TEORI BILANGAN

Universitas Muhammadiyah Kotabumi

ISBN 978-623-94801-3-4

TEORI BILANGAN

Ratih Handayani, S.Pd.,M.Pd.
Yulina, S.Kom.,MMSI.

TEORI BILANGAN

Dilengkapi Dengan Soal-Soal Non-Rutin

Ratih Handayani, S.Pd.,M.Pd.
Yulina, S.Kom.,MMSI.

TEORI BILANGAN

Dilengkapi dengan Soal-Soal Non Rutin

Ratih Handayani

Yulina

Universitas Muhammadiyah Kotabumi

TEORI BILANGAN
Dilengkapi dengan Soal-soal Non Rutin

Penulis:
Ratih Handayani
Yulina

Editor:
Dr. Sumarno, M.Pd.
Dr. Purna Bayu Nugroho,M.Pd.

Design Cover dan Tata Letak:
Martia Dwi Puspita Sari

ISBN: 9786239480134

Cetakan 1: Oktober 2020

Penerbit: Universitas Muhammadiyah Kotabumi

Alamat Redaksi:
Gedung C Universitas Muhammadiyah Kotabumi.
Jalan Hasan Kepala Ratu No.1052 Sindang Sari
Lampung Utara
Email: perpus@umko.ac.id
Website: www.umko.ac.id

Kata Pengantar

Alhamdulillah, Segala Puji bagi Allah SWT atas berkat Rahmat Nya penulis dapat menyelesaikan buku yang berjudul "Teori Bilangan". Buku ini dilengkapi dengan soal-soal non rutin. Penulisan buku ini bertujuan untuk menghasilkan bahan ajar teori bilangan yang sesuai dengan karakteristik mahasiswa universitas muhammadiyah kotabumi juga sesuai dengan karakteristik materi teori bilangan yang banyak memuat definisi, konsep, dan teorema.

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, sehingga buku ini dapat terselesaikan tepat waktu dan dapat digunakan sebagaimana mestinya. Penulis berharap buku ini dapat bermanfaat bagi mahasiswa program studi pendidikan matematika di universitas muhammadiyah kotabumi khususnya dan bagi pecintailmu pengetahuan pada umumnya. Penulis juga menerima saran dan kritik dari pembaca guna pengembangan buku ini secara berkelanjutan.

Kotabumi, September 2020

Penulis

DAFTAR ISI

BAB I
BILANGAN BULAT

A. Bilangan Bulat

Bilangan bulat adalah biangan yang terdiri dari bilangan asli, bilangan nol, dan bilangan negatif. Bilangan sebagai konsep abstrak mulai dipikirkan sejak periode sejarah, sekitar tahun 400 S.M. Permulaan perkembangan matematika berasal dari suku-suku yang tinggal disepanjang aliran sungai. Berbagai kegiatan praktis yang mereka lakukan membutuhkan bilangan-bilangan. Misalnya pada saat mereka menyebut tiga batu, tiga ranting, atau tiga binatang.

Pernyataan tersebut mempunyai sifat persekutuan yaitu suatu kuantitas yang disebut tiga. Keperluan tentang kuantitas merupakan kebutuhan dasar manusia dalam berkeluarga dan bermasyarakat, terutama untuk menghitung atau mencacah dan membandingkan jumlah barang atau benda. Keperluan ini mendorong orang untuk mencari cara yang mudah antara lain dengan membuat lambang bilangan dan cara aturan penggunaannya atau sistem numerasi. Sistem numerasi adalah pembuatan sekumpulan lambang dasar dan sejumlah aturan untuk menghasilkan lambang-lambang bilangan yang lain.

Dengan demikian telah ditemukan konsep bilangan asli dan lambang untuk menyatakan konsep bilangan asli yaitu 1,2,3,4,... . Untuk selanjutnya himpunan bilangan asli dinyatakan dengan $N = \{1,2,3,4, \dots\}$

Masyarakat pada zaman pertanian hanya memerlukan kegiatan untuk mencacah, menjumlah, dan mengalikan. Tetapi seiring dengan perkembangan zaman, masyarakat memerlukan sistem bilangan yang dapat memenuhi keperluan lain, yaitu mengurangkan dan membagi.

Misalnya pada saat proses menghitung hewan ternak yang tersisa setelah ada yang mati atau ketika dimakan oleh hewan buas lainnya.

Jika sebelumnya mereka menerima pernyataan tanpa bukti (postulat) jika p dan q adalah bilangan asli, maka $p + q$ adalah bilangan asli pula. Kesulitan akan muncul ketika melakukan operasi pengurangan. Pada awalnya mereka akan memahami bahwa jika mereka menggembala 3 domba, kemudian 2 ekor dimangsa hewan liar maka akan tersisa 1 ekor. Secara lambang bilangan akan ditulis $3 - 2 = 1$. Begitupun dengan $4 - 3 = 1$; $5 - 4 = 1$dan mulai bertanya, bagaimana menuliskan lambang bilangannya jika mereka menggembala 3 domba, kemudian semuanya dimangsa hewan liar yaitu jika $3 - 3 =?$, begitupun dengan $4 - 4 =?, 5 - 5 =?$

Pertanyaan-pertanyaan ini dapat dijawab jika mereka menambahkan bilangan baru, yang kemudian disebut dengan nol (0). Sekarang kita tambahkan unsur baru 0 kedalam sistem bilangan asli sehingga terbentuk himpunan baru yang disebut dengan himpunan bilangan cacah, dan dinyatakan dengan $W = \{0,1,2,3,4, \dots\}$

Dengan berkembangnya masyarakat industri, orang akan memerlukan bilangan baru untuk keperluan tabungan dan pinjaman, dll. Pertanyaan yang muncul adalah berapakah $6 - 7 =?, 8 - 10 =?$ Jawaban terhadap pertanyaan tersebut adalah tambahan bilangan-bilangan baru yang kemudian dilambangkan dengan $-1, -2, -3, -4, \dots$ Sehingga diperoleh himpunan baru yang disebut himpunan bilangan bulat dan dinyatakan dengan $Z = \{\dots, -3, -2, -1,0,1,2,3, \dots\}$

B. Sistem Bilangan Bulat

Untuk keperluan menghitung, kita dapat melakukan penjumlahan, pengurangan, perkalian, dan pembagian bilangan. Kegiatan tersebut sebagai suatu operasi. Operasi adalah mengambil sepasang bilangan untuk mendapatkan bilangan lain yang tunggal.

Definisi 1
Suatu sistem matematika adalah sebuah himpunan dengan satu atau lebih operasi biner yang terdefinisi pada himpunan itu.
Definisi 2
Operasi biner adalah suatu aturan yang menetapkan dua elemen dari suatu himpunan bilangan menjadi elemen lain yang tunggal dan berada dihimpunan tersebut.
Definisi 3
Notasi Suatu sistem matematika yang terdiri dari himpunan S dan operasi * pada S adalah ditunjukkan dengan (S,*). Jika # adalah operasi kedua pada S, maka (S,*,#) adalah sistem matematika yang terdiri dari himpunan S, operasi pertama *, dan operasi kedua #.

Sifat-Sifat Operasi

Definisi 4
Misalkan S adalah suatu himpunan. Ditentukan bahwa * adalah suatu operasi pada S.
Operasi * disebut bersifat Tertutup, jika untuk setiap $p \in S, q \in S$ berlaku $p * q \in S$

Definisi 5
Misalkan S adalah suatu himpunan. Ditentukan bahwa * adalah suatu operasi pada S.
Operasi * disebut bersifat Komutatif, jika untuk setiap $p \in S, q \in S$ berlaku $p * q = q * p$

Definisi 6
Misalkan S adalah suatu himpunan. Ditentukan bahwa * adalah suatu operasi pada S.

Operasi * disebut bersifat Asosiatif, jika untuk setiap $p, q, r \in S$ berlaku $p * (q * r) = (p * q) * r$

Definisi 7

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

Operasi * disebut bersifat Memiliki unsur identitas, jika untuk setiap $p \in S$ ada $i \in S$ sehingga $p * i = i * p = p$.

i disebut unsur identitas dari operasi *

Definisi 8

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

Operasi * disebut bersifat Memenuhi sifat inversi (invertibel), jika untuk setiap $p \in S$, ada $x \in S$ sehingga $p * x = x * p = i$.

x disebut invers dari p, dan p disebut invers dari x

Definisi 9

Misalkan S adalah suatu himpunan. Ditentukan bahwa * adalah suatu operasi pertama dan # adalah suatu operasi kedua pada himpunan S. operasi * bersifat distributive terhadap # jika

$p * (q \# r) = (p * q) \# (p * r)$ untuk setiap $p, q, r \in S$

Definisi 10

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:

a. $5 > 4$ sebab ada bilangan bulat positif 1 sehingga $5 - 4 = 1$
b. $2 < 7$ sebab ada bilangan bulat positif 5 sehingga $7 - 2 = 5$

Dua sifat dasar tentang urutan bilangan bulat yang perlu dipahami.

1. Ketertutupan bilangan bulat positif;
   $p + q$ dan pq adalah bilangan-bilangan bulat positif untuk setiap bilangan-bilangan bulat positif p dan q
2. Hukum Trikotomi;
   Untuk setiap $p \in Z$ berlaku salah satu dari $p > 0, p = 0$, atau $p < 0$

Contoh 2:

Buktikan jika $p < q$ dan $r > 0$, maka $pr < qr$

Bukti:

$p < q$	(Diketahui)
$q - p > 0$	(menurut definisi 4)
$r(q - p) > 0$	(diketahui $r > 0$,menurut sifat ketertutupan bil.bulat positif)
$rq - rp > 0$	(menurut sifat distributif)
$rp < rq$	(menurut definisi 4)
$pr < qr$	(sifat komutatif)

Terbukti

Definisi 11

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

Ingat kembali:
- $f(x) = [x]$ disebut dengan fungsi bilangan bulat terbesar kurang dari atau sama dengan x
- $g(x) = [x]$ disebut dengan fungsi bilangan bulat terkecil lebih dari atau sama dengan x

Contoh 3:

a. $\left\lfloor \frac{2}{3} \right\rfloor = 0$

b. $\left\lfloor \frac{2}{3} \right\rfloor = 1$

c. $\left\lfloor \frac{7}{3} \right\rfloor = 2$

d. $\left\lfloor -\frac{7}{3} \right\rfloor = -3$

e. $\left\lceil -\frac{7}{3} \right\rceil = -2$

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
- k disebut unsur terkecil dari himpunan S jika k kurang dari atau sama dengan x untuk semua $x \in S$ atau $k \leq x, \forall x \in S$ dan $k \in N$

Contoh 4:

a. $S = \{2,5,7\}$ mempunyai unsur terkecil 2, sebab $2 \leq x$, untuk semua $x \in S$ yaitu $2 \leq 2, 2 \leq 5, 2 \leq 7$

b. $M = \{3\}$ mempunyai unsur terkecil 3 sebab $3 \leq x$, untuk semua $x \in S$ yaitu $3 \leq 3$

Contoh 5:

a. $S = \{2,5,7\}$ adalah himpunan yang terurut rapi sebab setiap himpunan bagian dari S yang tidak kosong, yaitu

$\{2\}$ mempunyai unsur terkecil 2;

$\{5\}$ mempunyai unsur terkecil 5;

$\{7\}$ mempunyai unsur terkecil 7;

$\{2,5\}$ mempunyai unsur terkecil 2;

$\{2,7\}$ mempunyai unsur terkecil 2;

{5,7} mempunyai unsur terkecil 5;
{2,5,7} mempunyai unsur terkecil 2.

b. Z^+ adalah himpunan 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 $\{0, -1, -2, -3, \dots\}$

Latihan 1

Apakah sifat-sifat pada definisi berlaku pada himpunan bilangan bulat Z untuk operasi:

a. penjumlahan
b. pengurangan
c. perkalian
d. pembagian

Tugas:

1. Jika $a, b \in Z, a < b, c > 0$, maka buktikan bahwa $ac < bc$
2. Tentukan apakah himpunan –himpunan berikut terurut rapi
   a. $A = \{-2,3,4\}$
   b. Himpunan bilangan bulat negative
   c. Himpunan bilangan cacah
3. Carilah nilai dari
   a. $[0,12]$
   b. $\left[5\frac{2}{3}\right]$
   c. $\left[-1\frac{3}{5}\right]$

C. Prinsip Dasar Induksi Matematika

Salah satu prinsip dasar dalam matematika adalah induksi matematik. Induksi matematik merupakan salah satu metode pembuktian dari banyak teorema dalam teori bilangan maupun **dalam** matematika lainnya. Induksi matematik menjadi salah satu argument pembuktian suatu teorema atau pernyataan matematika yang semesta pembicaraan nya adalah himpunan bilangan asli. Dalam prinsip induksi matematik sering melibatkan notasi jumlah dan notasi kali. Kedua notasi ini digunakan untuk menyederhanakan tulisan sehingga menjadi lebih singkat dan mudah dipahami.

Notasi Jumlah dan Notasi Kali

Notasi jumlah adalah notasi yang dilambangkan dengan Σ (baca: *Sigma*) dan didefinisikan sebagai

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

Notasi kali adalah notasi yang dilambangkan dengan Π (baca: *Pi*) dan didefinisikan sebagai

$$\prod_{i=1}^{r} x_i = x_1 . x_2 . \ldots . x_r$$

Huruf I dari indeks notasi disebut variabel dummy karena dapat diganti oleh sebarang huruf, missal

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

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

$i = 1$ disebut batas bawah
r disebut batas atas

Indeks i tidak harus dimulai dari 1, artinya dapat dimulai dari bilangan bulat selain 1 asalkan batas bawah tidak melebihi batas atas.

Contoh 6:

$$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15$$

$$\sum_{i=3}^{6} i = 3 + 4 + 5 + 6 = 18$$

$$\sum_{j=1}^{4} 3 = 3 + 3 + 3 + 3 = 13$$

$$\sum_{k=2}^{4} (2k + 1) = (2.2 + 1) + (2.3 + 1) + (2.4 + 1) = 5 + 7 + 9 = 21$$

$$\sum_{t=1}^{3} t^2 = 1^2 + 2^2 + 3^2 = 1 + 4 + 9 = 14$$

$$\prod_{i=1}^{5} i = 1.2.3.4.5 = 120$$

$$\prod_{i=3}^{6} i = 3.4.5.6 = 360$$

$$\prod_{j=1}^{4} 3 = 3.3.3.3 = 81$$

$$\prod_{k=2}^{4}(k-1) = (2-1).(3-1).(4-1) = 1.2.3 = 6$$

$$\prod_{t=2}^{4} 2^t = 2^2.2^3.2^4 = 4.8.16 = 512$$

Sifat Notasi Jumlah:

Satu:

$$\sum_{i=r}^{s} kx_i = kx_r + kx_{r+1} + kx_{r+2} + \cdots + kx_s$$

$$= k(x_r + x_{r+1} + x_{r+2} + \cdots + x_s) = k\sum_{i=r}^{s} x_i$$

Dua:

$$\sum_{i=r}^{s}(x_i + y_i) = (x_r + y_r) + (x_{r+1} + y_{r+1}) + \cdots + (x_s + y_s)$$

$$= x_r + y_r + x_{r+1} + y_{r+1} + \cdots + x_s + y_s$$
$$= x_r + x_{r+1} + \cdots + x_s + y_r + y_{r+1} + \cdots + y_s$$
$$= (x_r + x_{r+1} + \cdots + x_s) + (y_r + y_{r+1} + \cdots + y_s)$$

$$= \sum_{i=r}^{s} x_i + \sum_{i=r}^{s} y_i$$

Tiga:

$$\sum_{i=a}^{b}\sum_{j=c}^{d} x_i y_j = \sum_{i=a}^{b}\left(x_i \sum_{j=c}^{d} y_j\right) = \sum_{i=a}^{b} x_i\,(y_c + y_{c+1} + \cdots + y_d)$$
$$= x_a(y_c + y_{c+1} + \cdots + y_d)$$
$$+ x_{a+1}(y_c + y_{c+1} + \cdots + y_d) + \cdots$$
$$+ x_b(y_c + y_{c+1} + \cdots + y_d)$$
$$= (x_a + x_{a+1} + \cdots + x_b)(y_c + y_{c+1} + \cdots + y_d)$$
$$= \left(\sum_{i=a}^{b} x_i\right)\left(\sum_{j=c}^{d} y_i\right)$$

Empat:

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

Prinsip Induksi Matematik

$1 + 2 + 3 + 4 + \cdots + n = \frac{1}{2}n(n+1)$; untuk setiap bilangan asli n.

Benarkah pernyataan tersebut?

Untuk menjawab pertanyaan di atas, dapat dilakukan dengan cara mensubstitusikan (mengganti) n dalam pernyataan itu dengan sebarang bilangan asli.

Misal $n = 1$, maka pernyataannya menjadi $1 = \frac{1}{2}.1.(1+1)$ yaitu $1 = 1$. Pernyataan benar.

Misal $n = 2$, maka pernyataan menjadi $1 + 2 = \frac{1}{2}.2.(2 + 1)$ yaitu $3 = 3$. Pernyataan benar.

Misal $n = 3$, maka pernyataan menjadi $1 + 2 + 3 = \frac{1}{2}.3.(3 + 1)$ yaitu $6 = 6$. Pernyataan benar.

Kalian dapat melanjutkan untuk $n = 4{,}5, dst$ dan akan selalu memperoleh pernyataan yang benar.

Apakah dengan memberi beberapa Contoh tersebut sudah memberikan bukti tentang kebenaran pernyataan tersebut?

Jawabannya adalah **BELUM.**

Dalam matematika, pemberian beberapa contoh seperti itu **BUKAN** merupakan bukti dari kebenaran suatu pernyataan yang berlaku dalam himpunan semestanya.

Jika kita dapat memberikan contoh **SETIAP** bilangan asli n pada pertanyaan tersebut dan masing-masing mendapatkan pernyataan yang benar, maka hal tersebut dapat menjadi bukti kebenaran dari pernyataan tersebut.

Tetapi hal ini tidak efisien dan tidak mungkin dilakukan, karena banyaknya anggota himpunan bilangan asli banyaknya tak berhingga.

Lalu bagaimana cara membuktikan pernyaan tersebut?

Dengan menggunakan **Induksi Matematik**

Langkah-langkah pembuktian dengan induksi matematik adalah sebagai berikut.

Misalkan $p(n)$ adalah suatu pernyataan yang akan dibuktikan kebenarannya untuk setiap bilangan asli n. Maka

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

Langkah 2: diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k dan

Ditunjukkan bahwa $p(k + 1)$ benar

Jika langkah 1 dan 2 berhasil menunjukkan kebenarannya maka selanjutkan disimpulkan bahwa $p(n)$ benar untuk setiap bilangan asli n

Contoh 7:

Buktikan bahwa $1+2+3+4+\cdots+n=\frac{1}{2}n(n+1)$, benar untuk setiap bilangan asli n

Bukti:

Misalkan $p(n)$ menyatakan $1+2+3+4+\cdots+n=\frac{1}{2}n(n+1)$

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

$p(n): 1+2+3+4+\cdots+n=\frac{1}{2}n(n+1)$

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

$1=\frac{1}{2}.1.2$

$1=1$

$p(1)$ benar

Langkah 2 : asumsikan bahwa $p(k)$ benar untuk suatu bilangan asli k, yaitu

$1+2+3+4+\cdots+k=\frac{1}{2}k(k+1)$ benar

Selanjutnya, tunjukkan bahwa $p(k+1)$ benar, yaitu

$1+2+3+4+\cdots+k+(k+1)=\frac{1}{2}(k+1)(k+2)$

Hal ini ditunjukkan sebagai berikut:

$=1+2+3+4+\cdots+k+(k+1)$

$=(1+2+3+4+\cdots+k)+(k+1)$

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

$=(k+1)\left(\frac{1}{2}k+1\right)$ (sama-sama punya factor $(k+1)$)

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

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

Jadi, $1+2+3+4+\cdots+k+(k+1) = \frac{1}{2}(k+1)(k+2)$ berarti $p(k+1)$ benar

Sehingga dapat disimpulkan bahwa $1+2+3+4+\cdots+n = \frac{1}{2}n(n+1)$, benar untuk setiap bilangan asli n

Contoh 8:

Buktikan bahwa $7^n - 2^n$ selalu terbagi habis oleh 5 untuk setiap bilangan asli n.

Bukti:

Misalkan $p(n)$ menyatakan $7^n - 2^n$ terbagi habis oleh 5

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

$p(1)$ adalah $7^1 - 2^1$ terbagi habis oleh 5, yaitu 5 terbagi habis oleh 5

Jadi, $p(1)$ benar

Langkah 2 : asumsikan bahwa $p(k)$benar unyuk suatu bilangan asli k, yaitu

$7^k - 2^k$ terbagi habis oleh 5,

Tunjukkan bahwa $p(k+1)$ benar, yaitu $7^{k+1} - 2^{k+1}$ terbagi habis oleh 5. Hal ini ditunjukkan sebagai berikut.

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7^k.7 - 2^k.2 \\ &= 7^k.7 - 2^k.2 + 2^k.7 - 2^k.7 \\ &= 7^k.7 - 2^k.7 + 2^k.7 - 2^k.2 \\ &= 7\left(7^k - 2^k\right) + 2^k(7-2) \\ &= 7\left(7^k - 2^k\right) + 2^k.5 \end{aligned}$$

Telah diasumsikan bahwa $7^k -; 2^k$ terbagi habis oleh 5 maka $7\left(7^k - 2^k\right)$ juga terbagi habis oleh 5.

$2^k.5$ jelas terbagi habis oleh 5 sebab mempunyai faktor 5.

Sehingga $7\left(7^k - 2^k\right) + 2^k.5$ terbagi habis oleh 5

Jadi, $7^{k+1} - 2^{k+1}$ terbagi habis oleh 5, maka $p(k+1)$ benar
Sehingga dapat disimpulkan bahwa $7^n - 2^n$ selalu terbagi habis oleh 5 untuk setiap bilangan asli n.

Tugas:

1. Buktikan bahwa $1 + 3 + 5 + \cdots + (2n-1) = n^2$ benar untuk setiap bilangan asli n
2. Buktikan bahwa $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ benar untuk setiap bilangan asli n.
3. Buktikan bahwa untuk setiap bilangan asli n berlaku $11^n - 4^n$ terbagi habis oleh oleh 7

BAB II
KETERBAGIAN BILANGAN BULAT

A. Konsep Dasar Keterbagian

Pembagian bilangan bulat merupakan materi pembelajaran yang telah diberikan pada tingkat sekolah dasar. Kemudian hal ini dikembangkan pada materi pembelajaran FPB dan KPK. Masih ingat apa itu FPB dan KPK? Jika bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka hasil baginya adalah suatu bilangan bulat atau suatu bilangan yang tidak bulat. Contoh, 30 dibagi 6 maka hasil baginya adalah bilangan bulat 5. Tetapi jika 30 dibagi 4 maka hasil baginya adalah 7,5. Keadaan yang seperti ini yang membutuhkan definisi yang jelas tentang keterbagian.

Definisi 12

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 q habis dibagi p atau p membagi habis q atau p faktor dari q atau q kelipatan dari p

p ł q dibaca q tidak habis dibagi p atau p tidak membagi q atau p bukan faktor dari q atau q bukan kelipatan dari p.

Contoh 9.

3|18 sebab ada bilangan bulat 6 sehingga 18=3.6

8 ł 12sebab tidak ada bilangan bulat x sehingga 12=8.x

5|-20 sebab ada bilangan bulat -4 sehingga -20=5.-4

Beberapa sifat sederhana keterbagian adalah

1. 1|p untuk setiap p ∈ Z
2. p|0 untuk setiap p ∈ Z dan p ≠ 0
3. p|p untuk setiap p ∈ Z dan p ≠ 0
4. Jika p|q maka kemungkinan hubungan antara p dan q adalah p < q, p = q, atau p > q

Teorema 1.

Jika p,q ∈ Z dan p|q, maka p|qr untuk semua r ∈ Z

Bukti:

Diketahui bahwa p | q berarti ada suatu x ∈ Z sehingga

q = px ,Ambil $r \in Z$

$qr = pxr$

$qr = p(x.r)$

karena x ∈ Z dan r ∈ Z , maka xr ∈ Z

karena qr = p(xr) , maka p | qr

Teorema 2.

Jika p,q,r ∈ Z, p|q, dan q|r maka p|r

Bukti:

p|q berari ada x ∈ Z sehingga q = px

q|r berarti ada y ∈ Z sehingga r = qy

karena r = qy dan q = px maka

r = (px)y

r = p(xy) dengan x,y ∈ Z

karena r = p(xy) maka p | r

Teorema 3.

Jika p,q ∈ Z, p|q dan q|p maka p = ± q

Bukti:

p|q berarti terdapat x ∈ Z sehingga p = qx

q|p berarti terdapat $y \in Z$ sehingga q = py
Perhatikan :
p = (py)x
p = p(yx)
p = p(xy)
p = (xy)p
1.p = (xy)p sehingga
xy = 1
karena xy ∈ Z dan xy = 1 kemungkinan yang diperoleh yaitu
untuk x = -1 = y maka p = -q
untuk x = 1 = y maka p = q
dengan demikian diperoleh p = $\pm q$

Teorema 4.
Jika p,q,r ∈Z, p|q, dan p|r maka p|q+r
Bukti:
p|q berarti ada x ∈ Z sehingga q = px
p|r berarti ada y ∈ Z sehingga r = py
perhatikan
q + r = px + py = p(x+y)
karena x,y ∈ Z maka x + y ∈ Z
karena q + r = p(x+y) maka p | q+r

Teorema 5.
Jika p,q,r ∈Z, p|q, dan p|r maka p|qx+ry untuk semua x,y ∈ Z
Buktikan.

Teorema 6.
Jika p,q,r ∈Z, p > 0, q > 0, dan p|q, maka p ≤ q
Bukti:
Karena p|q, maka menurut definisi 12, ada x € Z sehingga q = px

Karena $p > 0$, $q > 0$, dan $q = px$, maka $x > 0$
Karena $x \in Z$ dan $x > 0$, maka kemungkinan nilai-nilai x adalah 1, 2, 3, …, yaitu $x = 1$ atau $x > 1$
Jika $x = 1$, maka $q = px = p(1) = p$.
Jika $x > 1$, dan $q = px$, maka $p < q$
Jadi $p \leq q$

Teorema 7.
Jika $p,q,r \in Z$, $p > 0$, $q > 0$, $p|q$,dan $q|p$ maka $p=q$
Buktikan

Teorema 8.
$p|q$ jika dan hanya jika $kp|kq$ untuk semua $k \in Z$ dan $k \neq 0$
Buktikan

Teorema 9.
Jika $p,q,r \in Z$, $p \neq 0$, $p|q+r$, dan $p|q$ maka $p|r$
Bukti:
Karena $p|q+r$ berarti $q+r = xp$ untuk $x \in Z$
$p|q$ berarti $q = yp$ untuk suatu $y \in Z$
$q + r = xp$
$yp + r = xp$
$r = xp – yp$
$r = (x – y)\, p$
Karena $x \in Z$ dan $y \in Z$ maka $x-y \in Z$
Karena $r = (x – y)$ maka $p|r$

Teorema 10.
Jika $p,q \in Z$ dan $p>0$ maka ada bilangan-bilangan $r,s \in Z$ yang masing-masing tunggal sehingga $q=rp+s$ dengan $0 \leq s < p$

Dari pernyataan q=rp+s, $0 \leq s < p$ maka r disebut hasil bagi, s disebut sisa, q disebut yang dibagi, dan p disebut pembagi
Buktikan.

B. **Faktor Persekutuan Terbesar (FPB)**

Masih ingat apa itu FPB ?
Perhatikan ilustrasi berikut.
Misalkan $a = 12$ dan $b = 16$
Jika A adalah himpunan semua factor dari a dan B adalah himpunan semua factor dari b serta C adalah himpunan semua factor persekutuan dari a dan b maka
$A = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$
$B = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$
$C = A \cap B = \{-4, -2, -1, 1, 2, 4\}$
Anggota C yang terbesar adalah 4. 4 disebut factor persekutuan terbesar dari $a = 12$ dan $b = 16$

Sekarang bagaimana jika $a = -12$ dan $b = 16$
$A = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$
$B = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$
$C = A \cap B = \{-4, -2, -1, 1, 2, 4\}$
Anggota C yang terbesar adalah 4. 4 disebut factor persekutuan terbesar dari $a = -12$ dan $b = 16$

Bagaimana jika $a = -12$ dan $b = -16$
$A = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$
$B = \{-16, -8, -4, -2, -1, 1, 2, 4, 8, 16\}$
$C = A \cap B = \{-4, -2, -1, 1, 2, 4\}$
Anggota C yang terbesar adalah 4. 4 disebut factor persekutuan terbesar dari $a = -12$ dan $b = -16$

Apa yang dapat anda simpulkan terkait ilustrasi tersebut?

Perhatikan, bagaimana jika nilai a atau b (tidak keduanya) bernilai 0?

Misalkan $a = 0$ dan $b = 8$

$A = \{\dots, -4, -3, -2, -1,0,1,2,3,4, \dots\} B = \{-8, -4, -2, -1,1,2,4,8\} C$

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

Anggota C yang terbesar adalah 8. 8 disebut factor persekutuan terbesar dari $a = 0$ dan $b = 8$.

Apa yang dapat anda simpulkan terkait ilustrasi tersebut?

Lantas Bagaimana jika a dan b keduanya bernilai 0?

Definisi 13

Jika $a, b \in Z$, maka bilangan p disebut faktor persekutuan dari a dan b jika p habis membagi a dan habis membagi b atau $p|a$ dan $p|b$

Definisi 14

Jika $a, b \in Z$, yang keduanya tidak bersama-sama bernilai 0, maka faktor persekutuan terbesar dari a dan b adalah p yang merupakan bilangan bulat positif terbesar yang habis membagi a dan habis membagi b. Misalkan bilangan tersebut adalah d maka $d|a$ dan $d|b$

Definisi 15

faktor persekutuan terbesar dari a dan b dinotasikan dengan (a, b). $d = (a, b)$ dibaca d adalah faktor persekutuan terbesar dari a dan b

perlu diperhatikan bahwa (a, b) selalu bernilai bilangan bulat positif, yaitu $d \in Z$ dan $d \geq 1$

Teorema 11

jika $a, b \in Z$ dan $d = (a, b)$ maka $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Bukti:

misalkan $a, b \in Z$ dan $d = (a, b)$, akan ditunjukkan bahwa $\frac{a}{d}$ dan $\frac{b}{d}$ tidak mempunyai pembagi persekutuan yang positif selain 1.

Misalkan e adalah suatu bilangan bulat positif yang membagi habis $\frac{a}{d}$ dan $\frac{b}{d}$ yaitu $e|\frac{a}{d}$ dan $e|\frac{b}{d}$ maka menurut definisi $\frac{a}{d} = ke$ dan $\frac{b}{d} = le$ untuk suatu $k, l \in Z$ dengan demikian $a = dke$ dan $b = dle$

Keduanya memiliki factor persekutuan yaitu de. Karena de adalah factor persekutuan dari a dan b, dan d adalah FPB dari a dan b maka $de \leq d$ akibatnya e haruslah sama dengan 1.

Jadi $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Teorema 12

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

Bukti:

Diketahui $(p, q) = 1$, maka 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 1 karena $p|qr$ maka $p|qry$ untuk semua $y \in Z$

Selanjutnya karena $p|prx$ dan $p|qry$ maka menurut teorema .4

$p|prx + qry$ jadi $p|r$

Teorema 13. Algoritma Euclides

Ditentukan $s_0, s_1 \in Z, s_0 \geq s_1 > 0$,

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 pemabagian

Bukti.

Karena $s_0, s_1 \in Z, s_0 \geq s_1 > 0$, maka dengan menggunakan algoritma pembagian secara berturut-turut akan diperoleh:

$$\begin{aligned}
s_0 &= s_1k_1 + s_2, & 0 \leq s_2 < s_1\\
s_1 &= s_2k_2 + s_3, & 0 \leq s_3 < s_2\\
&\vdots\\
s_{t-2} &= s_{t-1}k_{t-1} + s_t, & 0 \leq s_t < s_{t-1}\\
&\vdots\\
s_{n-3} &= s_{n-2}k_{n-2} + s_{n-1}, & 0 \leq s_{n-1} < s_{n-2}\\
s_{n-2} &= s_{n-1}k_{n-1} + s_n, & 0 \leq s_n < s_{n-1}\\
s_{n-1} &= s_nk_n + s_{n+1}, & s_{n+1} = 0
\end{aligned}$$

Maka sesuai teorema pada materi sebelumnya

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

Contoh 10:

Carilah (963,657) dengan menggunakan Algoritma Euclides

Jawab

$$\begin{aligned}
963 &= 1.657 + 306 & 657 &\leq 306 < 657\\
&= 2.306 & 0 &\leq 45 < 306\\
&+ 45306 & 0 &\leq 36 < 45\\
&= 6.45 & 0 &\leq 9 < 36\\
&+ 3645\\
&= 1.36 + 936\\
&= 4.9 + 0
\end{aligned}$$

Jadi $(963,657) = 9$

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

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

$s_{n-2} = s_{n-1}k_{n-1} + s_n$ Maka $s_n = s_{n-2} - s_{n-1}k_{n-1}$

$s_{n-3} = s_{n-2}k_{n-2} + s_{n-1}$ Maka $s_{n-1} = s_{n-3} - s_{n-2}k_{n-2}$

$s_{n-4} = s_{n-3}k_{n-3} + s_{n-2}$ Maka $s_{n-2} = s_{n-4} - s_{n-3}k_{n-3}$

$\vdots$

$s_1 = s_2k_2 + s_3$ Maka $s_3 = s_1 - s_2k_2$

$s_0 = s_1k_1 + s_2$ Maka $s_2 = s_0 - s_1k_1$

Dengan demikian

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

Jika proses ini dilanjutkan dengan proses substitusi secara bereturut-turut:

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

Maka akan diperoleh bentuk

$$(s_0, s_1) = s_n$$
$$(s_0, s_1) = ms_0 + ns_1$$

Contoh 11:

Carilah nilai-nilai x dan y yang memenuhi hubungan

$(205{,}75) = 205x + 75y$

Jawab

$205 = 2.75 + 5575 = 1.55 + 2055$ $55 = 205 - 2.75$

$= 2.20 + 1520$ $20 = 75 - 1.55$

$= 1.15 + 515$ $15 = 55 - 2.20$

$= 3.5 + 0(205{,}75) = 5$ $5 = 20 - 1.15$

Dengan demikian

$(205{,}75) = 5 = 20 - 1.15 = 20 - 1.(55 - 2.20)$

$= 20 - 1.55 + 2.20 = 3.20 - 1.55$

$= 3.(75 - 1.55) - 1.15 = 3.75 - 3.55 - 1.55$

$= 3.75 - 4.55 = 3.75 - 4.(205 - 2.75)$

$= 3.75 - 4.205 + 8.75 = 11.75 - 4.205(205{,}75)$

$= 11.75 - 4.205$

Jadi nilai $x = -4, y = 11$

Latihan:

1. Buktikan jika $(x, y) = 1$ dan $z = x + y$ maka $(x, z) = (y, z) = 1$
2. Carilah $(67815{,}21480)$
3. Carilah m dan n jika $30745m + 17446n = (30745{,}17446)$

C. Kelipatan Persekutuan Terkecil (KPK)

Disekolah dasar kita telah mempelajari Kelipatan Persekutuan Terkecil (KPK) Misalnya

Kelipatan bulat positif dari 4adalah $4{,}8{,}12{,}16{,}20{,}24{,}28{,}32{,}36{,}40{,}44, \ldots$

Kelipatan bulat positif dari 5 adalah $5{,}10{,}15{,}20{,}25{,}30{,}35{,}40{,}45{,}50, \ldots$

Maka kelipatan persekutuan dari 4 dan 5 adalah $20{,}40{,}60, \ldots$

Definisi 16

Jika $a, b \in Z, a \neq 0, b \neq 0$ maka

a. m disebut kelipatan persekutuan dari a dan b jika $a|m$ dan $b|m$

b. m disebut kelipatan persekutuan terkecil dari a dan b jika$m$ adalah bilangan bulat positif terkecil sehingga $a|m$ dan $b|m$
c. m adalah kelipatan persekutuan terkecil dari a dan b, ditulis dengan $m = [a, b]$

Contoh 12:
Carilah $[6,8]$
Jawab.
Kelipatan bulat positif dari 6 adalah $6,12,18,24,30,36,42,48,54, ...$
Kelipatan bulat positif dari 8 adalah $8,16,24,32,40,48,56, ...$
kelipatan persekutuan dari 6 dan 8 adalah $24,48, ...$
kelipatan persekutuan terkecil dari 6 dan 8 adalah 24
sehingga $[6,8] = 24$

Teorema 14
ditentukan $a, b \in Z, a \neq 0, b \neq 0$
jika c adalah kelipatan persekutuan dari a dan b maka $[a, b]|c$
Bukti
misalkan $[a, b] = m$ maka harus ditunjukkan bahwa $m|c$.
Menurut algoritma pembagian, ada bilangan bulat q dan r sedemikian hingga
$c = qm + r$ dengan $0 \leq r < m$ sehingga $r = c - qm$
Karena c adalah kelipatan persekutuan dari a dan b maka $a|c$ dan $b|c$
Karena $[a, b] = m$ maka $a|m$ dan $b|m$
$a|m$ maka $a|qm$ dan $a|c$ maka $a|c - qm$ ini berarti $a|r$
Demikian pula dengan
$b|m$ maka $b|qm$ dan $b|c$ maka $b|c - qm$ ini berarti $b|r$
Karena $a|r$ dan $b|r$ maka r adalah kelipatan persekutuan dari a dan b
m dan r adalah kelipatan persekutuan dari a dan b
Tetapi karena $[a, b] = m$ yang berarti m adalah kelipatan persekutuan terkecil dari a dan b dan $0 \leq r < m$ maka jelas $r = 0$

Sehingga $c = qm$ atau $m|c$ atau $[a,b]|c$

Teorema 15

Jika $c \in N$ maka $[ca,cb] = c[a,b]$

Bukti

Misalkan $[a,b] = m$ maka $a|m$ dan $b|m$

Sehingga $ac|mc$ dan $bc|mc$

Hal ini berarti mc adalah kelipatan persekutuan dari ac dan bc

Dan menurut teorema sebelumnya $[ac,bc]|mc$

Karena $[ac,bc]$ adalah suatu kelipatan dari ac maka $[ac,bc]$adalah suatu kelipatan dari c pula

Misalkan $[ac,bc] = nc$ maka $nc|mc$ sehingga $n|m$

Karena $[ac,bc] = nc$ maka $ac|nc$ dan $bc|nc$ sehingga $a|n$ dan $b|n$

Menurut teorema sebelumnya maka $[a,b]|n$ yaitu $m|n$ dank arena $n|m$ maka $m = n$

Sehingga $mc = nc$ yaitu $[a,b]c = [ac,bc]$ atau $c[a,b] = [ac,bc]$

Teorema 16

Jika $a,b \in N$ dan $(a,b) = 1$ maka $[a,b] = ab$

Bukti

ab adalah suatu kelipatan persekutuan dari a dan b

Menurut teorema 1 maka $[a,b]|ab$

Karena $a|[a,b]$ dan $b|[a,b]$ dengan $(a,b) = 1$ maka $ab|[a,b]$ Karena $[a,b]|ab$ maka $[a,b] = ab$

Teorema 17

Jika $a,b \in Z$, maka $(a,b)[a,b] = ab$

Bukti

Misalkan $(a,b) = d$ maka sesuai Teorema 11 $\left(\frac{a}{d},\frac{b}{d}\right) = 1$

Sesuai teorema, karena $\left(\frac{a}{d},\frac{b}{d}\right) = 1$maka $\left[\frac{a}{d},\frac{b}{d}\right] = \frac{a}{d}.\frac{b}{d}$

Akibatnya

$$\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right] = 1.\frac{a}{d}.\frac{b}{d}\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right] = \frac{ab}{d^2}d^2.\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right]$$

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

$$= ab\left(d.\frac{a}{d},d.\frac{b}{d}\right)\left[d.\frac{a}{d},d.\frac{b}{d}\right] = ab(a,b)[a,b] = ab$$

Latihan:

Carilah buku referensi tentang teori bilangan, kemudian Jelaskan dan buktikan teorema dasar aritmatika

BAB III
KONGRUENSI

A. Konsep Dasar Kongruensi

Kongruensi secara tidak langsung sudah diperkenalkan dan dibahas sebagai bahan matematika disekolah dalam bentuk bilangan jam atau bilangan bersisa. Peragaan dengan menggunakan tiruan jam bermanfaat karena peserta didik akan langsung mengenal adanya system bilangan yang berbeda. Untuk bilangan jam duabelasan, peserta didik telah mengetahui bahwa bilangan-bilangan bulat lebih dari 12 dapat di "reduksi" menjadi 0,1,2,3,4,5,6,7,8,9,10,11,atau 12 dengan cara menyatakan sisanya jika bilangan itu dibagi dengan 12, misalnya 13 dapat direduksi menjadi 1, karena 13 dibagi 12 bersisa 1, 23 dapat direduksi menjadi 11 karena 23 dibagi 12 bersisa 11, dan dalam bahasa kongruensi dapat dinyatakan sebagai $13 \equiv 1\ (mod\ 12)$ dan $23 \equiv 11(mod\ 12)$.

Definisi 17

Jika p, q, m adalah bilangan-bilangan bulat, maka p disebut kongruen dengan q modulo m jika dan hanya jika m membagi $(p - q)$. Ditulis $p \equiv q(mod\ m)$ jika dan hanya $m|p - q$

Jika m tidak membagi $(p - q)$, maka disebut p tidak kongruen dengan q modulo m. Ditulis $p \not\equiv q\ (mod\ m)$ jika $m \nmid\ p - q$

Contoh 13:

a. $26 \equiv 1\ (mod\ 5)$ sebab $5|26 - 1$ atau $5|25$
b. $10 \equiv 4(mod\ 3)$ sebab $3|10 - 4$ atau $3|6$
c. $23 \equiv -1(mod\ 12)$ sebab $12|23 - (-1)$ atau $12|24$
d. $31 \not\equiv 5\ (mod\ 6)$ sebab $6 \nmid 31 - 5$ atau $6 \nmid 26$

Teorema 18

Jika $p, q,$ dan m adalah bilangan-bilangan bulat dan $m \neq 0$, maka $p \equiv q \ (mod\ m)$ jika dan hanya jika ada bilangan bulat t sehingga $p = q + tm$.

Bukti

Jika $p \equiv q \ (mod\ m)$ maka $m|p - q$. Ini berarti bahwa ada suatu bilangan bulat t sehungga $tm = p - q$ 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 $m|p - q$ akibatnya berlaku $p \equiv q \ (mod\ m)$

Contoh 14

a. $23 \equiv 3 \ (mod\ 5)$ sama artinya dengan $23 = 5.4 + 3$
b. $23 \equiv -1 (mod\ 12)$ sama artinya dengan $23 = 12.2 + (-1)$

Teorema 19

Ditentukan m adalah suatu bilangan bulat positif.

Kongruensi modulo m memenuhi sifat-sifat berikut:

a. Refleksif.
   Jika p adalah suatu bilangan bulat, maka $p \equiv p \ (mod\ m)$
b. Simetris.
   Jika p dan q adalah bilangan-bilangan bulat sedemikian hingga $p \equiv q \ (mod\ m)$ maka $q \equiv p (mod\ m)$
c. Transitif.
   Jika p, q, r adalah bilangan-bilangan bulat sedemikian hingga $p \equiv q \ (mod\ m)$ dan $q \equiv r (mod\ m)$ maka $p \equiv r \ (mod\ m)$

Bukti

a. Diketahui bahwa $m|0$ atau $m|p - p$ berarti $p \equiv p \ (mod\ m)$

b. Jika $p \equiv q\ (mod\ m)$ maka $m|p-q$ menurut definisi keterbagian, ada suatu bilangan bulat t sehingga $tm = p-q$ atau $(-t)m = q-p$ berarti $m|q-p$
   Dengan demikian $q \equiv p(mod\ m)$
c. Jika $p \equiv q\ (mod\ m)$ dan $q \equiv r(mod\ m)$ maka $m|p-q$ dan $m|q-r$ dan menurut definisi keterbagian, ada suatu bilangan bulat s dan t sehingga $sm = p-q$ dan $tm = q-r$
   Dengan demikian dapat ditunjukkan bahwa

$$p-r = p-r+q-q = (p-q)+(q-r) = sm+tm = m(s+t)$$

   Sehingga $m|p-r$ akibatnya $p \equiv r\ (mod\ m)$

Contoh 15:

a. $3 \equiv 3(mod\ 7)$ sebab $7|3-3$ atau $7|0$
b. $27 \equiv 6\ (mod\ 21)$ akibatnya $6 \equiv 27\ (mod\ 21)$ sebab $7|6-27$ atau $7|(-21)$
c. $28 \equiv 18(mod\ 5)$ dan $18 \equiv 3\ (mod\ 5)$ maka $28 \equiv 3\ (mod\ 5)$ sebab $5|28-3$ atau $5|25$

Teorema 20

Jika p, q, r, m adalah bilangan-bilangan bulat dan $m > 0$ sedemikian hingga $p \equiv q\ (mod\ m)$ maka:

a. $p+r \equiv q+r(mod\ m)$
b. $p-r \equiv q-r(mod\ m)$
c. $pr \equiv qr(mod\ m)$

Bukti:

a. Diketahui $p \equiv q\ (mod\ m)$ maka $m|p-q$ Selanjutnya
   $p-q = p-q+r-r = p+r-q-r = (p+r)-(q+r)$
   maka $m|(p+r)-(q+r)$
   dengan demikian $p+r \equiv q+r(mod\ m)$

b. Diketahui $p \equiv q\ (mod\ m)$ maka $m|p-q$ Selanjutnya
$p-q=p-q+r-r=p-r-q+r=(p-r)-(q-r)$
maka $m|(p-r)-(q-r)$
dengan demikian $p-r \equiv q-r(mod\ m)$

c. Diketahui $p \equiv q\ (mod\ m)$ maka $m|p-q$ dan menurut teorema keterbagian $m|r(p-q)$ untuk sebarang bilangan bulat r. Maka:
$m|r(p-q)=m|rp-rq=m|pr-qr$
Dengan demikian $pr \equiv qr(mod\ m)$

Contoh 16:

a. $24 \equiv 3\ (mod\ 7)$ maka $24+2 \equiv 3+2(mod\ 7)$ atau
$26 \equiv 5(mod\ 7)$

b. $24 \equiv 3\ (mod\ 7)$ maka $24-2 \equiv 3-2(mod\ 7)$ atau
$22 \equiv 1(mod\ 7)$

c. $24 \equiv 3\ (mod\ 7)$ maka $24.2 \equiv 3.2(mod\ 7)$ atau
$48 \equiv 6(mod\ 7)$

Teorema 21

Jika p, q, r, s, m adalah bilangan-bilangan bulat dan $m > 0$ sedemikian hingga
$p \equiv q\ (mod\ m)$ dan $r \equiv s\ (mod\ m)$ maka:

a. $p+r \equiv q+s(mod\ m)$
b. $p-r \equiv q-s(mod\ m)$
c. $pr \equiv qs(mod\ m)$

Bukti:

a. $p \equiv q\ (mod\ m)$ dan $r \equiv s\ (mod\ m)$, maka $m|p-q$ dan $m|r-s$ maka tentu ada bilangan bukat t dan u sedemikian hingga $tm = p-q$ dan $um = r-s$, maka
$(p+r)-(q+s)=p+r-q-s=p-q+r-s$
$=(p-q)+(r-s)=tm-um=m(t-u)$

Dengan demikian $m|(p+r)-(q+s)$ atau $p+r \equiv q+s(mod\ m)$

b. $p \equiv q\ (mod\ m)$ dan $r \equiv s\ (mod\ m)$, maka $m|p-q$ dan $m|r-s$ maka tentu ada bilangan bukat t dan u sedemikian hingga $tm = p-q$ dan $um = r-s$, maka

$(p-r)-(q-s) = p-r-q+s = p-q-r+s$

$= (p-q)-(r-s) = tm-um = m(t-u)$

Dengan demikian $m|(p-r)-(q-s)$ atau

$p-r \equiv q-s(mod\ m)$

c. $p \equiv q\ (mod\ m)$ dan $r \equiv s\ (mod\ m)$, maka $m|p-q$ dan $m|r-s$ maka tentu ada bilangan bukat t dan u sedemikian hingga $tm = p-q$ dan $um = r-s$, maka

$(pr)-(qs) = pr-qs+qr-qr = pr-qr+qr-qs$

$= r(p-q)+q(r-s) = tm-um = m(t-u)$

Dengan demikian $m|(p+r)-(q+s)$

atau $p+r \equiv q+s(mod\ m)$

Contoh 17:

a. $23 \equiv 7\ (mod\ 4)$ dan $15 \equiv 3\ (mod\ 4)$, maka:
$23+15 \equiv 7+3\ (mod\ 4)$ atau $38 \equiv 10(mod\ 4)$

b. $23 \equiv 7\ (mod\ 4)$ dan $15 \equiv 3\ (mod\ 4)$, maka:
$23-15 \equiv 7-3\ (mod\ 4)$ atau $8 \equiv 4\ (mod\ 4)$ atau $8 \equiv 0(mod\ 4)$

c. $23 \equiv 7\ (mod\ 4)\ dan\ 15 \equiv 3\ (mod\ 4)$, maka:
$23.15 \equiv 7.3\ (mod\ 4)$ atau $345 \equiv 21(mod\ 4)$

Teorema 22

a. Jika $p \equiv q\ (mod\ m)$, maka $pr \equiv qr(mod\ mr)$

b. Jika $p \equiv q\ (mod\ m)$ dan $d|m$ maka $p \equiv q\ (mod\ d)$

Bukti:

a. Diketahui $p \equiv q \ (mod\ m)$ maka $m|p-q$ dan menurut teorema $rm|r(p-q)$ atau $mr|pr-qr$ maka $pr \equiv qr \ (mod\ mr)$

b. Diketahui $p \equiv q \ (mod\ m)$ maka $m|p-q$ dan menurut teorema, karena $d|m$ dan $m|p-q$ berarti $d|p-q$ maka $p \equiv q \ (mod\ d)$

Contoh 18:

a. $21 \equiv 3 \ (mod\ 6)$ maka $21.4 \equiv 3.4 (mod\ 6.4)$ atau
$84 \equiv 12 (mod\ 24)$

b. $27 \equiv 3 \ (mod\ 8)$ dan $4|8$ maka $27 \equiv 3 \ (mod\ 4)$

Teorema 23

Diketahui bilangan-bilangan bulat a, p, q, m dan $m > 0$

a. $ap \equiv aq (mod\ m)$ jika dan hanya jika $p \equiv q \ (mod\ \frac{m}{(a,m)})$

b. $p \equiv q (mod\ m_1)$ dan $p \equiv q (mod\ m_2)$ jika dan hanya jika $p \equiv q (mod [m_1, m_2])$

Bukti

a. $(\rightarrow)$

Misalkan $ap \equiv aq (mod\ m)$, maka $m|ap-aq$. Sesuai definisi

$ap - aq = tm$ untuk suatu $t \in Z$

$a(p-q) = tm$;Karena $(a,m)|a$ dan $(a,m)|m$ maka

$\left(\frac{a}{(a,m)}\right)(p-q) = t\left(\frac{m}{(a,m)}\right)$ (sesuai definisi)

$\left(\frac{m}{(a,m)}\right) | \left(\frac{a}{(a,m)}\right)(p-q)$

Menurut teorema 11, $\left(\frac{m}{(a,m)}\right), \left(\frac{a}{(a,m)}\right) = 1$ dan menurut teorema 12, jika $\left(\frac{m}{(a,m)}\right), \left(\frac{a}{(a,m)}\right) = 1$ dan $\left(\frac{m}{(a,m)}\right) | \left(\frac{a}{(a,m)}\right)(p-q)$ berakibat $\left(\frac{m}{(a,m)}\right) | (p-q)$

Jadi menurut definisi, $p \equiv q \ (mod\ \frac{m}{(a,m)})$

(←)

Misalkan $\equiv q\ (mod\ \frac{m}{(a,m)})$, menurut teorema 18..a maka

$ap \equiv aq\ (mod\ \frac{am}{(a,m)})$.

Selanjutnya karena $m|\frac{am}{(a,m)}$ dan $ap \equiv aq\ (mod\ \frac{am}{(a,m)})$. Maka berdasarkan teorema 18b. $ap \equiv aq\ (mod\ m)$.

b. Misalkan $p \equiv q(mod\ m_1)$ dan $p \equiv q(mod\ m_2)$ maka $m_1|p-q$ dan $m_2|p-q$
   Dengan demikian $p-q$ adalah kelipatan persekutuan dari m_1 dan m_2 dan berdasarkan teorema $[m_1, m_2]|p-q$
   Jadi $p \equiv q(mod[m_1, m_2])$

Contoh 19:

a. $8p \equiv 8q(mod\ 6)$ karena $(8,6) = 2$ maka $p \equiv q\ (mod\ \frac{6}{2})$ atau $p \equiv q\ (mod\ 3)$
b. $p \equiv q\ (mod\ 6)$ dan $p \equiv q\ (mod\ 8)$ maka $p \equiv q\ (mod\ [6,8])$ atau $p \equiv q\ (mod\ 24)$

Latihan:

1. Diketahui $p, q, m \in Z$ dan $m > 0$ sedemikian hingga $p \equiv q\ (mod\ m)$ buktikan
   $(p, m) = (q, m)$
2. Buktikan bahwa: Jika $p, q \in Z$ dan $m_1, m_2, \dots, m_t \in Z^+$ sedemikian hingga
   $p \equiv q(mod\ m_1)$,$p \equiv q(mod\ m_2)$, ... , dan $p \equiv q(mod\ m_t)$ maka $p \equiv q(mod\ [m_1, m_2, \dots, m_t])$,
3. Buktikan jika p adalah suatu bilangan genap, maka $p^2 \equiv 0\ (mod\ 4)$

4. Buktikan jika p adalah suatu bilangan ganjil, maka $p^2 \equiv 1\ (mod\ 4)$
5. Carilah sisa positif terkecil dari $1! + 2! + \cdots + 100!$ Modulo 2
6. Carilah sisa positif terkecil dari $1! + 2! + \cdots + 100!$ Modulo1 2
7. Carilah dua angka terakhir dari lambang bilangan decimal 28^{75}
8. Carilah tiga angka terakhir dari lambang bilangan decimal 23^{95}

B. Sistem Residu

Definisi 18

Suatu himpunan $\{x_1, x_2, \dots, x_m\}$ disebut suatu system 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 hinggay$\equiv x_i(mod\ m)$ atau $x_i \equiv y\ (mod\ m)$

Penjelasan:

- Perhatikan bahwa indeks dari x yang terakhir adalah m. Hal ini menunjukkan bahwa banyaknya unsur dalam suatu system residu lengkap modulo m adalah m.
- Dengan demikian, jika ada suatu himpunan yang banyaknya unsur kurangdari$m$ atau lebih dari m, maka himpunan itu bukan merupakan system residu lengkap modulo m.
- Karena pasangan-pasangan kongruensi antara$y$ dan $x_i$adalah tunggal, maka tidak ada y yang kongruen dengan dua unsur x yang berbeda.

Contoh 20:

1. Himpunan $A = \{5,6,7\}$bukan merupakan system residu lengkap modulo 4 sebab banyaknya unsur A kurang dari4
2. Himpunan $B = \{5,6,7,8\}$ adalah suatu system residu 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 $y \equiv x_i (mod\ 4)$ atau $x_i \equiv y\ (mod\ 4)$. Nilai-nilai y yang memenuhi $0 \leq y \leq 4$, adalah $y = 0, y = 1, y = 2, y = 3$

Jika kita selidiki maka akan diperoleh

$8 \equiv 0 (mod\ 4)$

$7 \equiv 3 (mod\ 4)$

$6 \equiv 2 (mod\ 4)$

$5 \equiv 1 (mod\ 4$

Dengan demikian untuk setiap y dengan $y = 0,1,2,3$ ada satu dan hanya satu x_i dengan $x_i = 5,6,7,8$ sedemikian hingga $x_i \equiv y\ (mod\ m)$. Jadi B adalah suatu sistem residu lengkap modulo 4

3. Himpunan $C = \{-33, -13,14,59,32,48,12\}$ adalah suatu sistem residu 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 $x_i \equiv y\ (mod\ 7)$.

$$-33 \equiv 2 (mod\ 7)$$
$$-13 \equiv 1 (mod\ 7)$$
$$14 \equiv 0 (mod\ 7)$$
$$59 \equiv 3 (mod\ 7)$$
$$32 \equiv 4 (mod\ 7)$$
$$48 \equiv 6 (mod\ 7)$$
$$12 \equiv 5 (mod\ 7)$$

4. Himpunan $D = \{10, -5,27\}$ bukan merupakan sistem residu lengkap modulo 3 sebab untuk $y = 1$ dengan $0 \leq y < 3$ ada lebih dari satu x_i yaitu 10 dan -5 sehingga

$$10 \equiv 1 (mod\ 3)$$
$$-5 \equiv 1 (mod\ 3)$$

Definisi 19

Suatu himpunan bilangan bulat $\{x_1, x_2, \dots, x_k\}$ disebut suatu sistem residu tereduksi modulo m jika dan hanya jika

a. $(x_i, m) = 1, 1 \leq i < k$
b. $x_i \equiv x_j (mod\ m)$ untuk setiap $i \neq j$
c. Jika $(y, m) = 1$, maka $y \equiv x_i (mod\ m)$ untuk suatu $i = 1,2, \dots, k$

Suatu sistem residu tereduksi modulo m dengan membuang unsur-unsur yang tidak prima relatif dengan m

Contoh 21:

a. 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
   $(0,8) = 8 \neq 1$
   $(2,8) = 2 \neq 1$
   $(4,8) = 4 \neq 1$
   $(6,8) = 2 \neq 1$
   Misalkan B adalah himpunan dari unsur-unsur yang tersisa maka $B = 1,3,5,7$ dan B merupakan suatu sistem residu tereduksi modulo 8 karena memenuhi definisi

b. Himpunan $A = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13\}$ adalah suatu sistem residu lengkap modulo 14. Jika unsur-unsur A yang tidak prima relatif dibuang maka unsur-unsur yang tertinggal adalah $1,3,5,9,11,13$ dan $B = \{1,3,5,9,11,13\}$ merupakan suatu sistem residu tereduksi modulo 14

Definisi

Misalkan m adalah suatu bilangan positif. Banyaknya residu di dalam suatu sistem residu tereduksi modulo m disebut fungsi $\phi - E$uler dari m dan dinyatakan dengan $\phi(m)$.

Contoh 22:

$\phi(2) = 1$ diperoleh dari unsur 1
$\phi(3) = 2$ diperoleh dari unsur 1 dan 2
$\phi(4) = 2$ diperoleh dari unsur 1 dan 3
$\phi(5) = 4$ diperoleh dari unsur 1, 2, 3, dan 4
$\phi(6) = 2$ diperoleh dari unsur 1 dan 5
$\phi(7) = 6$ diperoleh dari unsur 1, 2, 3, 4, 5,dan 6
$\phi(12) = 4$ diperoleh dari unsur 1, 5, 7, dan 11
$\phi(16) = 8$ diperoleh dari unsur 1, 3, 5, 7, 9, 11, 13, dan 15
$\phi(p) = p - 1$ jika p adalah suatu bilangan prima

Teorema 24

Ditentukan $(a, m) = 1$
Jika $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residu modulo m yang lengkap atau tereduksi maka $\{ax_1, ax_2, \dots, ax_k\}$ juga merupakan suatu sistem residu modulo m yang lengkap atau tereduksi.

Bukti

Ditentukan bahwa $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residu lengkap modulo m, 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 $ax_i \equiv ax_j \ (mod\ m)$. Karena $(a, m) = 1$ dan $ax_i \equiv ax_j \ (mod\ m)$ maka menurut teorema 6 dapat ditunjukkan bahwa $x_i \equiv x_j \ (mod\ m)$. Hal ini tidak sesuai dengan aturan $\{x_1, x_2, \dots, x_k\}$

adalah suatu sistem residu lengkap modulo m. Jadi tentu ax_i tidak kongruen ax_j modulo m

Selanjutnya dibuktikan bahwa jika $\{x_1, x_2, \dots, x_k\}$ adalah suatu sistem residu modulo m yang tereduksi

Contoh 23:

a. Himpunan $P = \{0,1,2,3,4\}$ adalah merupakan suatu sistem residu lengkap modulo 5. Jika masing-masing unsur A dikalikan 4 yang mana $(4,5) = 1$ dan setelah dikalikan dimasukkan sebagai unsur himpunan Q maka dapat ditunjukkan bahwa $Q = \{0,4,8,12,16\}$ merupakan suatu sistem residu lengkap modulo 5 karena setiap unsur Q kongruen dengan satu dan hanya satu $0 \leq y < 5$ yaitu
   $0 \equiv 0\ (mod\ 5)$
   $4 \equiv 4\ (mod\ 5)$
   $8 \equiv 3\ (mod\ 5)$
   $12 \equiv 2\ (mod\ 5)$
   $16 \equiv 1\ (mod\ 5)$

b. Himpunan $P = \{1,3,5,7\}$ adalah merupakan suatu sistem residu tereduksi modulo 8. Jika masing-masing unsur P dikalikan 5 dengan $(5,8) = 1$ dan setelah dimasukkan dalam himpunan Q maka dapat ditunjukkan bahwa $Q = \{5,15,25,35\}$ merupakan suatu sistem residu tereduksi modulo 8. Sebab setiap unsur Q relatif prima dengan 8 dan tidak ada sepasang unsur Q yang kongruen sesuai dengan definisi 3

Teorema 25 (Teorema Euler)

Jika $a, m \in Z$ dan $m > 0$ sehingga $(a, m) = 1$maka $a^{\phi(m)} \equiv 1\ (mod\ m)$

Buktikan!

Contoh 24:

Carilah dua digit terakhir lambang bilangan desimal dari 23^{500}

Penyelesaian:

Pertanyaan ini dapat disajikan dalam bentuk lain yaitu $23^{500} \equiv x \ (mod\ 100)$

Kemudian bentuk tersebut dapat disederhanakan lagi menjadi $23^{500} \equiv x \ (mod\ 4)$ dan $23^{500} \equiv x \ (mod\ 25)$

- Mencari x dari $23^{500} \equiv x \ (mod\ 4)$

  Kita mulai dengan mencari 23 pangkat berapa yang memberikan sisa 1 atau -1.

  $23 \equiv 3 \ (mod\ 4)$

  $23^2 \equiv 3^2 (mod\ 4) \equiv 9 (mod\ 4) \equiv 1 (mod\ 4)$

  sehingga

  $23^{500} = (23^2)^{250} \equiv 1^{250} (mod\ 4)$ atau $x \equiv 1 \ (mod\ 4)$

- Mencari x dari $23^{500} \equiv x \ (mod\ 25)$

  $23 \equiv -2 \ (mod\ 25)$

  $23^2 \equiv -2^2 \ (mod\ 25) \equiv 4 \ (mod\ 25)$

  $23^4 \equiv 4^2 (mod\ 25) \equiv 16 (mod\ 25)$

  $23^8 \equiv 16^2 (mod\ 25) \equiv 256 (mod\ 25) \equiv 6 (mod\ 25)$

  $23^{16} \equiv 6^2 (mod\ 25) \equiv 36 (mod\ 25) \equiv 11 (mod\ 25)$

  $23^{32} \equiv 11^2 (mod\ 25) \equiv 121 (mod\ 25) \equiv -4 (mod\ 25)$

  $23^{64} \equiv -4^2 (mod\ 25) \equiv 16 (mod\ 25)$

  $23^{128} \equiv 16^2 (mod\ 25) \equiv 6 (mod\ 25)$

  $23^{256} \equiv 6^2 (mod\ 25) \equiv 11 (mod\ 25)$

  sehingga

  $23^{500} = 23^{256}.23^{128}.23^{64}.23^{32}.23^{16}.23^4$

  $\equiv 11.6.16.-4.11.16 \ (mod\ 25) \equiv 1 (mod\ 25)$

  Atau $x \equiv 1 \ (mod\ 25)$

Dari hasil dua point di atas yaitu $x \equiv 1\ (mod\ 4)$ dan $x \equiv 1\ (mod\ 25)$ maka berdasarkan teorema 6, $x \equiv 1\ (mod\ [4,25])$ maka $x \equiv 1\ (mod\ 100)$

Jadi, $23^{500} \equiv 1\ (mod\ 100)$ berarti dua digit terakhir lambang bilangan desimal dari 23^{500} adalah 0 dan 1

Contoh 25:

jika bulan ini adalah bulan Juni, maka carilah nama bulan setelah 239^{43} bulan lagi?

Penyelesaian:

$239^{43} \equiv x\ (mod\ 12)$

; 12 karena bulan berulang setiap 12

Karena $(239,12) = 1$ maka menurut teorema 7

$239^{\phi(12)} \equiv 1\ (mod\ 12)$; $\phi(12) = 4$

$239^4 \equiv 1\ (mod\ 12)$

maka

$239^{43} = 239^{4.10+3} = (239^4)^{10}.239^3 \equiv 1^{10}.239^3\ (mod\ 12)$

$\equiv 1.(-1)^3 (mod\ 12) \equiv -1\ (mod\ 12) \equiv 11 (mod\ 12)$

Jadi nama bulan setelah 239^{43} bulan lagi dari bulan Juni adalah 11 bulan setelah Juni yaitu Mei

Teorema 26

Jika p adalah suatu bilangan prima dan p tidak membagi a maka $a^{p-1} \equiv 1\ (mod\ p)$

Bukti:

Karena p adalah suatu bilangan prima dan p tidak membagi a maka $(p, a) = 1$

Selanjutnya karena $(p, a) = 1$ maka menurut teorema 8 , $a^{\phi(p)} \equiv 1\ (mod\ p)$

Karena p adalah bilangan prima maka $\phi(p) = p - 1$ dan

$$a^{\phi(p)} \equiv 1\ (mod\ p)$$
$$a^{p-1} \equiv 1\ (mod\ p)$$

Contoh 26:

Carilah nilai x jika $2^{250} \equiv x\ (mod\ 7)$

Penyelesaian:

Karena 7 adalah bil;angan prima, $(2,7) = 1$ dan $\phi(7) = 7 - 1 = 6$ maka

$2^{\phi(7)} \equiv 1\ (mod\ 7) 2^6 \equiv 1 (mod\ 7)$

Sehingga

$2^{250} = 2^{6.41+4} = (2^6)^{41}.2^4 \equiv 1^7.2^4 (mod\ 7) \equiv 16 (mod\ 7)$
$\equiv 2 (mod\ 7)$

Jadi $x = 2$

Teorema 27

Jika $(a, m) = 1$ maka hubungan $ax \equiv b\ (mod\ m)$ mempunyai selesaian $x = a^{\phi(m)-1}.b + tm$

Bukti.

$ax \equiv b\ (mod\ m)$ kita manipulasi bentuk tersebut sehingga x memiliki koefisien 1.

Bentuk manipulasi nya adalah dengan mengalikan $a^{\phi(m)-1}$ pada kedua ruas .

Nilai $a^{\phi(m)-1}$ ini dipilih karena $a^{\phi(m)} = 1\ (\ mod\ m)$ maka $a.a^{\phi(m)-1} = a^{\phi(m)}$

Sehingga

$a^{\phi(m)-1}.ax \equiv a^{\phi(m)-1}.b\ (mod\ m) a^{\phi(m)}.x$
$\equiv a^{\phi(m)-1}.b\ (mod\ m) x \equiv a^{\phi(m)-1}.b\ (mod\ m)$

Karena $tm \equiv 0\ (mod\ m)$ untuk setiap bilangan bulat t maka:

$$x \equiv a^{\phi(m)-1} . b + tm \ (mod\ m)$$

Jadi $x \equiv a^{\phi(m)-1} . b + tm$ adalah selesaian dari $ax \equiv b \ (mod\ m)$

Latihan:

1. Carilah satu contoh sistem residu tereduksi modulo 12 yang mempunyai dua unsur negatif
2. Carilah sisanya jika 11^{35}dibagi 13
3. Jika hari ini hari kamis, maka carilah hari apa 97^{101} hari lagi
4. Carilah digit terakhir lambang bilangan desimal dari 2^{500}
5. Carilah dua digit terakhir lambang bilangan desimal dari 39^{125}

BAB IV
KONGRUENSI LINIER

Pada materi aljabar, kajian utama pada prsamaan adalah adalah mencari akar atau penyelesaian dari sebuah persamaan $f(x) = 0$. Akar atau penyelesaian dari persamaan ini adalah nilai x yang memenuhi persamaan $f(x) = 0$. Sama halnya dengan persamaan pada materi aljabar, kajian utama pada kongruensi adalah mencari nilai bilangan-bilangan bulat yang memenuhi $f(x) \equiv 0(mod\ m)$. Kalimat terbuka yang menggunakan relasi kekongruenan disebut pengkongruenan. Jika suatu pengkongruenan variabelnya berpangkat tertinggi satu disebut pengkongruenan linier atau kongruensi linier.

Misalnya $f(x) = x^3 + 6x^2 - 11 \equiv 0\ (mod\ 5)$

Pengkongruenan tersebut dipenuhi oleh nilai $x = 3$, sebab jika nilai x diganti 3 maka pengkongruenan tersebut akan bernilai benar.

$f(x) = x^3 + 6x^2 - 11 \equiv 0\ (mod\ 5)$

$f(3) = 3^3 + 6.3^2 - 11 \equiv 0\ (mod\ 5)$

$27 + 54 - 11 \equiv 0\ (mod\ 5) 70 \equiv 0\ (mod\ 5)$

Definisi 21

Bentuk umum kongruensi linier adalah $ax \equiv b\ (mod\ m)$

Dengan $a, b, m\ \in Z, a \not\equiv 0\ (mo$

$d\ m)$

Contoh 27:

$3x \equiv 4(mod\ 5)$

Pengkongruenan tersebut bernilai benar jika $x = 3$, yaitu

$3x \equiv 4(mod\ 5) 3.3 \equiv 4(mod\ 5) 9 \equiv 4(mod\ 5)$

Berlaku hal yang sama jika nilai x diganti dengan $\ldots, -2, 8, 13, \ldots$. pengkongruenan tersebut juga akan bernilai benar.

Kita telah mengetahui bahwa $ax \equiv b\ (mod\ m)$ berarti $ax = b + tm$ untuk suatu bilangan bulat t. Misalkan r memenuhi kongruensi linier $ax \equiv b\ (mod\ m)$ maka setiap bilangan bulat $r + m, r + 2m, r + 3m, \dots, r - m, r - 2m, r - 3m, \dots$ juga memenuhi kongruensi linier tersebut. Banyaknya penyelesaian suatu kongruensi linier modulo m adalah banyaknya penyelesaian tidak kongruen modulo m yaitu banyaknya m kelas kongruensi modulo m yang memberikan penyelesaian.

Definisi 22

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 penyelesaian kongruensi

$$f(x) \equiv 0(mod\ m)$$

Adalah banyaknya a_i, dengan $a_i = 0,1,2, \dots, m - 1$ yang memenuhi kongruensi $f(a_i) \equiv 0(mod\ m)$

Contoh 28:

Penyelesaian dari kongruensi linier $f(x) = 2x - 4 \equiv 0(mod\ 6)$ adalah. Langkah pertama yang mudah adalah dengan memilih sistem residu lengkap modulo 6, karena unsur-unsur himpunan tersebut tidak ada yang kongruen . maka penyelesaian dari $2x - 4 \equiv 0(mod\ 6)$ dapat dilakukan denga memilih unsur-unsur $\{0,1,2,3,4,5\}$ yang memenuhi kongruensi, yaitu:

$f(0) = 2.0 - 4 = -4 \not\equiv 0\ (mod\ 6)$
$f(1) = 2.1 - 4 = -2 \not\equiv 0\ (mod\ 6)$
$f(2) = 2.2 - 4 = 0 \equiv 0\ (mod\ 6)$

$f(3) = 2.3 - 4 = 2 \not\equiv 0\ (mod\ 6)$
$f(4) = 2.4 - 4 = 4 \not\equiv 0\ (mod\ 6)$
$f(5) = 2.5 - 4 = 6 \equiv 0\ (mod\ 6)$
Dengan demikian penyelesaian kongruensi adalah $x \equiv 2\ (mod\ 6)$ dan $x \equiv 5\ (mod\ 6)$

Contoh 29:
Kongruensi linier $7x \equiv 3(mod\ 12)$ mempunyai satu penyelesaian, yaitu $x \equiv 9\ (mod\ 12)$ karena dari system residu lengkap modulo 12 yaitu $\{0,1,2,3,4,5,6,7,8,9,10,11\}$ hanya 9 yang memenuhi kongruensi.

Contoh 30:
kongruensi linear $6x \equiv 9\ (mod\ 15)$memiliki tiga penyelesaian. Dengan cara yang sama yaitu memilih anggota dari system residu lengkap modulo 15 yang memenuhi kongruensi. System residu lengkap modulo 15 yaitu $\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$. Kemudian substitusikan anggota dari himpunan tersebut kedalam kongruensi linier,maka nilai yang memenuhi hanya 4,9,14
yaitu.
$6x \equiv 9\ (mod\ 15)$
$6.4 \equiv 24\ (mod\ 15) \equiv 9\ (mod\ 15)$
$6.9 \equiv 54\ (mod\ 15) \equiv 9\ (mod\ 15)$
$6.14 \equiv 84\ (mod\ 15) \equiv 9\ (mod\ 15)$

Teorema 28
Jika $(a, b) = d$ dan kongruensi $ax \equiv b(mod\ m)$mempunyai penyelesaian, maka $d|b$. Jika $d|b$ maka kongruensi $x \equiv b(mod\ m)$ mempunyai d penyelesaian.
Bukti:
$x \equiv b(mod\ m)$ maka menurut definisi $m|ax - b$

Diketahui $d = (a, m)$ maka menurut definisi $d|a$ dan $d|m$
Karena $d|a$ maka sesuai teorema 2.1 $d|ax$ untuk sembarang bilangan bulat x
Selanjutnya, $d|m$ dan $m|ax - b$ sesuai teorema 2,2 $d|ax - b$ berakibat $d| - b$ sehingga $d|b$

Selanjutnya $ax \equiv b(mod\ m)$ dapat dinyatakan sebagai $d\left(\frac{a}{d}\right)x \equiv d\left(\frac{b}{d}\right)\ (mod\ m)$
Sesuai dengan teorema 3.6 a dapat ditentukan $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right)\ (mod\ \frac{m}{d})$
Karena $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ dan $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right)\ (mod\ \frac{m}{d})$ maka menurut teorema 3.10 kongruensi linier $\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right)\ (mod\ \frac{m}{d})$ mempunyai suatu penyelesaian $x = x_0 + t.\frac{m}{d}$ dengan $x_0 \equiv \left(\frac{a}{d}\right)^{\phi(m)-1}.\left(\frac{b}{d}\right)\ (mod\ m)$ dan $t \in Z$
Dengan demikian seluruh penyelesaian 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 31:
Selesaikan kongruensi linier berikut
1. $36x \equiv 8\ (mod\ 102)$
Jawab.
Karena $(36{,}102) = 6$ dan 6 tidak membagi 8 maka $36x \equiv 8\ (mod\ 102)$ tidak memiliki penyelesaian.

2. $3x \equiv 2(mod\ 5)$
Jawab
Karena $(3{,}5) = 1$ dan $1|2$ maka $3x \equiv 2(mod\ 5)$ memiliki 1 penyelesaian yaitu

$x \equiv 4\ (mod\ 5)$

3. $15x \equiv 6\ (mod\ 18)$

Jawab

$(15,18) = 3$ dan $3|6$ maka $15x \equiv 6\ (mod\ 18)$ memiliki 3 penyelesaian, yaitu

$x \equiv 4,10,16\ (mod\ 18)$

4. $144x \equiv 216\ (mod\ 360)$

Jawab

FPB dari 144 dan 360 dapat dicari menggunakan Algoritma Euclides

$360 = 2.144 + 72$

$144 = 2.72 + 0$

Maka $(144,360) = 72$

Kemudian $72|216$ maka $144x \equiv 216\ (mod\ 360)$ memiliki 72 penyelesaian.

Seluruh penyelesaian dapat dicari dengan cara berikut

$$144x \equiv 216\ (mod\ 360) 72\left(\frac{144}{72}\right)x \equiv 72\left(\frac{216}{72}\right)\ (mod\ 360)\left(\frac{144}{72}\right)x$$

$$\equiv \left(\frac{216}{72}\right)\left(mod\left(\frac{360}{72}\right)\right)2x \equiv 3\ (mod\ 5)x$$

$$\equiv 2^3.3(mod\ 5)x \equiv 8.3\ (mod\ 5)x \equiv 24\ (mod\ 5)x$$

$$\equiv 4\ (mod\ 5)$$

Penyelesaian seluruhnya adalah $= x_0, x_0 + 1\left(\frac{m}{d}\right), x_0 + 2\left(\frac{m}{d}\right), \dots, x_0 + (d-1)\left(\frac{m}{d}\right)$

$$x \equiv 4\ , 4 + 1.5\ , 4 + 2.5\ , \dots, 4 + (72-1).5\ (mod\ 360)$$

$$\equiv 4, 9, 14, \dots\ , 359\ (mod\ 360)$$

Dalam menyelesaikan kongruensi linier perhatikan tiga hal

1. $ax \equiv ay\ (mod\ m)$ diselesaikan dengan $x \equiv y\ \left(mod\ \frac{m}{(a,m)}\right)$

2. $ax \equiv ay\ (mod\ m)$ dan $(a, m) = 1$ diselesaikan dengan $x \equiv y\ (mod\ m)$
3. $ax \equiv b\ (mod\ m)$ dengan nilai a, b, m yang relative besar dilakukan dengan menyederhanakan kongruensi. Penyederhanaan kongruensi dapat dilakukan dengan cara.

$ax \equiv b\ (mod\ m)\ maka\ m|ax - b$ sehingga $ax - b = my, \quad \forall y \in Z$
$ax - b = my$ berarti $my + b = ax$ dan akibatnya $a|my + b$ atau $my \equiv -b\ (mod\ a)$
Karena $m > a$ maka m dapat dikecilkan dengan mencari residu terkecil dari m modulo a.
Selanjutnya selesaikan $my \equiv -b\ (mod\ a)$ yang lebih sederhana.
Misalkan penyelesaian nya adalah $y = y_0$ dapat ditentukan. $x_0 = \frac{my_0 + b}{a}$ yang merupakan penyelesaian akhir.

$ax - b = my$ maka $x = \frac{my - b}{a}$

Contoh 32:
Selesaikan kongruensi linier $67320x \equiv 136\ (mod\ 96577)$
Jawab
$(67320,96577)$ dapat dicari mengguanakan Algoritma Euclides:
$96577 = 1.67320 + 29257$
$67320 = 2.29257 + 8806$
$29257 = 3.8806 + 2839$
$8806 = 3.2839 + 2892839 = 9.289 + 238289$
$= 1.238 + 51238 = 4.51 + 3451$
$= 1.34 + 1734 = 2.17 + 0$
$(67320,96577) = 17$ dan $17|136$ maka kongruensi tersebut dapat diselesaikan dan memiliki 17 penyelesaian.
Selanjutnya

$67320x \equiv 136\ (mod\ 96577)$
$17.3960\ x\ \equiv 17.8\ (mod\ 96577)$
$3960x \equiv 8\ \left(mod\ \frac{96577}{17}\right)$
$3960x \equiv 8\ (mod\ 5681)$
Kongruensi $3960x \equiv 8\ (mod\ 5681)$ dapat diselesaikan dengan cara:

$3960x \equiv 8\ (mod\ 5681)$ → $x_0 = \frac{5681\ y_0 + 8}{3960} = 4694$

$5681\ y \equiv\ -8\ (mod\ 3960)$
$1721\ y\ \equiv -8\ (mod\ 3960)$ → $y_0 = \frac{3960\ z_0 - 8}{1721} = 3272$

$3960\ z \equiv 8\ (mod\ 1721)$
$518\ z \equiv 8\ (mod\ 1721)$ → $z_0 = \frac{1721 p_0 + 8}{518} = 1422$

$1721p \equiv -8\ (mod\ 518)$
$167p \equiv -8\ (mod\ 518)$ → $p_0 = \frac{518 q_0 - 8}{167} = 428$

$518q \equiv 8\ (mod\ 167)$
$17q \equiv 8 (mod\ 167)$ → $q_0 = \frac{167 r_0 + 8}{17} = 138$

$167r \equiv -8\ (mod\ 17)$
$14r \equiv -8\ (mod\ 17)$ → $r_0 = \frac{17 s_0 - 8}{14} = 14$

$17s \equiv 8\ (mod\ 14)$
$3s \equiv 8 (mod\ 14)$ → $s_0 = 12$

Penyelesaian kongruensi adalah
$x \equiv 4694, 4694 + 1.5681, \ldots\ , 4694 + 16.5681\ (mod\ 96577)$
$x \equiv 4694, 10375, \ldots\ , 95560\ (mod\ 96577)$

Kita akan lanjutkan pembahasan tentang gabungan dari dua atau lebih kongruensi linier dengan satu variabel. Gabungan ini disebut dengan system kongruensi linier simultan.

Definisi 23:
System kongruensi linier satu variabel
$x \equiv a_1 (mod\ m_1), x \equiv a_2 (mod\ m_2), \ldots\ , x \equiv a_r (mod\ m_r)$ disebut system kongruensi linier simultan

Teorema 29
System kongruensi linier simultan: $x \equiv a_1 (mod\ m_1), x \equiv a_2 (mod\ m_2)$ dapat diselesaikan jika dan hanya jika $a_1 \equiv a_2 (mod\ (m_1, m_2))$

Bukti:
$(\rightarrow)$ diketahui $x \equiv a_1 (mod\ m_1)$ maka sesuai teorema 3.1 $x = a_1 + m_1 k, k \in Z$ selanajutnya dari $x = a_1 + m_1 k$ dan $x \equiv a_2 (mod\ m_2)$ atau $m_1 k \equiv a_2 - a_1 (mod\ m_2)$
Sesuai teorema 4.1 kongruensi linear $x \equiv a_2 (mod\ m_2)$ dapat diselesaikan jika $(m_1, m_2) | a_2 - a_1$ dan sesuai definisi 3.1 $a_1 \equiv a_2 (mod\ (m_1, m_2))$
$(\leftarrow)$ buktikan

Ada tiga cara yang dapat digunakan untuk menyelesaikan system kongruensi linier simultan, yaitu cara biasa, cara iterasi, dan cara china. Kita kan bahas satu persatu

Cara Biasa

Cara ini disebut cara biasa karena kita hanya membuat barisan bilangan yang memenuhi masing-masing kongeuensi lalu mencari nilai perseketuan untuk semua kongruensi.

Contoh 33:

Selesaikan system kongruensi linier simultan $x \equiv 13(mod\ 16)$ dan $x \equiv 5\ (mod\ 14)$

Jawab

Sesuai teorema system kongruensi linier simultan dapat diselesaikan jika dan hanya jika

$a_1 \equiv a_2\big(mod\ (m_1, m_2)\big)$

diketahui $a_1 = 13,\ a_2 = 5,\ m_1 = 16,\ m_2 = 14$

maka

$13 \equiv 5\ \big(mod\ (16,14)\big)13 - 5 \equiv 5 - 5\ (mod\ 2)8 \equiv 0(mod\ 2)$

Kongruensi tersebut benar maka system kongruensi linier tersebut dapat diselesaikan, yaitu

$x \equiv 13(mod\ 16) = 13,29,45,61,77,93,\ldots\ (mod\ 16)$

$x \equiv 5\ (mod\ 14) = 5,19,33,47,61,75,\ldots\ (mod\ 14)$

Unsur persekutuan dari barisan bilangan tersebut adalah 61 sehingga $x \equiv 61\ (mod\ 16)$ dan $x \equiv 61\ (mod\ 14)$

Dan sesuai dengan teorema 3.6 b, $x \equiv 61(mod\ [16,14]) \equiv 61\ (mod\ 112)$

Contoh 34:

Selesaikan system kongruensi linier simultan $x \equiv 15(mod\ 51)$ dan $x \equiv 7\ (mod\ 42)$

Jawab

Diketahui $a_1 = 15,\ a_2 = 7,\ m_1 = 51,\ m_2 = 42$
Maka
$15 \not\equiv 7\ (mod\ (51{,}42))15 - 7 \not\equiv 7 - 7(mod\ 3)8 \not\equiv 0\ (mod\ 3)$
Karena tidak terpenuhi maka system kongruensi linier simultan tersebut tidak dapat diselesaikan

Cara Iterasi

Iterasi berarti proses yang berulang, maka cara ini berarti langkah selanjutnya adalah langkah yang sama seperti langkah sebelumnya, dan terus berulanga.

Contoh 35:

Selesaikan system kongruensi linier simultan $2x \equiv 3\ (mod\ 5), 3x \equiv 2\ (mod\ 7)$, dan $5x \equiv 8\ (mod\ 12)$
Jawab
Terlebih dahulu ubah bentuk konngruensi menjadi bentuk baku, yaitu

$$2x \equiv 3\ (mod\ 5) \quad \rightarrow \quad x \equiv 4\ (mod\ 5)$$
$$3x \equiv 2\ (mod\ 7) \quad \rightarrow \quad x \equiv 3\ (mod\ 7)$$
$$5x \equiv 8\ (mod\ 12) \quad \rightarrow \quad x \equiv 4\ (mod\ 12)$$

Kita selesaikan dua kongruensi terlebih dahulu, sampai ditemukan penyelesaian,
Kemudian penyelesaian yang ditemukan digunakan bersama dengan kongruensi ketiga untuk mendapatkan penyelesaian akhir.
Dari kongruensi pertama $x \equiv 4\ (mod\ 5)$ diperoleh $x = 4 + 5s$,
substitusikan $x = 4 + 5s$ pada kongruensi kedua
$x \equiv 3\ (mod\ 7)4 + 5s \equiv 3(mod\ 7)5s \equiv -1(mod\ 7)5s \equiv 6(mod\ 7)s$
$\equiv 4\ (mod\ 7)$
Atau $s = 4 + 7t$

Substitusi nilai $s = 4 + 7t$ ke $x = 4 + 5s$

$x = 4 + 5s$
$x = 4 + 5(4 + 7t)$
$x = 4 + 20 + 35t$
$x = 24 + 35t$
$x \equiv 24\ (mod\ 35)$

Selanjutnya kita memukan penyelesaian dari kongruensi ketiga dan dari hasil penyelesaian sebelumnya yaitu $x \equiv 24\ (mod\ 35)$ dan $x \equiv 4\ (mod\ 12)$ dengan cara yang sama seperti sebelumnya.

Dari kongruensi $x \equiv 24\ (mod\ 35)$ diperoleh $x = 24 + 35s$
Substitusikan $x = 24 + 35s$ pada kongruensi ketiga
$x \equiv 4\ (mod\ 12) 24 + 35s \equiv 4\ (mod\ 12) 35s \equiv 4 - 24 (mod\ 12) 35s$
$\equiv -20 (mod\ 12) 35s \equiv 4\ (mod\ 12) 11s$
$\equiv 4\ (mod\ 12) s \equiv 8 (mod\ 12)$
Atau $s = 8 + 12t$

Substitusi nilai $s = 8 + 12t$ ke $x = 24 + 35s$ maka
$x = 24 + 35s$
$x = 24 + 35(8 + 12t)$
$x = 24 + 280 + 420t$
$x = 304 + 420t$
$x \equiv 304\ (mod\ 420)$

Cara China

Cara china didasarkan pada teorema sisa china. Sebelum teorema sisa china, kita bahas dulu beberapa teorema sebelumnya

Teorema 30

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 $x, y \in Z$ sehingga $xp_1q + yp_2q = q$

Karena $p_1|q, p_2|q$ 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 $p_1p_2|px_1q$ dan berdasarkan teorema 2,4 $pr|xpq + yqr$ atau $p_1, p_2|q$

Teorema 31 Teorema sisa china

Ditentukan bahwa $m_1, m_2, \ldots, m_r$ adalah bilangan-bilangan positif yang setiap pasang adalah relaatif prima, dan $a_1, a_2, \ldots, a_r$ adalah sebarang r bilangan bulat.

Maka system kongruensi linier simultan:

$$x \equiv a_1 (mod\ m_1), x \equiv a_2 (mod\ m_2), \ldots, x \equiv a_r (mod\ m_r)$$

Mempunyai suatu penyelesaian tunggal modulo $M = m_1.m_2. \ldots .m_r$

Bukti:

Buktikan

Misalkan $M = m_1.m_2. \ldots .m_r$ Ambil $M_i = \frac{M}{m_i}$, 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 ada satu $b_i \in Z$ sedemikian hingga $M_ib_i \equiv 1 (mod\ m_i)$ dan $M_ib_i \equiv 0 (mod\ m_j)$ jika $i \neq j$

Ambil $x = M_1b_1a_1 + M_2b_2a_2 + \ldots + M_rb_ra_r$ maka x adalah suatu penyelesaian simultan dari r kongruensi linier. Untuk menunjukkan hal ini, kita harus membuktikan bahwa $wax \equiv a_i (mod\ m_i)$ untuk $i = 1,2,3, \ldots, r$

$$x = M_1 b_1 a_1 + M_2 b_2 a_2 + \ldots + M_r b_r a_r$$
$$\equiv M_1 b_1 a_1 + M_2 b_2 a_2 + \ldots + M_i b_i a_i + \cdots + M_r b_r a_r \ (mod\ m_i)$$
$$\equiv 0.a_1 + 0.a_2 + \ldots + M_i b_i a_i + \cdots + M_r b_r a_r \ (mod\ m_i)$$

Contoh 36:

Selesaikan sistem kongruensi linier simultan
$x \equiv 5(mod\ 8), x \equiv 3(mod\ 7)$, dan $x \equiv 4(mod\ 9)$

Jawab

$x \equiv 5(mod\ 8) \rightarrow a_1 = 5, m_1 = 8$
$x \equiv 3(mod\ 7) \rightarrow a_2 = 3, m_2 = 7$
$x \equiv 4(mod\ 9) \rightarrow a_3 = 4, m_3 = 9$

- $(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$
- $M = m_1 m_2 m_3 = 8.7.9 = 504$
- $\left(\frac{M}{m_1}\right) b_1 \equiv 1(mod\ m_1)$, maka
  $7.9.b_1 \equiv 1(mod\ 8) 7.1 b_1 \equiv 1\ (mod\ 8) 7b_1 \equiv 1(mod\ 8) b_1 = 7$
- $\left(\frac{M}{m_2}\right) b_2 \equiv 1(mod\ m_2)$, maka
  $8.9.b_2 \equiv 1(mod\ 7) 1.2.b_2 \equiv 1\ (mod\ 7) 2b_2 \equiv 1\ (mod\ 7) b_2 = 4$
- $\left(\frac{M}{m_3}\right) b_3 \equiv 1(mod\ m_3)$, maka
  $8.7.b_3 \equiv 1(mod\ 9) - 1.-2.b_3 \equiv 1\ (mod\ 9) 2b_3 \equiv 1\ (mod\ 9) b_3 = 5$

Jadi

$x = M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3$
$= m_2 m_3 b_1 a_1 + m_1 m_3 b_2 a_2 + m_1 m_2 b_3 a_3$
$= 7.9.7.5 + 8.9.4.3 + 8.7.5.4$

$= 4189x$
$\equiv 4189\ (mod\ 504)$
$x \equiv 157(mod\ 504)$

Contoh 37:
selesaikan system kongruensi linier simultan $3x \equiv 2(mod\ 5), 4x \equiv 3(mod\ 7), 8x \equiv 5(mod\ 9), 4x \equiv 7(mod\ 11)$
jawab
ubah masing-masing kongruensi linier menjadi bentuk baku

$3x \equiv 2(mod\ 5) \rightarrow x \equiv 4(mod\ 5)$
$4x \equiv 3(mod\ 7) \rightarrow x \equiv 6\ (mod\ 7)$
$8x \equiv 5(mod\ 9) \rightarrow x \equiv 4(mod\ 9)$
$4x \equiv 7(mod\ 11) \rightarrow x \equiv 10(mod\ 11)$

Diketahui:

- $a_1 = 4, a_2 = 6, a_3 = 4, a_4 = 10, m_1 = 5, m_2 = 7, m_3 = 9, m_4 = 11$
- $(m_1, m_2) = (m_1, m_3) = (m_1, m_4) = (m_2, m_3) = (m_2, m_4) = (m_3, m_4) = 1$
- $M = m_1 m_2 m_3 m_4 = 5.7.9.11 = 3465$
  Kemudian:
- $\left(\frac{M}{m_1}\right) b_1 \equiv 1(mod\ m_1)$, maka
  $7.9.11.\, b_1 \equiv 1(mod\ 5) 2.4.1.\, b_1 \equiv 1\ (mod\ 5) 8b_1 \equiv 1(mod\ 5) b_1 = 2$
- $\left(\frac{M}{m_2}\right) b_2 \equiv 1(mod\ m_2)$, maka
  $5.9.11.\, b_2 \equiv 1(mod\ 7) 5.2.4.\, b_2 \equiv 1\ (mod\ 7) 40b_2 \equiv 1\ (mod\ 7) 5b_2 \equiv 1\ (mod\ 7) b_2 = 3$
- $\left(\frac{M}{m_3}\right) b_3 \equiv 1(mod\ m_3)$, maka

$5.7.11.\, b_3 \equiv 1(mod\ 9) 5.7.2.\, b_3 \equiv 1\ (mod\ 9) 70 b_3$
$\equiv 1\ (mod\ 9) 7 b_3 \equiv 1(mod\ 9) b_3 = 4$

- $\left(\frac{M}{m_4}\right) b_4 \equiv 1(mod\ m_4)$, maka
  $5.7.9.\, b_4 \equiv 1(mod\ 11) 315.\, b_4 \equiv 1\ (mod\ 11) 7 b_4 \equiv 1(mod\ 11) b_4$
  $= 8$

$$x = M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 + M_4 b_4 a_4$$
$$= m_2 m_3 m_4 b_1 a_1 + m_1 m_3 m_4 b_2 a_2$$
$$+ m_1 m_2 m_4 b_3 a_3 + m_1 m_2 m_3 b_3 a_3$$
$$= 7.9.11.2.4 + 5.9.11.3.6 + 5.7.11.4.4$$
$$+ 5.7.9.8.10 = 4581 x \equiv 4581\ (mod\ 3465) x$$
$$\equiv 769 (mod\ 3465)$$

Latihan

1. Selesaikan system kongruensi linier $29393x \equiv 4743(mod\ 2805)$
2. Selesaikan system kongruensi linier simultan $2x \equiv 8\ (mod\ 20)$ dan $3x \equiv 2\ (mod\ 7)$
3. Selesaikan system kongruensi linier simultan $x \equiv 1\ (mod\ 2), x \equiv 1(mod\ 3), x \equiv 1(mod\ 4), x \equiv 1(mod\ 5), x \equiv 2(mod\ 7), x \equiv 2(mod\ 11)$
4. 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 didalam keranjang?

Daftar Pustaka

Muhsetyo, Gatot. 2011. *Teori Bilangan*. Jakarta: Universitas Terbuka

Sukirman. 2006. *Pengantar Teori Bilangan*. Yogyakarta: Hanggar Kreator