Zenbaki lehenen amai gabeko historia

Javier Duoandikoetxea

Matematika saila
Zientzia eta Teknologia Fakultatea/EHU
644 p.k., 48080 Bilbo
javier.duoandikoetxea@ehu.es

Laburpena. Zenbakiak biderkatzen ikasi eta laster, zenbaki lehenaren kontzeptua agertzen da, eskolan ikasten den horietakoa da. Hain oinarrizkoak izanik ere, zenbaki lehenak behin eta berriro agertzen dira matematikaren historian, Grezia zaharreko lehen dokumentuetatik gaur egungo ikerketaraino. Bide luze horretako urrats batzuk erakustea da artikuluaren asmoa, Euklidesen garaiko kontu batzuekin hasi eta berriki frogatu den emaitza bateraino. Amaitzeko, ebazpenaren zain dauden zenbait problema ere aipatuko ditugu.

1. SARRERA

Batek daki noiztik erabiltzen diren zenbakiak, eta noiztik batzen eta biderkatzen diren. Batek daki zenbat denbora igaroko zen baten bat konturatu arte zenbaki batzuk zenbaki txikiagoak biderkatuz lortzen direla eta beste batzuk aldiz ezin direla horrela lortu. Kontu zaharrak dira hauek, matematikaren historia idatzia hasi baino lehenagokoak. Guretzat ere zaharrak dira, umetan eskolan ikasitakoak. Horregatik, harrigarria izango da askorentzat jakitea goi mailako matematikan behin eta berriro agertzen direla, benetako historia amaigabean.

Zalantzarik gabe, irakurleak jakingo du zenbaki txikiagoak biderkatuz lortu ezin direnak *zenbaki lehenak* direla, eta beste guztiak, *konposatuak*. Horrela, 7 edo 13 lehenak dira, eta $24 = 4 \times 6$ eta $35 = 5 \times 7$, konposatuak. Bestetik, komeni da 1 zenbakia ez sartzea lehenen zerrendan, definizioko propietatea bete arren; bestela esanda, 2-tik gorako zenbakietarako balio du eman dugun definizioak.

Esan gabe doa zenbaki hitza hemen zenbaki arruntari dagokiola, kontatzeko erabiltzen diren zenbakiez ari garela, alegia. Zenbaki arrunten mul-

tzoa bitan banatzen da, beraz, zenbaki lehenak eta konposatuak. Baina are gehiago dugu: *edozein zenbaki arrunt,* 1 *baino handiagoa, zenbaki lehenak biderkatuz lor daiteke, eta modu bakarrean, gainera. Aritmetikaren oinarrizko teorema* deitzen den horrek ematen dio benetako zentzua *lehen* berbari zenbakien testuinguruan. Ez baitu esan nahi arrunten zerrendako lehenak direnik, zenbaki guztiak sortzeko *lehengaia* direla baizik.

Zenbaki arrunten propietateak aztertzen dituen matematikaren atalari *Zenbakien teoria* deritzo. Erabiltzen dituen metodoen arabera azpiatalak ditu —aljebraikoa, analitikoa, geometrikoa—. Zenbaki lehenak teoriako toki askotan agertzen dira, batzuetan tresna, beste batzuetan aztergai. Azken alde honi helduko diogu artikuluan, haien zenbait propietate erakutsiz.

Hartu zenbakien zerrenda, banandu alde batean lehenak, bestean konposatuak, eta erraz sortzen dira galderak: zenbat dira zenbaki lehenak?, zeintzuk dira?, zelan daude banatuta? Pentsa liteke hain kontzeptu oinarrizkoak eta zaharrak izanik, haien inguruko galdera *gehienak* aspaldian erantzun direla. Baina, hona hemen zer utzi zigun idatzita Eulerek 1751an: «Orain arte alferrik ibili dira matematikariak zenbaki lehenen segidan ordenaren bat bilatzen, eta baditugu arrazoiak pentsatzeko gizakiaren buruak inoiz ulertuko ez duen misterioren bat dagoela». Ez dakit misterio kontua den, baina galderak egitea erraza bada ere, erantzunak ez dira beti erraz aurkitzen. Erantzun batzuk aspaldikoak dira, Euklidesen *Elementuetan* datoz. Beste batzuk mendeetan zehar heldu dira, galdera berriekin etorri ere, sarritan. Euleren garaitik hona asko aurreratu dugun arren, ugari dira oraindik irekita dauden problemak. Oso modu adierazgarrian esan zuen XX. mendeko aditu handienetako batek, Paul Erdós hungariarrak: «Milioi bat urte joango dira, gutxienez, zenbaki lehenak ulertu baino lehen».

Galdera-erantzun horietako batzuk aukeratu eta matematikaren historian egin duten ibilbidea aurkeztuko dugu artikuluan. Zati batzuk kenduta, gehiena ulertzeko matematikako oinarrizko kontzeptuak baino ez dira behar. Bestalde, asko dira zenbakien teoriazko liburuak. Horietako gutxi batzuk eta zenbait artikulu agertzen dira bibliografian, irakurleak bertan aurki ditzakeelako aipatuko ditugun emaitzak eta informazio gehiago, baina beste batzuk ere hauta zitezkeen helburu berberarekin. Interneten dauden orrietatik *The Prime Pages* izenekoa ([16]) kontsulta daiteke, adibidez.

2. **ZENBAT DIRA?**

Euklidesen *Elementuak* da guregana heldu den matematikako libururik zaharrena, K. a. IV. mendekoa. Oso lan heldua da, lehena izanagatik. Hamahiru liburutan banatzen da eta horietako hirutan (VII, VIII eta IX)

aritmetika aztertzen du. Bertan dugu zenbaki lehenen definizioa eta zenbait propietate. Zenbat diren jakin nahi badugu, hona hemen zer dioen Euklidesek.

> **Elementuak, IX. liburua, 20. proposizioa.** Zenbaki lehenak gehiago dira zenbaki lehenen edozein kopuru proposatu baino.

Gure hitzetan esanda, *infinitu zenbaki lehen daude*. Esan eta gehiago egin zuen Euklidesek, frogatu ere bai. Ezin genezakeen besterik espero, hori baita Euklidesen liburuaren ezaugarria, baieztapenak frogatu egiten direla, matematikaren metodo bilakatu denaren eredua hasiera-hasieratik agertzen da. Hona hemen Euklidesen froga, moldatua.

Demagun p, q eta r zenbaki lehenak proposatu direla. Egin $N = pq + 1$. p ez da N-*ren* zatitzailea. Izan ere, zatitzailea balitz, N eta pqr zatituko lituzke, hortaz, $N - pqr$ ere bai. Baina hau ezinezkoa da, $N - pqr = 1$ delako. Modu berean, q eta r ez dira N-*ren* zatitzaileak. Badugu ez p, ez q, ez r ez den zenbaki lehen bat: N bera, lehena bada; edo haren edozein zatitzaile lehen, konposatua bada.

Horrela dakar Euklidesek froga, hiru zenbaki lehenekin. Bistan da bide berak hasierakoen artean ez dagoen zenbaki lehen batera —edo gehiagora— garamatzala hiru ez den beste edozein kopuru hartuta ere. Eta hori bakarrik gerta daiteke zenbaki lehenen multzoa infinitua izanda.

Harrigarria da zein era erraz eta argian asmatu zuen Euklidesek —edo haren aurreko batek— emaitza sakon hori frogatzen. Euklidesen froga ederra izanagatik, matematikariak beti ibiltzen dira froga berrien bila, hobeto ulertzeko-edo. Baditugu beste zenbait, ikus [13, 1. kapitulua].

3. ZEINTZUK DIRA? (ERATOSTENESEN BAHEA)

Hartu lehen N zenbakiak, 2-tik hasita, eta jarri zerrenda batean. 2 bera utzi eta kendu haren multiploak (hau da, zenbaki bikoitiak). Kendu bako lehenengoa 3 denez, utzi eta kendu 3-ren multiploak. 5 da kendu bako hurrengoa, kendu 5-en multiploak; gero 7-renak, 11-renak, eta abar. $\sqrt{\tilde{N}}$-ra heltzean geldi gaitezke eta ezabatu bako guztiak lehenak dira. Zergatik $\sqrt{\tilde{N}}$-*n* gelditu? $\sqrt{\tilde{N}}$ baino handiagoak diren bi zenbaki (edo gehiago) biderkatuz, N baino zenbaki handiagoa lortzen delako, hain zuzen ere. Zenbaki lehenen zerrendak egiteko bide horri *Eratostenesen bahea* deitzen diogu eta Nikomakok deskribatu zuen *Aritmetikaren sarrera* liburuan, K. o. II. mendean. *Bahea* deitu zion, lehenak eta konposatuak elkarren artetik banandu egiten dituelako. Eratostenes K. a. III. mendeko matematikaria izan zen, Alexandriako Liburutegiko arduraduna.

Hau da 100 baino txikiago diren zenbaki lehenen zerrenda:

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.

Eratostenesen bahearekin berehala egin dezake irakurleak.

Baina, zerrenda luze bat egin gabe, jakin daiteke zenbaki bat lehena den edo ez? Adibide batekin esateko: zelan jakin 2935433 zenbakia lehena den edo ez? Eratostesenen bidetik hau esan genezake: $\sqrt{2935433}$ baino txikiago diren zenbaki lehenen artean zatitzailerik ez badu, lehena da. Horrek 1713tik behera dauden 267 zenbaki lehenekin egiaztatzea eskatzen du, lehena dela ziurtatzeko. Bide segurua da, baina bistan da zenbakia handia izanez gero, oso luzea izan daitekeela. Horregatik galdera: badago bidezidorrik? Betidanik izan da matematikarien artean arazoarekiko jakinmina, eta zenbaki bat lehena den edo ez erabakitzeko hainbat test asmatu dira. Kriptografiako metodo modernoekin lotura duen gaia izanik, garrantzi handikoa da gaur egun. Dena dela, ez dugu hemen gehiago esango, eta [13, 2. kapitulua] eta [4, 3. kapitulua] irakur ditzake interesa duen irakurleak.

4. ZENBAT DIRA ZENBAKI BATEN AURRETIK?

Badakigu infinitu zenbaki lehen ditugula eta horrek kopuruaren auzia ebazten du; aipatu dugu zenbaki jakin bat lehena den edo ez erabakitzea zaila izan daitekeela; baina, jakin liteke multzo *handi* batean gutxi gorabehera zenbat diren lehenak, adibidez? Estatistika Ikuspegia da, nolabait, ez zeintzuk baina zenbat kontuan hartzen dituena. Arazo horrek funtzio baten definizioa iradokitzen du: x baino txikiagoak edo berdinak diren zenbaki lehenen kopurua kontatzen duena, alegia. $\pi(x)$ izendatu ohi da funtzio hori:

$$\pi(x) = \#\{p : p \text{ lehena eta } p \leq x\}.$$

(# ikurrak multzoaren elementu kopurua adierazten du. π izendatu arren, ez du izen bereko zenbakiarekin zerikusirik.) Definizio horretan zenbaki erreal positibo guztiak har daitezke aldagaitzat, ez da zertan arruntetara mugatu. Bistan da $\pi(x)$ zatika konstantea eta gorakorra dela, eta unitate bateko jauzia egiten duela zenbaki lehen batetik igarotzean. Bistan da, halaber, $\pi(x)$-ren balioak jakitea zenbaki lehenen posizio zehatzak ezagutzea izango litzatekeela, eta ez gatzaizkio hasiko π-ri eskatzen zenbaki lehenen segidarako ezagutzen ez dugun hori. Zer bilatuko dute bada matematikariek? Lehen asmoa, $\pi(x)$ «hurbiltzeko» balioko zuen funtzio bat aurkitzea izan zen, erraz deskribatzeko moduko funtzioa, jakina. Geroago, eskakizuna zehaztu egin zen: π-ren joera asintotikoa, hau da, x infiniturantz

doanean π-k duen joera emango duen «funtzio on» bat aurkitu nahi zen. Zerbait badakigu,

$$\lim_{x\to+\infty} \pi(x) = +\infty.$$

Hori da, hain zuzen ere, zenbaki lehenen kopurua infinitua dela esateko modua. Joera asintotikoa ematea hau da: aurkitu infiniturantz π (x)-ren abiadura berean doan funtzio bat. Esan nahi baita, aurkitu f (x),

$$\lim_{x\to+\infty} \frac{\pi(x)}{f(x)} = 1 \qquad (1)$$

izan dadin.

4.1. **Legendre**

Adrien Marie Legendre matematikari frantsesari zor zaio zenbakien teoria aztergai duen lehen monografia: *Essai sur la théorie des nombres,* 1798an kaleratua. Bigarren argitalpenean (1808) π (x)-rako hurbilketa hau proposatu zuen:

$$\frac{x}{\log x - 1,08366}.$$

(Hemen eta aurrerantzean log idatziko dugu logaritmo nepertarra adierazteko.) Legendreren liburuak izan zituen gero ere beste argitalpen batzuk, zuzenduak eta handituak, eta azkena 1830ekoa da, *Théorie des nombres* izen soilarekin. Ondorengo argitalpenak horren kopia dira.

Harrigarria izan daiteke izendatzaileko 1.08366 zenbakia. Baina gogoan izan Legendreren helburua π (x)-ren balio zehatza ahalik eta hobetoen hurbiltzea zela eta ez haren joera asintotikoa ematea. Legendrek

$$\pi(x) = \frac{x}{(\log x - A)x}$$

idatzi zuen, eta A (x) gutxi gorabehera 1,08366 dela esan zuen. Ez dago argi, baina baliteke horrekin $\lim_{x\to+\infty} A$ (x) = 1,08366 esan nahi izana. Bere garaian eskura zituen lehenen tauletan oinarrituta eman zuen balio hori. Taula luzeagoak izan balitu eskura, edo txikiagoa hartuko zuen zenbakia, edo beste aieru bat egingo zuen. Izan ere, $\lim_{x\to+\infty} A$ (x) = 1 da.

Bistan da Legendrek ematen duen funtzioak (1) limitea lortzeko balio badu, berdin balioko duela $x/\log x$ funtzioak ere. Horregatik, joera asintotikoari dagokionez, $x/\log x$ funtzioa har dezakegu Legendreren aierutzat.

4.2. **Gauss**

Gaussek $\pi(x)$ hurbiltzeko

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,\mathrm{d}t$$

funtzioa proposatu zuen. Funtzio horri *logaritmo integrala* deritzo eta hortik datorkio Li notazioa.

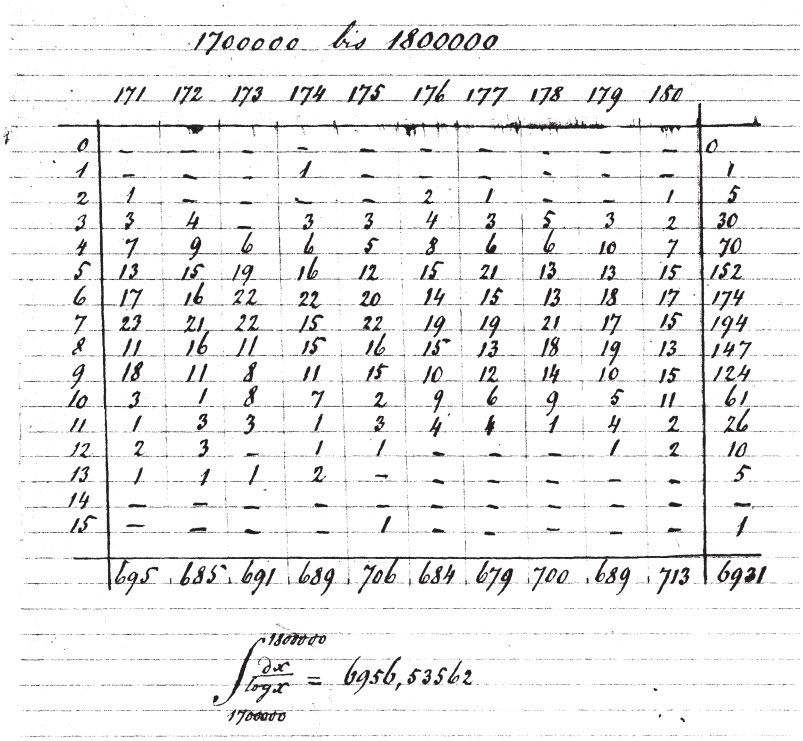
Gaussek berak eman zituen bere ahaleginen berri 1849an, Encke izeneko ikasle ohi bati igorri zion eskutitz batean ([8], [9]). Antza denez, 1792an hasi zen gaia aztertzen, artean 15 urte baino ez zituela. Zenbakiak milakako tartetan banatu eta tarte bakoitzean lehenak zein proportziotan agertzen ziren neurtu zuen. Horrela ikusi zuen zenbaki lehenen kopuruaren dentsitatea $1/\log x$-ren moduan jaisten dela zenbakiak handitu ahala. Hortik ondorioztatu zuen deribatu modura $1/\log x$ duen funtzioak, $\mathrm{Li}(x)$ funtzioak, balio beharko lukeela π-ren hurbilketarako.

Gaussen aierua 1792koa bada, Legendrerena baino lehenagokoa da. Baina Legendrek ezin zezakeen izan haren berri, ez baitzuen Gaussek ezer argitaratu gai horretaz. Enckeri azaldu zionez, bizitza osoan arduratu zen gaztetako aieru haren egokitasunaz eta zenbaki lehenen zerrenda luzeagoak eskuratu ahala, berriro hasten zen kontatzen eta formulak ematen zion balioarekin konparatzen. Hau guztia Gaussen eskuizkribuetan heldu zaigu eta haren lan guztien bilduman jasota dago (ikus adibide bat 1. irudian). 3.000.000rainoko zenbaki lehenak erabili zituen! Enckek eman zion Gaussi Legendreren proposamenaren berri, eta Gaussek eskutitz berean egin zion haren analisi arin bat. Batetik, Legendreren konstante bitxia (1,08366) txikituz joan beharko zela zenbakiak handitu ahala —Legendrek eskura izan zituen taulak baino luzeagoak erabiltzen zituen Gaussek artean—; bestetik, ez zela ausartzen esaten limitean 1 izango zela (eta bada, lehenago esan dugunez).

Galdera bat datorkigu berehala: baliteke Gaussen eta Legendreren proposamenak bateragarriak izatea (1) formularen ikuspegitik? Bai, noski, baina horretarako,

$$\lim_{x\to+\infty} \int_2^{+\infty} \frac{1}{\log t}\,\mathrm{d}t : \frac{x}{\log x} = 1$$

beharko genuke. Erraz ikusten da horrela dela, l'Hópitalen erregela erabiliz, adibidez.



1. irudia. Gaussen eskuizkribua: 1.700.000tik 1.800.000rainoko zenbaki lehenen kontua eta logaritmo integralak ematen duen balioa ([8]).

4.3. **Txebishev**

Txebishev matematikari errusiarrari urrats handi bat zor zaio problemaren bilakaeran. Hark erakutsi zuen $x/\log x$ ordena zuzena izan zitekeela $\pi(x)$ neurtzeko eta hori, batez ere, emaitza bitan:

— *Existitzen dira A eta B zenbakiak,* $0 < A < 1 < B < \infty$ *eta*

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}$$

betetzen dutenak; areago, $A = 0{,}92$ *eta* $B = 1{,}11$ *har daitezke.*

— $\lim_{x\to+\infty} \dfrac{\pi(x)}{x/\log x}$ *existitzen bada,* 1 *da.*

1. taula. $\pi(x)$, Li(x), $x/\log x$ eta $x/(\log x - 1)$ funtzioen balioak aldagaiaren zenbait baliotarako

x	$\pi(x)$	Li(x)	$x/\log x$	$x/(\log x - 1)$
100	25	29,0	21,7	27,7
1.000	168	176,6	144,8	169,3
10.000	1.229	1.245,1	1.085,8	1.218,0
100.000	9.592	9.628,8	8.685,9	9.512,1
1.000.000	78.498	78.626,5	72.382,4	78.030,4
1.000.000	664.579	664.917,4	620.420,7	661.459,0
10.000.000	5.761.455	5.762.208,3	5.428.681,0	5.740.303,8
100.000.000	50.847.534	50.849.233,9	48.254.942,4	50.701.542,5

1852 inguruan argitaratu ziren Txebisheven lan horiek, eta bide bi hartzeko aukera iradokitzen dute: lehen emaitzarako, *A* eta *B*-ren balioak hobetu, gutxienez x jakin batetik aurrera; bigarrenerako, frogatu limitea badagoela, Legendreren eta Gaussen aieruek $\pi(x)$-ren joera asintotikoa ematen dutela berretsiz.

4.4. **Euler**

Euler XVIII. mendeko matematikaria zenez, denboran atzera egitea da Gauss, Legendre edo Txebishev baino beranduago aipatzea, baina badu Euleren formula batek zerikusirik π-ren joera asintotikoa zehaztera eraman zuen bidearekin, eta horregatik dakargu hona. Eulerek 1737an asmatu zuen formula ederra hau da:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ lehena}} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{2}$$

Hemen $s > 1$ da, ezker aldeko gaian zenbaki arrunt guztiak agertzen dira eta eskuin aldeko biderketan zenbaki lehen guztiak.

Ikus dezagun Euleren formularen arrazoia. Har dezagun

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \dots$$

berdintza ($|x| < 1$ denean balio du) eta egin dezagun $x = 1/p^s$. Orduan,

$$\left(1-\frac{1}{p^s}\right)^{-1} = 1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\frac{1}{p^{4s}}+\ldots \qquad (3)$$

Demagun p_1 eta p_2 zenbaki lehenak direla, eta elkarren arteko desberdinak. Bakoitzerako (3) erako garapena idatziz eta eskuin atalak gaiz gai biderkatuz,

$$1+\frac{1}{p_1^s}+\frac{1}{p_2^s}+\frac{1}{p_1^s p_2^s}+\frac{1}{p_1^{2s}}+\frac{1}{p_2^{2s}}+\frac{1}{p_1^s p_2^{2s}}+\frac{1}{p_1^{3s}}+\frac{1}{p_2^{3s}}+\ldots$$

lortzen da. Hau da, agertzen diren gaiak $1/n^s$ erakoak dira, non n-ren balioak p_1 eta p_2 faktore lehenekin idazten diren zenbaki guztiak diren. Geroz eta biderkagai gehiago sartu eta n-rako faktore lehen gehiago dira onargarriak. Zenbaki bakoitzaren faktore lehenen bidezko deskonposizioa bakarra izatea erabakigarria da Euleren formula ondorioztatzeko. Biderketa infinitua denez, kontuz idatzi behar da froga konbergentzia-arazoak gainditzeko, baina aipatutakoa da ildo nagusia.

$s = 1$-erako ere ontzat eman zuen formula, atal bien balioa infinitu dela adieraziz. Horrek, ezinbestean, infinitu zenbaki lehen egotea eskatzen du, zenbaki lehenen kopurua finitua balitz, biderkadura finitua izango bailitzateke. Zenbaki lehenen infinitutasuna erakusteko froga hau eta Euklidesena erabat desberdinak dira. Infinitu izatea baino gehiago ere ematen du Euleren frogak: zenbaki lehenen alderantzizkoen batura infinitua da.

4.5. **Riemann**

Riemannek bospasei lan «historiko» utzi zituen, bakoitza matematikaren arlo baterako mugarritzat har dezakeguna, eta hori berrogei urte bete baino lehen hil zela. Zenbakien teorian argitaratu zuen bakarra da lan horietako bat. *Emandako kantitate baten azpitik dauden zenbaki lehenen kopuruaz* du izenburua, eta laburra da, zortzi orrialdekoa ([6] liburuan testu osoa irakur daiteke, ingelesez). Aipatu berri dugun Euleren berdintzan agertzen den s-ren funtzioa *(Riemannen zeta funtzioa* esaten diogu gaur egun) aldagai konplexuko funtziotzat hartu zuen, hau da, s-rako balio konplexuak onartu zituen. Baina

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

definizioak Re $s > 1$ hartzera behartzen gaitu, bestela serie dibergentea izango genukeelako. (Hemen Res, s-ren zati erreala da.) Aldagai konplexuko funtzioen teoria XIX. mendean garatu zen eta hiru matematikari handiren lana dela esan daiteke: Cauchy, Riemann eta Weierstrass. Riemannen ekarpenen artean funtzio konplexuen *hedapen analitikoa* dago. Eta ζ funtzioarekin izan zuen bide hori erabiltzeko aukera bikaina: plano konplexu osora hedatu zuen funtzio analitiko modura, salbu $s = 1$ puntura, non ezinbestez infinitu izan behar duen *(polo* bat izango du bertan, analisi konplexuan erabiltzen den terminoa erabiliz).

Riemannen zeta funtzioaren eta zenbaki lehenen arteko lotura ez da bakarrik Euleren formulatik ateratzen dena $s > 1$-erako. Oso erlazio estua da eta hainbat formula idatz daitezke ζ, ζ-ren deribatua eta zenbaki lehenak lotuz. Horietako batean *(Riemannen formula esplizitua)* zenbaki lehenen banaketa eta ζ-ren zeroak ($\zeta(s) = 0$ egiten duten s-ren balioak) elkartzen dira. Hortaz, funtsezkoa da zeroak non dauden jakitea.

Ez dago zerorik Re $s > 1$ bada. Zeroak daude -2, -4, -6 eta beste zenbaki negatibo bikoiti guztietan, baina horiek hedapenerako formulak (ζ-ren ekuazio funtzionalak) berehala erakusten dituenez, *zero nabariak* deitzen dira. Beste zeroek, egotekotan, $0 <$ Re $s < 1$ bandan egon behar dute eta Re $s = 1/2$ zuzenarekiko simetrikoak izan behar dute. Hauek dira, hain zuzen ere, aipatu dugun Riemannen formulan esku hartzen dutenak. $\pi(x)$-ren joera asintotikoari dagokionez, Gaussek eta Legendrek proposaturiko funtzioek (1) betetzen dutela egiaztatzeko nahikoa da Re $s = 1$ bada $\zeta(s)$ anulatzen ez dela erakustea.

Baldintza hori baino gehiago espero zuen Riemannek: zero eznabari guztiak Re $s = 1/2$ zuzenean egongo zirela esan zuen, baina ez zen gauza izan horrelakorik frogatzeko. Ez berak ez beste inork ez du gaur arte frogatu, ezta ezeztatu ere. Analisi matematikoko problema irekirik ospetsuena da eta *Riemannen hipotesia* deritzo. Clay Institute-k (2000): urtean *milurtekoko problema* izendatu zuen, beste seirekin batera, eta milioi bat dolarreko saria ezarri zuen frogatzeagatik (ikus [15]).

4.6. **Hadamard eta de la Vallée-Poussin**

XIX. mendea amaitu baino lehen heldu zen desiraturiko teorema. Riemannek ereindako hazitik matematikari bik atera zuten fruitua, nork bere aldetik: Jacques Hadamard frantziarra bata, Charles de la Vallée-Poussin belgiarra bestea. Emaitza bera eta urte berean, 1896an. *Zenbaki lehenen teorema* deitu zaio emaitzari eta aurreratu dugun hori da.

Teorema. $\lim_{x\to+\infty} \dfrac{\pi(x)}{x/\log x} = \lim_{x\to+\infty} \dfrac{\pi(x)}{\mathrm{Li}(x)} = 1$ da.

Esan dugunez, nahikoa zen Re $s = 1$ bada $\zeta(s)$ anulatzen ez dela ikustea, eta hori da matematikari biek erakutsi zutena. De la Vallée-Poussin urrunago joan zen beste lan batean eta errorearen borne bat ere eman zuen:

$$\left|\pi(x) - \mathrm{Li}(x)\right| \leq Cxe^{-a\sqrt{\log x}}, \tag{4}$$

non C eta a konstanteak diren eta $a > 0$. (Ezker ataleko gaiari esaten zaio errorea, benetako balioaren eta balio hurbilduaren arteko aldeari, alegia.) Asintotikoki baliokideak diren arren, $x/\log x$ eta $\mathrm{Li}(x)$ desberdinak dira errorearen ikuspegitik: bigarrenak errore txikiagoa ematen du. (4) desberdintzaren eskuin aldean espero daitekeen funtziorik onena $\sqrt{x}\log x$ da eta Riemannen hipotesia frogatuz gero, korolario modura aterako litzateke. Baina alderantzizkoa ere egia da, eta errorerako $\sqrt{x}\log x$ tamaina lortuz gero, Riemannen hipotesia ondorioztatuko litzateke. Gauza biak baliokideak izanik, ezin pentsa daiteke laster ezagutuko dugun emaitza izango denik.

Zenbaki lehenen teoremak probabilitateen erako irakurketa iradokitzen du: x zenbaki *handi* bat zoriz hartuz gero, lehena izateko probabilitatea $1/\log x$ ingurukoa da.

4.7. **Erdös eta Selberg**

ζ funtzioaren eta zenbaki lehenen arteko erlazioa hain estua zenez, zenbaki lehenen teoremaren frogapenerako beharrezkotzat jo zen funtzio konplexuen analisitik igarotzea. Baina 1949an, ezustean, Paul Erdös hungariarrak eta Atle Selberg norvegiarrak analisi konplexuaren bidea erabat saihestuz heldu ziren zenbaki lehenen teoremara. Selbergen formula batean oinarritu ziren biak eta elkarren arteko komunikazioa izan zen arren, azkenean artikulu bana argitaratu zuten, nork bere ñabardurak sartuz. *Froga elementalak* deitzen diren arren, argi gera bedi analisi konplexua saihesteagatik erabiltzen dela terminoa eta ez froga errazagoa izateagatik.

5. **ZENBAKI LEHENAK SEGIDA ARITMETIKOETAN**

Zenbakiak binaka hartuta multzo bi ditugu: bakoitiak eta bikoitiak. Bigarrenean zenbaki lehen bakarra dagoenez, infinitu zenbaki lehen daude bakoitien artean.

Zenbakiak hirunaka hartuz hiru multzo ditugu: 3n erakoak (3, 6, 9, 12, . . .), $3n + 1$ erakoak (4, 7, 10, 13, . . .) eta $3n + 2$ erakoak (2, 5, 8, 11, . . .). Lehen multzoak zenbaki lehen bakarra du, baina zenbat daude beste bietan? Bietan daude infinitu zenbaki lehen ala bietako batean bakarrik? Ez dirudi erantzuna bistakoa denik.

Hartu orain zenbakiak launaka. $\{4n\}$ segidak ez du zenbaki lehenik eta $\{4n + 2\}$ segidan lehen bakarra dago. Beraz, $\{4n + 1\}$ eta $\{4n + 3\}$ segiden artean infinitu zenbaki lehen daude; bakoitzak ditu infinitu zenbaki lehen ala batek bakarrik?

Zenbaki batean hasi eta gai batetik hurrengora kopuru finko bat gehituz doan segidari *aritmetikoa* deritzo. Gai orokorrak $a + nd$ itxura du, a eta d finkoak izanik; a lehen gaia da ($n = 0$ hartuz) eta d ondoz ondoko gai biren arteko aldea. Zenbaki batek a eta d zatitzen baditu eta 1 baino handiagoa bada, segidako gai guztiak zatituko ditu. Kasu horretan, edo ez dago zenbaki lehenik segidan edo a bakarrik izango da lehena. Baina a eta d zenbakien zatitzaile komun bakarra 1 bada, $a + nd$ segidako zenbaki lehenen kopurua infinitua da ala finitua izan daiteke?

Erraz asma daitekeen galdera da eta ez dakigu nori bururatu zitzaion lehen aldiz. Badakigu, ordea, Legendrek ekarri zuela hizpidera gorago aipatu dugun *Essai de théorie des nombres* liburuan, 1798an. Eta bertan esan zuen horrelako segida batean beti infinitu zenbaki lehen daudela. Esan bai, baina frogatu ez. Ez zebilen oker, hala ere.

> **Teorema.** Izan bitez a eta d zenbaki arruntak eta demagun z.k.h.$(a, d) = 1$ dela. Orduan, $a + nd$ erako infinitu zenbaki lehen daude.

P. Lejeune-Dirichlet matematikari alemaniarrak 1837ko lan batean eman zuen teorema horren froga, Legendrek arrazoi zuela erakutsiz. Froga ez zen erraza eta Eulerek zenbaki lehen guztien infinitutasuna frogatzeko egin zuen moduan, Dirichlet ere gauza izan zen segida aritmetikoko zenbaki lehen guztien alderantzizkoen batura infinitua dela frogatzeko. Baina Euleren frogan ez bezala, hemen bidea are zailagoa zen eta berenberegi sorturiko kontzeptuak erabili zituen Dirichletek: froga horretarako asmatu zituen, hain zuzen ere, *Dirichleten serieak* deitzen ditugunak. Serie horiek bide luzea egin dute harrezkero Zenbakien teorian. Dirichleten teoremaren froga ikusi nahi duen irakurleak [1], [2] edo [14] liburuetan ikus dezake. Inork ez zuen Dirichleten aurretik analisi matematikoa erabili zenbakien teoriako problema batean eta, alde horretatik, zenbakien teoria analitikoaren sortzailetzat hartzen da. Behin Dirichleten eta zenbaki lehenen teoremak eskutan, segida aritmetiko jakin baterako *x-ren* azpitik dauden lehenen kopuruaren joera asintotikoa aztertzea berez agertzen den galdera da. Kopurua emango duen funtzioa $\pi(x)$-ren antzera definitzen da:

$$\pi(x; d, a) = \#\{n : a + dn \text{ lehena eta } a + dn < x\}.$$

De la Vallée-Poussin izan zen $\pi(x;d,a)$ funtzioaren joera asintotikoa argitzeko gauza: z.k.h.$(a_1, d) = 1$ *eta* z.k.h.$(a_2, d) = 1$ *badira,* $\pi(x; d, a_1)$ *eta* $\pi(x; d, a_2)$ *funtzioek joera asintotiko bera dute*. Zenbaki lehenen teoremarekin batuta beste modu batez adieraziko dugu joera hori.

Demagun toki batetik aurrera bat datozen segidak baliokidetzat hartzen ditugula ($\{3n + 2\}$ eta $\{3n + 8\}$, adibidez). Orduan, d-ren balio finko baterako d segida desberdin ditugu, a-ren balioak 1-etik d-raino hartuz. Horietako zenbat segidatan dauden infinitu zenbaki lehen jakiteko, zenbat bider den a d-rekiko lehena kontatu behar da. Kopuru hori $\varphi(d)$ idazten da, hau da,

$$\varphi(d) = \#\{a : 1 < a < d \text{ eta z.k.h.}(a, d) = 1\}.$$

Orduan, $\pi(x; d, a)$ funtzioek joera asintotiko berbera dutenez a-ren $\varphi(d)$ baliotarako, hau aterakodugu: z.k.h.$(a, d) = 1$ *bada,* $\pi(x; d, a)$ *eta* $\pi(x)/\varphi(d)$ *bat datoz asintotikoki*. Eta zenbaki lehenen teorema baliatuz,

$$\lim_{x\to+\infty} \frac{\pi(x;d,a)}{x/\log x} = \lim_{x\to+\infty} \frac{\pi(x;d,a)}{\mathrm{Li}(x)} = \frac{1}{\varphi(d)}.$$

6. ZENBAKI LEHENEN PROGRESIO ARITMETIKOAK

Aurreko ataleko izenburuarekin antz handia duen arren, desberdina da orain aurkitu nahi duguna. Zenbaki lehenak segida aritmetiko batean egongo dira, bai, baina hurrenez hurren agertzea eskatuko diegu. Erraz ikusten da zerrenda finituak soilik espero ditzakegula. Horregatik erabili dugu *progresio aritmetiko* terminoa. Adibidez, 3-5-7 edo 7-13-19 hiru gaiko progresio aritmetikoak dira eta zenbaki lehenak dira denak. Katea luzeagoak egin daitezke? Erraz aurkitzen da boskote bat zenbaki lehen txikien artean; hau da: 5-11-17-23-29. Eta gehiago? Seikote baten bila hasiz gero, hona hemen txikiena: 7-37-67-97-127-157.

Har beza irakurleak zenbaki lehenen taula bat eta saia bedi progresio «luzeak» aurkitzen. Ez zaio erraza gertatuko... Ez dakigu ez non hasi ez zenbanaka hartu, beraz arrakasta izateko denbora luzea eta pazientzia beharko da. Hamar gaiko zerrenda txikiena, adibidez, hau da:

199-409-619-829-1.039-1.249-1.459-1.669-1.879-2.089.

Zenbat denbora eman behar da taularen aurrean emaitza horretara heltzeko? Galderak egiteko orduan hauek ekar ditzakegu:

— k emanda, badago k luzerako zenbaki lehenen progresio aritmetikorik?;
— baiezkoan, kopuru finituan ala infinituan?;
— infinitu badira, eman daiteke x-ren azpitik dauden k luzerako progresioen kopururako joera asintotikoa?

Berriro ere galderak —lehen biak gutxienez— aspaldikoak izan zitezkeen, nahiz ez dugun horren agerpen idatzirik XX. mendera arte. 1923an Hardy eta Littlewood ingelesen aierua dugu: edozein k-tarako progresioak badaudela, eta kopuru infinituan; gainera, x-ren azpitiko kopuruaren joera asintotikoa zein izan zitekeen aurreratu zuten. Lehen emaitza van der Corput matematikari holandarrak eman zuen 1939an: $k = 3$-rako infinitu progresio aurki daitezke eta x-ren azpitikoen kopurua $Ax/\log^3 x$ da asintotikoki *(A*-ren balio zehatza Hardy eta Littlewood-en aieruarekin bat zetorren).

Urteak joan, urteak etorri, ez zen aurrerapenik egin eta $k = 4$-rako ere ez zen ezagutzen progresio kopurua infinitua zen edo ez. Bitarteko emaitza bat Heath-Brown-ek emandako hau: infinitu progresio daude non hiru gai lehenak diren eta laugarrenak gehienez bi faktore lehen dituen (1981). Bestalde, ordenadoreen kalkulu-ahalmena handitu ahala geroz eta k handiagoetarako aurkitu dituzte progresio zehatzak. Hala ere, ezagutzen ditugun luzeenek 23 gai baino ez dituzte; 2004an lortu zen horietako lehena eta 56211383760397 + 44546738095860n da, $n = 0$-tik $n = 22$-raino hartuta.

Aurrekari urri horiekin ezustekoa izan zen Ben Green britainiarrak eta Terence Tao australiarrak 2004an lortu zuten emaitza ([10]).

> **Teorema.** Edozein k-tarako zenbaki lehenez osaturiko eta k luzerako infinitu progresio aritmetiko daude. Gainera, x-ren azpitik dagoen progresio kopurua $\gamma\,(k)\, x/\log^k x$ baino handiagoa da, $\gamma\,(k) > 0$ baterako.

Teorema honek ia guztiz erabakita utzi zuen aurreko galderen erantzuna. *Ia* diogu, joera asintotikoaren balioa barik, behe bornea baino ez duelako ematen. Hardy eta Littlewooden aierura heltzeko $\gamma\,(k)$ konstantea hobetu beharko lukete (laguntzen doakion $x/\log^k x$ funtzioa ona da, hori bai). Hala ere, baliteke laster «ia» hori ere kendu behar izatea, aurten bertan egile berek beste lan batean $k = 4$-rako konstanterik onena lortu baitute.

Terence Tao izan da 2006ko Fields dominaren irabazleetako bat. Lau urtean behin ematen diren Fields dominak Matematikako Nobel saritzat hartzen dira batzuetan, nahiz berrogei urtetik beherakoek bakarrik irabaz dezaketen. Tao saritzeko arrazoien artean emaitza eder hori ere nabarmendu zuten.

Denbora luzez irekita egon diren beste problema batzuen ebazpenean gertatu den bezala, hemen ere beste arlo batzuetako ideiak eta teknikak erabiltzetik etorri da bat-bateko arrakasta. Adituek diotenez, zenbakien teoria analitikora bide berriak ekarri dituzte, beste problema batzuetarako egokiak ere agian, eta baliteke emaitza eder gehiagoren atarian egotea.

7. **ETA BIHAR?**

Astiro bada ere, zenbaki lehenen misterioak —Euleren hitzekin esateko— apur bat argituz doaz. Eta gehiago jakingo dugu, hortik zehar dauden problemetarako erantzunak iritsi ahala. Non lan egin badago, [11] liburuan ikus daitekeenez. Oso planteamendu erraza duten hiru problema zahar aukeratu ditugu eredu modura.

7.1. **Golbachen aierua**

Hona hemen teorema izan nahi duten bi baieztapen:

— *Zenbaki bikoiti guztiak (4-tik aurrera) bi zenbaki lehenen batura modura idatz daitezke.*
— *Zenbaki bakoiti guztiak (7-tik aurrera) hiru zenbaki lehenen batura mo dura idatz daitezke.*

1742an Christian Goldbachek eskutitz bat igorri zion Euleri. Bertan lehen baieztapena frogatzeko proposatu zion, eskuz egiazta daitekeen zerrenda luze batek haren alde egiten zuela eta. Ezin izan zuen Eulerek frogarik eman, eta gaur arte inork ez du frogatu.

Lehenaren frogak bigarrena emango luke, baina baliteke bigarrena frogatzea eta ez lehenengoa. Eta hala da, neurri batean, gaurko egoera. 1937an Vinogradovek hau frogatu zuen: *zenbaki batetik gorako bakoiti guztiak hiru zenbaki lehenen batura modura idatz daitezke*. Nondik gora? Zenbaki *txikietarako* eskuz —edo ordenagailuz— froga baitaiteke. Vinogradoven frogak ematen zuen behe muga oso handia zen, eta ondoren 10^{1346}-raino jaitsi bada ere (2002), zenbaki hori ordenagailuek egiazta ditzaketen zenbakietatik oso goiti gelditzen da (3×10^7-raino heldu zen egiaztapena 2005ean).

Jing Run Chen txinatarrarena da Goldbachen jatorrizko galderarako dugun emaitzarik onena (1966): $2k = p_1 + p_2p_3$ *idatz daiteke, non* p_1 *eta* p_2 *lehenak diren, eta* $p_3 = 1$ *edo lehena*. Bistan denez, p_3-ri lehena izateko aukera kendu behar zaio, baina Chenen teorematik berrogei urte igaro dira aurrera egin barik.

7.2. **Zenbaki lehen bikiak**

2-ko aldea duten zenbaki lehenak *bikiak* dira. (Kontuan izan edozein bikoteren aldea 2 edo gehiago dela, 2 — 3 bikotea kenduta.) Zenbaki lehen bikiak erraz aurkitzen dira taula eskuan hartuta: 3-5, 5-7, 11-13, 17-19,

29-31, 41-43, 59-61, 71-73 eta abar. Espero dezakegun teorema hau da: *infinitu zenbaki lehen biki daude*. Baina ez dakigu egia den edo ez. Gorago aipatu dugun Euleren eta Dirichleten lanen bidetik, nahikoa izango zen horien alderantzizkoen batura infinitua dela frogatzea, baina finitua da (Viggo Brun, 1926), eta teoremaren frogak beste bide bat eskatzen du.

7.3. **Zenbaki lehenen arteko tarteak**

Demagun era honetako emaitza baten bila gabiltzala: $n \leq n_0$ *bada, n eta* $n + d\,(n)$ *artean zenbaki lehen bat dago, gutxienez*. Zein $d\,(n)$ funtzio har dezakegu? Jakina, $d(n)$ ahalik eta txikien nahi dugu. Zenbaki lehenak kontatzeko sartu dugun π funtzioa erabiliz, $\pi\,(n + d\,(n)) - \pi\,(n) > 0$ eskatzen ari gara.

Bertranden postulatua deritzo $d\,(n) = n$ kasuari, hau da, n eta $2n$ artean beti zenbaki lehen bat dagoela dioen baieztapenari (hemen $n_0 = 2$ har daiteke). Joseph Bertrand frantsesak enuntziatu zuen arren (1845), Txebishevek eman zuen lehenengo froga, 4.3 atalean aipatu dugun haren lehen emaitzatik $\pi\,(2n) - \pi\,(n) > 0$ ateratzen baita. Harrezkero $d\,(n)$ hobetu egin da eta tamaina txikiagoko tarteetan koka ditzakegu lehenak: ezaguna da $d\,(n) = Cn^{\theta}$ erako funtzioetan $\theta > 6/11$ har daitekeela. Baina ez dakigu $\theta = 1/2$ nahikoa den edo ez. Edo, ia gauza bera dena, era politagoan galdetuta: *beti dago zenbaki lehen bat* n^2 *eta* $(n + 1)^2$*-ren artean?*

8. **BIBLIOGRAFIA**

[1] E. Aparicio: *Teoría de los números,* UPV/EHUko Argitalpen Zerbitzua, 1993.

[2] T.M. Apóstol: *Introduction to Analytic Number Theory,* Springer-Verlag, 1976 (gaztelaniaz, Editorial Reverte, Barcelona, 1984).

[3] P.T. Bateman eta H.G. Diamond: «A hundred years of prime numbers», Amer. Math. *Monthly* 103 (1996), 729-741.

[4] R. Crandall eta C. Pomerance: *Prime numbers. A computational perspective,* Springer-Verlag, New York, 2005.

[5] H.G. Diamond: «Elementary methods in the study of the distribution of prime numbers», *Bull. Amer. Math. Soc. (N.S.)* 7 (1982), 553-589.

[6] H.M. Edwards: *Riemann's Zeta Function,* Academic Press, NewYork, 1974.

[7] Euklides: *Elementuak* (Patxi Anguloren itzulpena), Elhuyar, Donostia, 2005.

[8] C.F. Gauss: *Werke,* 2. bol., Georg Olms Verlag, New York, 1973.

[9] L.J. Goldstein: «A history of the prime number theorem», *Amer. Math. Monthly* 80 (1973), 599-615.

[10] B. GREEN eta T. TAO: *The primes contain arbitrarily long arithmetic progressions,* Annals of Math., argitaratzeko.
[10] R.K. GUY: *Unsolved Problems in Number Theory,* 3. arg., Springer-Verlag, 2004.
[12] G.H. HARDY eta E.M. WRIGHT: *An introduction to the theory of numbers,* Oxford University Press, 1979.
[13] P. RIBENBOIM: *The little book of big primes,* Springer-Verlag, 1991.
[14] G. TENENBAUM eta M. MENDES-FRANCE: «Les nombres premiers», *Que Sais-je?* 571 zenb., PUF, Paris 1997.
[15] *http://www.claymath.org/millennium.*
[16] *http://primes.utm.edu.*