Teori Bilangan

R. Rosnawati

Jurusan Pendidikan Matematika
FMIPA UNY

Induksi Matematika

- Induksi matematika adalah :

  Salah satu metode pembuktian untuk proposisi perihal bilangan bulat

- Induksi matematika merupakan teknik pembuktian yang baku di dalam matematika

Prinsip Induksi Sederhana

- Misalkan $p(n)$ adalah proposisi bilangan bulat positif dan ingin dibuktikan bahwa $p(n)$ adalah benar untuk semua bilangan bulat positif n. Maka langkah-langkahnya adalah sebagai berikut :
  1. $p(n)$ benar
  2. Jika $p(n)$ benar, maka $p(n+1)$ juga benar untuk setiap n ñ 1
- Sehingga $p(n)$ benar untuk semua bilangan bulat positif n

Prinsip Induksi Sederhana

- Basis induksi
  - Digunakan untuk memperlihatkan bahwa pernyataan benar bila *n* diganti dengan 1, (bila 1 merupakan bilangan bulat positif terkecil yang berlaku pada pernyataan tersebut)
  - Buat implikasi untuk fungsi berikutnya benar untuk setiap bilangan bulat positif
- Langkah induksi
  - Berisi asumsi (pengandaian) yang menyatakan bahwa p(n) benar.
  - Asumsi tersebut dinamakan hipotesis induksi.
  - Dibuktikan kebenaran pernyataan untuk p(n+1)
- Bila kedua langkah tersebut benar maka pembuktian bahwa p(n) benar untuk semua bilangan positif *n*.

Contoh 1:

- Tunjukkan bahwa untuk n ñ 1, 1+2+3+...+n = n(n+1)/2 melalui induksi matematika

Jawab Contoh 1

Pernyataan *p(n)* : $1+2+3+\ldots+n = n(n+1)/2$ untuk n ñ 1

i. Basis induksi

p(1) benar → n = 1 diperoleh dari :

$1 = 1(1+1)/2$

$= 1(2)/2$

$= 2/2$

$= 1$

ii. Langkah induksi

Misalkan p(n) benar → asumsi bahwa :

$1+2+3+\ldots+n = n(n+1)/2$

Adalah benar (hipotesis induksi). Perlihatkan bahwa p(n+1) juga benar yaitu :

$1+2+3+\ldots+n+(n+1) = (n+1)[(n+1)+1]/2$

$1+2+3+\ldots+n+(n+1) = (1+2+3+\ldots+n)+(n+1)$

$= [n(n+1)/2]+(n+1)$

$= [(n^2+n)/2]+(n+1)$

$= [(n^2+n)/2]+[(2n+2)/2]$

$= (n^2+3n+2)/2$

$= (n+1)(n+2)/2$

$= (n+1)[(n+1)+1]/2$

Langkah (i) dan (ii) telah terbukti benar, maka untuk semua bilangan bulat positif *n*, terbukti bahwa untuk semua n ñ 1, $1+2+3+\ldots+n = n(n+1)/2$

Contoh 2

- Gunakan induksi matematika untuk membuktikan bahwa jumlah n buah bilangan ganjil positif pertama adalah n^2.

Jawab Contoh 2

Pernyataan $p(n)$: $1+3+5+\ldots+(2n-1) = n^2$

i. Basis induksi

p(1) benar → jumlah 1 buah bilangan ganjil positif pertama adalah $1^2 = 1$

ii. Langkah induksi

Misalkan p(n) benar → asumsi bahwa :

$1+3+5+\ldots+(2n-1) = n^2$ adalah benar (hipotesis induksi)

Akan ditunjukkan bahwa p(n+1) juga benar, yaitu :

$1+3+5+\ldots+(2n-1)+(2n+1) = (n+1)^2$

Hal ini dapat ditunjukkan sebagai berikut :

$$1+3+5+\ldots+(2n-1)+(2n+1) = [1+3+5+\ldots+(2n-1)]+(2n+1)$$
$$= n^2 + (2n+1)$$
$$= n^2 + 2n + 1$$
$$= (n+1)^2$$

Langkah (i) dan (ii) terbukti benar, maka untuk jumlah *n* buah bilangan ganjil positif pertama adalah n^2.

Contoh 3

- Buktikan dengan induksi matematika bahwa $3^n < n!$ untuk n bilangan bulat positif yang lebih besar dari 6

Jawab Contoh 3

Misalkan p(n) adalah pernyataan bahwa $3^n < n!$, untuk n bilangan bulat positif yang lebih besar dari 6

i. Basis induksi

p(7) benar → $3^7 < 7! \leftrightarrow 2187 < 5040$

ii. Langkah induksi

Misalkan bahwa p(n) benar, yaitu asumsikan bahwa $3^n < n!$ adalah benar. Akan ditunjukkan bahwa p(n+1) juga benar, yaitu $3^{n+1} < (n+1)!$

Hal ini dapat ditunjukkan sbb :

$3^{n+1} < (n+1)!$

$3 \cdot 3^n < (n+1) \cdot n!$

$3^n \cdot 3 / (n+1) < n!$

Menurut hipotesis induksi, $3^n < n!$, sedangkan untuk $n > 6$, nilai $3/(n+1) < 1$, sehingga $3/(n+1)$ akan memperkecil nilai di ruas kiri persamaan.

$3^n \cdot 3/(n+1) < n!$ jelas benar

Dari langkah (i) dan (ii) terbukti benar, maka terbukti bahwa $3^n < n!$ untuk *n* bilangan bulat positif lebih besar dari 6

Bilangan Bulat

- Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 4, 25, 999, -37, 0

- Bukan 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 $4 \nmid 15$ karena $15:4 = 3.75$ (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) 1987/95 = 21, sisa 8:

$$1987 = 97 \cdot 21 + 47$$

(ii) −22/3 = −8, sisa 2:

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

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

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

Faktor Pembagi Bersama (FB)

- Misalkan a dan b bilangan bulat tidak nol.

- Pembagi bersama dari a dan b adalah bilangan bulat d sedemikian hingga $d \mid a$ dan $d \mid b$.

- **Contoh**

  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

Faktor Persekutuan Terbesar (FPB)

- 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
  1. $d \mid a$ dan $d \mid b$.
  2. Bila $c \mid a$ dan $c \mid b$, *maka* d ñ c

- Dalam hal ini kita nyatakan bahwa FPB$(a, b) = d$.

- **Contoh .**

  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

FPB(45, 36) = 9.

Teorema

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

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

$$60 = 18 \cdot 3 + 12$$

- maka FPB(60, 18) = FPB(18, 12) = 6

Algoritma Euclidean

- Tujuan: algoritma untuk mencari FPB 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

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

Menurut Teorema 2,

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

Jadi, FPB dari m dan n adalah sisa terakhir yang tidak nol dari runtunan pembagian tersebut

Contoh. $m = 82$, $n = 12$ dan dipenuhi syarat $m \geq n$

$82 = 6.\ 12 + 10$

$12 = 1.10 + 2$

$10 = 5.2 + 0$

Sisa pembagian terakhir sebelum 0 adalah 2, maka FPB(82, 12) = 2.

Kombinasi Linear

- FPB(a,b) dapat dinyatakan sebagai **kombinasi linear** (*linear combination*) a dan b dengan dengan koefisien-koefisennya.
- Contoh: FPB(82, 12) = 2 ,

$$2 = (-1) \cdot 82 + 7 \cdot 12.$$

- **Teorema.** Misalkan a dan b bilangan bulat positif, maka terdapat bilangan bulat m dan n sedemikian sehingga FPB(a, b) = $ma + nb$.

Contoh: Nyatakan FPB(312, 70) = 2 sebagai kombinasi lanjar dari 312 dan 70.

Penyelesaian:

Terapkan algoritma Euclidean untuk memperoleh FPB(312, 70) = 2:

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

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

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

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

Susun pembagian nomor (iii) menjadi

$2 = 32 - 5 \cdot 6$ (iv)

Susun pembagian nomor (ii) menjadi

$6 = 70 - 2 \cdot 32$ (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, FPB(312, 70) $= 2 = 11 \cdot 312 - 49 \cdot 70$

■

Relatif Prima

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

- **Contoh .**

  (i) 23 dan 2 relatif prima sebab FPB(23, 2) = 1.
  (ii) 7 dan 12 relatif prima karena FPB(7, 12) = 1.
  (iii) 30 dan 5 tidak relatif prima sebab

  FPB(30, 5) = 5 ≠ 1.

- Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga $ma + nb = 1$

- **Contoh.** Bilangan 23 dan 2 adalah relatif prima karena FPB(23, 2) =1, atau dapat ditulis

  $$1 \cdot 23 + (-11) \cdot 2 = 1 \quad (m = 1, n = -11)$$

  Tetapi 30 dan 5 tidak relatif prima karena FPB(20, 5) = $5 \neq 1$ sehingga 30 dan 5 tidak dapat dinyatakan dalam

  $m \cdot 20 + n \cdot 5 = 1$.

Kelipatan Persekutuan Terkecil (KPK)

- Misalkan *a* dan *b* bilangan bulat tidak nol.

- Kelipatan perekutuan terkecil (KPK – **least common multiples** atau *lcm*) dari *a* dan *b* adalah bilangan bulat terbesar *m* sedemikian hingga
  1. *a*| *m* dan *b* | *m*.
  2. Bila *a*| *n* dan *b* | n, *maka n* ñ *m*

- Dalam hal ini kita nyatakan bahwa KPK[*a*, *b*] = *m*.

Contoh :

KPK [5,4]= 20

KPK [7, 6] =42

KPK [15, 12] = 60.

Cara Menentukan KPK

1. Menemukan himpunan kelipatan persekutuan dan kemudian memilih yang terkecil

   contoh

   Kelipatan Persekutuan Terkecil dari: 10, 12, dan 18

   Kelipatan dari 10 : 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, **180**,190

   Kelipatan dari 12 : 12, 24, 36, 48, 60, 72, 84, 96, 108, 120, 132, 144, 156, 168, **180**, 192, 204

   Kelipatan dari 18 : 18, 36, 54, 72, 90, 108, 126, 144, 162, **180**, 198

   Jadi KPK (10,12,18) = 180

2. Teorema

$(p,q)]x\ [p,q] = p \times q$

contoh :

$[146,124] = (146 \times 124) \div (146, 124)$

$= 18104 \div 2$

$= 9052$

- KPK tiga atau lebih bilangan bulat positip dapat ditemukan dengan terlebih dahulu mencari KPK dari bilangan-bilangan itu; sepasang demi sepasang.
- Misalkan akan dicari KPK dari p, q, r, s,

  maka dicari dulu KPK bilangan p dan q misalkan terdapat m_1, kemudian dicari KPK bilangan r dan s misalkan terdapat m_2.
- Maka KPK (p,q,r,s) = KPK (m_1, m_2).
- Contoh :

  Carilah KPK dari 42, 96, 104. 18.

  Jawab:

  KPK (42. 96) = 672 dan KPK (104, 18) = 936

  KPK (42, 96, 104, 18) = KPK (672, 936) = 26208

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.

- 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) $\sqrt{171} = 13.077$. 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

(***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)

Aplikasi Teorema :

Menentukan FPB dan KPK dari dua bilangan

Dengan faktorisasi prima.

$24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$ $\qquad$ $36 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$

Faktor yang sama 2^3 dan 2^2, faktor berpangkat terkecilnya 2^2

Faktor yang sama 3 dan 3^2 , faktor berpangkat terkecilnya 3.

Jadi FPBnya = $2^2 \times 3 = 4 \times 3 = 12$

Faktorisasi prima dengan pangkat terbesar adalah 2^3 dan 3^2.

Jadi KPKnya = $2^3 \times 3^2 = 8 \times 9 = 72$.

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 $0 \leq r < m$.

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

- **Contoh.**
- Beberapa hasil operasi dengan operator modulo:
  i. $20 \bmod 5 = 0$ $(20 = 5 \cdot 4 + 0)$
  ii. $27 \bmod 4 = 3$ $(27 = 4 \cdot 6 + 3)$
  iii. $6 \bmod 8 = 6$ $(6 = 8 \cdot 0 + 6)$
  iv. $0 \bmod 5 = 0$ $(0 = \cdot 0 + 0)$
  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 $a \equiv b \pmod m$ 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 .**
  $17 \equiv 2 \pmod{3}$ ➔ $17 = 2 + 5 \cdot 3$
  $-7 \equiv 15 \pmod{11}$ ➔ $-7 = 15 + (-2)11$

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

  $a \equiv r \pmod{m}$

- **Contoh 11.**

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

  (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 bilagan 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,

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

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

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

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

- 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 $7 \not\equiv 4 \pmod 6$.

(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 $33 + 35k_2 \equiv 7 \pmod{11}$, 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 $77 \cdot 3 \equiv 1 \pmod 5$,

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

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

  maka solusi unik dari sistem kongruen tersebut adalah

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

  $\equiv 3813 \pmod{385}$

  $\equiv 348 \pmod{385}$

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

Contoh

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

Ambil $a = 2$ karena FPB(17, 2) = 1 dan FPB(21, 2) = 1.

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

karena 17 habis membagi 65536 – 1 = 65535

Jadi, 17 prima.

(ii) $2^{21-1} = 1048576 \equiv\ 1 \pmod{21}$

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.

Aplikasi Teori Bilangan

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

ISBN

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

- ISBN terdiri atas empat bagian kode:

- kode yang mengidentifikasikan bahasa,
- kode penerbit,
- kode unik untuk buku tersebut,
    - karakter uji (angka atau huruf X (=10)).

- Karakter uji dipilih sedemikian sehingga

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

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

- Contoh: ISBN 0–3015–4561–8

  0 : kode kelompok negara berbahasa Inggris,

  3015 : kode penerbit

  4561 : kode unik buku yang diterbitkan

  8 : karakter uji.

  Karakter uji ini didapatkan sebagai berikut:

  $$1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 +$$
  $$7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 = 151$$

- Jadi, karakter ujinya adalah 151 mod 11 = 8.

Catatlah bahwa untuk kode ISBN ini,

$$\sum_{i=i}^{10} ix_i = \sum_{i=i}^{9} ix_i + 10x_{10} = 151 + 10 \cdot 8 = 231$$

dan 231 mod 11 = 0 atau 231 ≡ 0 (mod 11).

Fungsi *Hash*

- Tujuan: menentukan alamat di memori

- Bentuk: $h(k) = k \bmod m$

  - m : jumlah lokasi memori yang tersedia
  - k : kunci (*integer*)
  - $h(k)$: lokasi memori untuk *record* dengan kunci k

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.

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

- Sumber :

  Sukirman, *Teori Bilangan*, Yogyakarta : FMIPA UNY