Teori Bilangan

Bahan Kuliah IF2091 Struktur Diskrit

Bilangan Bulat

- Bilangan bulat 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 terdapat bilangan bulat unik q (*quotient*) dan r (*remainder*), sedemikian sehingga

$$m = nq + r \qquad (1)$$

dengan $0 \leq r < n$.

Contoh 2.

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

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

(ii) –22/3 = –8, sisa 2:

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

tetapi $-22 = 3(-7) - 1$ salah

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

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 PBB(a, b) = d.

Contoh 3.

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

→ PBB(45, 36) = 9.

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

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

maka PBB(m, n) = PBB(n, r)

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

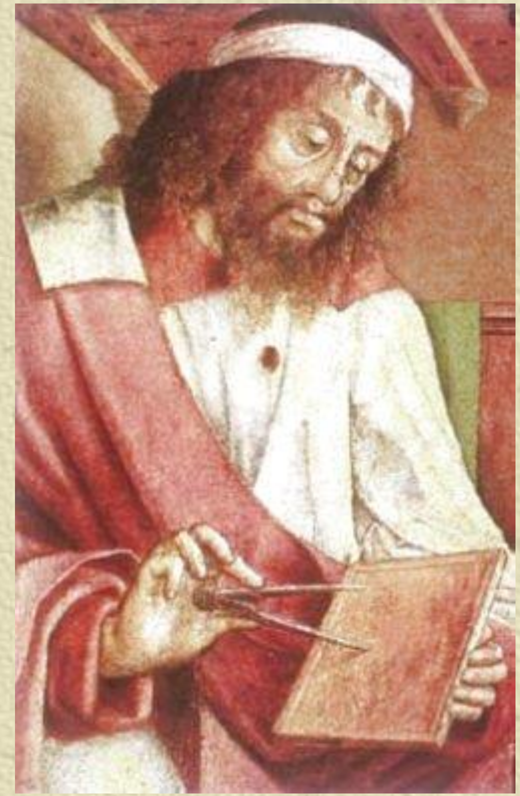
$$60 = 18 \cdot 3 + 6$$

maka PBB(60, 18) = 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

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

Menurut Teorema 2,

$$
\text{PBB}(m, n) = \text{PBB}(r_0, r_1) = \text{PBB}(r_1, r_2) = \ldots = \text{PBB}(r_{n-2}, r_{n-1}) = \text{PBB}(r_{n-1}, r_n) = \text{PBB}(r_n, 0) = r_n
$$

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

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 ≥ n
  Masukan: m dan n, m ≥ n dan m, n ≥ 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 $m \geq n$

$$80 = 6 \cdot 12 + 8$$

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

$$8 = 2 \cdot 4 + 0$$

Sisa pembagian terakhir sebelum 0 adalah 4, maka PBB(80, 12) = 4.

Kombinasi Lanjar

- PBB(a,b) dapat dinyatakan sebagai **kombinasi lanjar** (*linear combination*) a dan b dengan dengan koefisien-koefisennya.

- **Contoh 6**: 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 PBB(a, b) = $ma + nb$.

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

  45 = 2 (21) + 3

  21 = 7 (3) + 0

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

  Substitusi dengan persamaan–persamaan di atas menghasilkan:

  3 = 45 – 2 (21)

  yang merupakan kombinasi lanjar dari 45 dan 21

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

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

$312 = 4 \cdot 70 + 32$ (i)

$70 = 2 \cdot 32 + 6$ (ii)

$32 = 5 \cdot 6 + 2$ (iii)

$6 = 3 \cdot 2 + 0$ (iv)

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

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

$2 = 32 – 5 \cdot 6$ (iv)

$6 = 70 – 2 \cdot 32$ (v)

Sulihkan (v) ke dalam (iv) menjadi

$2 = 32 – 5\cdot(70 – 2\cdot32) = 1\cdot32 – 5\cdot70 + 10\cdot32 = 11 \cdot 32 – 5 \cdot 70$ (vi)

Susun pembagian nomor (i) menjadi

$32 = 312 – 4 \cdot 70$ (vii)

Sulihkan (vii) ke dalam (vi) menjadi

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

Jadi, 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.

- 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 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 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* mod *m (dibaca "*a* modulo *m*")

  memberikan sisa jika a dibagi dengan m.

- Notasi: $a \bmod m = r$ sedemikian sehingga

  $a = mq + r$, dengan $0 \le r < m$.

- m disebut **modulus** atau **modulo**, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m - 1\}$.

- **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) $-41 \bmod 9 = 4$ $(-41 = 9(-5) + 4)$
  (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 $-41 \bmod 9 = 9 - 5 = 4$.

Kongruen

- Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka dikatakan $38 \equiv 13 \pmod 5$

  (baca: 38 kongruen dengan 13 dalam modulo 5).

- Misalkan a dan b bilangan bulat dan m adalah bilangan > 0, maka $\boldsymbol{a \equiv b \pmod{m}}$ jika m habis membagi $a - b$.

- 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)*

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

(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)

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

  $a = b + km$ (*k* adalah bilangan bulat)

- **Contoh 13.**

  $17 \equiv 2 \pmod{3}$ ➔ $17 = 2 + 5 \cdot 3$

  $-7 \equiv 15 \pmod{11}$ ➔ $-7 = 15 + (-2)11$

- $a \bmod m = r$ dapat juga ditulis sebagai

  $a \equiv r \pmod{m}$

- **Contoh 14.**

  (i) $23 \bmod 5 = 3$ ➔ $23 \equiv 3 \pmod{5}$

  (ii) $27 \bmod 3 = 0$ ➔ $27 \equiv 0 \pmod{3}$

  (iii) $6 \bmod 8 = 6$ ➔ $6 \equiv 6 \pmod{8}$

  (iv) $0 \bmod 12 = 0$ ➔ $0 \equiv 0 \pmod{12}$

  (v) $-41 \bmod 9 = 4$ ➔ $-41 \equiv 4 \pmod{9}$

  (vi) $-39 \bmod 13 = 0$ ➔ $-39 \equiv 0 \pmod{13}$

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):

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

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

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

$\Leftrightarrow ac = bc + Km$

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

2(i) $a \equiv b \pmod{m} \quad \Leftrightarrow \quad a = b + k_1 m$

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

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

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

$\Leftrightarrow \quad (a + c) = (b + d) \pmod{m}$ ■

Contoh 15.

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

$17 + 5 = 2 + 5 \pmod 3 \quad \Leftrightarrow \quad 22 = 7 \pmod 3$

$17 \,.\, 5 = 5 \cdot 2 \pmod 3 \quad \Leftrightarrow \quad 85 = 10 \pmod 3$

$17 + 10 = 2 + 4 \pmod 3 \quad \Leftrightarrow \quad 27 = 6 \pmod 3$

$17 \,.\, 10 = 2 \cdot 4 \pmod 3 \quad \Leftrightarrow \quad 170 = 8 \pmod 3$

- 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

Jika $a \equiv b \pmod{m}$ dan $c \equiv$ d $\pmod{m}$ adalah sembarang bilangan bulat maka buktikan bahwa

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

•

Solusi

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

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

maka

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

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

$\Leftrightarrow ac = bd + Km$ dengan $K = bk_2 + dk_1 + k_1 k_2 m$

$\Leftrightarrow$ $\boldsymbol{ac \equiv bd \pmod{m}}$ (terbukti)

Balikan Modulo (modulo invers)

- Di dalam aritmetika bilangan riil, inversi (*inverse*) dari perkalian adakah pembagian.

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

- Di dalam aritmetika modulo, masalah menghitung inversi modulo lebih sukar.

- Jika a dan m relatif prima dan $m > 1$, maka balikan (*invers*) dari a modulo m ada.

- Balikan dari a modulo m adalah bilangan bulat x sedemikian sehingga

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

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

Bukti: a dan m relatif prima, jadi 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 $ym \equiv 0 \pmod{m}$, maka

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

Kekongruenan yang terakhir ini berarti bahwa x adalah balikan dari a modulo m. ■

- Pembuktian di atas juga menceritakan bahwa untuk mencari balikan dari *a* modulo *m*, kita harus membuat kombinasi lanjar dari *a* dan *m* sama dengan 1.

- Koefisien *a* dari kombinasi lanjar tersebut merupakan balikan dari *a* modulo *m*.

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

  Solusi:

- (a) Karena PBB(4, 9) = 1, maka balikan dari 4 (mod 9) ada. Dari algoritma Euclidean diperoleh bahwa

$$9 = 2 \cdot 4 + 1$$

Susun persamaan di atas menjadi

$$-2 \cdot 4 + 1 \cdot 9 = 1$$

Dari persamaan terakhir ini kita peroleh –2 adalah balikan dari 4 modulo 9.

Periksa bahwa $-2 \cdot 4 \equiv 1 \pmod 9$

- Catatan: setiap bilangan yang kongruen dengan

  $-2 \pmod{9}$

  juga adalah inversi dari 4, misalnya 7, –11, 16, dan seterusnya, karena

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

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

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

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

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

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

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

Susun (ii) menjadi:

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

Susun (i) menjadi

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

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

$$-2 \cdot 17 + 5 \cdot 7 = 1$$

Dari persamaan terakhir diperoleh –2 adalah balikan dari 17 (mod 7)

* $-2 \cdot 17 \equiv 1 \pmod 7$ (7 habis membagi $-2 \cdot 17 - 1 = -35$)

(c) Karena PBB(18, 10) = 2 $\neq$ 1, maka balikan dari 18 (mod 10) tidak ada.

Cara lain menghitung balikan

- Ditanya: balikan dari a (mod m)
- Misalkan x adalah balikan dari a (mod m), maka

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

  atau dalam noatsi 'sama dengan':

  $ax = 1 + km$

  atau

  $x = (1 + km)/a$

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

  Solusinya adalah semua bilangan bulat yang memenuhi.

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

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

Untuk $k = 0 \rightarrow x$ tidak bulat

$k = 1 \rightarrow x$ tidak bulat

$k = 2 \rightarrow x$ tidak bulat

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

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

Balikan dari 4 (mod 9) adalah 7 (mod 9),

-2 (mod 9), dst

Latihan

- Tentukan semua balikan dari 9 (mod 11).

Solusi:

- 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, ..., 1, 2, ...) maka
- diperoleh $x = 5$. Semua bilangan lain yang kongruen dengan 5 (mod 11) juga merupakan solusi, yaitu –6, 16, 27, ...

Kekongruenan Lanjar

- Kekongruenan lanjar berbentuk:

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

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

  Pemecahan: $ax = b + km$ ➔ $x = \dfrac{b + km}{a}$

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

Contoh 19.

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

Penyelesaian:

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

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

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

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

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

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

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

…

$k = –1 \rightarrow x = (3 – 1 \cdot 9)/4 = –6/4$ (bukan solusi)

$k = –2 \rightarrow x = (3 – 2 \cdot 9)/4 = –15/4$ (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, …

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

- Seperti dalam persamaan biasa,

  $4x = 12$ → kalikan setiap ruas dengan 1/4 (yaitu invers 4), maka $1/4 \cdot 4x = 12 \cdot 1/4$ → $x = 3$

- $4x \equiv 3 \pmod 9$ → kalikan setiap ruas dengan balikan dari 4 (mod 9) (dalam hal ini sudah kita hitung, yaitu –2)

  $(-2) \cdot 4x \equiv (-2) \cdot 3 \pmod 9 \Leftrightarrow -8x \equiv -6 \pmod 9$

Karena $-8 \equiv 1 \pmod 9$, maka $x \equiv -6 \pmod 9$. Semua blangan bulat yang kongruen dengan –6 (mod 9) adalah solusinya, yitu 3, 12, …, dan –6, -15, …

(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 $2x \equiv 3 \pmod 5$.

Latihan

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

Solusi

Misal : bilangan bulat = x

$x \bmod 3 = 2 \rightarrow x \equiv 2 \pmod 3$

$x \bmod 5 = 3 \rightarrow x \equiv 3 \pmod 5$

Jadi, terdapat sistem kekongruenan:

$x \equiv 2 \pmod 3$ (i)

$x \equiv 3 \pmod 5$ (ii)

Untuk kongruen pertama:

$x = 2 + 3k_1$ (iii)

Substitusikan (iii) ke dalam (ii):

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

diperoleh

$k_1 \equiv 2 \pmod 5$ atau $k_1 = 2 + 5k_2$

$x = 2 + 3k_1$

$= 2 + 3\ (2 + 5k_2)$

$= 2 + 6 + 15k_2$

$= 8 + 15k_2$

atau

$x \equiv 8 \pmod{15}$

Semua nilai x yang kongruen dengan 8 (mod 15) adalah solusinya, yaitu

$x = 8$, $x = 23$, $x = 38$, …, $x = -7$, dst

Chinese Remainder Problem

- Pada abad pertama, 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 kongruen lanjar:

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

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

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

Teorema 5. (*Chinese Remainder Theorem*) Misalkan $m_1, m_2, \ldots, m_n$ adalah bilangan bulat positif sedemikian sehingga PBB(m_i, m_j) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar

$$x \equiv a_k \pmod{m_k}$$

mempunyai sebuah solusi unik dalam modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Contoh 15.
Tentukan solusi dari pertanyaan Sun Tse di atas.

Penyelesaian:

$x \equiv 3 \pmod 5$ → $x = 3 + 5k_1$ (i)

Sulihkan (i) ke dalam kongruen kedua menjadi:

$3 + 5k_1 \equiv 5 \pmod 7$ → $k_1 \equiv 6 \pmod 7$, atau $k_1 = 6 + 7k_2$ (ii)

Sulihkan (ii) ke dalam (i):

$x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2$ (iii)

Sulihkan (iii) ke dalam kongruen ketiga menjadi:

$33 + 35k_2 \equiv 7 \pmod{11}$ → $k_2 \equiv 9 \pmod{11}$ atau $k_2 = 9 + 11k_3$.

Sulihkan k_2 ini ke dalam (iii) menghasilkan:

$x = 33 + 35(9 + 11k_3) = 348 + 385k_3$

atau $x \equiv 348 \pmod{385}$. Ini adalah solusinya.

348 adalah bilangan bulat positif terkecil yang merupakan solusi sistem kekongruenan di atas. Perhatikan bahwa 348 mod 5 = 3, 348 mod 7 = 5, dan 348 mod 11 = 7. Catatlah bahwa $385 = 5 \cdot 7 \cdot 11$.

- Solusi unik ini mudah dibuktikan sebagai berikut. Solusi tersebut dalam modulo:

  $m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 5 \cdot 77 = 11 \cdot 35.$

  Karena $77 \,.\, 3 \equiv 1 \pmod 5$,

  $55 \cdot 6 \equiv 1 \pmod 7$,

  $35 \cdot 6 \equiv 1 \pmod{11}$,

  maka solusi unik dari sistem kongruen tersebut adalah

  $x \equiv 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \pmod{385}$

  $\equiv 3813 \pmod{385}$

  $\equiv 348 \pmod{385}$

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.

$9 = 3 \times 3$

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

$13 = 13$ (atau 1×13)

* Tes bilangan prima:

(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) √171 = 13.077. Bilangan prima yang ≤ √171 adalah 2, 3, 5, 7, 11, 13.

Karena 171 habis dibagi 3, maka 171 adalah bilangan komposit.

(ii) √199 = 14.107. Bilangan prima yang ≤ √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 PBB(a, p) = 1, maka

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

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

Ambil a = 2 karena PBB(17, 2) = 1 dan 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.