

Teori Bilangan

(Bagian 1)

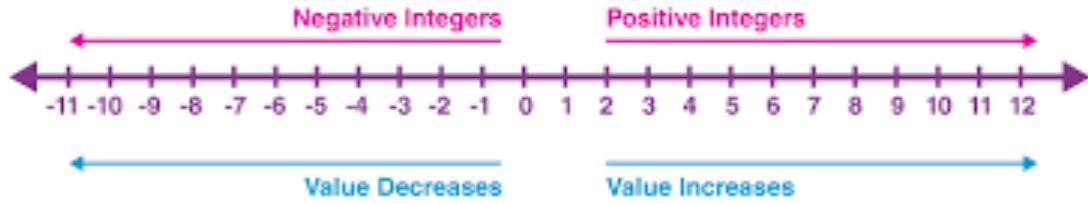
(Update 2023)

Bahan Kuliah IF2120 Matematika Diskrit

Oleh: Rinaldi Munir

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*) adalah 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: $a \mid b$ jika $b = ac$, $c \in \mathbb{Z}$ dan $a \neq 0$.
- **Contoh 1:** $4 \mid 12$ 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

sisa tidak boleh negatif,,
↳ selalu positif.

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 $0 \leq r < n$.

Contoh 2.

(i) $1987/97 = 20$, sisa 47

$$1987 = 20 \cdot 97 + 47$$

(ii) $-22/3 = -8$, sisa 2

$$-22 = (-8) \cdot 3 + 2$$

tetapi jika pembagiannya sebagai berikut:

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

$$-22 = (-7) \cdot 3 - 1 \quad (\text{salah!!})$$

karena $r = -1$ (syarat $0 \leq r < n$)

Pembagi Bersama Terbesar (PBB)

- Misalkan a dan b bilangan bulat tidak nol.

$\text{gcd}(m, n) \rightarrow$

basis: $n = 0 \rightarrow m$

rekursif:

$\text{gcd}(n, m \bmod n)$

$$\begin{aligned}\text{gcd}(8, 12) &:= \text{gcd}(12, 8) \\ &:= \text{gcd}(8, 4) \\ &:= \text{gcd}(4, 0) \\ &:= 4\end{aligned}$$

$$\begin{aligned}12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0\end{aligned}$$

dahberes

$m = q \cdot n + r$
sampai $r \rightarrow 0$, Pbb \rightarrow
sis^q
terakhir
sblm
nol.

$$4 = 12 - 1 \cdot 8$$

- 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 $\text{PBB}(a, b) = d$.

Q smqt.

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

$$m = nq + r, \quad 0 \leq r < n \quad \longrightarrow \text{teorema euclidian}$$

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

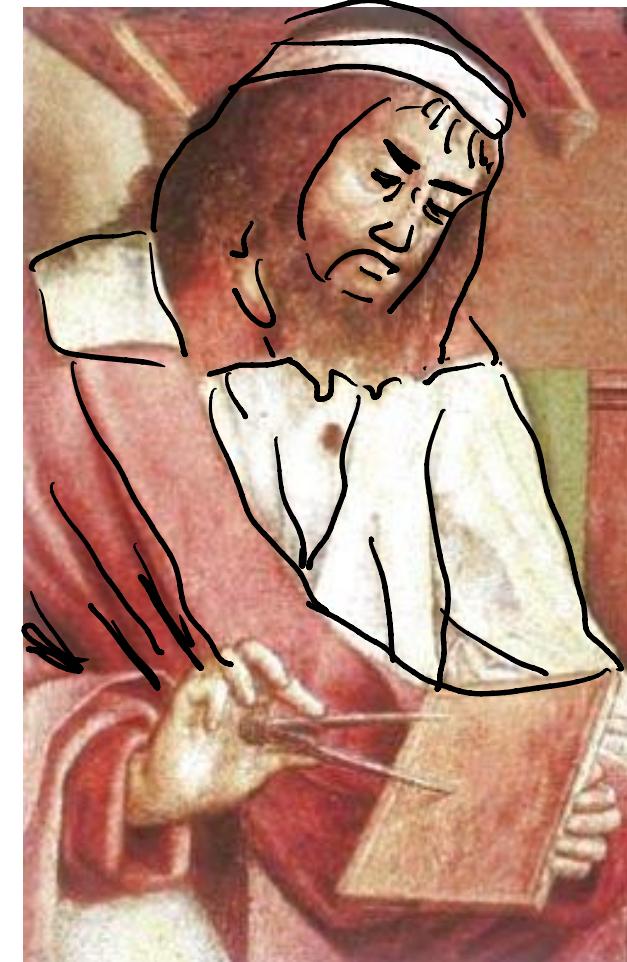
- **Contoh 4:** $m = 60, n = 18,$

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

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

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1,$$

$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2,$$

⋮

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = r_n q_n + 0$$

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

$$\text{PBB}(m, n) = \text{PBB}(r_0, r_1) = \text{PBB}(r_1, r_2) = \dots =$$

$$\text{PBB}(r_{n-2}, r_{n-1}) = \text{PBB}(r_{n-1}, r_n) = \text{PBB}(r_n, 0) = r_n$$

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

q^{ak}
pakai rekurens,
pakai iterasi

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 ≠ 0 do
    r ← m mod n
    m ← n
    n ← r
endwhile
{ n = 0, maka  $PBB(m, n) = m$  }
PBB ← m

```

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

$$\begin{array}{l} 80 = 6 \cdot 12 + 8 \\ \downarrow \quad \downarrow \\ 12 = 1 \cdot 8 + 4 \\ \downarrow \quad \downarrow \\ 8 = 2 \cdot 4 + 0 \end{array}$$

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

Kombinasi Linier

- PBB(a,b) dapat dinyatakan sebagai **kombinasi linier** (*linear combination*) a dan b dengan koefisien-koefisennya.
- **Contoh 6:** $\text{PBB}(80, 12) = 4$,
$$4 = (-1) \cdot 80 + 7 \cdot 12.$$
- **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:

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

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

ambil nq
sblm 0

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

Dari persamaan (i) dapat dituliskan:

$$3 = 45 - 2 \cdot 21 = 1 \cdot 45 - 2 \cdot 21$$

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

untuk
membuktikan dia
kombinasi
linear

Relatif Prima

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

- 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 Modulo

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

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

(i) $23 \bmod 5 = 3$	$(23 = 5 \cdot 4 + 3)$
(ii) $27 \bmod 3 = 0$	$(27 = 3 \cdot 9 + 0)$
(iii) $6 \bmod 8 = 6$	$(6 = 8 \cdot 0 + 6)$
(iv) $0 \bmod 12 = 0$	$(0 = 12 \cdot 0 + 0)$
(v) $-41 \bmod 9 = -5$	$(-41 = (9)(-4) - 5) \rightarrow$ salah karena $r < 0$
$-41 \bmod 9 = 4$	$(-41 = 9(-5) + 4) \rightarrow$ betul
(vi) $-39 \bmod 13 = 0$	$(-39 = 13(-3) + 0)$

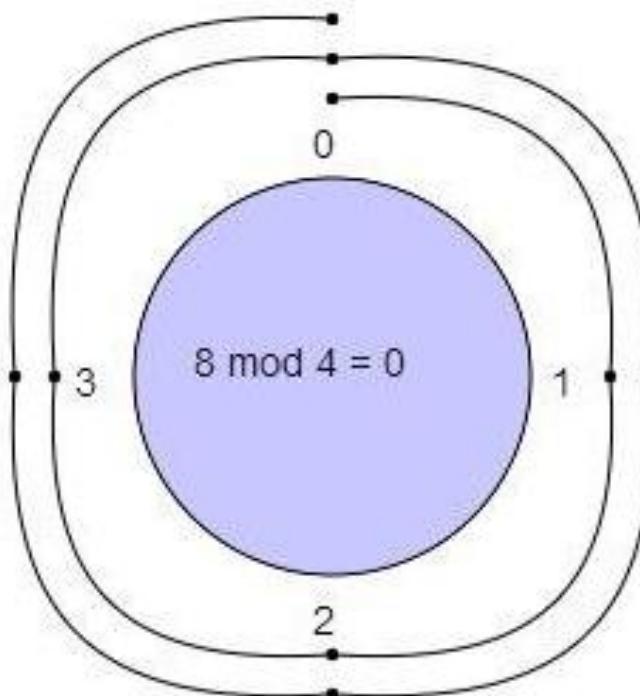
- *Penjelasan untuk (v):* Karena a negatif, bagi $|a|$ dengan m mendapatkan sisa r' . Maka $a \bmod m = m - r'$ bila $r' \neq 0$.

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.khanacademy.org

$$-5 \bmod 3 = ?$$

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

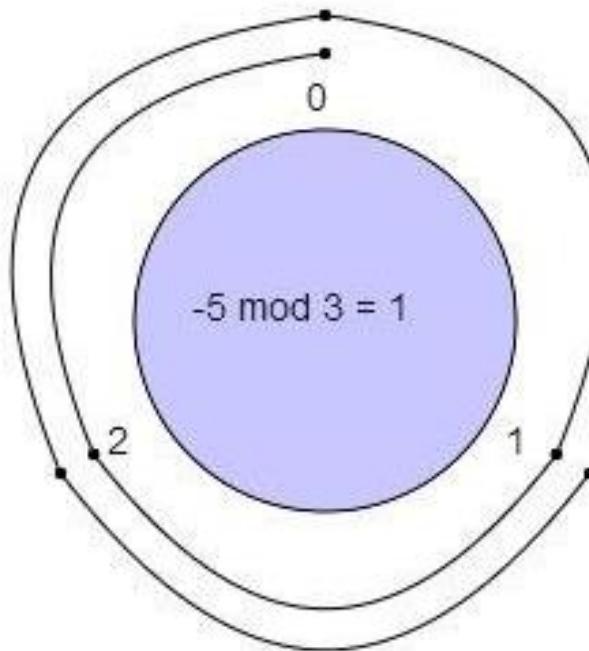
We start at 0 and go through 5 numbers in counter-clockwise sequence (5 is negative)

2,1,0,2,1

We ended up at 1

so:

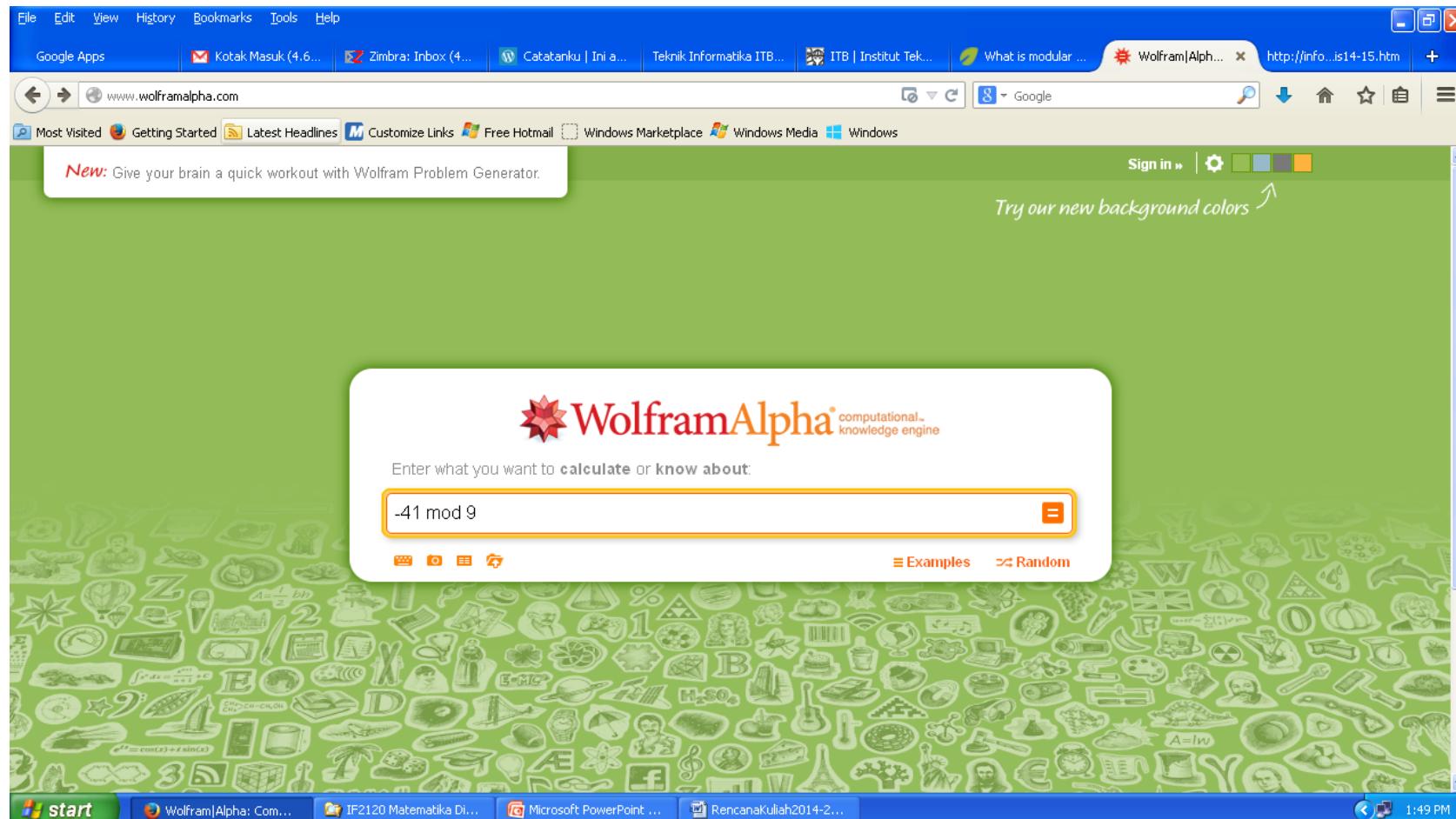
$$-5 \bmod 3 = 1$$



Sumber: www.khanacademy.org

Aritmetika Modulo di dalam Wolfram Alpha

- Kunjungi: www.wolframalpha.com



File Edit View History Bookmarks Tools Help

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

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

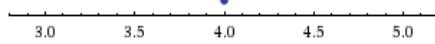
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Input:
 $(-41) \text{ mod } 9$

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, ...

Clock representation:


New to Wolfram|Alpha?

[Take the Tour >>](#)

Perplexed by a problem?


Share:
[!\[\]\(d12552b5dea3f95c35a7fe43b424c389_img.jpg\)](#)
[!\[\]\(932f13edf7fa8855dd6d0667a5d2d6f0_img.jpg\)](#)
[!\[\]\(2c9d1ab469f44273ac65c8612d0fbfa7_img.jpg\)](#)
[!\[\]\(ab67d3359a9f82ffa88a35cd19809142_img.jpg\)](#)
[more](#)

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

Kongruen

- 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:

$$\text{jam 14.00} = \text{jam 2 siang} \quad \rightarrow 14 \equiv 2 \pmod{12}$$

$$\text{jam 18.00} = \text{jam 6 sore} \quad \rightarrow 18 \equiv 6 \pmod{12}$$

$$\text{jam 21.00} = \text{jam 9 malam} \quad \rightarrow 21 \equiv 9 \pmod{12}$$

$$\text{jam 24.00} = \text{jam 0} \quad \rightarrow 24 \equiv 0 \pmod{12}$$

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

- **Contoh 12.**

$$17 \equiv 2 \pmod{3} \quad (3 \text{ habis membagi } 17 - 2 = 15)$$

$$21 \equiv 9 \pmod{12} \quad (12 \text{ habis membagi } 21 - 9 = 12)$$

$$-7 \equiv 15 \pmod{11} \quad (11 \text{ habis membagi } -7 - 15 = -22)$$

$$12 \not\equiv 2 \pmod{7} \quad (7 \text{ tidak habis membagi } 12 - 2 = 10)$$

$$-7 \not\equiv 15 \pmod{3} \quad (3 \text{ tidak habis membagi } -7 - 15 = -22)$$

Latihan 1

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

Tentukan semua bilangan yang kongruen dengan $5 \pmod{11}$.

Penyelesaian: Misalkan bilangan yang kongruen dengan $5 \pmod{11}$ adalah x .

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

tambah 11 ke kanan \rightarrow mis $5+11, 5+11+11\dots$
atau kurangkan 11 ke kiri
mis $5-11, 5-11-11, \text{dst.}$

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

Nilai x yang memenuhi adalah $16, 27, 38, \dots$, lalu $-6, -17, \dots$

- Jadi, nilai-nilai yang kongruen dengan $5 \pmod{11}$ adalah $\dots, -17, -6, 16, 27, 38, \dots$

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

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

a^{-q} bukan $\frac{1}{a^q}$
tapi invers dari a
di pangkatin q

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:

\swarrow
a kalo dibagi m
sisa nya b.

$$\Leftrightarrow a = b + km$$

$$\Leftrightarrow a - b = km$$

$$\Leftrightarrow (a - b)c \xrightarrow{\text{supaya ada } c.} ckm \quad \begin{matrix} \text{dikali } c \text{ kedua} \\ \text{ruasnya} \end{matrix}$$

$$\Leftrightarrow ac = bc + Km$$

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

+ tetapi bisa dibagi m, namun sisanya bukan b lagi namun bc

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

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

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

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

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

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

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 modulo, balikan modulo sebuah bilangan bulat lebih sukar dihitung.

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

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

$\hookrightarrow xa$ kalo dibagi m sisanya 1

- Dalam notasi lainnya, $a^{-1}(\text{mod } m) = x$

$$\begin{aligned} &xa \equiv 1 \pmod{m} \\ \Leftrightarrow &xa = 1 + k \cdot m \quad \rightarrow x = \frac{1 + km}{a} \end{aligned}$$

balikan sebuah angka
 di modulus tertentu bisa
 banyak.
 k nya dijgnn²
 dgn bil. bulat,
 hasilnya hrs
 bil. bulat juga.

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 $4 \pmod{9}$, $17 \pmod{7}$, dan $18 \pmod{10}$.

Penyelesaian:

*Kalau PBBnya ≠ 1,
qubisa dibalikin*

- (a) Karena $\text{PBB}(4, 9) = 1$, maka balikan dari $4 \pmod{9}$ 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 $4 \pmod{9}$. atau dapat juga ditulis $4^{-1} \pmod{9} = -2 \pmod{9}$.

- Catatan: setiap bilangan yang kongruen dengan
 $-2 \pmod{9}$
juga adalah balikan dari $4 \pmod{9}$, misalnya ..., $-20, -11, 7, 16, \dots$
 - $-20 \equiv -2 \pmod{9}$ (karena 9 habis membagi $-20 - (-2) = -18$)
 - $-11 \equiv -2 \pmod{9}$ (karena 9 habis membagi $-11 - (-2) = -9$)
 - $7 \equiv -2 \pmod{9}$ (karena 9 habis membagi $7 - (-2) = 9$)
 - $16 \equiv -2 \pmod{9}$ (karena 9 habis membagi $16 - (-2) = 18$)
- ..., $-20, -11, \textcolor{red}{-2}, 7, 16, \dots$ diperoleh dengan menambahkan 9 ke kiri atau ke kanan dari -2

(b) Karena $\text{PBB}(17, 7) = 1$, maka balikan dari $17 \pmod{7}$ 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 $17 \pmod{7}$, 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 (mod m)
- Misalkan x adalah balikan dari a (mod m), maka

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

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 $4 \pmod{9}$ adalah x sedemikian sehingga $4x \equiv 1 \pmod{9}$

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

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

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

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

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

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

Balikan dari $4 \pmod{9}$ adalah $7 \pmod{9}$, $-2 \pmod{9}$, dst

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

Latihan 3

- Tentukan semua balikan dari 9 (mod 11).

$$9x \equiv 1 \pmod{11}$$

$$9x = 1 + 11k$$

$$x = \frac{1+11k}{9}$$

KONKA

$k: 1 \rightarrow x: \frac{12}{9}$	$k: -2 \rightarrow x: \frac{1+(-22)}{9}$
$k: 2 \rightarrow x: \frac{23}{9}$	$k: -3 \rightarrow x: \frac{1+(-33)}{9}$
$k: -1 \rightarrow x: \frac{1-11}{9}$	$k: -4 \rightarrow x: \frac{1+(-44)}{9}$
$k: 3 \rightarrow x: \frac{34}{9}$	$k: -5 \rightarrow x: \frac{1+(-55)}{9}$
$k: 4 \rightarrow x: \frac{45}{9} = 5$	$\vdots \quad \frac{-54}{9} = 6$

Invers : 5(mod 11), -6(mod 11), dst.

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 solusi, yaitu $-6, 16, 27, \dots$

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, ...

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

$$x : \frac{3 + 4k}{2} \rightarrow \begin{cases} \text{genap} \\ \text{ganjil} \end{cases} \rightarrow \begin{cases} \text{ganjil} \\ \text{pasti ga bil. bulat} \end{cases}$$

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

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

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

$$(1/4) \cdot 4x = 12 \cdot (1/4) \rightarrow x = 12/4 = 3$$

balikan yg (bil. rill)

- $4x \equiv 12 \pmod{9} \rightarrow$ kalikan setiap ruas dengan balikan dari $4 \pmod{9}$ (dalam hal ini sudah kita hitung, yaitu -2)

$$(-2) \cdot 4x \equiv (-2) \cdot 12 \pmod{9} \Leftrightarrow -8x \equiv -24 \pmod{9}$$

*sama
saja kek yg
tadi*

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

$$a. 4x \equiv 8 \pmod{11}$$

$$4x = 8 + 11k$$

$$x : \frac{8 + 11k}{4}$$

$$k=0 \rightarrow \frac{8+11(0)}{4} = 2$$

sehingga inversnya $2 \pmod{11}$

$$x = 2 + 11k_{11}$$

$$c. 2x \equiv 1 \pmod{8}$$

$$x : \frac{1 + 8k}{2} \rightarrow \text{genap} \rightarrow \text{ganjil}$$

ganjil ga ada yg bulat

$$b. 5x \equiv 1 \pmod{61}$$

$$5x = 1 + 61k$$

$$x = \frac{1 + 61k}{5}$$

$$k \rightarrow 4 = x : \frac{1 + 61(4)}{5} \\ \therefore \frac{245}{5} \cdot 49$$

sehingga $49 \pmod{61}$

$$x = 49 + 61k_{11}$$

$$d. x = 0$$

$$\boxed{2^x = 1}$$

$\hookrightarrow x$ nya cuma 0 doang.

Latihan Soal Teori Bilangan

Soal 1

- Buktikan untuk setiap bilangan bulat positif n dan a , $\text{PBB}(a, a + n)$ habis bagi n .

Jawaban:

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

Maka:

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

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

$$\overline{a + n - a = (k_1 - k_2)d}$$

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

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

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 :

$$m = k_1 \cdot n \quad \dots \text{(i)}$$

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

$$a = b + k_2 \cdot m \quad \dots \text{(ii)}$$

Substitusikan (i) ke dalam (ii):

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

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

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

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

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) :

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

$$2 = 11.312 - 44.70 - 5.70$$

$$2 = 11.312 - 49.70 \quad (\text{ix})$$

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