Informatikai biztonság alapjai 1. gyakorlat

Oláh Norbert

2025.

Tartalom

Jégtörés

- Milyen tapasztalataid vannak a számítógépes biztonsággal kapcsolatosan a hétköznapjaidban?

Mi az a fenyegetésmodellezés?

- Egy számítógépes rendszer biztonságának elemzésére szolgáló megközelítés.
- A rendszer potenciális sebezhetőségének és kockázatainak vizsgálata, és azt, hogy a támadók hogyan közelíthetik meg
  - Mit védünk?
  - Mit nyerhet a támadó?
  - Hogyan próbálná meg egy támadó kihasználni a rendszert?

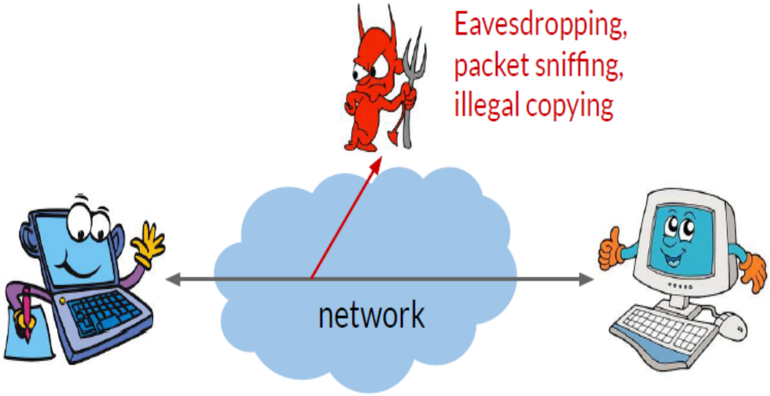
Mit jelent ”biztonságban lenni”?

A biztonság hagyományos céljai a következők:

- Bizalmasság
- Sértetlenség
- Rendelkezésre állás
- hitelesség

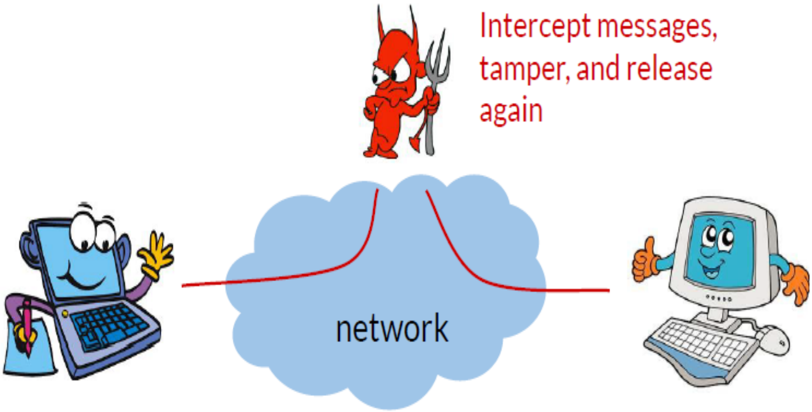
Bizalmasság

A bizalmasság az információ elrejtése.



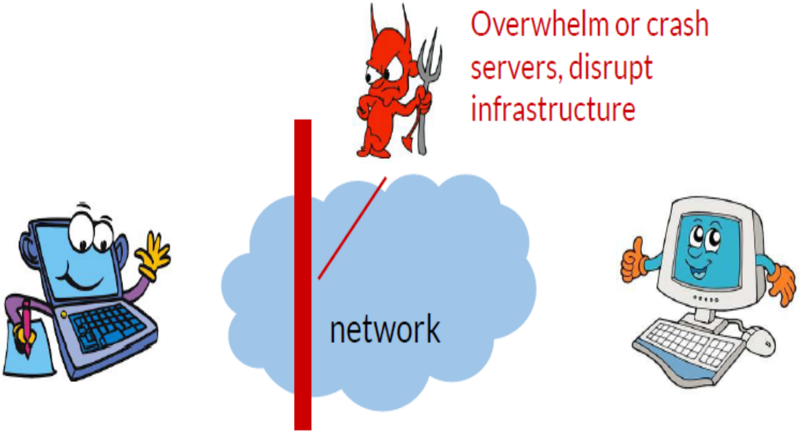
Sértetlenség

A sértetlenség a jogosulatlan változtatások megakadályozása.



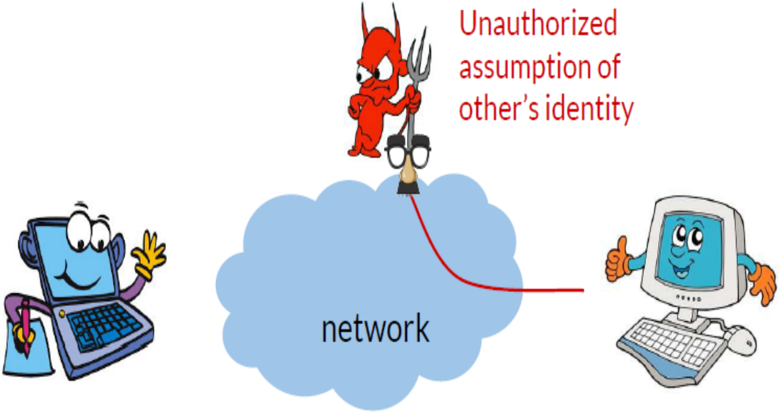
Rendelkezésre állás

A rendelkezésre állás az információ vagy az erőforrások használatának képessége.



Hitelesség

A hitelesség azt jelenti, hogy tudod, kivel beszélsz.



Fenyegetésmodellezési példa: Közösségi média szolgáltatások

- Mit védesz?
- Mit nyerhet egy támadó?
- Hogyan használhatná ki a támadó a rendszert?

Fenyegetés modell

- Eszközök
  Mit próbálunk megvédeni? Milyen szempontból értékesek ezek az eszközök?
- Támadók
  Ki próbálhat meg támadni, és miért?
- Sebezhető pontok
  Miben lehet gyenge a rendszer?
- Fenyegetések
  Milyen lépéseket tehet egy támadó a sebezhetőségek kihasználására?
- Kockázat
  Mennyire fontosak az eszközök? Mennyire valószínű, hogy a kihasználás?
- Lehetséges védekezés

Eszközök

Mit próbálunk megvédeni?

- Felhasználói adatok
  - Személyes adatok (születési dátum, SSN, telefonszám)
  - Hirdetések célzására vonatkozó információk
  - Felhasználó által generált tartalom (üzenetek, fényképek, hozzászólások)
- Mennyire értékesek ezek az eszközök?
  - Potenciálisan nagyon személyes
  - Pénzben nem mérhető

Támadók

Ki és miért próbálhat meg támadni?

- Külföldi kormányok
- Más vállalatok
- Hackerek
- Alkalmazottak
- Egyéb felhasználók

Tipp:Néhány ellenfél nem biztos, hogy egyértelmű.
A felhasználói visszaélések nem szándékos problémákat okozhatnak.

Sérülékenységek & Fenyegetések

Hogyan lehet gyenge a rendszer?
Hogyan használhatja ki egy ellenfél a sebezhetőségeket?

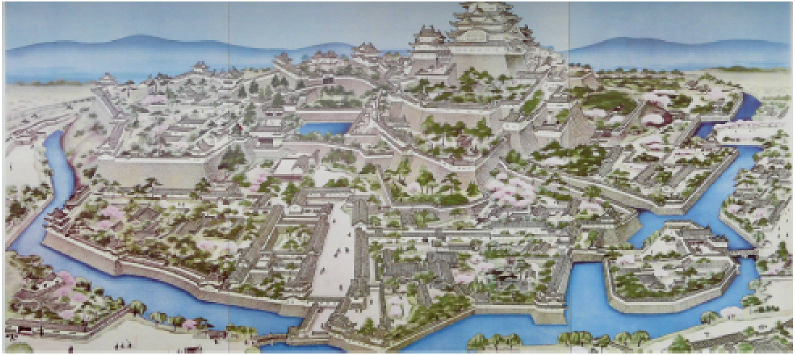
- Kód sebezhetőségek
- Gyenge jelszavak
- Social engineering
- Belső fenyegetések (alkalmazottak)
- Fizikai fenyegetések

Kockázat

Mennyire valószínű egy sikeres támadás?

- Mennyi erőforrásra lenne szüksége a támadónak ahhoz, hogy a támadást sikeresen végrehajtsa?
- Elrettentő lehet, de a támadók aszimmetrikus előnnyel rendelkeznek.
- Jogi és etikai szempontok
    - Jogi következmények
    - A vállalat hírneve
    - Az ügyfelek személyes adatai

Mélységi védekezés

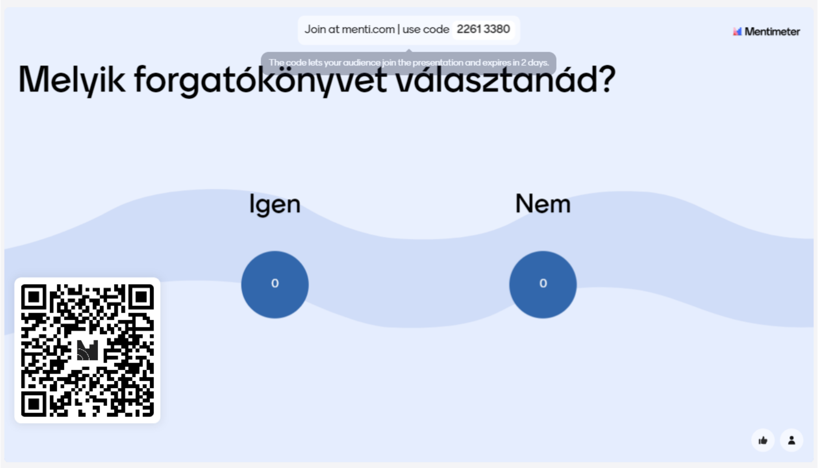


A támadónak csak egy helyen kell nyernie
A védő válasza: Védekezés a mélységben

Etikai esettanulmány

- Tegyük fel, hogy az A, B és C vállalatok mindegyike ugyanazzal a sebezhetőséggel rendelkezik, de még nem hozták nyilvánosságra.
- Az A vállalatnak van egy szoftverfrissítése, amely készen áll, és amint leszállításra kerül, kijavítja a sebezhetőséget
- A B és a C még mindig dolgozik a sebezhetőség javítócsomagának kifejlesztésén
- Az A vállalat tudomást szerez arról, hogy a támadók kihasználják ezt a sebezhetőséget a ”vadonban”.
- *Az A vállalatnak közzé kell-e tennie a javítást, még akkor is, ha ez azt jelenti, hogy a sebezhetőség nyilvánosságra kerül és más szereplők elkezdhetik a B és C vállalat támadni?*
- *Vagy az A vállalatnak meg kell várnia, amíg a B és C vállalat is elkészíti a javításokat?*

Mélységi védekezés



Az etikáról való gondolkodás különböző keretei

Nem feltétlenül létezik egyértelmű ”helyes” válasz!
Például

- Következményelvű: Figyelembe veszi a hatásokat/következményeket különböző döntések
- Deontológiai: Kötelességek és jogok kérdéseit vizsgálja (pl, magánélethez való jog)

Lásd később a klasszikus kocsi problémát...

A kurzus első nagyobb szakasza:

Kriptográfia

Terminológiai megjegyzés: ”blokklánc” és ”kripto”

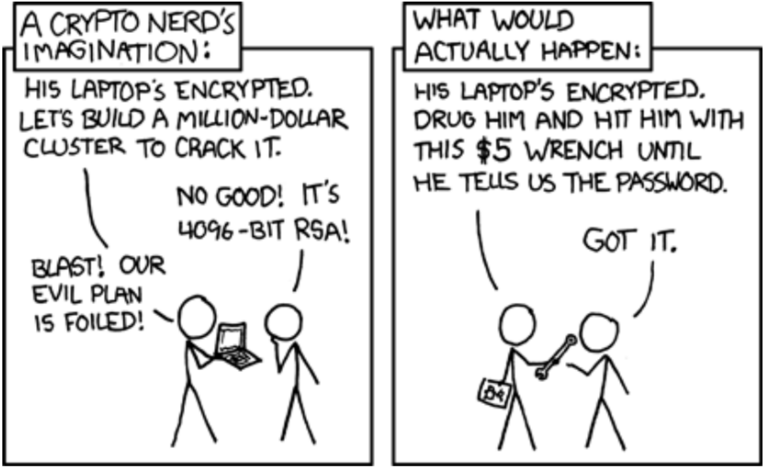
- Növekvő érdeklődés, főként a kriptopénzek terén.
- Ibizán: kripto jelentése ”kriptográfia”.

Hívjuk elő a nagyobb képet

- A kriptográfia csak egy kis darabja egy nagyobb rendszernek.
- A teljes rendszert kell védenie
  - Fizikai biztonság
  - Az operációs rendszer biztonsága
  - Hálózati biztonság
  - Felhasználók
  - Kriptográfia (következő diák)
- Emlékezz a leggyengébb láncszemre
- A kriptográfia mindig az eszköztárunk kulcsfontosságú része.

XKCD

http://xkcd.com/538/



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology. - Bruce Schneier

If you think cryptography is the answer to your problem, then you don't know what your problem is." - Dr. Peter G. Neumann

Leggyengébb láncszem!

Algebrai struktúrák

Definíció

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

Jelöljük ezt az elemet *xoy*-nal, ahol a művelet jele: *o*. Általában két műveletet különböztetünk meg, az összeadást és a szorzást.

Definíció

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

$$xoy = yox.$$

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*

$$(xoy)oz = xo(yoz).$$

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

Definíció

Ha S-ben definiálva van az összeadás és a 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.

Oszthatóság

Definíció

A b egész számot az a egész szám osztójának nevezzük, ha létezik olyan q egész szám, amelyre $a = bq$.
Jelölés: $b|a$.

- a az osztandó
- b az osztó
  Osztó: azokat a számokat, amelyekkel egy a szám osztható, az a szám osztóinak nevezzük. Minden számnak legalább két osztója van, 1 és önmaga.
- q hányados

Oszthatóság

Definíció

Ha egy szám minden számnak osztója, akkor egységnek nevezzük.

Tétel

Az egész számok körében két egység van, az 1 és a -1.

Bizonyítás: Az 1 és a -1 valóban egységek: bármely a-ra $\pm 1 \mid a$, hiszen $a = (\pm 1)(\pm a)$.

Oszthatóság

Tétel

- *Minden a-ra* $a \mid a$
- *Ha* $c \mid b$ *és* $b \mid a$, *akkor* $c \mid a$
- *Az* $a \mid b$ *és* $b \mid a$ *oszthatóságok egyszerre akkor és csak akkor teljesülnek, ha az* a *a* b*-nek egységszerese.*
- *Ha* $c \mid a$ *és* $c \mid b$ *akkor* $c \mid a + b$, $c \mid a - b$, *tetszőleges (egész)* k*-ra* $c \mid ka$, *és tetszőleges (egész)* r, s*-re* $c \mid ra + sb$.

Maradék osztás tétele

Tétel

Tetszőleges a *és* $b \neq 0$ *egész számokhoz léteznek olyan egyértelműen meghatározott* q *és* r *egész számok, melyekre* $a = b * q + r$, *ahol* $0 \leq r < |b|$.

Ilyenkor azt mondjuk, hogy b megvan a-ban q-szor és maradék az r.
Bizonyítás: Legyen először $b > 0$. A

$$0 \leq r = a - bq < b$$

azaz

$$q \leq a/b < q + 1.$$

folyt.

Maradék osztás tétele

Ilyen q egész szám pontosan egy létezik; q az a/b (alsó) *egészrésze*, $q = \lfloor a/b \rfloor$, azaz a legnagyobb olyan egész szám, amely még kisebb vagy egyelő, mint a/b.
Ha $b < 0$, akkor a

$$0 \leq r = a - bq < |b| = -b$$

feltétel

$$q \geq a/b > q - 1$$

teljesülésével ekvivalens, ami pontosan egy q egészre áll fenn.

Alapok

Definíció

A p egységtől (és nullától) különböző számot felbonthatatlan számnak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység. Azaz

$$p = ab \rightarrow a \text{ vagy } b \text{ egység}.$$

Definíció

A p egységtől (és nullától) különböző számot prímszámnak nevezzük, ha csak úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$p = ab \rightarrow p|a \text{ vagy } p|b.$$

Prímszám (törzsszám): csak két osztója van, 1 és önmaga, pl. 2, 3, 5, 7.

Alapok

Definíció

Ha egy nemnulla számnak triviálistól különböző osztója is van, akkor összetett számnak nevezzük.

Az egység definíciója alapján bármely ϵ egység esetén $\epsilon | a$ és $\epsilon a | a$. Ezeket az a triviális osztóinak nevezzük.
Összetett szám: 1-en és önmagán kívül más osztója is van, pl. 4, 6, 10.
Minden összetett szám felbontható prímszámok szorzatára, pl. $60 = 2 * 2 * 3 * 5$

Legnagyobb közös osztó

Definíció

Az a és b számok legnagyobb közös osztója d, ha

- $d|a$ *és* $d|b$ *; és*
- *ha egy* c*-re* $c|a$, $c|b$ *teljesül akkor* $|c| \leq |d|$

Kitüntetett közös osztó

Definíció

Az a és b számok kitüntetett közös osztója δ, ha

- $\delta | a$ *és* $\delta | b$ *; és*
- *ha egy c-re $c|a$, $c|b$ teljesül akkor $c|\delta$*

Tétel

Bármely két egész számnak létezik kitüntetett közös osztója.

Bizonyítás: euklideszi algoritmus.

Euklideszi algoritmus

Az egyik számot maradékosan elosztjuk a másikkal, majd a másik számot a maradékkal stb., mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk.
Tegyük fel, hogy $b \neq 0$. Ha $b|a$, akkor $\delta = b$ megfelel. Ha $b \nmid a$ akkor alkalmas q_i, r_i egészekkel
$a = bq_1 + r_1$, ahol $0 < r_1 < |b|$,
$b = r1q_2 + r_2$, ahol $0 < r_2 < r_1$,
$r1 = r2q_3 + r_3$, ahol $0 < r_3 < r_2$,
...
$r_{n-1} = r_n q_{n+1}$ $(r_{n+1} = 0)$

Euklideszi algoritmus

$(80, 50)$ legnagyobb közös osztója?

80	50	30	20	**10**	0
-	1	1	1	2	

(845,68) LNKO?

Relatív prímek

Definíció

Az $a_1, a_2, \ldots, a_k$ számok relatív prímek, ha nincs egységtől különböző közös osztójuk, azaz $(a_1, a_2, \ldots, a_k) = 1$.

Euklideszi algoritmus

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

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

Programozási feladat 1.

Feladat: Programozd le az általad preferált programozási nyelven az Euklideszi algoritmust. Segítségként felhasználhatod az alábbi pszeudó kódot:

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

Etikai esettanulmány - offtopic

Klasszikus kocsi probléma:
https://securityethics.cs.washington.edu/

Kibővített Euklideszi algoritmus

Tétel

Az a és b számok legnagyobb közös osztója alkalmas x és y egészekkel kifejezhető $(a, b) = ax + by$ alakban.

Kibővített Euklideszi algoritmus

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

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

Mindig!

$x_0 = 1$ $x_1 = 0$

$y_0 = 0$ $y_1 = 1$

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	

$(-1)^2$ és $(-1)^{2+1}$

1=280*1+3*-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	

$(-1)^4$ és $(-1)^{4+1}$
17=544*2+119*-9

Programozási feladat 2.

Feladat: Programozd le az általad preferált programozási nyelven a Kibővített Euklideszi algoritmust. Segítségként felhasználhatod a következő dián lévő pszeudó kódot:

Programozási feladat 2.

- 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 $(b \neq 0)$
- $r \leftarrow a\ mod\ b$, $q \leftarrow a\ div\ b$
- $a \leftarrow b$, $b \leftarrow r$
- $x \leftarrow x_1$, $y \leftarrow y_1$
- $x_1 \leftarrow q * x_1 + x_0$, $y_1 \leftarrow q * y_1 + y_0$
- $x_0 \leftarrow x$, $y_0 \leftarrow y$
- $s \leftarrow -s$
- End While
- $x \leftarrow s * x_0$, $y \leftarrow -s * y_0$
- $(d, x, y) \leftarrow (a, x, y)$
- Return (d, x, y)

Kongruencia

Definíció

*Legyenek a és b egész számok és m pozitív egész. Aztmondjuk, hogy a **kongurens** 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:*
  $a \equiv a \pmod{m}$
- *tranzítiv:*
  ha $a \equiv b \pmod{m}$ *és ha* $b \equiv c \pmod{m}$ *akkor ha* $a \equiv c \pmod{m}$
  Példa: $18 \equiv 13 \pmod{5}$ *és ha* $13 \equiv 8 \pmod{5}$ *akkor* $18 \equiv 8 \pmod{5}$
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ *akkor* $a + c \equiv b + d \pmod{m}$ *és* $a - c \equiv b + d \pmod{m}$
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ *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

Tétel

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* $(a)_m$ *ellentetje* $(-a)_m$ *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.

Köszönöm a figyelmet!