



BUKU MATERI POKOK
MPMT5202/3skS/MODUL 1 - 9

EDISI 1

TEORI BILANGAN

■ GATOT MUHSETYO

$$X \equiv 13 \pmod{16}$$

$$= 13, 29, 45, 61, 77, 93, 109, \dots \pmod{16}$$

PENERBIT UNIVERSITAS TERBUKA

Hak Cipta © dan Hak Penerbitan dilindungi Undang-undang ada pada
Universitas Terbuka - Kementerian Riset, Teknologi, dan Pendidikan Tinggi
Jalan Cabe Raya, Pondok Cabe, Pamulang, Tangerang Selatan - 15418
Banten – Indonesia
Telp.: (021) 7490941 (hunting); Fax.: (021) 7490147;
laman: www.ut.ac.id

Dilarang mengutip sebagian ataupun seluruh buku ini
dalam bentuk apa pun, tanpa izin dari penerbit

Edisi Kesatu
Cetakan pertama, Juli 2011
Cetakan kedua, Februari 2014

Penulis : Prof. Drs. Gatot Muhsetyo, M.Sc.
Penelaah Materi : Dylmoon Hidayat, Ph.D.
Pengembang Desain Instruksional : Dra. Dwi Astuti Aprijani, M.Kom.

Desain Cover & Ilustrator : Zulkarnaini
Lay-outter : Nono Suwarno, dkk.
Copy Editor : Edi Purwanto

518.4

MUHSETYO, Gatot
m Materi pokok teori bilangan, 1 – 9/ MPMT5202/ 3 sks/
Gatot Muhsetyo. -- Cet.2; Ed.1 --. Tangerang Selatan:
Universitas Terbuka, 2014.
402 hal; 21 cm
ISBN: 978-979-011- 629-0

I. teori bilangan
I. Judul

Daftar Isi

TINJAUAN MATA KULIAH	ix
MODUL 1: BILANGAN BULAT	1.1
Kegiatan Belajar 1:	
Bilangan Bulat	1.3
Latihan	1.10
Rangkuman	1.12
Tes Formatif 1	1.13
Kegiatan Belajar 2:	
Prinsip Dasar Matematika	1.15
Latihan	1.23
Rangkuman	1.26
Tes Formatif 2	1.27
KUNCI JAWABAN TES FORMATIF.....	1.29
DAFTAR PUSTAKA.....	1.32
MODUL 2: KETERBAGIAN BILANGAN BULAT	2.1
Kegiatan Belajar 1:	
Konsep Dasar Keterbagian	2.3
Latihan	2.16
Rangkuman	2.18
Tes Formatif 1	2.20
Kegiatan Belajar 2:	
Faktor Persekutuan Terbesar (FPB) dan Kelipatan Persekutuan Terkecil (KPK)	2.22
Latihan	2.48

Rangkuman	2.51
Tes Formatif 2	2.52
KUNCI JAWABAN TES FORMATIF.....	2.55
DAFTAR PUSTAKA.....	2.60
MODUL 3: KONGRUENSI	3.1
Kegiatan Belajar 1:	
Konsep Dasar Kongruensi	3.3
Latihan	3.10
Rangkuman	3.12
Tes Formatif 1	3.13
Kegiatan Belajar 2:	
Sistem Residu	3.15
Latihan	3.28
Rangkuman	3.30
Tes Formatif 2	3.31
KUNCI JAWABAN TES FORMATIF.....	3.33
DAFTAR PUSTAKA.....	3.37
MODUL 4: KONGRUENSI LINIER	4.1
Kegiatan Belajar 1:	
Kongruensi Linier	4.3
Latihan	4.18
Rangkuman	4.21
Tes Formatif 1	4.22
Kegiatan Belajar 2:	
Sistem Kongruensi Linier	4.24
Latihan	4.37

Rangkuman	4.39
Tes Formatif 2	4.40
KUNCI JAWABAN TES FORMATIF.....	4.42
DAFTAR PUSTAKA.....	4.48
MODUL 5: RESIDU KUADRATIS	5.1
Kegiatan Belajar 1:	
Kongruensi Kuadratis	5.3
Latihan	5.18
Rangkuman	5.21
Tes Formatif 1	5.22
Kegiatan Belajar 2:	
Kebalikan Kuadratis	5.25
Latihan	5.37
Rangkuman	5.39
Tes Formatif 2	5.41
KUNCI JAWABAN TES FORMATIF.....	5.43
DAFTAR PUSTAKA.....	5.48
MODUL 6: FUNGSI-FUNGSI MULTIPLIKATIF	6.1
Kegiatan Belajar 1:	
Fungsi-fungsi Multiplikatif	6.3
Latihan	6.19
Rangkuman	6.21
Tes Formatif 1	6.23
Kegiatan Belajar 2:	
Bilangan Perfek dan Bilangan Mersenne	6.25
Latihan	6.32

Rangkuman	6.35
Tes Formatif 2	6.36
KUNCI JAWABAN TES FORMATIF.....	6.39
DAFTAR PUSTAKA.....	6.44
MODUL 7: PERSAMAAN DIOPHANTINE	7.1
Kegiatan Belajar 1:	
Persamaan Diophantine Linier	7.3
Latihan	7.12
Rangkuman	7.14
Tes Formatif 1	7.15
Kegiatan Belajar 2:	
Persamaan Diophantine Non Linier	7.17
Latihan	7.33
Rangkuman	7.35
Tes Formatif 2	7.37
KUNCI JAWABAN TES FORMATIF.....	7.39
DAFTAR PUSTAKA.....	7.44
MODUL 8: KRIPTOLOGI	8.1
Kegiatan Belajar 1:	
Pengodean Monografik	8.3
Latihan	8.12
Rangkuman	8.14
Tes Formatif 1	8.14
Kegiatan Belajar 2:	
Pengkodean Poligrafik	8.16
Latihan	8.22

Rangkuman	8.25
Tes Formatif 2	8.26
KUNCI JAWABAN TES FORMATIF.....	8.28
DAFTAR PUSTAKA.....	8.32
MODUL 9: AKAR PRIMITIF DAN ARITMETIKA INDEKS	9.1
Kegiatan Belajar 1:	
Akar Primitif	9.3
Latihan	9.13
Rangkuman	9.15
Tes Formatif 1	9.17
Kegiatan Belajar 2:	
Aritmetika Indeks	9.19
Latihan	9.30
Rangkuman	9.32
Tes Formatif 2	9.34
KUNCI JAWABAN TES FORMATIF.....	9.36
DAFTAR PUSTAKA.....	9.40

Tinjauan Mata Kuliah

Mata kuliah Teori Bilangan merupakan salah satu mata kuliah Keahlian Bidang Studi Matematika yang bertujuan memperkuat landasan materi matematika terutama yang mempunyai hubungan dengan matematika sekolah, yaitu materi tentang bilangan, dan memperluas wawasan ke dalam kajian materi matematika terutama yang mempunyai hubungan dengan persamaan Aljabar. Melalui mata kuliah Teori Bilangan ini Anda akan mempunyai kesempatan untuk mengkaji lebih mendalam berbagai sifat dan penerapan Teori Bilangan untuk kepentingan matematika sekolah, perluasan wawasan terkait dengan bagian matematika yang lain, dan pemahaman Teori Bilangan sebagai bagian dari matematika yang mandiri.

Setelah mempelajari mata kuliah Teori Bilangan ini, Anda diharapkan mempunyai kompetensi dalam:

1. penguasaan sifat-sifat keterbagian (*divisibility*);
2. pemahaman konsep dasar dan sifat-sifat FPB, KPK, dan Keprimaan;
3. pemahaman konsep dasar dan sifat-sifat kongruensi linier dan kuadratis;
4. pemahaman konsep dasar dan sifat-sifat fungsi khas dalam teori bilangan;
5. pemahaman penyelesaian Persamaan Diophantine linier dan non-linier;
6. pemahaman analisis pengodean dalam Kriptologi;
7. pemahaman akar primitif dan aritmetika indeks dalam konteks penyelesaian kongreansi non-linier.

Sesuai dengan tujuan yang ingin dicapai serta bobot sks, maka organisasi mata kuliah Teori Bilangan disusun dalam 9 (sembilan) modul dengan urutan sebagai berikut.

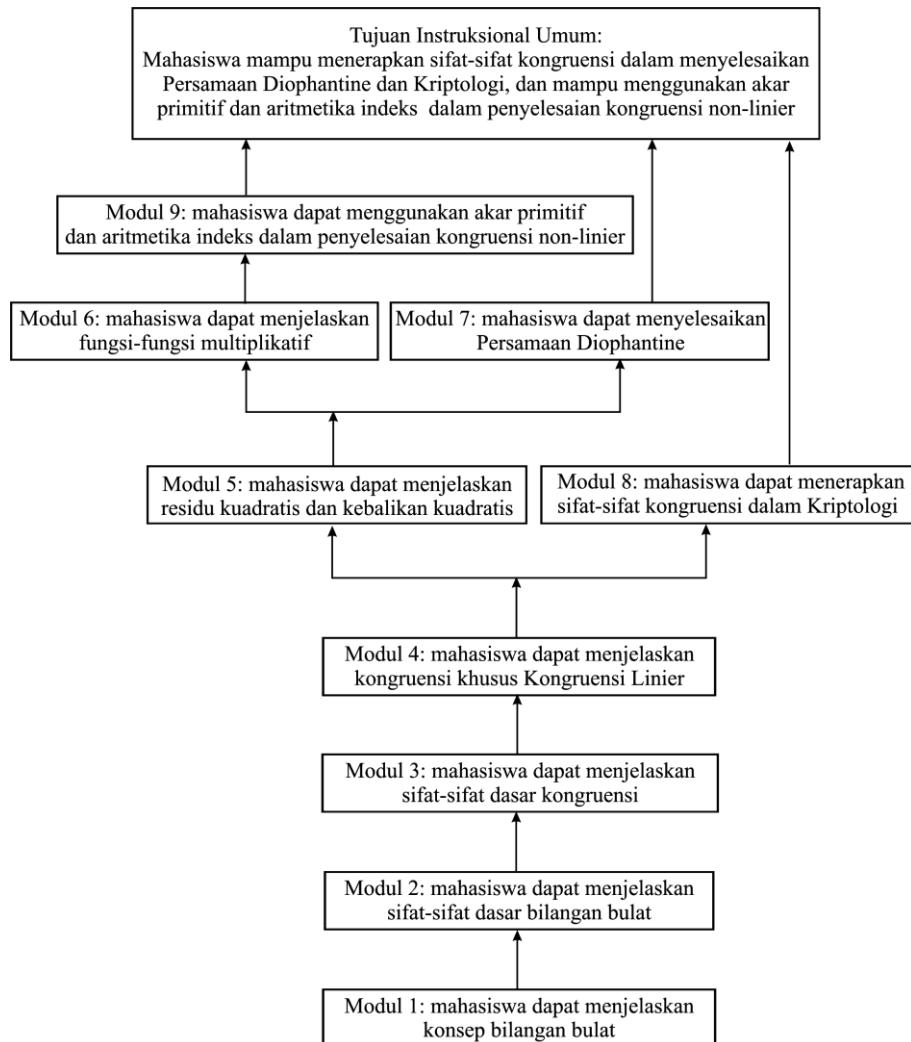
1. Bilangan Bulat;
2. Keterbagian Bilangan Bulat;
3. Kongruensi;
4. Kongruensi Linier;
5. Residu Kuadratis;
6. Fungsi-fungsi Multiplikatif;
7. Persamaan Diophantine;
8. Kriptologi;
9. Akar Primitif dan Aritmetika Indeks.

x

Dengan mempelajari setiap modul dengan cermat, sungguh-sungguh, tekun, dan tertib berdasarkan petunjuk mengerjakan semua tugas, latihan, dan tes formatif yang diberikan, maka Anda akan berhasil memahami dan menguasai kompetensi yang telah ditetapkan.

Selamat Belajar, semoga berhasil dengan sebaik-baiknya.

**Peta Kompetensi
Teori Bilangan MPMT5202/3 sks**



Bilangan Bulat

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul Bilangan Bulat ini diuraikan tentang awal pembahasan bilangan sebagai kebutuhan hidup manusia, meliputi bilangan asli, bilangan cacah, dan bilangan bulat. Sebagai objek matematika, bilangan bulat dan operasinya dapat membentuk suatu sistem atau struktur. Uraian berikutnya tentang prinsip induksi matematika sebagai alat pembuktian teorema yang penggunaannya tersebar luas di dalam berbagai topik matematika.

Sifat-sifat operasi bilangan bulat diuraikan kembali sebagai dasar pembicaraan berikutnya, meliputi sifat komutatif, sifat asosiatif, sifat distributif, sifat unsur identitas, sifat inversi, dan sifat kanselasi.

Pembahasan Induksi matematika dimulai dengan notasi jumlah dan notasi kali beserta sifat-sifat dan penggunaannya, dan dilanjutkan penjelasan tentang konsep induksi matematika beserta penerapannya untuk membuktikan hubungan-hubungan tertentu.

Secara keseluruhan, materi pokok dalam modul ini meliputi bilangan asli, bilangan cacah, bilangan bulat, operasi bilangan bulat dan sifat-sifatnya, prinsip urutan yang rapi, bilangan bulat terbesar, sedikit uraian tentang bilangan rasional dan bilangan irasional, notasi jumlah dan notasi kali, dan diakhiri dengan prinsip induksi matematika.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep bilangan bulat, operasi bilangan bulat, sistem bilangan bulat, induksi matematika sifat, dan keterkaitan antara topik-topik bilangan bulat dengan induksi matematika.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep bilangan bulat, konsep operasi bilangan bulat dan sifat-sifatnya, sistem bilangan bulat, penggunaan notasi jumlah, penggunaan notasi kali, induksi matematika, serta keterkaitan satu sama lain untuk menyelesaikan masalah-masalah matematika tertentu.

Susunan Kegiatan Belajar

Modul 1 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Bilangan Bulat, dan Kegiatan Belajar 2 adalah Induksi Matematika. Setiap kegiatan belajar memuat uraian, contoh, tugas dan latihan, petunjuk jawaban tugas dan latihan, rangkuman, dan tes formatif. Pada bagian akhir Modul 1 ini ditempatkan kunci jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah uraian dan contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi pembahasan.
2. Kerjakan tugas dan latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab, maka pelajari lah petunjuk jawaban tugas dan latihan. Jika langkah ini belum berhasil menjawab permasalahan, maka mintalah bantuan tutor Anda atau orang lain yang lebih tahu.
3. Kerjakan tes formatif secara mandiri dan periksalah tingkat penguasaan Anda dengan cara mencocokkan jawaban Anda dengan kunci jawaban tes formatif. Ulangilah pengeraaan tes formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Bilangan Bulat**

 embahasan tentang bilangan bulat (*integers*) tidak bisa dipisahkan dari uraian tentang bilangan asli (*natural numbers*) dan bilangan cacah (*whole numbers*) karena kreasi tentang bilangan-bilangan ini merupakan proses sosial dan budaya yang telah berlangsung berurutan dalam waktu ribuan tahun.

Konsep tentang bilangan dan cara mencacah atau menghitung, (*counting*) berkembang selama sekitar 15.000 tahun, mulai dari zaman prasejarah (*paleolithic, old stone age*) sampai dengan zaman sejarah (sekitar tahun 400 S.M.). Dalam periode atau zaman ini, manusia diduga telah mempelajari cara bertani atau bercocok tanam, cara beternak, cara menggunakan kalender, cara mengukur atau menimbang berat, cara memindahkan barang dengan kereta atau gerobak, cara membuat perahu, cara berburu, cara pengobatan tradisional, dan cara berhitung.

A. BILANGAN ASLI

Sejak periode sejarah, diduga dimulai sekitar tahun 400 S.M., orang mulai memikirkan bilangan sebagai konsep abstrak. Misalnya, mereka menyebut tiga kerikil dan tiga binatang mempunyai sifat persekutuan, yaitu suatu kuantitas yang disebut tiga. Sifat persekutuan tiga ini bisa dimiliki oleh kelompok benda apa saja sehingga sifat ini menjadi terbatas dari obyek atau sasaran pembicaraan. Dalam istilah yang lebih sederhana, sifat-sifat persekutuan satuan (*oneness*), duaan (*twoness*), atau tigaan (*threeness*) merupakan sifat persekutuan yang dimiliki oleh sebarang kumpulan benda untuk menunjukkan kesamaan kuantitas.

Keperluan tentang kuantitas merupakan kebutuhan dasar manusia dalam kehidupan berkeluarga dan bermasyarakat, terutama untuk menghitung atau mencacah dan membandingkan jumlah barang atau benda. Keperluan menghitung mendorong orang untuk mencari cara yang mudah, antara lain dengan membuat lambang bilangan (*numeral*) dan cara aturan penggunaannya atau sistem numerasi. Sistem numerasi adalah pembuatan sekumpulan lambang dasar dan sejumlah aturan untuk menghasilkan lambang-lambang bilangan yang lain.

Beberapa peradaban yang telah mengembangkan sistem numerasi antara lain adalah Mesir (sekitar tahun 3000 S.M.), Babylonia (sekitar tahun 2000 S.M.), Yunani atau Greek (sekitar tahun 600 S.M.), Maya (sekitar tahun 300 S.M.), Jepang – China (sekitar tahun 200 S.M.), Romawi (sekitar tahun 100 M), dan Hindu-Arab (mulai sekitar tahun 300 S.M. di India, sistem numerasi mengalami perubahan di wilayah timur tengah sekitar tahun 750 Masehi). Sistem numerasi berkembang di Eropa dan dipakai di seluruh dunia sampai sekarang.

Dari uraian di atas dengan singkat kita telah melihat perjalanan pengembangan konsep bilangan sejak pertama kali pada zaman Paleolithic sampai pada zaman sejarah. Dengan demikian kita perlu membuat asumsi bahwa manusia telah menemukan konsep bilangan asli (*counting/natural number*) dan telah menemukan himpunan lambang untuk menyatakan konsep bilangan asli yaitu 1, 2, 3, 4, Untuk selanjutnya himpunan bilangan asli dinyatakan dengan

$$N = \{1, 2, 3, 4, \dots\}$$

B. BILANGAN CACAH

Masyarakat pada zaman pertanian dan sebelum zaman revolusi, hanya memerlukan mencacah, menjumlah, dan mengalikan. Seiring dengan perkembangan zaman, masyarakat memerlukan sistem bilangan yang dapat memenuhi keperluan lain, yaitu mengurangkan dan membagi. Dengan demikian mereka mempunyai tuntutan pekerjaan yang tidak sekedar berhitung (aritmetika) tetapi hal lain yang lebih luas.

Jika sebelumnya mereka menerima pernyataan tanpa bukti (postulat): jika p dan q adalah bilangan asli, maka $p + q$ adalah suatu bilangan asli, maka kesulitan akan muncul ketika pengertian pengurangan mulai diperkenalkan melalui penjumlahan:

$$p - q = r \text{ jika ada } r \text{ bilangan asli sedemikian hingga } p = q + r$$

Kita bisa melihat kesulitan itu. Pengurangan pada unsur-unsur himpunan bilangan asli dapat dilakukan hanya jika p lebih dari q , artinya himpunan bilangan asli tidak bersifat tertutup terhadap pengurangan. Pada awalnya tentu mereka memahami bahwa:

$$3 - 2 = 1, 4 - 3 = 1, 5 - 4 = 1$$

dan mulai mempertanyakan bagaimana dengan

$$3 - 3 = ?, 4 - 4 = ?, 5 - 5 = ?$$

Jawabannya adalah mereka perlu “tambahan” bilangan baru, yang kemudian disebut dengan nol (*zero*), yang diberi makna:

$$3 = 3 + 0, 4 = 4 + 0, 5 = 5 + 0$$

Sekarang kita telah menambahkan unsur baru 0 ke dalam sistem bilangan asli, sehingga diperoleh himpunan baru yang disebut himpunan bilangan cacah, dinyatakan dengan:

$$W = \{0, 1, 2, 3, 4, \dots\}$$

C. BILANGAN BULAT

Dengan berkembangnya masyarakat industri, manusia memerlukan bilangan untuk keperluan pembukuan tingkat lanjut, antara lain untuk menghitung hutang dan piutang, serta tabungan dan pinjaman. Pertanyaan yang muncul adalah berapakah

$$6 - 7 = ?, 8 - 10 = ?, 3 - 10 = ?$$

Permasalahan ini serupa dengan usaha menambah bilangan-bilangan baru di dalam W sehingga mereka dapat melakukan semua pengurangan, atau himpunan baru yang diperoleh bersifat tertutup terhadap pengurangan.

Jawaban terhadap kesulitan mereka adalah tambahan bilangan-bilangan baru yang diperoleh dari:

$$0 - 1, 0 - 2, 0 - 3, 0 - 4, \dots$$

yang kemudian dilambangkan dengan:

$$-1, -2, -3, -4, \dots$$

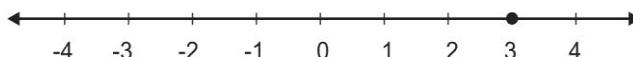
sehingga diperoleh himpunan baru yang disebut himpunan bilangan bulat, dan dinyatakan dengan:

$$Z = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

Dengan digunakannya garis bilangan untuk menyatakan bilangan, dan memberi makna terhadap bilangan-bilangan di sebelah kanan nol sebagai bilangan positif serta di sebelah kiri nol sebagai bilangan negatif, maka himpunan bilangan bulat dapat dinyatakan sebagai:

$$Z = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

Dalam garis bilangan, maka bilangan 3 bulat diletakkan sebagai



D. SISTEM BILANGAN BULAT

Untuk keperluan menghitung, orang dapat melakukan penjumlahan, pengurangan, perkalian, atau pembagian bilangan. Apa yang dilakukan oleh orang itu kemudian disebut sebagai suatu operasi. Pada dasarnya suatu operasi adalah mengambil sepasang bilangan untuk mendapatkan bilangan lain yang tunggal. Bilangan yang diperoleh mungkin unsur atau bukan unsur dari himpunan tertentu.

Definisi 1.1

Suatu sistem matematika adalah suatu himpunan bersama-sama dengan satu atau lebih operasi pada himpunan itu.

Notasi

Suatu sistem matematika yang terdiri dari himpunan S dan operasi $*$ pada S ditunjukkan dengan $(S, *)$.

Jika $\#$ adalah operasi kedua pada S , maka $(S, *, \#)$ adalah sistem matematika yang terdiri dari himpunan S , operasi pertama $*$, dan operasi kedua $\#$.

Berdasarkan pengetahuan yang telah kita pelajari sebelumnya, kita catat beberapa definisi yang berkaitan dengan sifat operasi adalah:

Definisi 1.2

Misalkan S adalah suatu himpunan. Ditentukan bahwa $*$ adalah suatu operasi pada S . Operasi $*$ disebut bersifat:

- tertutup jika $p * q \in S$ untuk setiap $p, q \in S$.
- komutatif jika $p * q = q * p$ untuk setiap $p, q \in S$.
- asosiatif jika $p * (q * r) = (p * q) * r$ untuk setiap $p, q, r \in S$.
- mempunyai unsur identitas jika untuk semua $p \in S$, ada $i \in S$, sehingga $p * i = i * p = p \cdot i$ disebut unsur identitas dari operasi $*$.
- memenuhi sifat inversi (*invertibel*) jika untuk setiap $p \in S$, ada $x \in S$, sehingga $p * x = x * p = i \cdot x$ disebut inversi dari p , dan p disebut inversi dari x .

Definisi 1.3

Misalkan S adalah suatu himpunan. Ditentukan bahwa $*$ adalah suatu operasi pertama dan $\#$ adalah suatu operasi kedua pada himpunan S . Operasi $*$ bersifat distributif terhadap $\#$ jika

$$p * (q \# r) = (p * q) \# (p * r) \text{ untuk semua } p, q, r \in S.$$

Selanjutnya, sifat-sifat operasi penjumlahan ($+$) dan perkalian (\times) pada himpunan bilangan bulat Z , merupakan aksioma sistem bilangan bulat $F(Z, +, \times)$, yaitu:

1. tertutup : $p + q \in Z$ dan $p \times q \in Z$ untuk semua $p, q \in Z$.
2. komutatif : $p + q = q + p$ dan $p \times q = q \times p$ untuk semua $p, q \in Z$.
3. asosiatif : $p + (q + r) = (p + q) + r$ dan $p \times (q \times r) = (p \times q) \times r$
untuk semua $p, q, r \in Z$.
4. mempunyai unsur identitas penjumlahan 0, dan unsur identitas perkalian 1, yang bersifat
 $p + 0 = p$ dan $p \times 1 = p$ untuk semua $p \in Z$.
5. memenuhi sifat inversi (*invertibel*) penjumlahan:
untuk semua $p \in Z$, ada $x \in Z$, sehingga $p + x = 0$
 x disebut inversi dari p , ditunjukkan dengan $x = -p$.
6. distributif perkalian terhadap penjumlahan
 $(p + q) \cdot r = (p \cdot r) + (q \cdot r)$.
7. memenuhi hukum kanselasi:
jika $p, q, r \in Z$, $r \neq 0$, dan $pr = qr$, maka $p = q$
 $p, q, r \in Z$ dan $p + r = q + r$, maka $p = q$.

Dalam kaitannya dengan urutan bilangan bulat, kita akan menggunakan istilah himpunan bilangan bulat positif untuk himpunan bilangan asli $Z^+ = \{1, 2, 3, \dots\}$. Urutan yang dimaksud adalah hubungan lebih kecil (atau lebih besar) antara dua bilangan bulat.

Definisi 1.4

Ditentukan $p, q \in Z$.

p disebut kurang dari q (atau q disebut lebih dari p), ditulis $p < q$ atau $q > p$, jika ada suatu bilangan bulat positif r sehingga $q - p = r$.

Contoh 1.1

- (a) $5 > 4$ sebab ada bilangan bulat positif 1 sehingga $5 - 4 = 1$
- (b) $2 < 7$ sebab ada bilangan bulat positif 5 sehingga $7 - 2 = 5$
- (c) $p > 0$ untuk setiap $p \in \{1, 2, 3, \dots\}$ sebab ada bilangan bulat positif p
sehingga $p - 0 = p$.

Dua sifat dasar tentang urutan bilangan bulat yang perlu dipahami adalah:

- (1) ketertutupan bilangan bulat positif:
 $p + q$ dan pq adalah bilangan-bilangan bulat positif untuk semua bilangan-bilangan bulat positif p dan q .
- (2) hukum trikotomi
Untuk setiap $p \in Z$ berlaku salah satu dari $p > 0$, $p = 0$, atau $p < 0$.

Himpunan bilangan bulat Z disebut suatu himpunan yang terurut karena Z memenuhi hukum trikotomi.

Contoh 1.2

Buktikan: Jika $p < q$ dan $r > 0$, maka $pr < qr$.

Bukti:

Diketahui bahwa $p < q$, maka menurut definisi 1.4, $q - p > 0$. Selanjutnya, karena $q - p > 0$ dan $r > 0$, maka menurut sifat dasar ketertutupan perkalian urutan bilangan bulat positif, $r(q - p) > 0$. Menurut sifat distributif, $r(q - p) = rq - rp$, dengan demikian $r(q - p) > 0$ berakibat $rq - rp > 0$.

Dari definisi 1.4, diperoleh $rp < rq$, dan menurut sifat komutatif perkalian, $pr < qr$.

Contoh 1.3

Buktikan: $(-1)p = -p$

Bukti: $(-1)p + 1.p = (-1+1).p = 0$ dan $-p + p = -p + 1.p = 0$, sehingga $(-1)p + 1.p = -p + 1.p$. Berdasarkan hukum kanselasi, $(-1)p = -p$.

Contoh 1.4

Sistem $(Z, +)$, yaitu sistem bilangan bulat terhadap operasi penjumlahan, merupakan suatu grup, dan juga merupakan grup Abel, sebab operasi $+$

terhadap bilangan bulat memenuhi sifat-sifat terhadap asosiatif, mempunyai unsur identitas, dan memenuhi sifat inversi.

Prinsip Urutan yang Rapi (*Well Ordering Principle*)

Suatu himpunan H disebut terurut rapi (*well ordered*) jika setiap himpunan bagian dari H yang tidak kosong mempunyai unsur terkecil.

Perlu diingat kembali bahwa k disebut unsur terkecil suatu himpunan S jika k kurang dari atau sama dengan x untuk semua $x \in S$ atau $k \leq x, \forall x \in S$.

Contoh 1.5

- (a) $S = \{2, 5, 7\}$ mempunyai unsur terkecil 2 sebab $2 \leq x$ untuk semua $x \in S$, yaitu $2 \leq 2, 2 \leq 5$, dan $2 \leq 7$.
- (b) $M = \{3\}$ mempunyai unsur terkecil 3 sebab $3 \leq x$ untuk semua $x \in M$, yaitu $3 \leq 3$.

Contoh 1.6

- (a) $S = \{2, 5, 7\}$ adalah himpunan yang terurut rapi sebab setiap himpunan bagian dari S yang tidak kosong, yaitu $\{2\}, \{5\}, \{7\}, \{2, 5\}, \{2, 7\}, \{5, 7\}$ dan $\{2, 5, 7\}$ mempunyai unsur terkecil berturut-turut adalah 2, 5, 7, 2, 2, 5, dan 2.
- (b) Z^+ adalah himpunan yang terurut rapi sebab semua himpunan bagian dari Z^+ yang tidak kosong mempunyai unsur terkecil.
- (c) Z adalah himpunan yang tidak terurut rapi sebab ada himpunan bagian dari Z yang tidak kosong dan tidak mempunyai unsur terkecil, misalnya $\{0, -1, -2, \dots\}$.

Definisi 1.5

Bilangan riil terbesar $[x]$ adalah bilangan bulat terbesar kurang dari atau sama dengan x , yaitu $[x]$ adalah bilangan bulat yang memenuhi $[x] \leq x \leq [x]+1$.

Sebagai catatan perlu diingat kembali bahwa fungsi $f(x) = [x]$ disebut dengan fungsi bilangan bulat terbesar, atau juga disebut dengan fungsi lantai

(*floor function*). Fungsi $g(x) = \lceil x \rceil$ disebut fungsi atap (*ceiling function*), di mana $\lceil x \rceil$ adalah bilangan bulat terkecil lebih dari atau sama dengan x , misalnya $\lceil 2/3 \rceil = 1$ dan $\lceil -7/3 \rceil = -2$.

Suatu bilangan riil x disebut **rasional** jika dan hanya jika ada bilangan-bilangan bulat a dan b , $b \neq 0$, dan $x = a/b$. Suatu bilangan yang tidak rasional disebut bilangan **irasional**, misalnya $\log 5$, $\sqrt{3}$, bilangan $e = 2,71828 \dots$, dan bilangan $\pi = 3,14\dots$.

Contoh 1.7

- (a) $\lceil 2/3 \rceil = 0$, $\lceil 7/3 \rceil = 2$, dan $\lceil \pi \rceil = 3$.
- (b) $\lceil -2/3 \rceil = -1$, $\lceil -7/3 \rceil = -3$.
- (c) $\lceil 1,3 \rceil = 1$, $\lceil \sqrt{3} \rceil = 1$.



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

Tugas

Untuk memperluas wawasan Anda tentang sistem numerasi, carilah dan bacalah sumber-sumber pustaka yang memuat sejarah bilangan. Selanjutnya jawablah beberapa pertanyaan berikut

- 1) Apa yang dimaksud dengan sistem numerasi bersifat aditif?
- 2) Apa yang disebut dengan sistem numerasi menggunakan nilai tempat?
- 3) Apa yang dimaksud dengan sistem numerasi bersifat multiplikasi?
- 4) Sebutkan beberapa cara menuliskan lambang bilangan dan terjadi pada sistem numerasi yang mana!
- 5) Sebutkan basis-basis bilangan yang pernah digunakan!

Latihan

- 1) Tunjukkan bahwa $p + (-q) = p - q$ untuk semua $p, q, \in Z$!
- 2) Tunjukkan bahwa $-(p \cdot q) = p \cdot (-q)$ untuk semua $p, q, \in Z$!
- 3) Diketahui $p, q, r \in Z$, $p < q$ dan $r < 0$.

Buktikan: $p + r < q + r$!

- 4) Diketahui $p, q, r \in Z$, $p > r$ dan $q > r$.

Tunjukkan: $p > r$!

- 5) Diketahui $C = \{1, -1\}$ merupakan bagian dari bilangan bulat.

Selidiki apakah (C, x) merupakan sistem grup?

Petunjuk Jawaban Tugas dan Latihan

- 1) Sistem numerasi disebut bersifat aditif jika nilai bilangan sama dengan jumlah nilai setiap lambang bilangan yang digunakan.

Contoh:

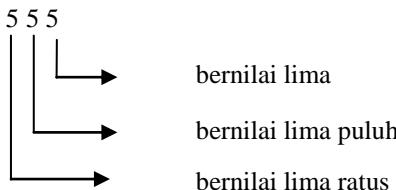
Mesir Kuno: Lambang ፩ ፩ ፩ ፩ ፩ ፩ ፩ ፩ | | |

- 2) Sistem numerasi disebut menggunakan nilai tempat jika nilai lambang bilangan didasarkan pada tempat atau posisi lambang bilangan, artinya lambang yang sama bernilai berbeda karena posisinya berbeda.

Contoh:

Babylonia : Lambang :	$\triangle < \nabla$
	Nilai 71 : $(1 \times 60) + 10 + 1$

Desimal : Lambang :	5 5 5
	Nilai setiap lambang 5 berbeda karena letaknya yang berbeda



- 3) Sistem numerasi disebut multiplikatif jika mempunyai lambang untuk bilangan-bilangan $1, 2, 3, \dots, b-1, b, b^2, b^3, \dots$, tidak mempunyai lambang nol, dan menggunakan nilai tempat.

Contoh:

Jepang-China: Lambang: ~ □ ξ □ ፩ ጥ ተ) (ክ f
Nilai : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 100, 1000

- 4) Cara menuliskan lambang bilangan

(a) Acak, untuk sistem numerasi Mesir Kuno

- (b) Mendatar (horizontal), untuk sistem-sistem numerasi Babylonia, Yunani (*Greek*), Romawi, Hindu-Arab
 - (c) Tegak (vertikal), untuk sistem-sistem numerasi Jepang-China dan Maya
- 5) Basis bilangan yang pernah digunakan
- (a) Basis 10 : sistem numerasi Jepang-China, Hindu Arab
 - (b) Basis 20 : sistem numerasi Maya
 - (c) Basis 60 : sistem numerasi Babylonia



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi definisi, teorema, contoh, dan latihan tentang bilangan bulat, terutama tentang konsep bilangan bulat, sistem bilangan bulat, operasi bilangan bulat dan sifat-sifatnya, dan aksioma sifat-sifat operasi penjumlahan dan perkalian bilangan bulat. Paparan kemudian dilanjutkan dengan prinsip urutan yang rapi serta hubungan dua bilangan bulat (sama dengan, lebih dari, kurang dari), dilengkapi dengan pengertian bilangan bulat terbesar, fungsi lantai, dan fungsi atap. Pada bagian akhir diingatkan kembali pengertian bilangan rasional dan bilangan irasional.

1. Himpunan bilangan bulat dinyatakan dengan $Z = \{ \dots, -2, -1, 0, 1, 2, \dots \}$
2. **Definisi 1.1**

Suatu sistem matematika adalah suatu himpunan bersama-sama dengan satu atau lebih operasi pada himpunan itu.

3. **Definisi 1.2**

Ditentukan bahwa $*$ adalah suatu operasi pada himpunan S .

Operasi $*$ disebut bersifat:

- a. tertutup jika $p * q \in S$ untuk setiap $p, q \in S$.
- b. komutatif jika $p * q = q * p$ untuk setiap $p, q \in S$.
- c. asosiatif jika $p * (q * r) = (p * q) * r$ untuk setiap $p, q, r \in S$.
- d. mempunyai unsur identitas jika untuk semua $p \in S$, ada $i \in S$, sehingga $p * i = i * p = p$. i disebut unsur identitas operasi $*$.

4. **Definisi 1.3**

Ditentukan bahwa $*$ adalah suatu operasi pertama dan $\#$ adalah suatu operasi kedua pada himpunan S .

Operasi $*$ bersifat distributif terhadap $\#$ jika

$p^*(q \ # r) = (p^*q) \ #(p^*r)$ untuk semua $p, q, r \in S$.

5. **Definisi 1.4**

Ditentukan $p, q \in Z$.

p disebut kurang dari q (atau q disebut lebih dari p), ditulis $p < q$ atau $q > p$, jika ada suatu bilangan bulat positif r sehingga $q - p = r$.

6. **Definisi 1.5**

Bilangan riil terbesar $[x]$ adalah bilangan bulat terbesar kurang dari atau sama dengan x , yaitu $[x]$ adalah bilangan bulat yang memenuhi $[x] \leq x \leq [x]+1$.

7. **Prinsip Urutan yang Rapi (Well Ordering Principle)**

Suatu himpunan H disebut terurut rapi (*well ordered*) jika setiap himpunan bagian dari H yang tidak kosong mempunyai unsur terkecil.



TES FORMATIF 1

Pilihlah satu jawaban yang paling tepat!

1) Skor 10

Jika $a, b \in Z, a < b, c > 0$, maka buktikan bahwa $ac < bc$.

2) Skor 10

Buktikan bahwa tidak ada bilangan bulat positif kurang dari 1

3) Skor 10

Tentukan apakah himpunan-himpunan berikut terurut rapi

(a) $A = \{-2, 3, 4\}$

(b) $B = \left\{ \frac{2}{3}, 2, \sqrt{5} \right\}$

(c) himpunan bilangan bulat negatif

(d) himpunan bilangan cacah

(e) himpunan bilangan rasional

(f) himpunan bilangan riil

4) Skor 10

Carilah nilai-nilai dari:

(a) $[0, 12]$

(b) $\left[\begin{array}{c} 7 \\ 9 \end{array} \right]$

(c) $\left[\begin{array}{c} 5 \frac{2}{3} \\ 3 \end{array} \right]$

(d) $\left[\begin{array}{c} -1 \frac{3}{5} \\ 5 \end{array} \right]$

5) Skor 20

Jika k adalah suatu bilangan bulat, maka buktikan bahwa:

$$[x+k] = [x] + k \text{ untuk setiap bilangan riil } x.$$

6) Skor 10

Carilah nilai $[x] + [-x]$ jika x adalah suatu bilangan riil.

7) Skor 20

Buktikan bahwa $[x] + \left[x + \frac{1}{2} \right] = [2x]$ jika x adalah suatu bilangan riil.

8) Skor 10

Buktikan bahwa $\sqrt{2}$ adalah suatu bilangan irasional.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Prinsip Dasar Matematika**

 Prinsip induksi matematika merupakan suatu alat berharga untuk membuktikan hasil-hasil yang terkait dengan bilangan asli, atau hubungan tertentu yang dapat diperluas berlaku untuk semua bilangan asli. Hasil-hasil yang terkait terutama tentang penjumlahan, dan hubungan tertentu antara lain dapat berupa ketidaksamaan, keterbagian, atau diferensial.

Dalam kaitannya dengan hasil penjumlahan, prinsip induksi matematika melibatkan notasi jumlah (*summation*) dan notasi kali (*product*). Kedua notasi ini sangat bermanfaat untuk menyederhanakan tulisan sehingga menjadi lebih singkat dan lebih mudah dipahami.

A. NOTASI JUMLAH DAN NOTASI KALI

Notasi jumlah adalah notasi yang dilambangkan dengan Σ , dan notasi kali adalah notasi yang dilambangkan dengan Π , dan didefinisikan sebagai:

$$\sum_{i=1}^r x_i = x_1 + x_2 + \dots + x_r$$

$$\prod_{i=1}^r x_i = x_1 \cdot x_2 \dots x_r$$

Huruf i dari indeks notasi jumlah atau notasi kali disebut variabel *dummy* karena dapat diganti oleh sebarang huruf, misalnya:

$$\sum_{i=1}^r x_i = \sum_{j=1}^r x_j = \sum_{k=1}^r x_k$$

$$\prod_{i=1}^r x_i = \prod_{j=1}^r x_j = \prod_{k=1}^r x_k$$

$i = 1$ disebut batas bawah (*lower limit*) dan $i = r$ disebut batas atas (*upper limit*).

Contoh 1.1

$$(a) \sum_{i=1}^4 i = 1+2+3+4=10$$

$$(b) \prod_{i=1}^4 i = 1 \cdot 2 \cdot 3 \cdot 4 = 24$$

$$(c) \sum_{k=1}^5 3 = 3+3+3+3+3 = 15$$

$$(d) \prod_{k=1}^5 3 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 243$$

$$(e) \sum_{t=1}^3 t^2 = 1^2 + 2^2 + 3^2 = 14$$

$$(f) \prod_{t=1}^3 t^2 = 1^2 \cdot 2^2 \cdot 3^2 = 36$$

Selanjutnya, indeks jumlah tidak harus dimulai dari 1, artinya dapat dimulai dari bilangan bulat selain 1 asalkan batas bawah tidak melebihi batas atas.

Contoh 1.2

$$(a) \sum_{i=3}^5 i = 3+4+5=12$$

$$(b) \sum_{t=4}^6 (2t-1) = (2 \cdot 4 - 1) + (2 \cdot 5 - 1) + (2 \cdot 6 - 1) = 27$$

$$(c) \prod_{k=2}^4 2^k = 2^2 \cdot 2^3 \cdot 2^4 = 4 \cdot 8 \cdot 16 = 512$$

$$(d) \prod_{t=2}^4 (t-1) = (2-1)(3-1)(4-1) = 1 \cdot 2 \cdot 3 = 6$$

Beberapa sifat yang terkait dengan notasi jumlah adalah:

$$(1) \sum_{i=r}^s tx_i = tx_r + tx_{r+1} + \dots + tx_s \\ = t(x_r + x_{r+1} + \dots + x_s)$$

$$= t \sum_{i=r}^s x_i$$

$$\begin{aligned}
 (2) \quad \sum_{i=r}^s (x_i + y_i) &= (x_r + y_r) + (x_{r+1} + y_{r+1}) + \dots + (x_s + y_s) \\
 &= (x_r + x_{r+1} + \dots + x_s) + (y_r + y_{r+1} + \dots + y_s) \\
 &= \sum_{i=r}^s x_i + \sum_{i=r}^s y_i
 \end{aligned}$$

$$\begin{aligned}
 (3) \quad \sum_{i=a}^b \sum_{j=c}^d x_i y_j &= \sum_{i=a}^b \left(x_i \sum_{j=c}^b y_j \right) \\
 &= \sum_{i=a}^b x_i (y_c + y_{c+1} + \dots + y_d) \\
 &= x_a (y_c + y_{c+1} + \dots + y_d) + x_{a+1} (y_c + y_{c+1} + \dots + y_d) + \dots + \\
 &\quad x_b (y_c + y_{c+1} + \dots + y_d) \\
 &= (x_a + x_{a+1} + \dots + x_d) (y_c + y_{c+1} + \dots + y_d) \\
 &= \left(\sum_{i=a}^b x_i \right) \left(\sum_{j=c}^d y_j \right).
 \end{aligned}$$

$$\begin{aligned}
 (4) \quad \sum_{i=a}^b \sum_{j=c}^d x_i y_j &= \left(\sum_{i=a}^b x_i \right) \left(\sum_{j=c}^d y_j \right) \\
 &= \left(\sum_{j=c}^d y_j \right) \left(\sum_{i=a}^b x_i \right) \\
 &= \sum_{j=c}^d \sum_{i=a}^b y_j x_i \\
 &= \sum_{j=c}^d \sum_{i=a}^b x_i y_j.
 \end{aligned}$$

Contoh 1.3

- (a) $\sum_{i=3}^5 2x_i = 2x_3 + 2x_4 + 2x_5 = 2(x_3 + x_4 + x_5) = 2 \sum_{i=3}^5 x_i$
- (b) $\sum_{i=2}^4 (2a_i + 3b_i) = (2a_2 + 3b_2) + (2a_3 + 3b_3) + (2a_4 + 3b_4)$

$$\begin{aligned}
 &= (2a_2 + 2a_3 + 2a_4) + (3b_2 + 3b_3 + 3b_4) \\
 &= 2(a_2 + a_3 + a_4) + 3(b_2 + b_3 + b_4) \\
 &= 2\sum_{i=2}^4 a_i + 3\sum_{i=2}^4 b_i.
 \end{aligned}$$

$$\begin{aligned}
 (\text{c}) \quad \sum_{i=1}^3 \sum_{j=1}^2 ij^2 &= \sum_{i=1}^3 (i \cdot 1^2 + i \cdot 2^2) \\
 &= \sum_{i=1}^3 5i = 5 \cdot 1 + 5 \cdot 2 + 5 \cdot 3 = 30
 \end{aligned}$$

$$\begin{aligned}
 (\text{d}) \quad \sum_{j=1}^2 \sum_{i=1}^3 ij^2 &= \sum_{j=1}^2 (1 \cdot j^2 + 2 \cdot j^2 + 3 \cdot j^2) \\
 &= \sum_{j=1}^2 6j^2 = 6 \cdot 1^2 + 6 \cdot 2^2 = 6 \cdot 1 + 6 \cdot 4 = 30
 \end{aligned}$$

B. PRINSIP INDUKSI MATEMATIKA (*PRINCIPLE OF MATHEMATICAL INDUCTION*)

S adalah suatu himpunan bagian dari himpunan bilangan asli yang unsur-unsurnya memenuhi hubungan

Jika: (a) $1 \in S$

(b) $k \in S$ berakibat $(k+1) \in S$

maka: S memuat semua bilangan asli, yaitu $S = N$.

Bukti:

Misalkan $S \subset N$ dan unsur-unsur S memenuhi suatu hubungan (a) dan (b). Harus dibuktikan bahwa $S = N$. Untuk membuktikan $S = N$ digunakan bukti tidak langsung.

Anggaplah $S \neq N$, maka tentu ada $F \subset N$ dan $F \neq \emptyset$ yang mana $F = \{t \in N \mid t \notin S\}$.

Karena $F \neq \emptyset$ dan $F \subset N$, maka menurut prinsip urutan rapi F mempunyai unsur terkecil misalkan $k \in F$ tetapi $k \notin S$.

$k \neq 1$ sebab $1 \in S$, berarti $k > 1$, dan akibatnya $k-1 \in N$.

k adalah unsur terkecil F , maka $k-1 \notin F$ sebab $k-1 < k$, berarti $k-1 \in S$.

$k-1 \in S$ dan S memenuhi (b), maka

$(k-1)+1 \in S$, atau $k-1+1 \in S$, yaitu $k \in S$.

Terjadi kontradiksi karena $k \notin S$ dan $k \in S$, jadi $S = N$.

Dalam pernyataan lain, prinsip induksi matematika dapat ditulis dengan $S(n)$ adalah suatu pernyataan yang memenuhi hubungan untuk satu atau lebih $n \in N$.

Jika: (a) $S(1)$ benar

(b) $S(k)$ benar berakibat $S(k+1)$ benar

maka $S(k)$ benar untuk semua $n \in N$.

Contoh 1.4

Buktikan untuk sebarang $n \in Z^+$, $\sum_{i=1}^n i = 1 + 2 + 3 + \dots + n = \frac{1}{2}n(n+1)$

Bukti:

Misalkan $S(n)$: $\sum_{i=1}^n i = \frac{1}{2}n(n+1)$, maka

$S(1)$ benar sebab untuk $n = 1$:

$$\sum_{i=1}^n i = \sum_{i=1}^1 i = 1 \text{ dan } \frac{1}{2}n(n+1) = \frac{1}{2} \cdot 1(1+1) = \frac{1}{2} \cdot 2 = 1$$

Misalkan $S(k)$ benar, yaitu untuk $n = k$:

$$\sum_{i=1}^k i = 1 + 2 + \dots + k = \frac{1}{2}k(k+1)$$

Harus dibuktikan $S(k+1)$ benar, yaitu:

$$\sum_{i=1}^{k+1} i = 1 + 2 + 1 + \dots + k + k + 1 = \frac{1}{2}(k+1)(k+1+1) = \frac{1}{2}(k+1)(k+2)$$

$$\sum_{i=1}^{k+1} i = \underbrace{1 + 2 + \dots + k}_{\frac{1}{2}k(k+1)} + k + 1 = \frac{1}{2}k(k+1) + k + 1$$

$$\begin{aligned} \frac{1}{2}k(k+1) &= (k+1)\left(\frac{1}{2}k+1\right) = (k+1) \cdot \frac{1}{2}(k+2) \\ &= \frac{1}{2}(k+1)(k+2) = \frac{1}{2}(k+1)\{(k+1)+1\}. \end{aligned}$$

Jadi: $S(n)$ benar untuk sebarang $n \in Z^+$.

Contoh 1.5

Buktikan untuk sebarang $n \in Z^+$, $\sum_{i=1}^n i^2 = 1^2 + 2^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1)$

Bukti:

Misalkan $S(n) : \sum_{i=1}^n i^2 = \frac{1}{6}n(n+1)(2n+1)$, maka

$S(1)$ benar, sebab untuk $n = 1$:

$$\sum_{i=1}^n i^2 = \sum_{i=1}^1 i^2 = 1^2 = 1 \text{ dan } \frac{1}{6}n(n+1)(2n+1) = \frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1.$$

Misalkan $S(k)$ benar, yaitu untuk $n = k$:

$$\sum_{i=1}^k i^2 = 1^2 + 2^2 + \dots + k^2 = \frac{1}{6}k(k+1)(2k+1).$$

Harus dibuktikan $S(k+1)$ benar, yaitu

$$\sum_{i=1}^{k+1} i^2 = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 = \frac{1}{6}(k+1)(k+2)(2k+3)$$

$$\sum_{i=1}^{k+1} i^2 = \underbrace{1^2 + 2^2 + \dots + k^2}_{\frac{1}{6}k(k+1)(2k+1)} + (k+1)^2 = \frac{1}{6}k(k+1)(2k+1) + (k+1)^2$$

$$= (k+1) \left\{ \frac{1}{6}k(2k+1) + (k+1) \right\}$$

$$= \frac{1}{6}(k+1) \{k(2k+1) + 6(k+1)\}$$

$$= \frac{1}{6}k(k+1) + (2k^2 + k + 6k + 6)$$

$$= \frac{1}{6}(k+1)(2k^2 + 7k + 6)$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3)$$

Jadi, $S(n)$ benar untuk sebarang $n \in Z^+$.

Contoh 1.6

Buktikan: untuk semua $n \in Z^+$, dan $n \geq 6$, $4n < n^2 - 7$

Bukti:

$$S(n) : 4n < n^2 - 7, n \geq 6$$

$S(6)$ benar sebab untuk $n = 6$

$$4n = 4 \cdot 6 = 24, n^2 - 7 = 6^2 - 7 = 36 - 7 = 31, \text{ dan } 24 < 31$$

Misalkan $S(k)$ benar, yaitu untuk $n = k \geq 6$.

$$4k < k^2 - 7$$

Harus dibuktikan bahwa $S(k+1)$ benar, yaitu untuk $n = k + 1$.

$$4(k+1) < (k+1)^2 - 7, \text{ perhatikan}$$

$$4(k+1) = 4k + 4 < (k^2 - 7) + 4$$

$$4k + 4 < (k^2 - 7) + 13, \text{ sebab } 4 < 13$$

$$4k + 4 < (k^2 - 7) + (2k + 1), \text{ sebab } 2k + 1 \geq 13 \text{ untuk } n \geq 6$$

$$4k + 4 < (k^2 + 2k + 1) - 7$$

$$4k + 4 < (k+1)^2 - 7$$

Jadi: $4n < n^2 - 7$ untuk semua bilangan bulat $n \geq 6$.

Contoh 1.7

Buktikan: $6^{n+2} + 7^{2n+1}$ habis dibagi oleh 43 untuk semua $n \in \mathbb{Z}^+$.

Bukti:

Misalkan $S(n): 6^{n+2} + 7^{2n+1}$ habis dibagi oleh 43

$S(1)$ benar sebab untuk $n = 1$: maka

$$6^{n+2} + 7^{2n+1} = 6^3 + 7^5 = 559 = 43(13) \text{ habis dibagi oleh 43}$$

Misalkan $S(k)$ benar, yaitu untuk $n = k$:

$$6^{k+2} + 7^{2k+1} \text{ habis dibagi oleh 43}$$

Misalkan $6^{k+2} + 7^{2k+1} = p \cdot 43$ untuk suatu $p \in \mathbb{Z}^+$.

Harus dibuktikan bahwa $S(k+1)$ benar, yaitu untuk

$$n = k + 1, 6^{k+3} + 7^{2k+3} \text{ habis dibagi oleh 43}$$

$$(6^{k+3} + 7^{2k+3}) - (6^{k+2} + 7^{2k+1})$$

$$= (6^{k+3} - 6^{k+2}) + (7^{2k+3} - 7^{2k+1})$$

$$= 6^{k+2}(6-1) + 7^{2k+1}(7^2 - 1)$$

$$= 5 \cdot 6^{k+2} + 48 \cdot 7^{2k+1}$$

$$= 5 \cdot 6^{k+2} + (5 + 43) \cdot 7^{2k+1}$$

$$= 5(6^{k+2} + 7^{2k+1}) + 43 \cdot 7^{2k+1}$$

$$= 5 \cdot 43p + 43 \cdot 7^{2k+1}$$

$$6^{k+3} + 7^{2k+3} - 43p = 5 \cdot 43p + 43 \cdot 7^{2k+1}$$

$$6^{k+3} + 7^{2k+3} = 6(43p) + 43 \cdot 7^{2k+1}$$

$$= 43(6p + 7^{2k+1})$$

$6^{k+3} + 7^{2k+3}$ habis dibagi oleh 43 sebab mempunyai faktor 43

Jadi: $6^{n+3} + 7^{2n+3}$ habis dibagi oleh 43 untuk semua $n \in \mathbb{Z}^+$.

Tugas

Buktikan dengan induksi matematika

- 1) $n < 2^n$ untuk semua $n \in \mathbb{Z}^+$.
- 2) $n^3 - n$ habis dibagi 3 untuk semua $n \in \mathbb{Z}^+$.
- 3) $2^n < n!$ untuk setiap bilangan bulat positif $n \geq 4$.

Petunjuk Jawaban Tugas

- 1) $S(n) : n < 2^n$

$S(1)$: benar sebab untuk $n = 1$: $n = 1$, $2^n = 2^1 = 2$, dan $1 < 2$

Misalkan $S(k)$ benar, yaitu $k < 2^k$

Harus dibuktikan bahwa $S(k+1)$ benar, yaitu $(k+1) < 2^{k+1}$

$$k < 2^k \rightarrow k+1 < 2^k + 1$$

$$\rightarrow k+1 < 2^k + 2^k \text{ (sebab } 2^k \geq 1 \text{ untuk sebarang } k \geq 1\text{)}$$

$$\rightarrow k+1 < 2 \cdot 2^k$$

$$\rightarrow k+1 < 2^{k+1}$$

Jadi: $n < 2^n$ untuk setiap $n \in \mathbb{Z}^+$.

- 2) $S(n) : n^3 - n$ habis dibagi oleh 3

$S(1)$ benar sebab untuk $n = 1$:

$$n^3 - n = 1^3 - 1 = 1 - 1 = 0 \text{ dan } 0 \text{ habis dibagi oleh 3.}$$

Misalkan $S(k)$ benar, yaitu $k^3 - k$ habis dibagi oleh 3, sebut $k^3 - k = p \cdot 3$ untuk suatu $p \in \mathbb{Z}^+$

Harus dibuktikan bahwa $S(k+1)$ benar, yaitu

$$(k+1)^3 - (k+1) \text{ habis dibagi oleh 3}$$

$$(k+1)^3 - (k+1) = (k^3 + 3k^2 + 3k + 1) - (k+1)$$

$$= (k^3 - k) + 3(k^2 + k)$$

$$= 3p + 3(k^2 + k)$$

$$= 3(p + k^2 + k)$$

$(k+1)^3 - (k+1)$ habis dibagi 3 sebab mempunyai faktor 3

Jadi: $n^2 - n$ habis dibagi 3 untuk setiap $n \in \mathbb{Z}^+$.

- 3) $S(n): 2^n < n!$ untuk setiap bilangan bulat positif $n \geq 4$

$S(4)$ benar sebab untuk $n = 4$:

$$2^n = 2^4 = 16, n! = 4! = 24, \text{ dan } 16 < 24$$

Misalkan $S(k)$ benar, yaitu $2^k < k!$

Harus dibuktikan bahwa $S(k+1)$ benar yaitu:

$$2^{k+1} < (k+1)!$$

$$2^{k+1} = 2^k \cdot 2 < 2 \cdot k!$$

$$2^{k+1} < (k+1) \cdot k! \text{ sebab } k+1 \geq 2 \text{ untuk sebarang } k \in \mathbb{Z}^+$$

$$2^{k+1} < (k+1)!$$

Jadi: $2^{k+1} < (k+1)!$ untuk setiap bilangan asli n .



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

Buktikan dengan induksi matematika

- 1) Di dalam barisan harmonis:

$$H_t = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{t}.$$

berlaku

$$H_{2^n} \geq 1 + \frac{n}{2}, \text{ untuk setiap bilangan bulat } n \geq 0.$$

- 2) $\frac{dx^n}{dx} = nx^{n-1}$ untuk setiap bilangan bulat $n \geq 0$.

$$3) \sum_{k=1}^n \frac{1}{k(k+1)} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

$$4) \sum_{t=1}^r t^2 = 1^2 + 2^2 + 3^2 + \dots + r^2 = r(r+1)(2r+1)/6 \text{ untuk setiap } n \in \mathbb{Z}^+.$$

$$5) \sum_{r=2}^s \frac{1}{r^2 - 1} = \frac{1}{3} + \frac{1}{8} + \frac{1}{15} + \frac{1}{24} + \dots + \frac{1}{s^2 - 1} = \frac{3}{4} - \frac{2s+1}{2s(s+1)}$$

dengan menggunakan hubungan:

$$\frac{1}{s^2 - 1} = \frac{1}{2} \left(\frac{1}{s-1} - \frac{1}{s+1} \right)$$

Petunjuk Jawaban Latihan

1) $S(n): H_{2^n} \geq 1 + \frac{n}{2}$ untuk setiap bilangan bulat $n \geq 0$

$$H_t = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{t}$$

$S(0)$ benar sebab untuk $n = 0$:

$$H_{2^0} = H_1 = 1, 1 + \frac{n}{2} = 1 + 0, \text{ dan } 1 \geq 0$$

Misalkan H_{2^k} benar, yaitu untuk $n = k$:

$$H_{2^k} \geq 1 + \frac{k}{2}$$

Harus dibuktikan $H_{2^{k+1}}$ benar, yaitu untuk $n = k + 1$:

$$H_{2^{k+1}} \geq 1 + (k+1)/2$$

Perhatikan

$$\begin{aligned} H_{2^{k+1}} &= 1 + \underbrace{\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k}}_{H_{2^k}} + \frac{1}{2^k + 1} + \frac{1}{2^k + 2} + \dots + \frac{1}{2^{k+1}} \\ &= H_{2^k} + \frac{1}{2^k + 1} + \dots + \frac{1}{2^{k+1}} \\ &\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2^k + 1} + \dots + \frac{1}{2^{k+1}} \\ &\geq \left(1 + \frac{k}{2}\right) + 2^k \cdot \frac{1}{2^{k+1}} + \dots + \frac{1}{2^{k+1}} \text{ sebab terdapat } 2^n \text{ suku masing-masing} \end{aligned}$$

tidak kurang dari $\frac{1}{2^{k+1}}$

$$\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2}$$

$$H_{2^{k+1}} \geq 1 + (k+1)/2$$

Jadi $H_{2^{n+1}} \geq 1 + (n+1)/2$ untuk sebarang bilangan bulat $n \geq 0$.

2) $S(n): \frac{dx^n}{dx} = nx^{n-1}$ untuk setiap bilangan bulat $n \geq 0$.

$S(0)$ benar sebab $\frac{dx^0}{dx} = \frac{d}{dx} = 0$, dan $nx^{n-1} = 0 \cdot x^{-1} = 0$

Misalkan $S(k)$ benar, yaitu $\frac{dx^k}{dx} = kx^{k-1}$

Harus dibuktikan $S(k+1)$ benar, yaitu $\frac{dx^{k+1}}{dx} = (k+1)x^k$. Dari Kalkulus,

$$\frac{dx^k}{dx} = \lim_{\Delta x \rightarrow 0} \frac{(x + \Delta x)^k - x^k}{\Delta x}. \text{ Maka}$$

$$\begin{aligned}\frac{dx^{k+1}}{dx} &= \lim_{\Delta x \rightarrow 0} \frac{(x + \Delta x)^{k+1} - x^{k+1}}{\Delta x} \\ &= \lim_{\Delta x \rightarrow 0} \frac{(x + \Delta x)^k \cdot (x + \Delta x) - x^{k+1}}{\Delta x} \\ &= \lim_{\Delta x \rightarrow 0} \frac{(x + \Delta x)^k x + (x + \Delta x)^k \cdot \Delta x - x^k \cdot x}{\Delta x} \\ &= \lim_{\Delta x \rightarrow 0} \left\{ x \frac{(x + \Delta x)^k - x^k}{\Delta x} + \frac{(x + \Delta x)^k \cdot \Delta x}{\Delta x} \right\} \\ &= xk^k x^{k-1} + x^k \\ &= kx^k + x^k \\ &= (k+1)x^k\end{aligned}$$

3) Cara 1:

Gunakan hubungan:

$$\frac{1}{t(t+1)} = \frac{1}{t} - \frac{1}{t+1} \text{ untuk mengganti setiap suku deret.}$$

Cara ini disebut cara teleskopis

Cara 2:

Gunakan induksi matematika, tunjukkan:

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

4) Tunjukkan bahwa

$$k(k+1)(2k+1)/6 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$$

$$\begin{aligned} 5) \quad \sum_{r=2}^s \frac{1}{r^2 - 1} &= \sum_{r=2}^s \frac{1}{2} \left(\frac{1}{r-1} - \frac{1}{r+1} \right) = \frac{1}{2} \sum_{r=2}^s \left(\frac{1}{r-1} - \frac{1}{r} + \frac{1}{r} - \frac{1}{r+1} \right) \\ &= \frac{1}{2} \sum_{r=2}^s \left\{ \left(\frac{1}{r-1} - \frac{1}{r} \right) + \left(\frac{1}{r} - \frac{1}{r+1} \right) \right\} \\ &= \frac{1}{2} \sum_{r=2}^s \left(\frac{1}{r-1} - \frac{1}{r} \right) + \frac{1}{2} \sum_{r=2}^s \left(\frac{1}{r} - \frac{1}{r+1} \right) \\ &= \frac{1}{2} \left(1 - \frac{1}{s} \right) + \frac{1}{2} \left(\frac{1}{2} - \frac{1}{s+1} \right) \\ &= \frac{3}{4} - \frac{2s+1}{2s(s+1)} \end{aligned}$$



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang induksi matematika, terutama tentang notasi jumlah dan sifat-sifatnya, notasi kali dan sifat-sifatnya, prinsip pertama induksi matematika, dan pernyataan lain induksi matematika. Hal lain yang ditampilkan berkaitan dengan hubungan jumlah deret, hubungan pertidaksamaan, hubungan keterbagian, dan hubungan diferensial.

1. Notasi Jumlah dan Kali

$$\sum_{i=1}^r x_i = x_1 + x_2 + \dots + x_r$$

$$\prod_{i=1}^r x_i = x_1 \cdot x_2 \cdot \dots \cdot x_r$$

2. Sifat-sifat:

$$(a) \quad \sum_{i=r}^s t x_i = t \sum_{i=r}^s x_i$$

$$(b) \quad \sum_{i=r}^s (x_i + y_i) = \sum_{i=r}^s x_i + \sum_{i=r}^s y_i$$

$$(c) \quad \sum_{i=a}^b \sum_{j=c}^d x_i y_j = \left(\sum_{i=a}^b x_i \right) \left(\sum_{j=c}^d y_j \right)$$

$$(d) \sum_{i=a}^b \sum_{j=c}^d x_i y_j = \sum_{j=c}^d \sum_{i=a}^b x_i y_j$$

3. Prinsip Induksi Matematika

S adalah suatu himpunan bagian dari himpunan bilangan asli yang unsur-unsurnya memenuhi hubungan:

Jika: (a) $1 \in S$

(b) $k \in S$ berakibat $(k+1) \in S$

maka: S memuat semua bilangan asli, yaitu $S = N$.

4. Pernyataan Lain Induksi Matematika

$S(n)$ adalah suatu pernyataan yang memenuhi hubungan untuk satu atau lebih $n \in N$.

Jika: (a) $S(1)$ benar

(b) $S(k)$ benar berakibat $S(k+1)$ benar

maka $S(k)$ benar untuk semua $n \in N$.



TES FORMATIF 2

Pilihlah satu jawaban yang paling tepat!

1) Skor 10

$$\text{Carilah } \sum_{t=2}^5 3$$

2) Skor 10

$$\text{Carilah } \prod_{k=3}^6 2$$

3) Skor 15

$$\text{Carilah } \sum_{r=1}^5 \sum_{s=1}^6 rs$$

4) Skor 15

$$\text{Carilah } \sum_{s=1}^3 \prod_{t=1}^4 st$$

5) Skor 20

$$\text{Carilah } \sum_{s=1}^t \frac{1}{s(s+1)}$$

6) Skor 10

$$\text{Carilah } \sum_{k=1}^{50} k^2$$

7) Skor 10

$$\text{Carilah } \sum_{m=1}^n m(m+1)$$

8) Skor 5

$$\text{Carilah } \sum_{r=0}^{10} (-2)^r$$

9) Skor 5

$$\text{Carilah } 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + 10 \cdot 11$$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) Misalkan $a, b, c \in \mathbb{Z}, a < b$ dan $c > 0$, maka sesuai definisi $b - a > 0$. Karena himpunan bilangan bulat positif tertutup terhadap perkalian, $c > 0$, dan $b - a > 0$, maka $c(b - a) > 0$ atau $cb - ca > 0$, berarti $ca < cb$ atau $ac < bc$.
- 2) Misalkan ada bilangan bulat positif kurang dari 1, maka sesuai dengan prinsip urutan yang rapi, $\mathbb{Z}^+ \subset \mathbb{Z}^+$ dan \mathbb{Z}^+ tidak kosong dan mempunyai unsur terkecil a sehingga $a < 1$, dengan $a > 0$. Selanjutnya $a^2 = a \cdot a < 1 \cdot a = a$. Karena $a^2 > 0$, berarti a^2 adalah suatu bilangan bulat positif kurang dari a , merupakan kontradiksi.
- 3)
 - (a) terurut rapi
 - (b) terurut rapi
 - (c) tidak terurut rapi
 - (d) terurut rapi
 - (e) tidak terurut rapi
 - (f) tidak terurut rapi
- 4)
 - (a) 0
 - (b) 0
 - (c) 5
 - (d) -2
- 5) Dari $[x] \leq x \leq [x]+1$ dapat ditentukan bahwa $[x]+k \leq x+k \leq [x]+k+1$. Karena $[x]+k$ adalah suatu bilangan bulat, maka $[x+k]=[x]+k$.
- 6) Jika x adalah suatu bilangan bulat, maka $[x]+[-x]=x-x=0$. Jika x bukan bilangan bulat, maka $x=z+r$, di mana z adalah suatu bilangan bulat dan r adalah suatu bilangan riil dengan $0 < r < 1$. Dengan demikian dapat ditentukan bahwa

$$[x]+[-x]=[z+r]+[-z-r]=z+(-z-1)=-1.$$
- 7) Misalkan $x=[x]+r$ dengan $0 \leq r < 1$. Jika $r < (1/2)$, maka $x+(1/2)=[x]+\{r+(1/2)\} < [x]+1$ karena $r+(1/2) < 1$. Akibatnya, $[x+(1/2)]=[x]$, berarti $2x=2[x]+2r < 2[x]+1$ karena $2r < 1$. Jadi $[2x]=2[x]$.

Jika $(1/2) \leq r < 1$, maka $[x]+1 \leq x + \{r + (1/2)\} < [x]+2$, berarti
 $[x] + (1/2) < [x] + 1$.

Akibatnya,

$$2[x]+1 \leq 2[x]+2r = 2([x]+r) = 2x < 2[x]+2$$

Sehingga

$$[2x] = 2[x]+1, \text{ dan } [x] + [x + (1/2)] = [x] + [x] + 1 = 2[x] + 1 = [2x]$$

- 8) Misalkan $\sqrt{2}$ adalah suatu bilangan rasional, maka tentu ada bilangan-bilangan bulat a dan b sehingga $\sqrt{2} = a/b$. Akibatnya, $S = \{k\sqrt{2} \mid k \in \mathbb{Z}^+\}$ adalah suatu himpunan bilangan bulat positif yang tidak kosong, sehingga S mempunyai unsur terkecil $s = t\sqrt{2}$. Dengan demikian $s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s-t)\sqrt{2}$.

Karena $s\sqrt{2} = 2t$ dan s merupakan bilangan-bilangan bulat, maka:

$s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s-t)\sqrt{2}$ juga merupakan suatu bilangan bulat, dan $s\sqrt{2} - s = s(\sqrt{2} - 1) > 0$ karena $\sqrt{2} > 1$, $s\sqrt{2} - s < s$ karena $s = t\sqrt{2}$, $s\sqrt{2} = 2t$ dan $\sqrt{2} < 2$. Hal ini bertentangan dengan pemilihan s sebagai unsur bulat positif terkecil dari S . Jadi $\sqrt{2}$ adalah irasional.

Tes Formatif 2

Gunakan Prinsip Induksi Matematika beserta sifat-sifat notasi jumlah dan kali sehingga diperoleh:

$$1) \quad \sum_{t=2}^5 3 = 3+3+3+3 = 12$$

$$2) \quad \prod_{k=2}^6 2 = 2.2.2.2 = 16$$

$$3) \quad \sum_{r=1}^5 \sum_{s=1}^6 rs = \sum_{r=1}^5 (r+2r+3r+4r+5r+6r) = \sum_{r=1}^5 21r = 21 \sum_{r=1}^5 r$$

$$4) \quad \sum_{s=1}^3 \prod_{t=1}^4 st = \sum_{s=1}^3 (s.2s.3s.4s) = \sum_{s=1}^3 24s^4 = 24 \sum_{s=1}^3 s^4$$

$$5) \quad \sum_{s=1}^t \frac{1}{s(s+1)} = \sum_{s=1}^t \left(\frac{1}{s} - \frac{1}{s+1} \right) = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \dots + \left(\frac{1}{t} - \frac{1}{t+1}\right)$$

$$6) \quad \sum_{k=1}^{50} k^2 = \frac{1}{6}(50)(50+1)(100+1) = 42925$$

$$\begin{aligned}7) \quad \sum_{m=1}^n m(m+1) &= \sum_{m=1}^n (m^2 + m) = \sum_{m=1}^n m^2 + \sum_{m=1}^n m = \frac{1}{6}n(n+1)(2n+1) + \frac{1}{2}n(n+1) \\&= \frac{1}{3}n(n+1)(n+2) \\8) \quad \sum_{r=0}^{10} (-2)^r &= 1 - 2 + 4 - 8 + 16 - 32 + 64 - 128 + 256 - 512 + 1024 = 683 \\9) \quad 2 + 6 + 12 + \dots + 110 &= 1.2 + 2.3 + 3.4 + \dots + 10.11 = \frac{1}{3}.10.11.12 = 440\end{aligned}$$

Daftar Pustaka

- Agnew, J. (1972). *Exploration in Number Theory*. Belmont: Brooks/Cole.
- Anderson, J.A. and Bell, J.M. (1977). *Number Theory with Applications*. New Jersey: Prentice-Hall.
- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Ore, O. (1948). *Number Theory and Its History*. New York: McGraw-Hill.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Keterbagian Bilangan Bulat

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul Keterbagian Bilangan Bulat ini diuraikan tentang sifat-sifat dasar keterbagian, algoritma pembagian, konsep-konsep dasar faktor persekutuan terbesar (FPB) dan kelipatan persekutuan terkecil (KPK) dan penerapannya, Algoritma Euclides, serta keprimaan.

Keterbagian (*divisibility*) merupakan bahan dasar dalam uraian lebih lanjut tentang pembahasan teori bilangan. Setelah pembahasan tentang FPB dan KPK, sifat-sifat dasar keterbagian dapat diperluas menjadi lebih lengkap dan mendalam. Demikian pula pembahasan tentang FPB dan KPK beserta sifat-sifatnya dapat lebih dikembangkan dan dikaitkan dengan keterbagian. Penerapan Algoritma Euclides dalam pembahasan FPB dan KPK merupakan bahan yang memberikan peluang kemudahan untuk mencari FPB dan KPK dari bilangan-bilangan yang relatif besar, dan untuk menyatakan suatu FPB sebagai kombinasi linier dari bilangan-bilangan komponennya.

Secara keseluruhan, materi pokok dalam modul ini meliputi keterbagian, FPB dan KPK, dan keprimaan. Keterkaitan antara ketiga materi pokok menjadi lebih jelas setelah berbagai kasus dipaparkan dan diselesaikan melalui contoh, tugas, latihan, dan tes formatif.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep dan sifat keterbagian, FPB dan KPK, keprimaan, dan keterkaitan antara ketiga topik pokok.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep keterbagian dan sifat-sifatnya, konsep FPB dan KPK serta sifat-sifatnya, konsep keprimaan dan sifat-sifatnya, serta keterkaitan satu sama lain untuk menyelesaikan masalah-masalah tertentu.

Susunan Kegiatan Belajar

Modul 2 ini terdiri dari dua Kegiatan Belajar. Kegiatan Belajar 1 adalah Keterbagian Bilangan Bulat, dan Kegiatan Belajar 2 adalah FPB dan KPK. Setiap kegiatan belajar memuat Uraian, Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 2 ini ditempatkan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi pembahasan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab, maka pelajari Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum berhasil menjawab permasalahan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Penguasaan Anda dengan cara mencocokkan jawaban Anda dengan Petunjuk Jawaban Tes Formatif. Ulangilah penggerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Konsep Dasar Keterbagian**

embagian bilangan bulat merupakan bahan pelajaran matematika yang sudah diberikan di Sekolah Dasar. Bahan pelajaran ini diperluas penggunaannya sampai pada pemfaktoran prima, faktor persekutuan terbesar (FPB), kelipatan persekutuan terkecil (KPK), dan keterbagian oleh bilangan tertentu (misalnya keterbagian oleh 2, 3, atau 9). Untuk memberikan dasar atau landasan yang lebih kuat, maka guru matematika di sekolah perlu belajar lebih mendalam tentang konsep-konsep dasar keterbagian.

Keterbagian (*divisibility*) merupakan dasar pengembangan teori bilangan, sehingga konsep-konsep keterbagian akan banyak digunakan di dalam uraian atau penjelasan matematis tentang pembuktian teorema.

Jika suatu bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka hasil baginya adalah suatu bilangan bulat atau suatu bilangan yang tidak bulat, misalnya, jika 40 dibagi 8, maka hasil baginya adalah bilangan bulat 5; tetapi jika 40 dibagi 16, maka hasil baginya adalah 2,5. Keadaan inilah yang memberikan gagasan tentang perlunya definisi keterbagian.

Definisi 2.1

Suatu bilangan bulat q habis dibagi oleh suatu bilangan bulat $p \neq 0$ jika ada suatu bilangan bulat x sehingga $q = px$.

Notasi

$p | q$ dibaca p membagi q , p faktor dari q , q habis dibagi p , atau q kelipatan dari p .

$p \nmid q$ dibaca p tidak membagi q , p bukan faktor dari q , q tidak habis dibagi p , atau q bukan kelipatan dari p .

Contoh 2.1

- $6 | 18$ sebab ada bilangan bulat 3 sehingga $18 = 6 \cdot 3$
- $12 \nmid 15$ sebab tidak ada bilangan bulat x sehingga $15 = 12 \cdot x$
- $5 | -30$ sebab ada bilangan bulat -6 sehingga $-30 = 5 \cdot (-6)$
- $-4 | 20$ sebab ada bilangan bulat 5 sehingga $20 = (-4) \cdot 5$

Berdasarkan Definisi 2.1 di atas jelas bahwa faktor-faktor suatu bilangan bisa merupakan bilangan bulat positif atau merupakan bilangan bulat negatif. Dengan demikian, faktor-faktor dari:

6, adalah 1, -1, 2, -2, 3, -3, 6, dan -6

15, adalah 1, -1, 3, -3, 5, -5, 15, dan -15

Beberapa sifat sederhana keterbagian adalah:

1. $1|p$ untuk setiap $p \in \mathbb{Z}$
2. $p|0$ untuk setiap $p \in \mathbb{Z}$ dan $p \neq 0$
3. $p|p$ untuk setiap $p \in \mathbb{Z}$ dan $p \neq 0$
4. Jika $p|q$, maka kemungkinan hubungan antara p dan q adalah $p < q$, $p = q$, atau $p > q$ (misalnya $3|6$, $3|3$, atau $3|-3$).

Teorema 2.1

Jika $p, q \in \mathbb{Z}$ dan $p|q$, maka $p|qr$ untuk semua $r \in \mathbb{Z}$

Bukti:

Diketahui bahwa $p|q$, maka menurut Definisi 2.1, ada suatu $x \in \mathbb{Z}$ sehingga $q = px$. $q = px$ berarti $qr = pxr$, atau $qr = p(x.r)$ dengan $xr \in \mathbb{Z}$ (sebab $x \in \mathbb{Z}$ dan $r \in \mathbb{Z}$).

Sesuai dengan Definisi 2.1, karena $qr = p(xr)$ maka $p|qr$.

Teorema 2.2

Jika $p, q, r \in \mathbb{Z}$, $p|q$, dan $q|r$, maka $p|r$.

Bukti:

Diketahui $p|q$ dan $q|r$, maka menurut Definisi 2.1, tentu ada $x, y \in \mathbb{Z}$ sehingga $q = px$ dan $r = qy$. $r = qy$ dan $q = px$, maka $r = (px)y$ atau $r = p(xy)$ dengan $x, y \in \mathbb{Z}$.

Sesuai dengan Definisi 2.1, karena $r = p(xy)$, maka $p|r$.

Teorema 2.3

Jika $p, q \in \mathbb{Z}$, $p|q$ dan $q|p$, maka $p = \pm q$

Bukti:

Diketahui $p \mid q$ dan $q \mid p$ maka menurut Definisi 2.1, terdapat $x, y \in Z$ sehingga $p = qx$ dan $q = py$.

Jadi $p = qx = (py)x = p(yx) = p(xy) = (xy)p$, atau $1 \cdot p = (xy)p$, sehingga $xy = 1$. Dengan demikian, karena $x, y \in Z$ dan $xy = 1$, maka diperoleh $x = -1 = y$ atau $x = 1 = y$.

Jika $x = -1 = y$, maka $p = -q$

Jika $x = 1 = y$, maka $p = q$

Teorema 2.4

Jika $p, q, r \in Z$, $p \mid q$ dan $p \mid r$, maka $p \mid q+r$

Bukti:

Karena $p \mid q$ dan $p \mid r$, maka menurut Definisi 2.1, ada $x, y \in Z$ sehingga $q = px$ dan $r = py$. Dengan demikian $q + r = px + py = p(x + y)$

Karena $x, y \in Z$, maka sesuai dengan sifat tertutup penjumlahan bilangan bulat, $x + y \in Z$. Jadi $p \mid q+r$.

Teorema 2.4 dapat diperluas tidak hanya berlaku untuk q, r tetapi untuk q, r, s, t, \dots , artinya jika $p \mid q, p \mid r, p \mid s, p \mid t, \dots$, maka $p \mid q+r+s+t+\dots$

Selanjutnya, Teorema 2.4 tetap berlaku jika operasi penjumlahan (+) diganti dengan operasi pengurangan (-), buktikan!

Teorema 2.5

Jika $p, q, r \in Z$, $p \mid q$ dan $p \mid r$, maka $p \mid qx+ry$ untuk semua $x, y \in Z$ ($qx + ry$ disebut kombinasi linear dari q dan r).

Buktikan!

Teorema 2.6.

Jika $p, q, r \in Z$, $p > 0$, $q > 0$, dan $p \mid q$, maka $p \leq q$

Bukti:

Karena $p \mid q$, maka menurut Definisi 2.1, ada $x \in \mathbb{Z}$ sehingga $q = px$.

Karena $p > 0$, $q > 0$, dan $q = px$, maka $x > 0$, atau $x \in \mathbb{N}$. Karena \mathbb{N} himpunan bilangan bulat positif. Karena himpunan bilangan bulat positif terurut rapi, maka terdapat unsur terkecil yaitu 1, sehingga $q = px \geq p \cdot 1 = p$.

Jadi $p \leq q$.

Teorema 2.7

Jika $p, q, r \in \mathbb{Z}$, $p > 0$, $q > 0$, $p \mid q$ dan $q \mid p$, maka $p = q$.

Buktikan!

Teorema 2.8

$p \mid q$ jika dan hanya jika $kp \mid kq$ untuk semua $k \in \mathbb{Z}$ dan $k \neq 0$.

Buktikan!

Teorema 2.9

Jika $p, q, r \in \mathbb{Z}$, $p \neq 0$, $p \mid q+r$, dan $p \mid q$, maka $p \mid r$.

Buktikan!

Uraian berikutnya membahas tentang algoritma pembagian. Suatu algoritma didefinisikan sebagai serangkaian langkah-langkah atau prosedur yang jelas dan terhingga untuk menyelesaikan suatu masalah. Kita lazim menggunakan istilah algoritma pembagian (*division algorithm*) meskipun istilah ini tidak menunjukkan adanya algoritma. Pembicaraan algoritma sebagai prosedur dalam menyelesaikan masalah terdapat pada pembahasan tentang Algoritma Euclides.

Teorema 2.10, Algoritma Pembagian

Jika $p, q \in \mathbb{Z}$ dan $p > 0$, maka ada bilangan-bilangan $r, s \in \mathbb{Z}$ yang masing-masing tunggal sehingga $q = rp + s$ dengan $0 \leq s < p$.

Jika p tidak membagi q , maka s memenuhi ketidaksamaan $0 < s < p$.

Dari pernyataan $q = rp + s$, $0 \leq s < p$, maka r disebut hasil bagi (*quotient*), s disebut sisa (*remainder*), q disebut yang dibagi (*dividend*), dan p disebut pembagi (*divisor*). Kita secara tradisi menggunakan istilah algoritma

meskipun sesungguhnya algoritma pembagian bukan merupakan suatu algoritma.

Sebelum membuktikan Teorema 2.10, agar lebih mudah dalam memahami langkah-langkah pembuktian, simaklah dengan cermat uraian berikut:

Ditentukan dua bilangan bulat 4 dan 7 dengan, maka dapat dibuat barisan aritmetika $7 - (r \cdot 4)$ dengan $r \in \mathbb{Z}$

$$\text{untuk } r = 3, 7 - (r \cdot 4) = 7 - 12 = -5$$

$$\text{untuk } r = 2, 7 - (r \cdot 4) = 7 - 8 = -1$$

$$\text{untuk } r = 1, 7 - (r \cdot 4) = 7 - 4 = 3$$

$$\text{untuk } r = 0, 7 - (r \cdot 4) = 7 - 0 = 7$$

$$\text{untuk } r = -1, 7 - (r \cdot 4) = 7 - (-4) = 11$$

dan seterusnya

sehingga diperoleh barisan $\dots, -5, -1, 3, 7, 11, \dots$

Barisan ini mempunyai suku-suku yang negatif, dan suku-suku yang tidak negatif. Misalkan T adalah himpunan suku-suku tersebut yang tidak negatif, maka

$$T = \{3, 7, 11, \dots\} \text{ atau } T = \{7 - (4 \cdot r) \mid r \in \mathbb{Z}, 7 - (4 \cdot r) \geq 0\}$$

Karena $T \subset N$ dan N adalah himpunan yang terurut rapi, maka menurut prinsip urutan rapi, T mempunyai unsur terkecil yaitu 3. Karena $3 \in T$, maka $3 = 7 - (4 \cdot r)$ untuk suatu $r \in \mathbb{Z}$. dalam hal ini $r = 1$, sehingga $3 = 7 - (4 \cdot 1)$, atau $7 = 1 \cdot 4 + 3$. Dengan demikian dapat ditentukan bahwa: $7 = 1 \cdot 4 + 3$ dengan $0 \leq 3 < 4$, sehingga $7 = r \cdot 4 + s$ dengan $r = 1$ dan $s = 3$.

Oleh karena itu untuk $4, 7 \in \mathbb{Z}$, ada $r, s \in \mathbb{Z}$ sehingga $7 = r \cdot 4 + s$ dengan $0 \leq s < 4$.

Marilah sekarang kita membuktikan Teorema 2.10

Bukti:

Misalkan $p, q \in \mathbb{Z}$ dan $p > 0$ suatu barisan aritmetika $(q - rp)$ dengan $r \in \mathbb{Z}$, yaitu $\dots, q - 3p, q - 2p, q - p, q, q + 2p, q + 3p, \dots$ yang mempunyai bentuk umum $q - rp$.

Ambil suatu himpunan T yang unsur-unsurnya adalah suku barisan yang tidak negatif, yaitu: $T = \{q - rp \mid r \in \mathbb{Z}, q - rp \geq 0\}$.

Karena $T \subset N$ dan N adalah himpunan yang terurut rapi, maka menurut prinsip urutan rapi, T mempunyai unsur terkecil, misalnya s .

Karena $s \in T$, maka $s = q - rp$ untuk suatu $r \in \mathbb{Z}$, sehingga $q = rp + s$.

Sampai di sini pembuktian baru pada tahap menunjukkan eksistensi dari r dan s . Berikutnya akan dibuktikan bahwa $0 \leq s < p$ dengan menggunakan bukti tidak langsung.

Anggaplah bahwa $0 \leq s < p$ tidak benar, jadi $s < 0$ atau $s \geq p$.

Karena $s \in T$, maka s tidak mungkin negatif, sehingga kemungkinannya tinggal $s \geq p$. Karena $s \geq p$, maka $s - p \geq 0$, maka

$$s - p = (q - rp) - p = q - (r + 1)p \geq 0, \text{ sehingga } 3 - p \in T.$$

Karena $p > 0$, maka $s - p < s$, sehingga $s - p$ merupakan unsur T yang lebih kecil dari s . Hal ini bertentangan dengan pengambilan s sebagai unsur terkecil dari T .

Jadi $0 \leq s < p$.

Selanjutnya, buktikan sendiri ketunggalan dari r dan s .

Petunjuk: gunakan bukti tidak langsung, misalnya r dan s tidak tunggal, yaitu ada $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ yang memenuhi:

$$q = r_1 p + s_1, 0 < s_1 < p \text{ dan } q = r_2 p + s_2, 0 < s_2 < p$$

Contoh 2.1

Tunjukkan:

- Jika $p \mid q$, maka $p^2 \mid q^2$
- Jika $p \mid q$, maka $p \mid 3q^2$

Jawab:

- Karena $p \mid q$, maka sesuai dengan Definisi 2.1, ada bilangan $k \in \mathbb{Z}$ sehingga $q = kp$, dengan demikian $q^2 = k^2 p^2$. Karena $k^2 \in \mathbb{Z}$, maka $q^2 \mid p^2$.
- Karena $p \mid q$, maka sesuai dengan Teorema 2.1, $p \mid qr$ untuk semua $r \in \mathbb{Z}$. Ambil $r = 3q$, maka $3q \in \mathbb{Z}$ untuk sebarang $q \in \mathbb{Z}$.

Dengan demikian, dari $p|qr$ dan $r = 3q \in Z$, maka $p|q(3q)$ atau $p|3q^2$.

Contoh 2.2

Diketahui: $t = (a_1 a_0) = a_1 \cdot 10 + a_0$ dan $3|t$

Tunjukkan bahwa $t|a_1 + a_0$.

Jawab:

$$t = a_1 \cdot 10 + a_0 = a_1(9+1) + a_0 = 9a_1 + (a_1 + a_0)$$

$3|t$ atau $3|9a_1 + (a_1 + a_0)$ dan $3|9a_0$, maka menurut Teorema 2.9, $3|a_1 + a_0$

Contoh 2.3

Diketahui:

$$t = (a_4 \ a_3 \ a_2 \ a_1 \ a_0) = a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + 40 \text{ dan } 11|t$$

Tunjukkan bahwa $t|a_0 - a_1 + a_2 - a_3 + a_4$.

Jawab:

$$\begin{aligned} t &= a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &= a_0 + a_1(11-1) + a_2(99+1) + a_3(1001-1) + a_4(9999+1) \\ &= (11a_1 + 99a_2 + 1001a_3 + 9999a_4) + (a_0 - a_1 + a_2 - a_3 + a_4) \end{aligned}$$

$$t = 11(a_1 + 9a_2 + 91a_3 + 909a_4) + (a_0 - a_1 + a_2 - a_3 + a_4)$$

Karena $11|t$, yaitu $11|11(a_1 + 9a_2 + 91a_3 + 909a_4) + (a_0 - a_1 + a_2 - a_3 + a_4)$

dan $11|11(a_1 + 9a_2 + 91a_3 + 909a_4)$ maka menurut Teorema 2.9,

$$11|(a_0 - a_1 + a_2 - a_3 + a_4).$$

Contoh 2.4

Menurut Teorema Algoritma Pembagian, nyatakan berikut ini sebagai $q = rp + s$, $0 \leq s < p$, jika:

- $p = 7$ dan $q = -100$
- $p = 12$ dan $q = -150$

Jawab:

- a. $-100 = (-15)(7) + 5, 0 \leq 5 < 7$
 b. $-150 = (-13)(12) + 6, 0 \leq 6 < 12$

Teorema Algoritma Pembagian dapat digunakan untuk memilahkan atau memisahkan himpunan bilangan bulat menjadi n himpunan bagian yang saling lepas (*disjoint*) dengan $n \in \{2, 3, 4, \dots\}$.

Jika $p = 2$ dan q adalah sebarang bilangan bulat, maka menurut Teorema Algoritma Pembagian, q dapat dinyatakan sebagai: $q = 2p + s, 0 \leq s < 2$.

Karena $r \in \mathbb{Z}$ dan $0 \leq r < 2$, maka kemungkinan nilai-nilai s adalah $s = 0$ dan $s = 1$:

$$\text{untuk } s = 0, q = 2p + s = 2p + 0 = 2p$$

$$\text{untuk } s = 1, q = 2p + s = 2p + 1$$

$q = 2p$ dengan $p \in \mathbb{Z}$ disebut bilangan bulat genap (*even integer*) dan $q = 2p + 1$ dengan $p \in \mathbb{Z}$ disebut bilangan bulat ganjil atau gasal (*odd integer*). Dengan demikian himpunan bilangan bulat dapat dipisahkan menjadi dua himpunan bagian yang lepas, yaitu himpunan bilangan bulat genap dan himpunan bilangan bulat ganjil. Dengan kata lain, setiap bilangan bulat selalu dapat dinyatakan sebagai salah satu dari:

$$q = 2p \text{ atau } q = 2p + 1, p \in \mathbb{Z}$$

Dengan jalan lain yang sama, setiap bilangan bulat selalu dapat dinyatakan sebagai:

$$q = 3p, q = 3p + 1, q = 3p + 2, p \in \mathbb{Z}$$

$$q = 4p, q = 4p + 1, q = 4p + 2, q = 4p + 3, p \in \mathbb{Z}$$

$$q = 5p, q = 5p + 1, q = 5p + 2, q = 5p + 3, q = 5p + 4, p \in \mathbb{Z}$$

dan seterusnya.

Contoh 2.5

Buktikan: $2 \mid n^3 - n$ untuk sebarang $n \in \mathbb{Z}$

Bukti:

Menurut Teorema 2.10 (Algoritma Pembagian), setiap bilangan bulat n dapat dinyatakan sebagai $n = 2p$ atau $n = 2p + 1$.

Untuk $n = 2p$, dapat ditentukan:

$$\begin{aligned} n^3 - n &= n(n^2 - 1) \\ &= n(n-1)(n+1) \\ &= 2p(2p-1)(2p+1) \end{aligned}$$

Jadi $2 \mid n^3 - n$

Untuk $n = 2p + 1$, dapat ditentukan

$$\begin{aligned} n^3 - n &= n(n^2 - 1) \\ &= n(n-1)(n+1) \\ &= (2p+1)(2p+1-1)(2p+1+1) \\ &= 2p(2p+1)(2p+2) \end{aligned}$$

Jadi $2 \mid n^3 - n$

Dengan demikian $2 \mid n^3 - n$ untuk sekarang $n \in \mathbb{Z}$.

Selanjutnya, marilah kita lihat cara mengganti suatu bilangan dalam basis 10 menjadi basis yang lain dengan menggunakan Teorema 2.11 yang dibuktikan dengan Teorema Algoritma Pembagian.

Teorema 2.11

Jika $q \in \mathbb{Z}$ dan $q > 1$, maka setiap $n \in \mathbb{Z}^+$ dapat dinyatakan secara tunggal dalam bentuk $n = p_k q^k + p_{k-1} q^{k-1} + \dots + p_2 q^2 + p_1 q^1 + p_0 q^0$, yang mana $k \in \mathbb{Z}$, $k \geq 0$, $p_t \in \mathbb{Z}$, $0 \leq p_t < q-1$, $t = 0, 1, \dots, k$ dan $p_k \neq 0$.

Bukti:

Karena $q \in \mathbb{Z}$ dan $q > 1$, maka $q > 0$, sehingga menurut Teorema Algoritma pembagian, hubungan antara n dan q adalah:

$$n = qr_0 + p_0, \quad 0 \leq p_0 < q \quad (0 \leq p_0 \leq q-1)$$

Jika $r_0 \neq 0$, maka hubungan antara r_0 dan q menurut Teorema Algoritma Pembagian adalah:

$$r_0 = qr_1 + p_1, \quad 0 \leq p_1 < q \quad (0 \leq p_1 \leq q-1)$$

Jika langkah serupa dikerjakan, maka diperoleh:

$$r_1 = qr_2 + p_2, \quad 0 \leq p_2 < q \quad (0 \leq p_2 \leq q-1)$$

$$r_2 = qr_3 + p_3, \quad 0 \leq p_3 < q \quad (0 \leq p_3 \leq q-1)$$

⋮

$$r_{k-2} = qr_{k-1} + p_{k-1}, \quad 0 \leq p_{k-1} < q \quad (0 \leq p_{k-1} \leq q-1)$$

$$r_{k-1} = qr_k + p_k, \quad 0 \leq p_k < q \quad (0 \leq p_k \leq q-1)$$

Ambil $r_k = 0$, maka barisan r_0, r_1, \dots, r_k merupakan barisan bilangan bulat tidak negatif yang menurun, paling banyak mempunyai suku-suku bernilai nol (yaitu r_k), dan k suku yang positif (yaitu r_0, r_1, \dots, r_{k-1}). Dari hubungan antara n , q , dan r_i ($i = 0, 1, 2, \dots, k$) di atas dapat ditentukan bahwa:

$$\begin{aligned} n &= qr_0 + p_0 \\ &= q(qr_1 + p_1) + p_0 = q^2r_1 + qp_1 + p_0 \\ &= q^2(qr_2 + p_2) + qp_1 + p_0 = q^3r_2 + q^2p_2 + qp_1 + p_0 \\ &= \dots \\ &= q^{k-1}r_{k-2} + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0 \\ &= q^{k-1}(qr_{k-1} + p_{k-1}) + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0 \\ &= q^k r_{k-1} + q^{k-1}p_{k-1} + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0 \\ &= q^k (qr_k + p_k) + q^{k-1}p_{k-1} + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0 \\ n &= q^{k+1}r_k + q^k p_k + q^{k-1}p_{k-1} + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0 \end{aligned}$$

Karena $r_k = 0$, maka:

$$n = q^k p_k + q^{k-1}p_{k-1} + q^{k-2}p_{k-2} + q^{k-3}p_{k-3} + \dots + qp_1 + p_0$$

$$n = p_k q^k + p_{k-1} q^{k-1} + p_{k-2} q^{k-2} + p_{k-3} q^{k-3} + \dots + p_1 q + p_0$$

$$n = (p_k p_{k-1} p_{k-2} p_{k-3} \dots p_1 p_0) q$$

Ini berarti bilangan asli n yang ditulis dalam lambang bilangan basis 10, dapat diubah menjadi lambang bilangan basis $q > 1$.

Agar langkah-langkah dalam pembuktian Teorema 2.10 dapat dipahami dengan sebaik-baiknya, marilah kita lihat suatu peragaan berikut ini.

Ambil $n = 985$ dan $q = 6$

$$985 = 6 \cdot 164 + 1 \quad (n = qr_0 + p_0, r_0 = 164, p_0 = 1)$$

$$164 = 6 \cdot 27 + 2 \quad (r_0 = qr_1 + p_1, r_1 = 27, p_1 = 2)$$

$$27 = 6 \cdot 4 + 3 \quad (r_1 = qr_2 + p_2, r_2 = 4, p_2 = 3)$$

$$4 = 6 \cdot 0 + 4 \quad (r_2 = qr_3 + p_3, r_3 = 0, p_3 = 4)$$

Dengan demikian dapat ditentukan bahwa:

$$985 = 6 \cdot 164 + 1$$

$$= 6(6 \cdot 27 + 2) + 1 = 6^2 \cdot 27 + 6 \cdot 2 + 1$$

$$= 6^2(6 \cdot 4 + 3) + 6 \cdot 2 + 1 = 63 \cdot 4 + 62 \cdot 3 + 6 \cdot 2 + 1$$

Jadi $(985)_{10} = (4321)_6$

Perhatikan pola yang terdapat pada lambang bilangan basis 6 yang dicari. Angka-angka pada lambang bilangan basis 6 yang dicari merupakan sisa dari masing-masing Algoritma Pembagian.

Contoh 2.6.

Tuliskan $(985)_{10}$ dalam lambang bilangan basis 4 dan basis 3.

Jawab:

Ambil $n = 985$ dan $q = 4$. Perhatikan proses berikut ini:

$$985 = 4 \cdot 246 + 1$$

$$246 = 4 \cdot 61 + 2$$

$$61 = 4 \cdot 15 + 1$$

$$15 = 4 \cdot 3 + 3$$

$$3 = 4 \cdot 0 + 3$$

Maka $(985)_{10} = (33121)_4$

Pemeriksaan:

$$\begin{aligned}(33121)_4 &= 3 \cdot 4^4 + 3 \cdot 4^3 + 1 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0 \\&= 768 + 192 + 16 + 8 + 1 \\&= 985.\end{aligned}$$

Ambil $n = 985$ dan $q = 3$. Perhatikan proses berikut ini:

$$985 = 3 \cdot 328 + 1$$

$$385 = 3 \cdot 109 + 1$$

$$109 = 3 \cdot 36 + 1$$

$$36 = 3 \cdot 12 + 0$$

$$12 = 3 \cdot 4 + 0$$

$$4 = 3 \cdot 1 + 1$$

$$1 = 3 \cdot 0 + 1$$

Maka $(985)_{10} = (1100111)_3$

Pemeriksaan:

$$\begin{aligned}(1100111)_3 &= 1 \cdot 3^6 + 1 \cdot 3^5 + 0 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 3^0 \\&= 729 + 243 + 0 + 0 + 9 + 3 + 1 = 985.\end{aligned}$$

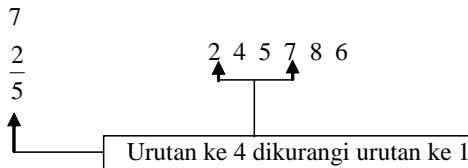
Tugas

Carilah suatu sumber pustaka yang membicarakan tentang pembagian oleh 1001 dengan menggunakan cara pencoretan (*scratch method*). Ambil suatu bilangan, lakukan pembagian bilangan itu oleh 1001 dengan cara biasa dan jelaskan bagaimana proses pembagian itu dapat diganti dengan cara pencoretan untuk memperoleh sisa pembagian.

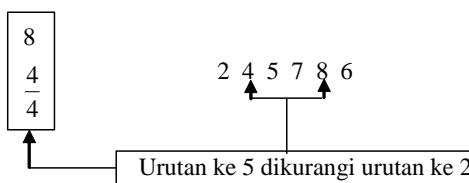
Berikan satu contoh pembagian suatu bilangan oleh 1001 dengan menggunakan cara pencoretan. Jelaskan manfaat dari cara pencoretan terhadap pembagian bilangan 7, 11 dan 13.

Petunjuk Jawaban Tugas

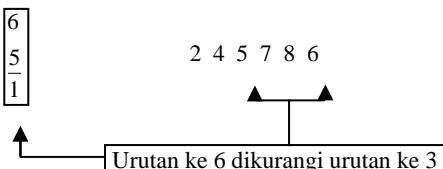
$$\begin{array}{r}
 & 245 \\
 1001) & 245786 \\
 & 2002 \\
 \hline
 & 4558 \\
 & 4004 \\
 \hline
 & 5546 \\
 & 5005 \\
 \hline
 \text{Sisa ?} & 541
 \end{array}$$



$$\begin{array}{r}
 & 245 \\
 1001) & 245786 \\
 & 2002 \\
 \hline
 & 4558 \\
 & 4004 \\
 \hline
 & 5546 \\
 & 5005 \\
 \hline
 \text{Sisa ?} & 541
 \end{array}$$



$$\begin{array}{r}
 & 245 \\
 1001) & 245786 \\
 & 2002 \\
 \hline
 & 4558 \\
 & 4004 \\
 \hline
 & 5546 \\
 & 5005 \\
 \hline
 \text{Sisa ?} & 541
 \end{array}$$



Gabungan dari tiga keadaan di atas dapat disederhanakan menjadi :

$$\begin{array}{r}
 541 \\
 245786
 \end{array}$$

Sisa pembagian adalah 541

Satu contoh pembagian 23569127418 oleh 1001 dengan cara pencoretan untuk memperoleh sisa pembagian adalah sebagai berikut:

$$\begin{array}{r}
 5548 \\
 46682937 \\
 \underline{\underline{23569+274+8}}
 \end{array}$$

Sisa pembagian adalah 837

Keadaan ini menunjukkan bahwa:

$$23569127418 = 1001x + 837 \text{ untuk suatu } x \in \mathbb{Z}^+$$

$$23569127418 = 7.11.13.x + 837$$

Dengan demikian penyelidikan suatu bilangan habis dibagi oleh 7, 11 atau 13 dapat dijelaskan lebih mudah karena:

jika $7|837$, maka $7|7.11.13x + 837$ atau $7|23569127418$

jika $11|837$, maka $11|7.11.13x + 837$ atau $11|23569127418$

jika $13|837$, maka $13|7.11.13x + 837$ atau $13|23569127418$

Karena $7|837$, $11|837$, dan $13|837$, maka 7, 11, dan 13 tidak habis membagi atau bukan faktor dari 23569127418.



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Buktikan: jika $a, b, c \in \mathbb{Z}$, $a|b$ dan $a|c$, maka $a|b + c$
- 2) Nyatakan q dalam bentuk $q = rp + s$, $0 \leq s < p$, jika :
 - a) $q = 79$ dan $p = 8$
 - b) $q = 203$ dan $p = 13$
 - c) $q = -110$ dan $p = 7$
 - d) $q = -156$ dan $p = 8$
- 3) Buktikan ketunggalan dari r dan s pada Teorema Algoritma Pembagian.

- 4) Diketahui: $t = (a_5 \ a_4 \ a_3 \ a_2 \ a_1 \ a_0)$ dan $7 | t$
 Tunjukkan bahwa $7 | (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5)$

5) Buktikan: $3 | n^3 - n$ untuk setiap $n \in \mathbb{Z}$

6) Nyatakan $(475)_{10}$ dalam lambang bilangan basis 7 dan basis 5

Petunjuk Jawaban Latihan

- 1) Gunakan Definisi 2.1

Karena $a|b$, maka $b = xa$ untuk suatu $x \in \mathbb{Z}$

Karena $a|c$, maka $c = ya$ untuk suatu $y \in \mathbb{Z}$

$b = xa$ dan $c = ya$, maka $b + c = xa + ya = (x + y)a$

Jadi $a \mid b + c$.

- $$2) \quad a. \quad 79 = 9.8 + 7$$

$$c. \quad -110 = (-16) \cdot 7 + 2$$

- $$\text{b. } 203 = 15 \cdot 13 + 8$$

$$d. \quad -156 = (-20) \cdot 8 + 4$$

- 3) Jika $p, q \in \mathbb{Z}$ dan $p > 0$, maka ada bilangan-bilangan $r, s \in \mathbb{Z}$ yang masing-masing tunggal sehingga $q = rp + s$ dengan $0 \leq s < p$.

Untuk membuktikan ketunggalan r dan s akan digunakan bukti tidak langsung.

Misalkan r dan s masing-masing tidak tunggal, yaitu ada $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ sedemikian hingga:

$$q = r_1 p + s_1, \quad 0 \leq s_1 < p$$

$$q = r_2 p + s_2, \quad 0 \leq s_2 < p$$

dengan $r_1 \neq r_2$ dan $s_1 \neq s_2$

Misalkan $s_1 > s_2$, maka dari: $r_1 p + s_1 = r_2 p + s_2$

diperoleh: $s_1 - s_2 = p(r_2 - s_1)$ berarti $p \mid s_1 - s_2$

Karena $0 \leq s_1 < p$ dan $0 \leq s_2 < p$, maka $-p < s_1 - s_2 < p$, sehingga:

- a. Misalkan $0 < s_1 - s_2 < p$, karena $p \mid s_1 - s_2$, maka tidak mungkin $0 < s_1 - s_2 < p$

b. Misalkan $-p < s_1 - s_2 < 0$, maka $0 < s_2 - s_1 < p$, sehingga $p | s_2 - s_1$ karena $p | s_1 - s_2$, maka tidak mungkin $-p < s_1 - s_2 < 0$.

Karena 1 dan 2 salah, maka $s_1 - s_2 = 0$, berarti $s_1 = s_2$.

Karena $s_1 = s_2$ dan $s_1 - s_2 = p(r_2 - r_1)$, maka $p(r_2 - r_1) = 0$.

Karena $p \neq 0$ dan $p(r_2 - r_1) = 0$, maka $r_2 - r_1 = 0$ atau $r_1 = r_2$.

4) $t = (a_5 \ a_4 \ a_3 \ a_2 \ a_1 \ a_0) = a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

t dapat dinyatakan sebagai:

$$t = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + a_5 \cdot 10^5$$

$$= a_0 + a_1(7+3) + a_2(98+2) + a_3(1001-1) + a_4(10003-3) +$$

$$a_5(100002-2)$$

$$t = (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + 7(a_1 + 14a_2 + 143a_3 + 1429a_4 + 14286a_5)$$

Karena $7 | t$ dan $7 | 7(a_1 + 14a_2 + 143a_3 + 1429a_4 + 14286a_5)$, maka sesuai Teorema 2.9, $t | (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5)$.

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

Selidiki apakah $3 | n^3 - n$ jika n diganti dengan $n = 3k$, $n = 3k + 1$, dan $n = 3k + 2$.

6) $475 = 7.67 + 6 \quad 475 = 5.95 + 0$

$$67 = 7.9 + 4 \quad 95 = 5.19 + 0$$

$$9 = 7.1 + 2 \quad 19 = 5.3 + 4$$

$$1 = 7.0 + 1 \quad 3 = 5.0 + 3$$

$$(475)_{10} = (1246)_7 \quad (475)_{10} = (3400)_5$$



RANGKUMAN

Dalam Kegiatan Belajar 1 ini, beberapa bagian yang perlu diperhatikan adalah definisi keterbagian, teorema-teorema keterbagian, dan penerapan keterbagian.

1. Definisi keterbagian terkait dengan konsep membagi atau konsep faktor, dan konsep bilangan bulat genap atau bilangan bulat ganjil yang diperoleh sebagai akibat Teorema Algoritma Pembagian.
2. Terdapat 10 teorema keterbagian
 - a. Jika $p, q \in \mathbb{Z}$ dan $p|q$, maka $p|qr$ untuk semua $p \in \mathbb{Z}$
 - b. Jika $p, q, r \in \mathbb{Z}$, $p|q$, dan $q|r$ maka $p|r$
 - c. Jika $p, q \in \mathbb{Z}$, $p|q$, dan $q|p$, maka $p = \pm q$
 - d. Jika $p, q, r \in \mathbb{Z}$, $p|q$, dan $p|r$, maka $p|q+r$
 - e. Jika $p, q, r \in \mathbb{Z}$, $p|q$, dan $p|r$, maka $p|qx+ry$
 - f. Jika $p, q, r \in \mathbb{Z}$, $p > 0$, $q > 0$, dan $p|q$, maka $p \leq q$
 - g. Jika $p, q, r \in \mathbb{Z}$, $p > 0$, $q > 0$, $p|q$, dan $q|p$, maka $p = q$
 - h. $p|q$ jika dan hanya jika $kp|kp$ untuk semua $k \in \mathbb{Z}$ dan $k \neq 0$
 - i. Jika $p, q, r \in \mathbb{Z}$, $p \neq 0$, $p|q+r$, dan $p|q$, maka $p|r$
 - j. Algoritma Pembagian
Jika $p, q \in \mathbb{Z}$ dan $p > 0$, maka ada bilangan-bilangan $r, s \in \mathbb{Z}$ yang masing-masing tunggal sehingga $q = rp + s$ dengan $0 \leq s < p$.
 - k. Jika $q \in \mathbb{Z}$ dan $q > 1$, maka setiap $n \in \mathbb{Z}^+$ dapat dinyatakan secara tunggal dalam bentuk:

$$n = p_k q^k + p_{k-1} q^{k-1} + \dots + p_2 q^2 + p_1 q^1 + p_0 q^0, k \in \mathbb{Z}, k \geq 0,$$

$$p_t \in \mathbb{Z}, 0 \leq p_t < q-1, t = 0, 1, \dots, k, \text{ dan } p_k \neq 0.$$
3. Penerapan keterbagian dapat ditunjukkan dalam :
 - a. Menjabarkan sifat keterbagian oleh 3, 7, 11, dan 13, dan dapat diperluas menjadi keterbagian oleh 2, 4, 5, 6, 8, dan 9
 - b. Mengganti lambang-lambang bilangan dalam basis 10 menjadi lambang-lambang bilangan dalam basis bukan 10.



TES FORMATIF 1

1) Skor: 20

Carilah masing-masing paling sedikit satu contoh untuk menunjukkan bahwa pernyataan-pernyataan berikut adalah salah.

- A. Jika $p|q+r$, maka $p|q$ atau $p|r$
- B. Jika $p|qr$, maka $p|q$ atau $p|r$
- C. Jika $(p+q)|r$, maka $p|r$ atau $q|r$
- D. Jika $p|r$ dan $q|r$, maka $p=q$
- E. Jika $p|q$ dan $p|r$, maka $q=r$

2) Skor: 20

A. Tunjukkan : jika $n = (a_7a_6a_5a_4a_3a_2a_1a_0)$ dan $99|n$,

$$\text{maka } 99|(a_1a_0)+(a_3a_2)+(a_5a_4)+(a_7a_6)$$

B. Tunjukkan : jika $n = (a_7a_6a_5a_4a_3a_2a_1a_0)$ dan $101|n$

$$\text{maka } 101|(a_1a_0)-(a_3a_2)+(a_5a_4)-(a_7a_6)$$

3) Skor: 20

Buktikan Teorema 2.9 :

Jika $p, q, r \in \mathbb{Z}$, $p \neq 0$, $p|q+r$, dan $p|q$, maka $p|r$

4) Skor: 20

Buktikan $3|n^3 + 6n^2 + 8n$ untuk semua $n \in \mathbb{Z}$

5) Skor: 20

a. Pilihlah suatu bilangan yang terdiri atas 5 angka.

Tulislah bilangan itu dalam basis 2, dan dalam basis 12

b. Pilihlah suatu bilangan yang terdiri atas 10 angka.

Dengan menggunakan metode pencoretan, selidiki apakah bilangan itu habis dibagi oleh 77 dan habis dibagi oleh 143.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2

Faktor Persekutuan Terbesar (FPB) dan Kelipatan Persekutuan Terkecil (KPK)

Sebelum kita bahas tentang faktor (pembagi) persekutuan terbesar, marilah kita lihat beberapa peragaan berikut:

Perhatikan dua bilangan $a = 6$ dan $b = 8$.

Jika A adalah himpunan semua faktor dari a , dan B adalah himpunan semua faktor dari b , serta C adalah himpunan semua faktor persekutuan dari a dan b , maka:

$$A = \{-6, -3, -2, -1, 1, 2, 3, 6\}$$

$$B = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

$$C = A \cap B = \{-2, -1, 1, 2\}$$

Unsur (anggota, elemen) dari C yang terbesar adalah 2. Dalam hal ini, 2 disebut faktor persekutuan yang terbesar dari $a = 6$ dan $b = 8$.

2 juga disebut bilangan bulat positif terbesar yang membagi $a = 6$ dan $b = 8$.

Sekarang bagaimana kalau diambil $a = -6$ dan $b = 8$.

$$A = \{-6, -3, -2, -1, 1, 2, 3, 6\}$$

$$B = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

$$C = A \cap B = \{-2, -1, 1, 2\}$$

Unsur dari C yang terbesar adalah 2. Dalam hal ini, 2 disebut faktor persekutuan yang terbesar dari $a = -6$ dan $b = 8$.

2 juga disebut bilangan bulat positif terbesar yang membagi $a = -6$ dan $b = 8$.

Dengan jalan yang sama, jika diambil $a = -6$ dan $b = -8$, maka juga akan diperoleh faktor persekutuan terbesar dari a dan b adalah 2.

Jika untuk menyatakan faktor persekutuan terbesar dari a dan b digunakan lambang (a, b) , maka dapat ditentukan bahwa:

$$(6, 8) = 2$$

$$(-6, 8) = 2$$

$$(-6, -8) = 2$$

Ternyata, faktor persekutuan terbesar dari dua bilangan bulat a dan b , apapun tanda masing-masing, selalu diperoleh nilai yang bertanda positif. Bagaimana keadaan faktor persekutuan terbesar ini jika a atau b (tidak keduanya) bernilai nol?

Ambil $a = 0$ dan $b = 6$

$$A = \text{himpunan semua faktor } a = 0$$

$$= \{\dots, -7, -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6, 7, \dots\}$$

$$B = \text{himpunan semua faktor } b = 6$$

$$= \{-6, -3, -2, -1, 1, 2, 3, 6\}$$

$$C = A \cap B$$

$$= \{-6, -3, -2, -1, 1, 2, 3, 6\}$$

Unsur yang terbesar dari C adalah 6, berarti $(a, b) = (0, 6) = 6$.

Untuk $a = 0$ dan $b = 0$, perhatikan bahwa:

$$A = \{\dots, -4, -3, -2, -1, 1, 2, 3, 4, \dots\}$$

$$B = \{\dots, -4, -3, -2, -1, 1, 2, 3, 4, \dots\}$$

$$C = \{\dots, -4, -3, -2, -1, 1, 2, 3, 4, \dots\}$$

Sehingga tidak mungkin menentukan unsur yang terbesar dari C , atau faktor persekutuan terbesar dari $a = 0$ dan $b = 0$ tidak ada.

Definisi 2.3

Ditentukan $x, y \in Z$, x dan y keduanya tidak bersama-sama bernilai 0.

$p \in Z$ disebut pembagi (faktor) persekutuan (*common divisor, common factor*) dari x dan y jika $p | x$ dan $p | y$

$p \in Z$ disebut pembagi (faktor) persekutuan terbesar (*gcd = greatest common divisor, gcf = greatest common factor*) dari x dan y jika p adalah bilangan bulat positif terbesar yang membagi x (yaitu $p | x$) dan membagi y (yaitu $p | y$).

Notasi:

$d = (x, y)$ dibaca d adalah faktor (pembagi) persekutuan terbesar dari x dan y

$d = (x_1, x_2, \dots, x_n)$ dibaca d adalah faktor (pembagi) persekutuan terbesar dari x_1, x_2, \dots, x_n

Perlu diperhatikan bahwa $d = (a, b)$ didefinisikan untuk setiap pasang bilangan bulat $a, b \in \mathbb{Z}$ kecuali $a = 0$ dan $b = 0$ secara bersama-sama.

Demikian pula, perlu dipahami bahwa (a, b) selalu bernilai bilangan bulat positif, yaitu $d \in \mathbb{Z}$ dan $d > 0$ (atau $d \geq 1$).

Contoh 2.7

1. Himpunan semua faktor dari 16 adalah:

$$A = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$$

Himpunan semua faktor dari 24 adalah:

$$B = \{-24, -12, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 12, 24\}$$

Himpunan semua faktor persekutuan dari 16 dan 24 adalah:

$$C = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

Karena unsur C yang terbesar adalah 8, maka $(16, 24) = 8$

Cobalah cari $(-16, 24), (16, -24), (-16, -24), (24, -16)$, dan $(-24, 16)$

2. Himpunan semua faktor dari 12 adalah

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$$

Himpunan semua faktor dari 18 adalah

$$\{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}$$

Himpunan semua faktor persekutuan dari 12 dan 18 adalah

$$\{-6, -3, -2, -1, 1, 2, 3, 6\}$$

Jadi $(12, 18) = 6$

3. Perhatikan:

$$(6, 9) = 3 \text{ dan } 3 = (2)(6) + (-1)(9)$$

$$(16, 40) = 8 \text{ dan } 8 = (3)(16) + (-1)(40)$$

$$(60, 105) = 15 \text{ dan } 15 = (2)(60) + (-1)(105)$$

Dari ketiga kasus di atas tampak adanya pola bahwa (p, q) dapat dinyatakan sebagai kombinasi linier $px + qy$ dengan $x, y \in \mathbb{Z}$

4. Perhatikan bahwa $(6, 9) = 3$

Sekarang dibentuk kombinasi linear $px + qy$ dengan $x, y \in \mathbb{Z}$

Nilai-nilai $6p + 9q$ adalah sebagai berikut:

$$p = 0 \text{ dan } q = 0 \rightarrow 6p + 9q = 0$$

$$p = 0 \text{ dan } q = 1 \rightarrow 6p + 9q = 9$$

$$p = 1 \text{ dan } q = 0 \rightarrow 6p + 9q = 6$$

$$p = 1 \text{ dan } q = -1 \rightarrow 6p + 9q = -3$$

$$p = -1 \text{ dan } q = 1 \rightarrow 6p + 9q = 3$$

$$p = -1 \text{ dan } q = 2 \rightarrow 6p + 9q = 12$$

$$p = 2 \text{ dan } q = -1 \rightarrow 6p + 9q = 3$$

$$p = 1 \text{ dan } q = -2 \rightarrow 6p + 9q = -12$$

$$p = 0 \text{ dan } q = -1 \rightarrow 6p + 9q = -9$$

$$p = 2 \text{ dan } q = -2 \rightarrow 6p + 9q = -6$$

Nilai-nilai itu dapat disusun menjadi barisan:

$$\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots$$

Ambil $S = \{3, 6, 9, 12, \dots\}$, yaitu himpunan yang unsur-unsurnya adalah suku-suku barisan yang positif, yaitu:

$$S = \{6p + 9q \mid 6p + 9q > 0 \text{ dan } p, q \in \mathbb{Z}\}$$

Karena $S \subset N$ dan N adalah himpunan terurut rapi, maka S mempunyai unsur terkecil, yaitu 3. Karena $3 \in S$, maka $3 = 6p + 9q$ dengan $p = 2$ dan $q = -1$, atau $p = -1$ dan $q = 1$.

Jelas bahwa $3 \mid 6$ dan $3 \mid 9$.

Teorema 2.12

Jika $d = (x, y)$, maka d adalah bilangan bulat positif terkecil yang mempunyai bentuk $px + qy$ untuk suatu $p, q \in \mathbb{Z}$, yaitu d dapat dinyatakan sebagai kombinasi linear dari x dan y .

Bukti:

Dibentuk kombinasi linear $px + qy$ dengan $p, q \in \mathbb{Z}$

Barisan bilangan $px+qy$ memuat bilangan-bilangan yang bernilai negatif, bilangan nol (untuk $p=0$ dan $q=0$), dan bilangan-bilangan yang bernilai positif.

Ambil $S = \{px+qy \mid px+qy > 0 \text{ dan } p, q \in \mathbb{Z}\}$, maka dapat ditentukan bahwa $S \subset N$. Karena $S \subset N$ dan N merupakan himpunan yang terurut rapi, maka S mempunyai unsur terkecil, sebutlah dengan t .

Karena $t \in S$, maka tentu ada $p=m$ dan $q=n$ sehingga $t = mx+ny$. Selanjutnya dapat dibuktikan bahwa $t \mid x$ dan $t \mid y$.

Untuk membuktikan $t \mid x$ digunakan bukti tidak langsung.

Misalkan $t \nmid x$, maka menurut Teorema 2.9, ada $r, s \in \mathbb{Z}$ sehingga

$$x = tr + s, \quad 0 < s < t$$

$$x = tr + s$$

$$s = x - tr$$

$$= x - (mx + ny)r$$

$$= (1 - mr)x + (-ny)r$$

$$s = ix + jy \text{ dengan } i = 1 - mr \in \mathbb{Z} \text{ dan } j = -nr \in \mathbb{Z}$$

Jadi $s = ix + jy \in S$ dengan $s < t$.

Dengan anggapan $t \nmid x$ ternyata menghasilkan kontradiksi karena t adalah unsur terkecil S , dengan demikian anggapan $t \nmid x$ adalah salah, berarti $t \mid x$.

Dengan jalan yang sama dapat ditunjukkan bahwa $t \mid y$.

Dari $t \mid x$ dan $t \mid y$ berarti t adalah faktor persekutuan dari x dan y . Karena t adalah faktor persekutuan dari x dan y , dan d adalah faktor persekutuan terbesar dari x dan y , maka $t \geq d$.

Selanjutnya akan dibuktikan bahwa $d \leq t$.

$d = (x, y)$, maka menurut Definisi 2.3, $d \mid x$ dan $d \mid y$.

Karena $d \mid x$ dan $d \mid y$, maka menurut Definisi 2.1, $x = dv$ untuk suatu $v \in \mathbb{Z}$ dan $y = dw$ untuk suatu $w \in \mathbb{Z}$.

Perhatikan:

$$\begin{aligned} t &= mx + ny \\ &= m(dv) + n(dw) \\ t &= d(mv + nw), \text{ berarti } d | t \end{aligned}$$

Karena $d | t$, $d > 0$, dan $t > 0$, maka sesuai dengan Teorema 2.6, $d \leq t$

Karena $t \leq d$ dan $d \leq t$, maka $d = t$.

Jadi d adalah bilangan bulat positif terkecil yang mempunyai bentuk $mx + ny$ dengan $m, n \in \mathbb{Z}$.

Teorema 2.13

Jika $k \in \mathbb{N}$, maka $k(x, y) = (kx, ky)$

Bukti:

Misalkan $d = (x, y)$ dan $e = (kx, ky)$, maka menurut Teorema 2.11, $d = rx + sy$ dan $e = mkx + nky$ untuk suatu $r, s, m, n \in \mathbb{Z}$.

$d = rx + sy$, maka $kd = krx + ksy$. Karena $d = (x, y)$, maka menurut

Definisi 2.3, $d | x$ dan $d | y$, dan menurut Teorema 2.8, $kd | kx$ dan $kd | ky$.

Menurut Teorema 2.1, $kd | kx$ dan $kd | ky$ berakibat $kd | mkx$ dan $kd | nky$, dan menurut Teorema 2.4, $kd | mkx + nky$ atau $kd | e$.

Jadi $k(x, y) | (kx, ky)$.

Selanjutnya, karena $e = (kx, ky)$, maka menurut Definisi 2.3, $e | kx$ dan $e | ky$, dan menurut Teorema 2.8, $e | krx$ dan $e | ksy$. Menurut Teorema 2.4, $e | krx$ dan $e | ksy$ berakibat $e | krx + ksy$, atau $e | khd$.

Jadi $(kx, ky) | k(x, y)$.

Karena $k(x, y) > 0$, $(kx, ky) > 0$, $k(x, y) | (kx, ky)$, dan $(kx, ky) | k(x, y)$, maka menurut Teorema 2.7, $k(x, y) = (kx, ky)$.

Contoh 2.8.

$$(60, 102) = (6 \cdot 10, 6 \cdot 17) = 6(10, 17) = 6 \cdot 1 = 6$$

$$(108, 207) = (9 \cdot 12, 9 \cdot 23) = 9(12, 23) = 9 \cdot 1 = 9$$

Teorema 2.14

Jika $x, y \in Z$ dan $d = (x, y)$, maka $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$

Bukti:

Misalkan $x, y \in Z$ dan $(x, y) = d$. Kita akan tunjukkan bahwa $\frac{x}{d}$ dan $\frac{y}{d}$ tidak mempunyai pembagi persekutuan yang positif kecuali 1.

Misalkan e adalah suatu bilangan bulat positif yang membagi $\frac{x}{d}$ dan membagi $\frac{y}{d}$, yaitu $e \mid \frac{x}{d}$ dan $e \mid \frac{y}{d}$, maka menurut Definisi 2.1, $\frac{x}{d} = ke$ dan $\frac{y}{d} = te$ untuk suatu $k, t \in Z$. Dengan demikian $x = dek$ dan $y = det$, berarti de adalah faktor persekutuan dari x dan y . Karena de adalah faktor persekutuan dari x dan y , dan d adalah faktor persekutuan terbesar dari x dan y , maka $de \leq d$. Akibatnya e haruslah sama dengan 1.

Jadi $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$.

Teorema 2.15

Jika $p, q, r \in Z$, $p \mid qr$, dan $(p, q) = 1$, maka $p \mid r$.

Bukti:

Diketahui $(p, q) = 1$, maka menurut Teorema 2.11, 1 adalah bilangan bulat positif terkecil yang dapat dinyatakan sebagai $px + qy$ dengan $x, y \in Z$, yaitu $px + qy = 1$.

Karena $px + qy = 1$, maka $rpx + rqy = r$, atau $prx +qry = r$.

Menurut Teorema 2.1, karena $p \mid qr$, maka $p \mid qry$ untuk semua $y \in Z$. Selanjutnya, karena $p \mid prx$ dan $p \mid qry$, maka menurut Teorema 2.4, $p \mid prx + qry$.

Jadi $p \mid r$.

Teorema 2.16

Jika $(x, t) = 1$ dan $(y, t) = 1$, maka $(xy, t) = 1$.

Bukti:

Diketahui $(x, t) = 1$ dan $(y, t) = 1$, maka menurut Teorema 2.11, ada $p, q, r, s \in \mathbb{Z}$ sehingga $px + qt = 1$ dan $ry + st = 1$.

Dari $1 = px + qt$ dan $1 = ry + st$ dapat ditentukan bahwa:

$$\begin{aligned} 1.1 &= (px + qt)(ry + st) \\ 1 &= prxy + pstx + qryt + qst^2 \\ 1 &= (pr)(xy) + (psx + qry + qst)t. \end{aligned}$$

Dengan demikian, sesuai Teorema 2.11, karena 1 merupakan bilangan bulat positif terkecil yang merupakan kombinasi linear dari xy dan t , maka $(xy, t) = 1$.

Teorema 2.17

Ditentukan $x, y \in \mathbb{Z}$.

$d = (x, y)$ jika dan hanya jika $d > 0$, $d | x$, $d | y$, dan $f | d$ untuk setiap pembagi persekutuan f dari x dan y .

Bukti:

Kita buktikan jika $d = (x, y)$, maka $d > 0$, $d | x$, $d | y$, dan $f | d$.

$d = (x, y)$, maka menurut Definisi 2.3, d adalah bilangan bulat positif ($d > 0$) terbesar yang membagi x dan membagi y . Selanjutnya, menurut Teorema 2.11, jika $d = (x, y)$, maka $d = mx + ny$ untuk suatu $m, n \in \mathbb{Z}$.

Misalkan f adalah sebarang pembagi persekutuan dari x dan y , maka $f | x$ dan $f | y$, dan menurut Teorema 2.1, $f | mx$ dan $f | ny$ untuk sebarang $m, n \in \mathbb{Z}$.

Menurut Teorema 2.4, $f | mx$ dan $f | ny$ berakibat $f | mx + ny$. Karena $f | mx + ny$ dan $d = mx + ny$, maka $f | d$.

Kita buktikan jika $d > 0$, $d \mid x$, $d \mid y$, dan $f \mid d$ untuk sebarang pembagi persekutuan f dari x dan y , maka $d = (x, y)$.

Karena $d > 0$, $d \mid x$ dan $d \mid y$, maka d adalah faktor persekutuan dari x dan y . Selanjutnya, karena f adalah sebarang faktor persekutuan dari x dan y dan $f \mid d$, maka $f \leq d$, d dan f adalah faktor-faktor persekutuan dari x dan y , f adalah sebarang faktor persekutuan dari x dan y , dan $f \leq d$, maka d adalah faktor persekutuan yang terbesar dari x dan y .

Jadi $d = (x, y)$.

Contoh 2.9

Faktor-faktor persekutuan dari 4 dan 6 adalah $-1, 1, -2$, dan 2. Faktor persekutuan terbesar dari 4 dan 6 adalah 2. Perhatikan bahwa sebarang faktor persekutuan dari 4 dan 6 membagi faktor persekutuan terbesar dari 4 dan 6, yaitu: $-1 \mid 2, 1 \mid 2, -2 \mid 2$, dan $2 \mid 2$.

Contoh 2.10

$$(18, 24) = 6.$$

Faktor-faktor persekutuan dari 18 dan 24 adalah $-1, 1, -2, 2, -3, 3, -6$, dan 6. Perhatikan bahwa sebarang faktor persekutuan 18 dan 24 membagi 6, yaitu $\pm 1 \mid 6, \pm 2 \mid 6, \pm 3 \mid 6$, dan $\pm 6 \mid 6$.

Teorema 2.18

$$(x, y) = (y, x) = (x, -y) = (-x, y) = (-x, -y) \text{ untuk sebarang } x, y \in Z.$$

Buktikan!

Teorema 2.19

- a. $(x, y) = (x, y + ax)$ untuk sebarang $a \in Z$
- b. $(x, y) = (x + yb, y)$ untuk sebarang $b \in Z$

Bukti:

- a. Sesuai Definisi 2.3, $(x, y) > 0$ dan $(x, y + ax) > 0$.

Karena $(x, y) > 0$ dan $(x, y+ax) > 0$ maka untuk membuktikan $(x, y) = (x, y+ax)$ sesuai dengan Teorema 2.7 kita harus membuktikan bahwa $(x, y)|(x, y+ax)$ dan $(x, y+ax)|(x, y)$. Kita akan membuktikan lebih dahulu $(x, y)|(x, y+ax)$.

Sesuai Definisi 2.3, $(x, y)|x$ dan $(x, y)|y$. Menurut Teorema 2.1, karena $(x, y)|x$, maka $(x, y)|ax$ untuk semua $a \in \mathbb{Z}$.

Selanjutnya, sesuai dengan Teorema 2.4, karena $(x, y)|ax$ dan $(x, y)|y$, maka $(x, y)|y+ax$.

$(x, y)|x$ dan $(x, y)|y+ax$, maka menurut Definisi 2.3, (x, y) adalah faktor persekutuan dari x dan $y+ax$, dan akibatnya, sesuai dengan Teorema 2.16, (x, y) membagi $(x, y+ax)$.

Jadi $(x, y)|(x, y+ax)$.

Selanjutnya kita akan membuktikan $(x, y+ax)|(x, y)$.

Sesuai Definisi 2.3, $(x, y+ax)|x$, sehingga menurut Teorema 2.1, $(x, y+ax)|ax$ untuk semua $a \in \mathbb{Z}$; demikian pula, sesuai Definisi 2.3, $(x, y+ax)|y+ax$.

Selanjutnya, sesuai Teorema 2.9, karena: $(x, y+ax)|ax$ dan $(x, y+ax)|y+ax$, maka $(x, y+ax)|y$.

Karena $(x, y+ax)|x$ dan $(x, y+ax)|y$, maka sesuai Definisi 2.3, $(x, y+ax)$ merupakan faktor persekutuan dari x dan y , dan sesuai Teorema 2.16 setiap faktor persekutuan x dan y tentu membagi (x, y) .

Jadi $(x, y+ax)|(x, y)$.

Karena $(x, y) > 0$, $(x, y+ax) > 0$, $(x, y)|(x, y+ax)$, dan $(x, y+ax)|(x, y)$, maka menurut Teorema 2.7: $(x, y) = (x, y+ax)$.

b. Buktikan!

Contoh 2.11.

$$(6, 9) = (6, 9 + 7 \cdot 6) = (6, 51)$$

$$(12, 18) = (12, 18 + 5 \cdot 12) = (12, 78)$$

$$(40, 16) = (40, 16 + 9 \cdot 40) = (40, 376)$$

$$(40, 16) = (40 + 5 \cdot 16, 16) = (120, 16)$$

$$(12, 18) = (12 + 7 \cdot 18, 18) = (138, 18)$$

$$(36, 15) = (6 + 2 \cdot 15, 15) = (6, 15) = (6, 3 + 2 \cdot 6) = (6, 3) = 3(2, 1) = 3 \cdot 1 = 3$$

$$(84, 175) = (84, 7 + 2 \cdot 84) = (84, 7) = 7(12, 1) = 7 \cdot 1 = 7$$

Contoh 2.12

Ditentukan $s_0 = 48$, $s_1 = 27$, $s_2 = 21$, $s_3 = 6$, $s_4 = 3$, dan $s_5 = 0$.

Maka menurut Teorema 2.9 (Teorema Algoritma Pembagian), kita dapat melakukan langkah-langkah berikut:

$$48 = 1 \cdot 27 + 21, \quad 0 \leq 21 < 27, \quad 0 \leq s_2 < s_1$$

$$27 = 1 \cdot 21 + 6, \quad 0 \leq 6 < 21, \quad 0 \leq s_3 < s_2$$

$$21 = 3 \cdot 6 + 3, \quad 0 \leq 3 < 6, \quad 0 \leq s_4 < s_3$$

$$6 = 2 \cdot 3 + 0 \quad s_5 = 0$$

Selanjutnya, menurut Teorema 2.11, kita dapat mencari $(s_0, s_1) = (48, 27)$:

$$(s_0, s_1) = (48, 27)$$

$$= (21 + 1 \cdot 27, 27) = (21, 27)$$

$$= (s_2, s_1)$$

$$= (21, 6 + 1 \cdot 21) = (21, 6)$$

$$= (s_2, s_3)$$

$$= (3 + 3 \cdot 6, 6) = (3, 6)$$

$$= (s_4, s_3)$$

$$= (3, 3 + 1 \cdot 3) = (3, 3) = (3, 0 + 1, 3)$$

$$= (3, 0)$$

$$= (s_4 + s_5)$$

$$= s_5$$

Perhatikan bahwa secara bertahap dapat ditentukan:

$$(s_0, s_1) = (s_2, s_1) = (s_2, s_3) = (s_4, s_3) = (s_4, s_4) = s_4$$

Contoh 2.12. di atas memberi gambaran tentang langkah-langkah yang jelas dan terhingga untuk memperoleh faktor persekutuan terbesar dua bilangan secara sistematis. Marilah sekarang kita lihat suatu cara yang sistematis, dan disebut algoritma, untuk mencari faktor persekutuan terbesar dari dua bilangan bulat positif.

Algoritma ini disebut Algoritma Euclides, dan istilah ini digunakan setelah Euclid, matematikawan Yunani (350 S.M.), menjelaskan algoritma ini dalam bukunya *The Elements* (Rosen K., 1993: 80).

Teorema 2.20 Algoritma Euclides

Ditentukan $s_0, s_1 \in \mathbb{Z}$, $s_0 \geq s_1 > 0$.

Jika Algoritma Pembagian digunakan secara berturut-turut untuk memperoleh

$s_t = s_{t+1}k_{t+1} + s_{t+2}$, $0 \leq s_{t+2} \leq s_{t+1}$, $t = 0, 1, 2, \dots, n-2$ dan $s_{n+1} = 0$, maka $(s_0, s_1) = s_n$, sisa yang tidak nol dalam Algoritma Pembagian.

Bukti:

Karena $s_0, s_1 \in \mathbb{Z}$, $s_0 \geq s_1 > 0$, maka dengan menggunakan Algoritma Pembagian secara berturut-turut akan diperoleh:

$$s_0 = s_1 k_1 + s_2, \quad 0 \leq s_2 < s_1$$

$$s_1 = s_2 k_2 + s_3, \quad 0 \leq s_3 < s_2$$

⋮

$$s_{t-2} = s_{t-1} k_{t-1} + s_t, \quad 0 \leq s_t < s_{t-1}$$

⋮

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

$$s_{n-2} = s_{n-1} k_{n-1} + s_n, \quad 0 \leq s_n < s_{n-1}$$

$$s_{n-1} = s_n k_n + s_{n-1}, \quad s_{n+1} = 0$$

maka sesuai Teorema 2.19:

$$\begin{aligned}
 (s_0, s_1) &= (s_1 + s_2, s_1) \\
 &= (s_2, s_1) \\
 &= (s_2, s_2 + s_3) \\
 &= (s_2, s_3) \\
 &= \dots \\
 &= (s_{n-3}, s_{n-2}) \\
 &= (s_{n-2}, s_{n-1}) \\
 &= (s_{n-1}, s_n) \\
 &= (s_n, 0)
 \end{aligned}$$

$$(s_0, s_1) = s_n$$

Contoh 2.12

Carilah $(963, 657)$ dengan menggunakan Algoritma Euclides.

Jawab:

$$963 = 1.657 + 306, \quad 0 \leq 306 < 657$$

$$657 = 2.306 + 45, \quad 0 \leq 45 < 306$$

$$306 = 6.45 + 36, \quad 0 \leq 36 < 45$$

$$45 = 1.36 + 9, \quad 0 \leq 9 < 36$$

$$36 = 4.9 + 0$$

$$\text{Jadi } (963, 657) = 9.$$

Menurut Teorema 2.12, jika $d = (x, y)$, maka d dapat dinyatakan sebagai kombinasi linear dari x dan y . Algoritma Euclides dapat digunakan untuk mencari kombinasi linear d dari x dan y .

Dalam kaitannya dengan Algoritma Euclides, jika $d = (s_0, s_1)$, maka dapat ditentukan bahwa $d = ms_0 + ns_1$:

$$\begin{aligned}
 s_{n-2} &= s_{n-1}k_{n-1} + s_n, & \text{maka } s_n &= s_{n-2} - s_{n-1}k_{n-1} \\
 s_{n-3} &= s_{n-2}k_{n-2} + s_{n-1}, & \text{maka } s_{n-1} &= s_{n-3} - s_{n-2}k_{n-2} \\
 s_{n-4} &= s_{n-3}k_{n-3} + s_{n-2}, & \text{maka } s_{n-2} &= s_{n-4} - s_{n-3}k_{n-3} \\
 &\vdots \\
 s_1 &= s_2k_2 + s_3, & \text{maka } s_3 &= s_1 - s_2k_2 \\
 s_0 &= s_1k_1 + s_2, & \text{maka } s_2 &= s_0 - s_1k_1
 \end{aligned}$$

Dengan demikian:

$$\begin{aligned}
 sn &= s_{n-2} - s_{n-1}k_{n-1} \\
 &= s_{n-2} - (s_{n-3} - s_{n-2}k_{n-2})k_{n-1} \\
 &= s_{n-2}(1 + k_{n-2}k_{n-1}) - s_{n-3} \\
 &= (s_{n-4} - s_{n-3}k_{n-3})(1 + k_{n-2}k_{n-1}) - s_{n-3} \\
 &= s_{n-4}(1 + k_{n-2}k_{n-1}) + s_{n-3}\{k_{n-3}(1 + k_{n-2}k_{n-1})\}
 \end{aligned}$$

Jika proses serupa diteruskan dengan substitusi berturut-turut:

$$s_{n-3}, s_{n-4}, \dots, s_3, s_2$$

maka akan diperoleh bentuk:

$$\begin{aligned}
 (s_0, s_1) &= sn \\
 (s_0, s_1) &= s_0m + s_1n = ms_0 + ns_1
 \end{aligned}$$

Ini berarti bahwa (s_0, s_1) dapat dinyatakan sebagai kombinasi linear dari s_0 dan s_1 .

Contoh 2.13

Nyatakan $(205, 75)$ sebagai kombinasi linear dari 205 dan 75

Jawab:

$$\begin{array}{ll}
 205 = 2.75 + 55, & 55 = 205 - 2.75 \\
 75 = 1.55 + 20, & 20 = 75 - 1.55 \\
 55 = 2.20 + 15, & 15 = 55 - 2.20 \\
 20 = 1.15 + 5, & 5 = 20 - 1.15 \\
 15 = 3.5 + 0 & \\
 (205, 75) = 5 &
 \end{array}$$

Dengan demikian dapat ditentukan:

$$\begin{aligned}
 (205, 75) &= 5 \\
 &= 20 - 1.15 = 20 - 1 \cdot (55 - 2.20) \\
 &= 3.20 - 1.55 = 3 \cdot (75 - 1.55) - 1.55 \\
 &= 3.75 - (4) \cdot 55 = 3.75 - 4(205 - 2.75) \\
 (205, 75) &= 11.75 + (-4) \cdot 205.
 \end{aligned}$$

Contoh 2.14

Carilah nilai-nilai m, n yang memenuhi hubungan
 $(7897, 4399) = m(7897) + n(4399)$

Jawab:

$$\begin{array}{ll}
 7897 = 1.4399 + 3498, & 3498 = 7897 - 1.4399 \\
 4399 = 1.3498 + 901, & 901 = 4399 - 1.3498 \\
 3498 = 3.901 + 795, & 795 = 3498 - 3.901 \\
 901 = 1.795 + 106, & 106 = 901 - 1.795 \\
 795 = 7.106 + 53, & 53 = 795 - 7.106 \\
 106 = 2.53 + 0 &
 \end{array}$$

Dengan demikian dapat ditentukan:

$$(7897, 4399) = 53$$

$$\begin{aligned} &= 795 - 7 \cdot 106 = 795 - 7 \cdot (901 - 1 \cdot 795) \\ &= 8 \cdot 795 - 7 \cdot 901 = 8(3498 - 3 \cdot 901) - 7 \cdot 901 \\ &= 8 \cdot 3498 - 31 \cdot 901 = 8 \cdot 3498 - 31(4399 - 1 \cdot 3498) \\ &= 39 \cdot 3498 - 31 \cdot 4399 = 39(7897 - 1 \cdot 4399) - 31 \cdot 4399 \end{aligned}$$

$$(7897, 4399) = 39 \cdot 7897 + (-70) \cdot 4399$$

Jadi $m = 7897$ dan $n = -70$.

Cara untuk menyatakan (p, q) sebagai kombinasi linear dari p dan q memerlukan pemrosesan yang panjang karena perlu kerja berdasarkan langkah-langkah Algoritma Euclides, dan dilanjutkan kerja mundur berdasarkan modifikasi dari setiap langkah dalam Algoritma Euclides.

Terdapat cara lain untuk menyatakan (p, q) sebagai kombinasi linear dari p dan q , yang secara langsung dapat menggunakan langkah-langkah Algoritma Euclides.

Teorema 2.2.1

Ditentukan $p, q \in N$.

Maka $(p, q) = r_n p + l_n q$, $n = 0, 1, 2, \dots$, yang mana r_n dan k_n adalah suku ke n dari barisan-barisan yang secara rekursif didefinisikan sebagai:

$$r_0 = 1, l_0 = 0$$

$$r_1 = 0, l_1 = 1$$

dan

$$r_i = r_{i-2} - k_{i-1} r_{i-1}$$

$$l_i = l_{i-2} - k_{i-1} l_{i-1}$$

untuk $i = 2, 3, \dots, n$ dengan k_i adalah hasil bagi dalam Algoritma Euclides memperoleh (p, q) .

Bukti:

Berdasarkan langkah-langkah Algoritma Euclides pada Teorema 2.20, dipilih $p = s_0$ dan $q = s_1$, kemudian kita gunakan cara pembuktian induksi matematika untuk membuktikan $(p, q) = s_n = r_n p + l_n q$

untuk $i = 0$, $p = s_0 = 1 \cdot p + 0 \cdot q = r_0 p + l_0 q$,

untuk $i = 1$, $q = s_1 = 0 \cdot p + 1 \cdot q = r_1 + l_1 q$

Sekarang, anggaplah bahwa $s_i = r_i p + l_i q$, $i = 1, 2, \dots, n-1$.

Sesuai dengan keadaan langkah ke n dalam pembuktian Algoritma Euclides dapat ditunjukkan bahwa:

$$s_{n-2} = s_{n-1} k_{n-1} + s_n \text{ atau } s_n = s_{n-2} - s_{n-1} k_{n-1}$$

Dengan demikian, sesuai dengan prinsip induksi matematika:

$$\begin{aligned} s_n &= s_{n-2} - s_{n-1} k_{n-1} \\ &= (r_{n-2} p + l_{n-2} q) - (r_{n-1} p + l_{n-1} q) k_{n-1} \\ &= (r_{n-2} - r_{n-1} k_{n-1}) p + (l_{n-2} - l_{n-1} k_{n-1}) q \\ &= (r_{n-2} - k_{n-1} r_{n-1}) p + (l_{n-2} - k_{n-1} l_{n-1}) q \\ s_n &= r_n p + l_n q \end{aligned}$$

Contoh 2.15

Carilah $(205, 75)$ dan nyatakan sebagai kombinasi linear dari 205 dan 75 .

Jawab:

$$205 = 2.75 + 55, \quad k_1 = 2$$

$$75 = 1.55 + 20, \quad k_2 = 1$$

$$55 = 2.20 + 15, \quad k_3 = 2$$

$$20 = 1.15 + 5, \quad k_4 = 1$$

$$15 = 3.5 + 0$$

Jadi $(205, 75) = 5$

$$\begin{aligned}
 r_0 &= 1 & l_0 &= 0 \\
 r_1 &= 0 & l_1 &= 1 \\
 r_2 &= r_0 - k_1 \cdot r_1 & l_2 &= l_0 - k_1 l_1 \\
 &= 1 - 2 \cdot 0 & &= 0 - 2 \cdot 1 \\
 &= 1 & &= -2 \\
 r_3 &= r_1 - k_2 - r_2 & l_3 &= l_1 - k_2 l_2 \\
 &= 0 - 1 \cdot 1 & &= 1 - 1(-2) \\
 &= 1 & &= 3 \\
 r_4 &= r_2 - k_3 \cdot r_3 & l_4 &= l_2 - k_3 l_3 \\
 &= 1 - 2(-1) & &= -2 - 2 \cdot 3 \\
 &= 3 & &= -8 \\
 r_5 &= r_3 - k_4 r_4 & l_5 &= l_3 - k_4 l_4 \\
 &= -1 - 1(3) & &= 3 - 1 \cdot (-8) \\
 &= -4 & &= 11
 \end{aligned}$$

Jadi $(205, 75) = (-4).205 + 11.75$.

Contoh 2.16

Langkah-langkah pada Contoh 2.15 memerlukan tempat mencari yang luas dan waktu yang panjang. Untuk menyederhanakan langkah-langkah pencarian, kita dapat mengurangi tempat dan waktu dengan mengoperasikan atau menggunakan tabel. Dengan menggunakan tabel, Contoh 2.15 dapat dikerjakan sebagai berikut:

n	r	l	k
1	1	0	2
2	0	1	1
3	1	-2	2
4	-1	3	1
5	3	-8	
6	-4	11	

Jadi $(205, 75) = (-4).205 + 11.75$

Contoh 2.17

Carilah m dan n jika $(8517, 2669) = m \cdot 8517 + n \cdot 2669$

Jawab:

$$8517 = 3 \cdot 2669 + 510, \quad k_1 = 3$$

$$2669 = 5 \cdot 510 + 119, \quad k_2 = 5$$

$$510 = 4 \cdot 119 + 34, \quad k_3 = 4$$

$$119 = 3 \cdot 34 + 17, \quad k_4 = 3$$

$$34 = 2 \cdot 17 + 0$$

n	r	l	k
1	1	0	3
2	0	1	5
3	1	-3	4
4	-5	16	3
5	21	-67	
6	-68	217	

$$\text{Jadi } (8517, 2669) = (-68) \cdot 8517 + 217 \cdot 2669$$

$$m = -68 \text{ dan } n = 217.$$

Marilah sekarang kita mempelajari pasangan pembahasan FPB (Faktor Persekutuan Terbesar) dan KPK (Klipatan Persekutuan Terkecil). Topik FPB dan KPK merupakan materi pelajaran matematika yang dimulai di Sekolah Dasar.

Definisi 2.4

Jika $x, y \in \mathbb{Z}$, $x \neq 0$, dan $y \neq 0$, maka:

- m disebut kelipatan persekutuan (*common multiple*) dari x dan y jika $x|m$ dan $y|m$.
- m disebut kelipatan persekutuan terkecil (*least common multiple*) dari x dan y jika m adalah bilangan bulat positif terkecil sehingga $x|m$ dan $y|m$.

Notasi:

$m = [x, y]$ dibaca m adalah kelipatan persekutuan terkecil dari x dan y .

Dengan jalan yang sama dapat didefinisikan kelipatan persekutuan terkecil dari 3 bilangan, 4 bilangan, ..., n bilangan, misalnya:

$n = [x, y, z]$ dibaca n adalah kelipatan persekutuan terkecil dari x, y , dan z .

$p = [a, b, c, d]$ dibaca p adalah kelipatan persekutuan terkecil dari a, b, c , dan d .

Contoh 2.18

- a. Carilah $[12, 16]$.

Jawab:

Karena $[12, 16]$ bernilai positif, maka $[12, 16]$ dapat dicari dari kelipatan persekutuan 12 dan 16 yang positif.

Kelipatan 12 yang positif adalah 12, 24, 36, 48, 60, ...

Kelipatan 16 yang positif adalah 16, 32, 48, 64, 80, ...

48 adalah kelipatan persekutuan 12 dan 16 sebab $12|48$ dan $16|48$

96 adalah kelipatan persekutuan 12 dan 16 sebab $12|96$ dan $16|96$

Kelipatan-kelipatan persekutuan 12 dan 16 adalah 48, 96, 144, 192, ...

Dari barisan bilangan kelipatan persekutuan 12 dan 16, yang terkecil adalah 48, sehingga $[12, 16] = 48$.

- b. Carilah $[25, 15]$

Jawab:

Kelipatan 25 yang positif adalah 25, 50, 75, ...

Kelipatan 15 yang positif adalah 15, 30, 45, ...

Kelipatan-kelipatan persekutuan 25 dan 15 yang positif adalah 75, 150, 225, ...

Kelipatan-kelipatan persekutuan 25 dan 15 yang positif dan terkecil adalah 75, sehingga $[25, 15] = 75$.

Perhatikan kelipatan-kelipatan persekutuan 4 dan 5 yang positif, yaitu: 20, 40, 60, 80, ... dan yang terkecil adalah 20, sehingga $[4, 5] = 20$.

Ternyata $20|20$, $20|40$, $20|60$, $20|80, \dots, 20|k$ untuk sebarang kelipatan persekutuan k dari 4 dan 5.

Teorema 2.22

Ditentukan $x, y \in \mathbb{Z}$, $x \neq 0$, dan $y \neq 0$

$m = [x, y]$ jika dan hanya jika $x|m, y|m$, $m > 0$, dan untuk sebarang kelipatan persekutuan n dari x dan y berlaku $m|n$.

Bukti:

(\rightarrow)

Ambil $m = [x, y]$, maka menurut Definisi 2.4, $x|m, y|m$, $m > 0$.

Misalkan n adalah sebarang kelipatan persekutuan x dan y , maka $x|n$ dan $y|n$. Harus ditunjukkan bahwa $m|n$. Menurut Algoritma Pembagian, karena $m \leq n$, maka tentu ada $k, s \in \mathbb{Z}$ sehingga $n = km + s$, $0 \leq s < m$.

Untuk membuktikan $m|n$, harus ditunjukkan bahwa $n = km$, atau harus ditunjukkan bahwa $s = 0$.

Perhatikan bahwa $n = km + s$, maka $s = n - km$.

$x|m$ dan $y|m$, maka $x|am$ dan $y|am$

$x|n$ dan $x|am$, maka $x|n - am$

$y|n$ dan $y|am$, maka $y|n - am$

$x|n - am$ dan $y|n - am$, maka $n - am$ adalah kelipatan persekutuan x dan y .

$s = n - km$, $x|n - km$, dan $y|n - km$, maka $x|s$ dan $y|s$.

$x|s$ dan $y|s$, maka s kelipatan persekutuan x dan y .

Karena s dan m adalah kelipatan-kelipatan persekutuan x dan y , dan m adalah yang terkecil, serta $0 \leq s < m$, maka jelas bahwa $s = 0$, sehingga $n = km$, atau $m|n$.

(\leftarrow)

Ambil $m > 0$, $x|m, y|m$, dan untuk sebarang kelipatan persekutuan n dari x dan y berlaku $m|n$. Ini berarti bahwa m adalah suatu kelipatan persekutuan dari x dan y yang membagi semua kelipatan persekutuan dari x dan y yang lain. Jadi $m = [x, y]$.

Teorema 2.23

$[mx, my] = m[x, y]$ untuk sebarang $m \in N$.

Bukti:

Ambil $K = [mx, my]$ dan $k = [x, y]$

$K = [mx, my]$, maka sesuai Definisi 2.4, $mx \mid k$ dan $my \mid k$

$k = [x, y]$, maka sesuai Definisi 2.4, $x \mid k$ dan $y \mid k$

$x \mid k$, maka menurut Teorema 2.8, $mx \mid mk$.

$y \mid k$, maka menurut Teorema 2.8, $my \mid mk$

$mx \mid mk$ dan $my \mid mk$, maka menurut Definisi 2.4, mk adalah kelipatan persekutuan dari mx dan my . Karena K adalah kelipatan persekutuan terkecil dari mx dan my , dan mk adalah kelipatan persekutuan mx dan my , maka menurut Teorema 2.22, $K \mid mk$.

Jadi $[mx, my] \mid m[x, y]$

Selanjutnya, karena $mx \mid k$ dan $my \mid K$, maka sesuai Definisi 2.1, $K = amx$ dan

$K = bmy$ untuk suatu $a, b \in Z$, berarti $\frac{K}{m} = ax$ dan $\frac{K}{m} = by$, atau $x \mid \frac{K}{m}$

dan $y \mid \frac{K}{m}$. Karena $x \mid \frac{K}{m}$ dan $y \mid \frac{K}{m}$, maka menurut Definisi 2.4, $\frac{K}{m}$ adalah kelipatan persekutuan x dan y .

Akibatnya, sesuai dengan Teorema 2.22, $[x, y]$ membagi $\frac{K}{m}$, yaitu

$[x, y] \mid \frac{K}{m}$. Karena $[x, y] \mid \frac{K}{m}$, maka menurut Teorema 2.8, $m[x, y] \mid m \cdot \frac{K}{m}$,

atau $m[x, y] \mid K$.

Jadi $m[x, y] \mid [mx, my]$.

Akhirnya, karena $[mx, my] > 0, m[x, y] > 0, [mx, my] \mid m[x, y]$, dan

$m[x, y] \mid [mx, my]$, maka menurut Teorema 2.7, $[mx, my] = m[x, y]$.

Teorema 2.24

Jika $x, y \in N$ dan $[x, y] = 1$, maka $[x, y] = xy$.

Bukti:

$[x, y] = 1$, maka menurut Teorema 2.12, $mx + ny = 1$ untuk suatu $m, n \in Z$, sehingga $[x, y][mx + ny] = [x, y]$, atau $[x, y]mx + [x, y]ny = [x, y]$.

$[x, y]$ adalah kelipatan persekutuan terkecil x dan y , maka sesuai Definisi 2.4, $x | [x, y]$, $y | [x, y]$, berarti sesuai dengan Teorema 2.8.

$xy | [x, y]y$ dan $xy | [x, y]y$. Dengan demikian, sesuai Teorema 2.1, $xy | [x, y]ny$ dan $xy | [x, y]mx$, dan sesuai Teorema 2.5, $xy | [x, y]mx + [x, y]ny$.

Jadi $xy | [x, y][x, y]$ adalah kelipatan persekutuan terkecil x dan y , dan xy adalah kelipatan x dan y , maka menurut Teorema 2.22, $[x, y] | xy$.

Dari $xy | [x, y]$ dan $[x, y] | xy$, maka Teorema 2.7, $xy = [x, y]$, atau $[x, y] = [x, y]$.

Contoh 2.19

- $(2, 3) = 1$, maka $[2, 3] = 2 \cdot 3 = 6$
- $(7, 11) = 1$, maka $[7, 11] = 7 \cdot 11 = 77$
- $(16, 13) = 1$, maka $[16, 13] = 16 \cdot 13 = 208$

Teorema 2.25

Jika $x, y \in Z$, maka $(x, y)[x, y] = xy$.

Bukti:

Ambil $d = (x, y)$, maka sesuai Teorema 2.14, $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$.

Sesuai Teorema 2.24, karena $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$, maka $\left[\frac{x}{d}, \frac{y}{d}\right] = \frac{x}{d} \cdot \frac{y}{d}$, akibatnya $\left(\frac{x}{d}, \frac{y}{d}\right)\left[\frac{x}{d}, \frac{y}{d}\right] = 1 \cdot \frac{x}{d} \cdot \frac{y}{d} = \frac{x}{d} \cdot \frac{y}{d}$

$$\begin{aligned}
 d^2 \left(\frac{x}{d}, \frac{y}{d} \right) \left[\frac{x}{d}, \frac{y}{d} \right] &= d^2 \cdot \frac{xy}{d^2} \\
 d \left(\frac{x}{d}, \frac{y}{d} \right) \cdot d \left(\frac{x}{d}, \frac{y}{d} \right) &= xy, \text{ dan sesuai Teorema 2.13 serta Teorema 2.23,} \\
 \text{diperoleh } \left(d \cdot \frac{x}{d}, d \cdot \frac{y}{d} \right) \cdot \left(d \cdot \frac{x}{d}, d \cdot \frac{y}{d} \right) &= xy \\
 (x, y)[x, y] &= xy.
 \end{aligned}$$

Contoh 2.20

- $(6, 9)[6, 9] = 6 \cdot 9 = 54$
- $(12, 18) = 6$, maka $6[12, 18] = 12 \cdot 18$, sehingga $[12, 18] = \frac{1}{6} \cdot 12 \cdot 18 = 36$
- $(24, 16) = 8$, maka $8[24, 16] = 24 \cdot 16$, sehingga
 $[24, 16] = \frac{1}{8} \cdot 24 \cdot 16 = 48$
- $[36, 48] = \frac{36 \cdot 48}{(36, 48)} = \frac{36 \cdot 48}{12} = 144$

Tugas

Carilah buku bacaan tentang Teori Bilangan, misalnya *Elementary Number Theory and Its Applications* yang ditulis oleh Kenneth H. Rosen, dan diterbitkan oleh Addison-Wesley Publishing Company.

- 1) Jelaskan dan buktikan Teorema Dasar Aritmetika.
- 2) Buktiakan $p, q = pq$ dengan menggunakan Teorema Dasar Aritmetika.
- 3) Nyatakan bentuk umum (p, q) dan $[p, q]$ dengan menggunakan pemfaktoran prima, dan berilah masing-masing dua contoh.

Petunjuk Jawaban Tugas

- 1) Teorema Dasar Aritmetika
 Setiap bilangan bulat positif lebih dari satu dapat dinyatakan sebagai kelipatan atau faktor-faktor prima secara tunggal, dalam urutan yang tidak menurun.

Bukti :

Untuk membuktikan Teorema Dasar Aritmetika diperlukan dua teorema pendukung yaitu:

- (a) jika $p, q, r \in \mathbb{Z}^+, (p, q) = 1$ dan $p | qr$, maka $p | r$
- (b) jika p adalah suatu bilangan prima, $p | x_1 x_2 \dots x_n$, dan $x_1, x_2, \dots, x_n \in \mathbb{Z}^+$, maka tentu ada bilangan bulat i dengan $1 \leq i \leq n$ sedemikian hingga $p | x_i$

Selanjutnya akan dibuktikan dengan cara tidak langsung.

Anggaplah ada bilangan-bilangan bulat positif yang tidak dapat ditulis sebagai faktor-faktor prima. Ambil bilangan-bilangan itu yang terkecil, maka menurut prinsip urutan rapi, n pasti ada.

Jika n adalah suatu bilangan prima, maka n memuat faktor prima yaitu n sendiri. Jika n bukan suatu bilangan prima, maka n adalah suatu bilangan komposit, misalkan $n = ab$, $1 < a < n$, dan $1 < b < n$.

Karena $a < n$ dan $b < n$, maka sesuai dengan teorema (b) di atas, a dan b masing-masing mempunyai faktor prima, dengan demikian n dapat dinyatakan sebagai kelipatan bilangan-bilangan prima.

Untuk membuktikan ketunggalan pemfaktoran, dimisalkan pemfaktoran n tidak tunggal, yaitu n dapat dinyatakan dalam dua pemfaktoran yang berbeda:

$$N = p_1 p_2 \dots p_i \text{ dan } n = q_1 q_2 \dots q_j$$

dimana p_1, p_2, \dots, p_i dan $n = q_1, q_2, \dots, q_j$ semuanya adalah bilangan-bilangan prima dan $p_1 \leq p_2 \leq \dots \leq p_i$ dan $n = q_1 \leq q_2 \leq \dots \leq q_j$.

Dengan demikian dapat ditentukan bahwa: $p_1 p_2 \dots p_i = q_1 q_2 \dots q_j$

Jika faktor-faktor prima persekutuan ruas kiri dan ruas kanan dihapus, maka setelah pengaturan ulang diperoleh :

$$p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$$

$$p_1 (p_2 \dots p_m) = q_1 q_2 \dots q_n$$

Dengan demikian $p_1 | q_1 q_2 \dots q_n$, dan sesuai dengan teorema (b) di atas, $p_1 | q_r$ untuk suatu r yang mana $1 \leq r \leq n$. Karena p_1 dan q_r keduanya adalah bilangan prima, maka $p_1 = q_r$, terjadi kontradiksi, yaitu $p_1 p_2 \dots p_m$ dan $q_1 q_2 \dots q_n$ masih mempunyai faktor persekutuan. Jadi pemfaktoran prima dari n adalah tunggal.

2) Misalkan pemfaktoran prima dari x dan y adalah:

$$x = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m} \text{ dan } y = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}$$

dimana masing-masing bilangan pangkat adalah suatu bilangan bulat tidak negatif, dan bilangan-bilangan prima yang menjadi faktor x sama dengan yang menjadi faktor y , yaitu dengan pangkat bilangan nol.

Dengan demikian:

$$(x, y) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \dots p_m^{\min(r_m, s_m)}$$

$$[x, y] = p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \dots p_m^{\max(r_m, s_m)}$$

Jika $\min(r_i, s_i) = k_i$ dan $\max(r_i, s_i) = K_i$ maka:

$$(x, y) = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

$$[x, y] = p_1^{K_1} p_2^{K_2} \dots p_m^{K_m}$$

sehingga:

$$\begin{aligned} (x, y)[x, y] &= \left(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \right) \left(p_1^{K_1} p_2^{K_2} \dots p_m^{K_m} \right) \\ &= p_1^{k_1+K_1} p_2^{k_2+K_2} \dots p_m^{k_m+K_m} \end{aligned}$$

Kita dapat membuktikan suatu teorema bahwa

$$\min(r, s) + \max(r, s) = r + s \text{ sebagai berikut:}$$

Jika $r \geq s$, maka $\min(r, s) = s$ dan $\max(r, s) = r$ sehingga

$$\min(r, s) + \max(r, s) = r + s$$

Jika $r < s$, maka $\min(r, s) = r$ dan $\max(r, s) = s$ sehingga

$$\min(r, s) + \max(r, s) = r + s .$$

Akibatnya, kita dapat menentukan bahwa :

$$p_i^{k_i+K_i} = p_i^{\min(r_i, s_i) + \max(r_i, s_i)} = p_i^{r_i+s_i}$$

Dengan demikian:

$$\begin{aligned} (x, y)[x, y] &= p_1^{k_1+K_1} p_2^{k_2+K_2} \dots p_m^{k_m+K_m} \\ &= p_1^{r_1+s_1} p_2^{r_2+s_2} \dots p_m^{r_m+s_m} \\ &= \left(p_1^{r_1} p_2^{r_2} \dots p_m^{r_m} \right) \left(p_1^{s_1} p_2^{s_2} \dots p_m^{s_m} \right) \\ &= xy \end{aligned}$$

3) Jika $x = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ dan $y = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}$, maka:

$$(x, y) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \dots p_m^{\min(r_m, s_m)}$$

$$[x, y] = p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \dots p_m^{\max(r_m, s_m)}$$

Contoh :

$$1. \quad x = 18 = 2^1 \cdot 3^2$$

$$y = 24 = 2^3 \cdot 3^1$$

$$(x, y) = 2^{\min(1, 3)} \cdot 3^{\min(2, 1)} = 2^1 \cdot 3^1 = 2 \cdot 3 = 6$$

$$[x, y] = 2^{\max(1, 3)} \cdot 3^{\max(2, 1)} = 2^3 \cdot 3^2 = 8 \cdot 9 = 72$$

$$2. \quad x = 36 = 2^2 \cdot 3^2 \cdot 5^0$$

$$y = 45 = 2^0 \cdot 3^2 \cdot 5^1$$

$$(x, y) = 2^{\min(2, 0)} \cdot 3^{\min(2, 2)} \cdot 5^{\min(0, 1)} = 2^0 \cdot 3^2 \cdot 5^0 = 1 \cdot 9 \cdot 1 = 9$$

$$[x, y] = 2^{\max(2, 0)} \cdot 3^{\max(2, 2)} \cdot 5^{\max(0, 1)} = 2^2 \cdot 3^2 \cdot 5^1 = 4 \cdot 9 \cdot 5 = 180$$



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Nyatakan $(2345)_{10}$ dalam notasi lambang bilangan

(a) basis 7

(b) basis 8

2) Diketahui $p, q \in \mathbb{Z}$ dan $(p, q) = 1$

Carilah semua kemungkinan nilai $d = (p+q, p-q)$

3) Tunjukkan bahwa $(3t+2)$ dan $(5t+3)$ adalah prima relatif, $t \in \{0, 1, 2, 3, \dots\}$

4) Carilah m dan n jika :

$$(a) \quad 67815m + 21480n = (67815, 21480)$$

$$(b) \quad 30745m + 17446n = (30745, 17446)$$

- 5) Buktikan : jika $(x, y) = 1$ dan $z = x + y$, maka $(x, z) = (y, z) = 1$
- 6) Buktikan : $(r + ts, s) = (r, s)$
- 7) Diketahui : $(4, p) = 2$ dan $(4, q) = 2$. Carilah $(4, p + q)$
- 8) Diketahui p adalah suatu bilangan prima $m, n \in \mathbb{Z}$ dan memenuhi hubungan, $(p^2, m) = p$ dan $(p^3, n) = p^2$
Carilah (p^4, mn)
- 9) Carilah $(x^2, 108)$ jika diketahui $(x, 18) = 6$

Petunjuk Jawaban Latihan

- 1) a. $2345 = 7.335 + 0$ b. $2345 = 8.293 + 1$
 $335 = 7.47 + 6$ $293 = 8.36 + 5$
 $47 = 7.6 + 5$ $36 = 8.4 + 4$
 $6 = 7.0 + 6$ $4 = 8.0 + 4$
 $(2345)_{10} = (6560)_7$ $(2345)_{10} = (4451)_8$
- 2) $d = (p+q, p-q)$ maka $d | p+q$ dan $d | p-q$ sehingga
 $d | (p+q) - (p-q)$ atau $d | 2p$ dan $d | 2q$.
Dengan demikian d adalah faktor persekutuan dari $2p$ dan $2q$, berarti
 $d | (2p, 2q)$, atau $d | 2(p, q)$.
Karena $(p, q) = 1$ dan $d | 2(p, q)$, maka $d | 2$, berarti $d = 1$ atau $d = 2$.

- 3) $(3t+2, 5t+3) = (3t+2, 5t+3-3t-2) = (3t+2, 2t+1) =$
 $(3t+2-2t-1, 2t+1) = (t+1, 2t+1) = (t+1, 2t+1-t-1) = (t+1, t) =$
 $(t+1-t, t) = (1, t) = 1$.

Atau

karena $5(3t+2) - 3(5t+3) = 1$, maka 1 adalah bilangan bulat positif terkecil yang merupakan kombinasi linier dari $3t+2$ dan $5t+3$, jadi $(3t+2, 5t+3) = 1$.

4) a. $67815 = 3.21480 + 3375$
 $21480 = 6.3375 + 1230$
 $3375 = 2.1230 + 915$
 $1230 = 1.915 + 315$
 $915 = 2.315 + 285$
 $315 = 1.285 + 30$
 $285 = 9.30 + 15$
 $30 = 2.15 + 0$

n	s	t	q
1	1	0	3
2	0	1	6
3	1	-3	2
4	-6	19	1
5	13	-41	2
6	-19	60	1
7	51	-161	9
8	-70	221	-
9	681	-2150	-

Jadi $m = 681$ dan $n = -2150$.

b. Kerjakan dengan jalan yang sama, $m = 21$ dan $n = -37$.

- 5) Misalkan $d = (x, z)$, maka $d \mid x$ dan $d \mid z$
 $d \mid z$ dan $z \mid x+y$, maka $d \mid x+y$; $d \mid x+y$ dan $d \mid x$, maka $d \mid y$
 $d \mid x$ dan $d \mid y$, maka d adalah faktor persekutuan dari x dan y , sehingga
 $d \mid (x, y)$. Karena $d \mid (x, y)$ dan $(x, y) = 1$, maka $d \mid 1$.

Jadi $(x, z) = 1$

- 6) Harus dibuktikan $(r+ts) \mid (r, s)$ dan $(r, s) \mid (r+ts, s)$
 $(r+ts, s) \mid s$, maka $(r+ts, s) \mid ts$
Karena $(r+ts, s) \mid ts$ dan $(r+ts, s) \mid r+ts$, maka $(r+ts, s) \mid r$.
Selanjutnya $(r+ts, s) \mid r$ dan $(r+ts, s) \mid s$ maka $(r+ts, s)$ adalah faktor persekutuan dari r dan s , dengan demikian $(r+ts, s) \mid (r, s)$.

Teruskan untuk membuktikan $(r, s) \mid (r+ts, s)$.

- 7) $(4, p) = 2$, maka $2 \mid p$, berarti $p = 2r$ untuk suatu $r \in \mathbb{Z}$
 $(4, q) = 2$, maka $2 \mid q$, berarti $q = 2s$ untuk suatu $s \in \mathbb{Z}$

r dan s tidak mungkin bilangan genap, sebab untuk $r = 2m$ dan $s = 2n$ berakibat $p = 4m$, dan $q = 4n$, sehingga $(4, p) = (4, 4m) = 4(1, m) = 4 \cdot 1 = 4$ dan juga $(4, q) = 4$.

Dengan demikian r dan s keduanya harus bilangan ganjil, misalnya $r = 2m+1$ dan $s = 2n+1$, maka

$$(4, p + q) = (4, 4m + 2 + 4n + 2) = 4(1, m + n + 1) = 4 \cdot 1 = 4.$$

8) $(p^2, m) = p$, maka $(p, m/p) = 1$

$$(p^3, n) = p^2, \text{ maka } (p, n/p^2) = 1$$

Karena $(p, m/p) = 1$ dan $(p, n/p^2) = 1$, maka $(p, mn/p^3) = 1$, atau $p^3 \cdot (p, mn/p^3) = p^3$.

Jadi $(p^4, mn) = p^3$

9) $(x, 18) = 6$, maka $(x/6, 3) = 1$ sehingga $(x^2/36, 3) = 1$, akibatnya

$$36(x^2/36, 3) = 36$$

Dengan demikian $(x^2, 108) = 36$.



RANGKUMAN

Dalam Kegiatan Belajar 2 ini, secara keseluruhan materi pembahasan terkait dengan konsep FPB dan KPK, didalamnya banyak berbicara tentang definisi dan teorema, serta beberapa penerapannya.

1. (x, y) adalah notasi untuk menyatakan FPB dari x dan y
 (x, y) adalah suatu bilangan bulat positif terbesar yang membagi x dan membagi y .
2. $[x, y]$ adalah notasi untuk menyatakan KPK dari x dan y
 $[x, y]$ adalah suatu bilangan bulat positif terkecil yang habis dibagi oleh x dan oleh y .
3. Terdapat 14 teorema tentang FPB dan KPK

- 2.12 $d = (x, y)$ adalah suatu bilangan bulat positif terkecil yang merupakan kombinasi linier dari x dan y
- 2.13 Jika $k \in N$, maka $k(x, y) = (kx, ky)$
- 2.14 Jika $d = (x, y)$, maka $(x/d, y/d) = 1$
- 2.15 Jika $p | qr$ dan $(p, q) = 1$, maka $p | r$
- 2.16 Jika $(x, t) = 1$ dan $(y, t) = 1$, maka $(xy, t) = 1$
- 2.17 Jika f adalah suatu faktor persekutuan dari x dan y maka $f | (x, y)$
- 2.18 $(x, y) = (y, x) = (x, -y) = (-x, y) = (-x, -y)$
- 2.19 $(x, y) = (x, y + ax) = (x + by, y)$ untuk sebarang $a, b \in Z$
- 2.20 Algoritma Euclides
- 2.21 Teknik mencari m dan n jika $(x, y) = mx + ny$
- 2.22 $[x, y] | k$ untuk sebarang kelipatan x dan y
- 2.23 Jika $m \in N$, maka $m[p, q] = [mp, mq]$
- 2.24 Jika $(x, y) = 1$, maka $[x, y] = xy$
- 2.25 $(x, y)[x, y] = xy$



TES FORMATIF 2

- 1) Skor 20
Carilah kemungkinan nilai-nilai d jika:
 $(a, b) = 1$ dan $d = (a^2 + b^2, a + b)$
 $(a, b) = 1$ dan $d = (a + b, a^2 - ab + b^2)$
- 2) Skor 20
Carilah nilai-nilai x dan y jika :
 $67320x + 96577y = (67320, 96577)$

3) Skor 20

Carilah nilai-nilai x dan y jika: $(34709,100319) = 34709x + 100319y$

4) Skor 10

Nyatakan $(2008)_{10}$ dalam notasi basis 2

5) Skor 20

Dengan menggunakan Teorema Dasar Aritmetika, carilah faktor persekutuan terbesar dari 1815156 dan 686000.

6) Skor 10

Nyatakan dengan B (Benar) atau S (Salah)

(a) Jika $(a, b) = (a, c)$, maka $b = c$

(b) $(-12, -16) = -4$

(c) $(2p, 20+2p)$ tidak membagi 20

(d) $(-5, 0)$ tidak didefinisikan

(e) Jika $t = [2x, 3y]$, maka x membagi t dan y membagi t

(f) Jika $[p, q] = [r, s]$, maka $p = r$ dan $q = s$

(g) $3x$ membagi $[x, y]$

(h) $(2x-7, 2x)$ membagi 7

(i) (p, q) membagi $5p$

(j) $(r, r-4) = 1, 2$, atau 4.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) a. $3|12$, $3|8+4$, tetapi $3 \nmid 8$ dan $3 \nmid 4$
 b. $4|20$, $4|2.10$, tetapi $4 \nmid 2$ dan $4 \nmid 10$
 c. $8|16$, $3+5|16$, tetapi $3 \nmid 16$ dan $5 \nmid 16$
 d. $2|6$ dan $3|6$, tetapi $2 \neq 3$
 e. $2|4$ dan $2|6$, tetapi $4 \neq 6$
- 2) a.
$$\begin{aligned} n &= a_7 \cdot 10^7 + a_6 \cdot 10^6 + a_5 \cdot 10^5 + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &= (a_0 + 10a_1) + (99a_2 + a_2) + (990a_3 + 10a_3) + (9999a_4 + a_4) + \\ &\quad (99990a_5 + 10a_5) + (999999a_6 + a_6) + (9999990a_7 + 10a_7) \\ n &= (a_0 + 10a_1) + (a_2 + 10a_3) + (a_4 + 10a_5) + (a_6 + 10a_7) + \\ &\quad 99(a_2 + 10a_3 + 101a_4 + 1010a_5 + 10101a_6 + 101010a_7) \end{aligned}$$

 Karena $99|n$ dari

$$\begin{aligned} 99|(a_2 + 10a_3 + 101a_4 + 1010a_5 + 10101a_6 + 101010a_7) \text{ maka} \\ 99|(a_0 + 10a_1) + (a_2 + 10a_3) + (a_4 + 10a_5) + (a_6 + 10a_7) \\ 99|(a_1 \cdot 10 + a_0) + (a_3 \cdot 10 + a_2) + (a_5 \cdot 10 + a_4) + (a_7 \cdot 10 + a_6) \end{aligned}$$

 Jadi $99|(a_1a_0) + (a_3a_2) + (a_5a_4) + (a_7a_6)$
- b. Serupa dengan jawaban a, gantilah:
 $100a_2$ dengan $(101a_2 - a_2)$, $1000a_3$ dengan $(1010a_3 - 10a_3)$,
 $10000a_4$ dengan $(9999a_4 + a_4)$, $100000a_5$ dengan $(99990a_5 - 10a_5)$,
 $1000000a_6$ dengan $(1000001a_6 - a_6)$, $1000000a_7$ dengan $(10000010a_7 - 10a_7)$.
- 3) Sesuai dengan Definisi 2.1:
 $p|(q + r)$, maka $q + r = xp$ untuk suatu $x \in \mathbb{Z}$
 $p|q$ maka $q = yp$ untuk suatu $y \in \mathbb{Z}$
 $q + r = xp$ dan $q = yp$, maka $yp + r = xp$, $r = (x - y)p$
 Jadi $p|r$.

$$4) \quad n^3 + 6n^2 + 8n = n(n^2 + 6n + 8) = n(n+2)(n+4)$$

Sesuai dengan Teorema Algoritma Pembagian, n dapat dinyatakan sebagai salah satu dari $n = 3k$, $n = 3k + 1$, atau $n = 3k + 2$.

$n(n+2)(n+4)$ memuat faktor 3 jika n diganti dengan $n = 3k$, $n = 3k + 1$, atau $n = 3k + 2$.

- 5) a. 37859

$$37859 = 2.18929 + 1$$

$$18929 = 2.9464 + 1$$

$$9464 = 2.4732 + 0$$

$$4732 = 2.2366 + 0$$

$$2366 = 2.1183 + 0$$

$$1183 = 2.591 + 1$$

$$591 = 2.295 + 1$$

$$295 = 2.147 + 1$$

$$147 = 2.73 + 1$$

$$73 = 2.36 + 1$$

$$36 = 2.18 + 1$$

$$18 = 2.9 + 1$$

$$9 = 2.4 + 1$$

$$4 = 2.2 + 0$$

$$2 = 2.1 + 0$$

$$1 = 2.0 + 1$$

$$(37859)_{10} = (1001111111|00011)_2$$

- b. 1 6

$$\begin{array}{r} 3246793 \\ 2475619839 \\ \hline 7 | 693,11 | 693 \end{array}$$

$$2475619839 \text{, tetapi } 143 \nmid 2475619839$$

$$7 | 693,11 | 693, \text{ dan } 13 \nmid 693$$

$$\text{Jadi } 77 | 2475619839, \text{ tetapi } 143 \nmid 2475619839$$

Tes Formatif 2

- 1) (a) $d = \gcd(a^2 + b^2, a+b)$, maka menurut Definisi 2.3, $d \mid a^2 + b^2$ dan $d \mid a+b$. $d \mid a+b$ maka sesuai Teorema 2.1, $d \mid (a+b)(a+b)$ atau $d \mid (a+b)^2$, berarti $d \mid a^2 + 2ab + b^2$ dan $d \mid a^2 + b^2$, maka berdasarkan Teorema 2.4, dapat ditentukan bahwa $d \mid ((a^2 + 2ab + b^2) - (a^2 + b^2))$, atau $d \mid 2ab$.

Karena $d \mid a+b$ dan $(a, b) = 1$ maka dapat dibuktikan bahwa $(a, d) = (b, d) = 1$ sebagai berikut :

Misalkan $(a, d) = t$, maka menurut Definisi 2.3, $t \mid a$ dan $t \mid d$ $t \mid a$ dan $a \mid a+b$, maka menurut Teorema 2.2, $t \mid b$, dengan demikian dari $t \mid a$ dan $t \mid b$, sesuai dengan Definisi 2.3, t adalah faktor persekutuan dari a dan b , dan sesuai dengan Teorema 2.17, $t \mid (a, b)$ atau $t \mid 1$, berarti $t = 1$ sebab $t > 0$.

Jadi $t = (a, d) = 1$, dan dengan jalan yang sama, dapat ditentukan $(b, d) = 1$.

Selanjutnya, karena $(a, d) = 1$ dan $d \mid 2ab$, atau $d \mid a(2b)$, maka sesuai Teorema 2.15, $d \mid 2b$, atau $d \mid b$. (2), berarti menurut Teorema 2.15, $d \mid 2$ karena $(d, b) = 1$.

Karena $d > 0$ dan $d \mid 2$, maka $d = 1$ atau $d = 2$.

- (b) $d = \gcd(a^2 - ab + b^2, a+b)$, maka menurut Definisi 2.3, $d \mid a^2 - ab + b^2$ dan $d \mid a+b$.

Kerjakan serupa dengan (a) sehingga diperoleh $d \mid 3ab$

Karena $d \mid 3ab$, $(d, a) = 1$, dan $(d, b) = 1$, maka $d \mid 3$. Jadi $d = 1$, $d = 2$, atau $d = 3$ karena $d > 0$ dan $d \mid 3$.

- | | | | | | |
|----|---------------------------|-----|-----|-----|-----|
| 2) | $96577 = 1.67320 + 29257$ | n | s | t | q |
| | $67320 = 2.29257 + 8806$ | 1 | 1 | 0 | 1 |
| | $29257 = 3.8806 + 2839$ | 2 | 0 | 1 | 2 |

8806	$= 3.2839 + 289$	3	1	-1	3
2839	$= 9.289 + 238$	4	-2	3	3
289	$= 1.238 + 51$	5	7	-10	9
238	$= 4.51 + 34$	6	-23	33	1
51	$= 1.34 + 17$	7	214	-307	4
34	$= 2.17 + 0$	8	-237	340	1
		9	1162	-1667	
		10	-1399	2007	

$$(96577, 67320) = 17 = (-1399)(96577) + (2007)(67320)$$

Jadi $m = -1399$ dan $n = 2007$.

3)	100313	$= 2.34709 + 30895$	n	s	t	q
	34709	$= 1.30895 + 3814$	1	1	0	2
	30895	$= 8.3814 + 383$	2	0	1	1
	3814	$= 9.383 + 367$	3	1	-2	8
	383	$= 1.367 + 16$	4	-1	3	9
	367	$= 22.16 + 15$	5	9	-26	1
	16	$= 1.15 + 1$	6	-82	237	22
	15	$= 15.1 + 0$	7	91	-263	1
			8	-2084	6023	
			9	2175	-6286	

$$(100313, 34709) = 1 = (2175)(100313) + (-6286)(34709)$$

Jadi $m = 2175$ dan $n = -6286$

- 4) $2008 = 2.1004 + 0$
 1004 = 2.502 + 0
 502 = 2.251 + 0
 251 = 2.125 + 1
 125 = 2.62 + 1
 62 = 2.31 + 0
 31 = 2.15 + 1
 15 = 2.7 + 1
 7 = 2.3 + 1

$$3 = 2.1+1$$

$$1 = 2.0+1$$

$$(2008)_{10} = (11111011000)_2$$

5) $1815156 = 2.907578 = 2.2.453789 = 2.2.3.151263 = 2.2.3.3.50421 = 2.2.3.3.3.16807$
 $= 2.2.3.3.3.7.2401 = 2.2.3.3.3.7.7.343 = 2.2.3.3.3.7.7.7.49$
 $= 2.2.3.3.3.7.7.7.7$
 $= 2^2 \cdot 3^3 \cdot 7^5$
 $686000 = 2.343000 = 2.2.171500 = 2.2.2.85750 = 2.2.2.2.42875 = 2.2.2.2.5.8575$
 $= 2.2.2.2.5.5.1715 = 2.2.2.2.5.5.5.343 = 2.2.2.2.5.5.5.7.49$
 $= 2.2.2.2.5.5.5.7.7.7$
 $= 2^4 \cdot 5^3 \cdot 7^3$
 $(1815156, 686000) = 2^2 \cdot 7^3 = 4.343 = 1372$

Cara di atas dapat dinyatakan dengan cara serupa:

$$2 \quad 1815156 \quad 686000$$

$$2 \quad 907578 \quad 343000$$

$$7 \quad 64827 \quad 24500$$

$$7 \quad 9261 \quad 3500$$

$$7 \quad 1323 \quad 500$$

Karena $(1323, 500) = 1$, maka $(1815156, 686000) = 2.2.7.7.7 = 1372$

- 6) (a) S (f) S
(b) S (g) S
(c) S (h) B
(d) S (i) B
(e) B (j) B

Daftar Pustaka

- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Kongruensi

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul Kongruensi ini diuraikan tentang sifat-sifat dasar kongruensi, keterkaitan kongruensi dengan FPB dan KPK, sistem residu yang lengkap dan sistem residu yang tereduksi, Teorema Euler, Teorema Kecil Fermat, dan Teorema Wilson.

Kongruensi merupakan kelanjutan dari keterbagian, dan didefinisikan berdasarkan konsep keterbagian. Dengan demikian penjelasan dan pembuktian teorema-teoremanya dikembalikan ke konsep keterbagian. Bahan utama kongruensi adalah penggunaan bilangan sebagai modulo, dan bilangan modulo ini dapat dipandang sebagai perluasan dari pembahasan yang sudah ada di sekolah dasar sebagai bilangan jam, dan pada tingkat lebih lanjut disebut dengan bilangan bersisa.

Dengan bertambahnya uraian tentang sistem residu, pembahasan tentang kongruensi menjadi lebih lengkap sebagai persiapan penjelasan Teorema Euler, Teorema Kecil Fermat, dan Teorema Wilson, serta bahan penerapan yang terkait dengan Teorema Kongruensi dan Teorema Euler.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep kongruensi, penerapan dan hubungan dengan konsep keterbagian, pengembangan dalam sistem residu, dan peranannya dalam penjabaran Teorema Euler, Teorema Kecil Fermat, dan Teorema Wilson.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep kongruensi dan sifat-sifatnya, konsep sistem residu yang lengkap dan sistem residu yang tereduksi, peranan FPB dan KPK dalam pengembangan sifat-sifat kongruensi, pembuktian dan penerapan Teorema Euler, Teorema Kecil Fermat, dan Teorema Wilson.

Susunan Kegiatan Belajar

Modul 3 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Kongruensi, dan Kegiatan Belajar 2 adalah Sistem Residu. Setiap kegiatan belajar memuat Uraian, Contoh/Bukan Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 3 ini ditempatkan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi paparan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab/menyelesaikan permasalahan, maka lihatlah Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum banyak membantu Anda keluar dari kesulitan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah tingkat kemampuan Anda dengan jalan mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah pengerojan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Konsep Dasar Kongruensi**

Kongruensi merupakan bahasa teori bilangan karena pembahasan teori bilangan bertumpu pada kongruensi. Bahasa kongruensi ini diperkenalkan dan dikembangkan oleh Karl Friedrich Gauss, matematis paling terkenal dalam sejarah, hidup pada awal abad sembilan belas, sehingga sering disebut sebagai Pangeran Matematisi (*The Prince of Mathematicians*). Meskipun Gauss tercatat karena temuan-temuannya di dalam geometri, aljabar, analisis, astronomi, dan fisika matematika, ia mempunyai minat khusus di dalam teori bilangan dan mengatakan bahwa “**mathematics is the queen of sciences, and the theory of numbers is the queen of mathematics**”. Gauss merintis untuk meletakkan teori bilangan modern di dalam bukunya *Disquisitiones Arithmeticae* pada tahun 1801.

Secara tidak langsung kongruensi sudah dibahas sebagai bahan matematika di sekolah dalam bentuk bilangan jam atau bilangan bersisa. Peragaan dengan menggunakan tiruan jam dipandang bermanfaat karena peserta didik akan langsung praktik untuk lebih mengenal adanya sistem bilangan yang berbeda yaitu sistem bilangan jam, misalnya bilangan jam duaan, tigaan, empatan, limaan, enaman, dan seterusnya.

Kemudian, kita telah mengetahui bahwa bilangan-bilangan bulat lebih dari 4 dapat di “reduksi” menjadi 0, 1, 2, 3, atau 4 dengan cara menyatakan sisanya jika bilangan itu dibagi dengan 5, misalnya 13 dapat direduksi menjadi 3 karena 13 dibagi 5 bersisa 3, 50 dapat direduksi menjadi 0 karena 50 dibagi 5 bersisa 0, dan dalam bahasa kongruensi dapat dinyatakan sebagai $13 \equiv 3 \pmod{5}$ dan $50 \equiv 0 \pmod{5}$.

Definisi 3.1

Ditentukan p, q, m adalah bilangan-bilangan bulat dan $m \neq 0$

p disebut kongruen dengan q modulo m , ditulis $p \equiv q \pmod{m}$, jika dan hanya jika $m | p - q$.

Jika $m \nmid p - q$ maka ditulis $p \not\equiv q \pmod{m}$, dibaca p tidak kongruen dengan q modulo m .

Contoh 3.1

$10 \equiv 6 \pmod{2}$ sebab $2|10-6$ atau $2|4$

$13 \equiv -5 \pmod{9}$ sebab $9|13-(-5)$ atau $9|18$

$107 \equiv 2 \pmod{15}$ sebab $15|(107-2)$ atau $15|105$

Teorema 3.1

Jika p , q dan m adalah bilangan-bilangan bulat dan $m \neq 0$, maka $p \equiv q \pmod{m}$ jika dan hanya jika ada bilangan bulat t sehingga $p = q + tm$.

Bukti:

Jika $p \equiv q \pmod{m}$, maka $m|p-q$. Ini berarti bahwa ada suatu bilangan bulat t sehingga $tm = p-q$, atau $p = q + tm$.

Sebaliknya, jika ada suatu bilangan bulat t yang memenuhi $p = q + tm$, maka dapat ditunjukkan bahwa $tm = p-q$, dengan demikian $m|p-q$, dan akibatnya berlaku $p \equiv q \pmod{m}$.

Contoh 4.2

$23 \equiv -17 \pmod{8}$ dan $23 = -17 + 5.8$

Teorema 3.2

Ditentukan m adalah suatu bilangan bulat positif.

Kongruensi modulo m memenuhi sifat-sifat berikut:

(a) Sifat Refleksif.

Jika p adalah suatu bilangan bulat, maka $p \equiv p \pmod{m}$.

(b) Sifat Simetris.

Jika p dan q adalah bilangan-bilangan bulat sedemikian hingga $p \equiv q \pmod{m}$, maka $p \equiv q \pmod{m}$.

(c) Sifat Transitif.

Jika p , q , dan r adalah bilangan-bilangan bulat sedemikian hingga $p \equiv q \pmod{m}$ dan $q \equiv r \pmod{m}$, maka $p \equiv r \pmod{m}$.

Bukti:

- (a) Kita tahu bahwa $m|0$, atau $m|p-p$, berarti $p \equiv q \pmod{m}$.
- (b) Jika $p \equiv q \pmod{m}$, maka $m|p-q$, dan menurut definisi keterbagian, ada suatu bilangan bulat t sehingga $tm = p-q$, atau $(-t)m = q-p$, berarti $m|q-p$.
- Dengan demikian $q \equiv p \pmod{m}$.
- (c) Jika $p \equiv q \pmod{m}$ dan $q \equiv r \pmod{m}$, maka $m|p-q$ dan $m|q-r$, dan menurut definisi keterbagian, ada bilangan-bilangan bulat s dan t sehingga $sm = p-q$ dan $tm = q-r$. Dengan demikian dapat ditunjukkan bahwa $p-r = (p-q)+(q-r) = sm+tm = (s+t)m$. Jadi $m|p-r$, dan akibatnya $p \equiv r \pmod{m}$.

Contoh 4.3

$5 \equiv 5 \pmod{7}$ dan $-10 \equiv -10 \pmod{15}$ sebab $7|5-5$ dan $15|-10-(-10)$.
 $27 \equiv 6 \pmod{7}$ akibatnya $6 \equiv 27 \pmod{7}$ sebab $7|6-27$ atau $7|(-21)$.
 $45 \equiv 21 \pmod{3}$ dan $21 \equiv 9 \pmod{3}$, maka $45 \equiv 9 \pmod{3}$ sebab $3|45-9$ atau $3|36$.

Teorema 3.3

Jika p , q , r , dan m adalah bilangan-bilangan bulat dan $m > 0$ sedemikian hingga $p \equiv q \pmod{m}$, maka:

- (a) $p+r \equiv q+r \pmod{m}$
 (b) $p-r \equiv q-r \pmod{m}$
 (c) $pr \equiv qr \pmod{m}$

Bukti:

- (a) Diketahui $p \equiv q \pmod{m}$, maka $m|p-q$.

Selanjutnya dapat ditunjukkan bahwa $p-q = (p+r)-(q+r)$, sehingga $m|(p+r)-(q+r)$. Dengan demikian $p+r \equiv q+r \pmod{m}$.

- (b) Kerjakan, ingat bahwa $p - q = (p - r) - (q - r)$.
- (c) Diketahui $p \equiv q \pmod{m}$, maka $m \mid p - q$, dan menurut Teorema Keterbagian, $m \mid r(p - q)$ untuk sebarang bilangan bulat r , dengan demikian $m \mid pr - qr$. Jadi $pr \equiv qr \pmod{m}$.

Contoh 4.4

$43 \equiv 7 \pmod{6}$, maka $43 + 5 \equiv 7 + 5 \pmod{6}$ atau $48 \equiv 12 \pmod{6}$

$27 \equiv 6 \pmod{7}$, maka $27 - 4 \equiv 6 - 4 \pmod{7}$ atau $23 \equiv 2 \pmod{7}$

$35 \equiv 3 \pmod{8}$, maka $35 \cdot 4 \equiv 3 \cdot 4 \pmod{8}$ atau $140 \equiv 12 \pmod{8}$

Contoh 4.5

Perhatikan bahwa Teorema 3.3.(c) tidak bisa dibalik, artinya jika $pr \equiv qr \pmod{m}$, maka belum tentu bahwa $p \equiv q \pmod{m}$, misalnya $4 \cdot 6 \equiv 4 \cdot 3 \pmod{6}$, tetapi $6 \not\equiv 3 \pmod{6}$.

Teorema 3.4

Jika p, q, r, s, m adalah bilangan-bilangan bulat dan $m > 0$ sedemikian hingga $p \equiv q \pmod{m}$ dan $r \equiv s \pmod{m}$, maka :

- (a) $p + r \equiv q + s \pmod{m}$
- (b) $p - r \equiv q - s \pmod{m}$
- (c) $pr \equiv qs \pmod{m}$

Bukti:

- (a) $p \equiv q \pmod{m}$ dan $r \equiv s \pmod{m}$, maka $m \mid p - q$ dan $m \mid r - s$, maka tentu ada bilangan-bilangan bulat t dan u sehingga $tm = p - q$ dan $um = r - s$, dan $(p + r) - (q + s) = tm - um = m(t - u)$. Dengan demikian $m \mid (p + r) - (q + s)$, atau $p + r \equiv q + s \pmod{m}$.
- (b) Kerjakan, perhatikan bahwa $(p - r) - (q - s) = (p - q) - (r - s)$.
- (c) $p \equiv q \pmod{m}$ dan $r \equiv s \pmod{m}$, maka $m \mid p - q$ dan $m \mid r - s$, maka tentu ada bilangan-bilangan bulat t dan u sehingga $tm = p - q$ dan $um = r - s$, dan $pr - qs = pr - qr + qr - qs = r(p - q) + q(r - s)$

$$= rtm + qum = m(rt + qu).$$

Dengan demikian $m|pr - qs$, atau $pr \equiv qs \pmod{m}$.

Contoh 3.6

$36 \equiv 8 \pmod{7}$ dan $53 \equiv 4 \pmod{7}$, maka $36 + 53 \equiv 8 + 4 \pmod{7}$ atau

$$89 \equiv 12 \pmod{7}$$

$72 \equiv 7 \pmod{5}$ dan $43 \equiv 3 \pmod{5}$, maka $72 - 43 \equiv 7 - 3 \pmod{5}$ atau

$$29 \equiv 4 \pmod{5}$$

$15 \equiv 3 \pmod{4}$ dan $23 \equiv 7 \pmod{4}$ maka $15 \cdot 23 \equiv 3 \cdot 7 \pmod{4}$ atau

$$345 \equiv 21 \pmod{4}$$

Teorema 3.5

(a) Jika $p \equiv q \pmod{m}$, maka $pr \equiv qr \pmod{mr}$.

(b) Jika $p \equiv q \pmod{m}$ dan $d|m$, maka $p \equiv q \pmod{d}$.

Bukti:

(a) Misalkan $p \equiv q \pmod{m}$, maka sesuai Definisi 3.1, $m|p - q$, dan menurut Teorema 2.8 dapat ditentukan bahwa $rm|r(p - q)$ atau $mr|pr - qr$, dan berdasarkan Definisi 3.1 dapat ditentukan bahwa $pr \equiv qr \pmod{mr}$.

(b) Misalkan $p \equiv q \pmod{m}$, maka sesuai Definisi 3.1, $m|p - q$.

Berdasarkan Teorema 2.2, karena $d|m$ dan $m|p - q$ berakibat $d|p - q$, dan sesuai dengan Definisi 3.1, $p \equiv q \pmod{d}$.

Teorema 3.6

Diketahui bilangan-bilangan bulat a, p, q, m , dan $m > 0$.

(a) $ap \equiv aq \pmod{m}$ jika dan hanya jika $p \equiv q \pmod{m/(a,m)}$

(b) $p \equiv q \pmod{m_1}$ dan $p \equiv q \pmod{m_2}$ jika dan hanya jika
 $p \equiv q \pmod{[m_1, m_2]}$

Bukti:(a) (\rightarrow)

Misalkan $ap \equiv aq \pmod{m}$, maka sesuai Definisi 3.1, $m | ap - aq$, dan sesuai Definisi 2.1 $ap - aq = tm$ untuk suatu $t \in \mathbb{Z}$, berarti $a(p - q) = tm$. Karena $(a, m) | a$ dan $(a, m) | m$ maka $(a / (a, m))(p - q) = (m / (a, m))t$, dan sesuai dengan Definisi 2.1, dapat ditentukan bahwa $(m / (a, m)) | (a / (a, m))(p - q)$.

Menurut Teorema 2.14, $(m / (a, m), a / (a, m)) = 1$, dan menurut Teorema 2.15, dari $(m / (a, m), a / (a, m)) = 1$ dan $(m / (a, m)) | (a / (a, m))(p - q)$ berakibat $(m / (a, m)) | (p - q)$.

Jadi menurut Definisi 3.1, $p \equiv q \pmod{m / (a, m)}$.

(\leftarrow)

Misalkan $p \equiv q \pmod{m / (a, m)}$, maka menurut Teorema 3.5(a), $ap \equiv aq \pmod{am / (a, m)}$. Selanjutnya, karena $m | (am / (a, m))$ dan $ap \equiv aq \pmod{am / (a, m)}$, maka berdasarkan pada Teorema 3.5 (b), $ap \equiv aq \pmod{m}$.

(b) Buktikan !

Contoh 3.7

Misalkan $8p \equiv 8q \pmod{6}$, karena $(8, 6) = 2$, maka $p \equiv q \pmod{6/2}$ sehingga $p \equiv q \pmod{3}$

Misalkan $12p \equiv 12q \pmod{16}$, karena $(12, 16) = 4$, maka $p \equiv q \pmod{16/4}$, sehingga $p \equiv q \pmod{4}$

Contoh 3.8

Misalkan $p \equiv q \pmod{6}$ dan $p \equiv q \pmod{8}$. Maka $p \equiv q \pmod{[6, 8]}$, sehingga $p \equiv q \pmod{24}$

Misalkan $p \equiv q \pmod{16}$ dan $p \equiv q \pmod{24}$. Maka $p \equiv q \pmod{[16, 24]}$, sehingga $p \equiv q \pmod{48}$.

Tugas

Bacalah suatu buku teori bilangan, dan carilah teorema-teorema yang belum dibuktikan dalam Kegiatan Belajar 1. Selanjutnya buktikan bahwa:

- 1) Jika p, q, t , dan m adalah bilangan-bilangan bulat sedemikian hingga $t > 0, m > 0$ dan $p \equiv q \pmod{m}$, maka $p^t \equiv q^t \pmod{m}$.
- 2) Jika $p, q \in \mathbb{Z}$ dan $m_1, m_2, \dots, m_t \in \mathbb{Z}^+$ sedemikian hingga $p \equiv q \pmod{m_1}, p \equiv q \pmod{m_2}, \dots$, dan $p \equiv q \pmod{m_t}$, maka $p \equiv q \pmod{[m_1, m_2, \dots, m_t]}$

Petunjuk Jawaban Tugas

- 1) Misalkan $p \equiv q \pmod{m}$, maka $m | p - q$.

$$p^t - q^t = (p - q)(p^{t-1} + p^{t-2}q + \dots + pq^{t-2} + q^{t-1}).$$

Perhatikan bahwa $(p - q) | p^t - q^t$.

Karena $m | p - q$ dan $(p - q) | p^t - q^t$, maka $m | p^t - q^t$.

Jadi $p^t \equiv q^t \pmod{m}$.

- 2) Misalkan $p \equiv q \pmod{m_1}, p \equiv q \pmod{m_2}, \dots$, dan $p \equiv q \pmod{m_t}$, maka $m_1 | p - q, m_2 | p - q, \dots, m_t | p - q$.

Dengan demikian $p - q$ adalah kelipatan persekutuan dari m_1, m_2, \dots, m_t , dan berdasarkan Teorema 2.22, $[m_1, m_2, \dots, m_t] | p - q$.

Jadi $p \equiv q \pmod{[m_1, m_2, \dots, m_t]}$.



Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Diketahui p, q, m adalah bilangan-bilangan bulat dan $m > 0$ sedemikian hingga $p \equiv q \pmod{m}$. Buktikan: $(p, m) = (q, m)$.
- 2) Buktikan
 - (a) jika p adalah suatu bilangan genap, maka $p^2 \equiv 0 \pmod{4}$
 - (b) jika p adalah suatu bilangan ganjil, maka $p^2 \equiv 1 \pmod{4}$
- 3) Buktikan jika p adalah suatu bilangan ganjil, maka $p^2 \equiv 1 \pmod{8}$
- 4) Carilah sisa positif terkecil dari $1! + 2! + \dots + 100!$
 - (a) modulo 2
 - (b) modulo 12
- 5) Tunjukkan bahwa jika n adalah suatu bilangan genap positif, maka:

$$1 + 2 + 3 + \dots + (n + 1) \equiv 0 \pmod{n}$$
 Bagaimana jika n adalah suatu bilangan ganjil positif?
- 6) Dengan menggunakan induksi matematika, tunjukkan bahwa $4^n \equiv 1 + 3n \pmod{9}$ jika n adalah suatu bilangan bulat positif.

Petunjuk Jawaban Latihan

- 1) Misalkan $p \equiv q \pmod{m}$, maka $p - q = tm$ untuk suatu bilangan bulat t . Menurut Definisi 2.3, $(p, m) | p$ dan $(p, m) | m$. Dari $(p, m) | m$, berdasarkan Teorema 2.1, $(p, m) | tm$. Selanjutnya, dari $(p, m) | p$ dan $(p, m) | tm$, berdasarkan Teorema 2.4, $(p, m) | p - tm$. Karena $p - q = tm$, atau $q = p - tm$, maka $(p, m) | q$. Karena $(p, m) | m$ dan $(p, m) | q$, maka (p, m) merupakan faktor persekutuan dari m dan q , dan sesuai Teorema 2.17, $(p, m) | (q, m)$. Dengan jalan yang sama dapat ditunjukkan bahwa $(q, m) | (p, m)$. Dari $(p, m) | (q, m)$ dan $(q, m) | (p, m)$, $(p, m) > 0$, dan $(q, m) > 0$, sesuai Teorema 2.7, dapat disimpulkan $(p, m) = (q, m)$.

- 2) (a) Sesuai Definisi 2.2, jika p merupakan suatu bilangan genap, maka p dapat dinyatakan sebagai $p = 2t$ untuk suatu bilangan bulat t , dengan demikian $p^2 = 4t^2$. Akibatnya, sesuai Definisi 2.1, $4 \mid p^2$, atau $4 \mid p^2 - 0$, dan berdasarkan definisi 3.1, $p^2 \equiv 0 \pmod{4}$.
- (b) Sesuai Definisi 2.2, jika p merupakan suatu bilangan ganjil, maka p dapat dinyatakan sebagai $p = 2t + 1$ untuk suatu bilangan bulat t , dengan demikian dapat dicari $p^2 = 4t^2 + 4t + 1$, atau $p^2 = 4t(t+1) + 1$, atau $p^2 - 1 = 4t(t+1)$. Akibatnya, sesuai Definisi 2.1, $4 \mid p^2 - 1$, dan berdasarkan Definisi 3.1, $p^2 \equiv 1 \pmod{4}$.
- 3) Sesuai Definisi 2.2, jika p merupakan suatu bilangan ganjil, maka p dapat dinyatakan sebagai $p = 2t + 1$ untuk suatu bilangan bulat t . Dengan demikian $p^2 = 4t^2 + 4t + 1$, atau $p^2 = 4t(t+1) + 1$. Jika t adalah suatu bilangan genap, sesuai Definisi 2.2, $t = 2r$ untuk suatu bilangan bulat r , sehingga $p^2 = 8r(2r+1) + 1$, atau $p^2 - 1 = 8r(2r+1)$. Akibatnya, sesuai Definisi 2.1, $8 \mid p^2 - 1$, dan berdasarkan pada Definisi 3.1, $p^2 \equiv 1 \pmod{8}$.
- Kerjakan dengan jalan yang sama jika t adalah suatu bilangan ganjil.
- 4) (a) $n! = 1.2.3\dots n$, berarti $2! = 1.2 = 2 \equiv 0 \pmod{2}$,
- $$3! = 1.2.3 = 2.3 \equiv 0 \pmod{2}, \quad n! = 1.2.3\dots n = 2.1.3\dots n \equiv 0 \pmod{2}.$$
- Dengan demikian dapat dicari bahwa
- $$1! + 2! + \dots + n! \equiv 1 + 0 \pmod{2} + 0 \pmod{2} + \dots + 0 \pmod{2} \equiv 0 \pmod{2}.$$
- (b) $n! = 1.2.3.4\dots n \equiv 0 \pmod{12}$ jika $n \geq 4$,
- akibatnya dapat ditunjukkan bahwa
- $$1! + 2! + \dots + 100! \equiv 1! + 2! + 3! + 0 + 0 + \dots + 0 \pmod{12} \equiv 9 \pmod{12}.$$
- 5) $1 + 2 + \dots + (n+1) = (n-1)n/2$.

Jika n adalah suatu bilangan ganjil, maka $n - 1$ adalah suatu bilangan genap, sehingga $(n-1)/2$ adalah suatu bilangan bulat, dengan demikian $n \mid (1 + 2 + \dots + (n+1))$ atau $1 + 2 + \dots + (n+1) \equiv 0 \pmod{n}$.

Jika n adalah suatu bilangan genap, maka $n = 2r$ untuk suatu bilangan bulat r , dengan demikian $(n-1)n/2 = (n-1)r$, berarti n tidak membagi

$(n-1)r$ karena $(n, n-1) = 1$ dan $r < n$. Jadi $1+2+\dots+(n+1)$ tidak kongruen dengan 0 modulo n jika n adalah suatu bilangan genap.

- 6) Untuk $n = 1$ memenuhi hubungan karena $4^1 = 4 = 1 + 3 \cdot 1 \dots 1 + 3 \cdot 1 \pmod{9}$.
 Anggaplah bahwa $4^n \equiv 1 + 3(n+1) \pmod{9}$, harus dibuktikan
 $4^{n+1} \equiv 1 + 3(n+1+1) \pmod{9}$
 $4^{n+1} = 4 \cdot 4^n \equiv 4(1 + 3n) \pmod{9} \equiv 4 + 12n \pmod{9} \equiv 4 + 3n \pmod{9}$.



RANGKUMAN

Dari materi Kegiatan Belajar 1 ini, beberapa bagian yang perlu diperhatikan adalah definisi kongruensi, teorema-teorema kongruensi, dan keterkaitan konsep kongruensi dengan keterbagian, FPB, dan KPK.

1. **Definisi 3.1 :** $p \equiv q \pmod{m}$ jika dan hanya jika $m \mid p - q$
2. Terdapat 6 Teorema kongruensi.

Teorema 3.1 : $p \equiv q \pmod{m}$ jika dan hanya jika $p = q + tm$

Teorema 3.2 : Kongruensi modulo m memenuhi sifat-sifat

- (a) refleksif: $p \equiv p \pmod{m}$
- (b) simetris: jika $p \equiv q \pmod{m}$, maka

$$q \equiv p \pmod{m}$$
- (c) transitif: jika $p \equiv q \pmod{m}$, $q \equiv r \pmod{m}$,
 maka $p \equiv r \pmod{m}$

Teorema 3.3 : Jika $p \equiv q \pmod{m}$, maka:

- (a) $p + r \equiv q + r \pmod{m}$
- (b) $p - r \equiv q - r \pmod{m}$
- (c) $pr \equiv qr \pmod{m}$

Teorema 3.4 : Jika $p \equiv q \pmod{m}$ dan $r \equiv s \pmod{m}$, maka:

- (a) $p + r \equiv q + s \pmod{m}$
- (b) $p - r \equiv q - s \pmod{m}$
- (c) $pr \equiv qs \pmod{m}$

Teorema 3.5 : (a) jika $p \equiv q \pmod{m}$, maka $pr \equiv qr \pmod{mr}$

(b) jika $p \equiv q \pmod{m}$ dan $d | m$, maka

$$p \equiv q \pmod{d}$$

Teorema 3.6 : (a) $ap \equiv aq \pmod{m}$ jika dan hanya jika

$$p \equiv q \pmod{m/(a,m)}$$

(b) $p \equiv q \pmod{m_1}$ dan $p \equiv q \pmod{m_2}$ jika

dan hanya jika $p \equiv q \pmod{[m_1, m_2]}$



TES FORMATIF 1

1) Skor 10

Nyatakan dengan B (Benar) atau S (Salah)

(a) Jika $p \equiv q \pmod{7}$, maka $3p \equiv 3q \pmod{7}$

(b) Jika $2p \equiv 3q \pmod{5}$, maka $10p \equiv 10q \pmod{25}$

(c) Jika $p \equiv q \pmod{11}$, maka $23p - 44 \equiv 12q + 22 \pmod{11}$

(d) Jika $2p \equiv 2q \pmod{5}$, maka $p \equiv q \pmod{5}$

(e) Jika $4p \equiv 4q \pmod{6}$, maka $p \equiv q \pmod{6}$

(f) Jika $6p \equiv 9q \pmod{15}$, maka $2p \equiv 3q \pmod{5}$

(g) Jika $p \equiv 2q \pmod{24}$, maka $p \equiv 2q \pmod{8}$

(h) Jika $p \equiv q \pmod{7}$, maka $14p^2 + 8p - 21 \equiv 15p + 28 \pmod{7}$

(i) Jika $p \equiv q \pmod{8}$ dan $p \equiv q \pmod{12}$, maka $p \equiv q \pmod{96}$

(j) Jika $p \equiv q \pmod{24}$ dan $p \equiv q \pmod{36}$, maka $p \equiv q \pmod{72}$

2) Skor 10

(a) Carilah 2 angka terakhir dari lambang bilangan desimal dari 28^{75}

(b) Carilah 3 angka terakhir dari lambang bilangan desimal dari 23^{95}

3) Skor 20.

Tunjukkan bahwa $1^3 + 2^3 + \dots + (n-1)^3 \equiv 0 \pmod{n}$ jika n adalah suatu bilangan bulat positif atau jika n adalah habis dibagi 4.

Apakah pernyataan masih benar jika n adalah genap tetapi tidak habis dibagi 4 ?

4) Skor 20

Buktikan dengan induksi matematika bahwa $5^n \equiv 1 + 4n \pmod{16}$ jika n adalah suatu bilangan bulat positif.

5) Skor 20

Carilah sisa positif terkecil dari $1! + 2! + \dots + 100!$

- (a) modulo 7
- (b) modulo 25

6) Skor 20

Carilah sisa positif terkecil dari:

- (a) $6!$ modulo 7
- (b) $12!$ modulo 13
- (c) $18!$ modulo 19
- (d) $22!$ modulo 23

Cobalah menebak suatu teorema dari hasil-hasil jawaban Anda!

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: $90 - 100\% = \text{baik sekali}$

$80 - 89\% = \text{baik}$

$70 - 79\% = \text{cukup}$

$< 70\% = \text{kurang}$

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Sistem Residu**

Sistem residu merupakan topik yang memberikan dasar untuk mengembangkan pembahasan menuju Teorema Euler, dan pada bagian lain terkait dengan fungsi-fungsi khas (*special functions*) dalam teori bilangan.

Bagian-bagian dari sistem residu meliputi sistem residu yang lengkap dan sistem residu yang tereduksi. Sebagai suatu sistem, sistem residu mempunyai sifat-sifat khusus yang terkait dengan bagaimana membuat sistem residu, atau mencari contoh yang memenuhi syarat tertentu.

Definisi 3.2

Suatu himpunan $\{x_1, x_2, \dots, x_m\}$ disebut suatu sistem residu lengkap modulo m jika dan hanya jika untuk setiap y dengan $0 \leq y < m$, ada satu dan hanya satu x_i dengan $1 \leq i < m$, sedemikian hingga $y \equiv x_i \pmod{m}$ atau $x_i \equiv y \pmod{m}$.

Perhatikan bahwa indeks dari x yang terakhir adalah m , dan hal ini menunjukkan bahwa banyaknya unsur dalam suatu sistem residu lengkap modulo m adalah m . Dengan demikian, jika ada suatu himpunan yang banyaknya unsur kurang dari m atau lebih dari m , maka himpunan itu tentu bukan merupakan suatu sistem residu lengkap modulo m .

Selanjutnya, karena pasangan-pasangan kongruensi antara y dan x_i adalah tunggal, maka tidak ada y yang kongruen dengan dua unsur x yang berbeda, misalnya x_i dan x_j , dan tidak ada x_i yang kongruen dengan dua nilai y . Dengan demikian, tidak ada dua unsur x yang berbeda dan kongruen, artinya x_i tidak kongruen x_j modulo m jika $i \neq j$.

Contoh 3.9

1. Himpunan $A = \{6, 7, 8, 9\}$ bukan merupakan sistem residu lengkap modulo 5 sebab banyaknya unsur A kurang dari 5.

2. Himpunan $A = \{6, 7, 8, 9, 10\}$ adalah suatu sistem residi lengkap modulo 5 sebab untuk setiap y dengan $0 \leq y < 5$, ada satu dan hanya satu x_i dengan $1 \leq i < 5$ sedemikian hingga $y \equiv x_i \pmod{5}$ atau $x_i \equiv y \pmod{5}$. Nilai-nilai y yang memenuhi $0 \leq y < 5$, adalah $y = 0, y = 1, y = 2, y = 3$, dan $y = 4$. Jika kita selidiki, maka kita peroleh bahwa:

$$10 \equiv 0 \pmod{5} \quad 8 \equiv 3 \pmod{5} \quad 6 \equiv 1 \pmod{5}$$

$$9 \equiv 4 \pmod{5} \quad 7 \equiv 2 \pmod{5}$$

Dengan demikian untuk setiap y dengan $y = 0, 1, 2, 3, 4$, ada satu dan hanya satu x_i dengan $x_i = 6, 7, 8, 9, 10$, sedemikian hingga $x_i \equiv y \pmod{5}$. Jadi A adalah suatu sistem residi lengkap modulo 5.

3. Himpunan $B = \{4, 25, 82, 107\}$ adalah suatu sistem residi lengkap modulo 4 sebab untuk setiap y dengan $0 \leq y < 4$, ada satu dan hanya satu x_i dengan $1 \leq i < 4$ sedemikian hingga $y \equiv x_i \pmod{4}$ atau $x_i \equiv y \pmod{4}$.

$$4 \equiv 0 \pmod{4} \quad 82 \equiv 2 \pmod{4}$$

$$25 \equiv 1 \pmod{4} \quad 107 \equiv 3 \pmod{4}$$

4. Himpunan $C = \{-33, -13, 14, 59, 32, 48, 12\}$ adalah suatu sistem residi lengkap modulo 7 sebab untuk setiap y dengan $0 \leq y < 7$, ada satu dan hanya satu x_i dengan $1 \leq i < 7$ sedemikian hingga $y \equiv x_i \pmod{7}$ atau $x_i \equiv y \pmod{7}$.

$$-33 \equiv 2 \pmod{7} \quad 59 \equiv 3 \pmod{7} \quad 48 \equiv 6 \pmod{7}$$

$$-13 \equiv 1 \pmod{7} \quad 32 \equiv 4 \pmod{7} \quad 12 \equiv 5 \pmod{7}$$

$$14 \equiv 0 \pmod{7}$$

5. Himpunan $D = \{10, -5, 27\}$ adalah bukan suatu sistem residi lengkap modulo 3 sebab untuk suatu $y = 1$ dengan $0 \leq y < 3$, ada lebih dari satu x_i (yaitu 10 dan -5) sehingga

$$10 \equiv 1 \pmod{3} \quad -5 \equiv 1 \pmod{3}$$

6. Algoritma pembagian menunjukkan bahwa himpunan bilangan bulat $0, 1, \dots, m-1$ merupakan suatu sistem residi lengkap modulo m , dan disebut sebagai residi nonnegatif terkecil modulo m .

Definisi 3.3

Suatu himpunan bilangan bulat $\{x_1, x_2, \dots, x_k\}$ disebut suatu sistem residu tereduksi modulo m jika dan hanya jika:

- $(x_i, m) = 1, 1 \leq i < k$
- $x_i \equiv x_j \pmod{m}$ untuk setiap $i \neq j$
- Jika $(y, m) = 1$, maka $y \equiv x_i \pmod{m}$ untuk suatu $i = 1, 2, \dots, k$

Contoh 3.10

- Himpunan $\{1, 5\}$ adalah suatu sistem residu tereduksi modulo 6 sebab:
 - $(1, 6) = 1$ dan $(5, 6) = 1$
 - $5 \equiv 1 \pmod{6}$
- Himpunan $\{17, 91\}$ adalah suatu sistem residu tereduksi modulo 6 sebab:
 - $(17, 6) = 1$ dan $(91, 6) = 1$
 - $91 \equiv 17 \pmod{6}$

Suatu sistem residu tereduksi modulo m dapat diperoleh dari sistem residu lengkap modulo m dengan membuang unsur-unsur yang tidak prima relatif dengan m . Hal ini dapat dilakukan karena $\{0, 1, 2, \dots, m-1\}$ adalah suatu sistem residu yang lengkap modulo m . Perhatikan bahwa untuk setiap y dengan $y = 0, 1, 2, \dots, m-1$, ada satu dan hanya satu $x_i = 0, 1, 2, \dots, m-1$ sehingga $y \equiv x_i \pmod{m}$. Keadaan $y \equiv x_i \pmod{m}$ selalu dapat terjadi dengan memilih $y = 0$ dan $x_1 = 0$, $y = 1$ dan $x_2 = 1, \dots, y = m-1$ dan $x_m = m-1$.

Karena unsur-unsur $\{0, 1, 2, \dots, m-1\}$ memenuhi tidak ada sepasang yang kongruen, maka setelah unsur-unsur yang tidak prima relatif dengan m dibuang, yang tertinggal adalah unsur-unsur yang prima relatif dengan m dan tidak ada sepasang yang kongruen. Dengan demikian unsur-unsur yang tertinggal memenuhi Definisi 3.2.

Contoh 3.11

- Himpunan $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ adalah suatu sistem residu lengkap modulo 8. Unsur-unsur A yang tidak prima relatif dengan 8 adalah 0, 2, 4, dan 6 karena $(0, 8) = 8 \neq 1$, $(2, 8) = 2 \neq 1$, $(4, 8) = 4 \neq 1$, dan

$(6,8) = 2 \neq 1$. Misalkan B adalah himpunan dari unsur-unsur yang tertinggal, maka $B = \{1, 3, 5, 7\}$, dan B merupakan suatu sistem residu tereduksi modulo 8 karena memenuhi Definisi 3.2.

2. Himpunan $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$ adalah suatu sistem residu lengkap modulo 20. Jika unsur-unsur A yang tidak prima relatif dengan 20 dibuang, yaitu 0, 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, dan 18, maka unsur-unsur yang tertinggal adalah 1, 3, 7, 9, 11, 13, 17, dan 19, dan $B = \{1, 3, 7, 9, 11, 13, 17, 19\}$ merupakan suatu sistem residu tereduksi modulo 20.

Defini 3.4

Misalkan m adalah suatu bilangan bulat positif. Banyaknya residu di dalam suatu sistem residu tereduksi modulo m disebut fungsi ϕ -Euler dari m , dan dinyatakan dengan $\phi(m)$.

Contoh 3.12

$\phi(2) = 1$, diperoleh dari unsur 1

$\phi(3) = 2$, diperoleh dari unsur-unsur 1 dan 2

$\phi(4) = 2$, diperoleh dari unsur-unsur 1 dan 3

$\phi(5) = 4$, diperoleh dari unsur-unsur 1, 2, 3, dan 4

$\phi(16) = 8$, diperoleh dari unsur-unsur 1, 3, 5, 7, 9, 11, 13, dan 15

$\phi(27) = 18$, diperoleh dari unsur-unsur 1, 2, 4, 5, 7, 8, 11, 13, 14, 16, 17,

19, 20, 22, 23, 25, dan 26

$\phi(p) = p - 1$ jika p adalah suatu bilangan prima

Perhatikan bahwa himpunan $\{1, 2, 3, 4\}$ merupakan suatu sistem residu tereduksi modulo 5. Sekarang, coba Anda selidiki, jika masing-masing unsur himpunan dikalikan dengan suatu bilangan yang prima relatif dengan 5, misalnya 2, 3, atau 4, sehingga diperoleh himpunan yang lain, maka apakah himpunan-himpunan yang lain tersebut merupakan sistem-sistem residu yang tereduksi modulo 5?

Teorema 3.7

Ditentukan $(a,m) = 1$.

Jika $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residi modulo m yang lengkap atau tereduksi, maka $\{ax_1, ax_2, \dots, ax_k\}$ juga merupakan suatu sistem residi modulo m yang lengkap atau tereduksi.

Bukti:

Ditentukan bahwa $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residi modulo m yang lengkap, maka x_i tidak kongruen x_j modulo m jika $x_i \neq x_j$. Harus dibuktikan bahwa ax_i tidak kongruen ax_j modulo m jika $i \neq j$.

Misalkan dari unsur-unsur $\{ax_1, ax_2, \dots, ax_k\}$ terdapat $i \neq j$ sehingga berlaku hubungan $ax_i \equiv ax_j \pmod{m}$. Karena $(a,m)=1$ dan $ax_i \equiv ax_j \pmod{m}$, maka menurut Teorema 3.6 (a), dapat ditunjukkan bahwa $x_i \equiv x_j \pmod{m}$, bertentangan dengan ketentuan $\{x_1, x_2, \dots, x_k\}$ merupakan suatu sistem residi lengkap modulo m . Jadi tentu ax_i tidak kongruen ax_j modulo m .

Selanjutnya buktikan jika $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residi modulo m yang tereduksi.

Contoh 3.13

(a) Himpunan $A = \{0, 1, 2, 3, 4, 5\}$ adalah merupakan suatu sistem residi lengkap modulo 6. Jika masing-masing unsur A dikalikan dengan 5, yang mana $(5,6) = 1$, dan setelah dikalikan dimasukkan sebagai unsur himpunan B , maka dapat ditunjukkan bahwa $B = \{0, 5, 10, 15, 20, 25\}$.

Himpunan B merupakan suatu sistem residi yang lengkap modulo 6 sebab setiap unsur B kongruen dengan satu dan hanya satu $y \in \{0, 1, 2, 3, 4, 5\}$, yaitu:

$$\begin{array}{lll} 0 \equiv 0 \pmod{6} & 10 \equiv 4 \pmod{6} & 20 \equiv 2 \pmod{6} \\ 5 \equiv 5 \pmod{6} & 15 \equiv 3 \pmod{6} & 25 \equiv 1 \pmod{6} \end{array}$$

(b) Himpunan $A = \{1, 5, 7, 11\}$ adalah merupakan suatu sistem residi tereduksi modulo 12. Jika masing-masing unsur A dikalikan dengan 17

dengan $(17,12)=1$, dan setelah dikalikan dimasukkan sebagai unsur himpunan B , maka dapat ditunjukkan bahwa $B = \{17, 85, 119, 187\}$. Himpunan B merupakan suatu sistem residu tereduksi modulo 12 sebab setiap unsur B relatif prima dengan 12, dan tidak ada sepasang unsur B yang kongruen, yaitu :

$$(17,12) = (85,12) = (119,12) = (187,12) = 1$$

$$17 \equiv 85 \pmod{12} \quad 17 \equiv 119 \pmod{12} \quad 17 \equiv 187 \pmod{12}$$

$$85 \equiv 119 \pmod{12} \quad 85 \equiv 187 \pmod{12} \quad 119 \equiv 187 \pmod{12}$$

Teorema 3.8 (Teorema Euler)

Jika $a, m \in \mathbb{Z}$ dan $m > 0$ sehingga $(a,m) = 1$, maka $a^{\phi(m)} \equiv 1 \pmod{m}$

Bukti:

Misalkan bahwa $\{x_1, x_2, \dots, x_{\phi(m)}\}$ adalah suatu sistem residu tereduksi modulo m dengan unsur-unsur bilangan bulat positif kurang dari m dan prima relatif dengan m , maka menurut Teorema 3.7, karena $(a,m) = 1$, maka $\{ax_1, ax_2, \dots, ax_{\phi(m)}\}$ juga merupakan suatu sistem residu tereduksi modulo m . Dengan demikian, residu-residu positif terkecil dari $ax_1, ax_2, \dots, ax_{\phi(m)}$ adalah bilangan-bilangan bulat yang terdapat pada $\{x_1, x_2, \dots, x_{\phi(m)}\}$ dengan urutan tertentu. Akibatnya kita dapat mengalikan semua suku dari masing-masing sistem residu tereduksi, sehingga diperoleh:

$$ax_1 \cdot ax_2 \cdot \dots \cdot ax_{\phi(m)} = x_1 \cdot x_2 \cdot \dots \cdot x_{\phi(m)} \pmod{m}$$

Dengan demikian dapat ditunjukkan bahwa :

$$a^{\phi(m)} x_1 \cdot x_2 \cdot \dots \cdot x_{\phi(m)} \equiv x_1 \cdot x_2 \cdot \dots \cdot x_{\phi(m)} \pmod{m}$$

Selanjutnya, $\{x_1, x_2, \dots, x_{\phi(m)}\}$ adalah suatu sistem residu tereduksi modulo m , maka menurut Definisi 3.3, berlaku $(x_i, m) = 1$.

Berdasarkan Teorema 2.16, karena $(x_i, m) = 1$, untuk semua i , yaitu $(x_1, m) = (x_2, m) = \dots = (x_{\phi(m)}, m) = 1$, maka dapat ditentukan bahwa $(x_1 \cdot x_2 \cdot \dots \cdot x_{\phi(m)}, m) = 1$.

Dari dua keadaan:

$$a^{\phi(m)} x_1 \cdot x_2 \dots x_{\phi(m)} \equiv x_1 \cdot x_2 \dots x_{\phi(m)} \pmod{m} \text{ dan } \left(x_1 \cdot x_2 \dots x_{\phi(m)}, m \right) = 1,$$

dapat ditunjukkan berdasarkan Teorema 3.6 (a) bahwa $a^{\phi(m)} \equiv 1 \pmod{m}$.

Kita dapat menggunakan Teorema Euler untuk mencari inversi modulo m .

Jika a dan m adalah prima relatif, maka dapat ditunjukkan bahwa

$$a^{\phi(m)} \equiv 1 \pmod{m}. \text{ Dengan demikian } a^{\phi(m)} = a. a^{\phi(m)-1} \equiv 1 \pmod{m}.$$

Jadi $a^{\phi(m)-1}$ adalah inversi dari a modulo m .

Contoh 3.14

Carilah dua digit terakhir lambang bilangan desimal dari 23^{500} .

Soal ini dapat dijawab dengan menyatakan maknanya dalam bentuk lain, yaitu sama dengan mencari x jika $23^{500} \equiv x \pmod{100}$. Kemudian bentuk $23^{500} \equiv x \pmod{100}$ dapat dipecah menjadi $23^{500} \equiv x \pmod{4}$ dan $23^{500} \equiv x \pmod{25}$.

(a) mencari x dari $23^{500} \equiv x \pmod{4}$.

$$23 \equiv 3 \pmod{4}. \quad \text{Maka} \quad 23^2 \equiv 9 \pmod{4} \equiv 1 \pmod{4}, \quad \text{sehingga} \\ 23^{500} = (23^2)^{250}.$$

$$\text{Dengan demikian } 23^{500} = (23^2)^{250} \equiv 1^{250} \pmod{4}, \text{ atau } x \equiv 1 \pmod{4}.$$

(b) mencari x dari $23^{500} \equiv x \pmod{25}$.

$$23 \equiv -2 \pmod{25}. \text{ Maka } 23^2 \equiv 4 \pmod{25}, 23^4 \equiv 16 \pmod{25},$$

$$23^8 \equiv 6 \pmod{25}, 23^{16} \equiv 11 \pmod{25}, 23^{32} \equiv -4 \pmod{25},$$

$$23^{64} \equiv 16 \pmod{25}, 23^{128} \equiv 6 \pmod{25}, \text{ dan } 23^{256} \equiv 11 \pmod{25}$$

Dengan demikian

$$23^{500} = 23^{256} \cdot 23^{128} \cdot 23^{64} \cdot 23^{32} \cdot 23^{16} \cdot 23^4 \equiv 11 \cdot 6 \cdot 16 \cdot (-4) \cdot 11 \cdot 16 \pmod{25}$$

$$\equiv (-4) \cdot 6 \cdot (-4) \cdot 6 \pmod{25} \equiv 576 \pmod{25} \equiv 1 \pmod{25}, \text{ yaitu}$$

$$x \equiv 1 \pmod{25}$$

Dari hasil (a) dan (b), yaitu $x \equiv 1 \pmod{4}$ dan $x \equiv 1 \pmod{25}$ maka berdasarkan pada Teorema 3.6 (b), $x \equiv 1 \pmod{[4, 25]}$, $x \equiv 1 \pmod{100}$

Jadi $23^{500} \equiv 1 \pmod{100}$, berarti dua digit terakhir lambang bilangan desimal dari 23^{500} adalah 0 dan 1.

Contoh 3.15

Tunjukkan jika $(n, 7) = 1$, $n \in N$, maka $7 \mid n^7 - n$

Jawab: Karena $(n, 7) = 1$, maka menurut Teorema Euler, $n^{\phi(7)} \equiv 1 \pmod{7}$.

Selanjutnya $\phi(7) = 6$, sehingga diperoleh $n^6 \equiv 1 \pmod{7}$, dan sesuai dengan Definisi 3.1, $7 \mid n^6 - 1$, dan akibatnya, sesuai dengan Teorema 2.1, $7 \mid n(n^6 - 1)$ atau $7 \mid n^7 - n$.

Contoh 3.16

Jika bulan ini adalah bulan Mei, maka carilah nama bulan setelah 239^{43} bulan lagi.

Jawab:

Permasalahan ini dapat diganti dengan mencari x jika $239^{43} \equiv x \pmod{12}$.

Karena $(239, 12) = 1$, maka menurut Teorema Euler, $239^{\phi(12)} \equiv 1 \pmod{12}$.

Selanjutnya $\phi(12) = 4$, sehingga diperoleh $239^4 \equiv 1 \pmod{12}$.

$$239^{43} = (239^4)^{10} \cdot 239^3 \equiv 1 \cdot 239^3 \pmod{12} \equiv (-1)(-1)(-1)(\pmod{12}) \equiv 11 \pmod{12}$$

Jadi $x = 11$, dengan demikian 239^{43} bulan lagi adalah bulan April.

Contoh 3.16

Kongruensi linier $ax \equiv b \pmod{m}$ dapat diselesaikan dengan menggunakan Teorema Euler sebagai berikut:

$$ax \equiv b \pmod{m}$$

$$a^{\phi(m)-1} \cdot ax \equiv a^{\phi(m)-1} \cdot b \pmod{m}$$

$$x \equiv a^{\phi(m)-1} \cdot b \pmod{m}$$

Jawab:

$7x \equiv 3 \pmod{12}$ adalah $x \equiv 7^{\phi(12)-1} \cdot 3 \pmod{12} \equiv 7^{4-1} \cdot 3 \pmod{12} \equiv 7^3 \cdot 3 \pmod{12} \equiv 21 \pmod{12} \equiv 9 \pmod{12}$.

Teorema 3.9. Teorema Kecil Fermat

Jika p adalah suatu bilangan prima dan p tidak membagi a , maka $a^{p-1} \equiv 1 \pmod{p}$.

Bukti:

Karena p adalah suatu bilangan prima dan p tidak membagi a , maka $(p,a)=1$ (jika $(p,a) \neq 1$ yaitu p dan a tidak prima relatif, maka p dan a mempunyai faktor selain 1 dan p , bertentangan dengan sifat p sebagai bilangan prima).

Selanjutnya, karena $(p,a)=1$, maka menurut Teorema 3.8, $a^{\phi(p)} \equiv 1 \pmod{p}$, p adalah suatu bilangan prima, berarti dari bilangan-bilangan bulat $0, 1, 2, 3, \dots, p-1$ yang tidak prima relatif dengan p hanya $0 \equiv p \pmod{p}$, sehingga $\{1, 2, 3, \dots, p-1\}$ merupakan sistem residu tereduksi modulo dengan $(p-1)$ unsur, dengan demikian $\phi(p) = p-1$.

Karena $\phi(p) = p-1$ dan $a^{\phi(p)} \equiv 1 \pmod{p}$, maka $a^{\phi(p)} \equiv 1 \pmod{p}$.

Contoh 3.17

Carilah suatu x jika $22^{50} \equiv x \pmod{7}$ dan $0 \leq x < 7$.

Jawab:

Karena 7 adalah bilangan prima, $(2,7) = 1$, dan $\phi(7) = 7 - 1 = 6$, maka:

$$2^{\phi(7)} \equiv 1 \pmod{7}$$

$$2^6 \equiv 1 \pmod{7}$$

$$2^{250} = (2^6)^{41} \cdot 2^4 \equiv 1 \cdot 2^4 \pmod{7} \equiv 16 \pmod{7} \equiv 2 \pmod{7}$$

Jadi $x = 2$.

Contoh 3.18

Carilah satu digit terakhir lambang bilangan basis 10 dari:

(a) 2^{500}

(b) 7^{175}

Jawab:

Untuk mencari digit terakhir dari lambang bilangan basis 10, permasalahan dapat dipandang sebagai mencari x jika $y \equiv x \pmod{10}$. Karena $2 \cdot 5 = 10$ dan $(2,5) = 1$, maka $y \equiv x \pmod{10}$ dapat dinyatakan sebagai: $y \equiv x \pmod{2}$ dan $y \equiv x \pmod{5}$.

- (a) Karena $2 \equiv 0 \pmod{2}$, maka $2^{500} \equiv 0, 2, 4, 6, 8, \dots \pmod{2}$

$$\phi(5) = 4 \text{ dan } (2,5) = 1, \text{ maka } 2^4 \equiv 1 \pmod{5}, \text{ sehingga}$$

$$2^{500} = (2^4)^{125} \cdot 1 \pmod{5} \equiv 1, 6, 11, 16, 21, \dots \pmod{5}$$

Dengan demikian $2^{500} \equiv 6 \pmod{2}$ dan $2^{500} \equiv 6 \pmod{5}$, berarti

$2^{500} \equiv 6 \pmod{10}$. Satu digit terakhir lambang bilangan basis 10 dari 2^{500} adalah 6.

- (b) Karena $7 \equiv 1 \pmod{2}$, maka $7^{175} \equiv 1, 3, 5, \dots \pmod{2}$

$$\phi(5) = 4 \text{ dan } (7,5) = 1, \text{ maka } 7^4 \equiv 1 \pmod{5}, \text{ sehingga}$$

$$7^{175} = (7^4)^{43} \cdot 7^3 \equiv 7^3 \pmod{5} \equiv 2 \cdot 2 \cdot 2 \pmod{5} \equiv 8 \pmod{5} \equiv 3 \pmod{5} \\ \equiv 3, 8, 13, 18, \dots \pmod{5}.$$

Dengan demikian $7^{175} \equiv 3 \pmod{2}$ dan $7^{175} \equiv 3 \pmod{5}$, berarti

$7^{175} \equiv 3 \pmod{10}$. Satu digit terakhir lambang bilangan basis 10 dari 7^{175} adalah 3.

Teorema 3.10

Jika $(a, m) = 1$, maka hubungan $ax \equiv b \pmod{m}$ mempunyai selesaian
 $x = a^{\phi(m)-1} \cdot b + tm$.

Bukti:

Dari hubungan $ax \equiv b \pmod{m}$, ruas kiri dan kanan perlu dikalikan dengan suatu faktor sehingga koefisien a menjadi 1. Pilihan faktor adalah $a^{\phi(m)-1}$ sebab sesuai dengan Teorema Euler, $a^{\phi(m)-1} \cdot a = a^{\phi(m)} \equiv 1 \pmod{m}$.

$$\begin{aligned}
 ax &\equiv b \pmod{m} \\
 \Leftrightarrow a^{\phi(m)-1} \cdot ax &\equiv a^{\phi(m)-1} \cdot b \pmod{m} \\
 \Leftrightarrow a^{\phi(m)}x &\equiv a^{\phi(m)-1} \cdot b \pmod{m} \\
 \Rightarrow x &\equiv a^{\phi(m)-1} \cdot b \pmod{m}
 \end{aligned}$$

Karena $tm \equiv 0 \pmod{m}$ untuk setiap bilangan bulat t , maka:

$$x \equiv a^{\phi(m)-1} \cdot b + tm \pmod{m}$$

Jadi $x = a^{\phi(m)-1} \cdot b + tm$ adalah solusi $ax \equiv b \pmod{m}$.

Teorema 3.11. Teorema Wilson

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

Bukti:

Untuk $p = 2$, kita dapat menentukan bahwa $(p-1)! = 1! = 1 \equiv -1 \pmod{2}$, dengan demikian teorema benar untuk $p = 2$.

Untuk $p > 2$, berdasarkan Teorema 3.9 dan Teorema 3.10, jika $ax \equiv 1 \pmod{p}$, dan $(a, p) = 1$, maka $x \equiv a^{\phi(m)-1}$, a dan x disebut saling inverse modulo p .

Dengan demikian, setiap bilangan a yang memenuhi $1 \leq a \leq p-1$, tentu ada a^* yang memenuhi $1 \leq a^* \leq p-1$, sehingga $a \cdot a^* \equiv 1 \pmod{p}$.

Perhatikan perkalian bilangan-bilangan:

$$2 \cdot 3 \cdot \dots \cdot (p-3) \cdot (p-2)$$

yang dapat dipasangkan-pasangkan ke dalam $(p-3)/2$ pasangan, masing-masing pasangan mempunyai hasil kali sama dengan 1 modulo p . Hal ini dapat dilakukan karena masing-masing bilangan prima relatif dengan p , yaitu $(a, p) = 1$, sehingga masing-masing bilangan mempunyai inverse. Akibatnya

$2 \cdot 3 \cdot \dots \cdot (p-3) \cdot (p-2) \equiv 1 \pmod{p}$, sehingga:

$$\begin{aligned}
 (p-1)! &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-3) \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \pmod{p} \\
 &\equiv p-1 \pmod{p}
 \end{aligned}$$

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

Contoh 3.19

$$(7-1)! = 6! = 1.2.3.4.5.6 = 1.(2.4).(3.5).6 = 1.8.15.6 \equiv 1.1.1.6 \pmod{7} \equiv -1 \pmod{7}$$

$$(13-1)! = 12! = 1.2.3.4.5.6.7.8.9.10.11.12 = 1.(2.7).(3.9).(4.10).(5.8).(6.11).12$$

$$= 1.14.27.40.40.66.12 \equiv 1.1.1.1.1.12 \pmod{13} \equiv -1 \pmod{13}$$

Teorema 3.13

Jika n adalah suatu bilangan bulat positif sehingga $(n-1)! \equiv -1 \pmod{n}$, maka n adalah suatu bilangan prima.

Buktikan!

Teorema 3.12 dan Teorema 3.13 memberikan petunjuk kepada kita untuk menggunakan teorema-teorema itu dalam pengujian keprimaan suatu bilangan.

Contoh 3.20

$$(15-1)! = 14! = 1.2.3.4.5.6.7.8.9.10.11.12.13.14 = 1.2.(15)4.6.7.8.9.10.11.12.13.14$$

$$\equiv 0 \pmod{15}$$

$(15-1)! = 14!$ tidak kongruen dengan $-1 \pmod{15}$, maka 15 bukan suatu bilangan prima.

Tugas

Carilah suatu buku teori bilangan yang membahas tentang Metode $(p-1)$ Pollard .

Jelaskan Metode Pollard itu untuk apa, dan uraikan secara lengkap.

Berikan paling sedikit satu contoh penggunaan Metode $(p-1)$ Pollard .

Petunjuk Jawaban Tugas

Metode $(p-1)$ Pollard adalah metode untuk mencari suatu faktor dari suatu bilangan bulat n apabila n mempunyai suatu faktor prima p sehingga prima-prima yang membagi $p-1$ adalah prima-prima yang cukup kecil. Kita ingin $(p-1)$ hanya memiliki faktor-faktor prima yang kecil sehingga ada suatu bilangan k yang tidak terlalu besar dan $(p-1)$ membagi $k!$

Kita menginginkan $(p-1)$ membagi $k!$ agar kita dapat dengan mudah menggunakan Teorema Kecil Fermat, yaitu $2^{p-1} \equiv 1 \pmod{p}$. Karena ditentukan $(p-1)$ membagi $k!$, maka sesuai Definisi 2.1, $k! = (p-1)t$ untuk suatu bilangan bulat t , sehingga:

$2^{k!} = 2^{(p-1)t} = (2^{p-1})^t \equiv 1^t \pmod{p} \equiv 1 \pmod{p}$ dan akibatnya, sesuai dengan Definisi 3.1, $p \mid 2^{k!} - 1$. Misalkan s adalah residu positif terkecil dari $2^{k!} - 1$ modulo n , maka $2^{k!} - 1 \equiv s \pmod{n}$, berarti $2^{k!} - 1 = s + nq$ untuk suatu bilangan bulat q , dan $s = (2^{k!} - 1) - nq$. Selanjutnya, karena n mempunyai faktor prima p , maka $p \mid n$, dan sesuai Teorema 2.1, $p \mid nq$. Dengan demikian, dari keadaan $p \mid 2^{k!} - 1$ dan $p \mid nq$, sesuai Teorema 2.4, diperoleh $p \mid (2^{k!} - 1) - nq$ atau $p \mid s$.

Untuk mencari suatu faktor n , kita hanya perlu mencari FPB dari s dan n , misalkan dengan menggunakan Algoritma Euclides, dan diperoleh $(s, n) = d$. Tentu saja diperlukan $s \neq 0$ sebab untuk $s = 0$ akan berakibat $d = (s, n) = (0, n) = n$.

Langkah-langkah menggunakan metode $(p-1)$ Pollard dimulai dengan mencari $2^{k!}$ untuk suatu bilangan bulat positif k . Berikutnya, untuk menghitung sisa positif terkecil dari $2^{k!}$ modulo n , kita tentukan $r_1 = 2$, dan serangkaian hitungan:

$$r_2 \equiv r_1^2 \pmod{n}, r_3 = r_2^3 \pmod{n}, \dots, r_k = r_{k-1}^k \pmod{n}.$$

Sebagai contoh kita akan mencari suatu faktor prima dari 689.

$$r_1 = 2, r_2 = r_1^2 = 4, r_3 = r_2^3 = 64, r_4 = r_3^4 = 16777216 \equiv 66 \pmod{689}.$$

Perhatikan $(r_k - 1, 689) = 1$ untuk $k = 1, 2, 3$, tetapi $(r_4 - 1, 689) = (65, 689) = 13$ (dicari dengan menggunakan Algoritma Euclides). Dengan demikian suatu faktor prima dari 689 adalah 13.



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Carilah satu contoh sistem residu tereduksi modulo 16 yang mempunyai dua unsur negatif!
- 2) Jelaskan mengapa $S = \{-9, -33, 37, 67\}$ bukan merupakan sistem residu tereduksi modulo 10!
- 3) Carilah satu contoh sistem residu A yang lengkap modulo 12. Tambah setiap unsur dalam sistem residu dengan sebarang bilangan kelipatan 12, sehingga diperoleh himpunan B . Selidiki apakah B merupakan sistem residu lengkap modulo 12!
- 4) Carilah sisanya jika 11^{35} dibagi 13!
- 5) Jika hari ini hari Rabu, maka carilah hari apa 97^{101} hari lagi!
- 6) Carilah dua digit terakhir lambang bilangan desimal dari 39^{125} !
- 7) Carilah suatu bilangan bulat positif terkecil x yang memenuhi $61! \equiv x - 1 \pmod{71}$!
- 8) Carilah suatu bilangan bulat positif terkecil x yang memenuhi $7x \equiv 9 \pmod{20}$!

Petunjuk Jawaban Latihan

- 1) Suatu contoh sistem residu tereduksi modulo 16 adalah $A = \{1, 3, 5, 7, 9, 11, 13, 15\}$.
Jika unsur-unsur A ditambah atau dikurangi dengan kelipatan 16 sehingga diperoleh himpunan B , maka B juga merupakan suatu sistem residu tereduksi modulo 16.
Tiga contoh sistem residu tereduksi modulo 16 dengan dua unsur negatif adalah $\{-15, -29, 5, 7, 9, 11, 13, 15\}$, $\{1, 3, 5, -41, 9, -5, 13, 15\}$, dan $\{1, 3, 5, 7, -71, 11, 13, -1\}$.
- 2) $S = \{-9, -33, 37, 67\}$ bukan merupakan sistem residu tereduksi modulo 10 sebab $-33 \equiv 37 \pmod{10}$, $-33 \equiv 67 \pmod{10}$, dan atau $37 \equiv 67 \pmod{10}$.

3) $A = \{1, 5, 7, 11\}$ dan $B = \{13, 29, 67, 131\}$.

B merupakan suatu sistem residu tereduksi modulo 12 karena $(13, 12) = (29, 12) = (67, 12) = (131, 12) = 1$ dan tidak ada satu pun sepasang unsur B yang kongruen.

4) Kita harus mencari x dari $11^{35} \equiv x \pmod{13}$.

Karena $(11, 13) = 1$, maka dan $\phi(13) = 12$, maka menurut Teorema Kecil Fermat, kita dapat menunjukkan bahwa $11^{12} \equiv 1 \pmod{13}$.

$$\begin{aligned} 11^{35} &= (11^{12})^2 \cdot 11^{11} \equiv 11^{11} \pmod{13} \equiv (-2)^{11} \pmod{13} \\ &\equiv 4.4.4.4.4.11 \pmod{13} \equiv 3.3.5 \pmod{13} \equiv 6 \pmod{13} \end{aligned}$$

Jadi $x = 6$.

5) Kita harus mencari x dari $97^{101} \equiv x \pmod{7}$

$$(97, 7) = 1, \text{ maka } 97^6 \equiv 1 \pmod{7}$$

$$97^{101} = (97^6)^6 \cdot 97^5 \equiv 97^5 \pmod{7} \equiv 97 \cdot 97 \cdot 97 \cdot 97 \cdot 97 \pmod{7} \equiv 6 \pmod{7}$$

Jadi 97^{101} hari lagi adalah hari Selasa.

6) Misalkan $(39, 25) = 1$, maka menurut Teorema Euler,

$$39^{\phi(25)} \equiv 1 \pmod{25} \text{ atau } 39^{20} \equiv 1 \pmod{25}$$

$$39^{125} = (39^{20})^6 \cdot 39^5 \equiv 39^5 \pmod{25} \equiv 14^5 \pmod{25} \equiv 4 \pmod{25}$$

$$(39, 4) = 1, \text{ maka menurut Teorema Euler, } 39^{\phi(4)} \equiv 1 \pmod{4},$$

$$39^2 \equiv 1 \pmod{4}, 39^{125} = (39^2)^{62} \cdot 39 \equiv 3 \pmod{4}.$$

Selanjutnya dari:

$$39^{125} \equiv 4 \pmod{25} \equiv 4, 29, 54, 79 \pmod{25} \text{ dan}$$

$$39^{125} \equiv 3 \pmod{4} \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55,$$

$$59, 63, 67, 71, 75, 79, 83, 87, 91, 95, 99 \pmod{4}$$

dapat ditunjukkan bahwa $39^{125} \equiv 79 \pmod{100}$.

Jadi dua digit terakhir lambang bilangan desimal 39^{125} adalah 79.

7) Karena 71 adalah suatu bilangan prima, maka menurut Teorema Wilson,

$$(71-1)! = 70! \equiv -1 \pmod{71}$$

$$(61!).62.63.64.65.66.67.68.69.70.71 \equiv -1 \pmod{71}$$

$$(61!)(-9)(-8)(-7)(-6)(-5)(-4)(-3)(-2)(-1) \equiv -1 \pmod{71}$$

$$(61!)(72)(-72)(70) \equiv -1 \pmod{71}$$

$$61! \equiv -1 \pmod{71}$$

$61! \equiv -1 \pmod{71}$ dan $61! \equiv x-1 \pmod{71}$, maka $x-1 \equiv -1 \pmod{71}$,

atau $x \equiv 0 \pmod{71} \equiv 0, 71, 142, 213, \dots \pmod{71}$.

Karena x yang dicari adalah yang terkecil, maka $x = 71$.

8) Misalkan $7x \equiv 9 \pmod{20}$, maka

$$x = 7^{\phi(20)-1} \cdot 9 \equiv 7^{8-1} \cdot 9 \pmod{20} \equiv 7^7 \cdot 9 \pmod{20}$$

$$\equiv 49.49.49.7.9 \pmod{20}$$

$$\equiv (9)(9)(9).63 \pmod{20}$$

$$\equiv 9.3 \pmod{20}$$

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

Jadi $x \equiv 7 \pmod{20}$.



RANGKUMAN

Secara keseluruhan, bagian-bagian utama yang perlu diperhatikan dalam Kegiatan Belajar 2 adalah Definisi dan Teorema, yaitu:

1. **Definisi 3.2** tentang sistem residu yang lengkap modulo m

2. **Definisi 3.3** tentang sistem residu tereduksi modulo m

3. **Definisi 3.4** tentang fungsi ϕ -Euler

4. **Teorema-teorema:**

3.7. Jika $(a, m) = 1$ sedemikian hingga x_1, x_2, \dots, x_k adalah suatu sistem residu yang lengkap atau tereduksi, maka ax_1, ax_2, \dots, ax_k juga merupakan sistem residu yang lengkap atau tereduksi modulo m .

3.8. Teorema Euler

Jika $a, m \in \mathbb{Z}$ dan $m > 0$ sehingga $(a, m) = 1$, maka $a^{\phi(m)} \equiv 1 \pmod{m}$.

3.9. Teorema Kecil Fermat

Jika p adalah suatu bilangan prima dan p tidak membagi a , maka $a^{p-1} \equiv 1 \pmod{p}$.

3.10. Jika $(a,m)=1$, maka hubungan $ax \equiv b \pmod{m}$ mempunyai solusi $x = a^{\phi(m)-1} \cdot b + tm$.

3.11. Teorema Wilson

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

**TES FORMATIF 2**

1) Skor 10

Carilah suatu x jika $5x \equiv 7 \pmod{23}$.

2) Skor 10

Tunjukkan jika n adalah suatu bilangan komposit dan $n \neq 4$, maka $(n-1)! \equiv 0 \pmod{n}$.

3) Skor 10

Tunjukkan jika p adalah suatu bilangan prima ganjil, maka $2(p-3)! \equiv -1 \pmod{p}$.

4) Skor 10

Tunjukkan jika n adalah suatu bilangan ganjil dan n tidak membagi tiga, maka $n^2 \equiv 1 \pmod{24}$.

5) Skor 10

Tunjukkan jika p dan q adalah bilangan-bilangan prima yang berbeda, maka $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

6) Skor 10

Tunjukkan jika p adalah suatu bilangan prima ganjil, maka $1^2 3^2 \dots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

7) Skor 10

Tunjukkan jika p adalah suatu bilangan prima ganjil dan $p \equiv 3 \pmod{4}$, maka $((p-1)/2)! \equiv \pm 1 \pmod{p}$.

8) Skor 20

Carilah bilangan-bilangan bulat positif n yang menyebabkan $n^4 + 4^n$ adalah bilangan prima.

9) Skor 10

Tunjukkan jika p adalah suatu bilangan prima dan a adalah suatu bilangan bulat, maka $p \mid (a^p + (p-1)!a)$.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

mungkin kongruen dengan 0 modulo n (n adalah suatu bilangan bulat genap).

- 4) Perhatikan bahwa $n=1$ memenuhi hubungan sebab

$$5 = 5^1 = 1 + 4(1) \equiv 1 + 4(1) \pmod{16}.$$

Misalkan hubungan berlaku untuk $n=k$, yaitu $5^k \equiv 1 + 4k \pmod{16}$,

harus dibuktikan hubungan berlaku untuk $n=k+1$,

yaitu $5^{k+1} \equiv 1 + 4(k+1) \pmod{16}$

$$5^{k+1} = 5^k \cdot 5 \equiv 5(1 + 4k) \pmod{16} \equiv 1 + 4(k+1) \pmod{16}.$$

- 5) (a) $n! = 1.2.3\dots n \equiv 0 \pmod{7}$ jika $n \geq 7$.

Karena $1! \equiv 1 \pmod{7}, 2! \equiv 2 \pmod{7}, 3! \equiv 6 \pmod{7}, 4! \equiv 3 \pmod{7}$,

$5! \equiv 1 \pmod{7}, 6! \equiv 6 \pmod{7}$, maka

$$1! + 2! + 3! + 4! + 5! + 6! + 7! + \dots + 100! \equiv 1! + 2! + 3! + 4! + 5! + 6! \pmod{7}$$

$$\equiv 1 + 2 + 6 + 3 + 1 + 6 \pmod{7} \equiv 5 \pmod{7}.$$

- (b) $n! = 1.2.3\dots n \equiv 0 \pmod{25}$ jika $n \geq 10$

$$1! + 2! + 3! + 4! + 5! + 6! + 7! + \dots + 100! \equiv 1! + 2! + 3! + \dots + 9! \pmod{25}$$

$$\equiv 1 + 2 + 6 + 24 + 20 + 20 + 15 + 20 + 5 \pmod{25} \equiv 13 \pmod{25}.$$

- 6) (a) Jika secara berurutan kita kerjakan, maka dapat kita cari bahwa:

$$1! \equiv 1 \pmod{7}, 2! \equiv 2 \pmod{7}, 3! \equiv 6 \pmod{7}, 4! \equiv 3 \pmod{7},$$

$$5! \equiv 1 \pmod{7}, \text{ sehingga } 6! \equiv 6 \pmod{7}$$

- (b) $1! \equiv 1 \pmod{13}, 2! \equiv 2 \pmod{13}, 3! \equiv 6 \pmod{13}, 4! \equiv 11 \pmod{13}$,

$$5! \equiv 5.11 \pmod{13} \equiv 3 \pmod{13}, 6! \equiv 6.3 \pmod{13} \equiv 5 \pmod{13},$$

$$7! \equiv 7.5 \pmod{13} \equiv 9 \pmod{13}, 8! \equiv 8.9 \pmod{13} \equiv 7 \pmod{13},$$

$$9! \equiv 9.7 \pmod{13} \equiv 11 \pmod{13}, 10! \equiv 10.11 \pmod{13} \equiv 6 \pmod{7},$$

$$11! \equiv 11.6 \pmod{13} \equiv 1 \pmod{13}, 12! \equiv 12.1 \pmod{13} \equiv 12 \pmod{7}.$$

- (c) Kerjakan seperti (a) dan (b), diperoleh $18! \equiv 18 \pmod{19}$

- (d) Kerjakan seperti (a) dan (b), diperoleh $22! \equiv 22 \pmod{19}$

Dari hasil (a), (b), (c), dan (d) dapat diduga adanya suatu teorema:

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

Tes Formatif 2

- 1) $5x \equiv 7 \pmod{23}$, maka $x \equiv 5^{21}.7 \pmod{23} \equiv (5^2)^{10}.5.7 \pmod{23}$

$$\equiv 2^{10}.12 \pmod{23} \equiv 2^5 \cdot 2^5 \cdot 12 \pmod{23} \equiv 9.9.12 \pmod{23} \equiv 6 \pmod{23}$$

- 2) Jika n adalah suatu bilangan komposit, maka n mempunyai faktor f yang kurang dari \sqrt{n} dengan $1 < n/f < n$. Dengan demikian faktor f dan n/f keduanya muncul di antara faktor-faktor $(n-1)! = 1.2.3.\dots.(n-1)$. Jika $f \neq n/f$, maka $n|(n-1)!$
 Karena f dan n/f adalah faktor-faktor $(n-1)!$, berarti $(n-1)! \equiv 0 \pmod{n}$.
 Jika $f = n/f$, maka $f \cdot f = f \cdot (n/f) = n$, atau $f^2 = n$.
 Karena $2f < n$, maka $2f^2 = 2n$ merupakan faktor dari $(n-1)!$, berarti $(n-1)! \equiv 0 \pmod{n}$.
- 3) Diketahui bahwa p adalah suatu bilangan prima ganjil, maka menurut Teorema Wilson, $(p-1)! \equiv -1 \pmod{p}$, berarti $(p-1)(p-2)(p-3) \equiv -1 \pmod{p}$ atau $(-1)(-2)(p-3) \equiv -1 \pmod{p}$
 Jadi $2(p-1)! \equiv -1 \pmod{p}$.
- 4) Karena n tidak membagi 3, maka $(3,n)=1$, sehingga $n^2 \equiv 1 \pmod{3}$, atau $3|n^2 - 1$. Selanjutnya diketahui bahwa n adalah suatu bilangan ganjil, maka $n = 2t + 1$ untuk suatu bilangan bulat t . Dengan demikian $n^2 - 1 = (2t+1)^2 - 1$ atau $n^2 - 1 = 4(t^2 + t) = 4t(t+1)$. Karena t dan t^2 harus berparitas sama, yaitu keduanya genap atau keduanya ganjil, maka $n^2 - 1 = 4t(t+1) = 8r$, atau $8|n^2 - 1$. Karena $3|n^2 - 1$, $8|n^2 - 1$, dan $(3,8) = 1$, maka $3 \cdot 8 = 24|n^2 - 1$, berarti $n^2 \equiv -1 \pmod{24}$.
- 5) Karena $(p,q) = 1$, maka sesuai dengan Teorema Kecil Fermat, $p^{q-1} \equiv 1 \pmod{q}$ dan $q^{p-1} \equiv 1 \pmod{p}$. Akibatnya, $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$ dan $q^{p-1} + p^{q-1} \equiv 1 \pmod{p}$. Dengan demikian, sesuai dengan Teorema 3.6 (b), $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
- 6) $1^2 3^2 \dots (p-4)^2 (p-2)^2$
 $\equiv (-1)^{(p-1)/2} \cdot 1 \cdot (-1) \cdot 2 \cdot (-2) \dots (p-4)(4-p)(p-2)(2-p)$
 $\equiv (-1)^{(p-1)/2} 1 \cdot (p-1) \cdot 2 \cdot (p-2) \dots (p-4) \cdot 4 \cdot 2$
 $\equiv (-1)^{(p-1)/2} (p-1)! \equiv (-1)^{(p-1)/2} (-1) \equiv (-1)^{(p+1)/2} \pmod{p}$

- 7) p adalah suatu bilangan prima, maka $p-1 \equiv -1 \pmod{p}$, $p-2 \equiv -2 \pmod{p}$, $p-3 \equiv -3 \pmod{p}$, ..., $(p+1)/2 \equiv (p-1)/2 \pmod{p}$. Dengan demikian dapat ditentukan bahwa $\left(\frac{p-1}{2}\right)!^2 \equiv -1(p-1)! \equiv 1 \pmod{p}$.

Jika $k = \left(\frac{p-1}{2}\right)!$, maka $k^2 \equiv 1 \pmod{p}$, yaitu $p | k^2 - 1$, $p | (k-1)(k+1)$, berarti $k \equiv \pm 1 \pmod{p}$, atau $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

- 8) Jika n adalah suatu bilangan bulat genap, maka $n^4 + 4^n$ adalah suatu bilangan genap positif dan lebih dari 2 sehingga tentu n adalah bukan suatu bilangan prima. Jika n adalah suatu bilangan bulat positif ganjil, maka perhatikan bahwa:

$$\begin{aligned} n^4 + 4^n &= n^4 + 2n^2 2^n + 2^{2n} - 2n^2 2^n \\ &= (n^2 + 2^n)^2 - (n \cdot 2^{(n+1)/2})^2 2^n + n \cdot 2^{(n+1)/2} (n^2 + 2^n - n \cdot 2^{(n+1)/2}). \end{aligned}$$

Jika $n > 1$, maka masing-masing faktor $n^4 + 4^n$ adalah lebih dari 1, sehingga jelas bahwa $n^4 + 4^n$ bukan merupakan suatu bilangan prima. Jadi $n = 1$, sehingga dapat ditentukan bahwa $n^4 + 4^n = 1^4 + 4^n = 1 + 4 = 5$.

- 9) Diketahui p adalah suatu bilangan prima, maka sesuai dengan Teorema Kecil Fermat dapat ditunjukkan bahwa $a^{p-1} \equiv 1 \pmod{p}$, atau $a^p \equiv a \pmod{p}$ untuk setiap bilangan bulat a , dan sesuai dengan Teorema Wilson, $(p-1)! \equiv -1 \pmod{p}$ atau $(p-1)!a \equiv -a \pmod{p}$. Akibatnya, $a^p + (p-1)!a \equiv a + (-a) \pmod{p} \equiv 0 \pmod{p}$, dengan demikian $p | a^p + (p-1)!a$.

Daftar Pustaka

- Niven, I., Zuckerman, H.S. and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Kongruensi Linier

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul kongruensi linier ini diuraikan tentang sifat-sifat dasar kongruensi linier dan penyelesaiannya, kongruensi linier simultan, Teorema Sisa China, sistem kongruensi linier, dan penerapan kongruensi linier.

Sebagai bahasan yang berkaitan dengan Aljabar (biasa), kongruensi linier serupa dengan persamaan linier, tetapi dengan semesta pembicaraan himpunan bilangan modulo. Meskipun demikian, terdapat banyak uraian dalam kongruensi linier yang memerlukan pemahaman yang berbeda dengan persamaan linier, misalnya terkait dengan banyaknya solusi, yaitu kongruensi linier dapat tidak mempunyai solusi, dan mempunyai satu atau lebih solusi. Berikutnya, berbeda dengan persamaan linier satu variabel yang tidak bisa digabung dengan persamaan linier satu variabel yang lain, dua atau lebih kongruensi linier dapat digabung dan gabungannya disebut kongruensi linier simultan. Pada akhirnya pembahasan kongruensi linier yang serupa dengan persamaan linier adalah sistem kongruensi linier, dengan banyak variabel sama dengan banyaknya kongruensi.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep dan sifat kongruensi linier, penyelesaian kongruensi linier, kongruensi linier simultan, dan sistem kongruensi linier.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep kongruensi linier dan sifat-sifatnya, konsep kongruensi linier simultan dan sifat-sifatnya, konsep sistem kongruensi linier dan sifat-sifatnya, serta keterkaitan satu sama lain untuk diterapkan dalam menyelesaikan masalah-masalah tertentu.

Susunan Kegiatan Belajar

Modul 4 ini terdiri dari dua Kegiatan Belajar. Kegiatan Belajar 1 adalah Kongruensi Linier, dan Kegiatan Belajar 2 adalah Sistem Kongruensi Linier. Setiap kegiatan belajar memuat Uraian, Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 4 ini ditempatkan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi pembahasan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab, maka pelajari Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum berhasil menjawab permasalahan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Penguasaan Anda dengan cara mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah pengerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1

Kongruensi Linier

 Dalam Aljabar (biasa), pembahasan utama tentang persamaan adalah mencari **akar**, atau **selesaian** dari persamaan polinomial dengan koefisien bulat $f(x) = 0$ dengan:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

Nilai-nilai x yang memenuhi persamaan $f(x) = 0$ disebut akar atau selesaian persamaan $f(x) = 0$. Persamaan $f(x) = 0$ berderajat n paling banyak mempunyai n selesaian.

Serupa dengan persamaan Aljabar, pembahasan utama kongruensi adalah mencari bilangan-bilangan bulat yang memenuhi $f(x) \equiv 0 \pmod{m}$ dengan:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

Sebagai peragaan, kongruensi

$$f(x) = x^3 + 6x^2 - 11 \equiv 0 \pmod{5}$$

dipenuhi oleh $x = 3$ sebab jika x diganti 3 diperoleh pernyataan yang benar:

$$f(3) = 3^3 + 6 \cdot 3^2 - 11 = 27 + 54 - 11 \equiv 0 \pmod{5}$$

Nilai $x = 3$ disebut **selesaian** kongruensi $f(x) = x^3 + 6x^2 - 11 \equiv 0 \pmod{5}$. Menyelesaikan kongruensi berarti mencari selesaian kongruensi.

Definisi 4.1

Ditentukan $f(x)$ adalah suatu polinomial dengan koefisien-koefisien bulat, dan $\{a_0, a_1, \dots, a_{m-1}\}$ adalah suatu sistem residu yang lengkap modulo m . Banyaknya selesaian kongruensi:

$$f(x) \equiv 0 \pmod{m}$$

Adalah banyaknya a_i , dengan $a_i = 0, 1, 2, \dots, m-1$ yang memenuhi kongruensi:

$$f(a_i) \equiv 0 \pmod{m}$$

Kita perlu memperhatikan bahwa jika $x = x_0$ adalah suatu selesaian kongruensi $f(x) \equiv 0 \pmod{m}$, dan diketahui $x_1 \equiv x_0 \pmod{m}$, maka:

$$f(x_1) \equiv f(x_0) \pmod{m} \equiv 0 \pmod{m}$$

Dengan demikian x_1 adalah juga suatu selesaian. Jadi, jika satu unsur dari suatu kelas kongruensi modulo m adalah suatu selesaian, maka semua unsur dari kelas kongruensi modulo m adalah juga selesaian-selesaian. Banyaknya selesaian suatu kongruensi modulo m adalah banyaknya selesaian tidak kongruen modulo m , yaitu banyaknya m kelas kongruensi modulo m yang memberikan selesaian.

Contoh 4.1

Diketahui $f(x) = 2x - 4$

Banyaknya selesaian dari $f(x) = 2x - 4 \equiv 0 \pmod{6}$ ditentukan oleh banyaknya unsur tidak kongruen dari suatu sistem residu lengkap modulo 6, atau dari banyaknya kelas residu modulo 6 yang memberikan satu unsur yang memenuhi kongruensi. Untuk keperluan menyelesaikan $f(x) = 2x - 4 \equiv 0 \pmod{6}$, suatu langkah yang lebih mudah adalah dengan mengambil $\{0, 1, 2, 3, 4, 5\}$ sebagai suatu sistem residu yang lengkap modulo 6. Karena pasangan unsur-unsur himpunan $\{0, 1, 2, 3, 4, 5\}$ tidak ada yang kongruen, maka selesaian dari $f(x) = 2x - 4 \equiv 0 \pmod{6}$ dapat dilakukan dengan mencari unsur-unsur $\{0, 1, 2, 3, 4, 5\}$ yang memenuhi kongruensi, yaitu:

$$f(0) = 2 \cdot 0 - 4 = -4, \text{ tidak kongruen } 0 \pmod{6}$$

$$f(1) = 2 \cdot 1 - 4 = -2, \text{ tidak kongruen } 0 \pmod{6}$$

$$f(2) = 2 \cdot 2 - 4 = 0 \equiv 0 \pmod{6}$$

$$f(3) = 2 \cdot 3 - 4 = 2, \text{ tidak kongruen } 0 \pmod{6}$$

$$f(4) = 2 \cdot 4 - 4 = 4, \text{ tidak kongruen } 0 \pmod{6}$$

$$f(5) = 2 \cdot 5 - 4 = 6 \equiv 0 \pmod{6}$$

Dengan demikian selesaian kongruensi adalah $x \equiv 2 \pmod{6}$ dan $x \equiv 5 \pmod{6}$, dan banyaknya selesaian adalah dua.

Definisi 4.2

Suatu kongruensi yang mempunyai bentuk:

$$ax \equiv b \pmod{m}$$

dengan $a, b, m \in \mathbb{Z}$ disebut suatu **kongruensi linier satu variabel**.

Perhatikan bahwa jika $x = x_0$ adalah suatu selesaian $ax \equiv b \pmod{m}$, dan jika diketahui bahwa $x_1 \equiv x_0 \pmod{m}$, maka $ax_1 \equiv ax_0 \pmod{m}$, dengan demikian x_1 juga suatu selesaian.

Contoh 4.2

Kongruensi linier $7x \equiv 3 \pmod{12}$ mempunyai satu selesaian $x \equiv 9 \pmod{12}$ sebab $x = 9$ merupakan satu-satunya unsur dalam suatu kelas residu modulo 12 yang memberikan satu unsur yang memenuhi kongruensi. Dengan demikian $x = 9$ merupakan satu unsur dari suatu sistem residu yang lengkap modulo 12 yang memenuhi kongruensi, $x = 9$ adalah satu unsur dari sistem residu lengkap modulo 12 yaitu $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Contoh 4.3

Kongruensi linier $6x \equiv 9 \pmod{15}$ mempunyai tiga selesaian, $x = 4 + 15r$, $x = 9 + 15r$, dan $x = 4 + 15r$ untuk sebarang bilangan bulat r .

Nilai-nilai $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ tidak ada yang memenuhi kongruensi $6x \equiv 9 \pmod{15}$ selain 4, 9, dan 14.

Berikut ini adalah suatu teorema yang penting karena dapat memberikan alasan dapat atau tidak dapat suatu kongruensi linier diselesaikan, serta memberikan jawaban tentang banyaknya selesaian suatu kongruensi linier.

Teorema 4.1

Jika $(a, m) = d$ dan kongruensi $ax \equiv b \pmod{m}$ mempunyai selesaian, maka $d | b$. Jika $d | b$, maka kongruensi $ax \equiv b \pmod{m}$ mempunyai d selesaian.

Bukti:

$ax \equiv b \pmod{m}$, maka menurut definisi 3.1, $m | ax - b$

Diketahui $d = (a, m)$, maka menurut definisi 2.3, $d | a$ dan $d | m$. Karena $d | a$, maka sesuai Teorema 2.1, $d | ax$ untuk sebarang bilangan bulat x . Selanjutnya, dari $d | m$ dan $m | ax - b$, sesuai dengan Teorema 2.2, $d | ax - b$. Berdasarkan Teorema 2.9, $d | ax$ dan $d | ax - b$, berakibat $d | -b$, sehingga $d | b$.

Selanjutnya, $ax \equiv b \pmod{m}$ dapat dinyatakan sebagai $d\left(\frac{a}{d}\right)x \equiv d\left(\frac{b}{d}\right) \pmod{m}$, dan sesuai dengan Teorema 3.6 (a), dapat ditentukan $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\left(\frac{m}{d}\right)}$. Karena $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ dan $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{m}{d}}$, maka menurut Teorema 3.10, kongruensi linier $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{m}{d}}$ mempunyai suatu selesaian $x = x_0 + t \cdot \frac{m}{d}$ dengan $x_0 \equiv \left(\frac{a}{d}\right)^{\phi(m)-1} \cdot \left(\frac{b}{d}\right) \pmod{m}$ dan $t \in \mathbb{Z}$.

Dengan demikian seluruh selesaian kongruensi adalah:

$$x = x_0, x_0 + 1\left(\frac{m}{d}\right), x_0 + 2\left(\frac{m}{d}\right) + \dots + x_0 + (d-1)\left(\frac{m}{d}\right)$$

Contoh 4.4

Selesaikan kongruensi-kongruensi linier:

- 1) $36x \equiv 8 \pmod{102}$
- 2) $3x \equiv 2 \pmod{5}$
- 3) $15x \equiv 6 \pmod{18}$

Jawab:

- 1) Karena $(36,102) = 6$ dan 6 tidak membagi 8, maka $36x \equiv 8 \pmod{102}$ tidak mempunyai selesaian.
- 2) Karena $(3,5) = 1$ dan $1|2$, maka $3x \equiv 2 \pmod{5}$ mempunyai satu selesaian yaitu $x \equiv 4 \pmod{5}$.
- 3) $(15,18) = 3$ dan $3|6$, maka $15x \equiv 6 \pmod{18}$ mempunyai tiga selesaian, yaitu $x \equiv 4, 10, 16 \pmod{18}$.

Contoh 4.5

Selesaikan kongruensi linier $144x \equiv 216 \pmod{360}$.

Jawab:

FPB dari 144 dan 360 dicari dengan menggunakan Teorema 2.20 Algoritma Euclides

$$360 = 2 \cdot 144 + 72$$

$$144 = 2 \cdot 72 + 0$$

$$(144, 360) = 72$$

$72|216$, maka $144x \equiv 216 \pmod{360}$ mempunyai 72 selesaian. Seluruh selesaian dicari sebagai berikut :

$$144x \equiv 216 \pmod{360}$$

$$2x \equiv 3 \pmod{5}$$

$$x \equiv 2^3 \cdot 3 \pmod{5} = 8 \cdot 3 \pmod{5} = 4 \pmod{5}$$

Selesaian kongruensi linier $144x \equiv 216 \pmod{360}$ adalah:

$$x \equiv 4, 4+1 \cdot 5, 4+2 \cdot 5, \dots, 4+(72-1) \cdot 5 \pmod{360}$$

$$x \equiv 4, 9, 14, \dots, 359 \pmod{360}$$

Perhatikan tiga hal dalam menyelesaikan kongruensi linier

- 1) $ax \equiv ay \pmod{m}$ diselesaikan melalui $x \equiv y \pmod{\frac{m}{(a,m)}}$
- 2) $ax \equiv ay \pmod{m}$ dan $(a,m)=1$ diselesaikan melalui $x \equiv y \pmod{m}$

- 3) $ax \equiv b \pmod{m}$ dengan nilai-nilai a , b , dan m yang relatif besar dilakukan dengan menyederhanakan kongruensi, yaitu mengganti kongruensi semula dengan kongruensi lain yang mempunyai bilangan modulo lebih kecil. Prosedur ini bisa diulangi sampai diperoleh suatu kongruensi yang selesaiannya mudah ditentukan.

Diketahui kongruensi linier $ax \equiv b \pmod{m}$, misalkan $a < m$ (jika $a > m$, maka a dapat “dikecilkan” dengan jalan mencari residu (sisa) positif terkecil dari a modulo m).

$ax \equiv b \pmod{m}$, maka $m | ax - b$, sehingga $ax - b = my$ untuk suatu $y \in \mathbb{Z}$, berarti $my + b = ax$, dan akibatnya $a | my + b$, atau $my \equiv -b \pmod{a}$. Karena $m > a$, maka m dapat “dikecilkan” dengan jalan mencari residu positif terkecil dari m modulo a . Sampai pada tahap ini jelas bahwa kongruensi linier semula $ax \equiv b \pmod{m}$ berubah menjadi kongruensi linier $my \equiv -b \pmod{a}$ yang lebih “sederhana” karena mempunyai modulo a yang lebih kecil dari a .

Selesaikan kongruensi linier $my \equiv -b \pmod{a}$ jika memang sudah menjadi lebih mudah untuk diselesaikan, misalkan selesaiannya adalah $y = y_0$. Dengan demikian dari $ax - b = my$, atau $x = \frac{my + b}{a}$, dapat

ditentukan bahwa $x_0 = \frac{my_0 + b}{a}$ merupakan suatu selesaian kongruensi linier $ax \equiv b \pmod{m}$.

Ulangi langkah serupa jika memang kongruensi linier $my \equiv -b \pmod{a}$ masih sulit untuk diselesaikan. Misalkan residu positif terkecil m modulo a adalah k , maka $my \equiv -b \pmod{a}$ dapat diubah menjadi $az \equiv b \pmod{a}$. Demikian seterusnya sehingga pada tahapan tertentu dapat diperoleh suatu selesaian, dan dari selesaian yang diperoleh dapat diproses mundur sehingga diperoleh selesaian dari kongruensi $ax \equiv b \pmod{m}$.

Contoh 4.6

Selesaikan $10x \equiv 3 \pmod{23}$

Jawab:

Dari $10x \equiv 3 \pmod{23}$ dapat diperoleh kongruensi lain yang lebih “sederhana”, misalnya dengan variabel y , yaitu $23y \equiv -3 \pmod{10}$, dan berikutnya dapat dicari residu positif terkecil 23 modulo 10, yaitu 3, sehingga diperoleh kongruensi $3y \equiv -3 \pmod{10}$, dan kita sudah dapat menentukan selesaian $3y \equiv -3 \pmod{10}$ yaitu $y \equiv -1 \pmod{10}$ atau $y \equiv 9 \pmod{10}$, dan ini berarti $y_0 = 9$, sehingga dapat ditentukan

$$x_0 = \frac{23y_0 + 3}{10} = \frac{23.9 + 3}{10} = 21$$
Contoh 4.7.

Selesaikan $19x \equiv 2 \pmod{49}$

Jawab:

Dari $19x \equiv 2 \pmod{49}$ dapat diperoleh kongruensi lain $49y \equiv -2 \pmod{19}$ atau $11y \equiv -2 \pmod{19}$. Karena kita relatif masih sulit untuk menentukan selesaian $11y \equiv -2 \pmod{19}$, maka langkah serupa dilakukan dengan memilih suatu variabel lain sehingga diperoleh $19z \equiv 2 \pmod{11}$, atau $8z \equiv 2 \pmod{11}$. Karena kita merasakan masih sulit untuk menyelesaikan, langkah serupa dilangung sehingga diperoleh $11r \equiv -2 \pmod{8}$, atau $3r \equiv -2 \pmod{8}$. Ternyata kita sudah lebih mudah memperoleh selesaian, yaitu $r_0 \equiv 2 \pmod{8}$, selanjutnya $z_0 = (11r_0 + 2)/8 = 3$, $y_0 = (19z_0 - 2)/11 = 5$, dan $x_0 = (49y_0 + 2)/19 = 13$. Selesaian kongruensi adalah $x \equiv 13 \pmod{49}$.

Jika kita cermati Contoh 4.7, langkah-langkah memperoleh selesaian dapat diperagakan sebagai berikut:

$$19x \equiv 2 \pmod{49} \rightarrow x_0 = \frac{49y_0 + 2}{19} = 13$$

$$49y \equiv -2 \pmod{19}$$

$$11y \equiv -2 \pmod{19} \rightarrow y_0 = \frac{19z_0 - 2}{11} = 5$$

$$19z \equiv 2 \pmod{11}$$

$$8z \equiv 2 \pmod{11} \rightarrow z_0 = \frac{11r_0 + 2}{8} = 3$$

$$11r \equiv -2 \pmod{8}$$

$$3r \equiv -2 \pmod{8} \rightarrow r_0 = 2$$

Contoh 4.8

Selesaikan kongruensi linier $67320x \equiv 136 \pmod{96577}$

Jawab:

$(67320, 96577)$ dicari dengan menggunakan Teorema 2.20 Algoritma Euclides:

$$96577 = 1.67320 + 29257$$

$$67320 = 2.29257 + 8806$$

$$29257 = 3.8806 + 2839$$

$$8806 = 3.2839 + 289$$

$$2839 = 9.289 + 238$$

$$289 = 1.238 + 51$$

$$238 = 4.51 + 34$$

$$51 = 1.34 + 17$$

$$34 = 2.17 + 0$$

Karena $(67320, 96577) = 17$, dan $17 \mid 136$, maka kongruensi dapat diselesaikan dan mempunyai 17 selesaian.

Selanjutnya, dari $67320x \equiv 136 \pmod{96577}$, atau:

$$17.3960x \equiv 17.8 \pmod{17.5681}$$

dengan $(67320, 96577) = 17$, kita dapat menggunakan Teorema 3.6 (a) sehingga diperoleh $3960x \equiv 8 \pmod{5681}$, dan diselesaikan seperti uraian sebelumnya.

$$3960x \equiv 8 \pmod{5681} \rightarrow x_0 = \frac{5681y_0 + 8}{3960} = 4694$$

$$5681y \equiv -8 \pmod{3960}$$

$$1721y \equiv -8 \pmod{3960} \rightarrow y_0 = \frac{3960z_0 - 8}{1721} = 3272$$

$$3960z \equiv 8 \pmod{1721}$$

$$518z \equiv 8 \pmod{1721} \rightarrow z_0 = \frac{1721r_0 + 8}{518} = 1422$$

$$1721r \equiv -8 \pmod{518}$$

$$167r \equiv -8 \pmod{518} \rightarrow r_0 = \frac{518s_0 - 8}{167} = 428$$

$$518s \equiv 8 \pmod{167}$$

$$17s \equiv 8 \pmod{167} \rightarrow s_0 = \frac{167t_0 + 8}{17} = 138$$

$$167t \equiv -8 \pmod{17}$$

$$14t \equiv -8 \pmod{17} \rightarrow t_0 = \frac{17m_0 - 8}{14} = 14$$

$$17m \equiv 8 \pmod{14}$$

$$3m \equiv 8 \pmod{14} \rightarrow m_0 = 12$$

Selesaian kongruensi adalah:

$$x \equiv 4694, 4694+1.5681, \dots, 4694+16.5681 \pmod{96577}$$

$$x \equiv 4694, 10375, \dots, 95560 \pmod{96577}$$

Marilah sekarang kita bahas lebih lanjut gabungan dari dua atau lebih kongruensi linier dengan satu variabel, dan gabungan ini disebut **sistem kongruensi linier simultan**.

Definisi 4.3

Sistem kongruensi linier satu variabel:

$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_r \pmod{m_r}$ disebut sistem kongruensi linear simultan

Untuk mencari solusi sistem kongruensi linier simultan, kita memerlukan pembahasan awal tentang sistem yang terdiri dari dua kongruensi linier.

Teorema 4.2

Sistem kongruensi linier simultan:

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

dapat diselesaikan jika dan hanya jika $a_1 \equiv a_2 \pmod{(m_1, m_2)}$

Bukti:

(→) Diketahui $x \equiv a_1 \pmod{m_1}$, maka sesuai Teorema 3.1, $x = a_1 + m_1k$, $k \in \mathbb{Z}$. Selanjutnya, dari $x = a_1 + m_1k$ dan $x \equiv a_2 \pmod{m_2}$, dapat ditunjukkan bahwa $a_1 + m_1k \equiv a_2 \pmod{m_2}$, atau $m_1k \equiv a_2 - a_1 \pmod{m_2}$.

Sesuai Teorema 4.1, kongruensi linier $m_1k \equiv a_2 - a_1 \pmod{m_2}$ dapat diselesaikan jika $(m_1, m_2) | a_2 - a_1$, dan sesuai Definisi 3.1, $a_1 \equiv a_2 \pmod{(m_1, m_2)}$

(←) Buktikan!

Teorema 4.2 juga memberikan petunjuk, jika banyaknya kongruensi linear dalam sistem yang simultan lebih dari dua, maka penyelidikan dapat dilakukan untuk semua kemungkinan pasangan kongruensi. Demikian pula dapat ditentukan, jika $(m_1, m_2) = 1$, maka sistem kongruensi linier simultan $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ selalu dapat diselesaikan, dan hal ini dapat diperluas untuk sistem kongruensi linier simultan yang terdiri lebih dari dua kongruensi linier.

Berikutnya, beberapa cara yang dapat digunakan menyelesaikan sistem kongruensi linier simultan adalah cara **biasa**, cara **iterasi**, dan cara sisa **China**.

Cara Biasa

Cara ini disebut biasa karena kita hanya membuat barisan bilangan yang memenuhi masing-masing kongruensi, dan dilanjutkan dengan pencarian unsur persekutuan dari semua kongruensi. Penetapan selesaian didasarkan pada Teorema 3.6 (b).

Contoh 4.9

Selesaikan sistem kongruensi linier simultan $x \equiv 13 \pmod{16}$ dan $x \equiv 5 \pmod{14}$

Jawab:

$13 \equiv 5 \pmod{(16,14)}$ atau $8 \equiv 0 \pmod{2}$, maka sistem kongruensi dapat diselesaikan.

$$x \equiv 13 \pmod{16} = 13, 29, 45, 61, 77, 93, 109, \dots \pmod{16}$$

$$x \equiv 5 \pmod{14} = 5, 19, 33, 47, 61, 75, 89, 103, \dots \pmod{14}$$

Unsur persekutuan dari kedua kongruensi linier tersebut adalah 61, sehingga:

$$x \equiv 61 \pmod{16} \text{ dan } x \equiv 61 \pmod{14}$$

dan sesuai dengan Teorema 3.6 (b), $x \equiv 61 \pmod{[16,14]} \equiv 61 \pmod{112}$.

Contoh 4.10

Sistem kongruensi linier simultan $x \equiv 15 \pmod{51}$ dan $x \equiv 7 \pmod{42}$ tidak mempunyai selesaian sebab 15 tidak kongruen 7 modulo $(51,42) = 3$.

Meskipun sederhana dan mudah, cara biasa menjadi semakin sulit dan tidak efisien jika banyaknya kongruensi linier bertambah banyak, yaitu barisan atau daftar bilangan yang dibuat menjadi panjang.

Cara Iterasi

Makna iterasi memuat adanya langkah atau proses berulang. Ini berarti bahwa langkah berikutnya dikerjakan serupa setelah langkah sebelumnya

dilakukan. Sebagai ilustrasi, jika ada tiga kongruensi linier yang simultan, maka dua kongruensi diselesaikan lebih dahulu, sehingga diperoleh selesaian, dilanjutkan dengan penyelesaian kongruensi ketiga dengan selesaian dua kongruensi yang telah dikerjakan.

Contoh 4.11

Selesaikan sistem kongruensi linier simultan $2x \equiv 3 \pmod{5}$, $3x \equiv 4 \pmod{7}$, dan $5x \equiv 8 \pmod{12}$.

Jawab:

Ketiga kongruensi belum memenuhi syarat “baku”, sehingga masing-masing perlu disesuaikan, diperoleh $x \equiv 4 \pmod{5}$, $x \equiv 3 \pmod{7}$, dan $x \equiv 4 \pmod{12}$.

Dari $x \equiv 4 \pmod{5}$ diperoleh $x = 4 + 5t$. Substitusi $x = 4 + 5t$ kepada

$x \equiv 3 \pmod{7}$ diperoleh $4 + 5t \equiv 3 \pmod{7}$, atau

$5t \equiv -1 \pmod{7} = 6 \pmod{7}$, sehingga $t \equiv 4 \pmod{7}$, atau $t = 4 + 7s$.

Dari substitusi $t = 4 + 7s$ kepada $x = 4 + 5t$ diperoleh

$x = 4 + 5(4 + 7s) = 24 + 35s$. Dengan demikian $x \equiv 24 \pmod{35}$.

Berikutnya kita akan menyelesaikan $x \equiv 24 \pmod{35}$ dan $x \equiv 4 \pmod{12}$.

$x \equiv 24 \pmod{35}$, berarti $x = 24 + 35s$.

Substitusi $x = 24 + 35s$ kepada $x \equiv 4 \pmod{12}$ diperoleh

$24 + 35s \equiv 4 \pmod{12}$, $11s \equiv 4 \pmod{12}$, atau $s \equiv 8 \pmod{12}$, sehingga

$s = 8 + 12r$.

Dari substitusi $s = 8 + 12r$ kepada $x = 24 + 35s$ diperoleh

$x = 24 + 35(8 + 12r) = 304 + 420s$. Dengan demikian $x \equiv 304 \pmod{420}$

Sebelum kita membicarakan cara China, marilah kita lihat suatu teorema yang diperlukan untuk membuktikan Teorema Sisa China.

Teorema 4.3

Jika $p_1 | q$, $p_2 | q$, dan $(p_1, p_2) = 1$, maka $p_1 p_2 | q$

Bukti:

Misalkan $(p_1, p_2) = 1$. Maka sesuai Teorema 2.12, $xp_1 + yp_2 = 1$ untuk suatu $x, y \in \mathbb{Z}$, sehingga $xp_1q + yp_2q = q$.

Karena $p_1 | q$ dan $p_2 | q$, maka sesuai Teorema 2.8, $p_1p_2 | p_2q$ dan $p_1p_2 | p_1q$.

Selanjutnya, dari $p_1p_2 | p_2q$ dan $p_1p_2 | p_1q$ sesuai Teorema 2.1, $p_1p_2 | yp_2q$ dan $p_1p_2 | xp_2q$, dan berdasarkan Teorema 2.4, $pr | xpq + yqr$, atau $pr | q$.

Teorema 4.4.

Jika $p_1 | q, p_2 | q, \dots, p_r | q$, dan $(p_1, p_2, \dots, p_r) = 1$, maka $p_1p_2 \dots p_r | q$

Buktikan!**Cara China**

Masalah kongruensi linier muncul pada awal abad satu, dan dapat ditemukan di dalam aritmetika matematisi China yang bernama Sun-Tsu (Rosen, 1993:136). Cara China untuk menyelesaikan sistem kongruensi linier didasarkan pada suatu Teorema yang disebut **Teorema Sisa China**, di mana pasangan dari setiap dua modulo dari kongruensi adalah relatif prima.

Teorema 4.5. Teorema Sisa China

Ditentukan bahwa m_1, m_2, \dots, m_r adalah bilangan-bilangan bulat positif yang setiap pasang adalah relatif prima, dan a_1, a_2, \dots, a_r adalah sebarang r bilangan bulat.

Maka sistem kongruensi linier simultan :

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_r \pmod{m_r}$$

mempunyai suatu selesaian yang tunggal modulo $M = m_1.m_2 \dots m_r$

Bukti:

Misalkan $M = m_1.m_2 \dots m_r$. Ambil $M_i = M/m_i$, maka $m_i | M$ sehingga $(M_i, m_i) = 1$ dengan $1 \leq i \leq r$. Sesuai dengan Teorema 4.1, karena $(M_i, m_i) = 1$, maka tentu ada satu $b_i \in \mathbb{Z}$ sedemikian hingga $M_i b_i \equiv 1 \pmod{m_i}$, dan $M_i b_i \equiv 0 \pmod{m_j}$ jika $i \neq j$.

Ambil $x = M_1 b_1 a_2 + M_2 b_2 a_2 + \dots + M_r b_r a_r$, maka x adalah suatu selesaian simultan dari r kongruensi linier. Untuk menunjukkan hal ini, kita harus membuktikan bahwa $wa_i x \equiv a_i \pmod{m_i}$ untuk $i = 1, 2, \dots, r$

$$\begin{aligned} x &= M_1 b_1 a_2 + M_2 b_2 a_2 + \dots + M_r b_r a_r \\ &\equiv (M_1 b_1 a_1 + M_2 b_2 a_2 + \dots + M_i b_i a_i + \dots + M_r b_r a_r) \pmod{m_i} \\ &= (0.a_1 + 0.a_2 + \dots + 1.a_i + \dots + 0.a_r) \pmod{m_i} \\ x &\equiv a_i \pmod{m_i}, \quad i = 1, 2, \dots, r \end{aligned}$$

Untuk menunjukkan ketunggalan selesaian, dimisalkan ada dua selesaian yaitu x_0 dan x_1 , maka $x_0 \equiv x_1 \equiv a_i \pmod{m_i}$, yaitu $x_0 \equiv x_1 \pmod{m_i}$, atau $m_i | x_0 - x_1$.

Dengan demikian $m_1 | x_0 - x_1$, $m_2 | x_0 - x_1, \dots, m_r | x_0 - x_1$, dan sesuai dengan Teorema 4.4, $m_1 m_2 \dots m_r | x_0 - x_1$, atau $M | x_0 - x_1$, berarti $x_0 \equiv x_1 \pmod{M}$. Jadi selesaian simultan dari r kongruensi linier adalah tunggal dengan modulo m .

Contoh 4.12

Selesaikan sistem kongruensi linier simultan $x \equiv 5 \pmod{8}$, $x \equiv 3 \pmod{7}$, dan $x \equiv 4 \pmod{9}$.

Jawab:

$$a_1 = 5, \quad a_2 = 3, \quad a_3 = 4, \quad m_1 = 8, \quad m_2 = 7, \quad \text{dan } m_3 = 9$$

$$(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$$

$$M = m_1 m_2 m_3 = 8 \cdot 7 \cdot 9 = 504$$

$$(M/m_1)b_1 \equiv 1 \pmod{m_1}, \text{ maka } 7.9b_1 \equiv 1 \pmod{8}, \text{ sehingga } b_1 = 7$$

$$(M/m_2)b_2 \equiv 1 \pmod{m_2}, \text{ maka } 8.9b_2 \equiv 1 \pmod{7}, \text{ sehingga } b_2 = 4$$

$$(M/m_3)b_3 \equiv 1 \pmod{m_3}, \text{ maka } 8.7b_3 \equiv 1 \pmod{9}, \text{ sehingga } b_3 = 5$$

$$\text{Jadi } x = 7.9.7.5 + 8.9.4.3 + 8.7.5.4 = 4189$$

$$x \equiv 157 \pmod{504}$$

Contoh 4.13

Selesaikan sistem kongruensi linier simultan $3x \equiv 2 \pmod{5}$, $4x \equiv 3 \pmod{7}$, $8x \equiv 5 \pmod{9}$, dan $4x \equiv 7 \pmod{11}$

Jawab:

Masing-masing kongruensi linier perlu diubah menjadi kongruensi lain dengan koefisien x adalah 1 :

$$3x \equiv 2 \pmod{5}, \text{ maka } x \equiv 4 \pmod{5}$$

$$4x \equiv 3 \pmod{7}, \text{ maka } x \equiv 6 \pmod{7}$$

$$8x \equiv 5 \pmod{9}, \text{ maka } x \equiv 4 \pmod{9}$$

$$4x \equiv 7 \pmod{11}, \text{ maka } x \equiv 10 \pmod{11}$$

$$a_1 = 4, a_2 = 6, a_3 = 4, a_4 = 10, m_1 = 5, m_2 = 7, \text{ dan } m_3 = 9, m_4 = 11$$

$$(m_1, m_2) = (m_1, m_3) = (m_1, m_4) = (m_2, m_3) = (m_2, m_4) = (m_3, m_4) = 1$$

$$M = m_1 m_2 m_3 m_4 = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$$

$$(M/m_1)b_1 \equiv 1 \pmod{m_1}, \text{ maka } 7 \cdot 9 \cdot 11 b_1 \equiv 1 \pmod{5}, \text{ sehingga } b_1 = 2$$

$$(M/m_2)b_2 \equiv 1 \pmod{m_2}, \text{ maka } 5 \cdot 9 \cdot 11 b_2 \equiv 1 \pmod{7}, \text{ sehingga } b_2 = 3$$

$$(M/m_3)b_3 \equiv 1 \pmod{m_3}, \text{ maka } 5 \cdot 7 \cdot 11 b_3 \equiv 1 \pmod{9}, \text{ sehingga } b_3 = 4$$

$$(M/m_4)b_4 \equiv 1 \pmod{m_4}, \text{ maka } 5 \cdot 7 \cdot 9 b_4 \equiv 1 \pmod{11}, \text{ sehingga } b_4 = 8$$

$$\text{Jadi } x = 7 \cdot 9 \cdot 11 \cdot 2 \cdot 4 + 5 \cdot 9 \cdot 11 \cdot 3 \cdot 6 + 5 \cdot 7 \cdot 11 \cdot 4 \cdot 4 + 5 \cdot 7 \cdot 9 \cdot 8 \cdot 10 = 4581$$

$$x \equiv 769 \pmod{3465}$$

Tugas

Setelah banyak mempelajari tentang bahan paparan pada Kegiatan Belajar 1 ini, maka cobalah jelaskan atau uraikan bagaimana cara menyelesaikan suatu sistem kongruensi linier simultan yang dapat diselesaikan tetapi tidak semua pasangan modulo adalah relatif prima.

Berikutnya, dari suatu kongruensi linier $ax \equiv b \pmod{m}$, pilih suatu nilai m lebih dari 10000, nilai a lebih dari 1000, dan nilai b lebih dari 10, sedemikian hingga $(a, m) > 1$ dan $(a, m) \mid b$. Selesaikan kongruensi linier ini.

Petunjuk Jawaban Tugas

Bagian dari kongruensi-kongruensi linier yang memenuhi syarat $(m_i, m_j) = 1$ untuk $i \neq j$ diselesaikan dengan Teorema Sisa China, dan bagian dari kongruensi-kongruensi yang lain diselesaikan dengan iterasi, kemudian gabungannya diselesaikan dengan memilih cara yang memungkinkan untuk digunakan.

Pilih suatu kongruensi $3375x \equiv 30 \pmod{21480}$. Gunakan Algoritma Euclides untuk mencari $(3375, 21480)$ sehingga diperoleh 15. Karena 15 membagi 30, maka kongruensi linier mempunyai selesaian. Selesaikan dengan cara bertahap sehingga diperoleh:

$$x \equiv 1362, 2794, \dots, 21410 \pmod{21480}$$



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Selesaikan kongruensi linier $19x \equiv 1 \pmod{140}$ menggunakan Teorema Sisa China!
- 2) Selesaikan kongruensi linier $29393x \equiv 4743 \pmod{2805}$!
- 3) Selesaikan sistem kongruensi linier simultan $2x \equiv 8 \pmod{20}$ dan $3x \equiv 2 \pmod{7}$
- 4) Selesaikan sistem kongruensi linier simultan $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{7}$, dan $x \equiv 2 \pmod{11}$
- 5) Seorang gadis membawa sekeranjang telur. Jika telur-telur itu dihitung dua-dua, maka akan tertinggal satu telur. Jika telur-telur itu dihitung tiga-tiga, maka akan tertinggal dua telur. Jika dilanjutkan dengan menghitung lima-lima dan tujuh-tujuh, maka secara berturut-turut akan tertinggal empat telur dan enam telur. Tidak ada telur yang tertinggal jika dihitung sebelas-sebelas. Berapa banyaknya telur minimal di dalam keranjang?

Petunjuk Jawaban Latihan

- 1) $140 = 4 \cdot 5 \cdot 7$ dan $(4,5) = (4,7) = (5,7) = 1$, sehingga kongruensi $19x \equiv 30 \pmod{140}$ dapat dipecah menjadi sistem kongruensi linier simultan $19x \equiv 30 \pmod{4}$, $19x \equiv 30 \pmod{5}$, dan $19x \equiv 30 \pmod{7}$

Masing-masing kongruensi linier secara berturut-turut diubah menjadi $x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{5}$, dan $x \equiv 3 \pmod{7}$.

$$35b_1 \equiv 1 \pmod{4}, \text{ maka } b_1 = 3$$

$$28b_2 \equiv 1 \pmod{5}, \text{ maka } b_2 = 2$$

$$20b_3 \equiv 1 \pmod{7}, \text{ maka } b_3 = 6$$

$$x = 35 \cdot 3 \cdot 3 + 28 \cdot 2 \cdot 4 + 20 \cdot 6 \cdot 3 = 899 \equiv 59 \pmod{140}$$

- 2) $29393x \equiv 4743 \pmod{2805}$ diubah menjadi $1343x \equiv 1938 \pmod{2805}$

$$2805 = 2 \cdot 1343 + 119$$

$$1343 = 11 \cdot 119 + 34$$

$$119 = 3 \cdot 34 + 17$$

$$34 = 2 \cdot 17 + 0$$

$(1343, 2845) = 17$ dan $17 \mid 1938$, berarti terdapat 17 selesaian

$$1343x \equiv 1938 \pmod{2805}$$

$$\frac{79x \equiv 114 \pmod{165}}{165y \equiv -114 \pmod{79}} \rightarrow x_0 = \frac{165 \cdot 74 + 114}{79} = 156$$

$$165y \equiv -114 \pmod{79}$$

$$\frac{7y \equiv 44 \pmod{79}}{79z \equiv -44 \pmod{7}} \rightarrow y_0 = \frac{79 \cdot 6 + 44}{7} = 74$$

$$79z \equiv -44 \pmod{7}$$

$$2z \equiv 5 \pmod{7} \rightarrow z_0 = 6$$

Jadi $x \equiv 156, 321, \dots, 2796 \pmod{2805}$

- 3) $2x \equiv 8 \pmod{20}$, maka $x \equiv 4 \pmod{20}$ dan $x \equiv 14 \pmod{20}$

$$3x \equiv 2 \pmod{7}, \text{ maka } x \equiv 3 \pmod{7}$$

Dari kongruensi linier simultan $x \equiv 4 \pmod{20}$ dan $x \equiv 3 \pmod{7}$, dengan cara biasa atau cara iterasi dapat diperoleh $x \equiv 24 \pmod{140}$

Dari kongruensi linier simultan $x \equiv 14 \pmod{20}$ dan $x \equiv 3 \pmod{7}$, dengan cara biasa atau cara iterasi dapat diperoleh $x \equiv 94 \pmod{140}$

- 4) Dari $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{4}$, dan $x \equiv 1 \pmod{6}$, dapat ditentukan bahwa $x \equiv 1 \pmod{[2,3,4,5]}$, atau $x \equiv 1 \pmod{60}$.

Selanjutnya, dari $x \equiv 2 \pmod{7}$, dan $x \equiv 2 \pmod{11}$ dapat ditentukan bahwa $x \equiv 2 \pmod{77}$.

Dengan demikian $77b_1 \equiv 1 \pmod{60}$ dan $60b_2 \equiv 1 \pmod{77}$, sehingga diperoleh $b_1 = 53$ dan $b_2 = 9$

Jadi $x = 77.53.1 + 60.9.2 = 5161 \equiv 541 \pmod{4620}$.

- 5) Misalkan banyaknya telur sekeranjang adalah x , maka: $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 2 \pmod{7}$, dan $x \equiv 0 \pmod{11}$.

Dari $x \equiv 2 \pmod{3}$, $x \equiv 2 \pmod{5}$, dan $x \equiv 2 \pmod{7}$ dapat ditentukan bahwa $x \equiv 2 \pmod{105}$

Dengan demikian dapat ditentukan suatu sistem kongruensi linier simultan $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{105}$ dan $x \equiv 0 \pmod{11}$ kemudian dapat dicari:

$$105.11b_1 \equiv 1 \pmod{2}, \text{ atau } b_1 = 1$$

$$2.11b_2 \equiv 1 \pmod{105}, \text{ atau } b_2 = 43$$

$$105.2b_3 \equiv 1 \pmod{11}, \text{ atau } b_3 = 1$$

Jadi $x = 105.11.1.1 + 2.11.43.2 + 105.2.1.0 = 3047 \equiv 737 \pmod{2310}$

Banyaknya telur minimal dalam keranjang adalah 737.

Jika tidak dibatasi oleh minimal, maka jawaban yang diperoleh banyak, yaitu: $737, 737 + 2310, 737 + 2.2310, \dots, 737 + k.2310$ dengan $k \in \mathbb{Z}^+$.



Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep kongruensi linier, cara menyelesaikan kongruensi linier, konsep sistem kongruensi linier simultan, dan cara menyelesaikan sistem kongruensi linier simultan.

1. **Definisi 4.1** tentang banyaknya selesaian kongruensi.
2. **Definisi 4.2** tentang kongruensi linier simultan satu variabel.
3. Tiga hal yang perlu diperhatikan dalam menyelesaikan kongruensi linier:
 - a) $ax \equiv ay \pmod{m}$ jika $(a,m) = 1$;
 - b) $ax \equiv ay \pmod{m}$ jika $(a,m) \neq 1$;
 - c) $ax \equiv b \pmod{m}$ untuk nilai-nilai a , b , dan m yang relatif besar.
4. **Definisi 4.3** tentang sistem kongruensi linier simultan.
5. **Teorema 4.2.**

Sistem kongruensi linier simultan:

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

dapat diselesaikan jika dan hanya jika $a_1 \equiv a_2 \pmod{(m_1, m_2)}$.

6. Cara-cara menyelesaikan sistem kongruensi linier simultan: cara biasa, cara iterasi, dan cara China
7. **Teorema 4.3**

Jika $p_1 | q, p_2 | q$, dan $(p_1, p_2) = 1$, maka $p_1 p_2 | q$

8. **Teorema 4.4**

Jika $p_1 | q, p_2 | q, \dots, p_r | q$, dan $(p_1, p_2, \dots, p_r) = 1$, maka $p_1 p_2 \dots p_r | q$

9. **Teorema 4.5.**

Teorema Sisa China

Ditentukan bahwa m_1, m_2, \dots, m_r adalah bilangan-bilangan bulat positif yang setiap pasang adalah relatif prima, dan a_1, a_2, \dots, a_r adalah sebarang r bilangan bulat. Sistem kongruensi linier simultan:

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_r \pmod{m_r}$$

mempunyai suatu selesaian yang tunggal modulo $M = m_1 \cdot m_2 \dots m_r$



TES FORMATIF 1

1) Skor 20

Selesaikan kongruensi linier $23x \equiv 17 \pmod{180}$ dengan dua cara:

- (a) cara penyelesaian kongruensi linier
- (b) cara penyelesaian sistem kongruensi linier simultan

2) Skor 20

Sekelompok perompak terdiri dari 13 orang akan membagikan sekantung butir berlian.

Dalam usaha pembagian pertama, ternyata tersisa 5 butir berlian, dan karena dirasa tidak adil, terjadi perkelahian dan 4 perompak terbunuh.

Dalam usaha pembagian kedua, ternyata tersisa 6 butir berlian, dan karena dirasa masih belum adil, terjadi perkelahian dan 2 perompak terbunuh.

Dalam usaha pembagian ketiga, ternyata tersisa 3 butir berlian, dan perkelahian kembali terjadi dengan 2 orang terbunuh.

Dalam usaha pembagian keempat, ternyata tidak ada butir berlian yang tersisa, semua perompak yang masih hidup menerima bagian yang banyaknya sama.

Berapa banyaknya butir berlian minimal dalam kantung?

3) Skor 20

Selesaikan sistem kongruensi linier simultan $5x \equiv 1 \pmod{6}$,

$$3x \equiv 10 \pmod{11}, 2x \equiv 7 \pmod{13}, 3x \equiv 4 \pmod{5}, 4x \equiv 3 \pmod{7}$$

4) Skor 10

Selesaikan sistem kongruensi linier simultan $9x \equiv 4 \pmod{14}$,

$$5x \equiv 17 \pmod{21} \text{ dan } 7x \equiv 10 \pmod{30}$$

5) Skor 20

Carilah suatu bilangan kelipatan 13 yang bersisa 2 jika dibagi 3,5,7, dan 8, serta bersisa 10 jika dibagi 17.

6) Skor 10

Selesaikan $26733x \equiv 133 \pmod{54340}$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2

Sistem Kongruensi Linier

ada pembahasan tentang Aljabar (biasa), salah satu topik di dalamnya adalah sistem persamaan linier. Dua persamaan linier dua variabel, tiga persamaan linier tiga variabel, atau n persamaan linier n variabel membentuk suatu sistem persamaan linier.

Penyelesaian sistem persamaan linier dapat dilakukan dengan cara eliminasi, cara substitusi, cara matriks atau cara determinan. Masing-masing cara mempunyai langkah-langkah dan aturan-aturan tertentu dalam memperoleh selesaian.

Serupa dengan pembahasan di Aljabar, salah satu topik di Teori Bilangan adalah sistem kongruensi linier. Sistem kongruensi linier n variabel adalah gabungan dari n kongruensi linier bermodulo sama yang masing-masing memuat paling banyak n variabel.

Penyelesaian sistem kongruensi linier dapat dilakukan dengan substitusi, eliminasi, atau dengan menggunakan matriks dan determinan.

Marilah kita mulai pembahasan tentang sistem kongruensi linier ini dengan sebuah peragaan, yaitu kita akan mencari semua bilangan bulat x dan y sehingga:

$$2x + 3y \equiv 7 \pmod{11}$$

$$3x + 5y \equiv 6 \pmod{11}$$

Jika kita menggunakan cara **substitusi**, maka $2x + 3y \equiv 7 \pmod{11}$ diubah menjadi kongruensi $2x \equiv 7 - 3y \pmod{11}$ atau $3y \equiv 2x \pmod{11}$, kemudian disubstitusikan ke kongruensi $3x + 5y \equiv 6 \pmod{11}$. Misalkan kita memilih $2x \equiv 7 - 3y \pmod{11}$, maka kita kalikan kedua ruas kongruensi dengan 6, sehingga diperoleh:

$$12x \equiv 42 - 18y \pmod{11}, \text{ atau } x \equiv 9 - 7y \pmod{11}.$$

Substitusi $x \equiv 9 - 7y \pmod{11}$ ke dalam $3x + 5y \equiv 6 \pmod{11}$ diperoleh:

$$3(9 - 7y) + 5y \equiv 6 \pmod{11}, \quad \text{atau} \quad -16y \equiv -21 \pmod{11}, \quad \text{atau}$$

$$6y \equiv 1 \pmod{11}, \text{ atau } y \equiv 2 \pmod{11}$$

Dengan demikian $x \equiv 9 - 7.2 \pmod{11} = -5 \pmod{11} = 6 \pmod{11}$.

Jadi sistem kongruensi linier mempunyai selesaian $x \equiv 6 \pmod{11}$ dan $y \equiv 2 \pmod{11}$.

Selesaian x dan y yang diperoleh dapat diperiksa kebenarannya dengan mensubstitusikannya ke dalam masing-masing kongruensi linier.

Jika kita menggunakan cara eliminasi, maka kita perlu menetapkan lebih dahulu yang dieliminasi, yaitu x atau y . Misalkan kita tetapkan y dieliminasi, maka kongruensi pertama dikalikan 5 dan kongruensi kedua dikalikan 3, sehingga diperoleh:

$$10x + 15y \equiv 35 \pmod{11}$$

$$9x + 15y \equiv 18 \pmod{11}$$

Jika kongruensi pertama dikurangi kongruensi kedua, maka diperoleh:

$$x \equiv 17 \pmod{11}, \text{ atau } x \equiv 6 \pmod{11}$$

Dengan jalan yang sama, jika x yang dieliminasi, maka kongruensi pertama dikalikan 3 dan kongruensi kedua dikalikan 2, sehingga diperoleh:

$$6x + 9y \equiv 21 \pmod{11}$$

$$6x + 10y \equiv 12 \pmod{11}$$

Jika kongruensi kedua dikurangi kongruensi pertama, maka diperoleh:

$$y \equiv -9 \pmod{11}, \text{ maka } y \equiv 2 \pmod{11}$$

Dengan cara substitusi ini kita dapat menyelesaikan sebarang sistem kongruensi linier dua variabel.

Teorema 4.6.

Ditentukan $a, b, c, d, e, f, m \in \mathbb{Z}$, $m > 0$, dan $\Delta = ad - bc$ sehingga $(\Delta, m) = 1$.

Maka sistem kongruensi linier:

$$ax + by \equiv e \pmod{m}$$

$$cx + dy \equiv f \pmod{m}$$

mempunyai suatu selesaian tunggal yaitu:

$$x \equiv \bar{\Delta}(de - bf)(\pmod{m})$$

$$y \equiv \bar{\Delta}(af - ce)(\pmod{m})$$

di mana $\bar{\Delta}$ adalah inverse dari Δ modulo m .

Bukti:

Jika y akan dieliminasi, maka kongruensi pertama dikalikan d dan kongruensi kedua dikalikan b , sehingga diperoleh:

$$adx + bdy \equiv de \pmod{m}$$

$$bcx + bdy \equiv bf \pmod{m}$$

Jika kongruensi pertama dikurangi kongruensi kedua, maka diperoleh:

$$(ad - bc)x \equiv (de - bf) \pmod{m} \quad \text{atau} \quad \Delta x \equiv (de - bf) \pmod{m} \quad \text{sehingga}$$

$$\bar{\Delta}\Delta x \equiv \bar{\Delta}(de - bf) \pmod{m}$$

Karena $\bar{\Delta}\Delta \equiv 1 \pmod{m}$, maka diperoleh $x \equiv \bar{\Delta}(de - bf) \pmod{m}$

Selanjutnya, jika x akan dieliminasi, maka kongruensi pertama dikalikan c dan kongruensi kedua dikalikan a , sehingga diperoleh:

$$acx + bcy \equiv ce \pmod{m}$$

$$acx + ady \equiv af \pmod{m}$$

Jika kongruensi kedua dikurangi kongruensi pertama, maka diperoleh:

$$(ad - bc)y \equiv (af - ce) \pmod{m} \quad \text{atau} \quad \Delta y \equiv (af - ce) \pmod{m} \quad \text{sehingga}$$

$$\bar{\Delta}\Delta y \equiv \bar{\Delta}(af - ce) \pmod{m}$$

Karena $\bar{\Delta}\Delta \equiv 1 \pmod{m}$, maka diperoleh $y \equiv \bar{\Delta}(af - ce) \pmod{m}$.

Contoh 4.14

Selesaikan sistem kongruensi linier:

$$4x - 7y \equiv 6 \pmod{17}$$

$$5x + 2y \equiv 9 \pmod{17}$$

Jawab:

$$\Delta = 4.2 - (-7)(5) = 43 \equiv 9 \pmod{17} \quad \text{dan} \quad \bar{\Delta} = 2, \quad \text{sebab} \quad \bar{\Delta}\Delta = 18 \equiv 1 \pmod{17}$$

Dengan demikian

$$x \equiv \bar{\Delta}(de - bf) \pmod{m} \equiv 2(2.6 + 7.9) \pmod{17} \equiv 14 \pmod{17} \quad \text{dan}$$

$$y \equiv \bar{\Delta}(af - ce) \pmod{m} \equiv 2(4.9 - 5.6) \pmod{17} \equiv 12 \pmod{17}$$

Pemeriksaan: jika $x = 14$ dan $y = 12$ disubstitusikan pada masing-masing

$$\text{kongruensi diperoleh } 4x - 7y = 56 - 84 = -28 \equiv 6 \pmod{17}$$

$$\text{dan } 5x + 2y = 5.14 + 2.12 = 70 + 24 = 94 \equiv 9 \pmod{17}$$

Untuk menyelesaikan sistem kongruensi linier 3 variabel atau lebih dengan cara eliminasi memerlukan langkah-langkah yang lebih panjang karena tahapan memperoleh x melalui eliminasi variabel-variabel yang lain.

Cara menyelesaikan sistem kongruensi linier n variabel yang relatif mudah adalah dengan menggunakan Aljabar Linier, yaitu persamaan matriks.

Definisi 4.3

Ditentukan A dan B adalah matriks-matriks berukuran $p \times q$ dengan unsur-unsur bulat, a_{ij} merupakan unsur A pada baris ke- i kolom ke- j , dan b_{ij} merupakan unsur B pada baris ke- i kolom ke- j .

A disebut kongruen dengan B modulo m jika $a_{ij} \equiv b_{ij} \pmod{m}$ untuk semua pasangan (i, j) dengan $1 \leq i \leq n$ dan $1 \leq j \leq n$, ditulis $A \equiv B \pmod{m}$.

Contoh 4.15

$$(a) \begin{bmatrix} 34 & 46 \\ 23 & 29 \end{bmatrix} \equiv \begin{bmatrix} 8 & 7 \\ 10 & 3 \end{bmatrix} \pmod{13}$$

$$(b) \begin{bmatrix} -20 & 5 & 39 \\ 15 & 7 & 58 \\ -62 & 12 & 41 \end{bmatrix} \equiv \begin{bmatrix} 1 & 5 & 4 \\ 1 & 0 & 2 \\ 1 & 5 & 6 \end{bmatrix} \pmod{7}$$

Teorema 4.7.

Jika A dan B adalah matriks-matriks berukuran $p \times q$, $A \equiv B \pmod{m}$, dan C adalah suatu matriks berukuran $q \times r$, D adalah suatu matriks berukuran $r \times p$, semuanya dengan unsur-unsur bulat, maka $AC \equiv BC \pmod{m}$ dan $DA \equiv DB \pmod{m}$

Bukti:

Misalkan unsur-unsur A adalah a_{ij} , unsur-unsur B adalah b_{ij} dengan $1 \leq i \leq p$ dan $1 \leq j \leq q$, dan unsur-unsur C adalah c_{ij} dengan $1 \leq i \leq q$ dan $1 \leq j \leq r$.

Unsur AC dan BC pada baris ke- i kolom ke- j berturut-turut adalah:

$$\sum_{k=1}^q a_{ik} c_{kj} \text{ dan } \sum_{k=1}^q b_{ik} c_{kj}, 1 \leq i \leq p \text{ dan } 1 \leq j \leq r$$

Diketahui bahwa $A \equiv B \pmod{m}$, maka sesuai Definisi 4.3,

$a_{ik} \equiv b_{ik} \pmod{m}$ untuk semua i dan k , yaitu:

$$\sum_{k=1}^q a_{ik} c_{kj} = \sum_{k=1}^q b_{ik} c_{kj}, 1 \leq i \leq p \text{ dan } 1 \leq j \leq r$$

Akibatnya, $AC \equiv BC \pmod{m}$.

Dengan jalan yang sama, buktikan $DA \equiv DB \pmod{m}$.

Contoh 4.16

Diketahui: A dan B keduanya berukuran 3×2 , $A = \begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix}$ dan $B = \begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix}$

C berukuran 2×4 , D berukuran 2×3 , $C = \begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix}$ dan $D = \begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \end{bmatrix}$

$$AC = \begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix} = \begin{bmatrix} 78 & 72 & 78 & 93 \\ 76 & 82 & 98 & 83 \\ 75 & 101 & 134 & 69 \end{bmatrix} \equiv \begin{bmatrix} 6 & 0 & 6 & 5 \\ 4 & 2 & 2 & 3 \\ 3 & 5 & 6 & 5 \end{bmatrix} \pmod{8}$$

$$BC = \begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix} = \begin{bmatrix} 22 & 16 & 14 & 29 \\ 20 & 26 & 34 & 19 \\ 43 & 37 & 38 & 53 \end{bmatrix} \equiv \begin{bmatrix} 6 & 0 & 6 & 5 \\ 4 & 2 & 2 & 3 \\ 3 & 5 & 6 & 5 \end{bmatrix} \pmod{8}$$

$$DA = \begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix} = \begin{bmatrix} 28 & 58 \\ 1 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix} \pmod{8}$$

$$DB = \begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \\ 4 & 7 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 28 & 58 \\ 9 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} (\text{mod } 8)$$

Perhatikan bahwa $AC \equiv BC (\text{ mod } 8)$ dan $DA \equiv DB (\text{ mod } 8)$

Marilah sekarang kita lihat cara memperoleh selesaian sistem kongruensi linier dengan menggunakan persamaan matriks, suatu cara yang serupa dengan cara memperoleh selesaian sistem persamaan linier di dalam Aljabar Linier.

Secara umum, suatu sistem kongruensi linier dapat dinyatakan sebagai:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \equiv b_1 (\text{ mod } m)$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \equiv b_2 (\text{ mod } m)$$

.

.

.

$$a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n \equiv b_n (\text{ mod } m)$$

Dalam bentuk persamaan matriks, sistem kongruensi linier ini dapat ditulis dengan:

$$AX \equiv B (\text{ mod } m)$$

di mana:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \text{dan } B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Contoh 4.17

Suatu sistem kongruensi linier :

$$2x + 3y + 4z \equiv 2 (\text{ mod } 11)$$

$$3x + y + 2z \equiv 7 (\text{ mod } 11)$$

$$4x + 2y + z \equiv 3 (\text{ mod } 11)$$

dapat dinyatakan sebagai:

$$\begin{bmatrix} 2 & 3 & 4 \\ 3 & 1 & 2 \\ 4 & 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \\ 3 \end{bmatrix} (\text{mod } 11)$$

Selesaian sistem kongruensi linier :

$$AX \equiv B \pmod{m}$$

diperoleh dari :

$$A^{-1}AX \equiv A^{-1}B \pmod{m}, A^{-1} \text{ adalah inverse } A \text{ modulo } m$$

$$IX \equiv A^{-1}B \pmod{m}, I \text{ adalah matriks identitas}$$

$$X \equiv A^{-1}B \pmod{m}$$

dengan A^{-1} didefinisikan sebagai berikut:

Definisi 4.4

Jika A dan A^{-1} adalah matriks-matriks dengan unsur-unsur bilangan bulat, dan berukuran $n \times n$, serta $A^{-1}A \equiv AA^{-1} \equiv I \pmod{m}$, dengan:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \text{ adalah matriks identitas berderajat } n,$$

maka A^{-1} disebut inverse matriks A modulo m .

Teorema 4.8

Diketahui suatu matriks:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

dengan unsur-unsur bilangan bulat, $\Delta = \det A = ad - bc$, dan $(\Delta, m) = 1$.

Maka inversi matriks A modulo m adalah:

$$A^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

dengan Δ^{-1} adalah inversi Δ modulo m .

Bukti:

Untuk membuktikan A^{-1} adalah inversi A modulo m , kita harus membuktikan bahwa $AA^{-1} \equiv A^{-1}A \pmod{m}$.

$$\begin{aligned} AA^{-1} &\equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv \Delta^{-1} \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} \\ &\equiv \Delta^{-1} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv 1 \pmod{m} \end{aligned}$$

Dengan jalan yang sama, buktikan bahwa $A^{-1}A \equiv I \pmod{m}$

Contoh 4.18.

Diketahui $A = \begin{bmatrix} 5 & 3 \\ 7 & 8 \end{bmatrix}$, dengan demikian $\Delta = 5.8 - 7.3 = 19$

Inversi dari $\Delta = 19$ modulo 11 adalah $\Delta^{-1} = 7$ sebab

$$\Delta\Delta^{-1} = 19.7 = 133 \equiv 1 \pmod{11}$$

Jadi inversi A adalah $A^{-1} = 7 \begin{bmatrix} 8 & -3 \\ -7 & 5 \end{bmatrix} = \begin{bmatrix} 56 & -21 \\ -49 & 35 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 6 & 2 \end{bmatrix} \pmod{11}$

Selanjutnya, seperti uraian yang telah kita pelajari dalam Aljabar Linier terutama pada topik matriks dan determinan, kita mengenal dan memahami tentang matriks adjoint dan rumusan mencari inversi matriks dengan menggunakan matriks adjoint dan determinan. Secara rinci Anda dipersilakan membaca ulang materi-materi itu, termasuk diantaranya minor dan kofaktor.

Definisi 4.5.

Ditentukan A adalah suatu matriks berukuran $n \times n$.

Adjoint dari matriks A , ditulis $\text{adj } A$, adalah suatu matriks berukuran $n \times n$ yang unsur-unsurnya adalah α_{ji} di mana α_{ij} sama dengan $(-1)^{i+j}$ dikalikan determinan suatu matriks yang diperoleh dengan menghapus semua unsur A pada baris ke- i dan kolom ke- j .

Teorema 4.9.

Jika A adalah suatu matriks berukuran $n \times n$ dan A bukan matriks nol, maka $A(\text{adj } A) = \Delta I$

Buktikan (lihat di buku-buku Aljabar Linier)

Teorema 4.10.

Jika A adalah suatu matriks berukuran $n \times n$ dan semua unsur-unsurnya adalah bilangan bulat, serta m adalah bilangan bulat positif sehingga $(\Delta, m) = 1$, maka inversi dari A adalah:

$$A^{-1} = \Delta^{-1} (\text{adj } A)$$

Bukti:

Karena $(\Delta, m) = 1$, maka $\Delta \neq 0$, dan sesuai Teorema 4.9, $A(\text{adj } A) = \Delta I$.

Selanjutnya, dari $(\Delta, m) = 1$ dapat ditentukan bahwa Δ mempunyai invers Δ^{-1} modulo m , sehingga:

$$A(\Delta^{-1})(\text{adj } A) \equiv A(\text{adj } A)(\Delta^{-1}) \equiv (\Delta I)\Delta^{-1} \equiv \Delta\Delta^{-1}I \equiv I \pmod{m}, \text{ dan}$$

$$\Delta^{-1}(\text{adj } A)A \equiv \Delta^{-1}(\text{adj } A \cdot A) \equiv \Delta^{-1}\Delta I \equiv I \pmod{m}$$

Jadi $\Delta^{-1}(\text{adj } A)$ adalah inversi A , atau $A^{-1} = \Delta^{-1}(\text{adj } A)$

Contoh 4.19.

Diketahui $A = \begin{bmatrix} 2 & 2 & -2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$, maka $\Delta = 4$, dan $\Delta^{-1} \equiv 3 \pmod{11}$

$$\begin{aligned}
 A^{-1} &= \Delta^{-1} (\text{adj } A) = 3 \begin{bmatrix} -1 & -14 & 10 \\ 2 & 12 & -8 \\ -1 & -2 & 2 \end{bmatrix} = \begin{bmatrix} -3 & -42 & 30 \\ 6 & 36 & -24 \\ -3 & -6 & 6 \end{bmatrix} \\
 &= \begin{bmatrix} 8 & 2 & 8 \\ 6 & 3 & 9 \\ 8 & 5 & 6 \end{bmatrix} \pmod{11}
 \end{aligned}$$

Pemeriksaan:

$$\begin{aligned}
 AA^{-1} &= \begin{bmatrix} 2 & 2 & -2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 8 & 2 & 8 \\ 6 & 3 & 9 \\ 8 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 12 & 0 & 22 \\ 44 & 23 & 44 \\ 66 & 33 & 67 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{11}
 \end{aligned}$$

Sekarang kita dapat menggunakan inverse A modulo m untuk menyelesaikan suatu kongruensi linier:

$$AX \equiv B \pmod{m} \text{ di mana } (\Delta, m) = 1.$$

Berdasarkan Teorema 4.10, karena $(\Delta, m) = 1$, maka A mempunyai invers, misalnya A^{-1} sehingga jika kedua ruas $AX \equiv B \pmod{m}$ dikalikan A^{-1} diperoleh:

$$\begin{aligned}
 A^{-1}(AX) &= A^{-1}B \pmod{m} \\
 (A^{-1}A)X &= A^{-1}B \pmod{m} \\
 IX &= A^{-1}B \pmod{m} \\
 X &= A^{-1}B \pmod{m}
 \end{aligned}$$

Dengan demikian selesaian kongruensi linier simultan adalah $X = A^{-1}B \pmod{m}$

Contoh 4.20.

Selesaikan sistem kongruensi linier:

$$x + 2y + z \equiv 4 \pmod{7}, \quad x - y + z \equiv 5 \pmod{7}, \quad 2x + 3y + z \equiv 1 \pmod{7}$$

Jawab:

$$\begin{bmatrix} 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 3 & 1 \end{bmatrix}, X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \text{ dan } B = \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix}$$

$$\Delta = 3, \text{ dan } (\Delta, 7) = (3, 7) = 1, \text{ maka } \Delta^{-1} \equiv 5 \pmod{7}$$

$$A^{-1} = \Delta^{-1} (\text{adj } A) = 5 \begin{bmatrix} -4 & 1 & 3 \\ 1 & -1 & 0 \\ 5 & 1 & -3 \end{bmatrix} = \begin{bmatrix} -20 & 5 & 15 \\ 5 & -5 & 0 \\ 25 & 5 & -15 \end{bmatrix} \equiv \begin{bmatrix} 1 & 5 & 1 \\ 5 & 2 & 0 \\ 4 & 5 & 6 \end{bmatrix}$$

$$X = A^{-1}B = \begin{bmatrix} 1 & 5 & 1 \\ 5 & 2 & 0 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 30 \\ 30 \\ 47 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 5 \end{bmatrix}$$

Tugas

Bacalah suatu buku tentang teori bilangan, misalnya *Elementary Number Theory and Its Applications* yang ditulis oleh Kenneth H. Rosen, dan diterbitkan oleh Addison-Wesley Publishing Company, carilah topik tentang Metode Monte Carlo.

Jelaskan topik itu terkait dengan masalah teori bilangan yang mana, bagaimana langkah-langkahnya, dan berilah paling sedikit satu contoh.

Petunjuk Jawaban Tugas

Metode Monte Carlo adalah suatu metode pemfaktoran yang didasarkan pada kongruensi dan dikembangkan oleh J.M. Pollard pada tahun 1974 (Rosen, 1993:156).

Ditentukan n adalah bilangan komposit yang relatif cukup besar dan p adalah faktor prima n yang terkecil. Keinginan kita adalah memilih bilangan-bilangan bulat: x_0, x_1, \dots, x_s sedemikian hingga mempunyai residu-residu non-negatif terkecil modulo n yang berbeda, tetapi tidak untuk kejadian yang sama modulo p .

Misalkan kita sudah temukan x_i dan x_j , $0 \leq i \leq j \leq s$ sehingga $x_i \equiv x_j \pmod{p}$ tetapi x_i tidak kongruen dengan x_j modulo n , maka $p | x_i - x_j$ tetapi n tidak membagi $x_i - x_j$ sehingga $(x_i - x_j, n)$ adalah faktor non-trivial dari n , dan dapat dicari dengan mudah menggunakan Algoritma Euclides.

Untuk mencari bilangan-bilangan bulat x_i dan x_j digunakan langkah-langkah:

- mulailah dengan suatu nilai awal (babit) x_0 yang dipilih secara random
- ambil suatu polinomial $f(x)$ dengan koefisien-koefisien bulat dan berderajat lebih dari 1.
- Hitunglah suku-suku x_k , $k = 1, 2, 3, \dots$ dengan menggunakan definisi rekursif:

$$x_{k+1} \equiv f(x_k) \pmod{n}, \quad 0 \leq x_{k+1} < n$$

- Polinomial $f(x)$ seharusnya mempunyai sifat bahwa barisan x_0, x_1, \dots, x_s mempunyai tingkah laku seperti barisan random yang diinginkan.

Sebagai peragaan, ambil $n = 8051$.

- ambil suatu nilai awal $x_0 = 2$
- ambil suatu polinomial $f(x) = x^2 + 1$
- Hitung x_k secara rekursif

$$x_0 = 2$$

$$x_1 = f(x_0) = f(2) = 2^2 + 1 = 5$$

$$x_2 = f(x_1) = f(5) = 5^2 + 1 = 26$$

$$x_3 = f(x_2) = f(26) = 26^2 + 1 = 677$$

$$x_4 = f(x_3) = f(677) = 677^2 + 1 \equiv 7474 \pmod{8051}$$

$$x_5 = f(x_4) = f(7474) = 7474^2 + 1 \equiv 2839 \pmod{8051}$$

$$x_6 = f(x_5) = f(2839) = 2839^2 + 1 \equiv 871 \pmod{8051}$$

dan seterusnya.

Berikutnya, berdasarkan definisi rekursif x_k , jika d adalah suatu bilangan bulat positif, dan $x_i \equiv x_j \pmod{d}$, maka :

$$x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \pmod{d}$$

Hal ini berarti barisan x_k bersifat periodik dengan periode $(j-i)$, $x_q \equiv x_r \pmod{j-i}$ dengan $q \geq i$ dan $r \geq j$, dan akibatnya, jika s adalah bilangan bulat positif kelipatan $j-i$, maka $x_s \equiv x_{2s} \pmod{d}$.

Untuk memperoleh suatu faktor dari n , kita cari FPB dari $x_{2k} - x_k$ dan $n, k = 1, 2, 3, \dots$, yaitu setelah kita memperoleh k yang mana $1 < x_{2k} - x_k < n$.

Secara praktis, apabila metode rho Pollard digunakan, polinomial yang sering dipilih adalah $f(x) = x^2 + 1$, dan nilai awal yang dipilih adalah $x_0 = 2$.

Contoh:

Dengan menggunakan metode rho Pollard (atau metode Monte Carlo), dengan $x_0 = 2$ dan polinomial pembangkit $f(x) = x^2 + 1$ untuk memperoleh faktor non-trivial dari suatu bilangan komposit $n = 8051$.

Jawab:

Dari hasil hitungan $x_0, x_1, x_2, x_3, x_4, x_5$, dan x_6 di atas, dan berdasarkan hitungan Algoritma Euclides, dapat ditentukan bahwa:

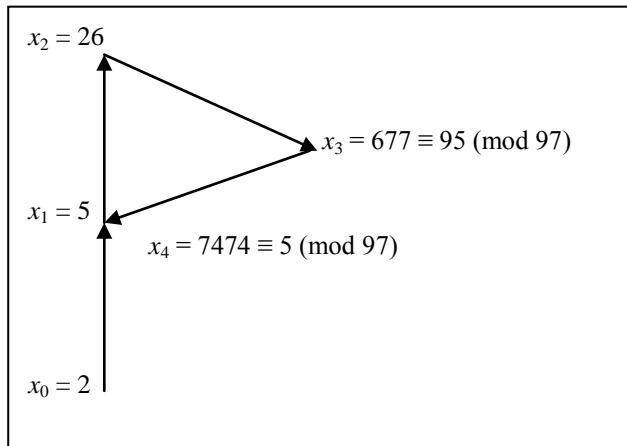
$$(x_2 - x_1, 8051) = (21, 8051) = 1$$

$$(x_4 - x_2, 8051) = (7448, 8051) = 1$$

$$(x_6 - x_3, 8051) = (194, 8051) = 97$$

Jadi 97 adalah suatu faktor dari 8051.

Tingkah laku periodik dari barisan x_i dengan $x_0 = 2$ dan $x_{i+1} = x_i^2 + 1 \pmod{97}$ dan $i \geq 1$, dapat terlihat seperti model berikut:

**LATIHAN**

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Selesaikan sistem kongruensi linier:

$$(a) \begin{aligned} x + 2y &\equiv 1 \pmod{5} \\ 2x + y &\equiv 1 \pmod{5} \end{aligned} \quad (b) \begin{aligned} x + 3y &\equiv 1 \pmod{5} \\ 3x + 4y &\equiv 1 \pmod{5} \end{aligned}$$

- 2) Carilah inversi matriks A modulo 7 jika:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

- 3) Selesaikan sistem kongruensi linier:

$$x + y \equiv 1 \pmod{7}$$

$$x + z \equiv 2 \pmod{7}$$

$$y + z \equiv 3 \pmod{7}$$

- 4) Selesaikan sistem kongruensi linier:

$$2x + 5y + 6z \equiv 3 \pmod{7}$$

$$2y + z \equiv 4 \pmod{7}$$

$$x + 2y + 3z \equiv 3 \pmod{7}$$

- 5) Carilah matriks T jika:

$$T \equiv \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 4 & 0 \\ 2 & 1 \end{bmatrix} \pmod{5}$$

dan semua unsur T adalah bilangan-bilangan bulat tidak negatif kurang dari 5

Petunjuk Jawaban Latihan

- 1) (a) Ada tiga pilihan cara menyelesaikan: substitusi, eliminasi, atau matriks. Misalkan digunakan cara substitusi.

$$\begin{aligned} x + 2y &\equiv 1 \pmod{5}, \text{ atau } x \equiv 1 - 2y \pmod{5}, \text{ substitusikan ke} \\ 2x + y &\equiv 1 \pmod{5} \text{ diperoleh } 2(1 - 2y) + y \equiv 1 \pmod{5}, \text{ atau} \\ -3y &\equiv -1 \pmod{5}, 2y \equiv 4 \pmod{5}, \text{ sehingga } y \equiv 2 \pmod{5}. \\ x &\equiv 1 - 2 \cdot 2 \pmod{5} \equiv -3 \pmod{5}, \text{ sehingga } x \equiv 2 \pmod{5} \end{aligned}$$

- (b) Misalkan digunakan cara eliminasi

x akan dieliminasi, maka kongruensi pertama dikalikan dengan 3, dan kongruensi kedua tetap:

$$3x + 9y \equiv 3 \pmod{5}$$

$$3x + 4y \equiv 2 \pmod{5}$$

Jika kongruensi pertama dikurangi kongruensi kedua diperoleh:

$$5y \equiv 1 \pmod{5}$$

Kongruensi tidak mempunyai selesaian sebab $(5,5) = 5$ tidak membagi 1

- 2) $\Delta = -2 \equiv 5 \pmod{7}$, maka $\Delta^{-1} \equiv 3 \pmod{7}$

$$A^{-1} = \Delta^{-1} (\text{adj } A) = 3 \begin{bmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -3 & -3 & 3 \\ -3 & 3 & -3 \\ 3 & -3 & -3 \end{bmatrix} \equiv \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{bmatrix}$$

- 3) Gunakan persamaan matriks untuk menyelesaikan

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \pmod{7} \text{ atau } AX \equiv B \pmod{7}$$

$$X \equiv A^{-1}B \pmod{7} \equiv \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \pmod{7} \equiv \begin{bmatrix} 21 \\ 22 \\ 23 \end{bmatrix} \pmod{7} \equiv \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

4) $\begin{bmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix} \pmod{7}$ atau $AX \equiv B \pmod{7}$

$$X \equiv A^{-1}B \pmod{7} \equiv \begin{bmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix} \pmod{7} \equiv \begin{bmatrix} 32 \\ 8 \\ 24 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 1 \\ 3 \end{bmatrix}$$

5) $T \equiv \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 4 & 0 \\ 2 & 1 \end{bmatrix} \pmod{5} \equiv \begin{bmatrix} 10 & 1 \\ 22 & 3 \end{bmatrix} \pmod{5} \equiv \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \pmod{5}$



Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep sistem kongruensi linier, cara menyelesaikan sistem kongruensi linier yang terdiri dari substitusi, eliminasi, dan matriks, dan metode rho Pollard atau metode Monte Carlo untuk mencari faktor prima suatu bilangan komposit dengan menggunakan kongruensi.

1. **Definisi 4.3** tentang dua matriks A dan B yang kongruen modulo m .
2. **Definisi 4.4** tentang inversi suatu matriks A modulo m .
3. **Definisi 4.5** tentang adjoint suatu matriks A modulo m .
4. **Teorema 4.6** tentang ketunggalan selesaian sistem kongruensi linier:

$$ax + by \equiv e \pmod{m}$$

$$cx + dy \equiv f \pmod{m}$$

jika $(\Delta, m) = 1$ dengan $\Delta = ad - bc$

5. **Teorema 4.7.**

Jika A dan B adalah matriks-matriks berukuran $p \times q$, $A \equiv B \pmod{m}$, dan C adalah suatu matriks berukuran $q \times r$, D adalah suatu matriks berukuran $r \times p$, semuanya dengan unsur-unsur bulat, maka $AC \equiv BC \pmod{m}$ dan $DA \equiv DB \pmod{m}$

6. Teorema 4.8.

Inversi matriks $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ adalah $A^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

7. Teorema 4.9.

Jika A adalah suatu matriks berukuran $n \times n$ dan A bukan matriks nol, maka $A(\text{adj } A) = \Delta I$.

8. Teorema 4.10.

Jika A adalah suatu matriks berukuran $n \times n$ dan semua unsur-unsurnya adalah bilangan bulat, serta m adalah bilangan bulat positif sehingga $(\Delta, m) = 1$, maka inversi dari A adalah:

$$A^{-1} = \Delta^{-1} (\text{adj } A)$$

**TES FORMATIF 2**

1) Skor 10

Selesaikan sistem kongruensi linier :

$$(a) 4x + y \equiv 2 \pmod{5}$$

$$2x + 3y \equiv 1 \pmod{5}$$

$$(b) 2x + 3y \equiv 5 \pmod{5}$$

$$x + 5y \equiv 6 \pmod{5}$$

2) Skor 20

Carilah inversi dari A modulo 7 jika:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{bmatrix}$$

3) Skor 20

Selesaikan sistem kongruensi linier:

$$x + y + z \equiv 1 \pmod{7}$$

$$x + y + w \equiv 1 \pmod{7}$$

$$x + z + w \equiv 1 \pmod{7}$$

$$y + z + w \equiv 1 \pmod{7}$$

4) Skor 10

Carilah banyaknya selesaian tidak kongruen dari sistem kongruensi linier:

$$2x + 3y + z \equiv 3 \pmod{5}$$

$$x + 2y + 3z \equiv 1 \pmod{5}$$

$$2x + z \equiv 1 \pmod{5}$$

5) Skor 20

Carilah pemfaktoran prima dari 1927 menggunakan metode rho Pollard dengan $x_0 = 2$ dan $f(x) = x^2 + 1$

6) Skor 20

Carilah pemfaktoran prima dari 1387 menggunakan metode rho Pollard dengan $x_0 = 3$ dan $f(x) = x^2 + 1$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1) a) $23x \equiv 17 \pmod{180}$

$(23, 180) = 1 | 17$, maka kongruensi linier mempunyai satu solusi.

$$\frac{23x \equiv 17 \pmod{180}}{180y \equiv -17 \pmod{23}} \rightarrow x_0 = \frac{180 \cdot 10 + 17}{23} = 79$$

$$180y \equiv -17 \pmod{23}$$

$$\frac{19y \equiv -17 \pmod{23}}{23z \equiv 17 \pmod{19}} \rightarrow y_0 = \frac{23 \cdot 9 - 17}{19} = 10$$

$$23z \equiv 17 \pmod{19}$$

$$\frac{4z \equiv 17 \pmod{19}}{19r \equiv -17 \pmod{4}} \rightarrow z_0 = \frac{19 \cdot 1 + 17}{4} = 9$$

$$19r \equiv -17 \pmod{4}$$

$$3r \equiv 3 \pmod{4} \rightarrow r_0 = 1$$

Penyelesaian : $x \equiv 79 \pmod{180}$

- b) $180 = 4 \cdot 5 \cdot 9$, maka kongruensi linier dapat dinyatakan dalam sistem kongruensi linier simultan:

$$23x \equiv 17 \pmod{4}, \text{ atau } x \equiv 3 \pmod{4}$$

$$23x \equiv 17 \pmod{5}, \text{ atau } x \equiv 4 \pmod{5}$$

$$23x \equiv 17 \pmod{9}, \text{ atau } x \equiv 7 \pmod{9}$$

Dengan demikian dapat dicari b_1 , b_2 , dan b_3 :

$$5.9b_1 \equiv 1 \pmod{4}, \text{ maka } b_1 = 1$$

$$4.9b_2 \equiv 1 \pmod{5}, \text{ maka } b_2 = 1$$

$$4.5b_3 \equiv 1 \pmod{9}, \text{ maka } b_3 = 5$$

$$x = 5.9.1.3 + 4.9.1.4 + 4.5.5.7 = 979$$

Jadi : $x \equiv 79 \pmod{180}$

- 2) Permasalahan banyaknya butir berlian dalam kantung dapat dinyatakan dalam suatu bentuk sistem kongruensi linier simultan. Misalkan banyaknya butir berlian dalam kantung adalah x , maka keadaan pertama dapat dinyatakan dengan $x \equiv 5 \pmod{13}$.

Setelah terjadi 4 orang terbunuh, maka keadaan kedua dapat dinyatakan dengan $x \equiv 6 \pmod{9}$. Demikian seterusnya sehingga diperoleh lagi dua kongruensi linier yaitu $x \equiv 3 \pmod{7}$ dan $x \equiv 0 \pmod{5}$.

$$9.7.5b_1 \equiv 1 \pmod{13}, b_1 = 9$$

$$13.7.5b_2 \equiv 1 \pmod{9}, b_2 = 2$$

$$13.9.5b_3 \equiv 1 \pmod{7}, b_3 = 2$$

$$13.9.7b_4 \equiv 1 \pmod{5}, b_4 = 4$$

$$x = 9.7.5.9.5 + 13.7.5.2.6 + 13.9.5.2.3 + 13.9.7.4.0 = 23145 \equiv 2670 \pmod{4095}$$

Banyaknya butir berlian minimal dalam kantung adalah 2670

- 3) Sistem kongruensi linier simultan dapat dinyatakan dengan
 $x \equiv 5 \pmod{6}$, $x \equiv 7 \pmod{11}$, $x \equiv 10 \pmod{13}$, $x \equiv 3 \pmod{5}$, dan
 $x \equiv 6 \pmod{7}$ sehingga:

$$11.13.5.7b_1 \equiv 1 \pmod{6}, b_1 = 1$$

$$6.13.15.7b_2 \equiv 1 \pmod{11}, b_2 = 6$$

$$6.11.5.7b_3 \equiv 1 \pmod{13}, b_3 = 3$$

$$6.11.13.7b_4 \equiv 1 \pmod{5}, b_4 = 1$$

$$6.11.13.5b_5 \equiv 1 \pmod{7}, b_5 = 6$$

$$x = 11.13.5.7.5.1 + 6.13.15.7.7.6 + 6.11.5.7.10.3 + 6.11.13.7.3.1 + 6.11.13.5.6.6$$

$$= 25025 + 114660 + 69300 + 18018 + 154440 = 381443 \equiv 21083 \pmod{30030}$$

- 4) Dengan cara biasa dapat dibuat barisan bilangan yang memenuhi masing-masing kongruensi, kemudian dicari suku atau unsur yang sama.

$$9x \equiv 4 \pmod{14}, \text{ maka } x \equiv 2, 16, 44, 58, 72, 86, 100, \dots, 310, \dots \pmod{14}$$

$$5x \equiv 17 \pmod{21}, \text{ maka } x \equiv 16, 37, 58, 79, 100, \dots, 310, \dots \pmod{21}$$

$$7x \equiv 10 \pmod{20}, \text{ maka } x \equiv 10, 30, 50, 70, \dots, 310, \dots \pmod{20}$$

$$x \equiv 310 \pmod{14}, x \equiv 310 \pmod{21}, \text{ dan } x \equiv 310 \pmod{30}, \text{ maka:}$$

$$x \equiv 310 \pmod{[14, 21, 30]} \equiv 310 \pmod{420}$$

Coba kerjakan dengan cara iterasi, untuk memeriksa apakah hasilnya sama.

- 5) Misalkan bilangan itu adalah x , maka:

$$x \equiv 0 \pmod{13}, x \equiv 2 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 2 \pmod{7}, \\ x \equiv 2 \pmod{8}, \text{ dan } x \equiv 10 \pmod{17}$$

Dari $x \equiv 2 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 2 \pmod{7}$, dan $x \equiv 2 \pmod{8}$ dapat ditentukan bahwa $x \equiv 2 \pmod{[3,5,7,8]}$, atau $x \equiv 2 \pmod{840}$.

Dengan demikian terdapat sistem kongruensi linier simultan $x \equiv 0 \pmod{13}$, $x \equiv 2 \pmod{840}$, dan $x \equiv 10 \pmod{17}$

$$840 \cdot 17 b_1 \equiv 1 \pmod{13}, b_1 = 11$$

$$13 \cdot 17 b_2 \equiv 1 \pmod{840}, b_2 = 821$$

$$13 \cdot 840 b_3 \equiv 1 \pmod{17}, b_3 = 3$$

$$x = 840 \cdot 17 \cdot 0.11 + 13 \cdot 17 \cdot 2.821 + 13 \cdot 840 \cdot 10.3 = 690482 \equiv 133562 \pmod{185640}$$

- 6) Langkah pertama adalah mencari $(26733, 54340)$ dengan menggunakan Algoritma Euclides:

$$54340 = 2.26733 + 874$$

$$26733 = 30.874 + 513$$

$$874 = 1.513 + 361$$

$$513 = 1.361 + 152$$

$$361 = 2.152 + 57$$

$$152 = 2.57 + 38$$

$$57 = 1.38 + 19$$

$$38 = 2.19 + 0$$

$(26733, 54340) = 19 | 133$, maka kongruensi linier mempunyai 19 selesaian.

$$26733x \equiv 133 \pmod{54340}$$

$$\frac{1407x \equiv 7 \pmod{2860}}{2860y \equiv -7 \pmod{1407}} \rightarrow x_0 = \frac{2860 \cdot 581 + 7}{1407} = 1181$$

$$\frac{46y \equiv -7 \pmod{1407}}{1407z \equiv 7 \pmod{46}} \rightarrow y_0 = \frac{1407 \cdot 19 - 7}{46} = 581$$

$$\begin{array}{rcl}
 \frac{27z \equiv 7 \pmod{46}}{46r \equiv -7 \pmod{27}} & \rightarrow & z_0 = \frac{46 \cdot 11 + 7}{27} = 19 \\
 \frac{19r \equiv -7 \pmod{27}}{27s \equiv 7 \pmod{19}} & \rightarrow & r_0 = \frac{27 \cdot 8 - 7}{19} = 11 \\
 \frac{8s \equiv 7 \pmod{19}}{19t \equiv -7 \pmod{8}} & \rightarrow & s_0 = \frac{19 \cdot 3 + 7}{8} = 8 \\
 \frac{3t \equiv -7 \pmod{8}}{8k \equiv 7 \pmod{3}} & \rightarrow & t_0 = \frac{8 \cdot 2 - 7}{3} = 3 \\
 \frac{2k \equiv 1 \pmod{3}}{} & \rightarrow & k_0 = 2
 \end{array}$$

Penyelesaian: $x \equiv 1181, 4041, 6901, \dots, 52661 \pmod{54340}$

Tes Formatif 2

- 1) a) $4x + y \equiv 2 \pmod{5}$, maka $y \equiv 2 - 4x \pmod{5}$
 $2x + 3y \equiv 1 \pmod{5}$, maka $2x + 3(2 - 4x) \equiv 1 \pmod{5}$,
 $-10x \equiv -5 \pmod{5}$ atau $10x \equiv 5 \pmod{5}$, dengan demikian
 $x \equiv 0, 1, 2, 3, 4 \pmod{5}$, sehingga $y \equiv 2, 3, 4, 0, 1 \pmod{5}$
- b) $2x + 3y \equiv 5 \pmod{5}$
 $x + 5y \equiv 6 \pmod{5}$

- 2) Semua selesaian adalah: $(0,4), (1,1), (2,5), (3,2), (4,6), (5,3)$, dan $(6,0)$

$$\begin{array}{l}
 3) \left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & x \\ 1 & 1 & 0 & 1 & y \\ 1 & 0 & 1 & 1 & z \\ 0 & 1 & 1 & 1 & w \end{array} \right] \equiv \left[\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \end{array} \right] \pmod{7} \\
 \left[\begin{array}{c} x \\ y \\ z \\ w \end{array} \right] \equiv \left[\begin{array}{cccc|c} 5 & 5 & 5 & 4 & 1 \\ 5 & 5 & 4 & 5 & 1 \\ 5 & 4 & 5 & 5 & 1 \\ 4 & 5 & 5 & 5 & 1 \end{array} \right] \pmod{7} \equiv \left[\begin{array}{c} 5 \\ 5 \\ 5 \\ 5 \end{array} \right] \pmod{7}
 \end{array}$$

- 4) Jika kongruensi pertama dikurangi kongruensi ketiga, maka diperoleh :

$$3y \equiv 2 \pmod{5}, \text{ atau } y \equiv 4 \pmod{5}$$

Selanjutnya, jika $x = 0, 1, 2, 3, 4$, maka diperoleh $z = 1, 4, 2, 0, 3$

Jadi terdapat lima selesaian tidak kongruen $(0, 4, 1), (1, 4, 4), (2, 4, 2), (3, 4, 0), (4, 4, 3)$

- 5) $x_0 = 2$

$$x_1 = f(x_0) = f(2) = 2^2 + 1 = 5$$

$$x_2 = f(x_1) = f(5) = 5^2 + 1 = 26$$

$$x_3 = f(x_2) = f(26) = 26^2 + 1 = 677$$

$$x_4 = f(x_3) = f(677) = 677^2 + 1 \equiv 1631 \pmod{1927}$$

$$x_5 = f(x_4) = f(1631) = 1631^2 + 1 \equiv 902 \pmod{1927}$$

$$x_6 = f(x_5) = f(902) = 902^2 + 1 \equiv 411 \pmod{1927}$$

$$x_7 = f(x_6) = f(411) = 411^2 + 1 = 1273 \pmod{1927}$$

Ternyata, $(x_7 - x_0, 1927) = (1273 - 2, 1927) = (1271, 1927) = 41$

Jadi $1927 = 41 \cdot 47$

- 6) $x_0 = 3$

$$x_1 = f(x_0) = f(3) = 3^2 + 1 = 10$$

$$x_2 = f(x_1) = f(10) = 10^2 + 1 = 101$$

$$x_3 = f(x_2) = f(101) = 101^2 + 1 = 493 \pmod{1387}$$

$$x_4 = f(x_3) = f(493) = 493^2 + 1 \equiv 325 \pmod{1387}$$

$$x_5 = f(x_4) = f(325) = 325^2 + 1 \equiv 214 \pmod{1387}$$

$$x_6 = f(x_5) = f(214) = 214^2 + 1 \equiv 26 \pmod{1387}$$

$$x_7 = f(x_6) = f(26) = 26^2 + 1 \equiv 677 \pmod{1387}$$

$$x_8 = f(x_7) = f(677) = 677^2 + 1 \equiv 620 \pmod{1387}$$

$$x_9 = f(x_8) = f(620) = 620^2 + 1 \equiv 202 \pmod{1387}$$

$$x_{10} = f(x_9) = f(202) = 202^2 + 1 \equiv 582 \pmod{1387}$$

$$x_{11} = f(x_{10}) = f(582) = 582^2 + 1 \equiv 297 \pmod{1387}$$

$$x_{12} = f(x_{11}) = f(297) = 297^2 + 1 \equiv 829 \pmod{1387}$$

Ternyata, $(x_{12} - x_6, 1387) = (829 - 26, 1387) = (803, 1387) = 73$
Jadi $1387 = 73 \cdot 19$

Daftar Pustaka

- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Residu Kuadratis

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul residu kuadratis ini diuraikan tentang keadaan kongruensi kuadratis dan penyelesaiannya, konsep dasar residu kuadratis, lambang Legendre dan sifat-sifatnya, kriteria Euler, lemma Gauss, kebalikan kuadrat dan sifat-sifatnya, lambang Jacobi dan sifat-sifatnya, serta penerapan teorema-teorema residu kuadratis dalam menyelesaikan kongruensi kuadratis satu variabel.

Sebagai bahasan yang berkaitan dengan Aljabar (biasa), kongruensi kuadratis serupa dengan persamaan kuadrat, tetapi ternyata cara menyelesaiannya jauh berbeda dengan persamaan kuadrat karena semesta pembicaraannya adalah himpunan bilangan modulo. Meskipun kelihatannya sederhana, ternyata terdapat banyak uraian dalam residu kuadratis yang memerlukan pemahaman lebih dalam dan sulit dibandingkan dengan persamaan kuadrat, misalnya terkait dengan dapat atau tidak dapat diselesaikannya, dan penerapan berbagai teorema dalam menyelidiki keterselesaian kongruensi kuadratis.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep dan sifat kongruensi kuadratis, residu kuadratis, kriteria Euler dan lemma Gauss, selesaian kongruensi kuadratis, sifat-sifat lambang Legendre dan Jacobi, dan sifat-sifat kebalikan kuadrat.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep kongruensi kuadratis dan sifat-sifatnya, konsep residu kuadratis dan sifat-sifatnya, konsep dan sifat lambang Legendre dan Jacobi, serta konsep dan sifat kebalikan kuadratis.

Susunan Kegiatan Belajar

Modul 5 ini terdiri dari dua Kegiatan Belajar. Kegiatan Belajar 1 adalah Kongruensi Kuadratis, dan Kegiatan Belajar 2 adalah Kebalikan Kuadratis.

Setiap kegiatan belajar memuat Uraian, Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 5 ini ditempatkan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi pembahasan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab, maka pelajariyah Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum berhasil menjawab permasalahan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Penguasaan Anda dengan cara mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah penggerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Kongruensi Kuadratis**

Kongruensi kuadratis adalah kongruensi yang mempunyai bentuk umum:

$$ax^2 = bx + c \equiv 0 \pmod{p}$$

dengan $a \neq 0$, p adalah suatu bilangan prima ganjil, dan $(a, p) = 1$

Keadaan $(a, p) = 1$ mengakibatkan adanya suatu kongruensi linier:

$$ak \equiv 1 \pmod{p}$$

mempunyai satu solusi sebab $(a, p) = 1 | 1$. Dengan demikian a mempunyai inversi perkalian (multiplikatif) $a^{-1} = k \pmod{p}$ sehingga $ak \equiv 1 \pmod{p}$, sehingga kongruensi kuadratis dapat disederhanakan menjadi:

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

$$akx^2 + bkx + ck \equiv 0 \pmod{p}$$

$$1 \cdot x^2 + bkx + ck \equiv 0 \pmod{p}$$

$$x^2 + bkx + ck \equiv 0 \pmod{p}$$

Dengan memilih $p = bk$ dan $q = ck$, maka $x^2 = bkx + ck \equiv 0 \pmod{p}$ dapat dinyatakan dengan:

$$x^2 = qx + r \equiv 0 \pmod{p}$$

Contoh 5.1

Kongruensi kuadratis $4x^2 - 9x + 5 \equiv 0 \pmod{17}$ menunjukkan bahwa $a = 4 \neq 0$, $p = 17$, dan $(a, p) = 1$, serta inversi perkalian 4 adalah $k = 13$ sebab $4 \cdot 13 = 52 \equiv 1 \pmod{17}$, sehingga:

$$4 \cdot 13 \equiv 1 \pmod{17}$$

Dengan demikian koefisien $a = 4$ dapat direduksi menjadi 1 setelah dikalikan dengan $k = 13$.

$$4x^2 - 9x + 5 \equiv 0 \pmod{17}$$

$$4 \cdot 13x^2 - 9 \cdot 13x + 5 \cdot 13 \equiv 0 \pmod{17}$$

$$52x^2 - 117x + 65 \equiv 0 \pmod{17}$$

$$x^2 + 2x + 14 \equiv 0 \pmod{17}$$

Contoh 5.2

Kongruensi kuadratis $5x^2 + 4x + 17 \equiv 0 \pmod{13}$ menunjukkan bahwa $a = 5 \neq 0$, $p = 13$, dan $(a, p) = 1$, serta inversi perkalian 5 adalah $k = 8$ sebab $5 \cdot 8 = 40 \equiv 1 \pmod{13}$, sehingga:

$$5 \cdot 8 \equiv 1 \pmod{13}$$

Dengan demikian koefisien $a = 5$ dapat direduksi menjadi 1 setelah dikalikan dengan $k = 8$.

$$5x^2 + 4x + 17 \equiv 0 \pmod{13}$$

$$5 \cdot 8x^2 + 4 \cdot 8x + 17 \cdot 8 \equiv 0 \pmod{13}$$

$$40x^2 + 32x + 136 \equiv 0 \pmod{13}$$

$$x^2 + 6x + 6 \equiv 0 \pmod{13}$$

Marilah sekarang kita kembali ke kongruensi kuadratis:

$$x^2 + qx + r \equiv 0 \pmod{p}$$

Dengan keadaan p adalah suatu bilangan prima ganjil, dan karena 2 adalah bilangan prima genap, maka dapat ditentukan bahwa $(2, p) = 1|1$, sehingga ada suatu bilangan bulat m yang memenuhi:

$$2m \equiv 1 \pmod{p}$$

Ini berarti bahwa bilangan bulat m merupakan inversi perkalian 2 modulo m , dan adanya m dapat digunakan untuk menentukan selesaian:

$$x^2 + qx + r \equiv 0 \pmod{p}$$

dengan jalan mengusahakan menjadi bentuk kuadrat sempurna:

$$x^2 + qx + r \equiv 0 \pmod{p}$$

$$x^2 + q \cdot 1x + r \equiv 0 \pmod{p}$$

$$x^2 + q \cdot 2mx + r \equiv 0 \pmod{p}$$

$$x^2 + q \cdot 2mx + [(qm)^2 - (qm)^2] + r \equiv 0 \pmod{p}$$

$$[x^2 + q \cdot 2mx + (qm)^2] - (qm)^2 + r \equiv 0 \pmod{p}$$

$$[x + (qm)]^2 \equiv [(qm)^2 - r] \pmod{p}$$

$$(x + qm)^2 \equiv [(qm)^2 - r] \pmod{p}$$

Misalkan $y = x + qm$ dan $k = (qm)^2 - r$, maka hasil terakhir dapat dinyatakan sebagai $y^2 \equiv k \pmod{p}$.

Dengan demikian kongruensi semula dapat diubah menjadi kongruensi dalam bentuk kuadrat sempurna, dan selesaian kongruensi kuadratis ditentukan oleh keadaan k dan p .

Contoh 5.3

Selesaian kongruensi $4x^2 + 9x + 5 \equiv 0 \pmod{17}$ dapat diperoleh dengan cara mengubah kongruensi semula sehingga diperoleh kongruensi dalam bentuk kuadrat sempurna.

$$\begin{aligned} 4x^2 - 9x + 5 &\equiv 0 \pmod{17} \\ 4.13x^2 - 9.13x + 5.13 &\equiv 0 \pmod{17}, 13 \text{ adalah inversi } 4 \text{ modulo } 17. \\ 52x^2 - 117x + 65 &\equiv 0 \pmod{17} \\ x^2 + 2x + 14 &\equiv 0 \pmod{17} \\ x^2 + 2.1x + 14 &\equiv 0 \pmod{17} \\ x^2 + 2.(2.9)x + (2.9)^2 - (2.9)^2 + 14 &\equiv 0 \pmod{17} \\ x^2 + 2.18x + (18)^2 - (18)^2 + 14 &\equiv 0 \pmod{17} \\ (x+18)^2 &\equiv (18)^2 - 14 \pmod{17} \equiv 1^2 - 14 \pmod{17} \equiv -13 \pmod{17} \\ &\equiv 4 \pmod{17} \\ (x+1)^2 &\equiv 4 \pmod{17}, \text{ maka } x+1 \equiv 2 \pmod{17} \text{ atau } x+1 \equiv -2 \pmod{17} \\ \text{Jadi } x &\equiv 1 \pmod{17} \text{ atau } x \equiv -3 \pmod{17} \equiv 14 \pmod{17} \end{aligned}$$

Contoh 5.4

Selesaian kongruensi $3x^2 + 5x - 4 \equiv 0 \pmod{17}$ dapat diperoleh dengan cara mengubah kongruensi semula sehingga diperoleh kongruensi dalam bentuk kuadrat sempurna.

$$\begin{aligned} 3x^2 + 5x - 4 &\equiv 0 \pmod{7} \\ 3.5x^2 + 5.5x - 5.4 &\equiv 0 \pmod{7}, 5 \text{ adalah inversi } 3 \text{ modulo } 17 \\ 15x^2 + 25x - 20 &\equiv 0 \pmod{7} \\ x^2 + 4x - 20 &\equiv 0 \pmod{7} \\ x^2 + 4.1x - 20 &\equiv 0 \pmod{7} \\ x^2 + 4.(2.4)x + (2.4)^2 - (2.4)^2 - 20 &\equiv 0 \pmod{7} \\ x^2 + 2.8x + (2.8)^2 - (2.8)^2 - 6 &\equiv 0 \pmod{7} \\ (x+16)^2 &\equiv (16)^2 + 6 \pmod{7} \equiv 2^2 + 6 \pmod{7} \equiv 10 \pmod{7} \equiv 3 \pmod{7} \\ (x+2)^2 &\equiv 3 \pmod{7}, \text{ atau } y^2 \equiv 3 \pmod{7} \text{ dengan } y = x+2 \\ \text{Kongruensi tidak mempunyai selesaian karena tidak ada } y &= 0, 1, 2, 3, 4, 5, 6 \text{ yang memenuhi kongruensi.} \end{aligned}$$

Definisi 5.1

Jika $k, p \in \mathbb{Z}, p > 0$, dan $(k, p) = 1$, maka:

- (a) k disebut residu kuadratis modulo p jika $x^2 \equiv k \pmod{p}$ mempunyai selesaian.
- (b) k disebut bukan residu kuadratis modulo p jika $x^2 \equiv k \pmod{p}$ tidak mempunyai selesaian.

Contoh 5.5

Kongruensi $x^2 \equiv k \pmod{7}$ mempunyai selesaian:

$$x = 1 \text{ dan } x = 6 \text{ jika } k = 1$$

$$x = 3 \text{ dan } x = 4 \text{ jika } k = 2$$

$$x = 2 \text{ dan } x = 5 \text{ jika } k = 4$$

dan tidak mempunyai selesaian jika $k = 3, k = 5$, atau $k = 6$

Residu-residu kuadratis modulo 7 adalah 1, 2, dan 4

Bukan residu-residu kuadratis modulo 7 adalah 3, 5, dan 6

Contoh 5.6

Residu-residu kuadratis modulo 11 adalah 1, 3, 4, 5, dan 9 sebab:

$$x^2 \equiv 1 \pmod{11} \text{ mempunyai selesaian, yaitu } x = 1 \text{ atau } x = 10$$

$$x^2 \equiv 3 \pmod{11} \text{ tidak mempunyai selesaian, yaitu } x = 5 \text{ atau } x = 6$$

$$x^2 \equiv 4 \pmod{11} \text{ mempunyai selesaian, yaitu } x = 2 \text{ atau } x = 9$$

$$x^2 \equiv 5 \pmod{11} \text{ tidak mempunyai selesaian, yaitu } x = 4 \text{ atau } x = 7$$

$$x^2 \equiv 9 \pmod{11} \text{ mempunyai selesaian, yaitu } x = 3 \text{ atau } x = 8$$

Bukan residu-residu kuadratis modulo 11 adalah 2, 6, 7, 8, dan 10 sebab:

$$x^2 \equiv 2 \pmod{11} \text{ tidak mempunyai selesaian}$$

$$x^2 \equiv 6 \pmod{11} \text{ tidak mempunyai selesaian}$$

$$x^2 \equiv 7 \pmod{11} \text{ tidak mempunyai selesaian}$$

$$x^2 \equiv 8 \pmod{11} \text{ tidak mempunyai selesaian}$$

$$x^2 \equiv 10 \pmod{11} \text{ tidak mempunyai selesaian}$$

Teorema 5.1

Ditentukan p adalah suatu bilangan prima ganjil. Setiap sistem residu tereduksi modulo p tepat memuat $(p-1)/2$ residu-residu kuadratis, dan tepat memuat $(p-1)/2$ bukan residu-residu kuadratis modulo p .

Residu-residu kuadratis merupakan unsur dari kelas residu yang memuat bilangan-bilangan: $1^2, 2^2, 3^2, \dots, [(p-1)/2]^2$.

Bukti:

Unsur-unsur $1^2, 2^2, 3^2, \dots, [(p-1)/2]^2$ semuanya berbeda atau tidak ada yang kongruen modulo p . Misalkan ada yang sama, atau ada yang kongruen modulo p , yaitu: $x^2 \equiv y^2 \pmod{p}$, berarti $p|x^2 - y^2$ atau $p|(x+y)(x-y)$, di mana $1 \leq x \leq (p-1)/2$ dan $1 \leq y \leq (p-1)/2$, sehingga $2 \leq x+y \leq p-1$ dan $(3-p)/2 \leq x-y \leq (p-3)/2$.

Karena p adalah bilangan prima dan $p|(x+y)(x-y)$, maka $p|(x+y)$ atau $p|(x-y)$.

p tidak mungkin membagi $x+y$ sebab $2 \leq x+y \leq p-1$, dengan demikian $p|(x-y)$.

Karena $(3-p)/2 \leq x-y \leq (p-3)/2$ dan $p|(x-y)$, maka $x-y=0$ atau $x=y$.

Selanjutnya, karena $(p-k)^2 \equiv k^2 \pmod{p}$, maka setiap residu kuadratis modulo p adalah kongruen dengan satu dari $1^2, 2^2, 3^2, \dots, [(p-1)/2]^2$.

Jadi banyaknya residu kuadratis adalah $(p-1)/2$ dan bukan residu kuadratis juga $(p-1)/2$.

Contoh 5.7

Carilah semua residu kuadratis modulo p jika:

1. $p = 19$
2. $p = 37$

Jawab:

1. Semua residu kuadratis modulo 19 terdapat di dalam kelas residu yang ditunjukkan oleh $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2$ atau ditunjukkan oleh residu-residu positif terkecil dari $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2$:
1, 4, 9, 16, 6, 17, 11, 7, 5
2. Semua residu kuadratis modulo 37 terdapat di dalam kelas residu yang ditunjukkan oleh:
 $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2$

atau ditunjukkan oleh residu-residu positif terkecilnya, yaitu:

1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28

Teorema 5.2

Ditentukan k adalah suatu bilangan bulat, p adalah suatu bilangan prima ganjil, dan $(k, p) = 1$. Jika kongruensi $x^2 \equiv k \pmod{p}$ dapat diselesaikan, maka terdapat tepat dua selesaian yang tidak kongruen modulo p .

Bukti:

Misalkan kongruensi $x^2 \equiv k \pmod{p}$ dapat diselesaikan, dan selesaiannya adalah $x = x_1$, maka $x_1^2 \equiv k \pmod{p}$. Karena $(-x_1)^2 = x_1^2 \equiv k \pmod{p}$, maka $x = -x_1$ memenuhi kongruensi.

Dengan demikian $x = x_1$ dan $x = -x_1 \equiv x_1 + p \pmod{p}$ adalah dua selesaian $x^2 \equiv k \pmod{p}$. Untuk menunjukkan bahwa x_1 dan $-x_1$ adalah dua selesaian yang tidak kongruen, digunakan bukti tidak langsung, yaitu misalkan $x_1 \equiv -x_1 \pmod{p}$.

Dari $x_1 \equiv -x_1 \pmod{p}$ dapat ditunjukkan bahwa $p | 2x_1$, dan karena p adalah bilangan prima ganjil maka $(2, p) = 1$.

Dengan demikian, dari $p | 2x_1$ dan $(2, p) = 1$, maka $p | x_1$, akibatnya $p | x_1^2$.

Karena $p | x_1^2$ dan $x_1^2 \equiv k \pmod{p}$, maka $p | k$, terjadi kontradiksi sebab $(k, p) = 1$.

Hal ini berarti x_1 dan $-x_1$ adalah dua selesaian yang tidak kongruen.

Untuk menunjukkan bahwa kongruensi tepat mempunyai dua selesaian, digunakan juga bukti tidak langsung, misalkan ada selesaian lain yang tidak kongruen, yaitu $x = x_2$. Dari $x_1^2 \equiv k \pmod{p}$ dan $x_2^2 \equiv k \pmod{p}$ dapat ditunjukkan bahwa $x_1^2 - x_2^2 \equiv 0 \pmod{p}$.

Ini berarti $p | x_1^2 - x_2^2$, $p | (x_1 - x_2)(x_1 + x_2)$, $p | (x_1 - x_2)$, atau $p | (x_1 + x_2)$.

Akibatnya, $x_1 \equiv x_2 \pmod{p}$ atau $x_1 \equiv -x_2 \pmod{p}$. Karena terjadi kontradiksi, maka dapat ditentukan bahwa tidak ada selesaian lain $x = x_2$, berarti banyaknya selesaian adalah tepat dua.

Contoh 5.8

Selesaian $x^2 \equiv 5 \pmod{11}$ adalah

$x \equiv 4 \pmod{11}$ atau $x \equiv -4 \pmod{11} = 7 \pmod{11}$

Selesaian $x^2 \equiv 11 \pmod{19}$ adalah

$$x \equiv 7 \pmod{19} \text{ atau } x \equiv -7 \pmod{19} = 12 \pmod{19}$$

Definisi 5.2

Ditentukan p adalah suatu bilangan prima ganjil dan k adalah suatu bilangan bulat yang tidak habis dibagi oleh p .

Lambang Legendre $\left[\frac{k}{p} \right]$ didefinisikan sebagai:

$$\left[\frac{k}{p} \right] = \begin{cases} 1, & \text{jika } k \text{ adalah suatu residi kuadratis modulo } p \\ -1, & \text{jika } k \text{ adalah bukan suatu residi kuadratis modulo } p \end{cases}$$

Contoh 5.9

Untuk $p = 5$ dapat ditunjukkan bahwa:

$$\left[\frac{1}{5} \right] = 1 \text{ sebab } 1 \text{ adalah suatu residi kuadratis modulo } 5,$$

yaitu $x^2 \equiv 1 \pmod{5}$ dapat diselesaikan dengan selesaian $x \equiv 1 \pmod{5}$ dan $x \equiv 4 \pmod{5}$

$$\left[\frac{4}{5} \right] = 1 \text{ sebab } 4 \text{ adalah suatu residi kuadratis modulo } 5,$$

yaitu $x^2 \equiv 4 \pmod{5}$ dapat diselesaikan dengan selesaian $x \equiv 2 \pmod{5}$ dan $x \equiv 3 \pmod{5}$

$$\left[\frac{2}{5} \right] = -1 \text{ sebab } 2 \text{ adalah bukan suatu residi kuadratis modulo } 5,$$

yaitu $x^2 \equiv 2 \pmod{5}$ tidak dapat diselesaikan.

Contoh 5.10

Untuk $p = 31$ dapat ditunjukkan bahwa:

$$\begin{aligned} \left[\frac{1}{31} \right] &= \left[\frac{7}{31} \right] = \left[\frac{4}{31} \right] = \left[\frac{5}{31} \right] = \left[\frac{7}{31} \right] = \left[\frac{8}{31} \right] = \left[\frac{9}{31} \right] = \left[\frac{10}{31} \right] = \left[\frac{14}{31} \right] = \left[\frac{16}{31} \right] \\ &= \left[\frac{18}{31} \right] = \left[\frac{19}{31} \right] = \left[\frac{20}{31} \right] = \left[\frac{25}{31} \right] = \left[\frac{28}{31} \right] = +1 \end{aligned}$$

$$\begin{aligned} \left[\frac{3}{31} \right] &= \left[\frac{6}{31} \right] = \left[\frac{11}{31} \right] = \left[\frac{12}{31} \right] = \left[\frac{13}{31} \right] = \left[\frac{15}{31} \right] = \left[\frac{17}{31} \right] = \left[\frac{21}{31} \right] = \left[\frac{22}{31} \right] = \left[\frac{23}{31} \right] \\ &= \left[\frac{24}{31} \right] = \left[\frac{26}{31} \right] = \left[\frac{27}{31} \right] = \left[\frac{29}{30} \right] = \left[\frac{30}{31} \right] = -1 \end{aligned}$$

Teorema 5.3 Kriteria Euler

Jika p adalah suatu bilangan prima dan k adalah suatu bilangan bulat positif yang tidak habis dibagi oleh p , maka

$$\left[\frac{k}{p} \right] \equiv a^{(p-1)/2} \pmod{p}$$

Bukti:

Kemungkinan nilai-nilai $\left[\frac{k}{p} \right]$ adalah 1 atau -1

1. Jika $\left[\frac{k}{p} \right] = 1$, maka $x^2 \equiv k \pmod{p}$ mempunyai suatu selesaian, misalnya $x = x_0$, maka menurut Teorema Kecil Fermat berlaku $x_0^{p-1} \equiv 1 \pmod{p}$. Dengan demikian,

$$x_0^{p-1} = (x_0^2)^{(p-1)/2} = k^{(p-1)/2} \equiv 1 \pmod{p} \text{ atau } 1 \equiv k^{(p-1)/2} \equiv 1 \pmod{p}.$$

$$\text{Jadi } \left[\frac{k}{p} \right] \equiv k^{(p-1)/2} \pmod{p}$$

2. Jika $\left[\frac{k}{p} \right] = -1$, maka $x^2 \equiv k \pmod{p}$ tidak mempunyai selesaian.

Sekarang perhatikan jika $1 \leq i \leq (p-1)$, maka untuk masing-masing i berlaku $(i, p) = 1$ sehingga setiap kongruensi linier $ix \equiv k \pmod{p}$ mempunyai selesaian yang tunggal modulo p , misalnya $x = j$, dengan $1 \leq j \leq (p-1)$. Selanjutnya, karena $x^2 \equiv k \pmod{p}$ tidak mempunyai selesaian, maka $i \neq j$. Jadi kita mempunyai barisan bilangan bulat $1, 2, 3, \dots, p-1$ yang dapat dikelompokkan menjadi $(p-1)/2$ pasangan yang hasil kali setiap pasangan adalah k .

$$1, 2, 3, \dots, (p-1) \equiv k^{(p-1)/2} \pmod{p} \text{ atau } (p-1)! \equiv k^{(p-1)/2} \pmod{p}.$$

Menurut Teorema Wilson, $(p-1)! \equiv -1 \pmod{p}$, berarti

$$-1 \equiv k^{(p-1)/2} \pmod{p}$$

$$\text{Jadi } \left[\frac{k}{p} \right] \equiv k^{(p-1)/2} \pmod{p}.$$

Contoh 5.11

Ditentukan $x^2 \equiv 3 \pmod{7}$ tidak mempunyai selesaian, akan ditunjukkan bahwa $\left[\frac{3}{7} \right] = -1$.

Bilangan-bilangan bulat 1, 2, 3, 4, 5, dan 6 dapat dipasangkan-pasangkan dalam bentuk perkalian $ij \equiv 3 \pmod{7}$, yaitu:

$$1.3 = 3 \equiv 3 \pmod{7}$$

$$2.5 = 10 \equiv 3 \pmod{7}$$

$$4.6 = 24 \equiv 3 \pmod{7}$$

sehingga:

$$1.2.3.4.5.6 \equiv 3^3 \pmod{7}, 6! \equiv 3^3 \pmod{7}, \text{ atau } -1 \equiv 27 \pmod{7}$$

Jadi $\left[\frac{3}{7} \right] = -1$

Contoh 5.12

Selesaikan $x^2 \equiv 5 \pmod{23}$.

Jawab:

Menurut Kriteria Euler,

$$\left[\frac{5}{23} \right] = 5^{(23-1)/2} = 5^{11} = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 \cdot 5$$

$$\equiv 2.2.2.2.2.5 \pmod{23}$$

$$\equiv 32.5 \pmod{23} \equiv 9.5 \pmod{23} \equiv 45 \pmod{23} \equiv -1 \pmod{23}$$

Karena $\left[\frac{5}{23} \right] = -1$, maka kongruensi tidak mempunyai selesaian.

Teorema 5.4

Ditentukan bahwa $m, n \in \mathbb{Z}, p$ adalah suatu bilangan prima ganjil, p tidak membagi m dan n , maka:

$$(a) \quad \left[\frac{m}{p} \right] \left[\frac{n}{p} \right] = \left[\frac{mn}{p} \right]$$

$$(b) \quad \text{jika } m \equiv n \pmod{p}, \text{ maka } \left[\frac{m}{p} \right] = \left[\frac{n}{p} \right]$$

$$(c) \quad \left[\frac{m^2}{p} \right] = 1$$

$$(d) \left[\frac{m^2 n}{p} \right] = \left[\frac{n}{p} \right]$$

$$(e) \left[\frac{1}{p} \right] = +1 \text{ dan } \left[\frac{-1}{p} \right] = (-1)^{(p-1)/2}$$

Bukti:

$$(a) \text{ Sesuai Teorema 5.3, } \left[\frac{m}{p} \right] \equiv m^{(p-1)/2} (\text{mod } p) \text{ dan } \left[\frac{n}{p} \right] \equiv n^{(p-1)/2} (\text{mod } p).$$

Dengan demikian

$$\left[\frac{mn}{p} \right] \equiv (mn)^{(p-1)/2} (\text{mod } p) \equiv (m^{(p-1)/2})(n^{(p-1)/2}) (\text{mod } p)$$

$$\equiv \{m^{(p-1)/2} (\text{mod } p)\} \{n^{(p-1)/2} (\text{mod } p)\} \equiv \left[\frac{m}{p} \right] \left[\frac{n}{p} \right]$$

$$\text{Jadi } \left[\frac{m}{p} \right] \left[\frac{n}{p} \right] = \left[\frac{mn}{p} \right]$$

$$(b) \text{ Sesuai Teorema 5.3, } \left[\frac{n}{p} \right] \equiv n^{(p-1)/2} (\text{mod } p), \text{ dan diketahui}$$

$m \equiv n (\text{mod } p)$, maka

$$\left[\frac{m}{p} \right] \equiv m^{(p-1)/2} (\text{mod } p) \equiv n^{(p-1)/2} (\text{mod } p) \equiv \left[\frac{n}{p} \right]$$

$$\text{Jadi } \left[\frac{m}{p} \right] = \left[\frac{n}{p} \right]$$

$$(c) \left[\frac{m^2}{p} \right] \equiv (m^2)^{(p-1)/2} (\text{mod } p) \equiv m^{p-1} (\text{mod } p) \equiv 1 (\text{mod } p)$$

$$\text{Jadi } \left[\frac{m^2}{p} \right] = 1$$

$$(d) \left[\frac{m^2 n}{p} \right] \equiv (m^2 n)^{(p-1)/2} (\text{mod } p) \equiv \{m^2 (\text{mod } p)\} \{n^{(p-1)/2} (\text{mod } p)\}$$

$$\equiv \{1 (\text{mod } p)\} \{n^{(p-1)/2} (\text{mod } p)\} \equiv n^{(p-1)/2} (\text{mod } p)$$

$$\text{Jadi } \left[\frac{m^2 n}{p} \right] = \left[\frac{n}{p} \right]$$

$$(e) \left[\frac{1}{p} \right] \equiv (1)^{(p-1)/2} \pmod{p} \equiv 1 \pmod{p}$$

$$\left[\frac{-1}{p} \right] \equiv (-1)^{(p-1)/2} \pmod{p}$$

$$\text{Jadi } \left[\frac{1}{p} \right] = +1 \text{ dan } \left[\frac{-1}{p} \right] = (-1)^{(p-1)/2}$$

Contoh 5.13

Tunjukkan apakah masing-masing kongruensi berikut dapat diselesaikan

$$(a) x^2 \equiv 3 \pmod{41}$$

$$(b) x^2 + 1 \equiv 0 \pmod{127}$$

Jawab:

$$(a) \left[\frac{3}{41} \right] \equiv 3^{(41-1)/2} \pmod{41} = 3^{20} \pmod{41} = (3^4)^5 \pmod{41}$$

$$= (81^2)^5 \pmod{41} \equiv (-1)^5 \pmod{41} \equiv -1 \pmod{41}$$

Karena $\left[\frac{3}{41} \right] = -1$ maka $x^2 \equiv 3 \pmod{41}$ tidak dapat diselesaikan.

$$(b) x^2 + 1 \equiv 0 \pmod{127}, \text{ maka } x^2 \equiv -1 \pmod{127}$$

$$\left[\frac{-1}{127} \right] \equiv (-1)^{(127-1)/2} \pmod{127} = (-1)^{63} \pmod{127} = -1 \pmod{127}$$

$\left[\frac{-1}{127} \right] = -1$, maka kongruensi $x^2 + 1 \equiv 0 \pmod{127}$ tidak mempunyai

solusi

Teorema 5.5

Jika p adalah suatu bilangan prima ganjil, maka:

$$\left[\frac{-1}{p} \right] = \begin{cases} 1, & \text{jika } p \equiv 1 \pmod{4} \\ -1, & \text{jika } p \equiv 3 \pmod{4} \end{cases}$$

Bukti:

Karena p adalah suatu bilangan prima ganjil, maka p tidak mungkin dinyatakan sebagai $p \equiv 0 \pmod{4}$ atau $p \equiv 2 \pmod{4}$.

Menurut Teorema 5.3 , $\left[\frac{-1}{p} \right] \equiv (-1)^{(p-1)/2} (\text{mod } p)$

(a) Jika $p \equiv 1 \pmod{4}$, atau $p = 4k + 1$ dengan $k \in \mathbb{Z}$, maka:

$$(-1)^{(p-1)/2} = (-1)^{\lfloor \frac{(4k+1)-1}{2} \rfloor / 2} = (-1)^{2k} = 1$$

Jadi $\left[\frac{-1}{p} \right] = 1$ untuk $p \equiv 1 \pmod{4}$

(b) Jika $p \equiv 3 \pmod{4}$, atau $p = 4k + 3$ dengan $k \in \mathbb{Z}$, maka:

$$(-1)^{(p-1)/2} = (-1)^{\lfloor \frac{(4k+3)-1}{2} \rfloor / 2} = (-1)^{2k+1} = -1$$

Jadi $\left[\frac{-1}{p} \right] = -1$ untuk $p \equiv 3 \pmod{4}$

Contoh 5.14

Kongruensi kuadratis $x^2 \equiv -1 \pmod{11}$ tidak mempunyai selesaian sebab

$$11 \equiv 3 \pmod{4} \text{ sehingga } \left[\frac{-1}{11} \right] = -1$$

Contoh 5.15

Kongruensi kuadratis $x^2 \equiv -1 \pmod{29}$ dapat diselesaikan sebab $29 \equiv 1 \pmod{4}$ sehingga $\left[\frac{-1}{29} \right] = +1$. Untuk memperoleh selesaian, kita perlu menambah -1 dengan $29.k$ yang mana $k = 1, 2, 3, \dots$ sehingga diperoleh suatu bilangan kuadrat. Dengan demikian kongruensi dapat diubah menjadi: $x^2 \equiv -1 \pmod{29} \equiv (-1 + 29.k) \pmod{29} \equiv (-1 + 29.10) \pmod{29} = 289 \pmod{29}$ sehingga $x^2 - 289 \equiv 0 \pmod{29}$, $(x - 17)(x + 17) \equiv 0 \pmod{29}$. Selesaian kongruensi adalah $x \equiv 17 \pmod{29}$ atau $x \equiv 12 \pmod{29}$.

Teorema 5.6 (Lemma Gauss)

Ditentukan p adalah suatu bilangan prima ganjil, $k \in \mathbb{Z}$, dan $(k, p) = 1$

Jika r adalah banyaknya residu positif terkecil dari $k, 2k, 3k, \dots, \left(\frac{p-1}{2} \right)k$

yang lebih dari $\frac{p}{2}$ maka $\left[\frac{k}{p} \right] = (-1)^r$.

Bukti:

Perhatikan barisan $k, 2k, 3k, \dots, \left(\frac{p-1}{2}\right)k$.

Jika unsur-unsur barisan dinyatakan dalam modulo p sehingga diperoleh suatu barisan baru dengan unsur-unsur positif dan kurang dari p , maka barisan baru ini disebut barisan residu positif terkecil modulo p , dan memuat dua barisan bagian, yaitu u_1, u_2, \dots, u_i dengan $u_r > \frac{p}{2}$, $r = 1, 2, \dots, i$ yang disebut barisan residu positif terkecil yang lebih dari $\frac{p}{2}$, dan v_1, v_2, \dots, v_j dengan $v_s < \frac{p}{2}$, $s = 1, 2, \dots, j$ yang disebut barisan residu positif terkecil yang kurang dari $\frac{p}{2}$.

Jika $u_i \times v_j$ dinyatakan dalam modulo p , maka diperoleh:

$$\begin{aligned} (u_1, u_2, \dots, u_i)(v_1, v_2, \dots, v_j) &\equiv k \cdot 2k \cdots \left(\frac{p-1}{2}\right)k \pmod{p} \\ &\equiv k^{(p-1)/2} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right) \pmod{p} \\ &\equiv k^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned}$$

Karena $(tk, p) = 1$ untuk semua t yang mana $0 \leq t \leq \frac{p-1}{2}$, maka barisan residu positif terkecil $u_1, u_2, \dots, u_i, v_1, v_2, \dots, v_j$ merupakan bagian barisan $1, 2, 3, \dots, p-1$.

Perhatikan barisan: $p - u_1, p - u_2, \dots, p - u_i, v_1, v_2, \dots, v_j$. Karena unsur-unsur barisan ini sebanyak $(p-1)/2$ dan merupakan bilangan bulat positif tidak lebih dari $(p-1)/2$, maka tidak ada dua unsur barisan yang kongruen modulo p . Jika ada dua u_i atau dua v_j yang kongruen, maka $mk \equiv nk \pmod{p}$ dengan $m, n \in \mathbb{Z}$ dan $0 < x, y \leq (p-1)/2$, akibatnya $m \equiv n \pmod{p}$ karena $(k, p) = 1$. Hal ini tidak mungkin terjadi.

Demikian pula jika ada $(p - u_i)$ yang kongruen dengan v_j , maka $mk \equiv (p - na) \pmod{p}$, atau $mk \equiv -nk \pmod{p}$, akibatnya $m \equiv -n \pmod{m}$ karena $(k, p) = 1$. Hal ini tidak mungkin terjadi karena m dan n di dalam barisan $1, 2, \dots, (p-1)/2$.

Jadi semua unsur barisan $p - u_1, p - u_2, \dots, p - u_i, v_1, v_2, \dots, v_j$ sama dengan unsur-unsur barisan $1, 2, \dots, (p-1)/2$, sehingga:

$$(p - u_1), (p - u_2), \dots, (p - u_i), v_1, v_2, \dots, v_j \equiv 1, 2, \dots, (p-1)/2$$

$$(-u_1), (-u_2), \dots, (-u_i), v_1, v_2, \dots, v_j \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$(-1)^i (u_1)(u_2) \dots (u_i) \cdot v_1, v_2, \dots, v_j \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$(-1)^i k^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p} \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

Karena $\left(\left(\frac{p-1}{2}\right)!, p\right)$, maka

$$(-1)^i k^{(p-1)/2} \equiv 1 \pmod{p} \text{ atau } k^{(p-1)/2} \equiv (-1)^i \pmod{p}.$$

$$\text{Jadi } \left(\frac{k}{p}\right) \equiv (-1)^i \pmod{p}$$

Contoh 5.16

Kongruensi kuadratis $x^2 \equiv 7 \pmod{13}$ akan diselidiki dengan menggunakan Lemma Gauss. Kita buat barisan $7k$ dengan $k = 1, 2, \dots, (13-1)/2$, kita peroleh 7, 14, 21, 28, 35, 42, dan dalam modulo 13 diperoleh barisan residu terkecil 7, 1, 8, 2, 9, 3, sehingga dapat dikelompokkan menjadi barisan residu positif terkecil lebih dari $(13/2)$ yaitu 7, 8, 9, dan barisan residu positif terkecil kurang dari $(13/2)$ yaitu 1, 2, 3.

Dengan demikian:

$$u_1 = 7 \equiv 7 \pmod{13}, u_2 = 8 \equiv 21 \pmod{13}, u_3 = 9 \equiv 35 \pmod{13}$$

$$v_1 = 1 \equiv 14 \pmod{13}, v_2 = 2 \equiv 28 \pmod{13}, v_3 = 3 \equiv 42 \pmod{13}$$

sehingga:

$$u_1 u_2 u_3 \cdot v_1 v_2 v_3 \equiv 7 \cdot 21 \cdot 35 \cdot 14 \cdot 28 \cdot 42 \pmod{13} \equiv 7^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{13}$$

Sekarang kita buat barisan $p - u_1, p - u_2, p - u_3, v_1, v_2, v_3$, kita peroleh barisan 6, 5, 4, 1, 2, 3, yang mana tidak memuat dua suku yang kongruen.

$$(p - u_1) \cdot (p - u_2) \cdot (p - u_3) \cdot v_1 \cdot v_2 \cdot v_3 \equiv 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \pmod{13}$$

$$(-1)^3 u_1 u_2 u_3 v_1 v_2 v_3 \equiv 6! \pmod{13}$$

$$(-1)^3 7^6 \cdot 6! \equiv 6! \pmod{13}$$

$$7^6 \equiv -1 \pmod{13}, \text{ berarti } \left(\frac{7}{13}\right) \equiv 7^6 \pmod{13} \equiv -1 \pmod{13}$$

Jadi kongruensi $x^2 \equiv 7 \pmod{13}$ tidak mempunyai selesaian.

Tugas

Bacalah suatu buku Teori Bilangan, buktikan suatu Teorema bahwa:

$$\left[\frac{2}{p} \right] = (-1)^{\frac{p^2-1}{8}}$$

jika p adalah suatu bilangan prima ganjil.

Selanjutnya, berdasarkan teorema tersebut, buktikan akibatnya:

$$\left(\frac{2}{p} \right) = \begin{cases} +1, & \text{jika } p \equiv 1 \pmod{8} \text{ atau } p \equiv 7 \pmod{8} \\ -1, & \text{jika } p \equiv 3 \pmod{8} \text{ atau } p \equiv 5 \pmod{8} \end{cases}$$

Petunjuk Jawaban Tugas

Sesuai dengan Lemma Gauss, jika i adalah banyaknya residu positif terkecil modulo p : $1.2, 2.2, 3.2, \dots, \left(\frac{p-1}{2}\right).2$ yang lebih dari $p/2$, maka

$$\left[\frac{2}{p} \right] \equiv (-1)^i \pmod{p}.$$

Sekarang akan dihitung banyaknya residu positif terkecil yang kurang dari $p/2$. Bilangan bulat $2j$, dengan $1 \leq j \leq (p-1)/2$, adalah kurang dari $p/2$ jika $j \leq p/4$, dengan demikian terdapat $[p/4]$ bilangan bulat kurang dari $p/2$. Akibatnya, terdapat $i = (p-1)/2 - [p/4]$ bilangan bulat lebih dari $p/2$, sehingga sesuai dengan Lemma Gauss:

$$\left[\frac{2}{p} \right] = (-1)^{\frac{p-1}{2} - [p/4]}$$

Ini berarti harus dibuktikan bahwa $\left[\frac{2}{p} \right] = (-1)^{\frac{p-1}{2} - [p/4]} \equiv (p^2 - 1)/8 \pmod{2}$

Marilah kita lihat berbagai keadaan dari $(p^2 - 1)/8$

- (1) p tidak mungkin dalam bentuk $p \equiv 2, 4, 6 \pmod{8}$ sebab p adalah bilangan prima ganjil

(2) $p \equiv \pm 1 \pmod{8}$, atau $p = 8t \pm 1$, maka

$$(p^2 - 1)/8 = \{(8t \pm 1)^2 - 1\}/8 \equiv 0 \pmod{2}$$

(3) $p \equiv \pm 3 \pmod{8}$, atau $p = 8t \pm 3$, maka

$$(p^2 - 1)/8 = \{(8t \pm 3)^2 - 1\}/8 \equiv 1 \pmod{2}$$

Marilah sekarang kita lihat berbagai keadaan $(p - 1)/2 - [p/4]$

(1) $p \equiv 1 \pmod{8}$, atau $p = 8t + 1$, maka

$$(p - 1)/2 - [p/4] = 4t - [2t + 1/4] = 4t - 2t \equiv 0 \pmod{2}$$

(2) $p \equiv -1 \pmod{8}$, atau $p = 8t + 7$, maka

$$(p - 1)/2 - [p/4] = (4t + 3) - [2t + 7/4] \equiv 0 \pmod{2}$$

(3) $p \equiv 3 \pmod{8}$, atau $p = 8t + 3$, maka

$$(p - 1)/2 - [p/4] = (4t + 1) - [2t + 3/4] \equiv 1 \pmod{2}$$

(4) $p \equiv -3 \pmod{8}$, atau $p = 8t + 5$, maka

$$(p - 1)/2 - [p/4] = (4t + 2) - [2t + 5/4] \equiv 1 \pmod{2}$$

Dengan demikian dapat ditentukan bahwa:

$$\{(p - 1)/2 - [p/4]\} \equiv \{(p^2 - 1)/8\} \pmod{2}$$

$$\text{sehingga } \left[\frac{2}{p} \right] = (-1)^{\frac{p^2-1}{8}}.$$

Jika $p \equiv 1 \pmod{8}$ atau $p \equiv 7 \pmod{8}$, maka $p \equiv 8m+1$ atau $p \equiv 8n+7$

dengan $m, n \in \mathbb{Z}$ sehingga substitusi pada $(p^2 - 1)/8$ diperoleh $2r$ atau $2s$,

$$\text{akibatnya } \left[\frac{2}{p} \right] = (-1)^{\frac{p^2-1}{8}} = 1.$$

Jika $p \equiv 3 \pmod{8}$ atau $p \equiv 5 \pmod{8}$, maka $p \equiv 8m+3$ atau $p \equiv 8n+5$

dengan $m, n \in \mathbb{Z}$, sehingga substitusi pada $(p^2 - 1)/8$ diperoleh $2r+1$ atau

$$2s+1, \text{ akibatnya } \left[\frac{2}{p} \right] = (-1)^{\frac{p^2-1}{8}} = -1.$$



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Selesaikan $5x^2 + 4x + 17 \equiv 0 \pmod{13}$!
- 2) Carilah residu-residu kuadratis dan bukan residu-residu kuadratis modulo 5!

- 3) Selesaikan!
- $x^2 \equiv 5 \pmod{11}$
 - $x^2 \equiv 72 \pmod{11}$
- 4) Selesaikan!
- $x^2 \equiv 5 \pmod{19}$ dengan menggunakan Lemma Gauss
 - $x^2 \equiv 58 \pmod{77}$ dengan menggunakan Teorema Sisa China
- 5) Carilah $\begin{bmatrix} -15 \\ 61 \end{bmatrix}$ dengan menggunakan Kriteria Euler!

Petunjuk Jawaban Latihan

- 1) $5x^2 + 4x + 17 \equiv 0 \pmod{13}$ dikalikan 8 (sebab 8 adalah inversi 5 modulo 13) diperoleh $40x^2 + 32x + 136 \equiv 0 \pmod{13}$ atau $x^2 + 6x + 6 \equiv 0 \pmod{13}$, kemudian dapat diubah menjadi $x^2 + 6(2.7)x + (6.7)^2 - (6.7)^2 + 6 \equiv 0 \pmod{13}$ karena $2.7 \equiv 1 \pmod{13}$, dan dapat disederhanakan menjadi $x^2 + 2(42)x + (42)^2 - (42)^2 + 6 \equiv 0 \pmod{13}$ atau $(x+42)^2 \equiv 3^2 - 6 \pmod{13}$. Dengan demikian $(x+3)^2 \equiv 16 \pmod{13}$, sehingga $x \equiv 1 \pmod{13}$ atau $x \equiv 6 \pmod{13}$.
- 2) Dari bilangan-bilangan 1, 2, 3, 4 dapat ditentukan bahwa $1^2 \equiv 1 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, $3^2 \equiv 9 \equiv 4 \pmod{5}$, dan $4^2 \equiv 16 \equiv 1 \pmod{5}$. Dengan demikian $x^2 \equiv 1 \pmod{5}$ mempunyai dua solusi $x = 1$ dan $x = 4$, $x^2 \equiv 4 \pmod{5}$ mempunyai dua solusi $x = 2$ dan $x = 3$, sedangkan $x^2 \equiv 2 \pmod{5}$ dan $x^2 \equiv 3 \pmod{5}$ tidak mempunyai solusi.
- Jadi residu-residu kuadratis modulo 5 adalah 1 dan 4, dan bukan residu-residu kuadratis modulo 5 adalah 2 dan 3.
- 3) (a) Menurut Teorema 5.3, $\begin{bmatrix} 5 \\ 11 \end{bmatrix} \equiv 5^{(11-1)/2} \pmod{11} \equiv 5^5 \pmod{11} \equiv 5^2 \cdot 5^2 \cdot 5 \pmod{11} \equiv 3.3.5 \pmod{11} \equiv 45 \pmod{11} \equiv 1 \pmod{11}$, berarti kongruensi dapat diselesaikan.
 $x^2 \equiv 5 \pmod{11} \equiv 16 \pmod{11}$.
Jadi $x \equiv 4 \pmod{11}$ atau $x \equiv 7 \pmod{11}$

(b) Menurut Teorema 5.4. (a) dan (c):

$$\left[\frac{72}{11} \right] = \left[\frac{36 \cdot 2}{11} \right] = \left[\frac{36}{11} \right] \left[\frac{2}{11} \right] = \left[\frac{6^2}{11} \right] \left[\frac{2}{11} \right] = 1 \cdot \left[\frac{2}{11} \right] = \left[\frac{2}{11} \right]$$

dan menurut Teorema 5.3,

$$\left[\frac{2}{11} \right] \equiv 2^{(11-1)/2} \pmod{11} \equiv 2^5 \pmod{11} \equiv -1 \pmod{11}$$

Karena $\left[\frac{2}{11} \right] = -1$, maka kongruensi tidak mempunyai selesaian.

- 4) (a) Buat barisan $5k$ dengan $k = 1, 2, 3, \dots, (19-1)/2$ diperoleh $5, 10, 15, 20, 25, 30, 35, 40, 45$, sehingga barisan residu positif terkecil modulo 5 adalah $5, 10, 15, 1, 6, 11, 16, 2, 7$. Banyaknya unsur barisan residu positif terkecil yang lebih dari $(19/2)$ adalah 4, yaitu $10, 15, 11, 16$.

Dengan demikian sesuai Lemma Gauss $\left[\frac{5}{19} \right] = (-1)^4 = 1$, berarti

kongruensi dapat diselesaikan.

Karena $x^2 \equiv 5 \pmod{19} \equiv 5 + 4 \cdot 19 \pmod{19} \equiv 81 \pmod{19}$, maka selesaian kongruensi adalah $x \equiv 9 \pmod{19}$ atau $x \equiv 10 \pmod{19}$.

- (b) $x^2 \equiv 58 \pmod{77} \equiv 58 \pmod{7 \cdot 11}$. Karena $7 \mid 77$ dan $11 \mid 77$, maka $x^2 \equiv 58 \pmod{7}$ dan $x^2 \equiv 58 \pmod{11}$, atau $x^2 \equiv 2 \pmod{7}$ dan $x^2 \equiv 3 \pmod{11}$.

Dari $x^2 \equiv 2 \pmod{7}$ diperoleh $x \equiv 3 \pmod{7}$ atau $x \equiv 4 \pmod{7}$, dan dari $x^2 \equiv 3 \pmod{11}$ diperoleh $x \equiv 5 \pmod{11}$ atau $x \equiv 6 \pmod{11}$.

Dengan demikian terdapat 4 kemungkinan sistem kongruensi linier simultan, $x \equiv 3 \pmod{7}$ dan $x \equiv 5 \pmod{11}$, $x \equiv 3 \pmod{7}$ dan $x \equiv 6 \pmod{11}$, $x \equiv 4 \pmod{7}$ dan $x \equiv 5 \pmod{11}$, $x \equiv 4 \pmod{7}$ dan $x \equiv 6 \pmod{11}$, dan menghasilkan 4 selesaian $x \equiv 38, 17, 39, 60 \pmod{77}$.

- 5) $\left[\frac{-15}{61} \right] \equiv (-15)^{(p-1)/2} \pmod{61} \equiv (-15)^{(61-1)/2} \pmod{61} \equiv (-15)^{30} \pmod{61}$
 $\equiv 15^{30} \pmod{61}$

$15 \equiv 15 \pmod{61}$, $15^2 = 225 \equiv 42 \pmod{61}$, $15^4 = 1764 \equiv 56 \pmod{61}$,
 $15^8 = 3136 \equiv 25 \pmod{61}$, dan $15^{16} = 625 \equiv 15 \pmod{61}$

$$\left[\frac{-15}{61} \right] \equiv 15^{30} \pmod{61} \equiv 15^{16} \cdot 15^8 \cdot 15^4 \cdot 15^2 \pmod{61}$$

$$\equiv 15 \cdot 25 \cdot 56 \cdot 42 \pmod{61} \equiv 1 \pmod{61}$$

Jadi $x^2 + 15 \equiv 0 \pmod{61}$ mempunyai selesaian, diperoleh dengan cara:

$$x^2 \equiv -5 \pmod{61} \equiv 46 \pmod{61} \equiv 46 + 14 \cdot 61 \pmod{61} \equiv 900 \pmod{61}$$

Selesaian $x \equiv 30 \pmod{61}$ dan $x \equiv 31 \pmod{61}$.



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep kongruensi kuadratis, konsep residu kuadratis, lambang Legendre dan manfaatnya untuk menetapkan keterselesaian kongruensi kuadratis, kriteria Euler dan Lemma Gauss untuk menghitung nilai Lambang Legendre, cara memperoleh selesaian kongruensi kuadratis, dan keterkaitan sistem kongruensi linier simultan untuk menyelesaikan kongruensi kuadratis tertentu.

1. **Definisi 5.1** tentang residu kuadratis dan bukan residu kuadratis

2. **Definisi 5.2** tentang Lambang Legendre

3. Teorema 5.1

Ditentukan p adalah suatu bilangan prima ganjil. Setiap sistem residu tereduksi modulo p tepat memuat $(p-1)/2$ residu-residu kuadratis, dan tepat memuat $(p-1)/2$ bukan residu-residu kuadratis modulo p .

Residu-residu kuadratis merupakan unsur dari kelas residu yang memuat bilangan-bilangan: $1^2, 2^2, 3^2, \dots, [(p-1)/2]^2$.

4. Teorema 5.2

Ditentukan k adalah suatu bilangan bulat, p adalah suatu bilangan prima ganjil, dan $(k, p) = 1$. Jika kongruensi $x^2 \equiv k \pmod{p}$ dapat diselesaikan, maka terdapat tepat dua selesaian yang tidak kongruen modulo p .

5. Teorema 5.3 Kriteria Euler

Jika p adalah suatu bilangan prima dan k adalah suatu bilangan bulat positif yang tidak habis dibagi oleh p , maka:

$$\left[\frac{k}{p} \right] \equiv a^{(p-1)/2} \pmod{p}$$

6. Teorema 5.4

Ditentukan bahwa $m, n \in \mathbb{Z}$, p adalah suatu bilangan prima ganjil, p tidak membagi m dan n , maka:

(a) $\left[\frac{m}{p} \right] \left[\frac{n}{p} \right] = \left[\frac{mn}{p} \right]$

(b) jika $m \equiv n \pmod{p}$, maka $\left[\frac{m}{p} \right] = \left[\frac{n}{p} \right]$

(c) $\left[\frac{m^2}{p} \right] = 1$

(d) $\left[\frac{m^2 n}{p} \right] = \left[\frac{n}{p} \right]$

(e) $\left[\frac{1}{p} \right] = +1$ dan $\left[\frac{-1}{p} \right] = (-1)^{(p-1)/2}$

7. Teorema 5.5

Jika p adalah suatu bilangan prima ganjil, maka:

$$\left[\frac{-1}{p} \right] = \begin{cases} 1, & \text{jika } p \equiv 1 \pmod{4} \\ -1, & \text{jika } p \equiv 3 \pmod{4} \end{cases}$$

8. Teorema 5.6 (Lemma Gauss)

Ditentukan p adalah suatu bilangan prima ganjil, $k \in \mathbb{Z}$, dan $(k, p) = 1$. Jika r adalah banyaknya residu positif terkecil dari

$k, 2k, 3k, \dots, \left[\frac{p-1}{2} \right] k$ yang lebih dari $\frac{p}{2}$ maka $\left[\frac{k}{p} \right] = (-1)^r$.



- 1) Skor 5
Carilah residu-residu kuadratis dan bukan residu kuadratis modulo 7
- 2) Skor 5
Selidiki apakah 8 merupakan suatu residu kuadratis modulo 17, dan 7 merupakan residu kuadratis modulo 23
- 3) Skor 10
Carilah semua selesaian dari $x^2 \equiv 207 \pmod{1001}$

4) Skor 10

Selesaikan $x^2 + 995x - 1110 \equiv 0 \pmod{1009}$

5) Skor 10

Selesaikan sistem kongruensi kuadratis $3x^2 \equiv 7 \pmod{17}$ dan $5x^2 - 2x \equiv 3 \pmod{12}$

6) Skor 10

Selesaikan $21x^2 - 23x - 19 \equiv 0 \pmod{71}$

7) Skor 10

Selesaikan $19x^2 - 12x + 8 \equiv 0 \pmod{97}$

8) Skor 10

Tunjukkan bahwa jika p adalah suatu bilangan prima, maka:

$$\left[\frac{-2}{p} \right] = \begin{cases} +1, & \text{jika } p \equiv 1, 3 \pmod{8} \\ -1, & \text{jika } p \equiv 5, 7 \pmod{8} \end{cases}$$

9) Skor 10

Tunjukkan bahwa jika pemfaktoran prima dari n adalah:

$$n = p_1^{2t_1+1} p_2^{2t_2+1} \cdots p_k^{2t_k+1} p_{k+1}^{2t_{k+1}+1} \cdots p_m^{2t_m}.$$

dan q adalah suatu bilangan prima yang tidak membagi n , maka

$$\left[\frac{n}{q} \right] = \left[\frac{p_1}{q} \right] \left[\frac{p_2}{q} \right] \cdots \left[\frac{p_k}{q} \right].$$

10) Skor 10

Tunjukkan bahwa jika b adalah suatu bilangan bulat positif tidak habis dibagi oleh p , maka:

$$\left[\frac{b}{p} \right] + \left[\frac{2b}{p} \right] + \left[\frac{3b}{p} \right] + \cdots + \left[\frac{(p-1)b}{p} \right] = 0$$

11) Skor 10

Tunjukkan bahwa jika a adalah suatu residu kuadratis modulo p , maka selesaian dari:

$$x^2 \equiv a \pmod{p} \text{ adalah } x \equiv \pm a^{n+1} \pmod{p} \text{ jika } p = 4n+3.$$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$
--

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Kebalikan Kuadratis**

Kebalikan kuadrat merupakan pembahasan yang terkait dengan cara mencari nilai lambang Legendre yang langkahnya dilakukan dengan membalik letak lambangnya setelah syarat-syarat tertentu dipenuhi.

Jika p dan q adalah bilangan-bilangan prima ganjil, dan p adalah residu kuadratis modulo q , yaitu:

$$\left[\frac{p}{q} \right] = 1$$

maka apakah q merupakan suatu residu kuadratis modulo p , yaitu:

$$\left[\frac{q}{p} \right] = 1 ?$$

Secara empiris pertanyaan ini telah dijawab oleh Euler pada pertengahan abad 17, dengan menggunakan bukti numerik. Secara eksplisit bukti formal pertama telah dibuat oleh Gauss, yang kemudian dikembangkan secara modern dan ketat oleh Legendre pada tahun 1785, yang kemudian dikenal dengan **Hukum Kebalikan Kuadrat**.

Untuk mengetahui apakah $x^2 \equiv q \pmod{p}$ mempunyai solusi, maka sesuai dengan hukum kebalikan kuadrat, perlu diselidiki apakah $x^2 \equiv p \pmod{p}$ mempunyai solusi. Penyelidikan ini menjadi semakin jelas jika kita menggunakan teorema lain yang terkait dengan Teorema 5.6 (Lemma Gauss). Karena teorema ini relatif sulit dipahami, maka marilah kita lihat peragaan yang dapat memberikan kejelasan dalam langkah-langkah menuju pembuktian hukum kebalikan kuadrat.

Misalkan ditentukan bahwa $k = 7$ dan $p = 17$, berarti k adalah suatu bilangan bulat positif ganjil, p adalah suatu bilangan prima ganjil, dan $(k, p) = 1$. Barisan residu positif terkecil modulo p adalah barisan ak , dengan $k = 7$ dan $a = 1, 2, 3, \dots, (17 - 1)/2$, yaitu:

1.7, 2.7, 3.7, 4.7, 5.7, 6.7, 7.7, 8.7, atau 7, 14, 21, 28, 35, 42, 49, 56
dan dalam modulo $p = 17$ dapat dinyatakan sebagai:

$$7, 14, 4, 11, 1, 8, 15, 5$$

Barisan residu positif terkecil lebih dari $p/2 = 17/2 = 8.5$ adalah:

$$u_1 = 11, u_2 = 14, u_3 = 15$$

dan barisan residu positif terkecil kurang dari $p/2 = 17/2 = 8.5$ adalah:

$$v_1 = 1, v_2 = 4, v_3 = 5, v_4 = 7, v_5 = 8$$

Perhatikan bahwa:

$$7 = 1.7 = 17[(1.7)/17] + 7$$

$$14 = 2.7 = 17[(2.7)/17] + 14$$

$$21 = 3.7 = 17[(3.7)/17] + 4$$

$$28 = 4.7 = 17[(4.7)/17] + 11$$

$$35 = 5.7 = 17[(5.7)/17] + 1$$

$$42 = 6.7 = 17[(6.7)/17] + 8$$

$$49 = 7.7 = 17[(7.7)/17] + 15$$

$$56 = 8.7 = 17[(8.7)/17] + 5$$

yang mana masing-masing keadaan sesuai dengan pembagian algoritma, yaitu:

$$ak = p[(ik)/p] + r_k, \text{ dengan } r_k = u_k \text{ atau } r_k = v_k$$

Jumlah dari semua keadaan adalah:

$$\sum_{a=1}^{(p-1)/2} ak = \sum_{a=1}^{(p-1)/2} p[(ak)/p] + \sum_{a=1}^i u_a + \sum_{a=1}^j v_a \quad \dots \quad (1)$$

Sesuai dengan Teorema 5.6 Lemma Gauss, barisan bilangan:

$$p - u_1 = 6, p - u_2 = 3, p - u_3 = 2, v_1 = 1, v_2 = 4, v_3 = 5, v_4 = 7, v_5 = 8$$

merupakan barisan bilangan 1, 2, 3, 4, 5, 6, 7, $(17 - 1)/2 = 8$ dengan urutan yang berbeda. Jika semua suku barisan dijumlahkan, maka diperoleh:

$$\sum_{a=1}^{(p-1)/2} a = \sum_{a=1}^{(p-1)/2} (p - u_a) + \sum_{a=1}^j v_a = \sum_{a=1}^i p - \sum_{a=1}^i u_a + \sum_{a=1}^j v_a$$

$$\sum_{a=1}^{(p-1)/2} a = pi - \sum_{a=1}^i u_a + \sum_{a=1}^j v_a \quad \dots \quad (2)$$

Jika keadaan (1) dikurangi (2), maka diperoleh:

$$\sum_{a=1}^{(p-1)/2} ak - \sum_{a=1}^{(p-1)/2} a = \sum_{a=1}^{(p-1)/2} p[(ak)/p] - pi + 2\sum_{a=1}^i u_a$$

$$(k-1) \sum_{a=1}^{(p-1)/2} a = p \sum_{a=1}^{(p-1)/2} [(ak)/p] - pi + 2\sum_{a=1}^i u_a$$

Jika ditentukan bahwa $H(k, p) = \sum_a^{(p-1)/2} [(ak)/p]$, maka:

$$(k-1) \sum_{a=1}^{(p-1)/2} a = pH(a, p) - pi + 2\sum_{a=1}^i u_a \quad \dots \quad (3)$$

Karena k adalah suatu bilangan ganjil, maka $k \equiv 1 \pmod{2}$, sehingga $(k-1) \equiv 0 \pmod{2}$.

Demikian pula, karena p adalah suatu bilangan ganjil, maka $p \equiv 1 \pmod{2}$, sehingga jika (3) dinyatakan dalam modulo 2, maka diperoleh:

$$0 \equiv \{1.H(k, p) - 1.i + 0\} \pmod{2} \equiv \{H(k, p) - i\} \pmod{2}$$

$$H(k, p) \equiv i \pmod{2}$$

Karena $\left(\frac{k}{p}\right) = (-1)^i$ dan $i = H(k, p)$, maka $\left(\frac{k}{p}\right) = (-1)^{H(k, p)}$

Teorema 5.7

Jika k adalah suatu bilangan bulat ganjil, p adalah suatu bilangan prima ganjil, $(k, p) = 1$, dan $H(k, p) = \sum_{a=1}^{(p-1)/2} [(ak)/p]$, maka $\left(\frac{k}{p}\right) = (-1)^{H(k, p)}$

Bukti:

Barisan residu positif terkecil ak , dengan $a = 1, 2, 3, \dots, (p-1)/2$, adalah

$$k, 2k, 3k, \dots, [(p-1)/2]k,$$

dimana suku-suku barisan yang nilainya lebih dari $p/2$ adalah u_1, u_2, \dots, u_i dan suku-suku barisan yang nilanya kurang dari $p/2$ adalah v_1, v_2, \dots, v_j .

Menurut Teorema Pembagian Algoritma, suku-suku barisan ak dapat dinyatakan sebagai:

$$\sum_{a=1}^{(p-1)/2} ak = \sum_{a=1}^{(p-1)/2} p[(ak)/p] + \sum_{a=1}^i u_a + \sum_{a=1}^j v_a \quad \dots \quad (4)$$

Menurut Teorema 5.6 Lemma Gauss, barisan

$$p - u_1, p - u_2, \dots, p - u_i, v_1, v_2, \dots, v_j$$

sama dengan barisan $1, 2, 3, \dots, (p-1)/2$ dengan urutan yang berbeda sehingga:

$$\begin{aligned} \sum_{a=1}^{(p-1)/2} a &= \sum_{a=1}^{(p-1)/2} (p - u_a) + \sum_{a=1}^j v_a = \sum_{a=1}^i p - \sum_{a=1}^i u_a + \sum_{a=1}^j v_a \\ \sum_{a=1}^{(p-1)/2} a &= pi - \sum_{a=1}^i u_a + \sum_{a=1}^j v_a \quad \dots \quad (5) \end{aligned}$$

Jika keadaan (4) dikurangi keadaan (5), maka diperoleh:

$$\begin{aligned} \sum_{a=1}^{(p-1)/2} ak - \sum_{a=1}^{(p-1)/2} a &= \sum_{a=1}^{(p-1)/2} p[(ak)/p] - pi + 2 \sum_{a=1}^i u_a \\ (k-1) \sum_{a=1}^{(p-1)/2} a &= p \sum_{a=1}^{(p-1)/2} [(ak)/p] - pi + 2 \sum_{a=1}^i u_a \quad \dots \quad (6) \end{aligned}$$

Karena $H(k, p) = \sum_a^{(p-1)/2} [(ak)/p]$ dengan k adalah suatu bilangan ganjil, $k \equiv 1 \pmod{2}$, dan p adalah suatu bilangan prima ganjil, $p \equiv 1 \pmod{2}$, maka dalam modulo 2, hubungan (3) dapat dinyatakan sebagai:

$$(1-1) \quad \sum_{a=1}^{(p-1)/2} a \equiv \{1 \sum_{a=1}^{(p-1)/2} [(ak)/p] - 1i + 0\} \pmod{2}$$

$$0 \equiv \{H(k, p) - i\} \pmod{2}, \text{ atau } i = H(k, p)$$

Jadi, sesuai Teorema 5.6 Lemma Gauss, karena $\left(\frac{k}{p}\right) = (-1)^i$ dan $i = H(k, p)$,

maka $\left(\frac{k}{p}\right) = (-1)^{H(k, p)}$

Contoh 5.17

Carilah nilai dari masing-masing lambang Legendre:

(a) $\left(\frac{3}{11}\right)$

(b) $\left(\frac{11}{17}\right)$

Jawab:

(a) $\frac{p-1}{2} = \frac{11-1}{2} = 5$

$$H(3,11) = \sum_{a=1}^5 [(3a)/11] = [3/11] + [6/11] + [9/11] + [12/11] + [15/11]$$

$$= 0 + 0 + 0 + 1 + 1 = 2$$

$$\left(\frac{3}{11}\right) = (-1)^{H(3,11)} = (-1)^2 = 1$$

(b) $\frac{p-1}{2} = \frac{17-1}{2} = 8$

$$H(11,17) = \sum_{a=1}^8 [(11a)/17]$$

$$= [11/17] + [22/17] + [33/17] + [44/17] + [55/17] + [66/17]$$

$$= [11/17] + [22/17] + [33/17] + [44/17] + [55/17] + [66/17]$$

$$+ [77/17] + [88/17]$$

$$\begin{aligned}
 &= 0 + 1 + 1 + 2 + 3 + 3 + 4 + 5 = 19 \\
 \left(\frac{11}{17}\right) &= (-1)^{H(11,17)} = (-1)^{19} = -1
 \end{aligned}$$

Marilah sekarang kita melihat suatu peragaan sebelum kita membuktikan hukum kebalikan kuadratis. Peragaan ini perlu dilakukan untuk memudahkan pemahaman kita dalam mengikuti langkah-langkah pembuktian hukum kebalikan kuadratis.

Kita tentukan dua bilangan prima ganjil $p = 5$ dan $q = 13$, kemudian kita buat barisan a dengan nilai-nilai $1 \leq a \leq (5-1)/2$ dan barisan b dengan nilai-nilai $1 \leq b \leq (13-1)/2$, sehingga diperoleh:

$$\begin{aligned}
 a &= 1, 2 \\
 b &= 1, 2, 3, 4, 5, 6
 \end{aligned}$$

Banyaknya pasangan (a, b) adalah 12, yaitu:

$$(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,1), (2,2), (2,3), (2,4), (2,5), (2,6).$$

Masing-masing pasangan tidak ada yang memenuhi hubungan $13a = 5b$ sebab kalau $5b = 13a$, maka $13 \mid 5b$, dan karena $(13,5) = 1$, maka seharusnya $13 \mid b$. Hal ini tidak mungkin terjadi karena $b = 1, 2, 3, 4, 5, 6 < 13$.

Pasangan (a, b) dipisahkan menjadi dua kelompok , yaitu

$$(1) \quad 1 \leq a \leq 2, 1 \leq b \leq 6, 13a < 5b, \text{diperoleh } (1,3), (1,4), (1,5), (1,6), (2,6)$$

Banyaknya pasangan adalah 5, dan dapat dicari bahwa:

$$\begin{aligned}
 \sum_{i=1}^6 [(5i)/13] &= [(5.1)/13] + [(5.2)/13] + [(5.3)/13] + [(5.4)/13] \\
 &\quad + [(5.5)/13] + [(5.6)/13] \\
 &= [5/13] + [10/13] + [15/13] + [20/13] + [25/13] + [30/13] \\
 &= 0+0+1+1+1+2 = 5
 \end{aligned}$$

$$(2) \quad 1 \leq a \leq 2, 1 \leq b \leq 6, 13a > 5b, \text{diperoleh}$$

$$(1,1), (1,2), (2,1), (2,2), (2,3), (2,4), (2,5)$$

Banyaknya pasangan adalah 7, dan dapat dicari bahwa:

$$\sum_{i=1}^2 [(3i)/5] = [(13.1)/5] + [(13.2)/5] = [13/5] + [26/5] = 2 + 5 = 7$$

Karena kedua kelompok merupakan hasil pemisahan 12 pasangan (a, b) , maka

$$\frac{5-1}{2} \cdot \frac{13-1}{2} = 2 \cdot 6 = 12$$

$$\sum_{i=1}^6 [(5i)/13] + \sum_{i=1}^2 [(3i)/5] = 5 + 7 = 12,$$

$$\text{sehingga } \frac{5-1}{2} \cdot \frac{13-1}{2} = \sum_{i=1}^6 [(5i)/13] + \sum_{i=1}^2 [(3i)/5].$$

Dengan demikian dapat ditunjukkan bahwa:

$$\begin{aligned} (-1)^{\{(5-1)/2\}\{(13-1)/2\}} &= (-1)^{\sum_{i=1}^6 [(5i)/13] + \sum_{i=1}^2 [(13i)/5]} \\ (-1)^{12} &= (-1)^{\sum_{i=1}^6 [(5i)/13]} \cdot (-1)^{\sum_{i=1}^2 [(13i)/5]} \end{aligned}$$

Menurut Teorema 5.7,

$$\begin{aligned} (1) \quad H(5,13) &= \sum_{a=1}^6 [(5a)/13] = [5/13] + [10/13] + [15/13] + [20/13] \\ &\quad + [25/13] + [30/13] \\ &= 0 + 0 + 1 + 1 + 1 + 2 = 5 \end{aligned}$$

$$\left[\frac{5}{13} \right] = (-1)^{H(5,13)} = (-1)^5$$

$$(2) \quad H(13,5) = \sum_{a=1}^2 [(13a)/5] = [13/5] + [26/5] = 2 + 5 = 7$$

$$\left[\frac{13}{5} \right] = (-1)^{H(13,5)} = (-1)^7$$

$$\text{Jadi } \left[\frac{5}{13} \right] \left[\frac{13}{5} \right] = (-1)^5 \cdot (-1)^7 = (-1)^{12} = (-1)^{2 \cdot 6} = (-1)^{\{(5-1)/2\}\{(13-1)/2\}}$$

Teorema 5.8 Hukum Kebalikan Kuadrat

Jika p dan q adalah bilangan-bilangan prima ganjil, maka:

$$\left[\frac{p}{q} \right] \left[\frac{q}{p} \right] = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$$

Bukti:

Kita buat suatu barisan a dengan $1 \leq a \leq (p-1)/2$ dan suatu barisan b dengan $1 \leq b \leq (q-1)/2$, maka diperoleh pasangan (a,b) sebanyak $\{(p-1)/2\}\{(q-1)/2\}$. Pasangan-pasangan ini kemudian kita pisahkan menjadi dua kelompok:

- (1) Kelompok yang unsur-unsurnya memenuhi hubungan $1 \leq a \leq (p-1)/2$, $1 \leq b \leq (q-1)/2$, dan $qa < pb$. Untuk suatu nilai tertentu b dengan $1 \leq b \leq (q-1)/2$, terdapat $[(pb)/q]$ bilangan bulat yang memenuhi $1 \leq a \leq (pb)/q$. Banyaknya pasangan (a,b) yang memenuhi hubungan tersebut adalah $\sum_{i=1}^{(q-1)/2} [(pi)/q]$.
- (2) Kelompok yang unsur-unsurnya memenuhi hubungan $1 \leq a \leq (p-1)/2$, $1 \leq b \leq (q-1)/2$, dan $qa > pb$. Untuk suatu nilai tertentu a dengan $1 \leq a \leq (p-1)/2$, terdapat $[(qa)/p]$ bilangan bulat yang memenuhi $1 \leq b \leq (qa)/p$. Banyaknya pasangan (a,b) yang memenuhi hubungan tersebut adalah $\sum_{i=1}^{(p-1)/2} [(qi)/p]$

Dari hasil (1) dan (2) dapat kita tentukan bahwa

$$\sum_{i=1}^{(q-1)/2} [(pi)/q] + \sum_{i=1}^{(p-1)/2} [(qi)/p] = \frac{q-1}{2} \cdot \frac{p-1}{2}$$

$$H(p, q) + H(q, p) = \frac{q-1}{2} \cdot \frac{p-1}{2}$$

$$(-1)^{H(p,q)+H(q,p)} = (-1)^{\{(q-1)/2\}\{(p-1)/2\}}, \text{ atau}$$

$$(-1)^{H(p,q)} = (-1)^{H(q,p)} = (-1)^{\{(q-1)/2\}\{(p-1)/2\}}$$

Jadi $\left[\frac{p}{q} \right] \left[\frac{q}{p} \right] = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$

Contoh 5.18

Carilah nilai dari $\left(\frac{p}{q} \right) \left(\frac{q}{p} \right)$ jika:

- (a) $p = 7$ dan $q = 17$
 (b) $p = 13$ dan $q = 23$

Jawab:

$$(a) \left(\frac{7}{17} \right) \left(\frac{17}{7} \right) = (-1)^{\{(7-1)/2\}\{(17-1)/2\}} = (-1)^{3.8} = (-1)^{24} = 1$$

$$(b) \left(\frac{13}{23}\right)\left(\frac{23}{13}\right) = (-1)^{\{(13-1)/2\}\{(23-1)/2\}} = (-1)^{6.11} = (-1)^{66} = 1$$

Teorema 5.9

Jika p dan q adalah bilangan-bilangan prima ganjil, maka:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{jika } p \equiv 1 \pmod{4} \text{ atau } q \equiv 1 \pmod{4} \\ -1, & \text{jika } p \equiv 3 \pmod{4} \text{ dan } q \equiv 3 \pmod{4} \end{cases}$$

Bukti:

- (1) Jika $p \equiv 1 \pmod{4}$ atau $p = 4k + 1$, dengan $k \in \mathbb{Z}$, maka

$$(p-1)/2 = (4k+1-1)/2 = (4k)/2 = 2k$$

Dengan demikian $\frac{p-1}{2} \cdot \frac{q-1}{2}$ merupakan bilangan bulat genap.

- (2) Jika $q \equiv 1 \pmod{4}$ atau $q = 4t + 1$, dengan $t \in \mathbb{Z}$, maka

$$(q-1)/2 = (4t+1-1)/2 = (4t)/2 = 2t$$

Dengan demikian $\frac{p-1}{2} \cdot \frac{q-1}{2}$ merupakan bilangan bulat genap.

Dari keadaan (1) dan (2) dapat ditentukan bahwa jika $p \equiv 1 \pmod{4}$ atau

$q \equiv 1 \pmod{4}$ maka nilai $\frac{p-1}{2} \cdot \frac{q-1}{2}$ merupakan bilangan bulat genap,

sehingga sesuai dengan Teorema 5.8, dapat disimpulkan bahwa

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(q-1)/2\}\{(p-1)/2\}}$$

- (3) p dan q masing-masing tidak mungkin kongruen dengan 2 modulo 4 sebab jika $p \equiv 2 \pmod{4}$ atau $q \equiv 2 \pmod{4}$, maka $p = 4r + 2 = 2(2r + 1)$ dan $q = 4s + 2 = 2(2s + 2)$, yaitu p dan q merupakan bilangan bulat genap, bukan bilangan prima ganjil.

- (4) Jika $p \equiv 3 \pmod{4}$ atau $p = 4m + 3$, maka

$(p-1)/2 = (4m+3-1)/2 = 2m+1$ merupakan suatu bilangan bulat ganjil.

- (5) Jika $q \equiv 3 \pmod{4}$ atau $q = 4n + 3$, maka

$(q-1)/2 = (4n+3-1)/2 = 2n+1$ merupakan suatu bilangan bulat ganjil.

Dari keadaan (4) dan (5) dapat ditentukan bahwa jika $p \equiv 3(\text{mod } 4)$ dan $q \equiv 3(\text{mod } 4)$ maka nilai $\frac{p-1}{2} \cdot \frac{q-1}{2}$ merupakan bilangan bulat ganjil, sehingga sesuai dengan Teorema 5.8, dapat disimpulkan bahwa $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(q-1)/2\}\{(p-1)/2\}} = -1$.

Teorema 5.10

Jika p dan q adalah bilangan-bilangan prima ganjil, maka

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{jika } p \equiv 1(\text{mod } 4) \text{ atau } q \equiv 1(\text{mod } 4) \\ -1\left(\frac{q}{p}\right), & \text{jika } p \equiv 3(\text{mod } 4) \text{ atau } q \equiv 3(\text{mod } 4) \end{cases}$$

Bukti:

Sesuai dengan Teorema 5.9, kemungkinan nilai $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ adalah 1 atau -1.

(1) Jika $p \equiv 1 (\text{mod } 4)$ atau $q \equiv 1 (\text{mod } 4)$, maka $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. Dengan demikian $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$ atau $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$.

Jadi $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ jika $p \equiv 1 (\text{mod } 4)$ atau $q \equiv 1 (\text{mod } 4)$

(2) Jika $p \equiv 3 (\text{mod } 4)$ atau $q \equiv 3 (\text{mod } 4)$, maka $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$.

Dengan demikian $\left(\frac{p}{q}\right) = 1$ dan $\left(\frac{q}{p}\right) = -1$, yaitu $\left(\frac{p}{q}\right) = -1\left(\frac{q}{p}\right)$

atau $\left(\frac{p}{q}\right) = -1$ dan $\left(\frac{q}{p}\right) = 1$, yaitu $\left(\frac{p}{q}\right) = -1\left(\frac{q}{p}\right)$

Jadi $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ jika $p \equiv 3 (\text{mod } 4)$ dan $q \equiv 3 (\text{mod } 4)$

Contoh 5.19

Selesaikan kongruensi-kongruensi kuadratis.

- $x^2 \equiv 7 \pmod{19}$
- $x^2 \equiv 11 \pmod{17}$

Jawab:

- Karena $19 \equiv 3 \pmod{4}$ dan $7 \equiv 3 \pmod{4}$, maka sesuai Teorema 5.10:

$$\left(\frac{7}{19}\right) = -1 \left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right)$$

Karena $5 \equiv 1 \pmod{4}$, maka sesuai Teorema 5.10:

$$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right)$$

dan sesuai jawaban tugas pada Kegiatan Belajar 1:

$$\left(\frac{2}{5}\right) = (-1)^{(5^2-1)/8} = (-1)^{(25-1)/8} = (-1)^3 = -1$$

Dengan demikian $\left(\frac{7}{19}\right) = -1 \left(\frac{2}{5}\right) = (-1)(-1) = 1$, berarti $x^2 \equiv 7 \pmod{19}$

dapat diselesaikan dan

$$x^2 \equiv 7 \pmod{19} \equiv 7 + 3 \cdot 19 \pmod{19} \equiv 64 \pmod{19}, \quad x \equiv 8 \pmod{19}.$$

- Karena $17 \equiv 1 \pmod{4}$, meskipun $11 \equiv 3 \pmod{4}$ maka sesuai Teorema 5.10:

$$\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{17}\right) = \left(\frac{2 \cdot 3}{17}\right) = \left(\frac{2}{17}\right) \left(\frac{3}{17}\right)$$

$$\left(\frac{2}{11}\right) = (-1)^{(11^2-1)/8} = (-1)^{(121-1)/8} = (-1)^{15} = -1$$

$$\left(\frac{3}{11}\right) = -1 \left(\frac{11}{3}\right) = -1 \left(\frac{2}{3}\right) = (-1)(-1) = 1$$

Karena $\left(\frac{11}{17}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) = (-1)(1) = -1$, maka $x^2 \equiv 11 \pmod{17}$

tidak dapat diselesaikan.

Tugas

Bacalah suatu buku tentang teori bilangan, misalnya *Elementary Number Theory and Its Applications* dari Kenneth Rosen, carilah topik Lambang Jacobi.

Sebutkan definisi tentang Lambang Jacobi, berilah dua contoh, jelaskan hubungannya dengan Lambang Legendre, sebutkan teorema-teorema yang terkait dengan Lambang Jacobi, kemudian carilah:

$$(a) \left(\begin{matrix} 105 \\ 317 \end{matrix} \right)$$

$$(b) \left(\begin{matrix} 213 \\ 499 \end{matrix} \right)$$

Petunjuk Jawaban Tugas

Lambang Jacobi diperkenalkan oleh Carl Gustav Jacob Jacobi, seorang matematisi Jerman tahun 1804-1851. Lambang Jacobi merupakan penggeneralisasian dari Lambang Legendre, mempunyai sifat-sifat yang bersesuaian dengan Lambang Legendre.

Definisi

Jika q adalah suatu bilangan bulat positif, maka q mempunyai faktor-faktor prima sehingga q dapat dinyatakan sebagai $q = q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}$, $p \in \mathbb{Z}$ sehingga

$(p, q) = 1$, maka lambang Jacobi $\left[\frac{p}{q} \right]$ didefinisikan sebagai:

$$\left[\frac{p}{q} \right] = \left[\frac{p}{q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}} \right] = \left[\frac{p}{q_1} \right]^{k_1} \left[\frac{p}{q_2} \right]^{k_2} \dots \left[\frac{p}{q_t} \right]^{k_t} = \prod_{j=1}^t \left(\frac{p}{q_j} \right)$$

yang mana $\left(\frac{p}{q_j} \right)$ dengan $j = 1, 2, \dots, t$ adalah lambang-lambang Legendre.

Contoh:

$$(1) \left[\frac{7}{75} \right] = \left[\frac{7}{25 \cdot 3} \right] = \left[\frac{7}{5^2 \cdot 3} \right] = \left(\frac{7}{5^2} \right) \left(\frac{7}{3} \right) = \left(\frac{2}{5} \right)^2 \left(\frac{1}{3} \right) = (-1)^2 \cdot 1 = 1$$

$$(2) \left[\frac{88}{105} \right] = \left[\frac{88}{3 \cdot 5 \cdot 7} \right] = \left[\frac{88}{3} \right] \left[\frac{88}{5} \right] \left[\frac{88}{7} \right] = \left[\frac{1}{3} \right] \left[\frac{3}{5} \right] \left[\frac{4}{7} \right] = 1 \cdot 1 \cdot 1 = 1$$

Hubungan antara Lambang Jacobi dan Lambang Legendre adalah apabila q adalah suatu bilangan prima, maka Lambang Jacobi menjadi Lambang

Legendre, tetapi apabila q adalah suatu bilangan komposit, nilai dari $\left(\frac{k}{q}\right)$ tidak ada hubungannya dengan keterselesaian $x^2 \equiv k \pmod{q}$. Sebagai peragaan, $\left[\frac{2}{15}\right] = \left[\frac{2}{3.5}\right] = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, tetapi $x^2 \equiv 2 \pmod{15}$ tidak mempunyai selesaian karena $x \equiv 2 \pmod{3}$ dan $x \equiv 2 \pmod{5}$ tidak mempunyai selesaian.

Beberapa teorema tentang Lambang Jacobi adalah:

$$(1) \text{ jika } p \equiv r \pmod{q}, \text{ maka } \left[\frac{p}{q}\right] = \left[\frac{r}{q}\right]$$

$$(2) \left[\frac{pr}{q}\right] = \left[\frac{p}{q}\right]\left[\frac{r}{q}\right]$$

$$(3) \left[\frac{-1}{q}\right] = (-1)^{(n-1)/2}$$

$$(4) \left[\frac{2}{q}\right] = (-1)^{(n^2-1)/8}$$

$$(5) \left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}}$$

$$(6) \left[\frac{-1}{q}\right] = (-1)^{(q-1)/2} \text{ dan } \left[\frac{2}{q}\right] = (-1)^{(q^2-1)/2}$$

(7) Jika p dan q adalah bilangan-bilangan prima dan $(p, q) = 1$, maka:

$$\left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \text{ dan } \left[\frac{p}{q}\right] = \left[\frac{q}{p}\right](-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Selanjutnya dapat dicari bahwa:

$$(a) \left[\frac{105}{317}\right] = \left[\frac{317}{105}\right] = \left[\frac{2}{105}\right] = (-1)^{(105^2-1)/8} = +1$$

$$(b) \left[\frac{213}{499}\right] = \left[\frac{499}{213}\right] = \left[\frac{73}{213}\right] = \left[\frac{67}{73}\right] = \left[\frac{73}{67}\right] = \left[\frac{6}{67}\right] = \left[\frac{2}{67}\right]\left[\frac{3}{67}\right] \\ = (-1)^{(67^2-1)/8} \left[\frac{3}{67}\right] = -\left[\frac{3}{67}\right] = \left[\frac{67}{3}\right] = \left[\frac{1}{3}\right] = +1$$



Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Carilah $\left(\frac{7}{79}\right)$ dan $\left(\frac{15}{101}\right)$
- 2) Carilah $\left(\frac{713}{1009}\right)$
- 3) Carilah suatu kongruensi dari semua bilangan prima sehingga 5 merupakan residi kuadratis.
- 4) Selesaikan $x^2 \equiv 150 \pmod{1009}$
- 5) Dengan menggunakan hukum kebalikan kuadratis, jika p adalah suatu bilangan prima ganjil, maka buktikan

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & \text{jika } p \equiv \pm 1 \pmod{12} \\ -1, & \text{jika } p \equiv \pm 5 \pmod{12} \end{cases}$$

Petunjuk Jawaban Latihan

- 1) Karena $79 \equiv 1 \pmod{4}$, maka $\left(\frac{7}{79}\right) = \left(\frac{79}{7}\right) = \left(\frac{2}{7}\right) = 1$

$$\left(\frac{15}{101}\right) = \left(\frac{3.5}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{5}{101}\right)$$
, karena $101 \equiv 1 \pmod{4}$, maka

$$\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$$
 dan $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$
Jadi $\left(\frac{15}{101}\right) = \left(\frac{3.5}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{5}{101}\right) = (-1)(1) = -1$
- 2) $\left(\frac{713}{1009}\right) = \left(\frac{23.31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$, karena $1009 \equiv 1 \pmod{4}$, maka

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right)$$
 dan $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right)$ sehingga

$$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2 \cdot 5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right)$$

$$\begin{aligned}
 &= \left(\frac{3}{5} \right) = \left(\frac{5}{3} \right) = \left(\frac{2}{3} \right) = -1 \\
 \left(\frac{1009}{31} \right) &= \left(\frac{17}{31} \right) = \left(\frac{31}{17} \right) = \left(\frac{14}{17} \right) = \left(\frac{2}{17} \right) \left(\frac{7}{17} \right) = \left(\frac{17}{7} \right) = \left(\frac{3}{7} \right) = -\left(\frac{7}{3} \right) \\
 &= -\left(\frac{4}{3} \right) = -\left(\frac{2^2}{3} \right) = -1
 \end{aligned}$$

Jadi $\left(\frac{713}{1009} \right) = \left(\frac{23 \cdot 31}{1009} \right) = \left(\frac{23}{1009} \right) \left(\frac{31}{1009} \right) = (-1)(-1) = 1$

3) $\left(\frac{5}{p} \right) = \left(\frac{p}{5} \right)$ sebab $5 \equiv 1 \pmod{4}$, $\left(\frac{1}{5} \right) = \left(\frac{4}{5} \right) = 1$ dan $\left(\frac{2}{5} \right) = \left(\frac{3}{5} \right) = -1$,

maka 5 adalah suatu residu kuadratis modulo p jika dan hanya jika $p \equiv 1, 4 \pmod{5}$.

4) $\left(\frac{150}{1009} \right) = \left(\frac{2 \cdot 3 \cdot 5^2}{1009} \right) = \left(\frac{2}{1009} \right) \left(\frac{3}{1009} \right) \left(\frac{5^2}{1009} \right) = 1 \cdot 1 \cdot 1 = 1$

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

p adalah suatu bilangan prima ganjil, maka $p \equiv 1 \pmod{3}$ atau $p \equiv 2 \pmod{3}$ sehingga:

untuk $p \equiv 1 \pmod{3}$, $\left(\frac{p}{3} \right) = \left(\frac{1}{3} \right) = 1$

untuk $p \equiv 2 \pmod{3}$, $\left(\frac{p}{3} \right) = \left(\frac{2}{3} \right) = -1$

p adalah suatu bilangan prima ganjil, maka $p \equiv 1 \pmod{4}$ atau $p \equiv 3 \pmod{4}$, yaitu $p = 4t+1$ atau $p = 4k+3$, sehingga:

untuk $p \equiv 1 \pmod{4}$, $(-1)^{(p-1)/2} = (-1)^{(4t+1-1)/2} = (-1)^{2t} = 1$

untuk $p \equiv 3 \pmod{4}$, $(-1)^{(p-1)/2} = (-1)^{(4t+3-1)/2} = (-1)^{2k+1} = -1$

Gabungan kemungkinan nilai-nilai p adalah:

(a) $p \equiv 1 \pmod{3}$ dan $p \equiv 1 \pmod{4}$, sehingga $p \equiv 1 \pmod{12}$

(b) $p \equiv 1, 4, 7 \pmod{3}$ dan $p \equiv 3 \pmod{4} \equiv 3, 7 \pmod{4}$,
sehingga $p \equiv 7 \pmod{12}$

(c) $p \equiv 2 \pmod{3} \equiv 2, 5 \pmod{3}$ dan $p \equiv 1 \pmod{4} \equiv 1, 5 \pmod{4}$,
sehingga $p \equiv 5 \pmod{12}$

(d) $p \equiv 2, 5, 8, 11 \pmod{3}$ dan $p \equiv 3, 7, 11 \pmod{4}$, maka $p \equiv 11 \pmod{12}$

Selanjutnya dapat kita cari nilai-nilai $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)$ dari 4 kemungkinan di atas:

$$(a) \text{ jika } p \equiv 1 \pmod{12}, \text{ maka } \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$$

$$(b) \text{ jika } p \equiv 7 \pmod{12}, \text{ maka } \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = -1$$

$$(c) \text{ jika } p \equiv 5 \pmod{12}, \text{ maka } \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = -1$$

$$(d) \text{ jika } p \equiv 11 \pmod{12}, \text{ maka } \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$$



Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep kebalikan kuadratis untuk mencari nilai lambang Legendre dan manfaatnya untuk menetapkan keterselesaian kongruensi kuadratis, dan konsep lambang Jacobi sebagai penggeneralisasian lambang Legendre.

1. Teorema 5.7

Jika k adalah suatu bilangan bulat ganjil, p adalah suatu bilangan prima ganjil, $(k, p) = 1$, dan

$$H(k, p) = \sum_{a=1}^{(p-1)/2} [(ak)/p] \text{ maka } \left(\frac{k}{p}\right) = (-1)^{H(k, p)}$$

2. Teorema 5.8 Hukum Kebalikan Kuadrat

Jika p dan q adalah bilangan-bilangan prima ganjil, maka:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$$

3. Teorema 5.9

Jika p dan q adalah bilangan-bilangan prima ganjil, maka:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{jika } p \equiv 1 \pmod{4} \text{ atau } q \equiv 1 \pmod{4} \\ -1, & \text{jika } p \equiv 3 \pmod{4} \text{ atau } q \equiv 3 \pmod{4} \end{cases}$$

4. Teorema 5.10

Jika p dan q adalah bilangan-bilangan prima ganjil, maka:

$$\left(\frac{p}{q} \right) = \begin{cases} \left(\frac{q}{p} \right), & \text{jika } p \equiv 1 \pmod{4} \text{ atau } q \equiv 1 \pmod{4} \\ -1 \left(\frac{q}{p} \right), & \text{jika } p \equiv 3 \pmod{4} \text{ dan } q \equiv 3 \pmod{4} \end{cases}$$

5. Definisi Lambang Jacobi

Jika q adalah suatu bilangan bulat positif, q mempunyai faktor-faktor prima sehingga q dapat dinyatakan sebagai $q = q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}$,

$p \in \mathbb{Z}$ sehingga $(p, q) = 1$, maka Lambang Jacobi $\left[\frac{p}{q} \right]$ didefinisikan

sebagai:

$$\left[\frac{p}{q} \right] = \left[\frac{p}{q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}} \right] = \left[\frac{p}{q_1} \right]^{k_1} \left[\frac{p}{q_2} \right]^{k_2} \dots \left[\frac{p}{q_t} \right]^{k_t} = \prod_{j=1}^t \left(\frac{p}{q_j} \right)$$

yang mana $\left(\frac{p}{q_j} \right)$ dengan $j = 1, 2, \dots, t$ adalah lambang-lambang

Legendre.

6. Teorema-teorema tentang Lambang Jacobi

$$(1) \text{ jika } p \equiv r \pmod{q}, \text{ maka } \left[\frac{p}{q} \right] = \left[\frac{r}{q} \right]$$

$$(2) \left[\frac{pr}{q} \right] = \left[\frac{p}{q} \right] \left[\frac{r}{q} \right]$$

$$(3) \left[\frac{-1}{q} \right] = (-1)^{(n-1)/2}$$

$$(4) \left[\frac{2}{q} \right] = (-1)^{(n^2-1)/8}$$

$$(5) \left[\frac{p}{q} \right] \left[\frac{q}{p} \right] = (-1)^{\frac{q-1}{2} \frac{p-1}{2}}$$

$$(6) \left[\frac{-1}{q} \right] = (-1)^{(q-1)/2} \text{ dan } \left[\frac{2}{q} \right] = (-1)^{(q^2-1)/2}$$

(7) Jika p dan q adalah bilangan-bilangan prima dan $(p, q) = 1$, maka:

$$\left[\frac{p}{q} \right] \left[\frac{q}{p} \right] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \text{ dan } \left[\frac{p}{q} \right] \left[\frac{q}{p} \right] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$



TES FORMATIF 2

- 1) Skor 10

Tunjukkan bahwa 19 tidak membagi $(4n^2 + 4)$ untuk sebarang bilangan bulat n .

- 2) Skor 20

Ditentukan bahwa $p \equiv 5 \pmod{12}$. Dengan menggunakan hukum kebalikan kuadratis, tunjukkan $\left(\frac{3}{p} \right) = -1$.

- 3) Skor 20

Tentukan apakah kongruensi $x^2 \equiv -5 \pmod{503}$ dapat diselesaikan?

- 4) Skor 20

Jika p adalah suatu bilangan prima ganjil, tunjukkan bahwa:

$$\left(\frac{-3}{p} \right) = \begin{cases} +1, & \text{jika } p \equiv +1 \pmod{6} \\ -1, & \text{jika } p \equiv +1 \pmod{6} \end{cases}$$

- 5) Skor 20

Tentukan p jika 7 adalah suatu residu kuadratis modulo p .

- 6) Skor 10

$$\text{Carilah } \left[\frac{10001}{20003} \right].$$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1) Residu-residu kuadratis modulo 7 adalah 1, 2, dan 4 sebab

$$x^2 \equiv 1 \pmod{1} \text{ mempunyai selesaian } x \equiv 1, 6 \pmod{7},$$

$$x^2 \equiv 2 \pmod{7} \text{ mempunyai selesaian } x \equiv 3, 4 \pmod{7} \text{ dan}$$

$$x^2 \equiv 4 \pmod{7}.$$

Bukan residu-residu kuadratis modulo 7 adalah 3, 5, dan 6 sebab

$$x^2 \equiv 3, 5, 6 \pmod{7} \text{ tidak mempunyai selesaian.}$$

$$2) \left[\frac{8}{17} \right] \equiv 8^{\frac{17-1}{2}} \pmod{17} \equiv 8^8 \pmod{17} \equiv (8^2)^4 \pmod{8} \equiv (-4)^4 \pmod{17}$$

$$\equiv 1 \pmod{17}$$

Jadi 8 adalah suatu residu kuadratis modulo 17.

$$\left[\frac{7}{23} \right] \equiv 7^{\frac{23-1}{2}} \pmod{23} \equiv 7^{11} \pmod{23} \equiv (7^2)^5 \cdot 7 \pmod{23} \equiv 3^5 \cdot 7 \pmod{23}$$

$$\equiv -1 \pmod{23}$$

Jadi 7 adalah bukan suatu residu kuadratis modulo 23.

$$3) x^2 \equiv 207 \pmod{1001} \equiv 207 \pmod{7 \cdot 11 \cdot 13}.$$

$$x^2 \equiv 207 \pmod{7} \equiv 4 \pmod{7}, \text{ maka } x \equiv 2 \pmod{7} \text{ dan } x \equiv 5 \pmod{7}.$$

$$x^2 \equiv 207 \pmod{11} \equiv 9 \pmod{11}, \text{ maka } x \equiv 3 \pmod{11} \text{ dan}$$

$$x \equiv 8 \pmod{11}.$$

$$x^2 \equiv 207 \pmod{13} \equiv 12 \pmod{13}, \text{ maka } x \equiv 5 \pmod{13} \text{ dan}$$

$$x \equiv 8 \pmod{13}.$$

Dengan demikian terdapat 8 kongruensi linier simultan, salah satu di antaranya adalah:

$$x \equiv 2 \pmod{7}, x \equiv 3 \pmod{11}, \text{ dan } x \equiv 5 \pmod{13}$$

yang dapat diselesaikan dengan Teorema Sisa China,

$$11 \cdot 13 b_1 \equiv 1 \pmod{7}, \text{ maka } b_1 = 5$$

$$7 \cdot 13 b_2 \equiv 1 \pmod{11}, \text{ maka } b_2 = 4$$

$$7 \cdot 11 b_3 \equiv 1 \pmod{13}, \text{ maka } b_3 = 12$$

$$\text{sehingga } x = 11 \cdot 13 \cdot 5 \cdot 2 + 7 \cdot 13 \cdot 4 \cdot 3 + 7 \cdot 11 \cdot 12 \cdot 5 = 7142 \equiv 135 \pmod{1001}$$

Selesaian yang lain dapat diperoleh dengan cara yang sama, dan seluruh selesaian adalah:

$$x \equiv 47, 96, 135, 278, 723, 866, 905, 954 \pmod{1001}$$

$$4) x^2 + 995x - 1110 \equiv 0 \pmod{1009} \text{ disederhanakan menjadi}$$

$$x^2 - 14x - 101 \equiv 0 \pmod{1009},$$

$$x^2 - 14x + 49 - 49 - 101 \equiv 0 \pmod{1009}, (x - 7)^2 \equiv 150 \pmod{1009}$$

$$\left[\begin{array}{c} 150 \\ 1009 \end{array} \right] = \left[\begin{array}{c} 6.25 \\ 1009 \end{array} \right] = \left[\begin{array}{c} 6 \\ 1009 \end{array} \right] = \left[\begin{array}{c} 2 \\ 1009 \end{array} \right] \left[\begin{array}{c} 3 \\ 1009 \end{array} \right]$$

$$\left[\begin{array}{c} 2 \\ 1009 \end{array} \right] \equiv 2^{504} \pmod{1009} \equiv 1 \pmod{1009} \text{ sebab } 1009 \equiv 1 \pmod{8}$$

$$\left[\begin{array}{c} 3 \\ 1009 \end{array} \right] \equiv 3^{504} \pmod{1009} \equiv (3^7)^{72} \pmod{1009} \equiv (169^2)^{36} \pmod{1009}$$

$$\equiv (309^2)^{18} \pmod{1009} \equiv 635^{18} \pmod{1009} \equiv 374^{18} \pmod{1009}$$

$$\equiv 634^9 \pmod{1009} \equiv 374.634 \pmod{1009}$$

$$\equiv 237116 \pmod{1009} \equiv 1 \pmod{1009}$$

$$\left[\begin{array}{c} 2 \\ 1009 \end{array} \right] \left[\begin{array}{c} 3 \\ 1009 \end{array} \right] = 1.1 = 1, \text{ maka kongruensi dapat diselesaikan.}$$

$$(x-7)^2 \equiv 150 \pmod{1009} \equiv 150 + 19.1009 \pmod{1009}$$

$$\equiv 19321 \pmod{1009}$$

$$x \equiv 139, 877 \pmod{1009}$$

- 5) $3x^2 \equiv 7 \pmod{17}$, $18x^2 \equiv 42 \pmod{17}$, $x^2 \equiv 25 \pmod{17}$, maka
 $x \equiv 5, 12 \pmod{17}$

$$5x^2 - 2x \equiv 3 \pmod{12}, 25x^2 - 10x - 15 \equiv 0 \pmod{12},$$

$$x^2 + 2x + 1 \equiv 0 \pmod{12}, \text{ atau } (x+1)^2 \equiv 4 \pmod{12}, \text{ maka}$$

$$x \equiv 1, 9 \pmod{12}$$

Akibatnya terdapat 4 pasang sistem kongruensi linier simultan, dapat diselesaikan dengan cara biasa, cara iterasi, atau cara Sisa China, sehingga diperoleh $x \equiv 73, 97, 141, 165 \pmod{204}$.

- 6) $21x^2 - 23x - 19 \equiv 0 \pmod{71}$, $44.21x^2 - 41.23x - 44.19 \equiv 0 \pmod{71}$,
 $x^2 - 1012x - 836 \equiv 0 \pmod{71}$, $x^2 - 18x - 55 \equiv 0 \pmod{71}$,
 $(x-9)^2 \equiv 6 \pmod{71}$

$$\left[\begin{array}{c} 6 \\ 71 \end{array} \right] = \left[\begin{array}{c} 2 \\ 71 \end{array} \right] \left[\begin{array}{c} 3 \\ 71 \end{array} \right] = 1.1 = 1 \text{ sebab } \left[\begin{array}{c} 2 \\ 71 \end{array} \right] = (-1)^{\frac{71^2-1}{8}} = (-1)^{630} = 1$$

$$\left[\begin{array}{c} 3 \\ 71 \end{array} \right] = 3^{\frac{71-1}{2}} \equiv 3^{35} \equiv (3^4)^8 \cdot 3^3 \equiv 10^8 \cdot 3^3 \equiv (29)^4 \cdot 3^3 \equiv 60^2 \cdot 27 \equiv 50.27$$

$$\equiv 1 \pmod{71}$$

Jadi kongruensi dapat diselesaikan, dikerjakan sebagai berikut:

$$(x-9)^2 \equiv 6 \pmod{71} \equiv 6 + 5.71 \pmod{71} \equiv 361 \pmod{71},$$

$$x-9 \equiv 19 \pmod{71} \text{ dan } x-9 \equiv 52 \pmod{71}, \text{ sehingga}$$

$$x \equiv 28, 61 \pmod{71}.$$

7) $19x^2 - 12x + 8 \equiv 0 \pmod{97}$

Kerjakan serupa butir 6 sampai diperoleh $(x+15)^2 \equiv 11 \pmod{97}$, hitung $\left[\frac{11}{97} \right]$ sampai diperoleh nilai 1, berarti kongruensi dapat diselesaikan.

$$(x+15)^2 \equiv 11 \pmod{97} \equiv 11 + 14 \cdot 97 \pmod{97} \equiv 1369 \pmod{97}$$

Jadi $x \equiv 22, 35 \pmod{97}$

8) $\left[\frac{-2}{p} \right] = \left[\frac{-1}{p} \right] \left[\frac{2}{p} \right]$

Jika $p \equiv 1 \pmod{8}$, maka:

(a) $p \equiv 1 \pmod{4}$ sebab $4 \mid 8$, dan sesuai Teorema 5.5, $\left[\frac{-1}{p} \right] = 1$

(b) $p = 8k + 1$, dan sesuai jawaban tugas, $\left[\frac{2}{p} \right] = (-1)^{\frac{p^2-1}{8}} = (-1)^{8k^2+2k} = 1$

sehingga $\left[\frac{-2}{p} \right] = \left[\frac{-1}{p} \right] \left[\frac{2}{p} \right] = 1 \cdot 1 = 1$

Dengan menggunakan cara yang sama, berdasarkan Teorema 5.5 dan jawaban tugas, dapat ditentukan bahwa:

$$\left[\frac{-2}{p} \right] = 1 \text{ jika } p \equiv 3 \pmod{8}, \quad \left[\frac{-2}{p} \right] = -1 \text{ jika } p \equiv 5 \pmod{8} \text{ dan}$$

$$\left[\frac{-2}{p} \right] = -1 \text{ jika } p \equiv 7 \pmod{8}$$

9)
$$\left[\frac{n}{q} \right] = \left[\frac{p_1^{2t_1+1}}{q} \right] \left[\frac{p_2^{2t_2+1}}{q} \right] \dots \left[\frac{p_k^{2t_k+1}}{q} \right]$$

$$= \left[\frac{p_1^{2t_1}}{q} \right] \left[\frac{p_1}{q} \right] \cdot \left[\frac{p_2^{2t_2}}{q} \right] \left[\frac{p_2}{q} \right] \dots \left[\frac{p_k^{2t_k}}{q} \right] \left[\frac{p_k}{q} \right]$$

$$= 1 \cdot \left[\frac{p_1}{q} \right] \cdot 1 \cdot \left[\frac{p_2}{q} \right] \dots 1 \cdot \left[\frac{p_k}{q} \right] = \left[\frac{p_1}{q} \right] \cdot \left[\frac{p_2}{q} \right] \dots \left[\frac{p_k}{q} \right]$$

10)
$$\left[\frac{b}{p} \right] + \left[\frac{2b}{p} \right] + \dots + \left[\frac{(p-1)b}{p} \right] = \left[\frac{b}{p} \right] \left[\left[\frac{1}{p} \right] + \left[\frac{2}{p} \right] + \dots + \left[\frac{p-1}{p} \right] \right]$$

$$= \left[\frac{b}{p} \right] \cdot 0 = 0$$

sebab terdapat sejumlah sama residu kuadratis dan bukan residu kuadratis modulo p di dalam barisan bilangan $1, 2, 3, \dots, (p-1)$.

- 11) Harus ditunjukkan bahwa $x \equiv \pm a^{n+1} \pmod{p}$ memenuhi $x^2 \equiv a \pmod{p}$
jika $p = 4n + 3$, maka $p + 1 = 4n + 4$, sehingga $(p + 1)/2 = 2n + 2$
 $x^2 \equiv (\pm a^{n+1})^2 \equiv a^{2n+2} \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \cdot a \equiv 1 \cdot a \equiv a \pmod{p}$

Tes Formatif 2

- 1) Harus dibuktikan $4n^2 + 4 = 4(n^2 + 1) \equiv 0 \pmod{19}$ tidak mempunyai selesaian. Karena $(4, 19) = 1$ maka harus ditunjukkan $n^2 + 1 \equiv 0 \pmod{19}$ atau $n^2 \equiv -1 \pmod{19}$ tidak mempunyai selesaian.

$$\left(\frac{-1}{19}\right) = \left(\frac{18}{19}\right) = \left(\frac{2 \cdot 9}{19}\right) = \left(\frac{2}{19}\right) \left(\frac{9}{19}\right) = \left(\frac{2}{19}\right) \cdot 1 = \left(\frac{2}{19}\right) \equiv 2^9 \pmod{19}$$

$$\equiv 512 \pmod{19} = -1$$

- 2) $p \equiv 5 \pmod{12}$, maka $p = 12n + 5$ untuk sebarang bilangan bulat n

$$\begin{aligned} \left(\frac{3}{p}\right) &= (-1)^{\frac{p-1}{2} \binom{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{12n+5-1}{2}} \left(\frac{p}{3}\right) \\ &= (-1)^{2(3n+2)} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) \\ &= \left(\frac{12n+5}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{aligned}$$

$$\begin{aligned} 3) \quad \left(\frac{-5}{503}\right) &= \left(\frac{-1}{503}\right) \left(\frac{5}{503}\right) = (-1)^{\frac{503-1}{2}} \left(\frac{5}{503}\right) = (-1) \left(\frac{5}{503}\right) = (-1)^{2.251} \left(\frac{503}{5}\right) \\ &= \left(\frac{3}{5}\right) = -1 \end{aligned}$$

Jadi $x^2 \equiv -1 \pmod{503}$ tidak mempunyai selesaian.

- 4) Jika $p \equiv 1 \pmod{6}$ maka ada dua keadaan: jika $p \equiv 1 \pmod{4}$, maka

$$\begin{aligned} \left(\frac{-1}{p}\right) &= 1, \quad \text{dan berikutnya} \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1, \quad \text{demikian pula} \\ \left(\frac{-3}{p}\right) &= 1; \quad \text{jika } p \equiv 3 \pmod{4}, \quad \text{maka} \quad \left(\frac{-1}{p}\right) = -1 \quad \text{dan} \quad \left(\frac{3}{p}\right) = -1 \left(\frac{p}{3}\right), \\ \text{sehingga} \quad \left(\frac{-3}{p}\right) &= (-1)(-1) = 1. \end{aligned}$$

Jika $p \equiv -1 \pmod{6}$ dan $p \equiv 1 \pmod{4}$, maka

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = 1 \cdot \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

Jika $p \equiv 3 \pmod{4}$, maka

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1)\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

- 5) Sesuai dengan hukum kebalikan kuadrat, jika $p \equiv 1 \pmod{4}$, maka $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$, dan jika $p \equiv 3 \pmod{4}$, maka $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. Jadi 7 adalah suatu residu kuadratis modulo p jika $p \equiv 1 \pmod{4}$ jika $p \equiv \left(\frac{p}{7}\right) = 1$, atau $p \equiv 1, 2, 4 \pmod{7}$. Dengan menggunakan Teorema Sisa China, dapat ditentukan bahwa 7 adalah suatu residu kuadratis dari p jika $p \equiv 5, 13, 17 \pmod{28}$.
- Demikian pula, 7 adalah suatu residu kuadratis modulo $p \equiv 3 \pmod{4}$ jika $\left(\frac{p}{7}\right) = -1$, yaitu jika $p \equiv 3, 5, 6 \pmod{7}$. Dengan menggunakan Teorema Sisa China, 7 adalah suatu residu kuadratis modulo p jika $p \equiv 3, 19, 27 \pmod{28}$, dan 7 adalah bukan suatu residu kuadratis modulo p jika $p \equiv 11, 15, 23 \pmod{28}$. Jadi 7 adalah suatu residu kuadratis modulo p jika $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$.
- 6) Karena $10001 \equiv 1 \pmod{4}$, maka $\left[\frac{10001}{20003}\right] = \left[\frac{20003}{10001}\right] = \left[\frac{1}{10001}\right] = 1$

Daftar Pustaka

- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Fungsi-fungsi Multiplikatif

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul fungsi-fungsi multiplikatif ini diuraikan tentang sifat-sifat dasar fungsi-fungsi aritmetika khusus yang multiplikatif yaitu fungsi phi-Euler, fungsi jumlah pembagi, dan fungsi cacah pembagi, serta diuraikan tentang sifat-sifat dasar bilangan-bilangan khusus yaitu bilangan perfek (sempurna), dan bilangan-bilangan prima Mersenne.

Pembahasan tentang fungsi-fungsi aritmetika yang multiplikatif berkaitan dengan ulasan teorema-teorema dalam mencari nilai fungsi dari bilangan bulat positif yang dinyatakan dalam bentuk pemfaktoran prima dari bilangan itu.

Pembahasan tentang bilangan-bilangan khusus, yaitu bilangan-bilangan perfek dan bilangan-bilangan prima Mersenne, berkaitan dengan pengertian, cara mencari, hubungan antara kedua jenis bilangan khusus, dan kemungkinan hubungan dengan bilangan khusus yang lain.

Dengan bertambahnya uraian tentang fungsi-fungsi multiplikatif, wawasan kita tentang teori bilangan menjadi lebih banyak dan lebih lengkap sehingga keterkaitan dan ketergantungan antara berbagai topik menjadi kelihatan lebih nyata dan jelas.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep fungsi aritmetika, fungsi multiplikatif, hubungan fungsi multiplikatif dan pemfaktoran prima, pengertian bilangan perfek dan bilangan prima Mersenne, hubungan bilangan perfek dan bilangan prima Mersenne, serta kemungkinan hubungan bilangan prima Mersenne dengan bilangan-bilangan khusus yang lain.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep dan sifat-sifat fungsi multiplikatif khusus yang meliputi phi-Euler, fungsi jumlah pembagi, fungsi cacah pembagi, dan menjelaskan bilangan-bilangan khusus yaitu bilangan perfek dan bilangan-bilangan prima Mersenne serta keterkaitannya dengan bilangan segibanyak (*polygonal numbers*).

Susunan Kegiatan Belajar

Modul 6 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Fungsi-fungsi Multiplikatif, dan Kegiatan Belajar 2 adalah Bilangan Perfek dan Bilangan Prima Mersenne. Setiap kegiatan belajar memuat Uraian, Contoh/Bukan Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 6 ini dijelaskan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi paparan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab/menyelesaikan, maka lihatlah Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum banyak membantu Anda keluar dari kesulitan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Kemampuan Anda dengan jalan mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah pengerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Fungsi-fungsi Multiplikatif**

Fungsi-fungsi multiplikatif merupakan fungsi-fungsi khusus dalam teori bilangan, antara lain fungsi-phi Euler, fungsi banyak pembagi, dan fungsi jumlah pembagi. Salah satu sifat penting fungsi-phi Euler adalah nilai fungsi untuk suatu bilangan bulat n sama dengan hasil kali nilai fungsi-phi Euler dari masing-masing perpangkatan prima dalam pemfaktoran prima dari n . Fungsi-fungsi yang mempunyai sifat seperti ini disebut multiplikatif, dan fungsi multiplikatif semacam ini sering muncul sepanjang pembahasan teori bilangan.

Definisi 6.1

1. Suatu fungsi yang didefinisikan pada himpunan bilangan bulat positif disebut dengan fungsi aritmetika.
2. Suatu fungsi aritmetika f disebut suatu fungsi multiplikatif jika $f(mn) = f(m)f(n)$ untuk sebarang bilangan-bilangan bulat positif m dan n yang relatif prima.
3. Suatu fungsi multiplikatif f disebut lengkap jika $f(mn) = f(m)f(n)$ untuk semua bilangan-bilangan bulat positif m dan n .

Contoh 6.1

1. $f(n) = 0$ adalah suatu fungsi multiplikatif lengkap sebab untuk semua bilangan-bilangan bulat positif m dan n , $f(mn) = 0 = 0 \cdot 0 = f(0)f(0) = f(m)f(n)$.
2. $f(x) = x^2$ adalah suatu fungsi multiplikatif lengkap sebab untuk semua bilangan-bilangan bulat positif x dan y , $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$.
3. $f(s) = 3s + 2$ adalah bukan suatu fungsi multiplikatif lengkap sebab $f(st) = 3st + 2$, $f(s) = 3s + 2$, $f(t) = 3t + 2$, $f(s)f(t) = (3s + 2)(3t + 2) = 9st + 6s + 6t + 4$, dan $f(st) \neq f(s)f(t)$ untuk $s, t \in \mathbb{Z}^+$

Contoh 6.2

Ditentukan $f(x) = x$. Ambil $m = 2^3$ dan $n = 3^4$, maka

$$f(mn) = f(2^3 \cdot 3^4) = 2^3 \cdot 3^4 = f(2^3) \cdot f(3^4) = f(m) \cdot f(n).$$

Jadi f adalah suatu fungsi multiplikatif.

Teorema 6.1

Jika f adalah suatu fungsi multiplikatif, dan $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari suatu bilangan bulat positif n , maka $f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_t^{k_t})$.

Bukti:

Teorema dibuktikan dengan menggunakan induksi matematika.

Untuk $t=1$, sebab ruas kiri $f(n) = f(p_1^{k_1})$ dan ruas kanan $f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_t^{k_t}) = f(p_1^{k_1})$. Jadi hubungan berlaku untuk $t=1$.

Misalkan hubungan berlaku untuk $t=r$, yaitu:

$$f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r})$$

Harus dibuktikan hubungan berlaku untuk $t=r+1$, yaitu:

$$f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r}) f(p_{r+1}^{k_{r+1}})$$

Karena $(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, p_{r+1}^{k_{r+1}}) = 1$ dan f adalah fungsi multiplikatif, maka:

$$\begin{aligned} f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) &= f[(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})(p_{r+1}^{k_{r+1}})] \\ &= [f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r})] [f(p_{r+1}^{k_{r+1}})] \end{aligned}$$

$$\text{Jadi } f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} p_{r+1}^{k_{r+1}}) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r}) f(p_{r+1}^{k_{r+1}})$$

Sekarang perhatikan kembali Definisi 3.3 tentang sistem residu tereduksi modulo m :

Suatu himpunan bilangan bulat $\{x_1, x_2, \dots, x_k\}$ disebut suatu sistem residu tereduksi modulo m jika dan hanya jika :

- $(x_i, m) = 1$, $1 \leq i < k$
- $x_i \equiv x_j \pmod{m}$ untuk setiap $i \neq j$

- c. Jika $(y, m) = 1$, maka $y \equiv x_i \pmod{m}$ untuk suatu $i = 1, 2, \dots, k$ dan Definisi 3.4 tentang fungsi ϕ -Euler

Ditentukan m adalah suatu bilangan bulat positif. Banyaknya residi di dalam suatu sistem residi yang tereduksi modulo m disebut Fungsi ϕ -Euler dari m , dan dinyatakan dengan $\phi(m)$.

Berdasarkan Definisi 3.3 dan Definisi 3.4 kita dapat mencari nilai-nilai $\phi(m)$ untuk sebarang bilangan bulat positif m , misalnya $\phi(2) = 1$, $\phi(3) = 2$, dan $\phi(10) = 4$. Selanjutnya kita bisa mencari $\phi(p)$ untuk sebarang bilangan prima p .

Teorema 6.2

Jika p adalah suatu bilangan prima, maka $\phi(p) = p - 1$, dan jika $\phi(p) = p - 1$, maka p adalah suatu bilangan prima.

Bukti:

(\rightarrow)

Misalkan p adalah suatu bilangan prima, maka himpunan $S = \{0, 1, 2, \dots, p-1\}$ merupakan suatu sistem residi yang lengkap modulo p . Unsur-unsur S yang tidak relatif prima dengan p hanya 0 sebab $(0, p) = p \neq 1$. Dengan demikian setiap bilangan bulat positif unsur S yang kurang dari p adalah relatif prima terhadap p . Karena banyaknya bilangan bulat positif unsur S yang kurang dari p adalah $(p-1)$, maka $\phi(p) = p - 1$.

(\leftarrow)

Selanjutnya, jika p adalah suatu bilangan bulat positif dan $\phi(p) = p - 1$, maka kemungkinannya adalah p merupakan suatu bilangan prima atau p merupakan suatu bilangan komposit.

Jika p merupakan suatu bilangan komposit, maka p mempunyai suatu pembagi d yang mana $1 < d < p$ dengan $(d, p) \neq 1$. Karena kita ketahui bahwa paling sedikit ada satu dari $(p-1)$ bilangan bulat di dalam

$\{0, 1, 2, \dots, p-1\}$, yaitu d , yang tidak relatif prima dengan p , maka $\phi(p) \leq p - 2$, bertentangan dengan yang diketahui, yaitu $\phi(p) = p - 1$.

Jadi p bukan suatu bilangan komposit tetapi suatu bilangan prima.

Contoh 6.3

- $\phi(5) = 5 - 1 = 4$
- $\phi(23) = 23 - 1 = 22$
- $\phi(37) = 37 - 1 = 36$

Teorema 6.3

Jika p adalah suatu bilangan prima dan k adalah suatu bilangan bulat positif, maka $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

Bukti:

Bilangan-bilangan bulat positif kurang dari p^k yang tidak relatif prima dengan p^k adalah bilangan-bilangan bulat positif yang tidak lebih dari p^k tetapi habis dibagi oleh p , yaitu $p, 2p, 3p, \dots, p^{k-1} \cdot p$. Ini berarti banyaknya bilangan-bilangan itu adalah p^{k-1} . Jadi banyaknya bilangan bulat positif yang kurang dari p^k dan relatif prima dengan p^k adalah:

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Contoh 6.4

- $\phi(2^3) = 2^2(2-1) = 4 \cdot 1 = 4$
- $\phi(7^3) = 7^2(7-1) = 49 \cdot 6 = 294$
- $\phi(11^4) = 11^3(11-1) = 1331 \cdot 10 = 13310$

Uraian berikutnya akan membuktikan bahwa fungsi ϕ -Euler adalah suatu **fungsi multiplikatif**. Sebelum membuktikan, marilah kita melihat suatu peragaan berikut.

Kita tentukan dua bilangan bulat positif $m = 7$ dan $n = 6$ yang memenuhi hubungan $(m, n) = 1$. Perkalian m dan n menghasilkan $mn = 7 \cdot 6 = 42$,

kemudian semua bilangan bulat positif dari 1 sampai dengan 42 disusun dalam 7 baris dan 6 kolom sebagai berikut:

1	8	15	22	29	36
2	9	16	23	30	37
3	10	17	24	31	38
4	11	18	25	32	39
5	12	19	26	33	40
6	13	20	27	34	41
7	14	21	28	35	42

Ambil suatu baris ke r , misalnya $r = 5$, maka $(m, r) = (7, 5) = 1$, maka semua bilangan pada baris ke $r = 5$ relatif prima terhadap $m = 7 : (7, 5) = (7, 12) = (7, 19) = (7, 26) = (7, 33) = (7, 40) = 1$.

Bilangan-bilangan pada baris ke $r = 5$ juga membentuk sistem residu yang lengkap modulo 6: $5 \equiv 5 \pmod{6}$, $12 \equiv 0 \pmod{6}$, $19 \equiv 1 \pmod{6}$, $26 \equiv 2 \pmod{6}$, $33 \equiv 3 \pmod{6}$, $40 \equiv 4 \pmod{6}$.

Dari bilangan-bilangan pada baris ke 5 yang relatif prima dengan 42 sebanyak dua, yaitu 5 dan 19 yaitu $\phi(6) = 2$. Kalau diselidiki lebih lanjut, jika diambil $r = 6$, maka bilangan-bilangan pada baris ke $r = 6$ yang relatif prima dengan 42 sebanyak dua, yaitu 13 dan 41, berarti juga $\phi(6) = 2$, dan hal ini juga berlaku untuk $r = 1, r = 2, r = 3, r = 4$, kecuali untuk $r = 7$ tidak ada bilangan yang relatif prima dengan 42. Dengan demikian dapat disimpulkan bahwa ada 6 baris, dan setiap baris memuat 2 bilangan yang relatif prima dengan 42, jadi banyaknya seluruh bilangan yang relatif prima dengan 42 adalah $\phi(42) = 6 \cdot 2 = \phi(7) \cdot \phi(6)$.

Teorema 6.4

Jika $p, q \in \mathbb{Z}^+$ dan $(p, q) = 1$, maka $\phi(pq) = \phi(p)\phi(q)$

Bukti:

Bilangan-bilangan bulat positif tidak lebih dari pq disusun p baris dan q kolom sebagai berikut:

1	$p+1$	$2p+1$	\cdots	$(q-1)p+1$
2	$p+2$	$2p+2$	\cdots	$(q-1)p+2$
3	$p+3$	$2p+3$	\cdots	$(q-1)p+3$
.	.	.	\cdots	.
.	.	.	\cdots	.
.	.	.	\cdots	.
p	$2p$	$3p$	\cdots	pq

Misalkan r adalah suatu bilangan bulat positif tidak lebih dari p , dan $(p,r)=d>1$. Maka tidak ada bilangan pada baris ke r yang relatif prima dengan pq karena sebarang bilangan pada baris ini mempunyai bentuk $kp+r$ dengan $k \in \mathbb{Z}^+$ dan $1 \leq k \leq (q-1)$, $d|p$, $d|r$. Ini berakibat $d|kp+r$, dan $d|pq$ sehingga d merupakan faktor persekutuan dari pq dan $kp+r$. Jadi $d|(pq, kp+r)$ atau $(pq, kp+r) \neq 1$.

Untuk mencari bilangan-bilangan yang relatif prima dengan pq , pilihlah baris ke r jika $(p,r)=1$. Jika $(p,r)=1$, $1 \leq r \leq p$, maka bilangan-bilangan pada baris ke r : $p, p+r, \dots, (q-1)p+r$ relatif prima dengan p karena $(p,r)=1$, lihat Teorema 2.19: $(x,y)=(x,y+ax)$ dan $(x,y)=(x+by, y)$, berarti $(p,r)=(kp+r, r)$, $k=0, 1, 2, \dots, (q-1)$. Barisan bilangan ini membentuk suatu sistem residu lengkap modulo q karena tidak ada dua bilangan yang kongruen modulo q . Andaikan $ip+r \equiv jp+r \pmod{q}$, dengan $0 \leq i, j \leq q-1$, maka $ip \equiv jp \pmod{q}$ atau $i \equiv j \pmod{q}$ karena $(p,q)=1$. Dengan demikian terdapat sebanyak $\phi(q)$ bilangan bulat positif pada baris ke r yang relatif prima dengan p , maupun relatif prima dengan pq . Karena terdapat $\phi(p)$ baris yang semacam baris ke r , dan masing-masing baris memuat $\phi(q)$ bilangan yang relatif prima dengan pq , maka dapat disimpulkan bahwa $\phi(pq)=\phi(p)\phi(q)$.

Contoh 6.7

- (a) $\phi(3)=2$, $\phi(4)=2$, dan $\phi(12)=4$, berarti $\phi(12)=\phi(3 \cdot 4)=\phi(3) \cdot \phi(4)$
- (b) $\phi(4)=2$, $\phi(6)=2$, dan $\phi(24)=8$, berarti

$$\phi(24) = \phi(4 \cdot 6) \neq \phi(4) \cdot \phi(6) \text{ karena } (4, 6) = 2 \neq 1$$

Teorema 6.5

Jika $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari $n \in \mathbb{Z}^+$, maka:

$$\phi(n) = \{p_1^{k_1-1}(p_1-1)\} \{p_2^{k_2-1}(p_2-1)\} \dots \{p_t^{k_t-1}(p_t-1)\}$$

Bukti :

Karena ϕ adalah suatu fungsi multiplikatif, maka:

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \dots \phi(p_t^{k_t})$$

Sesuai Teorema 6.3, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$, dengan demikian:

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \dots \phi(p_t^{k_t})$$

$$= \{p_1^{k_1-1}(p_1-1)\} \{p_2^{k_2-1}(p_2-1)\} \dots \{p_t^{k_t-1}(p_t-1)\}$$

Contoh 6.8

$$(a) \quad \phi(100) = \phi(2^2 \cdot 5^2) = \{2^{2-1}(2-1)\} \{5^{2-1}(5-1)\} = \{2(1)\} \{5(4)\} = 40$$

$$(b) \quad \phi(720) = \phi(2^4 \cdot 3^2 \cdot 5^1) = \{2^3(2-1)\} \{3^1(3-1)\} \{5^0(5-1)\} = 8 \cdot 6 \cdot 4 = 192$$

$$(c) \quad \phi(1000) = \phi(2^3 \cdot 5^3) = \{2^2(2-1)\} \{5^2(5-1)\} = 4 \cdot 100 = 400$$

Teorema 6.6

Jika $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari $n \in \mathbb{Z}^+$, maka :

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right)$$

Bukti:

Sesuai Teorema 6.3, $\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$, dengan demikian:

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \phi(p_1^{k_1})\phi(p_2^{k_2})\dots\phi(p_t^{k_t})$$

$$= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_t^{k_t} \left(1 - \frac{1}{p_t}\right)$$

$$= p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right)$$

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right)$$

Contoh 6.9

$$(a) \quad \phi(75) = \phi(3^1 5^2) = 75 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 75 \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) = 40$$

$$(b) \quad \phi(7000) = \phi(2^3 5^3 7^1) = 7000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) =$$

$$7000 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = 2400$$

$$(c) \quad \phi(8000) = \phi(2^6 5^3) = 8000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 8000 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 3200$$

Teorema 6.7

Jika $n \in Z^+$ dan $n > 2$, maka $\phi(n)$ adalah suatu bilangan bulat genap.

Bukti :

Misalkan $n \in Z^+$ dan $n > 2$. Misalkan pemfaktoran prima dari n adalah $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, maka sesuai Teorema 6.4 dapat ditunjukkan bahwa:

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \phi(p_1^{k_1})\phi(p_2^{k_2})\dots\phi(p_t^{k_t}) = \prod_{i=1}^t \phi(p_i^{k_i})$$

Sesuai dengan Teorema 6.3, $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i-1}(p_i - 1)$, sehingga kemungkinan nilai-nilai p_i adalah suatu bilangan bulat ganjil atau $p_i = 2$

(a) jika p_i adalah suatu bilangan bulat ganjil, maka $(p_i - 1)$ adalah suatu bilangan bulat genap, sehingga $(p_i - 1) = 2r$, dan akibatnya

$\phi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1) = p_i^{k_i-1}(2t)$ merupakan bilangan genap. Dengan demikian $\phi(n) = \prod_{i=1}^t \phi(p_i^{k_i})$ merupakan bilangan bulat genap.

- (b) jika $p_i = 2$, maka $p_i^{k_i-1} = 2^{k_i-1}(p_i - 1) = 2s(p_i - 1)$ sehingga $\phi(n) = \prod_{i=1}^t \phi(p_i^{k_i})$ merupakan bilangan bulat genap.

Dari hasil (a) dan (b) dapat disimpulkan bahwa $\phi(n)$ adalah suatu bilangan bulat genap.

Sebelum kita membuktikan Teorema 6.8, marilah kita memperhatikan peragaan berikut.

Ambil $n = 24$, maka pembagi n yang positif adalah 1, 2, 3, 4, 6, 8, 12, dan 24, dan $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(6) = 2$, $\phi(8) = 4$, $\phi(12) = 4$, dan $\phi(24) = 8$.

Jika bilangan-bilangan 1, 2, 3, ..., 24 dikelompokkan menjadi himpunan-himpunan F_i dengan $i = 1, 2, 3, 4, 6, 8, 12, 24$, dan $F_i = \{x \mid (x, 24) = i\}$, maka:

$F_1 = \{1, 5, 7, 11, 13, 17, 19, 23\}$ mempunyai unsur sebanyak

$$\phi(24/1) = \phi(24) = 8$$

$F_2 = \{2, 10, 14, 22\}$ mempunyai unsur sebanyak $\phi(24/2) = \phi(12) = 4$

$F_3 = \{3, 9, 15, 21\}$ mempunyai unsur sebanyak $\phi(24/3) = \phi(8) = 4$

$F_4 = \{4, 20\}$ mempunyai unsur sebanyak $\phi(24/4) = \phi(6) = 2$

$F_6 = \{6, 18\}$ mempunyai unsur sebanyak $\phi(24/6) = \phi(4) = 2$

$F_8 = \{8, 16\}$ mempunyai unsur sebanyak $\phi(24/8) = \phi(8) = 2$

$F_{12} = \{12\}$ mempunyai unsur sebanyak $\phi(24/12) = \phi(2) = 1$

$F_{24} = \{24\}$ mempunyai unsur sebanyak $\phi(24/24) = \phi(1) = 1$

Jika $|F_i|$ menyatakan banyaknya unsur F_i , maka dapat ditentukan bahwa :

$$n = 24 = 8 + 4 + 4 + 2 + 2 + 2 + 1 + 1 = F_1 + F_2 + F_3 + F_4 + F_6 + F_8 + F_{12} + F_{24}$$

$$\begin{aligned} &= \phi(24/1) + \phi(24/2) + \phi(24/3) + \phi(24/4) + \phi(24/6) + \phi(24/8) + \phi(24/12) \\ &\quad + \phi(24/24) \end{aligned}$$

$$n = \sum_{i|n} \phi(i) = \sum_{i|n} \phi(n/i)$$

Teorema 6.8

$$\text{Jika } n \in \mathbb{Z}^+, \text{ maka } n = \sum_{i|n} \phi(i) = \sum_{i|n} \phi(n/i)$$

Bukti:

Bilangan-bilangan $1, 2, 3, \dots, n$ dikelompokkan ke dalam himpunan F_i yang mana $x \in F_i$. Jika $(x, n) = i$, dan akibatnya $(x/i, n/i) = 1$. Ini berarti bahwa banyaknya bilangan di dalam F_i tidak lebih dari n/i , dan masing-masing bilangan relatif prima dengan n/i . Dengan demikian F_i memuat bilangan sebanyak $\phi(n/i)$. Selanjutnya, karena bilangan-bilangan bulat dari 1 sampai n dikelompokkan ke dalam himpunan-himpunan yang lepas, dan masing-masing bilangan hanya ada tepat di dalam satu himpunan, maka n merupakan jumlah dari banyaknya bilangan seluruh himpunan.

$$\text{Jadi } n = \sum_{i|n} \phi(i) = \sum_{i|n} \phi(n/i)$$

Contoh 6.10

Ambil $n=12$, maka pembagi-pembagi yang positif dari n adalah $1, 2, 3, 4, 6, 12$. Bilangan-bilangan $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ dikelompokkan ke dalam himpunan-himpunan :

$$F_1 = \{1, 5, 7, 11\}, F_2 = \{2, 10\}, F_3 = \{3, 9\}, F_4 = \{4, 8\}, F_6 = \{6\}, F_{12} = \{12\}$$

$$\phi(12/1) = \phi(12) = 4, \phi(12/2) = \phi(6) = 2, \phi(12/3) = \phi(4) = 2, \phi(12/4) = \phi(3) = 2$$

$$\phi(12/6) = \phi(2) = 1, \phi(12/12) = \phi(1) = 1$$

$$n = 12 = 1 + 1 + 2 + 2 + 2 + 4 = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)$$

$$n = \sum_{i|12} \phi(i) = \sum_{i|12} \phi(12/i)$$

Setelah kita melihat fungsi ϕ -Euler sebagai fungsi multiplikatif, marilah sekarang kita lanjutkan untuk melihat fungsi multiplikatif yang lain, yaitu fungsi jumlah pembagi dan fungsi banyak (cacah) pembagi. Kita akan menunjukkan bahwa kedua fungsi tersebut adalah fungsi multiplikatif dan akan kita pelajari teorema-teorema yang terkait. Pada akhir uraian dapat kita lihat bahwa mencari nilai fungsi multiplikatif adalah pekerjaan yang relatif lebih mudah daripada mencari nilai bilangan jika nilai fungsi bilangan itu diketahui.

Definisi 6.2

- (a) Fungsi jumlah pembagi, ditunjukkan dengan σ , didefinisikan dengan aturan $\sigma(n)$ sama dengan jumlah semua pembagi yang positif dari n , dinyatakan dengan $\sigma(n) = \sum_{d|n} d$.
- (b) Fungsi banyak pembagi, ditunjukkan dengan τ , didefinisikan dengan aturan $\tau(n)$ sama dengan banyaknya semua pembagi yang positif dari n , dinyatakan dengan $\tau(n) = \sum_{d|1} 1$.

Contoh 6.11

- (a) Pembagi yang positif dari 1 adalah 1, maka $\sigma(1) = 1$ dan $\tau(1) = 1$
- (b) Pembagi-pembagi yang positif dari 2 adalah 1 dan 2, maka $\sigma(2) = 3$ dan $\tau(2) = 2$
- (c) Pembagi-pembagi yang positif dari 6 adalah 1, 2, 3, 6, maka $\sigma(6) = 1 + 2 + 3 + 6 = 12$ dan $\tau(6) = 4$

Sebelum kita membuktikan suatu teorema yang akan digunakan untuk menunjukkan bahwa fungsi jumlah pembagi dan fungsi banyak pembagi merupakan fungsi-fungsi multiplikatif, marilah kita memperhatikan peragaan berikut.

Misalkan ditentukan $n = 60$, dan kita akan mencari $F(60) = \sum_{d|60} f(d)$

dengan f adalah suatu fungsi multiplikatif. Pembagi-pembagi yang positif dari 60 adalah 1,2,3,4,5,6,10,12,15,20,30,60. Perhatikan bahwa $60 = 4 \cdot 15$, kemudian pembagi-pembagi yang positif dari 60 dinyatakan sebagai perkalian dua bilangan, bilangan pertama faktor 4 dan bilangan kedua faktor 60, sehingga diperoleh :

$$1 = 1 \cdot 1$$

$$5 = 1 \cdot 5$$

$$15 = 1 \cdot 15$$

$$2 = 2 \cdot 1$$

$$6 = 2 \cdot 3$$

$$20 = 4 \cdot 5$$

$$3 = 1 \cdot 3$$

$$10 = 2 \cdot 5$$

$$30 = 2 \cdot 15$$

$$4 = 4 \cdot 1$$

$$12 = 4 \cdot 3$$

$$60 = 4 \cdot 15$$

dan kita dapat mencari $F(60)$

$$\begin{aligned}
 F(60) &= \sum_{d|60} f(d) \\
 &= f(1) + f(2) + f(3) + f(4) + f(5) + f(6) + f(10) + f(12) + f(15) + \\
 &\quad f(20) + f(30) + f(60) \\
 &= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(1 \cdot 5) + f(2 \cdot 3) + f(2 \cdot 5) + f(4 \cdot 3) + \\
 &\quad f(1 \cdot 15) + f(4 \cdot 5) + f(2 \cdot 15) + f(4 \cdot 15) \\
 &= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(1)f(5) + f(2)f(3) + \\
 &\quad f(2)f(5) + f(4)f(3) + f(1)f(15) + f(4)f(5) + f(2)f(15) + f(4)f(15) \\
 &= \{f(1) + f(2) + f(4)\} \{f(1) + f(3) + f(5) + f(15)\}
 \end{aligned}$$

Karena $F(4) = \sum_{d|4} f(d) = f(1) + f(2) + f(4)$ dan $F(15) = \sum_{d|15} f(d) = f(1) + f(3) + f(5) + f(15)$, maka $F(60) = \sum_{d|60} f(d) = \{f(1) + f(2) + f(4)\}$
 $\{f(1) + f(3) + f(5) + f(15)\} = F(4)F(15)$.

Teorema 6.9

Jika f adalah suatu fungsi multiplikatif, maka fungsi F yang didefinisikan dengan $F(n) = \sum_{d|n} f(d)$ juga merupakan fungsi multiplikatif.

Bukti:

Untuk menunjukkan bahwa F adalah suatu fungsi multiplikatif, harus ditunjukkan bahwa jika a dan b adalah bilangan-bilangan bulat positif dan $(a, b) = 1$, maka $F(ab) = F(a)F(b)$.

Ambil $a, b \in \mathbb{Z}^+$ dan $(a, b) = 1$, kemudian pembagi-pembagi yang positif dari ab dinyatakan sebagai perkalian dua bilangan r dan s dengan $(r, s) = 1$, sedemikian hingga r membagi a dan s membagi b .

Untuk masing-masing pasangan r dan s berlaku $d = r.s$

Sekarang ambil $n = ab$, maka $F(n) = F(ab) = \sum_{\substack{r|a \\ s|b}} f(rs)$

Karena f adalah suatu fungsi multiplikatif dan $(r, s) = 1$, maka:

$$F(n) = F(ab) = \sum_{\substack{r|a \\ s|b}} f(r, s) = \sum_{r|a} f(r) \sum_{s|b} f(s) = F(a)F(b)$$

Teorema 6.10

Fungsi jumlah pembagi σ dan fungsi banyak pembagi τ adalah fungsi-fungsi multiplikatif

Bukti:

Kita tentukan $f(n) = n$ dan $g(n) = 1$. Fungsi f dan fungsi g adalah fungsi-fungsi multiplikatif sebab $f(mn) = mn = f(m)f(n)$ dan $g(mn) = 1 \cdot 1 = g(m)g(n)$.

Karena $\sigma(n) = \sum_{d|n} d = \sum_{d|n} f(d)$ dan $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} g(d)$, maka sesuai

Teorema 6.9, σ dan τ adalah fungsi-fungsi multiplikatif.

Teorema 6.11

Jika p adalah suatu bilangan prima dan $k \in \mathbb{Z}^+$, maka:

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1} \text{ dan } \tau(p^k) = k + 1$$

Bukti :

Pembagi-pembagi p^k adalah $1, p, p^2, p^3, \dots, p^{k-1}, p^k$, berarti p^k tepat mempunyai $(k+1)$ pembagi, dengan demikian $\tau(p^k) = k+1$. Selanjutnya, karena deret $1 + p + p^2 + \dots + p^k$ merupakan deret geometri dengan suku pertama 1 dan pembanding p , maka dapat ditentukan bahwa:

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

Teorema 6.12

Jika n adalah suatu bilangan bulat positif yang mempunyai pemfaktoran prima: $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ maka:

$$(a) \quad \sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_t^{k_t+1} - 1}{p_t - 1}$$

$$(b) \quad \tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_t + 1)$$

Bukti :

Sesuai dengan Teorema 6.10, σ dan τ adalah fungsi-fungsi multiplikatif, sehingga:

$$\sigma(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\dots\sigma(p_t^{k_t}) \text{ dan}$$

$$\tau(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \tau(p_1^{k_1})\tau(p_2^{k_2})\dots\tau(p_t^{k_t})$$

Selanjutnya, dengan menggunakan Teorema 6.11 dapat ditentukan bahwa:

$$(a) \quad \sigma(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\dots\sigma(p_t^{k_t}) =$$

$$\frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \dots \frac{p_t^{k_t+1}-1}{p_t-1} = \prod_{j=1}^t \frac{p_j^{k_j+1}-1}{p_j-1}$$

$$(b) \quad \tau(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = \tau(p_1^{k_1})\tau(p_2^{k_2})\dots\tau(p_t^{k_t}) = (k_1+1)(k_2+1)\dots(k_t+1)$$

$$= \prod_{j=1}^t (k_j+1)$$

Contoh 6.12

$$(a) \quad \sigma(125) = \sigma(5^3) = 1 + 5 + 5^2 + 5^3 = \frac{5^4 - 1}{5 - 1} = 156$$

$$\tau(125) = \tau(5^3) = 3 + 1 = 4$$

$$(b) \quad \sigma(200) = \sigma(2^3 5^2) = \sigma(2^3)(5^2) = \frac{2^4 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15 \cdot 31 = 465$$

$$\tau(200) = \tau(2^3 5^2) = \tau(2^3)\tau(5^2) = (3 + 1)(2 + 1) = 4 \cdot 3 = 12$$

Tugas

Jika n diketahui, maka cara untuk mencari $\phi(n)$, $\sigma(n)$ dan $\tau(n)$ sudah diuraikan dengan jelas dan rinci. Permasalahan berikutnya adalah bagaimana mencari n jika $\phi(n)$, $\sigma(n)$ dan $\tau(n)$ diketahui. Uraikan dengan jelas bagaimana menjawab pertanyaan-pertanyaan berikut:

- 1) Carilah n jika $\phi(n) = 1, 2, 3, 6$
- 2) Carilah semua bilangan bulat positif n jika $\sigma(n) = 12, 18$
- 3) Carilah bilangan bulat positif terkecil n jika $\tau(n) = 2, 3$

Apa komentar Anda setelah memperoleh jawaban, adakah cara yang sistematis yang dapat digunakan untuk menjawab?

Buatlah tabel nilai $\phi(n)$, $\sigma(n)$ dan $\tau(n)$ untuk $n = 1, 2, 3, \dots, 60$

Petunjuk Jawaban Tugas

1) Ambil

$$n = 2^s p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}, \phi(n) = 2^{s-1} \left(p_1^{k_1} - p_1^{k_1-1} \right) \left(p_2^{k_2} - p_2^{k_2-1} \right) \dots \left(p_t^{k_t} - p_t^{k_t-1} \right)$$

$$\text{atau } \phi(n) = 2^{s-1} p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_t} \right)$$

Jika $\phi(n) = 1$, maka $n = 1$, atau $s = 1$ dan $n = 2$

Jika $\phi(n) = 2$, maka $s = 2$ dan $n = 2^2$, atau $s = 1$ dan $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 2$

berarti $p_1^{k_1} = 3$ dan $n = 2^1 3^1$, atau $s = 0$ dan $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 2$ berarti $p_1^{k_1} = 3$ dan $n = 3^1$.

Jika $\phi(n) = 3$, maka $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 3$, tidak mungkin, berarti tidak ada jawaban.

Jika $\phi(n) = 6$, maka $s = 2$ dan $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 3$ berarti tidak ada jawaban; atau $s = 1$ dan $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 6$ sehingga $p_1^{k_1} = 9$ dan $n = 2^1 \cdot 3^2$ atau $p_1^{k_1} = 7$ dan $n = 2^1 7^1$; atau $k = 0$ dan $\left(p_1^{k_1} - p_1^{k_1-1} \right) = 6$ sehingga $p_1^{k_1} = 9$ dan $n = 3^2$ atau $p_1^{k_1} = 7$ dan $n = 7^1$

2) Misalkan $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, maka $\sigma(n) = \prod_{i=1}^t (1 + p_i + p_i^2 + \dots + p_i^{k_i})$

Jika $\sigma(n) = 12$, maka masing-masing faktor $\sigma(n)$ membagi 12, sehingga kemungkinan memperoleh faktor 12 selain 1 adalah $3 = 1+2$, $4 = 1+3$, $6 = 1+5$, dan $12 = 1+11$. Dari faktor-faktor itu diperoleh nilai n yang memenuhi yaitu $n = 2, 3, 5, 11$.

Jika $\sigma(n) = 18$, maka masing-masing faktor $\sigma(n)$ membagi 18, sehingga kemungkinan memperoleh faktor 18 selain 1 adalah $3 = 1+2$, $6 = 1+5$, dan $18 = 1+17$. Dari faktor-faktor itu diperoleh nilai n yang memenuhi yaitu $n = 2, 5, 17$

3) Misalkan $n = \prod_{j=1}^t p_j^{k_j}$ dan $\tau(n) = \prod_{j=1}^t (k_j + 1)$

Jika $\tau(n) = 2$, maka kita perlu mempunyai $n = p$ dengan p adalah suatu bilangan prima, akibatnya nilai terkecil n agar $\tau(n) = 2$ adalah $n = p = 2$.

Jika $\tau(n) = 3$, maka kita perlu mempunyai $n = p^2$ dengan p adalah suatu bilangan prima, akibatnya nilai terkecil n agar $\tau(n) = 3$ adalah $n = 2^2$.

Dari hasil memperoleh jawaban di atas dapat diketahui bahwa tidak mudah mencari n jika $\phi(n)$, $\sigma(n)$ dan $\tau(n)$ diketahui, apalagi untuk nilai-nilai n yang semakin besar.

Tabel Nilai Fungsi-fungsi Aritmetika

n	$\phi(n)$	$\tau(n)$	$\sigma(n)$	n	$\phi(n)$	$\tau(n)$	$\sigma(n)$	n	$\phi(n)$	$\tau(n)$	$\sigma(n)$
1	1	1	1	21	12	4	32	41	40	2	42
2	1	2	3	22	10	4	36	42	12	8	96
3	2	2	4	23	22	2	24	43	42	2	44
4	2	3	7	24	8	8	60	44	20	6	84
5	4	2	6	25	20	3	31	45	24	6	78
6	2	4	12	26	12	4	42	46	22	4	72
7	6	2	8	27	18	4	40	47	46	2	48
8	4	4	15	28	12	6	56	48	16	10	124
9	6	3	13	29	28	2	30	49	42	3	57
10	4	4	18	30	8	8	72	50	20	6	93
11	10	2	12	31	30	2	32	51	32	4	72
12	4	6	28	32	16	6	63	52	24	6	98
13	12	2	14	33	20	4	48	53	52	2	54
14	6	4	24	34	16	4	54	54	18	8	120
15	8	4	24	35	24	4	48	55	40	4	72
16	8	5	31	36	12	9	91	56	24	8	120
17	16	2	18	37	36	2	38	57	36	4	80
18	6	6	39	38	18	4	60	58	28	4	90
19	18	2	20	39	24	4	56	59	58	2	60
20	8	6	42	40	16	8	90	60	16	12	168

**LATIHAN**

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Jelaskan apakah fungsi-fungsi aritmetika berikut merupakan fungsi multiplikatif lengkap
 - (a) $f(n) = 3$
 - (b) $f(n) = n!$
 - (c) $f(n) = 4n + 5$
 - (d) $f(n) = n^n$
- 2) Carilah:
 - (a) $\phi(360)$
 - (b) $\phi(144000)$
- 3) Carilah bilangan bulat positif n jika $\phi(3n) = 3\phi(n)$
- 4) Carilah $\sigma(n)$ dan $\tau(n)$ jika:
 - (a) $n = 720$
 - (b) $n = 8!$
- 5) Carilah bilangan-bilangan bulat positif yang:
 - (a) mempunyai sebanyak ganjil pembagi
 - (b) tepat mempunyai dua pembagi yang positif
 - (c) tepat mempunyai tiga pembagi yang positif

Petunjuk Jawaban Latihan

- 1) (a) $f(n) = 3$, maka $f(m) = 3$, $f(mn) = 3$, $f(m)f(n) = 3 \cdot 3 = 9 \neq f(mn)$, tidak multiplikatif
- (b) $f(n) = n!$, maka $f(m) = m!$, $f(mn) = (mn)!$ $\neq m! n!$ atau $f(mn) \neq f(m)f(n)$, tidak multiplikatif
- (c) $f(n) = 4n + 5$, maka $f(m) = 4m + 5$, $f(mn) = 4(mn) + 5 \neq (4m + 5)(4n + 5)$ atau $f(mn) \neq f(m)f(n)$, tidak multiplikatif

(d) $f(n) = n^n$, maka $f(m) = m^m$, $f(mn) = (mn)^{mn} \neq m^m n^n$ atau $f(mn) \neq f(m)f(n)$, tidak multiplikatif.

2) (a) $\phi(360) = \phi(2^3 3^2 5^1) = 2^2 (2-1) 3^1 (3-1) 5^0 (5-1) = 4 \cdot 1 \cdot 3 \cdot 2 \cdot 1 \cdot 4 = 96$

(b) $\phi(144000) = \phi(2^7 3^2 5^3) = 2^6 (2-1) 3^1 (3-1) 5^2 (5-1) = 512 \cdot 1 \cdot 3 \cdot 2 \cdot 25 \cdot 4 = 307200$

3) Ambil $n = 3^k m$, yaitu $3|n$ untuk $k \geq 1$, dan $(3, m) = 1$.

Jika $k = 0$, maka $\phi(n) = \phi(m)$ dan $\phi(3n) = \phi(3 \cdot 3^k m) = \phi(3^{k+1} m) = \phi(3m) = \phi(3)\phi(m) = 2\phi(m) = 2\phi(n) \neq 3\phi(n)$. Dengan demikian $k \geq 1$
 $\phi(3n) = \phi(3 \cdot 3^k m) = \phi(3^{k+1} m) = \phi(3^{k+1})\phi(m) = (3^{k+1} - 3^k)\phi(m) = 3(3^k - 3^{k-1})\phi(m) = 3\phi(3^k)\phi(m) = 3\phi(3^k m) = 3\phi(n)$.

Jadi $\phi(3n) = 3\phi(n)$ jika $3|n$.

4) (a) $\sigma(720) = \sigma(2^4 3^2 5^1) = \sigma(2^4)\sigma(3^2)\sigma(5^1) = \frac{2^5 - 1}{2-1} \cdot \frac{3^3 - 1}{3-1} \cdot \frac{5^2 - 1}{5-1} = 31 \cdot 13 \cdot 6 = 2418$

$\tau(720) = \tau(2^4 3^2 5^1) = \tau(2^4)\tau(3^2)\tau(5^1) = (4+1)(2+1)(1+1) = 30$

(b) $8! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 1 \cdot 2 \cdot 3 \cdot 2 \cdot 2.5 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 2 = 2^7 5^1 7^1$

$\sigma(8!) = \sigma(2^7 5^1 7^1) = \sigma(2^7)\sigma(5^1)\sigma(7^1) = \frac{2^8 - 1}{2-1} \cdot \frac{5^2 - 1}{5-1} \cdot \frac{7^2 - 1}{7-1} = 256 \cdot 6 \cdot 8 = 12288$

5) (a) Misalkan $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, maka $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_t + 1)$.

Karena $\tau(n)$ ganjil, maka masing-masing faktor $(k_i + 1)$ harus ganjil, dengan demikian k_i harus genap, berarti masing-masing p_i berpangkat genap, atau $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ merupakan kuadrat sempurna.

(b) Bilangan bulat positif yang tepat mempunyai dua pembagi positif adalah bilangan prima.

(c) Bilangan bulat positif yang tepat mempunyai tiga pembagi yang positif adalah bilangan-bilangan yang mempunyai bentuk p^2 dengan p adalah bilangan prima.

Karena $\tau(p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}) = (k_1 + 1)(k_2 + 1) \dots (k_t + 1)$ merupakan hasil perkalian dari faktor-faktor untuk memperoleh tiga. Ini berarti salah satu faktor adalah 3, dan yang lain adalah 0. Jadi tepat satu $k_i = 2$, dan $n = p_i$ atau $n = p_i^2$.



Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang fungsi-fungsi aritmetika, terutama tentang konsep fungsi multiplikatif, konsep fungsi ϕ -Euler, fungsi jumlah pembagi, fungsi banyak pembagi, dan keterkaitannya dengan pemfaktoran prima. Penentuan nilai $\phi(n)$, $\tau(n)$, dan $\sigma(n)$ untuk sebarang bilangan bulat positif n , dapat dilakukan dengan mudah berdasarkan teorema-teorema yang telah dibuktikan, tetapi penentuan n jika $\phi(n)$, $\tau(n)$ dan $\sigma(n)$ diketahui tidaklah mudah karena memerlukan analisis yang cermat. Untuk memudahkannya, telah dibuat tabel harga $\phi(n)$, $\tau(n)$ dan $\sigma(n)$ untuk nilai-nilai n sampai batas tertentu.

1. **Definisi 6.1** tentang fungsi aritmetika, fungsi multiplikatif, dan fungsi multiplikatif lengkap.
2. **Definisi 6.2** tentang jumlah pembagi dan fungsi banyak pembagi.
3. **Teorema 6.1**

Jika f adalah suatu fungsi multiplikatif, dan $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari suatu bilangan bulat positif n , maka $f(n) = f(p_1^{k_1})f(p_2^{k_2}) \dots f(p_t^{k_t})$

4. **Teorema 6.2**
Jika p adalah suatu bilangan prima, maka $\phi(p) = p - 1$, dan jika $\phi(p) = p - 1$, maka p adalah suatu bilangan prima.
5. **Teorema 6.3**
Jika p adalah suatu bilangan prima dan k adalah suatu bilangan bulat positif, maka: $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$
6. **Teorema 6.4**
Jika $p, q \in \mathbb{Z}^+$ dan $(p, q) = 1$, maka $\phi(pq) = \phi(p)\phi(q)$

7. Teorema 6.5

Jika $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari $n \in Z^+$, maka:

$$\phi(n) = \left\{ p_1^{k_1-1} (p_1 - 1) \right\} \left\{ p_2^{k_2-1} (p_2 - 1) \right\} \dots \left\{ p_t^{k_t-1} (p_t - 1) \right\}$$

8. Teorema 6.6

Jika $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ adalah pemfaktoran prima dari $n \in Z^+$, maka:

$$\phi(n) = n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_t} \right)$$

9. Teorema 6.7

Jika $n \in Z^+$, dan $n > 2$, maka $\phi(n)$ adalah suatu bilangan bulat genap

10. Teorema 6.8

Jika $n \in Z^+$, maka $n = \sum_{i|n} \phi(i) = \sum_{i|n} \phi(n/i)$

11. Teorema 6.9

Jika f adalah suatu fungsi multiplikatif, maka fungsi F yang didefinisikan dengan: $F(n) = \sum_{d|n} f(d)$ juga merupakan fungsi multiplikatif.

12. Teorema 6.10

Fungsi jumlah pembagi σ dan fungsi banyak pembagi τ adalah fungsi-fungsi multiplikatif.

13. Teorema 6.11

Jika p adalah suatu bilangan prima dan $k \in Z^+$, maka:

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1} \text{ dan } \tau(p^k) = k + 1$$

14. Teorema 6.12

Jika n adalah suatu bilangan bulat positif yang mempunyai pemfaktoran prima: $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, maka:

$$(a) \quad \sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_t^{k_t+1} - 1}{p_t - 1}$$

$$(b) \quad \tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_t + 1)$$



TES FORMATIF 1

- 1) Skor 20
 - (a) Carilah $\phi(9000)$
 - (b) Carilah $\sigma(n)$ dan $\tau(n)$ jika $n = 200772$
- 2) Skor 10

Buktikan: jika $x, y \in N$, maka $\phi(x^y) = x^{y-1}\phi(x)$
- 3) Skor 10

Carilah bilangan bulat positif n jika $\phi(n)$ habis dibagi oleh 4
- 4) Skor 10

Carilah bilangan bulat positif n jika $\phi(n) | n$
- 5) Skor 10

Jika n adalah suatu bilangan bulat positif, tunjukkan bahwa :

$$\phi(2n) = \begin{cases} \phi(n) & \text{jika } n \text{ adalah ganjil} \\ 2\phi(n) & \text{jika } n \text{ adalah genap} \end{cases}$$
- 6) Skor 10

Carilah bilangan-bilangan bulat positif n yang tepat mempunyai empat pembagi
- 7) Skor 20

$\sigma_k(n)$ menyatakan jumlah pangkat k dari pembagi-pembagi n , yaitu:

$$\sigma_k(n) = \sum_{d|n} d^k, \quad \sigma_1(n) = \sigma(n)$$

Carilah $\sigma_3(4), \sigma_3(6)$, dan $\sigma_3(12)$

Carilah aturan mencari $\sigma_k(p)$ jika p adalah suatu bilangan prima

Carilah aturan mencari $\sigma_k(p^t)$ jika p adalah suatu bilangan prima dan $t \in \mathbb{Z}^+$

Tunjukkan bahwa σ_k adalah multiplikatif
- 8) Skor 10

Carilah hasil kali dari pembagi-pembagi n yang positif.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Bilangan Perfek dan Bilangan Mersenne**

Kajian sistematis pertama tentang sifat-sifat bilangan, sebagai pengembangan teori bilangan, merupakan kerja dari kelompok Pythagoras (*Pythagoreans*) pada sekitar tahun 550 SM. Menurut rekaman sejarah, Pythagoras merupakan matematisi Yunani kuno sebelum Euclides. Ia diperkirakan lahir di Pulau Samos tahun 569 SM, dan pada masa hidupnya pernah berkelana ke Mesir dan Babylonia untuk belajar tentang bilangan dari para pemimpin agama (*priests*).

Menjelang akhir hidupnya, Pythagoras menetap di kota Crotona (Italia Selatan), menghimpun sekelompok masyarakat ilmuwan secara rahasia (*secret society*) dari sekitar 60 orang bangsawan (*aristocrats*), dan disebut *Pythagoreans*. Filsafat yang dianut oleh *Pythagoreans* adalah bilangan mengatur alam (*number rules universe*), artinya mereka mempercayai adanya hubungan mistik antara bilangan dan realitas kehidupan.

Kontribusi *Pythagoreans* dalam mempelajari sifat-sifat bilangan adalah:

1. sifat bilangan yang dikaitkan dengan jumlah pembagi, sehingga muncul istilah bilangan defisien (*deficient numbers*), bilangan abundan (*abundant numbers*), dan bilangan perfek (*perfect numbers*).
2. sifat bilangan yang dikaitkan dengan bangun geometri, sehingga muncul istilah bilangan segibanyak (*polygonal numbers*) yang juga disebut bilangan gambar (*figurate numbers*) atau bilangan geometri (*geometric numbers*).

Definisi 6.3

Jika n adalah suatu bilangan bulat positif, maka n disebut suatu :

- (a) bilangan defisien jika $\sigma(n) < 2n$
- (b) bilangan abundan jika $\sigma(n) > 2n$
- (c) bilangan perfek jika $\sigma(n) = 2n$

Contoh 6.13

- (a) 4 adalah suatu bilangan defisien sebab $\sigma(4) = 1 + 2 + 4 = 7 < 2 \cdot 4$

10 adalah suatu bilangan defisien sebab $\sigma(10) = 1 + 2 + 5 + 10 = 18 < 2 \cdot 10$

(b) 12 adalah suatu bilangan abundan sebab

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

18 adalah suatu bilangan abundan sebab

$$\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39 > 2 \cdot 18$$

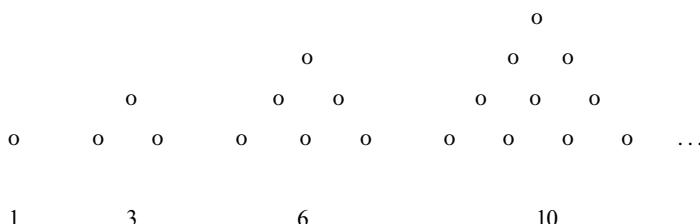
(c) 6 adalah suatu bilangan perfek sebab $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$

28 adalah suatu bilangan perfek sebab

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$$

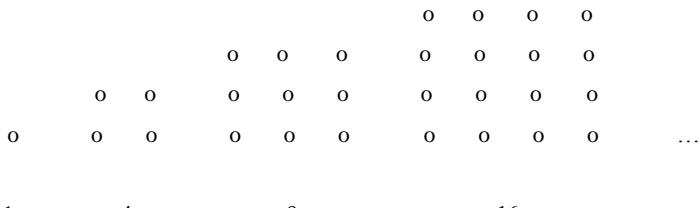
Contoh 6.14

(a) bilangan segitiga dikaitkan dengan bangun datar segitiga



Persoalan yang dikaitkan dengan bilangan segitiga adalah mencari banyaknya noktah pada segitiga ke n dengan n adalah suatu bilangan bulat positif, misalnya mencari banyaknya noktah pada segitiga ke 50, ke 75, atau ke 100.

(b) bilangan persegi (*square numbers*) dikaitkan dengan bangun datar persegi:



Persoalan serupa dengan bilangan segitiga adalah mencari banyaknya noktah pada persegi ke n .

(c) bilangan-bilangan segibanyak yang lain antara lain adalah bilangan segilima (*pentagonal numbers*), bilangan segienam (*hexagonal*

numbers), bilangan segitujuh (*heptagonal numbers*) dan bilangan segidelapan (*octagonal numbers*).

Dari bilangan-bilangan defisien, abundan, dan perfek, yang banyak dikaji dan dibahas lebih lanjut adalah bilangan perfek, sehingga pembahasan berikutnya lebih banyak tentang bilangan perfek dan bilangan Mersenne yang mempunyai kaitan dengan bilangan perfek.

Matematisi Yunani kuno mempunyai cara khusus untuk membuat daftar bilangan perfek dengan menggunakan serangkaian langkah-langkah sistematis berikut :

- (1) ambil bilangan 1
- (2) tambah dengan 2 kali 1, atau tambah dengan 2
- (3) jika hasilnya suatu bilangan prima, kalikan dengan jumlah yang diperoleh dengan bilangan pangkat dua yang terakhir, maka diperoleh suatu bilangan perfek, teruskan seperti langkah (2).
- (4) jika hasilnya bukan bilangan prima, teruskan seperti langkah (2), tambah dengan dua kali bilangan terakhir, atau tambah dengan perpangkatan dua yang terakhir.

Contoh 6.15

Cara mencari bilangan perfek dapat ditabelkan sebagai berikut :

No.	Penjumlahan	Jumlah	Prima	Perkalian	Perfek
1.	$1 + 2$	3	ya	3×2	6
2.	$1 + 2 + 4$	7	ya	7×4	28
3.	$1 + 2 + 4 + 8$	15	bukan	----	---
4.	$1 + 2 + 4 + 8 + 16$	31	ya	31×16	496
5.	$1 + 2 + 4 + 8 + 16 + 32$	63	bukan	----	---
6.	$1 + 2 + 4 + 8 + 16 + 32 + 64$	127	ya	127×64	8128
7.	$1 + 2 + 4 + 8 + 16 + 32 + 64 + 128$	255	bukan	----	---

Teorema 6.13

Suatu bilangan bulat positif n adalah suatu bilangan perfek jika dan hanya jika $n = 2^{m-1} (2^m - 1)$ yang mana $m \in \mathbb{Z}$, $m \geq 2$ dan $2^m - 1$ adalah suatu bilangan prima.

Bukti :

(\leftarrow) Karena 2^{m-1} dan 2^m adalah bilangan-bilangan genap, maka $2^m - 1$ adalah suatu bilangan prima ganjil dan $(2^{m-1}, 2^m - 1) = 1$. Selanjutnya σ adalah suatu fungsi multiplikatif, maka:

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

Menurut Teorema 6.11, $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$, maka $\sigma(2^{m-1}) = \frac{2^{m-1+1} - 1}{2 - 1} =$

$$\frac{2^m - 1}{1} = 2^m - 1 \quad \text{dan karena } (2^m - 1) \text{ adalah bilangan prima, maka}$$

$$\sigma(2^m - 1) = (2^m - 1) + 1 = 2^m, \quad \text{akibatnya:}$$

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

Jadi n adalah suatu bilangan perfek.

(\rightarrow) Misalkan n adalah suatu bilangan perfek, $n = 2^s t$ di mana s dan t adalah bilangan-bilangan bulat positif dan t adalah ganjil. Karena $(2^s, t) = 1$, maka menurut Teorema 2.11 :

$$\sigma(n) = \sigma(2^s \cdot t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t).$$

Selanjutnya, n adalah suatu bilangan perfek, maka $\sigma(n) = 2n = 2^{s+1}t$.

$$\text{Dengan demikian } (2^{s+1} - 1)\sigma(t) = 2^{s+1}t$$

Karena $(2^{s+1} - 1, 2^{s+1}) = 1$, maka $2^{s+1} \mid \sigma(t)$, akibatnya ada suatu bilangan bulat q sehingga $\sigma(t) = q \cdot 2^{s+1}$, dan :

$$(2^{s+1} - 1)q \cdot 2^{s+1} = 2^{s+1}t$$

$$(2^{s+1} - 1)q = t, \quad \text{berarti } q \mid t \text{ dan } q \neq t$$

$$\text{Karena } (2^{s+1} - 1)q = t, \quad \text{maka } t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t)$$

Kita akan tunjukkan bahwa $q = 1$. Misalkan $q \neq 1$, maka ada paling sedikit tiga pembagi positif dari t yang berbeda, yaitu 1, q , dan t , akibatnya $\sigma(t) \geq t + q + 1$, bertentangan dengan $t + q = \sigma(t)$.

Jadi t merupakan suatu bilangan prima karena hanya mempunyai pembagi positif 1 dan t , berarti $n = 2^s(2^{s+1} - 1)$ di mana $2^{s+1} - 1$ adalah suatu bilangan prima.

Teorema 6.14

Jika m adalah suatu bilangan bulat positif dan $2^m - 1$ adalah suatu bilangan prima, maka m adalah suatu bilangan prima.

Bukti:

Misalkan bahwa m adalah bukan suatu bilangan prima, maka m adalah bilangan komposit, yaitu $m = ab$ di mana $1 < a < m$ dan $1 < b < m$, dan:

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$$

Karena dua faktor ruas kanan lebih dari 1, maka $2^m - 1$ adalah suatu bilangan komposit jika m adalah bukan suatu bilangan prima. Dengan demikian jika $2^m - 1$ adalah suatu bilangan prima, maka m adalah juga bilangan prima.

Marilah sekarang kita mempelajari bilangan yang disebut dengan bilangan Mersenne.

Definisi 6.4

Jika m adalah suatu bilangan bulat positif, maka $M_k = 2^k - 1$ disebut bilangan Mersenne ke k , dan jika p adalah suatu bilangan prima dan $M_p = 2^p - 1$ adalah juga suatu bilangan prima, maka M_p disebut suatu bilangan prima Mersenne.

Contoh 6.16

- (a) Bilangan Mersenne ke 1 adalah $M_1 = 2^1 - 1 = 1$
- (b) Bilangan Mersenne ke 2 adalah $M_2 = 2^2 - 1 = 3$
- (c) Bilangan Mersenne ke 3 adalah $M_3 = 2^3 - 1 = 7$
- (d) Bilangan Mersenne ke 4 adalah $M_4 = 2^4 - 1 = 15$
- (e) Bilangan Mersenne ke 5 adalah $M_5 = 2^5 - 1 = 31$

Contoh 6.17

- (a) Bilangan prima Mersenne ke 1 adalah $M_2 = 2^2 - 1 = 3$
- (b) Bilangan prima Mersenne ke 2 adalah $M_3 = 2^3 - 1 = 7$
- (c) Bilangan prima Mersenne ke 3 adalah $M_5 = 2^5 - 1 = 31$
- (d) Bilangan prima Mersenne ke 4 adalah $M_7 = 2^7 - 1 = 127$
- (e) Bilangan prima Mersenne ke 5 adalah $M_{13} = 2^{13} - 1 = 8191$

Contoh 6.18

Bilangan Mersenne ke 11 adalah $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$, merupakan bilangan komposit, dengan demikian M_{11} adalah bukan suatu bilangan prima Mersenne.

Sebelum membuktikan Teorema 6.15, marilah kita lihat dua lemma berikut :

Lemma 6.1

- (a) jika m dan n adalah bilangan-bilangan bulat positif, maka residu positif terkecil $2^m - 1$ modulo $2^n - 1$ adalah $2^r - 1$, di mana r adalah residu positif terkecil dari m modulo n
- (b) Jika m dan n adalah bilangan-bilangan bulat positif, maka $\left(2^m - 1, 2^n - 1\right) = 2^{\left(m,n\right)} - 1$

Bukti:

- (a) Dari algoritma pembagian dapat ditentukan bahwa $m = nq + r$ di mana r adalah residu positif terkecil dari m modulo n .

$$\text{Karena } 2^m - 1 = 2^{nq+r} - 1 = (2^n - 1)(2^{n(q-1)r} + \dots + 2^{n+r} + 2^r) + (2^r - 1),$$

maka sisa pembagian $2^m - 1$ dibagi $2^n - 1$ adalah $2^r - 1$, sehingga $2^r - 1$ adalah residu positif terkecil $2^m - 1$ modulo $2^n - 1$

- (b) Buktikan!

Teorema 6.15

Jika p adalah suatu bilangan prima ganjil, maka sebarang pembagi dari bilangan Mersenne $M_p = 2^p - 1$ mempunyai bentuk $2kp + 1$ di mana k adalah suatu bilangan bulat positif.

Bukti :

Misalkan q adalah suatu bilangan prima yang membagi $M_p = 2^p - 1$.

Teorema Kecil Fermat menyatakan bahwa jika p suatu bilangan prima dan a suatu bilangan bulat positif dengan $(a, p) = 1$, maka $a^{p-1} \equiv 1 \pmod{p}$ atau $p \mid (a^{p-1} - 1)$ dengan demikian $q \mid (2^{q-1} - 1)$.

Selanjutnya, sesuai dengan Lemma 6.1 (b), $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$.

Karena $q \mid 2^p - 1$ dan $q \mid 2^{q-1} - 1$, maka q adalah faktor persekutuan $2^p - 1$ dan $2^{q-1} - 1$, sehingga $q \mid (2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$, berarti $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1 \neq 1$ sebab q adalah suatu bilangan prima.

Jika kita cari, maka kemungkinan nilai $(p, q-1)$ adalah p atau 1 karena bilangan-bilangan yang membagi p adalah 1 dan p . Jika $p = 1$, maka $(2^p - 1, 2^{q-1} - 1) = 1$. Hal ini tidak mungkin karena q tidak membagi $(2^p - 1, 2^{q-1} - 1) = 1$. Jadi $(p, q-1) = p$, dengan demikian ada suatu bilangan bulat positif m sehingga $q-1 = mp$. Karena q adalah ganjil, maka $q-1$ adalah genap, dan pm adalah genap, sehingga m adalah genap. Misalkan $m = 2k$, k adalah suatu bilangan bulat positif, maka dari $q-1 = mp$, diperoleh $q = mp + 1 = 2kp + 1$.

Contoh 6.19

Untuk mengetahui apakah $M_{13} = 2^{13} - 1 = 8191$ adalah suatu bilangan prima, maka perlu dicari faktor-faktor prima yang kurang dari $\sqrt{8191} = 90,504\dots$. Sesuai dengan Teorema 6.15, sebarang faktor prima dari 8191 mempunyai bentuk $26k+1$, sehingga kemungkinan bilangan prima yang kurang dari $\sqrt{M_{13}} = \sqrt{8191} = 90,504\dots$ dan mempunyai bentuk $26k+1$ adalah 53 dan 79. Ternyata keduanya tidak membagi 8191, jadi 8191 adalah prima.

Tugas

Bacalah suatu buku Teori Bilangan, kemudian buktikan Lemma 6.1 (b).

Petunjuk Jawaban Tugas

Lemma 6.1 (b)

Jika $m, n \in \mathbb{Z}^+$, maka $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$

Bukti :

Sesuai dengan Algoritma Euclides, untuk $m = r_0$ dan $n = r_1$ dapat ditentukan bahwa :

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

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

$$\vdots \quad \vdots$$

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

$$r_{k-2} = q_{k-1} r_{k-1} + r_k \quad r_k = 0$$

sehingga $(m, n) = r_{k-1}$

Dengan menggunakan Lemma 6.1 dan langkah-langkah Algoritma Euclides, untuk $R_0 = 2^m - 1$ dan $R_1 = 2^n - 1$ dapat ditentukan bahwa:

$$R_0 = q_1 R_1 + R_2 \quad R_2 = 2^{r_2} - 1$$

$$R_1 = q_2 R_2 + R_3 \quad R_3 = 2^{r_3} - 1$$

$$\vdots \quad \vdots$$

$$R_{k-3} = q_{k-2} R_{k-2} + R_{k-1} \quad R_{k-1} = 2^{r_{k-1}} - 1$$

$$R_{k-2} = q_{k-1} R_{k-1} + R_k \quad R_k = 0$$

sehingga $(R_0, R_1) = R_{k-1}$

Dengan demikian $R_{k-1} = 2^{r_{k-1}} - 1 = 2^{(m,n)} - 1 = (R_0, R_1)$



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Carilah pembagi-pembagi yang positif dari
 - (a) $2^{15} - 1$
 - (b) $2^{111} - 1$

- 2) Carilah 6 bilangan bulat positif abundan terkecil!
- 3) Tunjukkan bahwa setiap perpangkatan prima adalah defisien!
- 4) Tunjukkan bahwa jika $n = 2^{m-1}(2^m - 1)$, m adalah bilangan bulat positif sehingga $2^m - 1$ adalah bilangan komposit, maka n adalah suatu bilangan abundan!
- 5) Dua bilangan bulat positif r dan s disebut bersekawan (*amicable*) jika $\sigma(r) = \sigma(s) = r + s$. Tunjukkan bahwa 220 dan 284 adalah dua bilangan bersekawan!
- 6) Suatu bilangan bulat positif disebut perfek- k jika $\sigma(n) = kn$ (bilangan perfek adalah perfek-2). Tunjukkan bahwa 120 adalah perfek-3!
- 7) Suatu bilangan bulat positif disebut abundan- k jika $\sigma(n) > (k+1)n$. Carilah k jika 2700 merupakan abundan- k !
- 8) Suatu bilangan bulat positif disebut super perfek jika $\sigma(\sigma(n)) = 2n$
Tunjukkan bahwa 16 adalah super perfek!
- 9) Selidiki apakah M_{17} dan M_{29} merupakan bilangan Mersenne prima.
- 10) Tunjukkan bahwa jika n adalah suatu bilangan bulat positif dan $2n+1$ adalah prima, maka $(2n+1) | M_n$ atau $(2n+1) | (M_n + 2)$

Petunjuk Jawaban Latihan

- 1) (a) $2^{15} - 1 = (2^5)^3 - 1^3 = (2^5 - 1)(2^{10} + 2^5 + 1)$, maka $2^5 - 1 = 31$ adalah pembagi $2^{15} - 1$
(b) $3 | 111$, maka $2^3 - 1 = 7 | 2^{111} - 1$
- 2) 12, 18, 20, 24, 30, 36
 $\sigma(12) = 28 > 24$, $\sigma(18) = 39 > 36$, $\sigma(20) = 42 > 40$, $\sigma(24) = 60 > 48$,
 $\sigma(30) = 72 > 60$, $\sigma(36) = 91 > 72$
- 3) Misalkan $n = p^k$, p adalah suatu bilangan prima dan $k \in \mathbb{Z}^+$,
maka $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$. $2p^k - 1 < p^{k+1}$ karena $p \geq 2$, sehingga
 $2p^k(p-1) < 2(p^{k+1} - p^k) = 2p^k(p-1)$.

Dengan demikian $\frac{p^{k+1}-1}{p-1} < 2p^k = 2n$, berarti $n = p^k$ adalah defisien.

- 4) $n = 2^{m-1}(2^m - 1)$, maka $\sigma(n) = \sigma\{2^{m-1}(2^m - 1)\} = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)\sigma(2^m - 1)$.

$$\frac{\sigma(n)}{n} = \frac{(2^m - 1)\sigma(2^m - 1)}{2^{m-1}(2^m - 1)} = \frac{\sigma(2^m - 1)}{2^{m-1}} > 2 \quad \text{atau} \quad \sigma(n) > 2n, \quad \text{dipenuhi}$$

jika n adalah suatu bilangan prima.

- 5) $220 = 2^2 \cdot 5^1 \cdot 11^1$, maka

$$\sigma(220) = \sigma(2^2)\sigma(5)\sigma(11) = (1+2+4)(1+5)(1+11) = 504$$

$$84 = 2^2 \cdot 71^1, \quad \text{maka} \quad \sigma(284) = \sigma(2^2)\sigma(71) = (1+2+4)(1+71) = 504$$

Karena $\sigma(220) = \sigma(284) = 220 + 284 = 504$, maka 220 dan 284 adalah suatu pasangan yang bersekawan.

- 6) $120 = 2^3 \cdot 3^1 \cdot 5^1$, maka

$$\sigma(120) = \sigma(2^3)\sigma(3)\sigma(5) = (1+2+4+8)(1+3)(1+5) = 15 \cdot 4 \cdot 6 = 360 = 3 \cdot 120, \\ \text{sehingga } 120 \text{ adalah perfek-3.}$$

- 7) $2700 = 2^2 \cdot 3^3 \cdot 5^2$, maka

$$\sigma(2700) = \sigma(2^2)\sigma(3^3)\sigma(5^2) = \frac{2^3-1}{2-1} \cdot \frac{3^4-1}{3-1} \cdot \frac{5^3-1}{5-1} = 7 \cdot 40 \cdot 31 = 8680$$

$8680 > (2+1) \cdot 2700$, maka 2700 adalah abundan- k dengan $k = 2$

- 8) $16 = 2^4$, maka $\sigma(16) = \frac{2^5-1}{2-1} = 31$

$\sigma(\sigma(16)) = \sigma(31) = 1+31 = 32 = 2 \cdot 16$, maka 16 adalah suatu super perfek.

- 9) Untuk mengetahui apakah $M_{17} = 2^{17} - 1 = 131071$ suatu bilangan prima, maka perlu dicari faktor-faktor prima yang kurang dari $\sqrt{131071} = 362,037\dots$. Sesuai dengan Teorema 6.15, sebarang faktor prima dari 131071 mempunyai bentuk $34k+1$, sehingga kemungkinan bilangan prima yang kurang dari $\sqrt{M_{17}} = \sqrt{131071} = 362,037\dots$ dan mempunyai bentuk $34k+1$ adalah 103, 137, 239, dan 307, tetapi tidak ada yang membagi 131071. Jadi 131071 adalah suatu bilangan prima.

Dengan jalan yang sama, $M_{29} = 536870911$, $\sqrt{536870911} = 23170,474 \dots$, kemungkinan faktor prima mempunyai bentuk $58k+1$, antara lain 59 dan 117 yang tidak membagi 536870911. Tetapi, $233 = 58 \cdot 4 + 1$ membagi 536870911 karena $536870911 = 233 \cdot 2304167$. Jadi M_{29} adalah bukan suatu bilangan prima.

- 10) $M_n(M_n + 2) = (2^n - 1)(2^n + 1) = 2^{2n} - 1$. Jika $2n+1$ adalah suatu bilangan prima, maka $\phi(2n+1) = (2n+1) - 1 = 2n$. Sesuai dengan Teorema ϕ -Euler, karena $(2, 2n+1) = 1$, maka dapat ditunjukkan bahwa $2^{\phi(2n+1)} \equiv 1 \pmod{2n+1}$, atau $2^{2n} \equiv 1 \pmod{2n+1}$. Dengan demikian $(2n+1)|M_n$ atau $(2n+1)|(M_n + 2)$.



Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang bilangan perfek dan bilangan Mersenne, terutama tentang pengertian bilangan perfek dan bilangan Mersenne, hubungan bilangan prima dengan bilangan Mersenne, serta keterkaitan bilangan perfek dan bilangan Mersenne dengan fungsi-fungsi multiplikatif. Pada bagian akhir dibicarakan tentang manfaat dari bilangan Mersenne untuk menyelidiki keprimaan bilangan melalui kemungkinan faktor-faktor prima yang dapat dicari atau tidak dapat dicari.

1. Definisi 6.3

Jika n adalah suatu bilangan bulat positif, maka n disebut suatu :

- (a) bilangan defisien jika $\sigma(n) < 2n$
- (b) bilangan abundan jika $\sigma(n) > 2n$
- (c) bilangan perfek jika $\sigma(n) = 2n$

2. Definisi 6.4

Jika m adalah suatu bilangan bulat positif, maka $M_k = 2^k - 1$ disebut bilangan Mersenne ke k , dan jika p adalah suatu bilangan prima dan $M_p = 2^p - 1$ adalah juga suatu bilangan prima, maka M_p disebut suatu bilangan prima Mersenne.

3. Teorema 6.13

Suatu bilangan bulat positif n adalah suatu bilangan perfek jika dan hanya jika $n = 2^{m-1} (2^m - 1)$ yang mana $m \in \mathbb{Z}$, $m \geq 2$ dan $2^m - 1$ adalah suatu bilangan prima.

4. Teorema 6.14

Jika m adalah suatu bilangan bulat positif dan $2^m - 1$ adalah suatu bilangan prima, maka m adalah suatu bilangan prima.

5. Lemma 6.1

(a) Jika m dan n adalah bilangan-bilangan bulat positif, maka residi positif terkecil $2^m - 1$ modulo $2^n - 1$ adalah $2^r - 1$, di mana r adalah residi positif terkecil dari m modulo n .

(b) Jika m dan n adalah bilangan-bilangan bulat positif, maka $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$

6. Teorema 6.15

Jika p adalah suatu bilangan prima ganjil, maka sebarang pembagi dari bilangan Mersenne $M_p = 2^p - 1$ mempunyai bentuk $2kp + 1$ di mana k adalah suatu bilangan bulat positif.

**TES FORMATIF 2**

1) Skor 10

Carilah suatu faktor dari :

- (a) $2^{91} - 1$
- (b) $2^{289} - 1$

2) Skor 10

Tunjukkan bahwa sebarang pembagi dari bilangan defisien adalah defisien!

3) Skor 10

Tunjukkan bahwa 1184 dan 1210 adalah pasangan yang bersekawan!

4) Skor 10

Tunjukkan bahwa :

- (a) 30240 adalah perfek-4
- (b) 14182439040 adalah perfek-5

5) Skor 10

Tunjukkan bahwa jika $n = 2^q$ dan $2^{q+1} - 1$ adalah prima, maka n adalah super perfek!

6) Skor 15

Tunjukkan bahwa jika $n = p^k m^2$ adalah bilangan perfek ganjil, dan p adalah bilangan prima, maka $n \equiv p \pmod{8}$.

7) Skor 10

Tunjukkan bahwa jika n adalah suatu bilangan perfek ganjil, maka 3, 5, dan 7 tidak semua pembagi n .

8) Skor 10

- Carilah banyaknya titik pada bilangan segitiga ke 100
- Carilah banyaknya titik pada bilangan pentagonal ke 200

9) Skor 5

Carilah jumlah dari kebalikan semua pembagi dari suatu bilangan perfek. Nyatakan apakah ada kecenderungan suatu pola yang diperoleh.

10) Skor 5

Carilah 10 bilangan segitiga yang pertama, dan amatilah apakah ada bilangan perfek yang juga merupakan bilangan segitiga.

11) Skor 5

Carilah 10 bilangan heksagonal yang pertama, dan amatilah apakah ada bilangan perfek yang juga merupakan bilangan heksagonal.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) (a) $\phi(9000) = \phi(2^3 3^2 5^3) = 2^2 (2-1) 3^1 (3-1) 5^2 (5-1) = 4 \cdot 1 \cdot 3 \cdot 2 \cdot 25 \cdot 4 = 2400$
- (b) $\sigma(200772) = \sigma(2^2 3^3 11^1 13^2) = \frac{2^3 - 1}{2-1} \cdot \frac{3^4 - 1}{3-1} \cdot \frac{11^2 - 1}{11-1} \cdot \frac{13^3 - 1}{13-1} = \frac{7}{1} \cdot \frac{80}{2} \cdot \frac{120}{10} \cdot \frac{2196}{12} = 7 \cdot 40 \cdot 12 \cdot 183 = 614880.$
- 2) Misalkan pemfaktoran prima dari x adalah $x = \prod_{i=1}^t p_i^{k_i}$, maka $\phi(x) = \prod_{i=1}^t \phi(p_i^{k_i})$. Karena $x^y = \prod_{i=1}^t p_i^{y k_i}$, maka $\phi(x^y) = \prod_{i=1}^t \phi(p_i^{y k_i}) = \phi(p_i^{y k_i}) = p_i^{y k_i - 1} (p_i - 1) = p_i^{(y-1)k_i} p_i^{k_i - 1} (p_i - 1) = p_i^{(y-1)k_i} \phi(p_i^{k_i})$
Jadi $\phi(x^y) = \prod_{i=1}^t p_i^{(y-1)k_i} \phi(p_i^{k_i}) = \prod_{i=1}^t p_i^{(y-1)k_i} \prod \phi(p_i^{k_i}) = x^{y-1} \phi(x)$
- 3) Jika $n = 2^s p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ maka $\phi(n) = 2^{s-1} p_1^{k_1 - 1} (p_1 - 1) p_2^{k_2 - 1} (p_2 - 1) \dots p_t^{k_t - 1} (p_t - 1)$
Karena p_i adalah bilangan-bilangan prima ganjil, maka $p_i - 1$ adalah bilangan genap. Jadi $\phi(n)$ habis dibagi 4 jika n memenuhi salah satu dari: (a) $n = 2^s$ dengan $s \geq 3$, (b) n mempunyai pembagi prima ganjil dalam bentuk $4s+1$, (c) n habis dibagi oleh 4 (yaitu $k = 2$), dan (d) n mempunyai dua pembagi prima ganjil.
- 4) Jika $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ dan $\phi(n) | n$, maka $k \phi(n) = kn \left(\frac{p_1 - 1}{p_1} \frac{p_2 - 1}{p_2} \dots \frac{p_t - 1}{p_t} \right)$ sehingga $k = \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1} \dots \frac{p_t}{p_t - 1}$ adalah suatu bilangan bulat. Pembilang paling banyak mempunyai satu faktor 2 dan penyebut paling banyak mempunyai satu faktor dalam bentuk $p_i - 1$ di mana p_i suatu bilangan prima ganjil. Dengan demikian $n = 2^{k_1}$ dan $\phi(n) = 2^{k_1} \frac{2-1}{2} = \frac{2^{k_1}}{2} = \frac{n}{2} | n$, atau $n = 2^{k_1} p^{k_2}$ dan $\phi(n) = n \left(\frac{2-1}{2} \right) \left(\frac{p-1}{p} \right)$ dengan $m = \frac{2}{2-1} \cdot \frac{p}{p-1} = \frac{2p}{p-1}$. Jadi $p-1 = 2$

atau $p=3$ sehingga kita peroleh $n=2^{k_1}3^{k_2}$, yaitu $n=1, 2^{k_1}, 2^{k_1}3^{k_2}$ dengan $k_1, k_2 \geq 1$.

- 5) Jika n adalah bilangan ganjil, maka $(2, n)=1$ dan $\phi(2n)=\phi(2)\phi(n)=1 \cdot \phi(n)=\phi(n)$. Jika n adalah suatu bilangan genap, misalkan $n=2^s t$ dan t adalah suatu bilangan ganjil, maka:

$$\begin{aligned}\phi(2n) &= \phi(2 \cdot 2^s t) = \phi(2^{s+1} t) = \phi(2^{s+1}) \phi(t) = 2^s \phi(t) = 2(2^{s-1} \phi(t)) = \\ &2 \cdot (\phi(2^s) \phi(t)) = 2 \cdot \phi(2^s t) = 2 \phi(n).\end{aligned}$$

- 6) Jika $n=p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ dan $\tau(n)=4$, maka $\tau(n)=(k_1+1)(k_2+1)\dots(k_t+1)=4$ sehingga ada dua kemungkinan yaitu $(k_1+1)=4$ atau $(k_1+1)=(k_2+1)=2$. Dengan demikian dapat ditunjukkan bahwa $k_1=3$ dan $n=p^3$, atau $k_1=k_2=1$ dan $n=p_1 p_2$.

7) (a) $\sigma_3(4)=\sum_{d|4} d^3 = 1^3 + 2^3 + 4^3 = 73$

$$\sigma_3(6)=\sum_{d|6} d^3 = 1^3 + 2^3 + 3^3 + 6^3 = 252$$

$$\sigma_3(12)=\sum_{d|12} d^3 = 1^3 + 2^3 + 3^3 + 4^3 + 6^3 + 12^3 = 2044$$

(b) $\sigma_k(p)=\sum_{d|p} d^k = 1^k + p^k = 1 + p^k$

(c) $\sigma_k(p^t)=\sum_{d|p^t} d^k = 1^k + p^k + (p^2)^k + \dots + (p^t)^k = 1^k + p^k + p^{2k} + \dots + p^{tk} = \frac{(p^{tk}-1)}{p-1}$

(d) Misalkan r dan s adalah bilangan-bilangan bulat positif dan $(r, s)=1$, maka $\sum_{d|rs} d^k = \sum_{d_1|r, d_2|s} (d_1 d_2)^k = \sum_{d_1|r} d_1^k \sum_{d_2|s} d_2^k = \sigma_k(r) \sigma_k(s)$.

- 8) Jika n bukan suatu bilangan kuadrat sempurna, maka pembagi-pembagi n berpasangan, artinya jika d adalah suatu pembagi, maka n/d juga suatu pembagi. Karena terdapat $\tau(n)/2$ pasangan, maka hasil kali semua pembagi adalah $n^{\tau(n)/2}$.

Jika n adalah suatu bilangan kuadrat sempurna, maka terdapat $\frac{\tau(n)-1}{2}$ pasangan yang hasil kalinya n , dan satu pembagi tambahan yaitu \sqrt{n} .

Jadi perkalian semua pembagi n adalah $n^{(\tau(n)-1)/2} \cdot n^{1/2} = n^{\tau(n)/2}$

Tes Formatif 2

- 1) (a) $7|91$, dan $2^7 - 1 = 127$, maka $127|2^{91} - 1$
 (b) $17|289$, dan $2^{17} - 1 = 131071$, maka $131071|2^{289} - 1$
- 2) Misalkan $r, s \in \mathbb{Z}$ dan $rs = \prod p_i^{m_i}$ dan $s = \prod p_i^{n_i}$, p_i adalah prima-prima yang berbeda dan $m_i > n_i$, maka

$$\frac{\sigma(mn)}{mn} = \prod \frac{p_i - p_i^{-m_i}}{p_i - 1} > \prod \frac{p_i - p_i^{-n_i}}{p_i - 1} = \frac{\sigma(n)}{n}$$
. Jadi, jika mn adalah defisien, maka $\frac{\sigma(n)}{n} < \frac{\sigma(mn)}{mn} < 2$, atau n juga defisien.
- 3) $1184 = 2^5 \cdot 37$, maka

$$\sigma(1184) = \sigma(2^5)\sigma(37) = \left(\frac{2^6 - 1}{2 - 1}\right)(37 + 1) = 63 \cdot 38 = 2394$$

$1210 = 2^1 \cdot 5^1 \cdot 11^2$, maka

$$\sigma(1210) = \sigma(2)\sigma(5)\sigma(11^2) = (2 + 1)(5 + 1)\left(\frac{11^3 - 1}{11 - 1}\right) = 2394$$

1184 dan 1210 adalah bersekawan sebab

$$\sigma(1184) = \sigma(1210) = 2394 = 1184 + 1210 = 2394.$$

- 4) (a) $30240 = 2^5 \cdot 3^3 \cdot 5^1 \cdot 7^1$, $\sigma(30240) = \sigma(2^5)\sigma(3^3)\sigma(5)\sigma(7) = 63 \cdot 40 \cdot 6 \cdot 8 = 120960 = 4 \cdot 30240$
 (b) $14182439040 = 2^7 \cdot 3^4 \cdot 5^1 \cdot 7^1 \cdot 11^2 \cdot 17^1 \cdot 19^1$
 $\sigma(14182439040) = 255 \cdot 121 \cdot 6 \cdot 8 \cdot 133 \cdot 18 \cdot 20 = 5 \cdot 14182439040$
- 5) $\sigma(\sigma(2q)) = \sigma(2^{q+1} - 1) = (2^{q+1} - 1) + 1 = 2^{q+1} = 2 \cdot 2^q$
- 6) m ganjil, maka $m^2 \equiv 1 \pmod{8}$, sehingga $n = p^k m^2 \equiv p^k \pmod{8}$. Dapat ditunjukkan bahwa $k \equiv 1 \pmod{4}$, sehingga $p^k = p^{4t} p \equiv p \pmod{8}$ karena p^{4t} adalah suatu kuadrat bilangan ganjil. Jadi $n \equiv p \pmod{8}$.

- 7) Ambil $n = 3^r 5^s 7^t \prod p_i^{m_i}$. Karena 3 dan 7 tidak kongruen dengan 1 modulo 4, maka haruslah $r, t \geq 2$, maka

$$2 < \frac{13.6.57}{9.5.49} = \frac{\sigma(3^2.5.7^2)}{3^2.5.7^2} \leq \frac{\sigma(n)}{n} = 2, \text{ terjadi kontradiksi.}$$

- 8) Usahakan menemukan pola (*pattern*) untuk mencari banyaknya noktah (titik) pada bangun ke n .

- (a) Jika banyaknya titik pada segitiga ke n dinyatakan dengan T_n , maka:

$$T_1 = 1$$

$$T_2 = 3 = 1 + 2$$

$$T_3 = 6 = 1 + 2 + 3$$

$$T_4 = 10 = 1 + 2 + 3 + 4$$

Dengan demikian $T_{100} = 1 + 2 + 3 + \dots + 100 = 5050$

- (b) Jika banyaknya titik pada segilima ke n dinyatakan dengan L_n , maka:

$$L_1 = 1 = (1/2)(2) = (1/2)(1)(3.1 - 1)$$

$$L_2 = 5 = 1 + 4 = (1/2)(2)(3.2 - 1)$$

$$L_3 = 12 = 1 + 4 + 7 = (1/2)(3)(3.3 - 1)$$

$$L_4 = 22 = 1 + 4 + 7 + 10 = (1/2)(4)(3.4 - 1)$$

Dengan demikian

$$L_{100} = 1 + 4 + 7 + \dots + 298 = (1/2)(100)(3.100 - 1) = 14950$$

- 9) Faktor-faktor yang positif dari 6 adalah 1, 2, 3, dan 6

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1 + 1 = 2$$

Faktor-faktor yang positif dari 28 adalah 1, 2, 4, 7, 14, dan 28

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \frac{1}{7} + \frac{1}{14} + \frac{1}{28} = 1 + \frac{14}{28} + \frac{7}{28} + \frac{4}{28} + \frac{2}{28} + \frac{1}{28} = 1 + 1 = 2$$

Dengan demikian dapat diduga bahwa jika n adalah bilangan perfek,

$$\text{maka } \sum_{d|n} \frac{1}{d} = 2.$$

- 10) Sepuluh bilangan segitiga yang pertama adalah :

1, 3, 6, 10, 15, 21, 28, 36, 45, 55

Bilangan perfek 6 dan 28 terdapat dalam barisan sepuluh bilangan segitiga yang pertama.

- 11) Sepuluh bilangan segienam yang pertama adalah:

1, 6, 15, 28, 45, 66, 91, 120, 153, 190

Bilangan perfek 6 dan 28 terdapat dalam barisan sepuluh bilangan segienam yang pertama.

Daftar Pustaka

- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Persamaan Diophantine

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul Persamaan Diophantine ini diuraikan tentang sifat-sifat dasar Persamaan Diophantine linier dan tidak linier, yaitu persamaan-persamaan yang menuntut penyelesaian bulat. Menyelesaikan Persamaan Diophantine berarti mencari bilangan-bilangan bulat yang memenuhi persamaan tersebut. Bentuk Persamaan Diophantine tidak berbeda dengan persamaan pada umumnya, yaitu memuat dua atau lebih variabel tetapi cara menyelesaikan banyak menggunakan sifat-sifat kongruensi, keterbagian, FPB dan KPK, serta keprimaan.

Pembahasan tentang persamaan Diophantine linier ditekankan pada bagaimana memperoleh selesaian dengan cara biasa, cara reduksi, dan cara kongruensi. Persamaan yang akan diselesaikan terbatas pada persamaan-persamaan dengan dua variabel dan tiga variabel.

Pembahasan tentang persamaan Diophantine non linier meliputi triple Pythagoras dan bilangan jumlah kuadrat, serta persamaan lain yang sejenis. Meskipun pada awalnya secara sistematis kita dapat mempelajari langkah-langkah penyelesaian persamaan Diophantine non linier, ternyata jenis dan ragam persamaan ini menjadi banyak dan perlu perlakuan khusus penyelesaian yang tidak selalu sama dengan cara yang telah diketahui sebelumnya.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep persamaan Diophantine linier dan non linier, mampu menyelesaikan persamaan Diophantine linier dan non linier, serta memahami keterkaitan persamaan Diophantine dengan topik-topik tertentu di dalam teori bilangan.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep persamaan Diophantine linier dan non linier, menyelesaikan persamaan Diophantine linier dengan cara biasa, cara reduksi, dan cara kongruensi, menjelaskan triple Pythagoras

primitif dan non primitif dengan sifat-sifatnya, menyelesaikan persamaan Diophantine non linier yang serupa triple Pythagoras, dan menjelaskan sifat-sifat dan cara memperoleh bilangan jumlah kuadrat.

Susunan Kegiatan Belajar

Modul 7 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Persamaan Diophantine Linier, dan Kegiatan Belajar 2 adalah Persamaan Diophantine Non Linier. Setiap kegiatan belajar memuat uraian, contoh/bukan contoh, tugas dan latihan, petunjuk jawaban tugas dan latihan, rangkuman, dan tes formatif. Pada bagian akhir Modul 7 ini dijelaskan Kunci Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah uraian dan contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi paparan.
2. Kerjakan tugas dan latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab/menyelesaikan, maka lihatlah petunjuk jawaban tugas dan latihan. Jika langkah ini belum banyak membantu Anda keluar dari kesulitan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan tes formatif secara mandiri, dan periksalah tingkat kemampuan Anda dengan jalan mencocokkan jawaban Anda dengan kunci jawaban tes formatif. Ulangilah pengerajan tes formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Persamaan Diophantine Linier**

 persoalan Persamaan Diophantine Linier berkaitan dengan mencari selesaian bulat dari persamaan-persamaan linier dengan dua atau lebih variabel. Sebagai awal pembahasan, marilah kita perhatikan dua peragaan berikut:

1. Terdapat sejumlah sepeda roda dua dan sejumlah becak roda tiga di suatu tempat parkir. Jika jumlah roda sepeda dan roda becak sama dengan 17, maka berapa banyaknya sepeda dan berapa banyaknya becak di tempat parkir itu?

Untuk menjawab persoalan di atas jelas bukan hal yang sulit karena permasalahannya dapat diganti dengan suatu model matematika persamaan linier dua variabel. Jika x menyatakan banyaknya sepeda, y menyatakan banyaknya becak, banyaknya roda setiap sepeda adalah dua, dan banyaknya roda setiap becak adalah tiga, maka seluruh roda sepeda adalah $2x$ dan seluruh roda becak adalah $3y$, sehingga dapat ditentukan model matematika persamaan linier yaitu:

$$2x + 3y = 17$$

Persamaan ini menuntut penyelesaian bulat karena banyaknya sepeda dan banyaknya becak tidak mungkin pecahan atau bilangan lain kecuali bulat. Dengan demikian persamaan ini adalah persamaan Diophantine linier. Secara sistematis selesaian dari persamaan ini dapat dicari dengan menggunakan tabel, atau mencoba-coba, sehingga diperoleh pasangan (x, y) sebagai selesaian persamaan linier, yaitu:

$$(1,5), (4,3), \text{ dan } (7,1)$$

2. Seseorang membeli suatu barang dengan harga 100 ribu rupiah. Jenis mata uang yang tersedia (di dalam dompet) adalah 5 ribuan, 10 ribuan, dan 20 ribuan. Berapa banyaknya lembar masing-masing jenis mata uang rupiah yang diperlukan untuk membayar barang itu?

Permasalahan di atas dapat dinyatakan dalam model matematika persamaan linier tiga variabel. Jika x menyatakan banyaknya lembar 5 ribuan, y menyatakan banyaknya lembar 10 ribuan, dan z menyatakan banyaknya lembar 20 ribuan, maka dapat ditentukan suatu model matematika persamaan linier tiga variabel:

$$5x + 10y + 20z = 100 \text{ atau } x + 2y + 4z = 20$$

Persamaan ini mempunyai selesaian berupa tripel bilangan (x, y, z) , yaitu $(20, 0, 0), (0, 10, 0), (0, 0, 5), (2, 1, 4), (2, 5, 2)$, dan $(6, 1, 3)$.

Dari dua peragaan di atas dapat dikatakan bahwa kenyataan menunjukkan adanya persoalan keseharian yang memang menuntut selesaian atau jawaban berupa bilangan bulat dan terkait dengan persamaan linier.

Apabila kita mempersyaratkan bahwa selesaian dari persamaan khusus adalah bilangan-bilangan bulat, maka kita sedang membicarakan **Persamaan Diophantine**. Persamaan Diophantine $ax + by = c$, dengan $a, b, c \in \mathbb{Z}$, disebut Persamaan Diophantine Linier Dua Variabel, dan Persamaan Diophantine $ax + by + cz = d$, dengan $a, b, c, d \in \mathbb{Z}$, disebut Persamaan Diophantine Linier Tiga Variabel.

Teorema 7.1

Ditentukan $a, b, c \in \mathbb{Z}$, dan $d = (a, b)$.

- a. jika d tidak membagi c , maka persamaan $ax + by = c$ tidak mempunyai selesaian;
- b. jika d membagi c , maka persamaan $ax + by = c$ mempunyai selesaian bulat yang tak hingga banyaknya, yaitu pasangan (x, y) di mana:

$$x = x_0 + \left(\frac{b}{d} \right) n \text{ dan } y = y_0 - \left(\frac{a}{d} \right) n, \text{ dengan } n \in \mathbb{Z} \text{ dan } (x_0, y_0) \text{ adalah suatu selesaian khusus.}$$

Bukti:

- a. Misalkan persamaan $ax + by = c$ mempunyai selesaian (x, y) dengan $x, y \in \mathbb{Z}$. Karena $d = (a, b)$, maka $d | a$ dan $d | b$, sehingga $d | ax$ dan $d | by$, akibatnya $d | ax + by$, atau $d | c$. Jadi jika d tidak membagi c , maka persamaan tidak mempunyai selesaian.
- b. Karena $d = (a, b)$, maka tentu ada bilangan-bilangan bulat x_1 dan y_1 sehingga $ax_1 + by_1 = d$. Selanjutnya, karena $d | c$, maka tentu ada bilangan bulat t sehingga $c = dt$. Dari $ax_1 + by_1 = d$ dapat ditentukan bahwa $atx_1 + bty_1 = dt$, berarti $atx_1 + bty_1 = c$, atau $a(tx_1) + b(ty_1) = c$. Dengan demikian satu selesaian persamaan adalah $x = x_0$ dan $y = y_0$

dengan $x_0 = tx_1$ dan $y_0 = ty_1$, berarti persamaan mempunyai selesaian jika $d|c$, dengan $ax_0 + by_0 = c$.

Untuk membuktikan bahwa terdapat tak hingga banyaknya selesaian, ambil $x = x_0 + \left(\frac{b}{d}\right)n$ dan $y = y_0 - \left(\frac{a}{d}\right)n$, dimana $n \in \mathbb{Z}$, kemudian harus ditunjukkan bahwa (x, y) adalah suatu selesaian. Substitusi x dan y ke dalam persamaan diperoleh:

$$ax + by = a\left\{x_0 + \left(\frac{b}{d}\right)n\right\} + b\left\{y_0 - \left(\frac{a}{d}\right)n\right\} = ax_0 + by_0 = c$$

Jadi terdapat tak hingga banyaknya selesaian:

$$x = x_0 + \left(\frac{b}{d}\right)n \text{ dan } y = y_0 - \left(\frac{a}{d}\right)n, \text{ dengan } n \in \mathbb{Z}.$$

Untuk membuktikan bahwa setiap selesaian mempunyai bentuk:

$x = x_0 + \left(\frac{b}{d}\right)n$ dan $y = y_0 - \left(\frac{a}{d}\right)n$, dengan $n \in \mathbb{Z}$, dimisalkan bahwa x dan y adalah bilangan-bilangan bulat yang memenuhi persamaan $ax + by = c$. Karena $ax_0 + by_0 = c$ dan $ax + by = c$, maka

$(ax + by) - (ax_0 + by_0) = 0$ atau $a(x - x_0) + b(y - y_0) = 0$ dan akibatnya dapat ditentukan bahwa

$$\left(\frac{a}{d}\right)(x - x_0) = \left(\frac{b}{d}\right)(y_0 - y), \text{ atau } \left(\frac{a}{d}\right)\left(\frac{b}{d}\right)(y_0 - y)$$

Karena $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, maka $\left(\frac{a}{d}\right)\left(\frac{b}{d}\right)| (y_0 - y)$, berarti ada $n \in \mathbb{Z}$, sehingga

$$(y_0 - y) = \left(\frac{a}{d}\right)n \text{ atau } y = y_0 - \left(\frac{a}{d}\right)n.$$

Substitusi $y = y_0 - \left(\frac{a}{d}\right)n$ pada $a(x - x_0) + b(y - y_0) = 0$ diperoleh

$$a(x - x_0) + b\left\{y_0 - \left(\frac{a}{d}\right)n - y_0\right\} = 0 \text{ atau } a(x - x_0) - b\left(\frac{a}{d}\right)n = 0$$

$$\text{atau } x = x_0 + \left(\frac{b}{d}\right)n.$$

Contoh 7.1

Selesaikan persamaan Diophantine Linier:

- $4x + 5y = 10$
- $9x + 12y = 21$

Jawab:

- $(4, 5) = 1 | 10$, maka persamaan mempunyai selesaian.

$(4, 5) = 1$, maka menurut Teorema 7.1, tentu ada $x_1, y_1 \in \mathbb{Z}$ sehingga $4x_1 + 5y_1 = 1$.

Karena $5 = 1 \cdot 4 + 1$, atau $(4)(-1) + (5)(1) = 1$, dan $4x_1 + 5y_1 = 1$, maka $x_1 = -1$ dan $y_1 = 1$, sehingga dari $(4)(-1) + (5)(1) = 1$ dapat ditentukan $10\{(4)(-1) + (5)(1)\} = 10 \cdot 1$.

Dengan demikian $4(-10) + 5(10) = 10$, berarti $x_0 = -10$ dan $y_0 = 10$.

Selesaian persamaan adalah (x, y) dengan $x = -10 + 5k$, $y = 10 - 4k$, dan $k \in \mathbb{Z}$.

- $(9, 12) = 3 | 21$, maka persamaan mempunyai selesaian.

$(9, 12) = 3$, maka menurut Teorema 7.1, tentu ada $x_1, y_1 \in \mathbb{Z}$ sehingga $9x_1 + 12y_1 = 3$, karena $12 = 1 \cdot 9 + 3$, atau $(9)(-1) + (12)(1) = 3$, dan $9x_1 + 12y_1 = 3$, maka $x_1 = -1$ dan $y_1 = 1$, sehingga dari $(9)(-1) + (12)(1) = 3$, dapat ditentukan $7\{(9)(-1) + (12)(1)\} = 7 \cdot 3$.

Dengan demikian $9(-7) + 12(7) = 21$, berarti $x_0 = -7$ dan $y_0 = 7$.

Selesaian persamaan adalah (x, y) dengan $x = -7 + 4k$ dan $y = 7 - 3k$, dan $k \in \mathbb{Z}$.

Cara yang dapat dipakai untuk menyelesaikan persamaan Diophantine Linier adalah cara biasa, cara reduksi, dan cara kongruensi. Marilah kita lihat masing-masing cara tersebut.

Cara biasa adalah cara yang biasa digunakan dan didasarkan pada Teorema Algoritma Euclides. Teorema 7.1 pada dasarnya memberi petunjuk memperoleh selesaian khusus melalui bentuk persamaan: $ax + by = (a, b)$ karena memang (a, b) selalu dapat dinyatakan dalam bentuk $ax + by$ dengan $x, y \in \mathbb{Z}$.

Sekarang akan kita pelajari bagaimana memperoleh selesaian $ax+by=c$ di mana $(a,b)|c$ dengan menggunakan Algoritma Euclides dan Teorema 2.21 berikut ini:

Teorema 2.21

Ditentukan $p, q \in N$. Maka $(p, q) = r_n p + l_n q, n = 0, 1, 2, \dots$, yang mana r_n dan k_n adalah suku ke n dari barisan-barisan yang secara rekursif didefinisikan sebagai:

$$\begin{aligned} r_0 &= 1, l_0 = 0 & \text{dan} & \quad r_i = r_{i-2} - k_{i-1} r_{i-1} \\ r_1 &= 0, l_1 = 1 & \quad l_i = l_{i-2} - k_{i-1} l_{i-1} \end{aligned}$$

untuk $i = 2, 3, \dots, n$ dengan k_i adalah hasil bagi dalam Algoritma Euclides memperoleh (p, q) .

Bukti:

Berdasarkan langkah-langkah Algoritma Euclides pada Teorema 2.20, dipilih $p = s_0$ dan $q = s_1$, kemudian kita gunakan cara pembuktian induksi matematika untuk membuktikan $(p, q) = s_n = r_n p + l_n q$

$$\text{untuk } i = 0, p = s_0 = 1.p + 0.q = r_0 p + l_0 q,$$

$$\text{untuk } i = 1, q = s_1 = 0.p + 1.q = r_1 + l_1 q$$

Sekarang, anggaplah bahwa:

$$s_i = r_i p + l_i q, i = 1, 2, \dots, n-1$$

Sesuai dengan keadaan langkah ke n dalam pembuktian Teorema 2.20 (Algoritma Euclides) dapat ditunjukkan bahwa:

$$s_{n-2} = s_{n-1} k_{n-1} + s_n \text{ atau } s_n = s_{n-2} - s_{n-1} k_{n-1}$$

Dengan demikian, sesuai dengan prinsip induksi matematika:

$$\begin{aligned} s_n &= s_{n-2} - s_{n-1} k_{n-1} \\ &= (r_{n-2} p + l_{n-2} q) - (r_{n-1} p + l_{n-1} q) k_{n-1} \\ &= (r_{n-2} - r_{n-1} k_{n-1}) p + (l_{n-2} - l_{n-1} k_{n-1}) q \\ &= (r_{n-2} - k_{n-1} r_{n-1}) p + (l_{n-2} - k_{n-1} l_{n-1}) q \\ s_n &= r_n p + l_n q \end{aligned}$$

Contoh 7.2

Selesaikan persamaan Diophantine Linier $221x + 91y = 1066$

Jawab:

$$221 = 91 \cdot 2 + 39, q_2 = 2$$

$$91 = 39 \cdot 2 + 13, q_3 = 2$$

$$39 = 13 \cdot 3, n = 3$$

Karena $(91, 221) = 13 | 1066$, maka persamaan tersebut dapat diselesaikan.

n	r	l	k
1	1	0	2
2	0	1	2
3	1	-2	
4	-2	5	

Dengan demikian $(-2)(221) + (91)(5) = -442 + 455 = 13 = (221, 91)$.

Karena $1066 = 82 \cdot 13$, maka $(82)(-2)(221) + (82)(5)(91) = 82 \cdot 13 = 1066$, sehingga dapat ditentukan bahwa $(221)(-164) + (91)(410) = 1066$, berarti $x_0 = -164$ dan $y_0 = 410$. Selesaian persamaan adalah (x, y) dengan $x = -164 + 7k$, $y = 410 - 17k$, $k \in \mathbb{Z}$.

Contoh 7.3

Selesaikan persamaan Diophantine Linier $2669x + 8517y = 85$

Jawab:

$$8517 = 3 \cdot 2669 + 51, k_1 = 3$$

$$2669 = 5 \cdot 510 + 119, k_2 = 5$$

$$510 = 4 \cdot 119 + 34, k_3 = 4$$

$$119 = 3 \cdot 34 + 17, k_4 = 3$$

$$34 = 2 \cdot 17 + 0$$

n	r	l	k
1	1	0	3
2	0	1	5
3	1	-3	4
4	-5	16	3
5	21	-67	
6	-68	217	

Karena $(2669, 8517) = 17|85$, maka persamaan tersebut mempunyai selesaian. Selesaian persamaan $2669x + 8517y = 17$ adalah (x, y) dengan $x = 217$ dan $y = -68$, sehingga salah satu selesaian $2669x + 8517y = 85 = 17 \cdot 5$ adalah $x_0 = 1085$ dan $y_0 = -340$. Selesaian persamaan tersebut adalah (x, y) dengan $x = 1085 + 501k, y = -340 - 157k, k \in \mathbb{Z}$.

Cara berikutnya bisa disebut sebagai metode reduksi, yaitu mereduksi koefisien (bukan mereduksi variabel) melalui pembagian berulang (serupa pembagian Algoritma), sehingga diperoleh suatu bentuk yang tanpa pecahan. Selanjutnya, dengan bekerja mundur, nilai-nilai selesaian akan diperoleh. Semua variabel yang digunakan, meskipun tanpa keterangan, bernilai bulat.

Contoh 7.4

Selesaikan persamaan Diophantine Linier $4x + 5y = 10$.

Jawab:

$4x + 5y = 10$, maka $4x = 10 - 5y$, sehingga:

$$x = \frac{10 - 5y}{4} = \frac{8 - 4y + 2 - y}{4} = \frac{8 - 4y}{4} + \frac{2 - y}{4} = (2 - y) + \frac{2 - y}{4}$$

Sekarang kita tentukan bahwa $t = \frac{2 - y}{4}$, atau $2 - y = 4t$, atau $y = 2 - 4t$,

sehingga:

$$x = (2 - y) + \frac{2 - y}{4} = (2 - y) + t = 2 - (2 - 4t) + t = 5t$$

Selesaian persamaan adalah (x, y) dengan $x = 0 + 5t, y = 2 - 4t$, dengan $t \in \mathbb{Z}$. Jika dibandingkan dengan selesaian 7.1 (a), maka hasil yang diperoleh nampak berbeda meskipun sesungguhnya adalah sama.

$$x = -10 + 5k = 5(-2 + k) = 5t \text{ dengan } t = -2 + k \text{ atau } k = t + 2$$

$$y = 10 - 4k = 10 - 4(t + 2) = 10 - 4t - 8 = 2 - 4t$$

Contoh 7.5

Selesaikan persamaan Diophantine Linier $x + 2y + 3z = 1$.

Jawab:

$x + 2y + 3z = 1$ maka $2y = -x - 3z + 1$, sehingga

$$y = \frac{-x - 3z + 1}{2} = \frac{-x - 2z - z + 1}{2}. \text{ Dengan demikian } y = -z + \frac{-x - z + 1}{2}.$$

Sekarang kita pilih $t = \frac{-x - z + 1}{2}$, maka $2t = -x - z + 1$,

atau $z = -x - 2t + 1$, sehingga $z = u$ dengan $u = -x - 2t + 1$

atau $x = 1 - u - 2t$, dan $y = -z + t$.

Selesaian persamaan tersebut adalah (x, y, z) dengan
 $x = 1 - u - 2t$, $y = -z + t$, dan $z = u$.

Untuk memeriksa kebenaran jawaban, kita perlu menentukan beberapa pasangan nilai u dan t , sehingga diperoleh nilai-nilai x , y , dan z . Berikutnya nilai $x + 2y + 3z$ dapat dihitung dan dicocokkan apakah hasil perhitungan sama dengan 1.

n	t	x	$2y$	$2z$	$x + 2y + 3z$
1	1	-2	0	3	1
2	1	-3	-2	6	1
2	3	-7	2	6	1
3	2	-6	-2	9	1

Dari tabel nilai di atas dapat diketahui bahwa beberapa tripel (x, y, z) yang merupakan selesaian persamaan adalah $(-2, 0, 1), (-3, -1, 2), (-7, 1, 2)$, dan $(-6, -1, 3)$.

Cara lain untuk menyelesaikan persamaan Diophantine Linier adalah cara kongruensi, yaitu suatu cara yang didasarkan pada penyelesaian kongruensi linier dan/atau sistem kongruensi linier. Meskipun hasil penyelesaian mungkin nampak berbeda, tetapi sebenarnya hasil itu adalah sama.

Contoh 7.6

Selesaikan persamaan Diophantine Linier $2x + 5y = 11$.

Jawab:

$2x + 5y = 11$, maka $5y = 11 - 2x$ berarti $5y \equiv 11 \pmod{2}$ atau $y \equiv 1 \pmod{2}$

Dengan demikian $y = 1 + 2t$ dengan $t \in \mathbb{Z}$, dan dari $2x + 5y = 11$, dapat diperoleh $2x = 11 - 5y = 11 - 5(1 + 2t) = 6 - 10t$, atau $x = 3 - 5t$.

Selesaian persamaan tersebut adalah (x, y) dengan $x = 3 - 5t$, $y = 1 + 2t$, yang mana $t \in \mathbb{Z}$.

Pemeriksaan kebenaran beberapa penyelesaian dapat ditentukan dengan menggunakan pilihan nilai-nilai t tertentu, sehingga diperoleh nilai-nilai x dan y yang terkait, dan nilai $2x + 3y$.

t	x	y	$2x$	$5y$	$2x + 3y$
0	3	1	6	5	11
1	-2	3	-4	15	11
2	-7	5	-14	25	11
3	-12	7	-24	35	11

Beberapa selesaian adalah $(3, 1), (-2, 3), (-7, 5), (-12, 7)$

Contoh 7.7

Selesaikan persamaan Diophantine Linier $17x + 13y = 21$.

Jawab:

$17x + 13y = 21$, maka $13y = 21 - 17x$, berarti $13y \equiv 21 \pmod{17}$ atau $13y \equiv 4 \pmod{17}$

$$13y \equiv 4 \pmod{17} \quad \rightarrow \quad y = \frac{17(12) + 4}{13} = 16$$

$$17x \equiv -4 \pmod{13}$$

$$4x \equiv 9 \pmod{13} \quad \rightarrow \quad x = \frac{13(3) + 9}{4} = 12$$

$$13t \equiv -9 \pmod{4}$$

$$t \equiv 3 \pmod{4} \quad \rightarrow \quad t = 3$$

Selesaian persamaan adalah (x, y) dengan $x = -11 - 13t$, $y = 16 + 17t$, dan $t \in \mathbb{Z}$.

Tugas:

Jika x dan y adalah bilangan-bilangan bulat, maka carilah semua selesaian

Persamaan Diophantine $\frac{1}{x} + \frac{1}{y} = \frac{1}{14}$.

Petunjuk Jawaban Tugas

Misalkan $\frac{1}{x} + \frac{1}{y} = \frac{1}{14}$, maka $14x + 14y = xy$, berarti

$xy - 14x - 14y + 196 = 196$, dengan demikian $(x-14)(y-14) = 196$, sehingga $(x-14)$ dan $(y-14)$ adalah pembagi-pembagi 196. Akibatnya nilai-nilai $(x-14)$ dan $(y-14)$ adalah pasangan-pasangan bilangan 1 dan 196, 2 dan 98, 4 dan 49, 7 dan 28, 14 dan 14, 28 dan 7, 49 dan 4, 98 dan 2, atau negatif dari pasangan-pasangan bilangan tersebut. Dengan demikian selesaian dari persamaan tersebut adalah $(x, y) = (15, 210), (16, 112), (18, 63), (21, 42), (28, 28), (42, 21), (63, 18), (112, 16), (210, 15), (13, -182), (12, -84), (10, -35), (7, -14), (-14, 7), (-35, 10), (-84, 12), (-182, 13)$.

**LATIHAN** _____

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Selesaikan Persamaan Diophantine $11x + 7y = 50$ dengan cara biasa.
- 2) Selesaikan Persamaan Diophantine $7x + 3y + 4z = 5$ dengan metode reduksi.
- 3) Selesaikan Persamaan Diophantine $2x + 3y + 7z = 15$ dengan metode reduksi.
- 4) Selesaikan Persamaan Diophantine $2x + 5y + 4z + 3w = 5$.
- 5) Selesaikan sistem Persamaan Diophantine Linier:

$$x + y + z = 100$$

$$x + 8y + 50z = 156$$

Petunjuk Jawaban Latihan

- Perhatikan bahwa $(11, 7) = 1 | 50$, maka persamaan dapat diselesaikan karena $(11, 7) = 1$, maka tentu ada $x_1, y_1 \in \mathbb{Z}$ sehingga $11x_1 + 7y_1 = 1$. Sesuai dengan Algoritma Euclides, dapat ditunjukkan bahwa:

$$11 = 1.7 + 4$$

$$7 = 1.4 + 3$$

$$4 = 1.3 + 1$$

$$3 = 3.1$$

$$\begin{aligned} \text{sehingga } 1 &= 4 - 1.3 = 4 - (7 - 1.4) = 2.4 - 1.7 = 2(11 - 1.7) - 1.7 \\ &= (11)(2) + (7)(-3) \end{aligned}$$

Karena $(11)(2) + (7)(-3) = 1$, maka $(11)(2)(50) + (7)(-3)(50) = 1.50$, atau $11(100) + 7(-150) = 50$, berarti $x_0 = 100$ dan $y_0 = -150$.

Selesaian persamaan tersebut adalah (x, y) dengan $x = 100 + 7r$ dan $y = -150 - 11r$, $r \in \mathbb{Z}$.

- 2) $7x + 3y + 4z = 5$, maka $3y = -7x - 4z + 5$ sehingga dapat ditentukan

$$\text{bahwa } y = \frac{-7x - 4z + 5}{3} = (-2x - z + 1) + \frac{-x - z + 2}{3}$$

$$\text{Ambil: } t = \frac{-x - z + 2}{3}, \text{ maka } 3t = -x - z + 2, \text{ atau } z = -x - 3t + 2$$

$$u = -x - 3t + 2, \text{ maka } x = -3t - u + 2, \text{ dan } z = u$$

$$\text{sehingga } y = -2x - z + 1 + t = -2(-3t - u + 2) - u + 1 + t = u + 7t - 3.$$

Selesaian persamaan tersebut adalah (x, y, z) dengan

$$x = -u - 3t + 2, y = u + 7t - 3, z = u, \text{ di mana } u, t \in \mathbb{Z}.$$

- 3) $2x + 3y + 7z = 15$, maka $3y + 7z \equiv 15 \pmod{2}$, atau $y + z \equiv 1 \pmod{2}$,

$$\text{sehingga } y \equiv (1 - z) \pmod{2}, \text{ dan untuk } z = t,$$

$$y = (1 - z) + 2u = (1 - t) + 2u = 2u - t + 1$$

$$2x + 3y + 7z = 15, \text{ maka}$$

$$2x = 15 - 3y - 7z = 15 - 6u + 3t - 3 - 7t = -6u - 4t + 12 \text{ atau}$$

$$x = -3u - 2t + 6.$$

Selesaian persamaan tersebut adalah (x, y, z) dengan:

$$x = -3u - 2t + 6, y = 2u - t + 1, z = t, \text{ di mana } u, t \in \mathbb{Z}.$$

- 4) Dari $2x + 5y + 4z + 3w = 5$ dapat diperoleh bahwa $2x + 3w = 5 - 5y - 4z$. Karena $(2,3) = 1$, maka 1 dapat dinyatakan sebagai kombinasi linier dari 2 dan 3, $2(-1) + 3(1) = 1$, sehingga $2\{-1(5 - 5y - 4z)\} + 3\{(5 - 5y - 4z)\} = 5 - 5y - 4z$.

Selesaian persamaan tersebut adalah

$$x = -5 + 5y + 4z + 3t, y = y, z = z, \text{ dan } w = 5 - 5y - 4z - 2t$$

- 5) Misalkan $x + y + z = 100$, maka $x = 100 - y - z$, sehingga: $(100 - y - z) + 8y + 50z = 156$ atau $7y + 49z = 56$ atau $y + 7z = 8$
Ambil $z = t$, maka $y = 8 - 7z = 8 - 7t$, dan
 $x = 100 - y - z = 100 - 8 + 7t - t$ atau $x = 92 + 6t$.
Selesaian persamaan adalah: $x = 92 + 6t$, $y = 8 - 7t$, dan $z = t$.



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang persamaan Diophantine Linier dua variabel dan tiga variabel, terutama tentang konsep persamaan Diophantine Linier yang menuntut selesaian bulat, dan cara atau metode menyelesaikan persamaan Diophantine Linier. Beberapa cara yang dapat digunakan untuk mencari selesaian persamaan Diophantine Linier adalah cara biasa, metode reduksi, dan cara kongruensi. Cara biasa melibatkan sifat-sifat keterbagian dan FPB, metode reduksi digunakan untuk mereduksi koefisien dengan pembagian berulang dan kerja mundur, dan cara kongruensi yang menggunakan sifat-sifat kongruensi linier.

- Pengertian persamaan Diophantine Linier yang merupakan persamaan linier tetapi ditetapkan dengan semesta pembicaraan adalah himpunan bilangan bulat.

2. Teorema 7.1

Ditentukan $a, b, c \in \mathbb{Z}$ dan $d = (a, b)$

- jika d tidak membagi c , maka persamaan $ax + by = c$ tidak mempunyai selesaian.
- jika d membagi c , maka persamaan $ax + by = c$ mempunyai selesaian bulat yang tak hingga banyaknya, yaitu pasangan (x, y) di mana:

$$x = x_0 + \left(\frac{b}{d} \right) n \text{ dan } y = y_0 - \left(\frac{a}{d} \right) n$$

dengan $n \in \mathbb{Z}$ dan (x_0, y_0) adalah suatu solusi khusus.

3. Penyelesaian persamaan dengan cara biasa, menggunakan sifat-sifat keterbagian dan FPB.
4. Penyelesaian persamaan dengan metode reduksi untuk mereduksi koefisien.
5. Penyelesaian persamaan dengan cara kongruensi, menggunakan sifat-sifat kongruensi linier.



TES FORMATIF 1

- 1) Skor 20
Selesaikan persamaan Diophantine Linier $67815x + 21480y = 120$.
- 2) Skor 20
Selesaikan persamaan Diophantine Linier $96577x + 67320y = 340$.
- 3) Skor 20
Selesaikan persamaan Diophantine Linier $8x - 5y + 7z = 21$.
- 4) Skor 20
Selesaikan persamaan Diophantine Linier $101x + 102y + 103z = 1$.
- 5) Skor 20
Selesaikan sistem persamaan Diophantine Linier:

$$\begin{aligned} x + y + z + w &= 100 \\ x + 2y + 3z + 4w &= 300 \\ x + 4y + 9z + 16w &= 1000 \end{aligned}$$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Persamaan Diophantine Non Linier**

Bilangan merupakan bagian dari kajian matematis tertua dan banyak menarik perhatian manusia sepanjang sejarah. Kajian bilangan dikatakan tertua karena keperluan membilang datang lebih awal dari keperluan bentuk atau bangun (*shape*) dalam geometri. Dalam pengertian yang sederhana, kajian bilangan merupakan pembahasan dari bilangan itu sendiri sebagai kreasi budaya manusia yang tumbuh dan berkembang selama ribuan tahun di berbagai belahan dunia.

Masyarakat banyak yang berpendapat bahwa bilangan diciptakan manusia karena kebutuhan mereka berkomunikasi dalam kehidupan sosial kemasyarakatan, yaitu untuk membilang, mengungkapkan perbandingan, mengadakan transaksi atau tukar-menukar barang, menghitung waktu, dan menandai hasil pengukuran, serta menggunakan untuk hal-hal yang kadang-kadang tidak rasional.

Kajian sistematis pertama tentang bilangan diduga merupakan kerja dari kelompok Pythagoras yang disebut Pythagoreans pada sekitar tahun 550 SM. Filsafat dari Pythagoreans adalah “bilangan mengatur alam semesta” (*number rules universe*), artinya mereka mempercayai adanya hubungan mistik atau magis antara bilangan dan realitas kehidupan (perhatikan adanya angka sial, angka keberuntungan, perhitungan bilangan untuk keperluan hajatan tertentu termasuk perkawinan dan pindah rumah), serta mempercayai bahwa masih banyak “rahasia” yang perlu dipelajari di balik keberadaan bilangan.

Salah satu hasil kajian bilangan dari Pythagoreans yang menonjol adalah mengaitkan tiga bilangan asli dengan panjang sisi-sisi suatu segitiga siku-siku yang disebut Teorema Pythagoras. Banyak cara telah dilakukan orang untuk membuktikan Teorema Pythagoras, antara lain secara analitis menggunakan analisis hubungan tertentu dan secara praktis dengan menggunakan luas daerah.

Teorema Pythagoras menyatakan bahwa jika suatu segitiga siku-siku mempunyai sisi miring z dan sisi-sisi yang lain adalah x dan y , maka hubungan antara x , y dan z adalah:

$$x^2 + y^2 = z^2$$

Sebaliknya, jika $x^2 + y^2 = z^2$, maka tentu dapat dibuat suatu segitiga siku-siku dengan sisi miring z dan sisi-sisi yang lain adalah x dan y .

Banyak tiga bilangan yang memenuhi hubungan $x^2 + y^2 = z^2$, bilangan-bilangan itu dapat berupa bilangan pecahan, bilangan desimal, bilangan irasional, atau bilangan bulat. Jika tiga bilangan bulat positif x , y , dan z memenuhi hubungan Teorema Pythagoras, yaitu $x^2 + y^2 = z^2$, maka tiga bilangan itu disebut **Triple Pythagoras**, dinyatakan dengan (x,y,z) .

Contoh 7.8

1. $(3,4,5)$ adalah suatu triple Pythagoras sebab $3^2 + 4^2 = 5^2$.
2. $(15,20,25)$ adalah suatu triple Pythagoras sebab $15^2 + 20^2 = 25^2$.
3. $(7,24,25)$ adalah suatu triple Pythagoras sebab $7^2 + 24^2 = 25^2$.
4. $\left(\frac{3}{7}, \frac{4}{7}, \frac{5}{7}\right)$ bukan suatu triple Pythagoras meskipun $\left(\frac{3}{7}\right)^2 + \left(\frac{4}{7}\right)^2 = \left(\frac{5}{7}\right)^2$
sebab $\frac{3}{7}$, $\frac{4}{7}$, dan $\frac{5}{7}$ bukan bilangan-bilangan bulat positif.

Persamaan $x^2 + y^2 = z^2$ merupakan persamaan kuadrat, bukan persamaan linier, dan memuat tiga variabel, dengan solusi bilangan bulat atau bilangan tidak bulat. Dengan demikian persamaan $x^2 + y^2 = z^2$ merupakan persamaan Diophantine non-linier jika semesta pembicaranya adalah himpunan bilangan bulat.

Definisi 7.1

Suatu triple Pythagoras (x,y,z) disebut primitif jika $(x,y,z) = 1$.

Contoh 7.9

Triple-triple Pythagoras $(3,4,5)$, $(5,12,13)$, $(8,15,17)$, dan $(9,40,41)$ adalah primitif.

Triple-triple Pythagoras $(6,4,9)$, $(15,36,39)$, dan $(24,45,51)$ adalah tidak primitif.

Misalkan (x_0, y_0, z_0) adalah suatu triple Pythagoras primitif maka $x_0^2 + y_0^2 = z_0^2$. Jika masing-masing bilangan dikalikan dengan k , maka

diperoleh kx_0, ky_0 , dan kz_0 , dan dapat ditentukan dari $x_0^2 + y_0^2 = z_0^2$ bahwa:

$$x_0^2 + y_0^2 = z_0^2$$

$$k^2(x_0^2 + y_0^2) = k^2 z_0^2, k^2 x_0^2 + k^2 y_0^2 = k^2 z_0^2$$

$$(kx_0)^2 + (ky_0)^2 = (kz_0)^2$$

Kedua ini menunjukkan bahwa (kx_0, ky_0, kz_0) adalah juga triple Pythagoras.

Misalkan (x,y,z) adalah suatu triple Pythagoras dan $(x,y,z) = d$, maka tentu ada bilangan-bilangan bulat x_1, y_1 , dan z_1 sehingga $x = dx_1, y = dy_1$, dan $z = dz_1$, dapat ditentukan bahwa $\frac{x}{d}, \frac{y}{d}, \frac{z}{d} \in \mathbb{Z}$, akibatnya $\frac{x^2}{d^2}, \frac{y^2}{d^2}, \frac{z^2}{d^2} \in \mathbb{Z}$.

Selanjutnya dari $x^2 + y^2 = z^2$ dapat ditentukan bahwa:

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \left(\frac{z}{d}\right)^2 \text{ atau } x_1^2 + y_1^2 = z_1^2.$$

Dengan demikian (x_1, y_1, z_1) adalah triple Pythagoras primitif, dan triple Pythagoras (x,y,z) merupakan kelipatan bulat dari triple Pythagoras primitif (x_1, y_1, z_1) .

Lemma 7.1

Jika (x,y,z) adalah suatu triple Pythagoras primitif, maka $(x,y) = (x,z) = (y,z) = 1$.

Bukti:

Misalkan (x,y,z) adalah suatu triple Pythagoras primitif dan $(x,y) > 1$, maka tentu (x,y) merupakan bilangan prima, atau (x,y) merupakan bilangan komposit yang dapat difaktorkan menjadi faktor-faktor prima, berarti jelas bahwa ada suatu bilangan prima p yang membagi (x,y) .

Misalkan $p|(x,y)$, maka $p|x$ dan $p|y$, sehingga $p|x^2$ dan $p|y^2$, akibatnya $p|x^2 + y^2$, berarti $p|z^2$ karena $x^2 + y^2 = z^2$.

Selanjutnya dari $p|z^2$ dapat ditentukan bahwa $p|z$ karena p adalah bilangan prima. Dengan demikian $p|x, p|y$, dan $p|z$, berarti $(x,y,z) \neq 1$, terjadi

pertentangan karena $(x, y, z) = 1$. Jadi $(x,y) = 1$, dan dengan jalan yang sama dapat ditunjukkan bahwa $(x,z) = (y,z) = 1$.

Lemma 7.2

Jika (x,y,z) adalah suatu triple Pythagoras primitif, maka x adalah genap dan y adalah ganjil, atau x adalah ganjil dan y adalah genap.

Bukti:

Misalkan (x, y, z) adalah suatu triple Pythagoras primitif, maka menurut Lemma 7.1 dapat ditentukan bahwa $(x,y) = 1$, sehingga tidak mungkin x dan y keduanya genap, dan tidak mungkin x dan y keduanya ganjil. Jika x dan y keduanya genap, misalkan x dan y keduanya genap, yaitu $x = 2s$ dan $y = 2t$, dengan $s, t \in \mathbb{Z}$, maka $(x,y) = (2s,2t) = 2(s,t) \neq 1$. Jika x dan y keduanya ganjil, maka ada tiga kemungkinan:

- a. jika $x \equiv 1 \pmod{4}$ dan $y \equiv 1 \pmod{4}$, maka $x^2 \equiv 1 \pmod{4}$ dan $y^2 \equiv 1 \pmod{4}$, sehingga $x^2 + y^2 \equiv 2 \pmod{4}$. Hal ini tidak mungkin karena tidak ada bilangan kuadrat yang mempunyai bentuk $2 \pmod{4}$.
- b. jika $x \equiv 1 \pmod{4}$ dan $y \equiv 3 \pmod{4}$, atau $x \equiv 3 \pmod{4}$ dan $y \equiv 1 \pmod{3}$, maka $x^2 \equiv 1 \pmod{4}$ dan $y^2 \equiv 1 \pmod{4}$, sehingga $x^2 + y^2 \equiv 2 \pmod{4}$. Hal ini tidak mungkin karena tidak ada bilangan kuadrat yang mempunyai bentuk $2 \pmod{4}$.
- c. jika $x \equiv 3 \pmod{4}$ dan $y \equiv 3 \pmod{4}$, maka $x^2 \equiv 1 \pmod{4}$ dan $y^2 \equiv 1 \pmod{4}$, sehingga $x^2 + y^2 \equiv 2 \pmod{4}$. Hal ini tidak mungkin karena tidak ada bilangan kuadrat yang mempunyai bentuk $2 \pmod{4}$.

Dengan demikian dapat ditentukan bahwa x adalah genap dan y adalah ganjil, atau x adalah ganjil dan y adalah genap.

Lemma 7.3

Jika r, s , dan t adalah bilangan-bilangan bulat positif sehingga $(r,s) = 1$ dan $rs = t^2$, maka tentu ada bilangan-bilangan bulat m dan n sehingga $r = m^2$ dan $s = n^2$.

Bukti:

Jika $r = 1$ dan $s = 1$, maka jelas bahwa $(r,s) = 1$, $rs = 1 = 1^2$, $r = 1 = 1^2$ dan $s = 1 = 1^2$ sehingga dapat ditentukan bahwa $r > 1$ dan $s > 1$. Misalkan pemfaktoran prima r dan s dapat dinyatakan dengan:

$$r = p_1^{i_1} p_2^{i_2} \dots p_g^{i_g}, \quad s = p_{g+1}^{i_{g+1}} p_{g+2}^{i_{g+2}} \dots p_h^{i_h}, \quad \text{dan} \quad t = q_1^{j_1} q_2^{j_2} \dots q_k^{j_k}$$

Bilangan-bilangan prima pada r dan s tentu berbeda karena $(r,s) = 1$.

Diketahui $rs = t^2$, maka dapat ditentukan bahwa:

$$p_1^{i_1} p_2^{i_2} \dots p_g^{i_g} \cdot p_{g+1}^{i_{g+1}} p_{g+2}^{i_{g+2}} \dots p_h^{i_h} = q_1^{2j_1} q_2^{2j_2} \dots q_k^{2j_k}$$

Sesuai dengan teorema dasar aritmetika, bilangan-bilangan prima ruas kiri dan ruas kanan persamaan adalah sama, sehingga untuk masing-masing p_a tentu ada q_b sehingga $i_a = 2j_b$. Akibatnya setiap i_a adalah genap, dan $(i_a/2)$ adalah suatu bilangan bulat. Dengan demikian $r = m^2$ dan $s = n^2$, di mana:

$$m = p_1^{i_1/2} p_2^{i_2/2} \dots p_g^{i_g/2} \quad \text{dan} \quad n = p_{g+1}^{i_{g+1}/2} p_{g+2}^{i_{g+2}/2} \dots p_h^{i_h/2}$$

Berdasarkan Lemma 7.3 di atas, kita akan membuktikan Teorema 7.1, suatu teorema yang dapat digunakan untuk membuat daftar semua triple Pythagoras primitif.

Teorema 7.2

Suatu triple (x, y, z) , dengan y adalah genap, adalah suatu triple Pythagoras primitif jika dan hanya jika ada dua bilangan bulat positif relatif prima m dan n , $m > n$, dengan m ganjil dan n genap, atau m genap dan n ganjil, sehingga $x = m^2 - n^2$, $y = 2mn$, dan $z = m^2 + n^2$.

Bukti:

Misalkan (x, y, z) adalah suatu triple Pythagoras primitif, maka sesuai dengan Lemma 7.2, x adalah ganjil dan y adalah genap, atau sebaliknya. Diketahui bahwa y adalah genap, maka x dan z adalah ganjil, akibatnya $z + x$ dan $z - x$ keduanya adalah genap, berarti ada bilangan-bilangan bulat positif r dan s dengan $r = (z + x)/2$ dan $s = (z - x)/2$.

Karena $x^2 + y^2 = z^2$, atau $y^2 = z^2 - x^2 = (z + x)(z - x)$, maka

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = rs, \text{ di mana } r = \frac{z+x}{2} \text{ dan } s = \frac{z-x}{2}, \text{ sehingga}$$

$$r+s = \frac{z+x}{2} + \frac{z-x}{2} = z \text{ dan } r-s = \frac{z+x}{2} - \frac{z-x}{2} = x$$

Dapat kita tunjukkan bahwa $(r,s)=1$. Misalkan $(r,s)=d$, maka $d|r$ dan $d|s$, sehingga $d|r+s$ dan $d|r-s$, atau $d|z$ dan $d|x$, akibatnya $d|(z,x)=1$, jadi $d=(r,s)=1$.

Sesuai dengan Lemma 7.3, terdapat bilangan-bilangan bulat positif m dan n sehingga $r=m^2$ dan $s=n^2$. Dengan demikian x, y , dan z dapat dinyatakan menjadi:

$$x = r - s = m^2 - n^2$$

$$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn$$

$$z = r + s = m^2 + n^2$$

Sebarang pembagi persekutuan m dan n juga membagi $x=m^2-n^2$, $y=2mn$, dan $z=m^2+n^2$, dan $(x,y,z)=1$. Demikian pula m dan n keduanya tidak ganjil sebab jika keduanya ganjil akan berakibat x, y , dan z semuanya genap sehingga $(x,y,z) \neq 1$, bertentangan dengan yang diketahui. Karena $(m,n)=1$, serta m dan n keduanya tidak ganjil, maka m adalah genap dan n adalah ganjil, atau sebaliknya.

Untuk menunjukkan bahwa setiap triple :

$x = m^2 - n^2$, $y = 2mn$, dan $z = m^2 + n^2$, dengan $m, n \in \mathbb{Z}^+$, $m > n$, $(m, n) = 1$, dan m tidak kongruen dengan $n \pmod{2}$ merupakan suatu triple Pythagoras primitif, kita tunjukkan bahwa $x^2 + y^2 = z^2$

$$x^2 + y^2 = (m^2 - n^2)^2 + (2mn)^2 = (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 = m^4 + 2m^2n^2 + n^4$$

$$= (m^2 + n^2)^2 = z^2$$

Untuk menunjukkan bahwa nilai-nilai x, y , dan z adalah saling relatif prima, anggaplah bahwa $(x, y, z) = d > 1$, maka tentu ada suatu bilangan prima p sehingga $p|d$ atau $p|(x, y, z)$. Nilai $p \neq 2$ karena x adalah ganjil (sebab $x = m^2 - n^2$ di mana m^2 dan n^2 mempunyai paritas yang berbeda, yaitu tidak keduanya ganjil atau tidak keduanya genap). Selanjutnya, dari $p|x$ dan $p|z$, dapat ditentukan bahwa $p|x+z=2m^2$ dan juga $p|x-z=2n^2$. Dengan

demikian $p \mid 2(m^2, n^2)$, akibatnya $p \mid (m, n)$, berarti $p \mid m$ dan $p \mid n$ atau bertentangan dengan $(m, n) = 1$, jadi $(x, y, z) = 1$, dan x, y, z adalah suatu triple Pythagoras primitif.

Contoh 7.10

Secara sistematis, kita dapat membuat daftar triple Pythagoras primitif dengan memilih harga-harga m dan n yang sesuai.

m	n	m^2	n^2	$2mn$	$x = m^2 - n^2$	$y = 2mn$	$z = m^2 + n^2$
2	1	4	1	4	3	4	5
3	2	9	4	12	5	12	13
4	1	16	1	8	15	8	17
4	3	16	9	24	7	24	25
5	2	25	4	20	21	20	29
5	4	25	16	40	9	40	41
6	1	36	1	12	35	12	37
6	5	36	25	60	9	60	61
7	6	49	36	84	13	84	85
7	4	49	16	56	33	56	65
7	2	49	4	28	45	28	53
8	1	64	1	16	63	16	65
8	3	64	9	48	55	48	73
8	5	64	25	80	39	80	89
8	7	64	49	112	15	112	113

Contoh 7.11

Carilah semua triple Pythagoras primitif x, y, z yang mana selisih antara z^2 dengan salah satu dari x^2 atau y^2 adalah t .

Jawab:

Misalkan x, y, z adalah suatu triple Pythagoras, maka ada dua kemungkinan, yaitu t adalah ganjil atau t adalah genap. Ambil z adalah ganjil dan y adalah genap (x dengan sendirinya ganjil)

- (a) jika t adalah ganjil, maka t merupakan selisih z^2 yang ganjil dan y^2 yang genap, sehingga $z^2 - y^2 = t$, berarti $m^2 + n^2 - 2mn = t$, atau

$(m - n)^2 = t$. Jika $k = m - n$, maka $t = k^2$ dan $m = n + k$. Selesaian persamaan Diophantine $x^2 + y^2 = z^2$ adalah:

$$x = (n+k)^2 - n^2 = k(2n+k), \quad y = 2(n+k)n = 2n(n+k), \quad \text{dan}$$

$$z = (n+k)^2 + n^2 = 2n^2 + 2nk + k^2$$

Sebagai peragaan untuk $t = 9$, maka $k = 3$, sehingga $x = 3(2n+3)$, $y = 2n(n+3)$ dan $z = 2n^2 + 6n + 9$, sebagai contoh $(15,8,17)$, $(21,20,29)$, dan $(27,36,45)$.

- (b) jika t adalah genap, maka t merupakan selisih z^2 yang ganjil dan x^2 yang ganjil, sehingga $z^2 - x^2 = t$, berarti $m^2 + n^2 - m^2 + n^2 = t$, atau $2n^2 = t$. Jika $t = 2k^2$, maka $2n^2 = 2k^2$, sehingga $n = k$. Selesaian persamaan Diophantine $x^2 + y^2 = z^2$ adalah:

$$x = m^2 - n^2 = m^2 - k^2, \quad y = 2mn = 2mk, \quad \text{dan} \quad z = m^2 + n^2 = m^2 + k^2$$

Sebagai peragaan, untuk $t = 8$, maka $k = 2$, sehingga $x = m^2 - 4$, $y = 4m$, dan $z = m^2 + 4$, sebagai contoh $(5,12,13)$, $(21,20,29)$, dan $(45,28,43)$.

Teorema 7.3

Jika $x, y, z \in N$ dan $(x, y, z) = 1$, maka persamaan Diophantine $x^2 + 2y^2 = z^2$ mempunyai selesaian: $x = |r^2 - 2s|^2$, $y = 2rs$, dan $z = r^2 + 2s^2$ di mana $r, s > 0$ dan $(r, 2s) = 1$.

Bukti:

Ambil x ganjil, y genap, $y = 2m$, dan z ganjil, maka dari $x^2 + 2y^2 = z^2$ dapat ditentukan bahwa $x^2 + 2(2m)^2 = z^2$, atau

$$2m^2 = (z^2 - x^2)/4 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right). \quad \text{Karena } \left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1, \quad \text{maka sesuai}$$

dengan sifat ketunggalan pemfaktoran, dapat ditentukan bahwa $r^2 = \frac{z+x}{2}$

dan $2s^2 = \frac{z-x}{2}$ atau $2r^2 = \frac{z+x}{2}$ dan $s^2 = \frac{z-x}{2}$ dengan

$(r, 2s) = 1$ atau $(2r, s) = 1$. Selanjutnya, ambil $r^2 = \frac{z+x}{2}$ dan $2s^2 = \frac{z-x}{2}$,

maka dapat dicari $z + x = 2r^2$ dan $z - x = 4s^2$, serta $2z = 2r^2 + 4s^2$ atau $z = r^2 + 2s^2$, dan $2x = 2r^2 - 4s^2$ atau $x = r^2 - 2s^2$. Demikian pula $2m^2 = (r^2)(2s^2)$ atau $m = rs$, dan $y = 2m = 2rs$.

Contoh 7.12

Sebagai fakta bahwa $x^2 + 2y^2 = z^2$ mempunyai selesaian, ambil beberapa nilai r dan s yang memenuhi $(r, 2s) = 1$ atau $(2r, s) = 1$.

r	s	$x = r^2 - 2s^2 $	$y = 2rs$	$z = r^2 + 2s^2$
3	1	7	6	11
1	3	17	6	19
2	3	14	12	22

Sepanjang sejarah, banyak matematisi yang tertarik tentang perwujudan bilangan bulat sebagai jumlah kuadrat dua bilangan atau lebih, disebut **bilangan jumlah kuadrat (BJK)**. Permasalahan di dalam BJK adalah mencari bilangan-bilangan bulat n yang dapat dinyatakan sebagai jumlah kuadrat dua bilangan atau lebih. Jika kita mengambil jumlah dua bilangan, maka permasalahan BJK adalah mencari bilangan bulat n sehingga:

$$n = x^2 + y^2, \text{ dengan } x \text{ dan } y \text{ adalah bilangan-bilangan bulat.}$$

Beberapa matematisi yang memberikan sumbangan berharga tentang BJK antara lain adalah Diophantus, Euler, Fermat, dan Lagrange (Rossen, K.: 447).

Sesuai dengan Teorema Algoritma Pembagian, setiap bilangan bulat dapat dinyatakan sebagai $x = 4k$ atau $x \equiv 0 \pmod{4}$, $x = 4k + 1$ atau $x \equiv 1 \pmod{4}$, $x = 4k + 2$ atau $x \equiv 0 \pmod{4}$, $x = 4k + 3$ atau $x \equiv 3 \pmod{4}$, sehingga kuadrat dari masing-masing kemungkinan nilai x adalah $x^2 \equiv 0, 1, 4, 9 \pmod{4} = 0, 1 \pmod{4}$. Ini berarti bahwa 0 dan 1 merupakan residu-residu kuadratis modulo 4, sedangkan 2 dan 3 bukan merupakan residu-residu kuadratis modulo 4.

Sekarang, jika diambil dua bilangan kuadrat x^2 dan y^2 , maka kemungkinan jumlahnya adalah $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$. Dari keadaan di atas jelas bahwa:

Jika $x^2 + y^2 \equiv k \pmod{4}$, maka kemungkinan nilai k adalah $k \equiv 0, 1, 2 \pmod{4}$, dan tidak mungkin k kongruen dengan 3 modulo 4.

Marilah sekarang kita selidiki keadaan $k \equiv 0, 1, 2 \pmod{4}$ dalam pembahasan BJK.

Jika $k = 0$, maka $x^2 + y^2 \equiv 0 \pmod{4}$, dan solusi kongruensi adalah $x = 0$ dan $y = 0$. Bagaimana dengan nilai-nilai $k = 4, 8, 12, 16, \dots \equiv 0, 0, 0, 0, \dots \pmod{4}$? Bagaimana jika $k = 1$ atau $k = 2$, dan $k = 1, 5, 9, \dots \equiv 1 \pmod{4}$ atau $k = 2, 6, 10, \dots \equiv 2 \pmod{4}$?

Misalkan kita mencoba untuk menjawab pertanyaan-pertanyaan di atas dengan mencari pola BJK dengan menggunakan daftar atau tabel sistematis berikut.

n	Bentuk Jumlah Kuadrat	n	Bentuk Jumlah Kuadrat		
1.	$4k + 1$	$0^2 + 1^2$	16.	$4k$	$0^2 + 4^2$
2.	$4k + 2$	$1^2 + 1^2$	17.	$4k + 1$	$1^2 + 4^2$
3.	$4k + 3$	---	18.	$4k + 2$	$3^2 + 3^2$
4.	$4k + 0$	$0^2 + 2^2$	19.	$4k + 3$	---
5.	$4k + 1$	$1^2 + 2^2$	20.	$4k$	$2^2 + 4^2$
6.	$4k + 2$	---	21.	$4k + 1$	---
7.	$4k + 3$	---	22.	$4k + 2$	---
8.	$4k + 0$	$2^2 + 2^2$	23.	$4k + 3$	---
9.	$4k + 1$	$0^2 + 3^2$	24.	$4k$	---
10.	$4k + 2$	$1^2 + 3^2$	25.	$4k + 1$	$3^2 + 4^2$
11.	$4k + 3$	---	26.	$4k + 2$	$1^2 + 5^2$
12.	$4k + 0$	---	27.	$4k + 3$	---
13.	$4k + 1$	$2^2 + 3^2$	28.	$4k$	---
14.	$4k + 2$	---	29.	$4k + 1$	$2^2 + 5^2$
15.	$4k + 3$	---	30.	$4k + 2$	---

Dari daftar di atas dapat kita ketahui bahwa pola bilangan (*number pattern*) yang kita cari belum nampak, sehingga kita perlu mencari cara lain, misalnya menggunakan pemfaktoran prima.

Teorema 7.4

Jika r dan s adalah bilangan-bilangan jumlah kuadrat, maka rs juga merupakan BJK.

Bukti:

Diketahui bahwa r adalah BJK dan s adalah juga BJK, berarti r dan s dapat dinyatakan sebagai $r = a^2 + b^2$ dan $s = c^2 + d^2$, sehingga:

$$\begin{aligned} rs &= (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (a^2c^2 + b^2d^2) + (a^2d^2 + b^2c^2) \\ &= (a^2c^2 + 2abcd + b^2d^2) + (a^2d^2 - 2abcd + b^2c^2) \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

Jadi rs merupakan BJK.

Contoh 7.13

Perhatikan bahwa 4, 5, 8, 9 dan 10 adalah BJK - BJK, dan:

$$\begin{array}{lll} 4.5 = 20 = 2^2 + 4^2 & 5.9 = 45 = 3^2 + 6^2 & 4.4 = 16 = 0^2 + 4^2 \\ 5.8 = 40 = 2^2 + 6^2 & 8.9 = 72 = 6^2 + 6^2 & 9.10 = 90 = 3^2 + 9^2 \\ 8.10 = 80 = 4^2 + 8^2 & 9.9 = 81 = 0^2 + 9^2 & 5.10 = 50 = 1^2 + 7^2 \end{array}$$

Teorema 7.5

Jika p adalah suatu bilangan prima ganjil yang mempunyai bentuk $4k + 1$, maka tentu ada $m, n \in \mathbb{Z}$ sehingga $m^2 + n^2 = tp$ dengan $t \in \mathbb{Z}^+$ dan $t < p$.

Bukti:

Berdasarkan Teorema 5.5 dalam pembahasan residu kuadratis, dapat ditunjukkan bahwa $x^2 \equiv -1 \pmod{p}$ mempunyai selesaian jika $p \equiv 1 \pmod{4}$ atau $p = 4k + 1$ dengan $x < p$.

Dengan demikian $x^2 + 1 \equiv 0 \pmod{p}$, akibatnya $p|x^2 + 1$ atau $x^2 + 1^2 = tp$.

Jika dipilih $m = x$ dan $n = 1$, maka ada $m, n \in \mathbb{Z}$ sehingga $m^2 + n^2 = tp$

Berikutnya akan ditunjukkan bahwa $t < p$. Karena $m^2 + n^2 = tp$ di mana $m = x$ dan $n = 1$, maka $tp = m^2 + n^2 = x^2 + 1 < (p-1)^2 + 1 < p^2$, atau $tp < p^2$, berarti $t < p$.

Contoh 7.14

- a. 5 adalah bilangan prima yang mempunyai bentuk $4k + 1$, maka $2^2 + 4^2 = 4.5$

- b. 13 adalah bilangan prima yang mempunyai bentuk $4k+1$, maka $1^2 + 5^2 = 2.13$
c. 29 adalah bilangan prima yang mempunyai bentuk $4k+1$, maka $3^2 + 7^2 = 2.29$

Teorema 7.6

Jika p adalah suatu bilangan prima, dan p tidak kongruen dengan 3 modulo 4, maka tentu ada $m, n \in \mathbb{Z}$ sehingga $m^2 + n^2 = p$, yaitu p merupakan BJK.

Bukti:

Karena p tidak kongruen dengan 3 modulo 4, maka $p \equiv 2 \pmod{4}$ atau $p \equiv 1 \pmod{4}$. Jika $p = 2$, maka dapat ditentukan bahwa $p = 1+1 = 1^2 + 1^2$ berarti p merupakan BJK. Jika $p \equiv 1 \pmod{4}$ maka sesuai Teorema 7.4, ada bilangan bulat positif terkecil $t < p$ sehingga $m^2 + n^2 = tp$ mempunyai selesaian $m, n \in \mathbb{Z}$. Dengan demikian harus ditunjukkan bahwa $t = 1$.

Anggaplah bahwa $t > 1$, kemudian ambil dua bilangan bulat r dan s sehingga $r \equiv m \pmod{t}$ dan $s \equiv n \pmod{t}$, dengan $(-t/2) < r, s < (t/2)$. Maka dapat diperoleh $r^2 \equiv m^2 \pmod{t}$ dan $s^2 \equiv n^2 \pmod{t}$. Akibatnya, $r^2 + s^2 \equiv m^2 + n^2 \pmod{t}$ sehingga $tp \equiv 0 \pmod{t} \equiv t(r^2 + s^2) \pmod{t}$, berarti $r^2 + s^2 = tq$, dan $(m^2 + n^2)(r^2 + s^2) = tp \cdot tq = t^2 pq$. Selanjutnya, dari $r \equiv m \pmod{t}$ dapat ditunjukkan $mr \equiv m^2 \pmod{t}$ dan $nr \equiv mn \pmod{t}$, dan dari $s \equiv n \pmod{t}$ dapat ditunjukkan $ns \equiv n^2 \pmod{t}$ dan $ms \equiv mn \pmod{t}$.

Akibatnya, $mr + ns \equiv m^2 + n^2 \pmod{t} = 0 \pmod{t}$, $ms - nr \equiv 0 \pmod{t}$, $(mr + ns)/t$ dan $(ms - nr)/t$ merupakan bilangan-bilangan bulat. Dengan demikian, dari $(m^2 + n^2)(r^2 + s^2) = t^2 pq$, dapat ditunjukkan:

$$\left(\frac{mr + ns}{t}\right)^2 + \left(\frac{ms - nr}{t}\right)^2 = \frac{t^2 pq}{t^2} = pq$$

Berarti pq merupakan BJK. Dari $r^2 + s^2 = tq$ dengan $(-t/2) < r, s < (t/2)$ dapat ditunjukkan bahwa $q < t$.

$r^2 + s^2 = tq \geq 0$ dan $r^2 + s^2 \leq \{(t^2/4) + (t^2/4)\} = t^2/2$, maka $0 \leq (r^2 + s^2) \leq t^2/2$ atau $0 \leq tq \leq (t^2/2)$, atau $0 \leq q \leq t/2$, sehingga $q < t$.

Hal ini tidak mungkin terjadi sebab t adalah suatu bilangan bulat positif terkecil sehingga $m^2 + n^2 = tp$ mempunyai solusi $m, n \in \mathbb{Z}$, yang mana:

$$m^2 + n^2 \equiv r^2 + s^2 = tp \equiv 0 \pmod{t} \text{ dan } q < t \text{ memenuhi}$$

$$r^2 + s^2 = tq \equiv m^2 + n^2 \pmod{t}.$$

Jadi t tidak lebih dari 1.

Berikutnya akan ditunjukkan bahwa untuk $q = 0$ diperoleh nilai $t = 1$

Jika $q = 0$, maka $r^2 + s^2 = tq = 0$, sehingga $r = s = 0$ dan $m^2 + n^2 \equiv r^2 + s^2 \equiv 0 \pmod{t}$ atau $m \equiv n \equiv 0 \pmod{t}$, jadi $t|m$ dan $t|n$, $t^2|m^2$ dan $t^2|n^2$, $t^2|m^2 + n^2$, $t^2|tp$, $t|p$, $t < p$, $t|p$ dan p adalah bilangan prima, maka $t = 1$.

Dengan demikian $m^2 + n^2 = p$. Hal ini berarti p merupakan BJK.

Contoh 7.15

- a. $p = 13$, maka $13 = 2^2 + 9^2$
- b. $p = 17$, maka $17 = 1^2 + 4^2$
- c. $p = 29$, maka $29 = 2^2 + 5^2$
- d. $p = 53$, maka $53 = 2^2 + 7^2$

Teorema 7.7

Suatu bilangan bulat positif n adalah BJK jika dan hanya jika faktor-faktor prima dalam pemfaktoran prima n yang mempunyai bentuk $3 \pmod{4}$, mempunyai pangkat yang genap.

Bukti:

Misalkan dalam pemfaktoran prima dari n tidak ada faktor dalam bentuk $3 \pmod{4}$ yang berpangkat ganjil, yaitu $n = t^2 u$ dengan u memuat perkalian prima yang berbeda. Maka $p \equiv 3 \pmod{4}$ bukan faktor u karena masing-masing bilangan prima berpangkat ganjil 1.

Akibatnya, masing-masing faktor prima dari u mempunyai bentuk $1 \pmod{4}$, berarti faktor-faktor prima itu merupakan BJK. Dengan demikian u adalah BJK karena u merupakan hasil kali BJK, misalkan $u = x^2 + y^2$, dan n adalah juga BJK karena $n = t^2 u = t^2(x^2 + y^2) = t^2 x^2 + t^2 y^2$ maka $n = (tx)^2 + (ty)^2$.

Misalkan n merupakan BJK, yaitu $n = x^2 + y^2$, dan ada bilangan prima $p \equiv 3(\text{mod } 4)$ yang adalah faktor n berpangkat ganjil $(2i+1)$, dan ditentukan $d = (x, y)$, $m = (n/d^2)$, $a = x/d$, dan $b = y/d$, maka

$(a, b) = (x/d, y/d) = 1$ dan $a^2 + b^2 = (x/d)^2 + (y/d)^2 = (x^2 + y^2)/d^2 = n/d^2$ atau $a^2 + b^2 = m$. Jika p^k adalah pangkat tertinggi dari p yang membagi d , maka m habis dibagi oleh $p^{2i+1-2k}$ dengan $(2i+1-2k) \geq 1$, sehingga $p|m$. Selanjutnya, p tidak membagi a , sebab jika $p|a$, $b^2 = m - a^2$, dan $(a, b) = 1$, maka $p|b$.

Jadi ada bilangan bulat z sehingga $az \equiv b(\text{mod } p)$, dan:

$$a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1+z^2) \equiv a^2(1+z^2)(\text{mod } p)$$

Karena $a^2 + b^2 = m$ dan $p|m$, maka $a^2(1+z^2) \equiv 0(\text{mod } p)$.

Karena $(a, p) = 1$, maka $1+z^2 \equiv 0(\text{mod } p)$ atau $z^2 \equiv -1(\text{mod } p)$, dan hal ini tidak mungkin terjadi sebab -1 bukan residu kuadratis dari $p \equiv 3(\text{mod } 4)$.

Jadi n bukan merupakan BJK jika $p \equiv 3(\text{mod } 4)$ merupakan faktor n berpangkat ganjil.

Contoh 7.16

- (a) $n = 6125 = 5^3 7^2$, maka $n = 70^2 + 35^2$
- (b) $n = 3887 = 13^2 \cdot 23^1$, maka n bukan BJK sebab $23 \equiv 3(\text{mod } 4)$ dan 23 berpangkat ganjil
- (c) $13 \equiv 1(\text{mod } 4)$ dan $29 \equiv 1(\text{mod } 4)$, maka $13 = 2^2 + 3^2$ dan $29 = 2^2 + 5^2$, berarti 13 dan 29 adalah BJK, akibatnya $377 = 13 \cdot 29$ merupakan perkalian dua BJK, sehingga menurut Teorema 7.3, 377 merupakan perkalian dua BJK, dan akibatnya 377 juga merupakan BJK, kenyataannya $377 = 4^2 + 19^2$.

Teorema 7.8

Jika r dan s adalah bilangan-bilangan bulat positif dan masing-masing merupakan bilangan jumlah empat kuadrat, maka rs juga merupakan bilangan jumlah empat kuadrat.

Bukti:

Misalkan $r = a^2 + b^2 + c^2 + d^2$ dan $s = e^2 + f^2 + g^2 + h^2$, maka dapat ditentukan:

$$\begin{aligned} rs &= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \\ &= (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 + (ag - bh - ce + df)^2 \\ &\quad + (ah + bg - cf - de)^2 \end{aligned}$$

Contoh 7.17

$$7 = 1^2 + 1^2 + 1^2 + 2^2 \text{ dan } 15 = 1^2 + 1^2 + 2^2 + 3^2$$

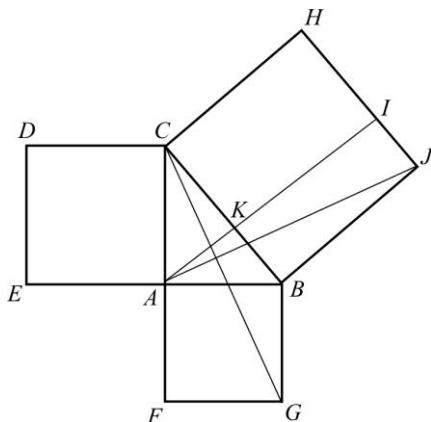
105 = 7.15 merupakan perkalian dua bilangan jumlah empat kuadrat, maka 105 juga merupakan suatu bilangan jumlah empat kuadrat, yaitu $105 = 0^2 + 1^2 + 2^2 + 10^2$.

Tugas

- 1) Bacalah suatu buku yang memuat Teorema Pythagoras, kemudian tunjukkan paling sedikit satu bukti tentang Teorema Pythagoras.
- 2) Buktikan: jika x dan y adalah panjang kaki-kaki suatu segitiga siku-siku, dan z adalah panjang sisi miring, maka tentu ada bilangan-bilangan $s, t \in R$, $s \geq t$ sehingga $x = s - t$, $y = 2\sqrt{st}$, dan $z = s + t$.
- 3) Tunjukkan bahwa dua hipotesis berikut tidak benar, dengan cara mencari contoh yang benar, dan mencari contoh yang salah.
 - (a) Jika ada suatu triple dengan unsur terkecil n , unsur genap $(n^2 - 1)/2$, dan unsur terbesar $(n^2 + 1)/2$, maka triple ini adalah triple Pythagoras.
 - (b) Jika ada suatu triple dengan unsur terkecil $2n$, unsur-unsur berikutnya $(n^2 - 1)$ dan $(n^2 + 1)$, maka triple ini adalah triple Pythagoras.

Petunjuk Jawaban Tugas

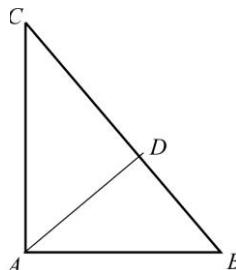
- 1) (a) Segitiga ABC siku-siku di A , dan AK garis tinggi



Ambil $|AB| = x$, $|AC| = y$, dan $|BC| = z$

Dapat ditunjukkan bahwa luas $BJIK = \text{luas } ABGF = 2 \times \text{luas } ABJ$ dan luas $KIHC = \text{luas } ACDE = 2 \times \text{luas } CBG$.

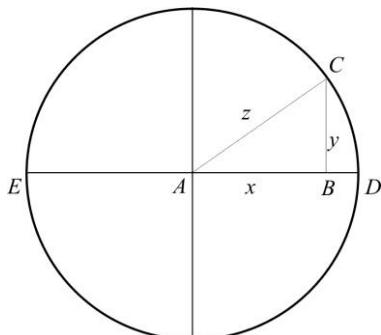
(b)



Segitiga ABC siku-siku di A , dan AD garis tinggi. Ambil $|AB| = x$, $|AC| = y$, dan $|BC| = z$

Gunakan kesebangunan segitiga ABC , segitiga DBA dan segitiga DAC untuk membuktikan teorema Pythagoras berdasarkan perbandingan senilai.

2)



Buat gambar seperti di samping.
Tentukan $|EB| = 2s$ dan $|BD| = 2t$,
maka $s \geq t$ dan:

$$\begin{aligned} |ED| &= |EB| + |BD| = 2s + 2t \\ |EA| &= |AD| = |AC| = (\frac{1}{2})|EB| \\ &= (\frac{1}{2})(2s + 2t) = s + t = y \\ |AB| &= |EB| - |EA| = 2s - (s + t) \\ &= s - t = x. \end{aligned}$$

$$\begin{aligned} |BD| - |AD| - |AB| &= (s+t) - (s-t) = 2t \\ |BC|^2 &= |AC|^2 - |AB|^2 = (s+t)^2 - (s-t)^2 = 4st, BC = 2\sqrt{st} = y. \end{aligned}$$

- 3) (a) $\left(\frac{n^2+1}{2}\right)^2 = n^2 + \left(\frac{n^2-1}{2}\right)^2$ benar untuk beberapa triple $(3,4,5)$, $(5,12,13)$, $(7,24,25)$, $(9,40,41)$ dan $(11,60,61)$, tetapi tidak benar untuk suatu triple $(8,15,17)$.
- (b) $(n^2+1)^2 = (2n)^2 + (n^2-1)^2$ benar untuk beberapa triple $(4,3,5)$, $(6,8,10)$, $(8,15,17)$.
Tetapi tidak benar untuk triple-triple $(72,65,97)$, $(120,119,169)$ dan $(240,161,289)$.



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Sebutkan semua triple Pythagoras primitif (x, y, z) jika $x < 30$.
- 2) Jika (x, y, z) adalah suatu triple Pythagoras primitif, maka tunjukkan bahwa x atau y habis dibagi oleh 3.
- 3) Jika (x, y, z) adalah suatu triple Pythagoras primitif, maka tunjukkan bahwa tepat satu dari x , y , atau z habis dibagi 5.
- 4) Jika $x_1 = 3$, $y_1 = 4$, dan $z_1 = 5$, dan x_n , y_n , z_n untuk $n = 2, 3, 4, \dots$ didefinisikan secara rekursif dengan:

$$x_{n+1} = 3x_n + 2z_n + 1$$

$$y_{n+1} = 3x_n + 2z_n + 2$$

$$z_{n+1} = 4x_n + 3z_n + 2$$

Tunjukkan bahwa x_n , y_n , z_n adalah suatu triple Pythagoras primitif.

- 5) Selesaikan persamaan Diophantine $x^2 + y^2 = z^4$.

Petunjuk Jawaban Latihan

- 1) $(3,4,5), (5,12,13), (7,24,25), (8,15,17), (9,40,41), (11,60,61), (12,35,37), (13,84,85), (15,112,113), (16,63,65), (17,144,145), (19,180,181), (20,21,29), (20,99,101), (23,264,265), (24,143,145), (25,312,313), (27,364,365), (28,45,53), (28,195,197), (29,420,421).$
- 2) Jika 3 tidak membagi x atau 3 tidak membagi y , maka $x, y \equiv 1, 2 \pmod{3}$, berarti $x^2, y^2 \equiv 1, 4 \pmod{3} \equiv 1, 4 \pmod{3}$, akibatnya $z^2 \equiv 1+1 \pmod{3} \equiv 2 \pmod{3}$, hal ini tidak mungkin sebab kongruensi $z^2 \equiv 2 \pmod{3}$ tidak mempunyai solusi.
- 3) Sesuai dengan Lemma 7.1, $(x, y) = (x, z) = (y, z)$, sehingga 5 membagi paling banyak satu dari x, y , atau z . Jika 5 tidak membagi x atau 5 tidak membagi y , maka dapat ditentukan $x, y \equiv 1, 2, 3, 4 \pmod{5}$, berarti $x^2, y^2 \equiv 1, 4, 1, 1 \pmod{5} \equiv 1, 4 \pmod{5}$. Akibatnya $z^2 \equiv 0, 2, 3 \pmod{5}$. Karena 2 dan 3 bukan residu kuadratis modulo 5, maka dapat ditentukan $z \equiv 0 \pmod{5}$, berarti $5|z$. Dengan demikian 5 membagi paling banyak satu dari x, y , atau z .
- 4) Dibuktikan dengan menggunakan induksi matematika.
Hubungan berlaku untuk $n=1$ sebab $x_1 = 3, y_1 = 4, z_1 = 5$ dan $x_1^2 + y_1^2 = 9 + 16 = 25 = 5^2 = z_1^2$, berarti (x_1, y_1, z_1) adalah suatu Triple Pythagoras. Misalkan hubungan berlaku untuk $n=k$, artinya (x_k, y_k, z_k) adalah suatu Triple Pythagoras. Harus dibuktikan hubungan berlaku untuk $n=k+1$

$$\begin{aligned} x_{n+1}^2 + y_{n+1}^2 &= (3x_n + 2z_n + 1)^2 + (3x_n + 2z_n + 2)^2 \\ &= 18x_n^2 + 8z_n^2 + 5 + 24x_n y_n + 16x_n + 12z_n + 4 \\ &\quad + (2x_n^2 - z_n^2 + 2x_n + 1) \\ &= z_{n+1}^2 + \{x_n^2 + 2x_n + 1 + (x_n^2 - z_n^2)\} = z_{n+1}^2 + (x_n + 1)^2 - y_n^2 \\ &= z_{n+1}^2 \end{aligned}$$

- 5) $x^2 + y^2 = z^4$, maka $x^2 + y^2 = (z^2)^2$, berarti ada $m, n \in \mathbb{Z}, m > n$ sehingga $x = m^2 - n^2, y = 2mn$, dan $z^2 = m^2 + n^2$
Selanjutnya, karena $z^2 = m^2 + n^2$, maka ada $r, s \in \mathbb{Z}, r > s$ sehingga:
 $m = r^2 - s^2, n = 2rs$, dan $z = r^2 + s^2$

Dengan demikian dapat ditentukan bahwa:

$$x = (r^2 - s^2)^2 - (2rs)^2 = |r^4 - 6r^2s^2 + s^4|, y = 2(r^2 - s^2)2rs, z = r^2 + s^2$$

Beberapa selesaian dapat diperoleh dengan mengambil $(r, s) = 1, r > s > 0, r$ dan s mempunyai paritas yang berbeda, dengan menggunakan tabel berikut:

r	s	$x = r^4 - 6r^2s^2 + s^4 $	$y = 4rs(r^2 - s^2)$	$z = r^2 + s^2$
2	1	7	24	25
3	2	119	120	169
4	1	161	240	289
4	3	527	336	625



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang persamaan Diophantine non-linier, terutama yang mempunyai bentuk sebagai triple Pythagoras, bentuk yang serupa dengan triple Pythagoras, dan bentuk bilangan jumlah kuadrat (BJK), termasuk bilangan jumlah empat kuadrat. Ragam permasalahan dan penyelesaian menjadi lebih luas dan mendalam karena memerlukan banyak konsep terdahulu yang diperlukan, misalnya keprimaan, keterbagian, FPB, dan kongruensi.

1. **Definisi 7.1** Suatu triple Pythagoras (x, y, z) disebut primitif jika $(x, y, z) = 1$.
2. **Permasalahan BJK:** mencari bilangan bulat n sehingga $n = x^2 + y^2$, dengan x dan y adalah bilangan-bilangan bulat.
3. **Lemma 7.1**
Jika (x, y, z) adalah suatu triple Pythagoras primitif, maka $(x, y) = (x, z) = (y, z) = 1$.
4. **Lemma 7.2**
Jika (x, y, z) adalah suatu triple Pythagoras primitif, maka x adalah genap dan y adalah ganjil, atau x adalah ganjil dan y adalah genap.

5. Lemma 7.3

Jika r , s , dan t adalah bilangan-bilangan bulat positif sehingga $(r,s)=1$ dan $rs=t^2$, maka tentu ada bilangan-bilangan bulat m dan n sehingga $r=m^2$ dan $s=n^2$.

6. Teorema 7.1

Ditentukan $a, b, c \in \mathbb{Z}$, dan $d = (a, b)$

- jika d tidak membagi c , maka persamaan $ax+by=c$ tidak mempunyai selesaian;
- jika d membagi c , maka persamaan $ax+by=c$ mempunyai selesaian bulat yang tak hingga banyaknya, yaitu pasangan (x, y) di mana:

$$x = x_0 + \left(\frac{b}{d} \right) n \text{ dan } y = y_0 - \left(\frac{a}{d} \right) n$$

dengan $n \in \mathbb{Z}$ dan (x_0, y_0) adalah suatu selesaian khusus.

7. Teorema 7.2

Suatu triple (x, y, z) , dengan y adalah genap, adalah suatu triple Pythagoras primitif jika dan hanya jika ada dua bilangan bulat positif relatif prima m dan n , $m > n$, dengan m ganjil dan n genap, atau m genap dan n ganjil, sehingga:

$$x = m^2 - n^2, y = 2mn, \text{ dan } z = m^2 + n^2.$$

8. Teorema 7.3

Jika $x, y, z \in \mathbb{N}$ dan $(x, y, z) = 1$, maka persamaan Diophantine $x^2 + 2y^2 = z^2$ mempunyai selesaian: $x = |r^2 - 2s|^2$, $y = 2rs$, dan $z = r^2 + 2s^2$ di mana $r, s > 0$ dan $(r, 2s) = 1$.

9. Teorema 7.4

Jika r dan s adalah bilangan-bilangan jumlah kuadrat, maka rs juga merupakan BJK.

10. Teorema 7.5

Jika p adalah suatu bilangan prima ganjil yang mempunyai bentuk $4k+1$, maka tentu ada $m, n \in \mathbb{Z}$ sehingga $m^2 + n^2 = tp$ dengan $t \in \mathbb{Z}^+$ dan $t < p$.

11. Teorema 7.6

Jika p adalah suatu bilangan prima, dan p tidak kongruen dengan 3 modulo 4, maka tentu ada $m, n \in \mathbb{Z}$ sehingga $m^2 + n^2 = p$, yaitu p merupakan BJK.

12. Teorema 7.7

Suatu bilangan bulat positif n adalah BJK jika dan hanya jika faktor-faktor prima dalam pemfaktoran prima n yang mempunyai bentuk $3(\text{mod } 4)$, mempunyai pangkat yang genap.

13. Teorema 7.8

Jika r dan s adalah bilangan-bilangan bulat positif dan masing-masing merupakan bilangan jumlah empat kuadrat, maka rs juga merupakan bilangan jumlah empat kuadrat.

**TES FORMATIF 2**

1) Skor 10

Selesaikan persamaan Diophantine $x^4 + y^2 = z^2$ jika x, y, z saling relatif prima.

2) Skor 10

Carilah rumus memperoleh semua triple Pythagoras x, y, z jika $z = y + 1$.

3) Skor 15

Buktikan jika y dan z adalah bilangan-bilangan genap, maka selesaian persamaan:

$$x^2 + y^2 + z^2 = t^2$$

adalah:

$$x = \frac{p^2 + q^2 - r^2}{r}, y = 2p, z = 2q, t = \frac{p^2 + q^2 + r^2}{r}$$

dengan $p, q \in N$, $r < p^2 + q^2$ dan $r \mid p^2 + q^2$.

4) Skor 10

Tentukan semua triple Pythagoras (x, y, z) jika $z \leq 40$.

5) Skor 10

Jika (x, y, z) adalah suatu triple Pythagoras primitif, maka buktikan bahwa paling sedikit satu dari x , y , dan z habis dibagi oleh 4.

6) Skor 10

Nyatakan bilangan-bilangan berikut sebagai jumlah dua kuadrat

- (a) 650
- (b) 1450

7) Skor 10

Nyatakan bilangan-bilangan berikut sebagai jumlah dua kuadrat

- (a) 21658
- (b) 324608

8) Skor 5

Nyatakan bilangan-bilangan berikut sebagai jumlah tiga kuadrat

- (a) 11
- (b) 19

9) Skor 10

Nyatakan bilangan-bilangan berikut sebagai jumlah empat kuadrat

- (a) 510
- (b) 3570

10) Skor 10

Tunjukkan bahwa jika $n \in \mathbb{Z}^+$ dan $n = (8k + 7)$, k adalah suatu bilangan bulat, maka n bukan merupakan suatu bilangan jumlah tiga kuadrat.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1)	$67815 = 3.21480 + 3375$	n	s	t	q
	$21480 = 6.3375 + 1230$	1	1	0	3
	$3375 = 2.1230 + 915$	2	0	1	6
	$1230 = 1.915 + 315$	3	1	-3	2
	$915 = 2.315 + 285$	4	-6	19	1
	$315 = 1.285 + 30$	5	13	-41	2
	$285 = 9.30 + 15$	6	-19	60	1
	$30 = 2.15 + 0$	7	51	-161	9
		8	-70	221	-
		9	681	-2150	-

Dengan demikian $(67815)(681) + (21480)(-2150) = 15$, sehingga dapat ditentukan bahwa:

$$(67815)(681).8 + (21480)(-2150).8 = 15.8$$

$$(67815)(5448) + (21480)(-17200) = 120$$

Selesaian persamaan adalah (x, y) dengan

$$x = 5448 + 1432t, y = -17200 - 4521t, t \in \mathbb{Z}.$$

2)	$96577 = 1.67320 + 29257$	n	s	t	q
	$67320 = 2.29257 + 8806$	1	1	0	1
	$29257 = 3.8806 + 2839$	2	0	1	2
	$8806 = 3.2839 + 289$	3	1	-1	3
	$2839 = 9.289 + 238$	4	-2	3	3
	$289 = 1.238 + 51$	5	7	-10	9
	$238 = 4.51 + 34$	6	-23	33	1
	$51 = 1.34 + 17$	7	214	-307	4
	$34 = 2.17 + 0$	8	-237	340	1
		9	1162	-1667	
		10	-1399	2007	

$$(96577, 67320) = 17 = (96577)(-1399) + (67320)(2007)$$

$$(96577)(-1399)(20) + (67320)(2007)(20) = 17.20$$

$$(96577)(-27980) + (67320)(40140) = 340$$

Selesaian persamaan adalah (x, y) dengan $x = -27980 + 5681t$,
 $y = 40140 - 3960t$, dan $t \in \mathbb{Z}$.

$$3) \quad 8x - 5y + 7z = 21, \quad \text{maka} \quad -5y = -8x - 7z + 21, \quad \text{sehingga}$$

$$y = \frac{-8x - 7z + 21}{-5} \text{ atau } y = (x + z - 4) + \frac{-3x - 2z + 1}{-5}$$

Ambil $t = \frac{-3x - 2z + 1}{-5}$, maka $-5t = -3x - 2z + 1$,

$$\text{atau } -2z = 3x - 5t - 1, \text{ sehingga } z = \frac{3x - 5t - 1}{-2} = (-x + 2t) + \frac{x - t - 1}{-2}$$

$$u = \frac{x-t-1}{-2}, \text{ maka } -2u = x-t-1, \text{ atau } x = -2u + t + 1$$

$$z \equiv (-x + 2t) + y \equiv 3y + t - 1$$

$$\gamma = (x+z-4) + t = u + 3t - 4$$

Selesaian persamaan adalah (x, y) dengan

$$x = -2u + t + 1, \quad y = u + 3t - 4, \quad z = 3u + t - 1$$

$$4) \quad 101x + 102y + 103z = 1, \text{ maka } 101x + 102y = 1 - 103z$$

Karena $(101, 102) = 1$, maka dapat ditentukan bahwa 1 merupakan kombinasi linier dari 101 dan 102, yaitu $(101)(-1) + (102)(1) = 1$, sehingga dapat ditentukan bahwa:

$$(101)(103z - 1) + (102)(1 - 103z) = 1 - 103z$$

Dengan demikian $x = 103z - 1 + 102t$, $y = 1 - 103z - 101t$, dan untuk $z = u$ dapat ditentukan $x = 103u - 1 + 102t = 102u + u - 1 + 102t = 102(u + t) + u - 1$ atau $x = 102k + u - 1$, $y = 1 - 103u - 101t$

$$= -1 - 101a - \Sigma_{ii} - 101n + 1 - 101(a+i) - \Sigma_{ii} \text{ and } y = -1 - 101k - \Sigma_{ii}$$

5) Jika persamaan kedua dikurangi persamaan pertama

$$y + 2z + 3w = 200 \quad \text{.....(a)}$$

$$3x + 6z + 12y = 700 \text{ atau } x + 2z + 4y = 350 \quad (\text{b})$$

Jika (b) dikurangi (a) maka diperoleh:

$$5 + 3w = 150$$

Ambil $w = t$, maka $z = 150 - 3t$, $v = 350 - 3z - 6w$

$$= 350 - 450 + 9t - 6t = -100 + 3t \text{ dan } x = 100 - y - z - w$$

$$= 100 + 100 - 3t - 150 + 3t - t = 50 - t$$

Tes Formatif 2

- 1) $x^4 + y^2 = z^2$, maka $(x^2)^2 + y^2 = z^2$, berarti ada $m, n \in \mathbb{Z}$, $m > n$, sehingga: $x^2 = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$
 $x^2 = m^2 - n^2$, maka $x^2 + n^2 = m^2$, maka $x = r^2 - s^2$, $n = 2rs$, dan $m = r^2 + s^2$

Dengan demikian dapat ditentukan bahwa:

$$x = r^2 - s^2$$

$$y = 2mn = 4rs(r^2 + s^2)$$

$$z = m^2 + n^2 = (r^2 + s^2)^2 + (2rs)^2 = |r^4 + 6r^2s^2 + s^4|$$

Beberapa selesaian adalah triple $(3, 40, 41)$, $(5, 312, 313)$, $(15, 272, 353)$, $(7, 1200, 1201)$.

- 2) $x^2 + y^2 = z^2$, dan $z = y + 1$, maka $x^2 + y^2 = (y+1)^2$ atau $x^2 = y^2 + 2y + 1 - y^2$, berarti $2y = x^2 - 1$, atau $y = (x^2 - 1)/2$.

Berikutnya $z = 1 + y = 1 + \{(x^2 - 1)/2\} = (x^2 + 1)/2$.

Rumus yang dicari adalah:

$$x = m, y = (m^2 - 1)/2, \text{ dan } z = (m^2 + 1)/2$$

- 3) Tidak mungkin semua x, y, z adalah bilangan ganjil sebab jika $x, y, z \equiv 1, 3, 5, 7 \pmod{8}$, maka $x^2, y^2, z^2 \equiv 1 \pmod{8}$, sehingga $t^2 = x^2 + y^2 + z^2 \equiv 3 \pmod{8}$ tidak dapat diselesaikan karena 3 bukan residu kuadratis modulo 8.

Tidak mungkin salah satu dari x, y, z adalah genap, dan dua yang lain adalah ganjil sebab kuadrat dari yang ganjil adalah kuadrat dari $1, 3 \pmod{4}$ akan menghasilkan $1 \pmod{4}$, dan jumlah dari dua kuadrat yang ganjil adalah $1 \pmod{4}$, kuadrat yang genap menghasilkan $0 \pmod{4}$, sehingga $t^2 = x^2 + y^2 + z^2 \equiv 2 \pmod{4}$ tidak dapat diselesaikan karena 2 bukan residu kuadratis modulo 4.

Dengan demikian satu dari x, y, z adalah ganjil, yang lain adalah genap, misalnya $y = 2p$ dan $z = 2q$. Ambil $u = t - x$ atau $t = x + u$, maka:

$$(x+u)^2 = (x+t-x)^2 = t^2 = x^2 + y^2 + z^2 = x^2 + (2p)^2 + (2q)^2 \\ = x^2 + 4p^2 + 4q^2$$

$$x^2 + 2xu + u^2 = x^2 + 4p^2 + 4q^2, \text{ maka}$$

$$u^2 = 4p^2 + 4q^2 - 2xu$$

$$= 2(2p^2 + 2q^2 - xu)$$

Karena u^2 adalah genap, maka u adalah juga genap, misalnya $u = 2r$, maka $u^2 = 4r^2$, $4r^2 = u^2 = 4p^2 + 4q^2 - 2x(2r)$, maka $r^2 = p^2 + q^2 - xr$, berarti $r(r+x) = p^2 + q^2$, dengan demikian $r | p^2 + q^2$

Selanjutnya, dari $r^2 = p^2 + q^2 - xr$, dapat ditentukan bahwa

$$x = \frac{p^2 + q^2 - r^2}{r} \quad \text{dan} \quad \text{dari} \quad u = t - x, \quad \text{dapat} \quad \text{ditentukan}$$

$$t = u + x = 2r + \frac{p^2 + q^2 - r^2}{r} = \frac{p^2 + q^2 + r^2}{r}$$

Karena x ditentukan positif, maka $r^2 < p^2 - q^2$.

- 4) (6,8,10),(9,12,15), 12,16,20),(15,20,25),(18,24,30),(21,28,35),(24,32,40), (10,24,26) (10,24,26), (15,36,39), dan (30,16,34)
- 5) Berdasarkan Teorema 7.1, satu dari m atau n adalah genap, berarti $2 | mn$, sehingga dapat ditentukan bahwa $2 | 2mn$, atau $2 | y$.
- 6) (a) $650 = 13 \cdot 50 = (2^2 + 3^2)(1^2 + 7^2) = (2.1 + 3.7)^2 + (2.7 - 3.1)^2 = 23^2 + 11^2$
(b) $1450 = 29 \cdot 50 = (2^2 + 5^2)(1^2 + 7^2) = (2.1 + 5.7)^2 + (2.7 - 5.1)^2 = 37^2 + 9^2$
- 7) (a) $21658 = 2^1 7^2 13^1 17^1 = (1^2 + 1^2)(0^2 + 7^2)(2^2 + 3^2)(1^2 + 4^2)$
 $= \{(1.0 + 1.7)^2 + (1.7 - 1.0)^2\} \{(2.1 + 3.4)^2 + (2.4 - 3.1)^2\}$
 $= (7^2 + 7^2)(14^2 + 5^2) = (7.14 + 7.5)^2 + (7.5 - 7.14)^2 = 133^2 + 63^2$
(b) $324608 = 2^{10} 317^1 = 32^2(11^2 + 14^2) = (0^2 + 32^2)(11^2 + 14^2)$
 $= (0.11 + 32.14)^2 + (0.14 - 32.11)^2 = 448^2 + 352^2$
- 8) (a) $11 = 1^2 + 1^2 + 3^2$
(b) $19 = 1^2 + 3^2 + 3^2$
- 9) (a) $510 = 15 \cdot 34 = (1^2 + 1^2 + 2^2 + 3^2)(1^2 + 1^2 + 4^2 + 4^2)$
 $= (1.1 + 1.1 + 2.4 + 3.4)^2 + (1.1 - 1.1 + 2.4 - 3.4)^2$
 $+ (1.4 - 1.4 - 2.1 + 3.1)^2 + (1.4 + 1.4 - 2.1 - 3.1)^2$
 $= 22^2 + 4^2 + 1^2 + 3^2$

- (b) $3570 = 15.238 = (12 + 12 + 22 + 32)(12 + 42 + 52 + 142)$
 $= (1.1 + 1.4 + 2.5 + 3.14)2 + (1.4 - 1.1 + 2.14 - 3.5)2$
 $+ (1.5 - 1.14 - 2.1 + 3.4)2 + (1.14 + 1.5 - 2.4 - 3.1)2$
 $= 572 + 162 + 12 + 82$
- 10) $x \equiv 0, 1, 2, 3, 4, 5, 6, 7 \pmod{8}$, maka $x^2 \equiv 0, 1, 4 \pmod{8}$, dan dapat ditentukan bahwa: $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{8}$. Dengan demikian $x^2 + y^2 + z^2 \not\equiv 7 \pmod{8}$ tidak mempunyai selesaian.

Daftar Pustaka

- Agnew, J. (1972). *Exploration in Number Theory*. Belmont: Brooks/Cole.
- Anderson, J.A. and Bell, J.M. (1977). *Number Theory with Applications*. New Jersey: Prentice-Hall.
- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Ore, O. (1948). *Number Theory and Its History*. New York: McGraw-Hill.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Kriptologi

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul kriptologi ini diuraikan tentang cara-cara pembuatan kode dengan menggunakan aritmetika modulo 26, atau membaca kembali kode yang diterima juga dengan menggunakan aritmetika modulo 26. Jika kode yang dikirim disebut naskah biasa, maka kode yang diterima disebut naskah rahasia. Mengganti, mentranslasikan, atau mentransformasikan naskah biasa menjadi naskah rahasia disebut mengenkripsi (*enciphering*), sedangkan membaca kembali naskah rahasia menjadi naskah biasa disebut mendekripsi (*deciphering*).

Pembahasan tentang kriptologi ditekankan pada mengubah naskah biasa menjadi naskah rahasia dengan suatu transformasi, atau mengubah kembali naskah rahasia menjadi naskah biasa dengan suatu transformasi, antara lain dengan pilihan transformasi biasa berupa kongruensi linier, atau dengan pilihan transformasi matriks yang melibatkan sistem kongruensi linier.

Langkah-langkah yang ditempuh dalam proses pembuatan kode meliputi mengganti huruf atau kelompok huruf menjadi lambang bilangan atau blok lambang bilangan, mentransformasikan setiap bilangan atau blok bilangan menjadi bilangan-bilangan ekuivalensinya, kemudian diakhiri dengan penggantian kembali lambang bilangan atau blok bilangan menjadi lambang-lambang huruf. Untuk jenis transformasi tertentu, kita dapat menggunakan kripta analisis, yaitu studi tentang frekuensi kemunculan terbanyak dari huruf atau kelompok huruf dari suatu bahasa, sebagai dasar untuk menentukan translasi dari naskah rahasia dengan huruf atau kelompok huruf yang mempunyai frekuensi terbanyak.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu memahami konsep kriptologi, mengganti naskah biasa menjadi naskah rahasia, mengganti naskah rahasia menjadi naskah biasa, dan mencari bentuk-bentuk kongruensi linier atau sistem kongruensi linier yang diperlukan untuk mengenkripsi atau mendekripsi naskah.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep kriptologi, naskah biasa, naskah rahasia, inkripsi, dekripsi, monografik, poligrafik, dan kripta analisis.

Modul 8 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Pengodean Monografik, dan Kegiatan Belajar 2 adalah Pengodean Poligrafik. Setiap kegiatan belajar memuat Uraian, Contoh/Bukan Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 8 ini dijelaskan Rambu-Rambu Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi paparan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab/menyelesaikan, maka lihatlah Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum banyak membantu Anda keluar dari kesulitan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Kemampuan Anda dengan jalan mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah penggerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Pengodean Monografik**

Komunikasi antar manusia dapat dilakukan secara terbuka yang boleh diketahui orang/pihak lain atau masyarakat umum, atau secara tidak terbuka yang tidak boleh diketahui oleh orang/pihak lain atau masyarakat umum karena yang dikomunikasikan bersifat rahasia. Bahan yang dikomunikasikan berupa informasi atau pesan, dalam bentuk kalimat-kalimat yang disampaikan secara lisan atau secara tertulis.

Informasi atau pesan rahasia yang perlu dikomunikasikan perlu dikirim ke pihak sasaran karena diperlukan untuk kegiatan rahasia dalam diplomasi, atau kegiatan militer dalam peperangan/pertempuran untuk menyampaikan perintah/instruksi tentang strategi penyerangan/pertahanan yang harus dilakukan. Penyampaian pesan rahasia ini tentu sudah dilakukan manusia sejak zaman kuno, menurut cara mereka saat itu, dengan menggunakan kode-kode atau lambang-lambang yang tentu mempunyai makna khusus yang tidak mudah diketahui atau dipecahkan (kode rahasianya) oleh orang lain yang bukan kelompok sasaran.

Dengan adanya kreasi manusia berupa alfabet, dan banyaknya keperluan manusia untuk melakukan berbagai transaksi rahasia dengan menggunakan lambang alfabet, maka manusia mulai memikirkan dan membuat kode-kode rahasia dengan menggunakan alfabet, yaitu pesan/naskah asli dinyatakan dengan kata-kata atau kalimat dalam alfabet (yang terbaca bermakna), dan pesan/naskah yang rahasia juga dinyatakan dengan rangkaian kata-kata atau kalimat dalam alfabet (yang terbaca tidak bermakna).

Salah satu sistem pengodean yang pertama tercatat, digunakan pada zaman Julius Caesar, sehingga sering disebut pengodean Caesar. Sistem pengodean rahasia Caesar ini didasarkan pada aritmetika modulo, sehingga membuatnya menjadi kode, atau membaca kodennya memerlukan pengetahuan yang cukup tentang teori bilangan, khususnya kongruensi.

Dalam pembahasan sistem pengodean diperlukan istilah-istilah baku untuk memudahkan pembicaraan. Beberapa istilah itu adalah (1) ilmu yang mempelajari sistem pengodean rahasia disebut **criptologi**, (2) bagian dari criptologi yang berkaitan dengan perencanaan dan implementasi sistem rahasia disebut **criptografi**, (3) naskah/pesan yang akan diubah/dikodekan menjadi naskah/pesan rahasia disebut **naskah biasa (plaintext)**, dan naskah/pesan rahasia

yang dihasilkan dari pengodean disebut **naskah chipper** (*chipertex*), (4) proses mengubah naskah biasa menjadi naskah *chipper* disebut dengan **dekripsi** atau **enchipper**, dan proses mengubah naskah *chipper* menjadi naskah biasa disebut **enkripsi** atau **dechipper**, (5) *chipper* adalah suatu metode untuk mengubah naskah biasa menjadi naskah rahasia.

Sistem pengkodean rahasia terbaru yang akan dibicarakan adalah suatu sistem yang ditemukan pada tahun 1970, yang menggunakan alfabet baku huruf Inggris dan mentranslasikannya menjadi bilangan-bilangan bulat dari 0 sampai 25, sesuai dengan tabel berikut.

Tabel 8.1.
Ekuivalensi Huruf dan Bilangan

HURUF	A	B	C	D	E	F	G	H	I	J	K	L	M
BILANGAN	0	1	2	3	4	5	6	7	8	9	10	11	12

HURUF	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
BILANGAN	13	4	15	16	17	18	19	20	21	22	23	24	25

Definisi 8.1

Ditentukan suatu alfabet.

Suatu kode adalah pemetaan (*mapping*) antara huruf-huruf alfabet, dengan domain (daerah asal) naskah biasa dan dengan *range* (daerah hasil) naskah *chipper*.

Ekuivalensi huruf dan bilangan dapat juga dilakukan sesuai dengan alfabet dari bahasa selain bahasa Inggris. Tanda-tanda misalnya koma, titik koma, titik dua, jarak kosong, garis miring, dan tanda-tanda lain, sebagai bagian dari naskah/pesan dapat juga dirancang lambang bilangannya, tetapi untuk kesederhanaan, yang menjadi pembahasan hanya huruf-huruf alfabet Inggris.

Pasangan huruf dan bilangan pada Tabel 8.1 di atas dapat dibuat lain atau berbeda, sehingga ada $26!$ cara yang dapat dilakukan untuk membuat pasangan, dan diperoleh sistem-sistem yang berbeda karena perbedaan pasangan huruf dan bilangan. Masing-masing sistem didasarkan pada transformasi masing-masing huruf naskah biasa menjadi huruf-huruf yang berbeda untuk menghasilkan naskah *chipper*. *Chipper* semacam ini disebut dengan **chipper monografik** atau **chipper karakter**.

Chiper Caesar didasarkan pada transformasi masing-masing huruf dengan huruf lain pada posisi tiga urutan berikutnya, dan tiga urutan huruf terakhir menjadi tiga urutan huruf pertama alphabet. Dengan menggunakan aritmetika modulo, chiper Caesar dapat dijelaskan sebagai berikut.

Jika B adalah ekuivalensi bilangan dari huruf-huruf pada naskah biasa, dan R menyatakan ekuivalensi bilangan dari pasangan huruf pada naskah rahasia, maka $R \equiv B + 3 \pmod{26}$, $0 \leq R \leq 25$

Contoh 8.1

1. Huruf A pada naskah biasa berpasangan dengan bilangan nol, maka bilangan transformasi adalah $0 + 3 = 3$, sehingga huruf A pada naskah rahasia diganti D
2. Huruf X pada naskah biasa berpasangan dengan bilangan 23, maka bilangan transformasi adalah $23 + 3 = 26 \equiv 0 \pmod{26}$, sehingga X pada naskah rahasia diganti A

Secara keseluruhan, transformasi dari huruf, ke bilangan pasangan huruf, ke bilangan pengganti, dan ke huruf pasangan bilangan pengganti, dapat ditabelkan sebagai berikut:

Tabel 8.2.
Pasangan Huruf pada Naskah Biasa dan Naskah Rahasia

BIASA	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
RAHASIA	3	4	5	6	7	8	9	10	11	12	13	14	15
	D	E	F	G	H	I	J	K	L	M	N	O	P

BIASA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
RAHASIA	16	17	18	19	20	21	22	23	24	25	0	1	2
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Untuk membuat kode naskah biasa dengan transformasi aritmetika modulo, kelompokkan huruf-huruf dalam blok dengan ukuran sama (misalnya pengelompokan lima huruf), ubahlah huruf-huruf menjadi bilangan-bilangan

ekuivalen, carilah pasangan bilangan-bilangan dengan aritmetika modulo, kemudian gantilah bilangan-bilangan yang diperoleh dengan huruf-huruf yang bersesuaian sehingga diperoleh naskah *cipher* (rahasia) yang dicari. Naskah rahasia ini oleh penerima pesan perlu dibaca melalui transformasi balik.

Contoh 8.2

Pesan berupa naskah biasa "SAYA SUKA BELAJAR TEORI BILANGAN" akan diubah menjadi naskah *cipher* untuk dikirim ke sasaran tertentu. Langkah-langkah memperoleh jawaban adalah:

- pengelompokan 5 huruf menjadi: SAYAS UKABE LAJAR TEORI BILAN GAN
- pengubahan menjadi bilangan-bilangan ekuivalen
18 0 24 0 18 20 10 0 1 4 11 0 9 0 17 19 4 14 17 8 1 8 11 0 13 6 0 13
- pencarian pasangan bilangan dengan aritmetika modulo 26: $R \equiv B \pmod{26}$
21 3 1 21 23 13 3 4 7 14 3 12 3 20 22 7 17 20 11 4 11 14 3 16 9 3 16
- penggantian bilangan-bilangan dengan huruf ekuivalen, sehingga diperoleh:
VDBV XNDEH OMDU WHRUL ELODQ JDQ
- pengiriman naskah rahasia ke sasaran

Penerima pesan rahasia harus bisa memecahkan atau membaca kode sehingga pesan sesungguhnya bisa dipahami, dan tentu saja dikerjakan kalau pesan itu suatu perintah yang penting. Untuk keperluan membaca pesan, huruf-huruf diubah ke bilangan, kemudian diubah menjadi bilangan lain menggunakan hubungan $B \equiv R - 3 \pmod{26}$, dengan $0 \leq B \leq 25$, dan terakhir pesan itu ditransformasikan menjadi huruf-huruf.

Contoh 8.3

Mencari naskah biasa dari pesan rahasia dalam tulisan:

NEUMN DQWHV IRUPD WLIGH QJDQV HULXV

Langkah-langkah yang digunakan adalah:

- Pengubahan ke bilangan-bilangan ekuivalen
13 7 20 12 13 3 16 22 7 21 8 17 19 15 3 22 11 8 6 7 16 9 3 16 21
7 20 11 23 21
- Pencarian bilangan dengan aritmetika modulo 26 : $B \equiv R - 3 \pmod{26}$
10 4 17 9 0 10 0 13 19 4 18 5 14 17 12 0 19 8 5 3
4 13 6 0 13 18 4 17 8 20 18

3. Penggantian bilangan dengan huruf-huruf ekuivalen
KERJA KANTE SFORM ATIFD ENGAN SERIU S
4. Penggabungan huruf-huruf yang sesuai sehingga terbaca maknanya
KERJAKAN TES FORMATIF DENGAN SERIUS

Pengkodean dalam *cipher* Caesar merupakan satu keluarga *cipher* yang serupa dan disebut dengan suatu **transformasi penggantian** (*shift transformation*), yaitu:

$$R \equiv B + k \pmod{26}, \quad 0 \leq R \leq 25$$

di mana k disebut **kunci** dari besarnya penggantian huruf dalam alfabet. Dengan demikian terdapat 26 transformasi yang berbeda, termasuk untuk $k \equiv 0 \pmod{26}$, yaitu huruf-huruf tidak berubah karena $R \equiv B \pmod{26}$.

Secara umum dapat ditentukan suatu jenis transformasi:

$$R \equiv pB + q \pmod{26}, \quad 0 \leq R \leq 25$$

di mana $p, q \in \mathbb{Z}$, dan $(p, 26) = 1$ yang disebut **transformasi affin**. Transformasi penggantian adalah transformasi affin dengan $p = 1$.

Dengan mempersyaratkan $(p, 26) = 1$, maka R dan B bergerak dalam suatu sistem residi lengkap modulo 26, sehingga terdapat $\phi(26) = 12$ pilihan untuk p dan 26 pilihan untuk q , akibatnya ada $12 \cdot 26 = 312$ pilihan transformasi affin, termasuk untuk $R \equiv B \pmod{26}$ yang dipilih bila $p = 1$ dan $q = 0$. Jika hubungan antara naskah biasa dan naskah rahasia dinyatakan dengan $R \equiv pB + q \pmod{26}$, maka hubungan inversinya adalah:

$$B = \bar{p} (R - q) \pmod{26}, \quad 0 \leq B < 25$$

di mana \bar{p} adalah suatu inversi dari $p \pmod{26}$.

Jika $p = p = 7$ dan $q = 10$, maka $R \equiv 7B + 10 \pmod{26}$, sehingga $B \equiv 15(R - 10)$ atau $B \equiv 15R + 6 \pmod{26}$ karena 15 adalah suatu inversi 7 modulo 26. Hubungan antara huruf seperti Tabel 8.3 berikut.

Tabel 8.3
Korespondensi Huruf dari Cipher $R \equiv 7B + 10 \pmod{26}$

BIASA	A	B	C	D	E	F	G	H	I	J	K	L	M
RAHASIA	0	1	2	3	4	5	6	7	8	9	10	11	12
RAHASIA	10	17	24	5	12	19	0	7	14	21	2	9	16
RAHASIA	K	R	Y	F	M	T	A	H	O	V	C	J	Q

BIASA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
RAHASIA	13	14	15	16	17	18	19	20	21	22	23	24	25
RAHASIA	23	4	11	18	25	6	13	20	1	8	15	22	3
RAHASIA	X	E	L	S	Z	G	N	U	B	I	P	W	D

Sebagai peragaan, huruf J ekuivalen dengan $B = 9$, sehingga $R \equiv 7.9 + 10 \pmod{26}$ atau $R \equiv 73 \pmod{26} \equiv 21 \pmod{26}$. Dengan demikian $B = 9$ berpasangan dengan $R = 21$ sehingga J berkorespondensi dengan V.

Contoh 8.4

Pesan naskah biasa BACALAH URAIAN TEORI BILANGAN DENGAN CERMAT ditransformasikan menjadi naskah rahasia RKYKJ KHUZK OKXNM EZORO JKXAK XFMXA KXYMZ QKN

Contoh 8.5

Naskah rahasia VKXAK XNUXF KCMZV KCIOCU JKXAJ KNOHK X berkorespondensi dengan naskah biasa JANGA NTUND AKERJ AKANU LANGL ATIHA N yaitu pesan yang sesuai JANGAN TUNDA KERJAKAN ULANG LATIHAN

Marilah sekarang kita bahas tentang suatu teknik yang disebut analisis kripta (*cryptanalysis*) dari *cipher* yang didasarkan pada transformasi affine. Dalam usaha memilih karakter atau monografik *chiper*, frekuensi huruf pada naskah rahasia dibandingkan dengan frekuensi huruf pada naskah secara umum, sehingga diperoleh korespondensi di antara huruf-huruf. Dari pengamatan terhadap naskah umum berbahasa Inggris dapat diperoleh suatu persentase frekuensi dari 26 huruf alfabet sebagai berikut.

Tabel 8.4.
Frekuensi Kemunculan Huruf-huruf Alfabet

HURUF	A	B	C	D	E	F	G	H	I	J	K	L	M
Frekuensi %	7	1	3	4	13	3	2	3	8	< 1	< 1	4	3

HURUF	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frekuensi %	8	7	3	< 1	8	6	9	3	1	1	< 1	2	< 1

Dari tabel di atas dapat diketahui bahwa kelompok huruf-huruf yang mempunyai frekuensi kemunculan terbanyak adalah E, T, N, R, I, O, dan A. Kita dapat menggunakan informasi ini untuk menentukan *chiper* berdasarkan pada transformasi affin.

Misalkan kita akan menyelidiki suatu pesan yang telah ditransformasikan dengan aturan $R \equiv k \pmod{26}$, $0 \leq R \leq 25$. Naskah R yang akan dikriptasi analisis adalah:

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDL PD

Langkah awal yang ditempuh adalah menghitung frekuensi kemunculan masing-masing huruf dalam naskah rahasia, sehingga diperoleh

HURUF	A	B	C	D	E	F	G	H	I	J	K	L	M
Frekuensi %	1	0	4	5	1	3	0	0	0	1	0	1	1

HURUF	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frekuensi %	1	0	7	2	2	2	3	0	0	1	2	3	2

Dari tabel di atas dapat diketahui bahwa huruf-huruf naskah rahasia yang mempunyai frekuensi kemunculan paling banyak adalah P, C, D, F, T, dan Y. Tebakan utama kita adalah P merupakan pengganti E karena E adalah suatu huruf dalam naskah berbahasa Inggris yang mempunyai frekuensi kemunculan terbanyak. Dengan demikian dapat ditentukan bahwa $15 \equiv 4 + k \pmod{26}$ karena bilangan ekuivalen P adalah 15, dan bilangan ekuivalen E adalah 4. Ini berarti bahwa $k \equiv 11 \pmod{26}$. Akibatnya, $R \equiv B + 11 \pmod{26}$ atau $B \equiv R - 11 \pmod{26}$, dan korespondensi huruf dapat ditabelkan sebagai berikut:

RAHASIA	A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
BIASA	15 P	16 Q	17 R	18 S	19 T	20 U	21 V	22 W	23 X	24 Y	25 Z	0 A	1 B

RAHASIA	N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25
BIASA	2 C	3 D	4 E	5 F	6 G	7 H	8 I	9 J	10 K	11 L	12 M	13 N	14 O

Berdasarkan tabel korespondensi di atas dapat *didecipher* naskah rahasia sehingga diperoleh:

NUMBE RTHEO RYISU SEFUL FOREN CIPHE RINGM ESSAG ES dan kemudian dibaca sebagai:

NUMBER THEORY IS USEFUL FOR ENCHIPHERING MESSAGES

Jadi tebakan kita benar. Bisa jadi kita peroleh naskah yang kacau (terbaca tidak bermakna), sehingga kita perlu mencoba transformasi lain berdasarkan frekuensi kemunculan huruf naskah rahasia.

Tugas

Bacalah buku *Elementary Number Theory And Its Application* dari Kenneth H. Rosen tentang *Cryptology*. Jelaskan bagaimana Anda memecahkan pesan rahasia berbahasa Inggris:

USLEL JUTCC YRTPS URKLT YGGFV ELYUS LRYXD JURTU
ULVCU

URJRK QLLQL YXSRV LBRYZ CYREK LVXEB RYZDG HRGUS
LJLLM

LYPDJ LJTJU FALGU PTGVT JULYU SLDAL TJRWU SLJFE OLPU dengan menggunakan analisis kripta, yaitu menghitung frekuensi kemunculan masing-masing karakter, kemudian gunakan suatu sistem kongruensi linier dua variabel untuk memperoleh korespondensi huruf pada naskah biasa dan naskah rahasia.

Petunjuk Jawaban Tugas

Daftar frekuensi kemunculan masing-masing huruf dalam naskah rahasia adalah sebagai berikut.

HURUF	A	B	C	D	E	F	G	H	I	J	K	L	M
FREKUENSI	2	2	4	4	5	3	6	1	0	10	3	22	1

HURUF	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
FREKUENSI	0	1	4	2	12	7	8	16	5	1	3	10	2

Dengan demikian dapat kita ketahui bahwa dua huruf dengan frekuensi muncul terbanyak adalah L dan U. Jika dua huruf naskah Bahasa Inggris yang mempunyai frekuensi kemunculan terbanyak adalah E dan T, maka L mempunyai korespondensi dengan E dan mempunyai korespondensi dengan T. Akibatnya, jika transformasi mempunyai bentuk $R \equiv pB + q \pmod{26}$, maka diperoleh suatu sistem kongruensi linier dua variabel:

$$11 \equiv p(4) + q \pmod{26} \text{ atau } 4p + q \equiv 11 \pmod{26}$$

$$20 \equiv p(19) + q \pmod{26} \text{ atau } 19p + q \equiv 20 \pmod{26}$$

Dengan menggunakan substitusi atau eliminasi, maka dapat kita peroleh selesaian sistem kongruensi linier dua variabel tersebut, yaitu:

$$p \equiv 11 \pmod{26} \text{ dan } q \equiv 19 \pmod{26}$$

berarti transformasi yang dicari mempunyai bentuk:

$$R \equiv 11B + 19 \pmod{26}, \text{ sehingga } 19R \equiv 19 \cdot 11B + 19 \cdot 19 \pmod{26} \text{ atau}$$

$$19R \equiv B - 3 \pmod{26}$$

Ini berarti bahwa transformasi balik adalah $B \equiv 19R + 3 \pmod{26}$, dengan $0 \leq B \leq 25$. Akibatnya, korespondensi seluruh huruf dapat ditentukan sebagai berikut:

RAHASIA	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	
BIASA	3	22	15	8	1	20	13	6	25	18	11	4	23
	D	W	P	I	B	U	N	G	Z	S	L	E	X

RAHASIA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
BIASA	16	9	2	21	14	7	0	19	12	5	24	17	10
	Q	J	C	V	O	H	A	T	M	P	Y	R	K

Berdasarkan tabel korespondensi di atas kita dapat membaca atau menerjemahkan pesan rahasia, yaitu:

THEBE STAPP ROACH TOLEA RNNUM
 BERTH EORYI STOAT TEMPT TOSOL
 VEEVE RYHOM EWORK PROBL EMBYW
 ORKIN GONTH ESEEX ERCIS ESAST
 UDENT CANMA STERT HEIDE ASOFT
 HESUB JECT

Dengan menggabungkan huruf-huruf yang sesuai, maka pesan dalam naskah biasa adalah

THE BEST APPROACH TO LEARN NUMBER THEORY IS TO ATTEMPT TO SOLVE EVERY HOMEWORK PROBLEM BY WORKING ON THESE EXERCISES A STUDENT CAN MASTER THE IDEAS OF THE SUBJECT



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Dengan menggunakan cipher Caesar, nyatakan naskah biasa berikut menjadi naskah rahasia:
 - a) MATEMATIKA ITU INDAH
 - b) NUMBER RULES UNIVERSE
- 2) Nyatakan naskah rahasia JANGAN BEKERJA SAMA DALAM UJIAN dengan menggunakan transformasi affin $R \equiv 11B + 18 \pmod{26}$.
- 3) Nyatakan naskah rahasia KERJAKAN TIGA SOALINI DALAM SERATUS MENIT dengan menggunakan transformasi $R \equiv 21B + 5 \pmod{26}$.
- 4) Jika huruf yang paling banyak muncul dalam naskah suatu bahasa adalah I dan huruf yang paling banyak muncul pada naskah rahasia adalah T, maka carilah k apabila kita menggunakan transformasi $R \equiv B + k \pmod{26}$.
- 5) Jika dua huruf yang paling banyak muncul dalam naskah Bahasa Indonesia adalah I dan N, dan dua huruf yang paling banyak muncul dalam naskah rahasia adalah O dan R, maka carilah p dan q apabila kita menggunakan transformasi $R \equiv pB + q \pmod{26}$.

Petunjuk Jawaban Latihan

- 1) Gunakan Tabel 7.2
 - a) MATEMATIKA ITU INDAH ditulis menjadi MATEM ATIKA ITUIN DAH kemudian ditransfer menjadi PDWHP DWLND LWXLQ GDK
 - b) NUMBER RULES UNIVERSE ditulis menjadi NUMBE RRULE SUNIV ERSE
Kemudian ditransfer menjadi QXPEH UUXOH VXQLY HUVH
- 2) Ubahlah naskah biasa JANGAN BEKERJASAMA DALAM UJIAN menjadi bilangan pengganti berdasarkan Tabel 8.1 sehingga diperoleh:
9 0 13 6 0 13 1 4 10 4 17 9 0 18 0 12 0 3 0 11 0 12 20 9 8 0 13
kemudian kita enkripsi dengan menggunakan transformasi
 $R \equiv 11B + 18 \pmod{26}$ sehingga diperoleh:
13 18 5 6 18 5 3 10 24 10 23 13 18 8 18 20 18 25 18 9 18 20 4 13 2 18 5
Setelah ditranslasikan kembali ke huruf diperoleh
NSFGS KYKXN SISUS ZSJSJ SUENC SF
- 3) Ubahlah naskah biasa KERJAKAN TIGA SOALINI DALAM SERATUS MENIT menjadi bilangan pengganti berdasarkan Tabel 8.1 sehingga diperoleh: 10 4 17 9 0 10 0 13 19 8 6 0 18 16 0 11 8 13 8 3 0 11 0 12 18 4 17 0 19 20 18 12 4 13 8 19
kemudian kita enkripsi dengan menggunakan transformasi
 $R \equiv 21B + 5 \pmod{26}$ sehingga diperoleh bilangan-bilangan:
7 11 24 12 5 7 5 18 14 17 1 5 19 3 5 2 17 18 17 16 5 2 5 23 19 11 24 5
14 9 19 23 11 18 17 14
Setelah ditranslasikan kembali ke huruf diperoleh
HLYMF HFSOR BFTDF CRSRQ FCFXT LYFOJ TXLSR O
- 4) I adalah huruf dengan frekuensi terbanyak dalam suatu bahasa ditransfer menjadi T dalam naskah rahasia, berarti bilangan pengganti dari I ditransfer ke bilangan pengganti dari T, yaitu 8 ditransfer ke 19. Dengan demikian $8 + k - 7 = 19 \pmod{26}$, sehingga dapat ditentukan bahwa $k = 11$.
- 5) $I \equiv 8$ ditransfer ke $0 = 14$, dan $N = 13$ ditransfer ke $R = 17$, maka:
 $14 \equiv p \cdot 8 + q \pmod{26}$ dan $17 \equiv p \cdot 13 + q \pmod{26}$, atau
 $8p + q \equiv 14 \pmod{26}$ dan $13p + q \equiv 17 \pmod{26}$
Dengan menggunakan eliminasi dapat ditentukan bahwa $p = 11$ dan $q = 4$



Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Konsep, Contoh, dan Latihan tentang pengkodean, terutama tentang konsep membuat kode rahasia dan membaca kode rahasia, mengganti huruf dengan bilangan, mentransfer bilangan dengan pasangan bilangan lain yang bersesuaian dengan menggunakan transformasi tertentu, dan mengganti bilangan hasil transformasi kembali ke huruf. Proses membuat kode naskah biasa menjadi kode naskah rahasia disebut inkripsi, dan proses membaca kode naskah rahasia menjadi kode naskah biasa disebut dekripsi.

1. Definisi 8.1

Ditentukan suatu alfabet. Suatu **kode** adalah pemetaan (*mapping*) antara huruf-huruf alfabet, dengan domain (daerah asal) naskah biasa, dan dengan *range* (daerah hasil) naskah *chiper*.

2. Jika B adalah ekuivalensi bilangan dari huruf-huruf pada naskah biasa, dan R menyatakan ekuivalensi bilangan dari pasangan huruf pada naskah rahasia, maka $R \equiv B + 3 \pmod{26}$, $0 \leq R \leq 25$.
3. Pengkodean dalam cipher Caesar merupakan satu keluarga cipher yang serupa dan disebut dengan suatu **transformasi penggantian (shift transformation)**, yaitu $R \equiv B + k \pmod{26}$, $0 \leq R \leq 25$ di mana k disebut kunci dari besarnya penggantian huruf dalam alfabet. Dengan demikian terdapat 26 transformasi yang berbeda, termasuk untuk $k \equiv 0 \pmod{26}$, yaitu huruf-huruf tidak berubah karena $R \equiv B \pmod{26}$.
4. Analisis kripto adalah analisis untuk inkripsi dan dekripsi berdasarkan kajian kelompok huruf-huruf yang muncul dengan frekuensi terbanyak dalam suatu bahasa. Hasil analisis kripto diselesaikan dengan menggunakan kongruensi linier atau sistem kongruensi linier sehingga diperoleh bentuk transformasi yang diperlukan.



1. Skor 20

Dengan dekripsi Caesar, carilah naskah biasa dari naskah rahasia:
WLJDH PSDPO LPDDG DODKW ULSOH SBWKD JRUDV SULPL
WLI

2. Skor 20

Dengan dekripsi transformasi penggantian $R \equiv 7B + 10 \pmod{26}$, carilah naskah biasa dari naskah rahasia:

FUKLU JUHFM JKLKX KFKJK HRGJK XAKXL MZTMC

3. Skor 20

Gunakan analisis kripto untuk mendekripsi naskah rahasia berbahasa Inggris berdasarkan satu huruf yang paling sering muncul:

HTCSB TBDGT BDCTN

4. Skor 20

Gunakan analisis kripto untuk mendekripsi naskah rahasia berbahasa Inggris: MJMZK CXUNM GWIRY VCPUW MPRRW GMIOP MSNYS RYRAZ PXMCD WPRYE YXD

dengan inkripsi transformasi affin $R \equiv pB + q \pmod{26}$ dan berdasarkan frekuensi huruf-huruf terbanyak

5. Skor 20

Naskah rahasia WEZBF TBBNJ THNBT ADZQE TGTYR BZAJN ANOOZ ATWGN ABOVG FNWZV A dienkripsi menggunakan transformasi affin $R \equiv pB + q \pmod{26}$. Carilah naskah biasanya jika huruf-huruf yang paling sering muncul pada naskah biasa A, E, N, dan S.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Pengkodean Poligrafik**

 embahasan tentang pengkodean monografik didasarkan pada penggantian lambang huruf menjadi lambang bilangan, kemudian dilanjutkan dengan transformasi kembali dari bilangan ke huruf sehingga diperoleh naskah rahasia yang diperlukan. Dalam tingkatan yang lebih sulit, analisis kripto digunakan berdasarkan frekuensi kemunculan terbanyak dari huruf pada naskah biasa terhadap suatu bahasa.

Terdapat sistem pengkodean yang dapat digunakan untuk menghindari frekuensi kemunculan terbanyak huruf yang disebut dengan sistem pengkodean blok, atau pengkodean poligrafik. Dalam sistem pengkodean blok, huruf-huruf pada naskah biasa di blok menurut panjang tertentu, kemudian masing-masing blok diganti dengan bilangan. Dengan transformasi tertentu, bilangan pengganti diubah menjadi bilangan lain, dan terakhir menjadi naskah rahasia.

Misalnya kita akan mengubah naskah biasa dengan menggunakan blok dua (*diagraphic cipher*), maka masing-masing blok dua huruf pada naskah biasa diganti menjadi blok huruf yang lain pada naskah rahasia. Naskah biasa:

SEMUA ORANG MEMERLUKAN BILANGAN
diblok menjadi

SE MU AO RA NG ME ME RL UK AN BI LA NG AN

Kemudian, masing-masing blok dua huruf ini diganti bilangan seperti yang dilakukan pada pengkodean monografik sehingga diperoleh:

18 4 12 20 0 14 17 0 12 4 12 4 17 11 20 10 0 13
1 8 11 0 13 6 0 13

Masing-masing blok bilangan naskah biasa B_1B_2 diubah menjadi suatu blok bilangan naskah rahasia R_1R_2 dengan mendefinisikan R_1 sebagai residu non-negatif modulo 26 dari suatu kombinasi linier B_1 dan B_2 , serta R_2 sebagai residu non-negatif modulo 26 dari suatu kombinasi linier B_1 dan B_2 yang lain. Sebagai contoh, jika kita tentukan:

$$R_1 \equiv 5B_1 + 17B_2 \pmod{26}, 0 \leq R_1 < 26$$

$$R_2 \equiv 4B_1 + 15B_2 \pmod{26}, 0 \leq R_2 < 26$$

maka dapat kita cari konversi masing-masing blok dua, misalnya:

$$\text{Blok 19 2 : } R_1 \equiv 5.18 + 17.4 = 158 \equiv 2 \pmod{26}$$

$$R_2 = 4.18 + 15.4 = 132 \pmod{26}$$

$$\text{Blok 12 20 : } R_1 \equiv 5.12 + 17.20 = 400 \equiv 10 \pmod{26}$$

$$R_2 \equiv 4.12 + 15.20 = 348 \equiv 10 \pmod{26}$$

Secara keseluruhan, konversi semua blok dua adalah:

$$\begin{matrix} 2 & 2 & 10 & 10 & 4 & 2 & 7 & 16 & 10 & 2 & 10 & 2 & 7 & 1 & 10 & 22 & 4 & 13 \\ 11 & 20 & 1 & 4 & 13 & 12 & 4 & 13 \end{matrix}$$

Jika blok-blok dua ini kembali ditransfer ke huruf-huruf, maka diperoleh:

BB KK EC HQ KC KC HB KW EN LU BE NM EN

Cara mendeskripsi dari sistem blok dua di atas diperoleh dengan menggunakan Teorema 4.6. Untuk mencari naskah biasa B_1B_2 dari naskah rahasia R_1R_2 , kombinasi linier yang digunakan adalah:

$$B_1 \equiv 17R_1 + 5R_2 \pmod{26}$$

$$B_2 \equiv 18R_1 + 23R_2 \pmod{26}$$

Berdasarkan Teorema 4.6 dapat ditentukan bahwa kombinasi linier yang diperlukan untuk mentransfer adalah:

$$\begin{bmatrix} R_1 \\ R_2 \end{bmatrix} \equiv \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \pmod{26}$$

Selanjutnya, sesuai Teorema 4.8, dapat ditentukan bahwa inversi matriks:

$$\begin{bmatrix} 5 & 17 \\ 17 & 15 \end{bmatrix} \text{ adalah } \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix}$$

sehingga persamaan matriks yang digunakan untuk mendekripsi adalah:

$$\begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \equiv \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \pmod{26}$$

Contoh 8.6

Gunakan *cipher* digrafik untuk mengubah blok B_1B_2 menjadi blok R_1R_2 jika naskah biasa yang dikirimkan adalah BILANGAN ITU DIMANA MANA dengan menggunakan sistem kongruensi linier:

$$R_1 \equiv 3B_1 + 10B_2 \pmod{26}$$

$$R_2 \equiv 9B_1 + 7B_2 \pmod{26}$$

Jawab:

BILANGAN ITU DIMANA MANA diblok dua menjadi BI LA NG AN IT UD IM AN AM AN AX, dengan X hanya sebagai pelengkap, sehingga lambang bilangan pengganti adalah 1 8 11 0 13 6 0 13 8 19 20 3 8 12 0 13 0 12 0 13 0 23

Masing-masing blok dua dienkripsi dengan menggunakan:

$$R_1 \equiv 3B_1 + 10B_2 \pmod{26}$$

$$R_2 \equiv 9B_1 + 7B_2 \pmod{26}$$

sehingga diperoleh:

- | | | |
|-------|---|--|
| 1 8 | : | $R_1 = 3.1 + 10.8 = 83 \equiv 5 \pmod{26}$, $R_2 = 9.1 + 7.8 = 65 \equiv 13 \pmod{26}$ |
| 11 0 | : | $R_1 = 3.11 + 0.8 = 33 \equiv 7 \pmod{26}$, $R_2 = 9.11 + 7.0 = 99 \equiv 21 \pmod{26}$ |
| 13 6 | : | $R_1 = 3.13 + 10.6 = 21 \pmod{26}$, $R_2 = 9.13 + 7.6 \equiv 3 \pmod{26}$ |
| 0 13 | : | $R_1 = 3.0 + 10.13 \equiv 0 \pmod{26}$, $R_2 = 9.0 + 7.13 \equiv 13 \pmod{26}$ |
| 18 19 | : | $R_1 = 3.18 + 10.19 \equiv 10 \pmod{26}$, $R_2 = 9.18 + 7.19 \equiv 9 \pmod{26}$ |
| 20 3 | : | $R_1 = 3.20 + 10.3 \equiv 12 \pmod{26}$, $R_2 = 9.20 + 7.3 \equiv 19 \pmod{26}$ |
| 8 12 | : | $R_1 = 3.8 + 10.12 \equiv 14 \pmod{26}$, $R_2 = 9.8 + 7.12 \equiv 0 \pmod{26}$ |
| 0 12 | : | $R_1 = 3.0 + 10.12 \equiv 16 \pmod{26}$, $R_2 = 9.0 + 7.12 \equiv 6 \pmod{26}$ |
| 0 23 | : | $R_1 = 3.0 + 10.23 \equiv 22 \pmod{26}$, $R_2 = 9.0 + 7.23 \equiv 21 \pmod{26}$ |

Dengan demikian hasil transformasi blok dua adalah:

5 13 7 21 21 3 0 13 10 9 12 19 14 0 0 13 16 6 0 13 22 21

dan naskah rahasia yang dicari adalah:

FN HV VD AN KJ MT OA AN QG AD WV

Secara umum sistem poligrafik chiper dapat diperoleh dengan memisahkan naskah biasa dalam blok n huruf, mentranslasikan huruf-huruf menjadi bilangan-bilangan ekuivalen yang bersesuaian, dan menyatakan naskah rahasia menggunakan persamaan matriks:

$$R \equiv AB \pmod{26}$$

di mana A adalah suatu matriks berdimensi $n \times n$, $(\det A, 26) = 1$, serta:

$$R = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ \vdots \\ R_4 \end{bmatrix} \text{ dan } B = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ \vdots \\ B_4 \end{bmatrix}$$

$R_1 R_2 \dots R_n$ adalah blok naskah rahasia yang berkaitan dengan blok naskah biasa $B_1 B_2 \dots B_n$. Selanjutnya, bilangan pengganti naskah rahasia diubah kembali menjadi huruf-huruf.

Untuk mendekripsi suatu naskah rahasia, kita perlu mencari suatu persamaan matriks yang menyatakan B dalam R , dan diperoleh dari $R \equiv AB \pmod{26}$

$$R \equiv AB \pmod{26}$$

$\bar{A}R \equiv \bar{A} (A B) \pmod{26} = (\bar{A} A) B \pmod{26} = B \pmod{26}$
sehingga:

$$B \equiv \bar{A} R \pmod{26}$$

Contoh 8.7

Kita mau menginkripsi naskah biasa ENAM ADALAH BILANGAN PERFEK dengan menggunakan poligrafik blok 3, dan menggunakan matriks transformasi:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix}$$

Karena $\det A = 1$, maka $(\det A, 26) = 1$, maka pengkodean dapat diteruskan.
Bentuk persamaan matriks yang diperlukan adalah:

$$\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix} \equiv A \begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \pmod{26}$$

Pesan naskah biasa di blok tiga sehingga diperoleh:

ENA MAD ALA HBI LAN GAN PER FEK

Jika huruf-huruf blok tiga ditransformasikan menjadi bilangan, maka diperoleh:

4 13 0 12 0 3 0 11 0 7 1 8 11 0 13 6 0 13 15 4 17 5 4 10

Masing-masing blok tiga diubah dengan menggunakan matriks transformasi, sehingga untuk blok tiga yang pertama, diperoleh:

$$\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 4 \\ 13 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix}$$

dan untuk blok tiga yang kedua, diperoleh:

$$\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 21 \\ 24 \end{pmatrix}$$

serta untuk blok tiga yang ketiga, diperoleh:

$$\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 0 \\ 11 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 7 \\ 22 \end{pmatrix}$$

Secara keseluruhan hasil transformasi adalah

4 17 4 21 21 24 22 7 22 7 8 15 24 24 11 19 19 6 22 0 13 17 21 1

sehingga naskah rahasia yang diperoleh dari translasi ke huruf-huruf, adalah:

ERE VVY WHW HIP YYL TTG WAN RVB

Cara yang digunakan untuk menerjemahkan naskah rahasia menjadi naskah biasa dalam sistem poligrafik serupa dengan cara membuat naskah rahasia dari naskah biasa, yaitu menggunakan persamaan matriks, dengan mengoperasikan inverse dari matriks transformasi yang telah ditetapkan. Dengan demikian bentuk transformasi yang digunakan adalah:

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} = \bar{A} \begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix}$$

Contoh 8.8

Langkah awal untuk mendekripsi naskah rahasia yang diterima:

EREVVY WHWHIP YYL TTGWAN RVB

adalah mengubah menjadi blok tiga:

ERE VVY WHW HIP YYL TTG WAN RVB

kemudian mentranslasikannya menjadi lambang bilangan, sehingga diperoleh:

4 17 4 21 21 24 22 7 22 7 8 15 24 24 11 19 19 6 22 0 13 17 21 1

Jika bentuk matriks transformasi adalah:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix}$$

maka dapat dicari inversi A , yaitu:

$$A^{-1} \equiv \begin{pmatrix} 6 & 24 & 23 \\ 25 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} (\text{mod } 26)$$

Bentuk matriks transformasi adalah:

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 23 \\ 25 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix}$$

Masing-masing blok tiga diubah dengan menggunakan matriks transformasi, sehingga untuk blok tiga yang pertama, diperoleh:

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 23 \\ 25 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 13 \\ 0 \end{pmatrix} \pmod{26}$$

dan untuk blok tiga yang kedua, diperoleh:

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 23 \\ 25 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} \begin{pmatrix} 21 \\ 21 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \\ 3 \end{pmatrix} \pmod{26}$$

serta untuk blok tiga yang ketiga, diperoleh:

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 23 \\ 25 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} \begin{pmatrix} 22 \\ 7 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 11 \\ 0 \end{pmatrix} \pmod{26}$$

Secara keseluruhan hasil transformasi adalah:

4 13 0 12 0 3 0 11 0 7 1 8 11 0 13 6 0 13 15 4 17 5 4 10

sehingga naskah biasa yang diperoleh dari translasi ke huruf-huruf, adalah:

ENA MAD ALA HBI LAN GAN PER FEK

Dengan menggunakan penalaran makna bahasa, maka naskah biasa yang diperoleh dibaca sebagai ENAM ADALAH BILANGAN PERFEK

Tugas

Pengkodean poligrafik dapat dibentuk juga dengan menggunakan analisis kriptografi dari blok. Berikan paling sedikit satu contoh inkripsi blok dua jika pasangan suku kata yang sering muncul dalam suatu bahasa adalah DH dan RU, dan pasangan suku kata yang paling sering muncul dalam suatu naskah biasa adalah PE dan JL.

Petunjuk Jawaban Tugas

Lambang numerik blok DI adalah 3 7 ditransfer ke 15 4 , dan lambang numerik 17 20 ditransfer ke 9 11, dengan demikian jika A adalah matriks inkripsi, maka kita dapat memperoleh hubungan:

$$A = \begin{pmatrix} 3 & 17 \\ 7 & 20 \end{pmatrix} \equiv \begin{pmatrix} 15 & 9 \\ 4 & 11 \end{pmatrix} \pmod{26}$$

Inversi dari $\begin{pmatrix} 3 & 17 \\ 7 & 20 \end{pmatrix}$ adalah $\begin{pmatrix} 12 & 21 \\ 1 & 7 \end{pmatrix} \pmod{26}$, maka matriks transformasi adalah:

$$A = \begin{pmatrix} 12 & 21 \\ 1 & 7 \end{pmatrix} \begin{pmatrix} 15 & 9 \\ 4 & 11 \end{pmatrix} \equiv \begin{pmatrix} 24 & 7 \\ 17 & 8 \end{pmatrix} \pmod{26}$$



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Dengan menggunakan digrafik *chiper* yang mengubah blok B_1B_2 menjadi R_1R_2 yang mana:

$$R_1 \equiv 2B_1 + 5B_2 \pmod{26}$$

$$R_2 \equiv 5B_1 + 7B_2 \pmod{26}$$

maka inkripsi naskah biasa RAJIN DAN TEKUN

- 2) Dengan menggunakan digrafik *chiper* yang mengubah blok B_1B_2 menjadi R_1R_2 yang mana:

$$R_1 \equiv 3B_1 + 7B_2 \pmod{26}$$

$$R_2 \equiv 5B_1 + 9B_2 \pmod{26}$$

maka inkripsi naskah biasa FUNGSI JUMLAH PEMBAGI

- 3) Dekripsi naskah rahasia ZZ HD YP AN RM SS IF yang diperoleh dari mengenkripsi naskah biasa dengan menggunakan digrafik *chiper* yang mentranslasikan B_1B_2 ke R_1R_2 jika:

$$R_1 \equiv 3B_1 + 6B_2 \pmod{26}$$

$$R_2 \equiv 5B_1 + 9B_2 \pmod{26}$$

- 4) Carilah banyaknya pasangan huruf yang tidak berubah apabila suatu inkripsi dilakukan dengan menggunakan digrafik *chiper*:

$$R_1 \equiv 4B_1 + 5B_2 \pmod{26}$$

$$R_2 \equiv 3B_1 + B_2 \pmod{26}$$

- 5) Carilah matriks transformasi yang diperoleh dari penggunaan digrafik matriks:

$$\begin{pmatrix} 2 & 3 \\ 1 & 17 \end{pmatrix}$$

dilanjutkan dengan digrafik matriks:

$$\begin{pmatrix} 5 & 1 \\ 25 & 4 \end{pmatrix}$$

Petunjuk Jawaban Latihan

- 1) Naskah biasa RAJIN DAN TEKUN dikelompokkan menjadi blok dua, dan diteruskan dengan mengubah menjadi lambang numerik, sehingga diperoleh:

17 0 9 8 13 3 0 13 19 4 10 20 13 23 (23 adalah tambahan, pengganti X)

Matriks transformasi untuk penggantian dapat dinyatakan dengan:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

sehingga tiga lambang numerik yang pertama dapat ditranslasikan menjadi:

$$17 \ 0 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 0 \end{pmatrix} = \begin{pmatrix} 34 \\ 85 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 7 \end{pmatrix} \pmod{26}$$

$$9 \ 8 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 9 \\ 8 \end{pmatrix} = \begin{pmatrix} 58 \\ 101 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 23 \end{pmatrix} \pmod{26}$$

$$13 \ 3 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 3 \end{pmatrix} = \begin{pmatrix} 41 \\ 86 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 8 \end{pmatrix} \pmod{26}$$

Dengan demikian keseluruhan hasil translasi adalah:

8 7 6 23 15 8 13 13 6 0 16 4 11 5

dan hasil mengenkripsi adalah naskah rahasia:

IH GX PI NN GA QE LF

- 2) Naskah biasa FUNGSI JUMLAH PEMBAGI dikelompokkan menjadi blok dua, dan diteruskan dengan mengubah menjadi lambang numerik, sehingga diperoleh:

5 20 13 6 18 8 9 20 12 0 7 15 4 12 1 0 6 8

Matriks transformasi untuk penggantian dapat dinyatakan dengan:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

sehingga tiga lambang numerik yang pertama dapat ditranslasikan menjadi

$$17 \ 0 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 5 \\ 20 \end{pmatrix} = \begin{pmatrix} 155 \\ 205 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 22 \end{pmatrix} \pmod{26}$$

$$9 \ 8 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 6 \end{pmatrix} = \begin{pmatrix} 81 \\ 119 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 15 \end{pmatrix} \pmod{26}$$

$$13 \ 3 : \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 18 \\ 8 \end{pmatrix} = \begin{pmatrix} 110 \\ 162 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 6 \end{pmatrix} \pmod{26}$$

Dengan demikian keseluruhan hasil translasi adalah:

25 22 3 15 6 6 11 17 10 8 22 14 20 24 3 5 22 24

dan hasil mengenkripsi adalah naskah rahasia:

ZW DP GG LR KI WO UY DF WY

- 3) ZZ HD XP AN RM SS IF diubah menjadi lambang numerik, sehingga diperoleh

25 25 7 3 23 15 0 13 17 12 18 18 8 5

Matriks transformasi untuk mendekripsi dapat diperoleh sebagai berikut:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \text{ berarti } \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = \bar{\Delta} \begin{pmatrix} 3 & 6 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = 17 \begin{pmatrix} 9 & -6 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

$$\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv 17 \begin{pmatrix} 9 & 20 \\ 21 & 3 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 153 & 340 \\ 357 & 51 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \pmod{26}$$

$$\equiv \begin{pmatrix} 23 & 2 \\ 19 & 25 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \pmod{26}$$

sehingga tiga lambang numerik yang pertama adalah:

$$25 \ 25 : \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \begin{pmatrix} 23 & 2 \\ 19 & 25 \end{pmatrix} \begin{pmatrix} 25 \\ 25 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 1 \\ 8 \end{pmatrix} \pmod{26}$$

$$7 \ 3 : \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \begin{pmatrix} 23 & 2 \\ 19 & 25 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 11 \\ 0 \end{pmatrix} \pmod{26}$$

$$23 \ 15 : \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \begin{pmatrix} 23 & 2 \\ 19 & 25 \end{pmatrix} \begin{pmatrix} 23 \\ 15 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 13 \\ 6 \end{pmatrix} \pmod{26}$$

Dengan demikian keseluruhan hasil translasi adalah:

1 8 11 0 13 6 0 13 15 17 8 12 0 23

dan hasil mendekripsi adalah naskah rahasia:

BI LA NG AN PR IM AX

kemudian dibaca BILANGAN PRIMA

- 4) Jika pasangan B_1B_2 tidak berubah, maka dapat ditentukan bahwa:

$$B_1 \equiv 4B_1 + 5B_2 \pmod{26}$$

$$B_2 \equiv 3B_1 + B_2 \pmod{26}$$

sehingga diperoleh $B_1 \equiv 0 \pmod{26}$ dan $B_2 \equiv 0 \pmod{26}$.

Dengan demikian pasangan yang tidak berubah adalah AA

$$5) \begin{pmatrix} 5 & 1 \\ 25 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 1 & 17 \end{pmatrix} = \begin{pmatrix} 11 & 6 \\ 2 & 13 \end{pmatrix}$$



Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang pengkodean poligrafik, terutama yang mempunyai bentuk blok, salah satu di antaranya adalah blok dua atau disebut digrafik *chiper*. Bentuk-bentuk transformasi yang digunakan banyak melibatkan persamaan matriks dan akibatnya memerlukan selesaian yang mengoperasikan sistem kongruensi linier.

1. Untuk mengenkripsi suatu naskah biasa digunakan persamaan matriks:

$$R \equiv A B \pmod{26}$$

yang mana:

$$R = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ \vdots \\ R_n \end{bmatrix} \text{ dan } B = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ \vdots \\ B_n \end{bmatrix}$$

dan A adalah suatu matriks transformasi persegi yang memenuhi $(\det A, 26) = 1$

2. Untuk mendekripsi suatu naskah rahasia digunakan persamaan matriks:

$$B \equiv A^{-1} R \pmod{26}$$

yang mana:

$$R = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ \vdots \\ R_n \end{bmatrix} \text{ dan } B = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ \vdots \\ B_n \end{bmatrix}$$

dan A^{-1} adalah inverse matriks transformasi persegi A yang memenuhi
 $(\det A, 26) = 1$



TES FORMATIF 2

1) Skor 20

Carilah naskah rahasia dari naskah biasa SELAMAT BEKERJA dengan menggunakan matriks transformasi:

$$R_1 \equiv 3B_1 + 10B_2 \pmod{26}$$

$$R_2 \equiv 9B_1 + 7B_2 \pmod{26}$$

2) Skor 10

Carilah naskah rahasia dari naskah biasa FUNGSI MULTIPLIKATIF dengan menggunakan matriks transformasi:

$$R_1 \equiv 8B_1 + 9B_2 \pmod{26}$$

$$R_2 \equiv 3B_1 + 11B_2 \pmod{26}$$

3) Skor 20

Suatu analisis kripta digunakan untuk membuat naskah rahasia. Jika dua pasangan huruf yang muncul terbanyak pada naskah rahasia adalah RH dan NI, dan dua pasangan huruf yang muncul terbanyak dari suatu bahasa adalah TH dan HE, serta bentuk matriks transformasi yang digunakan adalah:

$$R_1 \equiv pB_1 + qB_2 \pmod{26}$$

$$R_2 \equiv rB_1 + sB_2 \pmod{26}$$

maka carilah nilai-nilai p, q, r , dan s .

4) Skor 20

Carilah naskah biasa dari naskah rahasia yang diperoleh dari mengenkripsi naskah biasa dengan menggunakan matriks transformasi

$$R_1 \equiv 3B_1 + 10B_2 \pmod{26}$$

$$R_2 \equiv 9B_1 + 7B_2 \pmod{26}$$

5) Skor 10

Carilah naskah biasa dari naskah rahasia yang diperoleh dari mengenkripsi naskah biasa dengan menggunakan matriks transformasi

$$R_1 \equiv 8B_1 + 9B_2 \pmod{26}$$

$$R_2 \equiv 3B_1 + 11B_2 \pmod{26}$$

6) Skor 10

Carilah banyaknya pasangan huruf yang tidak berubah jika digrafik *chiper* yang digunakan adalah

$$R_1 \equiv 7B_1 + 17B_2 \pmod{26}$$

$$R_2 \equiv B_1 + 6B_2 \pmod{26}$$

7) Skor 10

Carilah naskah rahasia dari naskah biasa BILANGAN MERSENNE dengan menggunakan transformasi affin:

$$R \equiv \begin{pmatrix} 3 & 2 \\ 7 & 11 \end{pmatrix} B + \begin{pmatrix} 8 \\ 19 \end{pmatrix} \pmod{26}$$

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) Dengan menggunakan Tabel 8.2 diperoleh:
TIGA EMPAT LIMA ADALAH TRIPLE PYTHAGORAS PRIMITIF
- 2) $R \equiv 7B + 10 \pmod{26}$, maka $7B \equiv R - 10 \pmod{26}$, atau
 $15.7B \equiv 15(R - 10) \pmod{26}$ berarti $B \equiv 15R + 6 \pmod{26}$
Dengan demikian korespondensi huruf antara naskah biasa dan naskah rahasia adalah

RAHASIA	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
BIASA	10	17	24	5	12	19	0	7	14	21	2	9	16
	K	R	Y	F	M	T	A	H	O	V	J	C	Q

RAHASIA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
BIASA	23	4	11	18	25	6	13	20	1	8	15	22	3
	X	E	L	S	Z	G	N	U	B	I	P	W	D

sehingga naskah biasa yang dicari adalah

DUA PULUH DELAPAN ADALAH BILANGAN PERFEK

- 3) Huruf yang paling sering muncul dalam bahasa Inggris adalah E, dan huruf yang paling sering muncul pada naskah rahasia adalah T berarti pasangan E adalah T.
Dengan demikian $19 \equiv 4 + k \pmod{26}$, berarti $k \equiv 15 \pmod{26}$, sehingga dapat ditentukan bahwa $R \equiv B + 15 \pmod{26}$ atau $B \equiv R - 15 \pmod{26}$.
- 4) Secara berturut-turut, tiga huruf dengan frekuensi terbanyak adalah J, F, dan O, dengan demikian pasangan J adalah E dan pasangan F adalah T, sehingga:

$9 \equiv 4p + q \pmod{26}$ dan $5 \equiv 19p + q \pmod{26}$.

Ternyata setelah diselesaikan menghasilkan $p = 24$ dan $q = 26$, tetapi $(24, 26) = 2 \neq 1$ sehingga dicari pasangan lain, yaitu J dengan E dan O dengan T, berarti: $9 \equiv 4p + q \pmod{26}$ dan $14 \equiv 19p + q \pmod{26}$

dengan demikian $p = 3$ dan $q = 3$, dan bentuk transformasi yang dicari adalah: $R \equiv 3B + 3 \pmod{26}$.

Naskah biasa yang dicari adalah:

WE USE FREQUENCIES OF LETTERS TO DECRYPT SECRET MESSAGES

- 5) Tentukan dua huruf yang mempunyai frekuensi terbanyak, dan pasangkan dengan huruf A dan E. Carilah transformasi affin $R \equiv pB + q \pmod{26}$, p dan q dicari dari suatu sistem kongruensi linier dua variabel dalam p dan q . Hasil yang diperoleh adalah:

THIS MESSAGE WAS ENCHIPIRED USING AN AFFIN TRANSFORMATION

Tes Formatif 2

- 1) SELAMAT BEKERJA diubah menjadi blok 2:

SE LA MA TB EK ER JA

kemudian ditransfer ke lambang numerik:

18 4 11 0 12 0 19 1 4 10 4 17 9 0

Selanjutnya gunakan matriks transformasi:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 10 \\ 9 & 7 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

untuk memperoleh bilangan ekuivalensinya:

16 8 7 21 10 4 15 6 8 2 0 3 1 3

Dengan demikian naskah rahasia yang dicari adalah

QI HV KE PG IC AD BD

- 2) FUNGSI MULTIPLIKATIF diubah menjadi blok 2:

FU NG SI MU LT IP LI KA TI FX

kemudian ditransfer ke lambang numerik:

5 20 13 6 18 8 12 20 11 19 8 15 11 8 10 0 19 8 5 23

Selanjutnya gunakan matriks transformasi

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 3 & 10 \\ 9 & 7 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

untuk memperoleh bilangan ekuivalensinya:

5 20 13 6 18 8 12 20 11 19 8 15 11 8 10 0 19 8 5 23

Dengan demikian naskah rahasia yang dicari adalah:

MB CB IM QW ZI RH ER CE QP NI

- 3) Huruf-huruf dengan frekuensi kemunculan terbanyak RH NI dan TH HE diubah menjadi lambang numerik : 17 7 13 8 dan 19 7 7 4

Dengan demikian matriks transformasi yang dicari adalah:

$$\begin{pmatrix} 17 & 13 \\ 7 & 8 \end{pmatrix} \equiv \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} \pmod{26}$$

Karena inversi $\begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}$ modulo 26 adalah $\begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$ maka dapat ditentukan

$$\begin{pmatrix} 17 & 13 \\ 7 & 8 \end{pmatrix} \equiv \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \pmod{26}$$

Dengan demikian $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv \begin{pmatrix} 17 & 13 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \equiv \begin{pmatrix} 3 & 24 \\ 24 & 25 \end{pmatrix} \pmod{26}$

Jadi : $p = 3$, $q = 24$, $r = 24$, dan $s = 25$

- 4) Naskah rahasia BL OC EF ID VH FN EB IB IQ GB GK WF diubah menjadi lambang bilangan:

1 11 14 2 4 5 8 3 21 7 5 13 4 1 8 1 8 16 6 1 6 10 22 5

kemudian dari matriks inkripsi:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \equiv \begin{pmatrix} 3 & 10 \\ 9 & 7 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

dapat ditentukan bahwa matriks dekripsinya adalah:

$$\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \begin{pmatrix} 21 & 22 \\ 25 & 9 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

sehingga masing-masing lambang bilangan dapat dicari ekuivalensinya, diperoleh:

3 20 0 4 12 15 0 19 7 0 1 8 18 3 8 1 0 6 8 19 8 6 0 23

Naskah biasa yang dicari adalah

DU AE MP AT HA BI SD IB AG IT IG AX

dibaca

DUA EMPAT HABIS DIBAGI TIGA

- 5) Naskah rahasia CN KH GB NN YU QC ZP WS diubah menjadi lambang bilangan:

2 13 10 7 6 1 13 13 24 20 16 2 25 15 22 18

kemudian dari matriks inkripsi

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \equiv \begin{pmatrix} 8 & 9 \\ 3 & 11 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$

dapat ditentukan bahwa matriks dekripsinya adalah:

$$\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \equiv \begin{pmatrix} 7 & 25 \\ 17 & 24 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

sehingga masing-masing lambang bilangan dapat dicari ekuivalensinya, diperoleh :

1 8 11 0 13 6 0 13 18 4 6 8 19 8 6 0

Naskah biasa yang dicari adalah:

BI LA NG AN SE GI TI GA

dibaca:

BILANGAN SEGITIGA

- 6) Karena tidak ada pasangan huruf yang berubah, maka $B_1 \equiv 7B_1 + 17B_2$ dan $B_2 \equiv B_1 + 6B_2$, sehingga dengan menggunakan eliminasi dapat ditentukan bahwa $13B_2 \equiv 0 \pmod{26}$. Dengan demikian $B_2 \equiv 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24 \pmod{26}$

Dari $B_2 \equiv B_1 + 6B_2$ atau $B_1 \equiv -5B_2 \pmod{0}$ dapat ditentukan $B_1 \equiv 21B_2 \pmod{26}$, berarti $21B_2 \equiv 0 \pmod{26}$. Karena $(21, 26) = 1$, maka $21B_2 \equiv 0 \pmod{26}$ mempunyai satu solusi.

Jadi banyaknya pasangan solusi adalah 13.

- 7) BILANGAN MERSENNE dikelompokkan menjadi blok dua:

BI LA NG AN ME RS EN NE

kemudian diubah menjadi lambang bilangan:

1 8 11 0 13 6 0 13 12 4 17 18 4 13 13 4

Selanjutnya, karena matriks transformasi yang digunakan mempunyai persamaan:

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \equiv \begin{pmatrix} 3 & 2 \\ 2 & 11 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} + \begin{pmatrix} 8 \\ 19 \end{pmatrix}$$

maka hasil transformasi bilangan adalah bilangan-bilangan ekuivalensi

1 10 15 18 7 20 8 6 0 17 17 24 20 8 3 24

sehingga naskah rahasia yang dicari adalah:

BK PS HU IG AR RY UI DY

Daftar Kepustakaan

- Agnew, J. (1972). *Exploration in Number Theory*. Belmont: Brooks/Cole.
- Anderson, J.A. and Bell, J.M. (1977). *Number Theory with Applications*. New Jersey: Prentice-Hall.
- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Ore, O. (1948). *Number Theory and Its History*. New York: McGraw-Hill.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.

Akar Primitif dan Aritmetika Indeks

Prof. Drs. Gatot Muhsetyo, M.Sc.



PENDAHULUAN

Dalam modul Akar Primitif dan Aritmetika Indeks ini diuraikan tentang sifat-sifat dasar derajat/tingkat/order, akar primitif, eksistensi dari akar primitif, dan aritmetika indeks.

Pembahasan tentang persamaan tingkat (order) dikembangkan dari hubungan fungsi ϕ -Euler, ditekankan pada pengertian dan sifat-sifat dari tingkat sebagai dasar untuk pembahasan lanjutan tentang akar primitif dan aritmetika indeks.

Pembahasan tentang akar primitif dan aritmetika indeks merupakan bagian utama untuk menyelesaikan kongruensi non-linier, khususnya kongruensi yang terkait dengan perpangkatan bilangan prima yaitu variabel kongruensi merupakan pangkat. Di dalam uraian terdapat eksistensi akar primitif dari bilangan-bilangan prima dan bilangan-bilangan bulat positif yang bukan prima.

Secara umum kompetensi yang diharapkan setelah mempelajari modul ini adalah Anda mampu memahami konsep tingkat (order) bilangan bulat positif, akar primitif, aritmetika indeks, dan cara menyelesaikan kongruensi non-linier bentuk pangkat, serta memahami keterkaitan penyelesaian kongruensi bentuk pangkat dengan akar primitif.

Secara khusus kompetensi yang diharapkan setelah mempelajari modul ini adalah Anda mampu menjelaskan konsep tingkat bilangan bulat positif, akar primitif, eksistensi akar primitif, aritmetika indeks, keterkaitan tingkat dan akar primitif, menyelesaikan kongruensi berpangkat dengan menggunakan sifat-sifat akar primitif, dan aritmetika indeks.

SUSUNAN KEGIATAN BELAJAR

Modul 9 ini terdiri dari dua kegiatan belajar. Kegiatan Belajar 1 adalah Akar Primitif dan Kegiatan Belajar 2 adalah Aritmetika Indeks. Setiap kegiatan belajar memuat Uraian, Contoh/Bukan Contoh, Tugas dan Latihan, Petunjuk Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir Modul 9 ini dijelaskan Kunci Jawaban Tes Formatif.

PETUNJUK BELAJAR

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi paparan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab/menyesuaikan maka lihatlah Petunjuk Jawaban Tugas dan Latihan. Jika langkah ini belum banyak membantu Anda keluar dari kesulitan maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri dan periksalah tingkat kemampuan Anda dengan jalan mencocokkan jawaban Anda dengan Kunci Jawaban Tes Formatif. Ulangilah penggerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

KEGIATAN BELAJAR 1**Akar Primitif**

persoalan akar primitif diawali dari pengertian tingkat (order) dari suatu bilangan bulat, yaitu suatu konsep yang dikembangkan dari teorema ϕ -Euler, suatu teorema yang berkaitan dengan suatu residu positif terkecil modulo n . Jika tingkat dari suatu bilangan bulat r yang relatif prima dengan n sama dengan $\phi(n)$ maka r disebut suatu akar primitif modulo n .

Sesuai dengan teorema Euler, jika m adalah suatu bilangan bulat positif dan $(a,m)=1$ maka $a^{\phi(m)} \equiv 1 \pmod{m}$. Dengan demikian, paling sedikit ada satu bilangan bulat x yang memenuhi kongruensi $a^{\phi(m)} \equiv 1 \pmod{m}$. Keadaan ini menunjukkan bahwa berdasarkan prinsip urutan rapi, ada suatu bilangan bulat positif terkecil yang memenuhi kongruensi.

Definisi 9.1

Jika $a,b \in \mathbb{Z}^+$ dan $(a,b)=1$ maka suatu bilangan bulat positif terkecil x yang memenuhi $a^x \equiv 1 \pmod{b}$ disebut tingkat dari a modulo b , ditulis $x = O_b a$.

Dari definisi 9.1 dapat ditentukan bahwa $x = O_b a$ memenuhi $a^x \equiv 1 \pmod{b}$ berarti $a^{O_b a} \equiv 1 \pmod{b}$.

Contoh 9.1

Carilah $O_7 2$.

Jawab:

Untuk mencari $O_7 2$, kita harus mencari bilangan bulat positif terkecil x pangkat dari 2 sedemikian hingga $2^x \equiv 1 \pmod{7}$, dengan $1 \leq x \leq 7$.

Perhatikan bahwa $2^1 = 2 \equiv 2 \pmod{7}$, $2^2 = 4 \equiv 4 \pmod{7}$,

$$2^3 = 8 \equiv 1 \pmod{7}.$$

Dengan demikian, 3 adalah bilangan bulat positif terkecil x pangkat dari 2 sedemikian hingga $2^x \equiv 1 \pmod{7}$. Jadi, $O_7 2 = 3$.

Contoh 9.2

Carilah $O_8 3$.

Jawab:

Untuk mencari $O_8 3$, kita harus mencari bilangan bulat positif terkecil x pangkat dari 3 sedemikian hingga $3^x \equiv 1 \pmod{7}$, dengan $1 \leq x \leq 8$.

Perhatikan bahwa $3^1 = 3 \equiv 3 \pmod{8}$, $3^2 = 9 \equiv 1 \pmod{8}$.

Dengan demikian, 2 adalah bilangan bulat positif terkecil x pangkat dari 3 sedemikian hingga $3^x \equiv 1 \pmod{8}$. Jadi, $O_8 3 = 2$.

Contoh 9.3

Carilah $O_{11} 7$.

Jawab:

Untuk mencari $O_{11} 7$, kita harus mencari bilangan bulat positif terkecil x pangkat dari 7 sedemikian hingga $7^x \equiv 1 \pmod{11}$, dengan $1 \leq x < 11$.

Perhatikan bahwa $7^1 = 7 \equiv 7 \pmod{11}$, $7^2 = 49 \equiv 5 \pmod{11}$,

$7^3 = 343 \equiv 2 \pmod{11}$, $7^4 = 2401 \equiv 3 \pmod{11}$, $7^5 = 16807 \equiv 10 \pmod{11}$,

$7^6 = 117649 \equiv 4 \pmod{11}$, $7^7 \equiv 6 \pmod{11}$, $7^8 \equiv 9 \pmod{11}$,

$7^9 \equiv 8 \pmod{11}$, $7^{10} \equiv 1 \pmod{11}$.

Dengan demikian, 10 adalah bilangan bulat positif terkecil x pangkat dari 7 sedemikian hingga $7^x \equiv 1 \pmod{11}$. Jadi, $O_{11} 7 = 10$.

Sekarang mariyah kita perhatikan teorema-teorema yang dapat membantu kita dalam mencari semua solusi kongruensi $a^x \equiv 1 \pmod{b}$ untuk $(a,b)=1$ dan $1 \leq x \leq b$.

Teorema 9.1

Jika $b > 0$, dan $(a,b)=1$ maka $x \in \mathbb{Z}^+$ adalah memenuhi kongruensi $a^x \equiv 1 \pmod{b}$ jika dan hanya jika order a modulo b membagi x , yaitu $O_b a | x$.

Bukti:

(→)

Jika $a^x \equiv 1 \pmod{b}$ maka sesuai dengan teorema algoritma pembagian, dapat ditentukan bahwa $x = qO_b a + r, 0 \leq r < O_b a$ sehingga

$$a^x = a^{qO_b a + r} = (a^{qO_b a})^q \cdot a^r \equiv a^r \pmod{b}, \text{ berarti } a^x \equiv a^r \pmod{b}, \text{ dengan } 0 \leq r < O_b a.$$

Dengan demikian, $r = 0$ karena sesuai dengan definisi, $y = O_b a$ adalah bilangan bulat positif terkecil sehingga $a^y \equiv 1 \pmod{b}$. Dari $r = 0$ dapat ditentukan bahwa $x = qO_b a$, yaitu $O_b a | x$.

(←)

Jika $O_b a | x$ maka $x = kO_b a$ dengan $k \in \mathbb{Z}^+$ sehingga

$$a^x = a^{kO_b a} = (a^{O_b a})^k \equiv 1 \pmod{b}$$

Contoh 9.4

Sesuai dengan contoh 9.1, tingkat dari 2 mod 7 adalah 3, atau $O_7 2 = 3$. Karena 3 tidak membagi 13 maka $x = 13$ tidak memenuhi $2^x \equiv 1 \pmod{7}$, dan karena 3 membagi 18 maka $x = 18$ memenuhi $2^x \equiv 1 \pmod{7}$.

Contoh 9.5

Sesuai dengan contoh 9.3, tingkat dari 7 mod 11 adalah 10, atau $O_{11} 7 = 10$. Karena 10 tidak membagi 15 maka $x = 15$ tidak memenuhi $7^x \equiv 1 \pmod{11}$, dan karena 10 membagi 30 maka $x = 30$ memenuhi $7^x \equiv 1 \pmod{11}$.

Teorema 9.2

Jika $b > 0$ dan $(a, b) = 1$ maka $O_b a | \phi(b)$.

Bukti:

Diketahui $(a, b) = 1$, maka sesuai dengan teorema Euler, $a^{\phi(b)} \equiv 1 \pmod{b}$, dan sesuai dengan definisi 9.1, $a^{O_b a} \equiv 1 \pmod{b}$. Dengan demikian, sesuai dengan teorema 9.1 dapat ditentukan bahwa $O_b a | \phi(b)$.

Contoh 9.6

Carilah $O_{17}5$.

Jawab:

$(5, 17) = 1$ dan $\phi(17) = 16$, maka sesuai dengan teorema Euler, $5^{16} \equiv 1 \pmod{17}$. Dengan demikian, kemungkinan nilai-nilai $O_{17}5$ adalah pembagi (faktor) dari 16 yang positif, yaitu 1, 2, 4, 8, dan 16. Selanjutnya, dapat ditentukan bahwa $5^1 \equiv 5 \pmod{17}$, $5^2 \equiv 8 \pmod{17}$, $5^4 \equiv 13 \pmod{17}$, $5^8 \equiv 16 \pmod{17}$, dan $5^{16} \equiv 1 \pmod{17}$. Jadi, $O_{17}5 = 16$.

Teorema 9.3

Ditentukan $r, s \in \mathbb{Z}^+$, $(a, b) = 1$, dan $b > 0$.

$a^r \equiv a^s \pmod{b}$ jika dan hanya jika $r \equiv s \pmod{\phi_b(a)}$.

Bukti:

(\rightarrow)

$a^r \equiv a^s \pmod{b}$ dengan $r \geq s$, $(a, b) = 1$ maka $(a^s, b) = 1$, sehingga $a^r = a^s \cdot a^{r-s} \equiv a^s \pmod{b}$. Dengan demikian, dapat ditentukan bahwa $a^{r-s} \equiv 1 \pmod{b}$, dan menurut teorema 9.1, $\phi_b(a)$ membagi $r - s$, berarti $r \equiv s \pmod{\phi_b(a)}$.

(\leftarrow)

$r \equiv s \pmod{\phi_b(a)}$ dengan $0 \leq s \leq r$ maka $r = k\phi_b(a) + s$, $k \in \mathbb{Z}^+$

$$a^r = a^{s+k\phi_b(a)} = a^s (a^{\phi_b(a)})^k \equiv a^s \pmod{b}.$$

Contoh 9.7

Misalkan kita ambil $a = 3$ dan $b = 14$ maka menurut Teorema 9.3, $3^5 \equiv 3^{11} \pmod{14}$ sebab $\phi(14) = 6$ dan $5 \equiv 11 \pmod{16}$.

Selanjutnya, 3^9 tidak kongruen 3^{20} modulo 6 sebab $\phi(14) = 6$ dan $5 \equiv 11 \pmod{16}$ tetapi 9 tidak kongruen dengan 20 modulo 6.

Pembahasan tentang tingkat dari bilangan-bilangan bulat terhadap modulo tertentu beserta teorema-teoremanya akan membawa kita untuk melanjutkan pembahasan tentang akar primitif. Akar primitif berkaitan dengan keadaan tingkat suatu bilangan bulat a dengan modulo m yang mempunyai tingkat sama dengan $\phi(m)$, dan jika tingkat ini ada maka residu positif terkecil dari ke pangkatannya dicari dari semua bilangan bulat positif yang relatif prima dan kurang dari n .

Definisi 9.2

Jika $(r, m) = 1, m > 0$, dan $O_m r = \phi(m)$ maka r disebut suatu akar primitif modulo m .

Contoh 9.8

3 adalah suatu akar primitif modulo 7 sebab $3^6 \equiv 1 \pmod{7}$ dan $O_7 3 = 6 = \phi(7)$.

5 adalah suatu akar primitif modulo 7 sebab $5^6 \equiv 1 \pmod{7}$ dan $O_7 5 = 6 = \phi(7)$.

Contoh 9.9

Bilangan-bilangan yang relatif prima dengan 8 adalah 1, 3, 5, dan 7
Perhatikan bahwa:

$$1^1 \equiv 1 \pmod{8}, \text{ berarti } O_8 1 = 1$$

$$3^2 \equiv 1 \pmod{8}, \text{ berarti } O_8 3 = 2$$

$$5^2 \equiv 1 \pmod{8}, \text{ berarti } O_8 5 = 2$$

$$7^2 \equiv 1 \pmod{8}, \text{ berarti } O_8 7 = 2$$

$$\phi(8) = 4$$

Ternyata tidak ada bilangan x yang relatif prima dengan 8 dan $O_8 x = 4$, berarti tidak ada akar primitif modulo 8.

Teorema 9.4

Jika $r, m \in \mathbb{Z}^+, (r, m) = 1$, dan r adalah suatu akar primitif modulo m maka sistem residu tereduksi modulo m adalah $T = r^1, r^2, \dots, r^{\phi(m)}$.

Bukti:

Kita harus menunjukkan bahwa semua unsur T adalah relatif prima dengan m dan tidak ada dua unsur yang kongruen.

$(r, m) = 1$ maka $(r^k, m) = 1$ untuk sebarang $k \in \mathbb{Z}^+$, berarti semua kepangkatan dari r relatif prima terhadap m .

Misalkan $r^i \equiv r^j \pmod{m}$ untuk suatu $i \neq j$ maka sesuai dengan Teorema 9.2, $i \equiv j \pmod{\phi(m)}$.

$1 \leq i \leq \phi(m)$ dan $1 \leq j \leq \phi(m)$, maka dari kongruensi $i \equiv j \pmod{\phi(m)}$ dapat ditentukan bahwa $i = j$, bertentangan dengan keadaan $i \neq j$.

Jadi r^i tidak kongruen r^j modulo m .

Contoh 9.10

$2^6 \equiv 1 \pmod{9}$ maka 2 adalah suatu akar primitif modulo 9. Selanjutnya, $\phi(9) = 6$, berarti kepangkatan 2 dari $1, 2, \dots, 6$ membentuk suatu sistem residu yang tereduksi modulo 9, yaitu:

$2^1 = 2 \equiv 2 \pmod{9}$, $2^2 = 4 \equiv 4 \pmod{9}$, $2^3 = 8 \equiv 8 \pmod{9}$, $2^4 = 16 \equiv 7 \pmod{9}$, $2^5 = 32 \equiv 5 \pmod{9}$, dan $2^6 = 64 \equiv 1 \pmod{9}$.

$T = \{1, 2, 4, 5, 7, 8\}$ adalah suatu sistem residu yang tereduksi modulo 9.

Teorema 9.5

Jika $s \in N$ dan $O_m b = r$ maka $O_m(b)^s = r/(r, s) = O_m b / (O_b b, s)$

Bukti:

Kita tentukan $u = O_m(b^s)$, $v = (r, s)$, $r = r_1 v$, dan $s = s_1 v$, maka

$$(r_1, s_1) = \left(\frac{r}{v}, \frac{s}{v} \right) = 1. \text{ Dengan demikian, dapat ditentukan bahwa}$$

$$(b^s)^{r_1} = (b^{s_1 v})^{r/v} = (b^r)^{s_1} \equiv 1 \pmod{m}.$$

Selanjutnya, $O_m b = r$ maka menurut teorema 9.1, $u \mid r_1$, sehingga

$$(b^s)^u = b^{su} \equiv 1 \pmod{m}, \text{ berarti } r \mid su, \text{ akibatnya } r_1 v \mid s_1 v u \text{ atau } r_1 \mid s_1 u.$$

Dari $r_1 \mid s_1 u$ dan $(r_1, s_1) = 1$ dapat ditentukan bahwa $r_1 \mid u$. Berikutnya, dari hubungan $u \mid r_1$ dan $r_1 \mid u$ dapat ditentukan bahwa $u = r_1 = r/v$, yaitu: $u = r/(r, s)$. $O_m(b^s) = r/(r, s) = O_m b / (O_m b, s)$.

Contoh 9.11

Berdasarkan keadaan $3 \equiv 3(\text{mod } 7)$, $3^2 \equiv 2(\text{mod } 7)$, $3^4 \equiv 4(\text{mod } 7)$, dan $3^6 \equiv 1(\text{mod } 7)$ dapat ditentukan bahwa $O_7 3 = 6$. Dengan demikian, $O_7 3^2 = 6/(6, 2) = 3$, $O_7 3^3 = 6/(6, 3) = 2$, dan $O_7 3^4 = 6/(6, 4) = 3$.

Perhatikan bahwa:

$$3^2 = 9 \equiv 2(\text{mod } 7), \text{ sehingga } (3^2)^3 \equiv 2^3(\text{mod } 7) \equiv 1(\text{mod } 7).$$

$$3^3 = 27 \equiv 6(\text{mod } 7), \text{ sehingga } (3^3)^2 \equiv 6^2(\text{mod } 7) \equiv 1(\text{mod } 7).$$

$$3^4 = 81 \equiv 4(\text{mod } 7), \text{ sehingga } (3^4)^3 \equiv 4^3(\text{mod } 7) \equiv 1(\text{mod } 7).$$

Teorema 9.6

Jika $m \in \mathbb{Z}, m > 1$, dan x adalah suatu akar primitif modulo m maka x^t adalah suatu akar primitif modulo m jika dan hanya jika $(t, \phi(m)) = 1$.

Bukti:

(\rightarrow)

x^t adalah suatu akar primitif, maka sesuai dengan Definisi 9.2,

$O_m x^t = \phi(m)$. Selanjutnya, sesuai dengan Teorema 9.5,

$$O_m x^t = O_m x / (O_m x, t) = \phi(m) / (\phi(m), t).$$

Jadi $(\phi(m), t) = 1$.

(\leftarrow)

$(t, \phi(m)) = 1$, maka $O_m x^t = O_m x / (t, O_m x) = O_m x$.

$O_m x = \phi(m)$ sebab x adalah suatu akar primitif modulo m .

$O_m x^t = O_m x$ dan $O_m x = \phi(m)$, berarti x^t adalah suatu akar primitif modulo m .

Teorema 9.7

Jika $m \in \mathbb{Z}^+$ dan $m > 1$ mempunyai suatu akar primitif, maka banyaknya seluruh akar primitif yang tidak kongruen adalah $\phi(\phi(m))$.

Bukti:

Misalkan r adalah suatu akar primitif modulo m , maka sesuai dengan Teorema 9.4, bilangan-bilangan bulat $r^1, r^2, \dots, r^{\phi(m)}$ membentuk sistem residu tereduksi modulo m . Selanjutnya, sesuai dengan Teorema 9.6, r^t adalah suatu akar primitif modulo m jika dan hanya jika $(t, \phi(m)) = 1$. Banyaknya r^t yang memenuhi $(t, \phi(m)) = 1$ adalah $\phi(\phi(m))$, jadi banyaknya seluruh akar primitif modulo m adalah $\phi(\phi(m))$.

Contoh 9.12

Misalkan kita ambil $m=11$ maka $x=2$ adalah suatu akar primitif modulo 11 sebab $O_{11}2=10$, yaitu $2^{10} = 2^5 \cdot 2^5 \equiv 10 \cdot 10 \pmod{11} \equiv 100 \pmod{11} \equiv 1 \pmod{11}$, dan $\phi(11)=10$. Dengan demikian, $O_{11}2=\phi(11)$. Selanjutnya, sesuai dengan Teorema 9.6, banyaknya seluruh akar primitif modulo 11 adalah $\phi(\phi(11))=\phi(10)=4$.

Akar-akar primitif itu adalah $2^1, 2^3, 2^7$, dan 2^9 , yang secara berturut-turut kongruen dengan 2, 8, 7, dan 6 modulo 11.

Jadi, seluruh akar primitif dari modulo 11 adalah 2, 6, 7, dan 8.

Marilah sekarang kita mempelajari akar primitif dari bilangan-bilangan prima. Untuk mempelajari hal ini, seperti halnya dalam aljabar, kita perlu memahami tentang sifat-sifat tertentu persamaan polinomial dengan koefisien bulat.

Suatu persamaan polinomial berderajat n dengan koefisien bulat mempunyai bentuk umum:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Selanjutnya, suatu bilangan bulat t disebut akar dari $f(x)$ modulo m jika $f(t) \equiv 0 \pmod{m}$, dan dapat kita tunjukkan bahwa setiap bilangan bulat yang kongruen dengan t modulo m juga merupakan suatu akar.

Contoh 9.13

Polinomial $f(x) = 2x^2 + 3x + 4$ tepat mempunyai dua akar yang tidak kongruen modulo 3, yaitu $x \equiv 1(\text{mod } 3)$ dan $x \equiv 2(\text{mod } 3)$.

Contoh 9.14

Polinomial $f(x) = x^2 + 3x + 2$ tepat mempunyai dua akar yang tidak kongruen modulo 5, yaitu $x \equiv 3(\text{mod } 5)$ dan $x \equiv 4(\text{mod } 5)$.

Contoh 9.15

Polinomial $f(x) = 3x^2 + 5$ tidak mempunyai akar modulo 7.

Teorema 9.8 (Teorema Lagrange)

Jika $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ adalah suatu polinomial berderajat n dengan koefisien bulat dan a_n tidak habis dibagi oleh suatu bilangan prima p maka $f(x)$ paling banyak mempunyai r akar tidak kongruen modulo p .

Bukti:

Induksi matematika kita gunakan untuk membuktikan Teorema 9.8. Hubungan berlaku untuk $n=1$, yaitu $f(x) = a_1 x + a_0$ dengan p tidak membagi a_1 , mempunyai satu akar, karena banyaknya akar dari $f(x)$ modulo p adalah banyaknya selesaian dari kongruensi linier $a_1 x \equiv -a_0 \pmod{p}$. Kongruensi ini mempunyai satu selesaian sebab p tidak membagi a_1 atau $(a_1, p) = 1$.

Misalkan hubungan berlaku untuk polinomial berderajat $n-1$, dan $f(x)$ adalah polinomial berderajat n dengan koefisien pertama tidak habis dibagi oleh p :

$$f(x) = a_k x^n + a_{k-1} x^{n-1} + \dots + a_1 x + a_0$$

dan misalkan $f(x)$ mempunyai $k+1$ akar yang tidak kongruen, yaitu t_0, t_1, \dots, t_n sehingga $f(t_k) \equiv 0 \pmod{p}$ untuk $k = 0, 1, \dots, n$.

Dengan demikian

$$\begin{aligned}
 f(x) - f(t_0) &= a_n(x^n - t_0^n) + a_{n-1}(x^{n-1} - t_0^{n-1}) + \dots + a_1(x - t_0) \\
 &= a_n(x - t_0)(x^{n-1} + x^{n-2}t_0 + \dots + xt_0^{n-2} + t_0^{n-1}) + \\
 &\quad a_{n-1}(x - t_0)(x^{n-2} + x^{n-3}t_0 + \dots + xt_0^{n-3} + t_0^{n-2}) + \dots + a_1(x - t_0) \\
 &= (x - t_0)g(x)
 \end{aligned}$$

dengan $g(x)$ adalah polinomial berderajat $n-1$.

Kita akan tunjukkan bahwa t_1, \dots, t_{n-1}, t_n semuanya adalah akar dari $g(x)$ modulo p , dan ditentukan bahwa $k \in \mathbb{Z}$ dan $1 \leq k \leq n$. Selanjutnya,

$$f(t_n) \equiv f(t_0) \equiv 0 \pmod{p}, \text{ sehingga: } f(t_n) - f(t_0) = (t_n - t_0)g(t_n) \equiv 0 \pmod{p}$$

Dengan demikian, $g(t_n) \equiv 0 \pmod{p}$ karena $t_n - t_0$ tidak kongruen $0 \pmod{p}$. Jadi, t_n adalah akar dari $g(x)$ modulo p . Hal ini menunjukkan bahwa polinomial $g(x)$ yang berderajat $n-1$ dan koefisien pertama tidak habis dibagi p , mempunyai n akar yang tidak kongruen, berarti terjadi kontradiksi. Jadi, $f(x)$ mempunyai paling banyak n akar tidak kongruen modulo p .

Teorema 9.9

Jika p adalah suatu bilangan prima, dan d adalah suatu pembagi dari $p-1$ maka polinomial $x^d - 1$ tepat mempunyai d akar yang tidak kongruen modulo p .

Bukti:

$d \mid p-1$ maka $p-1 = dt$ dengan $t \in \mathbb{Z}$.

$$x^{p-1} - 1 = (x^d - 1)(x^{d(t-1)} + x^{d(t-2)} + \dots + x^d + 1) = (x^d - 1)g(x).$$

Menurut Teorema Kecil Fermat, dapat ditentukan bahwa $x^{p-1} - 1$ mempunyai $p-1$ akar tidak kongruen modulo p , atau suatu akar dari $g(x)$ modulo p . Sesuai dengan teorema Lagrange, $g(x)$ mempunyai paling banyak $d(t-1) = p-d-1$ akar modulo p . Karena akar dari $x^{p-1} - 1$ modulo p yang bukan akar dari $g(x)$ modulo p adalah akar dari $x^d - 1$ modulo p , maka dapat ditentukan bahwa polinomial $x^d - 1$ paling sedikit mempunyai $(p-1)-(p-d-1)=d$ akar yang tidak kongruen modulo p , sedangkan teorema Lagrange menyatakan bahwa $x^d - 1$ paling banyak mempunyai d

akar tidak kongruen modulo p . Jadi, $x^d - 1$ tepat mempunyai d akar tidak kongruen modulo p .

Teorema 9.10

Jika p adalah suatu bilangan prima dan d adalah pembagi positif dari $p-1$, maka bilangan bulat tingkat d yang tidak kongruen modulo p adalah sama dengan $\phi(d)$.

Buktikan.

Teorema 9.11

Setiap bilangan prima mempunyai suatu akar primitif.

Buktikan.

Tugas

Buktikan: $O_{F_n} \leq 2^{n+1}$ jika $F_n = 2^{2^n} + 1$

Petunjuk Jawaban Tugas

$F_n = 2^{2^n} + 1$ maka $2^{2^n} + 1 \equiv 0 \pmod{F_n}$, berarti $2^{2^n} \equiv -1 \pmod{F_n}$

Jadi, $(2^{2^n})^2 \equiv 1 \pmod{F_n}$. Jadi, $O_{F_n} \leq 2^n \cdot 2 = 2^{n+1}$.



LATIHAN

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Carilah:
 - a. $O_7 2$
 - b. $O_9 5$
 - c. $O_{10} 3$
 - d. $O_7 6$
 - e. $O_{13} 10$

- 2) Tunjukkan bahwa:
- 5 adalah suatu akar primitif dari 6
 - 2 adalah suatu akar primitif dari 11
- 3) Carilah suatu akar primitif dari:
- 4
 - 10
 - 14
- 4) Carilah banyaknya akar primitif tidak kongruen modulo 14
- 5) Buktikan: jika a^{-1} adalah inversi dari a modulo m maka $O_m a = O_m a^{-1}$

Petunjuk Jawaban Latihan

- 1) a. Tingkat dari suatu bilangan bulat modulo 7 membagi $\phi(7) = 6$, jadi kemungkinan-kemungkinannya adalah 1, 2, 3, atau 6. Selanjutnya, dapat ditentukan bahwa $2^2 = 4 \equiv 4 \pmod{7}$, $2^3 = 8 \equiv 1 \pmod{7}$, berarti $O_7 2 = 3$.
- b. Tingkat dari suatu bilangan bulat modulo 9 membagi $\phi(9) = 8$, jadi kemungkinan-kemungkinannya adalah 1, 2, 4, atau 8. Selanjutnya, dapat ditentukan bahwa $5^2 = 25 \equiv 1 \pmod{8}$. Jadi $O_8 5 = 2$.
- c. Tingkat dari suatu bilangan bulat modulo 10 membagi $\phi(10) = 4$, jadi kemungkinan-kemungkinannya adalah 1, 2, atau 4. Selanjutnya, dapat ditentukan bahwa $3^2 = 9 \equiv 9 \pmod{10}$, $3^4 = 81 \equiv 1 \pmod{10}$, jadi $O_{10} 3 = 4$.
- d. Tingkat dari suatu bilangan bulat modulo 7 membagi $\phi(7) = 6$, jadi kemungkinan-kemungkinannya adalah 1, 2, 3, atau 6. Selanjutnya, dapat ditentukan bahwa $6^1 = 6 \equiv 6 \pmod{7}$, $6^2 = 36 \equiv 1 \pmod{7}$, jadi $O_7 6 = 2$.
- e. Tingkat dari suatu bilangan bulat modulo 13 membagi $\phi(13) = 12$, jadi kemungkinan-kemungkinannya adalah 1, 2, 3, 4, 6, atau 12. Selanjutnya, dapat ditentukan bahwa:
 $10^1 = 10 \equiv 10 \pmod{13}$, $10^2 = 100 \equiv 9 \pmod{13}$,
 $10^3 = 1000 \equiv 12 \pmod{13}$, $10^4 = 10000 \equiv 3 \pmod{13}$,
 $10^6 \equiv 144 \pmod{13} \equiv 1 \pmod{13}$.
Jadi $O_{13}(10) = 6$.

- 2) a. $5^2 = 25 \equiv 1 \pmod{6}$ dan $\phi(6) = 2$, jadi $O_6 5 = \phi(6)$, 5 adalah suatu akar primitif 6.
 b. $2^2 = 4 \equiv 4 \pmod{11}$, $2^5 = 32 \equiv 10 \pmod{11} \equiv -1 \pmod{11}$,
 $2^{10} = 1 \equiv 1 \pmod{11}$.
 Jadi, $O_{11} 2 = 10$, 2 adalah suatu akar primitif 11.
- 3) a. $\phi(4) = 2$, dan $3^2 = 9 \equiv 1 \pmod{4}$, jadi 3 adalah suatu akar primitif 4.
 b. $\phi(5) = 4$, dan $2^4 = 16 \equiv 1 \pmod{5}$, jadi 2 adalah suatu akar primitif 5.
 c. $\phi(14) = 6$, dan $3^6 = 3^3 \cdot 3^3 \equiv (-1)(-1) \pmod{14} \equiv 1 \pmod{14}$, jadi 3 adalah suatu akar primitif 14.
- 4) $\phi(14) = 6$, $3^6 \equiv 1 \pmod{14}$, dan $5^6 = 5^2 \cdot 5^2 \cdot 5^2 \equiv 11 \cdot 11 \cdot 11 \pmod{14} \equiv (-3)(-3)(-3) \pmod{14} \equiv -27 \pmod{14} \equiv 1 \pmod{14}$, jadi banyaknya akar primitif 14 adalah dua, yaitu 3 dan 5.
- 5) Jika $a^k \equiv 1 \pmod{m}$ maka $a^{-k} \equiv a^{-k} \cdot 1 \equiv a^{-k} \cdot a^k \equiv 1 \pmod{m}$. Dengan demikian, $O_m a = O_m a^{-1}$.



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang tingkat (order), dan akar primitif, terutama tentang konsep tingkat, dan konsep akar primitif, yang dikaitkan dengan sistem residu tereduksi, Fungsi Euler, dan faktor persekutuan terbesar.

1. Definisi 9.1

Jika $a, b \in \mathbb{Z}^+$ dan $(a, b) = 1$ maka suatu bilangan bulat positif x yang memenuhi $a^x \equiv 1 \pmod{b}$ disebut tingkat dari a modulo b , ditulis $x = O_b a$.

2. Definisi 9.2

Jika $(r, m) = 1$, $m > 0$, dan $O_m r = \phi(m)$ maka r disebut suatu akar primitif modulo m .

3. Teorema 9.1

Jika $b > 0$, dan $(a,b) = 1$ maka $x \in \mathbb{Z}^+$ adalah memenuhi kongruensi $a^x \equiv 1 \pmod{b}$ jika dan hanya jika order a modulo b membagi x , yaitu $O_b a | x$.

4. Teorema 9.2

Jika $b > 0$ dan $(a,b) = 1$ maka $O_b a | \phi(b)$.

5. Teorema 9.3

Ditentukan $r, s \in \mathbb{Z}^+, (a,b) = 1$, dan $b > 0$

$a^r \equiv a^s \pmod{b}$ jika dan hanya jika $r \equiv s \pmod{\phi(b)}$.

6. Teorema 9.4

Jika $r, m \in \mathbb{Z}^+, (r,m) = 1$, dan r adalah suatu akar primitif modul m maka sistem residu tereduksi modulo m adalah $T = r^1, r^2, \dots, r^{\phi(m)}$.

7. Teorema 9.5

Jika $s \in N$ dan $O_m b = r$, maka $O_m(b)^s = r / (r,s) = O_m b / (O_b b, s)$.

8. Teorema 9.6

Jika $m \in \mathbb{Z}, m > 1$, dan x adalah suatu akar primitif modulo m maka x^t adalah suatu akar primitif modulo m jika dan hanya jika $(t, \phi(m)) = 1$.

9. Teorema 9.7

Jika $m \in \mathbb{Z}^+$ dan $m > 1$ mempunyai suatu akar primitif, maka banyaknya seluruh akar primitif yang tidak kongruen adalah $\phi(\phi(m))$.

10. Teorema 9.8

Jika $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ adalah suatu polinomial berderajat n dengan koefisien bulat dan a_n tidak habis dibagi oleh suatu bilangan prima p , maka $f(x)$ paling banyak mempunyai r akar tidak kongruen modulo p .

11. Teorema 9.9

Jika p adalah suatu bilangan prima, dan d adalah suatu pembagi dari $p-1$ maka polinomial $x^d - 1$ tepat mempunyai d akar yang tidak kongruen modulo p .

12. Teorema 9.10

Jika p adalah suatu bilangan prima dan d adalah pembagi positif dari $p-1$, maka bilangan bulat tingkat d yang tidak kongruen modulo p adalah sama dengan $\phi(d)$.

13. Teorema 9.11

Setiap bilangan prima mempunyai suatu akar primitif.

**TES FORMATIF 1**

- 1) Skor: 10

Carilah:

- A. $O_{15}7$
- B. $O_{20}9$
- C. $O_{21}10$
- D. $O_{29}3$
- E. $O_{17}9$

- 2) Skor 10

Carilah akar-akar primitif dari:

- A. 5
- B. 13
- C. 11
- D. 18
- E. 20

- 3) Skor 10

Tunjukkan bahwa:

- A. 12 tidak mempunyai akar primitif
- B. 20 tidak mempunyai akar primitif

- 4) Skor 15

Buktikan: jika m adalah suatu bilangan bulat positif, a dan b adalah bilangan-bilangan bulat yang relatif prima dengan m dan $(O_m a, O_m b) = 1$ maka $O_m ab = O_m a \cdot O_m b$.

5) Skor 15

Buktikan: jika $a \in \mathbb{Z}, m \in \mathbb{Z}^+, (a, m) = 1$, dan $O_m a = pq$ maka $O_m a^p = q$.

6) Skor 20

Buktikan: jika $a \in \mathbb{Z}, m \in \mathbb{Z}^+, (a, m) = 1$, dan $O_m a = m - 1$ maka m adalah prima.

7) Skor 20

Buktikan: jika p dan q adalah bilangan-bilangan prima ganjil maka pq adalah suatu prima semu jika dan hanya jika $O_q 2 | p - 1$ dan $O_p 2 | q - 1$.

Berdasarkan bukti tersebut, tentukan apakah bilangan-bilangan 13.67 dan 19.73 adalah prima-prima semu.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

KEGIATAN BELAJAR 2**Aritmetika Indeks**

Pembahasan tentang akar primitif dapat dipersempit hanya pada bilangan prima. Beberapa teorema yang dikembangkan, antara lain teorema Lagrange dan teorema yang terkait dengan polinomial, pada akhirnya dapat digunakan sebagai dasar untuk membuktikan bahwa setiap bilangan prima tentu mempunyai suatu akar primitif. Selanjutnya, dapat ditunjukkan bahwa semua bilangan bulat positif mempunyai akar-akar primitif.

Akar primitif juga dapat digunakan untuk mengerjakan aritmetika modulo. Aritmetika tentang modulo ini disebut dengan Aritmetika Indeks, yaitu suatu konsep khusus yang dapat digunakan untuk menyelesaikan kongruensi yang memuat perpangkatan.

Dari pembahasan sebelumnya diketahui bahwa jika suatu polinomial dengan koefisien bulat $f(x)$, maka suatu bilangan bulat k disebut suatu akar dari $f(x)$ modulo m jika $f(k) \equiv 0 \pmod{m}$, dan akibatnya setiap bilangan bulat yang kongruen dengan k modulo m juga merupakan suatu akar dari $f(x)$.

Teorema 9.12

Jika p adalah suatu bilangan prima ganjil dengan akar primitif a maka salah satu dari a atau $a + p$ merupakan suatu akar primitif modulo p^2 .

Bukti:

Karena a adalah suatu akar primitif modulo p , maka dapat kita ketahui bahwa $O_p a = \phi(p) = p - 1$.

Misalkan $n = O_{p^2} a$ sedemikian hingga $a^n \equiv 1 \pmod{p^2}$, maka berdasarkan $p \mid p^2$ dapat ditentukan bahwa $a^n \equiv 1 \pmod{p}$, dan sesuai dengan Teorema 9.1, $p - 1 = O_p a \mid n$. Dengan demikian, sesuai dengan Teorema 9.2,

$$n \mid \phi(p^2) = p \{1 - (1/p)\} = p(p - 1).$$

Selanjutnya, karena $n \mid p(p - 1)$ dan $p - 1 \mid n$ maka kemungkinannya $n = p - 1$ atau $n = p(p - 1)$.

Jika $n = p(p-1)$, maka a adalah suatu akar primitif modulo p^2 karena $O_{p^2}a = \phi(p^2)$.

Jika $n = p-1$, maka $a^{p-1} \equiv 1 \pmod{p^2}$.

Jika ditentukan $b = a + p$ maka $b \equiv a \pmod{p}$, berarti b adalah juga suatu akar primitif modulo p . Dengan demikian, nilai $O_{p^2}b$ kemungkinannya sama dengan $p-1$ atau $p(p-1)$.

Kita akan tunjukkan bahwa $O_{p^2}b$ tidak sama dengan $p-1$.

Sesuai dengan teorema binomial, dapat ditentukan bahwa:

$$\begin{aligned} b^{p-1} &= (a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2} + (1/2)(p-1)(p-2)a^{p-3}p^2 + \dots + p^{p-1} \\ &\equiv a^{p-1} + (p-1)p.a^{p-2} \pmod{p^2} \end{aligned}$$

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

$$b^{p-1} \equiv 1 + (p-1)p.a^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2}$$

berarti b^{p-1} tidak kongruen dengan $1 \pmod{p^2}$ sebab jika $b^{p-1} \equiv 1 \pmod{p^2}$, maka dapat ditentukan bahwa $pa^{p-2} \equiv 0 \pmod{p^2}$ sehingga $a^{p-2} \equiv 0 \pmod{p}$ dan hal ini tidak bisa terjadi karena p tidak membagi a (ingat bahwa a adalah suatu akar primitif dari p).

Jadi $O_{p^2}b = p(p-1) = \phi(p^2)$, yaitu $b = a + p$ adalah suatu akar primitif dari p^2 .

Contoh 9.16

- a. 2 adalah suatu akar primitif modulo 11, $2^{10} \equiv 1 \pmod{11}$, atau $O_{11}2 = 10 = \phi(11)$.

Untuk menentukan apakah 2 suatu akar atau bukan akar primitif modulo 11^2 , perlu diselidiki keadaan dari $2^{11-1} = 2^{10}$. Ternyata $2^{10} = 1024 \equiv 56$ tidak kongruen $1 \pmod{11^2}$ berarti kemungkinan yang lain benar, yaitu $2^{11(11-1)} = 2^{\phi(11^2)} \equiv 1 \pmod{11^2}$. Jadi 2 adalah juga suatu akar primitif modulo 11^2 .

- b. 3 adalah suatu akar primitif modulo 17, sesuai teorema Euler, karena $(3, 17) = 1$ maka $3^{\phi(17)} = 3^{16} \equiv 1 \pmod{17}$, berarti $O_{17}3 = 16 = \phi(17)$. $3^{17-1} = 3^{16} \equiv 243 \pmod{17^2}$ tidak kongruen $1 \pmod{17^2}$.

Dengan demikian, kemungkinan lain benar, yaitu $3^{17(17-1)} \equiv 1 \pmod{17^2}$,
 3 adalah juga suatu akar primitif modulo 17^2 .

- c. 10 adalah suatu akar primitif dari $p = 487$ karena $10^{487-1} = 10^{486} \equiv 1 \pmod{487}$, tetapi 10 bukan suatu akar primitif modulo 487^2 . Dengan demikian, sesuai Teorema 9.12, dapat ditentukan bahwa $10 + 487 = 497$ adalah suatu akar primitif modulo 487^2 .

Teorema 9.13

Jika p adalah suatu bilangan prima ganjil maka p^r mempunyai suatu akar primitif untuk semua $r \in N$, dan jika s adalah suatu akar primitif modulo p^2 maka s adalah suatu akar primitif modulo p^r untuk semua $r \in N$.

Bukti:

Sesuai dengan teorema 9.12, karena p adalah bilangan prima ganjil, maka p mempunyai suatu akar primitif r yang juga merupakan akar primitif modulo p^2 , berarti r^{p-1} tidak kongruen dengan

$$1(\text{mod } p^2) \dots (*)$$

Dengan menggunakan induksi matematika, akan kita buktikan bahwa:

$r^{p^{k-2}(p-1)}$ tidak kongruen dengan $1 \pmod{p^k}$, untuk semua $k \in N$ dan

$k \geq 2$ (**)

Jika hal ini bisa kita buktikan maka kita dapat menyatakan bahwa r adalah juga suatu akar primitif modulo p^k . Perlu diingat bahwa:

$$\phi(p^k) = p^k \left(1 - \frac{1}{p}\right) = p^k \left(\frac{p-1}{p}\right) = p^{k-1}(p-1)$$

Kita tentukan bahwa $n = O_{p^k} r$, atau $r^n \equiv 1 \pmod{p^k}$, maka sesuai dengan

Teorema 9.2, $O_{p^k} r \mid \phi(p^k)$ atau $n \mid \phi(p^k)$, berarti $n \mid p^{k-1}(p-1)$.

Selanjutnya, dari $p \mid p^k$ dan $r^n \equiv 1 \pmod{p^k}$, maka dapat ditentukan bahwa $r^n \equiv 1 \pmod{p}$.

Sesuai dengan Teorema 9.1, dari $r^n \equiv 1 \pmod{p}$ dapat ditentukan bahwa $\phi(p) = p-1 | n$.

Dari $p-1|n$ dan $n|p^{k-1}(p-1)$, berakibat $n=p^t(p-1)$, yang mana $t \in \mathbb{Z}$ sedemikian hingga $0 \leq t \leq k-1$.

Jika $n = p^t(p-1)$ dengan $t \leq k-2$ maka

$$r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv (r^n)^{k-2-t} \pmod{p^k} \equiv 1 \pmod{p^k}$$

bertentangan dengan keadaan (**).

Dengan demikian, $O_{p^k} r = p^{k-1}(p-1) = \phi(p^k)$ atau r adalah juga suatu akar primitif modulo p^k .

Marilah sekarang kita buktikan (**) dengan menggunakan induksi matematika.

Untuk $k=2$, berlaku (*), r^{p-1} tidak kongruen dengan $1 \pmod{p^2}$.

Anggaplah hubungan berlaku benar untuk $k \in N$ dan $k \geq 2$, yaitu:

$$r^{p^{k-2}(p-1)} \text{ tidak kongruen dengan } 1 \pmod{p^k}$$

Karena $(r, p)=1$ maka $(r, p^{k-1})=1$, akibatnya:

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$$

Dengan demikian, tentu ada bilangan bulat d sedemikian hingga:

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1}$$

p tidak membagi d sebab sesuai anggapan $r^{p^{k-2}(p-1)}$ tidak kongruen dengan $1 \pmod{p^k}$. Selanjutnya, dapat ditentukan bahwa

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1}$$

$$(r^{p^{k-2}(p-1)})^p = (1 + dp^{k-1})^p$$

$$r^{p^{k-2}(p-1)} = 1 + p(dp^{k-1}) + \binom{p}{2} (dp^{k-1})^2 + \dots + (dp^{k-1})^p \equiv 1 + dp^k \pmod{p^{k+1}}$$

Karena p tidak membagi d maka dapat disimpulkan bahwa $r^{p^{k-2}(p-1)}$ tidak kongruen dengan $1 \pmod{p^k}$.

Contoh 9.17

- 2 adalah suatu akar primitif modulo 3 dan suatu akar primitif modulo 3^2 karena $2^{3-1} = 2^2 = 4$ tidak kongruen dengan $1 \pmod{9}$. Dengan demikian, 2 adalah suatu akar primitif modulo 3^k untuk semua bilangan bulat positif k .

- b. 3 adalah suatu akar primitif modulo 17 dan suatu akar primitif modulo 17^2 . Dengan demikian, 3 adalah suatu akar primitif modulo 17^k untuk semua bilangan bulat positif k .

Teorema 9.14

Jika a adalah suatu bilangan bulat ganjil, k adalah suatu bilangan bulat, dan $k \geq 3$ maka $a^{\phi(2^k)/2} = a^{k-2} \equiv 1 \pmod{2^k}$.

Bukti:

a adalah suatu bilangan bulat positif maka $a = 2b + 1$, b adalah suatu bilangan bulat.

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1$$

Karena salah satu dari b atau $b+1$ adalah genap maka $8 | 4b(b+1)$, dan akibatnya $a^2 \equiv 1 \pmod{8}$.

Jadi hubungan berlaku untuk $k = 3$

Misalkan hubungan berlaku untuk $n = k$, yaitu: $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, maka tentu ada suatu bilangan bulat d sehingga $a^{2^{k-2}} = 1 + d \cdot 2^k$, akibatnya

$$(a^{2^{k-2}})^2 = (1 + d \cdot 2^k)^2$$

$$a^{2^{k-1}} = 1 + 2d \cdot 2^k + d^2 \cdot 2^2 k$$

$$a^{2^{k-1}} = 1 + d \cdot 2^{k+1} + d^2 \cdot 2^2 k$$

Jadi $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$

Teorema 9.14 menjelaskan bahwa tidak ada ke pangkat dari 2, kecuali 2 dan 4, yang mempunyai suatu akar primitif. Meskipun tidak ada akar primitif modulo 2^k untuk $k \geq 3$, tetapi selalu ada suatu unsur dari tingkat kemungkinan terbesar, yaitu $\phi(2^k)/2$.

Teorema 9.15

Jika k adalah suatu bilangan bulat dan $k \geq 3$ maka $O_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}$.

Bukti:

Sesuai dengan Teorema 9.14, untuk $k \geq 3$ berlaku $5^{2^{k-2}} \equiv 1 \pmod{2^k}$, dan sesuai dengan Teorema 9.1: $O_{2^k} 5 | 2^{k-2}$.

Dengan demikian, jika kita dapat tunjukkan bahwa $O_{2^k} 5 | 2^{k-3}$, maka kita dapat simpulkan bahwa $O_{2^k} 5 = 2^{k-2}$.

Untuk menunjukkan bahwa $O_{2^k} 5 = 2^{k-3}$, kita akan gunakan induksi matematika untuk nilai-nilai $k \geq 3$.

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \pmod{2^k}$$

Untuk $k = 3$ terdapat $5 \equiv 1 + 4 \pmod{8}$.

Anggaplah bahwa $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$, maka tentu ada suatu $d \in N$ sehingga $5^{2^{k-3}} \equiv 1 + 2^{k-1} + d \cdot 2^k$, maka

$$(5^{2^{k-3}})^2 \equiv (1 + 2^{k-1} + d \cdot 2^k)^2$$

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 + 2(1 + 2^{k-1})d \cdot 2^k + (d \cdot 2^k)^2$$

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \pmod{2^{k-1}}$$

Jadi $O_{2^k} 5 = \varphi(2^k)/2$.

Berdasarkan uraian yang telah dipaparkan dapat diketahui bahwa semua perpangkatan dari bilangan prima ganjil mempunyai akar primitif, tetapi perpangkatan 2 yang mempunyai akar primitif hanya 2 dan 4.

Teorema 9.16

Jika $n \in N$ dan n bukan ke pangkat suatu bilangan prima atau dua kali ke pangkat suatu bilangan prima maka n tidak mempunyai suatu akar primitif.

Bukti:

Misalkan $n \in N$ mempunyai pemfaktoran prima $n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$ dan mempunyai suatu akar primitif r , maka $(r, n) = 1$ dan $O_n r = \phi(n)$, maka dapat ditentukan bahwa $(r, p^t) = 1$ di mana p^t adalah satu dari perpangkatan prima yang muncul pada pemfaktoran prima. Sesuai dengan teorema Euler:

$$r^{\phi(p^t)} \equiv 1 \pmod{p^t}$$

Selanjutnya, jika U adalah kelipatan persekutuan terkecil dari $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_m^{t_m})$, yaitu $U = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_m^{t_m})]$, maka $\phi(p_i^{t_i}) \mid U$, dan $r^U \equiv 1 \pmod{p_i^{t_i}}, i=1,2,\dots,m$.

Sesuai dengan Teorema Sisa Cina, dapat ditentukan bahwa $r^U \equiv 1 \pmod{n}$, akibatnya $O_n r = \phi(n) \leq U$.

Karena $\phi(n)$ adalah suatu fungsi multiplikatif maka

$$\phi(n) = \phi(p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}) = \phi(p_1^{t_1}) \cdot \phi(p_2^{t_2}) \dots \phi(p_m^{t_m}) \text{ berarti}$$

$$\phi(p_1^{t_1}) \cdot \phi(p_2^{t_2}) \dots \phi(p_m^{t_m}) \leq [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_m^{t_m})].$$

Keadaan ini bisa terjadi jika $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_m^{t_m})$ berpasangan relatif prima. Berdasarkan keadaan $\phi(p^t) = p^{t-1}(p-1)$, dapat kita tentukan bahwa $\phi(p^t)$ adalah genap jika p adalah ganjil, atau jika $p=2$ dan $t \geq 2$.

Dengan demikian, bilangan-bilangan $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_m^{t_m})$ tidak berpasangan relatif prima kecuali $m=1$ dan n adalah perpangkatan suatu bilangan prima atau $m=2$ dan $n=2p^t$, di mana p adalah suatu bilangan prima dan r adalah suatu bilangan bulat positif.

Contoh 9.18

Bilangan-bilangan bulat positif yang mempunyai suatu akar primitif mempunyai bentuk p^t atau $2p^t$ dengan p adalah suatu bilangan prima dan t adalah suatu bilangan asli. Dengan demikian, 10 dan 22 mempunyai suatu akar primitif sebab $10 = 2 \cdot 5^1$ dan $22 = 2 \cdot 11^1$.

Teorema 9.17

Jika p adalah suatu bilangan prima ganjil dan t adalah suatu bilangan asli, maka $2p^t$ mempunyai suatu akar primitif.

Jika r adalah suatu akar primitif modulo p^t dan r adalah ganjil, maka r juga suatu akar primitif modulo $2p^t$.

Jika r adalah suatu akar primitif modulo p^t dan r adalah genap, maka $r + p^t$ adalah suatu akar primitif modulo $2p^t$.

Bukti:

r adalah suatu akar primitif modulo p^t maka $r^{\phi(p^t)} \equiv 1 \pmod{p^t}$.

Selanjutnya, $\phi(2p^t) = \phi(2)\phi(p^t) = \phi(p^t)$, berarti $r^{\phi(2p^t)} \equiv 1 \pmod{p^t}$.

Jika r adalah ganjil, maka $r^{\phi(2p^t)} \equiv 1 \pmod{2}$ sehingga

$r^{\phi(2p^t)} \equiv 1 \pmod{2p^t}$ sebab $(2, p^t) = 1$, $r^{\phi(p^t)} \equiv 1 \pmod{p^t}$, dan

$r^{\phi(2p^t)} \equiv 1 \pmod{2}$, berarti $2p^t$ mempunyai suatu akar primitif.

Jika r adalah genap, maka $r + p^t$ adalah ganjil, sehingga

$$(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2}.$$

Karena $r + p^t \equiv r \pmod{p^t}$ maka

$$(r + p^t)^{\phi(2p^t)} \equiv r^{\phi(2p^t)} \pmod{p^t} \equiv 1 \pmod{p^t}.$$

Dari $(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2}$ dan $(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{p^t}$ dapat

ditentukan bahwa $(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2p^t}$ dan tidak ada ke pangkatkan lebih kecil dari $r + p^t$ yang kongruen dengan 1 modulo $2p^t$.

Jadi $r + p^t$ adalah suatu akar primitif dari $2p^t$.

Contoh 9.19

5 adalah suatu bilangan prima ganjil dan 5 adalah suatu akar primitif dari 23. Sesuai dengan Teorema 9.14, 5 atau $23 - 5 = 18$ adalah suatu akar primitif modulo 23^2 , ternyata 5 adalah juga suatu akar primitif modulo 23^k untuk sebarang bilangan bulat positif k . Karena 5 adalah ganjil maka 5 juga suatu akar primitif dari $2 \cdot 23^k$ untuk semua bilangan bulat positif k , misalnya 5 adalah suatu akar primitif dari $2 \cdot 23 = 46$.

Contoh 9.20

2 adalah suatu bilangan prima genap dan 2 adalah suatu akar primitif dari 13. Sesuai dengan Teorema 9.14, $2 + 13^k$ adalah suatu akar primitif modulo $2 \cdot 13^k$ untuk semua bilangan bulat positif k , misalnya 171 adalah suatu akar primitif modulo 338.

Teorema 9.18

Ditentukan p adalah suatu bilangan prima ganjil, t adalah suatu bilangan bulat positif, n adalah bilangan bulat positif dan $n > 1$.
 n mempunyai suatu akar primitif jika dan hanya jika $n = 2$, $n = 4$, $n = p^t$, atau $n = 2p^t$.

Buktikan dengan menggunakan gabungan teorema 9.11, 9.13, 9.16, dan 9.17.

Dari pembahasan sebelumnya, Teorema 9.4 menyatakan bahwa jika r adalah suatu akar primitif modulo m , maka $T = r^1, r^2, \dots, r^{\phi(m)}$ membentuk suatu sistem residu tereduksi modulo m .

Dengan demikian, jika $a \in Z$ dan $(a, m) = 1$, maka tentu ada suatu bilangan bulat x yang tunggal dengan $1 \leq x \leq \phi(m)$ sedemikian hingga $r^x \equiv a \pmod{m}$

Definisi 9.3

Ditentukan $m \in N$ dan r adalah suatu akar primitif dari m . Jika $a \in N$ dan $(a, m) = 1$, maka x yang tunggal, $x \in Z$, $1 \leq x \leq \phi(m)$ dan $r^x \equiv a \pmod{m}$ disebut indeks dari a terhadap basis r modulo m , ditulis $x = \text{ind}_r a$, dan dinyatakan dengan $r^{\text{ind}_r a} \equiv a \pmod{m}$, atau $a \equiv r^{\text{ind}_r a} \pmod{m}$.

Dari Definisi 9.3 dapat ditentukan hubungan bahwa:

jika $(a, m) = (b, m) = 1$ dan $a \equiv b \pmod{m}$, maka $\text{ind}_r a = \text{ind}_r b$.

Contoh 9.21

Jika $m = 7$, maka 3 adalah suatu akar primitif modulo 7 sebab $3^6 = 3^{\phi(7)} \equiv 1 \pmod{7}$. Dari keadaan $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, dan $3^6 \equiv 1 \pmod{7}$, dapat ditentukan bahwa
 $\text{ind}_3 3 = 1$, $\text{ind}_3 2 = 2$, $\text{ind}_3 6 = 3$, $\text{ind}_3 4 = 4$, $\text{ind}_3 5 = 5$, dan $\text{ind}_3 1 = 6$.

Contoh 9.22

Jika $m=11$, maka 7 adalah suatu akar primitif modulo 11 sebab $7^{10} = 3^{\phi(11)} \equiv 1 \pmod{11}$. Dari keadaan $7^1 \equiv 7 \pmod{11}$, $7^2 \equiv 5 \pmod{11}$, $7^3 \equiv 2 \pmod{11}$, $7^4 \equiv 3 \pmod{11}$, $7^5 \equiv 10 \pmod{11}$, $7^6 \equiv 4 \pmod{11}$, $7^7 \equiv 6 \pmod{11}$, $7^8 \equiv 9 \pmod{11}$, $7^9 \equiv 8 \pmod{11}$, dan $7^{10} \equiv 1 \pmod{11}$, dapat ditentukan bahwa:

$\text{ind}_7 7 = 1$, $\text{ind}_7 5 = 2$, $\text{ind}_7 2 = 3$, $\text{ind}_7 3 = 4$, $\text{ind}_7 10 = 5$, $\text{ind}_7 4 = 6$, $\text{ind}_7 6 = 7$, $\text{ind}_7 9 = 8$ dan $\text{ind}_7 1 = 10$.

Teorema 9.19

Jika r adalah suatu akar primitif modulo $m \in N$, $a \in Z$, $b \in Z$, $(a, m) = (b, m) = 1$, maka:

- $\text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$
- $\text{ind}_r (ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$
- $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$ jika $k \in N$

Bukti:

- Sesuai teorema Euler, $r^{\phi(m)} \equiv 1 \pmod{m}$. Selanjutnya, tidak ada pangkat bilangan asli dari r yang kongruen dengan 1 modulo m .

Jadi $\text{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$

- Sesuai dengan Definisi 9.3, $r^{\text{ind}_r a} \equiv a \pmod{m}$,

berarti $r^{\text{ind}_r(ab)} \equiv ab \pmod{m}$, yaitu:

$$\begin{aligned} r^{\text{ind}_r(ab)} &\equiv ab \pmod{m} \equiv r^{\text{ind}_r a} (m) \cdot r^{\text{ind}_r b} (m) \equiv r^{\text{ind}_r a} \cdot r^{\text{ind}_r b} (m) \\ &\equiv r^{\text{ind}_r a + \text{ind}_r b} (m) \end{aligned}$$

Sesuai dengan Teorema 9.3, dari hubungan $r^{\text{ind}_r(ab)} \equiv r^{\text{ind}_r a + \text{ind}_r b} (m)$ dapat ditentukan bahwa $\text{ind}_r (ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$

- Sesuai dengan Definisi 9.3, $r^{\text{ind}_r a} \equiv a \pmod{m}$, berarti

$$r^{\text{ind}_r a^k} \equiv a^k \pmod{m} \text{ dan } r^{k \cdot \text{ind}_r a} \equiv (r^{\text{ind}_r a})^k \equiv a^k \pmod{m}.$$

Dengan demikian $r^{\text{ind}_r a^k} \equiv r^{k \cdot \text{ind}_r a} \pmod{m}$, dan sesuai dengan Teorema 9.3: $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$.

Contoh 9.23

Dari Contoh 9.22 dapat kita ketahui bahwa $\text{ind}_7 5 = 2$ dan $\text{ind}_7 2 = 3$ dan $\phi(11) = 10$, maka $\text{ind}_7 10 = \text{ind}_7 2 \cdot 5 = \text{ind}_7 2 + \text{ind}_7 5 = 2 + 3 = 5 \equiv 5(\text{mod } 10)$.

Demikian pula dari $\text{ind}_7 2 = 3$ dan $\text{ind}_7 3 = 4$, dapat dicari $\text{ind}_7 6 = \text{ind}_7 2 \cdot 3 = \text{ind}_7 2 + \text{ind}_7 3 = 3 + 4 = 7 \equiv 7(\text{mod } 10)$.

Selanjutnya, dari $\text{ind}_7 5 = 2$, dapat dicari bahwa

$$\text{ind}_7 5^3 \equiv 3 \cdot \text{ind}_7 5 \pmod{10} \equiv 3 \cdot 2 \pmod{10} \equiv 6 \pmod{10}.$$

Contoh 9.24

Selesaikan $6x^{12} \equiv 11 \pmod{17}$.

Jawab:

3 adalah suatu akar primitif dari 17 sebab $3^{16} = 3^{\phi(17)} \equiv 1 \pmod{17}$. Daftar indeks bilangan-bilangan bulat 1, 2, ..., 16 terhadap basis 3 modulo 17 adalah:

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 t$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$$6x^{12} \equiv 11 \pmod{17} \text{ maka } \text{ind}_3(6x^{12}) \equiv \text{ind}_3 11 \equiv 7 \pmod{16}.$$

Selanjutnya, berdasarkan Teorema 9.19(b) dan Teorema 9.19(c) dapat ditentukan bahwa $\text{ind}_3(6x^{12}) \equiv \text{ind}_3 6 + \text{ind}_3(x^{12}) \equiv 15 + 12 \text{ ind}_3 x \pmod{16}$.

Dari $\text{ind}_3(6x^{12}) \equiv \text{ind}_3 11 \equiv 7 \pmod{16}$ dan

$\text{ind}_3(6x^{12}) \equiv 15 + 12 \text{ ind}_3 x \pmod{16}$ diperoleh:

$$15 + 12 \text{ ind}_3 x \equiv 7 \pmod{16}$$

$$12 \text{ ind}_3 x \equiv 8 \pmod{16}$$

$$3 \text{ ind}_3 x \equiv 2 \pmod{4} \text{ sebab } (12, 16) = 4 \mid 8, \text{ mempunyai } 4 \text{ solusi}$$

$$\text{ind}_3 x \equiv 2 \pmod{4}$$

Dengan demikian, $\text{ind}_3 x \equiv 2, 6, 10, 14 \pmod{16}$, berarti:

$$x \equiv 3^2, 3^6, 3^{10}, 3^{14} \pmod{17}$$

$$x \equiv 9, 15, 8, 2 \pmod{17}$$

Tugas

- 1) Carilah semua akar primitif dari 22!
- 2) Carilah semua selesaian dari kongruensi $7^x \equiv 6 \pmod{17}$.

Petunjuk Jawaban Tugas

- 1) 2 adalah suatu akar primitif dari 11 karena $2^{10} = (2^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}$ dan $\phi(11) = 10$. Sesuai dengan Teorema 9.17, 11 adalah suatu bilangan prima ganjil maka $2 \cdot 11^t$ (dengan $t = 1$) mempunyai suatu akar primitif. Dari $r = 2$ maka r adalah bilangan genap, sehingga $2 + 11 = 13$ adalah suatu akar primitif modulo $2 \cdot 11^1 = 22$.

Akar-akar primitif dari 22 adalah residu-residu positif terkecil dari 13^k di mana $1 \leq k < \phi(22) = 10$ dan $(k, \phi(22)) = (k, 10) = 1$. Bilangan-bilangan bulat itu adalah $13^1 \equiv 13 \pmod{22}$, $13^3 \equiv 19 \pmod{22}$, $13^7 \equiv 7 \pmod{22}$, dan $13^9 \equiv 17 \pmod{22}$.

Akar-akar primitif dari 22 adalah 7, 13, 17, dan 19.

- 2) $\text{ind}_3(7x) \equiv \text{ind}_3 6$.

Karena $3^{15} \equiv 6 \pmod{17}$, maka $\text{ind}_3 6 = 15 \equiv 15 \pmod{16}$

$\text{ind}_3(7^x) \equiv x \cdot \text{ind}_3 7 \equiv 11x \pmod{16}$ sebab $3^{11} \equiv 7 \pmod{17}$.

Dengan demikian, $11x \equiv 15 \pmod{16}$, $3 \cdot 11x \equiv 45 \pmod{16}$, $x \equiv 13 \pmod{16}$. Selesaian dari $7^x \equiv 6 \pmod{17}$ adalah $x \equiv 13 \pmod{16}$.

**LATIHAN** _____

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

- 1) Bilangan-bilangan mana dari 4, 10, 16, 22, dan 28 yang tidak mempunyai suatu akar primitif.
- 2) Carilah suatu akar primitif dari 3^2 , 5^2 , dan 23^2 !
- 3) Carilah suatu akar primitif modulo 18 dan modulo 26!
- 4) Carilah semua akar primitif dari 25!
- 5) Selesaikan kongruensi $3x^5 \equiv 1 \pmod{23}$.

Petunjuk Jawaban Latihan

- 1) Bilangan-bilangan yang mempunyai suatu akar primitif adalah 2, 4, dan bilangan-bilangan yang mempunyai bentuk p^t dan $2p^t$ dengan p adalah suatu bilangan prima ganjil dan t adalah suatu bilangan bulat positif. Dengan demikian, yang mempunyai suatu akar primitif adalah 4, $10 = 2 \cdot 5^1$, dan $22 = 2 \cdot 11^1$, berarti yang tidak mempunyai suatu akar primitif adalah 16 dan 28.

- 2) 2 adalah suatu akar primitif 3^2 sebab $\phi(3^2) = 6$ dan $2^6 = 64 \equiv 1 \pmod{9}$.
 2 adalah suatu akar primitif 5^2 sebab $\phi(5^2) = 20$ dan
 $2^{20} = 2^5 \cdot 2^5 \cdot 2^5 = 32 \cdot 32 \cdot 32 \cdot 32 \equiv 7 \cdot 7 \cdot 7 \cdot 7 \equiv 49 \cdot 49 \equiv (-1) \cdot (-1) \equiv 1 \pmod{25}$.
 2 adalah suatu akar primitif dari 23 sebab $\phi(23) = 22$ dan
 $2^{22} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^2 = 32 \cdot 32 \cdot 32 \cdot 32 \cdot 4 \equiv 9 \cdot 9 \cdot 9 \cdot 9 \cdot 4 \equiv 81 \cdot 81 \cdot 4 \equiv 12 \cdot 12 \cdot 4 \equiv 144 \cdot 4 \equiv 6 \cdot 4 \equiv 24 \equiv 1 \pmod{23}$, dan $2^{22} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^2 = 32 \cdot 32 \cdot 32 \cdot 32 \cdot 4 \equiv 392 \pmod{23^2}$, tidak kongruen dengan $1 \pmod{23^2}$.

- 3) $18 = 2 \cdot 9 = 2 \cdot 3^2$, dan 2 adalah akar primitif dari 9 sebab
 $2^{\phi(9)} = 2^6 \equiv 1 \pmod{3^2}$, dan sesuai dengan Teorema 9.17,
 $2 + 3^2 = 11$ adalah suatu akar primitif modulo $2 \cdot 3^2$.
 $26 = 2 \cdot 13^1$, dan 2 adalah akar primitif dari 13 sebab
 $2^{\phi(13)} = 2^{12} \equiv 40 \equiv 1 \pmod{13}$, dan sesuai Teorema 9.17,
 $2 + 13^1 = 2 + 13 = 15$ adalah suatu akar primitif modulo $2 \cdot 13^1$.

- 4) 2 adalah akar primitif dari 25 sebab
 $2^{\phi(25)} = 2^{20} = 2^5 \cdot 2^5 \cdot 2^5 = 7 \cdot 7 \cdot 7 \cdot 7 \equiv 1 \pmod{25}$, dan sesuai dengan Teorema 9.7, banyaknya semua akar primitif yang tidak kongruen adalah $\phi(\phi(m)) = \phi(\phi(25)) = \phi(20) = 8$, yaitu mempunyai bentuk r^k dengan $(k, \phi(m)) = 1$, yaitu $(k, 20) = 1$, berarti $k = 1, 3, 7, 9, 11, 13, 17$, dan 19 . Dengan demikian, akar-akar primitif dari 25 adalah $2^1, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}$, dan 2^{19} , atau $2, 8, 3, 12, 23, 17, 22$, dan 13 modulo 25.

- 5) 5 adalah akar primitif terkecil modulo 23 sebab $5^{22} \equiv 5^{\phi(23)} \equiv 1 \pmod{23}$

Dari $3x^5 \equiv 1 \pmod{23}$ dapat ditentukan bahwa $\text{ind}_5 3x^5 \equiv \text{ind}_5 1 \pmod{22}$

dan sesuai Teorema 9.19 (b) dan (c),

$\text{ind}_5 3 + 5\text{ind}_5 x \equiv \text{ind}_5 1 \pmod{22}$. Misalkan, $y = \text{ind}_5 x$, maka

$\text{ind}_5 3 + 5y \equiv \text{ind}_5 1 \pmod{22}$. Karena $5^{16} \equiv 3 \pmod{23}$ dan

$5^{22} \equiv 1 \pmod{23}$, maka dapat ditentukan bahwa $\text{ind}_5 3 = 16$ dan

$\text{ind}_5 1 = 22$, sehingga $16 + 5y \equiv 22 \pmod{22}$. Selesaian kongruensi linier

$16 + 5y \equiv 22 \pmod{22}$ adalah $y \equiv 10 \pmod{22}$. Dengan demikian, dari

$y = \text{ind}_5 x$ dapat ditentukan $5^{10} \equiv x \pmod{23}$, berarti $x \equiv 9 \pmod{23}$.



RANGKUMAN

Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini maka garis besar bahan yang dibahas meliputi Definisi, Teorema, Contoh, dan Latihan tentang eksistensi akar-akar primitif dan indeks aritmetika, terutama jika dikaitkan dengan bilangan prima ganjil, fungsi ϕ -Euler dan penyelesaian kongruensi khusus bentuk pangkat.

1. Definisi 9.3

Ditentukan $m \in N$ dan r adalah suatu akar primitif dari m . Jika $a \in N$ dan $(a,m)=1$, maka x yang tunggal, $x \in Z$, $1 \leq x \leq \phi(m)$, dan $r^x \equiv a \pmod{m}$ disebut indeks dari a terhadap basis r modulo m , ditulis $x = \text{ind}_r a$, dan dinyatakan dengan $r^{\text{ind},a} \equiv a \pmod{m}$ atau $a \equiv r^{\text{ind},a} \pmod{m}$.

2. Teorema 9.12

Jika p adalah suatu bilangan prima ganjil dengan akar primitif a maka salah satu dari a atau $a+p$ merupakan suatu akar primitif modulo p^2 .

3. Teorema 9.13

Jika p adalah suatu bilangan prima ganjil maka p^r mempunyai suatu akar primitif untuk semua $r \in N$, dan jika s adalah suatu akar primitif modulo p^2 , maka s adalah suatu akar primitif modulo p^r untuk semua $r \in N$.

4. Teorema 9.14

Jika a adalah suatu bilangan bulat ganjil, k adalah suatu bilangan bulat dan $k \geq 3$, maka $a^{\phi(2^k)/2} = a^{k-2} \equiv 1 \pmod{2^k}$.

5. Teorema 9.15

Jika k adalah suatu bilangan bulat dan $k \geq 3$ maka $O_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}$.

6. Teorema 9.16

Jika $n \in N$ dan n bukan ke pangkat suatu bilangan prima atau dua kali ke pangkat suatu bilangan prima maka n tidak mempunyai suatu akar primitif.

7. Teorema 9.17

Jika p adalah suatu bilangan prima ganjil dan t adalah suatu bilangan asli, maka $2p^t$ mempunyai suatu akar primitif.

Jika r adalah suatu akar primitif modulo p^t dan r adalah ganjil, maka r juga suatu akar primitif modulo $2p^t$.

Jika r adalah suatu akar primitif modulo p^t dan r adalah genap maka $r + p^t$ adalah suatu akar primitif modulo $2p^t$.

8. Teorema 9.18

Ditentukan p adalah suatu bilangan prima ganjil, t adalah suatu bilangan bulat positif, n adalah bilangan bulat positif dan $n > 1$. n mempunyai suatu akar primitif jika dan hanya jika $n = 2$, $n = 4$, $n = p^t$, atau $n = 2p^t$.

9. Teorema 9.19

Jika r adalah suatu akar primitif modulo $m \in N$, $a \in Z$, $b \in Z$, $(a, m) = (b, m) = 1$ maka:

$$(a) \text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$$

$$(b) \text{ind}_r (ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$$

$$(c) \text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)} \text{ jika } k \in N$$

TES FORMATIF 2

1) Skor : 10

Dari bilangan-bilangan 8, 9, 12, 26, 27, 31, dan 33, sebutkan yang mempunyai suatu akar primitif.

2) Skor : 20

Carilah semua akar primitif dari 38.

3) Skor : 10

Tunjukkan bahwa banyaknya akar primitif modulo $2p^t$ sama dengan banyaknya akar primitif modulo p^t , p adalah suatu bilangan prima ganjil, dan $t \in N$.

4) Skor : 20

Selesaikan kongruensi $3x^{14} \equiv 2 \pmod{23}$.

5) Skor : 20

Carilah nilai-nilai a sedemikian hingga $ax^4 \equiv 2 \pmod{13}$ dapat diselesaikan.

6) Skor : 10

Tunjukkan bahwa jika p adalah suatu bilangan prima ganjil, dan r adalah suatu akar primitif dari p maka $\text{ind}_r(p-1) = (p-1)/2$.

7) Skor : 10

Diketahui p adalah suatu bilangan prima ganjil. Tunjukkan bahwa kongruensi $x^4 \equiv -1 \pmod{p}$ mempunyai selesaian jika dan hanya jika p mempunyai bentuk $8k+1$.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah skor jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Skor Jawaban yang Benar}}{100} \times 100\%$$

Arti tingkat penguasaan: 90 - 100% = baik sekali

80 - 89% = baik

70 - 79% = cukup

< 70% = kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat mengikuti Ujian Akhir Semester (UAS). **Selamat!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

- 1) a. $7^4 = 7^2 \cdot 7^2 = 49 \cdot 49 \equiv 4 \cdot 4 \pmod{15} \equiv 1 \pmod{15}$, maka $O_{15}7 = 4$.
 b. $9^2 = 81 \equiv 1 \pmod{20}$, maka $O_{20}9 = 2$.
 c. $10^6 = 10^2 \cdot 10^2 \cdot 10^2 \equiv 16 \cdot 16 \cdot 16 \pmod{21} \equiv (-5)(-5)(-5) \pmod{21} \equiv 1 \pmod{21}$ maka, $O_{21}10 = 6$.
 d. $3^{28} = 3^{14} \cdot 3^{14} \equiv (-1)(-1) \pmod{29} \equiv 1 \pmod{29}$, maka $O_{29}3 = 28$.
 e. $9^8 = 9^4 \cdot 9^4 \equiv (-1)(-1) \equiv 1 \pmod{17}$ maka $O_{17}9 = 5$.
- 2) a. $\phi(5) = 4$ dan $2^4 = 16 \equiv 1 \pmod{5}$,
 jadi 2 adalah suatu akar primitif 5.
 b. $\phi(13) = 12$, $26 \equiv 1 \pmod{13}$, atau $2^{12} \equiv 1 \pmod{13}$,
 jadi 2 adalah akar primitif 13.
 c. $\phi(14) = 6$, dan $3^6 = 3^3 \cdot 3^3 \equiv (-1)(-1) \pmod{14} \equiv 1 \pmod{14}$,
 jadi 3 adalah akar primitif 14.
 d. $\phi(18) = 12$, dan $2^{12} \equiv 1 \pmod{18}$, jadi 2 adalah akar primitif 18.
 e. $\phi(20) = 8$, dan $34 = 81 \equiv 1 \pmod{20}$, jadi 3 adalah akar primitif 20.
- 3) a. Bilangan-bilangan yang relatif prima dengan 12 adalah 1, 5, 7, dan 11
 $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$ berarti $O_{12}1 = O_{12}5 = O_{12}7 = O_{12}11 = 2 \neq \phi(12) = 4$, jadi 12 tidak mempunyai akar primitif.
 b. Bilangan-bilangan yang relatif prima dengan 20 adalah 1, 3, 7, 9, 11, 13, 17, 19.
 $\phi(20) = 8$ dan pembagi murni dari 8 adalah 1, 2, dan 4.
 Ternyata $1^4 \equiv 3^4 \equiv 7^4 \equiv 9^4 \equiv 11^4 \equiv 13^4 \equiv 17^4 \equiv 19^4 \equiv 1 \pmod{20}$,
 berarti $O_{20}1, 3, 7, 9, 11, 13, 17, 19 = 4 \neq \phi(20) = 8$, jadi 20 tidak mempunyai akar primitif.
- 4) Misalkan $O_m a = p$, $O_m b = q$, dan $O_m ab = r$ maka $a^p \equiv 1 \pmod{m}$,
 $b^q \equiv 1 \pmod{m}$ dan $(ab)^r \equiv 1 \pmod{m}$, sehingga

$(ab)^{pq} \equiv (a^p)^q \cdot (b^p)^p \equiv 1^q \cdot 1^p \equiv 1 \pmod{m}$, berarti dapat ditentukan bahwa $r \mid pq$. Selanjutnya, $1 \equiv (ab)^r \equiv (ab)^{pr} \equiv (a^p)^r \cdot b^{pt} \equiv b^{pr} \pmod{m}$, dan sesuai dengan Teorema 9.1, $q \mid pr$, akibatnya $q \mid r$ sebab $(q, p) = 1$. Dengan jalan yang sama dapat ditentukan bahwa $p \mid r$. Berikutnya, dari $p \mid r, q \mid r$, dan $(p, q) = 1$ (yaitu diketahui $(O_m a, O_m b) = (p, q) = 1$) dapat ditentukan bahwa $pq = r$.

- 5) $(a, m) = 1$ dan $O_m a = pq$, maka $a^{pq} \equiv 1 \pmod{m}$. Dengan demikian, dapat ditentukan bahwa $a^{pq} = (a^p)^q \equiv 1 \pmod{m}$, yaitu $O_m a^p = q$.
- 6) Misalkan bahwa m adalah bukan bilangan prima maka $\phi(m) < m - 1$.

Sesuai dengan Teorema 9.2, $O_m a \mid \phi(m)$, berarti $O_m a < m - 1$, yaitu jika ada suatu bilangan bulat a yang relatif prima dengan m sehingga $O_m a = m - 1$, maka m adalah prima.

- 7) Jika pq adalah suatu prima semu dengan basis 2, maka $2^{pq} \equiv 2 \pmod{pq}$, dan berdasarkan keadaan $p \mid pq$, berakibat $2^{pq} \equiv 2 \pmod{q}$. Sesuai dengan Teorema Sisa Cina, didasarkan pada keadaan p dan q adalah bilangan-bilangan prima ganjil maka tentu ada selesaian dari sistem kongruensi linear simultan $x \equiv 2 \pmod{p}$ dan $x \equiv 2 \pmod{q}$. Selanjutnya, 2 dan 2^{pq} adalah selesaian, maka $2 \equiv 2^{pq} \pmod{pq}$, berarti pq adalah prima semu basis 2.
- Sebaliknya, pq adalah prima semu basis 2 maka $2^{pq} \equiv 2 \pmod{pq}$ dan $2^{pq} \equiv 2 \pmod{p}$.

Sesuai dengan Teorema Kecil Fermat, $2^p \equiv 2 \pmod{p}$, sehingga $(2^p)^2 \equiv 2^q \equiv 2 \pmod{p}$.

Selanjutnya, dari $(2, p) = 1$ dapat ditentukan $2^{q-1} \equiv 1 \pmod{p}$, berarti $O_p 2 \mid (q-1)$. Dengan jalan yang sama, $O_q 2 \mid (p-1)$.

Berikutnya, 19.73 adalah prima semu, sedangkan 13.67 bukan prima semu.

Tes Formatif 2

- 1) Sesuai dengan Teorema 9.18, bilangan-bilangan yang mempunyai suatu akar primitif mempunyai bentuk p^t atau $2p^t$, p adalah bilangan prima ganjil, $t \in N$, dan $t > 1$.

Dengan demikian, bilangan-bilangan yang mempunyai suatu akar primitif adalah: $9 = 3^2$, $26 = 2 \cdot 13^1$, $27 = 3^3$, dan $31 = 31^1$.

- 2) 3 adalah akar primitif dari 38 sebab

$3^{\phi(38)} = 3^{18} = 3^9 \cdot 3^9 \equiv (-1)(-1) \equiv 1 \pmod{38}$, dan sesuai dengan Teorema 9.7, banyaknya semua akar primitif yang tidak kongruen adalah $\phi(\phi(m)) = \phi(\phi(38)) = \phi(18) = 6$, yaitu mempunyai bentuk r^k dengan $(k, \phi(m)) = 1$, yaitu $(k, 18) = 1$, berarti $k = 1, 5, 7, 11, 13$, dan 17.

Dengan demikian, akar-akar primitif dari 25 adalah $3^1, 3^5, 3^7, 3^{11}, 3^{13}$, dan 3^{17} , atau 3, 15, 21, 29, 33, dan 13 modulo 38.

$$\begin{aligned} 3) \quad \phi(\phi(p^t)) &= \phi\left\{ p^t \left(1 - \frac{1}{p}\right)\right\} = \phi\left\{ p^{t-1}(p-1)\right\} = \phi(p^t - p^{t-1}) \\ \phi(\phi(2p^t)) &= \phi\left\{ 2p^t \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p}\right)\right\} = \phi\left\{ 2p^t \frac{1}{2} \frac{p-1}{p}\right\} = \phi(p^t - p^{t-1}) \end{aligned}$$

- 4) 5 adalah akar primitif terkecil modulo 23 sebab $5^{22} \equiv 5^{\phi(23)} \equiv 1 \pmod{23}$

Dari $3x^{14} \equiv 2 \pmod{23}$, dapat ditentukan bahwa

$\text{ind}_5(3x^{14}) \equiv \text{ind}_5 2 \pmod{22}$, dan sesuai Teorema 9.19 (b) dan (c), $\text{ind}_5 3 + 14 \text{ ind}_5 x \equiv \text{ind}_5 2 \pmod{22}$.

Misalkan $y = \text{ind}_5 x$, maka $\text{ind}_5 3 + 14 y \equiv \text{ind}_5 2 \pmod{22}$. Karena $5^{16} \equiv 3 \pmod{23}$ dan $5^2 \equiv 2 \pmod{23}$, maka dapat ditentukan bahwa $\text{ind}_5 3 = 16$ dan $\text{ind}_5 2 = 2$, sehingga $16 + 14y \equiv 2 \pmod{22}$.

Selesaian kongruensi linier $16 + 14y \equiv 2 \pmod{22}$ adalah $y \equiv 10, 21 \pmod{22}$.

Dengan demikian, dari $y = \text{ind}_5 x$ dapat ditentukan $5^{10} \equiv x \pmod{23}$, berarti $x \equiv 9 \pmod{23}$, atau $5^{21} \equiv x \pmod{23}$, berarti $x \equiv 14 \pmod{23}$.

- 5) $ax^4 \equiv 2 \pmod{13}$ maka $\text{ind}_2(ax^4) \equiv \text{ind}_2 2 \pmod{12}$

$\text{ind}_2 a + 4 \text{ ind}_2 x \equiv \text{ind}_2 2 \pmod{12}$. Karena $2^1 \equiv 2 \pmod{23}$, maka $\text{ind}_2 2 = 1$, sehingga $\text{ind}_2 a + 4 \text{ ind}_2 x \equiv 1 \pmod{12}$ atau $4 \text{ ind}_2 x \equiv 1 - \text{ind}_2 a \pmod{12}$.

Kongruensi ini dapat diselesaikan jika $(4, 12) = 4 \mid 1 - \text{ind}_2 a$, yaitu jika $\text{ind}_2 a = 1, 5, 9$ atau jika $a \equiv 2^1 \pmod{23}$, $a \equiv 2^5 \pmod{23}$, atau

$a = 2^9 \pmod{23}$. Jadi, kongruensi dapat diselesaikan jika nilai-nilai a adalah $a \equiv 2, 5, 6 \pmod{13}$.

- 6) r adalah suatu akar primitif dari p , maka $(r^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$. Karena $r^{\frac{p-1}{2}}$ tidak kongruen $1 \pmod{p}$, maka $r^{\frac{p-1}{2}} \equiv -1 \equiv p-1 \pmod{p}$.

$$\text{Jadi } \text{ind}_r(p-1) = \frac{p-1}{2}.$$

- 7) $x^4 \equiv -1 \pmod{p}$ maka $\text{ind}_r x^4 \equiv \text{ind}_2 \{-1 \pmod{p}\}$, berarti:

$$4 \text{ind}_r x \equiv \frac{p-1}{2} \pmod{\phi(p)}. \text{ Dengan demikian, } 4 \mid \frac{p-1}{2}, \text{ atau}$$

$$p-1 = 2 \cdot 4 \cdot k, \text{ berarti } p = 8k+1.$$

Daftar Pustaka

- Agnew, J. (1972). *Exploration in Number Theory*. Belmont: Brooks/Cole.
- Anderson, J.A. and Bell, J.M. (1977). *Number Theory with Applications*. New Jersey: Prentice-Hall.
- Niven, I., Zuckerman, H.S., and Montgomery, H.L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons.
- Ore, O. (1948). *Number Theory and Its History*. New York: McGraw-Hill.
- Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.
- Rosen, K.H. (1993). *Elementary Number Theory and Its Applications*. Massachusetts: Addison-Wesley.