una primera proposta. Els responsables de cada àrea les estudien i envien els seus comentaris als organitzadors per millorar-la. Per exemple, una variable que el CIMPA té molt en compte és intentar trobar un equilibri entre el nombre d'homes i de dones participants. Un cop rebuts els comentaris, els organitzadors tornen a enviar la proposta abans de l'1 d'octubre.

Els projectes que s'envien l'any 2016 són d'escoles que se celebraran el 2018. I és que, en aquest període temps, un comitè científic extern al CIMPA estudia els projectes rebuts, els classifica i genera un informe. L'informe serveix al CIMPA per escollir les escoles que se celebraran. Una vegada escollides, s'han de distribuir i deixar un temps perquè s'hi registrin els participants. Aquest temps oscil·la sovint entre tres i sis mesos.

Després de ser admesa la proposta, i fins que s'acaba el termini d'inscripció, els organitzadors han de concretar qüestions ben determinades: decidir el pressupost, trobar el lloc per celebrar l'esdeveniment, buscar allotjament, etc. A continuació, juntament amb el CIMPA, es trien els participants i comença una tasca d'organització que els involucra personalment ja que cada participant prové d'un país diferent i cada país té la seva pròpia idiosincràsia. Per exemple, es necessita força temps entre la inscripció i la celebració de l'escola, per aconseguir visats per als participants estrangers, cosa que no sempre és fàcil i que de vegades resulta impossible. Per exemple, és el cas de participants del Pakistan que volen prendre part a les escoles que es duen a terme a l'Índia o viceversa.

Tot aquest «full de ruta» per organitzar una escola CIMPA es troba a la pàgina web. Per descomptat, també es pot preguntar als responsables del CIMPA, inclòs el que signa aquestes paraules, que amb molt gust farem el possible per aclarir-les. També podem intentar proporcionar algun contacte en països en vies de desenvolupament, si cal i és possible. Més informació de moltes altres activitats que promou el CIMPA la podeu trobar a la pàgina web `http://www.cimpa-icpam.org`.

Jorge Jiménez Urroz
Universitat Politècnica de Catalunya

La conjectura de Birch i Swinnerton-Dyer: la beca ERC de Víctor Rotger

El 24 de maig del 2000, el Clay Mathematics Institute (`www.claymath.org`) va anunciar al Collège de France de París els set problemes del mil·lenni, set qüestions fonamentals en la recerca matemàtica que plantegen alguns dels problemes més difícils i profunds que els matemàtics estan cridats a resoldre aquest mil·lenni. Alguns d'aquests interrogants romanen oberts sense resoldre des de fa alguns segles, altres tenen arrels més modernes. Un dels reptes, la conjectura de Poincaré, ha estat resolt recentment pel controvertit matemàtic rus Gregori Perelman. La resta dels problemes semblen, a ulls dels experts, molt lluny encara de ser resolts.

Un d'aquests problemes és la conjectura plantejada als anys seixanta pels matemàtics de Cambridge Brian Birch i sir Peter Swinnerton-Dyer sobre l'aritmètica de les corbes el·líptiques sobre el cos dels nombres racionals. Aquest problema i les generalitzacions proposades per Beilinson, Bloch i Kato en el context general de les varietats algebraiques sobre cossos de nombres constitueixen els objectius principals en què se centra el projecte que ha obtingut l'any 2015 una Consolidator

Grant (CoG) de l'European Research Council (ERC).

A continuació descriurem el context dins la teoria de nombres en què s'emmarquen aquestes conjectures, en desgranarem l'enunciat i explicarem les contribucions que s'hi han fet des de la dècada dels anys seixanta i els resultats que el meu equip de recerca espera obtenir durant els propers cinc anys.

Els matemàtics sempre han estat fascinats pel problema de descriure les solucions en nombres enters d'equacions diofantines, com ara l'equació de Fermat:

$$F_n : x^n + y^n = z^n, \quad n > 1.$$

Euclides va donar la solució completa per a F_2, però per a $n > 2$ això esdevé un problema extremadament difícil. Com és ben conegut, l'any 1637 Fermat va conjecturar que per a $n > 2$, les úniques solucions enteres de F_n són les que satisfan $xyz = 0$. De fet, va deixar escrit que havia trobat una demostració meravellosa d'aquesta afirmació, però mai no es va descobrir i no hi ha ningú que cregui de debò que Fermat va trobar la resolució correcta de la qüestió.

L'any 1995 Andrew Wiles finalment va provar la cèlebre conjectura de Shimura-Taniyama sobre la modularitat de les corbes el·líptiques, que implicava el teorema de Fermat gràcies als treballs anteriors de Gerhard Frey i Ken Ribet. Precisament aquest resultat l'ha convertit enguany en el flamant guanyador del premi Abel 2016. Tal com se'n fa ressò el comitè d'aquesta darrera edició (format, juntament amb altres quatre membres, per la nostra companya Marta Sanz-Solé), els treballs d'Andrew Wiles sobre la conjectura de Shimura-Taniyama van obrir tota una nova era en la teoria de nombres. No hi ha cap dubte que va ser així.

La conjectura de Birch i Swinnerton-Dyer s'ocupa d'un problema similar i alhora està íntimament relacionat amb el teorema de Fermat i els teoremes de modularitat de Wiles: l'estudi de les solucions racionals de les corbes el·líptiques. Aquests corbes, que en la indústria es fan servir per encriptar informació confidencial vénen donades per equacions molt senzilles, de la forma

$$E : y^2 = x^3 + Ax + B$$

on A, $B \in \mathbb{Q}$ són paràmetres racionals.

L'encant d'aquestes corbes rau en el fet que, per a qualsevol extensió finita $K/\mathbb{Q}$ del cos dels nombres racionals, el conjunt $E(K)$ de solucions d'aquesta equació amb coordenades (x, y) en K admet una estructura natural de grup abelià finitament generat que es pot definir en termes geomètrics. És a dir:

$$E(K) \simeq \mathbb{Z}^r \oplus T$$

on $r = r(E/K) \geq 0$ és un enter no negatiu i $T = T(E/K)$ és un grup abelià finit.

Conèixer el rang d'aquest grup i el seu comportament en famílies (tot fent variar els paràmetres A i B entre els nombres racionals, o bé fent variar l'extensió K sobre la qual admetem les coordenades de les solucions) és cabdal per a tota mena d'aplicacions. Fins a l'actualitat, però, aquesta qüestió segueix tenint tota una aura de misteri i són més els interrogants que les respostes que hi ha.

La conjectura de Birch i Swinnerton-Dyer suggereix una fórmula per al rang $r(E/K)$ que, en cas de demostrar-se, establiria un pont entre grans branques de la matèria: l'àlgebra, la geometria i l'anàlisi. Per descriure-la cal introduir la funció zeta $\zeta(E/K, s)$ associada al parell (E, K). Es tracta d'una funció holomorfa

en el semiplà complex $\{s \in \mathbb{C} : \mathrm{Re}(s) > 3/2\}$ que es defineix mitjançant un mecanisme molt similar al de la definició de la funció zeta $\zeta(s)$ de Riemann que tots coneixem i que consisteix a empaquetar en un sol objecte analític el comportament de la reducció de la corba el·líptica E mòdul tots els nombres primers.

Tant la funció zeta de Riemann com la funció zeta $\zeta(E/\mathbb{Q}, s)$ associada a la corba el·líptica E sobre $\mathbb{Q}$ admeten una representació integral en tant que es poden expressar com la transformada de Mellin d'una forma modular. En el primer cas, aquest fenomen ja era ben conegut per Riemann mateix i la forma modular en qüestió és l'omnipresent funció theta de Jacobi. En el segon cas, aquesta formulació és precisament el contingut de l'esmentada conjectura de modularitat de Shimura-Taniyama que va demostrar Wiles. Per a extensions finites arbitràries $K/\mathbb{Q}$ com les considerades més amunt, també es prediu que $\zeta(E/K, s)$ admet una representació integral, però aquest és un problema de difícil resolució emmarcat dins de l'anomenat «programa de Langlands», en el qual se centren els esforços de bona part de la teoria de nombres i geometria algebraica moderna.

La representació integral descrita anteriorment sovint permet demostrar que les funcions zeta satisfan una equació funcional i es poden estendre a tot el pla complex. En els casos de $\zeta(s)$ i $\zeta(E/\mathbb{Q}, s)$, aquesta equació relaciona

$$\zeta(s) \leftrightarrow \zeta(1-s) \text{ i } \zeta(E/\mathbb{Q}, s) \leftrightarrow \zeta(E/\mathbb{Q}, 2-s).$$

En el primer cas, el centre de simetria és $s_0 = \frac{1}{2}$ i la hipòtesi de Riemann (un altre dels set problemes del mil·lenni) conjectura que tots els zeros no trivials de $\zeta(s)$ haurien de concentrar-se en l'eix format pels nombres complexos amb la mateixa part real que s_0.

En analogia amb això, no és cap casualitat que la conjectura de Birch i Swinnerton-Dyer també se centri en el comportament de $\zeta(E/\mathbb{Q}, s)$ en el punt de simetria $s_0 = 1$ de la seva equació funcional. Concretament, prediu el següent:

Conjectura BSD: *L'ordre d'anul·lació de* $\zeta(E/K, s)$ *en* $s_0 = 1$ *és igual a* $r(E/K)$.

A més, la conjectura proposa una fórmula explícita per al primer coeficient no nul del desenvolupament de Taylor de $\zeta(E/K, s)$ en $s_0 = 1$ en termes d'invariants aritmètics globals de la corba el·líptica E sobre K. Entre aquests invariants n'hi ha un que sense cap dubte és el més profund i delicat: el cardinal del grup de Tate-Shafarevic de E/K. Aquest grup mesura l'error que es comet quan intentem descriure els punts de $E(K)$ en termes purament cohomològics; en analogia natural amb la conjectura de Hodge (encara un altre dels set problemes del mil·lenni) que prediu que els cicles algebraics donen peu a un subgrup d'índex finit en el grup de classes de Hodge en la cohomologia de Betti d'una varietat algebraica. En el context aritmètic que ens ocupa també es conjectura que el grup de Tate-Shafarevic de E/K és finit.

Aquesta finitud, però, està demostrada en molt pocs casos, així que en general ens trobem davant d'una conjectura que, tal com va escriure John Tate, prediu que «el terme principal de $\zeta(E/K, s)$ en un punt on no es coneix que la sèrie convergeix està relacionat amb el cardinal d'un grup que no se sap que és finit». Queda pal·lès que tenim molta feina per endavant per demostrar la conjectura en tota generalitat.

El lector interessat a aprofundir en la interpretació aritmètica del comportament de les funcions zeta associades a motius arbitraris en el centre de simetria de les seves equacions funcionals (i en altres punts crítics en el sentit de Deligne), pot consultar-ho en els treballs de Beilinson, Bloch i Kato.

Matemàtics de la talla de Jean Pierre Serre, John Tate, Pierre Deligne o Andrew Wiles (per esmentar quatre dels guardonats amb el premi Abel) han contribuït enormement a entendre millor aquest problema. Però les úniques contribucions directes a la seva resolució són el teorema de John Coates i Andrew Wiles [2], els teoremes de Benedict Gross i Don Zagier [5] i Viktor Kolyvagin [7] i les seves generalitzacions degudes a Shou-Wu Zhang i la seva escola, que ataquen la conjectura quan les dues hipòtesis següents es verifiquen:

(H1) K està contingut en un cos de classes H d'un cos quadràtic imaginari tal que $H/\mathbb{Q}$ és una extensió normal i el seu grup de Galois és dihedral, i

(H2) la funció $\zeta(E/K, s)$ té com a molt un zero simple en $s_0 = 1$.

Tot i que no és cert que la conjectura de Birch i Swinnerton-Dyer estigui completament resolta quan les hipòtesis (H1) i (H2) es compleixen, sí que es pot afirmar que en tenim un coneixement satisfactori i que està demostrada en molts casos, quan certes hipòtesis tècniques addicionals se satisfan.

L'objectiu principal del projecte de recerca és desenvolupar i portar a la pràctica una estratègia nova per entendre millor i resoldre nous casos de la conjectura de Birch i Swinnerton-Dyer i les seves generalitzacions que explicarem breument a continuació. Això es durà a terme durant els propers cinc anys, fins a l'estiu del 2021, amb els meus col·laboradors habituals Massimo Bertolini (Essen), Henri Darmon (Mont-real), Alan Lauder (Oxford), col·legues de Barcelona com ara Francesc Fité, Xavier Guitart i Santiago Molina, i el grup d'estudiants de doctorat i investigadors postdoctorals que es podran contractar amb el finançament obtingut. Confiem a assolir els objectius ambiciosos que ens hem proposat; el que sí tenim clar és que no no hauria estat possible arribar fins aquí sense tot el que hem après tots aquests anys dels nostres mestres: la Pilar Bayer (UB), qui va ser la meva directora de tesi i a qui tant li dec, l'Enric Nart (UAB), en Jordi Quer (UPC) i la resta de companys del Seminari de Teoria de Nombres de Barcelona (`www.stnb.cat`).

La idea principal subjacent en tots els projectes de la nostra proposta és la següent. Sigui r l'ordre d'anul·lació de la funció zeta $\zeta(E/K,s)$ en $s_0=1$. Per demostrar la conjectura, cal

- $(\geq)$ construir r punts $P_1,...,P_r$ linealment independents en $E(K)$, i
- $(\leq)$ demostrar que el subgrup $\langle P_1,...,P_r\rangle$ generat per aquests punts té índex finit en $E(K)$.

Quan $r=0$ la part $(\geq)$ és evidentment innecessària; quan $r=1$, l'esmentat treball de Gross i Zagier constitueix literalment la part $(\geq)$ en el context de la hipòtesi (H1), on P_1 es construeix utilitzant la teoria de la multiplicació complexa. D'altra banda, Kolyvagin utilitza també aquesta mateixa teoria (de manera independent i amb tècniques molt diferents) per demostrar la part $(\leq)$ per a $r=0$ i $r=1$; com que la multiplicació complexa només té sentit amb la hipòtesi (H1), és per això que els resultats només són vàlids en aquest escenari.

Per t descriure el nostre projecte, tornem ara al cas general en què $K/\mathbb{Q}$ és una extensió finita qualsevol i l'ordre d'anul·lació $r\geq 0$ és arbitrari. L'estratègia que proposem passa per fer més flexibles alguns dels objectes amb els quals treballem. Fixem un nombre primer p i substituïm $E(K)$ per una versió cohomològica del mateix objecte, anomenat «el grup de Selmer p-àdic», $\mathrm{Sel}_p(E/K)$. Hom espera que tots dos grups siguin pràcticament iguals, i el grup que en mesura l'error és precisament el grup de Tate-Shafarevic del que parlàvem abans. Això ens resulta útil, perquè hem trobat un nou mètode per construir elements $\mathcal{P}_i$ en $\mathrm{Sel}_p(E/K)$ que haurien de tenir el rol dels punts descrits en la part $(\geq)$. Aquests elements els introduïm com a límit p-àdic de punts (més precisament, cicles) en certes varietats superiors de Chow. No podem demostrar que el límit d'aquests punts sigui de nou un punt en $E(K)$, que és el que de fet conjecturem, però sí que podem demostrar que aquest límit existeix i és un element ben definit en $\mathrm{Sel}_p(E/K)$.

Quan $r=0$, és a dir, quan $\zeta(E/K,1)\neq 0$, esperem que amb això n'hi hagi prou per demostrar $(\leq)$ i, per tant, la conjectura de Birch i Swinnerton-Dyer segons aquestes hipòtesis per a molts cossos K que no satisfan la hipòtesi (H1). En particular, esperem generalitzar al context de cossos de nombres totalment reals el famós teorema de Kato [6] dels anys noranta, i assolir per fi una fita que molts altres matemàtics han intentat infructuosament per altres mitjans.

Quan $r=1$, el cas aparentment més senzill que continua per resoldre més enllà de la hipòtesi (H1) sorgeix quan K és un cos de classes d'un cos quadràtic real. Aquest és precisament el context de les conegudes conjectures de l'any 2000 de Darmon [4], i esperem que les nostres idees ens permetin demostrar-les en bona part.

Un cop aconseguim construir els elements $\mathcal{P}_i$ descrits abans —i el mecanisme depèn en cada cas del cos K sobre el qual treballem: vegeu [3] per a alguns exemples—, el més difícil és demostrar $(\geq)$, és a dir provar que en podem trobar r de linealment independents. De vegades només obtenim succedanis d'aquest resultat en què $\zeta(E/K,s)$ és reemplaçada per

una versió p-adica de la funció zeta. A partir d'aquí, i malgrat això, tenim l'esperança de trobar les tecles que posin en marxa la maquinària dels sistemes d'Euler [1] per demostrar també la part ($\geq$). En casos favorables, aquesta maquinària no només demostra ($\geq$) sinó que també dóna com a resultat que $E(K)$ i $\mathrm{Sel}_p(E/K)$ són essencialment el mateix grup, tal com esperàvem.

Els nostres experiments (sí, podem calcular aquests punts numèricament, tot un luxe en el nostre camp) ens indiquen que aquest mètode només és capaç de proporcionar com a molt dos elements independents $\mathcal{P}_1$, $\mathcal{P}_2$.

Durant dècades només disposàvem de la teoria de la multiplicació complexa, que com a màxim produïa un únic punt no trivial i per a una col·lecció molt més limitada de cossos, així que per a nosaltres és un gran pas cap endavant poder cobrir una classe molt més àmplia d'extensions de $\mathbb{Q}$ i trobar resultats sobre la conjectura en situacions de rang 2!

Referències

[1] M. Bertolini, F. Castellà, H. Darmon, S. Dasgupta, K. Prasanna, V. Rotger, «p-adic L-functions and Euler systems: a tale in two trilogies». Proceedings of the EPSRC Durham Symposium on *Automorphic forms and Galois representations*, London Math. Society Lecture Notes **414**, (2014), 52–101.

[2] J. Coates and A. Wiles, «Explicit reciprocity laws». *Astérisque*, **41-42**, Soc. Math. France, Paris, 1977.

[3] H. Darmon and V. Rotger, «Diagonal cycles and Euler systems II: the Birch and Swinnerton-Dyer conjecture for Hasse-Weil-Artin L-series», pendent de publicar al *Journal of the American Mathematical Society*.

[4] H. Darmon, «Heegner points, Stark-Heegner points, and values of L-series», *International Congress of Mathematicians* II, 313–345, European Math. Soc., Zurich, 2006.

[5] B. Gross and D. Zagier, «Heegner points and derivatives of L-series», *Inventiones Mathematicae* **84** (1986), 225-320.

[6] K. Kato, «p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmétiques III». *Astérisque*, **295**(9) (2004), 117–290.

[7] V.A. Kolyvagin, «Finiteness of $E(\mathbb{Q})$ and LLI(E,$\mathbb{Q}$) for a subclass of Weil curves». Izv. Akad. Nauk SSSR Ser. Mat. **52**(3) (1988), 670–671.

Víctor Rotger
Universitat Politècnica de Catalunya

Fotografia matemàtica. Vint anys mirant el món amb ulls matemàtics

Aquest mes d'abril del 2016 l'Associació de Barcelona per a l'Ensenyament i l'Aprenentatge de les Matemàtiques (ABEAM) ha estat reconeguda amb el premi Matemàtiques i Societat 2016, concedit per la Fundació Ferran Sunyer i Balaguer de l'Institut d'Estudis Catalans a la sèrie de Concursos de Fotografia Matemàtica que organitzem des de l'any 2000 «com una eina per interessar els alumnes a aprofundir en les matemàtiques i saber-les relacionar amb altres aspectes de la vida quotidiana».

Aquest guardó és un reconeixement compartit entre professorat, alumnat, pares i mares, personal no docent, equips directius i societat en general, que d'una manera o altra s'han implicat a tenir una mirada matemàtica amable del món que ens envolta; és també un reconeixement a l'esforç de totes les entitats que treballen amb la fotografia matemàtica com a element dinamitzador.

Ara fa ja més de vint anys que es van començar a convocar els primers concursos de fotografia matemàtica als instituts de Cardedeu, Canovelles i la Garriga. Aquells primers concursos van ser el resultat de la iniciativa de tres departaments didàctics de matemàtiques amics que compartíem la il·lusió per millorar la manera d'ensenyar les matemàtiques a fi