Zenbaki Teoria

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

Zenbaki teoria. Zenbaki osoak.

- Zenbaki osoen multzoa: $\mathbb{Z}$
- $\mathbb{Z}$ multzoan batuketa, kenketa eta biderketa barne eragiketak dira (emaitza 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: $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$
  - $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}$
- 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

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 zatitzaile 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. $1 \mid a; \quad a \mid a; \quad a \mid 0.$ $\qquad (a \neq 0)$
2. $(a \mid b) \wedge (b \mid a) \Rightarrow a = b \vee a = -b.$ $\qquad (a \neq 0, b \neq 0)$
3. $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c.$ $\qquad (a \neq 0, b \neq 0)$
4. $a \mid b \Rightarrow (\forall x \in \mathbb{Z}) \; a \mid xb.$ $\qquad (a \neq 0)$
5. $(a \mid b) \wedge (a \mid c) \Rightarrow (\forall x, y \in \mathbb{Z}) \; a \mid xb + yc$ $\qquad (a \neq 0)$
   $a \mid b_i \Rightarrow \forall x_i \in \mathbb{Z} \quad a \mid x_1 b_1 + \cdots + x_n b_n, \quad i = 1, \cdots, n$

Zatigarritasuna. Zenbaki lehenak

Definizioa (Zenbaki lehena)

Izan bedi $n \in \mathbb{Z}^+$, $n > 1$. n zenbaki lehena dela esango dugu bere zatitzaile positibo bakarrak n eta 1 badira:
$m \mid n, \quad m \in \mathbb{Z}^+ \implies m = 1 \vee m = n.$
n zenbakia lehena ez bada konposatua dela esango dugu:
$\exists m_1, m_2 \in \mathbb{Z}^+$ non $n = m_1 m_2, \quad 1 < m_1 < n, \; 1 < m_2 < n.$

Teorema
Zenbaki konposatu orok zatitzaile lehenen bat dauka.

$$n \in \mathbb{Z}^+, n > 1, n \text{ konposatua} \implies \exists p \in \mathbb{Z}^+, \, p \text{ lehena eta } p \mid n.$$

Teorema (Euklides, Elementuak, IX, 20)

Infinitu zenbaki lehen daude.

Zatiketa Euklidestarra

Teorema (Zatiketa Euklidestarra)
$a, b \in \mathbb{Z}$ emanik, $b > 0$ izanik,

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

q zatidura da, r hondarra, a zatikizuna eta b zatitzailea.

Definizioa (Zatitzaile komuna)
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 $c \mid a$ eta $c \mid b$ betetzen badira.

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:
$$d \mid a \text{ eta } d \mid b;$$
2. a eta b zenbakien edozein zatitzaile komunek d zatitzen badu:
$$(\forall c \in \mathbb{Z}^+) \quad c \mid a, \quad c \mid b \Rightarrow c \mid d.$$

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

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, $zkh(a, 0) = \mid a \mid$.
4. $a, b \in \mathbb{Z}$ emanik, beti existituko da $zkh(a, b)$ ($a = b = 0$ direnean izan ezik). $zkh(a, b) = zkh(\mid a \mid, \mid b \mid)$
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:
$$zkh(a, b) = \text{mín}\{xa + yb \ : \ x, y \in \mathbb{Z} \ \text{ eta } \ xa + yb > 0\}.$$
6. Aurreko konbinazio linealaren koefizienteak ez dira bakarrak.
$zkh(a, b) = xa + yb$ bada,
$zkh(a, b) = (x + pb)a + (y - pa)b, \ p \in \mathbb{Z}$

Zatitzaile komunetako handiena

Definizioa
$a, b \in \mathbb{Z}$ emanik, esango dugu a, b zenbakiak zenbaki lehen erlatiboak direla $zkh(a, b) = 1$ denean.

Ondorioa.
$a, b \in \mathbb{Z}$
a, b lehen erlatiboak $\iff \exists x, y \in \mathbb{Z}$ non $xa + yb = 1$ den.
Oro har, $d = xa + yb, \quad x, y \in \mathbb{Z} \implies d \geq zkh(a, b)$.

Zatitzaile komunetako handienaren kalkulua.
$a, b \in \mathbb{Z}^+$, $b < a$ izanik, $b \mid a \implies zkh(a, b) = b$.
Oro har, metodo bat behar dugu $a, b \in \mathbb{Z}^+$ zenbakien $zkh(a, b)$ kalkulatzeko: Euklidesen algoritmoa.

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, $\exists \mid q \in \mathbb{Z}$ zatidura $\exists \mid r \in \mathbb{Z}$ hondarra non $a = qb + r$ den, $0 \le r < b$.

Beraz,

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

Euklidesen algoritmoa

Ondoko zatiketak egingo ditugu:

$$
\begin{array}{r|l}
a & b \\ \hline
r_1 & q_1
\end{array}
\qquad a = q_1 b + r_1, \qquad 0 < r_1 < b;
$$

$$
\begin{array}{r|l}
b & r_1 \\ \hline
r_2 & q_2
\end{array}
\qquad b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1;
$$

$$
\begin{array}{r|l}
r_1 & r_2 \\ \hline
r_3 & q_3
\end{array}
\qquad r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2;
$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$
\begin{array}{r|l}
r_i & r_{i+1} \\ \hline
r_{i+2} & q_{i+2}
\end{array}
\qquad r_i = q_{i+2} r_{i+1} + r_{i+2}, \qquad 0 < r_{i+2} < r_{i+1};
$$

$$\vdots \qquad \vdots \qquad \vdots$$

Euklidesen algoritmoa

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

$$
\begin{array}{r|l}
r_{k-1} & r_k \\ \hline
0 & q_{k+1}
\end{array}
\qquad r_{k-1} = q_{k+1} r_k + 0;
$$

Hortaz,

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

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

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

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

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.

$$a \mid m \;\text{ eta }\; b \mid m.$$

2. a eta b zenbakien edozein multiplo komun m baino handiago edo berdina da.

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

Multiplo komunetako txikiena

Teorema
$a, b, m \in \mathbb{Z}^+$ emanik, $m = mkt(a, b)$ bada, a eta b zenbakien edozein multiplo komun m zenbakiaren multiploa 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 $mkt(a, b)$ kalkulatu ahal izango dugu.

Aritmetikaren oinarrizko teorema

Dagoeneko ikusi dugu zenbaki konposatu orok gutxienez zatitzaile lehen bat duela. Emaitza hori zabalduko 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

Aurreko emaitza frogatzeko bi lema hauek erabili ohi dira.

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

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

Lema
$a_1, \dots, a_n, p \in \mathbb{Z}^+$ emanik, p lehena izanik,

$$p \mid a_1 a_2 \cdots a_n \Longrightarrow p \mid a_j \quad j \in \{1, \cdots, n\} \text{ baterako.}$$

Bibliografia

- Matemáticas Discreta y Combinatoria.
  Ralph P. Grimaldi.
- Wikipedia.
  http://es.wikipedia.org/wiki/Teoría_de_números
  http://es.wikipedia.org/wiki/Factorización_de_enteros
  http://es.wikipedia.org/wiki/Máximo_común_divisor
  http://es.wikipedia.org/wiki/Mínimo_común_múltiplo
  http://es.wikipedia.org/wiki/Identidad_de_Bezout
  http://es.wikipedia.org/wiki/División_por_tentativa
- Wikipedia: Euklidesen Elementuak.
  (ikus artikulua euskaraz, gazteleraz eta ingelesez)
  http://eu.wikipedia.org/wiki/Euklidesen_Elementuak