Kongruensi Linear

Kongruensi Linear

- Definisi

Misalkan ***m*** bilangan bulat positif, ***a*** dan ***b*** bilangan bulat, dan ***x*** sebuah variabel, kongruensi linear adalah kongruensi yang berbentuk $ax \equiv b \pmod{m}$

- Tujuan: mencari solusi nilai ***x*** yang memenuhi kongruensi linear tersebut
- Kongruensi linear belum tentu memiliki solusi
  - Jika $\gcd(a, m) \nmid b$, maka kongruensi linear tidak memiliki solusi.
  - Jika $\gcd(a, m) \mid b$, maka kongruensi linear memiliki tak hingga solusi pada satu atau lebih kelas kongruensinya.
  - Jika $\gcd(a, m) = 1$, maka kongruensi linear memiliki solusi pada satu kelas kongruensi tertentu. Solusinya dapat dicari menggunakan invers modulo.

Invers Modulo

- Definisi

> Suatu bilangan bulat $\bar{a}$ adalah invers modulo dari a modulo m jika berlaku $\bar{a}.a \equiv 1 \pmod{m}$

- Catatan
  - Invers dari suatu bilangan bulat modulo m belum tentu ada

Invers Modulo

- Teorema IM1

> Jika ***a*** dan ***m*** bilangan-bilangan bulat yang relatif prima, dan ***m* > 1**, maka invers dari ***a*** modulo ***m*** dijamin ada.
>
> Invers dari ***a*** modulo ***m*** bersifat unik dalam modulo m. Artinya, dalam range 0 sampai ***m*** – 1 terdapat bilangan unik ***ā*** yang merupakan invers dari ***a*** modulo ***m.*** Semua bilangan yang kongruen dengan ***ā*** juga merupakan invers dari ***a*** modulo ***m***.

- Jika $\gcd(a, m) = 1$, invers dari ***a*** modulo ***m*** dapat dihitung dengan Bezout's Theorem

Mencari Invers Modulo

Carilah (jika ada) invers dari 3 modulo 7

- Perhatikan bahwa gcd(3, 7) = 1, maka invers modulonya dijamin ada
- Invers dari 3 mod 7 adalah suatu bilangan ($\bar{a}$) yang jika dikalikan dengan 3 maka mod 7 nya adalah 1: $3\,\bar{a} \equiv 1 \pmod 7$
- Terdapat setidaknya 2 cara untuk mencari $\bar{a}$:
  - Dengan algoritma pembagian, kita memperoleh:

$$3\,\bar{a} = 7\,q + 1$$
$$3 \,.\, (-2) = 7 \,.\, (-1) + 1$$

  - Dengan algoritma Euclidean, kita memperoleh: $7 = 3 \,.\, 2 + 1$

    $3 \,.\, (-2) + 7 \,.\, (1) = 1$ (ini adalah kombinasi linear dari gcd (3,7))

- Ini berarti bahwa 3 jika dikalikan dengan (-2) maka mod 7 nya adalah 1.

- Jadi, -2 adalah invers dari 3 modulo 7

  $3\ \bar{a} \equiv 1 \pmod 7$

  $3 \cdot (-2) \equiv 1 \pmod 7$

- Perhatikan bahwa semua bilangan yang kongruen dengan -2 modulo 7 juga merupakan invers dari 3 modulo 7
  - Contoh: …, -9, -2, 5, 12, … dst.

Invers Modulo

- Teorema IM2 (Konvers dari Teorema IM1)

> Jika ***m* > 1** dan ***a*** memiliki invers modulo ***m,*** maka ***a*** dan ***m*** relatif prima.

Bukti (lanjutan)

- Bukti

  Misal $\bar{a}$ adalah invers dari a modulo m, yaitu $a\bar{a} \equiv 1 \pmod{m}$, akan ditunjukkan bahwa gcd $(a,m) = 1$.

- $a\bar{a} \equiv 1 \pmod{m}$, maka $a\bar{a} = 1 + km$. Persamaan tersebut dapat diubah menjadi:

  $$a\bar{a} - km = 1.$$

- Perhatikan bahwa:
  - gcd $(a,m) \mid a$, sehingga gcd $(a,m) \mid a\bar{a}$
  - gcd $(a,m) \mid m$, sehingga gcd $(a,m) \mid -km$
- Sehingga, gcd $(a,m) \mid a\bar{a} - km$
- Maka, gcd $(a,m) \mid 1$.
- Karena gcd tidak negatif, maka gcd $(a,m) = 1$.

Invers Modulo

- Dari Teorema IM1 dan IM2, kita mendapatkan Teorema IM3 berikut.

> Untuk ***a*** sembarang bilangan bulat dan ***m* > 1,**
> ***a*** memiliki invers modulo ***m*** jika dan hanya jika ***a*** dan ***m*** relatif prima.

Mencari Invers Modulo

- Carilah (jika ada) invers dari 4 modulo 8
  - Jawaban versi 1:

  Invers dari 4 modulo 8 (jika ada) pastilah suatu bilangan *y* sehingga $4y \equiv 1 \pmod 8$

  Namun demikian jelas tidak ada *y* yang memenuhi karena:

    - apabila *y* genap maka $4y \equiv 0 \pmod 8$
    - apabila *y* ganjil maka $4y \equiv 4 \pmod 8$

  •Jawaban versi 2 (dengan teorema IM3):

  Tidak ada invers-nya, karena gcd (4,8) ≠ 1.

Menyelesaikan Kongruensi Linear dengan Invers Modulo

- Misal pada kongruensi linear $ax \equiv b \ (mod\ m)$, diketahui $\gcd(a, m) = 1$
  - Karena $\gcd(a, m) = 1$, maka invers a modulo m ada, yang diperoleh dengan Bezout's Theorem; anggap inversnya adalah $\bar{a}$.
  - Karena $\bar{a}$ merupakan invers dari a modulo m, maka $a\bar{a} \equiv 1 (\mathrm{mod}\ m)$
  - Dengan demikian $a\bar{a}x \equiv \bar{a}b \ \ (\mathrm{mod}\ m)$ mengimplikasikan bahwa solusi

$$x \equiv \bar{a}b \ \ (\mathrm{mod}\ m)$$

Menyelesaikan Kongruensi Linear

- Carilah solusi dari kongruensi linear:

  $3x \equiv 4 \pmod 7$

  - Langkah 1: Temukan invers dari 3 mod 7,
    - $a\bar{a} \equiv 1 \pmod m$
    - $3\bar{a} \equiv 1 \pmod 7$
    - Dari contoh sebelumnya, $\bar{a}$ = -2
  - Langkah 2: Kalikan kedua ruas kongruensi linear di atas dengan nilai $\bar{a}$ sehingga diperoleh,
    - $a\bar{a}\ x \equiv \bar{a}\ b \pmod m$, $x \equiv \bar{a}\ b \pmod m$ adalah solusi yang dicari.
    - $3.(-2)\ x \equiv (-2).4 \pmod 7$
    - $x \equiv -8 \pmod 7$

Menyelesaikan Kongruensi Linear

- Carilah solusi dari kongruensi linear:

  $3x \equiv 4 \pmod 7$

  - Langkah 3: Setiap bilangan bulat $\boldsymbol{x = \bar{a}\, b + mk}$ dimana $\boldsymbol{k}$ bilangan bulat adalah solusi dari kongruensi linear tersebut
    - Diketahui $\bar{a}b = (-2) \,.\, 4 = -8$
    - Jadi, solusi yang dicari adalah:
      - $x = -8 + 7k$
    - Solusi unik dimana $0 \le x < 7$ adalah $x = -8 \bmod 7 = 6$
      - Jadi, $x \equiv 6 \pmod 7$
    - Bilangan-bilangan yang merupakan solusi antara lain:
      - …, -15, -8, -1, 6, 13, 20, … dst.

Apakah $ax \equiv b \pmod{m}$ *selalu* memiliki solusi?

Untuk kongruensi linear $ax \equiv b \pmod{m}$:

- Jika a memiliki invers modulo m, maka solusi x pasti ada.
- Jika a tidak memiliki invers modulo m karena gcd $(a,m) \neq 1$, maka belum dapat dipastikan ada/tidaknya solusi untuk x.

Apakah $ax \equiv b \pmod{m}$ *selalu* memiliki solusi?

Jika *a* tidak memiliki invers modulo *m* karena gcd (*a*,*m*)≠ 1, maka ada dua kemungkinan:

- ada solusi *x* nya, contoh:

  2x ≡ 4 (mod 8)

  Nilai x yang memenuhi adalah:

  x ≡ 2 (mod 4), kedua ruas dibagi 2 termasuk modulonya.

  Atau jika ingin solusinya dalam modulo 8, maka solusinya adalah nilai x yang memenuhi salah satu dari kongruensi berikut:

  x ≡ 2 (mod 8), x ≡ 6 (mod 8)

- tidak ada solusi x nya, contoh:

  4x ≡ 5 (mod 6)

  Berapa pun nilai x, maka 4x pasti genap. Maka, 4x-5 pasti ganjil. 6 tidak mungkin habis membagi bilangan ganjil. Maka kongruensi tersebut tidak terpenuhi.

Chinese Remainder Theorem

Chinese remainder theorem:
Motivasi

Sebuah bilangan *n* jika dibagi 3 akan bersisa 2; jika dibagi 5, sisanya 3; dan jika dibagi 7, sisanya 2. Berapakah *n*?

Pertanyaan di atas ekivalen dengan mencari solusi dari sistem kongruensi berikut:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Chinese Remainder Theorem

Teorema CRT

Misalkan $m_1, \ldots, m_n$, bilangan bulat positif yang relatif prima sepasang-sepasang serta nilainya lebih dari satu. Lalu, $a_1, \ldots, a_n$ sembarang bilangan bulat. Maka, sistem kongruensi:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \ldots x &\equiv a_n \pmod{m_n} \end{aligned}$$

memiliki solusi unik modulo $m = m_1 m_2 \ldots m_n$.

Solusi unik yang dimaksud berbentuk $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$ yang mana $M_k = m/m_k$ untuk setiap $k = 1, \ldots, n$, serta y_k adalah invers dari M_k modulo m_k.

Chinese Remainder Theorem

Langkah 1

Hitung m di mana $m = m_1 m_2 \ldots m_n$

Hitung $M_k = m \,/\, m_k$ di mana $k = 1,2,\ldots,n$

Langkah 2

Cari y_k yang merupakan invers dari M_k modulo m_k di mana $k = 1,2,\ldots,n$

Langkah 3

Bangun solusi dalam bentuk

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n \pmod{m}$$

Chinese Remainder Theorem

Kembali ke pertanyaan sebelumnya untuk mencari solusi dari sistem kongruensi berikut:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Chinese Remainder Theorem

Langkah 1:

Hitung m di mana $m = m_1 m_2 \ldots m_n = 3 \cdot 5 \cdot 7 = 105$

Hitung $M_k = m / m_k$

$M_1 = m / m_1 = 105 / 3 = 35$

$M_2 = m / m_2 = 105 / 5 = 21$

$M_3 = m / m_3 = 105 / 7 = 15$

Chinese Remainder Theorem

Langkah 2:

Cari y_k yang merupakan invers dari M_k modulo m_k.

y_1 = inverse dari 35 modulo 3 = 2

y_2 = inverse dari 21 modulo 5 = 1

y_3 = inverse dari 15 modulo 7 = 1

Chinese Remainder Theorem

Langkah 3:

Maka solusinya adalah

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n \pmod{m}$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{m}$$
$$= 233 \equiv 23 \pmod{105}$$

Dengan demikian, n=23 adalah bilangan bulat positif di mana jika dibagi 3 akan bersisa 2; jika dibagi 5, sisanya 3; dan jika dibagi 7, sisanya 2.

Solusi dari dari n adalah semua bilangan bulat yang kongruen dengan 23 modulo 105.

Chinese Remainder Theorem

Collorary

Misalkan $m_1, \ldots, m_n$, bilangan bulat positif yang relatif prima sepasang-sepasang serta nilainya lebih dari satu, lalu, $a_1, \ldots, a_n$ sembarang bilangan bulat, maka sistem kongruensi:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots x \equiv a_n \pmod{m_n}$$

memiliki solusi unik modulo $m = m_1 m_2 \ldots m_n$. Ada x dengan $0 \leq x < m$ dan semua solusinya kongruen dengan x modulo m.

Aplikasi dari Chinese Remainder Theorem

Parallel computation

CRT digunakan dalam teknik untuk menggabungkan kembali hasil komputasi yang didistribusikan di beberapa prosesor.

Cryptography

CRT digunakan untuk mendukung proses komputasi dalam kriptografi yang melibatkan bilangan bulat besar.

Back Substitution

Back Substitution

Sistem kongruensi linier pada topik sebelumnya dapat diselesaikan dengan Chinese Remainder Theorem, karena modulonya adalah 3,5,7 yang merupakan pasangan relatif prima.

Sedangkan untuk Back Substitution tidak diperlukan kondisi modulo yang merupakan pasangan relatif prima.

Menyelesaikan sistem kongruensi linier menggunakan metode *Back Substitution*

Gunakan Back Substitution untuk mencari solusi x yang memenuhi sistem kongruensi linier berikut:

$$x \equiv 1 (mod\ 5)$$
$$x \equiv 2 (mod\ 6)$$
$$x \equiv 3 (mod\ 7)$$

Menyelesaikan sistem kongruensi linier menggunakan metode *Back Substitution* : $x \equiv 1(mod\ 5), x \equiv 2(mod\ 6), x \equiv 3(mod\ 7)$

$x \equiv 1(mod\ 5)$ sehingga $x = 1 + 5t$.

Substitusi $x = 1 + 5t$ ke $x \equiv 2(mod\ 6)$, menjadi:

$$1 + 5t \equiv 2(mod\ 6)$$
$$5t \equiv 1(mod\ 6)$$
$$5t \equiv -5(mod\ 6)$$
$$t \equiv -1(mod\ 6)$$
$$t \equiv 5(mod\ 6)$$

Sehingga $t = 5 + 6u$. **Substitusi balik** ke persamaan di atas, menjadi

$$x = 1 + 5(5 + 6u) = 26 + 30u$$

Menyelesaikan sistem kongruensi linier menggunakan metode *Back Substitution* : $x \equiv 1(mod\ 5), x \equiv 2(mod\ 6), x \equiv 3(mod\ 7)$

Substitusi $x = 26 + 30u$ ke $x \equiv 3(mod\ 7)$, menjadi:

$$26 + 30u \equiv 3(mod\ 7)$$
$$30u \equiv -23(mod\ 7)$$
$$30u \equiv -30(mod\ 7)$$
$$u \equiv -1(mod\ 7)$$
$$u \equiv 6(mod\ 7)$$

Sehingga $u = 6 + 7v$. **Substitusi balik** ke persamaan di atas, menjadi

$$x = 26 + 30(6 + 7v) = 206 + 210u$$

Solusi: $x \equiv 206(mod\ 210)$

Fermat’s Little Theorem

Fermat's Little Theorem

Teorema FLT

Jika p bilangan prima dan a bilangan bulat yang tak habis dibagi p, maka $a^{p-1} \equiv 1 \pmod{p}$. Lalu tidak hanya itu, untuk setiap bilangan bulat a berlaku bahwa $a^p \equiv a \pmod{p}$.

Jika kongruensi modulonya pada bilangan prima p, maka menghitung pemangkatan modular dapat memanfaatkan teorema di atas.

Hitung 7^{222} **mod** 11.

Fermat's Little Theorem

Aplikasi

FLT digunakan dalam uji primalitas probabilistik : tes untuk memeriksa apakah suatu bilangan prima atau tidak secara probabilistik.

Teknik FLT ini lebih cepat atau lebih efisien dibandingkan dengan teori dasar yang telah dipelajari sebelumnya.

Bilangan Prima Semu

- Menurut Teorema FLT, jika n prima ganjil, maka $2^{n-1} \equiv 1 \pmod{n}$.
- Namun, **belum tentu** bahwa apabila $2^{n-1} \equiv 1 \pmod{n}$ maka n pasti prima ganjil.

Definisi BPS (Bilangan Prima Semu)

Bilangan prima semu terhadap basis b untuk suatu $b \in Z^+$ adalah bilangan komposit n yang memenuhi $b^{n-1} \equiv 1 \pmod{n}$.

Contoh: 341 adalah pseudoprima terhadap basis 2. (Jelaskan!)

Bilangan Carmichael

Definisi BC (Bilangan Carmichael)

Bilangan komposit $n > 1$ disebut **bilangan Carmichael** jika n memenuhi kongruensi $b^{n-1} \equiv 1 \pmod{n}$ untuk setiap b dengan $\gcd(b, n) = 1$.

Bilangan Carmichael adalah bilangan yang prima semu terhadap semua basis yang relatif prima dengannya. Definisi ini berguna sebagai dasar algoritma probabilistik penentu prima yang efisien.

Contoh: 561 adalah bilangan Carmichael. (Jelaskan!)

Akar Primitif Modulo

(Ingat definisi Z_m untuk suatu bilangan bulat m?)

Definisi APM

Andaikan p prima. Bilangan $r \in Z_p$ disebut *akar primitif* modulo p jika setiap $a \in Z_p$, $a \neq 0$, adalah suatu hasil pangkat dari n. D.k.l. $n^a \in Z_p$ untuk setiap $a \in Z_p$, $a \neq 0$.

Contoh: 2 dan 3 adalah akar primitif modulo 11. (Jelaskan!)

Teorema APM

Setiap bilangan prima p memiliki akar primitif modulo p.

Logaritma Diskrit

Definisi LD

Andaikan p prima dan r akar primitif modulo p, serta a bilangan bulat sehingga $1 \leq a \leq p-1$. Maka, bilangan e, $0 \leq e \leq p-1$, disebut *logaritma diskrit* dari a modulo p pada basis r apabila $r^e \bmod p = a$.

Berapa logaritma diskrit dari 3 dan 5 modulo 11 pada basis 2?

Selamat belajar...