People
Innovation
Excellence

LECTURE NOTES

Week ke - 05

Teori Bilangan

LEARNING OUTCOMES

1. Peserta diharapkan mampu menjelaskan tentang teori himpunan, Fungsi, himpunan Fuzzy, metode-metode menghitung, dan teori bilangan.
2. Peserta diharapkan mampu menjelaskan mencari solusi penerapan teori himpunan, Fungsi, himpunan Fuzzy, metode-metode menghitung, dan teori bilangan.

OUTLINE MATERI :

1. Bilangan Bulat
2. Pembagi Bersama Terbesar (PBB)
3. Relatif Prima
4. Aritmetika Modulo

Teori Bilangan

5.1 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 adalah dua buah bilangan bulat dengan syarat $a \neq 0$. Kita menyatakan bahwa 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 $a \neq 0$. ($\mathbf{Z}$ = himpunan bilangan bulat)
- Kadang-kadang pernyataan "*a* habis membagi *b*" ditulis juga "*b* **kelipatan** *a*".

Contoh 1: $4 \mid 12$ karena $12 \div 4 = 3$ (bilangan bulat) atau $12 = 4 \times 3$. Tetapi $4 \mid 13$ karena $13 \div 4 = 3.25$ (bukan bilangan bulat).

Teorema 1 (Teorema Euclidean).

Misalkan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (*quotient*) dan r (*remainder*), sedemikian sehingga

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

dengan $0 \leq r < n$.

Contoh 2.

(i) 1987 dibagi dengan 97 memberikan hasil bagi 20 dan sisa 47: $1987 = 97.\ 20 + 47$

(ii) –22 dibagi dengan 3 memberikan hasil bagi –8 dan sisa 2:

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

tetapi $-22 = 3(-7) - 1$ salah karena $r = -1$ tidak memenuhi syarat $0 \le r < n$.

5.2 Pembagi Bersama Terbesar (PBB)

Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB – **greatest common divisor** atau *gcd*) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d \mid a$ 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 dari 45 dan 36 adalah 1, 3, 9

PBB(45, 36) = 9.

Algoritma Euclidean

- Algoritma Euclidean adalah algoritma untuk mencari PBB dari dua buah bilangan bulat.
- Euclid, penemu algoritma Euclidean, adalah seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam bukunya yang terkenal, *Element*.
- Diberikan dua buah bilangan bulat tak-negatif m dan n ($m \ge n$). 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 $n \ne 0$,

   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.

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.

5.3 Relatif Prima

- Dua buah bilangan bulat *a* dan *b* dikatakan *relatif prima* jika PBB(*a*, *b*) = 1.

  Contoh 5 :

  20 dan 3 relatif prima sebab PBB(20, 3) = 1. Begitu juga 7 dan 11 relatif prima karena PBB(7, 11) = 1. Tetapi 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

$$ma + nb = 1 \qquad (2)$$

  Contoh 6 :

  Bilangan 20 dan 3 adalah relatif prima karena PBB(20, 3) =1, atau dapat ditulis

$$2 \cdot 20 + (-13) \cdot 3 = 1$$

  dengan $m = 2$ dan $n = -13$. Tetapi 20 dan 5 tidak relatif prima karena PBB(20, 5) = 5 $\neq$ 1 sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \cdot 20 + n \cdot 5 = 1$.

5.4 Aritmetika Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi a mod m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m.

Notasi: a mod $m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.

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

Contoh 7. Beberapa hasil operasi dengan operator modulo:

(i) 23 mod 5 = 3	$(23 = 5 \cdot 4 + 3)$
(ii) 27 mod 3 = 0	$(27 = 3 \cdot 9 + 0)$
(iii) 6 mod 8 = 6	$(6 = 8 \cdot 0 + 6)$
(iv) 0 mod 12 = 0	$(0 = 12 \cdot 0 + 0)$
(v) – 41 mod 9 = 4	$(-41 = 9\,(-5) + 4)$
(vi) – 39 mod 13 = 0	$(-39 = 13(-3) + 0)$

Penjelasan (v): Karena a negatif, bagi $|a|$ dengan m mendapatkan sisa r'. Maka a mod $m = m - r'$ bila $r' \neq 0$. Jadi $|-41|$ mod 9 = 5, sehingga –41 mod 9 = 9 – 5 = 4.

Kongruen

- Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka kita katakan
  $38 \equiv 13 \pmod 5$ (baca: 38 kongruen dengan 13 dalam modulo 5).
- Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b \pmod m$ jika m habis membagi $a - b$.
- Jika a tdak kongruen dengan b dalam modulus m, maka ditulis $a \not\equiv b \pmod m$.

Contoh 8.

$17 \equiv 2 \pmod 3$	(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 $-7 - 15 = -22$)

- Kekongruenan a □ b (mod m) dapat pula dituliskan dalam hubungan

$$a = b + km \tag{3}$$

yang dalam hal ini k adalah bilangan bulat.

Contoh 9.

$17 \equiv 2 \pmod 3$	dapat ditulis sebagai $17 = 2 + 5 \cdot 3$
$-7 \equiv 15 \pmod{11}$	dapat ditulis sebagai $-7 = 15 + (-2)11$

- Berdasarkan definisi aritmetika modulo, kita dapat menuliskan a mod $m = r$ sebagai

$$a \equiv r \pmod m$$

Contoh 10.

Beberapa hasil operasi dengan operator modulo berikut:

(i) 23 mod 5 = 3 dapat ditulis sebagai $23 \equiv 3 \pmod 5$

(ii) 27 mod 3 = 0 dapat ditulis sebagai $27 \equiv 0 \pmod 3$

(iii) 6 mod 8 = 6 dapat ditulis sebagai $6 \equiv 6 \pmod 8$

(iv) 0 mod 12 = 0 dapat ditulis sebagai $0 \equiv 0 \pmod{12}$

(v) – 41 mod 9 = 4 dapat ditulis sebagai $-41 \equiv 4 \pmod 9$

(vi) – 39 mod 13 = 0 dapat ditulis sebagai $-39 \equiv 0 \pmod{13}$

Teorema 2. 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) $a^p \equiv b^p \pmod{m}$ untuk suatu bilangan bulat tak negatif p.

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

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

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

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

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

Contoh 11.

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

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

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

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

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

- Perhatikanlah bahwa Teorema 2 tidak memasukkan operasi pembagian pada aritmetika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi. Misalnya:

(i) $10 \equiv 4 \pmod 3$ dapat dibagi dengan 2 karena $10/2 = 5$ dan $4/2 = 2$, dan $5 \equiv 2 \pmod 3$

(ii) $14 \equiv 8 \pmod 6$ tidak dapat dibagi dengan 2, karena $14/2 = 7$ dan $8/2 = 4$, tetapi $7 \not\equiv 4 \pmod 6$

Balikan Modulo (modulo invers)

- Jika a dan m relatif prima dan $m > 1$, maka kita dapat menemukan balikan (*invers*) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga

  $$\bar{a}a \equiv 1 \pmod m$$

  Bukti: Dari definisi relatif prima diketahui bahwa PBB(a, m) = 1, dan menurut persamaan (2) terdapat bilangan bulat p dan q sedemikian sehingga

  $$pa + qm = 1$$

  yang mengimplikasikan bahwa

  $$pa + qm \equiv 1 \pmod m$$

  Karena $qm \equiv 0 \pmod m$, maka

  $$pa \equiv 1 \pmod m$$

  Kekongruenan yang terakhir ini berarti bahwa p 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 12.

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

Penyelesaian:

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

(b) 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. Periksalah bahwa

$$-2 \cdot 4 \equiv 1 \pmod 9 \qquad (9 \text{ habis membagi } -2 \cdot 4 - 1 = -9)$$

(c) 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 ini kita peroleh –2 adalah balikan dari 17 modulo 7.

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

(d) Karena PBB(18, 10) = 2 ≠ 1, maka balikan dari 18 (mod 10) tidak ada.

Kekongruenan Lanjar

- Kekongruenan lanjar adalah kongruen yang berbentuk

  $ax \equiv b \pmod m$

  dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

- Nilai-nilai x dicari sebagai berikut:

  $ax = b + km$

  yang dapat disusun menjadi

$$x = \frac{b + km}{a}$$

  dengan k adalah sembarang bilangan bulat. Cobakan untuk $k = 0, 1, 2, \ldots$ dan $k = -1, -2, \ldots$ yang menghasilkan x sebagai bilangan bulat.

Contoh 13.

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

Penyelesaian:

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

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

$k = 0 \rightarrow x = (3 + 0 \cdot 9)/4 = 3/4$ (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, …

KESIMPULAN

1. Bilangan bulat adalah bilangan yangtidak 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.
2. **Teorema 1 (Teorema Euclidean).**

   Misalkan *m* dan *n* adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika *m* dibagi dengan *n* maka terdapat dua buah bilangan bulat unik *q* (*quotient*) dan *r* (*remainder*), sedemikian sehingga

   $$m = nq + r$$

   dengan $0 \leq r < n$.
3. Pembagi bersama terbesar (PBB – **greatest common divisor** atau *gcd*) dari *a* dan *b* adalah bilangan bulat terbesar *d* sedemikian sehingga $d \mid a$ dan $d \mid b$. Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

4. 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
5. Dua buah bilangan bulat *a* dan *b* dikatakan *relatif prima* jika PBB(a, b) = 1.
6. Jika *a* dan *b* relatif prima, maka terdapat bilangan bulat *m* dan *n* sedemikian sehingga

   $$ma + nb = 1$$
7. Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > 0. Operasi *a* mod *m* (dibaca "*a* modulo *m*") memberikan sisa jika *a* dibagi dengan *m*.
8. Jika *a* dan *m* relatif prima dan $m > 1$, maka kita dapat menemukan balikan (*invers*) dari *a*

modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga

$$\bar{a}a \equiv 1 \pmod{m}$$

9. Kekongruenan lanjar adalah kongruen yang berbentuk

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

dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

Nilai-nilai x dicari sebagai berikut:

$$ax = b + km$$

yang dapat disusun menjadi

$$x = \frac{b + km}{a}$$

dengan k adalah sembarang bilangan bulat. Cobakan untuk $k = 0, 1, 2, \ldots$ dan $k = -1, -2, \ldots$ yang menghasilkan x sebagai bilangan bulat.

People
Innovation
Excellence

DAFTAR PUSTAKA

1. Rinaldi Munir, “Matematika Diskrit”, edisi 6, 2016, Informatika Bandung, Indonesia, ISBN 978-602-6232-13-7

2. Jong Jek Siang, Matematika Diskrit dan Aplikasinya pada Ilmu Komputer, Andi Offset, Yogyakarta.2009