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 124 = 3 (bilangan bulat) atau $12 = 4 \times 3$. Tetapi $4 \nmid 13$ karena 134 = 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 $0 \le r < n$.

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 dari 45 dan 36 adalah 1, 3, 9

PBB(45, 36) = 9.

- **Teorema 2.** Misalkan *m* dan *n* bilangan bulat, dengan syarat $n > 0$ sedemikian sehingga
- $$m = nq + r \quad , 0 \le r < n$$
- maka PBB(m, n) = PBB(n, r)

- **Contoh 3**: $m = 60$, $n = 18$,

  $$60 = 18 \cdot 3 + 12$$
- maka PBB(60, 18) = PBB(18, 12) = 6

Algoritma Euclidean

- Tujuan: algoritma untuk mencari PBB dari dua buah bilangan bulat.

- Penemu: Euclid, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, *Element*.

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,

$$
\begin{aligned}
&\mathrm{PBB}(m, n) = \mathrm{PBB}(r_0, r_1) = \mathrm{PBB}(r_1, r_2) = \ldots = \\
&\mathrm{PBB}(r_{n-2}, r_{n-1}) = \mathrm{PBB}(r_{n-1}, r_n) = \mathrm{PBB}(r_n, 0) = r_n
\end{aligned}
$$

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.

Kombinasi Lanjar

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

- Contoh: 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) = $ma + nb$.

Relatif Prima

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

- **Contoh 6.**

  (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 7.** 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 mod $m = r$ sedemikian sehingga

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

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

Contoh 8. Beberapa hasil operasi dengan operator modulo:

- (i) 23 mod 5 = 3 (23 = 5 · 4 + 3)

  (ii) 27 mod 3 = 0 (27 = 3 · 9 + 0)

  (iii) 6 mod 8 = 6 (6 = 8 · 0 + 6)

  (iv) 0 mod 12 = 0 (0 = 12 · 0 + 0)

  (v) – 41 mod 9 = 4 (–41 = 9 (–5) + 4)

  (vi) – 39 mod 13 = 0 (–39 = 13(–3) + 0)

Penjelasan untuk (v): Karena *a* negatif, bagi |*a*| dengan *m* mendapatkan sisa *r*'. Maka *a* mod *m* = *m* – *r*' bila *r*' ≠ 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 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 $a \equiv b \pmod m$ jika m habis membagi $a - b$.

- Jika a tidak kongruen dengan b dalam modulus m, maka ditulis $a \not\equiv b \pmod m$.

Contoh 9.

$17 \equiv 2 \pmod 3$ *(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)

- $a \equiv b \pmod{m}$ dapat dituliskan sebagai

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

- **Contoh 10.**

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

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

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

  $a \equiv r \pmod{m}$

- **Contoh 11.**

  (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 bilangn 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) $a \equiv b \pmod{m} \Leftrightarrow a = b + k_1 m$

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

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

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

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

Contoh 12.

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:

$10 \equiv 4 \pmod 3$ 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 $7 \not\equiv 4 \pmod 6$.

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 kita balikan (*invers*) dari a modulo m ada.

- Balikan dari a modulo m adalah bilangan bulat sedemikian sehingga

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

Bukti: a dan m relatif prima, jadi PBB(a, m) = 1, dan 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 13.** 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 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 modulo 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 ini kita peroleh –2 adalah balikan dari 17 modulo 7.

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

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

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 14.

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, …

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

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.*
- 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, …, 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 modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

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

Penyelesaian:

Menurut persamaan (5.6), kongruen pertama, $x \equiv 3 \pmod 5$, memberikan $x = 3 + 5k_1$ untuk beberapa nilai k. Sulihkan ini ke dalam kongruen kedua menjadi $3 + 5k_1 \equiv 5 \pmod 7$, dari sini kita peroleh $k_1 \equiv 6 \pmod 7$, atau $k_1 = 6 + 7k_2$ untuk beberapa nilai k_2. Jadi kita mendapatkan $x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2$ yang mana memenuhi dua kongruen pertama. Jika x memenuhi kongruen yang ketiga, kita harus mempunyai $33 + 35\mathrm{k}_2 \equiv 7 \pmod{11}$, yang mengakibatkan $k_2 \equiv 9 \pmod{11}$ atau $k_2 = 9 + 11k_3$. Sulihkan k_2 ini ke dalam kongruen yang ketiga menghasilkan $x = 33 + 35(9 + 11k_3) \equiv 348 + 385k_3 \pmod{11}$. Dengan demikian, $x \equiv 348 \pmod{385}$ yang memenuhi ketiga konruen tersebut. Dengan kata lain, 348 adalah solusi unik modulo 385. Catatlah bahwa $385 = 5 \cdot 7 \cdot 11$.

- Solusi unik ini mudah dibuktikan sebagai berikut. Solusi tersebut 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.