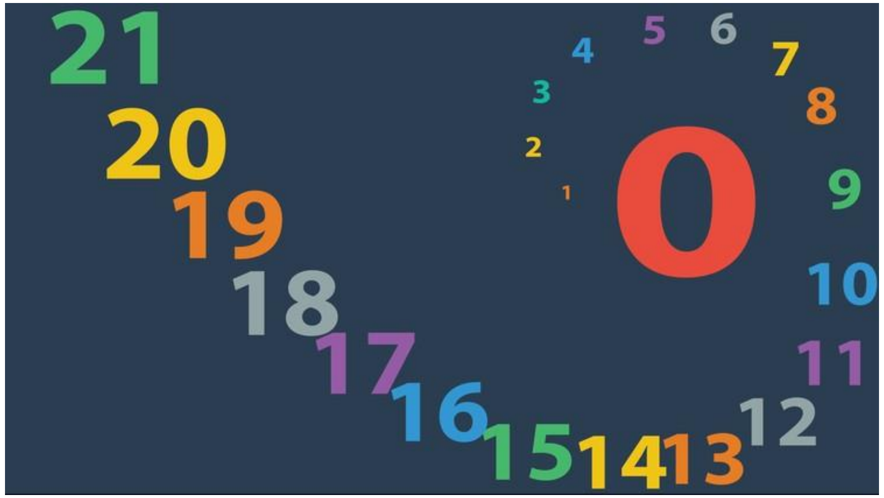
Teori Bilangan
(Bagian 2)



Bahan Kuliah IF2120 Matematika Diskrit

Oleh: Rinaldi Munir

Program Studi Teknik Informatika

STEI-ITB

Sistem Kekongruenan Linier

- Sistem kekongruenan linier terdiri dari lebih dari satu kekongruenan, yaitu:

$$x \equiv a_1 (\mathrm{mod}\ m_1)$$

$$x \equiv a_2 (\mathrm{mod}\ m_2)$$

$$\ldots$$

$$x \equiv a_n (\mathrm{mod}\ m_n)$$

Contoh: Sebuah bilangan bulat jika dibagi dengan 3 bersisa 2 dan jika ia dibagi dengan 5 bersisa 3. Berapakah bilangan bulat tersebut?

Penyelesaian:

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

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 kekongruenan 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 $k_1 = 2 + 5k_2$

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

Substitusikan $k_1 = 2 + 5k_2$ ke dalam persamaan (iii):

$$
\begin{aligned}
x &= 2 + 3k_1 \\
&= 2 + 3\,(2 + 5k_2) \\
&= 2 + 6 + 15k_2 \\
&= 8 + 15k_2
\end{aligned}
$$

atau

$x \equiv 8 \pmod{15}$ (periksa bahwa 8 mod 3 = 2 dan 8 mod 5 = 3)

Semua nilai x yang kongruen dengan 8 (mod 15) juga adalah solusinya, yaitu $x = 8$, $x = 23$, $x = 38$, …, $x = -7$, dst

Chinese Remainder Problem

- Pada abad pertama Masehi, 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 kekongruenan linier:

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

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

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

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 kekongruenan linier

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$\ldots$$
$$x \equiv a_n (\text{mod } m_n)$$

mempunyai sebuah solusi unik dalam modulus $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$. (yaitu, terdapat solusi x dengan $0 \leq x < m$ dan semua solusi lain yang kongruen dalam modulus m dengan solusi ini)

$x \equiv 3 \pmod 5$
$x \equiv 5 \pmod 7$
$x \equiv 7 \pmod{11}$

Contoh 15. Tentukan solusi dari pertanyaan Sun Tse tersebut

Penyelesaian:

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

Sulihkan (i) ke dalam kongruen kedua (yaitu $x \equiv 5 \pmod 7$) menjadi:

$3 + 5k_1 \equiv 5 \pmod 7 \rightarrow 5k_1 \equiv 2 \pmod 7 \rightarrow k_1 \equiv 6 \pmod 7$, 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 (yaitu $x \equiv 7 \pmod{11}$) menjadi:

$33 + 35k_2 \equiv 7 \pmod{11} \rightarrow 35k_2 \equiv -26 \pmod{11} \rightarrow k_2 \equiv 9 \pmod{11}$ 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. Periksa bahwa 348 mod 5 = 3, 348 mod 7 = 5, dan 348 mod 11 = 7.

Perhatikan juga bahwa $385 = 5 \cdot 7 \cdot 11$.

- Solusi unik ini, yaitu $x \equiv 348 \pmod{385}$, modulus 385 merupakan

$$m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 385$$

- Secara umum, solusi sistem kekongruenan linier adalah berbentuk

$$x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n$$

yang dalam hal ini

M_k adalah perkalian semua modulus kecuali m_k.

y_k adalah balikan M_k dalam modulus m_k

- Tinjau kembali persoalan *Chinese remainder problem*:

$x \equiv 3 \pmod 5$
$x \equiv 5 \pmod 7$
$x \equiv 7 \pmod{11}$

- Hitung: $m = 5 \cdot 7 \cdot 11 = 385$

$M_1 = 7 \cdot 11 = 77, \quad M_2 = 5 \cdot 11 = 55, M_3 = 5 \cdot 7 = 35$

$y_1 = 3$ karena $77 \cdot 3 \equiv 1 \pmod 5$

$y_2 = 6$ karena $55 \cdot 6 \equiv 1 \pmod 7$

$y_3 = 6$ karena $35 \cdot 6 \equiv 1 \pmod{11}$

maka solusi unik dari sistem kekongruenan tersebut adalah

$$
\begin{aligned}
x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\
&= 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \\
&= 3813 \\
&\equiv 348 \pmod{385}
\end{aligned}
$$

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 apakah n bilangan prima atau komposit:

  (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.

<u>Penyelesaian</u>*:*

(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 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:

Fermat dibaca *Fairma*

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

- Menurut teorema Fermat di atas, jika p adalah bilangan prima, maka $a^{p-1} \equiv 1 \pmod{p}$

- Tetapi, jika p bukan bilangan prima, maka $a^{p-1} \not\equiv 1 \pmod{p}$

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

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 · 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.

Contoh 19: Hitunglah sisa pembagian 2^{2020} dibagi dengan 73

Penyelesaian: Dengan menggunakan teorema Fermat kita dapat mengetahui bahwa $2^{73-1} = 2^{72} \equiv 1 \pmod{73}$.

$$
\begin{aligned}
2^{2020} &\equiv (2^{72 \cdot 28 + 4}) \pmod{73} \\
&\equiv (2^{72})^{28} \,.\, 2^4 \pmod{73} \\
&\equiv (1)^{28} \,.\, 2^4 \pmod{73} \\
&\equiv 2^4 \pmod{73} \\
&\equiv 16 \pmod{73} = 16
\end{aligned}
$$

Jadi sisa pembagiannya adalah 16

Contoh 20: Tiga kemunculan terakhir komet Halley adalah pada tahun 1835, 1910, dan 1986. Kemunculan berikutnya diprediksi akan terjadi pada tahun 2061. Dengan bantuan Teorema Fermat buktikan bahwa

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7)$$

Jawaban: Karena PBB(7, 1835) = 1 dan PBB(7, 1986) = 1, maka memenuhi syarat Teorema Fermat.

Selanjutnya, berdasarkan Teorema Fermat, $a^{p-1} \equiv 1 \pmod p$

$1835^{7-1} = 1835^6 \equiv 1 \pmod 7$

$1835^{1910} \pmod 7 \equiv 1835^{6 \cdot 318 + 2} \equiv (1835^6)^{318} \cdot 1835^2 \pmod 7 \equiv (1)^{318} \cdot 1835^2 \pmod 7$
$\equiv 1835^2 \pmod 7 \equiv 1^2 \pmod 7 \equiv 1 \pmod 7$

$1986^{7-1} = 1986^6 \equiv 1 \pmod 7$

$1986^{2061} \pmod 7 \equiv 1986^{6 \cdot 343 + 3} \equiv (1986^6)^{343} \cdot 1986^3 \pmod 7 \equiv (1)^{343} \cdot 1986^3 \pmod 7$
$\equiv 1986^3 \pmod 7 \equiv 5^3 \pmod 7 \equiv 125 \pmod 7 \equiv 6 \pmod 7$

Jadi,

$1835^{1910} + 1986^{2061} \pmod 7 \equiv 1 \pmod 7 + 6 \pmod 7 \equiv 0 \pmod 7$

Latihan soal (diambil dari soal kuis dan UAS)

1. Hartono memiliki banyak permen. Dia akan membagi permen kepada teman-temannya. Jika dia membagi kepada 7 orang temannya secara merata, maka akan tersisa 5permen. Jika dia membagi seluruhnya secara merata kepada 8 teman, tersisa 3. Jika ia membagi seluruhnya secara merata kepada 9 orang, akan tersisa 7 permen. Berapa paling sedikit jumlah permen yang dimiliki Hartono?

2. Hitunglah nilai dari 5^{2017} mod 7 dan 5^{2017} mod 11 dengan menggunakan Teorema Fermat.

3. (a) Gunakan Teorema Fermat untuk menghitung 3^{302} mod 5, 3^{302} mod 7, dan 3^{302} mod 11

   (b) Gunakan hasil dari (a) dan *Chinese Remainder Theorem* untuk menghitung nilai 3^{302} mod 385 (Petunjuk: $385 = 5 \cdot 7 \cdot 11$