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. 95 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 1 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 2 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 3 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 4 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 5 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 6 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 7 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 8 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 9 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 10 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 11 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 12 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 13 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 14 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 15 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 16 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 17 Modul Teori Biangan – Program Rekognisi Masa Lampau 18 Modul Teori Biangan – Program Rekognisi Masa Lampau 19 Modul Teori Biangan – Program Rekognisi Masa Lampau 20 Modul Teori Biangan – Program Rekognisi Masa Lampau 21 Modul Teori Biangan – Program Rekognisi Masa Lampau 22 Modul Teori Biangan – Program Rekognisi Masa Lampau 23 Modul Teori Biangan –

Program Rekognisi Masa Lampau 24 Modul Teori Biangan – Program Rekognisi Masa Lampau 25 Modul Teori Biangan – Program Rekognisi Masa Lampau 26 Modul Teori Biangan – Program Rekognisi Masa Lampau 27 Modul Teori Biangan – Program Rekognisi Masa Lampau 28 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 29 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 30 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 31 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 32 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 33 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 34 Modul Teori Bilangan 35 Modul Teori Bilangan 36 Modul Teori Bilangan 37 Modul Teori Bilangan 38 Modul Teori Bilangan 39 Modul Teori Bilangan 40 Modul Teori Bilangan 41 Modul Teori Bilangan 42 Modul Teori Bilangan 43 Modul Teori Bilangan 44 Modul Teori Bilangan 45 Modul Teori Bilangan 46 Modul Teori Bilangan 47 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 48 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 49 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 50 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 51 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 52 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 53 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 54 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 55 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 56 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 57 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 58 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 59 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 60 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 61 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 62 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 63 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 64 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 65 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 66 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 67 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 68 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 69 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 70 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 71 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 72 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 73 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 75 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 76 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 77 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 78 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 79 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 80 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 81 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 82 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 83 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 84 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 85 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 86 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 87 Modul Teori Bilangan – Program Rekognisi Pembelajaran Lampau 88 Modul Teori Bilangan 89 Modul Teori Bilangan 90 Modul Teori Bilangan 91 Modul Teori Bilangan 92 Modul Teori Bilangan 93 Modul Teori Bilangan 94 Modul Teori Bilangan 95 Modul Teori Bilangan 96 Modul Teori Bilangan 97 Modul Teori Bilangan 98 Modul Teori Bilangan 99 Modul Teori Bilangan 100 Modul Teori Bilangan 101

---

**sources:**

- 1 242 words / 1% - Internet from 07-Feb-2018 12:00AM  
[putriliaismawati.blogspot.com](http://putriliaismawati.blogspot.com)
- 2 115 words / 1% - from 30-Mar-2023 12:00AM  
[www.researchgate.net](http://www.researchgate.net)
- 3 109 words / 1% - from 30-Mar-2023 12:00AM  
[www.researchgate.net](http://www.researchgate.net)
- 4 215 words / 1% - Internet from 07-Dec-2019 12:00AM  
[usmcr010.blogspot.com](http://usmcr010.blogspot.com)
- 5 161 words / 1% - Internet from 16-Dec-2022 12:00AM  
[etheses.uin-malang.ac.id](http://etheses.uin-malang.ac.id)
- 6 157 words / 1% - Internet  
[Istiqomah, Istiqomah. "PENERAPAN TEOREMA BINOMIAL UNTUK MENENTUKAN PELUANG KEJADIAN \(KASUS :PERCOBAAN PELEMPARAN KOIN TAK SEIMBANG\)", 'Universitas Sarjanawiyata Tamansiswa', 2016](#)
- 7 166 words / 1% - from 11-Jun-2023 12:00AM  
[repository.uinsu.ac.id](http://repository.uinsu.ac.id)
- 8 141 words / 1% - Internet

- 9 123 words / 1% - Internet from 15-Jan-2017 12:00AM  
[lyanasikumbang.blogspot.com](#)
- 10 107 words / 1% - Internet from 07-Jan-2022 12:00AM  
[myblogmath2.blogspot.com](#)
- 11 104 words / 1% - Internet from 05-Mar-2023 12:00AM  
[ppjp.ulm.ac.id](#)
- 12 101 words / < 1% match - Internet from 29-Oct-2022 12:00AM  
[eprints.uny.ac.id](#)
- 13 91 words / < 1% match - Internet  
[Rininda Ulfa Arizka, -. "Penerapan Sistem Kriptografi ElGamal atas Dalam Pembuatan Tanda Tangan Digital", 2011](#)
- 14 10 words / < 1% match - Internet  
[Isnaini, Herdita Fajar, Karyati, Karyati. "PENERAPAN SKEMA TANDA TANGAN SCHNORR PADA PEMBUATAN TANDA TANGAN DIGITAL", 2016](#)
- 15 20 words / < 1% match - Internet from 21-May-2020 12:00AM  
[etheses.uin-malang.ac.id](#)
- 16 10 words / < 1% match - Internet  
[Maghfiroh, Jamilatul. "Pengamanan pesan menggunakan algoritma One Time Pad \(OTP\) dengan Linear Congruential Generator \(LCG\) sebagai pembangkit kunci", 2022](#)
- 17 10 words / < 1% match - Internet  
[Alvionita, Rena. "Implementasi algoritma super enkripsi \(Affine Cipher dan Route Cipher\) pada pesan teks", 2021](#)
- 18 12 words / < 1% match - Internet from 15-Sep-2021 12:00AM  
[jurnal.ustjogja.ac.id](#)
- 19 99 words / < 1% match - from 20-Mar-2023 12:00AM  
[pdfcookie.com](#)
- 20 54 words / < 1% match - Internet from 06-Jan-2023 12:00AM  
[dokumen.tips](#)
- 21 42 words / < 1% match - Internet from 10-Oct-2021 12:00AM  
[dokumen.tips](#)
- 22 72 words / < 1% match - from 22-Mar-2023 12:00AM  
[WWW.coursehero.com](#)
- 23 13 words / < 1% match - Internet from 28-Aug-2021 12:00AM  
[www.coursehero.com](#)
- 24 11 words / < 1% match - from 01-Apr-2024 12:00AM  
[WWW.coursehero.com](#)
- 25 89 words / < 1% match - Internet from 18-May-2019 12:00AM  
[helda-blog.blogspot.com](#)
- 26 87 words / < 1% match - Internet from 25-Nov-2020 12:00AM  
[indrawanpradinata.wordpress.com](#)

- 27 86 words / < 1% match - Internet from 30-Oct-2021 12:00AM  
[123dok.com](http://123dok.com)
- 28 72 words / < 1% match - from 19-Mar-2023 12:00AM  
[e-theses.iaincurup.ac.id](http://e-theses.iaincurup.ac.id)
- 29 64 words / < 1% match - Internet from 05-Nov-2015 12:00AM  
[repository.usu.ac.id](http://repository.usu.ac.id)
- 30 58 words / < 1% match - from 06-Apr-2023 12:00AM  
[odierealanalysis.blogspot.com](http://odierealanalysis.blogspot.com)
- 31 51 words / < 1% match - Internet from 12-Sep-2017 12:00AM  
[slimath.weebly.com](http://slimath.weebly.com)
- 32 48 words / < 1% match - Internet from 09-Nov-2020 12:00AM  
[jokoaguspurnomo.files.wordpress.com](http://jokoaguspurnomo.files.wordpress.com)
- 33 44 words / < 1% match - Internet from 17-Feb-2023 12:00AM  
[blogmeths.blogspot.com](http://blogmeths.blogspot.com)
- 34 43 words / < 1% match - Internet from 28-Dec-2021 12:00AM  
[www.kondiskorabat.com](http://www.kondiskorabat.com)
- 35 41 words / < 1% match - from 26-Dec-2023 12:00AM  
[www.powtoon.com](http://www.powtoon.com)
- 36 40 words / < 1% match - Internet  
[Gomes, Ataniel Rogério Gonçalves. "Uma abordagem do ensino de congruência na educação básica", 'FAI-UFSCar', 2015](#)
- 37 37 words / < 1% match - Internet from 24-Oct-2022 12:00AM  
[rstudio-pubs-static.s3.amazonaws.com](http://rstudio-pubs-static.s3.amazonaws.com)
- 38 36 words / < 1% match - Internet from 13-Jul-2020 12:00AM  
[spada.ristekdikti.go.id](http://spada.ristekdikti.go.id)
- 39 36 words / < 1% match - Internet from 21-Mar-2019 12:00AM  
[www.seratusinstitute.com](http://www.seratusinstitute.com)
- 40 35 words / < 1% match - Internet from 25-Mar-2019 12:00AM  
[fachruur.blogspot.com](http://fachruur.blogspot.com)
- 41 33 words / < 1% match - Internet from 03-Nov-2019 12:00AM  
[compilandoconocimiento.github.io](http://compilandoconocimiento.github.io)
- 42 32 words / < 1% match - Internet from 11-Jan-2020 12:00AM  
[ebooktake.in](http://ebooktake.in)
- 43 32 words / < 1% match - from 06-May-2024 12:00AM  
[html.pdfcookie.com](http://html.pdfcookie.com)
- 44 27 words / < 1% match - Internet from 02-Oct-2022 12:00AM  
[laurensommers.files.wordpress.com](http://laurensommers.files.wordpress.com)

- 45 26 words / < 1% match - from 25-Jan-2024 12:00AM  
[1library.org](http://1library.org)
- 46 26 words / < 1% match - Internet from 17-Nov-2020 12:00AM  
[fitrimheysuci.blogspot.com](http://fitrimheysuci.blogspot.com)
- 47 26 words / < 1% match - Internet from 28-Dec-2017 12:00AM  
[repository.uinjkt.ac.id](http://repository.uinjkt.ac.id)
- 48 25 words / < 1% match - Internet from 29-May-2021 12:00AM  
[dikdasmen.my.id](http://dikdasmen.my.id)
- 49 15 words / < 1% match - Internet from 01-Jan-2023 12:00AM  
"Persamaan Diophantus", [Wikipedia, id, 2023](https://id.wikipedia.org/wiki/Persamaan_Diophantus)
- 50 10 words / < 1% match - Internet from 01-Jan-2021 12:00AM  
"Eksponensiasi", [Wikipedia, id, 2021](https://id.wikipedia.org/wiki/Eksponensiasi)
- 51 24 words / < 1% match - Internet from 24-Aug-2016 12:00AM  
[mandiribelajarsains.blogspot.com](http://mandiribelajarsains.blogspot.com)
- 52 13 words / < 1% match - from 23-Oct-2023 12:00AM  
[idoc.tips](http://idoc.tips)
- 53 10 words / < 1% match - from 10-Oct-2023 12:00AM  
[idoc.tips](http://idoc.tips)
- 54 23 words / < 1% match - Internet  
[Handayanto, Agung. "PERANAN SISTEM MODULO DALAM PENENTUAN HARI DAN PASARAN", 'Universitas PGRI Semarang', 2012](https://doi.org/10.24054/ajg.v1i1.1234)
- 55 22 words / < 1% match - Internet from 18-Oct-2020 12:00AM  
[ugag.starserviceconsulting.it](http://ugag.starserviceconsulting.it)
- 56 11 words / < 1% match - from 13-Jun-2023 12:00AM  
[vdocuments.mx](http://vdocuments.mx)
- 57 11 words / < 1% match - from 24-Jun-2023 12:00AM  
[vdocuments.mx](http://vdocuments.mx)
- 58 22 words / < 1% match - Internet from 14-Nov-2020 12:00AM  
[www.slideshare.net](http://www.slideshare.net)
- 59 21 words / < 1% match - from 19-Sep-2023 12:00AM  
[educationbymath.blogspot.com](http://educationbymath.blogspot.com)
- 60 10 words / < 1% match - Internet from 28-Aug-2019 12:00AM  
[id.scribd.com](http://id.scribd.com)
- 61 10 words / < 1% match - Internet from 13-May-2020 12:00AM  
[id.scribd.com](http://id.scribd.com)
- 62 19 words / < 1% match - Internet from 22-Oct-2021 12:00AM  
[butsinegara.blogspot.com](http://butsinegara.blogspot.com)
- 63 19 words / < 1% match - Internet from 08-Feb-2019 12:00AM  
[cecepanwar.blogspot.com](http://cecepanwar.blogspot.com)



- 64 19 words / < 1% match - from 08-Apr-2023 12:00AM  
[ejournal.uin-suska.ac.id](http://ejournal.uin-suska.ac.id)
- 65 17 words / < 1% match - from 24-Jan-2024 12:00AM  
[isco-iss.faperta.unpad.ac.id](http://isco-iss.faperta.unpad.ac.id)
- 66 17 words / < 1% match - Internet from 06-Feb-2022 12:00AM  
[lp3.unism.ac.id](http://lp3.unism.ac.id)
- 67 16 words / < 1% match - from 05-Jan-2024 12:00AM  
[vdocuments.pub](http://vdocuments.pub)
- 68 16 words / < 1% match - Internet from 31-Jan-2019 12:00AM  
[zh.scribd.com](http://zh.scribd.com)
- 69 14 words / < 1% match - Internet from 29-Mar-2021 12:00AM  
[cdn-gbelajar.simpkb.id](http://cdn-gbelajar.simpkb.id)
- 70 14 words / < 1% match - Internet from 14-May-2020 12:00AM  
[fr.scribd.com](http://fr.scribd.com)
- 71 13 words / < 1% match - Crossref  
["A Concrete Introduction to Higher Algebra", Springer Science and Business Media LLC, 2009](https://doi.org/10.1007/978-1-4939-9888-8_1)
- 72 13 words / < 1% match - from 14-Mar-2024 12:00AM  
[ia803005.us.archive.org](http://ia803005.us.archive.org)
- 73 12 words / < 1% match - Internet  
[Sanchez-Rivero, Javier, Talaván, Daniel, Garcia-Alonso, Jose, Ruiz-Cortés, Antonio, Murillo, Juan Manuel. "Operating with Quantum Integers: an Efficient 'Multiples of' Oracle", 2023](https://arxiv.org/abs/2303.14812)
- 74 12 words / < 1% match - Internet from 26-Sep-2022 12:00AM  
[i-mes.org](http://i-mes.org)
- 75 12 words / < 1% match - Internet from 23-Nov-2020 12:00AM  
[matematikadw.files.wordpress.com](http://matematikadw.files.wordpress.com)
- 76 12 words / < 1% match - Internet from 12-Nov-2020 12:00AM  
[pangestuti-thecolourmath.blogspot.com](http://pangestuti-thecolourmath.blogspot.com)
- 77 12 words / < 1% match - from 01-Dec-2023 12:00AM  
[pdffox.com](http://pdffox.com)
- 78 12 words / < 1% match - Internet from 14-Nov-2020 12:00AM  
[soalterbaru.com](http://soalterbaru.com)
- 79 11 words / < 1% match - Internet from 11-Dec-2020 12:00AM  
[agus-chandra.blogspot.com](http://agus-chandra.blogspot.com)
- 80 11 words / < 1% match - Internet from 28-Oct-2018 12:00AM  
[docobook.com](http://docobook.com)
- 81 11 words / < 1% match - Internet from 12-Mar-2020 12:00AM  
[funwithmath18.blogspot.com](http://funwithmath18.blogspot.com)

- 82 11 words / < 1% match - Internet from 28-Jul-2016 12:00AM  
[issuu.com](http://issuu.com)
- 83 11 words / < 1% match - Internet from 18-Nov-2022 12:00AM  
[jurnal.lppm.unsoed.ac.id](http://jurnal.lppm.unsoed.ac.id)
- 84 11 words / < 1% match - Internet from 23-Nov-2020 12:00AM  
[kiseriotamatematika.blogspot.com](http://kiseriotamatematika.blogspot.com)
- 85 11 words / < 1% match - from 04-Oct-2023 12:00AM  
[php.math.unifi.it](http://php.math.unifi.it)
- 86 11 words / < 1% match - from 25-Jun-2023 12:00AM  
[repository.umsu.ac.id](http://repository.umsu.ac.id)
- 87 11 words / < 1% match - Internet from 16-Dec-2022 12:00AM  
[spada.uns.ac.id](http://spada.uns.ac.id)
- 88 11 words / < 1% match - Internet from 03-Nov-2021 12:00AM  
[text-id.123dok.com](http://text-id.123dok.com)
- 89 10 words / < 1% match - Internet from 22-Dec-2021 12:00AM  
[anianakcerdas.blogspot.com](http://anianakcerdas.blogspot.com)
- 90 10 words / < 1% match - Internet from 13-Jul-2020 12:00AM  
[jmua.fmipa.unand.ac.id](http://jmua.fmipa.unand.ac.id)
- 91 10 words / < 1% match - Internet from 14-Nov-2020 12:00AM  
[julanhernadi.files.wordpress.com](http://julanhernadi.files.wordpress.com)
- 92 10 words / < 1% match - Internet from 19-Aug-2019 12:00AM  
[jurnalabdul.blogspot.com](http://jurnalabdul.blogspot.com)
- 93 10 words / < 1% match - Internet from 12-Nov-2020 12:00AM  
[ovieciinduts.blogspot.com](http://ovieciinduts.blogspot.com)
- 94 10 words / < 1% match - Internet  
[Rifa'id, Rifa'id. "Kekongruenan Untuk Hasil Bagi Fermat Modulo P4", 2018](https://doi.org/10.24127/rifa.2018.12.1)
- 95 10 words / < 1% match - from 09-Jun-2023 12:00AM  
[statistika.fmipa.hamzanwadi.ac.id](http://statistika.fmipa.hamzanwadi.ac.id)
- 96 10 words / < 1% match - Internet from 03-Dec-2017 12:00AM  
[yudhadwinugroho.blogspot.com](http://yudhadwinugroho.blogspot.com)