

# Teori Bilangan

## (Bagian 1)



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
- Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02.

# 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  $b = ac$ ,  $c \in \mathbf{Z}$  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

**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.
- 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:**  $m = 60, n = 18,$

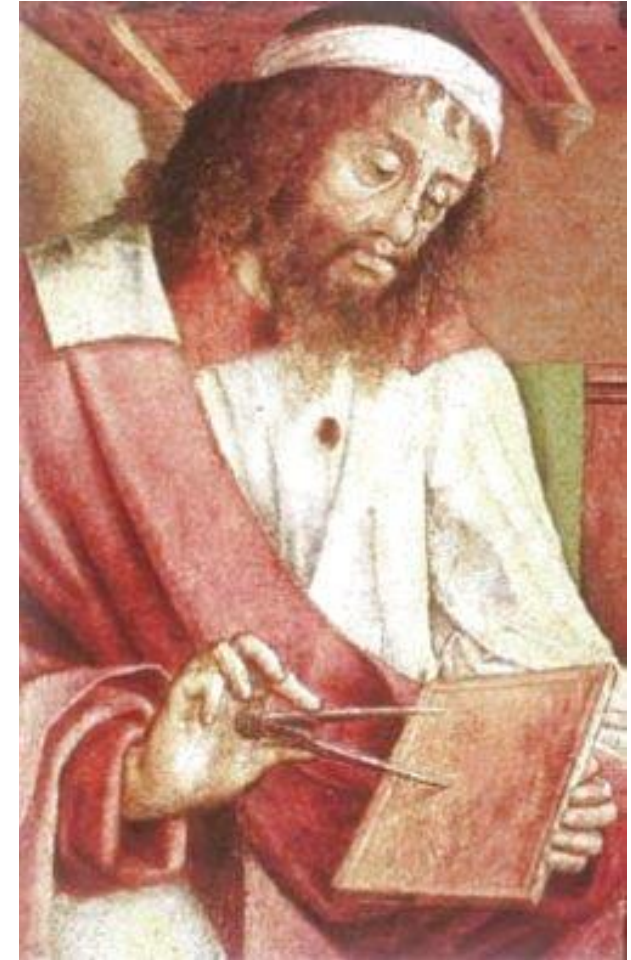
$$60 = 3 \cdot 18 + 6$$

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  $\text{PBB}(80, 12) = 4$ .

# Kombinasi Linier

- PBB( $a, b$ ) dapat dinyatakan sebagai **kombinasi linier** (*linear combination*)  $a$  dan  $b$  dengan koefisien-koefisiennya.
- **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:

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

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

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.

Solusi: 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  $PBB(20, 5) = 5 \neq 1$ .

- 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  $a \bmod m$  (dibaca “ $a$  modulo  $m$ ”) memberikan sisa jika  $a$  dibagi dengan  $m$ .
- Notasi:  $a \bmod m = r$  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:

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

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

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

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

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

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

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

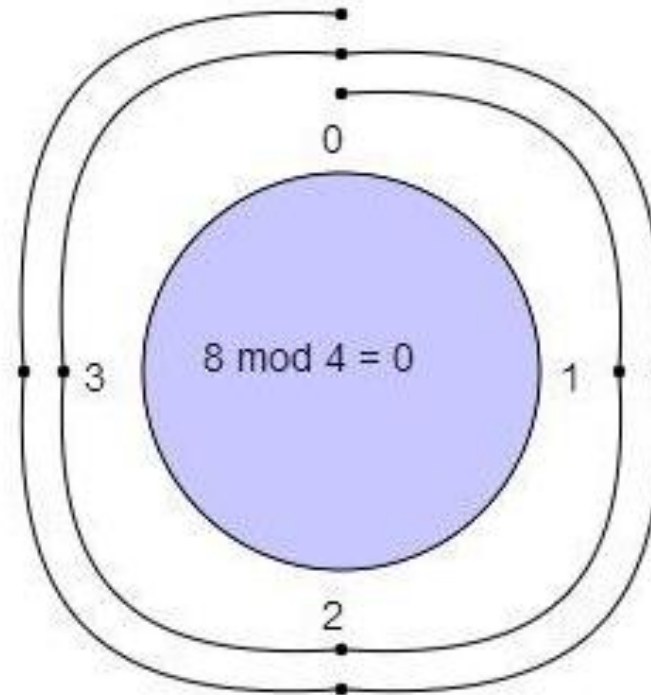
- *Penjelasan untuk (v):* Karena  $a$  negatif, bagi  $|a|$  dengan  $m$  mendapatkan sisa  $r'$ . Maka  $a \bmod m = m - r'$  bila  $r' \neq 0$ .

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:

$$8 \bmod 4 = 0$$

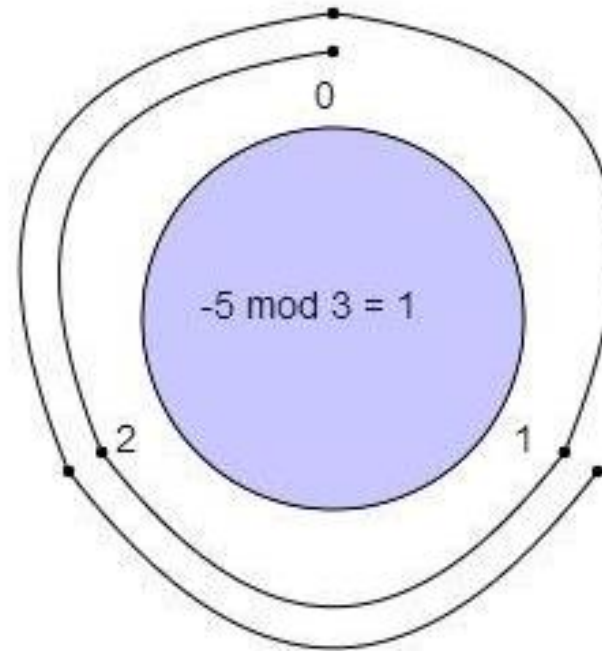
Sumber: [www.khancademy.org](http://www.khancademy.org)

# $-5 \bmod 3 = ?$

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

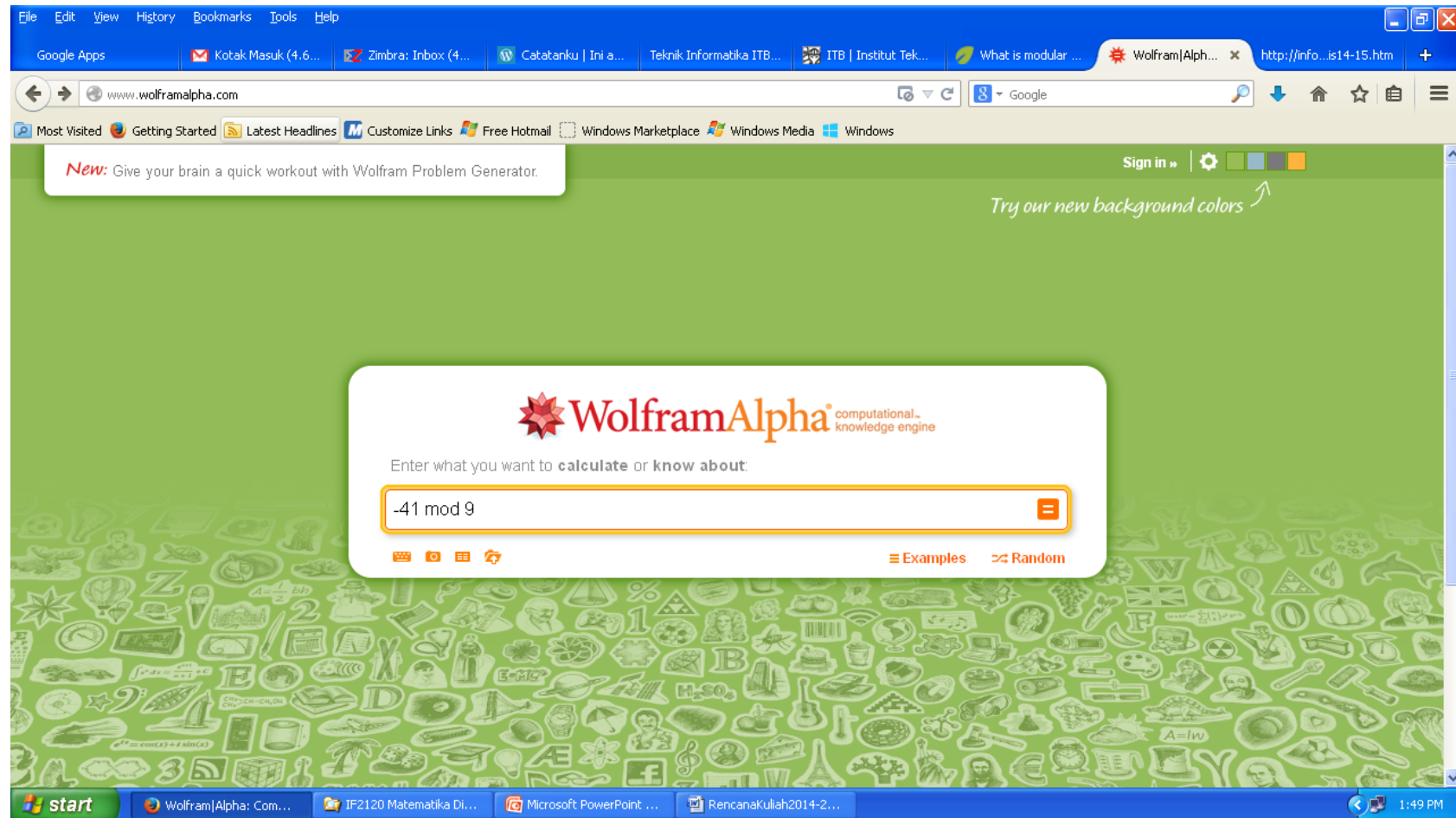
so:

$$-5 \bmod 3 = 1$$

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 - ... http://info...is14-15.htm

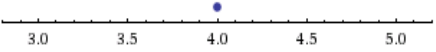
www.wolframalpha.com/input/?i=-41+mod+9

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, ...

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

# 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:  
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  $-7 - 15 = -22$  )*

**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: 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 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  $a \equiv r \pmod{m}$
- **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

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

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

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



*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 modulo, 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:  
$$xa \equiv 1 (\text{mod } m)$$
- Dalam notasi lainnya,  $a^{-1}(\text{mod } m) = x$

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  $4^{-1} \pmod{9} = -2 \pmod{9}$ .

- 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, ...

# 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 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  $-6, -15, \dots$

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

# Teori Bilangan

## (Bagian 2)



Bahan Kuliah IF2120 Matematika Diskrit

Oleh: Rinaldi Munir

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

# Sistem Kekongruenan Linier

- Sistem kekongruenan linier terdiri dari lebih dari satu kekongruenan, yaitu:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

**Contoh:** Sebuah bilangan bulat jika dibagi dengan 3 bersisa 2 dan jika ia dibagi dengan 5 bersisa 3. Berapakah bilangan bulat tersebut?

## Penyelesaian:

Sebuah bilangan bulat jika dibagi dengan 3 bersisa 2 dan jika ia dibagi dengan 5 bersisa 3. Berapakah bilangan bulat tersebut?

Misal bilangan bulat =  $x$

$$x \bmod 3 = 2 \quad \rightarrow \quad x \equiv 2 \pmod{3}$$

$$x \bmod 5 = 3 \quad \rightarrow \quad x \equiv 3 \pmod{5}$$

Jadi, terdapat sistem kekongruenan:

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

$$x \equiv 3 \pmod{5} \quad (ii)$$

Untuk kekongruenan pertama:

$$x = 2 + 3k_1 \quad (iii)$$

Substitusikan (iii) ke dalam (ii):

$$2 + 3k_1 \equiv 3 \pmod{5} \rightarrow 3k_1 \equiv 1 \pmod{5}$$

diperoleh

$$k_1 \equiv 2 \pmod{5} \text{ atau } k_1 = 2 + 5k_2$$

Sebuah bilangan bulat jika dibagi dengan 3 bersisa 2 dan jika ia dibagi dengan 5 bersisa 3. Berapakah bilangan bulat tersebut?

Substitusikan  $k_1 = 2 + 5k_2$  ke dalam persamaan (iii):

$$\begin{aligned}x &= 2 + 3k_1 \\&= 2 + 3(2 + 5k_2) \\&= 2 + 6 + 15k_2 \\&= 8 + 15k_2\end{aligned}$$

atau

$$x \equiv 8 \pmod{15} \quad (\text{periksa bahwa } 8 \bmod 3 = 2 \text{ dan } 8 \bmod 5 = 3)$$

Semua nilai  $x$  yang kongruen dengan 8 (mod 15) juga adalah solusinya, yaitu  $x = 8, x = 23, x = 38, \dots, x = -7, \text{ dst}$

# Chinese Remainder Problem



- Pada abad pertama Masehi, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan sebagai berikut:

*Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7.*

- Misakan bilangan bulat tersebut =  $x$ . Formulasikan kedalam sistem kekongruenan linier:

$$x \equiv 3 \pmod{5}$$

$$x \equiv 5 \pmod{7}$$

$$x \equiv 7 \pmod{11}$$

**Teorema 5. (*Chinese Remainder Theorem*)** Misalkan  $m_1, m_2, \dots, m_n$  adalah bilangan bulat positif sedemikian sehingga  $\text{PBB}(m_i, m_j) = 1$  untuk  $i \neq j$ . Maka sistem kekongruenan linier

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

mempunyai sebuah solusi unik dalam modulus  $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$ . (yaitu, terdapat solusi  $x$  dengan  $0 \leq x < m$  dan semua solusi lain yang kongruen dalam modulus  $m$  dengan solusi ini)

**Contoh 15.** Tentukan solusi dari pertanyaan Sun Tse tersebut

$$x \equiv 3 \pmod{5}$$

$$x \equiv 5 \pmod{7}$$

$$x \equiv 7 \pmod{11}$$

Penyelesaian:

$$x \equiv 3 \pmod{5} \rightarrow x = 3 + 5k_1 \quad (\text{i})$$

Sulihkan (i) ke dalam kongruen kedua ( yaitu  $x \equiv 5 \pmod{7}$  ) menjadi:

$$3 + 5k_1 \equiv 5 \pmod{7} \rightarrow 5k_1 \equiv 2 \pmod{7} \rightarrow k_1 \equiv 6 \pmod{7}, \text{ atau } k_1 = 6 + 7k_2 \quad (\text{ii})$$

Sulihkan (ii) ke dalam (i):

$$x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2 \quad (\text{iii})$$

Sulihkan (iii) ke dalam kongruen ketiga (yaitu  $x \equiv 7 \pmod{11}$  ) menjadi:

$$33 + 35k_2 \equiv 7 \pmod{11} \rightarrow 35k_2 \equiv -26 \pmod{11} \rightarrow k_2 \equiv 9 \pmod{11} \text{ atau } k_2 = 9 + 11k_3$$

Sulihkan  $k_2$  ini ke dalam (iii) menghasilkan:

$$x = 33 + 35(9 + 11k_3) = 348 + 385k_3 \text{ atau } x \equiv 348 \pmod{385}. \text{ Ini adalah solusinya.}$$

348 adalah bilangan bulat positif terkecil yang merupakan solusi sistem kekongruenan di atas. Periksa bahwa bahwa  $348 \bmod 5 = 3$ ,  $348 \bmod 7 = 5$ , dan  $348 \bmod 11 = 7$ .

Perhatikan juga bahwa  $385 = 5 \cdot 7 \cdot 11$ .



- Solusi unik ini, yaitu  $x \equiv 348 \pmod{385}$ , modulus 385 merupakan

$$m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 385$$

- Secara umum, solusi sistem kekongruenan linier adalah berbentuk

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$$

yang dalam hal ini

$M_k$  adalah perkalian semua modulus kecuali  $m_k$ .

$y_k$  adalah balikan  $M_k$  dalam modulus  $m_k$

$$\begin{aligned}x &\equiv 3 \pmod{5} \\x &\equiv 5 \pmod{7} \\x &\equiv 7 \pmod{11}\end{aligned}$$

- Tinjau kembali persoalan *Chinese remainder problem*:

- Hitung:  $m = 5 \cdot 7 \cdot 11 = 385$

$$M_1 = 7 \cdot 11 = 77, \quad M_2 = 5 \cdot 11 = 55, \quad M_3 = 5 \cdot 7 = 35$$

$$y_1 = 3 \text{ karena } 77 \cdot 3 \equiv 1 \pmod{5}$$

$$y_2 = 6 \text{ karena } 55 \cdot 6 \equiv 1 \pmod{7}$$

$$y_3 = 6 \text{ karena } 35 \cdot 6 \equiv 1 \pmod{11}$$

maka solusi unik dari sistem kekongruenan tersebut adalah

$$\begin{aligned}x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\&= 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \\&= 3813 \\&\equiv 348 \pmod{385}\end{aligned}$$

# Bilangan Prima

- Bilangan bulat positif  $p$  ( $p > 1$ ) disebut bilangan prima jika pembaginya hanya 1 dan  $p$ .
- Contoh: 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23.

- Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, ....
- Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.
- Bilangan selain prima disebut bilangan **komposit** (*composite*). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri.

**Teorema 6. (*The Fundamental Theorem of Arithmetic*).** Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

**Contoh 16.**

$$9 = 3 \times 3$$

$$100 = 2 \times 2 \times 5 \times 5$$

$$13 = 13 \quad (\text{atau } 1 \times 13)$$

- Tes apakah  $n$  bilangan prima atau komposit:
  - (i) bagi  $n$  dengan sejumlah bilangan prima, mulai dari 2, 3, ... , bilangan prima  $\leq \sqrt{n}$ .
  - (ii) Jika  $n$  habis dibagi dengan salah satu dari bilangan prima tersebut, maka  $n$  adalah bilangan komposit,
  - (ii) tetapi jika  $n$  tidak habis dibagi oleh semua bilangan prima tersebut, maka  $n$  adalah bilangan prima.

- **Contoh 17.** Tes apakah (i) 171 dan (ii) 199 merupakan bilangan prima atau komposit.

Penyelesaian:

(i)  $\sqrt{171} = 13.077$ . Bilangan prima yang  $\leq \sqrt{171}$  adalah 2, 3, 5, 7, 11, 13. Karena 171 habis dibagi 3, maka 171 adalah bilangan komposit.

(ii)  $\sqrt{199} = 14.107$ . Bilangan prima yang  $\leq \sqrt{199}$  adalah 2, 3, 5, 7, 11, 13. Karena 199 tidak habis dibagi 2, 3, 5, 7, 11, dan 13, maka 199 adalah bilangan prima.

- **Teorema 6 (Teorema Fermat).** Jika  $p$  adalah bilangan prima dan  $a$  adalah bilangan bulat yang tidak habis dibagi dengan  $p$ , yaitu  $\text{PBB}(a, p) = 1$ , maka:

*Fermat dibaca Fairma*

$$a^{p-1} \equiv 1 \pmod{p}$$

- Menurut teorema Fermat di atas, jika  $p$  adalah bilangan prima, maka  $a^{p-1} \equiv 1 \pmod{p}$
- Tetapi, jika  $p$  bukan bilangan prima, maka  $a^{p-1} \not\equiv 1 \pmod{p}$



$$a^{p-1} \equiv 1 \pmod{p}$$

**Contoh 18.** Tes apakah 17 dan 21 bilangan prima atau bukan dengan Teorema Fermat

Ambil  $a = 2$  karena  $\text{PBB}(17, 2) = 1$  dan  $\text{PBB}(21, 2) = 1$ .

(i)  $2^{17-1} = 65536 \equiv 1 \pmod{17}$

karena 17 habis membagi  $65536 - 1 = 65535$

Jadi, 17 prima.

(ii)  $2^{21-1} = 1048576 \not\equiv 1 \pmod{21}$

karena 21 tidak habis membagi  $1048576 - 1 = 1048575$ .

Jadi, 21 bukan prima

- Kelemahan Teorema Fermat: terdapat bilangan komposit  $n$  sedemikian sehingga  $2^{n-1} \equiv 1 \pmod{n}$ . Bilangan bulat seperti itu disebut bilangan **prima semu** (*pseudoprimes*).

- Contoh: 341 adalah komposit (karena  $341 = 11 \cdot 31$ ) sekaligus bilangan prima semu, karena menurut teorema Fermat,

$$2^{340} \equiv 1 \pmod{341}$$

- Untunglah bilangan prima semu relatif jarang terdapat.
- Untuk bilangan bulat yang lebih kecil dari  $10^{10}$  terdapat 455.052.512 bilangan prima, tapi hanya 14.884 buah yang merupakan bilangan prima semu terhadap basis 2.

**Contoh 19:** Hitunglah sisa pembagian  $2^{2020}$  dibagi dengan 73

Penyelesaian: Dengan menggunakan teorema Fermat kita dapat mengetahui bahwa  $2^{73-1} = 2^{72} \equiv 1 \pmod{73}$ .

$$\begin{aligned} 2^{2020} &\equiv (2^{72 \cdot 28 + 4}) \pmod{73} \\ &\equiv (2^{72})^{28} \cdot 2^4 \pmod{73} \\ &\equiv (1)^{28} \cdot 2^4 \pmod{73} \\ &\equiv 2^4 \pmod{73} \\ &\equiv 16 \pmod{73} = 16 \end{aligned}$$

Jadi sisa pembagiannya adalah 16

**Contoh 20:** Tiga kemunculan terakhir komet Halley adalah pada tahun 1835, 1910, dan 1986. Kemunculan berikutnya diprediksi akan terjadi pada tahun 2061. Dengan bantuan Teorema Fermat buktikan bahwa

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}$$

Jawaban: Karena  $\text{PBB}(7, 1835) = 1$  dan  $\text{PBB}(7, 1986) = 1$ , maka memenuhi syarat Teorema Fermat.

Selanjutnya, berdasarkan Teorema Fermat,  $a^{p-1} \equiv 1 \pmod{p}$

$$1835^{7-1} = 1835^6 \equiv 1 \pmod{7}$$

$$\begin{aligned} 1835^{1910} \pmod{7} &\equiv 1835^{6 \cdot 318 + 2} \equiv (1835^6)^{318} \cdot 1835^2 \pmod{7} \equiv (1)^{318} \cdot 1835^2 \pmod{7} \\ &\equiv 1835^2 \pmod{7} \equiv 1^2 \pmod{7} \equiv 1 \pmod{7} \end{aligned}$$

$$1986^{7-1} = 1986^6 \equiv 1 \pmod{7}$$

$$\begin{aligned} 1986^{2061} \pmod{7} &\equiv 1986^{6 \cdot 343 + 3} \equiv (1986^6)^{343} \cdot 1986^3 \pmod{7} \equiv (1)^{343} \cdot 1986^3 \pmod{7} \\ &\equiv 1986^3 \pmod{7} \equiv 5^3 \pmod{7} \equiv 125 \pmod{7} \equiv 6 \pmod{7} \end{aligned}$$

Jadi,

$$1835^{1910} + 1986^{2061} \pmod{7} \equiv 1 \pmod{7} + 6 \pmod{7} \equiv 0 \pmod{7}$$

# Latihan soal (diambil dari soal kuis dan UAS)

1. Hartono memiliki banyak permen. Dia akan membagi permen kepada teman-temannya. Jika dia membagi kepada 7 orang temannya secara merata, maka akan tersisa 5 permen. Jika dia membagi seluruhnya secara merata kepada 8 teman, tersisa 3. Jika ia membagi seluruhnya secara merata kepada 9 orang, akan tersisa 7 permen. Berapa paling sedikit jumlah permen yang dimiliki Hartono?
2. Hitunglah nilai dari  $5^{2017} \bmod 7$  dan  $5^{2017} \bmod 11$  dengan menggunakan Teorema Fermat.
3. (a) Gunakan Teorema Fermat untuk menghitung  $3^{302} \bmod 5$ ,  $3^{302} \bmod 7$ , dan  $3^{302} \bmod 11$   
(b) Gunakan hasil dari (a) dan *Chinese Remainder Theorem* untuk menghitung nilai  $3^{302} \bmod 385$  (Petunjuk:  $385 = 5 \cdot 7 \cdot 11$ )

# Teori Bilangan

## (Bagian 3)



Bahan Kuliah IF2120 Matematika Diskrit

Oleh: Rinaldi Munir

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

# Aplikasi Teori Bilangan

- *ISBN (International Standard Book Number)*
- Fungsi *hash*
- Kriptografi
- Pembangkit bilangan acak-semu

# *ISBN (International Standard Book Number)*

- Kode ISBN terdiri dari 10 angka, biasanya dikelompokkan dengan spasi atau garis, misalnya 0–3015–4561–9.

Catatan: Juga terdapat versi ISBN 13-angka

- ISBN terdiri atas empat bagian kode:
  - kode yang mengidentifikasikan negara atau kelompok negara,
  - kode penerbit,
  - kode unik untuk buku tersebut,
  - karakter uji (angka atau huruf X (=10)).





Contoh:



- 1 : kode negara-negara berbahasa Inggris (selain AS)
- 4028 : kode penerbit
- 9462 : kode unik buku yang diterbitkan oleh penerbit
- 7 : karakter uji.

- Misalkan 10 angka ISBN dinyatakan dengan  $x_1, x_2, \dots, x_{10}$
- Kode ISBN memenuhi kekongruenan

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

$$(1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + \dots + 10 \cdot x_{10}) \equiv 0 \pmod{11}$$

- Karakter uji dihitung sebagai berikut:

$$\left( \sum_{i=1}^9 ix_i \right) \pmod{11} = \text{karakter uji}$$

- Contoh: ISBN 0–3015–4561–8

0 : kode negara Amerika Serikat

3015 : kode penerbit

4561 : kode unik buku yang diterbitkan

8 : karakter uji.

Kode ISBN ini memenuhi kekongruenan:

$$\begin{aligned}\sum_{i=1}^{10} ix_i &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 + 10 \cdot 8 \\ &= 231 \equiv 0 \pmod{11}\end{aligned}$$

Karakter uji ini didapatkan sebagai berikut:

$$\begin{aligned}\sum_{i=1}^9 ix_i &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 \\ &= 151\end{aligned}$$

Jadi, karakter ujinya adalah  $151 \bmod 11 = 8$ .

# Latihan 1

Sebuah buku terbitan September 2018 memiliki ISBN 9

*p*7-2309-97. Tentukan nilai  $p$  dan karakter uji dari nomor ISBN tersebut jika diketahui  $3p \equiv 2 \pmod{5}$ .

## Jawaban:

- $3p \equiv 2 \pmod{5} \rightarrow 3p = 2 + 5k \rightarrow p = (2 + 5k)/3$  untuk  $k$  sembarang bilangan bulat

Untuk nilai  $k =$

$$k = 1 \rightarrow p = 2/3$$

$$k = 2 \rightarrow p = 4$$

$$k = 3 \rightarrow p = 17/3$$

$$k = 4 \rightarrow p = 22/3$$

$$k = 5 \rightarrow p = 9$$

$$k = 6 \rightarrow p = 32/3$$

$$k = 7 \rightarrow p = 37/3$$

$$k = 8 \rightarrow p = 14$$

...dst

- Dapat dilihat di atas, untuk  $k = 2, 5, 8, \dots$  nilai  $p$  bulat, namun untuk kode ISBN nilai  $p$  harus dalam rentang bilangan bulat 0-9, jadi nilai  $p$  yang memenuhi adalah **4** dan **9**.

Untuk mencari karakter uji, diketahui

$$\sum_{i=1}^9 ix_i \bmod 11 = \text{karakter uji}$$

Karakter uji untuk kode ISBN 947-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=1}^9 ix_i = (1)(9) + (2)(4) + (3)(7) + (4)(2) + (5)(3) + (6)(0) + (7)(9) + (8)(9) + (9)(7) = 259$$

Jadi karakter uji untuk ISBN di atas =  $259 \bmod 11 = 6 \rightarrow 947-2309-97-6$

Karakter uji untuk kode ISBN 997-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=1}^9 ix_i = (1)(9) + (2)(9) + 3(7) + (4)(2) + (5)(3) + 6(0) + (7)(9) + (8)(9) + (9)(7) = 269$$

Jadi karakter uji untuk ISBN di atas =  $269 \bmod 11 = 5 \rightarrow 997-2309-97-5$

# Fungsi *Hash*

- Kegunaan: pengalamatan data di dalam memori untuk tujuan pengaksesan data dengan cepat.
- Bentuk:  $h(K) = K \bmod m$ 
  - $m$  : jumlah lokasi memori yang tersedia
  - $K$  : kunci (*integer*)
  - $h(K)$  : lokasi memori untuk data dengan kunci unik  $K$

Contoh: data record mahasiswa, NIM adalah kunci ( $K$ )

NIM	Nama	MatKul	Nilai
13598011	Amir	Matematika Diskrit	A
13598012	Bonar	Arsitektur Komputer	B
13598014	Santi	Algoritma	D
13598015	Irwan	Algoritma	C
13598017	Rahman	Struktur Data	C
13598018	Ismu	Arsitektur Komputer	B
13598019	Tommy	Algoritma	E
13598021	Cecep	Algoritma	B
13598023	Badru	Arsitektur Komputer	B
13598025	Hamdan	Matematika Diskrit	B
13598027	Rohadi	Algoritma	A
13598028	Hans	Struktur Data	C
13598029	Maman	Arsitektur Komputer	B



Contoh:  $m = 11$  mempunyai sel-sel memori yang diberi indeks 0 sampai 10. Akan disimpan data *record* yang masing-masing mempunyai kunci 15, 558, 32, 132, 102, dan 5.

$$h(15) = 15 \bmod 11 = 4$$

$$h(558) = 558 \bmod 11 = 8$$

$$h(32) = 32 \bmod 11 = 10$$

$$h(132) = 132 \bmod 11 = 0$$

$$h(102) = 102 \bmod 11 = 3$$

$$h(5) = 5 \bmod 11 = 5$$

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

- Kolisi (*collision*) terjadi jika fungsi *hash* menghasilkan nilai  $h$  yang sama untuk  $K$  yang berbeda.
- Jika terjadi kolisi, cek elemen berikutnya yang kosong.

Contoh:  $K = 74 \rightarrow h(74) = 74 \bmod 11 = 8$

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

Oleh karena elemen pada indeks 8 sudah berisi 558, maka 74 ditaruh pada elemen kosong berikutnya: 9


132			102	15	5			558	74	32
0	1	2	3	4	5	6	7	8	9	10

- Fungsi *hash* juga digunakan untuk me-*locate* elemen yang dicari.

Misalkan akan dicari data dengan nilai  $K = 102$

Posisi 102 di dalam larik dihitung dengan fungsi *hash*  $\rightarrow h(102) = 102 \bmod 11 = 3$

132			102	15	5			558	74	32
0	1	2	3	4	5	6	7	8	9	10



Misalkan akan dicari data dengan nilai  $K = 214$

Posisi 214 di dalam larik dihitung dengan fungsi *hash*  $\rightarrow h(214) = 214 \bmod 11 = 5$

Karena pada sel dengan indeks 5 bukan berisi 214, maka disimpulkan  $K = 214$  tidak ditemukan di dalam larik.

## Latihan 2

Sebuah area parkir mempunyai sejumlah *slot* atau *space* yang dinomori 0 sampai 25. Mobil yang hendak parkir di area tersebut ditentukan dengan sebuah fungsi *hash*. Fungsi *hash* tersebut menentukan nomor *slot* yang akan ditempati mobil yang hendak parkir berdasarkan 3 angka terakhir pada plat nomor polisinya.

- (a) Tentukan fungsi *hash* yang dimaksudkan.
- (b) Tentukan nomor *slot* yang ditempati mobil yang datang berturut-turut dengan plat nomor polisinya adalah 423251, 76540, 17121, 2310, 4124, 1102, 1724

- Jawaban:

(a)  $h = x \bmod 26$

(b)  $423251 \rightarrow 3 \text{ angka terakhir} = 251 \rightarrow 251 \bmod 26 = 17$  (slot 17)

$76540 \rightarrow 3 \text{ angka terakhir} = 540 \rightarrow 540 \bmod 26 = 20$  (slot 20)

$17121 \rightarrow 3 \text{ angka terakhir} = 121 \rightarrow 121 \bmod 26 = 17$  (tetapi slot nomor 17 sudah terisi, jadi isi slot kosong berikutnya, yaitu 18)

$2310 \rightarrow 3 \text{ angka terakhir} = 310 \rightarrow 310 \bmod 26 = 24$  (slot 24)

$4124 \rightarrow 3 \text{ angka terakhir} = 124 \rightarrow 124 \bmod 26 = 20$  (slot 21 karena slot 20 sudah terisi)

$1102 \rightarrow 3 \text{ angka terakhir} = 102 \rightarrow 102 \bmod 26 = 24$  (slot 25 karena slot 24 sudah terisi)

$1724 \rightarrow 3 \text{ angka terakhir} = 724 \rightarrow 724 \bmod 26 = 22$  (slot 22)

Jadi, mobil-mobil yang datang mengisi slot 17, 20, 18, 24, 21, 25, dan 22

# Kriptografi



- Dari Bahasa Yunani yang artinya “*secret writing*”
- **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna.
- Tujuan: agar pesan yang bersifat rahasia tidak dapat dibaca oleh pihak yang tidak berhak.

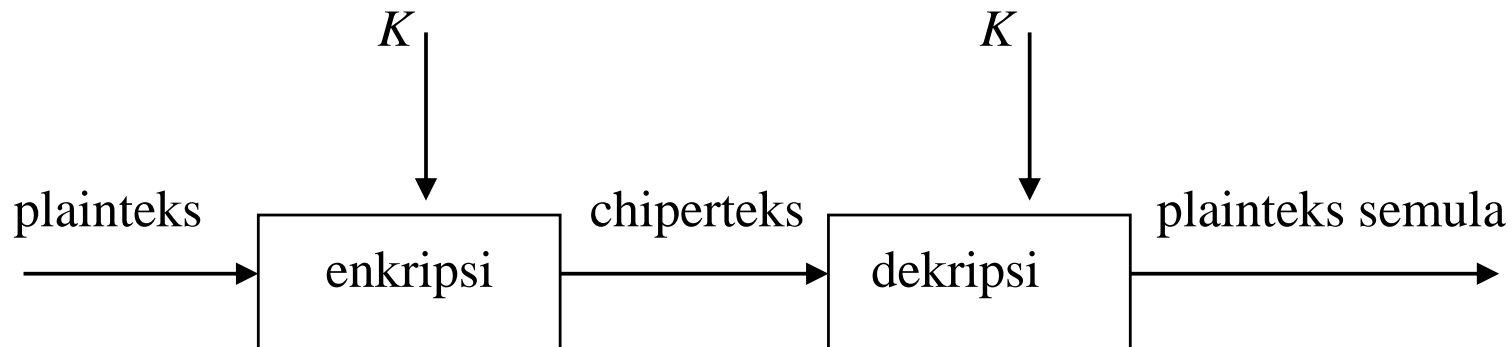
- **Pesan**: data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain: **plainteks** (*plaintext*)
- **Cipherteks** (*ciphertext*): pesan yang telah disandikan sehingga tidak memiliki makna lagi.

Contoh:

Plainteks:   culik anak itu jam 11 siang

Cipherteks:  t^\$gfUi9rewoFpfdWqL:[uTcxZy

- **Enkripsi** (*encryption*): proses menyandikan plainteks menjadi cipherteks.
- **Dekripsi** (*decryption*): Proses mengembalikan cipherteks menjadi plainteksnya.





# Aplikasi Enkripsi-Dekripsi

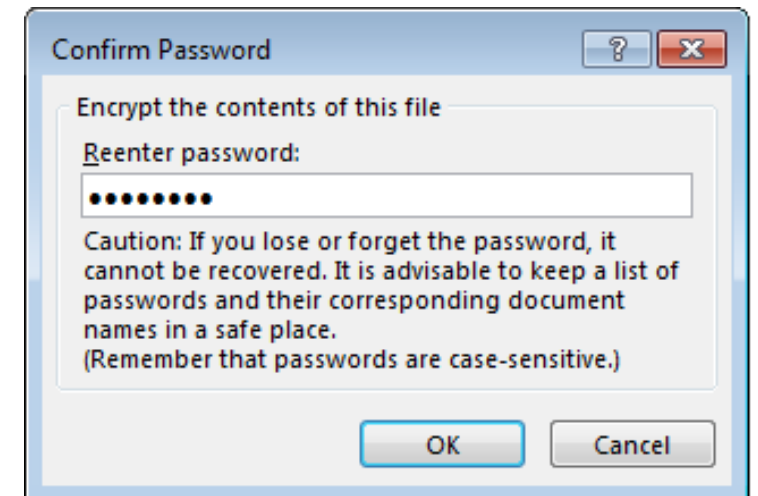
1. Pengiriman data melalui saluran komunikasi (*data encryption on motion*).

→ pesan dikirim dalam bentuk cipherteks



2. Penyimpanan dokumen di dalam *disk storage* (*data encryption at rest*)

→ data disimpan di dalam *disk* dalam bentuk cipherteks



# Contoh enkripsi pada dokumen

Plainteks (plain.txt):

Ketika saya berjalan-jalan di pantai,  
saya menemukan banyak sekali kepiting  
yang merangkak menuju laut. Mereka  
adalah anak-anak kepiting yang baru  
menetas dari dalam pasir. Naluri  
mereka mengatakan bahwa laut adalah  
tempat kehidupan mereka.

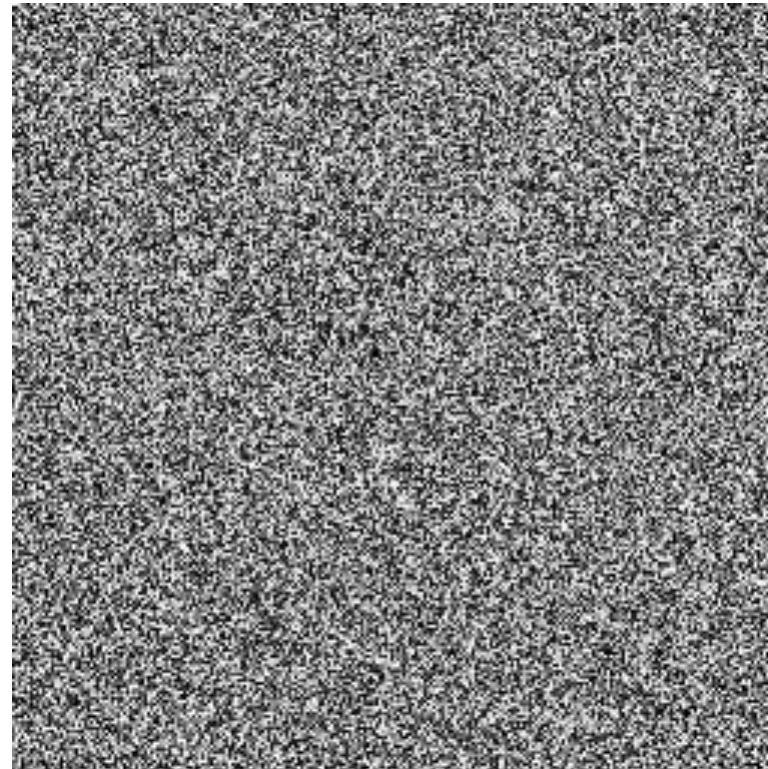
Cipherteks (cipher.txt):

Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/□p}âpx;  
épêp/|t}t|âzp}/qp}êpz/étzp{x/zt□xâx  
}v êp}v/|tüp}vzpz/|t}äyâ/{pââ=/\tütz  
p psp{pw/p}pz<p}pz/zt□xâx}v/êp}  
v/qpüä |t}tâpé/spüx/sp{p|/□péxü=/  
p{äüx |ttüzp/|t}vpâpzp}/qpwâp/{pââ  
/psp{pw ât|□pâ/ztwxsä□p}/|tützp=

Plainteks (lena.bmp):



Cipherteks (lena2.bmp):



Plainteks (siswa.dbf):

NIM	Nama	Tinggi	Berat
000001	Elin Jamilah	160	50
000002	Fariz RM	157	49
000003	Taufik Hidayat	176	65
000004	Siti Nurhaliza	172	67
000005	Oma Irama	171	60
000006	Aziz Burhan	181	54
000007	Santi Nursanti	167	59
000008	Cut Yanti	169	61
000009	Ina Sabarina	171	62

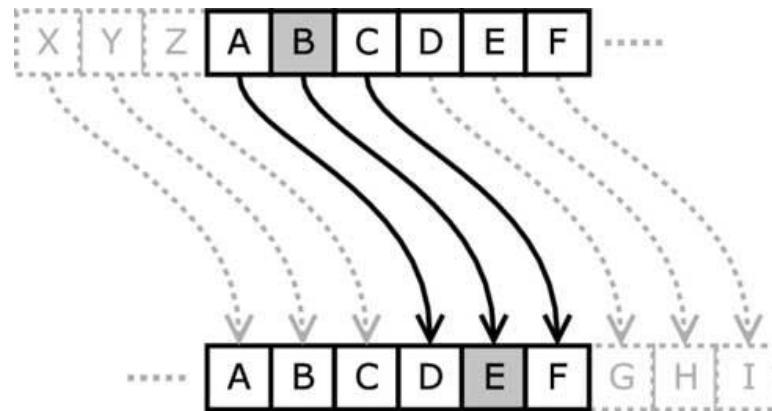
Cipherteks (siswa2.dbf):

NIM	Nama	Tinggi	Berat
000001	tüp}vzpz/ t}äyâ/{ää	äzp}	épêp
000002	t}tâpé/spüx/sp	péxü=	ztwxsä□
000003	ât □pâ/ztwxsä□p}/	}/ tü	spüx/
000004	épêp/ t}t äzp}/qpêpz	qp}êpz	wxsä
000005	étzp{x/zt□xâx}v êp}	pää/psp	étzp{
000006	spüx/sp{p /□péxü=/]	xâx}v	ttüzp/
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyâ/{
000008	qpwâp/{pää/psp{pw	Ztwxs	xâx}v
000009	}t äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

Keterangan: hanya *field* Nama, Berat, dan Tinggi yang dienkrpsi.

# Caesar Cipher

- Algoritma enkripsi sederhana pada masa raja Julius Caesar
- Tiap huruf alfabet digeser 3 huruf ke kanan secara *wrapping*



Contoh: Plainteks:    AWASI   ASTERIX   DAN   TEMANNYA   OBELIX

          Cipherteks:    **DZDVL   DVWHULA   GDQ   WHPDQQBA   REHOLA**



Copyright (c) 1999 Les Editions Albert René / Goscinny-Uderzo



- Misalkan setiap huruf dikodekan dengan angka:

$$A = 0, B = 1, C = 2, \dots, Z = 25$$

Misalkan huruf plainteks dinyatakan sebagai  $p$  dan huruf cipherteks sebagai  $c$ , maka secara matematis enkripsi dan dekripsi pada Caesar *cipher* dinyatakan dengan persamaan modulo berikut:

$$\text{Enkripsi: } c = E(p) = (p + 3) \bmod 26$$

$$\text{Dekripsi: } p = D(c) = (c - 3) \bmod 26$$



## Contoh:

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

### **Enkripsi:**

$$\begin{aligned} p_1 = 'A' = 0 & \rightarrow c_1 = E(0) = (0 + 3) \bmod 26 = 3 \bmod 26 = 3 = 'D' \\ p_2 = 'W' = 22 & \rightarrow c_2 = E(22) = (22 + 3) \bmod 26 = 25 \bmod 26 = 25 = 'Z' \\ p_3 = 'A' = 0 & \rightarrow c_3 = E(0) = (0 + 3) \bmod 26 = 3 \bmod 26 = 3 = 'D' \\ p_4 = 'S' = 18 & \rightarrow c_4 = E(18) = (18 + 3) \bmod 26 = 21 \bmod 26 = 21 = 'V' \\ & \text{dst...} \end{aligned}$$

### **Dekripsi:**

$$\begin{aligned} c_1 = 'D' = 3 & \rightarrow p_1 = D(3) = (3 - 3) \bmod 26 = 0 \bmod 26 = 0 = 'A' \\ c_2 = 'Z' = 25 & \rightarrow p_2 = D(25) = (25 - 3) \bmod 26 = 22 \bmod 26 = 22 = 'W' \\ c_3 = 'D' = 3 & \rightarrow p_3 = D(3) = (3 - 3) \bmod 26 = 0 \bmod 26 = 0 = 'D' \\ c_4 = 'V' = 21 & \rightarrow p_4 = D(21) = (21 - 3) \bmod 26 = 18 \bmod 26 = 18 = 'S' \\ & \text{dst..} \end{aligned}$$

- Jika pergeseran huruf sejauh  $k$ , maka:

Enkripsi:  $c = E(p) = (p + k) \bmod 26$

Dekripsi:  $p = D(c) = (c - k) \bmod 26$

$k$  = kunci rahasia

- Pada *Caesar Cipher*,  $k = 3$

- Untuk alfabet ASCII 256 karakter,

Enkripsi:  $c = E(p) = (p + k) \bmod 256$

Dekripsi:  $p = D(c) = (c - k) \bmod 256$

# Latihan 3

Salah satu program enkripsi di dalam sistem operasi *Linux* adalah **ROT13**. Enkripsi dilakukan dengan mengganti sebuah huruf dengan huruf ke-13 berikutnya dari susunan alfabet.

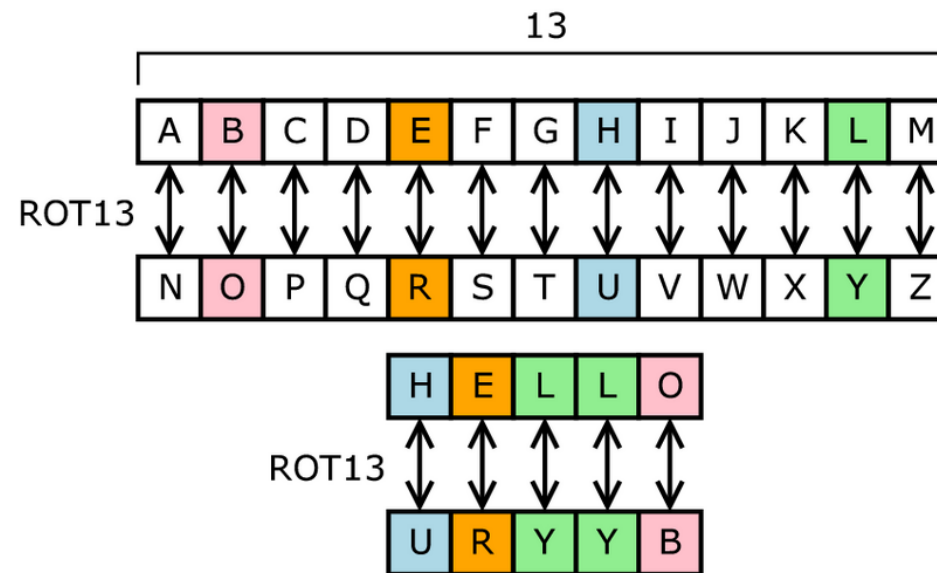
- (a) Nyatakan fungsi enkripsi dan dekripsi di dalam ROT13 sebagai persamaan aritmetika modulo dalam  $p$  dan  $c$ .
- (b) Jika enkripsi dilakukan dua kali berturut-turut terhadap plainteks, apa yang terjadi?

Jawaban:

a)  $c = E(p) = (p + 13) \bmod 26$

$p = D(c) = (c - 13) \bmod 26$

b) Jika dilakukan 2 kali enkripsi terhadap *plaintext*, maka hasilnya sama dengan *plaintext* awal.

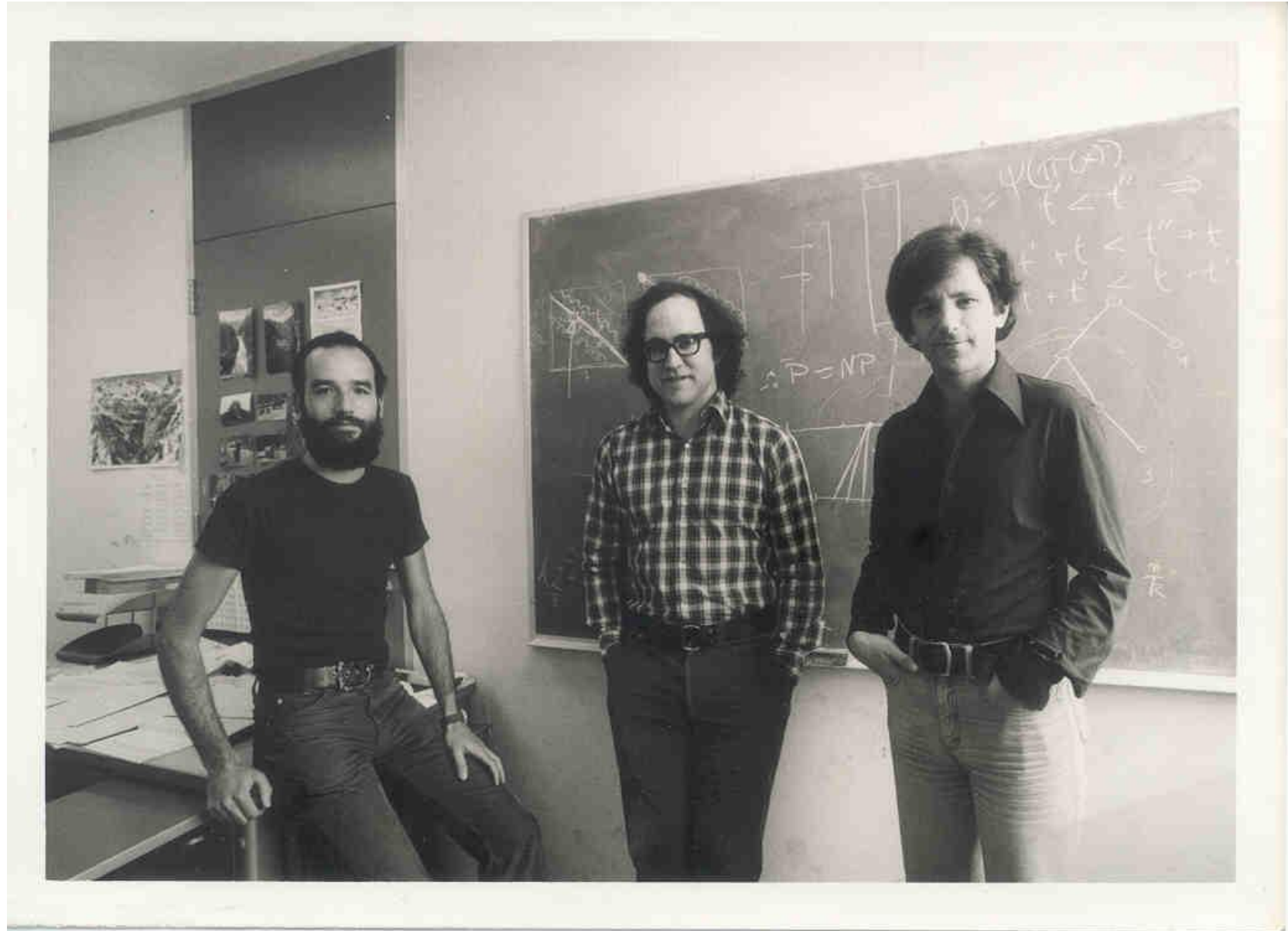


# Algoritma RSA

- Dibuat oleh tiga peneliti dari *MIT (Massachusetts Institute of Technology)*, yaitu Ronald Rivest, Adi Shamir, dan Leonard Adleman, pada tahun 1976.

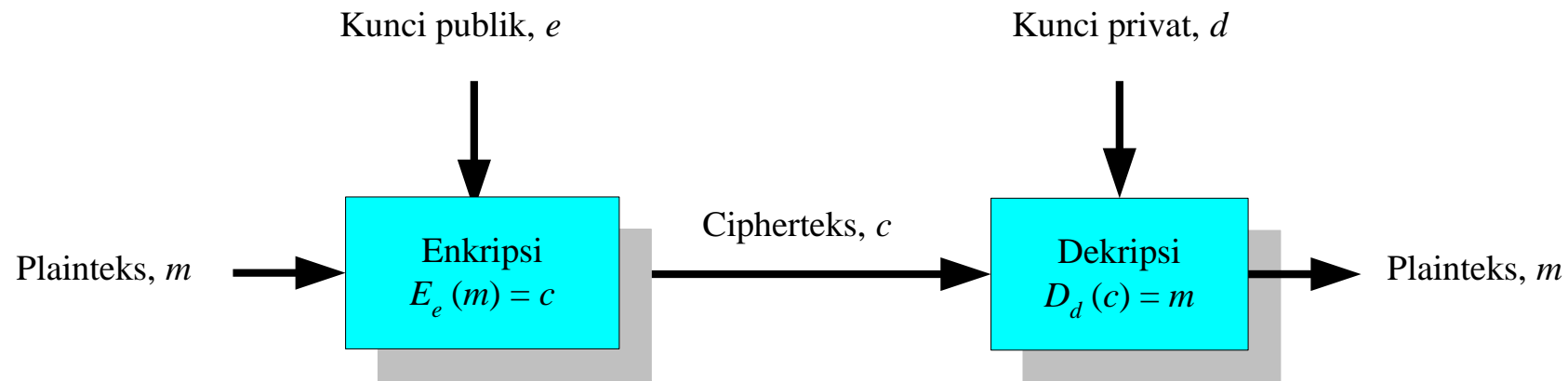


- Termasuk algoritma **kriptografi asimetri**.
- Asimetri: kunci untuk enkripsi berbeda dengan kunci untuk dekripsi



Rinaldi M/IF2120 Matematika Diskrit

- Di dalam Algoritma RSA, setiap pengguna memiliki sepasang kunci:
  1. Kunci publik,  $e$ : untuk mengenkripsi pesan
  2. Kunci privat,  $p$ : untuk mendekripsi pesan



- Kunci publik tidak rahasia (diumumkan kepada publik), sedangkan kunci privat rahasia, hanya diketahui oleh pemilik kunci.
- Dinamakan juga **kriptografi kunci-public** (*public-key cryptography*)

## Prosedur pembangkitan pasangan kunci di dalam RSA

1. Pilih dua bilangan prima,  $p$  dan  $q$  (rahasia)
2. Hitung  $n = pq$ . Besaran  $n$  tidak perlu dirahasiakan.
3. Hitung  $m = (p - 1)(q - 1)$ . (rahasia)
4. Pilih sebuah bilangan bulat untuk kunci publik,  $e$ , yang relatif prima terhadap  $m$ , yaitu  $\text{PBB}(e, m) = 1$ .
5. Hitung kunci dekripsi,  $d$ , melalui kekongruenan  $ed \equiv 1 \pmod{m}$ .



- **Contoh.** Misalkan  $p = 47$  dan  $q = 71$  (keduanya prima), maka dapat dihitung

$$n = pq = 47 \cdot 71 = 3337$$

$$m = (p - 1)(q - 1) = 3220.$$

Pilih kunci publik  $e = 79$  (yang relatif prima dengan 3220), yaitu.

Nilai  $e$  dan  $n$  dapat dipublikasikan ke umum.

- **Catatan:** Dalam praktek, nilai  $p$ ,  $q$ , dan  $e$  adalah bilangan yang sangat besar (minimal 200 digit)

- Selanjutnya dihitung kunci dekripsi  $d$  dengan kekongruenan:

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

yang dapat dihitung dengan

$$d = \frac{1+km}{e} = \frac{1+3220k}{79}$$

dengan mencoba  $k = 0, 1, 2, \dots$ , diperoleh nilai  $d$  bilangan bulat adalah

$$d = 1019$$

Ini adalah kunci dekripsi.

## Prosedur enkripsi-dekripsi:

**Enkripsi:**  $p^e \equiv c \pmod{n}$       atau dapat ditulis:  $c = p^e \bmod n$

**Dekripsi:**  $c^d \equiv p \pmod{n}$       atau dapat ditulis:  $p = c^d \bmod n$

- Misalkan plainteks: 'HARI INI'

atau dalam desimal ASCII: 7265827332737873

Pecah pesan menjadi blok yang lebih kecil (misal 3-angka) untuk memudahkan komputasi:

$$p_1 = 726$$

$$p_4 = 273$$

$$p_2 = 582$$

$$p_5 = 787$$

$$p_3 = 733$$

$$p_6 = 003$$

- *Enkripsi setiap blok (menggunakan kunci publik  $e = 79$ ) :  $c = p^e \bmod n$*

$$c_1 = 726^{79} \bmod 3337 = 215$$

$$c_2 = 582^{79} \bmod 3337 = 776$$

dst untuk sisa blok lainnya

Luaran: chiperteks  $C = 215\ 776\ 1743\ 933\ 1731\ 158$ .

- *Dekripsi (menggunakan kunci privat  $d = 1019$ ):  $p = c^d \bmod n$*

$$p_1 = 215^{1019} \bmod 3337 = 726$$

$$p_2 = 776^{1019} \bmod 3337 = 582$$

dst untuk sisi blok lainnya

Luaran: plainteks = 7265827332737873

atau dalam kode ASCII karakternya adalah HARI INI.

# Pembangkit Bilangan Acak

- Pembangkit bilangan acak yang berbasis kekongruenan linjar adalah *linear congruential generator* atau *LCG*:

$$X_n = (aX_{n-1} + b) \bmod m$$

$X_n$  = bilangan acak ke- $n$  dari deretnya

$X_{n-1}$  = bilangan acak sebelumnya

$a$  = faktor pengali

$b$  = *increment*

$m$  = modulus

Kunci pembangkit adalah  $X_0$  yang disebut **umpan** (*seed*).

Contoh:  $X_n = (7X_{n-1} + 11) \bmod 17$ , dan  $X_0 = 0$

$n$	$X_n$
0	0
1	11
2	3
3	15
4	14
5	7
6	9
7	6
8	2
9	8
10	16
11	4
12	5
13	12
14	10
15	13
16	0
17	11
18	3
19	15
20	14
21	7
22	9
23	6
24	2

# Latihan soal teori bilangan

(diambil dari soal kuis dan UAS)

1. Dengan menggunakan Teorema Fermat, hitunglah  $(5^{2017} \bmod 7 + 5^{2017} \bmod 11) \bmod 7$ . **(Nilai: 10)**
2. (a) Hitunglah  $51^{-1} \pmod{1008}$   
(b) Gunakan hasil jawaban a di atas untuk menemukan semua solusi bilangan bulat  $x$  yang memenuhi kongruensi  $51x \equiv 177 \pmod{1008}$
3. Sebuah buku memiliki kode ISBN **0-1p026-690-q**. Tentukan nilai  $(p + q) \bmod 3$  dari nomor ISBN tersebut jika diketahui  $6p \equiv 3 \pmod{7}$



4. (a) Carilah PBB (atau  $\gcd$ ) dari 621 dan 483  
 (b) Cari solusi dari  $621m + 483n = k$ , dimana  $k$  adalah PBB dari 621 dan 483  
 (c) Hitung  $3^{64} \bmod 67$  dengan menggunakan Fermat's Theorem
5. Berapakah nilai  $x$  dan  $y$  bilangan bulat yang memenuhi persamaan  $1757x - 1631y = 483$ ?
6. Salah satu penggunaan *Chinese Remainder Problem* adalah *Secret sharing* yang merupakan salah satu metode kriptografi. Misal terdapat sebuah rahasia  $S$ , maka rahasia tersebut dibagi menjadi beberapa bagian (*shares*). Rahasia  $S$  dapat dibangun kembali hanya jika seseorang memiliki set *shares* yang valid. Salah satu implementasi *secret sharing* adalah skema **Asmuth-Bloom**. Rahasia  $S$  akan dibagi ke dalam beberapa  $I_0, I_1, I_2, \dots, I_n$  *shares*. Bagian terakhir dari skema ini adalah mendapatkan nilai  $S$  dengan persamaan  $S = x_0 \bmod p_0$ ,  $p_0$  adalah sebuah bilangan yang ditentukan saat pembagian *shares*. Kemudian, diberikan sebuah baris bilangan  $m_0, m_1, \dots, m_k$  yang masing-masing saling relatif prima, maka  $x_0$  merupakan solusi unik modulo  $(m_0 \cdot m_1 \cdot m_2 \cdot \dots \cdot m_n)$  dari persamaan: **(Nilai = 25)**

$$x \equiv I_1 \bmod m_1, x \equiv I_2 \bmod m_2, x \equiv I_3 \bmod m_3, \dots, x \equiv I_n \bmod m_n$$

Untuk  $p_0 = 5$ ,  $\{(I_k, m_k)\} = \{(1,7), (9,11), (5,13)\}$ , tentukan nilai rahasia dari *secret sharing* !

TAMAT