

# Teori Bilangan

## (Bagian 1)

(Update 2026)

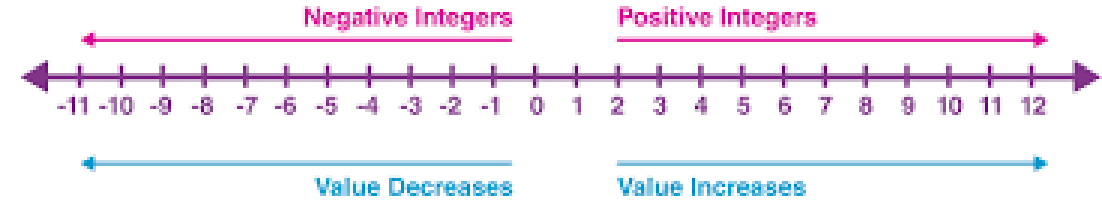


Bahan Kuliah IF1220 Matematika Diskrit

Oleh: Rinaldi M

**Program Studi Teknik Informatika**  
**STEI-ITB**

# Bilangan Bulat



- **Teori bilangan** adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (*integer*) atau fungsi bernilai bilangan bulat.
- Bilangan bulat (*integer*): bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, 8765, -34, 0, -13451, dsb
- Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02, -0.00234

# Sifat Pembagian pada Bilangan Bulat

- Misalkan  $a$  dan  $b$  bilangan bulat,  $a \neq 0$ .  
 $a$  **habis membagi**  $b$  ( $a$  divides  $b$ ) jika terdapat bilangan bulat  $c$  sedemikian sehingga  $b = ac$ .
- Notasi:  $a|b$  jika  $b = ac$ , yang dalam hal ini  $c \in \mathbf{Z}$  dan  $a \neq 0$ .
- **Contoh 1:**  $4|12$  karena  $12/4 = 3$  (bilangan bulat) atau  $12 = 4 \times 3$ .  
Tetapi  $4 \nmid 13$  karena  $13/4 = 3.25$  (bukan bilangan bulat).

# Teorema Euclidean

**Teorema 1 (Teorema Euclidean).** Misalkan  $m$  dan  $n$  bilangan bulat,  $n > 0$ . Jika  $m$  dibagi dengan  $n$  maka hasil pembagiannya adalah  $q$  (*quotient*) dan sisanya  $r$  (*remainder*), sedemikian sehingga

$$m = nq + r$$

dengan  $0 \leq r < n$ .

Catatan: Selalu diingat: sisa ( $r$ ) tidak boleh negatif

## Contoh 2.

(i)  $20/3 = 6$ , sisa 2  $\rightarrow 20 = 6 \cdot 3 + 2$

(ii)  $1987/97 = 20$ , sisa 47  $\rightarrow 1987 = 20 \cdot 97 + 47$

(iii)  $300/100 = 3$ , sisa 0  $\rightarrow 300 = 3 \cdot 100 + 0$

(iv)  $-22/3 = -8$ , sisa 2  $\rightarrow -22 = (-8) \cdot 3 + 2$

tetapi jika pembagiannya sebagai berikut:

$$-22/3 = -7 \text{ sisa } -1$$

$$-22 = (-7) \cdot 3 - 1 \quad (\text{salah!!}, \text{ karena } r = -1 \text{ (syarat } 0 \leq r < n))$$

# Pembagi Bersama Terbesar (PBB)

- Misalkan  $a$  dan  $b$  bilangan bulat tidak nol.
- Pembagi bersama terbesar (PBB – **greatest common divisor** atau  $\gcd$ ) dari  $a$  dan  $b$  adalah bilangan bulat terbesar  $d$  sedemikian hingga  $d \mid a$  dan  $d \mid b$ .
- Dalam hal ini kita nyatakan bahwa  $\text{PBB}(a, b) = d$ .

Di sekolah dasar, istilah “pembagi bersama terbesar” sering disebut “faktor persekutuan terbesar” atau FPB

- **Contoh 3.**  $PBB(45, 36) = ?$

Faktor pembagi 45: 1, 3, 5, 9, 15, 45;

Faktor pembagi 36: 1, 2, 3, 4, 9, 12, 18, 36;

Faktor pembagi bersama 45 dan 36: 1, 3, 9 → terbesar = 9

→  $PBB(45, 36) = 9$ .

- **Teorema 2.** Misalkan  $m$  dan  $n$  bilangan bulat, dengan syarat  $n > 0$  sedemikian sehingga

$$m = nq + r, \quad 0 \leq r < n$$

maka  $\text{PBB}(m, n) = \text{PBB}(n, r)$

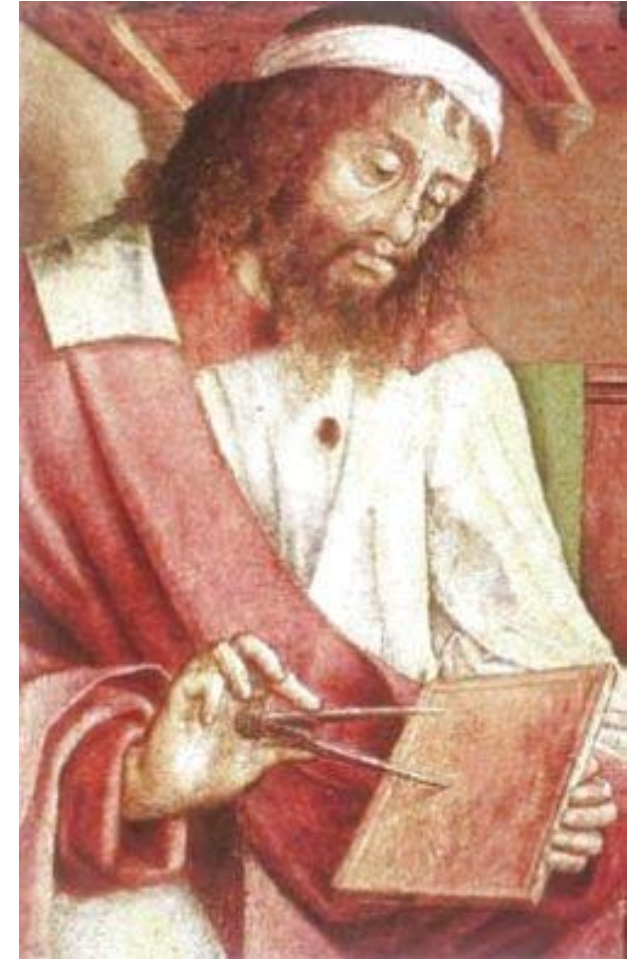
- **Contoh 4:**  $m = 60, n = 18,$

$$60 = 3 \cdot 18 + 6$$

maka  $\text{PBB}(60, 18) = \text{PBB}(18, 6) = 6$

# Algoritma Euclidean

- Tujuan: algoritma untuk mencari PBB dari dua buah bilangan bulat.
- Penemu: Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, *Element*.





- Lukisan Euclides versi lain

Misalkan  $m$  dan  $n$  adalah bilangan bulat tak negatif dengan  $m \geq n$ . Misalkan  $r_0 = m$  dan  $r_1 = n$ .  
Lakukan secara berturut-turut pembagian untuk memperoleh

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

Menurut Teorema 2,

**Teorema 2.** Misalkan  $m$  dan  $n$  bilangan bulat, dengan syarat  $n > 0$  sedemikian sehingga  $m = nq + r$ ,  $0 \leq r < n$  maka  $\text{PBB}(m, n) = \text{PBB}(n, r)$

$$\begin{aligned} \text{PBB}(m, n) &= \text{PBB}(r_0, r_1) = \text{PBB}(r_1, r_2) = \dots = \\ &\text{PBB}(r_{n-2}, r_{n-1}) = \text{PBB}(r_{n-1}, r_n) = \text{PBB}(r_n, 0) = r_n \end{aligned}$$

Jadi, PBB dari  $m$  dan  $n$  adalah sisa terakhir yang tidak nol dari runtunan pembagian tersebut

Diberikan dua buah bilangan bulat tak-negatif  $m$  dan  $n$  ( $m \geq n$ ). Algoritma Euclidean berikut mencari pembagi bersama terbesar dari  $m$  dan  $n$ .

### **Algoritma Euclidean**

1. Jika  $n = 0$  maka  
     $m$  adalah PBB( $m, n$ );  
    stop.  
tetapi jika  $n \neq 0$ ,  
    lanjutkan ke langkah 2.
2. Bagilah  $m$  dengan  $n$  dan misalkan  $r$  adalah sisanya.
3. Ganti nilai  $m$  dengan nilai  $n$  dan nilai  $n$  dengan nilai  $r$ , lalu ulang kembali ke langkah 1.

```

procedure Euclidean(input m, n : integer,
                     output PBB : integer)
{ Mencari PBB(m, n) dengan syarat m dan n bilangan tak-
  negatif dan  $m \geq n$ 
  Masukan: m dan n,  $m \geq n$  dan  $m, n \geq 0$ 
  Keluaran: PBB(m, n)
}

```

**Kamus**

r : integer

**Algoritma:**

```

while n  $\neq$  0 do
  r  $\leftarrow$  m mod n
  m  $\leftarrow$  n
  n  $\leftarrow$  r
endwhile
{ n = 0, maka PBB(m, n) = m }
PBB  $\leftarrow$  m

```

**Contoh 4.**  $m = 80$ ,  $n = 12$  dan dipenuhi syarat  $m \geq n$

$$\begin{array}{c} 80 = 6 \cdot 12 + 8 \\ \swarrow \quad \searrow \\ 12 = 1 \cdot 8 + 4 \\ \swarrow \quad \searrow \\ 8 = 2 \cdot 4 + 0 \end{array}$$

Sisa pembagian terakhir sebelum 0 adalah 4, maka  $\text{PBB}(80, 12) = 4$ .

**Contoh 5.** Tentukan PBB(312, 70).

Jawaban:

$$312 = 4 \cdot 70 + 32$$

$$70 = 2 \cdot 32 + 6$$

$$32 = 5 \cdot 6 + 2$$

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

Sisa pembagian terakhir sebelum 0 adalah 2, maka **PBB(312, 70) = 2**

# Kombinasi Linier

- $\text{PBB}(a,b)$  dapat dinyatakan sebagai **kombinasi linier** (*linear combination*)  $a$  dan  $b$  dengan koefisien-koefisiennya.
- **Contoh 6:**  $\text{PBB}(80, 12) = 4 \rightarrow 4 = (-1) \cdot 80 + 7 \cdot 12$ .
- **Teorema 3.** Misalkan  $a$  dan  $b$  bilangan bulat positif, maka terdapat bilangan bulat  $m$  dan  $n$  sedemikian sehingga  $\text{PBB}(a, b) = ma + nb$ .

- **Contoh 7:** Nyatakan PBB(21, 45) sebagai kombinasi linier dari 21 dan 45.

Penyelesaian:

$$45 = 2 \cdot 21 + 3 \quad (\text{i})$$

$$21 = 7 \cdot 3 + 0 \quad (\text{ii})$$

Sisa pembagian terakhir sebelum 0 adalah 3, maka **PBB(45, 21) = 3**

Dari persamaan (i) dapat dituliskan:

$$\mathbf{3 = 45 - 2 \cdot 21 = 1 \cdot 45 - 2 \cdot 21}$$

Jadi 3 merupakan kombinasi linier dari 45 dan 21

**Contoh 8:** Nyatakan PBB(312, 70) sebagai kombinasi linier 312 dan 70.

Jawaban: Terapkan algoritma Euclidean untuk memperoleh PBB(312, 70):

$$312 = 4 \cdot 70 + 32 \quad (\text{i})$$

$$70 = 2 \cdot 32 + 6 \quad (\text{ii})$$

$$32 = 5 \cdot 6 + 2 \quad (\text{iii})$$

$$6 = 3 \cdot 2 + 0 \quad (\text{iv})$$

Sisa pembagian terakhir sebelum 0 adalah 2, maka **PBB(312, 70) = 2**

Susun pembagian nomor (iii) dan (ii) masing-masing menjadi

$$2 = 32 - 5 \cdot 6 \quad (\text{iv})$$

$$6 = 70 - 2 \cdot 32 \quad (\text{v})$$

Sulihkan (v) ke dalam (iv) menjadi

$$2 = 32 - 5 \cdot (70 - 2 \cdot 32) = 1 \cdot 32 - 5 \cdot 70 + 10 \cdot 32 = 11 \cdot 32 - 5 \cdot 70 \quad (\text{vi})$$

Susun pembagian nomor (i) menjadi

$$32 = 312 - 4 \cdot 70 \quad (\text{vii})$$

Sulihkan (vii) ke dalam (vi) menjadi

$$2 = 11 \cdot 32 - 5 \cdot 70 = 11 \cdot (312 - 4 \cdot 70) - 5 \cdot 70 = 11 \cdot 312 - 49 \cdot 70$$

Jadi,  $\text{PBB}(312, 70) = 2 = 11 \cdot 312 - 49 \cdot 70$

# Relatif Prima

- Dua buah bilangan bulat  $a$  dan  $b$  dikatakan *relatif prima* jika  $PBB(a, b) = 1$ .
- **Contoh 9.**
  - (i) 20 dan 3 relatif prima sebab  $PBB(20, 3) = 1$
  - (ii) 7 dan 11 relatif prima karena  $PBB(7, 11) = 1$
  - (iii) 20 dan 5 tidak relatif prima sebab  $PBB(20, 5) = 5 \neq 1$
  - (iv) 31 dan 0 tidak relative prima sebab  $PBB(31, 0) = 31$

- Dikaitkan dengan kombinasi linier, jika  $a$  dan  $b$  relatif prima, maka terdapat bilangan bulat  $m$  dan  $n$  sedemikian sehingga

$$ma + nb = 1$$

- **Contoh 10.** Bilangan 20 dan 3 adalah relatif prima karena  $\text{PBB}(20, 3) = 1$ , atau dapat ditulis

$$2 \cdot 20 + (-13) \cdot 3 = 1 \quad (m = 2, n = -13)$$

Tetapi 20 dan 5 tidak relatif prima karena  $\text{PBB}(20, 5) = 5 \neq 1$  sehingga 20 dan 5 tidak dapat dinyatakan dalam  $m \cdot 20 + n \cdot 5 = 1$ .

# Aritmetika Modular

- Misalkan  $a$  dan  $m$  bilangan bulat ( $m > 0$ ). Operasi  $a \bmod m$  (dibaca “ $a$  modulo  $m$ ”) memberikan sisa  $r$  jika  $a$  dibagi dengan  $m$  ( $a \mathbf{div} m$ )
- Notasi:  $a \bmod m = r$  sedemikian sehingga  $a = mq + r$ , dengan  $0 \leq r < m$ , dan  $q = a \mathbf{div} m$
- $m$  disebut **modulus** atau **modulo**, dan hasil aritmetika dalam modulo  $m$  terletak di dalam himpunan  $\{0, 1, 2, \dots, m - 1\}$ .

- **Contoh 11.** Beberapa hasil operasi dengan operator modulo:

$$(i) \quad 23 \bmod 5 = 3 \qquad (23 = 5 \cdot 4 + 3)$$

$$(ii) \quad 27 \bmod 3 = 0 \qquad (27 = 3 \cdot 9 + 0)$$

$$(iii) \quad 6 \bmod 8 = 6 \qquad (6 = 8 \cdot 0 + 6)$$

$$(iv) \quad 0 \bmod 12 = 0 \qquad (0 = 12 \cdot 0 + 0)$$

$$(v) \quad -41 \bmod 9 = -5 \qquad (-41 = (9)(-4) - 5) \rightarrow \text{salah karena } r < 0$$

$$\quad -41 \bmod 9 = 4 \qquad (-41 = 9(-5) + 4) \rightarrow \text{betul}$$

$$(vi) \quad -39 \bmod 13 = 0 \qquad (-39 = 13(-3) + 0)$$

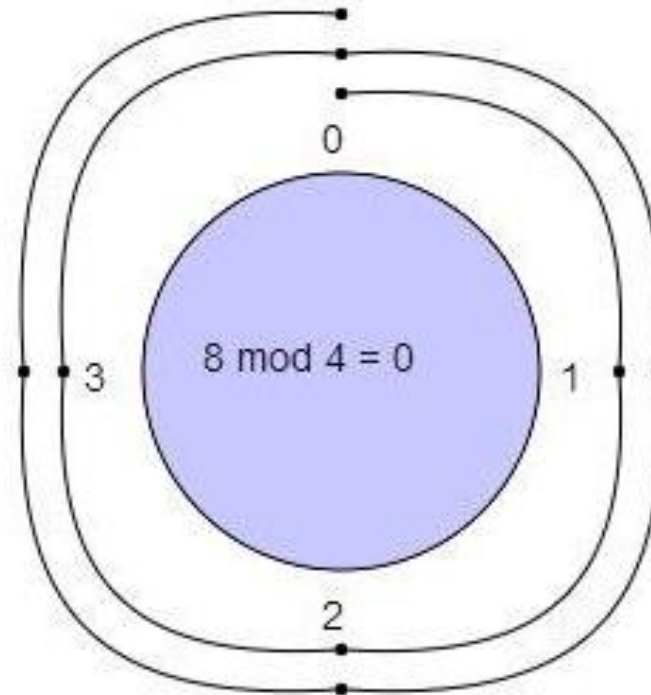
- *Penjelasan untuk (v):* Karena  $a$  negatif, bagi  $|a|$  dengan  $m$  mendapatkan sisa  $r'$ . Maka  $a \bmod m = m - r'$  bila  $r' \neq 0$ .

Jadi  $|-41| \bmod 9 = 5$ , sehingga  $-41 \bmod 9 = 9 - 5 = 4$ .

# $8 \bmod 4 = ?$

With a modulus of 4 we make a clock with numbers 0,1,2,3

We start at 0 and go through 8 numbers in a clockwise sequence 1,2,3,0,1,2,3,0



We ended up at 0

so:

$$8 \bmod 4 = 0$$

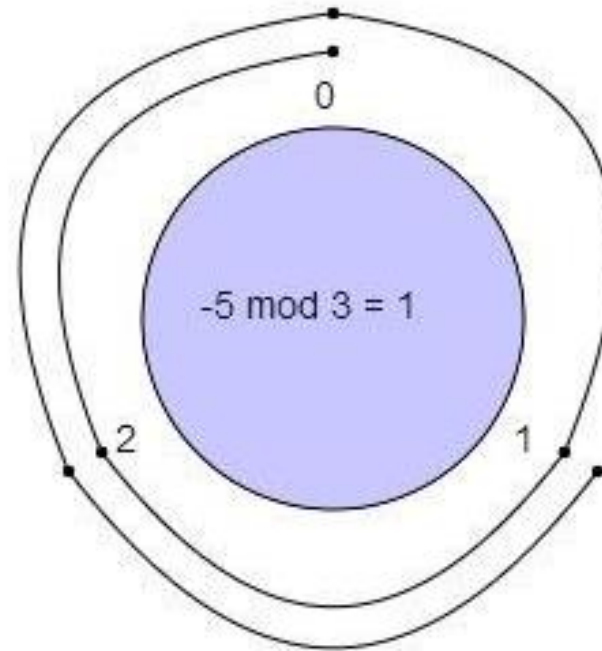
Sumber: [www.khancademy.org](http://www.khancademy.org)

# $-5 \bmod 3 = ?$

With a modulus of 3 we we make a clock with numbers 0,1,2

We start at 0 and go through 5 numbers in **counter-clockwise** sequence (5 is **negative**)

2,1,0,2,1



We ended up at 1

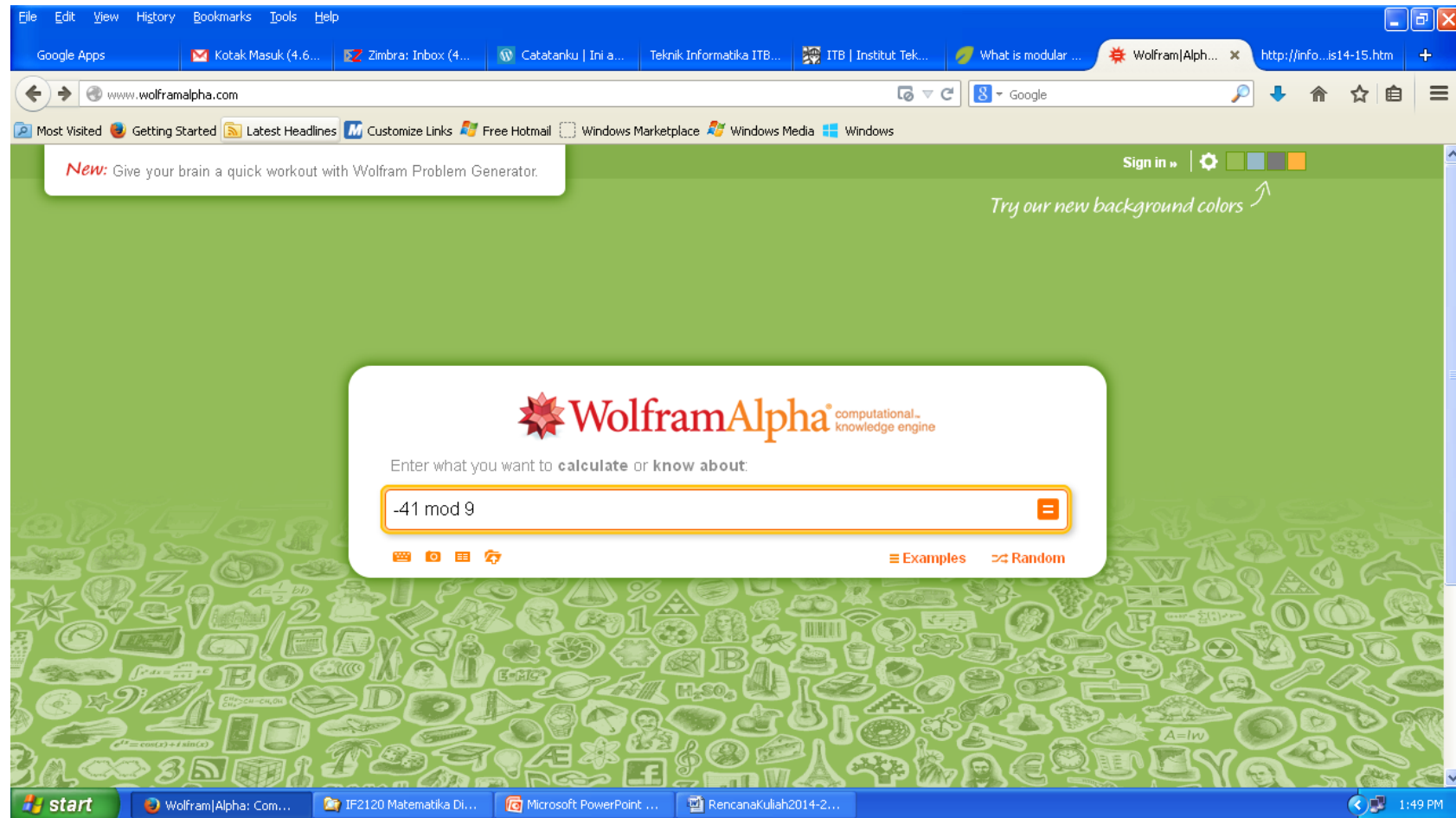
so:

$$-5 \bmod 3 = 1$$

Sumber: [www.khanacademy.org](http://www.khanacademy.org)

# Aritmetika Modulo di dalam Wolfram Alpha

- Kunjungi: [www.wolframalpha.com](http://www.wolframalpha.com)



File Edit View History Bookmarks Tools Help

Google Apps Kotak Masuk (4.6... Zimbra: Inbox (4... Catatanku | Ini a... Teknik Informatika ITB... ITB | Institut Tek... What is modular ... -41 mod 9 - ... x http://info...is14-15.htm +

www.wolframalpha.com/input/?i=-41+mod+9 Google

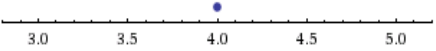
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Input:  
 $(-41) \bmod 9$

Result:  
4

Number name:  
four

Visual representation:  
• • • •

Number line:  


Integers congruent to 4 mod 9: 13, 22, 31, 40, 49, 58, 67, 76, 85, 94, ... [More](#)

Clock representation:  


Share:  
f  
t  
more

New to Wolfram|Alpha?  
  
[Take the Tour >>](#)

Perplexed by a problem?  


start -41 mod 9 - Wolfram|... IF2120 Matematika Di... Microsoft PowerPoint ... RencanaKuliah2014-2... 1:50 PM

# Kekongruenan

- Misalnya  $38 \bmod 5 = 3$  dan  $13 \bmod 5 = 3$ , maka dikatakan

$$38 \equiv 13 \pmod{5}$$

(dibaca: 38 kongruen dengan 13 dalam modulus 5).

- Dalam kehidupan sehari-hari menggunakan jam, kita mengenal:

jam 14.00 = jam 2 siang

$$\rightarrow 14 \equiv 2 \pmod{12}$$

jam 18.00 = jam 6 sore

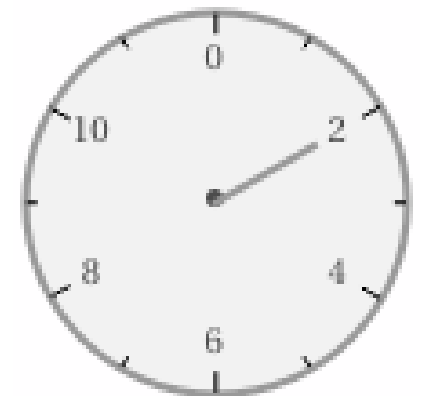
$$\rightarrow 18 \equiv 6 \pmod{12}$$

jam 21.00 = jam 9 malam

$$\rightarrow 21 \equiv 9 \pmod{12}$$

jam 24.00 = jam 0

$$\rightarrow 24 \equiv 0 \pmod{12}$$



- **DEFINISI:** Misalkan  $a$  dan  $b$  bilangan bulat dan  $m$  adalah bilangan  $> 0$ , maka  $a \equiv b \pmod{m}$  jika dan hanya jika  $m \mid (a - b)$ .
- Jika  $a$  **tidak** kongruen dengan  $b$  dalam modulus  $m$ , maka ditulis  $a \not\equiv b \pmod{m}$ .

- **Contoh 12.**

$$17 \equiv 2 \pmod{3}$$

*( 3 habis membagi  $17 - 2 = 15$  )*

$$21 \equiv 9 \pmod{12}$$

*( 12 habis membagi  $21 - 9 = 12$  )*

$$-7 \equiv 15 \pmod{11}$$

*( 11 habis membagi  $-7 - 15 = -22$  )*

$$12 \not\equiv 2 \pmod{7}$$

*( 7 tidak habis membagi  $12 - 2 = 10$  )*

$$-7 \not\equiv 15 \pmod{3}$$

*( 3 tidak habis membagi  $-7 - 15 = -22$  )*

## Catatan:

1. Tanda  $\equiv$  tidak sama maknanya dengan  $=$
2. Penulisan **mod** di dalam tanda kurung ( ) pada notasi  $b \equiv a \pmod{m}$  bukan menyatakan operasi perhitungan sisa pembagian seperti pada  $d = c \bmod m$ .  
 $25 \equiv 4 \pmod{7}$  artinya 25 kongruen dengan 4 di dalam modulus 7  
tetapi  
 $23 \bmod 7 = 2$  artinya 23 dibagi 7 adalah 3 dan memberikan sisa 2
3. Menuliskan  $a \equiv b \pmod{m}$  dan  $b \equiv a \pmod{m}$  sama saja  
Contoh:  $25 \equiv 4 \pmod{7}$  dan  $4 \equiv 25 \pmod{7}$  adalah sama
4. Jika  $a > m$  pada  $a \pmod{m}$ , maka penulisannya dapat disederhanakan dengan sisa pembagian  $a$  dengan  $m$   
Contoh:  $27 \pmod{4} \equiv 3 \pmod{4}$

**DEFINISI:** Misalkan  $a$  dan  $b$  bilangan bulat dan  $m > 0$ , maka  $a \equiv b \pmod{m}$  jika dan hanya jika  $m \mid (a - b)$ .

# Latihan 1

Tentukan semua bilangan yang kongruen dengan 5 (mod 11).

Penyelesaian:

**Cara 1:**

Tambahkan 5 dengan 11 ke kanan, hasilnya ditambah lagi dengan 11, begitu seterusnya secara berulang-ulang.

Kurangkan 5 dengan 11 ke kiri, hasilnya dikurangi lagi dengan 11, begitu seterusnya secara berulang-ulang.

$$\begin{array}{ccccccccccc} \dots & -28 & & -17 & & -6 & & 5 & & 16 & & 27 & & 38 & & 49 & \dots \\ & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & \underbrace{\hspace{1cm}} & & & \\ & -11 & & -11 & & -11 & & +11 & & +11 & & +11 & & +11 & & & \end{array}$$

Jadi, nilai-nilai yang kongruen dengan 5 (mod 11) adalah  $\dots, -17, -6, 16, 27, 38, \dots$

## Cara 2:

Misalkan bilangan yang kongruen dengan 5 (mod 11) adalah  $x$ .

$$x \equiv 5 \pmod{11}$$

Jadi,  $11 \mid (x - 5)$ , atau  $\frac{x-5}{11} = \text{bilangan bulat}$

Nilai  $x$  yang memenuhi sehingga  $(x - 5)/11$  hasilnya bilangan bulat adalah 16, 27, 38, ..., lalu -6, -17, ...

- Jadi, nilai-nilai yang kongruen dengan 5 (mod 11) adalah  
..., -17, -6, 16, 27, 38, ...

- $a \equiv b \pmod{m}$  dalam bentuk “sama dengan” dapat dituliskan sebagai:

$$a = b + km$$

( $k$  adalah bilangan bulat)

- **Contoh 13.**

$$17 \equiv 2 \pmod{3} \quad \rightarrow 17 = 2 + 5 \cdot 3 \quad (k = 5)$$

$$-7 \equiv 15 \pmod{11} \quad \rightarrow -7 = 15 + (-2)11 \quad (k = -2)$$

- $a \bmod m = r$  dapat juga ditulis sebagai  $a \equiv r \pmod{m}$

- **Contoh 14.**

- (i)  $23 \bmod 5 = 3 \quad \rightarrow 23 \equiv 3 \pmod{5}$
- (ii)  $27 \bmod 3 = 0 \quad \rightarrow 27 \equiv 0 \pmod{3}$
- (iii)  $6 \bmod 8 = 6 \quad \rightarrow 6 \equiv 6 \pmod{8}$
- (iv)  $0 \bmod 12 = 0 \quad \rightarrow 0 \equiv 0 \pmod{12}$
- (v)  $-41 \bmod 9 = 4 \quad \rightarrow -41 \equiv 4 \pmod{9}$
- (vi)  $-39 \bmod 13 = 0 \quad \rightarrow -39 \equiv 0 \pmod{13}$

**Teorema 4.** Misalkan  $m$  adalah bilangan bulat positif.

1) Jika  $a \equiv b \pmod{m}$  dan  $c$  adalah sembarang bilangan bulat maka

(i)  $(a + c) \equiv (b + c) \pmod{m}$

(ii)  $ac \equiv bc \pmod{m}$

(iii)  $a^p \equiv b^p \pmod{m}$  ,  $p$  bilangan bulat tak-negatif

artinya, kedua ruas dapat ditambah, dikali, atau dipangkatkan dengan sebuah konstanta

2) Jika  $a \equiv b \pmod{m}$  dan  $c \equiv d \pmod{m}$ , maka

(i)  $(a + c) \equiv (b + d) \pmod{m}$

(ii)  $ac \equiv bd \pmod{m}$

artinya, dua buah bilangan bulat dengan modulus yang sama dapat dijumlahkan atau dikalikan

*Bukti* (hanya untuk 1(ii) dan 2(i) saja):

$$ac \equiv bc \pmod{m}$$

1(ii)  $a \equiv b \pmod{m}$  berarti:

$$\Leftrightarrow a = b + km$$

$$\Leftrightarrow a - b = km$$

$$\Leftrightarrow (a - b)c = ckm$$

$$\Leftrightarrow ac = bc + Km$$

$$\Leftrightarrow ac \equiv bc \pmod{m} \quad \blacksquare$$

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

$$2(i) \quad a \equiv b \pmod{m} \quad \Leftrightarrow \quad a = b + k_1m$$

$$c \equiv d \pmod{m} \quad \Leftrightarrow \quad c = d + k_2m +$$

$$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$$

$$\Leftrightarrow (a + c) = (b + d) + km \quad (k = k_1 + k_2)$$

$$\Leftrightarrow (a + c) \equiv (b + d) \pmod{m} \quad \blacksquare$$

## Contoh 15.

Misalkan  $17 \equiv 2 \pmod{3}$  dan  $10 \equiv 4 \pmod{3}$ , maka menurut Teorema 4,

$$17 + 5 \equiv 2 + 5 \pmod{3} \iff 22 \equiv 7 \pmod{3} \quad \text{periksa } 3 \mid (22 - 7)$$

$$17 \cdot 5 \equiv 2 \cdot 5 \pmod{3} \iff 85 \equiv 10 \pmod{3} \quad \text{periksa } 3 \mid (85 - 10)$$

$$17 + 10 \equiv 2 + 4 \pmod{3} \iff 27 \equiv 6 \pmod{3} \quad \text{periksa } 3 \mid (27 - 6)$$

$$17 \cdot 10 \equiv 2 \cdot 4 \pmod{3} \iff 170 \equiv 8 \pmod{3} \quad \text{periksa } 3 \mid (170 - 8)$$

- Teorema 4 tidak memasukkan operasi pembagian pada aritmetika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi.

- **Contoh 16:**

$10 \equiv 4 \pmod{3}$  dapat dibagi dengan 2

karena  $10/2 = 5$  dan  $4/2 = 2$ , dan  $5 \equiv 2 \pmod{3}$

$14 \equiv 8 \pmod{6}$  tidak dapat dibagi dengan 2, karena  $14/2 = 7$  dan  $8/2 = 4$ , tetapi  $7 \not\equiv 4 \pmod{6}$ .

# Latihan 2

Buktikan Teorema 4.2(ii), jika  $a \equiv b \pmod{m}$  dan  $c \equiv d \pmod{m}$  maka buktikan bahwa  $ac \equiv bd \pmod{m}$

.

## Penyelesaian:

$$a \equiv b \pmod{m} \rightarrow a = b + k_1 m$$

$$c \equiv d \pmod{m} \rightarrow c = d + k_2 m$$

maka

$$\Leftrightarrow ac = (b + k_1 m)(d + k_2 m)$$

$$\Leftrightarrow ac = bd + bk_2 m + dk_1 m + k_1 k_2 m^2$$

$$\Leftrightarrow ac = bd + Km \quad \text{dengan } K = bk_2 + dk_1 + k_1 k_2 m$$

$$\Leftrightarrow \mathbf{ac \equiv bd \pmod{m}} \quad (\text{terbukti})$$

# Balikan Modulo (modulo invers)

- Di dalam aritmetika bilangan riil, balikan sebuah bilangan yang tidak-nol adalah bentuk pecahannya sedemikian sehingga hasil perkalian keduanya sama dengan 1.
- Jika  $a$  adalah sebuah bilangan tidak-nol, maka balikannya adalah  $1/a$  sedemikian sehingga  $a \times 1/a = 1$ .

Contoh: Balikan 4 adalah  $1/4$ , sebab  $4 \times 1/4 = 1$ .

- Balikan  $a$  dilambangkan dengan  $a^{-1}$ .
- Di dalam aritmetika modular, balikan modulo sebuah bilangan bulat lebih sukar dihitung.

- Diberikan sebuah bilangan bulat  $a(\text{mod } m)$ . Bagaimana menghitung balikan  $a(\text{mod } m)$ ?
- **Syarat:** Jika  $a$  dan  $m$  relatif prima dan  $m > 1$ , maka balikan (*invers*) dari  $a(\text{mod } m)$  ada.
- Balikan dari  $a(\text{mod } m)$  adalah bilangan bulat  $x$  sedemikian sehingga:  
$$xa \equiv 1 (\text{mod } m)$$
- Jadi,  $a^{-1}(\text{mod } m) = x$

Bukti:  $a$  dan  $m$  relatif prima, jadi  $\text{PBB}(a, m) = 1$ , dan terdapat bilangan bulat  $x$  dan  $y$  sedemikian sehingga:

$$xa + ym = 1$$

yang mengimplikasikan bahwa

$$xa + ym \equiv 1 \pmod{m}$$

Karena  $ym \equiv 0 \pmod{m}$  (kenapa?), maka

$$xa \equiv 1 \pmod{m}$$

Kekongruenan yang terakhir ini berarti bahwa  $x$  adalah balikan dari  $a \pmod{m}$ . ■

- Pembuktian di atas juga menceritakan bahwa untuk mencari balikan dari  $a \pmod{m}$ , kita harus membuat kombinasi linier dari  $a$  dan  $m$  sama dengan 1.
- Koefisien  $a$  dari kombinasi linier tersebut merupakan balikan dari  $a \pmod{m}$ .

**Contoh 17.** Tentukan balikan dari 4 (mod 9), 17 (mod 7), dan 18 (mod 10).

Penyelesaian:

(a) Karena  $\text{PBB}(4, 9) = 1$ , maka balikan dari 4 (mod 9) ada. Dari algoritma Euclidean diperoleh bahwa

$$9 = 2 \cdot 4 + 1 \quad (\text{i})$$

$$4 = 4 \cdot 1 + 0 \quad (\text{ii})$$

Susun persamaan (i) menjadi

$$-2 \cdot 4 + 1 \cdot 9 = 1 \quad \text{atau} \quad -2 \cdot 4 + 1 \cdot 9 \equiv 1 \pmod{9}$$

Karena  $1 \cdot 9 \equiv 0 \pmod{9}$ , maka

$$-2 \cdot 4 \equiv 1 \pmod{9}$$

Dari kekongruenan terakhir ini kita peroleh  $-2$  adalah balikan dari 4 (mod 9).

atau dapat juga ditulis  $4^{-1} \pmod{9} = -2 \pmod{9}$  atau  $x = -2 + 9k$ ,  $k \in \mathbb{Z}$ .

- Catatan: setiap bilangan yang kongruen dengan  $-2 \pmod{9}$

juga adalah balikan dari  $4 \pmod{9}$ , misalnya  $\dots, -20, -11, 7, 16, \dots$

$$-20 \equiv -2 \pmod{9} \quad (\text{karena } 9 \text{ habis membagi } -20 - (-2) = -18)$$

$$-11 \equiv -2 \pmod{9} \quad (\text{karena } 9 \text{ habis membagi } -11 - (-2) = -9)$$

$$7 \equiv -2 \pmod{9} \quad (\text{karena } 9 \text{ habis membagi } 7 - (-2) = 9)$$

$$16 \equiv -2 \pmod{9} \quad (\text{karena } 9 \text{ habis membagi } 16 - (-2) = 18)$$

- $\dots, -20, -11, -2, 7, 16, \dots$  diperoleh dengan menambahkan 9 ke kiri atau ke kanan dari  $-2$

(b) Karena  $\text{PBB}(17, 7) = 1$ , maka balikan dari 17 (mod 7) ada. Dari algoritma Euclidean diperoleh rangkaian pembagian berikut:

$$17 = 2 \cdot 7 + 3 \quad (\text{i})$$

$$7 = 2 \cdot 3 + 1 \quad (\text{ii})$$

$$3 = 3 \cdot 1 + 0 \quad (\text{iii}) \quad (\text{yang berarti: } \text{PBB}(17, 7) = 1)$$

Susun (ii) menjadi:

$$1 = 7 - 2 \cdot 3 \quad (\text{iv})$$

Susun (i) menjadi

$$3 = 17 - 2 \cdot 7 \quad (\text{v})$$

Sulihkan (v) ke dalam (iv):

$$1 = 7 - 2 \cdot (17 - 2 \cdot 7) = 1 \cdot 7 - 2 \cdot 17 + 4 \cdot 7 = 5 \cdot 7 - 2 \cdot 17$$

atau

$$-2 \cdot 17 + 5 \cdot 7 = 1 \quad (5 \cdot 7 \equiv 0 \pmod{7})$$

$$-2 \cdot 17 \equiv 1 \pmod{7} \quad (7 \text{ habis membagi } -2 \cdot 17 - 1 = -35)$$

Jadi,  $-2$  adalah balikan dari 17 (mod 7), atau dapat ditulis  $17^{-1} \pmod{7} = -2 \pmod{7}$ .

(c) Menghitung balikan  $18 \pmod{10}$ . Karena  $\text{PBB}(18, 10) = 2 \neq 1$ , maka balikan dari  $18 \pmod{10}$  tidak ada.

# Cara lain menghitung balikan modulo

- Ditanya: balikan dari  $a \pmod{m}$
- Misalkan  $x$  adalah balikan dari  $a \pmod{m}$ , maka

$$ax \equiv 1 \pmod{m} \text{ (definisi balikan modulo)}$$

atau dalam notasi 'sama dengan':

$$ax = 1 + km$$

atau

$$x = (1 + km)/a$$

Cobakan untuk  $k = 0, 1, 2, \dots$  dan  $k = -1, -2, \dots$

Solusinya adalah semua bilangan bulat yang memenuhi.

- **Contoh 18:** Balikan dari 4 (mod 9) adalah  $x$  sedemikian sehingga  $4x \equiv 1 \pmod{9}$

$$4x \equiv 1 \pmod{9} \rightarrow 4x = 1 + 9k \rightarrow x = (1 + 9k)/4$$

$$\text{Untuk } k = 0 \rightarrow x = (1 + 9 \cdot 0)/4 = 1/4 \rightarrow \text{tidak bulat}$$

$$k = 1 \rightarrow x = (1 + 9 \cdot 1)/4 = 10/4 \rightarrow \text{tidak bulat}$$

$$k = 2 \rightarrow x = (1 + 9 \cdot 2)/4 = 19/4 \rightarrow \text{tidak bulat}$$

$$k = 3 \rightarrow x = (1 + 9 \cdot 3)/4 = 7$$

$$k = -1 \rightarrow x = (1 + 9 \cdot -1)/4 = -2$$

Balikan dari 4 (mod 9) adalah 7 (mod 9), -2 (mod 9), dst

Catatan: cukup menemukan satu saja balikan dari 4(mod 9), maka semua bilangan lainnya dapat dicari dengan menambahkan 9 pada bilangan tersebut. Pada contoh di atas 7 adalah balikan 4(mod 9), maka dengan menambahkan 9 ke kiri dan ke kanan diperoleh ..., -11, -2, 7, 16, ...

Secara umum,  $4^{-1} \pmod{9} = 7 + 9k, k \in \mathbb{Z}$

# Latihan 3

- Tentukan semua balikan dari 9 (mod 11).

## Penyelesaian:

- Misalkan  $9^{-1} \pmod{11} = x$
- Maka  $9x \equiv 1 \pmod{11}$  atau  $9x = 1 + 11k$  atau
$$x = (1 + 11k)/9$$

Dengan mencoba semua nilai  $k$  yang bulat ( $k = 0, -1, -2, \dots, 1, 2, \dots$ ) maka diperoleh  $x = 5$ . Semua bilangan lain yang kongruen dengan 5 ( $\pmod{11}$ ) juga merupakan balikan dari 9 ( $\pmod{11}$ ), yaitu  $-6, 16, 27, \dots$

atau dapat ditulis  $9^{-1} \pmod{11} = 5 + 11k, k \in \mathbb{Z}$

# Kekongruenan Linier

- Kekongruenan linier (*linear congruence*) berbentuk:

$$ax \equiv b \pmod{m}$$

( $m > 0$ ,  $a$  dan  $b$  sembarang bilangan bulat, dan  $x$  adalah peubah bilangan bulat).

Pemecahan:  $ax = b + km \rightarrow x = \frac{b + km}{a}$

(Cobakan untuk  $k = 0, 1, 2, \dots$  dan  $k = -1, -2, \dots$  yang menghasilkan  $x$  sebagai bilangan bulat)

**Contoh 19.**

Tentukan solusi:  $4x \equiv 3 \pmod{9}$  dan  $2x \equiv 3 \pmod{4}$

Penyelesaian:

(i)  $4x \equiv 3 \pmod{9}$

$$x = \frac{3 + k \cdot 9}{4}$$

$$k = 0 \rightarrow x = (3 + 0 \cdot 9)/4 = 3/4 \quad (\text{bukan solusi})$$

$$k = 1 \rightarrow x = (3 + 1 \cdot 9)/4 = 3$$

$$k = 2 \rightarrow x = (3 + 2 \cdot 9)/4 = 21/4 \quad (\text{bukan solusi})$$

$k = 3, k = 4$  tidak menghasilkan solusi

$$k = 5 \rightarrow x = (3 + 5 \cdot 9)/4 = 12$$

...

$$k = -1 \rightarrow x = (3 - 1 \cdot 9)/4 = -6/4 \quad (\text{bukan solusi})$$

$$k = -2 \rightarrow x = (3 - 2 \cdot 9)/4 = -15/4 \quad (\text{bukan solusi})$$

$$k = -3 \rightarrow x = (3 - 3 \cdot 9)/4 = -6$$

...

$$k = -6 \rightarrow x = (3 - 6 \cdot 9)/4 = -15$$

...

Nilai-nilai  $x$  yang memenuhi: 3, 12, ... dan  $-6, -15, \dots$

Atau solusi cukup dinyatakan sebagai  $x \equiv 3 \pmod{9}$ , atau  $x = 3 + 9k$ ,  $k$  sembarang bilangan bulat

$$(ii) \ 2x \equiv 3 \pmod{4}$$

$$x = \frac{3 + k \cdot 4}{2}$$

Karena  $4k$  genap dan  $3$  ganjil maka penjumlahannya menghasilkan ganjil, sehingga hasil penjumlahan tersebut jika dibagi dengan  $2$  tidak menghasilkan bilangan bulat. Dengan kata lain, tidak ada nilai-nilai  $x$  yang memenuhi  $2x \equiv 3 \pmod{5}$ .

## Cara lain menghitung solusi $ax \equiv b \pmod{m}$

- Seperti dalam persamaan aljabar biasa (tanpa modulo),  
 $4x = 12 \rightarrow$  kalikan setiap ruas dengan  $1/4$  (yaitu invers 4), maka  
$$(1/4) \cdot 4x = 12 \cdot (1/4) \rightarrow x = 12/4 = 3$$
- $4x \equiv 12 \pmod{9} \rightarrow$  kalikan setiap ruas dengan balikan dari  $4 \pmod{9}$  (dalam hal ini sudah kita hitung, yaitu  $-2$ )  
$$(-2) \cdot 4x \equiv (-2) \cdot 12 \pmod{9} \Leftrightarrow -8x \equiv -24 \pmod{9}$$

Karena  $-8 \equiv 1 \pmod{9}$ , maka  $x \equiv -24 \pmod{9}$ . Semua bilangan bulat yang kongruen dengan  $-24 \pmod{9}$  adalah solusinya, yaitu ...,  $-33, -15, -6, 3, 12$ ,

# Latihan

Tentukan nilai-nilai  $x$  yang memenuhi masing-masing kekongruenan berikut:

(a)  $4x \equiv 8 \pmod{11}$

(b)  $5x \equiv 1 \pmod{61}$

(c)  $2x \equiv 1 \pmod{8}$

(d)  $2^x \equiv 1 \pmod{32}$

# Latihan Soal Teori Bilangan

# Soal 1

- Buktikan untuk setiap bilangan bulat positif  $n$  dan  $a$ ,  $PBB(a, a + n)$  habis membagi  $n$ .

Jawaban:

Misalkan  $\text{PBB}(a, a + n) = d$ .

Maka:

$$d \mid a + n \rightarrow a + n = k_1 d$$

$$d \mid a \rightarrow a = k_2 d -$$

$$\hline a + n - a = (k_1 - k_2)d$$

$$n = Kd \text{ (misal } k_1 - k_2 = K)$$

$$n = Kd \rightarrow d \mid n \text{ (terbukti)}$$

## Soal 2

Perlihatkan bahwa bila  $n \mid m$ , yang dalam hal ini  $n$  dan  $m$  adalah bilangan bulat positif yang lebih besar dari 1, dan jika  $a \equiv b \pmod{m}$  dengan  $a$  dan  $b$  adalah bilangan bulat, maka  $a \equiv b \pmod{n}$ .

- Jawaban:

Diketahui bahwa  $n \mid m$  atau dapat dituliskan sebagai :

$$m = k_1 \cdot n \dots (i)$$

Jika  $a \equiv b \pmod{m}$  maka :

$$a = b + k_2 \cdot m \dots (ii)$$

Substitusikan (i) ke dalam (ii):

$$a = b + k_2 \cdot k_1 \cdot n$$

$$a = b + k_3 \cdot n \quad (\text{misalkan } k_3 = k_2 \cdot k_1) \quad (iii)$$

$$a - b = k_3 \cdot n \quad \text{yang berarti bahwa } n \mid (a - b) \text{ atau}$$

$$a \equiv b \pmod{n} \quad \blacksquare$$

## Soal 3

- Carilah semua bilangan bulat positif yang tidak habis dibagi 2 dan bersisa 2 jika dibagi 3

Carilah semua bilangan bulat positif yang tidak habis dibagi 2 dan bersisa 2 jika dibagi 3

Penyelesaian:

Misal bilangan tersebut adalah  $x = 2k+1$

$$(2k + 1) \bmod 3 = 2 \rightarrow 2k + 1 \equiv 2 \pmod{3}$$

$$2k \equiv 2 - 1 \pmod{3}$$

$$2k \equiv 1 \pmod{3}$$

$$k \equiv 2 \pmod{3}$$

$$k = 2 + 3n$$

Berarti  $x = 2(2 + 3n)+1 = 6n + 5$ ,  $n$  sembarang bilangan bulat

Jadi bilangan-bilangan yang memenuhi adalah  $x = \{..., 5, 11, 17, 23, ...\}$

## Soal 4

- Tentukan  $x$  dan  $y$  bilangan bulat yang memenuhi persamaan
$$312x + 70y = 2,$$
lalu hitunglah nilai dari :  $y \bmod x$ .

$$312x + 70y = 2$$

Jawaban:

Dengan menggunakan algoritma Euclid, ditemukan bahwa :

$$312 = 4.70 + 32 \quad (\text{i})$$

$$70 = 2.32 + 6 \quad (\text{ii})$$

$$32 = 5.6 + 2 \quad (\text{iii})$$

$$6 = 3.2 + 0 \quad (\text{iv})$$

$$\text{Persamaan (iii) dapat dituliskan menjadi : } 2 = 32 - 5.6 \quad (\text{v})$$

$$\text{Persamaan (ii) dapat dituliskan menjadi : } 6 = 70 - 2.32 \quad (\text{vi})$$

Sulihkan persamaan (vi) ke persamaan (v) :

$$2 = 32 - 5.(70 - 2.32)$$

$$2 = 32 - 5.70 + 10.32$$

$$2 = 11.32 - 5.70 \quad (\text{vii})$$

$$\text{Persamaan (i) dapat dituliskan menjadi : } 32 = 312 - 4.70 \quad (\text{viii})$$

Sulihkan persamaan (viii) ke persamaan (vii) :

$$2 = 11.(312 - 4.70) - 5.70$$

$$2 = 11.312 - 44.70 - 5.70$$

$$2 = 11.312 - 49.70 \quad (ix)$$

Dari persamaan (ix) diketahui  $x$  dan  $y$  yang memenuhi adalah

$$x = 11 \text{ dan } y = -49, \text{ sehingga } y \bmod x = -49 \bmod 11 = 6$$

# Bersambung ke Bagian 2