Les matemàtiques, motor del món

Manuel Castellet, IEC
Director del Centre de Recerca Matemàtica

Ciència, cultura, saber, estètica, matemàtiques

El mot *ciència* (*scientia*) s'ha utilitzat, en molts contextos, de manera equivalent al de *saber*, o *coneixement*, tal com indica l'origen llatí: SCIRE. D'una banda, la ciència és un coneixement fruit del descobriment; d'una altra, és un coneixement derivat de l'experimentació o del càlcul. En la majoria de les ciències, el nou espai que ens obre el coneixement, a través d'una nova eina matemàtica, conceptual, és enorme i, sovint, el científic no busca descobrir per a saber, sinó, com deia Alfred North Whitehead, més aviat busca saber per a descobrir.

La ciència moderna pot conformar el pensament de diverses maneres, que no sempre propicien un saber més integrador. L'*Hypotheses non fingo* que ens proposà Isaac Newton a final del segle XVII no conté totes les realitats i una visió exhaustiva i completa d'aquestes realitats, sinó que és una gàbia extraordinària, com ho demostra que mai en la història cap línia de pensament, cap mètode de treballar els conceptes, no havia conduït a una revolució tan important com la ciència moderna. Com molt bé digué Konrad Knopp en la sessió inaugural de curs de la Universitat de Tübingen l'any 1927, «la matemàtica és la base de tot el coneixement i el contenidor de tota l'alta cultura».

Ciència, cultura i estètica. La ciència i els científics tenen una relació particularment significativa amb la bellesa. D'una banda, el descobriment d'objectes propers o llunyans, petits o grans, ha inspirat nombrosos artistes plàstics que estimulen la nostra curiositat per a conèixer-los millor, és a dir, per a progressar en la ciència. D'altra banda, la reflexió científica en ella mateixa ha originat unes línies de pensament de valors estètics elevats, apreciats sovint només per aquells que capten el significat, més o menys esotèric, de l'elaboració i la comunicació científiques.

Tanmateix, aquest concepte d'estètica no està renyit amb el llenguatge de la racionalitat. Els grecs i els escolàstics medievals l'utilitzaren ja en llur preocupació constant per una cosmovisió sistemàtica i globalitzadora: afirmació o tesi, explicació del significat dels termes emprats, argumentació i discussió. En les matemàtiques, professionalment, cal utilitzar un llenguatge, una notació, diferent de l'ordinari, que és indispensable per a la bona intercomunicació (com passa en la música, per esmentar un exemple ben assimilat). És fàcilment comprensible que aquest fet porta, sovint, a dificultats de comunicació.

En aquest article, pretenem establir ponts sòlids de connexió entre ciència, cultura, estètica i comunicació, a partir d'una sèrie de fets històrics que han mogut el món i d'uns de ben actuals que el mouen ara, posant èmfasi en la realitat del nostre país al llarg de la història i, molt especialment, en aquests darrers cent anys d'existència de l'Institut d'Estudis Catalans.

És un fet palpable que les eines matemàtiques són uns éssers desconeguts per a una bona part de la població i que la visibilitat de les matemàtiques a la cultura és força feble. D'exemples no en falten: fa un parell d'anys, un mitjà televisiu explicava com trisecar (dividir en tres parts) geomètricament els angles, quan fa temps que es va demostrar que no hi pot haver cap mètode per a fer-ho; o a la pel·lícula titulada *Pi*, en un moment de la qual es mostren una sèrie de xifres decimals del nombre transcendent π, xifres que a partir de la novena eren errònies. És bastant impensable que això pugui passar en altres disciplines sense que el públic se n'adoni.

Les matemàtiques, font de progrés

En aquest apartat, posaré uns pocs exemples de moments històrics, gairebé triats a l'atzar, en què les matemàtiques han exercit de veritable motor del món.

Al segle III abans de Crist, Arquimedes va inventar diverses màquines de guerra basades en palanques i politges que van dificultar enormement a l'exèrcit de Roma la conquesta de Grècia. «Doneu-me un punt de suport i mouré el món.» Amb aquesta frase anuncià la llei de la palanca. La llei de la palanca serveix de base a molts objectes quotidians, com ara les tenalles, les tisores, els obridors, els trencanous o les pinces. La diferència entre aquests rau en la situació del punt de suport.

Com podia navegar Cristòfor Colom sense cartes nàutiques, sense informació meteorològica i sense els moderns instruments de navegació dels quals disposem avui en dia? Ramon Llull fou l'autor del llibre *L'art de navegar*, que, escrit al segle XIII, fou un punt de referència fins ben entrat el segle XVI.

Al principi, els telescopis eren usats, únicament, amb finalitats comercials i militars. Encara que Galileu no va inventar el telescopi, va ser el primer a usar-lo, al segle XVI, per a estudiar el cel. Va observar els cràters de la Lluna, va descobrir els anells de Saturn, verificà les fases de Venus, i també va descobrir les quatre llunes de Júpiter.

La primera informació publicada sobre el càlcul diferencial i integral de Newton apareix indirectament en els famosos *Philosophiae naturalis principia mathematica*, del 1687. Aplica el seu mètode per a obtenir l'àrea compresa sota diverses corbes i per a resoldre nombrosos problemes que requereixen sumacions. Newton posà les bases i desenvolupà el càlcul diferencial i integral, que haurien d'ésser les eines sobre les quals es basaria la mecànica clàssica, fonament dels avenços científics i tecnològics durant més de dos-cents anys.

Bernhard Riemann, al segle XIX, va donar a conèixer una nova geometria. La utilització de l'espai multidimensional permeté simplificar la comprensió de les lleis de la natura. L'electricitat, el magnetisme i la gravetat no serien més que efectes causats per la distorsió de l'hiperespai. La força, segons Riemann, seria una conseqüència de la geometria de l'espai. Les idees de Riemann es van popularitzar: van arribar a Anglaterra i van penetrar en la literatura amb obres com *Alícia al país de les meravelles*, de Lewis Carroll, i *La màquina del temps*, de Herbert G. Wells. Però fou Albert Einstein qui, aplicant les idees de Riemann, va anunciar que la curvatura de l'espai està determinada per la quantitat de matèria i energia que conté i desenvolupà la teoria de la relativitat.

La (minsa) presència catalana en aquest procés històric

Catalunya és un país petit en superfície i en nombre d'habitants que no havia tingut mai una forta tradició matemàtica, ben diferent de la situació actual. Els exemples següents són pràcticament els únics fins ben entrat el segle XX.

Gerbert d'Orlhac, un monjo dels Pirineus catalans que l'any 1000 era ben conegut com a papa Silvestre II, estudià al segle X el quadrívium d'una manera profunda, i va renovar els sistemes de càlcul en l'àmbit europeu dos segles abans que Fibonacci, construint un àbac original.

El mallorquí Ramon Llull, un dels escriptors més importants en llengua catalana del segle XIII, comprenia ja l'esfericitat de la Terra i escrivia l'*Ars combinatoria* i l'*Art de navegar*, en el qual descriu l'astrolabi i s'esmenta l'ús de l'agulla magnètica, entre altres coneixements. Alexander von Humboldt afirmava, ara fa més de cent anys, que aquests progressos de la

ciència es van transmetre a la resta del món civilitzat des de Catalunya a través dels altres pobles de la Mediterrània.

Abraham Cresques, també mallorquí, dibuixà l'any 1375 el mapamundi anomenat *Atles català*, que fa una representació del món conegut aleshores i que fou fonamental per als navegants i viatgers de l'època.

El segon llibre de matemàtiques que es va imprimir a Europa (després de l'aritmètica anònima de Treviso) és la *Summa de l'art d'aritmètica*, de Francesc Santcliment, un llibre imprès en llengua catalana, l'any 1482, la traducció al castellà del qual fou la primera impressió a Espanya d'un llibre de matemàtiques.

El valencià Josep Chaix, autor de treballs de càlcul diferencial i integral, dugué a terme amb Pierre Méchain, l'any 1793, els càlculs per a mesurar l'arc de meridià entre els Pirineus i Barcelona.

Fins als anys setanta del segle passat, podem esmentar encara tres noms: Lluís Santaló, nascut a Girona i emigrat a l'Argentina, pioner de la geometria integral, l'estereologia i les probabilitats geomètriques; Frederic Alicart, castellonenc, depurat després de la guerra espanyola, que als anys seixanta escriví el primer manual d'ús dels ordinadors per als càlculs dels enginyers de camins, i Ferran Sunyer, físicament disminuït, possiblement el millor matemàtic a Catalunya a la meitat del segle XX, que treballà en anàlisi matemàtica i en honor del qual l'Institut d'Estudis Catalans, a través de la Fundació Ferran Sunyer i Balaguer, atorga anualment un premi internacional a una monografia que recopili i exposi els avenços més recents en una àrea activa de les matemàtiques.

Les matemàtiques, motor del món. Exemple 1: la teoria de nusos

L'any 1991, en el marc de l'Olimpíada Cultural, l'escultor britànic John Robinson presentava la seva darrera obra *Creation* en el Symposium on the Current State and Prospects of Mathematics, organitzat pel Centre de Recerca Matemàtica, un congrés en què assistiren sis matemàtics guardonats amb la medalla Fields, que analitzaren l'estat de la recerca en matemàtiques i les línies de futur.

Creation és una escultura de bronze, representació tridimensional d'allò que es coneix com *els anells de Borromeu*, tres cercles (o quadrats), dos dels quals no s'enllacen mai, però que formen una figura indesmuntable. Per a dissenyar-la, l'escultor es va inspirar en l'activitat del Centre de Recerca Matemàtica en el camp de la topologia, incrementant així la sèrie de figures amb motivacions geomètriques i, molt especialment, de la teoria de nusos, un dels exponents més importants de la qual és *Bonds of Friendship*, un bronze de 160 cm × 100 cm descobert a Sydney, l'any 1981, per la reina Isabel II d'Anglaterra.

Encara que els anells de Borromeu apareixen d'una manera clara i sistemàtica a Itàlia a partir del segle XIV, una figura de tres triangles entrellaçats ja fou utilitzada pels escandinaus al segle IX a Oseberg com un símbol associat al déu Odin, i una de tres anelles, al temple japonès de la religió xintoista O-Miwa Jinja al segle XII, que representen les tres terres: la dels déus, la dels homes i la dels morts.

El nom dels anells, associat a la família Borromeu, arrenca a la ciutat estat de Cremona, una moneda de la qual ja els inclou; Francesco Sforza adopta els anells en el seu escut i els concedeix a la família Borromeu com a agraïment quan, l'any 1450, esdevé duc de Milà. A partir d'aquest moment, els anells són representats en documents i edificis, entre els quals hi ha la tomba de Michelangelo, on simbolitzen els seus tres oficis: escultura, pintura i arquitectura. També l'Església els adoptà com a símbol de la Trinitat: Pare, Fill i Esperit Sant.

Però, des d'un punt de vista matemàtic, els anells de Borromeu constitueixen allò que s'anomena un *enllaç*, una estructura emanada de la teoria de nusos amb aplicacions interessants a la física teòrica i a la bioquímica.

Des d'un punt de vista topològic, un nus és una immersió d'una circumferència en l'espai tridimensional i dos nusos es consideren equivalents si es poden deformar isotòpicament l'un en l'altre. La unió d'un o més nusos s'anomena *enllaç*. Els anells de Borromeu constitueixen, doncs, un enllaç. Encara que la gent parli del nus de les sabates, aquests nusos es poden desfer per una deformació i, per tant, topològicament parlant no són considerats nusos. A part de la mateixa circumferència, el nus més simple és el trèvol, que només té tres encreuaments (el mínim possible).

El desenvolupament de la teoria de nusos al tombant dels segles XIX i XX està íntimament lligat al de la química. Les primeres idees sobre la teoria atòmica dels elements són de William Thomson, conegut més com a *Lord Kelvin*, que afirmava que els àtoms eren anells de vòrtexs en l'èter, anells que es nuaven i s'enllaçaven de diferents maneres creant els diversos elements. Intentant establir una taula periòdica dels elements, el seu deixeble Peter Tait no ho va aconseguir, però va classificar topològicament els nusos.

A partir d'aleshores i durant tot el segle XX, la teoria de nusos es desenvolupa com una branca pròpia de la topologia, estretament vinculada a l'estudi de les varietats de dimensió tres, un cop ja ben conegudes i classificades les de dimensió dos, és a dir, les superfícies. Esdevé un lligam perfecte entre la topologia, la geometria i l'àlgebra, com una eina per a atacar alguns del problemes que es resisteixen més als matemàtics, vinculats a les varietats de dimensió tres i quatre.

Però la vinculació a la química no es perdé mai del tot, una relació que s'estén també a la biologia molecular. Químics i biòlegs estan interessats en nusos i enllaços per a poder sintetitzar nous tipus de molècules amb propietats específiques, com ara que siguin suficientment grans per a perdre la rigidesa característica de les molècules petites. Així, l'any 1989 C. Dietrich-Buchecker i J.-P. Sauvage van sintetitzar, per primera vegada, un nus molecular format per cent

vint-i-quatre àtoms amb la forma del nus trèvol, un resultat que es perseguia des de feia més de trenta anys. I C. Liang i K. Mislov, els anys 1994 i 1995, van descobrir que els nusos i els enllaços apareixen, de manera natural, en les proteïnes, resultats que han portat els biòlegs moleculars a trobar ADN nuats i enllaçats a la natura i que poden ésser manipulats al laboratori.

No fou fins fa pocs anys que químics, farmacèutics i biòlegs moleculars descobrien la importància de conèixer la quiralitat de les molècules, és a dir, si la imatge especular de la molècula coincideix amb ella mateixa (aquiral), o, com si fossin dues mans, no hi coincideix (quiral). Recordem el famós cas de la talidomida, que va suavitzar el mareig de tantes embarassades als anys seixanta, però també va produir defectes horribles a molts nadons, ja que, en tractar-se d'una molècula quiral, el comportament era totalment diferent si actuava la molècula levogira o la dextrogira. La indústria farmacèutica es va revolucionar amb aquest descobriment. La quiralitat de les molècules sintetitzades a partir d'enllaços es pot determinar en termes de les propietats geomètriques i topològiques de l'enllaç, una nova aportació de la teoria de nusos a la biologia molecular.

Un bell exemple de ciència, cultura, estètica, matemàtiques i vinculació al món real.

Les matemàtiques, motor del món. Exemple 2: codificació i criptografia

Criptografia i teoria de codis són dues especialitats pròpies de la teoria de la informació i de la comunicació, una àrea de les matemàtiques desenvolupada a la segona meitat del segle passat. El naixement de la teoria de codis està íntimament lligat a les necessitats sorgides en el món digital, i la criptologia, els orígens de la qual es perden en el temps, no havia adquirit rang d'especialitat científica fins molt recentment.

En la transmissió d'informació hi ha quatre conceptes fonamentals:

— Un grau alt de fiabilitat: assegurar que el missatge no es pot alterar per error.
— Un grau alt de confidencialitat: el missatge només ha de poder ésser entès pel destinatari.
— Un grau alt d'autenticitat: evitar la suplantació de la personalitat.
— Un grau alt de no-repudiació: el remitent no ha de poder negar que l'ha enviat.

Els codis correctors d'errors

El primer concepte esmentat, la fiabilitat, forma part de la teoria de codis. S'introdueixen els anomenats *codis correctors d'errors*, desenvolupats a partir de l'any 1946 pel matemàtic

Richard W. Hamming. Un exemple senzill és el que s'utilitza en el document nacional d'identitat (DNI), introduint-hi la lletra final que defineix el número d'identificació fiscal (NIF). La lletra pertany a un alfabet reduït de vint-i-tres caràcters, i s'obté calculant la resta de dividir el número del DNI per vint-i-tres i aplicant la correspondència següent:

0 = T	4 = G	8 = P	12 = N	16 = Q	20 = C
1 = R	5 = M	9 = D	13 = J	17 = V	21 = K
2 = W	6 = Y	10 = X	14 = Z	18 = H	22 = E
3 = A	7 = F	11 = B	15 = S	19 = L	

La lletra del NIF, en ésser redundant, proporciona un símbol de control; és un codi corrector d'errors.

Alguns codis correctors d'errors més sofisticats, introduïts, entre altres, per R. Hamming, M. Golay, I. S. Reed, D. E. Muller, R. C. Bose, D. K. Ray-Chaudhuri i A. Hocquenghem, han estat utilitzats per la sonda espacial *Voyager* per a transmetre en color les fotografies de Júpiter i de Saturn, pel *Mariner 9* per a transmetre fotografies en blanc i negre des de Mart, o per l'empresa Philips en introduir el *Compact Disc Digital Audio System*. Els darrers es basen en la teoria dels cossos finits, un camp que combina l'àlgebra i la teoria de nombres.

També trobem exemples d'aplicació de la teoria dels codis correctors d'errors en la biologia. Tota la informació necessària per a la gènesi i el desenvolupament de la vida d'un organisme es troba en la seqüència de bases de les llargues cadenes de l'ADN, codificades segons els quatre àcids nucleics: A = adenina, T = timina, C = citosina i G = guanina. Un text format per paraules amb aquestes quatre lletres constitueix la informació genètica de cada organisme viu. L'existència del codi genètic, conjecturada l'any 1944 pel físic austríac Erwin Schrödinger, fou demostrada l'any 1953 per James Watson i Francis Crick.

En el procés complex de duplicació de l'ADN, hi té un paper essencial l'enzim ADN-polimerasa, l'activitat del qual és interpretada com un mecanisme de correcció d'errors, que encara comet un error d'aparellament de les bases d'un u per deu milions de bases. Entra, aleshores, en acció una maquinària enzimàtica que corregeix els errors comesos i dóna la increïble fiabilitat d'u per cada deu mil milions de bases.

Criptologia = criptografia + criptoanàlisi

La criptografia és la ciència que s'encarrega del disseny d'escriptures secretes, mentre que la criptoanàlisi és la ciència que estudia els procediments per a descobrir els secrets d'aquests sistemes d'escriptura. L'una la desenvolupa el «missatger», l'altra, l'«espia». La criptologia, que neix com a ciència a mitjan segle XX, engloba ambdues disciplines.

La *taula d'Esagil*, del segle VIII aC, utilitzada en l'endevinació, és probablement el primer document encriptat de què disposem, però, fins a èpoques relativament recents, l'ús de la criptografia es reduïa a l'àmbit militar i a l'espionatge. Ara bé, sempre que algú ha encriptat, d'altres s'han dedicat a desencriptar.

No falten a la història exemples prou curiosos, com el fet que la decapitació de Maria I d'Escòcia fou, en bona part, deguda al fet que un lingüista va descobrir el contingut dels textos xifrats que enviaven uns conspiradors catòlics. O que l'endemà de l'estrena d'una òpera de Verdi, els carrers eren plens de pintades que deien «Viva Verdi»; aquí s'utilitzava *Verdi* com acrònim de Vittorio Emanuele, Re D'Italia (el candidat a ocupar el tron a la futura monarquia italiana). O que l'any 1917 els serveis d'intel·ligència britànics van desxifrar el telegrama Zimmermann, enviat des d'Alemanya al seu ambaixador a Mèxic, en el qual es negociava l'entrada de Mèxic a la guerra, a favor dels alemanys, a canvi dels estats nord-americans de Texas, Nou Mèxic i Arizona. Això va propiciar l'entrada a la guerra dels EUA i la derrota d'Alemanya.

Però, des de fa uns quaranta anys els missatges codificats s'han estès a tots els àmbits de la vida. L'any 1970, en un dels darrers discos de The Beatles, *Sgt. Pepper's Lonely Hearts Club Band*, s'hi incloïa la cançó *Lucy in the Sky with Diamonds*, una apologia de la droga al·lucinògena LSD («Cellophane flowers of yellow and green towering over your head […]. Everyone smiles as you drift past the flowers that grow so incredibly high […]»). Els missatges SMS, la televisió digital o Internet són tres casos de comunicació entre individus o entre empreses i individus en els quals hi ha una «central» operadora. El missatge (enviat per una persona o per una televisió) es codifica (amb 0 i 1), passa per la «central» (que coneix el codi de l'emissor), el descodifica i el torna a codificar amb el codi del receptor. Els missatges han d'ésser prou distorsionats perquè no puguin ésser entesos per cap persona no autoritzada.

La confidencialitat és fonamental en el procés d'encriptació. Suposem que els alumnes d'una classe de tercer curs d'ESO volen comunicar als companys de classe el missatge següent sense que el professor se n'assabenti: «Demà farem campana i anirem a esquiar.» Inventen aleshores un «llenguatge» secret:

— La primera lletra (*d*) la canvien per la lletra de l'alfabet que és cinc llocs més endavant (*i*).
— La segona lletra (*e*) la canvien per la lletra de l'alfabet que és set llocs més endavant (*l*).
— La tercera lletra la canvien, un altre cop, per la que és cinc llocs més endavant, la quarta lletra per la que és set llocs més endavant, etc.

El missatge que enviaran serà: «ilrh khwlr jftwhsh n hspwlr h jzvbnhw, 35». Només qui conegui el significat de 35 (= 5 × 7) podrà desxifrar el missatge. Amb el 5 i el 7 és possible que algú (el professor de matemàtiques?), amb poc temps, desxifrés el missatge

i, de ben segur, que es quedarien sense anar a esquiar, però si en comptes d'haver fet servir el 5 i 7, que multiplicats donen 35, haguessin utilitzat el 102.197 i el 104.729, també primers, que multiplicats donen 10.702.989.613, el professor, amb l'ajut dels ordinadors actuals, hauria trigat dos dies a desxifrar la clau, i els alumnes ja haurien tornat d'esquiar. Aquesta segona clau donava un grau molt més elevat de confidencialitat que la primera.

Alguns mètodes clàssics per a encriptar

— *Per permutació*: permutant les lletres del text.

Text clar: QUEDEM A LA CABANA DEL LLAC A MITJANIT
Q E E A A A A A E L A A I J N T
U D M L C B N D L L C M T A I
Text xifrat: QEEAAAAAWLAAIJNTUDMLCBNDLLCMTAI

— *Per substitució*: substituint unes lletres per unes altres (com en el missatge per a anar a esquiar). Ja utilitzat per Juli Cèsar. És una funció del tipus $f(x) = x + n$. En el cas del missatge per a anar a esquiar era $f(x) = x + 5$, si x ocupa un lloc senar, i $f(x) = x + 7$, si x ocupa un lloc parell.

— *Per blocs*: dividint el text en blocs de n lletres (per exemple, 5), reordenant els nombres de l'1 al n (per exemple, 3, 1, 5, 2, 4) i permutant les lletres de cada bloc.

Text clar: QUEDEM A LA CABANA DEL LLAC A MITJANIT
QUEDE MALAC ABANA DELLL ACAMI TJANI T
UQEUD LMCAA AAABN LDLEL AAICM ATIJN T
Text xifrat: UQEUDLMCAAAAABNLDLELAAICMATIJNT

— *Per caixes*: una barreja del mètode per blocs i els altres. Utilitzat per l'Exèrcit espanyol fins a la dècada dels setanta. Com a anècdota curiosa, és bo saber que al segle XVI els governs europeus reclutaven matemàtics per desxifrar els missatges dels seus enemics. França havia contractat François Viète, que desxifrava tots els missatges enviats per Espanya. Felip II va voler que el papa Gregori XIII el jutgés per «activitats satàniques», però resultava que el Vaticà també interceptava els missatges dels espanyols!

— *Un codi molt modern: el codi ASCII*. És el que fan servir tots els ordinadors: 256 codis de 8 xifres (només 0 i 1), que codifiquen tots els caràcters possibles (majúscules, minúscules, punts, interrogants, lletres amb accents, espais en blanc, etc.). Cada ordinador codifica, primer, i descodifica, després. És utilitzat, doncs, per les màquines per a connectar el seu interior amb els perifèrics.

Exemples d'eines elementals de criptoanàlisi

La criptoanàlisi és, com hem dit, la part de la criptologia que s'encarrega de desenvolupar mètodes per a desxifrar els missatges encriptats. Clàssicament l'estructura de la llengua en què se suposava xifrat el missatge hi ha tingut un rol important. Vegem-ho.

— *La freqüència d'ús de les lletres*: en un text en català, la *e* surt estadísticament un 13,89 % de vegades; la *a*, un 12,55 %; la *s*, un 8,43 %; la *r*, un 7,74 %, etc. Es pot estudiar amb quina freqüència surten les diferents lletres en un text encriptat. Si una lletra surt més d'un 10 % de vegades, probablement representarà, en el text original, la *e* o la *a*, etc.

— *Les característiques de la llengua*: en català, la *q* sempre va seguida d'una *u* o d'una *ü*. Si en el text encriptat hi ha dos signes que apareixen seguits amb molta freqüència, representaran una *q* i una *u* (o una *ü*), molt probablement.

La criptologia moderna

La matematització de la criptologia és el fet fonamental que li permet ésser considerada una disciplina científica. Aquest canvi s'inicia amb els treballs de Claude E. Shannon de l'any 1948, i el gran avenç que s'ha produït en la criptologia en les darreres dècades es deu essencialment a l'existència d'ordinadors amb una potència de càlcul cada cop més gran i a la generalització de les comunicacions i altres transaccions telemàtiques que han fet necessari l'ús de la criptografia per a un nombre cada cop més gran d'usuaris.

La teoria desenvolupada per Shannon, dita *de la màquina del secret perfecte* (encara que no és realment perfecta), es basa en funcions del tipus $f(x) = ax + b \pmod{n}$; és a dir, utilitza l'aritmètica modular. Es basa en la idea de la seguretat limitada: tot missatge s'acabarà desxifrant, però cal que l'«espia» trigui prou temps fins que el missatge ja no tingui interès. Els mètodes utilitzats en aquest procés es basaven en la descomposició factorial de *n*; si *n* és prou gran, el temps necessari per al càlcul d'aquesta factorització serà molt gran i, quan s'hagi desencriptat el missatge, ja serà massa tard. És a partir d'aquí que la teoria de nombres esdevé, a la dècada dels setanta, la disciplina algebraica clau per a la criptologia. Però, de mica en mica, àrees de les matemàtiques que clàssicament es consideraven poc aplicables són utilitzades com una peça clau en avenços tecnològics importants: la teoria de cossos, la teoria de grafs, la combinatòria, les geometries finites, la geometria algebraica, el tractament d'imatges, les corbes el·líptiques o, més recentment, la teoria de grups.

El panorama de la criptologia va canviar radicalment a partir de l'any 1976, quan Whitfield Diffie i Martin E. Hellman van inventar els sistemes criptogràfics de clau pública, en què la clau consta ara de dues parts: la direcció del receptor del missatge, que és pú-

blica, i una part privada, que només coneix ell. Els criptosistemes de clau pública permeten transmetre missatges de manera confidencial, autentificar-los (signatures digitals), intercanviar claus, compartir secrets. S'utilitzen funcions que són calculables de manera eficient, però no ho són les seves inverses, ja que no es coneixen algorismes eficients (és a dir, en un temps polinomial en el nombre de bits de l'*input*) per a calcular-les.

La criptografia de clau pública i els esquemes per a compartir secrets són els dos components per a avançar en l'elaboració de protocols criptogràfics distribuïts, com són els casos de la televisió de pagament, l'ús de les targetes de crèdit o les votacions electròniques. La potència matemàtica necessària per a desenvolupar aquests protocols és impressionant, i aquí és on entren en joc els avenços més recents en algunes àrees que abans he esmentat.

El rol de l'Institut d'Estudis Catalans en aquests avenços (i en d'altres)

Quan l'Institut d'Estudis Catalans creà la Secció de Ciències, l'any 1911, l'objectiu fonamental era dotar el nostre país d'un entorn científic comparable al que en aquells moments s'estava establint a Europa: França, Alemanya, Itàlia i la Gran Bretanya, essencialment. Sense menystenir el gran rol dut a terme per al desenvolupament de la geologia, la botànica, la biologia o la medicina, em limitaré a parlar de les matemàtiques.

Ben aviat es deixaren veure les iniciatives capdavanteres d'alguns dels membres científics de l'Institut, que, en el camp de les matemàtiques, durant els anys vint del segle passat, liderà Esteve Terradas, en particular amb la col·lecció «Cursos de Física i Matemàtica», que permeté que els nostres científics tinguessin contacte i aprenguessin de personalitats com Jacques Hadamard, Francesco Severi, Tullio Levi-Civita, Hermann Weyl o el mateix Albert Einstein. Només les dues dictadures que havíem de patir pogueren estroncar aquesta prometedora renaixença.

L'any 1932 l'Institut creà la Societat Catalana de Ciències Físiques, Químiques i Matemàtiques, a partir de la qual, en subdividir-se en especialitats, sorgí la Societat Catalana de Matemàtiques (SCM) l'any 1986. És obligat parlar de tres períodes d'aquesta societat:

— 1978-1982. La societat passa de 16 a 400 associats, estableix convenis de reciprocitat amb quatre societats: l'americana, l'alemanya, la suïssa i l'espanyola, inicia la publicació d'un butlletí i organitza dos congressos d'alt contingut: les VI Jornades Matemàtiques Hispano-Lusitanes i *L'ensenyament de les matemàtiques i la formació del professorat*.

— 1995-2002. La societat passa de 400 a 900 associats, s'inicien les proves Cangur per als alumnes d'ensenyament secundari, s'intensifica la presència internacional amb membres de la SCM en el Consell Executiu de la Societat Matemàtica Europea i s'organitza el 3r Congrés Europeu de Matemàtiques.

— 2002-2006. El Cangur s'estén a totes les terres de parla catalana, amb divuit mil participants de 500 centres escolars; s'inicia ESTALMAT, un programa per a detectar i estimular el talent matemàtic; es digitalitza el *Butlletí*, i s'aprofundeix en la presència internacional de la societat.

Però, deixem el passat, i per a enfocar i analitzar el present, i sobretot el futur, permetin-me que citi unes frases de Josep Faulí arran d'unes disputades eleccions presidencials a l'Institut. Deia Faulí: «Les velles fórmules no serveixen, la lleialtat profunda de l'IEC no pot ésser la de fer el que feia el 1907, sinó d'aplicar els designis fundacionals a la realitat d'un segle després. Per a fer-ho, cal pensar menys en mèrits que en serveis i, sobretot, molt menys en la història que en l'actualitat i el futur.» Aquesta idea, junt amb la de Michel Foucault a *Les mots et les choses*, quan afirma que «és sempre sobre un fons de coses ja enceta des que l'home ha de pensar allò que per a ell vol com a punt de partida», facilitaren que l'any 1984 l'IEC creés el Centre de Recerca Matemàtica (CRM), un institut de recerca concebut per a la millora qualitativa i quantitativa de la recerca matemàtica al nostre país.

Es reprenia així la idea d'Esteve Terradas, però amb una concepció moderna, actual, que ja havia començat a donar fruits en uns pocs països d'aquests que nosaltres prenem sempre com a imatge. I novament prenien valor els designis fundacionals d'Enric Prat de la Riba en crear l'Institut, ara fa exactament cent anys, els criteris d'«exigència científica, catalanitat i obertura a l'exterior».

Durant aquests pocs més de vint anys d'existència del CRM, hi han treballat més de mil cent investigadors de seixanta països d'arreu, han rebut formació postdoctoral setanta-sis joves investigadors de vint-i-sis països, han estat organitzats un centenar de congressos, tallers i cursos avançats d'àmbit internacional, i l'editorial suïssa Birkhäuser Verlag ha posat al mercat la sèrie «Advanced Courses in Mathematics CRM Barcelona», de la qual ja s'han publicat onze volums. Totes aquestes activitats han estat promogudes i coordinades per matemàtics de les universitats catalanes.

Si les matemàtiques són un dels motors del món, podem dir que el CRM ha estat un dels motors de les matemàtiques a Catalunya, amb iniciatives innovadores que només una estructura àgil i flexible pot dur a terme. Aquesta estructura li ha permès situar-se com un dels centres més prestigiosos d'Europa, l'únic de l'Estat espanyol, que coordina actualment el projecte europeu Shaping New Directions in Mathematics for Science and Society (MATHFSS), una acció coordinadora del programa New and Emerging Science and Technology, en el qual participen tres instituts europeus de prestigi més.

MATHFSS és una acció impulsora de recerca matemàtica en àrees innovadores, amb aplicabilitat a quatre àmbits ben diferenciats: la biologia de sistemes, l'estimació de risc, la neurociència i la seguretat de continguts digitals, dos dels quals estan ben vinculats als dos casos triats en aquest article per a exemplificar el rol de les matemàtiques en el món.

Reprenent Prat de la Riba, l'«excel·lència científica» ha estat un dels *leimotiv* del CRM, que li ha permès enriquir la capacitat investigadora dels nostres matemàtics, «la catalanitat» ha estimulat i facilitat la plena integració d'investigadors forans al nostre país i la presència de matemàtics catalans arreu, i l'«obertura científica» ens ha permès ésser membres de prestigioses institucions internacionals com ERCOM (European Research Centres on Mathematics) o el selectiu EPDI (European Post-Doctoral Institute for Mathematical Sciences).

És cert que des de sempre hi ha hagut en algunes àrees de la ciència investigadors catalans coneguts internacionalment, i que en els darrers anys aquest reconeixement s'ha estès a moltes altres disciplines en les quals no teníem presència, com és el cas de les matemàtiques. Però una cosa és que individualment ja siguem coneguts i reconeguts i una altra de ben diferent és que ho sigui el país com a tal. Sense la primera no podríem aconseguir la segona, però aquest segon ha d'ésser un objectiu irrenunciable. L'Institut d'Estudis Catalans, en el camp de les matemàtiques, ha contribuït a fer que això sigui possible, mitjançant el CRM, que l'any 2002 es constituí en un consorci entre la Generalitat de Catalunya i l'IEC, amb personalitat jurídica pròpia, i al qual li fou atorgada la Placa Narcís Monturiol al mèrit científic i tecnològic.

Bibliografia

BAYER, Pilar; CASTELLET, Manuel. «Los números: de la simbología a la aplicabilidad». A: *La ciencia en tus manos*. Madrid: Espasa, 2000.

CASTELLET, Manuel. *Opening Ceremony of the Third European Congress of Mathematics*. Barcelona: Institut d'Estudis Catalans, 2000.

JUHER, David. *L'art de la comunicació secreta*. Barcelona: Llibres de l'Índex, 2004. (Descoberta; 35)

MORILLO, Paz. «Protocols criptogràfics distribuïts, esquemes per a compartir secrets». A: *Les bases matemàtiques de la civilització tecnològica*. Sabadell: Fundació Caixa de Sabadell, 1999. (Aula de Ciència i Cultura; 10)