

## Zenbaki teoria. Zenbaki osoak.

### Zenbaki Teoria

Irakasgaia: Matematika Diskretua  
Titulazioa: Informatikaren Ingeniaritzako Gradua  
Informatika fakultatea  
Donostia

- Zenbaki osoen multzoa:  $\mathbb{Z}$
- $\mathbb{Z}$  multzoan batuketa, kenketa eta biderketa barne eragiketak dira (emaizta osoa da),  $\forall x, y \in \mathbb{Z} \Rightarrow x + y, x - y, x \cdot y \in \mathbb{Z}$ , baina zatiketa ez. Adibidez:  $2, 3 \in \mathbb{Z}$ , baina  $\frac{2}{3} \notin \mathbb{Z}$ .
- Zenbaki teoria: Zenbaki osoen arteko zatiketa aztertzen duen matematikaren adarra.
  - Zenbaki oso positiboak:  $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\}$
  - Zenbaki oso negatiboak:  $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$
- Ordena onaren printzipioa:  $\mathbb{Z}$  multzoa erabat ordenatuta dago,  $\forall x, y \in \mathbb{Z} \quad x \leq y$  edo  $y \leq x$
- $\mathbb{Z}^+$  multzoaren edozein azpimultzo ez-hutsek elementu minimoa dauka

1

### Zatigarritasuna. Zenbaki lehenak

Definizioa (Zatigarritasuna)

$a, b \in \mathbb{Z}$  emanik,  $a \neq 0$ ,  $a$ -k  $b$  zatitzen duela esango dugu eta  $a|b$  notazioaz adierazi baldin  $\exists k \in \mathbb{Z}$  non  $b = ka$  den.  $a$   $b$ -ren zatitzale bat dela esango dugu eta  $b$   $a$ -ren multiplo bat.

Zera ondoriozta dezakegu:  $a, b \in \mathbb{Z}^+$  emanik,  $a|b \Rightarrow a \leq b$

Teorema (Zatigarritasunaren propietateak)

$a, b, c \in \mathbb{Z}$  emanik,

1.  $1 | a$ ;  $a | a$ ;  $a | 0$ .  
 $(a \neq 0)$
2.  $(a | b) \wedge (b | a) \Rightarrow a = b \vee a = -b$ .  
 $(a \neq 0, b \neq 0)$
3.  $(a | b) \wedge (b | c) \Rightarrow a | c$ .  
 $(a \neq 0)$
4.  $a | b \Rightarrow (\forall x \in \mathbb{Z}) a | xb$ .  
 $(a \neq 0)$
5.  $(a | b) \wedge (a | c) \Rightarrow (\forall x, y \in \mathbb{Z}) a | xb + yc$   
 $a | bi \Rightarrow \forall x_i \in \mathbb{Z} \quad a | x_1b_1 + \dots + x_n b_n, \quad i = 1, \dots, n$   
 $(a \neq 0)$

ZENBAKI TEORIA. ZENBAKI OSOAK. 2

### Zatigarritasuna. Zenbaki lehenak

Definizioa (Zenbaki lehena)

Izan bedi  $n \in \mathbb{Z}^+$ ,  $n > 1$ .  $n$  zenbaki lehena dela esango dugu bere zatitzale positibo bakarrak  $n$  eta 1 badira:  
 $m | n, \quad m \in \mathbb{Z}^+ \implies m = 1 \vee m = n$ .

$n$  zenbakia lehena ez bada konposatura dela esango dugu:  
 $\exists m_1, m_2 \in \mathbb{Z}^+ \text{ non } n = m_1m_2, \quad 1 < m_1 < n, \quad 1 < m_2 < n$ .

Teorema

Zenbaki konposatu orok zatitzale lehenen bat dauka.

$n \in \mathbb{Z}^+, n > 1, n$  konposatu  $\implies \exists p \in \mathbb{Z}^+, p$  lehena eta  $p | n$ .

Teorema (Euklides, Elementuak, IX, 20)

Infinitu zenbaki lehen daudet.

## Zatiketa Euklidestarra

Teorema (Zatiketa Euklidestarra)

$a, b \in \mathbb{Z}$  emanik,  $b > 0$  izanik,

$\exists | q \in \mathbb{Z} \quad \exists | r \in \mathbb{Z} \text{ non } a = qb + r \text{ den, } 0 \leq r < b$  izanik;

$q$  zatidura da,  $r$  hondarra,  $a$  zatikizuna eta  $b$  zatitzalea.

Definizioa (Zatitzaile komunak)

Izan bitez  $a, b \in \mathbb{Z}$  eta izan bedi  $c \in \mathbb{Z}^+$ .  $c$  zenbakia  $a$  eta  $b$  zenbakien zatitzaile komun bat dela esango dugu  $c | a$  eta  $c | b$  betetzen badira.

ZATIKETA EUKLIDESTARRA 5

## Zatitzaile komunetako handiena

Definizioa (Zatitzaile komunetako handiena,  $zkh(a, b)$ )

Izan bitez  $a, b \in \mathbb{Z}$ ,  $a \neq 0$  edo  $b \neq 0$ , eta izan bedi  $d \in \mathbb{Z}^+$ .

Esango dugu  $d$  zenbakia  $a$  eta  $b$  zenbakien zatitzaile komunetako handiena dela,  $zkh(a, b)$ , baldin

1.  $d$  bada  $a$  eta  $b$  zenbakien zatitzaile komun bat:

$$d | a \text{ eta } d | b;$$

2.  $a$  eta  $b$  zenbakien edozein zatitzaile komunek  $d$  zatitzenten badu:

$$(\forall c \in \mathbb{Z}^+) \quad c | a, \quad c | b \Rightarrow c | d.$$

Teorema  
 $a, b \in \mathbb{Z}^+$  emanik,  $a$  eta  $b$  zenbakien zatitzaile komunetako handiena existitzen da eta bakarra da.

ZATIKETA EUKLIDESTARRA 6

## Zatitzaile komunetako handiena

### Propietateak.

1.  $zkh(b, a) = zkh(a, b)$ .
2.  $zkh(0, 0)$  ez dago definiturik.
3.  $a \in \mathbb{Z}$ ,  $a \neq 0$  izanik,  $zkh(a, 0) = |a|$ .
4.  $a, b \in \mathbb{Z}$  emanik, beti existituko da  $zkh(a, b)$  ( $a = b = 0$  direnean izan ezik).  $zkh(a, b) = zkh(|a|, |b|)$
5.  $a, b \in \mathbb{Z}$  emanik,  $a \neq 0$  edo  $b \neq 0$ ,  $zkh(a, b)$  izango da  $a$  eta  $b$  zenbakien konbinazio lineal moduan adieraz daitekeen zenbaki oso positiborik txikiena:

$$zkh(a, b) = \min\{|xa + yb : x, y \in \mathbb{Z} \text{ eta } xa + yb > 0\}.$$

6. Aurreko konbinazio linealaren koefizienteak ez dira bakarrak.

$$\begin{aligned} zkh(a, b) &= xa + yb \text{ bada,} \\ zkh(a, b) &= (x + pb)a + (y - pa)b, \quad p \in \mathbb{Z} \end{aligned}$$

ZATIKETA EUKLIDESTARRA 7

## Zatitzaile komunetako handienaren kalkuluoa.

$a, b \in \mathbb{Z}^+$ ,  $b < a$  izanik,  $b | a \Rightarrow zkh(a, b) = b$ .

Oro har, metodo bat behar dugu  $a, b \in \mathbb{Z}^+$  zenbakien  $zkh(a, b)$  kalkulatzeko: Euklidesen algoritmoa.

ZATIKETA EUKLIDESTARRA 8

## Euklidesen algoritmoa

- Euklidesen algoritmoa  $a, b \in \mathbb{Z}^+$  zenbakien  $zkh(a, b)$  kalkulatzeko erabiliko dugu.
- Zatiketa Euklidestarrari esker zera dakigu:  $a, b \in \mathbb{Z}$  emanik,  $b > 0$  izanik,  $\exists | q \in \mathbb{Z}$  zatidura  $\exists | r \in \mathbb{Z}$  hondarra non  $a = qb + r$  den,  $0 \leq r < b$ .

Beraz,

$$\begin{array}{ll} a = q_1 b + r_1, & 0 < r_1 < b; \\ b = q_2 r_1 + r_2, & 0 < r_2 < r_1; \\ r_1 = q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_i = q_{i+2} r_{i+1} + r_{i+2}, & 0 < r_{i+2} < r_{i+1} \\ \vdots & \vdots \\ r_{i+2} & \vdots \\ r_i & \vdots \\ r_3 & \vdots \\ r_1 & \vdots \\ a & \vdots \end{array}$$

EUKLIDESEN ALGORITMOA9

## Euklidesen algoritmoa

Gero eta hondar txikiagoak lortzen ditugunez, noizbait 0 hondarra lortuko dugu:

$$r_{k-1} \mid \frac{r_k}{q_{k+1}} \quad r_{k-1} = q_{k+1} r_k + 0;$$

Hortaz,

$$b > r_1 > r_2 > \dots > r_{k-1} > r_k > 0 (= r_{k+1}).$$

$a, b \in \mathbb{Z}^+$  zenbakien  $zkh(a, b)$ : 0 ez den azkeneko hondarra.

$$\boxed{zkh(a, b) = r_k}$$

## Euklidesen algoritmoa

Ondoko zatiketak egingo ditugu:

$$\begin{array}{ll} a \mid \frac{b}{q_1} & a = q_1 b + r_1, \quad 0 < r_1 < b; \\ r_1 \mid \frac{r_2}{q_2} & b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1; \\ r_2 \mid \frac{r_3}{q_3} & r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2; \\ \vdots & \vdots \\ r_i \mid \frac{r_{i+1}}{q_{i+2}} & r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1}; \\ \vdots & \vdots \\ r_{i+2} & \vdots \\ r_i & \vdots \\ r_3 & \vdots \\ r_1 & \vdots \\ a & \vdots \end{array}$$

EUKLIDESEN ALGORITMOA10

## Multiplo komunetako txikiena

Definizioa (Multiplo komuna)

Izan bitez  $a, b, c \in \mathbb{Z}^+$ , esango dugu  $c$  zenbakia  $a$  eta  $b$  zenbakien multiplo komun bat dela baldin  $a \mid c$  eta  $b \mid c$  bada.

Definizioa (Multiplo komunetako txikiena)

Izan bitez  $a, b, m \in \mathbb{Z}^+$ .  $m$  zenbakia  $a$  eta  $b$  zenbakien multiplo komunetako txikiena dela esango dugu ( $mkt(a, b) = m$ )  $a$  eta  $b$  zenbakien multiplo komunen artean txikiena bada:

1.  $m$  zenbakia  $a$  eta  $b$  zenbakien multiplo komunetako bat da.
2.  $a$  eta  $b$  zenbakien edozein multiplo komun  $m$  baino handiago edo berdina da.

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \Rightarrow m \leq c.$$

Oharra: Euklidesen algoritmoari esker,  $a$  eta  $b$  zenbakien zatitzaien komunetako handiena  $a$  eta bren konbinazio lineal moduan adierazi ahal izango dugu, konbinazio linealaren koefizienteak kalkulatuko ditugulako.

EUKLIDESEN ALGORITMOA11

637 636

MULTIPLIO KOMUNETAKO TXIKIENA12

## Multiplo komunetako trikiiena

Teorema

$a, b, m \in \mathbb{Z}^+$  emanik,  $m = mkt(a, b)$  bada,  $a$  eta  $b$  zenbakien edozein multiplo komun  $m$  zenbakiaren multiplo da:

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \Rightarrow m \mid c.$$

Teorema

$a, b \in \mathbb{Z}^+$  emanik,

$$ab = mkt(a, b) \cdot zkh(a, b).$$

Teorema honi esker  $mkt(a, b)$  kalkulu ahal izango dugu.

MULTIPLIO KOMUNETAKO TRIKIENA 13

ARITMETIKAREN OINARRIZKO TEOREMA 11

## Aritmetikaren oinarrizko teorema

Teorema

Dagoeneko ikusi dugu zenbaki konposatu orok gutxienez zatitzale lehen bat duela. Emaitza hori zabaideko dugu atal honetan. Euklides-en Elementuak-eko IX liburuan honako teorema agertzen da.

Teorema (Aritmetikaren oinarrizko teorema)

Edozein  $n \in \mathbb{Z}^+, n > 1$ , emanik,  $n$  lehena da edo  $n$  zenbaki lehenen biderketa gisa idatz daiteke era bakarrean, faktoreen ordena kontuan izan gabe. ( $n$  lehena bada, bera da faktore lehen bakarra)

ARITMETIKAREN OINARRIZKO TEOREMA 11

## Aritmetikaren oinarrizko teorema

### Aritmetikaren oinarrizko teorema

Aurreko emaitza frogatzeko bi lema hauek erabili ohi dira.

Lema

$a, b, p \in \mathbb{Z}^+$  emanik,  $p$  lehena izanik,

$$p \mid ab \Rightarrow (p \mid a) \text{ edo } (p \mid b).$$

Lema

$a_1, \dots, a_n, p \in \mathbb{Z}^+$  emanik,  $p$  lehena izanik,  
 $p \mid a_1 a_2 \dots a_n \Rightarrow p \mid a_j \quad j \in \{1, \dots, n\}$  baterako.

### Bibliografia

- Matemáticas Discreta y Combinatoria.

Ralph P. Grimaldi.

- Wikipedia.  
[http://es.wikipedia.org/wiki/Teoría\\_de\\_números](http://es.wikipedia.org/wiki/Teoría_de_números)  
[http://es.wikipedia.org/wiki/Factorización\\_de\\_enteros](http://es.wikipedia.org/wiki/Factorización_de_enteros)  
[http://es.wikipedia.org/wiki/Máximo\\_común\\_divisor](http://es.wikipedia.org/wiki/Máximo_común_divisor)  
[http://es.wikipedia.org/wiki/Mínimo\\_común\\_múltiplo](http://es.wikipedia.org/wiki/Mínimo_común_múltiplo)  
[http://es.wikipedia.org/wiki/Identidad\\_de\\_Bezout](http://es.wikipedia.org/wiki/Identidad_de_Bezout)  
• Wikipedia: Euclidesen Elementuak.  
(ikus artikulua euskaraz, gazteleraz eta ingelesez)  
[http://eu.wikipedia.org/wiki/Euklidesen\\_Elementuak](http://eu.wikipedia.org/wiki/Euklidesen_Elementuak)

ARITMETIKAREN OINARRIZKO TEOREMA 15

ARITMETIKAREN OINARRIZKO TEOREMA 16



## Multiplo Komunetako txikienak

$\forall a, b, c \in \mathbb{Z}^+$  izanik  $c$  a eta  $b$ ren multiplo komunea izango da baldin  $a|c$  eta  $b|c$  bado.

Mkt izatello,  $a, b, m \in \mathbb{Z}^+$  izanik,  $mkt(a, b) = m$ , Multiplo komunetako txikiena beda:

1.  $m$   $\neq a$  eta  $b$ -ren Multiplo komunetako bat izango da.

$$a|m \text{ eta } b|m$$

2.  $a$  eta  $b$  zentzakien Multiplo komunen "ordaingo edo berdin" izan behar da.

$$(\forall c \in \mathbb{Z}^+) a|c \text{ eta } b|c \Rightarrow m \leq c$$

$a, b \in \mathbb{Z}^+$  emanik,

$$ab = mkt(a, b) \cdot \text{pkh}(a, b).$$

Hori esker mkt(a, b) kalkuluak izango dugu.

## Aritmetikaren oinarriko teorema

Edozein  $n \in \mathbb{Z}^+$ ,  $n \geq 1$  emanik,  $n$  zentzak lehen edo zentzak lehen gisa idatzitako faktoreen ordena kartzen izan behar da.  $n$  lehen bakoitzean bere faktore lehenak bakoitza.

Bi leme

1.  $a, b, p \in \mathbb{Z}^+$  emanik,  $p$  lehen izanik,

$$p|ab \Rightarrow (p|a) \text{ edo } (p|b)$$

2.  $a_1, \dots, a_n, p \in \mathbb{Z}^+$   $p$  lehen izanik.

$$p|a_1 a_2 \dots a_n \Rightarrow p|a_j \quad j \in \{1, \dots, n\}$$

## Zenbaki lehenak

$n \in \mathbb{Z}^+, n > 1$  n zenbaki lehenak beldin zatitzale positibo baliarrak metal badira.

$$m|n \quad m \in \mathbb{Z}^+ \Rightarrow m=1 \vee m=n$$

teorema

Zenbaki konpositu orokoreko dute zatitzale lehenak bat

$n \in \mathbb{Z}^+ \quad n > 1, n$  konpositua  $\Rightarrow \exists p_i \in \mathbb{Z}^+, p_i$  lehena eta  $p_i | n$ .

## Zatiltza Euclidestarrak

$$a, b \in \mathbb{Z} \quad b > 0$$

(3)  $\exists q \in \mathbb{Z}$   $\exists r \in \mathbb{Z}$  non  $a = qb + r$  den,  $0 \leq r < b$  izanik  
Lo existitzen da de  
baliarrak da

Hondarreko zero eran denez izen,  $\frac{-38}{4} = -6 \frac{2}{4}$ , horrela,  $-38 = -6 \cdot 2 + 4 = -42 + 4 = -38$

## Zatiltza euclidestarraren aplikazioak

Zenbaki oso baten beste adierazpen batzuk uzkurtzeko erabili  
deialdago.

Aldb: 6137 zenbakiaren oinarriak?

$$10\text{ oinarri } (6137) = 6 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$$

$$6137 = r_0 \cdot 10^0 + r_1 \cdot 10^1 + r_2 \cdot 10^2 + r_3 \cdot 10^3$$

$$\begin{matrix} " & " & " & " \\ 7 & 3 & 1 & 6 \end{matrix}$$

Nola idatziz 6137 oinarriak?

$$6137 = r_0 + r_1 \cdot 8 + r_2 \cdot 8^2 + r_3 \cdot 8^3$$

$r_k$  horiek zatiltza euclidestarrarekin uzkurtzeko ditugu: Hondarrek.

Adb  $a=3$   $b=6$

$$a|b, 3|6 \quad \exists \frac{6}{3} = 2 \in \mathbb{Z}$$

$b$ -ren Multiplikat =

$$x = -5, -5 \cdot 6 = -30$$

$$3|-30, \exists \frac{-30}{3} = -10 \in \mathbb{Z}$$

5.

$$(a|b) \wedge (a|c) \Rightarrow (\forall x, y \in \mathbb{Z}) \text{ al } xb+yc$$

$$a|bi \Rightarrow \exists k_i \in \mathbb{Z} \text{ al } x_1 b_1 + \dots + x_n b_n, i=1, \dots, n$$

$$\left\{ \begin{array}{l} a|b \Rightarrow \exists k_1 \in \mathbb{Z} \text{ non } b = k_1 \cdot a \\ \text{etc} \end{array} \right. \quad \begin{array}{l} \exists k_1 \in \mathbb{Z} \\ \vdots \\ \exists k_n \in \mathbb{Z} \end{array} \quad xb = xk_1 \cdot a \\ xb + yc = xk_1 \cdot a + yk_2 \cdot a \\ \vdots \\ xb + yc = xk_1 \cdot a + yk_2 \cdot a + zk_3 \cdot a$$

$$a|c \Rightarrow \exists k_2 \in \mathbb{Z} \text{ non } c = k_2 \cdot a \Rightarrow yc = zk_2 \cdot a$$

$$xb + yc = xk_1 \cdot a + yk_2 \cdot a + zk_3 \cdot a$$

$$xb + yc = (xk_1 + yk_2 + zk_3) \cdot a$$

$$xb + yc = k_3 \cdot a$$

$$\exists k_3 \in \mathbb{Z} = xk_1 + yk_2 \text{ non } xb + yc = k_3 \cdot a$$

beso,  $a|xb+yc$

a zahllich  $b$  etc  $c$  aufzitzen bedeu,  $b$ -ren da  $c$ -ren darstellen  
Kombinazio linear gretick ore aufzitzen ditt.

Adb

$$a=2 \quad b=4 \quad c=20$$

$$2|4 \quad \frac{4}{2} = 2 \in \mathbb{Z} \quad \text{Lp } b \text{ etc } c \text{-ren Kombinazio linear}$$

$$2|20 \quad \frac{20}{2} = 10 \in \mathbb{Z}$$

$$\left\{ \begin{array}{l} x = -1 \\ y = 5 \end{array} \right. \quad xb + yc$$

$$-1 \cdot 2 + 5 \cdot 20$$

$$-2 + 100 = 98 \rightarrow 2 \cancel{7} \cancel{6} \quad 98/2 = 49$$

Aufgabe:

$$k_1 = k_2 = 1 \rightarrow b = k_1 \cdot a \text{ etc. } a = k_2 \cdot b \Rightarrow b = a \text{ etc. } a = b$$

etc.

$$k_1 = k_2 = -1 \rightarrow b = k_1 \cdot a \text{ etc. } a = k_2 \cdot b \Rightarrow b = -a \text{ etc. } a = -b$$

Adb

$$a = 2 \quad b = -2$$

$$7 \mid -2 \Rightarrow \exists \frac{-2}{7} = -1 \in \mathbb{Z}$$

$$-2 \mid 2 \Rightarrow \exists \frac{2}{-2} = -1 \in \mathbb{Z}$$

$$3. |a|b) \wedge (b|c) \Rightarrow (a|c)$$

$$\exists k_3 = k_2 \cdot k_1 \in \mathbb{Z} \text{ non } c = k_3 \cdot a$$

$$\left\{ \begin{array}{l} a|b \Rightarrow \exists k_1 \in \mathbb{Z} \text{ non } b = k_1 \cdot a \\ \text{etc.} \\ b|c \Rightarrow \exists k_2 \in \mathbb{Z} \text{ non } c = k_2 \cdot b \end{array} \right. \Rightarrow c = \underbrace{k_2 \cdot k_1 \cdot a}_{\in \mathbb{Z}} \quad \begin{array}{l} k_3 \\ \uparrow \\ \mathbb{Z} \end{array}$$

Adb

$$a = 3 \quad b = 9 \quad c = 18$$

$$\left\{ \begin{array}{l} a|b \Rightarrow 3|9, \exists \frac{9}{3} = 3 \in \mathbb{Z} \\ \text{etc.} \\ b|c \Rightarrow 9|18, \exists \frac{18}{9} = 2 \in \mathbb{Z} \end{array} \right.$$

$$a|c \Rightarrow 3|18, \exists \frac{18}{3} = 6 \in \mathbb{Z}$$

$$4. a|b \Rightarrow (\forall x \in \mathbb{Z}) a|x_b \quad a \neq 0$$

$$a|b \Leftrightarrow \exists k \in \mathbb{Z} \text{ non } b = k \cdot a$$

$$a|x_b \rightarrow \exists k \in \mathbb{Z} \text{ non } x_b = k \cdot a \Rightarrow x_b = k_2 \cdot a \Rightarrow \exists k_2 \in \mathbb{Z} \text{ non } x_b = k_2 \cdot a$$

a  $\mathbb{Z}$ -ebenfalls teilen b und b  $\mathbb{Z}$ -ebenfalls teilen  
multiplikativ gleichzeitig teilen d.h.

$a|x_b$

## Zenbaki teoria

### Zenbaki osotzak

$\mathbb{Z}$  zenbaki osotzak multzoa, batuketea, heurketa eta biderketa berne eraginak, erantzera osoa, kifiketa ez

Zenbaki teoria: Zenbaki osoak arteko zatiketa astertoa.

$$\circ \text{Zenbaki oso positiboa} = \mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\}$$

$$\text{negatiboa} = \mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$$

$$\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}$$

$\mathbb{Z}$  multzoa ordenatua da.

### Zatigarruntasuna

$a, b \in \mathbb{Z}$  a  $\neq 0$  izanik alb egingo dugo baldin  $\exists k \in \mathbb{Z}$  baldin  $b = k.a$ . a b-oan zatitzakoe eta b-aren multiploa.

$$a, b \in \mathbb{Z}^* \text{ ematen, } alb = a \leq b$$

Propietateak

$$1. \quad ||a; ala; a||_0$$

$$||a \Rightarrow \exists k \in \mathbb{Z} \text{ non } a = k \cdot 1 \Rightarrow \exists k \in \frac{a}{1} = a \in \mathbb{Z}$$

$$a||_0 \Rightarrow \exists k \in \mathbb{Z} \text{ non } a = k \cdot a \Rightarrow \cancel{\exists k = 1 \in \mathbb{Z}}$$

$$a||_0 \Rightarrow \exists k \in \mathbb{Z} \text{ non } 0 = k \cdot a \Rightarrow \exists k = 0 \in \mathbb{Z}$$

$$2. \quad (alb) \wedge (b|a) \Rightarrow b|a \quad \forall a = -b$$

$$a \neq 0 \quad b \neq 0$$

$$alb \Rightarrow \exists k_1 \in \mathbb{Z} \text{ non } b = k_1 \cdot a$$

etc

$$b|a \Rightarrow \exists k_2 \in \mathbb{Z} \text{ non } a = k_2 \cdot b \Rightarrow a = \underbrace{k_1 k_2}_{1} \cdot a$$

berdinaz egia izatello  $k_1 \cdot k_2 = 1$  izan behar du.

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$\text{Indesp} \\ |A \cap B \cap C|$$

## Multzo baten partizioe

A multzoaren partizioe A-ren azpimultzo ez-hutsen familie bat da, non azpimultzo hauak elkarren artean disjuntuak diren eta gurekin bildura A den.

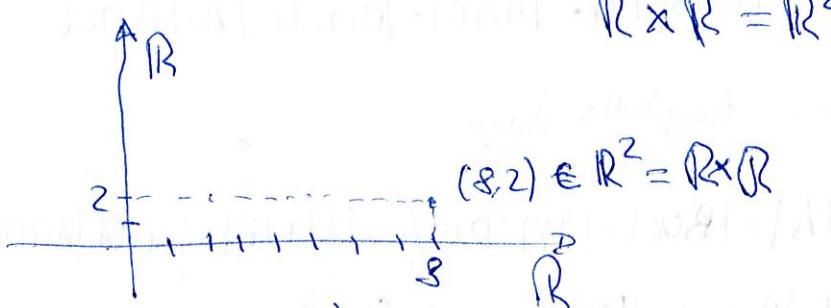
$$P = \{A_i / i \in I\} \quad I: \text{indize multzoa}$$

## Biderkadura kartelesia

A eta B multzoen biderkadura kartelesia  $(x, y)$  billete ordenuen multzoa da, non

$$A \times B := \{(x, y) : x \in A \text{ eta } y \in B\}$$

Adib



Adib

$$A = \{a, b\} \quad B = \{1, 2, 3\}$$

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

$$B \times A = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$$

DeM frogapene

$$A^c \cap B^c \subseteq (A \cup B)^c$$

$$\forall x \in A^c \cap B^c \stackrel{\text{def}}{\Rightarrow} \begin{cases} x \in A^c \\ x \in B^c \end{cases} \stackrel{\text{def}}{\Rightarrow} \begin{cases} x \notin A \\ x \notin B \end{cases} \stackrel{\text{def}}{\Rightarrow} x \notin A \cup B \stackrel{\text{def}}{\Rightarrow} x \in (A \cup B)^c$$

Bantze - proprietatea

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Berdinell direkte frogatello  $\subseteq$  cte  $\geq$  lastu beler ditugu

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C), \supseteq$$

$$\forall x \in A \cap (B \cup C) \stackrel{\text{def}}{\Rightarrow} \begin{cases} x \in A \\ x \in (B \cup C) \end{cases} \stackrel{\text{def}}{\Rightarrow} \begin{cases} x \in A \\ x \in B \\ x \in C \end{cases} \stackrel{\text{def}}{\Rightarrow} \begin{cases} x \in A \cap B \\ x \in A \cap C \end{cases} \stackrel{\text{def}}{\Rightarrow} x \in (A \cap B) \cup (A \cap C)$$

Kontaketa

A eta B izanile

$$|A \cup B| = |A| + |B| - |A \cap B|$$

A, B eta C

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Lehengangoe jallinde bigarren frogatello dugu.

$$|A \cup B \cup C| = |A \cup (B \cup C)| = |A| + |B \cup C| - |A \cap (B \cup C)| = |A| + |B| + |C| - |A \cap (B \cup C)|$$

$$= |A| + |B| + |C| - |(A \cap B) \cup (A \cap C)| - |B \cap C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|)$$

eller  
 $A \cap (B \cap C)$

frik  
 $A \cap (A \cap B) \cap C$

eller  
 $A \cap A \cap B \cap C$

Azpi multzoa propio

A multzoa B-en azpi multzoa propio de,  $A \neq B$ ,  $A \subseteq B$  etc  $A \neq B$

Potentzia multzoa

Aren "potentzia multzoa  $P(A)$ , A-ren azpi multzoa guztien

Batura...

$$\text{Adb: } C = \{1, 2, 3\}$$

$$P(C) = \{\emptyset, \{1\}, \{2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} = C\}$$

$$\text{Adb: } U = \{1, 2, 3, 4, 5, 6, x, y, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}\}$$

$$|U| = 11$$

$$A = \{1, 2, 3, 4\}$$

$$|A| = 4$$

$$B = \{5, 6, x, y, A\}$$

$$|B| = 5$$

$$A \in B, \{A\} \subseteq B, \{A\} \subset B, \{A\} \in B, A \subseteq B, A \subset B$$

Multzo - eragiketakoak

A eta B-ren bidezko  $A \cup B := \{x : x \in A \text{ edo } x \in B\}$

A eta B-ren ebalidura  $A \cap B := \{x : x \in A \text{ eta } x \in B\}$

A-ren osagiria B-n ( $A \subseteq B$  izenik)

$$A^c = \bar{A} := \{x : x \in B \text{ eta } x \notin A\}$$

Propietateak:

$$\text{Def: } (A \cup B)^c = A^c \cap B^c$$

Berdintza frogatzeko  $\subseteq$  eta 2 frogatu behar da

$$(A \cup B)^c \subseteq A^c \cap B^c$$

$$\forall x \in (A \cup B)^c \xrightarrow{\text{def}} x \notin A \cup B \xrightarrow{\text{Bildur. def}} \begin{cases} x \notin A \Rightarrow x \in A^c \\ x \notin B \Rightarrow x \in B^c \end{cases} \xrightarrow{\text{ebalidura}} x \in A^c \cap B^c$$



A eta B-en eragiketakoak  
elementu guztiek dantza  
 $A \cap B = \emptyset$

## Multzoen teoria

Multzoa ondo definitutako objektuen <sup>edo elementuen</sup> bilduma da.

Multzoako elementu guztiek ematen, edo propietate horri betetzen duten elementu bat emanez, definitu ditzake.

Adb

"Lehenengo 5 oso positiboen multzoa"

$$A = \{1, 2, 3, 4, 5\}$$

$$A = \{x \in \mathbb{Z} / 1 \leq x \leq 5\}$$

Multzoak hizki lerriz: A, B, ...

Multzoako elementuak hizki xehes: a, b, c, ...

x, A multzoako elementua dela esatuko,  $x \in A$ . Ez da goela  
esateko  $x \notin A$

$\emptyset$ , ez da dagoen multzoa, hots.  $\emptyset = \{\}$

U, Unibertsoko zenbalki guztiek

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$$
 zenbalki oso positiboa

Multzoaren kardinala

A multzoa finitua bada, A multzoako elementu kopurua itzenean  
Kardinala izango da.  $|A|$  Adb:  $A = \{1, 2, 3, 2\}$

Azpinmultzoa

$$|A| = 3$$

A multzoa B multzoaren azpinmultzoa d. (A parte B),  $A \subseteq B$ , baldin  
 $x \in A \Rightarrow x \in B$ .

Multzo berdinak

Bi multzo berdinak dire,  $B = A$  ordena.  $A \subseteq B$  eta  $B \subseteq A$



## Multzo baten partizioa

Definizioa ( $A$  multzoaren partizioa)

$A$  multzoaren partizioa  $A$ -ren azpimultzo ez-hutsen familia bat da, non azpimultzo hauek elkarren artean disjuntuak diren eta guztiendikura  $A$  den.

$$\mathcal{P} = \{A_i : i \in I\} \quad (I : \text{indize multzoa})$$

- $(\forall i \in I) \quad \emptyset \neq A_i \subseteq A$  azpimultzo ez-hutsak.
  - $(\forall i, j \in I) \quad A_i \neq A_j \Rightarrow A_i \cap A_j = \emptyset$
  - $\bigcup_{i \in I} A_i = A$ .
- $A_i$ : partizioaren klaseak.

## Biderkadura kartesiarra

Definizioa ( $A$  multzoaren partizioa)

$A$  multzoaren partizioa  $A$ -ren azpimultzo ez-hutsen familia bat da, non azpimultzo hauek elkarren artean disjuntuak diren eta guztiendikura  $A$  den.

Definizioa ( $B$  multzoaren biderkadura kartesiarra)

$A$  eta  $B$  multzoen biderkadura kartesiarra  $(x, y)$  bikote ordenatuena multzoa da, non

$$A \times B := \{(x, y) : x \in A \text{ eta } y \in B\}$$

$$\text{Ez nahastu: } (a, b) \neq (b, a), \quad \{a, b\} = \{b, a\}$$

## Aurkibidea

### Multzoen teoria

Multzoak eta Azpimultzoak

Irakasgai: Matematika Diskretua

Titulazioa: Informatikaren Ingeniaritzako Gradua  
Informatika fakultatea  
Donostia

1

Multzo baten partizioa  
Biderkadura kartesiarra

### Multzoak

Definizioa (Multzoa)

Ondo definitutako objektuen bilduma multzoa dela esaten da.

Objektuak elementu deituko ditugu.

Multzoa bi eratara defini dezakegu:

- Multzoko elemento guztiak emanaz.
- Multzoko elementuek betetzen duten propietatea adieraziz.
- Multzo batean elementuen ordena ez da kontuan hartzen, eta multzoko elementuak ematean ez ditugu errepikatuko. Horregatik,  $\{a, b\} = \{b, a\} = \{b, b, a, b\}$

Notazioa:

- Multzoak hizki larri:  $A, B, C, X, \dots$ .
- Multzoko elementuak hizki xehez:  $a, b, c, x, \dots$ .

- $x$  elementua  $A$  multzokoa dela adierazteko:  $x \in A$  ( $x$  barne  $A$ ). Ez dela:  $x \notin A$ .

MULTZOAK ETA AZPIMULTZOAK

2

### Multzoak eta azpimultzoak

Notazio berezia duten multzo batzuk:

- $\emptyset$ : Multzo hutsa, elementurik ez duen multzoa.  $\emptyset = \{ \}$
- $U$ ; Unibertsoa, testuinguru bateko elementu guztiak multzoa
- $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$  zenbaki osoen multzoa
- $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$  zenbaki oso positiboen multzoa
- $\mathbb{N} = \{0, 1, 2, \dots\}$  zenbaki arrunten multzoa
- $\mathbb{R}$  zenbaki errealeen multzoa

Definizioa (Multzoaren kardinala)

A multzo finitu izanik, A multzoak duen elementu kopurua Aren kardinala dela esango dugu eta  $|A|$  notazioaz adieraziko dugu.

Definizioa (Azpimultzoa)

A multzoa B multzoaren azpimultzo dela esango dugu (A parte  $B$ ),  $A \subseteq B$ , baldin  $\forall x \in A \implies x \in B$ .

MULTZOAK ETA AZPIMULTZOAK

## Multzoak eta azpimultzoak

Multzoen arteko erlazioak adierazteko Venn diagramak erabiltzen dira.  $A$  multzoa izanik,  $\emptyset \subseteq A$ ,  $A \subseteq U$ ,  $A \subseteq A$

*Definizioa (Multzo berdinak)*

Bi multzo  $A$  eta  $B$  berdinak dira,  $A = B$ , baldin elementu berberak badituzte, hau da  $A \subseteq B$  eta  $B \subseteq A$ .

*Definizioa (Azpimultzo propioa)*

A multzoa  $B$  multzoaren azpimultzo propioa da baldin  $A \subset B$ , hau da,  $A \subseteq B$  eta  $A \neq B$ .

*Definizioa (Potentzia multzoa)*

A multzoa izanik,  $A$ -ren potentzia multzoa,  $\mathcal{P}(A)$ ,  $A$ -ren azpimultzo guztien bilduma da.

MULTZOAK ETA AZPMULTZOAK5

## Multzo-eragiketak

$A$  eta  $B$  bi multzo izanik,

- $A$  eta  $B$ -ren bildura.  $A \cup B := \{x : x \in A \text{ edo } x \in B\}$
- $A$  eta  $B$ -ren ebakidura.  $A \cap B := \{x : x \in A \text{ eta } x \in B\}$  A eta  $B$  multzoek elementu komunik ez badute disjuntuak direla esango dugu,  $A \cap B = \emptyset$
- $A$  eta  $B$ -ren differentzia.  $B - A := \{x : x \in B \text{ eta } x \notin A\}$
- $A$ -ren osagarria  $B - n$  ( $A \subseteq B$  izanik).

$$A^C = \overline{A} := \{x : x \in B \text{ eta } x \notin A\}$$

MULTZO-ERAGIKETAK6

## Propietateak:

$A, B$  eta  $C$  multzoak izanik, honako propietateak betetzen dira.

• Trukakortze-proprietatea.

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned}$$

• Elkartzze-proprietatea.

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned}$$

• Banatze-proprietatea.

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

• De Morgan-en legeak.

$$\begin{aligned} (A \cup B)^C &= A^C \cap B^C \\ (A \cap B)^C &= A^C \cup B^C \end{aligned}$$

MULTZO-ERAGIKETAK7

## Propietateak:

- Idenpotentzia.
 
$$\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}$$
- Beste propietate batzuk.

$$\begin{array}{lll} A \cup U = U & A \cap U = A & U^C = \emptyset \\ A \cup A^C = U & A \cap A^C = \emptyset & \emptyset^C = U \\ A \cup \emptyset = A & A \cap \emptyset = \emptyset & (A^C)^C = A \\ A \subseteq A \cup B & A \cap B \subseteq A & \end{array}$$

$A$  eta  $B$  finituak izanik,  $|A \cup B| = |A| + |B| - |A \cap B|$   
 $A$  eta  $B$  disjuntuak badira,  $|A \cup B| = |A| + |B|$

$$\begin{aligned} A, B \text{ eta } C \text{ izanik, } |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \end{aligned}$$

PROPIETATEAK7