Butlletí de la Societat Catalana de Matemàtiques
Vol. 20, núm. 2, 2005. Pàg. 75–89

Els nombres primers poden tenir més protagonisme a secundària?

Grant Cairns*

Resum Traducció de l'article original «Is there a greater role for prime numbers in our schools?», de Grant Cairns, publicat a la revista *Australian Senior Mathematics Journal*, 19 (2005), 24-37. Està basat en una conferència pronunciada pel mateix autor el 4 de desembre de 2003 a la Mathematics Association of Victoria. L'autor opina que cal una certa maduresa matemàtica, poc freqüent en alumnes de secundària, per manipular amb naturalitat el concepte de *congruència*. Per tant, proposa tot un seguit de materials de teoria de nombres elemental, relacionats essencialment amb els nombres primers, que es poden abordar sense utilitzar l'aritmètica modular. La inclusió de part d'aquest material als temaris de secundària reportaria grans beneficis a la formació matemàtica dels estudiants preuniversitaris.

Paraules clau: nombres primers, ensenyament secundari, plans d'estudi.

Classificació MSC2000: 11A41, 97B10.

Els nombres primers tenen un paper extremadament important dins la matemàtica moderna. A banda de ser objecte d'una intensa tasca de recerca, les seves aplicacions en banca electrònica i seguretat posen de manifest un fenomen interessant: al món contemporani, les aplicacions de la matemàtica sovint sorgeixen de teories «purament» abstractes.

Curiosament, i malgrat la seva innegable importància, els nombres primers gairebé no apareixen a l'ensenyament secundari. Típicament, al setè any[1] s'in-

* Traducció de David Juher, Departament d'Informàtica i Matemàtica Aplicada, Universitat de Girona. Agraïm a l'autor i a la Australian Association of Mathematics Teachers, editora del *Australian Senior Mathematics Journal*, l'amable autorització per publicar aquesta traducció.

1 N. del t.: El setè any de les *high schools* australianes correspon al nostre primer d'ESO. Al sistema australià es numeren els sis anys d'ensenyament secundari de 7 a 12, en correspondència exacta amb els nostres quatre anys d'ESO més dos de batxillerat. La situació pel que fa als nombres primers també és la mateixa: apareixen només a primer d'ESO quan es parla de divisibilitat i del màxim comú divisor.

trodueix el garbell d'Eratòstenes, que els alumnes utilitzen per trobar tots els primers fins a un cert límit, diguem 100. També és freqüent explorar la conjectura de Goldbach: tot nombre parell diferent de 2 és suma de dos primers. Als alumnes se'ls pot demanar, per exemple, que calculin parelles de primers que sumin menys de 76. Desgraciadament, sovint aquest és tot el material sobre nombres primers que aprenen els estudiants de secundària.

A l'extrem oposat, hi ha una gran quantitat de literatura sobre primers, i teoria de nombres en general, a un nivell universitari introductori. Hi ha llibres excel·lents amb títols engrescadors com *My numbers, my friends* ([31]) i *A friendly introduction to Number Theory* ([37]). En particular, Dover edita molt bons llibres de teoria de nombres a un preu raonable. De tota manera, pocs d'aquests llibres escauen a l'ensenyament secundari: hi ha un abisme entre el setè any i la universitat, amb pocs textos apropiats i poques referències als nombres primers dins els plans d'estudi. Per què això és així, i com es pot introduir més material sobre nombres primers als temaris de secundària?

Opino que el problema fonamental que presenta el material escolar disponible sobre teoria de nombres és l'ús de l'*aritmètica modular*, o *aritmètica del rellotge*. En un rellotge d'agulles, les vuit en punt més sis hores són les dues en punt. En símbols, $8 + 6 \equiv 2 \pmod{12}$. En un context més general, per exemple en un rellotge basat en el nombre 9 en lloc del 12, tenim $8 + 6 \equiv 5 \pmod{9}$. Similarment, s'obtenen afirmacions com $8 \times 6 \equiv 9 \pmod{13}$. L'aritmètica modular és el punt de partida habitual en molts llibres d'introducció a la teoria de nombres i, tot i que no és fora de l'abast de molts estudiants de secundària, sí que requereix una certa maduresa matemàtica; sens dubte, fer-la servir a secundària per demostrar fets sobre nombres primers seria tot un repte.

L'objectiu d'aquest article és presentar diverses qüestions rellevants i idees elementals sobre teoria de nombres, i sobre nombres primers en particular, que es poden explorar sense aritmètica modular. De cap manera no és un recull de teoria de nombres moderna, sinó que pretén fer una selecció d'idees, algunes de clàssiques, altres de modernes, que es poden analitzar i entendre sense usar l'aritmètica modular. Crec que aquest material podria introduir-se als temaris de secundària i oferir als nombres primers un protagonisme més gran dins les matemàtiques a l'escola.

1 Hi ha infinits primers

Una bona introducció recent als nombres primers es por trobar a [29]. Recordem que un nombre primer és un enter $p \geq 2$ que té com a únics divisors positius 1 i ell mateix. Sigui p_i l'i-èsim primer, de manera que $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Un avenç conceptual significatiu, que es remunta a l'antiguitat, prové del fet d'entendre per què hi ha infinits primers; això és, per què la llista de primers continua indefinidament o, expressat encara d'una altra manera, per què no hi ha un darrer primer més enllà del qual no n'hi ha més.

Hi ha moltes maneres de demostrar aquest fet. La prova clàssica dels «Elements» d'Euclides utilitza el que avui anomenem *nombres primerials*. El nom-

bre primerial associat a un primer p es defineix com el producte de tots els primers menors o iguals que p. Així doncs, si p_k denota el k-èsim primer, el k-èsim primerial P_k ve donat per $P_k = p_1 p_2 \cdots p_k$. Per exemple,[2]

$$\begin{aligned} P_1 &= 2 \\ P_2 &= 2 \cdot 3 = 6 \\ P_3 &= 2 \cdot 3 \cdot 5 = 30 \\ P_4 &= 2 \cdot 3 \cdot 5 \cdot 7 = 210 \\ P_5 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 \\ P_6 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030. \end{aligned}$$

Suposeu que hi ha un darrer nombre primer, p_k. Llavors, P_k és el producte de tots els primers. Considereu $P_k + 1$. Com que tot natural més gran que 1 és divisible per algun primer, $P_k + 1$ és divisible per algun primer p_i. Per tant, $1 = (P_k + 1) - P_k$ és també divisible per p_i. Però això és impossible! Així doncs, l'afirmació que hi ha un darrer nombre primer ha de ser falsa. I, en conseqüència, hi ha infinits nombres primers.

Un aspecte remarcable d'aquesta demostració és l'ús que fa de l'«argument per contradicció». La prova comença suposant que hi ha un darrer primer. Això és, es comença admetent el contrari d'allò que es pretén demostrar. I s'obté una contradicció amb la impossibilitat que 1 sigui divisible per un primer. La conclusió és clara: la suposició inicial ha de ser falsa. La gent sol tenir una idea intuïtiva clara de l'argument per contradicció i l'utilitza quotidianament. Malgrat tot, fins i tot a la universitat, molts estudiants tenen problemes a l'hora de comprendre l'argument i, en particular, a l'hora d'escriure'l coherentment. Crec que aquesta prova clàssica n'és un exemple excel·lent, i que pot ajudar a aprendre a raonar per contradicció.

Un segon aspecte de la demostració és subtil i sol ser malinterpretat. Té a veure amb allò que la demostració no prova: que $P_k + 1$ és primer per a tot k. De fet, per a $k = 1, 2, 3, 4, 5$ els nombres $P_k + 1$ són 3, 7, 31, 211, 2311, que són primers, però $P_6 + 1 = 30.031$ no és primer: $30.031 = 59 \times 509$. Els primers de la forma $P_k + 1$ (o $P_k - 1$) s'anomenen *primers primerials*. No sabem si n'hi ha infinits, però s'ha conjecturat que sí ([7]).

1 CONJECTURA *Hi ha infinits primers primerials.*

Els nombres primers són una font generosa de preguntes fàcilment formulables, com la conjectura prèvia. És instructiu per als alumnes adonar-se que les matemàtiques s'estan desenvolupant contínuament i que hi ha molts problemes oberts que són objecte de recerca activa.

2 El terme *primerial* és una adaptació de *factorial*, que és un producte de nombres naturals, però també s'assembla a *primordial*, i de fet els nombres primerials són certament primordials des del punt de vista de la teoria de nombres.

2 Hi ha infinits primers, i són bastant freqüents

L'abundància de primers és un tema recurrent en teoria de nombres. No només hi ha infinits primers, sinó que n'hi ha infinits de molts diferents tipus. El més antic i famós resultat d'aquesta mena és el teorema de Dirichlet.

2 Teorema (Teorema de Dirichlet) *Si a i b són primers entre ells, llavors la progressió aritmètica a, $a+b$, $a+2b$, $a+3b,\ldots$ conté infinits primers.*

Per entendre l'enunciat del teorema de Dirichlet, recordem que, si a i b són dos enters, el *màxim comú divisor* d'a i b, denotat per $\mathrm{mcd}(a,b)$, és el més gran enter que divideix a i b alhora. El mcd es pot calcular amb l'*algorisme d'Euclides*, que fàcilment es pot executar en un full de càlcul o una calculadora: començant amb a i b, canviem el menor dels dos per la diferència entre els dos. Repetim aquest procediment fins que finalment un dels dos nombres és 0; l'altre nombre és precisament el mcd. Els càlculs de la taula següent mostren que $\mathrm{mcd}(1344,1162)=14$ (experimentant amb un full de càlcul sorgeix ràpidament la pregunta: com es pot modificar l'algorisme perquè produeixi el resultat amb menys iteracions?).

1344	182	182	182	182	182	182	182	112	42	42	14	14	0
1162	1162	980	798	616	434	252	70	70	70	28	28	14	14

Es diu que dos enters a i b són *primers entre ells* si el seu mcd és 1. En altres paraules, a i b no tenen factors en comú. Per exemple, 3 i 10 són primers entre ells. En aquest cas, el teorema de Dirichlet diu que hi ha infinits primers en la seqüència 3, 13, 23, 33, 43, ...

A més de resultats com el de Dirichlet, que dóna fe de l'abundància de primers, hi ha una superabundància de problemes oberts i conjectures que provenen de la convicció general que hi ha tants nombres primers que qualsevol cosa és possible. Dos dels més famosos són:

3 Conjectura (Conjectura dels primers bessons) *Hi ha infinits primers bessons.*

Una parella de primers *bessons* té, per definició, la forma $p, p+2$, com 5, 7 o 29, 31 o 347, 349 o 265237079981, 265237079983.

4 Conjectura (Conjectura de Goldbach) *Tot nombre parell és suma de dos primers.*

La conjectura de Goldbach s'ha verificat fins a 10^7 (vegeu [17]). Com a publicitat per a l'edició anglesa de la divertida novel·la de Doxiadis [14], es va oferir un premi temporal d'un milió de dòlars americans a la solució de la conjectura. Per a un recull d'articles clàssics sobre la conjectura de Goldbach, vegeu [39].

3 Hi ha infinits primers, però són poc densos

Hi ha famílies infinites que tenen més presència que altres. Per exemple, la família dels quadrats 1, 4, 9, 16, 25, 36, 49, ... és infinita, però el forat entre membres consecutius esdevé arbitràriament gran. En comparació, la família dels senars 1, 3, 5, 7, 9, ... no té més membres que la dels quadrats, però el forat entre membres consecutius és constant, 2.

La família dels nombres primers presenta forats arbitràriament grans. Considereu el k-èsim primerial P_k. El nombre $P_k + 1$ pot ser o no primer, com ja hem dit. En qualsevol cas, preneu els següents $p_{k+1} - 2$ enters:

$$P_k + 2, P_k + 3, P_k + 4, \ldots, P_k + p_{k+1} - 1.$$

Cap d'aquests nombres no és primer. En efecte, per a $2 \leq i \leq p_{k+1} - 1$ el nombre i és divisible per algun primer $p \leq p_k$, mentre que P_k és divisible per p, de manera que $P_k + i$ és divisible per p. Per tant, cap dels nombres $P_k + i$ no és primer per a $2 \leq i \leq p_{k+1} - 1$. Com que p_{k+1} esdevé arbitràriament gran amb k, això mostra que hi ha forats arbitràriament grans entre primers consecutius.

Per a un nombre primer p, la distància fins al següent primer s'anomena el *forat primer* i és denotat amb $g(p)$; això és, $g(p) = p_{k+1} - p_k$. Hi ha una gran quantitat de recerca sobre forats primers —com $g(p)$ creix amb p, quins nombres són forats primers, i amb quina freqüència apareixen— però encara hi ha moltes preguntes sense resposta. No se sap si tot nombre parell és un forat primer, ni tan sols si tot nombre parell es pot escriure com a diferència de dos primers (no necessàriament consecutius). Això és:

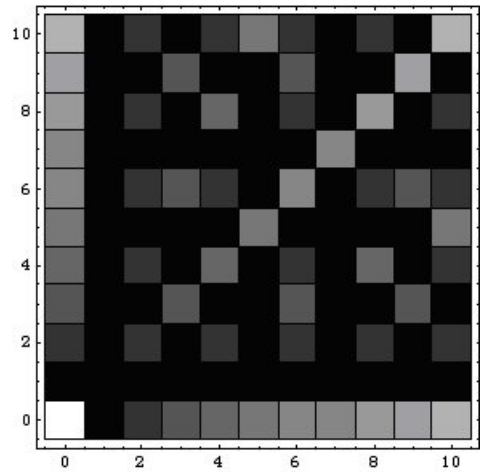

FIGURA 1

5 CONJECTURA (CONJECTURA DE POLIGNAC) *Tot nombre parell es pot escriure com a diferència de dos primers.*

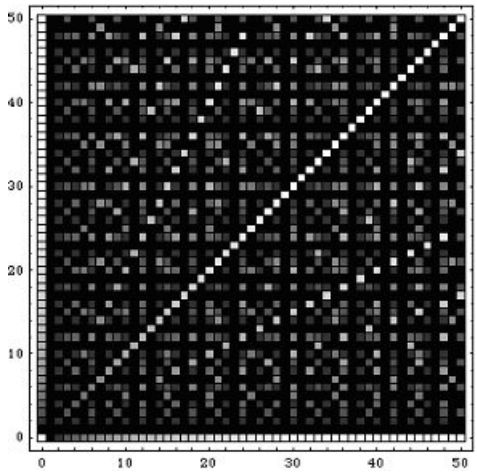

FIGURA 2

Observeu la similitud entre les conjectures de Goldbach i de Polignac. De fet, Polignac també va conjecturar que tot nombre parell es pot escriure d'infinites maneres com a diferència de dos primers. En particular, si això fos cert per al nombre 2 llavors la conjectura dels primers bessons seria certa.

És difícil visualitzar els nombres primers a la recta real, però la situació s'aclareix al pla euclidià. Considereu la graella definida pels enters, i ennegriu el quadrat unitari centrat al punt de coordenades enteres (x, y) amb un to que depengui de $\text{mcd}(x, y)$. La figura 1 mostra el dibuix per als nombres (x, y) amb x i y entre 0 i 10. Els quadrats amb $\text{mcd}(x, y) = 1$ són completament negres, mentre que els quadrats amb un mcd més alt són grisos, amb gradació progressiva cap al blanc com més gran és el mcd. A aquesta escala no s'aprecia gaire res d'interessant. Hi ha una línia negra vertical a $x = 1$: això és perquè $\text{mcd}(1, y) = 1$ per a tot y. Similarment, hi ha una línia negra horitzontal a $y = 1$. En efecte, la figura és simètrica respecte de la recta $y = x$.

La figura 2 correspon a valors de x i y entre 0 i 50. S'hi aprecien diversos patrons. Per a cada primer p la recta vertical $x = p$ és negra, excepte per a uns quants quadrats; això és perquè $\text{mcd}(p, y) = 1$ excepte quan y és múltiple de p. Per tant, a la figura 2 s'hi aprecien diverses línies verticals i horitzontals gairebé totalment negres. Observeu les dues línies negres verticals a $x = 29$ i $x = 31$. Corresponen a la parella 29,31 de primers bessons. Totes les parelles de primers bessons apareixen com a parells de línies negres verticals separades dues unitats. La parella corresponent als bessons 41 i 43 també és visible a la figura 2. D'altra banda, hi ha diverses línies negres a 45 graus dels eixos, sobre rectes de la forma $y + x = n$. Una d'aquestes és la recta $y + x = 37$. En efecte, si $y + x$ és un primer p, llavors $\text{mcd}(x, y) = 1$ excepte quan x i y són alhora múltiples de p. La conjectura de Goldbach diu que per a cada nombre parell n la recta $y + x = n$ conté un punt (x, y) tal que x i y són

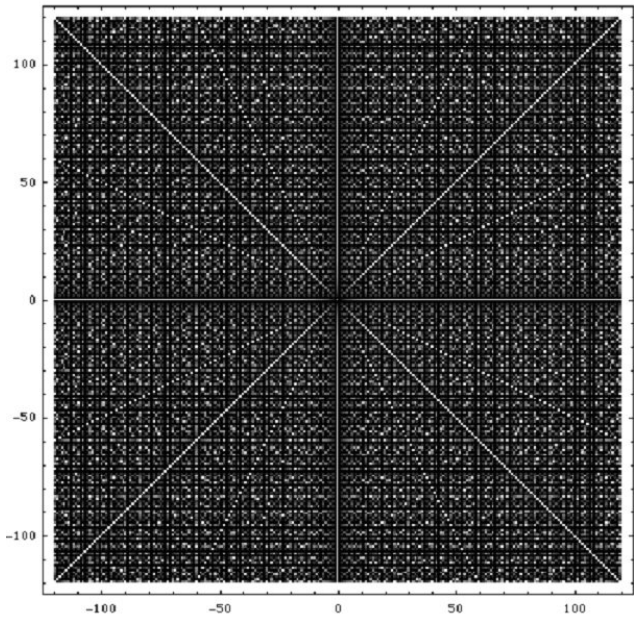

FIGURA 3

primers. Tot i que és difícil d'observar a la figura 2, hi ha també diverses línies negres de la forma $y - x = n$. Una d'aquestes és $y - x = 17$. La conjectura de Polignac diu que per a cada nombre parell n la recta $y - x = n$ conté un punt (x, y) tal que x i y són primers. La figura 3 conté el dibuix de la graella per a $|x|, |y| < 120$. A aquesta escala es fa difícil llegir els eixos, però suggereixo al lector que simplement contempli la figura a una certa distància i que admiri tota la bellesa dels nombres enters.

4 No sabem res

Tenint en compte el nombre de conjectures obertes que acabem de discutir, es podria creure que encara hi ha molt per descobrir sobre els nombres primers (i sobre les matemàtiques en general). De fet, ni tan sols no hem començat a gratar la superfície. Hi ha tants problemes oberts, fins i tot restringint-nos als nombres primers, que intentar aplegar-los tots esdevé una tasca descoratjadora. El problema més famós sobre nombres primers (i potser el més extraordinari problema obert en matemàtiques) és l'anomenada *hipòtesi de Riemann*. Es tracta d'un dels «problemes del mil·lenni», per a la solució dels quals s'ha ofert un premi d'un milió de dòlars americans. Hi ha un excel·lent recull sobre la hipòtesi de Riemann a [12], i també tres llibres recents i populars sobre el tema: [13], [15] i [35]. Abans de llegir-los, feu una ullada a les corresponents recensions de la Mathematical Association of America [24].

Per fer-vos una idea de la qualitat dels problemes oberts i les conjectures no resoltes (i del poc que realment sabem), considereu la conjectura dels primers bessons: hi ha infinits parells de primers de la forma $p, p+2$. També s'ha conjecturat que hi ha infinits triplets de primers de la forma $p, p+2, p+6$, i infinits quartets de primers de la forma $p, p+2, p+6, p+8$, i així successivament[3] (s'han trobat seqüències de fins a 18 primers, vegeu [20]). S'ha conjecturat que per a cada natural k hi ha infinits parells de primers de la forma $p, p+k$ (això és tan sols una reformulació de la conjectura de Polignac).

De fet, també s'ha conjecturat que, per a cada n, hi ha n primers consecutius en progressió aritmètica. Fins al moment en què s'ha redactat aquest text, la cadena més llarga que s'ha trobat amb aquesta propietat conté 10 primers (vegeu [9]). Ben Green i el matemàtic australià Terence Tao han fet un avenç significatiu en aquest sentit en demostrar que hi ha successions aritmètiques arbitràriament llargues de primers (no necessàriament consecutius): vegeu [28].

Ja hem dit que els nombres $P_k + 1$ a vegades són primers. Quan no ho són, preneu el menor natural d tal que $P_k + d$ és primer. Reo Fortune ha conjecturat que aquests nombres d són primers: s'anomenen *nombres afortunats* ([23]). Fortune va ser un antropòleg ben conegut; a [3] trobareu detalls divertits de la seva biografia.

Naturalment, és fàcil plantejar preguntes que no tenen resposta. A propòsit de la conjectura que hi ha infinits primers primerials, es diu que Pólya va comentar «hi ha moltes qüestions que els bojos poden plantejar i que els savis no saben respondre» ([19]). Algunes d'aquestes conjectures es basen en ben poques evidències. Per exemple, si considereu els forats entre primers consecutius, per a nombres petits trobareu que el forat més comú és 2. Per a nombres una mica més grans, els forats més comuns són 2 i 4, fins que arribeu al nombre 563, a partir del qual, i per a la majoria de nombres primers que se saben calcular a hores d'ara, el forat més freqüent (batejat per John H. Conway com *el campió de salt*) és 6. De tota manera, es creu que per a nombres molt grans (al voltant de 10^{35}?) el campió de salt és 30, i que més endavant torna a canviar (al voltant de 10^{425}?) i es transforma en 210... I que, de fet, a banda del nombre 4, en realitat els campions de salt són els nombres primerials 2, 6, 30, 210, 2310, etc.! (vegeu [27]).

5 Ho sabem tot

Sovint es diu que els nombres primers estan immersos en una boira de misteri que la humanitat no aconseguirà dissipar mai del tot. I molt sovint s'afirma que «no hi ha cap fórmula per al primer n-èsim, ni cap fòrmula recursiva que ens permeti trobar el primer $(n+1)$-èsim a partir dels n anteriors». Per això mateix, pot ser tota una sorpresa per a alguns lectors descobrir que, en rea-

3 És una pèrdua de temps buscar triplets de la forma $p, p+2, p+4$ perquè aquests triplets sempre contenen un múltiple de 3.

litat, es coneixen moltes fórmules per calcular el primer n-èsim; vegeu [16]. Potser la més sorprenent, per la seva simplicitat, és la de 1971 de J. M. Gandhi. Considereu els divisors del k-èsim primerial P_k. Hi ha, per descomptat, k divisors de P_k que consisteixen en un sol primer: justament són els primers $p_1, p_2, \ldots, p_k$. Hi ha $\binom{k}{2}$ divisors de P_k que són producte de 2 primers i, en general, hi ha $\binom{k}{i}$ divisors de P_k que són producte de i primers. Per tant, hi ha

$$1 + k + \binom{k}{2} + \cdots + \binom{k}{k-1} + 1 = 2^k$$

divisors de P_k. Per exemple, els 16 divisors de $P_4 = 2 \cdot 3 \cdot 5 \cdot 7$ són $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5$, $2 \cdot 3 \cdot 7$, $2 \cdot 5 \cdot 7$, $3 \cdot 5 \cdot 7$, $2 \cdot 3$, $2 \cdot 5$, $2 \cdot 7$, $3 \cdot 5$, $3 \cdot 7$, $5 \cdot 7$, 2, 3, 5, 7 i 1. Per a cada divisor d, definim $\mu(d) = 1$ si d conté un nombre parell de primers i $\mu(d) = -1$ si d conté un nombre senar de primers (μ s'anomena la funció de Möbius). Preneu la següent suma sobre tots els divisors d:

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

Per exemple, per a $k = 2$, el primerial P_2 és $2 \cdot 3$ i la suma anterior és:

$$\frac{1}{2^1 - 1} - \left(\frac{1}{2^2 - 1} + \frac{1}{2^3 - 1}\right) + \frac{1}{2^{2\cdot 3} - 1} = \frac{1}{1} - \left(\frac{1}{3} + \frac{1}{7}\right) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Finalment considereu el procediment següent: resteu $1/2$ a la suma anterior, preneu el logaritme en base 2, resteu el resultat de 1, i preneu la part entera del que obtingueu. El resultat és justament el següent primer!

Fórmula de Gandhi. El primer $(k+1)$-èsim és:

$$p_{k+1} = \left[1 - \log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right)\right].$$

Apliquem la fórmula de Gandhi al cas $k = 2$ i verifiquem que ens dóna el resultat esperat $p_3 = 5$: en aquest cas la suma, que ja hem calculat abans, és

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}.$$

Per tant,

$$\log_2\left(-\frac{1}{2} + \sum_{d|P_2} \frac{\mu(d)}{2^d - 1}\right) \sim \log_2(0,04) \sim -4,6.$$

Així doncs,

$$p_3 = [1 - (-4,6)] = [5,6] = 5,$$

tal com volíem.

Per què funciona la fórmula de Gandhi? No hi entrarem en detall aquí, però cal dir que s'obté de tan sols dues coses: el garbell d'Eratòstenes i l'expansió en sèrie infinita

$$\frac{1}{2^d - 1} = \frac{1}{2^d} + \frac{1}{2^{2d}} + \frac{1}{2^{3d}} + \cdots$$

Realment, el nombre 2 de la fórmula és irrellevant; si ho preferiu, el podeu substituir per e o per 10, sempre que llavors prengueu logaritmes neperians o en base 10 respectivament. A [30] trobareu un bonic recull de diverses demostracions de la fórmula de Gandhi.

6 Pseudoprimers al rescat

Naturalment, el problema que té la fórmula de Gandhi és que no és útil per calcular primers. El nombre de termes de la suma creix exponencialment, de manera que si preteneu calcular tan sols el vint-i-cinquè primer (que és el 97) haureu de sumar 30 milions de termes. Sortosament, hi ha maneres més ràpides de calcular primers. Una estratègia usual és dividir el problema en dues parts:

1. Trobar nombres que, amb molta probabilitat, són primers, i llavors
2. Comprovar que realment ho són.

Pel que fa a la primera part del problema, un dels mètodes estàndard consisteix a utilitzar *pseudoprimers*. Se sap des de fa centenars d'anys que si p és primer llavors $2^p - 2$ és divisible per p; això és una conseqüència del teorema petit de Fermat. Usualment es demostra fent servir aritmètica modular, però no és necessari. La prova original, d'Euler, és simple (vegeu Sandifer 2003): d'acord amb l'expansió binomial, tenim

$$(1 + 1)^p = 1 + p + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1.$$

Si p és primer, cada un dels termes $\binom{p}{i}$ és divisible per p i, per tant, $2^p - 2$ és divisible per p, tal com volíem.

Resulta que hi ha nombres que superen aquest test i no són primers. Per exemple, $2^{341} - 2$ és divisible per 341, però no és primer: $341 = 11 \times 31$. Aquesta mena de nombres s'anomenen *pseudoprimers*. Afortunadament són poc abundants, de manera que si un nombre p satisfà la condició que $2^p - 2$ és divisible per p llavors podem confiar que molt probablement és primer.[4]

Pel que fa a verificar que un nombre p és realment primer, fins fa poc es coneixien diversos mètodes aproximats i hi havia un gran interès per desenvolupar algorismes més ràpids. No se sabia si hi havia un algorisme que determinés si p era primer amb un temps de càlcul polinomial en termes del nombre

4 També es pot utilitzar un nombre diferent de 2: si $1 < a < p$, llavors l'argument de la prova d'Euler es pot estendre per demostrar que $a^p - a$ és divisible per p.

de dígits de p. Al 2002, Manindra Agrawal, Neeraj Kayal i Nitin Saxena, de l'Indian Institute of Technology de Kanpur, van sorprendre el món anunciant que havien trobat aquest algorisme. Tota la premsa internacional es va fer ressó del descobriment, i en deu dies la pàgina web que contenia el codi va registrar més de dos milions de connexions. Hi ha un article excel·lent sobre l'algorisme AKS a Folkmar (2003).[5] El punt de partida d'aquest algorisme remarcablement simple és una generalització del teorema petit de Fermat[6]: si $1 < a < p$, llavors p és primer si i només si els coeficients del polinomi $(x-a)^p - (x^p - a)$ són tots divisibles per p.

Actualment s'està fent molt de treball d'anàlisi de l'algorisme AKS. Tal com observa Chris Caldwell a [9], «en aquests moments aquest camp està sotmès a evolució constant».

7 Activitats amb primers

Una de les característiques de l'estudi dels nombres primers és que es pot adaptar fàcilment a la realització d'activitats: hi ha tants tipus de nombres primers (primers de Sophie Germain, de Fermat, de Mersenne, factorials, primerials, etc.) que sorgeix immediatament una gran varietat de preguntes. Per exemple, «trobeu què és un primer de Sophie Germain, quin és el més gran que es coneix, i expliqueu alguna cosa de la biografia de Sophie Germain».

La possibilitat de fer exploracions amb ordinadors és una altra característica interessant des del punt de vista docent. Si es té accés a determinades aplicacions, els estudiants aprenen i assimilen més profundament els conceptes quan els manipulen. Una de les activitats òbvies és construir un programa que calculi tots els primers fins a un límit fixat. També és possible d'involucrar-se en alguns dels projectes de col·laboració en xarxa sobre recerca de primers. Un d'ells és el projecte GIMPS [22].

Finalment, també es poden usar els nombres primers com a vehicle per a l'aprenentatge de les «demostracions». Encara que les demostracions no són gaire populars entre els alumnes, ni entre la major part dels professors, no deixen de ser l'eina de treball principal dels matemàtics. Els nombres primers ofereixen un context adequat per a l'exploració de les estratègies de demostració, i podrien representar avui en dia el paper que en altres temps havien ostentat admirablement els arguments lògics de la geometria clàssica. Potser l'exemple més clar el tenim en el teorema fonamental de l'aritmètica: tot enter es pot escriure de manera única com a producte de primers. El material que cal per provar aquest resultat és autocontingut, mentre que la seva demostració il·lustra la necessitat de claredat i rigor i és un bell exemple de la naturalesa de les demostracions matemàtiques.

A Internet podem trobar una gran quantitat d'informació relacionada amb l'estudi dels nombres primers a les escoles. Naturalment, cal anar una mica

5 N. del t.: Vegeu també J. Díaz, «L'algorisme de primalitat AKS», *Butlletí de la Societat Catalana de Matemàtiques*, vol. 17, núm. 2 (2002), p. 21–28.

6 Es pot demostrar també sense aritmètica modular, utilitzant l'expansió binomial.

amb compte: la xarxa està plena de pàgines que contenen demostracions espúries de conjectures importants, o que ens parlen del significat espiritual dels nombres primers, o fins i tot que declaren que «la distribució dels nombres primers és en realitat el pla estructural de l'univers». A banda d'aquestes, les referències següents, que el lector pot utilitzar com a punt de partida, són excel·lents: [25], [7], [21], [40], [33], [5], [32], [1], [26], [18]. També podeu provar d'unir-vos a la caça de primers ([10]), sintonitzar un programa de ràdio BBC ([38]), escoltar la música dels primers ([2]), explorar problemes sobre primers per a secundària ([5]) o enfrontar-vos a problemes computacionals sobre nombres primers ([34]).

A la xarxa també hi ha qüestions sobre primers que es poden atacar sense disposar de gaires coneixements previs. Aquí en teniu tres exemples, extrets de l'Olimpíada Matemàtica de Manhattan:

1. Proveu que, quan es divideix qualsevol primer per 30, la resta que obtenim és 1 o bé un nombre primer.
2. Busqueu tots els nombres primers p per als quals $p+10$ i $p+14$ són també primers.
3. Proveu que si un nombre primer m té la propietat que m^2+2 és primer, llavors m^3+2 també és primer.

8 Conclusions

Els nombres primers segueixen sent una part important i estimulant de les matemàtiques. Ofereixen problemes que els alumnes de secundària poden entendre. I són objecte d'una recerca activa i actual que produeix avenços sorprenents amb regularitat. Malauradament, no tenen gaire presència a l'ensenyament secundari. I, segons crec, part del problema prové del fet que usualment els materials docents d'introducció a la teoria de nombres parteixen de l'aritmètica modular, que, per la seva pròpia naturalesa, dóna lloc a un grau d'abstracció que pot no ser escaient des d'un punt de vista docent.

En aquest article he intentat mostrar que hi ha tot un seguit de material rellevant sobre els nombres primers que es pot explorar sense l'ajut de l'aritmètica modular. Tenim la recerca teòrica: el fet que el forat entre primers consecutius es fa arbitràriament gran (vegeu la secció 3) o el teorema petit de Fermat (vegeu la secció 6). Tenim la dimensió històrica dels primers, amb conjectures famoses com la de Goldbach o la dels primers bessons i personalitats com les de Reo Fortune i Sophie Germain. Tenim problemes que són tot un repte, i hi ha exploracions numèriques que es poden dur a terme amb fulls de càlcul o una simple calculadora. I potser el més important de tot: els nombres primers són un excel·lent vehicle d'aprenentatge d'habilitats analítiques i de raonament deductiu.

Així doncs, els nombres primers poden tenir més protagonisme a secundària? Els més realistes contestaran: «I quina part del temari sacrifiquem per incloure-hi els nombres primers?» Ningú no gosa afirmar que algun dels con-

tinguts actuals, ja molt migrats, no és essencial. De fet, el disseny dels continguts d'una assignatura és una tasca problemàtica. Els temaris tenen una càrrega considerable d'inèrcia, cosa que probablement és bona. I molts dels que ensenyem matemàtiques ens concentrem més en *com* ensenyar que no pas en *què* ensenyar, ja que allò és exactament el que podem controlar de la nostra activitat diària. Però en realitat els continguts són un tema clau, i, contra el corrent imperant que els pretén diluir, podem intentar oposar-hi la necessitat d'incloure-hi material com el que ofereixen els nombres primers.

Referències

[1] www.math.utah.edu/~alfeld/math/machine.html (ALFELD, P. *The prime machine*).

[2] www.2357.a-tu.net/index.php?link=Music (AT open publisher, *Aesthetics of the prime sequence*).

[3] algo.inria.fr/banderier/Computations/prime_factorial.html (BANDERIER, C. *Fortunate and unfortunate primes: nearest primes from a prime factorial*).

[4] BORNEMAN, F. «PRIMES is in P: a breakthrough for "Everyman"». *Notices of the American Mathematical Society*, 50 (2003), 545–552.

[5] www.bwctc.northants.sch.uk/html/master/maths/autumn99/primech.htm (Brooke Weston CTC *Mathematics masterclass: prime number challenges*).

[6] www.mathpages.com/home/inumber.htm (BROWN, K. *Mathpages: Number Theory*).

[7] www.utm.edu/research/primes/ (CALDWELL, C. K. *The prime pages*).

[8] primes.utm.edu/top20/page.php?id=13 (CALDWELL, C. K. *Consecutive primes in arithmetic progression*).

[9] www.utm.edu/research/primes/prove/prove4_3.html (CALDWELL, C. K. *Finding primes and proving primality*).

[10] primes.utm.edu/primes/background/finding.php (CALDWELL, C. K. *The top 5000, finding large primes*).

[11] CALDWELL, C. K.; GALLOT, Y. «On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$». *Mathematics of computation*, 71 (2002), 237, 441–448.

[12] CONREY, J. B. «The Riemann hypothesis». *Notices of the American Mathematical Society*, 50 (2003), 341–353.

[13] DERBYSHIRE, J. *Prime obsession*. Washington DC: Joseph Henry Press, 2003.

[14] DOXIADIS, A. *Uncle Petros and Goldbach's conjecture*. Nova York: Bloomsbury, 2000. Traducció catalana: *L'oncle Petros i la conjectura de Goldbach*. Barcelona: Suma de Lletres, 2002.

[15] DU SAUTOY, M. *The music of the primes*. Harper Collins, 2003.

[16] DUDLEY, U. «Formulas for primes». *Mathematics magazine*, 56 (1983), 17–22.

[17] www.ieeta.pt/~tos/goldbach.html (E SILVA, O. *Goldbach conjecture verification*).

[18] www.eff.org/awards/prime-info.html (EFF cooperative computing awards).

[19] EVES, H. *Return to mathematical circles*. Boston: PWS-KENT Publishing Co., 1988.

[20] www.ltkz.demon.co.uk/ktuplets.htm (FORBES, T. *Prime k-tuplets*).

[21] perso.wanadoo.fr/yves.gallot/primes/chrrcds.html (GALLOT, L., GALLOT, Y. *The chronology of prime number records*).

[22] www.mersenne.org/prime.htm (GIMPS: the great Internet Mersenne prime search).

[23] GOLOMB, S. W. «The evidence for Fortune's conjecture». *Mathematics magazine*, 54 (1981), 209–210.

[24] www.maa.org/reviews/reviews_index.html (MAA Online book review).

[25] www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html (MacTutor History of Mathematics archive: prime numbers).

[26] mathforum.org/library/drmath/sets/mid_prime_numbers.html (Math Forum: *middle school prime numbers*).

[27] ODLYZKO, A.; RUBINSTEIN, M.; WOLF, M. «Jumping champions». *Experimental Mathematics*, 8 (1999), 107–118.

[28] www.sciencenews.org/articles/20040424/mathtrek.asp (PETERSON, I. *Progressive numbers*. Science news online, abril 2004).

[29] RASMUSSEN, D. «Prime number». *Prime number*, 19 (2004), 23–28.

[30] RIBENBOIM, P. *The new book of prime number records*. Nova York: Springer-Verlag, 1996.

[31] RIBENBOIM, P. *My numbers, my friends*. Nova York: Springer-Verlag, 2000.

[32] www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html (RICHSTEIN, J. *Verifying the Goldbach conjecture up to* $4 \cdot 10^4$).

[33] www.primepuzzles.net/ (RIVERA, C. *The prime puzzles & problems connection*).

[34] www.olemiss.edu/mathed/pow/powold.htm (ROCK, D. *Ole Miss: problem of the week*).

[35] SABBAGH, K. *The Riemann hypothesis: the greatest unsolved problem in mathematics*. Farrar, Strauss and Giroux, 2003.

[36] www.maa.org/news/howeulerdidit.html (SANDIFER, E. *Fermat's little theorem: how Euler did it*).

[37] SILVERMAN, J. H. *A friendly introduction to number theory*. Prentice Hall, 1996.

[38] www.bbc.co.uk/radio4/science/another53.shtml (SINGH, S. *The largest prime*, BBC Radio 4).

[39] WANG, Y. *Goldbach conjecture*. Singapore: World Scientific Publishing Co., 1984.

[40] en.wikipedia.org/wiki/Prime_number (Wikipedia).

DEPARTMENT OF MATHEMATICS
LA TROBE UNIVERSITY
VICTORIA 3086, AUSTRALIA
g.cairns@latrobe.edu.au