Teori Bilangan

Egi Safitri, S.Mat., M.Si

Bilangan Bulat

Bilangan bulat
8, 21, 8765, -34, 0

Bilangan desimal
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

$$m = nq + r \tag{1}$$

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 $0 \leq r < n$)

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 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

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.

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

$2 = 32 - 5 \cdot (70 - 2 \cdot 32) = 1 \cdot 32 - 5 \cdot 70 + 10 \cdot 32 = 11 \cdot 32 - 5 \cdot 70$ (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) = $2 = 11 \cdot 312 - 49 \cdot 70$

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

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

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

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

(v) $-41 \bmod 9 = 4$ $\quad (-41 = 9(-5) + 4)$

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

- *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 mod 5 = 3 ➔ $23 \equiv 3 \pmod{5}$

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

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

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

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

  (vi) – 39 mod 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:

$$\Leftrightarrow a = b + km$$
$$\Leftrightarrow a - b = km$$
$$\Leftrightarrow (a - b)c = ckm$$
$$\Leftrightarrow ac = bc + Km$$
$$\Leftrightarrow ac \equiv bc \pmod{m} \quad \blacksquare$$

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

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

$$\Leftrightarrow \quad (a + c) = (b + d) + (k_1 + k_2)m$$
$$\Leftrightarrow \quad (a + c) = (b + d) + km \qquad (\, k = k_1 + k_2)$$
$$\Leftrightarrow \quad (a + c) = (b + d) \pmod{m} \qquad \blacksquare$$

Contoh 15.

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

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

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

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

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

- 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

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

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

maka

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

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

$\Leftrightarrow ac = bd + Km$ 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 adalah 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 (mod m) ada.

- Balikan dari a (mod m) adalah bilangan bulat x sedemikian sehingga

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

- Dalam notasi lainnya, $a^{-1} \pmod{m} = x$

- **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 (mod 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:

$17 = 2 \cdot 7 + 3$ (i)

$7 = 2 \cdot 3 + 1$ (ii)

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

Susun (ii) menjadi:

$1 = 7 - 2 \cdot 3$ (iv)

Susun (i) menjadi

$3 = 17 - 2 \cdot 7$ (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 notasi '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