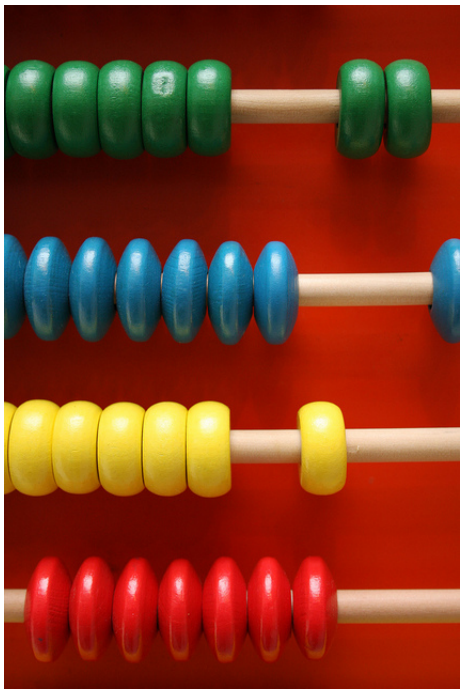
MATEMATIKARAKO SARRERA

OCW 2015



Leire Legarreta Solaguren
EHU-ko Zientzia eta Teknologia Fakultatea
Matematika Saila

4 GAIA: ZATIGARRITASUNA

Zenbaki osoak. Zatiketaren algoritmoa. Zenbatzeko sistemak. Zatitzaile komunetako haundiena eta Euclides-en algoritmoa. Zenbaki lehenak eta Eratóstenes-en kriba. Aritmetikako oinarrizko teorema

1 Zenbaki osoak

Zenbakien oinarrizko teorian, oinarrizko kontzeptuetariko bat, *zatigarritasunarena* da. Atal honen ideia garrantzitsuena, zenbaki osoen zatiketa hondarrarekin datza.

Definizioa. *Izan bitez $a, b \in \mathbb{Z}$, non $a \neq 0$ den. a-k b zatitzen duela esaten da, eta $a \mid b$ moduan idazten da, baldin eta existitzen bada $c \in \mathbb{Z}$ non $b = ac$ den. Kasu honetan a, b-ren zatitzailea dela, b, a-ren multiploa dela edo b, a-gatik zatigarria dela esaten da. Kontrako kasuan, $a \nmid b$ idazten da.*

Ondoko propietateak berehalakoak dira:

Propietateak. *Izan bitez $a, b, c, d \in \mathbb{Z}$. Orduan:*

(i) $a \mid b$ *baldin eta soilik baldin* $|a| \mid |b|$, *non* $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$

(ii) $a \mid 0$ *eta* $1 \mid a$

(iii) $a \mid 1$ *baldin eta soilik baldin* $a = \pm 1$.

(iv) $a \mid a$

(v) *Baldin eta* $a \mid b$ *eta* $b \mid a$ *badira, orduan* $a = \pm b$

(vi) *Baldin eta* $a \mid b$ *eta* $b \mid c$, *orduan* $a \mid c$

(vii) *Baldin eta* $a \mid b$, *eta* a *eta* b *biak zenbaki oso positiboak badira, orduan* $a \leq b$

(viii) *Baldin eta* $a \mid b$ *eta* $a \mid c$, *orduan* $a \mid (bx - cy)$, *edozein* $x, y \in \mathbb{Z}$ *zenbakietarako.*

2 Zatiketaren algoritmoa

Proposizioa. *Izan bitez a eta b bi zenbaki osoak, non $b \neq 0$ den. Orduan existitzen dira q eta r bi zenbaki osoak eta bakarrak non $a = qb + r$ den, $0 \leq r < |b|$ izanik. Kasu honetan, q-ri zatidura eta r-ri hondarra deitzen zaie.*

Froga 2.1. *Har dezagun $\frac{a}{b}$ zenbaki arrazionala (baldin eta a eta b kontrako zeinua badute, zeinu negatiboa a-ri pasatzen zaio eta frogan $b > 0$ dela suposatzen da). Existitzen da q zenbaki oso bat zeinentzat $q \leq \frac{a}{b} < q + 1$ den. Orain aurreko adierazpena b-gatik biderkatuz, $qb \leq a < (q+1)b$ lortzen dugu. Orduan, $r = a - qb$ hartuz, nabaria da arinago esandako propietateak betetzen direla ohartzea.*

Oharra. *Ondoko propietateak berehala frogatzen dira:*

(i) *Baldin eta $r = 0$ bada, a, b-gatik zatigarria da.*

(ii) *$0 \leq r < |b|$ baldintzak, zatiketa algoritmoa zehazten du. Adibidez, $21 = (-3)(-5)+6$ motatako adierazpena, ez da zatiketa algoritmoaren ondorioa.*

(iii) *b finkatuta, hondarren aukera posibleak kantitate finitua dira, hain zuzen ere, $0, 1, 2, \ldots |b| - 1$.*

Adibidea. *Edozein a zenbaki oso baten karratua $3k$ edo $3k+1$ motatakoa da, k zenbaki oso bat izanik. Hau da, a^2, 3-gatik zatitzerakoan lortutako hondarrak 0 edo 1-a dira.*

Froga 2.2. *Baldin eta zatitzen bada a, 3-gatik, orduan hondar posible bakarrak 0, 1 edo 2 dira. Hau da, hiru aukera existitzen dira:*

(i) *$a = 3q$, orduan $a^2 = 9q^2 = 3(3q^2) = 3k$;*

(ii) *$a = 3q + 1$, orduan $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$;*

(iii) *$a = 3q + 2$, orduan $a^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3k + 1$.*

3 Zenbakitzeko sistemak

Zenbakiak adierazteko era arruntena *hamartar sistema* da, zeinek 0, 1, 2, 3, 4, 5, 6, 7, 8 eta 9, digituak erabiltzen dituen. Adibidez, 108 zenbakia ondoko batura bezala adierazten da,

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

Oharra. *Atal honetan zenbaki osoekin baino ez dugu lan egingo, baina kasu orokorrean, zenbakian, koma bat agertzen baldin bada, komaren eskuma aldean dagoen lehenengo digitua 10^{-1}-gatik biderkatuta agertzen da, komaren eskuma aldeko bigarren digitua 10^{-2}-gatik, etabar.*

Baina ez dago inolako arrazorik beti hamartar sistemara murriztera behartzen duenik. Adibidez, ordenagailuek biko sistema, 8-koa edo 16-koa erabiltzen dituzte. Zenbakizko

kalkuluak egiteko ordenagailu batek, 108 zenbakiaren biren berreketen ondoko adierazpena erabiltzen du.

$$(*1)108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

Baldin eta 108 zenbakia 4-ren berreketen bidez adierazten baldin badugu, ondokoa lortzen da

$$108 = 1 \cdot 4^3 + 2 \cdot 4^2 + 3 \cdot 4^1 + 0 \cdot 4^0,$$

$(1230)_4$ bidez adierazten dena. Eta 9 oinarrian,

$$108 = 1 \cdot 9^2 + 3 \cdot 9^1 + 0 \cdot 9^0,$$

hau da, $(130)_9$. Adierazpen horiek lortzeko zatiketaren algoritmoa erabiltzen da.

Oharra. *Ohartu ondoko adierazpena ere lortzen dela,*

$$(*2)108 = 3 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 3 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

*(*1) Lehenengoko idazkeraren berezitasuna,*

$$(*1)108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$$

koefiziente guztiak 2 *baino txikiagoak direla da.*

Proposizioa. *Izan bedi* $b \geq 2$ *(*$b \in \mathbb{N}$*), oinarria deituko duguna. Edozein* $n \in \mathbb{N}$ *zenbaki arrunta, idatz daiteke* b*-ren berreketen konbinazio moduan, era bakar batetan:*

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

non $0 \leq a_i < b$*, edozein* i*-rentzako eta* $a_m \neq 0$*. Orduan,* $n = (a_m a_{m-1} \ldots a_2 a_1 a_0)_b$ *idazten da.*

Froga 3.1. *Zatiketa algoritmoa behin eta berriz aplikatu behar da. Lehenengo* $n = n_1 b + a_0$*, gero* $n_1 = n_2 b + a_1$*, eta honela* $n_{m-1} = n_m b + a_{m-1}$*, (*$a_{m-1} < b$ *izanik), adierazpen batetara heldu arte. Orain* $n = n_1 b + a_0$ *adierazpenean aurreko balioak ordezkatuz, ondokoa lortzen da,*

$$n = (((n_m b + a_{m-1} \ldots) b + a_2) b + a_1) b + a_0 = n_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0.$$

Adibidea. *Nola pasatzen da* b *oinarritik* 10 *oinarrira?*

Adibidez, $(3043)_5 = 3 \cdot 5^3 + 0 \cdot 5^2 + 4 \cdot 5 + 3 = 398$.

Adibidea. *Nola pasatzen da* 10 *oinarritik* b *oinarrira?*

Adibidez, 1025 zenbakia 7 oinarrira pasatzeko, 7-gatik zatitzen da; $1025 = 146 \cdot 7 + 3$. Ondoren, $146 = 20 \cdot 7 + 6$ eta $20 = 2 \cdot 7 + 6$. Beraz,

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

eta faktore komunak ateraz,

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

Oharra. *Bereziki* 16 *oinarriko sisteman* 16 *digitu behar dira. Beraz, 0, 1, 2, ..., 9 digituei, A (=10), B (=11), C (=12), D (=13), E (=14) eta F (=15) hizkiak gaineratzen zaie.*

Adibidea. *Nola pasatzen da* 10 *oinarritik* 16 *oinarrira? Adibidez,* $3027 = 189 \cdot 16 + 3$ *eta* $189 = 11 \cdot 16 + 13$*, eta ondorioz* $3027 = (BD3)_{16}$ *dugu.*

4 Zenbaki biren zatitzaile komunetako haundiena

Definizioa. *Izan bitez* a *eta* b *bi zenbaki osoak, behintzat bat zeroren desberdina. Definizioz,* a *eta* b*-ren zatitzaile komunetako haundiena, zkh*(a, b)*, ondoko baldintzak betetzen duen* d *zenbaki osoa eta positibo bakarra da:*

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

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

Adibidea. *zkh*$(-12, 18) = 6$*.*

Ohartu, -12-ren zatitzaileak ± 1, ± 2, ± 3, ± 4, ± 6 eta ± 12 direla, eta 18-ren zatitzaileak ± 1, ± 2, ± 3, ± 6 eta ± 18 direla.

Propietateak. *Ondoko propietateak betetzen dira:*

(i) *zkh*$(a, b) =$ *zkh*(b, a)*;*

(ii) *baldin eta* $a = 0 = b$*, ez da existitzen zkh*(a, b)*;*

(iii) *Baldin eta* a *edo* b *ez direnean* 0*, orduan beti existitzen da zkh*(a, b) *eta hori finitua da;*

(iv) *zkh*(a, b) *beti positiboa da; hain zuzen ere zkh*$(a, b) =$ *zkh*$(-a, b) =$ *zkh*$(a, -b) =$ *zkh*$(-a, -b) =$ *zkh*$(|a|, |b|)$ *dira;*

(v) *zkh*$(a, 0) = |a|$.

Proposizioa. *Baldin eta a eta b bi zenbaki osoak badira (gutxienez bat zeroren desberdina izanik), existitzen dira bi zenbaki osoak, x_0 eta y_0 zeinentzat zkh$(a, b) = ax_0 + by_0$ den. (***Bezòut-en identitatea)**

Froga 4.1. *Defini dezagun $C = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$ multzoa. $C \subseteq \mathbb{N}$ dago eta C ez da multzo hutsa (adibidez $a^2+b^2 \in C$ dago). C ordenatuta dagoenez, dei diezaiogun d bere lehenengo elementuari, hau da, existitzen dira $x_0, y_0 \in \mathbb{Z}$, zeinentzat $d = ax_0 + by_0$ diren. Ikus dezagun d zenbaki hori, a eta b-ren zatitzaile komunetako haundiena dela.*

1) Zatiketa algoritmoa erabiliz, idatz dezakegu $a = qd+r$, $0 \leq r < d$ izanik. Beraz,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Baldin eta $r > 0$ bada, $r \in C$ litzateke eta $r < d$ da, eta honela d-ren definizioaren aurkako adierazpena lortzen dugu. Beraz r ezin daiteke hertsiki 0 baino haundiago izan, eta ondorioz $r = 0$ dugu eta $d \mid a$. Antzeko eran frogatzen da $d \mid b$ dela.

2) Baldin eta $c \mid a$ eta $c \mid b$ badira, badakigu c-k, a eta b-ren edozein konbinazio lineala zatitzen duela, eta orduan $c \mid d$ dugu.

Oharra. *Aurreko adierazpen lineala ez da bakarra.*

Adibidez, $3 =$ zkh$(6, 9) = 6 \cdot (-1) + 9 \cdot 1 = 6 \cdot 5 + 9 \cdot (-3)$.

Definizioa. *Baldin eta a eta b bi zenbaki osoak eta ez nuluak badira, zenbaki horiek elkarrekiko lehenak direla esaten da, baldin eta zkh$(a, b) = 1$ bada.*

Korolarioa. *Izan bitez a eta b bi zenbaki osoak eta ez nuluak. Horiek elkarrekiko lehenak dira baldin eta soilik baldin existitzen badira $x_0, y_0 \in \mathbb{Z}$ zeinentzat $1 = ax_0 + by_0$ den.*

Ariketa. *Baldin eta $a \mid bc$ eta zkh$(a, b) = 1$ badira, orduan $a \mid c$.*

Proposizioa. *Baldin eta $a = qb + r$ bada, orduan zkh$(a, b) =$ zkh(b, r) dugu.*

Froga 4.2. *Deitu $d =$ zkh(a, b); $d \mid r$ (r, a eta b-ren konbinazio osoa izateagatik). Gainera d, b eta r-ren zatitzaile komunetako haundiena da. Hau da, existituko balitz c non $c \mid b$ eta $c \mid r$, orduan $c \mid a$, eta ondorioz d-ren definizioagatik, $c \mid d$ dugu, nahi genuen bezala.*

Adibidea. *Kalkulatu zkh$(1479, 272)$.*

Zatitzen dugu 1479 zenbakia, 272-gatik ($1479 = 5 \cdot 272 + 119$). Beraz,

$$\text{zkh}(1479, 272) = \text{zkh}(272, 119).$$

Errepikatzen dugu operaketa berdina eta $272 = 2 \cdot 119 + 34$ dugu. Ondorioz,

$$\text{zkh}(1479, 272) = \text{zkh}(272, 119) = \text{zkh}(119, 34).$$

Berriro, $119 = 3 \cdot 34 + 17$, eta ondorioz

$$\text{zkh}(1479, 272) = \text{zkh}(272, 119) = \text{zkh}(119, 34) = \text{zkh}(34, 17).$$

Azkenik, $34 = 2 \cdot 17 + 0$. Beraz,

$$\text{zkh}(1479, 272) = \text{zkh}(272, 119) = \cdots = \text{zkh}(17, 0) = 17.$$

5 Euclides-en algoritmoa

Izan bitez $a, b \in \mathbb{Z}$, (orokortasuna galdu gabe suposa dezakegu zenbaki horiek positiboak direla, $\text{zkh}(a, b) = \text{zkh}(|a|, |b|)$ delako). Demagun $a \geq b$ dela. Orduan a, b-gatik zatituz ondokoa lortzen dugu,

$$a = q_1 b + r_1, \quad \text{non} \quad 0 \leq r_1 < b.$$

Badakigu $\text{zkh}(a, b) = \text{zkh}(b, r_1)$ dela. Baldin eta $r_1 = 0$ bada, $\text{zkh}(a, b) = \text{zkh}(b, r_1) = b$, eta bukatu dugu. Kontrako kasuan, b, r_1-gatik zatitzen dugu,

$$b = q_2 r_1 + r_2, \quad \text{non} \quad 0 \leq r_2 < r_1.$$

Jakina da $\text{zkh}(a, b) = \text{zkh}(b, r_1) = \text{zkh}(r_1, r_2)$ dela. Baldin eta $r_2 = 0$ bada, $\text{zkh}(a, b) = \text{zkh}(r_1, r_2) = r_1$, eta bukatu dugu. Kontrako kasuan, r_1,r_2-gatik zatitzen dugu,

$$r_1 = q_3 r_2 + r_3, \quad \text{non} \quad 0 \leq r_3 < r_2.$$

Prozedurak jarraitzen du 0 hondarreko zatiketa batetara heldu arte, eta hori zatiketa kopurua finitu aldiz egin ondoren lortzen da, $r_1 > r_2 > r_3 > \cdots \geq 0$ izateagatik. Baldin eta lehenengo zatiketa 0 hondarrarekin, $(n+1)$garren zatiketa bada, orduan

$$r_{n-1} = q_{n+1} r_n + 0, \quad \text{eta}$$

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

Orain gure galdera da, nola erabili Euclidesen algoritmoa Bezòut-en identitatea lortzeko?

$$a = q_1 b + r_1, \quad \text{non} \quad 0 \leq r_1 < b$$

$$b = q_2 r_1 + r_2, \quad \text{non} \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \quad \text{non} \quad 0 \leq r_3 < r_2$$

$$\dots$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \quad \text{non} \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = q_n r_{n-1} + r_n, \quad \text{non} \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

Azken aurreko berdintzatik r_n isolatuz, $r_n = r_{n-2} - q_n r_{n-1}$ lortzen da, hau da, r_{n-2} eta r_{n-1}-ren konbinazio lineal bat. Aurreko berdintzatik, berriro r_{n-1} isolatuz,

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2},$$

(hau da, r_{n-3} eta r_{n-2}-ren konbinazio lineala). Orain emaitza hori, aurreko adierazpenean ordezkatuz,

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2})$$

dugu, hau da, r_n-ren adierazpen bat r_{n-3} eta r_{n-2}-ren konbinazio lineal gisa. Honela jarraituz, r_n, a eta b-ren konbinazio lineal gisa adieraz daiteke.

Ariketa. *Adierazi zkh*$(1479, 272)$*,* 1479 *eta* 272 *zenbakien konbinazio lineal gisa.*

$$1479 = 5 \cdot 272 + 119,$$

$$272 = 2 \cdot 119 + 34,$$

$$119 = 3 \cdot 34 + 17,$$

$$34 = 2 \cdot 17 + 0.$$

Orduan, zkh$(1479, 272) = 17$ dugu. Eta,

$$17 = 119 - 3 \cdot 34 = 119 - 3 \cdot (272 - 2 \cdot 119) =$$

$$7 \cdot 119 - 3 \cdot 272 = 7 \cdot (1479 - 5 \cdot 272) - 3 \cdot 272 = 7 \cdot 1479 - 38 \cdot 272.$$

Proposizioa. *Edozein* $k \neq 0$ *zenbaki oso batentzako, zkh*$(ka, kb) = |k|$*zkh*(a, b).

Froga 5.1. *Baldin eta $k > 0$ bada, zkh$(ka, kb) = k.$zkh(a, b) dela ikusi behar da. ka eta kb zenbaki positiboei Euclidesen algoritmoa aplikatuta, sortzen diren berdintzeen zutabea, a eta b-ri algoritmo bera aplikatuta agertzen diren berdintzeen zutabearekin konparatu behar da. Lehenengo zutabea, bigarrena k-gatik biderkatuz lortzen da. Bereziki, lenenengo zutabean lortzen den azken hondar ez nulua, bigarren zutabean lortzen den azken hondar ez nulua k-gatik biderkatuta da, eta honela froga bukatuta dago. Baldin eta $k < 0$ bada, zkh$(ka, kb) = -k.$zkh(a, b) dela ikusi behar da. Baina,*

$$\text{zkh}(ka, kb) = \text{zkh}(|k|a, |k|b) = |k|\text{zkh}(a, b) = -k.\text{zkh}(a, b).$$

(Ohartu hirugarren berdintzan frogaren lehenengo zatia aplikatu dela.)

Korolarioa. *Baldin eta zkh$(a, b) = d$ bada, orduan $a = da'$ eta $b = db'$, non zkh$(a', b') = 1$ den.*

Bi zenbakiren zatitzaile komunetako haundienaren pareko beste kontzeptu bat existitzen da.

Definizioa. *Baldin eta a eta b bi zenbaki osoak eta ez nuluak badira, definizioz a eta b-ren multiplo komunetako txikiena, mkt(a, b) bidez idazten dena, ondoko m zenbaki osoa eta positibo bakarra da:*

(i) $a \mid m$ *eta* $b \mid m$

(ii) *baldin eta* $a \mid c$ *eta* $b \mid c$*, orduan* $m \mid c$

Propietateak. *Betetzen dira ondoko propietateak:*

(i) *mkt$(a, b) =$ mkt(b, a);*

(ii) *multiploen existentzia ziurtatzeko zenbaki biak izan behar dute zeroren desberdinak*

(iii) *mkt(a, b) beti existitzen da*

(iv) *mkt(a, b) beti da positiboa. Hain zuzen ere, mkt$(a, b) =$ mkt$(-a, b) =$ mkt$(a, -b) =$ mkt$(-a, -b) =$ mkt$(|a|, |b|)$ dugu.*

Proposizioa. *Baldin eta a eta b bi zenbaki osoak eta ez nuluak badira, orduan zkh(a, b)mkt$(a, b) = |ab|$ da.*

Froga 5.2. *Nola zkh(a, b) eta mkt(a, b) beti positiboak diren, suposa dezakegu $a > 0$ eta $b > 0$ direla. Deitu $d =$ zkh(a, b). Orduan $a = da'$ eta $b = db'$ (a' eta b' elkarrekiko lehenak direlarik). Deitu $m = \frac{ab}{d}$. Ikusi behar dugu $m =$ mkt(a, b) dela.*

1) m, a-ren multiploa da, $m = ab'$ delako eta baita ere b-ren multiploa, $m = a'b$ delako.

2) Baldin eta $c > 0$, a eta b-ren multiplo komuna bada, existitzen dira r eta s zenbaki osoak non $c = ar = bs$ den. Orain, Bezòut-en identitateagatik existitzen dira x_0, y_0 zenbaki osoak non $d = ax_0 + by_0$ den. c, $m = \frac{ab}{d}$-gatik zatituz ondokoa lortzen da,

$$\frac{c}{m} = \frac{cd}{md} = \frac{cd}{ab} = \frac{c(ax_0 + by_0)}{ab} = \frac{c}{b}x_0 + \frac{c}{a}y_0 = sx_0 + ry_0,$$

zenbaki osoa dena. Beraz $m \mid c$.

6 Zenbaki lehenak

Definizioa. *$p > 1$ zenbaki osoa, zenbaki lehena dela esaten da, bere zatitzaile positibo bakarrak 1 eta p badira. Kontrako kasuan, zenbaki konposatua dela esaten da.*

Propietateak. *Ondoko propietateak betetzen dira:*

(i) *Edozein n zenbaki osoak, 1 eta n-a onartzen ditu zatitzaile gisa,*

(ii) *1-a ez da zenbaki lehena,*

(iii) *2-a da zenbaki lehen txikiena eta bakarra bikoitia dena,*

(iv) *p zenbaki lehen bat ezin daiteke deskonposatu, $p = ab$ moduan non $1 < a < p$ eta $1 < b < p$ diren,*

(v) *p zenbaki lehena eta a edozein zenbaki osoa badira, orduan*

$$zkh(a, p) = \begin{cases} p, & baldin \quad p \mid a \\ 1, & baldin \quad p \nmid a \end{cases}$$

Proposizioa. *Baldin eta p zenbaki lehena eta a eta b bi zenbaki osoak badira, non $p \mid ab$ den, orduan $p \mid a$ edo $p \mid b$.*

Froga 6.1. *Baldin eta $p \nmid a$, orduan $zkh(a, p) = 1$. Eta ondorioz, $p \mid b$ lor daiteke.*

Oharra. *Aurrekoa bakarrik gertatzen da zenbaki lehenentzako; adibidez $6 \mid 2 \cdot 3$, baina $6 \nmid 2$ eta $6 \nmid 3$.*

Korolarioa. Pitagorasen Teorema. *$\sqrt{2}$ zenbaki irrazionala da.*

Froga 6.2. *Absurdura eramanez, baldin eta $\sqrt{2}$ arrazionala dela suposatzen badugu, orduan $\sqrt{2} = \frac{a}{b}$ motatakoa izango litzateke, a eta b zenbaki osoak eta $b > 0$ direlarik. Beharrezkoa izango balitz, zatikia sinplifikatuz, suposa dezakegu a eta b elkarrekiko*

lehenak direla. Karratua eginez, $2b^2 = a^2$ *dugu, eta ondorioz* $2 \mid a^2 = aa$*. Orain* 2 *lehena denez,* $2 \mid a$ *ondorioztatzen da. Hau da, existitzen da* r *zenbaki oso bat non* $a = 2r$ *den. Ordezkatuz,* $2b^2 = a^2 = 4r^2$ *dugu, hau da,* $b^2 = 2r^2$*, eta orduan* $2 \mid b$ *lortzen da, baina azken emaitza hori kontraesana da,* a *eta* b *elkarrekiko lehenak izateagatik.*

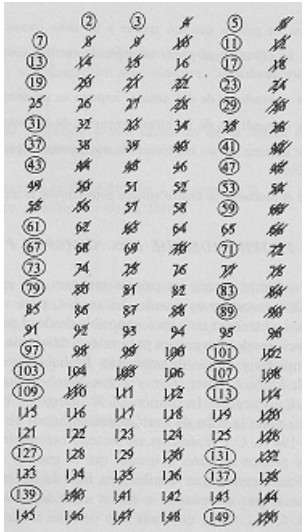
Korolarioa. *Baldin eta* p *zenbaki lehena, eta* $a_1, \ldots, a_n$ *zenbaki osoentzako,* $p \mid a_1 \ldots a_n$ *betetzen bada, orduan* $p \mid a_i$*,* $i \in \{1, \ldots, n\}$ *balioren batetarako.*

Korolarioa. *Baldin eta* p *zenbaki lehena eta* $p_1, \ldots, p_n$ *zenbaki lehenentzako,* $p \mid p_1 \ldots p_n$ *betetzen bada, orduan* p *zenbakia,* $p_1, \ldots, p_n$ *faktoreetako bat izan behar du.*

Eratóstenesen kriba: n zenbaki arrunta osoa eta positiboa haundia denean, aurkitzea bera baino txikiagoak edo berdinak diren zenbaki lehen guztiak problema zaila da. *Eratóstenesen kriba*-k, n baino txikiagoak edo berdinak diren zenbaki lehen guztiak kalkulatzeko zentzuzko metodoa adierazten du, n zenbakia txikia denean.

Idazten dira 2 eta n artean dauden zenbaki oso guztiak; ondoren 2-ren ostean dauden bigarren zenbaki guztiak ezabatzen dira (hau da, 2-ren multiploak diren zenbakiak ezabatzen dira); gero 3-ren ostean edozein hirugarren zenbakia ezabatzen da (hau da, 3-ren multiploak ezabatzen dira, ez direlako lehenak). Bigarrenez pasatzerakoan, jadanik ezabatuta zeuden zenbaki batzuk berriro ezabatzen dira. Ondoren, 5-ren ostean edozein bosgarren zenbakia ezabatzen da. Prozedura bukatzen da, p zenbaki lehenaren multiplo guztiak ezabatzen direnean, $p \leq \sqrt{n}$ izanik. Honela, geratzen diren zenbakiak dira, n baino txikiagoak edo berdinak diren zenbaki lehen guztiak.

Ondorengo grafikoan adierazten da metodoa hori, 150 baino txikiagoak diren zenbaki lehen guztiak aurkitzeko.



7 Aritmetikako Oinarrizko Teorema

Teorema. *Edozein $n > 1$ zenbaki osoa, zenbaki lehen batzuen biderkadura gisa jar daiteke. Gainera, adierazpen hori bakarra da faktoreen ordena ezik.*

Froga 7.1. *i) Faktorizazioaren existentzia: Demagun S, 1 baino haundiagoak eta zenbaki lehenen biderketa moduan adieraz ezin daitezkeen zenbaki oso guztien multzoa dela. Absurdura eramanez, demagun S ez dela hutsa. Deitu S multzoko lehen elementuari, a. Orduan, a ezin daiteke zenbaki lehena (ez konposatua) izan, bestalde, ez litzateke S-n egongo. Beraz, $a = mn$ da, $1 < m < a$ eta $1 < n < a$ izanik. Orain a, S-ko elementu txikiena denez, orduan $m \notin S$ eta $n \notin S$. Hau da, m eta n zenbaki lehen batzuen biderketa gisa jar daitezke. Adibidez, $m = p_1 p_2 \dots p_r$ eta $n = q_1 q_2 \dots q_s$. Orduan, $a = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ bai da, zenbaki lehenen biderketa, eta hori kontraesana da. Beraz, $S = \emptyset$.*
2) Bakartasuna faktoreen ordena ezik: demagun n-ren bi faktorizazio ditugula, $n = p_1 p_2 \dots p_r$ eta $n = q_1 q_2 \dots q_s$, eta adierazpen bakoitzean lehenak ordenatuta daudela modu gorakorrean: $p_1 \le p_2 \le \dots \le p_r$ eta $q_1 \le q_2 \le \dots \le q_s$. Frogatu behar dugu $r = s$ dela, eta indize bakoitzerako $p_i = q_i$ dela. Nola $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ den, p_1-k $q_1 q_2 \dots q_s$ zatitzen du, eta ondorioz $p_1 = q_k$ da, k-ren batetarako. Bereziki, $p_1 \ge q_1$ da. Modu berdinean, q_1-k $p_1 p_2 \dots p_r$ zatitzen duenez, $q_1 = p_i$ dela ondorioztatzen da, i-ren batentzako, eta bereziki, $q_1 \ge p_1$ dugu. Beraz, $p_1 = q_1$ lortzen da. n-ren faktorizazioan, aurreko p_1 faktorea ezabatuz, $p_2 \dots p_r = q_2 \dots q_s$ lortzen da. Argudio berdina errepikatuz, $p_2 = q_2$ dela lortzen da. Beraz, $p_3 \dots p_r = q_3 \dots q_s$ dugu. Baldin eta $r < s$ balitz, ondoz ondoko ezabapenak egin ondoren, $1 = q_{r+1} q_{r+2} \dots q_s$ dela lortuko genuke, eta hori ezinezkoa da, faktorizazioko zenbaki lehen guztiak 1 baino haundiagoak direlako. Ondorioz, $r = s$ dugu eta $p_i = q_i$, i indize bakoitzarentzako.

Oharra. *Baldin eta $n < -1$ bada, nola $-n > 1$ den, $-n = p_1 p_2 \dots p_r$ faktorizazioa dugu, eta orduan $n = -p_1 p_2 \dots p_r$ lortzen da. Gainera, faktorizazio horietan zenbaki lehenak errepikatuta egon daitezke, eta berdinak diren faktoreak elkartzen baldin badira, n zenbaki osoaren faktorizazio kanonikoa lortzen da.*

Teorema. *Edozein $n \neq 0, \pm 1$ modu bakarrean adieraz daiteke ondoko eran,*

$$n = \pm p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

non $p_1 < p_2 < \dots < p_r$ zenbaki lehenak eta $k_i > 0$ diren, edozein indizerako.

Proposizioa. *Baldin eta $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ bada, non $p_1 < p_2 < \dots < p_r$ zenbaki lehenak eta $k_i > 0$ diren, edozein indizerako, eta $m \mid n$ bada, orduan $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ adierazpena lortzen da, non $h_i \le k_i$ diren, edozein i baliorako.*

Froga 7.2. *Baldin eta $m \mid n$ bada, orduan $n = cm$ da, c osoa izanik. Zenbaki lehenen faktorizazio kanonikoak hartuta, $m = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s}$ eta $c = r_1^{l_1} r_2^{l_2} \dots r_t^{l_t}$ dira. Orduan,*

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_s} r_1^{l_1} r_2^{l_2} \dots r_t^{l_t}$$

Aritmetitako Oinarrizko Teoremagatik badakigu aurreko adierazpeneko alde bietako zenbaki lehenak eta baita, alde bietako berredurak, berdinak izan behar dutela. Beraz, q_j bakoitza, p_i baten berdina izan behar du, eta bere berredurari dagokionez, $h_j \leq k_i$ izan behar du.

Faktorizazioko teknika hau erabil daiteke zenbaki osoen arteko zatitzaile komunetako haundia eta multiplo komunetako txikiena kalkulatzeko, eta horrela Euclides-en algoritmoari alde egiten diogu.

Proposizioa. *Baldin eta $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ eta $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ badira, non $p_1 < p_2 < \dots < p_r$ zenbaki lehenak eta $k_i, h_i \geq 0$ diren, edozein indizerako, orduan*

(i) $\mathit{zkh}(m,n) = p_1^{\min(k_1,h_1)} p_2^{\min(k_2,h_2)} \dots p_r^{\min(k_r,h_r)}$;

(ii) $\mathit{mkt}(m,n) = p_1^{\max(k_1,h_1)} p_2^{\max(k_2,h_2)} \dots p_r^{\max(k_r,h_r)}$;

(iii) $mn = \mathit{mkt}(m,n) \cdot \mathit{zkh}(m,n)$.