7. Gaia: Aritmetika modularra

Oro har ez da erraza zenbaki oso handiekin lan egitea. Izan ere, zenbakien faktorizazioa problema zaila da oro har. Horregatik, batzuetan kongruentziekin egiten da lana eta kongruentzien laguntzarekin problemak ebazteari aritmetika modular esaten zaio. Era lauso batean esanda, zenbaki natural bat n aukeratzen da, "modulua" izango dena, eta eragiketak zenbakiekin egin ordez, n-rekin zatitzerakoan lortzen dugun hondarrarekin egiten dira. Definizio konkretuak ikusi aurretik ikus ditzagun zenbait adibide konkretu.

Adibideak 7.0.3. (i) Zein asteko egun izango da hemendik 100 egunetara? Aukera bat egutegi bat hartu eta 100 arte banan banan egunak kontatu eta ikustea litzateke. Baina hori baino modu eraginkorragoa litzateke ohartzea asteak 7 egun dauzkala. Eta $100 = 7\times14+2$ denez, gaurko egunetik 14 aste oso pasako dira, eta egun berean egongo gara, eta gero bi. Beraz, aski da gaurko egunari bi egun gehitzea. Adibidez, gaur ostirala bada, 100 egun barru igandea izango da. Igandea bada, asteartea, etab. Aurreko ideia lauso horri loturik, hemen $n = 7$ aukeratu dugu, eta hondarra 2 zen. Hau da, 100 2-rengatik ordezkatu dugu, nolabait.

(ii) Galde geniezaioke gure buruari ea 542136542 zenbakia karratu perfektua den. Hau da, ea existitzen den n non $n^2 = 542136542$ den. Aukera bat litzateke zenbaki hori faktorizatzen saiatu eta ikustea ea faktore guztiek potentzia bikoitia duten. Baina oro har zenbakiak faktorizatzea ez da lan erraza. Beste aukera bat banan-banan zenbakiak karratura jasotzen hasi eta ea gure zenbakia lortu dugun konprobatzen joatea da. Baina horrek ere denbora asko eskatuko liguke. Hala ere, badago ez den konprobatzeko oso modu azkar bat. Gogoan baduzue, lehen gaiko ariketa batean eskatzen ziguten n^2 beti dela $4k$ edo $4k + 1$ itxurakoa. Beraz, eman diguten zenbakiak ez badu itxura hori ezin da zenbaki baten karratua izan. Itxura hori duen ikusteko, 4-rekin zatitu eta zein hondar duen ikusi behar dugu.

$$542136542 = 5421365 \times 100 + 42 = 5421365 \times 25 \times 4 + 10 \times 4 + 2.$$

Beraz, hondarrak 2 emango du, eta ez dugu denbora alferrik galdu behar zenbaki hori karratua den aztertzen, ez delako izango. Kasu honetan $n = 4$ hartu dugu, eta gure zenbakia bere hondarragatik "ordezkatu", nolabait.

Ohartu 4-ren multiplo edo $4k + 1$ motakoa eman izan baligu ezingo genukeela ezer esan. Bakarrik posible litzatekeela printzipioz zenbaki hori

karratua izatea. Hori bai, proba egin genezake eta ikusi zer gertatzen den beste n batzuk hartuta.

Ariketa 7.i. Frogatu zenbaki bat beste baten karratua bada, orduan $5k$, $5k+1$ edo $5k+4$ motakoa dela. Zer ondoriozta dezakegu $2, 3, 7$ eta 8 amaitzen diren zenbakiei buruz?

7.1 Kongruentziak

Definizioa 7.1.1. Izan bedi $n \in \mathbb{N}$, orduan a eta b zenbaki osoak *kongruenteak* dira n-rekiko n-k $a-b$ zenbakia zatitzen badu, hau da $n \mid (a-b)$ bada. Kasu honetan, n zenbakiari kongruentziaren *modulua* esaten zaio. Baldin eta a eta b kongruenteak badira n moduluarekiko, $a \equiv b \pmod{n}$ idazten da.

Adibideak 7.1.2. (i) Zenbaki guztiak kongruenteak dira 1 moduluarekiko.

(ii) Baldin $n = 2$ bada, hondar posible bakarrak 0 eta 1 dira. $m \equiv 0 \pmod{2}$ da m bikoitia bada eta $m \equiv 1 \pmod{2}$ da m bakoitia bada.

(iii) Baldin $n = 5$ bada, $9 \equiv 19 \pmod{5}$, $-13 \equiv 2 \pmod{5}$ edo $5 \equiv -5 \pmod{5}$.

Ikus dezagun behin $n \in \mathbb{N}$ finkatuta, elkarrekin kongruenteak direla n-rekin zatitzerakoan hondar bera ematen duten zenbakiak.

Lema 7.1.3. *Izan bitez $a, b \in \mathbb{Z}$ eta $n \in \mathbb{N}$. Orduan $a \equiv b \pmod{n}$ baldin eta soilik baldin $a = nq_1 + r_1$ eta $b = nq_2 + r_2$ badira $0 \leq r_1, r_2 < n$ izanik, orduan $r_1 = r_2$ badugu.*

Froga. Norantza bat errazagoa da. Izan ere, argi dago "eskumako" baldintza egia bada, hau da, $a = nq_1 + r_1$ bada eta $b = nq_2 + r_2$ non $r_1 = r_2$ diren, orduan $a - b = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2)$ da, eta beraz n-k $a - b$ zatitzen du.

Demagun orain n-k $a-b$ zatitzen duela eta ikus dezagun derrigorrez hondar bera izan behar dutela n-rekin zatitzerakoan. Zatiketaren algortimotik badakigu existitzen direla q_1, q_2, r_1, r_2 bakarrak non $a = q_1 n + r_1$ den eta $b = q_2 n + r_2$; non gainera $0 \leq r_1, r_2 < n$ dugun. Orduan n-k $a - b$ zatitzen duenez, derrigorrez zatituko du $(q_1 - q_2)n + (r_1 - r_2)$. Eta lehen batugaia zatitzeagatik $r_1 - r_2$ ere zatitzen du. Suposa dezakegu $r_1 - r_2 \geq 0$ dela, bestela $-(r_1 - r_2) = r_2 - r_1 \geq 0$ genukeelako eta hori ere zatituko lukeelako n-k. Baina biak n baino txikiagoak direnez eta zero baino handiago edo berdinak $0 \leq r_1 - r_2 < n$ da, eta, beraz, n zatitzeko aukera bakarra 0 izatea da. Edo baliokidea dena $r_1 = r_2$ izatea. □

Proposizioa 7.1.4. *Izan bedi $n \in \mathbb{N}$. Propietate hauek betetzen dira:*

(i) $a \equiv a \pmod{n}$, *a guztietarako.*

(ii) $a \equiv b \pmod{n}$ *bada,* $b \equiv a \pmod{n}$ *da.*

(iii) $a \equiv b \pmod{n}$ *eta* $b \equiv c \pmod{n}$ *badira,* $a \equiv c \pmod{n}$ *da.*

Hortaz, n moduluarekiko kongruente izatea baliokidetasun-erlazioa da.

Ariketa 7.ii. Eman aurreko proposizioaren frogapen formala

Baliokidetasun-erlazioa denez, baliokidetasun-klaseak defini daitezke. Klase bakoitzean n-rekin zatitzean hondar bera ematen duten zenbakiak daude. Ondorioz, n hondar desberdin dauzkagunez, eta hondar posibleak $0, 1, \ldots, n-1$

direnez, n baliokidetasun-klase egongo dira eta ordezkari gisa $0, 1, \ldots, n-1$ zenbakiak aukera ditzakegu. Orduan,

$$\begin{aligned}[0] &= \{kn \mid k \in \mathbb{Z} \ldots\},\\ [1] &= \{kn+1 \mid k \in \mathbb{Z}\},\\ &\vdots\\ [n-1] &= \{kn+(n-1) \mid k \in \mathbb{Z}\}.\end{aligned}$$

Klase-multzo hori $\mathbb{Z}/n\mathbb{Z}$ bidez adieraziko dugu [11].

Notazioa 7.1.5. Batzuetan kortxeteen ordez marra baten bidez adierazten dira klaseak, hau da $[0] = \overline{0}$ modura idazten da. Honela,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

izango genuke.

Proposizioa 7.1.6. *Izan bedi $n \in \mathbb{N}$. Baldin eta $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ badira non $a_1 \equiv a_2 \pmod{n}$ eta $b_1 \equiv b_2 \pmod{n}$ diren, orduan*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \text{ eta } a_1 b_1 \equiv a_2 b_2 \pmod{n}$$

betetzen dira.

Froga. Badakigu $a_1 = nk_1 + a_2$ dela eta $b_1 = nk_2 + b_2$. Beraz, $a_1 + b_1 = n(k_1 + k_2) + (a_2 + b_2)$ eta beraz argi dago $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ dugula. Biderketaren kasuan, $a_1 b_1 = (nk_1 + a_2)(nk_2 + b_2) = nk_1 nk_2 + nk_1 b_2 + a_2 nk_2 + a_2 b_2 = n(nk_1 k_2 + a_2 k_2 + b_2 k_1) + a_2 b_2$, eta hemendik ondorioztatzen da bigarrena. □

A multzo baten gaineko eragiketa bat $A \times A \to A$ motako funtzio bat da. Kasu honetan $\mathbb{Z}/n\mathbb{Z}$ multzoaren gainean defini genitzake ondoko bi eragiketak, batura eta biderketa deituko ditugunak:

$$\begin{aligned}+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\ (\overline{a}, \overline{b}) &\mapsto \overline{a} + \overline{b} := \overline{a+b}\end{aligned}$$

eta

$$\begin{aligned}\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\ (\overline{a}, \overline{b}) &\mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}\end{aligned}$$

Kontua da ea definitu ditugun bi eragiketa hauek funtzioak diren. Gogoratu, funtzioek elementu bati irudi bakar bat esleitu behar dietela. Kasu honetan daukagun arazoa da $\overline{a_1} = \overline{a_2}$ izan dezakegula $a_1 \neq a_2$ izanik. Beraz, kontuz ibili behar dugu $\mathbb{Z}/n\mathbb{Z}$-ren gainean funtzioak definitzerakoan. Gerta litekeelako $\overline{a_1}$ leku batera bidaltzea eta $\overline{a_2}$ beste batera. Hau aurrerago ikusiko duzue bigarren mailatik aurrera beste zenbait egoeratan. Funtzioak zatiduretan definitzerakoan ondo definituta daudela egiaztatu behar da.

[11] Zenbait autorek $\mathbb{Z}_n$ erabiltzen du zenbaki hauek adierazteko, baina p lehena den kasuan zenbaki p-adikoak adierazteko notazio bera erabiltzen denez, guk goian aipatutakoa erabiliko dugu.

Gure kasuan, edozein kasutan, aurreko proposizioak ziurtatzen digu funtzio horiek biak, hau da, eragiketa biak, ondo definituta daudela. Izan ere, bi elementu berdin $(\overline{a_1}, \overline{b_1}) = (\overline{a_2}, \overline{b_2})$ baditugu, proposizioak dio $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ dela, eta biderkadurarako gauza bera. Beraz, posible da lehenengo ordezkariak batu (edo biderkatu) eta gero modulua hartzea, eta ez gara ezer gaizki egiten ariko.

Honek problemak ebazterakoan asko lagunduko digu, azken batean, honek ziurtatzen digulako "aritmetika" modularra egin dezakegula; hau da, klaseak batu eta biderkatu ditzakegula. Orokorpen hauek ere baliagarriak izango dira.

Korolarioa 7.1.7. *Izan bitez $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. Orduan*

(i) *$\overline{a} = \overline{b}$ bada $\overline{a^k} = \overline{b^k}$ edozein $k \in \mathbb{N}$-rako.*

(ii) *$\overline{a} = \overline{b}$ bada $\overline{p(a)} = \overline{p(b)}$ non $p(x) \in \mathbb{Z}[x]$ koefizienteak $\mathbb{Z}$-n dituen edozein polinomio den.*

Polinomioena baliagarria izan daiteke sarreran aipatutako moduko zenbait problemari ezezko erantzuna emateko.

Adibidea 7.1.8. Izan bedi $p(x) = x^5 - x^2 + x - 3$. Ikus dezagun ez daukala erro osorik. Suposa dezagun badaukala erro osoren bat $a \in \mathbb{Z}$ eta saia gaitezen kontraesan batera iristen. Aukera dezagun $n = 4$. Badakigu a $p(x)$-ren erroa dela, hau da $p(a) = 0$ da. Baina orduan, $\mathbb{Z}/n\mathbb{Z}$-n ere betetzen da berdintza hori. Hau da $\overline{a}^5 - \overline{a}^2 + \overline{a} + \overline{-3} = \overline{0}$. Orain $\overline{a}$-k lau aukera baino ez ditu $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Hau dugu lau kasuetan hurrenez hurren:

$$\begin{aligned}
\overline{0}^5 - \overline{0}^2 + \overline{0} + \overline{-3} &= \overline{-3} = \overline{1} \neq \overline{0},\\
\overline{1}^5 - \overline{1}^2 + \overline{1} + \overline{-3} &= \overline{1 - 1 + 1 - 3} = \overline{2} \neq \overline{0},\\
\overline{2}^5 - \overline{2}^2 + \overline{2} + \overline{-3} &= \overline{32 - 4 + 2 - 3} = \overline{3} \neq \overline{0},\\
\overline{-1}^5 - \overline{-1}^2 + \overline{-1} + \overline{-3} &= \overline{-1 - 1 - 1 - 3} = \overline{2} \neq \overline{0},
\end{aligned}$$

Beraz, ez du erro osorik izango polinomio horrek. Ohartu $\overline{3} = \overline{-1}$ erabili dugula. Batzuetan komenigarria da negatiboak erabiltzea, batez ere balio absolutuan txikiagoak diren kasuan biderkadura eta berreturak txikitze aldera.

Ariketa 7.iii. Frogatu ondoko polinomioek ez daukatela erro osorik:

(i) $x^3 - x + 1$,

(ii) $x^3 + x^2 - x + 1$,

(iii) $x^3 + x^2 - x + 3$.

Aurrerantzean, klaseak izan arren, batzuetan zuzenan $\overline{a}$-ren ordez zuzenean a idatziko dugu.

Adibidea 7.1.9. Hauek dira batuketa- eta biderketa-taulak $\mathbb{Z}/5\mathbb{Z}$-en eta $\mathbb{Z}/6\mathbb{Z}$-n.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Taldeen propietateei begiratzen badiegu $\mathbb{Z}/n\mathbb{Z}$-n erraz ikus daiteke $(\mathbb{Z}/n\mathbb{Z}, +)$ talde abeldar edo trukakorra dela. Ordea, biderketarekiko, oro har ez dauka talde egitura $\mathbb{Z}/n\mathbb{Z} - \{0\}$-k. Izan ere, badira elementuak alderantzizkorik ez daukatenik. Adibidez, $\mathbb{Z}/6\mathbb{Z}$-ren taulan erraz ikusten da 2 bider edozer gauza eginda ez dugula inoiz elementu neutroa lortuko, 1-a dena. Ez hori bakarrik, oro har zenbakietan gertatzen ez den gauza bat gertatzen da biderketa honekin. Posible dela $a \neq 0$ eta $b \neq 0$ izan eta $ab = 0$ izatea! Hau da adibidez $\mathbb{Z}/6\mathbb{Z}$-n 2 eta 3-ri gertatzen zaiena. Benetan hori gertatzen zaie ez direlako 6-rekiko elkarrekiko lehenak.

Proposizioa 7.1.10. *Izan bedi $n \in \mathbb{N}$ arrunta eta $a \in \mathbb{Z}$. Orduan existitzen da $b \in \mathbb{Z}$ non $ab \equiv 1 \pmod{n}$ baldin eta soilik baldin* $\operatorname{zkh}(a, n) = 1$ *bada.*

Froga. Hasteko, demagun existitzen dela halako b bat eta ikus dezagun orduan a eta n elkarrekiko lehenak izan behar direla. Baldin eta $ab \equiv 1 \pmod{n}$, esan nahi du existitzen dela $k \in \mathbb{Z}$ non $ab - 1 = nk$ den. Bestela esanda $1 = ab - nk$ da. Baina orduan, c bat balego non $c \mid a$ eta $c \mid n$ biak zatitzen dituena, beraien edozein konbinazio zatituko luke. Bereziki, $c \mid 1$ dugu, eta ondorioz $\operatorname{zkh}(a, n) = 1$ da.

Demagun orain a eta n elkarrekiko lehenak direla. Badakigu, beraz, $\operatorname{zkh}(a, n) = 1$ denez, existitzen direla $x, y \in \mathbb{Z}$ non $1 = ax + ny$ den. Baina orduan, x da bilatzen dugun b hori. Izan ere, kongruentziak hartuz berdintza horretan $\overline{1} = \overline{ax} + \overline{ny} = \overline{ax} + \overline{0} = \overline{ax}$ dugu. Hau da $ax \equiv 1 \pmod{n}$. □

Korolarioa 7.1.11. *Baldin eta $p \in \mathbb{N}$ zenbaki lehena bada, orduan $\mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ multzoak talde egitura du biderketarekiko.*

Froga. Nahikoa da ohartzea $\overline{a} \neq \overline{0}$ bada, p-k ez duela a zatitzen, eta p lehena izateagatik, $\operatorname{zkh}(a, p) = 1$ izango da. Beraz, existituko da $b \in \mathbb{Z}$ non $\overline{ab} = \overline{1}$ den $\mathbb{Z}/p\mathbb{Z}$-n. Faltako litzaiguke ziurtatzea $\overline{b} \neq \overline{0}$ dela, baina hori bistakoa da, bestela $\overline{ab} = \overline{0}$ genukeelako, baina $\overline{0} \neq \overline{1}$ dugu. □

Aritmetika modularrari esker hondar batzuk erraz kalkula ditzakegu orain

Adibideak 7.1.12. (i) Kalkula dezagun, adibidez, 37 bider 110-en hondarra 34-rekin zatitzerakoan. Alde batetik $\overline{37} = \overline{3}$ dugu $\mathbb{Z}/34\mathbb{Z}$-n. Bestalde, $34\times 3 = 102$ denez, $\overline{110} = \overline{8}$ da. Ondorioz, $\overline{3}\times\overline{8} = \overline{24}$ izango da biderkadura horren hondarra 34-rekin zatitzerakoan.

(ii) 3^{10}-en hondarra 16-rekin zatitzerakoan ere kalkula dezakegu, adibidez. Badakigu $3^3 = 27$ dela, eta $\overline{27} = \overline{11} = \overline{-5}$ da $\mathbb{Z}/16\mathbb{Z}$-n. Orain $3^{10} = 3^3\cdot 3^3\cdot 3^3\cdot 3$ dugunez, ondokoa izango dugu:

$$\begin{aligned}\overline{3^{10}} &= \overline{3^3}\cdot\overline{3^3}\cdot\overline{3^3}\cdot\overline{3}\\ &= \overline{-5}\cdot\overline{-5}\cdot\overline{-5}\cdot\overline{3}\\ &= \overline{25}\cdot\overline{-5}\cdot\overline{3}\\ &= \overline{9}\cdot\overline{-5}\cdot\overline{3}\\ &= \overline{9}\cdot\overline{-15}\\ &= \overline{9}\cdot\overline{1} = \overline{9}.\end{aligned}$$

7.2 Kongruentzia linealak

Lehenago aipatu dugu $\mathbb{Z}/n\mathbb{Z}$-n biderkadurarekiko alderanzgarriak diren elementuak $\overline{a}$ motakoak direla $\operatorname{zkh}(a,n) = 1$ izanik. Kasu horretan $ax \equiv 1 \pmod n$ kongruentzia ebatzi nahi genuen. Demagun orain, 1-aren lekuan beste edozein zenbakiren baliokidetasun klasea jarri nahi dugula. Hau da, demagun ebatzi nahi duguna $ax \equiv b \pmod n$ dela $a, b \in \mathbb{Z}$ izanik. Problema honen soluzioa ikusi aurretik ikus dezagun lagungarri egingo zaigun lema bat:

Lema 7.2.1. *Izan bedi* $\operatorname{zkh}(k,n) = d$. *Baldin* $ak \equiv bk \pmod n$ *bada, orduan* $a \equiv b \pmod{n/d}$ *da.*

Froga. $ak \equiv bk \pmod n$ izateak, $n|(a-b)k$ esan nahi du.

(i) $d = 1$ bada, n eta k elkarren arteko lehenak direnez, $n|(a-b)$ da.

(ii) $d > 1$ bada, $\operatorname{zkh}(n/d, k/d) = 1$ da. Gainera, $nt = (a-b)k$ baldin bada, bi aldeetan d-rekin zatituz $tn/d = (a-b)k/d$ dugu, hau da $n/d \mid (a-b)k/d$ da, eta, aurreko atalean bezala, $n/d \mid (a-b)$, edo $a \equiv b \pmod{n/d}$. □

Ondoko proposizioak ematen digu lehen planteaturiko problemaren soluzioa:

Proposizioa 7.2.2. *Izan bedi* $\operatorname{zkh}(a,n) = d$. *Orduan* $ax \equiv b \pmod n$ *ekuazioak soluzioa du baldin eta soilik baldin* $d|b$ *bada. Baldintza hori betetzen bada, eta* x_0 *soluzio bat bada,* $x \equiv x_0 \pmod{n/d}$ *guztiak dira soluzioak eta horiek dira soluzio posible guztiak.*

Froga. Batetik, soluzioa existitzen bada, $ax - b = nq$ izango da $q \in \mathbb{Z}$ baterako, hau da, $b = ax - nq$. Orduan, a eta n-ren zatitzaile komun handienak beraien edozein konbinazio zatituko du, bereziki, b.

Demagun orain $d|b$ betetzen dela eta idatz dezagun $b = dk$. Bézout-en identitateagatik badakigu existitzen direla $s, t \in \mathbb{Z}$ non $d = sa + tn$. Orain, berdintza hau k-rekin biderkatuz, $kd = ksa + ktn$ lortzen dugu. Baina ohartu $dk = b$ dela. Hau da, $ksa = b - ktn \equiv b \pmod n$ lortu dugu, eta beraz ks gure sistemaren soluzio bat da.

Emaitza denak $x \equiv x_0 \pmod{n/d}$ motakoak direla ikusteko, ohartu x_1 eta x_2 bi soluzio badira, $ax_1 \equiv ax_2 \pmod{n}$ dugula. Baina 7.2.1 Lema erabiliz, kongruentzia hori egia bada $x_1 \equiv x_2 \pmod{n/d}$ egia da, $d = \text{zkh}(a, n)$ izanik. Beraz, n moduluarekiko soluzio ezberdinak ondokoak izango dira:

$$\{x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}\}.$$

□

Adibidea 7.2.3. Aurki ditzagun $15x \equiv 18 \pmod{27}$ ekuazioaren soluzio guztiak.

Hasteko, azter dezagun ea soluziorik duen. Badakigu $\text{zkh}(15, 27) = 3$ dela, eta $3 \mid 18$ denez, sistemak soluzioren bat du. Soluzioa aurkitzeko, proposizioaren frogak diona da 3 zenbakia 15 eta 27-ren konbinazio gisa adierazi behar dugula, eta hori Bézout-en identitateari esker badakigu egiten. Kasu honetan $3 = 15 \cdot 2 - 27$ da. Frogapeneko a-ren papera 15-ek betetzen du, $s = 2$ dugu, $d = 3$ da eta $k = 18/3 = 6$ da. Beraz, $ks = 6 \cdot 2 = 12$ soluzio bat izango da. Gainera, badakigu 3 soluzio dauzkagula modulu 27, ondokoak direnak:

$$\{12, 12 + 9, 12 + 9 \cdot 2\} = \{12, 21, 3\}.$$

Beste aukera bat da ekuazioa hasieratik 3-rekin zatitzea. Orduan $5x \equiv 6 \pmod{9}$ geratzen zaigu, eta argi dago soluzio bat $x = 3$ dela, 15=6 delako $\mathbb{Z}/9\mathbb{Z}$-n. Ondoren, beste bi soluzioak zein diren ere proposizioak adierazten du.

7.2.1 Hondarren teorema txinatarra

Has gaitezen ariketa bat planteatzen. Talde bateko ikasleak hirunaka ipiniz gero, bat soberan geratzen da; bosnaka ipiniz gero, bi geratzen dira soberan; eta zazpinaka ipiniz gero, lau daude soberan. Zenbat ikasle dira denetara, 100 baino gutxiago direla jakinda?

Aritmetika modularrean hau da dugun informazioa:

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 4 \pmod{7}.$$

Beraz, kongruentzia bat ebatzi beharrean, sistema bat ebatzi behar dugu, eta $1 \leq x < 100$ betetzen duen soluzioa aurkitu behar dugu (edo soluzioak, aukera bat baino gehiago badago).

Modu orokorrean, hau da orain gure problema:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ x &\equiv b_2 \pmod{m_2}, \\ &\cdots \\ x &\equiv b_n \pmod{m_n}. \end{aligned} \tag{7.1}$$

Oharra 7.2.4. Ez dugu ekuazio bakoitza $a_j x \equiv b_j \pmod{m_j}$ eran idatzi. Halakoak badira, lehenengo forma honetara pasa ditzakegu, ekuazio bakarreko kasuan egin dugun bezala.

Teorema 7.2.5 (Hondarren teorema txinatarra)**.** *Demagun* (7.1) *kongruentzia-sistema dugula eta* $\text{zkh}(m_i, m_j) = 1$ *dela,* $i \neq j$ *bada. Orduan, sistemak soluzio bakarra du* $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ *moduluarekiko. Hau da,* $0 \leq x < M$ *betetzen duen soluzio bakar bat dago eta* $y \equiv x \pmod{M}$ *dira beste guztiak.*

Froga. Izan bedi M moduluen biderkadura, enuntziatuak dioen moduan, eta $M_j = M/m_j$ $(j = 1, 2, \ldots, n)$. Hipotesiagatik, zkh$(M_j, m_j) = 1$ da, eta beraz, $M_j x \equiv 1 \pmod{m_j}$-k soluzioa du eta bakarra da m_j moduluarekiko. Dei diezaiogun soluzio horri x_j. Orduan $x = b_1 M_1 x_1 + \cdots + b_n M_n x_n$ sistema osoaren soluzioa izango da. Sistemaren soluzioa dela ikusteko, ikus dezagun $x \equiv b_i \pmod{m_i}$ betetzen dela. Finka dezagun, beraz, i bat. Ohartu, hasteko M_j bakoitza m_i-gatik zatigarria dela $j \neq i$ denean. Beraz, $b_j M_j x_j \equiv 0 \pmod{m_j}$. Ondorioz, m_i-rekiko ezberdin zero den batugai bakarra $b_i M_i x_i$ izango da. Orain, x_i aukeratu dugu $M_i x_i \equiv 1 \pmod{m_i}$ izan zedin, eta beraz, $x \equiv b_i \pmod{m_i}$ izango da, nahi genuen bezala.

Soluzioa M moduluarekiko bakarra dela ikusteko, demagun x eta y soluzioak direla. Orduan, $x \equiv y \pmod{m_j}$, $j = 1, 2, \ldots, n$ guztietarako. Gogoratu $a \mid c$ eta $b \mid c$ badugu a eta b elkarrekiko lehenak izanik badakigula $ab \mid c$ dugula. Beraz, hori etengabe aplikatuz, eta moduluak elkarrekiko lehenak direnez, $x \equiv y \pmod{M}$ dugu. Horrela, sistemaren soluzio guztiak elkarren arteko kongruenteak dira M moduluarekiko. □

Adibidea 7.2.6. Egin dezagun lehen planteatu dugun ikasle-taldearen ariketa. Hau da sistema:

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 4 \pmod 7.$$

Egin ditzagun M_j, m_j erako bikoteak: 3 eta 5×7; 5 eta 3×7; 7 eta 3×5. Bézouten identitatea lortuko dugu bikote bakoitzerako:

$$1 = 3 \times 12 - 35, \quad 1 = 21 - 5 \times 4, \quad 1 = 15 - 7 \times 2.$$

Teoremaren frogan erabili dugun notazioarekin, $x_1 = -1$, $x_2 = 1$ eta $x_3 = 1$ ditugu. Horiekin soluzio bat idatziko dugu:

$$x = 1 \times -1 \times 35 + 2 \times 1 \times 21 + 4 \times 1 \times 15 = 67.$$

Sistemaren soluzio guztiak $x = 67 + 105k$ dira, $k \in \mathbb{Z}$ edozein izanik. Ikasle-kopurua 100 baino txikiagoa denez, 67 da erantzuna.

Posible da teorema moduluak elkarrekiko lehenak ez diren kasura ere orokortzea, baina orduan ez da egia soluzioa beti existitzen denik.

7.3 Fermaten teorema txikia. Eulerren funtzioa

Aipatu dugu $ax \equiv 1 \pmod{n}$-k soluzioa duela zkh$(a, n) = 1$ den kasuan eta kasu horretan soilik. Kasu berezi gisa, $n = p$ lehena bada, p-ren multiplo ez diren guztientzako, hau da $\overline{a} \neq \overline{0}$ den guztietarako dago soluzioa. Horrek ondorio interesgarri batzuk dakartza:

Teorema 7.3.1 (Fermaten teorema txikia)**.** *Izan bitez p zenbaki lehena eta $a \in \mathbb{N}$. Baldin a ez bada p-ren multiploa,*

$$a^{p-1} \equiv 1 \pmod p.$$

Froga. Har ditzagun $a, 2a, \ldots, (p-1)a$ zenbakiak. Zerrenda horretan ez daude bi zenbaki p moduluarekiko kongruenteak direnak. Izan ere, $ja \equiv ka \pmod p$

bada, $(j-k)a$ p-ren multiploa da. Baina p lehena denez eta ez denez a-ren zatitzailea, $(j-k)$-ren zatitzailea izango da. Orduan, $j-k=0$ da, $j,k \in \{1,\ldots,p-1\}$ direlako.

Hartu ditugun zenbakiek hondar desberdinak ematen dituztenez p-rekin zatitzean eta ez dagoenez p-ren multiplorik haien artean, $1,2,\ldots,p-1$ dira hondar horiek. Ondorioz,

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

edo, $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Hemendik, $a^{p-1} \equiv 1 \pmod{p}$ ondorioztatzen da, zkh$(p,(p-1)!)=1$ delako. □

Korolarioa 7.3.2. *Baldin eta p zenbaki lehena bada, edozein $a \in \mathbb{Z}$-rako*

$$a^p \equiv a \mod p$$

betetzen da.

Korolarioa 7.3.3. *Izan bitez p eta q zenbaki lehen desberdinak. Baldin $a \in \mathbb{N}$ ez bada ez p-ren ez q-ren multiploa, orduan*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Froga. Fermaten teorema txikia erabiliz, $a^{p-1} \equiv 1 \pmod{p}$ da eta, hortaz, $a^{(p-1)(q-1)} \equiv 1 \pmod{p}$. Era berean, $a^{q-1} \equiv 1 \pmod{q}$ eta $a^{(p-1)(q-1)} \equiv 1 \pmod{q}$. Orduan, $a^{(p-1)(q-1)}-1$ p-ren multiploa eta q-ren multiploa da. Zenbaki lehen desberdinak direnez, pq-ren multiploa da. □

Propietate hauek ere baliagarriak dira zenbait hondar azkarrago eta errazago kalkulatu ahal izateko.

Adibidea 7.3.4. (i) Kalkula dezagun 614^{6943} zenbakia 17-rekin zatitzerakoan lortutako hondarra. Nola $614 \equiv 2 \pmod{17}$ den, orduan $614^{6943} \equiv 2^{6943} \pmod{17}$ dugu. Orain $6943 = 433 \cdot 16 + 15$ denez,

$$2^{6943} \equiv 2^{433 \cdot 16+15} \equiv (2^{16})^{433}2^{15} \equiv 1^{433}2^{15} \equiv 2^{15} \pmod{17}.$$

Ohartu azken aurreko pausuan Fermaten teorema txikia erabili dugula, hau da $2^{16} \equiv 1 \pmod{17}$ dela. Azkenik $2^4 \equiv 16 \equiv -1 \pmod{17}$ denez,

$$2^{15} = 2^{4 \cdot 3+3} \equiv (2^4)^3 2^3 \equiv (-1)^3 2^3 \equiv -8 \equiv 9 \pmod{17}.$$

Bestelako problemak ebazteko ere lagungarri izan daitezke.

Adibidea 7.3.5. Kalkula ditzagun $f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod{5}$-en soluzio posible guztiak. Badakigunez 5 lehena dela, edozein x-rako $x^5 \equiv x \pmod{5}$ dugu. Beraz, $x^{17} = (x^5)^3 x^2 = x^5 = x$ izango da, $x^{14} = x^2$ eta $x^5 = x$. Beraz, ekuazioa honen baliokidea da $x+x^2+2x+1 \equiv x^2+3x+1 \equiv 0 \pmod{5}$. Ez dugu ikusiko oro har nola ebatzi ekuazio kuadratikoak aritmetika modularrean, baina kasu honetan $\mathbb{Z}/5\mathbb{Z}$-n 5 elementu baino ez ditugunez, besterik gabe proba egin dezakegu ikusteko ea zein diren soluzio eta zein ez. Argi dago $\overline{1}$ dela betetzen duen bakarra, beraz hori izango da erro bakarra. Ohartu bestela $(x-1)^2 \equiv x^2+3x+1 \pmod{5}$ ere badugula.

Fermaten teorema txikia gehiago orokortu daiteke.

Definizioa 7.3.6. Izan bedi $n \in \mathbb{N}$. Eulerren funtzioa hau da:

$$\phi(n) = \text{Card}\{k : 1 \leq k \leq n \text{ eta } \text{zkh}(n,k) = 1\}.$$

Bestela esanda, $\phi(n)$ funtzioak, $n > 1$ denean, n baino txikiagoak diren zenbakien artean zenbat diren n-rekin elkarren arteko lehenak kontatzen ditu.

Adibidez, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$ eta $\phi(8) = 4$. Argi dago, $\phi(p) = p - 1$ dela, p lehena bada. Ikus dezagun zenbat balio duen $\phi(n)$-k orokorrean.

Teorema 7.3.7. (i) $\phi(p^k) = p^k - p^{k-1}$ *da,* p *lehena bada.*

(ii) $\phi(m)\phi(n) = \phi(mn)$ *baldin eta* $\text{zkh}(m,n) = 1$ *bada.*

Froga. Ikus dezagun (i) lehenik. Baldin eta $\phi(p^k)$ zenbat den jakin nahi badugu $\{1, \ldots, p^k\}$ multzoan zenbat elementu diren p-rekin elkarrekiko lehenak jakin nahi dugu. Baina horiek denak dira p-ren multiploak izan ezik. Multzo horretan dauden p-ren multiplo kopurua p^k/p izango da, hau da p^{k-1}. Beraz, $\phi(p^k) = p^k - p^{k-1}$.

□

Bigarren atalaren froga ikusi gabe utziko dugu. Baina ohartu bi propietate hauei esker edozein zenbaki naturalen Eulerren zenbakia kalkulatzen dakigula. Izan ere, $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ baldin bada, orduan

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

izango da.

Euler, $\phi(n)$ funtzioa erabiliz, gai izan zen Fermaten teorema txikia orokortzeko.

Teorema 7.3.8. *Izan bitez* $m, a \in \mathbb{N}$. *Baldin* $\text{zkh}(a,m) = 1$ *bada,*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Oro har zenbaki bat lehena den jakitea ez da erraza, faktorizazioa prozesu luzea delako. Baina zenbaki bat lehena ez dela jakiteko Fermaten teorema txikia erabil daiteke. Izan ere, n lehena bada, $a^{n-1} \equiv 1 \pmod{n}$ bete beharko litzateke. Beraz, n emanik gai bagara aurkitzeko $a \not\equiv 0 \pmod{n}$ non $a^{n-1} \not\equiv 1 \pmod{n}$ den, frogatuta geratuko da n ez dela lehena. Adibidez, 247 ez da lehena, izan ere $2^{246} \equiv 220 \pmod{247}$ delako.