6. Gaia: Zatigarritasuna

Kapitulu honetan zenbaki osoekin egingo dugu lan. Gogoratu zenbaki arrunten multzoa $\mathbb{N} = \{1, 2, \dots\}$ dela eta zenbaki osoen multzoa $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Zenbaki arrazionalak ere agertuko dira. Horien multzoa $\mathbb{Q} = \{m/n : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\}$ da.

6.1 Zatitzaileak eta multiploak

Zenbaki osoen teorian zatigarritasunarena oinarrizko kontzeptuetariko bat da. Eta zenbaki osoen zatiketa hondarrarekin ere funtsezkoa da.

Definizioa 6.1.1. Izan bitez $a, b \in \mathbb{Z}$. Orduan, a b-ren *zatitzailea* da, eta a-k b zatitzen duela diogu, existitzen bada $k \in \mathbb{Z}$ zeinetarako $b = ak$ betetzen den.

Baldin a b-ren zatitzailea bada, b a-ren *multiploa* dela esaten da, baita b a-rekin zatigarria dela ere. Notazioa: $a \mid b$ idatziko dugu a b-ren zatitzailea dela adierazteko.

Proposizioa 6.1.2. *Izan bitez $a, b, c \in \mathbb{Z}$. Orduan,*

(i) $a \mid a$ *eta* $1 \mid a$, $\forall a \in \mathbb{Z}$.

(ii) $a \mid 0$, $\forall a \in \mathbb{Z}$.

(iii) $a \mid b$ *eta* $b \mid a$ *dira, baldin eta soilik baldin* $b = \pm a$ *bada.*

(iv) $a \mid b$ *eta* $b \mid c$ *badira, orduan* $a \mid c$ *da.*

(v) $a \mid b$ *eta* $a \mid c$ *badira, orduan* $a \mid nb + mc$ *da edozein* $m, n \in \mathbb{Z}$*-rako.*

Froga. (i) $a = a1$ dela ohartzea besterik ez da.

(ii) $0 = a0$ da $a \in \mathbb{Z}$ edozein izanik.

(iii) $ac = b$ eta $bd = a$ direnez, $acbd = ab$ dugu, eta sinplifikatuz, $cd = 1$. Beraz, c eta d-rako aukera bakarra biak 1 edo biak -1 izatea da. Kasu bakoitzean $b = a$ edo $b = -a$ lortzen da hurrenez hurren.

(iv) $b = ad$ eta $c = be$ ditugu, beraz, $c = a(de)$. Orduan, $a \mid c$.

(v) $b = ad$ eta $c = ae$ ditugu, beraz, $nb + mc = a(nd + me)$. □

Oharra 6.1.3. Proposizioa nahiz eta $\mathbb{Z}$-rako enuntziatu dugun, $\mathbb{N}$-rako ere enuntzia daiteke. Alegia, zatigarritasuna $\mathbb{N}$-koentzat soilik definituko bagenu, $a, b \in \mathbb{N}$ izanik $a \mid b$ baldin eta existitzen bada $c \in \mathbb{N}$ non $b = ac$ den. Orduan lehen hiru atalek honakoa diote: $a \mid a$ oraindik egia da. Kasu honetan $a \mid b$ eta $b \mid a$ badira, orduan $a = b$ eta $a \mid b$ eta $b \mid c$ badira $a \mid c$ dugu. Hau da, erlazio erreflexibo, antisimetriko eta trantsitibo bat dugu. Beraz, zatigarritasuna ordena erlazio bat da $\mathbb{N}$-n.

Gainera, $\mathbb{N}$-n ari garenean, zenbaki denak positiboak direnez, badakigu $n = ab$ baldin bada $1 \leq a, b \leq n$ direla. Eta jakingo bagenu, adibidez $1 < a < n$ dela, orduan derrigorrez $1 < b < n$ izango dugu. Hau baliagarria izango zaigu aurrerago.

Definizioa 6.1.4. $p \in \mathbb{N} \setminus \{1\}$ *lehena* da ez bada bera baino txikiago diren zenbaki biren biderkadura. Bestela esanda, p-ren zatitzaile bakarrak 1 eta p badira. Zenbaki arrunt bat *konposatua* da, lehena ez bada.

Horrela, 7 eta 17 lehenak dira, baina $8 = 2 \times 4$ eta $15 = 3 \times 5$ konposatuak dira. Lehen oharrean esandakoaren haritik, zenbaki natural bat konposatua bada, bera baino hertsiki txikiagoak diren bi zenbakiren biderkadura gisa idatz daiteke. Eta jakina, horrela idatz badaiteke konposatua izango da.

6.1.1 Zatiketaren algoritmoa

Proposizioa 6.1.5. *Izan bitez $a, b \in \mathbb{Z}$ non $b > 0$ den. Orduan existitzen dira $q, r \in \mathbb{Z}$ bakarrak non:*

$$a = bq + r \quad eta \quad 0 \leq r < b.$$

Froga. Izan bedi $S = \{n \in \mathbb{Z} \mid n = a - bx, \text{ non } x \in \mathbb{Z}\}$ eta $S_0 = \{n \in S \mid n \geq 0\}$; hau da, S-ko elementu ez-negatiboen azpimultzoa. Ohartu S_0 multzoa ez-hutsa dela, $a \geq 0$ baldin bada $a \in S_0$ dugu, $a = a - b \cdot 0$ delako (eta a ez-negatiboa). Aldiz, $a < 0$ bada, $a - b \cdot a \in S_0$ dugu. Izan ere $a - ba = a(1 - b) \geq 0$ da, $a < 0$ eta $1 - b \leq 0$ delako. Beraz, S_0 multzoa ez-hutsa da edozein kasutan.

Izan bedi $r = \min\{s \mid s \in S_0\}$, hau da, S_0-ko elementurik txikiena. [10]. Argi dago $0 \in S_0$ bada orduan $r = 0$ izango dela, eta bestela beste zenbakiren bat izango da, hertsiki positiboa dena.

Orain, $r \in S_0$ denez, badakigu $r = a - bq$ dela $q \in \mathbb{Z}$-ren batentzako, $r \geq 0$ izanik. Ikus dezagun r ezin dela b baino handiago edo berdina izan. Absurdura eramanez, demagun $r \geq b$. Orduan $r - b = a - bq - b = a - b(q+1) \in S_0$. Baina hau S_0-ko elementu bat da r baino hertsiki txikiagoa dena. Hau ezinezkoa da, r txikiena aukeratu dugulako. Beraz, derrigorrez $0 \leq r < b$ da.

Froga dezagun, azkenik, q eta r bakarrak direla. Demagun existitzen direla q_1 eta r_1 zenbaki osoak $0 \leq r_1 < b$ izanik, non $a = bq_1 + r_1$ den, eta demagun $r \geq r_1$ dela (beste kasua erabat antzera egingo litzateke). Orduan $b(q_1 - q) = r - r_1 \geq 0$ dugu.

Beraz, $q_1 - q \geq 0$ da. Baldin eta $q_1 - q \neq 0$ bada, orduan $r - r_1 \geq b$, baina hau ezinezkoa da $0 \leq r_1, r < b$ direlako. Beraz, derrigorrez $q = q_1$ eta $r = r_1$ dira. □

[10] Ez dugu frogatu, baina $\mathbb{N}$-ren edozein azpimultzo ez-hutsek elementu txikien bat badaukala erabiltzen ari gara hemen. Honi $\mathbb{N}$ ondo ordenatuta egotearen printzipio esaten zaio, eta multzo orokorrentzako axioma bat da. Honi buruz gehiago jakiteko: `https://en.wikipedia.org/wiki/Well-ordering_theorem`

6.2 Zatitzaile komun handiena

Ondoren bi zenbaki osoren zatitzaile komun handienaren definizioa emango dugu. Aurrerago ikusiko dugu ezagun dugun definizioaren baliokidea dela orain emango duguna.

Definizioa 6.2.1. Izan bitez $a, b \in \mathbb{Z}$. Orduan a eta b-ren *zatitzaile komun handiena*, $\text{zkh}(a, b)$ adieraziko duguna d zenbaki oso positiboa da, ondoko bi propietateak betetzen dituena:

(i) $d \mid a$ eta $d \mid b$;

(ii) baldin $c \mid a$ eta $c \mid b$ badira, orduan $c \mid d$.

Ohartu definizioa eman dugula, baina benetan ez litzateke matematikoki erabat zuzena izango definizioa hala ematea. Izan ere, hasteko, ez dakigu halako d-rik existitzen denik, eta gainera, ez dakigu existitzekotan bakarra den. Beraz, egon gintezke multzo hutsa edo elementu bat baino gehiago dauzkan multzo bat definitzen zenbaki bakar baten ordez. Hurrengo teoremak ziurtatzen du eman dugun definizioa zuzena dela matematikoki (behintzat biak zeroren ezberdinak direnean).

Teorema ikusi baino lehen pentsa dezagun zer gertatzen den biak zero edo bietako bat zero denean. Hasteko 0-a edozein zenbakik zatitzen duenez, baldin eta $\text{zkh}(0, 0) = d \neq 0$ balitz, orduan $d + 1$ harturik (ii) ez litzateke beteko. Izan ere $d + 1$-ek ere zatitzen du 0, baina ez du d zatitzen. Horregatik, normalean $\text{zkh}(0, 0) = 0$ bezala definitzen da. Ohartu hau ez datorrela bat gure ohiko definizioarekin, benetan 0 baino askoz zenbaki handiagoek zatitzen dituztelako aldi berean 0 eta 0. Baina beste definizio hau lagungarriagoa da orokorrean, eta bestelako identitate eta propietateek ondo funtzionatzen dute hau horrela definituz. (Ohartu edozein kasutan, beste definizioarekin ere ez genukeela handien bat hautatzeko modurik izango.) Hala ere, autore batzuek definitu gabe uzten dute $\text{zkh}(0, 0)$.

Ikus dezagun orain bietako bat $a = 0$ eta bestea $b \neq 0$ denean zer gertatzen den. Kasu honetan $\text{zkh}(0, b)$-rako bi hautagai dauzkagu: $-b$ eta b. Izan ere, bistakoa da definizioko (i) betetzen dutela biek, eta gainera beste edozein $c \in \mathbb{Z}$ badugu, non $c \mid 0$ (hau benetan ez da baldintza bat denek betetzen dutelako) eta $c \mid b$ betetzen dituena, derrigorrez $c \mid \pm b$. Beraz, bien artean positiboa dena aukeratuko dugu, definizioz zatitzaile komun handiena positiboa dela esan dugulako. Beraz, $\text{zkh}(0, b) = |b|$ izango da.

Teorema 6.2.2. *Izan bitez $a, b \in \mathbb{Z} - \{0\}$. Orduan a eta b-ren zatitzaile komun handiena, d, beti existitzen da eta bakarra da. Gainera, existitzen dira $x, y \in \mathbb{Z}$ non $d = ax + by$ den.*

Froga. Izan bedi $S = \{n \in \mathbb{Z} \mid n = ax + by,\ x, y \in \mathbb{Z} \text{ izanik}\}$. Argi dago $S \subseteq \mathbb{Z}$ dela, ez hutsa dena, $a = a \cdot 1 + b \cdot 0$ eta $b = a \cdot 0 + b \cdot 1$ direlako. Modu antzekoan lor daitezke $-a$ eta $-b$, eta beraz, S-n badaude positiboak diren zenbakiak. Izan bedi $d = \min\{s \mid s \in S \text{ eta } s > 0\}$, hau da, S-ko elementu positiborik txikiena. Frogatuko dugu $d = \text{zkh}(a, b)$ dela.

Hasteko ohartu $d \in S$ dela, eta beraz, existitzen dira $x, y \in \mathbb{Z}$ non $d = ax + by$. Beraz, teoremaren enuntziatuaren azken atala ez dugu frogatu beharko, behin d zatitzaile komun handiena dela frogatu dugunean.

Aplika diezaiegun zatiketaren algoritmoa a eta d-ri. Orduan existitzen dira $q, r \in \mathbb{Z}$ bakarrak, $0 \leq r < d$ izanik, non $a = qd + r$ den. Orain,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + (-yq)b$$

dugunez, horrek esan nahi du $r \in S$ dugula. Baina d zenez S-ko elementu positiborik txikiena, $r = 0$ izatea da aukera bakarra. Eta beraz, $d \mid a$. Argumentu bera a-rekin beharrean b-rekin erabiliz frogatzen da $d \mid b$ dugula.

Definizioko bigarren propietatea frogatzea baino ez zaigu falta. Demagun c badela a eta b-ren zatitzaile komuna (hau da, $c \mid a$ eta $c \mid b$) eta egiazta dezagun derrigorrez $c \mid d$ dela. Bien zatitzaile komuna izateagatik, existitzen dira u eta v non $a = cu$ eta $b = cv$ diren. Baina orduan $d = ax+by = cux+cvy = c(ux+vy)$ dugu, eta beraz, $c \mid d$. □

Definizioa 6.2.3. Izan bitez $a, b \in \mathbb{Z} - \{0\}$. Orduan $d = \text{zkh}(a, b)$ izanik $d = ax + by$ idazkerari *Bézout-en identitatea* esaten zaio.

Ohartu definizio hau bat datorrela guk orain arte ezagutzen genuenarekin. Hau da, $d = zkh(a, b)$, definitu dugun bezala, a eta b-ren zatitzaile komunen artean handiena da. Izan ere, bigarren baldintzak ziurtatzen du beste edozein zatitzailek d zatitu behar duela. Eta d positiboa izanik, edo beste faktore komun hori negatiboa da, eta orduan bistan dago d baino txikiagoa dela, edo positiboa da. Baina positiboa bada $d = ck$ da, hirurak zenbaki naturalak izanik, eta beraz, argi dago $c \leq d$ dela.

Notazioa 6.2.4. Batzuetan, laburtzeko, $\text{zkh}(a, b)$-ren ordez zuzenean (a, b) idatziko dugu a eta b-ren arteko zatitzaile komunetako handiena adierazteko.

Definizioa 6.2.5. *$a, b \in \mathbb{Z}$ elkarren arteko lehenak* dira, $\text{zkh}(a, b) = 1$ bada.

Esaterako, 12 eta 25 elkarren arteko lehenak dira. Ez bata ez bestea ez dira lehenak, ordea.

Oharra 6.2.6. Bi zenbaki $a, b \in \mathbb{Z}$ elkarrekiko lehenak badira, Bézouten identitateak ziurtatzen du existitzen direla $x, y \in \mathbb{Z}$ non $1 = ax + by$ den. Hau egoera askotan oso baliagarria den propietate bat da.

Korolarioa 6.2.7. *Izan bedi $d = \text{zkh}(a, b)$.*

(i) Baldin $n \in \mathbb{Z}$ izanik $n \neq 0$ bada, orduan $\text{zkh}(na, nb) = |n| \,\text{zkh}(a, b)$.

(ii) $\text{zkh}(a/d, b/d) = 1$.

Ariketa 6.i. Egin aurreko korolarioaren frogapena.

Korolarioa 6.2.8. *Izan bedi $a \in \mathbb{Z}$ eta p lehena. Orduan $p \mid a$ edo $\text{zkh}(p, a) = 1$.*

Froga. Demagun $\text{zkh}(a, p) = d > 1$ dela. Orduan $d \mid a$ eta $d \mid p$. Baina p-ren zatitzaile bakarrak 1 eta p direnez, derrigorrez $d = p$ izan behar da, eta beraz, $p \mid a$. □

Korolarioa 6.2.9. *(i) Baldin $a \mid bc$ bada eta $\text{zkh}(a, b) = 1$, orduan $a \mid c$.*

(ii) Baldin p lehena bada eta $p \mid ab$, orduan $p \mid a$ edo $p \mid b$.

Froga. (i) Badakigu existitzen direla $x, y \in \mathbb{Z}$ non $1 = ax + by$ dugun. Atal biak c-rekin biderkatuz, $c = axc + byc$. Baina eskuin atala a-ren multiploa da, $a \mid bc$ delako. Beraz, c a-ren multiploa da.

(ii) $p \mid a$ ez bada betetzen, $\text{zkh}(a, p) = 1$ da (p lehena delako), eta (i)-en ondorioz, $p \mid b$ da. □

6.2.1 Euklidesen algoritmoa

Ikusi dugu bi zenbakiren arteko zatitzaile komun handiena existitzen dela eta bakarra dela, baina, nola kalkulatu? Ondoren horretarako algoritmo bat ikusiko dugu. Ondoko lema lagungarri egingo zaigu.

Lema 6.2.10. *Izan bitez $a, b \in \mathbb{Z} - \{0\}$. Demagun existitzen direla q eta r zenbaki osoak non $a = qb + r$ den. Orduan* $\text{zkh}(a, b) = \text{zkh}(b, r)$.

Froga. Izan bitez $d_1 = (a, b)$ eta $d_2 = (b, r)$. Ikus dezagun elkar zatitzen dutela, eta beraz, biak positiboak izatearren, zenbaki bera izango dira.

Batetik, d_2-k b zatitzen duela bistakoa da, definiziotik. Bestalde, d_2-k r ere zatitzen duenez d_2-k zatitzen du b eta r-ren edozein konbinazio. Bereziki, $d_2 \mid bq + r = a$. Beraz, $d_2 \mid a$, eta bien faktore komuna denez, derrigorrez beraien zatitzaile komun handiena zatitzen du. Hau da, $d_2 \mid d_1$.

Orain, d_1-k b zatitzen duela bistakoa da. Baina $r = a - bq$ denez, eta d_1-k a eta b-ren edozein konbinazio zatitzen duenez, d_1-k r zatitzen du. Biak zatitzen dituenez $\text{zkh}(b, r) = d_2$ ere zatitzen du. □

Ohartu, zatitzaile komun handienaren definiziotik berehalakoa dela $\text{zkh}(a, b) = \text{zkh}(a, -b) = \text{zkh}(-a, b) = \text{zkh}(-a, -b)$. Beraz, nahikoa da $a, b > 0$ diren kasuan kalkulatzen jakitearekin.

Izan bitez a, b bi zenbaki oso positibo eta demagun $a > b$. Zatiketaren algoritmoa behin eta berriz aplikatzen badugu, ondokoa lortuko dugu:

$$\begin{aligned}
a &= bq_1 + r_1, && \text{non} \quad q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < b,\\
b &= r_1 q_2 + r_2, && \text{non} \quad q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, && \text{non} \quad q_3, r_3 \in \mathbb{Z}, 0 \leq r_3 < r_2,\\
&\vdots
\end{aligned}$$

Prozedura hau momenturen batean amaituko da, hondarrak beti hertsiki txikiagoak direlako. Beraz, momenturen baten egoera honetan egongo gara:

$$\begin{aligned}
r_{n-2} &= r_{n-1} q_n + r_n, && \text{non} \quad q_n, r_n \in \mathbb{Z}, 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, && \text{non} \quad q_{n+1}, r_{n+1} \in \mathbb{Z}, r_{n+1} = 0.
\end{aligned}$$

Aurreko lemagatik, ondoko katea daukagu

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Beraz, azken hondar ez nulua a eta b-ren zatitzaile komun handiena izango da.

Adibidea 6.2.11. Kalkula dezagun $\text{zkh}(1479, 272)$.

- $1479 = 272 \times 5 + 119$;
- $272 = 119 \times 2 + 34$;
- $119 = 34 \times 3 + 17$;

- $34 = 17 \times 2$.

Ondorioz, zkh$(1479, 272) = 17$ izango da.

Euklidesen algoritmoak, zatitzaile komun handiena kalkulatzeko modu bat ez ezik, zatitzaile komun handiena a eta b-ren konbinazio gisa nola idatzi jakiteko prozedura ematen digu. Alegia, Bézout-en identitatea lortzeko prozedura bat ematen digu.

Izan ere, zatiketaren algoritmoa erabiliz, hondar bakoitza aurrekoen konbinazio gisa idatz dezakegu. Prozedura hori errepika dezakegu a eta b-ra iritsi arte. Aurreko adibidearekin ikus dezagun.

Lehen ikusi dugu zkh$(1479, 272) = 17$, Euklidesen algoritmoaren laguntzaz. Hango kalkuluak erabiliz,

$$\begin{aligned} 17 &= 119 - 3 \times 34 = 119 - 3 \times (272 - 2 \times 119) = 7 \times 119 - 3 \times 272 \\ &= 7 \times (1479 - 5 \times 272) - 3 \times 272 = 7 \times 1479 - 38 \times 272. \end{aligned}$$

Beraz, Bézouten identitatea kasu honetan $17 = 7 \times 1479 - 38 \times 272$ da.

6.3 Zenbaki lehenak eta aritmetikaren oinarrizko teorema

Gorago esan dugunez, zenbaki lehen bat ez da bera baino zenbaki txikiagoen biderkadura.

Lema 6.3.1. *Izan bedi $n \in \mathbb{N}$ non $n \geq 1$. Baldin eta n konposatua bada, existitzen dira $1 < a, b < n$ non $n = ab$ den.*

Froga. Badakigu n konposatua dela, beraz ez da lehena. Orduan existitzen da n-ren zatitzaile bat ez dena ez 1 ez n, demagun a. Horrek esan nahi du $n = ab$ dela b-ren batentzat. Orain, zenbaki naturalekin ari garenez, $1 < a < n$ bistakoa da, eta b hala dela ere bai. □

Proposizioa 6.3.2. *Izan bedi $n \in \mathbb{N}$. Baldin eta $n > 1$ bada, orduan n zenbaki lehenen batek zatitzen du.*

Froga. Izan bedi

$$T = \{n \in \mathbb{N} \mid n > 1 \text{ eta } n \text{ ez du zenbaki lehen batek ere zatitzen}\}$$

multzoa. Ikusi nahi duguna da $T = \emptyset$ dela. Absurdura eramanez, demagun ezetz, demagun $T \neq \emptyset$. Orduan, existitzen da $n_0 = \min\{t \mid t \in T\}$ elementu txikien bat. Orain, n_0 ezin da lehena izan, bestela bere buruak (hau da, lehen batek) zatituko luke. Baina orduan konposatua da eta existitzen dira $1 < a, b < n_0$ bi zenbaki arrunt non $n_0 = ab$ den. Orain, $a < n_0$ denez, n_0 ezin da T-n egon. Orduan, T-ren osagarrian dago, hau da, bada zenbaki lehen batengatik zatigarria, demagun p. Baina orduan, $p \mid a$ bada, argi dago $p \mid n_0$ dela, eta kontraesan batera iritsi gara. □

Teorema 6.3.3. *Zenbaki lehenen multzoa infinitua da.*

Froga. Frogapen hau absurdura eramanez egiten da. Demagun zenbaki lehenen multzoa finitua dela, hau da $P = \{p_1, \ldots, p_n\}$ multzoan ditugula zenbaki lehen guztiak. Nahi izanez gero ordenatu ditzakegunez, demagun $p_1 < \cdots < p_n$ dugula. Har dezagun $N = p_1 \ldots p_n + 1$ zenbakia. Bistakoa denez $p_n < N$ da, eta beraz, gure hipotesiaren arabera p_n denez zenbaki lehenik handiena, N ezin da lehena izan.

Baina orduan, N ez bada lehena, aurreko proposizioaren arabera, derrigorrez zenbaki lehenen batek zatitzen du. Demagun $p_i \in P$ dela N zatitzen duen zenbaki lehen bat. Orduan, $N = p_i k$ da $k \in \mathbb{N}$ baterako. Baina horrek esan nahi du $1 = N - p_1 \ldots p_n = p_i(k - p_1 \ldots p_{i-1} p_{i+1} \ldots p_n)$ dela. Hau da, p_i-k 1 zatitzen duela. Baina p_i zenbaki lehena da, bereziki $p_i > 1$, eta beraz, ezin du 1 zatitu. Kontraesan batera iritsi gara. Ondorioz, zenbaki lehen kopurua ezin da finitua izan. □

Eratostenesen bahea

Ez dago zenbaki lehenen zerrendarik. Asko ezagutzen diren arren, oraindik ez dira denak ezagutzen. Hala ere, badago modu sistematiko bat n zenbaki bat baino txikiagoak diren zenbaki lehen guztiak zerrendatzeko (horretarako nahikoa espazio, denbora eta pazientzia izanez gero, jakina). Metodo horri Eratostenes-en bahea edo kriba esaten zaio, eta honela funtzionatzen du:

- Zerrendatu 2-tik n-rako zenbaki guztiak.
- Borobildu 2 zenbakia eta ezabatu 2-ren multiplo guztiak;
- ezabatu gabeko lehen zenbakia, (3-a izango da) borobildu eta, ezabatu haren multiploak;
- errepikatu prozedura ezabatu gabeko hurrengo zenbakiarekin, ezabatu gabeko zenbaki hori $\sqrt{n}$ baino txikiagoa den bitartean;
- $\ldots$;
- ezabatu gabeko lehen zenbakia $\sqrt{n}$ baino handiagoa bada, borobildu ezabatu gabe geratu diren zenbakiak.

Prozedura amaitutakoan borobilduta ageri diren zenbakiak lehenak izango dira, eta ezabatu ditugunak konposatuak.

Ohartu, baldin $n = ab$ bada, $a \leq \sqrt{n}$ edo $b \leq \sqrt{n}$ bete behar dela, biak $\sqrt{n}$ baino handiagoak balira, bien biderkadura n baino handiagoa izango litzatekeelako. Orduan, zenbaki bat $\sqrt{n}$ eta n artean badago, eta ez badago ezabatuta, $\sqrt{n}$ baino txikiagoa den zatitzailerik ez duelako da, baina orduan derrigorrez lehena da.

Hauek dira 2-tik 200-erako zenbaki lehen guztiak:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,$$
$$71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139,$$
$$149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199 \ldots$$

6.3.1 Aritmetikaren oinarrizko teorema

Teorema 6.3.4. *Izan bedi $n \in \mathbb{N} \setminus \{1\}$. Existitzen dira $p_1, p_2, \ldots, p_k$ zenbaki lehenak zeinetarako $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ den. Deskonposaketa hori bakarra da, salbu faktoreen ordena.*

Froga. Indukzio sendoaren printzipioa erabiliz egingo dugu. Argi dago $n = 2$ bada egia dela, 2 lehena delako. Demagun egia dela $2 \leq k < n$ guztietarako eta ikus dezagun n kasua.

Batetik, n lehena bada, bukatu dugu, badaukagulako zenbaki lehenen biderkadura gisa idatzita.

Bestetik, n ez bada lehena, 6.3.1 Lema erabiliz, badakigu $n = ab$ modukoa dela $1 < a, b < n$ izanik. Indukzio hipotesiagatik badakigu a eta b zenbaki lehenen biderkadura gisa adieraz daitezkeela, eta beraz, n ere bai.

Deskonposaketa bakarra dela ikusteko, demagun bi ditugula:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_m.$$

p_1 lehena eta $q_1 \cdot q_2 \cdot \ldots \cdot q_m$ biderkaduraren zatitzailea denez, faktore haueta-ko baten zatitzailea da. Faktore hori lehena denez, p_1-en berdina da. Orduan p_1-ekin zatitu ditzakegu bi aldeak eta arrazoiketa errepikatu p_2-rekin eta hurrengoekin. □

Faktorizazioan errepikatuta agertzen diren faktoreak berretura eran idatzita, honela eman dezakegu deskonposaketa:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_j^{\alpha_j},$$

non p_i guztiak desberdinak diren (are gehiago, nahi izanez gero, adierazpenean ageri diren lehenak ordenatuta eman daitezke: $p_1 < p_2 < \cdots < p_j$) eta $\alpha_1, \alpha_2, \ldots, \alpha_j \in \mathbb{N}$.

Adierazpen honek ondorio honetara garamatza.

Proposizioa 6.3.5. *Edozein $n \neq 0, \pm 1 \in \mathbb{Z}$ modu bakarrean adieraz daiteke ondoko eran:*

$$n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_j^{\alpha_j}$$

non $p_1 < p_2 < \cdots < p_j$ eta $\alpha_i \in \mathbb{N}$ den. Gainera $m \in \mathbb{Z}$ badugu eta $m \mid n$ da, baldin eta soilik baldin

$$m = \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_j^{\beta_j}$$

bada $0 \leq \beta_i \leq \alpha_i$ izanik $i = 1, \ldots, j$ guztietarako.

Proposizio honen bitartez, erraz kalkula dezakegu zenbaki baten zatitzaile-kopurua, faktorizaziotik abiatuta: β_1-erako $\alpha_1 + 1$ aukera ditugu, β_2-rako $\alpha_2 + 1$ aukera, eta abar.

Korolarioa 6.3.6. *Izan bedi $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_j^{\alpha_j}$ non p_i guztiak desberdinak diren. Orduan b-ren zatitzaile-kopurua $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_j + 1)$ da.*

6.4 Zenbakitze-sistemak

Zenbakiak idazteko erabiltzen dugun sistemari *hamartarra* deitzen diogu, 10 zenbakian oinarrituta dagoelako: hamar zifra (digitu) erabiltzen ditugu, 0-tik 9-ra, eta posizioaren araberako balioa 10-en berreturen bidez lortzen da. Adibidez, 108 zenbakia honela adierazi ohi dugu

$$108 = 1 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0.$$

Baina sistema horretan 10 oinarriak duen eginkizuna, 1 baino handiagoa den beste edozein zenbakik bete dezake.

Proposizioa 6.4.1. *Izan bedi $b \geq 2$, oinarria deituko duguna. Edozein $n \in \mathbb{N}$ zenbaki arrunt, era bakar batean adieraz daiteke*

$$n = a_m b^m + \cdots + a_1 b + a_0$$

moduan $a_i \in \{0, 1, \ldots, b-1\}$ izanik eta $a_m \neq 0$. Orduan $n = (a_m a_{m-1} \ldots a_1 a_0)_b$ idatziko dugu.

Froga. Nahikoa da zatiketaren algoritmoa behin eta berriz aplikatzea. Lehen urratsean $n = n_1 b + a_0$ lortuko dugu, $a_0 \in \{0, \ldots, b-1\}$ bakarra izanik. Baldin eta $n_1 < b$ baldin bada, bukatu dugu, bestela, $n_1 = n_2 b + a_1$ izango dugu, $a_1 \in \{0, \ldots, b-1\}$ izanik, eta n_1 ordezkatuz n-rentzako nahi dugun moduko adierazpena lortzen dugu. Prozesua errepikatuz n_m txikitzen goazenez, uneren batean b baino txikiagoa izango da, eta momentu horretan lortuko dugu n-ren aipaturiko adierazpena. □

Adibidea 6.4.2. Demagun 1025 zenbakia 7 oinarrian adierazi nahi dugula. Nahikoa da frogapeneko prozedura jarraitzea. $1025 = 146 \cdot 7 + 3$ da, beraz, $a_0 = 3$ izango da. Ondoren, $146 = 20 \cdot 7 + 6$ dugu, eta azkenik $20 = 2 \cdot 7 + 6$. Ondorioz,

$$1025 = 146 \cdot 7 + 3 = (20 \cdot 7 + 6) \cdot 7 + 3 = ((2 \cdot 7 + 6) \cdot 7 + 6) \cdot 7 + 3,$$

eta faktore komunak aterata

$$1025 = 2 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7 + 3 = (2663)_7.$$