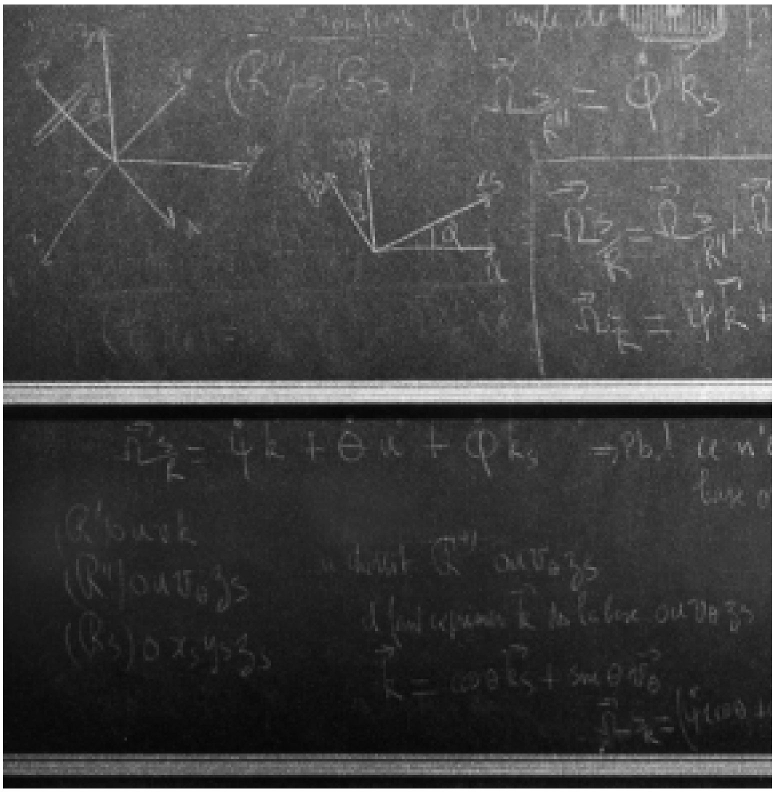


Fermat-en azken teoremaren inguruan

Javier Duoandikoetxea*

1993ko ekainaren 23an Cambridgeko Unibertsitateko Newton Institutuan, hiru hitzaldiko saioa amaitzen ari zelarik Andrew J. Wiles, Princetongo Unibertsitateko irakasle den matematikari ingelesak hauxe idatzi zuen frogatutako teoremaren ondorio gisa: *p zenbaki lehena bada, 2 baino handiagoa, u, v, eta w razionalak badira eta* $u^p + v^p + w^p = 0$ *bada, orduan* $uvw = 0$.

Entzuten ari ziren matematikariak berehala konturatu ziren Wiles-ek "Fermaten teorema" izenaz ezagutzen den Matematikaren problema korapilatsua horrenbestez askatutzat ematen zuela. Laster zabaldu zen berria munduko matematikari guztiengana. Baita matematikari ez zirenengana ere; egunkari, irrati eta telebistako aipamenak lekuko. Wilesen eskuizkribua, hala ere, gutxi batzuen eskuetan zegoen; frogapenak zeuzkan alderdi tekniko guztiak egiaztatu arte ez baitzuen egileak argitara eman nahi. Eta dirudienez, zati batek hutsuneak zeuzkan (ez erroreak) eta horiek estali arte Fermaten azken teoremak problema irekia izaten segitu beharko zuen. Zalantza honekin itxi nuen artikuluaren lehen bertsioa, baina duela egun batzuk zabaldu den berri baten arabera, falta zen kalkulua egin dute, eta adituen onespenaren zain egon behar badugu ere, badirudi oraingoan teorema izena bere benetako zentzuan jarri ahal izango diogula Fermatek proposatu zigun emaitzari.

Fermat

Problemari izena eman dion gizasemea, Pierre de Fermat alegia, 1601. urtean jaio zen Beaumont de Lomagne-n, gaurko Tarn eta Garona departamentuan, kokatuta dagoen herri gaskoian. Familia aberatseko semea zen (aita merkataria baitzuen) eta Legeak estudiatu zituen Tolosa, Bordele eta Orleans-ko Unibertsitateetan. 1631. urtetik aurrera Tolosako Parlamentuan lan egin zuen abokatu modura. Izan ere, Newton eta Leibnizekin batera XVII. mendeko Matematikaren gailurrean egon zen Fermat, ez zen inoiz erabat Matematikara dedikatu; lanetik kanpo baizik. Baina garai hartako Unibertsitateen egitura gaurkoaren alboan oso bestelakoa zen, eta zientzilari ez-profesionalengandik etorri zen askotan Zientzien aurrerapena. Castres-en hil zen 1655ean.

Bordelen egon zen bitartean ekin zion, antza denez, François Viète matematikariaren lana estudiatzeari eta honen idazkera sinbolikoak zekarren erraztasunaz baliatu zen Fermat bere lanetan. Diogun, bidenabar, Viète ere ezagunagoa zela bere garaian politiko gisa eta Enrike IV.aren (Nafarroako Enrike III.aren) kontseilari pertsonala izan zela. Matematikaren arlo guztietan ikus daitezke Fermaten ekarpenak: Geometria Analitikoaren hastapenak eman zituen Descartes-en garai berean, Analisian maximo eta minimoak kalkulatzeko eta koadraturak egiteko metodoak proposatu zituen, nahiz eta laster Newton eta Leibnizen Kalkulu Infinitesimalak ilunduta utzi, eta Zenbakien Teoria berarekin sortu zen alor independente gisa, esaten denez. Optikan ere argiaren errefrakzioaren legeari *Fermaten printzipioa* esaten zaio eta Probabilitatearen hastapenetan Pascalekin batera agertzen da. Hala ere, ez zuen bizi zen artean ospe handirik izan; ez baitzuen libururik argitaratu. Eskutitzetan, lan txiki batzuetan eta eskuizkributan heldu zaizkigu haren lanak. Ekarpen guztien aipamen soila egiteak ere luze joko liguke eta hemen Fermaten azken teoremaren bilakaerari baino ez gatzaizkio lotuko.

Grekoen artera jo behar dugu lehen aztarnen bila; haiek arduratu baitziren lehenengoz zenbaki eta irudi geometrikoez. K.o. III. mendean Alexandrian bizi zen Diofanto matematikariak idatzi zituen liburu batzuetan biltzen zen grekoek aritmetikaz zuten ezagutza. Liburu horiek arabierara itzuli ziren eta arabiarren Matematikan nabaria izan zen beren eragina. Erdi Aroan, Europako mendebaldera heldu zirenean jatorrizko hamalautik sei besterik ez ziren gelditzen. Galduta zeuden zazpi liburuetatik lau Irango Meshed-en aurkitu dituzte oraintsu, 1971. urtean, arabierazko itzulpenean. Aspaldiko sei haiek 1621. urtean eman zituen argitara Bachet de Mériziac-ek, grekoari latinezko itzulpena eta iruzkinak erantsiz. Hauxe izan zen Fermatentzat Zenbakien Teoriako emaitzen iturri nagusia. Hain zuzen, liburuan bertan idazten zituen Fermatek bere ohar eta iruzkinak eta hil eta gero semeak hartu zuen Diofantoren *Arithmetica* aitak eginiko oharrekin argitaratzeko ardura.

Problemari izena eman dion gizasemea, Pierre de Fermat alegia, 1601. urtean jaio zen Beaumont de Lomagne-n, gaurko Tarn eta Garona departamentuan, kokatuta dagoen herri gaskoian. Castres-en hil zen 1655ean.

Dagokigun problemari lehen aztarnak hirukote pitagorikoetan aurkituko dizkiogu, hau da, $x^2 + y^2 = z^2$ ekuazioa betetzen duten zenbaki osoen kalkuluan. Adibidez, (3, 4, 5) edo (5, 12, 13). Lan-pixka batekin, denak ematen dituen formula bat ere lor daiteke. Fermatek galdera orokortu eta karratuen lekuan beste edozein berretzaile erabiltzea proposatu zuen. Eta aipatu dugun *Arithmetica* liburuaren ertz batean hauxe idatzi zuen: "Ezinezkoa da kubo bat bi kubotan banatzea, eta bikoadratu bat bi bikoadratutan edo, oro har, karratua ez den beste edozein berredura, berretzaile bereko bi berreduratan. Honen frogapen benetan zoragarria aurkitu dut, baina orrialde-ertz hau txikiegia da bertan sartzeko". Hau da,

$$x^n + y^n = z^n$$

ekuazioak ez duela ebazpen oso positiborik, n bi baino handiagoa denean, aldarrikatu zuen Fermatek. Frogapenik gabe utzi zizkigun beste emaitza batzuetan hauxe bakarrik gelditu zen frogatu ezinik handik urte batzuetara, eta horrexegatik esaten zaio *Fermaten azken teorema*, berez frogatu gabeko emaitzak teorema izena merezi ez badu ere.

Gaur egun ez du inork sinesten Fermaten emaitza honek frogapena zuenik. Eskutitzetan $n = 3$ kasua bakarrik aipatu zuen eta $n = 4$ kasua beste problema baterako erabili zuen metodoak ebazten du. Baliteke bi hauetatik orokortzea posible zela uste izatea edo beste akatsen bat egitea, baina ez dago hori zehazteko modurik.

Kummer

Nahikoa da $n = 4$ eta n lehena bakoitia kontutan hartzea; beste guztiak hauetara labur baitaitezke. XIX. mendearen hasieran $n = 3$ eta 4 kasuak bakarrik ziren ezagu-

nak. Legendre-k lortu zuen $n = 5$e-rako erantzuna 1825ean eta Dirichlet-ek kasu horretarako beste frogapen bat eman ondoren, $n = 7$ kasua aztertu zuen. Hau frogatu ezinik, $n = 14$ ebatzi zuen 1832an eta zazpi urte geroago Lamé-ren eskutik etorri zen $n = 7$rentzako erantzuna. Bitartean Frantziako Akademiak sari bat eskaini zuen frogapen osoa ematearen truke.
Benetako aurrerapena 1844-47 urte-bitartean heldu zen Ernst Kummer-en lanarekin. Honek zenbaki *oso ziklotomikoak* estudiatu zituen, hots,

$$a_0 + a_1\omega + ... + a_{n-1}\omega^{n-1}$$

erakoak, non

$$a_0, a_1, ... , a_{n-1} \text{ osoak}$$

eta

$$\omega = e^{2\pi i/n} \text{ (beraz, } \omega^n = 1)$$

diren.

Zenbaki hauek, ohiko osoak bezala, zenbaki lehenetan faktoriza daitezke, baina ohikoekin ez bezala, kasu batzuetan faktorizazio bat baino gehiago egon daiteke zenbaki berarentzat. Ez zen hasieran arazo honetaz konturatu eta oker batzuk egin zituen, baina gero konpontzeko *zenbaki idealen* teoria sortu zuen alde batetik eta *klase-gorputzak*, bestetik. Faktorizazioa zein "txarra" izan daitekeen neurtzeko, *klase-kopurua* delako kontzeptua sartu zuen. Honekin lotuta *zenbaki lehen erregularrak* definitu zituen eta hauentzat Fermaten azken teorema egia dela frogatu ere egin zuen. Zenbaki hauek ezagutzeko irizpide bat erakutsi zuen eta 100dik beherako zenbaki lehenetatik 37, 59 eta 67 bakarrik dira irregularrak. Bapatean ikaragarrizko aurrerapena eragin zuen Kummer-en berrikuntzak.

1850ean Frantziako Akademiak bigarrenez saria eskaini zuen arren, handik urte batzuetara kendu eta sari nagusiko urrezko domina Kummerri ematea erabaki zuten, Cauchy-k proposatu bezala. Ehunen azpitik falta ziren kasuak aztertzeko metodoak garatu zituen gero Kummerrek baina XX. mendearen hasieran Vandiver-ek bete zituen hark utzitako zuloak.
XIX. mendean ez zen aurrerapauso osorik eman, baina zenbait emaitza partzial eskuratu ziren.

1850ean Frantziako Akademiak bigarrenez saria eskaini zuen arren, handik urte batzuetara kendu eta sari nagusiko urrezko domina Kummerri ematea erabaki zuten, Cauchy-k proposatu bezala.

XX. mendearen hasieran, 1905ean, Göttingen-go Zientzi Elkarteko Paul Wolfskehl-ek ehun mila marko eskaini zituen frogapena emango zuen lehenengoarentzat. Diruaren hotsak matematikari profesionalak ezezik, zaleak ere atera zituen plazara eta ehundaka ustezko ebazpen heldu zitzaizkien. Denak alferrik, ordea. Sariaren balioa oso murriztuta gelditu zen markoaren debaluazioak medio, baina badaude diru-saririk gabe ere bitarteko erabat elementalekin frogapena egin dutela uste dutenak.

XX. mendea

XX. mendean ordenadoreen kalkulu-ahalmena handiagotu den neurrian n-ren balio berezientzat egiaztapenak egitea posible izan da. Honek ezin du inola ere teorema osoa frogatu, baina $n = 4.000.000$ren azpitik egia dela jakiteak (horretara heldu ziren 1993an) nekez utz dezake aurkakoa sinesteko zirrikiturik. Hala ere, Matematikan frogapenak behar dira.
Geometria algebraikoaren garapenak ekarri zuen XX. mendean estrategi aldaketa Fermaten azken teoremari dagokionez. Kurba eta gainazalen estudioetan agertu diren problema batzuk Fermaten teoremarekin erlaziona daitezke. Hiru alorretan (geometria diofantikoan, gainazal aritmetikoetan eta kurba eliptikoetan) proposatu diren aieruetako batzuetatik berehala ondorioztatzen zen Fermatena.
1983. urtean Gerd Faltings alemaniarrak, Mordell-ek hirurogei urte lehenago proposatutako aieru bat frogatu zuen eta, ondorioz, $x^n + y^n = z^n$ ekuazioak n bakoitzeko "benetan" desberdin diren soluzioen kopurua finitua dela, $n \geq 3$ denean. Hona zer esan nahi dugun "benetan" desberdinak horrekin. (3, 4, 5) hirukoteak $x^2 + y^2 = z^2$ ekuazioa betetzen badu, bistan da (6, 8, 10), (9, 12, 15) eta, oro har, edozein multiplok ere betetzen duela. Horiek denak ebazpen berdintzat jo ditzakegu. Baina (5, 12, 13) eta (7, 24, 25) hirukoteak ere ebazpenak dira eta ez dira berdinak. Eta

erraz ikus daiteke $n = 2$ kasuan ebazpen desberdinak infinitu direla. Faltings-en teoremaren arabera ez da hori gertatzen $n \geq 3$ denean. Bat ere ez dagoela frogatzea da helburua, baina bitartean aurrerapauso sakona izan zen hura. Mordell-ena ezezik, beste bi aieru nagusi ebatzi zituen Faltingsek eta 1986an Fields domina irabazi zuen horiei esker.

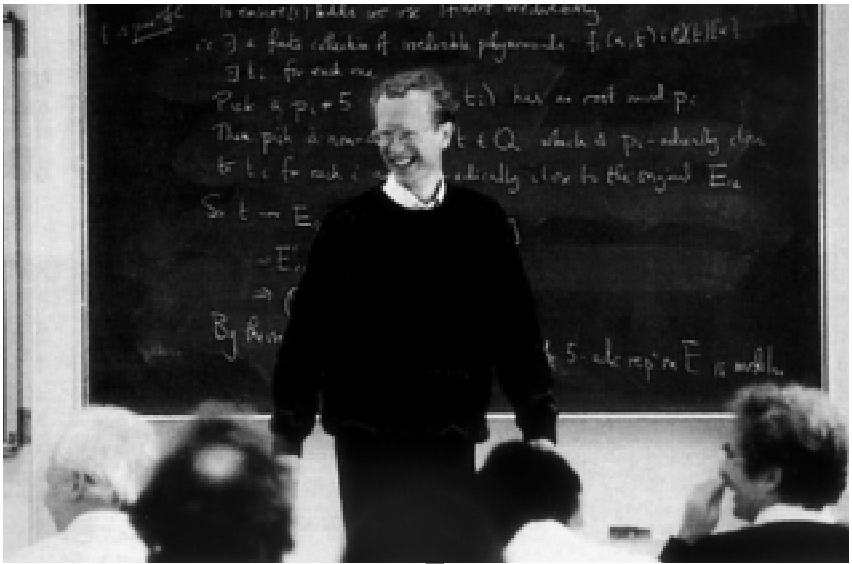
Bestetik, duela sei bat urte Miyaoka-k gainazal aritmetikoekin erlazioa duen desberdintza bat aldarrikatu zuen (Bogomolov-Miyaoka-Yau esaten zaio desberdintzari). Egia izan balitz, n-ren balio finko batetik gorakoentzat bederen Fermaten azken teorema betetzen dela ondorioztatuko genukeen, baina akats bat aurkitu zioten frogapenari eta bere horretan gelditu ginen.

Wilesen lana kurba eliptikoen alorrean kokatzen da. 1955ean Yukata Taniyama matematikari japoniarrak aieru bat proposatu eta hurrengo hamarkadan Goro Shimura-k zehaztu zuen. Algebrarien terminologian hauxe dio: “Zenbaki razionalen gaineko edozein kurba eliptiko, modularra da”. Urte askotan inori ez zitzaion bururatu aieru honek Fermaten teoremarekin zerikusia izan zezakeenik, harik eta Gerhard Frey alemaniarrak 1985-ean Taniyama-Shimura aierua Fermaten teorema baino gogorragoa dela esan zuen arte, hau da, lehenengoaren frogapenak bigarrena dakarrela berarekin adierazi arte. Ez zen zehazteko gauza izan, baina hurrengo urteetan Jean Pierre Serre-k bideratu eta Kenneth Ribet-ek bukatu zuen lanarekin Frey zuzen zegoela argi gelditu zen.

Andrew Wilesen azken urteotako lanaren helburua Taniyama-Shimuraren aierua izan da. Kasurik orokorrena frogatu ez arren, kurba askotarako egiaztatzea lortu omen zuen eta horietan zeuden Fermaten teorema erabakita uzten zutenak. Adituen esanetan frogapenak sinesgarritasun handia zuen eta horregatik zabaldu zen berria munduan zehar. Ohi den bezala, argitaratu aurretik lana aditu batzuen esku gelditu zen hauek onespena eman zezaten. Hilabete batzuk geroago, zerbait oker zegoela hasi ginen entzuten. Gauzak argitu nahian, Wilesek berak ohar bat kaleratu zuen 1993ko abenduan eta honakoa aitortu zuen: bere eskuizkribuan berrikuste-lanetan osatu beharreko puntu batzuk aurkitu zituztela eta gehienak konpondu zituela ere bai; bakar batek, hala ere, ihes egin ziola, eta horrek eskatzen zuen kalkulua menperatu arte bere lana amaitutzat ezin eman genezakeela. Bide batez, udaberrian eman behar zuen ikastarorako agintzen zituen egindakoaren xehetasunak eta falta zena orduarako betetzeko esperantza agertu zuen.

Udaberria eta uda joan ziren, eta beste berririk ez zegoenez, horrekin eta agian laster frogapena hel zitekeela esanez bukatu nuen artikulu honen lehen zirriborroa. Baina azken idazketa eta zuzenketak egiten ari nintzelarik heldu zen noizbait espero genuen berria.

1994ko urriaren 25ean zabaldu zen, aurrekoan baino zalaparta gutxiagorekin hala ere. Hasierako euforia haren ondotik berrikusi beharra Unibertsitateetan gelditu zen bezala, hau ere, seguru asko, inguru profesionaletara mugatuko da. Diotenez, konpondu beharreko arazoari beste bide batetik heldu diote eta arrakasta izan dute. Wilesek lehengoan zuhurtziaz jokatu eta gutxi batzuen esku utzi zuen eskuizkribua. Oraingoan ere berdin egingo zuen, noski, baina urriaren 25ean eskuizkribua zabaldu duenez, segurantza duen seinaletzat har dezakegu. Eta harekin batera Richard Taylor-ekin egin duen bigarren lana dator, antza denez hasierakoan falta zuen kalkulua nola egin daitekeen azaltzen duena. Eskarmentuak erakusten digunez, azken bedeinkapenak etorri arte ezin esan dezakegu behinbetirako frogapena daukagunik.



Andrew Wiles (1993). Andrew Wilesen azken urteotako lanaren helburua Taniyama-Shimuraren aierua izan da. Kasurik orokorrena frogatu ez arren, kurba askotarako egiaztatzea lortu omen zuen eta horietan zeuden Fermaten teorema erabakita uzten zutenak.

Baina, aldi berean, 350 urte luzetan matematikarien buruhauste famatuen bihurtu zen problema ebatzita dagoela sinesteko arrazoi asko ditugula ere esan beharra dago. Eta txantxetan esan denez, Fermatek arrazoi zuen orrialde-ertzean kabitzen ez zela idatzi zuenean.

*** Matematikaria eta Euskal Herriko Unibertsitateko irakaslea.**