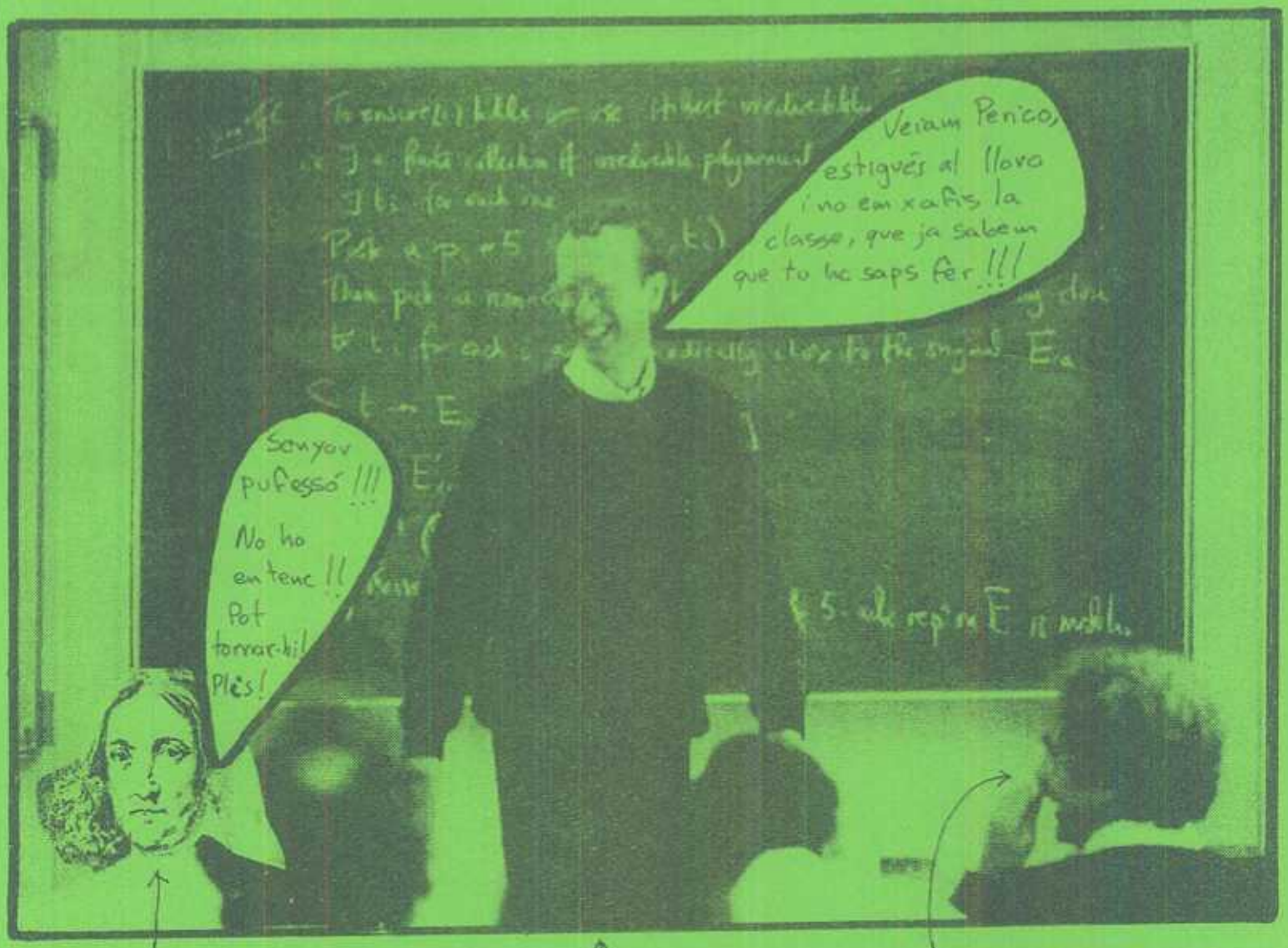
THE LAST FERMAT'S THEOREM

(o l'història de mai acabar, o l'última vacil· lada d'en Pere Fermat, o el perquè dels perquès, o de com 2 i 2 evidentment no fan 4)

Hi havia una vegada una aula de la Universitat de Cambridge on es va començar a coure una olla amb uns ingredients .gens habituals...



En Pere de Can Fermat :
El culpable de l'enrenou
(i perquè no es va fer pagès?)

El de peu :
Andrew Wiles
(el pare de la criatura)

Matemàtic aburrit posant-se el dit al nas!
(o era físic?)

DOCUMENT NO APTE PER A MALALTS DEL COR.

(Suplement de regal. Prohibida la venda.) 10 94

WILES vs FERMAT

A l'estiu, va esclatar la notícia: "ANDREW WILES DIU HAVER DEMOSTRAT EL DARRER TEOREMA DE FERMAT."

En la conferència d'inauguració del curs 93-94 la Marta Sanz va dir que just després d'exàmens es faria a la nostra facultat un seminari de dos dies sobre el teorema de Fermat. S'encarregaven de coordinar-lo la Pilar Bàyer i en Josep Pla. La idea era fer una visió històrica i introducció a la demostració a un nivell d'estudiant que ha cursat Àlgebra. Els redactors de l'ALEPH vam encarregar un article a en Josep Pla, previ al seminari. Aquest article ha esdevingut 18 pàgines i, per tant, mereixedor d'entitat pròpia. Agraïm de tot cor aquesta col·laboració amb un article excel·lent (pedagògic, amè, per a totes les edats,...).

La redacció de l'Aleph volia treure la revista, i amb ella l'article, abans del seminari per tal que no perdés actualitat. Com que el vist i plau de la demostració no va arribar, es va dubtar de fer el seminari previst. Es va postposar la decisió fins a finals de febrer. Al final s'ha aplaçat perquè -segons diu la nostra degana Marta Sanz- això està en mans de l'equip de teoria de nombres i no ha cregut convenient fer-lo encara. Li vam preguntar a la Pilar Bàyer i ens va dir que: "quan es difongui el treball d'en Wiles es podrà fer el seminari. No cal tenir la demostració del teorema de Fermat per fer-lo. Els avenços (donats per demostrats) que ha fet Wiles ja es mereixen per si sols el seminari de dos dies." (recordem que només hi ha 5 equips d'investigació al món que tinguin aquest treball) És a dir, el seminari ha quedat penjat "sine die".

Per això no calia donar-se pressa a treure l'Aleph i podria sortir després d'exàmens. D'aquesta manera no distrauriem, en epòca d'exàmens, els aplicats estudiants (!).

El desembre els diaris informaven d'un error en la demostració. Però, tal com ens informava la Núria Vila, no es tractava d'un error sinó d'una llacuna en la demostració. És a dir, no s'havien demostrat tots els casos. S'havien deixat per obvies coses que no ho eren (igual que fan els profes a classe) i a més ha oblidat estudiar un tipus de corbes -de possibles solucions-, les corbes el·líptiques semiestables.

El 4 de desembre Andrew Wiles enviava un "mail" (correu electrònic) informant que creia poder omplir les llacunes que havia deixat buides (és a dir, demostrar a classe allò que ell veia obvi i cap alumne veia per cap banda). Una fotocòpia reduïa del "mail" la podeu trobar a la pàgina següent. Afegim a continuació una traduccció al català:

Hallado un error en la demostración del teorema de Fermat

Washington.–El matemático británico Andrew Wiles, de la Universidad de Princeton, que en junio presentó una demostración del teorema de Fermat ha admitido la existencia de un error en su razonamiento tras intensas consultas con otros científicos. Wiles anunció que había resuelto el enigma del teorema, enunciado por Fermat hace 350 años pero nunca demostrado. –AFP.

"El Periódico" del dia 11 de desembre del 93

(TRADUCCIÓ:) "En vista de l'especulació sobre l'estat del meu treball sobre la conjectura de Taniyama-Shimura i l'últim Teorema de Fermat, donaré un breu informe sobre la situació. Durant el procés de revisió han aparegut alguns problemes, molts del quals han estat resolts, però n'hi ha un en particular que encara no l'he solucionat. La clau en la reducció de molts casos de la conjectura de Taniyama-Shimura per al càlcul del grup de Selmer és correcte. Malgrat tot, el càlcul final d'una cota superior precisa per al grup de Selmer en el cas semiestable (de la representació del quadrat simètric associada a la forma modular) no està completa encara que es digué així. Crec que seré capaç d'acabar-ho en un futur pròxim usant les idees explicades en les meves conferències a Cambridge. El fet que quedi una gran quantitat de treball per a fer en el meu manuscrit el fa encara inadequat per a un *preprint* (edició prèvia per compte de l'autor). En el meu curs a Princeton que començarà el febrer, donaré un complet informe d'aquest treball."

Hola!
Potser ja ho has rebut per altres vies, pero per si no es aixi t'envio el missatge que en Wiles es va veure obligat a escriure despres de la publicacio a Le Monde de les opinions d'en Coates i en Serre.

Anna

From: wiles@rugola.Princeton.EDU (Andrew Wiles)
Newsgroups: sci.math
Subject: Fermat status
Message-ID: <1993Dec4.013650.12700@Princeton.EDU>
Date: 4 Dec 93 01:36:50 GMT
Sender: news@Princeton.EDU (USENET News System)
Organization: Princeton University
Lines: 21
Originator: news@nimaster
Nntp-Posting-Host: rugola.princeton.edu

In view of the speculation on the status of my work on the Taniyama-Shimura conjecture and Fermat's Last Theorem I will give a brief account of the situation. During the review process a number of problems emerged, most of which have been resolved, but one in particular I have not yet settled. The key reduction of (most cases of) the Taniyama-Shimura conjecture to the calculation of the Selmer group is correct. However the final calculation of a precise upper bound for the Selmer group in the semistable case (of the symmetric square representation associated to a modular form) is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures.

The fact that a lot of work remains to be done on the manuscript makes it still unsuitable for release as a preprint . In my course in Princeton beginning in February I will give a full account of this work.

Andrew Wiles.

El primer dia del curs a Princeton va dir que no tenia el treball acabat. Segons la Pilar Bàyer, es creu que va per llarg.

És possible, doncs, que -finalment- el Teorema de Fermat sigui fals? Potser ens hem precipitat dedicant-li l´Aula 10 a Pierre de Fermat ?

ALEPH
Barcelona, març 1994.

Notes i reflexions a l'entorn de la demostració del Darrer Teorema de Fermat

JOSEP PLA I CARRERA

Facultat de Matemàtiques
Universitat de Barcelona

Ja fa uns mesos, quan l'eufòria de la descoberta ens envoltava a tots, els estudiants de la Facultat responsables de l'edició del proper número de la revista ALEPH van tenir la gentilesa de demanar-me si volia escriure unes ratlles sobre la Bona Nova:

> el professor ANDREW WILES de la UNIVERSITAT DE PRINCETON ha aconseguit de demostrar finalment el darrer teorema de Fermat.

Jo els vaig dir, deixant-me endur per l'eufòria, que ho intentaria, però la indolència que fa que deixem per l'endemà allò que hauríem d'haver resolt ahir —"No hi ha mai res tan urgent que no pugui esperar tres mesos", deia el meu antic professor FRANCESC D'ASSÍS SALES— m'ha portat a deixar passar tres mesos abans de posar-m'hi. I ara em trobo que l'eufòria ha passat i l'ambient s'ha anat enrarint a poc a poc fins que finalment sembla que, en la demostració d'ANDREW WILES, hi ha una llacuna que cal omplir.

A l'entremig i al nostre entorn immediat, s'han produït tanmateix dos fets que cal remarcar: d'una banda l'aparició del número 190 de *Ciencia y Tecnología* de LA VANGUARDIA, dedicat completament al darrer teorema de Fermat, ens ha proporcionat una excel·lent ocasió d'apropar-nos ben planerament, gràcies a un grapat d'articles molt acurats escrits per vertaders entesos en la qüestió, a les vicisituds històriques del preuat teorema; d'una altra, la professora i amiga PILAR BÀYER a la conferència inaugural de la SECCIÓ DE MATEMÀTIQUES de l'INSTITUT D'ESTUDIS CATALANS ens ha presentat, amb aquella dignitat i claredat que li són pròpies, els averanys tortuosos que ha seguit el camí que porta a la, aleshores encara, possible demostració del teorema de Fermat.

Aquestes circumstàncies, afegides a les meves pròpies limitacions, em deixen un espai ben estret —potser només el marge d'un llibre— per poder-me bellugar amb una certa comoditat i naturalitat. No puc pas refer els articles de LA VANGUARDIA i no puc pas repetir —tampoc no en seria capaç— la magistral lliçó de la professora BÀYER. Què és doncs el que puc dir?

Puc intentar de fer un apropament rònec i tan lúcid com sigui capaç d'algunes de les fites més notables del teorema; puc intentar d'analitzar el significat en el context històric i en el desenvolupament de la matemàtica i, finalment, puc agafar tota aquesta història per reflexionar sobre el procés creatiu de la matemàtica, els seus més i els seus menys, les seves clarors i les seves obagues.

Deixeu-me, almenys, intentar-ho; em fa molta il·lusió!

§1. Cronologia d'un teorema

De fet volem analitzar la següent qüestió:

> Fixat $n \in \mathbb{N}, n \geq 2$, existeixen tres nombres naturals [o sencers] a, b, c tals que siguin una solució de l'equació diofàntica
>
> $$x^n + y^n = z^n?$$

El cas $n = 2$ condueix al *teorema de Pitàgoras* i el *teorema de Fermat* fa referència a la totalitat de casos $n > 2$.

La cronologia d'aquest teorema abraça gairebé tota la història de la matemàtica, si considerem el problema en tota la seva generalitat.

El teorema de Pitàgoras

1900–1600 a.C. La TAULETA PLIMPTON 322. És una tauleta en escriptura cuneïforme que es conserva, possiblement incompleta, a la Universitat de Columbia. Conté tres columnes de nombres naturals escrits en sexagesimal. Les columnes contenen la hipotenusa i un catet d'un triangle rectangle aritmètic. La tercera conté la secant al quadrat d'un dels angles aguts. Té quinze files que corresponen, de grau en grau, als triangles rectangles de 45° a 30°. La seva construcció no es comprén si no s'accepta que el qui la va escriure coneixia l'algorisme de formació de ternes pitagòriques.

600 a.C. PITÀGORAS I LA SEVA ESCOLA van introduir un nombre important de classificacions dels nombres naturals entre les quals cal distingir els nombres primers, els compostos, els perfectes, etc. I, lligats a ells, la teoria de la divisibilitat, la unicitat de la descomposició en factors primers, el convenciment que els nombres naturals tenen la propietat del *descens finit*, l'algorisme d'Euclides, etc. També sembla que Pitàgoras coneixia un algorisme per a determinar ternes pitagòriques aritmètiques en les quals la hipotenusa i un catet eren nombres naturals consecutius: $\frac{n^2-1}{2}, n, \frac{n^2+1}{2}$.

400 a.C. PLATÓ s'adonà que hi havia d'altres ternes pitagòriques com ara $\langle 8, 15, 17\rangle$ i establí un algorisme per calcular les ternes pitagòriques en les quals la hipotenusa i un dels catets difereixen de dues unitats: $2n, n^2 - 1, n^2 + 1$.

300 a.C. Apareixen els *Elements* d'EUCLIDES i, en ells, hi trobem tres llibres —els llibres VII, VIII i IX— dedicats a establir certs resultats d'aritmètica: l'algorisme d'Euclides, el teorema d'unicitat i d'existència de la descomposició dels nombres naturals en producte de

nombres primers, l'algorisme d'Euclides per tal de determinar el m.c.d. de dos nombres, un algorisme que permet de determinar nombres perfectes parells, etc.

Al llibre X, 28, lemes 1 i 2, hi trobem la demostració de la fórmula que dóna totes les ternes pitagòriques aritmètiques simples: si $\langle p, q\rangle = 1$, aleshores $a = q^2 - p^2, b = 2pq, c = q^2 + p^2$ formen una terna pitagòrica simple i, recíprocament, qualsevol terna pitagòrica simple és d'aquesta forma.

300 d.C. DIOFANT D'ALEXANDRIA elabora la seva *Aritmètica*. En el problema 8 del llibre II se'ns ofereix una solució racional de l'equació $x^2+y^2 = z^2$. Al llibre VI, en canvi, es resolen un bon nombre de problemes indeterminats relatius a les ternes pitagòriques i, per fer-ho, utilitza en molts d'ells l'algorisme descrit en els *Elements*.

Sembla doncs que el problema pel cas $n = 2$ està resolt.

El teorema de Fermat per a $n < 10$

IX Segons ABŪ ĞA'FAR MUHAMAD IBN AL-HUSAYN, primera meitat del segle XI, ABU MUHAMAD HĀMID IBN AL-HIAR AL HUĞANDI [†1 000] va intentar de provar el teorema de Fermat pel cas $n = 3$, però la seva demostració va resultar insuficient.

XII-XIV Els matemàtics àrabs es plantegen la impossibilitat de resoldre l'equació pel cas $n = 4$.

XVI BAHA AL-DIN intenta una demostració del cas $n = 3$.

1 510 Es publica a PARÍS el *Liber de numeris perfectis* de PIETRO ANTONIO CATALDI en el qual trobem el primer avenç significatiu després de l'*Aritmètica* de TEÓ D'ALEXANDRIA. Estableix l'error de moltes de les conjectures fetes en relació amb els nombres perfectes —acaben alternativament amb 6 o 8; n'hi ha un de cada ordre decimal; etc.— i demostra que, per tal que $2^n - 1$ sigui primer cal que n ho sigui i, a partir d'aquest fet, calcula els set primers nombres perfectes.[1]

1 621 BACHET DE MERIZAC tradueix al llatí l'*Aritmètica* de *Diofant d'Alexandria*, una traducció molt acurada i amb notes personals importants.

~1 630 PIERRE DE FERMAT llegeix l'edició de l'*Aritmètica* de DIOFANT i, com era el seu costum quan llegia textos de matemàtica, hi va fer anotacions. En el problema 8 del llibre II va escriure el següents comentari —és la primera observació—

> *Si $n > 2$, no és possible de trobar solucions senceres positives a, b, c de l'equació $x^n + y^n = z^n$.*

[1] L'interès d'aquest estudi la va provocar una obra sobre nombres perfectes de CARLO DE BOUVELLES.

I afegeix

> *Disposo d'una demostració, però el marge és massa petit per poder-la contenir.*

En canvi a l'observació 45 —que correspon al problema de 26 llibre VI— afirma que "no hi ha cap triangle rectangle aritmètic l'àrea del qual sigui un quadrat" i n'ofereix l'esborrany de la demostració perquè la demostració completa no hi cap.

1644 Apareix la *Cogitata Physico-Mathematica* del pare mínim MARIN MERSENNE. En aquesta obra MERSENNE estudia els nombres, i els nombres primers, de Mersenne i estableix que, si p és un dels 55 nombres primers ≤ 257, $2^p - 1$ és primer solament quan

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

Aquesta llista té cinc errors. Hi sobren els casos $p = 67, 257$ i, en canvi, hi falten $p = 61, 91, 107$. Sembla que l'interès de l'estudi d'aquests nombres primers prové de la revifalla per l'interès en l'estudi dels nombres perfectes despertada per l'obra de PIETRO ANTONIO CATALDI.

1659 PIERRE DE FERMAT escriu una carta a CHRISTIAN HUYGENS a través de PIERRE DE CARCAVI. En ella FERMAT afirma que els "mètodes ordinaris dels llibres són insuficients per establir la demostració d'algunes proposicions difícils" i que, per aquesta raó, "s'ha dotat d'una eina completament singular que anomena el mètode de demostració per *descens infinit* o *il·limitat*". I entre els problemes que afirma que ha pogut demostrar amb el seu mètode hi trobem

- *no hi ha cap triangle rectangle que tingui per àrea un nombre quadrat.*
- *no hi ha cap solució sencera a, b, c de l'equació $x^3 + y^3 = z^3$.*

1713 JAKOB BERNOULLI, durant vint anys, havia anat escrivint l'*Ars Conjectandi*. Fou editada pel seu nebot NIKOLAS BERNOULLI l'any 1713 quan ell JAKOB ja era mort. Aquesta obra conté l'expressió general de la suma de les $m-1$ primeres potències k–èsimes [$k = 1, 2, 3, \ldots$] dels nombres naturals: $S_k(m) = 1^k + 2^k + \cdots + (m-1)^k$. Aleshores JAKOB BERNOULLI estableix que

$$S_k(m) = \frac{1}{k+1} m^{k+1} - \frac{1}{2} m^k + B_1 \binom{k}{1} \frac{m^{k-1}}{2} - B_2 \binom{k}{3} \frac{m^{k-3}}{4} + \cdots$$

Els nombres $B_1, B_2, B_3, \ldots$ són els nombres de Bernoulli.

1760 LEONHARD EULER elabora un treball d'aritmètica en el qual demostra el següent teorema

> *Si un nombre primer és de la forma $6n + 1$, necessàriament és també de la forma $p^2 + 3q^2$, amb $(p, q) = 1$.*

En aquest treball estableix un cert nombre de lemes previs entre els quals hi trobem la demostració del següent teorema

Si $p^2 + 3q^2$, amb $p, q \in \mathbb{N}$ i $(p, q) = 1$, és un cub, aleshores existeixen $a, b \in \mathbb{N}$ tals que

$$p = a^3 - 9ab^2, \qquad q = 3a^2b - 3b^3.$$

De retruc, usant el mètode del descens, és possible de demostrar el teorema de Fermat pel cas $n = 3$.

1770 L. EULER publica la seva *Àlgebra* i en ella dedica un apartat a demostrar el teorema de Fermat pel cas $n = 3$ i, per fer-ho, introdueix l'anell $\mathbb{Z}[\sqrt{-3}]$ dels nombres de la forma $a + b\sqrt{-3}$. Aleshores per tal d'establir el teorema de Fermat necessita del lema que havia establert l'any 1760, però ara ho fa usant el fet que, si un cub està descompost en nombres primers dins l'anell $\mathbb{Z}[\sqrt{-3}]$, cada un dels factors és un cub.

1825 Els matemàtics PETER-GUSTAV LEUJENE-DIRICHLET i ADRIEN MARIE LEGENDRE demostren la validesa del teorema de Fermat per a $n = 5$.

1830 P.-G. LEUJENE-DIRICHLET aconsegueix d'establir el cas $n = 14$.

1838 GABRIEL LAMÉ ho demostra per a $n = 7$.

Així hom disposa ja de la demostració del teorema de Fermat per a $n = 4$ i, per a tot nombre primer < 10 i, de retruc, per a qualsevol nombre compost tal que, a la seva descomposició en factors primers, solament intervinguin els nombres primers 2, 3, 5 i 7.

El dos casos del teorema de Fermat

1823 La prestigiosa matemàtica SOPHIE GERMAIN classifica el teorema en dos casos:

Primer cas: l'equació $x^p + y^p = z^p$, p primer senar, no té cap solució $a, b, c \in \mathbb{N}$, no trivial, en la qual p no divideixi cap dels nombres a, b, c.

Segon cas: l'equació $x^p + y^p = z^p$, p primer senar, no té cap solució $a, b, c \in \mathbb{N}$, no trivial, en la qual p divideixi un dels nombres a, b, c.

1832 SOPHIE GERMAIN demostra que, si p és un nombre primer senar tal que $2p + 1$ també és primer, aleshores val el primer cas del teorema de Fermat per a p.[2]

LEGENDRE ampliarà el resultat de SOPHIE provant el primer cas del teorema de Fermat

[2] Cal indicar que, malgrat que hi ha molts primers senars p que compleixen la condició de Germain, no sabem pas si n'hi ha infinits.

per a qualsevol nombre primer senar p tal que un dels nombres

$$4p+1, \quad 8p+1, \quad 10p+1, \quad 14p+1, \quad 16p+1$$

també és primer. Amb aquest resultat s'aconsegueix d'establir el primer cas per a tot nombre primer < 100, però aquest resultat és molt pobre al costat d'altres resultats que s'estaven aconseguint al mateix temps.

1 856 GRÜNERT demostra que, si $a, b, c, a < b < c$, satisfà l'equació de Fermat d'exponent p, aleshores $a > p$. És el primer resultat de fitació inferior: no hi ha mai solucions petites.

1 910 MIRIMANOFF demostra la validesa del teorema de Fermat en el primer cas per a tot primer senar p de la forma $2^a 3^b \pm 1$ o de la forma $\pm 2^a \pm 3^b$, on a, b són sencers no-negatius. Aquesta família inclou els nombres primers de Mersenne i, per tant, el primer cas val per a tot nombre primer de Mersenne.

1 953 INKIERI va aconseguir, en el primer cas, establir que qualsevol solució de l'equació, ha tenir més de mil tres-cents trilions de xifres decimals.

1 982 LEHMER prova el primer cas per a tot nombre primer més petit que 6 bilions.

1 985 La col·laboració d'un matemàtic americà, ADLEMAN, un de francès FOUVRY i un d'anglès HEATH-BROWN estableix la validesa del primer cas del teorema de Fermat per a una infinitat de nombres primers i ho fan basant-se en el criteri de GERMAIN.

HEATH-BROWN va establir, a més, que el nombre relatiu de primers positius pels quals podia fallar el teorema de Fermat, primer cas, relativament al total de nombres sencers, tendeix a zero quan els fem créixer.

1 988 Hom demostra que el nombre $2^{216\,091} - 1$ és un nombre primer de Mersenne[3] i, per tant, el primer cas del teorema de Fermat val per a aquest nombre primer que té 65 050 dígits.

Vers la primera demostració general

1 843 DIRICHLET sabia que no tot anell de sencers algèbrics té unicitat de descomposició en factors primers.

1 844 ERNS KUMMER havia provat que la unicitat de descomposició falla en l'anell dels sencers ciclotòmics, quan $n = 23$.

1 844 FERDINAND EISENSTEIN introdueix correctament l'anell d'enters del cos $\mathbb{Q}\left[\sqrt{-3}\right]$. És l'anell generat per 1 i per $\dfrac{1+\sqrt{-3}}{2}$. Dit d'una altra manera, EISENSTEIN determina tots els enters algèbrics dels cos $\mathbb{Q}\left[\sqrt{-3}\right]$.

[3] És el nombre primer més gran conegut fins aleshores.

1847 LAMÉ afirma que ha aconseguit una demostració del teorema de Fermat per a tot nombre primer senar p. Ho fa treballant dins de certs anells de nombres complexos: els anells dels sencers ciclotòmics. La idea de LAMÉ fou de descompondre $x^p + y^p$ en producte de factors lineals de la forma $(x + \alpha^k y)$, $k = 0, 1, \ldots, p-1$. Aleshores, aplicant la unicitat de descomposició, afirma que, si $x^p + y^p = z^p$, aleshores cada $x + \alpha^k y$ també és una potència p–èsima.

LIOUVILLE, que assistia a la sessió de la SOCIETAT DE CIÈNCIES de PARÍS en la qual LAMÉ va enunciar el resultat, li va fer notar que la demostració residia en la unicitat de descomposició en l'anell dels enters p–ciclotòmics i li va preguntar si havia establert aquesta unicitat per a qualsevol nombre primer senar p.

KUMMER introdueix els nombres ideals per tal de refer la unicitat de demostració en els anells de sencers ciclotòmics. Aleshores aconsegueix una demostració del teorema de Fermat per a tot primer senar $p < 100$, llevat dels casos $p = 37, 59$ i 67. Això li permet una classificació dels nombres primers en regulars i irregulars: els nombres primers regulars són aquells als quals és possible d'aplicar la seva demostració del teorema de Fermat; els irregulars són els altres. Curiosament els nombres primers regulars estan lligats amb els nombres de Bernoulli: un nombre primer p és regular si, i només si, no divideix cap dels numeradors dels nombres de Bernoulli $B_2, B_3, \ldots, B_{p-3}$. A més aconsegueix d'establir que els únics primers irregulars < 164 són els nombres $37, 59, 67, 101, 131, 149$ i 157.

1905 MIRIMANOFF demostra el teorema de Fermat pels casos $n = 37, 59$ i 67.

1915 JENSEN estableix l'existència d'infinits nombres primers irregulars.

1930 STAFFORD i VANDIVER amb calculadores personals van establir la caracterització de tots el primers fins el 617.

1954 LEHMER i VANDIVER, usant computadores electròniques, van ampliar l'estudi fins el 30 000.

1964 SIEGEL va observar que hi ha un 60% de primers regulars en el conjunt dels nombres primers. Malgrat tot no sabem si n'hi ha infinits.

1976 SAMUEL WAGSTAFF, usant IBM 360 – 65 i IBM 370 va establir l'estatus de regularitat o irregularitat de cada un dels nombres primers fins al 125 000 i va veure que el teorema era gairebé segur.

> S'havia obert un camí prou atractiu que reduïa el problema a l'estudi dels nombres primers regulars i irregulars. Aquest camí, però, no va resultar tan fàcil o segur com calia, però va anar convencent cada cop més de la veracitat de la conjectura de Fermat.

El camí que duu a ANDREW WILES

Aquesta cronologia segueix les pautes indicades a l'article de B. MAZUR "Number Theory as Gadfly" i pot ser completada amb la cronologia de LA VANGUARDIA que centra la seva atenció en les aportacions del segle XX.

~1 350 NICOLE ORESME va establir la divergència de la sèrie harmònica.

1 637 RENÉ DESCARTES introdueix la distinció entre corbes geomètriques i mecàniques. Aquestes corbes es distingien, de fet, per la possibilitat de ser descrites, o no, per funcions polinòmiques en dues variables. Foren rebatejades per GOTTFRIED WILHELM LEIBNIZ amb els noms respectius d'algèbriques i transcendents.

1 650 Amb PIETRO MENGOLI té lloc l'estudi de la convergència i divergència de les sèries numèriques per primera vegada a la història de la matemàtica d'una forma sistemàtica.

1 667 ISAAC NEWTON va elaborar un breu tractat en el qual classificava les cúbiques. Aquesta classificació fou completada per JAMES STIRLING l'any 1 717.

1 718 FAGNANO, i més tard EULER, es va adonar de la propietat additiva de les cúbiques el·líptiques: les cúbiques de la forma $y^2 = a x^3 + b x^2 + c x + d$.

1 748 LEONHARD EULER introdueix la família de sèries numèriques

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots.$$

És la funció zeta de Riemann i demostra, per exemple, que $\zeta(2) = \dfrac{\pi^2}{6}$.

1 768 EULER s'adona del vincle que hi ha entre les funcions el·líptiques i la teoria de nombres.

1 825 LEGENDRE aprofundeix la teoria de les integrals el·líptiques.

1 826 NOCOLAI IVANOVITCH LOBACHEVSKI publica per primera vegada un tractat de geometria hiperbòlica.

1 827 JACOBI introdueix les funcions el·líptiques, que ja havien sigut intuïdes per ABEL i GAUSS. Més tard, el 1 834 insinua la relació entre les integrals i els punts racionals de les corbes, lligant les integrals i la inversió.

La integral més adequada per ser usada com a base de la teoria de les funcions el·líptiques és la integral $\displaystyle\int \frac{dt}{\sqrt{4\,t^3 - g_2\,t - g_3}}$, sent la seva inversa la funció $\wp$ de Weierstrass. Ara el teorema d'addició per aquesta integral és

$$\int_0^{x_1} \frac{1}{\sqrt{4t^3 - g_2 t - g_3}} + \int_0^{x_2} \frac{1}{\sqrt{4t^3 - g_2 t - g_3}} = \int_0^{x_3} \frac{1}{\sqrt{4t^3 - g_2 t - g_3}},$$

on x_3 és el tercer punt de la recta que passa per (x_1, y_1) i (x_2, y_2) que es troba damunt de la cúbica el·líptica

$$y^2 = 4x^3 - g_2 x - g_3. \qquad (*)$$

De tot això en resulta que la corba $(*)$ és parametritzable per la funció $\wp$ de Weierstrass: $x = \wp(u), y = \wp'(u)$.

1847 EISENSTEIN descobria notables expansions en sèrie que eren doblement periòdiques. De fet va veure que funcions doblement periòdiques es poden posar en la forma

$$\sum_{m,n=-\infty}^{\infty} \frac{1}{(z + m\omega_1 + n\omega_2)^2}.$$

Així s'obté la funció $\wp$ de Weierstrass.

1851 RIEMANN analitza la integral complexa

$$\Phi^{-1}(z) = \int_0^z \frac{dt}{\sqrt{t(t-\alpha)(t-\beta)}}$$

i arriba a la conclusió que la relació inversa $\Phi(w) = z$, la funció el·líptica associada a la integral, satisfà

$$\Phi(w) = \Phi(w + m\omega_1 + n\omega_2), \text{ on } m, n \in \mathbb{Z}.$$

És a dir que Φ és doblement periòdica de períodes ω_1, ω_2.

1859 BERNHARD RIEMANN estudia a bastament la funció zeta i l'estén al camp complex, adonant-se de la gran riquesa i poder d'aquesta funció de variable complexa. Estableix una de les conjectures més pregones i útils de l'anàlisi complexa: la hipòtesi de Riemann diu que, dins la banda crítica $0 \leq \mathrm{Re}(z) \leq 1$, $\zeta(s) = 0$ solament quan $\mathrm{Re}(s) = \frac{1}{2}$.

1863 Karl Weierstarss troba les relacions existents entre g_2, g_3 i els períodes ω_1, ω_2:

$$\begin{aligned} g_2 &= 60 \sum \frac{1}{(m\omega_1 + n\omega_2)^4} \\ g_3 &= 140 \sum \frac{1}{(m\omega_1 + n\omega_2)^6}. \end{aligned}$$

A més, a partir de

$$\wp(z) = \frac{1}{z^2} + \sum{}' \left(\frac{1}{(z + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right),$$

on $\sum'$ indica que el sumatori pren tots els valors m, n enters, llevat del valor $m = n = 0$, va aconseguir per simple càlcul

$$[\wp'(z)]^2 = 4\,[\wp(z)]^3 - g_2\,\wp(z) - g_3.$$

Per tant el punt $\langle \wp(z), \wp'(z)\rangle$ pertany a la corba i aquesta corba és aleshores isomòrfica al torus $\mathbb{C}/\Lambda$, on Λ és el reticle de períodes de $\wp$.

A partir d'ací la recerca segueix el camí indicat a la cronologia de La Vanguradia i jo solament esmentaré algunes de les fites aconseguides.

1922 El grup additiu associat a la corba el·líptica —a cada parella de punts alineats P, Q de la corba el·líptica li associem el tercer punt de la corba $P + Q$ que es troba damunt la mateixa recta— té unes propietats notables. Si P, Q són racionals, aleshores $P + Q$ també ho és. El conjunt $E(\mathbb{Q})$ dels punts racionals de l'el·líptica E és un grup abelià de punts racionals finitament generat. Per tant l'el·líptica E té una infinitat de punts racionals sempre que el seu rang sigui > 0. Bé doncs, MORDELL conjectura que les úniques equacions que es coneixen amb una infinitat de solucions racionals són les de gènere 0 o 1. L'equació de Pitàgoras és de gènere 0 i les el·líptiques són de gènere 1. Les equacions de Fermat d'ordre $n \geq 2$ són de gènere $\frac{1}{2}(n-1)(n-2) > 1$, si $n > 3$.

MORDELL va conjecturar que qualsevol equació de gènere ≥ 2 solament té un nombre finit de solucions racionals i, per tant, les equacions de Fermat solament tenen un nombre finit de solucions senceres no equivalents. Aquesta conjectura era molt agossarada i no semblava que fos fàcil establir-la.

1950 ANDRÉ WEIL va pensar que fóra millor reduir el problema als cossos finits i considerar la varietat V de totes les solucions en els diferents cossos i va formular les seves conjectures en termes de la funció de Riemann relativa a la varietat de les solucions V.

1955 En un congrés internacional de teoria de nombres celebrat a Tokyo es proposa la demostració de la conjectura de TANIYAMA segons la qual tota corba el·líptica sobre $\mathbb{Q}$ és modular: de fet, lliga la corba el·líptica amb funcions semblants a la funció zeta de Riemann.

1975 PIERRE DELIGNE demostra la conjectura d'A. WEIL.

1983 GERD FALTINGS demostra algunes conjectures relacionades amb aquestes qüestions i, en particular, la de MORDELL.

1985 GERHARD FREY estableix el camí per demostrar que la conjectura de Taniyama implica el teorema de Fermat: Suposa que a, b, c és una solució de l'equació de Fermat $x^p + y^p = z^p, p \geq 3$. Li associa la corba el·líptica de FREY: $y^2 = x(x - a^p)(x + b^p)$. I resulta que és semiestable però en canvi no és modular i això contradiu la conjectura de Taniyama.

1993 ANDREW WILES anuncia que ha demostrat la conjectura de Taniyama per a una àmplia classe de corbes el·líptiques —les corbes el·líptiques semiestables— i, de retruc, el teorema de Fermat. Era el 23 de juny. Aquest anunci és explicitat al *Notices of the American Mathematical Society* de Juliol-Agost. Finalment, el 3 de desembre A. WILES reconeix que,

a la seva demostració, hi ha una imprecisió en el càlcul d'una certa fita superior del grup de Selmer en el cas semi-estable.[4]

> S'ha demostrat finalment que, si una equació de Fermat té solucions, solament en té un nombre finit. Ens hem apropat a la demostració del teorema de Fermat llevat del càlcul d'unes fites superiors d'un cert tipus de grups. Sembla que la fi és ben a prop.

§2. Reflexions sobre el teorema de Fermat

En relació amb el teorema de Fermat és força corrent una estranyesa per tres o quatre fets: la simplicitat de l'enunciat i la complexitat de la seva resolució; les mancances en el rigor que s'han produït en el seu desenvolupament; i finalment la inutilitat del teorema. I jo no voldria limitar la meva exposició a un grapat de dades cronològiques més o menys encertades. Voldria fer una reflexió més profunda per a tots aquells que, com vosaltres, esteu estudiant matemàtiques i encara no us heu enfrontat amb el món, ben diferent, de la recerca matemàtica. I voldria que l'exposició fos prou clara i senzilla per tal de posar de manifest que, a voltes, fem lectures massa pobres dels esdeveniments matemàtics perquè ens entestem en limitar-los a una situació molt local i a un cas massa particular i això ens fa perdre perspectiva.

La complexitat de la demostració

L'exposició anterior posa de manifest prou a les clares que els intents de demostració d'aquest teorema no han sigut gens fàcils. Ben al contrari han precisat d'un desenvolupament cada cop més afinat de diferents aspectes de la tasca i del coneixement matemàtics. Sense cap pretensió d'exhaustivitat vull posar de manifest alguns d'aquests entrebancs i algunes de les solucions.

1. El teorema de Fermat és un teorema negatiu i, a l'igual que els altres teoremes negatius, presenta dificultats d'ordre lògic. És necessari desenvolupar tècniques adequades de reducció a l'absurd. Aquest fet fou observat ja per FERMAT que proposava de demostrar-lo usant el *descens infinit* —una tècnica de reducció a l'absurd adequada a la naturalesa dels nombres naturals—. La demostració de FREY és, en definitiva, una demostració per reducció a l'absurd: si la solució de l'equació de Fermat existeix, disposarem d'una corba el·líptica semiestable, a la qual podrem associar una forma modular de pes 2 i nivell 2. Ara, com diu la Dra. PILAR BÀYER, "obrim la capsa d'aquestes formes modulars. És buida." La contradicció està servida.

[4] Queden fora de la seva demostració una família important de corbes el·líptiques semiestables i la corba el·líptique de Frey pertany precisament a aquesta família.
Aquest número de la revista ALEPH ofereix una fotocòpia de la circular de WILES.

2. En un primer estadi va ser necessari introduir noves classes de nombres sencers; va caldre estudiar les propietats aritmètiques de les estructures algebraiques que sorgien de la seva consideració. Així van aparèixer els nombres algèbrics, els sencers algèbrics, els sencers ciclotòmics, etc. Va ser indispensable restaurar la unicitat de la descomposició quan fos possible. D'ací a la teoria dels ideals de DEDEKIND hi havia un pas.

3. Les dificultats del teorema van permetre una clarificació i classificació del conjunt dels nombres primers i alhora un millor coneixement dels nombres de Bernoulli.

4. Es va fer imprescindible un coneixement cada cop més fi de les corbes el·líptiques i els lligams amb l'aritmètica dels cossos de nombres. Aquests estudis van obligar a afinar l'"olfacte" dels matemàtics que es van veure en la necessitat d'"intuir" els lligams existents entre l'aritmètica i la geometria algèbrica; van haver de copsar les topologies més adients a les estructures en qüestió i a la complexitat del problema. Això va provocar un allau de conjectures que calia resoldre o refutar.

5. Es va fer necessari ampliar l'estudi de les formes modulars, les varietats algèbriques, les varietats abelianes, etc.

I és aquesta complexitat la que, a voltes, ens fa creure que s'està errant el camí o bé que el teorema és independent de la matemàtica actual. En definitiva, la solució està massa lluny de la formulació. I és cert, no podem pas negar-ho: la demostració del teorema de Fermat sembla desproporcionada amb el seu enunciat i, encara més frustrant, la comprensió de la demostració està limitada a uns quants, mentre que la comprensió de l'enunciat és a l'abast de tots.

La complexitat en el quefer matemàtic

Tanmateix però, la complexitat no és pas estranya al desenvolupament de la matemàtica ni al quefer dels matemàtics. Els exemples són molts, però ens limitarem a un de sol, també de caire negatiu. En el llenguatge de la geometria grega la construcció amb regle i compàs era una qüestió ben consolidada i de fàcil comprensió. A més, era d'una enorme importància atès que un objecte geomètric existia sempre que fos construïble, i construïble volia dir precisament "construïble amb regle i compàs". Així doncs el problema d'establir l'existència de l'angle un terç d'un angle donat era un enunciat clar. La seva solució que, potser avui ens sembla força elemental, va necessitar 23 segles. Al seu costat els tres segles i mig del teorema de Fermat són una petitesa.

Per tal de poder-lo resoldre va ser necessari, però, una transformació radical del context i del llenguatge matemàtic. Va ser necessari disposar de l'àlgebra i de les idees elementals del procés d'extensió algèbrica d'un cos. Va caldre la introducció dels nombres complexos; adonar-se que la trisecció de l'angle estava molt fortament vinculada amb la resolució de la cúbica irreductible. A mesura que el problema s'anava perfilant sorgien qüestions de nou encuny a les que calia anar donant resposta: la classificació dels nombres complexos en algèbrics i transcendents; el

teorema fonamental de l'àlgebra i la seva demostració; la classificació dels nombres algèbrics en construïbles i no-construïbles; la resolució de la quíntica; aclarir quines equacions eren resolubles per radicals i quines no, etc.

Ben cert que no calen pas totes aquestes qüestions per tal d'establir una demostració de la impossibilitat de la trisecció de l'angle. Però això no significa que històricament no fos gràcies al seu planteig i resolució que es va poder aclarir on radica el nus del problema i es va poder resoldre.

I en el cas de la quadratura del cercle —un altre dels problemes clàssics— va ser necessari demostrar que el nombre π és transcendent.

Totes aquestes recerques van permetre afinar la matemàtica de tal manera que el jove GAUSS va poder sorprendre la humanitat —si més no, la humanitat matemàtica— establint l'existència d'altres polígons regulars diferents del triangle equilàter, el quadrat, el pentàgon i els que es podien deduir d'ells per bisecció. Aquest problema ni tan sols s'havia plantejat, tan convençuts estaven els matemàtics que no era possible de construir-ne cap més. La demostració va necessitar un coneixement profund dels nombres complexos, dels sencers ciclotòmics, dels nombres primers de Fermat, etc.

Probablement podríem trobar un problema d'aquesta mena en cada un dels àmbits de la matemàtica: la formalització del nombre real des de les primeres intuïcions pitagòriques fins a les construccions de CANTOR, DEDEKIND i WEIERSTRASS; la clarificació de la profunda naturalesa de la geometria [o de les geometries]; la consolidació del concepte d'infinitament petit amb la idea de límit; l'aclariment definitiu de la idea de corba des de la GRÈCIA CLÀSSICA als nostres dies, passant pel concepte de funció; etc. per esmentar-ne unes quantes prou elementals per tal que puguin ser enteses per tots nosaltres.

De les conjectures i de les hipòtesis

En el desenvolupament de les matemàtiques, les conjectures constitueixen una pedra de toc indispensable i és una concepte íntimament vinculat al rigor, una altra de les pedres de toc.

El paper fonamental de la conjectura és que constitueix l'olfacte del matemàtic al si de l'univers d'idees i conceptes —cada volta més complexos— que la seva tasca l'obliga a entendre i a manejar amb naturalitat.

M'atreviria a dir que les conjectures en l'esdevenir matemàtic són de tres menes, no absolutament excloents ni molt menys:

- les conjectures fonamentals;
- les conjectures auxiliars;
- les conjectures com a "intuïció".

Les conjectures fonamentals tenen com a objectiu precisar que és el que entenem, en cada moment o en cada problema concret, com a matemàtica o com és la part de la matemàtica que

cal usar per resoldre'ls adequadament. Aquestes conjectures són dessota de tota altra qüestió i reben el nom d'axiomes o postulats. Així, ja a la GRÈCIA CLÀSSICA, els matemàtics van voler delimitar l'objecte d'estudi de les matemàtiques —la geometria— fixant-ne els límits i possibilitats. Els matemàtics grecs, amb un a intuïció genial, van fixar la geometria euclidiana com a domini d'estudi. I per fixar-la van "conjecturar" els fonaments de la geometria, vinculant així la matemàtica amb el rigor d'una manera notable.

Aquestes conjectures fonamentals, però, no són pas lògicament diferents de les conjectures auxiliars. Entenc com a conjectura auxiliar aquella pressuposició que donem com a vàlida —la nostra intuïció de la món complex de la matemàtica així ens ho fa creure— per tal de poder establir un teorema concret la importància del qual se'ns ha mostrat en algun moment del procés matemàtic. La diferència entre les conjectures fonamentals —de les quals des d'ara en diré postulats— i les auxiliars és, de fet, l'abast del seu àmbit. El postulat és una conjectura que cal mantenir en la demostració de qualsevol teorema i/o en la resolució de qualsevol problema d'un cert àmbit de la matemàtica. La conjectura auxiliar apareix, de fet, en una demostració o resolució concreta i, en un primer moment, la seva utilitat és aquesta.

El matemàtic està fermament convençut què la conjectura és més clara i evident que no pas el teorema que, amb ella, vol demostrar i que, per tant, la demostració final i completa serà també més fàcil seguint aquesta drecera. L'ús de conjectures —explícites o implícites— és una constant de la matemàtica. N'esmentaré tres de ben elementals. Durant molts segles els matemàtics van estar convençuts que, si bé el postulat de les paral·leles era cert, no era pas un postulat; era solament una conjectura auxiliar que calia demostrar a partir de les conjectures bàsiques i van intentar de provar-lo durant més de vint segles; cada una de les "demostracions" del postulat de les paral·leles feia servir, inconscientment o conscient, una "conjectura", entenent que era òbviament evident [cas inconscient] i molt més fàcil d'establir més endavant [cas conscient]. Una altra situació indiscutible és el fet que, malgrat que la naturalesa del nombre natural no fou establerta fins al segle XIX, en qualsevol demostració, des d'EUCLIDES fins a PEANO, s'acceptava com a indiscutible i cert el principi dels descens finit: "qualsevol successió decreixent de nombres naturals s'acaba amb un nombre finit de passos". Aquest principi no és, però, mai explicitat fins a CAMPANUS DE NOVARA [s. XIII]. I finalment, des d'EUDOX hom suposa que el continu és infinitament divisible, dens i complet, malgrat que tampoc aquest fet s'explicita mai d'una forma correcta. Malgrat tot, els matemàtics xinesos i sobretot àrabs eren conscients de la validesa del teorema de Bolzano i l'usaven per tal d'aproximar les arrels de les equacions polinòmiques. Aquest mètode fou acceptat amb naturalitat per LEONARDO DA PISA en el primer text de matemàtica d'Occident, *Liber Abaci* [1202].

Finalment, cal considerar les conjectures com a intuïció. Aquestes conjectures són afirmacions que els matemàtics fan del que s'ha d'esdevenir en el si d'una teoria concreta en virtud del perfum que desprèn i gràcies a la finor del seu olfacte. I es converteixen aleshores en un final de destí que, podrà convertirse en principi d'un altre. La història de la matemàtica és plena de conjectures d'aquesta mena i en podem trobar en tots els àmbits. Algunes d'elles han estat falses, però això no desmereix pas la major part de les vegades la finor d'aquell que les ha enunciat. Una d'aquestes conjectures falses fou establerta precisament per FERMAT, quan va afirmar que tots els nombres de la forma $F_n = 2^{2^n} + 1$ són primers. Aquest geni, però, va enunciar també una altra conjectura : el **darrer teorema**, que és el motiu de tot aquest aldarull i de totes aquestes línies.

Aquestes conjectures —les intuïtives— són d'una importància molt notable perquè, de fet, són les que fan avançar la matemàtica d'una forma molt decidida. Algunes d'aquestes conjectures han enfrontat matemàtics de prestigi. Així per exemple, la conjectura que afirma que "tot polinomi de grau n té n arrels complexes" va enfrontar NIKOLAS BERNOULLI i CHRISTIAN GOLDBACH amb LEONHARD EULER. D'altres en canvi s'han acceptat com a ben naturals malgrat que la seva demostració es resisteix. En són exemples la conjectura de Fermat, la conjectura de Riemann, etc. I fins que no se n'aconsegueix la seva demostració actuen o bé com a conjectura auxiliar o bé com a conjectura fonamental.

El rigor en la matemàtica: evolució

És indubtable que la precisió en el rigor demostratiu està lligat amb la finor amb la qual coneixem el món d'objectes matemàtics —d'idees— en el qual ens movem. En el llibre I, proposició 1,—de fet és un problema— dels *Elements* d'Euclides —text emblemàtic per la perfecció en l'exposició, considerat durant segles el paradigma de la manera de fer matemàtiques—, es demana

Construïu un triangle equilàter de costat donat AB.

La demostració és simple i elegant. Dibuixem dos arcs de circumferència de radi AB, amb centres respectius en els punts A i B. Aquests dos arcs es tallen en un punt C. Aquest punt és el tercer vèrtex del triangle i el problema s'ha resolt. Aquesta demostració es basa tanmateix en una **conjectura** que diu,

quan veiem que dos arcs de circumferència es tallen "realment" es tallen.

De fet estem suposant que els arcs de circumferència en qüestió són "complets". Pensem per un moment que els extrems del segment AB fossin els punts $\langle 0,0\rangle$ i $\langle 1,1\rangle$ del pla de les coordenades i suposem que el nostre pla és un pla de coordenades racionals; només hi ha els punts $\langle p,q\rangle, p,q \in \mathbb{Q}$. Si ara repetim la demostració anterior no trobem cap punt C i, per tant no podem construir el triangle equilàter. De fet, no existeix.

Podem dir que el primer text rigorós de matemàtiques fou escrit per DAVID HILBERT l'any 1899. I què entenem quan diem que una construcció o una demostració és rigorosa? Doncs entenem que totes les conjectures —bàsiques o auxiliars— s'han explicitat i que cada un dels passos de la demostració troba la seva justificació final o bé en un o diversos postulats —conjectures bàsiques— o bé en alguna conjectura auxiliar. Aquesta tasca no és gens fàcil. De fet, aprendre matemàtiques és també aprendre a analitzar el "rigor", entès en el sentit anterior, d'una demostració i d'una construcció.

Així quan diem que la demostració de tal o qual teorema depèn de l'**A.C.** —l'axioma de l'elecció— entenem que en algun dels passos l'hem usat; si diem que depèn de **H.C.** —la hipòtesi del continu—, volem dir que en algun punt hem fet ús d'aquesta conjectura; etc. Que un teorema depengui d'una conjectura no li lleva pas el rigor i, per tant, el valor relatiu de veritat, sempre és clar que siguem conscients del següent fet: la validesa del resultat és una validesa relativa a

la validesa de la conjectura o conjectures que hem usat per tal d'establir-lo. Ara bé el teorema no quedarà "definitivament" demostrat fins que haguem demostrat la conjectura o bé l'haguem incorporat al món dels postulats.

El rigor no és pas quelcom acomplert i definitivament assolit. En la matemàtica hi ha problemes oberts, la solució dels quals de fet depèn dels postulats que ens volguem donar.[5] I hi ha problemes tancats que s'han establert de la forma que s'ha fet en virtud de les conjectures que s'han acceptat.[6] Pot fins i tot succeir que, segons quin sigui el problema que volguem resoldre, haguem de recórrer a uns postulats i segons quin sigui a uns altres. Pensem, per exemple, en les geometries no-euclidianes.[7]

Avui un teorema es considera completament demostrat si s'ha aconseguit donar-ne una demostració al si de la teoria de conjunts **Z.F.+A.C.** —és la teoria de conjunts Zermelo-Fraenkel amb axioma de l'elecció i constitueix el fonament actual del quefer matemàtic quotidià—, més, en alguns casos, la **H.G.C.** —la hipòtesi general del continu.[8] I, en aquesta perspectiva, quan s'envia un article de matemàtiques a una revista especialitzada per a la seva publicació, el prestigi de la publicació rau en el fet que la demostració sigui prou rigorosa per tal que no pugui ser "impugnada". Ben cert que, d'acord amb la qualitat de la revista, la importància del resultat que s'afirma haver demostrat, la categoria de l'autor, etc. l'anàlisi del valor del resultat i del seu rigor varien. Però també és cert que, en molts casos, els responsables de les revistes a través dels "referees" —persones qualificades per fer una valoració de l'article que es presenta per a ser publicat i del "rigor" de la seva demostració— aconsellen la no publicació de l'article, o bé la seva publicació després d'haver-ne esmenat tals errors o imperfeccions, d'haver-ne completat les seves conseqüències i aplicacions, o bé la seva publicació directa. Això és, avui dia, una manera de fer ben normal que, si bé no sorprèn o no ha de sorprendre ningú que estigui en l'entrallat de la recerca matemàtica, a vosaltres —i a tots els qui desconeixen els mecanismes actuals d'ús en l'acceptació dels resultats matemàtics— us pot cridar l'atenció.

Què és el que passa amb la demostració de WILES del teorema de Fermat?, podríeu preguntar-vos. La resposta és: no passa res que no passi cada dia un grapat de vegades, però la transcendència del teorema i la seva importància històrica fan que, en aquest cas, tot sembli més gran del que en realitat és.

Ben cert que hi ha molts teoremes que avui donem com a indiscutibles i que, de fet, tenen llacunes importants però que, malgrat tot, s'accepten. Per què doncs tants miraments amb la demostració de WILES? Bé, en part per la pretensió mateixa de WILES en afirmar que "havia demostrat el teorema de Fermat". La qüestió que la comunitat matemàtica ara es planteja, la qüestió que s'ha de plantejar —no oblidem que ens troben en una època en la qual el formalisme de Hilbert impregna encara l'ambient de la recerca matemàtica[9]—és la següent: però realment

[5] En aquest aspecte us aconsello l'article de JOSEP M. FONT i, molt més elaborat, el meu treball esmentats a les lectures recomanades.

[6] Per exemple, l'existència de subconjunts de la recta real no-mesurables de Lebesgue.

[7] La suma dels angles d'un triangle, quan val?

[8] És instructiu llegir el text de KURT GÖDEL sobre la, com a mínim, incertesa —per no dir, la certesa de la seva falsedat— de la veracitat d'aquesta hipòtesi.

[9] Per bé que no hauria pas d'impregnar el de la docència d'una forma exclusiva.

què és el que ha demostrat ANDREW WILES? Ha aconseguit una demostració completa o bé manquen algunes llacunes? Hi ha conjectures en la seva demostració? I cal que la comunitat matemàtica doni resposta a aquestes qüestions, ja que és la millor manera de conèixer cada cop amb més claredat i rigor —o així ens ho sembla— allò que fem i de poder avançar amb seguretat.[10]

De la utilitat i de la inutilitat

No voldria pas acabar senser fer una petita reflexió sobre un tema que, de tant trist, fa somriure. Però, quina és la utilitat d'aquest teorema? Per què serveix? La història ens dóna la resposta. Si més no ha servit per produir un desenvolupament en el coneixement matemàtic de l'home —i, de retruc, en el coneixement global de l'home, un dels tresors dels que disposem— i, per tant, directament o indirecta ha contribuït al desenvolupament de la matemàtica i, amb ella, de la ciència i de la tècnica.

És cert que la matemàtica —una part d'ella— "té una aplicació" important en la "filosofia de la naturalesa", en paraules de NEWTON. També és indiscutible que la matemàtica —una part d'ella— "té una influència molt notable i indiscutible" en la tècnica. I també ho és que la informàtica beu en la font cristal·lina de la matemàtica. Però cal dir que la matemàtica no és ni filosofia de la naturalesa —física—, ni tècnica, ni informàtica. La matemàtica és una ciència en ella mateixa que estudia els seus propis objectes, les lleis i propietats que els regeixen i els vinculen. I és precisament del coneixement profund d'aquests vincles i lligams que sorgeixen resultats aplicables a d'altres estudis més o menys propers. I el teorema de Fermat, com d'altres, ens ajuda a comprendre la complexitat d'un univers d'objectes matemàtics tan simple com és el dels nombres naturals. La seva resolució i estudi —i així ho demostra la història— és d'una utilitat matemàtica innegable amb tot el que això significa.

Més amunt deia que ens proporciona coneixement matemàtic i coneixement global i, com podem llegir a un llibre sagrat, "el cor de l'home és allà on es troba el seu tresor". És a dir, l'estudi d'un teorema com el teorema de Fermat, i d'altres, el fem, en paraules de JACOBI, "en honor de l'esperit humà", de la mateixa manera que el poeta, el compositor, el pintor, el literat, l'artista, en definitiva, produeixen obres que omplin l'esperit humà i l'enriqueixin.

I, en tot cas, ha servit per poder-ne parlar i això, amics, en aquests dies de televisió, és prou útil en si mateix.[11]

[10] En aquest sentit és aconsellable el text de DAVIS-HERSH i, en particular, el capítol 4, 120–200.

[11] Vull agrair a la professora PILAR BÀYER els seus consells i correccions que han contribuït a perfeccionar el meu redactat inicial, evitant que es filtressin errors en la interpretació que havia fet d'algun dels conceptes matemàtics relacionats amb l'evolució del teorema de Fermat, així com en algunes fórmules.

§3. Lectures alternatives i ulteriors

BÀYER, PILAR–LARIO, JOAN CARLES–NART, ENRIC–QUER, JORDI–TRAVESA, ARTUR– VILA, NÚRIA "El Teorema de Fermat". *La Vanguardia. Ciencia y Tecnología*. Dissabte, 13 de novembre de 1 993. Barcelona.

COX, DAVID A. "Introduction to Fermat's Last Theorem". *The American Mathematical Montly*, **101** (1994), 3–14.

DAVIS, PHILIP J.–REUBEN, HERSH *The Mathematical Experience*. Birkhäuser. Boston, 1 981. Hi ha traducció castellana a Editorial Labor. Barcelona, 1 985.

DEVLIN, KEITH *Mathematics: The New Golden Age*. Penguin Books. Londres, 1 988.

DIEUDONNÉ, JEAN *Pour l'honeur de l'esprit humain*. Hachette, París 1 987. Hi ha traducció castellana a la col·lecció Alianza Universidad, **611**. Madrid, 1 989.

FONT, JOSEP M. "Nous axiomes en la Teoria de Conjunts i les seves aplicacions en Matemàtiques." *Actes de II Congrés Català de Lògica*, 55–61. Barcelona, 1 983.

GÖDEL, KURT "What is Cantor's continuum problem?" *The American Mathematical Montly*, **54**(1 947), 55–61. En podeu trobar una traducció castellana a Alianza Universidad, **286**, 337–362. Madrid, 1 981.

MAZUR, B. "Number Theory as Gadfly." *American Mathematical Montly*, **98**(1 991), 593–610.

PLA, JOSEP *Axiomes alternatius de la teoria de conjunts i el quefer matemàtic*. Publicacions de l'Institut d'Estudis Catalans. Barcelona, 1 994. [En preparació.]

STEWART, IAN *The Problems of Mathematics*. Oxford University Press. Oxford, 1 987.

RIBET, KENNETH A. "Wiles Proves Taniyama's Conjecture; Fermat's Last Theorem Follows." *Notices of the American Mathematical Society*, **40** (6), juliol-agost, 1993.

STILWELL, JOHN *Mathematics and Its History*. Spirnger-Verlag. Nova York, 1 989.

XAMBÓ, SEBASTIÀ "Geometria i realitat (Lliçó inaugural del curs 1993–94)." Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya. Barcelona, 30 de setembre de 1993.

Nadal de 1993

ÚLTIMA HORA
Des de Princeton.

Els redactors de l'Aleph vam enviar un 'mail' (correu electrònic) a l'Anna Rio per tal de saber l'última hora. Molt amablement ella ens va contestar. L'Anna està seguint un curs a Princeton on entre d'altres coses en Wiles explica el seu treball. Aquest és el 'mail' que ens va enviar.

Hola, redactors de l'Aleph!

Perdoneu que m'hagi retrasat una mica en la resposta. Mentre rumiava que us podia dir (que no sabessiu) he vist que el Notices de la AMS d'aquest mes de marc conte un "Update on Fermat's Last Theorem" que crec que explica molt be l'estat de la questio. (Suposo que deu haver arribat a la Biblioteca)

El fet d'estar aqui no vol dir que un se n'enteri de molts mes detalls sobre els progressos del treball, sobre la possibilitat de completar-ho en un termini mes o menys curt, o sobre el grau de dificultat que implica eliminar el "gap".

D'una banda, en Wiles es mes aviat reservat i no deixa anar res. Amb posterioritat al missatge que va enviar via news per donar a conèixer l'estat de la questio (missatge que segurament ja coneixeiu i que en tot cas figura a l'article del Notices que mencionava) no ha tornat a dir res. D'altra banda, Princeton es un lloc tan acostumat als resultats espectaculars que s'ho prenen tot amb molta calma. Aixi que tambe pel que fa aquest tema volen mantenir una actitud de "no cal esverar-se".

Tot plegat fa que en la primera sessio del curs que esta fent, que era una mena d'"overview" i havia creat una certa expectacio, el comentari no va passar de "per si algu s'ho esta preguntant, haig de dir que no ho he acabat". Ni ell va donar mes detalls, ni ningu li va demanar (almenys publicament).

Aquest es un curs que es troba entre els que s'ofereixen als estudiants graduats (estudiants de doctorat) i consta de dues sessions setmanals, d'una hora cadascuna. Els dilluns, estudiants d'en Wiles expliquen temes de background i els dimecres ell mateix explica el seu treball, i encara no ha arribat a la part inacabada. En Deligne, en Faltings i en Katz son els "pesos pesants" que hi assisteixen, pero no sembla que estiguin fent un treball de col.laboracio amb ell. En canvi, qui si ho esta fent es en Richard Taylor, de Cambridge, (a qui en Wiles va dirigir la tesi) que ha arribat aqui aquest semestre per "ajudar-lo".

En resum, l'unic que es pot dir del cert es que en Wiles hi continua treballant. Saber si, ell sol o amb la col.laboracio d'algu, aconseguira aviat posar fi a la resistencia secular del Teorema de Fermat es quelcom que ens mante a tots a l'espera.

Be, no se si tot aixo us servira d'alguna cosa. En tot cas, si se us acut que us puc ajudar d'alguna altra manera, no dubteu a dir-ho.

Salutacions, i sort!

Anna

La redacció