

Informatika biztonság alapjai 2. gyakorlat

Oláh Norbert

2024.

Tartalom

- 1 Kongruencia és maradékosztályok
- 2 Algebrai struktúrák
- 3 Hagyományos titkosítások
- 4 Euklideszi algoritmus
- 5 Gyorshatványozás

Kongruencia

Definíció

*Legyenek a és b egész számok és m pozitív egész. Azt mondjuk, hogy a **kongruens** b -vel modulo m , ha $m \mid a - b$.*

Jelölés: $a \equiv b \pmod{m}$

- m modulusnak nevezzük.
- Két szám pontosan akkor kongruens modulo m , ha m -mel osztva ugyanazt a maradékot adják.
- ha nem ugyanazt a maradékot adják akkor inkongruensek

Példák: $13 \equiv 8 \pmod{5}$, $25 \equiv -10 \pmod{7}$, $25 \not\equiv 10 \pmod{7}$

Kongruencia elemi tulajdonságai

Tétel

- *szimmetrikus:*

ha $a \equiv b \pmod{m}$, akkor $b \equiv a \pmod{m}$

- *reflexív:*

$a \equiv a \pmod{m}$

- *tranzitív:*

ha $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}$, akkor $a \equiv c \pmod{m}$

Példa: $18 \equiv 13 \pmod{5}$ és $13 \equiv 8 \pmod{5}$, akkor $18 \equiv 8 \pmod{5}$

- *ha $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $a - c \equiv b - d \pmod{m}$*
- *ha $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, akkor $ac \equiv bd \pmod{m}$*

Maradékosztályok

Definíció

Rögzített m modulus mellett az a -val kongruens elemek halmazát az a által reprezentált maradékosztálynak nevezzük.

Jelölés $(a)_m$

Z_n olyan halmaz melynek elemei maradékosztályok

$Z_6 = \{(0)_6, (1)_6, (2)_6, (3)_6, (4)_6, (5)_6\}$

Teljes maradékrendszer

Definíció

Ha rögzített m modulus mellett minden maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo m teljes maradékrendszernek nevezzük

Feladat: $\{33, -5, 11, -11, 8\}$ teljes maradékrendszer modulo 5?

Tétel

Adott egész számok akkor és csak akkor alkotnak teljes maradékrendszert modulo m , ha

- számuk m , és
- páronként inkongruensek modulo m .

Maradékosztályok tulajdonságai

A modulo m maradékosztályok körében

- az összeadás asszociatív és kommutatív
hiszen $(a)_m + (b)_m = (a + b)_m$
- a $(0)_m$ nullelem, azaz minden $(a)_m$ -ra
 $(0)_m + (a)_m = (a)_m + (0)_m = (a)_m$
- az $(a)_m$ ellentettje $(-a)_m$ azaz
 $(a)_m + (-a)_m = (-a)_m + (a)_m = (0)_m$
- a szorzás asszociatív és kommutatív
hiszen $(a)_m * (b)_m = (ab)_m$
- a $(1)_m$ egységelem, azaz minden $(a)_m$ -ra
 $(1)_m(a)_m = (a)_m(1)_m = (a)_m$
- érvényes a disztributivitás.

Maradékosztályok tulajdonságai

- Példák:

$$(2)_6 + (5)_6 = (2 + 5)_6 = ?$$

$$(3)_6 + (3)_6 = ?$$

$$(4)_6 + (5)_6 = ?$$

$$(2)_6 * (5)_6 = ?$$

Algebrai struktúrát alkotnak.

Algebrai struktúrák

Adott egy $S = (x, y, z...)$ halmaz és ebben a halmazban definiálva van egy művelet. (általában összeadás és szorzás)

- félcsoport
- csoport
- Abel-csoport
- gyűrű
- test

Algebrai struktúrák

Definíció

Az $S = \{x, y, z, \dots\}$ halmazban definiálva van egy művelet, ha az S -nek minden x, y elempárjához hozzá van rendelve S -nek egy eleme.

Jelöljük ezt az elemet $x \circ y$ -nal, ahol a művelet jele: \circ . Általában két műveletet különböztetünk meg, az összeadást és a szorzást.

Definíció

A műveletet kommutatívnak nevezzük, ha bármely $x, y \in S$ esetén

$$x \circ y = y \circ x.$$

Példa: Az összeadás is és a szorzás is kommutatív az egész számok körében.

Definíció

A műveletet asszociatívnak nevezzük, ha bármely $x, y, z \in S$ esetén

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Példa: Az összeadás is és a szorzás is asszociatív az egész számok körében.

Definíció

Ha S -ben definiálva van az összeadás és szorzás művelete, és ha bármely $x, y, z \in S$ esetén

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

és

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

teljesül, akkor a szorzást disztributívnak nevezzük az összeadásra nézve.

Példa: Az egész számok körében a szorzás disztributív az összeadásra nézve.

Definíció

Az S -nek valamely e elemét egységelemnek vagy neutrális elemnek nevezzük, ha bármely $x \in S$ esetén

$$e \circ x = x \circ e = x.$$

Példa: Az egész számok halmazán szorzás műveletére nézve az egységelem az 1.

Definíció

Ha S -ben létezik e egységelem, és ha az x elemhez létezik olyan y elem, hogy

$$x \circ y = y \circ x = e,$$

akkor y -t az x inverzének nevezzük.

Példa: A valós számok halmazában 2 inverze $1/2$.

Definíció

- Egy S halmaz félcsoporth, ha definiálva van benne egy asszociatív művelet.
- Egy S halmaz csoport, ha definiálva van benne egy asszociatív művelet, létezik neutrális elem vagy egységelem, és minden elemnek létezik az inverze.
- Egy S halmaz Abel csoport, ha csoport és a művelet kommutatív is.
- Egy S halmaz gyűrű, ha definiálva van az összeadás és szorzás művelet, valamint a halmaz az összeadásra nézve Abel csoport, szorzásra nézve félcsoporth és a szorzás disztributív az összeadásra nézve. Az S kommutatív, egységelemes gyűrű, ha a szorzás kommutatív, valamint létezik egységelem a szorzásra nézve.
- Egy S halmaz test, ha kommutatív, egységelemes gyűrű és minden nem 0 elemnek van inverze a szorzás műveletére

Algebrai struktúra

Definíció

Az $(a)_m$ és $(b)_m$ maradékosztályok összegén az $(a + b)_m$, szorzatán pedig az $(ab)_m$ maradékosztályt értjük, azaz

$$(a)_m + (b)_m = (a + b)_m$$

és

$$(a)_m \cdot (b)_m = (ab)_m.$$

Bármely két modulo m maradékosztály összege, illetve szorzata egyértelműen meghatározott.

Kommutatív, egységelemes gyűrű

Tétel

A modulo m maradékosztályok esetén

- *az összeadás asszociatív és kommutatív,*
- *$(0)_m$ nullelem, azaz minden $(a)_m$ -ra*

$$(0)_m + (a)_m = (a)_m + (0)_m = (a)_m,$$
- *az $(a)_m$ ellentettje $(-a)_m$, azaz*

$$(-a)_m + (a)_m = (a)_m + (-a)_m = (0)_m,$$
- *a szorzás asszociatív és kommutatív,*
- *az $(1)_m$ egységelem, azaz minden $(a)_m$ -ra*

$$(1)_m \cdot (a)_m = (a)_m \cdot (1)_m = (a)_m,$$
- *érvényes a disztributivitás.*

Könnyen látható, hogy amennyiben a modulus prím, akkor a modulo m maradékosztályok halmaza testet alkot.

Feladat

- $Z_6 = \{(0)_6, (1)_6, (2)_6, (3)_6, (4)_6, (5)_6\}$
- $Z_5 = \{(0)_5, (1)_5, (2)_5, (3)_5, (4)_5\}$

Feladat

Test-e? (\mathbb{Z}_6 alaphalmaz;+)

asszociatív

kommutatív

\exists egységelem

(0_6)

minden elemnek \exists inverze

$(0)_6 \rightarrow (0)_6$

$(1)_6 \rightarrow (5)_6$

$(2)_6 \rightarrow (4)_6$

$(3)_6 \rightarrow (3)_6$

$(4)_6 \rightarrow (2)_6$

$(5)_6 \rightarrow (1)_6$

(\mathbb{Z}_6 alaphalmaz; \cdot)

asszociatív

kommutatív

\exists egységelem

(1_6)

nem minden nemnulla elemnek

\exists inverze

$(1)_6 \rightarrow (1)_6$

$(2)_6 \rightarrow$ nincs

$(3)_6 \rightarrow$ nincs

$(4)_6 \rightarrow$ nincs

$(5)_6 \rightarrow (5)_6$

Feladat

Test-e? $(\mathbb{Z}_5 \text{ alaphalmaz}; +)$

asszociatív

kommutatív

\exists egységelem

(0_5)

minden elemnek \exists inverze

$(0)_5 \rightarrow (0)_5$

$(1)_5 \rightarrow (4)_5$

$(2)_5 \rightarrow (3)_5$

$(3)_5 \rightarrow (2)_5$

$(4)_5 \rightarrow (1)_5$

$(\mathbb{Z}_5 \text{ alaphalmaz}; \cdot)$

asszociatív

kommutatív

\exists egységelem

(1_5)

\exists minden nemnulla elemnek

inverze

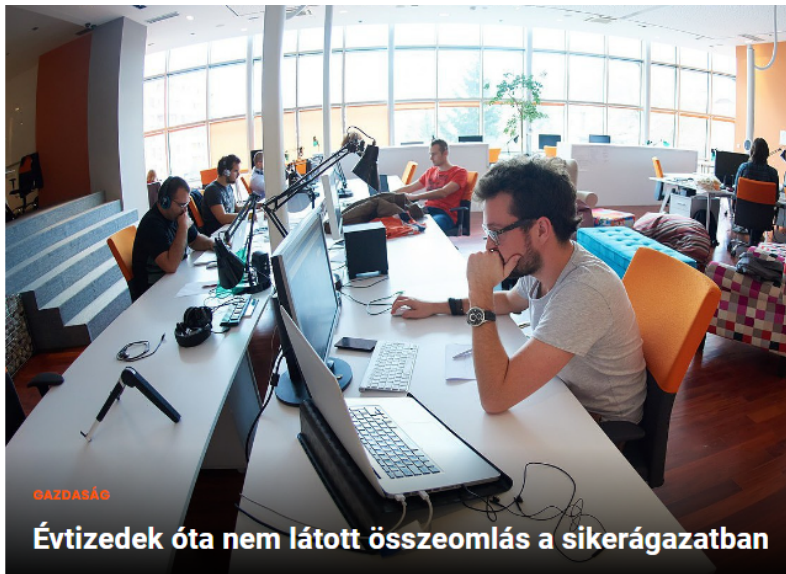
$(1)_5 \rightarrow (1)_5$

$(2)_5 \rightarrow (3)_5$

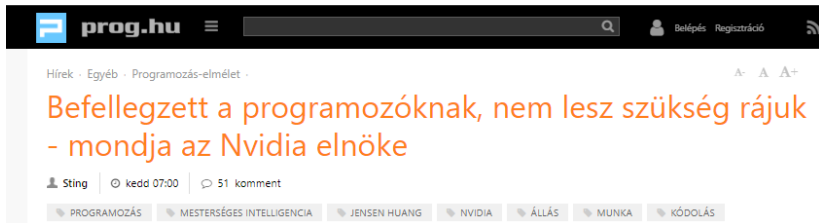
$(3)_5 \rightarrow (2)_5$

$(4)_5 \rightarrow (4)_5$

Offtopic - Mi a programozás jövője?



Offtopic - Mi a programozás jövője?



Offtopic - Mi a programozás jövője?



Szoftver

Jó tudni!

Megoldásaink ▼

Mi lesz a programozókkal? Már szoftver írja a szoftvert?

Offtopic - Mi a programozás jövője?

Vitaindító - Kellenek-e 5 év múlva
programozók?

Helyettesítéses titkosítás

● Caesar titkosítás

- nyílt szöveg (m)
- kulcs (k)
- titkosított szöveg $c = (m + k) \bmod 26 \rightarrow$ angol abc
- visszafejtett szöveg $m = (c - k) \bmod 26$

● Kulcsszavas Caesar titkosítás

- nyílt szöveg (m)
- kulcs ($k=8$ security)
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 O P Q V X Y Z S E C U R I T Y A B D F G H J K L M N
- az eltolásos ábécéhez képest, hogy lényegesen több ($n!$, ahol n az ábécé hossza) variációja van
- pusztán rotációval nem lehet feltörni

Affin titkosítás

- Betűnkénti titkosítás
- A kulcs egy számpár $K=(a,b) \rightarrow \text{LNKO}(a,26)=1$
- $c = (a * m + b) \bmod 26$
- $m = (a_1 * c - a_1 * b) \bmod 26$ ahol $a_1 * a = 1 \bmod 26$

Euklideszi algoritmus

80	50	30	20	10	0
-	1	1	1	2	

(845,68) LNKO?

Euklideszi algoritmus

845	68	29	10	9	1	0
-	12	2	2	1	9	

Így a két szám relatív prím, azaz: $(845, 68) = 1$

Euklideszi algoritmus pszeudó kód

- Euklidesz(a, b, d)
- $d \leftarrow a$
- If($b \neq 0$)
- Then Euklidesz($b, a \bmod b, d$)
- Return (d)

Kibővített Euklideszi algoritmus

Az a és b két egész szám legnagyobb közös osztója $x, y \in \mathbb{Z}$ számokkal kifejezhető a következő alakban:

$$(a, b) = a * x + b * y$$

Mindig!

$$x_0 = 1 \quad x_1 = 0$$

$$y_0 = 0 \quad y_1 = 1$$

Képlet:

$$x_{i+1} = x_i * q_i + x_{i-1}$$

$$y_{i+1} = y_i * q_i + y_{i-1}$$

$$x = (-1)^n * x_n$$

$$y = (-1)^{n+1} * y_n$$

Kibővített Euklideszi algoritmus 1 példa

k	0	1	2	-
r_k	280	3	1	0
q_k	-	93	3	
x_k	1	0	1	
y_k	0	1	93	

$$(-1)^2 \text{ és } (-1)^{2+1}$$

$$1 = 280 \cdot 1 + 3 \cdot (-93)$$

Kibővített Euklideszi algoritmus 2 példa

k	0	1	2	3	4	
r_k	544	119	68	51	17	0
q_k	-	4	1	1	3	
x_k	1	0	1	1	2	
y_k	0	1	4	5	9	

$$(-1)^4 \text{ és } (-1)^{4+1}$$

$$17 = 544 \cdot 2 + 119 \cdot (-9)$$

Kibővített Euklideszi algoritmus pszeudó kód

- $\text{KibővítettEuklidesz}(a, b, d, x, y)$
- $x_0 \leftarrow 1, x_1 \leftarrow 0, y_0 \leftarrow 0, y_1 \leftarrow 1, s \leftarrow 1$
- While ($b \neq 0$)
- $r \leftarrow a \bmod b, q \leftarrow a \div b$
- $a \leftarrow b, b \leftarrow r$
- $x \leftarrow x_1, y \leftarrow y_1$
- $x_1 \leftarrow q * x_1 + x_0, y_1 \leftarrow q * y_1 + y_0$
- $x_0 \leftarrow x, y_0 \leftarrow y$
- $s \leftarrow -s$
- End While
- $x \leftarrow s * x_0, y \leftarrow -s * y_0$
- $(d, x, y) \leftarrow (a, x, y)$
- Return (d, x, y)

Gyorshatványozás

Tétel

Legyen $$ egy bináris művelet a G halmazon és $b \in G$. Legyen $m \in \mathbb{N}$ és $n \in \mathbb{N}$ úgy hogy $m \leq 2^n$. Ekkor gyorshatványozással, b^m legfeljebb $2 \cdot n$ műveletben számítható ki.*

Gyorshatványozás

Az alábbi módszer alkalmazásával viszonylag kevés művelet elvégzésével megkapjuk a^b modulo m értékét, ahol a egész szám, b 1-nél nagyobb egész, m pozitív egész.

Algoritmus:

1. lépés: A kitevőt felírjuk 2 hatványainak összegeként:

$$b = 2^{b_1} + 2^{b_2} + \dots + 2^{b_r}$$

2. lépés: ismételt négyzetre emeléssel számoljuk ki a következő értékeket: $a^{2^0}, a^{2^1}, \dots, a^{2^r}$

$$a^{2^{k+1}} = a^{2^k * 2} = (a^{2^k})^2$$

3. lépés: megkapjuk a keresett hatványt:

$$a^b = a^{2^{b_1}} * a^{2^{b_2}} * \dots * a^{2^{b_r}} \pmod{m}$$

Példa

$$6^{73} \pmod{100}$$

$$73 = 2^6 + 2^3 + 2^0$$

$$6^{2^0} \equiv 6 \pmod{100}$$

$$6^{2^1} \equiv 36 \pmod{100}$$

$$6^{2^2} \equiv 96 \pmod{100}$$

$$6^{2^3} \equiv 16 \pmod{100}$$

$$6^{2^4} \equiv 56 \pmod{100}$$

$$6^{2^5} \equiv 36 \pmod{100}$$

$$6^{2^6} \equiv 96 \pmod{100}$$

$$6^{73} = 6^{2^6} * 6^{2^3} * 6^{2^0} = 96 * 16 * 6 \equiv 16 \pmod{100}$$

Feladat

$$129^{97} \pmod{171}$$

Feladat

$$129^{97} \pmod{171}$$

$$97 = 2^6 + 2^5 + 2^0$$

$$129^{2^0} \equiv 129 \pmod{171}$$

$$129^{2^1} \equiv 54 \pmod{171}$$

$$129^{2^2} \equiv 9 \pmod{171}$$

$$129^{2^3} \equiv 81 \pmod{171}$$

$$129^{2^4} \equiv 63 \pmod{171}$$

$$129^{2^5} \equiv 36 \pmod{171}$$

$$129^{2^6} \equiv 99 \pmod{171}$$

$$129^{97} = 129^{2^6} * 129^{2^5} * 129^{2^0} = 99 * 36 * 129 \equiv 108 \pmod{171}$$

Programozási feladat 3.

Feladat: Programozd le az általad preferált programozási nyelven a Gyorshatványozás algoritmusát. Segítségként felhasználhatod a következő dián lévő pszeudó kódot.

Gyorshatványozás pszeudó kód

- $\text{Gyorshatvany}(alap, exp, mod)$
- $alap = alap \% mod,$
- $\text{if}(exp == 0)$
- $\text{return } 1;$
- $\text{else if}(exp == 1)$
- $\text{return } alap;$
- $\text{else if}(exp \% 2 == 0)$
- $\text{return Gyorshatvany}(alap * alap \% mod, exp/2, mod);$
- else
- $\text{return } alap * \text{Gyorshatvany}(alap, exp - 1, mod) \% mod;$

Feladat - Prompt alapú programozás

Van-e a programozásnak jövője?

Lépj be az ChatGPT oldalára és a prompt-ok segítségével készítsd el a Kibővített Euklideszi és a Gyorshatványozás algoritmusát!

Feladat - Prompt alapú programozás

Milyen veszélyei vannak?

Feladat - Prompt alapú programozás

Milyen veszélyei vannak?

Próbálj legenerálni egy támadói kódot (xml bomba, sql injection példa, stb.)

A szoftverfejlesztés jövője: 2024-ben megfigyelendő trendek

- 1 AI-alapú fejlesztés
- 2 Kvantumszámítástechnikai integráció
- 3 Low-Code és No-Code fejlesztés
- 4 Edge számítás
- 5 Kibővített valóság (XR)
- 6 Cybersecurity-First Development
- 7 Etikus mesterséges intelligencia és felelős fejlesztés
- 8 Blockchain a szoftverbiztonságért
- 9 Sustainable Software Development

