Teori Bilangan (Aritmatika Modulo)

Prerequisites

- Teori Bilangan (FPB, KPK, Algoritma Euclid)

Outline

- Pengantar
- Aritmatika Modulo
- Modulo Kongruen
- Algoritma Pemangkatan
- Modulo Inverse

Pengantar

- Banyak bilangan bulat adalah tak hingga.
- Pada suatu kasus, kita hanya peduli hasil bagi suatu bilangan bulat (*modulo*) dengan bilangan bulat.
- Modulo akan membatasi ketidakhinggaan bilangan bulat.
- Contoh :
  - Pada jam dengan sistem 24 jam, jam ke-24 dianggap sama dengan jam ke-0 (*modulo* 24)
  - Pada penanggalan masehi, banyak bulan adalah 12. Bulan ke-13 dianggap sama dengan bulan ke-1 (modulo 12)
  - Pada kriptografi dan ISBN

Aritmatika 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 $\mathbf{0 \leq r < m}$.

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

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 unuk (v) :

-41 mod 9 = -5. karena kita ingin hasil modulo harus positif maka tambahkan 9 ke hasil modulo sehingga didapat -5 + 9 = 4

Kongruen Modulo

- Sebuah **bilangan bulat positif** *a* dan *b* merupakan ***kongruen modulo*** dari bilangan bulat positif *m* jika *(a-b)* dibagi *m* tidak memiliki sisa. (*m* habis membagi *a-b*)
- Atau *a* dan *b* memiliki sisa bagi yang sama ketika dibagi *m.*
- Notasi : a ≡ b (mod m) *baca : a* kongruen *b* modulo *m*
- Negasinya adalah a ≡/ b (mod m) *baca : a* tidak kongruen *b* modulo *m*

Contoh kongruen

- $14 \equiv 2 \pmod 3$
  - karena 3 habis membagi (14-2 = 12)
- $100 \equiv 30 \pmod{10}$
  - karena 10 habis membagi (100-30 = 70)
- $12 \not\equiv 5 \pmod 4$
  - karena 4 tidak habis membagi (12-5 = 7)
- $5 \not\equiv 4 \pmod 3$
  - karena 3 tidak habis membagi (5-4 = 1)

a mod $m = r$ dapat ditulis $a \equiv r$ (mod m)

Contoh :

i. 23 mod 4 = 3 -> $23 \equiv 3$ (mod 4)
ii. 27 mod 3 = 0 -> $27 \equiv 0$ (mod 3)
iii. 40 mod 13 = 1 -> $40 \equiv 1$ (mod 13)
iv. 0 mod 15 = 0 -> $0 \equiv 0$ (mod 15)
v. 6 mod 7 = 6 -> $6 \equiv 6$ (mod 7)

Ini hanya masalah mengubah notasi saja.

Sifat Kongruen Modulo

Jika $a \equiv b \pmod{m}$ dan c adalah sembarang bilangan bulat maka

- $(a + c) \equiv (b + c) \pmod{m}$
- $ac \equiv bc \pmod{m}$
- $a^p \equiv b^p \pmod{m}$, p bilangan bulat tak-negatif

Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

- $(a + c) \equiv (b + d) \pmod{m}$
- $ac \equiv bd \pmod{m}$

Sifat Modulo

- Berdasarkan sifat tersebut, kita dapat menentukan bahwa

1. $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
2. $(a – b) \bmod m = ((a \bmod m) – (b \bmod m)) \bmod m$
3. $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$
4. $a^p \bmod m = ((a^x \bmod m)(a^y \bmod m)) \bmod m$, dengan $x,y \geq 0$ dan $x+y = p$.

Contoh : hitunglah (100124) mod 25.

100124 mod 25 = (100000 + 124) mod 25

= ((100000 mod 25) + (124 mod 25)) mod 25

= (0 + (124 mod 25)) mod 25

= (125 – 1) mod 25

= ((125 mod 25) + (-1 mod 25)) mod 25)

= -1 mod 25 (karena negatif, +25 ke hasil)

= 24

Contoh : Hitunglah 5! mod 13

$5! \bmod 13 = 5 \times 4 \times 3! \bmod 13$

$= (20 \bmod 13)(6 \bmod 13) \bmod 13$

$= (7 \times 6) \bmod 13$

$= 42 \bmod 13$

$= 3$

Contoh : carilah 2 angka terakhir dari 2^{20} .

Jawab : 2 angka terakhir artinya sama dengan mencari 2^{20} mod 100.

2^{20} mod 100 = 2^{10} x 2^{10} mod 100

2^{10} mod 100 = 2^{5} x 2^{5} mod 100

Karena 2^{5} mod 100 = 32 mod 100, maka

2^{10} mod 100 = 32 x 32 mod 100

= 1024 mod 100

= (1000 + 24) mod 100

= 24

Karena 2^{10} mod 100 = 24 maka

2^{20} mod 100 = 24 x 24 mod 100

= 576 mod 100 = (500 + 76) mod 100 = 76

Algoritma Pemangkatan

$$f(a,p) = a * a * a * a * \cdots * a$$

- Menghitung f(2,8) dengan cara biasa

  $f(2,8) = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2$ 7 operasi perkalian

- Cara lain :

$$f(2,8) = f(2,4) * f(2,4)$$
$$f(2,4) = f(2,2) * f(2,2)$$
$$f(2,2) = f(2,1) * f(2,1)$$
$$f(2,1) = f(2,0) * 2$$
$$f(2,0) = 1$$

- Total ada 4 operasi !
- Kita akan menghitung $f(a,p)$ mod m jika *p* sangat besar

Algoritma Pemangkatan

- Berdasarkan sifat $a^p \bmod m = ((a^x \bmod m)(a^y \bmod m)) \bmod m$, kita dapat menghitung $a^p \bmod m$ dengan p yang sangat besar, misalnya p = 1.000.000 tanpa harus mengalikan a sebanyak 1.000.000 kali.
- Ide yang digunakan adalah :
  - Jika p = 0, maka $a^0 \bmod m = 1 \bmod m$.
  - Jika p ganjil, maka hitung $a^p \bmod m = (a \bmod m)(a^{p-1} \bmod m) \bmod m$
  - Jika p genap, maka hitung $a^{p/2} \bmod m$, misal hasilnya t.
    - Dengan rumus $a^p \bmod m = (a^{p/2} \bmod m)(a^{p/2} \bmod m) \bmod m$ maka $a^p \bmod m = t \times t \bmod m$
- Algoritma tersebut lebih cepat karena pada p genap, dia membagi dua nilai p dan hanya menghitung $(a^{p/2} \bmod m)$ sekali saja. Dan sifat tersebut berlaku rekursif!

Algoritma Pemangkatan

$$f(a,n) = \begin{cases} 1, & \text{jika}(n = 0) \\ \left(f\left(a, \frac{n}{2}\right)\right)^2, & \text{jika}(n \; mod \; 2 = 0) \\ a * f(a, n-1), & \text{jika}(n \; mod \; 2 = 1) \end{cases}$$

```
function pangkat(a,n : integer);
var
   tmp : integer;
begin
  if (n = 0) then pangkat := 1
  else
      if (n mod 2 = 1) then pangkat := a * pangkat(a,n-1);
      else
      begin
         tmp := pangkat(a,n div 2);
         pangkat := tmp * tmp;
         end;
end;
```

Question : kenapa pake tmp? Gak langsung pangkat(a,n div 2) * pangkat(a,n div 2)

Modulo Inverse

- Inverse : balikan.
- Dalam aritmatika biasa : inverse dari perkalian adalah pembagian
- Contoh : invers dari 5 adalah 1/5 karena 5 x 1/5 = 1

Invers dapat digunakan untuk menyelesaikan persamaan aritmatika biasa

Contoh : carilah solusi 4a = 36

Solusi dari persamaan tersebut adalah dengan mencari invers dari 4, yaitu ¼, sehingga

4a(¼) = 36 (¼)

a = 9

Invers dapat digunakan untuk menyelesaikan persamaan modulo

Contoh : carilah solusi $4a \equiv 5 \pmod 9$

Solusi dari persamaan tersebut dapat dicari dengan mengubah bentuk persamaan menjadi

$a \equiv$ *suatu_bilangan* (mod 9)

artinya, kita akan mencari invers dari *4 (mod 9)* dan mengalikannya ke kedua ruas $4a \equiv 5 \pmod 9$.

Apakah invers dari *4 (mod 9)* itu?

- Bentuk persamaan $4a \equiv 5 \pmod 9$ tersebut dapat kita ubah menjadi $px \equiv q \pmod m$
- Kalikan kedua ruas dengan suatu bilangan r

  $prx \equiv qr \pmod m$
- Ingat rumus : Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$, maka $ac \equiv bd \pmod m$
- Kita dapat mencari solusi x dari $prx \equiv qr \pmod m$ dengan membuat :

  $a \equiv b \pmod m$ menjadi $pr \equiv 1 \pmod m$

  $c \equiv d \pmod m$ menjadi $x \equiv qr \pmod m$
- Nah, berarti r ini harus sesuatu yang membuat $pr \equiv 1 \pmod m$
- r ini disebut invers dari p (mod m) atau $r = p^{-1} \pmod m$
- Dalam soal ini, artinya kita mencari $4r \equiv 1 \pmod 9$
- r ini disebut ***invers dari 4 (mod 9)***

- Suatu bilangan *r* disebut *invers modulo* dari *p* jika $pr \equiv 1 \pmod{m}$
- Pada soal tadi, artinya kita mencari $4r \equiv 1 \pmod{9}$
- Cara mencarinya bisa dengan coba-coba :
  - r = 1 -> $4(1) \not\equiv 1 \pmod{9}$
  - r = 2 -> $4(2) \not\equiv 1 \pmod{9}$
  - r = 3 -> $4(3) \not\equiv 1 \pmod{9}$
  - …
  - r = 7 -> $4(7) \equiv 1 \pmod{9}$

  Inverse dari 4 (mod 9) adalah 7

Kita kembali lagi ke soal : $4a \equiv 5 \pmod 9$

Kalikan kedua ruas dengan invers dari 4, yaitu 7, sehingga

$$4(7)\, a \equiv 35 \pmod 9$$

Karena $28 \equiv 1 \pmod 9$, maka hal tersebut sama dengan

$$(1)\, a \equiv 35 \pmod 9$$

$$a \equiv 8 \pmod 9$$

Artinya solusi dari $4a \equiv 5 \pmod 9$ adalah ***seluruh nilai a*** sehingga $a \equiv 8 \pmod 9$

Dengan mendaftar, a= … , -10, -1, 8, 17, 26, …

Atau dengan menggunakan sifat $a \bmod m = r$ sama dengan $a = mq + r$, maka $a = 9q + 8$ (suatu bilangan kelipatan 9 lalu ditambah 8)

- Mencari inverse 4 (mod 9) dengan mendaftar seluruh kemungkinan $4r \equiv 1 \pmod 9$ tentu membuat lelah.
- Ingat : $a \bmod m = r$ atau $a \equiv r \pmod m$ sama dengan $a = mn + r$
- Kita bisa menggunakan cara dengan mengembalikan arti modulo ke dalam bentuk aljabar, yaitu $4r = 9q + 1$
- Dengan aljabar, $r = (9q + 1)/4$
- Cara ini membuat perhitungan lebih mudah, dengan cara mencari $(9q + 1)/4$ yang bulat. namun ujung-ujungnya juga mendaftar lagi.

Inverse Modulo dengan Algoritma Euclid

- Ingat kembali definisi kongruensi modulo
- $4r \equiv 1 \pmod 9$ dapat diubah dengan mengubah bentuk tersebut menjadi $4r = 9q + 1$

$$4r - 9q = 1$$

- Perhatikan bahwa penyelesaian persamaan tersebut dapat diselesaikan dengan mencari kombinasi linear dari $4r - 9q = 1$.
- Kombinasi linear dapat dicari dengan menggunakan algoritma euclid!

Algoritma Euclid

- Mencari FPB dari dua buah bilangan

Misalkan m dan n adalah bilangan bulat tak negatif dengan $m \geq n$.

Misalkan $r_0 = m$ dan $r_1 = n$.

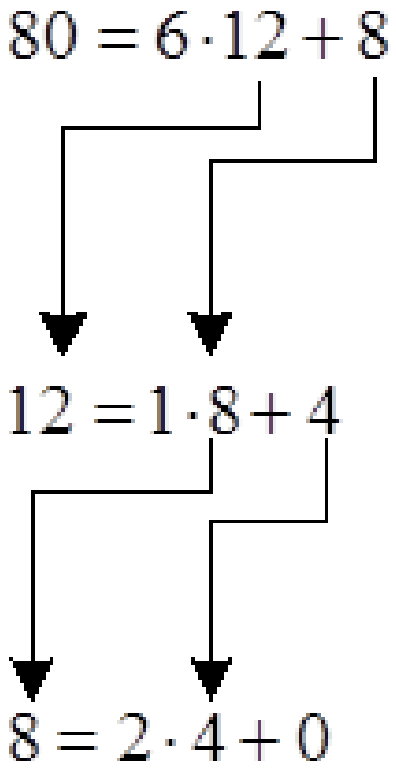
Lakukan secara berturut-turut pembagian untuk memperoleh

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 \leq r_1,$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 \leq r_2,$$
$$\ldots$$
$$r_{n-2} = r_{n-1}\, q_{n-1} + r_n \quad 0 \leq r_n \leq r_{n-1},$$
$$r_{n-1} = r_n q_n + 0$$

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

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

$m = 80$, $n = 12$ dan dipenuhi syarat $m \geq n$



Sisa pembagian terakhir sebelum 0 adalah 4, maka fpb(80, 12) = 4.

m = 312, n = 70

$$312 = 4 \times 70 + 32$$
$$70 = 2 \times 32 + 6$$
$$32 = 5 \times 6 + 2$$
$$6 = 3 \times 2 + 0$$

Hasil sisa sebelum nol adalah 2, maka FPB(312,70) = 2.

Kombinasi Linear (Extended Euclid)

- FPB dari 2 buah bilangan dapat ditulis dari penjumlahan dari 2 buah bilangan tersebut, Contoh : FBB(80,12) = 4 = -1 x 80 + 7 x 12.
- Jika m dan n adalah bilangan bulat positif maka terdapat bilangan bulat p dan q sehingga *pm + qn = FPB(m,n).*

Kombinasi Linear (ext. euclid)

- **Contoh 7**: Nyatakan fpb(21, 45) sebagai kombinasi lanjar dari 21 dan 45.
- Solusi:

  45 = 2 (21) + 3

  21 = 7 (3) + 0

  Sisa pembagian terakhir sebelum 0 adalah 3, maka **fpb(45, 21) = 3**

  Substitusi dengan persamaan–persamaan di atas menghasilkan:

  3 = 45 – 2 (21)

  yang merupakan kombinasi lanjar dari 45 dan 21

Nyatakan fpb(312, 70) sebagai kombinasi lanjar 312 dan 70.

Solusi: Terapkan algoritma Euclidean untuk memperoleh fpb(312, 70):

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

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

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

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

Sisa pembagian terakhir sebelum 0 adalah 2, maka **fpb(312, 70) = 2**

Susun pembagian nomor (iii) dan (ii) masing-masing menjadi

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

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

Inverse Modulo dengan Algoritma Euclid

- Inverse modulo *a (mod m)* dari persamaan $ax \equiv 1 \pmod{m}$ dapat dicari menyelesaikan persamaan linear ($ax = mq + 1$), atau $ax - mq = 1$
- Penyelesaian tersebut dapat dicari dengan mencari FPB dari a dan m.

Contoh : carilah inverse dari 4 (mod 9)

atau carilah $4x \equiv 1 \pmod 9$

FPB(4,-9) kita cari dengan algoritma euclid.

i. **-9** = **4**(-3) + **3**
ii. **4 = 3**(1) + **1**
iii. **3 = 1**(3) + 0

Balik ruas semua persamaan
iv. 1 = 4 – 3(1)
v. 3 = -9 – 4(-3)
Subtitusikan v ke iv
1 = 4 – (-9 – 4(-3))(1)
1 = (-1)(-9) + 4(-2)
Artinya inverse dari 4 (mod 9) = -2

- 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 kongruen 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 $k_1 = 2 + 5k_2$

Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7.

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

$x \equiv 3 \pmod 5 \rightarrow x = 3 + 5k_1$ (i)
Sulihkan (i) ke dalam kongruen kedua menjadi:
$3 + 5k_1 \equiv 5 \pmod 7 \rightarrow k_1 \equiv 6 \pmod 7$, 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 menjadi:
$33 + 35k_2 \equiv 7 \pmod{11} \rightarrow k_2 \equiv 9 \pmod{11}$ 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. Perhatikan bahwa 348 mod 5 = 3, 348 mod 7 = 5, dan 348 mod 11 = 7. Catatlah bahwa $385 = 5 \cdot 7 \cdot 11$.

Referensi

- Rinaldi Munir, *Slide Kuliah Matematika Diskrit*
- Kenneth H. Rosen, *Discrete Mathematics and Its Application 6th.*