

Teori Bilangan bag. 2

Jurusan Teknik Informatika
Politeknik Negeri Batam

Pokok Bahasan

- ❖ Aritmatika Modulo
- ❖ Kekongruenan Linier
- ❖ Invers Modulo
- ❖ Bilangan prima
- ❖ Teorema Fermat
- ❖ Fungsi Totient Euler
- ❖ Teorema Euler
- ❖ Akar primitive

Aritmetika Modulo

- Misalkan a dan m bilangan bulat ($m > 0$). Operasi $a \text{ mod } m$ (dibaca “ a modulo m ”) memberi sisa jika a dibagi dengan m .
- Notasi : $a \text{ mod } m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$.
- m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0,1,2,\dots,m-1\}$.

Contoh

- $6 \text{ mod } 8 =$
- $0 \text{ mod } 6 =$
- $-39 \text{ mod } 13 =$
- $-41 \text{ mod } 9 =$
- $-6 \text{ mod } 18 =$

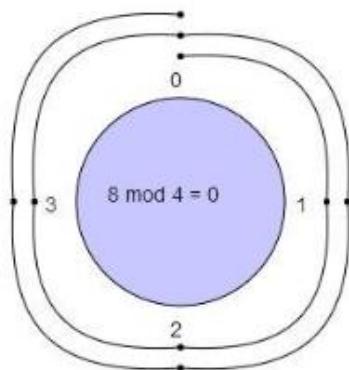
Catatan: a negatif, bagi $|a|$ dengan m mendapatkan sisa r' , maka $a \text{ mod } m = m - r'$, $r' \neq 0$.

Examples

$$8 \bmod 4 = ?$$

With a modulus of 4 we make a clock with numbers 0, 1, 2, 3.

We start at 0 and go through 8 numbers in a clockwise sequence 1, 2, 3, 0, 1, 2, 3, 0.

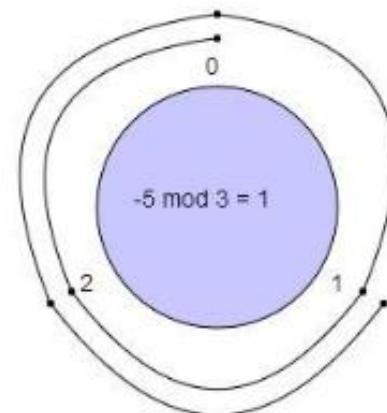
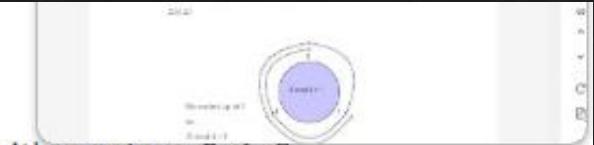


We ended up at **0** so $8 \bmod 4 = 0$.

$$-5 \bmod 3 = ?$$

With a modulus of 3 we make a clock with numbers 0, 1, 2.

We start at 0 and go through 5 numbers in **counter-clockwise** sequence (5 is **negative**) 2, 1, 0, 2, 1.



We ended up at **1** so $-5 \bmod 3 = 1$.

Kongruen

❖ Contoh

Misal $38 \bmod 5 = 3$ dan $13 \bmod 5 = 3$.
maka dikatakan $38 \equiv 13 \pmod{5}$

(dibaca 38 kongruen dengan 13 dalam
modulus 5)

❖ Contoh

Jam 15 = jam 3 sore
 $15 \equiv 3 \pmod{12}$

❖ Definisi

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0 , maka $a \equiv b \pmod{m}$ jika dan hanya jika $m|a - b$

❖ Contoh

Bilangan 38 kongruen dengan 13 modulo 5
karena 5 habis membagi $38 - 13 = 25$,
sehingga dapat ditulis bahwa $38 \equiv 13 \pmod{5}$

❖ Apakah 17 kongruen dengan 2 modulo 3?

❖ Apakah -7 kongruen dengan 15 modulo 11?

Sifat-sifat perhitungan Aritmetika Modulo

Theorem

Misalkan m adalah bilangan bulat positif

- ① *Jika $a \equiv b \pmod{m}$ dan c adalah sembarang bilangan bulat maka*
 - ① $(a + c) \equiv (b + c) \pmod{m}$
 - ② $ac \equiv bc \pmod{m}$
 - ③ $a^p \equiv b^p \pmod{m}$ untuk suatu bilangan bulat tak negatif p
- ② *Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka*
 - ① $(a + c) \equiv (b + d) \pmod{m}$
 - ② $ac \equiv bd \pmod{m}$

❖ Contoh

Misalkan $17 \equiv 2 \pmod{3}$ dan $10 \equiv 4 \pmod{3}$, berdasarkan teorema sifat-sifat aritmetika modulo maka,

$$17 + 5 \equiv 2 + 5 \pmod{3}$$

$$17 \cdot 5 \equiv 2 \cdot 5 \pmod{3}$$

$$17 + 10 \equiv 2 + 4 \pmod{3}$$

$$17 \cdot 10 \equiv 2 \cdot 4 \pmod{3}$$

Invers Modulo

- ❖ Jika a adalah sebuah bilangan tidak-nol, maka balikannya adalah $1/a$ sedemikian sehingga $a \times 1/a = 1$.
- ❖ Balikan a dilambangkan dengan a^{-1}
- ❖ Bagaimana menghitung balikan $a(mod m)$?
- ❖ **Syarat** : Jika a dan m relatif prima dan $m > 1$, maka balikan invers dari $a(mod m)$ ada.
- ❖ Balikan dari $a(mod m)$ adalah bilangan bulat x sedemikian sehingga $xa \equiv 1(mod m)$
- ❖ Notasi lain: $a^{-1}(mod m) = x$

❖ Contoh : Tentukan balikan dari $4(mod\ 9)$

Penyelesaian : PBB($4,9$)= 1 , maka balikan dari $4(mod\ 9)$ ada.

Perhatikan algoritma Euclidean berikut:

$$9 = 2 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

Dari persamaan diatas diperoleh $-2 \cdot 4 + 1 \cdot 9 = 1$ atau

$$-2 \cdot 4 + 1 \cdot 9 = 1(mod\ 9)$$

Karena $1 \cdot 9 \equiv 0 (mod\ 9)$, maka $-2 \cdot 4 \equiv 1(mod\ 9)$

Sehingga diperoleh $= 2$ adalah balikan dari $4(mod\ 9)$.

$$4^{-1}(mod\ 9) = -2(mod\ 9)$$

Cara lain menghitung invers modulo

- ❖ Misalkan x adalah balikan dari a ($mod\ m$) maka $ax \equiv 1(mod\ m)$ (definisi balikan modulo) atau dalam notasi ‘sama dengan’: $ax = 1 + km$ atau

$$x = \frac{1 + km}{a}$$

- ❖ Cobakan untuk $k = 0, 1, 2, \dots$ dan $k = -1, -2, \dots$
- ❖ Solusinya adalah semua bilangan bulat yang memenuhi.
- ❖ Contoh: Tentukan balikan dari $4(mod\ 9)$

Kekongruenan Linier

- ❖ Kekongruenan linier berbentuk $ax \equiv b \pmod{m}$. ($m > 0$, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat)
- ❖ Pemecahan : $ax = b + km \rightarrow x = \frac{b+km}{a}$
(Cobakan untuk $k = 0, 1, 2, \dots$ dan $k = -1, -2, \dots$ yang menghasilkan x sebagai bilangan bulat)
- ❖ Contoh : Tentukan solusi $4x \equiv 3 \pmod{9}$
Penyelesaian:
$$x = \frac{3 + k \cdot 9}{4}$$

Cobakan beberapa nilai k

Bilangan Prima

- ❖ **Definisi.** Bilangan bulat positif p ($p > 1$) disebut bilangan prima jika pembaginya hanya 1 dan p .
- ❖ Barisan bilangan prima yaitu 2, 3, 5, 7, 11, 13, .. Bilangan selain bilangan prima disebut bilangan komposit.
- ❖ **(Teorema fundamental aritmetik).** Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.
- ❖ **Teorema.** Jika n adalah bilangan komposit, maka n mempunyai faktor prima yang lebih kecil atau sama dengan \sqrt{n} .

Contoh : Apakah 199 adalah bilangan komposit?

Penyelesaian :

$$\sqrt{199} = 14,107$$

Bilangan prima yang $\leq \sqrt{199}$ adalah 2, 3, 5, 7, 11, 13.

Karena 199 tidak habis dibagi oleh 2, 3, 5, 7, 11, 13 maka 199 adalah bilangan prima.

Teorema Fermat

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

◊ Contoh : Apakah 17 Bilangan prima atau bukan dengan menggunakan teorema Fermat.

Penyelesaian :

Ambil $a = 2$, karena $PBB(17, 2) = 1$

Perhatikan bahwa $2^{17-1} = 65536 \equiv 1 \pmod{17}$ karena 17 habis membagi $65536 - 1 = 65535$

Jadi, 17 Bilangan prima

Fungsi Totient Euler

- ❖ Fungsi totient Euler ϕ mendefinisikan $\phi(n)$ untuk $n \geq 1$ yang menyatakan jumlah bilangan bulat positif $< n$ yang relatif prima dengan n
- ❖ Contoh:

Untuk $n = 20$, maka $\phi(n) = 8$. Bilangan bulat positif < 20 adalah 1 sampai 19. Terdapat $\phi(n) = 8$ buah yang relatif prima dengan 20, yaitu 1, 3, 7, 9, 11, 13, 17, 19.

Teorema Euler

- ❖ Misalkan a dan n adalah dua buah bilangan yang relatif prima, $\phi(n)$ adalah fungsi totient Euler, maka berlaku teorema Euler sebagai berikut

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- ❖ Contoh :

Misalkan $a = 7$ dan $n = 10$ (keduanya relatif prima), $\phi(10) = 4$, maka

$$7^4 = 2041 \equiv 1 \pmod{10}$$

Akar primitif

◇ Jika p adalah bilangan prima, maka a disebut akar primitif dari p jika perpangkatan a, a^2, \dots, a^{p-1} (dalam modulus p) menghasilkan nilai yang berbeda(ingatlah dari fungsi totient Euler, bahwa jika p prima maka $\phi(p) = p - 1$

◇ Contoh

Misalkan $p = 7$, maka $a = 3$ adalah akar primitif dari 7 karena

$$3^1 \pmod{7} = 3 \quad 3^2 \pmod{7} = 2 \quad 3^3 \pmod{7} = 6$$

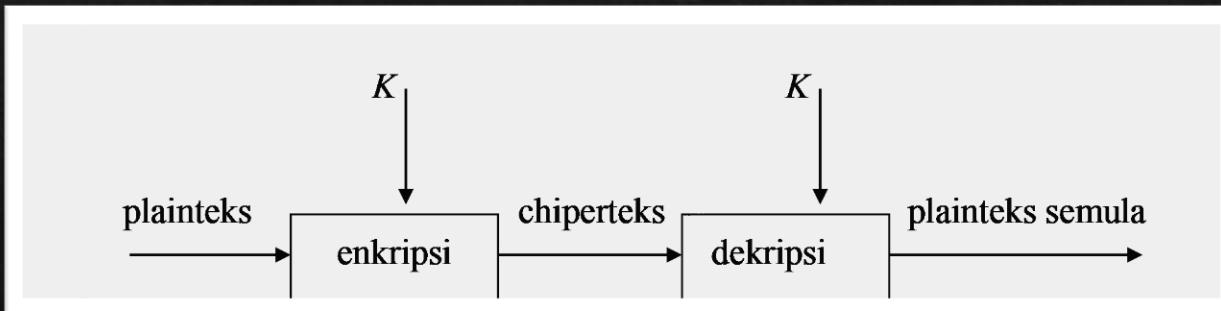
$$3^4 \pmod{7} = 4 \quad 3^5 \pmod{7} = 5 \quad 3^6 \pmod{7} = 1$$

◇ Jadi semua perpangkatan 3 menghasilkan nilai-nilai yang berbeda (3, 2, 6, 4, 5, 1), semua bilangan di dalam modulo7.

Kriptografi

- Bahasa Yunani yang artinya “secret writing”
- Merupakan ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna.
- Tujuannya agar pesan yang bersifat rahasia tidak dapat dibaca oleh pihak yang tidak berhak.

Kriptografi



- ❖ plainteks (plaintext) : data atau informasi yang dapat dibaca dan dimengerti maknanya.
- ❖ Cipherteks (ciphertext): pesan yang telah disandikan sehingga tidak memiliki makna lagi.
- ❖ Contoh:

Plainteks : Temui aku di tempat biasa

Cipherteks : HOM NAC GNL AHO MVC HFA CEC

Substitution Cipher

a. Caesar Cipher

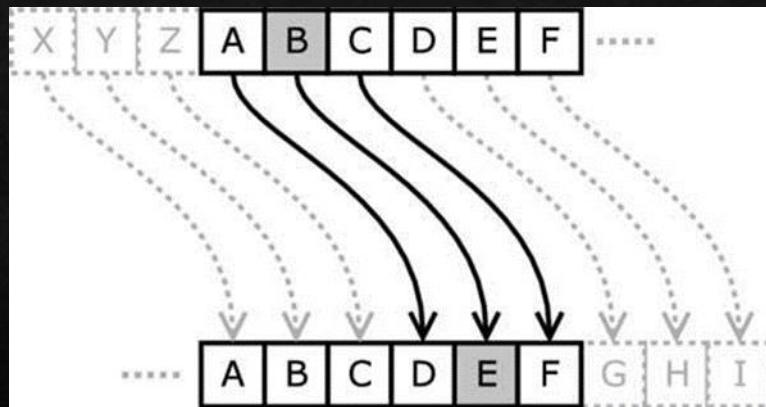
Merupakan algoritma substitusi monoalfabetik tertua, dimana setiap huruf digeser sejauh K posisi dalam alfabet.

Rumus :

$$E_K(x) = (x + K) \bmod 26$$

$$D_K(y) = (y - K) \bmod 26$$

- ❖ Algoritma enkripsi sederhana pada masa raja Julius Caesar
- ❖ Tiap huruf alfabet digeser 3 huruf ke kanan secara wrapping



- ❖ Contoh: Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
Cipherteks: DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Ilustrasi

Misalkan setiap huruf dikodekan dengan angka:

$$A = 0, B = 1, C = 2, \dots, Z = 25$$

Misalkan huruf plainteks dinyatakan sebagai p dan huruf cipherteks sebagai c , maka secara matematis enkripsi dan dekripsi pada Caesar cipher dinyatakan dengan persamaan modulo berikut:

- ❖ Enkripsi: $c = E(p) = (p + 3) \bmod 26$
- ❖ Dekripsi: $p = D(c) = (c - 3) \bmod 26$

Contoh

Tentukanlah enkripsi dari pesan “AWASI ASTERIX DAN TEMANNYA OBELIX” dengan menggunakan Caesar cipher!

Penyelesaian:

Enkripsi

Misal : $p_1 = 'A' = 0$, maka $c_1 = E(0) = (0 + 3) \text{ mod } 26 = 3 \text{ mod } 26 = 3 = 'D'$

$p_2 = 'W' = 22$, maka $c_2 = E(22) = (22 + 3) \text{ mod } 26 = 25 \text{ mod } 26 = 25 = 'Z'$

$p_3 = 'A' = 0$, maka $c_3 = E(0) = (0 + 3) \text{ mod } 26 = 3 \text{ mod } 26 = 3 = 'D'$

$p_4 = 'S' = 18$, maka $c_4 = E(18) = (18 + 3) \text{ mod } 26 = 21 \text{ mod } 26 = 21 = 'V'$

dst...

Diperoleh :

Cipherteks: DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Contoh

Tentukanlah Deskripsi dari Cipherteks: DZDVL DVWHULA GDQ WHPDQQBA REHOLA dengan menggunakan Caesar cipher!

Penyelesaian:

Dekripsi

Misal $c_1 = 'D' = 3$, maka $p_1 = D(3) = (3 - 3) \text{ mod } 26 = 3 \text{ mod } 26 = 3 = 'A'$

$c_2 = 'Z' = 25$, maka $p_2 = D(25) = (25 - 3) \text{ mod } 26 = 22 \text{ mod } 26 = 22 = 'W'$

$c_3 = 'D' = 3$, maka $p_3 = D(3) = (3 - 3) \text{ mod } 26 = 3 \text{ mod } 26 = 3 = 'A'$

$c_4 = 'V' = 21$, maka $p_4 = D(21) = (21 - 3) \text{ mod } 26 = 18 \text{ mod } 26 = 18 = 'S'$

dst...

Misal :Diperoleh :

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Aplikasi aritmatika modulo pada Kriptografi Klasik

Diberikan sistem kriptografi klasik Affine Cipher dengan fungsi enkripsi:

$$E_{a,b}(x) = (a \cdot x + b) \bmod 26$$

Dan fungsi dekripsi :

$$D_{a,b}(y) = a^{-1}(y - b) \bmod 26$$

Jika kunci yang digunakan adalah $a=7$ dan $b=3$, enkripsikan plaintext “SECURITY” dan lakukan dekripsinya kembali untuk memastikan hasilnya sesuai.

Gunakan konversi huruf ke angka: $A = 0, B = 1, C = 2, \dots, Z = 25$.

❖ **Penyelesaian :**
Fungsi enkripsi:

❖ $E(x) = (7x + 3) \text{ mod } 26$

❖ Ciphertext: ZFRNSHGP

	Huruf	Nilai x	Perhitungan	Nilai y	Cipher
	S	18	$(7 \times 18 + 3) \text{ mod } 26 = 129 \text{ mod } 26$	25	Z
	E	4	$(7 \times 4 + 3) \text{ mod } 26 = 31 \text{ mod } 26$	5	F
	C	2	$(7 \times 2 + 3) \text{ mod } 26 = 17 \text{ mod } 26$	17	R
	U	20	$(7 \times 20 + 3) \text{ mod } 26 = 143 \text{ mod } 26$	13	N
	R	17	$(7 \times 17 + 3) \text{ mod } 26 = 122 \text{ mod } 26$	18	S
	I	8	$(7 \times 8 + 3) \text{ mod } 26 = 59 \text{ mod } 26$	7	H
	T	19	$(7 \times 19 + 3) \text{ mod } 26 = 136 \text{ mod } 26$	6	G
	Y	24	$(7 \times 24 + 3) \text{ mod } 26 = 171 \text{ mod } 26$	15	P

Dekripsi,

- ❖ Tentukan a^{-1} (invers dari 7 modulo 26).
- ❖ $(7 \cdot a^{-1})mod\ 26 = 1$

Gunakan cara yang sudah dipelajari.

Diperoleh

- ❖ $7 \times 15 = 105 \rightarrow 105 mod 26 = 1$
- ❖ Jadi $a^{-1} = 15$

Fungsi dekripsi:

- ❖ $D(y) = 15 \cdot (y - 3)mod\ 26$

❖ Plaintext hasil dekripsi: SECURITY

Tugas

- ❖ Enkripsi nama mu dengan sistem kriptografi klasik Affine, kemudian deskripsikan. Nilai a dan b pada fungsi enkripsi tentukan sendiri.