un reflex de la intervenció del professorat que vol que els seus alumnes «facin matemàtiques», no solament exercicis repetitius sinó que hi busquin l'aspecte creatiu.

Perquè, doncs, la davallada del nombre d'alumnes? Perquè no és el mateix la tasca intensa d'un dia que l'exigència d'una feina continuada, no ho és en els concursos de matemàtiques i sabem que tampoc no ho és, per a la majoria de la gent, en la vida de cada dia. I com que veiem que el percentatge d'èxit va millorant, seguirem fent els concursos. Lectores i lectors que hi podeu ajudar, animeu els nois i les noies perquè hi participin!

Com a coordinador de les activitats telemàtiques no puc acabar aquest article sense fer arribar el meu agraïment, primer de tot, a tot el professorat que anima els seus alumnes a participar-hi i també, és clar, a totes les persones que hi han col·laborat durant el curs 2015–2016, en especial Joan Josep Carmona de la UAB pel que fa a l'Olitele, i Miquel Vilà i Dani Bosch pel que fa a la Marató, i a altres membres de la Comissió Cangur, que també hi intervenen en molts aspectes.

Podeu trobar informació detallada de les edicions d'aquests concursos a: `http://www.cangur.org/telematics/`.

Andrew Wiles, premi Abel 2016

Pilar Bayer
Universitat de Barcelona

El 15 de març passat, el president de l'Acadèmia Noruega de les Ciències i de les Lletres, Ole M. Sejersted, anunciava que el premi Abel 2016 havia estat concedit al matemàtic britànic Sir Andrew J. Wiles «per la seva impressionant demostració del darrer teorema de Fermat per mitjà de la conjectura de modularitat per a les corbes el·líptiques semiestables, i així obria una nova era en teoria de nombres».

En la seva catorzena edició, el comitè avaluador del premi havia estat format per John Rognes, president, professor de la Universitetet i Oslo, i pels vocals Luigi Ambrosio, professor de la Scuola Normale Superiore di Pisa; Marta Sanz-Solé, professora de la Universitat de Barcelona; Marie-France Vignéras, professora de l'Institut de Mathématiques de Jussieu-Paris Rive Gauche; i Ben J. Green, professor de l'Oxford University.

El 24 de maig, el príncep Haakon de Noruega lliurà el guardó a Wiles en el decurs d'una cerimònia solemne celebrada a la Universitat d'Oslo. L'acte, que es pot seguir per internet, s'inicià amb l'entrada al recinte de Wiles (acompanyat de cares nostrades) enmig d'un esclat de dues trompetes i un trombó de vares.

Tal com és habitual, l'endemà del lliurament del premi s'impartiren lliçons relacionades amb la seva temàtica. En aquesta ocasió foren: «Fermat's Last theorem: abelian and non-abelian approaches», a càrrec de Wiles; «Andrew Wiles' marvelous proof», a càrrec de Henri Darmon, professor de la Universitat McGill, de Mont-real, al Canadà i «What is the Birch and Swinnerton-Dyer Conjecture, and what is known about it?», a càrrec de Manjul Bhargava, professor de la Universitat de Princeton i medalla Fields l'any 2014. A més, es va pronunciar una conferència del conegut divulgador científic Simon Singh titulada «From Fermat's Last Theorem to Homer's Last Theorem».

Sir A. Wiles i el príncep Haakon.
Fotografia: Audun Braastad.

Del «teorema de Fermat» al «teorema de Fermat-Wiles»

Pensant especialment en el públic jove de la *SCM/Notícies*, i atès que Wiles ha estat premiat per un resultat de fa més de vint anys, començarem per recordar les circumstàncies que envoltaren l'assoliment d'aquella fita.

En un capvespre de l'any 1994, l'anterior a la nit de Sant Joan, varen saltar totes les alarmes dels ordinadors de la comunitat matemàtica amb l'anunci que Andrew Wiles hauria pogut demostrar el darrer teorema de Fermat. Wiles i el seu entorn eren ben coneguts pels teòrics dels nombres, la qual cosa induïa a pensar que la notícia podia ben bé ser certa.

L'any 1977, Wiles i el seu director de tesi a Cambridge, John Coates, havien obtingut el primer resultat general sobre la conjectura de Birch i Swinnerton-Dyer (avui, un dels set problemes del mil·lenni): la funció L d'una corba el·líptica $E|\mathbb{Q}$, dotada de multiplicació complexa, s'anul·la en $s = 1$ quan el rang de E és positiu [5]; les eines de la demostració d'aquest resultat provenien de la teoria d'Iwasawa, de la qual Coates era un reconegut expert. Recordo la presentació que Wiles havia fet l'any 1978 a les Journées Arithmétiques de Luminy del seu treball sobre lleis de reciprocitat explícites [22]; aquest treball estenia les lleis de reciprocitat de Kummer a grups formals, completava resultats de [4] i era emprat en [5]. L'any 1984, i després del seu pas per l'MIT i d'haver estat contractat a Princeton, Wiles i Barry Mazur [12] havien demostrat la impactant conjectura principal de la teoria d'Iwasawa. L'eina bàsica procedia d'un estudi de l'aritmètica de les corbes modulars $X_1(p^n)$, $p \neq 2$ primer, que desenvolupava l'iniciat anys abans per Mazur [11]. Mazur i Wiles traslladaven així les pautes de Kenneth Ribet [13] relatives a la construcció modular d'extensions no ramificades dels cossos ciclotòmics $\mathbb{Q}(e^{2\pi i/p})$ a la construcció modular d'extensions no ramificades de cossos de nombres abelians. A més, la prova de la conjectura principal de la teoria d'Iwasawa fou estesa posteriorment per Wiles a tots els cossos base totalment reals.

Els mesos que seguiren a l'anunci de la prova per Wiles del teorema de Fermat van ser de molta angoixa, causada principalment per una llacuna en la pretesa demostració que fou detectada pel seu col·lega de Princeton Nicholas Katz i que deixava la prova inacabada. La premsa es feu ressò de l'enrenou i, fet insòlit, mig món estigué pendent de si un matemàtic podia o no completar una «demostració meravellosa» recercada des de feia més de 350 anys. Amb uns quants mesos més de treball intens i la inestimable col·laboració de Richard Taylor, exalumne de Wiles, la qüestió es va poder tancar. Més endavant, els fets serviren fins i tot d'inspiració d'un musical: *Fermat's Last Tango* [7], ric en escenes delicioses, com ara la de l'After Math o espai de trobada en el més enllà de l'elit matemàtica.

Els articles de Wiles [23] i de Taylor–Wiles [20] posaren fi a un any d'incerteses en tant que la comunitat matemàtica pogué donar el vistiplau a la prova del famós teorema. El món va respirar tranquil, al mateix temps que els experts s'abocaven a copsar totes les subtileses de la demostració i de les eines que s'hi empraven. Els articles esmentats de Wiles i de Taylor-Wiles culminaven, d'una banda, l'esforç de molts matemàtics durant molts anys i, de l'altra, reunien una munió considerable de tècniques en les quals calia aprofundir i destinades a donar feina a molta gent, com el anys posteriors han anat posant de manifest. (Segons el Genealogy Project, Wiles té avui dia 178 descendents.)

Shimura-Taniyama-Weil *versus* Fermat

Moltes generacions de matemàtics s'han sentit atretes per l'equació

$$X^n + Y^n = Z^n \tag{1}$$

i hi han pogut fer les seves contribucions. La història és precedida pels babilonis i Diofant d'Alexandria amb la recerca de ternes pitagòriques ($n = 2$), però s'inicia amb Fermat ($n = 4$) i és considerada per Euler i Gauss ($n = 3$), Legendre i Dirichlet ($n = 5$), Lamé i Lebesgue ($n = 7$) i prossegueix amb Kummer ($n = p$, primer regular), Sophie Germain, Vandiver, Carlitz, Iwasawa, Wagstaff, etc. Tots aquests autors pogueren donar proves, parcials o completes, de la no-existència de solucions enteres (x, y, z), $xyz \neq 0$, per a exponents particulars. L'estudi d'aquesta equació no ha deixat mai d'avançar, al mateix temps que ha servit de pedra filosofal per al progrés de l'aritmètica.

Un gir important en la història del teorema de Fermat es produí l'any 1986 gràcies al treball de Gerhard Frey [9]. El sagaç Frey s'adonà que una hipotètica solució (a, b, c) de l'equació de Fermat d'exponent primer $p > 5$, $abc \neq 0$, donava lloc a una corba el·líptica

$$E_{a,b}: \quad Y^2 = X(X - a^p)(X + b^p)$$

que posseia una sèrie de propietats remarcables: (a) $E_{a,b}$ té reducció semiestable en tots els primers. (b) El seus punts de p divisió proporcionen una extensió $K_p|\mathbb{Q}$ que és no ramificada fora de $2p$ i poc ramificada en les places $\mathfrak{p}$ que divideixen (p). (c) El grup de Galois $\mathrm{Gal}(K_p|\mathbb{Q})$ és isomorf al grup lineal $\mathrm{GL}(2,\mathbb{F}_p)$ i és, així, el més gran possible.

En particular, la corba considerada per Frey posava de manifest que una hipotètica solució de l'equació de Fermat conduïa a l'existència d'extensions $K_p|\mathbb{Q}(e^{2\pi i/p})$ molt poc ramificades. Per tant, a fi d'arribar a una contradicció amb l'existència de solucions de l'equació (1) només calia provar que aquestes extensions, de fet, no podien existir. Atès que el grup de Galois $\mathrm{Gal}(K_p|\mathbb{Q}(e^{2\pi i/p}))$ era no resoluble, la teoria de cossos de classes no en donava informació, perquè aquesta tracta únicament de les extensions abelianes dels cossos de nombres [1]. Calia, per tant, un canvi de paradigma.

La idea de Frey va ser lligar aquest enfocament al d'una possible inexistència de determinades representacions galoisianes de dimensió 2; és a dir, d'homomorfismes continus

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2,R),$$

on $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ denota el grup de Galois absolut del cos dels racionals i $\mathrm{GL}(2,R)$ el grup lineal format per les matrius 2×2 invertibles i de coeficients en un anell topològic R. Pel que fa a això, Frey consultà Jean-Pierre Serre (premi Abel 2003). La resposta de Serre a Frey va cristal·litzar al cap d'un any amb la formulació d'unes conjectures molt precises, les anomenades «conjectures de modularitat de Serre», aplegades en l'article [16] i que tenien com a punt de partida els resultats de Serre que ell ens havia explicat a les Journées Arithmétiques de Bordeaux, el 1974 [15]. Per apropar-nos a la resposta de Serre a Frey, cal que recordem breument el concepte de forma modular.

Les formes modulars són funcions de variable complexa, definides en el semiplà de Poincaré, que satisfan certes equacions funcionals i que es poden introduir de maneres molt diferents. Des d'un punt de vista geomètric, les formes modulars clàssiques són seccions de fibrats de línia d'espais de moduli compactificats de corbes el·líptiques amb diferents estructures de nivell. Al seu torn, aquests espais de moduli donen lloc a corbes modulars, com ara $X_1(N)$ o bé $X_0(N)$, i als seus cossos de funcions modulars corresponents, ben coneguts ja des del temps de Dedekind, Klein, Fricke i Poincaré. Les formes modulars dites «cuspidals» són funcions de comportament local moderat i es distribueixen en espais vectorials de dimensió finita, $S(N,k,\chi)$, caracteritzats per tres paràmetres anomenats «nivell», «pes» i «caràcter», respectivament. Quan el caràcter és trivial, l'espai vectorial anterior es denota per $S_k(N)$; a continuació suposarem que k és un nombre parell i positiu. Des d'un punt de vista aritmètic, l'atractiu de les formes modulars rau en el fet que són expressables per mitjà de sèries de Fourier els coeficients de les quals són assequibles algorítmicament. A més, gràcies a l'existència d'operadors de Hecke que actuen en $S(N,k,\chi)$, aquests espais posseeixen bases formades per formes modulars de coeficients enters algebraics.

En una sèrie de remarcables treballs de la dècada dels setanta, Eichler, Shimura, Deligne (premi Abel 2013) i Deligne-Serre havien associat representacions galoisianes ρ_f, ℓ-àdiques i de dimensió 2, a les formes modulars f que eren vectors propis dels operadors de Hecke. En considerar una mena de recíproc, la idea de Serre és fàcil de resumir: certes representacions galoisianes ρ, senars, irreductibles i de dimensió 2, però ara valorades en cossos finits, havien de ser modulars; és a dir, havien de provenir per reducció dels seus coeficients de famílies de formes modulars f_ρ, vectors propis dels operadors de Hecke (conjectura de modularitat de Serre). A més, Serre era capaç, a partir de les propietats de ramificació de la representació ρ de partida, de conjecturar els paràmetres optimals $(N_\rho, k_\rho, \chi_\rho)$ de les formes f_ρ (conjectura de modularitat de Serre refinada). Si les conjectures de modularitat de Serre eren certes i la corba el·líptica $E_{a,b}$ era capaç de produir representacions galoisianes $\rho_{a,b}$ modulars, acabaríem, per refinament, en una forma modular no nul·la $f_{a,b}$ de tipus optimal ($N=2$, $k=2$, $\chi=1$). Però la corba modular de nivell $N=2$ és una recta projectiva, amb la qual cosa $S_2(2)=(0)$; s'arribaria així a una contradicció. Amb altres paraules, si Serre i Frey tenien raó, una solució (a,b,c) no trivial de l'equació de Fermat produïa una corba el·líptica $E_{a,b}$ que no podia

existir i, en conseqüència, la terna (a, b, c), tampoc.

Tot seguit es portaren a terme una sèrie de treballs orientats a la demostració de les conjectures de Serre en casos particulars, el més important dels quals fou obra de Ribet [14]. Aquest treball representà un altre *tour de force* en aquesta història ja que hi apareixen les corbes de Shimura, objectes subtils que apleguen en el seu interior l'aritmètica d'anells d'enters no commutatius que provenen d'àlgebres de quaternions. Diguem de passada que un dels pocs textos accessibles a l'època sobre aquest particular era el de Marie-France Vignéras [21].

T. Tamagawa, J-P. Serre, Y. Taniyama i A. Weil a Tòquio-Nikko, 1955. Font: G. Shimura [17].

A partir del treball de Ribet [14] s'arribava a la conclusió que el teorema de Fermat se seguia de la validesa de la conjectura de Shimura-Taniyama-Weil (STW), perfilada a partir del Simposi Internacional de Teoria Algebraica de Nombres celebrat a Tòquio-Nikko el 1955. A partir dels anys setanta, i de l'ús massiu dels ordinadors, s'havia aconseguit una gran evidència numèrica a favor d'aquesta conjectura. D'una banda, STW garantia que la representació galoisiana

$$\rho_{a,b}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \mathbb{F}_p)$$

definida pels punts de p divisió de la corba el·líptica $E_{a,b}$ havia de ser una representació modular de les considerades per Serre i, de l'altra, el treball de Ribet [14] permetia tot seguit deduir que els seus paràmetres optimals eren els predits per Serre: $(2, 2, 1)$ si $p \geq 11$. A més, atesa la natura de la corba de Frey, no calia demostrar STW en tota la seva generalitat, bastava fer-ho per a les corbes el·líptiques semiestables. Així, doncs, des de finals de la dècada dels vuitanta queda palès que se sabia de l'existència d'un camí que podia conduir a la prova del teorema de Fermat [2]. Això no obstant, el seu pendent lluïa massa pronunciat per intentar-ne el recorregut. Ningú no semblava tenir cap indici sobre la prova de STW; ningú, llevat de Wiles!

Les corbes modulars $X_1(N)$ són espais de moduli de corbes el·líptiques i es presenten en diferents nivells. Fotografia al·legòrica.

La prova per Wiles de STW-semiestable

La conjectura STW és una de les primeres conjectures de modularitat que es van formular; afirma que les corbes el·líptiques definides per una equació de coeficients racionals són parametritzables hiperbòlicament per funcions modulars. Això implica que, per a cada corba el·líptica $E|\mathbb{Q}$, existeix una forma modular f_E de manera que la funció L de Hasse-Weil de la corba el·líptica i la funció L associada a la forma modular per mitjà de la transformada de Mellin satisfan la identitat $L(E, s) = L(f_E, s)$, $\Re(s) > 3/2$. Ambdues funcions són de variable complexa; la funció $L(E, s)$ és un objecte d'origen aritmètic que s'obté en tenir en compte el nombre de punts de la corba en els diferents cossos finits $\mathbb{F}_q$, $q = p^k$; en principi està definida únicament per a $\Re(s) > 3/2$. La funció $L(f_E, s)$ és un objecte analític, definit per a tot $s \in \mathbb{C}$. Si una corba el·líptica $E|\mathbb{Q}$ satisfà STW, aleshores la igualtat anterior permet deduir el caràcter enter de la seva funció L convenientment completada i, en particular, la funció està definida per a tot s complex, es pot avaluar en $s = 1$ i (com en el cas de les corbes el·líptiques amb multiplicació complexa) la conjectura de Birch i Swinnerton-Dyer recupera sentit.

Una representació galoisiana ρ comporta informació algebraica i informació aritmètica, que es tradueix en les lleis de reciprocitat proporcionades pels elements de Frobenius (automorfismes de $\overline{\mathbb{Q}}$ associats als diferents primers). Ambdues informacions queden reflectides en la funció $L(\rho, s)$ associada a la representació. El reconeixement del caràcter modular d'una representació és d'importància extrema. De manera breu, si una representació de Galois és modular, aleshores la seva funció L proporcionarà, a més, informació analítica.

Donat un enter n, considerem el grup de les arrels n-èssimes complexes de la unitat, isomorf al grup cíclic C_n, d'ordre n, que té com a elements els punts de n divisió de la circumferència unitat. L'estudi dels cossos ciclotòmics $\mathbb{Q}(e^{2\pi i/n})$ s'inicià en el darrer capítol de les *Disquisicions aritmètiques* de Gauss, com a base del problema de la caracterització dels polígons regulars construïbles amb regle i compàs. Una de les fites clàssiques en la demostració del teorema de Fermat havia estat assolida per Ernst Kummer, continuador dels estudis de Gauss. Entre d'altres resultats, Kummer havia demostrat la validesa del teorema de Fermat per a tots els primers p dits «regulars» a partir de les propietats aritmètiques de l'anell dels enters $\mathbb{Z}[e^{2\pi i/p}]$ del cos ciclotòmic p-èssim. Els treballs de Kummer foren pioners i donaren lloc al naixement de l'estudi dels anells d'enters dels cossos de nombres, per part de Dirichlet i de Dedekind. En la primera meitat del segle XX, es desenvolupà la teoria de cossos de classes que s'ocupa de les lleis que regeixen l'aritmètica de les extensions abelianes dels cossos de nombres.

Donada una corba el·líptica E, la seva llei d'addició (visible a través de les propietats de la funció $\wp$ de Weierstrass i de la seva derivada, que la parametritzen) permet considerar els grups $E[n] \simeq C_n \times C_n$, d'ordre n^2, dels seus punts de n-divisió. Quan E està definida sobre $\mathbb{Q}$, les coordenades d'aquests punts són nombres algebraics i en adjuntar-les a $\mathbb{Q}$ se satisfà la inclusió de cossos: $\mathbb{Q}(e^{2\pi i/n}) \subseteq \mathbb{Q}(E[n])$. Per tant, l'estudi aritmètic dels cossos $\mathbb{Q}(E[n])$ es pot entendre com la continuació natural de l'estudi aritmètic dels cossos ciclotòmics portat a terme per Kummer.

La demostració de Wiles de la conjectura STW per a les corbes el·líptiques $E|\mathbb{Q}$ semiestables consistí a deduir la modularitat de la corba a partir de la modularitat de determinades representacions de Galois ℓ-àdiques. La idea principal prové del fet que la modularitat és, tanmateix, una propietat que s'encomana.

Wiles se submergeix en una teoria de deformacions de representacions, iniciada per Mazur, que li permet contagiar la modularitat a una corba el·líptica semiestable E a partir de la modularitat de certes representacions de Galois que provenen per deformació de les representacions de Galois definides pels seus punts de 3 o bé de 5 divisió. Si la representació $\rho_{E,3}$ associada als punts de 3-divisió de E és irreductible, la modularitat de E és contagiada a partir de la modularitat d'una deformació 3-àdica escollida *ad hoc* de $\rho_{E,3}$; la modularitat d'aquesta darrera s'obté a partir de resultats de Deligne-Serre i de R. P. Langlands (1980) i de J. Tunnell (1981), aquests darrers sobre representacions de Galois complexes, octaèdriques o tetraèdriques, respectivament. Si la representació $\rho_{E,3}$ redueix, la modularitat de E és contagiada a partir de la modularitat d'una deformació 5-àdica escollida *ad hoc* de la representació $\rho_{E',5}$ associada als punts de 5-divisió d'una altra corba el·líptica modular $E'|\mathbb{Q}$ i tal que $E[5] \simeq E'[5]$; l'existència de E' resulta de propietats de la corba modular $X_0(15)$, conegudes per [11].

Les deformacions de les representacions considerades $\rho_{E,p}$ es classifiquen d'acord amb uns certs tipus $\mathcal{D}$ i estan controlades per un anell universal de deformacions $R_{\mathcal{D}}$. Les deformacions modulars de les representacions considerades estan descrites per un anell $H_{\mathcal{D}}$ relacionat amb l'àlgebra de Hecke en operar sobre els espais de formes modulars. En les condicions de la demostració de STW, existeix un morfisme exhaustiu

$$\eta_{\mathcal{D}} \colon R_{\mathcal{D}} \longrightarrow H_{\mathcal{D}}.$$

La prova de STW s'obté en determinar l'existència d'un tipus optimal $\mathcal{D}$ per al qual el morfisme $\eta_{\mathcal{D}}$ és un isomorfisme. La part més difícil de la demostració consisteix a provar que si $\rho_{E,p}$, suposada modular, és no ramificada en un primer ℓ, aleshores admet una deformació modular en què aquest primer no divideix el nivell de la forma modular. Per a tal fi, Wiles necessita generalitzacions dels resultats de Ribet [14], que li foren propor-

cionades en un treball paral·lel de Diamond [6], exalumne seu.

Avenços posteriors

El coneixement adquirit fins ara de les representacions de $G_{\mathbb{Q}}$ de dimensió 2 suposa un avenç molt significatiu respecte de la teoria de cossos de classes, en tant que aquesta teoria és formulable en termes de representacions de $G_{\mathbb{Q}}$ de dimensió 1. L'estudi de les representacions galoisianes (complexes, ℓ-àdiques, de característica positiva, etc.) de dimensió $n \geq 1$ forma part del programa de Langlands, una teoria unificadora que comprèn moltes de les recerques que es fan en l'actualitat en teoria de nombres relatives a motius, les seves funcions L i els seus valors especials.

Les conjectures de modularitat de Serre formen part avui del programa de Langlands, han estat completament demostrades en els darrers anys i han conegut generalitzacions significatives quan es canvia el cos base $\mathbb{Q}$ per un cos de nombres F totalment real. També la conjectura STW per a les corbes el·líptiques $E|\mathbb{Q}$ ha estat demostrada en tots els casos i se'n cerquen generalitzacions escaients, en cossos base més generals o en varietats abelianes de dimensió superior i de tipus GL_2 sobre $\mathbb{Q}$. S'ha avançat també en el coneixement de les varietats de Shimura, de Hilbert i de Siegel, la qual cosa comporta que avui sigui abordable l'estudi d'altres equacions diofantines. Per a més informació sobre aquests resultats, podeu veure [3, 8, 10, 18, 19].

En aquesta nova era de la teoria de nombres, la comprensió de les representacions galoisianes segueix actuant com un dels catalitzadors més potents, la qual cosa equival a avançar en les tècniques utilitzades per Wiles en la seva prova de la modularitat de Shimura-Taniyama-Weil per a les corbes el·líptiques semiestables, objecte del premi Abel que hem comentat.

Referències

[1] E. Artin, J. Tate, «Class field theory». Reimpressió de l'original del 1967. AMS Chelsea Publishing, Providence, RI, 2009. VIII+194 p. ISBN: 978-0-8218-4426-7.

[2] P. Bayer, «Weil versus Fermat». Text presentat a les *XIII Jornadas Hispano-Lusas de Matemáticas*. Universidad de Valladolid, 1988.

[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, «On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises». *J. Amer. Math. Soc.* **14** (2001), 843–939.

[4] J. Coates and A. Wiles, «Explicit reciprocity laws». *Journées Arithmétiques de Caen* (Univ. Caen, Caen, 1976), p. 7–17, *Astérisque* 41–42, Soc. Math. France, Paris, 1977.

[5] J. Coates and A. Wiles, «On the conjecture of Birch and Swinnerton-Dyer». *Invent. Math.* **39**(3) (1977), 223–251.

[6] F. Diamond, «The refined conjecture of Serre». En el llibre *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), 22–37, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[7] *Fermat's Last Tango*. Lletra i música de J. Rosenblum; IMDb, 2001; musical basat en un text de Joanne Sydney Lessner. Director D. Stern.

[8] N. Freitas, B. Le Hung, and S. Siksek, «Elliptic curves over real quadratic fields are modular». *Inventiones Mathematicae* **201**(1) (2015), 159–206.

[9] G. Frey, «Links between stable elliptic curves and certain Diophantine equations», *Ann. Univ. Sarav. Ser. Math.* **1**(1) (1986), IV+40 p.

[10] C. Khare and J.-P. Wintenberger, «On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$». *Ann. of Math.* (2) **169**(1) (2009), 229–253.

[11] B. Mazur, «Modular curves and the Eisenstein ideal». *Inst. Hautes Études Sci*, Publ. Math. **47** (1977), 33–186 (1978).

[12] B. Mazur and A. Wiles, «Class fields of abelian extensions of $\mathbb{Q}$». *Invent. Math.* **76**(2) (1984), 179–330.

[13] K. Ribet, «A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$». *Invent. Math.* **34**(3) (1976), 151–162.

[14] K. Ribet, «On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ arising from modular forms». *Invent. Math.* **100**(2) (1990), 431–476.

[15] J.-P. Serre, «Valeurs propres des opérateurs de Hecke modulo l», *Journées Arithmétiques de Bordeaux* (Conf., Univ. Bordeaux, 1974). *Astérisque* (Paris: Société Mathématique de France), **24–25** (1975), 109–117.

[16] J.-P. Serre, «Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$». *Duke Math. J.* **54**(1) (1987), 179–230.

[17] G. Shimura, «Yutaka Taniyama and his time». *Bull. London Math. Soc.* **21** (1989), 186–196.

[18] C. Skinner and A. Wiles, «Residually reducible representations and modular forms». *Inst. Hautes Études Sci. Publ. Math.* **89** (1999), 5–126 (2000).

[19] C. Skinner and A. Wiles, «Nearly ordinary deformations of irreducible residual representations». *Ann. Fac. Sci. Toulouse Math.* (6) **10**(1) (2001), 185–215.

[20] R. Taylor and A. Wiles, «Ring-theoretic properties of certain Hecke algebras». *Ann. of Math.* (2) **141**(3) (1995), 553–572.

[21] Marie-France Vignéras, «Arithmétique des algèbres de quaternions». Lecture Notes in Mathematics, 800. Springer, Berlin, 1980. VII+169 pp. ISBN: 3-540-09983-2.

[22] A. Wiles, «Higher explicit reciprocity laws». *Ann. Math.* (2) **107**(2) (1978), 235–254.

[23] A. Wiles, «Modular elliptic curves and Fermat's last theorem». *Ann. of Math.* (2) **141**(3) (1995), 443–551.

Rutes matemàtiques en el Congrés d'Educació Matemàtica

Joan Girbau i Iolanda Guevara
Universitat Autònoma de Barcelona i adjunta a la vicepresidència de la SCM

En el marc del Segon Congrés d'Educació Matemàtica (C^2EM) organitzat per la Federació d'Entitats per a l'Ensenyament de les Matemàtiques a Catalunya (FEEMCAT) i la Facultat de Matemàtiques de la UB, celebrat els dies 11, 12 i 13 de juliol a Barcelona, es va dedicar una tarda als itineraris matemàtics per la ciutat de Barcelona.

L'objectiu d'incloure aquestes sortides en l'àmbit del congrés era doble: d'una banda, introduir unes activitats més lúdiques en el calendari del congrés i, de l'altra, confeccionar un catàleg de sortides que en el futur poguessin utilitzar els mestres i professors amb els alumnes.

El comitè científic del congrés va encomanar a la SCM que organitzés aquestes sortides i l'entitat va acceptar el repte. Es va constituir una comissió de persones per organitzar les sortides del 12 de juliol a la tarda. A més, cal no oblidar que el dilluns de 10 a 12 hores, els assistents al congrés també van tenir l'opció de visitar el Museu de les Matemàtiques de Catalunya (MMACA).

Una part de les sortides eren rutes matemàtiques, desplaçant-se per la ciutat de Barcelona, les cinc primeres de la taula següent; altres activitats se situaven en un lloc concret: un monestir, un temple o bé un museu. El denominador comú era la mirada matemàtica del lloc o del recorregut. També el fet que fos possible repetir la sortida amb alumnes de les diferents etapes educatives. Unes tenen material addicional per treballar amb els alumnes, mentre que d'altres ofereixen material adreçat al professorat que els acompanyi. Tot aquest material estarà disponible a partir del gener del 2017 al portal de la SCM.