MAT²
MATerials MATemàtics
Volum 2009, treball no. 7, 30 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/matmat

Fem matemàtiques treballant amb els nombres primers

Joan Gimbert Quintilla

1 Presentació

L'estudi dels nombres primers ha apassionat a molts matemàtics, i no matemàtics, de tots els temps. Al llarg d'aquesta notes[1], amb l'objectiu de contagiar-nos una mica d'aquest apassionament, ens anirem plantejant preguntes i cercant respostes sobre diferents aspectes dels nombres primers. I com l'essència de l'activitat matemàtica consisteix justament en saber fer-se preguntes i buscar-hi respostes, podem dir que "farem matemàtiques treballant amb els nombres primers".

2 Què són els nombres primers?

Per començar, *quins són els 10 primers nombres primers?* Aquests, com segurament tots ja sabeu, són

$$2, 3, 5, 7, 11, 13, 17, 19, 23 \text{ i } 29.$$

Quin ha estat el criteri que hem aplicat per triar aquests nombres i descartar-ne d'altres com el 4 *o el* 21*?* Els nombres triats no es poden expressar com a producte d'altres més petits, als quals se'ls anomena factors. Aquest fet no succeeix amb els nombres descartats com el $4 = 2 \cdot 2$ o el $21 = 3 \cdot 7$.

[1] Aquestes notes varen sorgir com a guió d'un seminari divulgatiu sobre nombres primers, que vàrem impartir a la Universitat de Lleida dins del curs *Lliçons populars de Matemàtiques*, impulsat pel Dr. Javier Chavarriga Soriano, a qui volem retre homenatge.

Donem, ara, la definició precisa de nombre primer. Un *nombre primer* és un enter més gran que 1 que només es divisible[2] per ell mateix i per la unitat. Als enters que no són primers, i són més grans que 1, se'ls anomena *nombres compostos*[3].

Un cop recordada la noció de nombre primer, anem a veure quin paper tenen aquests nombres en l'aritmètica[4]. Euclides, matemàtic grec del segle III aC, va demostrar que tot nombre enter positiu major que 1 es pot escriure de manera única com a producte de nombres primers[5]. Així, per exemple, $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$. Aquest resultat, conegut com a *teorema fonamental de l'aritmètica*, ens diu que els nombres primers juguen un paper en l'aritmètica semblant al que tenen els àtoms i els elements en la química.

Com es pot demostrar el teorema fonamental de l'aritmètica?

Si tenim un nombre enter compost n, aleshores sabem que n té almenys un divisor propi, és a dir, un divisor més petit que n i més gran que 1. Considerem el més petit dels divisors propis de n. Aquest divisor propi, diem-li p_1, haurà de ser primer, ja que si no ho fos tindria un divisor propi i aquest seria també un divisor de n, en contra de la suposició que p_1 era el més petit de tots. Així, podem escriure $a = p_1 \cdot a_1$, essent p_1 primer. Si a_1 fos primer, aleshores ja tindríem la descomposició buscada. En cas contrari, apliquem el mateix raonament al nombre enter a_1. D'aquesta manera, podrem expressar $n = p_1 \cdot a_1 = p_1 \cdot p_2 \cdot a_2$. Repetim aquest procés, un nombre finit de vegades, obtindrem $n = p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1} \cdot p_k$, on els nombres p_i són primers i $p_1 \leq p_2 \leq \ldots \leq p_k$.

Veiem com s'aplica el raonament anterior en un exemple concret. Així,

$$132 = 2 \cdot 66 = 2 \cdot 2 \cdot 33 = 2 \cdot 2 \cdot 3 \cdot 11 = 2^2 \cdot 3 \cdot 11.$$

La descomposició d'un nombre compost en producte de factors primers rep el nom de *factorització*.

[2] Donats dos enters positius a i b, direm que a és divisible per b (b és un divisor de a) si existeix un enter c tal que $b \cdot c = a$. Així, per exemple, 6 és divisible per 2 ja que tenim $2 \cdot 3 = 6$. L'anterior definició equival a dir que la resta de la divisió entera de a per b és 0.

[3] En el conjunt de nombres enters positius es distingeix entre nombres primers, nombres compostos i la unitat (1).

[4] L'aritmètica és la branca de les matemàtiques que té per objecte d'estudi els nombres enters i les seves operacions.

[5] Aquesta unicitat és llevat de l'ordre dels factors. Dit d'una altra manera, la descomposició en factors primers és única si fixem, per exemple, que els factors primers s'escriguin en ordre creixent. A més, entendrem que aquest "producte" es redueix a un únic factor quan el nombre és primer.

3 Quants nombres primers hi ha?

Un cop vist el paper rellevant que tenen els nombres primers en l'aritmètica, sembla bastant natural preguntar-nos si la successió de nombres primers és finita o, ben al contrari, sempre podrem trobar nombres primers tan grans com desitgem.

De nou, va ser Euclides qui va donar la resposta. Ell va demostrar, d'una manera senzilla i elegant, que hi ha infinits nombres primers, és a dir, que la llista de nombres primers no s'acaba mai.

Com es pot demostrar l'existència d'infinits nombres primers?[6]

Suposem que tenim la llista $\{2, 3, 5, \ldots, p_n\}$ dels n primers nombres primers. Si som capaços de deduir-ne l'existència d'un nombre primer major que p_n, aleshores haurem provat que la llista de nombres primers no s'acaba mai. Com deduïm, doncs, l'existència d'aquest nou nombre primer? Si considerem el nombre resultant de sumar una unitat al producte de tots els nombres de la llista, és a dir, si prenem $N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_n + 1$, aleshores N és un enter major que p_n i que no és divisible per cap dels primers de la llista, ja que la resta de la divisió entera de N per cadascun d'ells és 1. Aleshores, si N és compost tots els seus factors primers seran majors que p_n i, en cas que sigui primer, el propi N és un nombre primer major que p_n. Així, doncs, queda provada l'existència d'un nombre primer major que p_n i, conseqüentment, queda demostrada l'existència d'infinits nombres primers.

En la demostració anterior hem emprat uns nombres enters molt particulars, aquells que resulten de fer el producte de tots els nombres primers menors o iguals que un nombre primer fixat p. Aquests nombres s'anomenen *primerials* i es denoten per $\#p$. Així,

$$\begin{aligned}
\#2 &= 2 \\
\#3 &= 2 \cdot 3 &&= 6 \\
\#5 &= 2 \cdot 3 \cdot 5 &&= 30 \\
\#7 &= 2 \cdot 3 \cdot 5 \cdot 7 &&= 210 \\
\#11 &= \#7 \cdot 11 &&= 2310 \\
\#13 &= \#11 \cdot 13 &&= 30030.
\end{aligned}$$

Si sumem una unitat a cada nombre anterior, els nombres resultants seran

[6] En el llibre *Proofs from The Book*, d'en Martin Aigner i Günter M. Ziegler, es recullen fins a sis demostracions diferents (vegeu [2]).

tots primers? La resposta és negativa, tal com pot observar-se en la taula següent:

p	$\#p+1$		
2	3	primer	
3	7	primer	
5	31	primer	
7	211	primer	
11	2311	primer	
13	30031	compost	$59 \cdot 509$
17	510511	compost	$19 \cdot 97 \cdot 277$
19	9699691	compost	$347 \cdot 27953$

Observeu que si $\#p+1$ és compost, aleshores tots els seus factors són més grans que p, tal com hem raonat en la demostració de l'existència d'infinits nombres primers.

Com a curiositat podem dir que, segons la informació recollida i actualitzada pel professor Chris Caldwell (vegeu [6]), els únics nombres primers de la forma $\#p+1$, per a valors de $p < 100000$, s'obtenen prenent

$$p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029 \text{ i } 42209.$$

Cal dir, per adonar-nos de la magnitud dels nombres primerials, que el nombre $\#42209$ té 18241 xifres (el rècord pel que fa als nombres primers de la forma $\#p+1$ correspon a $p = 392113$ i té 169966 xifres).

Posat's a fer-nos preguntes, quants nombres primers de la forma $\#p+1$ hi ha? Doncs, a hores d'ara, no es coneix la resposta. És un dels molts problemes encara no resolts sobre els nombres primers. Més endavant en citarem d'altres.

4 Com podem trobar nombres primers "petits"?

4.1 Sedàs d'Eratòstenes

En el segle III aC un altre matemàtic grec, Eratòstenes, va idear un mètode que permet destriar els nombres primers d'entre tots els nombres més petits

o iguals que un enter donat. Aquest algorisme, conegut avui dia com a *sedàs d'Eratòstenes*, procedeix de la manera següent:

1. Disposem en una taula tots els nombres enters compresos entre 2 i N, essent N un enter fixat.

2. Marquem el 2 i anem suprimint tots els múltiples de 2 més grans que 2 i menors o iguals que N, és a dir, eliminem tots els nombres parells $4, 6, 8, \ldots$, fins a N o a $N-1$, segons correspongui.

3. Prenem el primer nombre enter i no marcat ni eliminat. Marquem aquest nombre i i eliminem tots els múltiples de i majors que i i menors o iguals que N, és a dir, nombres de la forma $k \cdot i$, essent $2 \leq k \leq [\frac{N}{k}]$, on $[x]$ denota la part entera[7] de x.

4. Si tots els nombres que resten estan marcats, aleshores acabem. En cas contrari, tornem al pas 3.

És clar que els nombres que queden després d'aplicar el sedàs d'Eratòstenes són justament els nombres primers menors o iguals que N.

Detallem, a continuació, com s'aplica el sedàs d'Eratòstenes per a trobar els nombres primers menors o iguals que 100.

Taula inicial:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

[7] La part entera d'un nombre real x, que es denota per $[x]$, es defineix com el més gran dels nombres enters menors o iguals que x. Així, per exemple, $[2{,}71] = 2$.

Taula per a $i = 2$:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Taula per a $i = 3$:

	2	**3**	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Taula per a $i = 5$:

	2	**3**	4	**5**	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Observem que cada vegada anem eliminant menys nombres. Això ens fa sospitar que en un determinat pas ja no s'eliminaran nous nombres. En el cas que ens ocupa tenim una nova taula per a $i = 7$,

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

i per a $i = 11$ pot comprovar-se que ja no s'eliminen més elements. *Podem concloure, aleshores, que tots els nombres restants són primers?* La resposta és afirmativa, ja que si un nombre $n \leq 100$ fos compost, aleshores, pel teorema fonamental de l'aritmètica, podríem escriure $n = p \cdot m$, on p és el factor primer més petit de n i on m és el producte dels factors restants. Aleshores, p ha de ser més petit o igual que 7, ja que en cas contrari p i m serien més grans que 10 i, per tant, el seu producte, que val n, seria més gran que 100, en contra de la suposició inicial de que n era menor o igual que 100. Aquest mateix raonament, però fet en general, ens permet demostrar que si n és un enter compost, aleshores n té un factor primer p que és menor o igual que la part entera de l'arrel quadrada de n, és a dir, $p \leq [\sqrt{n}\,]$. (Noteu que 7 és el nombre primer més gran que està per sota de $\sqrt{100} = 10$).

Així, doncs, el nombre d'iteracions del sedàs d'Eratòstenes, és a dir, el nombre de vegades que haurem d'aplicar el pas 3 de l'algorisme serà de l'ordre de l'arrel quadrada de n. Des del punt de vista computacional, aquest és un ordre molt elevat. Això significa que llevat que n sigui "petit" ($n \leq 1\,000\,000$) el temps requerit de còmput serà molt gran. Aquesta mateixa observació serveix també per l'anomenat *test de primalitat*[8] *basat en les divisions successives*. Aquest test determina si un nombre enter n és primer o és compost efectuant les divisions successives de n pels enters menors o iguals que $\sqrt{n}$. Si alguna d'aquestes divisions dóna de resta 0, aleshores es conclou que n

[8] Un test de primalitat és un algorisme capaç d'esbrinar si un nombre enter donat és primer o no ho és.

és compost. En cas contrari, es certifica que n és primer. Aquest mètode té un cost exponencial en relació al nombre de dígits de n, donat pel seu logaritme decimal, ja que $\sqrt{n} = e^{\frac{1}{2}\log n}$. Com que la funció exponencial creix molt ràpidament, seria desitjable trobar un test amb una funció cost de tipus polinòmic, les quals creixen molt més "moderadament". En aquest sentit, fa relativament poc temps, tres matemàtics indis, Manindra Agrawal, Neeraj Kayal i Nitin Saxena [1] varen idear un test de primalitat determinista[9] i amb un cost polinòmic respecte a la grandària del nombre d'entrada, demostrant d'aquesta manera que el problema de decidir si un nombre és primer o no ho és pertany a l'anomenada classe de complexitat $\mathcal{P}$.

4.2 Sedàs geomètric de Matiiassevitch

Als matemàtics russos Yuri Matiiassevitch i Boris Stechkin se'ls va ocórrer una manera gràfica de mostrar tots els divisors propis d'un enter (petit). Es parteix del dibuix, en uns eixos cartesians, d'una paràbola d'equació $y = x^2$ sobre la qual es marquen els punts de coordenades enteres. Llavors, es tracen les rectes que uneixen parelles d'aquests punts situats en branques diferents de la paràbola, és a dir, un dels punts té per coordenades $(-m, m^2)$ i l'altre (n, n^2). Resulta que la intersecció de cadascuna d'aquestes rectes $r_{m,n}$ amb l'eix vertical correspon al punt que té per ordenada el producte de m i n, ja que si en l'equació de dita recta,

$$y = (n - m) \cdot x + m \cdot n,$$

substituïm el valor de x per 0 obtenim $y = m \cdot n$. En la Figura 1 mostrem el cas particular en que $m = 2$ i $n = 3$.

Mitjançant aquesta enginyosa representació, els nombres primers apareixen com les ordenades enteres > 1 d'aquells punts de l'eix vertical pels quals no hi passa cap de les rectes $r_{m,n}$, per a $m > 1$ i $n > 1$. En la Figura 2 mostrem el gràfic que resultaria intercanviant (per conveniència) els eixos de les x's i de les y's, tal com apareix en el llibre *Merveilleux nombres premiers* d'en Jean-Paul Delahaye (vegeu [10]).

[9] Els tests deterministes garanteixen la primalitat del nombre, en cas que els passi, mentre que els tests probabilístics només ens la donen amb un cert grau (molt elevat) de confiança.

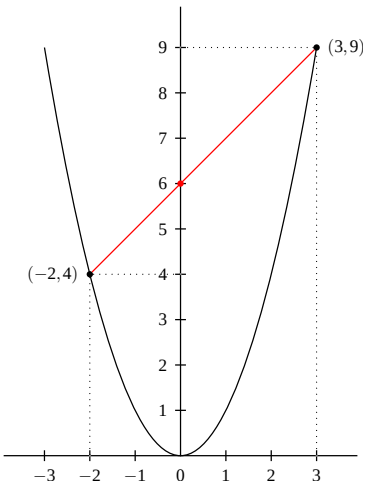

Figura 1: Representació geomètrica del producte dels nombres $m = 2$ i $n = 3$.

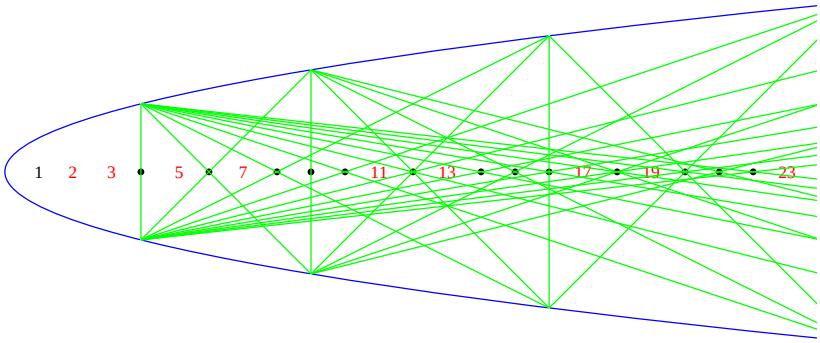

Figura 2: Els nombres primers ≤ 23 obtinguts mitjançant el sedàs de Matiiassevitch.

5 Hi ha fórmules per generar nombres primers?

És bastant probable que alguna vegada hàgiu hagut d'endevinar quin nombre segueix "lògicament" als primers nombres d'una certa seqüència d'enters com, per exemple,

$$1, 4, 7, 10, 13, \ldots \quad \text{o} \quad 1, 4, 9, 16, 25, \ldots .$$

Es tracta de descobrir quina llei segueixen (per exemple, cada terme –llevat del primer– s'obté de sumar tres unitats al terme anterior) o quina propietat els caracteritza (per exemple, ser un quadrat perfecte). Un pas més enllà consistiria en trobar una fórmula tancada per al terme general de la successió,

la qual ens permetria, en particular, obtenir directament qualsevol terme de la mateixa (per exemple, el terme general de la primera successió és $a_n = 3n+1$, on $n \geq 0$). Això ens duu a plantejar-nos si existeix una tal fórmula per als nombres primers. En aquesta direcció, podem començar per donar resposta a la següent qüestió:

Existeix una funció del tipus $f(n) = a \cdot n + b$ que sempre ens doni nombres primers?

Si fos així, com $f(0) = b$ tindríem que b hauria de ser primer. Llavors, tenint en compte que $f(b) = a \cdot b + b = (a+1)b$ també hauria de ser primer, deduïm que $a + 1 = 1$, és a dir, $a = 0$ i, en conseqüència, la funció esdevé constant, $f(n) = b$ (aquesta seria la situació trivial i no desitjada ja que només ens proporcionaria un nombre primer).

En quines situacions la funció $f(n) = a \cdot n + b$ permet obtenir infinits nombres primers o, dit d'una altra manera, per a quins valors de a i b existeixen infinits nombres primers dins la progressió aritmètica $b, b + a, b + 2a, \ldots$?

Certament si a i b comparteixen un factor primer p en comú llavors $f(n) = a \cdot n + b$ esdevé un múltiple de p, per a tot valor de $n \geq 1$. Així, doncs, és necessari que a i b siguin *primers entre ells*[10]. L'any 1837, Lejeune Dirichlet va demostrar que dita condició és suficient per garantir que hi hagi infinits nombres primers de la forma $a \cdot n + b$. Per exemple, la successió de terme general $a_n = 4n + 1$ conté infinits nombres primers (assenyalats en vermell):

$$1, 5, 9, 13, 17, 21, 25, 29, \ldots$$

I si ampliem la classe de funcions a considerar i admetem, per exemple, que $f(n)$ sigui una funció polinòmica (de qualsevol grau) amb coeficients enters?

L'any 1752, Christian Goldbach va demostrar que, tal com succeïa en el cas de grau 1, no existeix una funció polinòmica de grau $k \geq 1$ que sempre doni nombres enters. Això no impideix que hi hagi funcions d'aquesta mena que proporcionin un bon seguit de primers (vegeu [21]). Així, per exemple, la funció $f(n) = n^2 - n + 41$, donada per Leonhard Euler[11], proporciona tot de nombres primers per als 41 primers valors de $n \geq 0$. Així,

n	0	1	2	3	...	40	41
$f(n)$	41	41	43	47	...	1601	41^2

[10] Dos nombres enters positius són primers entre ells si el seu màxim comú divisor és 1.

[11] Leonhard Euler, matemàtic suís (1707-1783), es considerat com un dels matemàtics més rellevants de tota la història.

Emprant expressions més complicades que les polinòmiques, s'han trobat fórmules que sí cobreixen a tots els nombres primers però que no resulten útils per generar-los, degut al seus elevats requeriments computacionals. En aquest sentit podem esmentar la fórmula que J. Minác i C. Willans (1995) varen deduir per a l'n-èsim nombre primer p_n,

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor} \right\rfloor^{\frac{1}{n}} \right\rfloor$$

(vegeu [10]). La correctesa de dita fórmula es basa en el teorema de Wilson, el qual caracteritza als nombres primers com aquells enters $p > 1$ tals que p divideix a $(p-1)! + 1$, on $(p-1)!$ denota el *factorial*[12] de $p - 1$.

6 Com estan distribuïts els nombres primers?

Veient la llista dels nombres primers menors que 100, obtinguda mitjançant el sedàs d'Eratòstenes,

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 \\ , 59, 61, 67, 71, 73, 79, 83, 89, 97\},$$

sembla que els nombres primers estiguin repartits d'una manera molt irregular. Així, d'una banda, tenim nombres primers que difereixen només de dues unitats[13], com, per exemple, 17 i 19. D'altra banda, hi ha "forats grans" sense cap nombre primer com passa, per exemple, entre el 89 i el 97. Anem a estudiar, amb una mica de detall, aquests dos fenòmens locals.

6.1 Nombres primers bessons

Dos nombres primers que difereixen de dues unitats s'anomenen *nombres primers bessons*. Així,

$$(3, 5),\ (5, 7),\ (11, 13),\ (17, 19),\ (29, 31),\ (41, 43),\ (59, 61) \text{ i } (71, 73)$$

[12] El nombre factorial d'un enter positiu n, que es denota per $n!$, es defineix com el producte de tots els enters positius menors o iguals que n, és a dir, $n! = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2$. Per exemple, $5! = 5 \cdot 4 \cdot 3 \cdot 2 = 120$.

[13] La diferència entre dos nombres primers consecutius, més grans que 2, és un nombre parell, ja que tots els nombres primers, llevat del 2, són senars.

són les úniques parelles de primers bessons menors que 100.

En relació a aquests nombres tan peculiars quines preguntes creieu que seria interessant de plantejar-se? Un matemàtic, per exemple, voldria saber si hi ha un nombre infinit de nombres primers bessons. I què se'n sap? Es conjectura que hi ha un nombre infinit d'aquestes parelles. La convicció que tenen els matemàtics sobre la certesa d'aquesta conjectura rau, d'una banda, en el fet que s'han pogut trobar parelles de primers bessons tan grans com s'han buscat i, d'altra banda, com un argument de major pes, en el fet de tenir una "idea aproximada" sobre quantes parelles de primers bessons hi ha menors o iguals que un enter fixat n. La funció que es creu que aproxima tal quantitat pren valors tan grans com es vulguin, si n pren valors suficientment grans[14] (vegeu [15]).

En la taula següent, treta de [6], hi figuren les tres parelles de primers bessons més grans que es coneixen:

Primers bessons	**Dígits**	**Qui els va trobar?**	**Quan?**
$65516468355 \cdot 2^{333333} \pm 1$	100355	Kaiser i Klahn	agost 2009
$2003663613 \cdot 2^{195000} \pm 1$	58711	Vautier, McKibbon i Gribenko	gener 2007
$194772106074315 \cdot 2^{171960} \pm 1$	51780	Jarai, Farkas, Csajbok i Kasza	juny 2007

L'estimació que es dóna, malgrat encara no s'hagi demostrat, del nombre de parelles de primers bessons menors o iguals que un enter n és $b(n) = \frac{(1{,}32032\ldots)\cdot n}{(\ln n)^2}$, on $\ln n$ denota el logaritme neperià[15] de n. La taula següent, treta de [9], permet comparar els valors estimats i els valors reals del nombre de parelles de primers bessons compreses en els intervals que es detallen:

[14] D'una manera més precisa i rigurosa diríem que el límit de la funció en qüestió, en tendir n a infinit, és infinit.

[15] El logaritme en una base a d'un nombre real i positiu x, que es denota per $\log_a x$, es defineix com el nombre real y al qual hem d'elevar la base a per tal d'obtenir x, és a dir, $a^x = y$. Per exemple, $\log_{10} 1000 = 3$ ja que $10^3 = 1000$. Quan es pren com a base el nombre e, aleshores se'n diu logaritme neperià. Recordem que el nombre $e = 2,7182\ldots$ és el nombre irracional al qui tendeix la successió $(1 + \frac{1}{n})^n$ en anar augmentant el valor de n.

Interval $\Delta = 150000$	Parelles de primers bessons	
	Estimades	**Trobades**
$[10^{11}, 10^{11}+\Delta]$	309	276
$[10^{12}, 10^{12}+\Delta]$	259	276
$[10^{13}, 10^{13}+\Delta]$	221	208
$[10^{14}, 10^{14}+\Delta]$	191	186
$[10^{15}, 10^{15}+\Delta]$	166	161

6.1.1 Primers trigèmins i altres configuracions

De la mateixa manera que hem definit els primers bessons podríem també introduir la noció de primers trigèmins, és a dir, ternes de nombres primers de la forma $(p, p+2, p+4)$. Així, per exemple, la terna $(3, 5, 7)$ ho és.

Quantes ternes de primers trigèmins hi ha?

Per tal de respondre la pregunta fixeu-vos en què succeeix amb les ternes següents: $(5, 7, 9)$, $(7, 9, 11)$, $(11, 13, 15)$ i $(13, 15, 17)$. Podeu veure que en totes elles hi ha apareix un múltiple de 3. Aquesta observació ens pot dur a pensar que tota terna de la forma $(p, p+2, p+4)$ conté un múltiple de 3 i, per tant, llevat de la terna $(3, 5, 7)$ no hi cap altra on els tres components siguin nombres primers. Anem a provar, doncs, que si p és un nombre primer diferent de 3, aleshores o bé $p+2$ o bé $p+4$ és un múltiple de 3. Si p és primer i diferent de 3, aleshores la resta de la divisió entera de p per 3 és 1 o 2, és a dir, p pot escriure's d'una de les dues maneres següents: $p = 3k+1$ o $p = 3k+2$, on k és un enter. Si p és de la forma $3k+1$, aleshores $p+2 = 3k+3$ és un múltiple de 3, i si $p = 3k+2$, aleshores $p+4 = 3k+6$ és un múltiple de 3. Per tant, en tots dos casos es dedueix que un dels nombres de la terna $(p, p+2, p+4)$ és un múltiple de 3.

Què succeeix amb els patrons següents $(p, p+2, p+6)$ *i* $(p, p+4, p+6)$*?*

Les primeres ternes de nombres primers que segueixen aquests patrons són

$$(5, 7, 11), (11, 13, 17), (17, 19, 23), \ldots \text{ i } (7, 11, 13), (13, 17, 19), (37, 41, 43), \ldots$$

respectivament, mentre que la terna més gran coneguda, segons recull en Tony Forbes a la seva pàgina web sobre les anomenades *prime k-tuples* (vegeu [13]), és:

Terna	Dígits de p	Qui la va trobar?	Quan?
$(p, p+2, p+6)$, $p = 2072644824759 \cdot 2^{33333} - 1$	10047	Luhn i Morain	novembre 2008

Tal com succeeix amb la parella $(p, p+2)$, també es conjectura que hi ha infinites ternes de primers per a cadascuna de les tripletes $(p, p+2, p+6)$ i $(p, p+4, p+6)$. I si, posat's a generalitzar, com agrada als matemàtics, considerem configuracions de la forma $(p, p+a_1, \ldots, p+a_k)$ tals que siguin, en cert sentit, *minimals* (el rang a_k és el més petit possible per poder encabir a $k+1$ primers) i, a més, siguin *factibles* de tenir infinites realitzacions (no contenen cap *sistema complet de residus*[16] mòdul un primer, fet que ho impossibilitaria)? Doncs, bé, l'anomenada *conjectura de les constel·lacions*, formulada per en Hardy i Littlewood (vegeu [10]), afirma que per a cadascuna de les formes minimals i factibles hi ha infinites realitzacions constituïdes íntegrament per nombres primers, dites *constel·lacions*. Aquests dos matemàtics anglesos, reconegudes autoritats en teoria de nombres, també van conjecturar que el nombre de primers compresos entre $n+2$ i $n+k$ mai pot superar al nombre de primers entre 2 i k, per a qualsevol parella d'enters n i k. Tot i que totes dues conjectures han estat verificades numèricament per a un gran nombre de valors, Hensley i Richards van demostrar l'any 1973 que són incompatibles, en el sentit que la certesa d'una implicaria la falsedat de l'altra. Es creu que la segona d'elles és falsa (vegeu [8]).

6.2 Grans buits en la seqüència de nombre primers

En la taula dels nombres primers menors que 100 s'havia observat que després del 89 hi havia 7 enters consecutius que eren compostos. Si anem més endavant, podrem veure que al 113 li segueixen 13 nombres compostos. A la vista d'aquests resultats ens podem preguntar:

Hi ha, en la seqüència dels nombres enters, buits tan grans com es vulgui de nombres primers?

La resposta és afirmativa, tal i com a continuació provarem. Donat un nombre enter positiu n, els enters $n!+2, n!+3, \ldots, n!+n$, on $n!$ és el factorial de n, constitueixen una seqüència de $n-1$ enters consecutius compostos ja que $n!+k$, essent $k \leq n$, és divisible per k. Això ens diu que anant suficientment enllà en la seqüència d'enters trobarem buits de nombres primers tan

[16] Donat un enter positiu n, un sistema complet de residus mòdul n és un conjunt format per n nombres enters $\{a_1, \ldots, a_n\}$ tals que mòdul n tots ells són diferents entre si. Per exemple, $\{p, p+2, p+4\}$ és un sistema complet de residus mòdul 3.

grans com vulguem. Hem vist, concretament, que després del nombre $n!+2$ tenim un buit de longitud $n-1$. Ara bé, això no significa que abans no es pugui trobar un buit de la mateixa llargada. Així, per exemple, al nombre 42 842 283 925 351 (14 dígits) li segueixen 777 enters consecutius i compostos tal com succeeix amb el nombre $778!+1$ (1914 dígits), a qui li segueixen $778!+2,\ 778!+3,\ldots,778!+778$, tots ells compostos.

6.3 Ordre dins del desordre

En els apartats anteriors hem vist que en la successió formada per les diferències entre dos primers consecutius,

$$\{2,3,5,7,11,13,17,19,23,29,\ldots\}\longrightarrow\{1,2,2,4,2,4,2,4,6,\ldots\},$$

avançant-hi suficientment apareixen diferències tan grans com es vulguin i, d'altra banda, es creu que hi ha infinites diferències mínimes de 2 unitats. L'existència d'aquestes situacions extremes, reflex de la repartició molt irregular dels nombres primers dins del conjunt dels enters, no ens pot fer prendre l'esperança de trobar una regularitat en la distribució dels nombres primers, és a dir, de descobrir un cert ordre dins d'aquest desordre que ens permeti, per exemple, estimar el promig de les k-primeres diferències o, equivalentment, estimar l'ordre de magnitud del $(k+1)$-èsim nombre primer.

Si n és un nombre enter positiu, es denota per $\pi(n)$ el nombre de primers menors o iguals que n. Així, per exemple, $\pi(10)=4$ ja que només hi ha 4 nombres primers menors o iguals que 10. La funció $\pi(n)$ és una mesura de la distribució dels nombres primers. En la taula següent, treta de [9], podeu observar com varien els valors de $\pi(n)$ i de $n/\pi(n)$, quan n pren per valor diferents potències de 10.

n	$\pi(n)$	$n/\pi(n)$
10	4	2,5
100	25	4,0
1000	168	6,0
10000	1229	8,1
100000	9592	10,4
1000000	78498	12,7
10000000	664579	15,0
100000000	5761455	17,4
1000000000	50847534	19,7

Hi observeu alguna mena de regularitat en el comportament de la funció $f(n) = n/\pi(n)$*?*

Fixeu-vos que mentre la seqüència de valors de n constitueix una *progressió geomètrica*, ja que la raó entre dos termes consecutius és constant (10), la seqüència de valors de $f(n)$ s'aproxima molt a una *progressió aritmètica*, ja que la diferència entre dos termes consecutius és gairebé constant (2,3). *I quines funcions ens transformen progressions geomètriques en aritmètiques?* Doncs, les funcions logarítmiques ja que aquestes ens transformen productes i quocients en sumes i restes, respectivament. Així, sembla plausible conjecturar que $f(n) = n/\pi(n)$ pugui aproximar-se per $\ln n$. (El fet de prendre el logaritme neperià es deu a que $f(10^{k+1}) - f(10^k)$ és aproximadament 2,3 que és, a la seva vegada, molt proper a $\ln 10 = 2,30258\ldots$). Aquesta és la conjectura que va fer Gauss[17] quan tan sols tenia 15 anys. La formalització d'aquesta conjectura ens porta a l'enunciat del *teorema del nombre primer*. Aquest ens diu que la raó entre $\pi(n)$ i $n/\ln n$ pot fer-se tan propera a 1 com vulguem, si prenem valors de n suficientment grans. Això, pels qui estigueu familiaritzats amb el llenguatge dels límits, significa que $\lim_{n\to\infty} \pi(n)/(n/\ln n) = 1$. La demostració rigurosa d'aquest teorema data del 1896 i es fruit dels treballs independents de Hadamard i de la Vallée-Poussin[18]. Posteriorment s'han trobat aproximacions millors de la funció $\pi(x)$, vegeu el capítol 2 de [17] .

Una de les conseqüències del teorema del nombre primer és que l'ordre de magnitud del n-èsim nombre primer és $n \ln n$ i, per tant, el promig de les n primeres diferències entre nombres primers consecutius pot aproximar-se per $\ln n$.

7 I més conjectures ...

En aquesta exploració per l'univers dels nombres primers ja ens han aparegut un bon grapat de qüestions per les quals encara no tenim una resposta definitiva. Tot i que l'experimentació numèrica avali, en cada cas, una cer-

[17] Karl Friedrich Gauss, matemàtic alemany (1777-1855), ha estat un dels matemàtics més importants de tots els temps degut a les seves nombroses contribucions en les diverses àrees de la matemàtica (geometria, àlgebra, anàlisi, teoria de nombres, etc.)

[18] Jacques Hadamard, matemàtic francès (1865-1963), i Charles. J. de la Vallée-Poussin, matemàtic belga (1866-1962), varen demostrar el teorema del nombre primer emprant tècniques de l'anàlisi complexa.

ta conjectura aquesta no deixarà de ser-ho fins que algú trobi la clau per demostrar-la o, per contra, la refuti mitjançant un contraexemple (un exemple "rebel" que no la satisfà).

A continuació explicarem tres conjectures més. Les dues primeres han estat escollides per tenir un enunciat molt senzill i la darrera per la seva trascendència.

7.1 Conjectura de Gilbreath

Partim de la seqüència de nombres primers,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$$

i considerem les diferències entre dos termes consecutius de la mateixa,

$$1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, \ldots$$

A continuació prenem les diferències, en valor absolut, entre dos termes consecutius de la darrera seqüència:

$$1, 0, 2, 2, 2, 2, 2, 2, 4, 4, \ldots$$

Si apliquem reiteradament aquest mateix procediment a la seqüència resultant en cada pas, obtenim

2	3	5	7	11	13	17	19	23	29	31	37	
1	2	2	4	2	4	2	4	6	2	6		
1	0	2	2	2	2	2	2	4	4			
1	2	0	0	0	0	0	2	0				
1	2	0	0	0	0	2	2					
1	2	0	0	0	2	0						
1	2	0	0	2	2							
1	2	0	2	0								
1	2	2	2									
1	0	0										
1	0											
1												

Hi observeu alguna regularitat?

A Norman Gilbreath li va cridar l'atenció que totes les seqüències, llevat de la primera, comencessin per 1. El fet que aquesta regularitat es mantingués per més primers que agafés en la seqüència base, és a dir, per més files que afegís, li va dur a conjecturar, l'any 1953, que totes les noves files comencen per 1. Segons recull la història (vegeu [10]), aquesta observació ja havia estat feta, l'any 1878, per en François Proth, qui havia cregut haver aconseguit la seva demostració, però va resultar ser incorrecta. L'any 1993, Andrew Odlyzko va verificar la conjectura en el cas de prendre, com a seqüència de partida, tots els nombres primers $< 10^{13}$, fet que duu a calcular de l'ordre de $3 \cdot 10^{11}$ files.

I com s'ho va fer per comprovar-ho?

Va trobar una 'drecera', per estalviar-se còmputs, en adonar-se'n de que si alguna fila començava per un 1 seguit només per (k) 0's i 2's llavors les (k) noves files també comencen per 1 (vegeu [6]).

7.2 Conjectura de Goldbach

En la novel·la *El tío Petros y la conjetura de Goldbach*, escrita per Apostolos Doxiadis [11], el protagonista, un matemàtic fictici anomenat Petros Papachristos, li planteja al seu nebot, qui aleshores volia seguir els passos del seu oncle i estudiar matemàtiques, que demostri el següent enunciat:

Tot nombre parell major que 2 *pot escriure's com a suma de dos nombres primers.*

Així, per exemple,

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7 = 5 + 5,\ \ldots$$

El nebot de Petros, qui desconeixia que aquest enunciat, d'aparença innocent, corresponia a la difícil conjectura de Goldbach, es va passar tot un estiu barallant-se amb ella, sense èxit, com a molts altres els hi ha succeït des de que fou formulada per Christian Goldbach l'any 1742.

La conjectura de Goldbach ha estat verificada per a tots els nombres parells $\leq 1{,}5 \cdot 10^{18}$ (Tomás Oliveira, 2009; vegeu [16]). En d'altres ciències una tal "evidència numèrica" possiblement bastaria per acceptar-la com a llei, però en matemàtiques no! En la Figura 3 mostrem la gràfica de la funció $P(n)$ que compta el nombre de particions d'un nombre parell $n > 2$ com a suma de dos nombres primers (per exemple, $P(10) = 2$ ja que $10 = 3+7 = 5+5$). La gràfica de la dreta, corresponent als 10000 primers valors de n parell, ens

permet veure una certa tendència global. Així mateix, ens recorda a la forma d'un cometa (batejat com a cometa de Goldbach; vegeu [10, 22]).

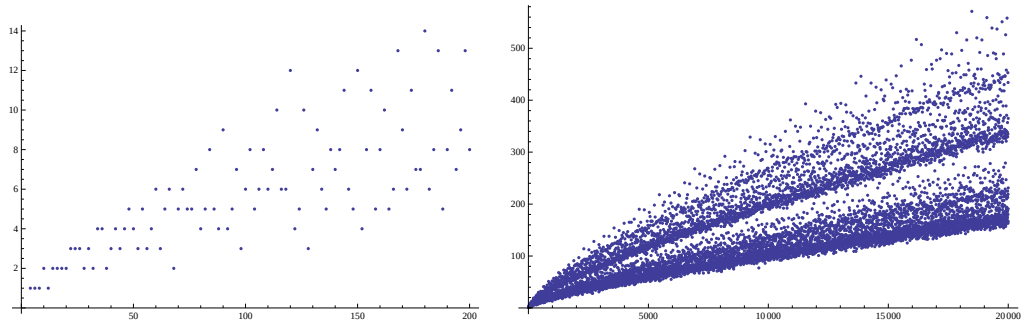

Figura 3: Gràfica del nombre de particions d'un enter parell n com a suma de dos nombres primers, per a $n \leq 2 \cdot 10^2$ (figura esquerra) i $n \leq 2 \cdot 10^4$ (figura dreta).

7.3 Hipòtesi de Riemann

Aquesta tercera conjectura és la més difícil d'exposar i, al mateix temps, la més trascendent[19] per les repercusions que tindria la seva resolució. Sort en tenim que en Marcus du Sautoy, professor de matemàtiques de la Universitat de Oxford i expert divulgador de les mateixes, ens ajuda a imaginar, a través del seu apassionant llibre *La música de los números primos* (vegeu [12]), el nou "paisatge" descobert per en Riemman, i a entendre la seva relació amb la "música" dels nombres primers.

Riemann[20] va idear una fórmula $R(n)$, prou complicada i que podeu consultar a [20], que permetia aproximar la funció de distribució dels nombres primers, $\pi(n)$, amb una precisió major que la donada per la coneguda expressió $n/\ln n$. I va descobrir que els errors de la seva nova estimació estaven

[19] És un dels set "problemes del mil·leni", la resolució del qual comportaria un premi, d'un mil·lió de dòlars, ofert pel *Clay Mathematics Institute* (vegeu [7]).

[20] Bernhard Riemann, matemàtic alemany (1826-1866) va realitzar contribucions molt rellevants en el camp de l'anàlisi i la geometria diferencial. Va escriure un únic article sobre teoria de nombres, el qual ha esdevingut clau pel desenvolupament de l'anomenada teoria analítica de nombres.

íntimament lligats amb el comportament de la funció

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

anomenada *funció zeta de Riemann*. Podem pensar $\zeta(s)$ com el valor al qual tendim a mesura que anem sumant més termes de dita suma infinita, anomenada *sèrie*, en cas que tal límit existís, és a dir, si la sèrie és convergent.

Observem que en el cas $s = 1$ obtenim la sèrie

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots,$$

anomenada *harmònica*, la suma de la qual és infinit ja que, tot i lentament, les seves sumes parcials arriben a superar qualsevol fita,

$$1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \geq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots$$

Vegem com en aquesta primera suma hi contribueixen tots els nombres primers,

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \cdots = (1 + \frac{1}{2} + \frac{1}{2^2} + \cdots)(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots) \ldots$$

Tenint en compte que la sèrie $1 + x + x^2 + \cdots$, anomenada *geomètrica*, té per suma $1/(1-x)$, si $|x| < 1$, resulta

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \text{ primer}} \frac{1}{1 - \frac{1}{p}}.$$

Indiquem que la infinitud dels nombres primers pot també deduir-se del fet que $\zeta(1) = \infty$, com Euler ja s'havia adonat. Emprant el teorema fonamental de l'aritmètica, Euler (1737) va demostrar la relació

$$\zeta(s) = \prod_{p \text{ primer}} \frac{1}{1 - p^{-s}}, \text{ si } s > 1,$$

anomenada *fórmula del producte*. Riemann va tenir la brillant idea d'extendre la definició de la funció zeta per als *nombres complexos*[21] i va mostrar com el coneixement dels zeros (no trivials) de $\zeta(s)$ permetria ajustar

[21] Nombres de la forma $z = x + iy$, on $x = \text{Re}(z)$ (part real) i $y = \text{Im}(z)$ (part imaginària) són nombres reals i i és l'anomenada *unitat imaginària* definida com $i = \sqrt{-1}$ (podem pensar els nombres complexos com a punts del pla amb els quals s'opera mitjançant una determinada aritmètica, coherent amb la dels nombres reals).

la seva fórmula $R(n)$ al valor exacte de $\pi(n)$ (vegeu la Figura 4). Tots els zeros de $\zeta(s)$ es troben en la franja $0 < \mathrm{Re}(s) < 1$, llevat dels valors $\zeta = -2, -4, -6, \ldots$ (anomenats zeros trivials). Riemann va conjecturar que tots els zeros no trivials de la funció $\zeta(s)$ es troben sobre la recta $\mathrm{Re}(s) = \frac{1}{2}$, afirmació que ha rebut el nom d'*hipòtesi de Riemann* i que ha esdevingut un dels problemes oberts més rellevants de la matemàtica. Segons la descripció poètica que ens fa Marcus du Sautoy [12], la correctesa de la hipòtesi de Riemann significaria que l'orquesta que toca la música dels nombres primers té una armonia perfecta (cap de les notes tindria un so més alt que les altres ja que els sons correspondrien als zeros i la seva intensitat al valor de la seva part real, la mateixa per a tots).

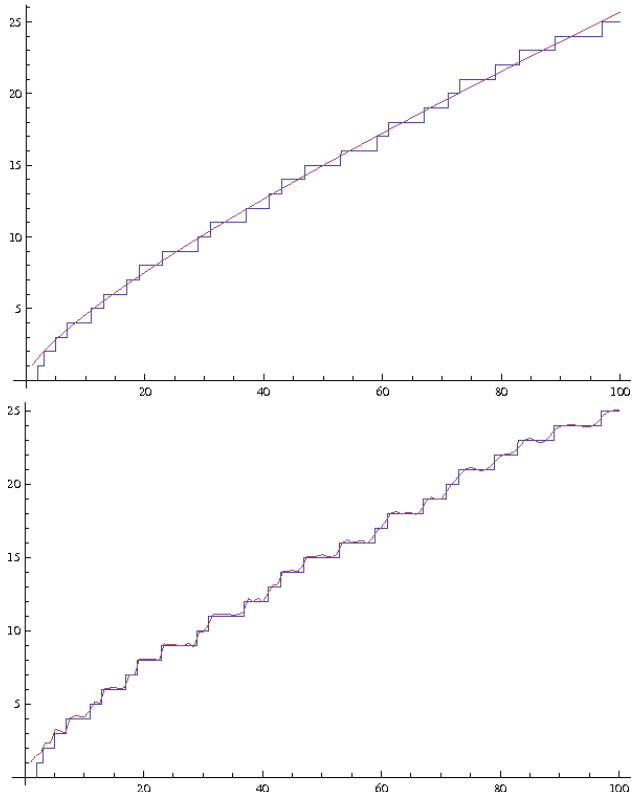

Figura 4: Aproximació de la funció $\pi(n)$ per mitjà de la funció de Riemann $R(n)$, sense corregir (gràfic de dalt) i corregida emprant els 50 primers zeros de la funció zeta (gràfic de baix). Aquests gràfics han estat generats emprant un *notebook* del *Mathematica* creat per en Robert Baillie (vegeu [20]).

8 Quins són els nombres primers més grans que es coneixen?

A mitjans dels anys 90, del segle passat, la major part dels rècords, pel que fa a la troballa de nombres primers, varen ser establerts per en David Slowinski i Paul Gage utilitzant un superordinador Cray. El seu rècord de l'any 1996 corresponia al nombre primer $2^{1257787} - 1$, amb 378632 xifres. Aquest mateix any, l'informàtic George Woltman va engegar un projecte col·laboratiu en xarxa, anomenat *The Great Internet Mersenne Prime Search* (GIMPS, vegeu [14]), amb l'objectiu d'aconseguir nous rècords de primers de la forma $2^p - 1$, anomenats primers de Mersenne. Es tractava de distribuir la feixuga cerca computacional entre l'extensa xarxa de PC's cedits, en el seu temps d'inactivitat, pels milers de voluntaris integrants del projecte. La raó de cercar primers de Mersenne rau en el coneixement d'un test de primalitat molt ràpid per a aquesta família de nombres, conegut com a *test de Lucas-Lehmer*.

En la taula següent, treta de [6], hi figuren els tres nombres primers més grans que es coneixen:

primer	**núm. dígits**	**Qui el va trobar?**	**Quan?**
$2^{43112609} - 1$	12 978 189	Smith, Woltman, Kurowski et al. [GIMPS]	agost 2008
$2^{42643801} - 1$	12 837 064	Strindmo, Woltman, Kurowski et al. [GIMPS]	juny 2009
$2^{37156667} - 1$	11 185 272	Elvenich, Woltman, Kurowski et al. [GIMPS]	setembre 2008

8.1 Nombres primers de Mersenne

Un *nombre primer de Mersenne* és un nombre primer de la forma $2^p - 1$. Així, per exemple,

p	2	3	5	7
$M_p = 2^p - 1$	3	7	31	127

són tots nombres primers de Mersenne.

En l'anterior taula hem posat únicament nombres de la forma 2^p-1, essent l'exponent p primer, ja que de la igualtat

$$2^{a\cdot b}-1=(2^a-1)(1+2^a+2^{2a}+\cdots+2^{a(b-1)})$$

es dedueix que si n és un nombre compost aleshores 2^n-1 també ho és i, per tant, si volem cercar nombres primers de Mersenne ho hem de fer prenent exponents primers. Ara, sembla natural preguntar-se si per a tot primer p, el nombre 2^p-1 es també primer. La resposta és negativa ja que, per exemple, $2^{11}-1=2047=23\cdot 89$ és un nombre compost.

Fent una mica d'història hem de dir que Marin Mersenne va ser un monjo francès qui en la seva obra *Cogitata Physica-Mathematica* (1644) va conjecturar, erròniament, que els nombres de la forma 2^p-1 eren primers per a $p=2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127$ i 257, i que per als altres valors de $p<258$ eren compostos. No va ser fins a l'any 1947 que es va poder completar la llista dels nombres primers de Mersenne per a valors de $p<258$ i es va veure que Mersenne s'havia deixat els nombres primers $2^{61}-1$, $2^{89}-1$ i $2^{107}-1$ i, en canvi, s'havia equivocat en dir que $2^{67}-1$ i $2^{257}-1$ eren primers quan en realitat no ho són. El fet que hagin passat tants anys fins que s'ha pogut completar aquesta llista s'explica per la grandària del nombres de Mersenne ja que, per exemple, $2^{257}-1$ té 78 dígits, i perquè encara no s'havien inventat les computadores electròniques.

I, d'on ve l'interès per l'estudi dels nombres de Mersenne?

Els nombres de Mersenne estan estretament lligats amb els anomenats *nombres perfectes*, nombres que ja varen ser estudiats pels antics grecs i més concretament pels Pitagòrics. Un nombre es diu que és *perfecte* si és igual a la suma de tots els seus divisors llevat d'ell mateix. Així,

$$\begin{aligned}
6 &= 1+2+3\\
28 &= 1+2+4+7+14\\
496 &= 1+2+4+8+16+31+62+124+248\\
8128 &= 1+2+4+8+16+32+64+127+254+508\\
&\qquad +1016+2032+4064
\end{aligned}$$

són els quatre primers nombres perfectes.

Quina relació hi ha entre els nombres perfectes i els nombres primers de Mersenne?

Observeu, en primer lloc, que els nombres perfectes 6, 28, 496 i 8128 es factoritzen de la manera següent:

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 28 &= 2^2 \cdot 7 \\ 496 &= 2^4 \cdot 31 \\ 8128 &= 2^6 \cdot 127. \end{aligned}$$

Hi veieu alguna mena de "patró comú"a tots aquests nombres? Doncs, si us fixeu veureu que tots ells són de la forma $2^{p-1} \cdot (2^p - 1)$, essent $2^p - 1$ un nombre primer de Mersenne. De fet Euler va demostrar, vegeu [18], que tot nombre perfecte i parell és de la forma $2^{p-1} \cdot (2^p - 1)$, essent $2^p - 1$ un nombre primer. Molt abans, Euclides havia provat que si $2^p - 1$ és un nombre primer, aleshores $2^{p-1} \cdot (2^p - 1)$ és un nombre perfecte parell. Veiem com fer-ho. Si $2^p - 1$ és un nombre primer els divisors de $2^{p-1}(2^p - 1)$ diferents d'ell mateix són:

$$\begin{gathered} 1, 2, 2^2, \ldots, 2^{p-1}, \\ (2^p - 1), 2(2^p - 1), 2^2(2^p - 1), \ldots, 2^{p-2}(2^p - 1) \end{gathered}$$

i la seva suma és

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^{p-1} + (2^p - 1)(1 + 2 + 2^2 + \cdots + 2^{p-2}) \\ = (2^p - 1) + (2^p - 1)(2^{p-1} - 1) = 2^{p-1}(2^p - 1), \end{aligned}$$

com volíem veure. Per tant, podem dir que el problema de trobar nombres perfectes parells és equivalent al de cercar nombres primers de Mersenne. *I quants nombres perfectes parells hi ha?* En aquests moments només s'han trobat 47 nombres primers de Mersenne i, conseqüentment, només es coneixen 47 nombres perfectes parells. Però, n'hi ha infinits? Es conjectura que sí però encara no s'ha pogut demostrar. Tampoc se sap si hi ha algun nombre perfecte que sigui senar[22]. Com veieu, doncs, ens tornem a trobar amb problemes, fàcils d'enunciar, però que encara no han estat resolts.

Com es pot determinar, donat un nombre primer p, si el nombre de Mersenne $M_p = 2^p - 1$ és primer?

[22] Es coneixen algunes propietats que haurien de satisfer aquests nombres, en cas d'existir, i també s'ha vist que no hi ha cap nombre perfecte senar de menys de 300 dígits.

François Lucas[23] va desenvolupar un test per determinar si un nombre de Mersenne M_p és primer i el va aplicar per a provar que M_{127} ho és. Posteriorment, Derrick Lehmer[24] va simplificar el test de Lucas. Actualment aquesta versió simplificada es coneix com a test de Lucas-Lehmer. Abans de exposar aquest algorisme hem de parlar de la *relació de congruència* definida en el conjunt dels enters.

Donats un nombre enter positiu m i dos nombres enters a i b, direm que a i b són *congruents mòdul* m, i ho denotarem per $a \equiv b \pmod{m}$, si les restes de les divisions enteres de a per m i de b per m són iguals o, equivalentment, si la diferència $a-b$ és un múltiple de m. Per exemple, $18 \equiv 3 \pmod{5}$ ja que la resta de la divisió entera de 18 per 5 és 3.

A continuació, detallem l'*algorisme de Lucas-Lehmer*:

1. Partim d'un nombre primer p i calculem $M = 2^p - 1$.

2. Definim, recursivament, la següent seqüència d'enters:

$$\begin{aligned} r_1 &= 4 \\ r_k &\equiv r_{k-1}^2 - 2 \pmod{M}, \text{ on } 0 \leq r_k < M, \text{ per a } k = 2, 3, \ldots, p-1. \end{aligned}$$

   (Això significa que $r_2 \equiv r_1^2 - 2 \pmod{M}$, $r_3 \equiv r_2^2 - 2 \pmod{M}$, etc.)

3. Si $r_{p-1} \equiv 0 \pmod{M}$, aleshores retornem que M és primer. En cas contrari, retornem que M és compost.

Demostrar la "correctesa d'aquest algorisme", és a dir, provar que realment un nombre de Mersenne $n = 2^p - 1$ és primer si, i només si, així ens ho retorna l'algorisme, requereix tècniques més avançades de la teoria de nombres (consulteu [3]). En quant a la implementació de l'algorisme hem de dir que és molt senzilla si es disposa d'una llibreria de càlcul per enters grans, és a dir, d'un conjunt de programes que permetin fer les operacions aritmètiques (suma, producte, divisió entera, etc.) amb enters de milers de xifres. Els calculadors numèrics i simbòlics, com el *Mathematica* i el *Maple*, permeten treballar amb enters de qualsevol grandària. Ara bé, com es lògic d'esperar, quan més gran és la precisió demanada més gran és el temps de còmput. Com a curiositat direm que la verificació de la primalitat de $M_{42643801}$ va trigar 29 dies en un processador Intel Core2 (vegeu [14]).

[23] François Lucas, matemàtic francès (1842-1891).
[24] Derrick H. Lehmer, matemàtic nord-americà (1905-1991).

9 Tenen els nombres primers aplicacions pràctiques?

Al segle XVII Pierre de Fermat, probablement el matemàtic "amateur"[25] més famós de la història, va demostrar que si p és un nombre primer i a és un nombre enter no divisible per p, aleshores

$$a^{p-1} \equiv 1 \pmod{p}.$$

Aquest resultat, conegut com a "petit teorema de Fermat"[26] , ens diu com reduir el càlcul d'una exponenciació modular quan el mòdul és un nombre primer. Així, per exemple, per calcular 3^{201} mòdul 11, com aquest teorema ens diu que $3^{10} \equiv 1 \pmod{11}$, tenim

$$3^{201} = 3^{10\cdot 20+1} = 3^{10\cdot 20} \cdot 3 = (3^{10})^{20} \cdot 3 \equiv 3 \pmod{11}.$$

Posteriorment, Euler va demostrar una generalització del teorema petit de Fermat. Aquest nou resultat, conegut com a teorema d'Euler, diu que si n és un enter positiu i a és un enter tal que a i n són primers entre ells, aleshores

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

on $\varphi(n)$ s'anomena funció d'Euler i es defineix com el nombre d'enters positius menors o iguals que n i que són primers amb n. Aquests resultats tenen moltes aplicacions dins la pròpia teoria de nombres. Així, per exemple, hi ha "tests de composició"[27] molt ràpids i que es fonamenten en el teorema petit de Fermat (vegeu [3] o el capítol 3 de [4]).

Poc es podien imaginar Fermat i Euler que els seus resultats i, en general, els nombres primers arribessin a tenir, a finals del segle XX, aplicacions tan pràctiques com és la de dissenyar *sistemes criptogràfics*, és a dir, algorismes de xifrat/desxifrat de missatges que permetin la comunicació segura entre

[25] Fermat era advocat de professió.

[26] S'anomena d'aquesta forma per a distingir-ho de la seva famosa conjectura coneguda com a "teorema últim de Fermat" que afirma que l'equació $x^n + y^n = z^n$ no té solucions enteres amb $x \cdot y \cdot z \neq 0$ per a $n > 2$. La búsqueda d'una demostració d'aquesta conjectura ha ocupat a molts matemàtics i, conseqüentment, ha suposat un gran avenç en la teoria de nombres. Finalment ha estat demostrada per Andrew Wiles (1995).

[27] Un test de composició verifica si un nombre enter satisfà un conjunt de condicions necessàries per tal que sigui primer, de manera que si alguna d'elles no la compleix, aleshores ens diu que el nombre és compost.

un emisor i un receptor a través d'un canal insegur, com és de fet una xarxa informàtica. Són moltes les situacions on cal garantir una privacitat (integritat, autentificació, etc.) de la informació transmesa. Així, per exemple, cal tenir un sistema que permiti xifrar el *password* entrat per un usuari des d'un terminal de manera que a un receptor no autoritzat, que hagi capturat el *password* xifrat, li sigui molt difícil obtenir el text en clar, és a dir, el *password* entrat.

Entre els sistemes criptogràfics més emprats avui en dia hi ha el sistema RSA, inventat l'any 1977 per Rivest, Shamir i Adleman. Aquest és un sistema de clau pública, és a dir, un sistema on l'emisor i el receptor tenen cadascun d'ells una clau secreta —que no comparteixen— i una clau que cadascun d'ells fa pública. Aquest sistema, que trobareu descrit en el capítol 4 de [3], es fonamenta justament en el teorema d'Euler. La seva seguretat rau en el fet que computacionalment resulta molt més costós factoritzar un nombre que passar-li un test de primalitat. Aquesta circumstància ha revifat la búsqueda de nous mètodes de factorització i de nous tests de primalitat, de caràcter general, que puguin aplicar-se a nombres de més d'un centenar de xifres.

En quant a la cerca de nombres primers gegants, nombres de més de 10000 xifres, com els descoberts per Slowinski i Gage, cal dir que més que els nombres trobats, que no deixen de ser una simple curiositat matemàtica, és el procés seguit per la seva certificació el que té aplicacions pràctiques. El propi Slowinski diu que el seu test representa una veritable "tortura" per a l'ordinador que el passa ja que testeja tots els seus components. D'aquí que hagi estat emprat, com una mena de test de control de qualitat, per empreses que construeixen supercomputadors tals com la Cray Research.

Com a resum d'aquest apartat podem dir que la investigació en el camp dels nombres primers i, més en general, de la teoria de nombres constitueix un exemple paradigmàtic de com la matemàtica pura pot esdevenir, molts anys més tard que hagi estat creada, font de moltes aplicacions pràctiques del món real. I, recíprocament, aquestes aplicacions pràctiques poden suggerir noves línies de recerca en matemàtica.

10 Apunt final

Citant al professor Grant Cairns (La Trobe University, Australia), "els nombres primers són una font generosa de preguntes fàcilment formulables", les quals han donat peu a nombroses conjectures, moltes d'elles encara no resol-

tes. Al llarg d'aquesta exposició n'hem fet un petit tast, que desitgem hagi servit per copçar els continuats avenços en el coneixement d'aquests fascinants nombres. Tant de bo els nombres primers tinguessin més presència dins de l'ensenyament de les matemàtiques a l'Escola, tal com molt bé argumenta Cairns en el seu article *Els nombres primers poden tenir més protagonisme a secundària?* (vegeu [5]).

Referències

[1] Agrawal, M., Kayal, N. and Saxena, N. Primes is in P, *Annals of Mathematics* **160** (2) (2004), 781–793.

[2] Aigner, M., Ziegler, G.M. *El libro de las demostraciones*. Nivola, 2005.

[3] Bressoud, D.M. *Factorization and Primality Testing*. Springer-Verlag, 1989.

[4] Burgués, X. *Reconeixement de primers. Implementació del test de primalitat basat en les sumes de Jacobi*. Treball fi de carrera, 1995. Escola Universitària Politècnica (UdL).

[5] Cairns, G., Els nombres primers poden tenir més protagonisme a secundària?, *Butlletí de la Societat Catalana de Matemàtiques* **20** (2) (2005), 75–89.

[6] Caldwell, C.K. *The Prime Pages* [en línia]. [Consultat: 12 d'octubre de 2009]. Disponible a Internet: http://primes.utm.edu/

[7] Clay Mathematics Institute. *Riemann Hypothesis* [en línia]. [Consultat: 8 d'octubre de 2009]. Disponible a Internet: http://www.claymath.org/millennium/Riemann_Hypothesis/

[8] Crandall, R., Pomerance, C. *Prime Numbers: A Computational Perspective*. Springer, 2001.

[9] Davis, P.J., Hersh R. *Experiencia Matemática*. Labor, 1988.

[10] Delahaye, J.P. *Merveilleux nombres premiers*. Belin, 2000.

[11] Doxiadis, A. *El tío Petros y la conjetura de Goldbach*. Ediciones B, 2000.

[12] Du Sautoy, M. *La música de los números primos*. Acantilado, 2007.

[13] Forbes, T. *Prime k-tuples* [en línia]. [Consultat: 6 d'octubre de 2009]. Disponible a Internet: http://anthony.d.forbes.googlepages.com/ktuplets.htm#largest3

[14] Great Internet Mersenne Prime Search [en línia]. [Consultat: 12 d'octubre de 2009] Disponible a Internet: http://www.mersenne.org/

[15] Lang, S. *El placer estético de las matemáticas*. Alianza Universidad, 1992.

[16] Oliveira, T. *Goldbach conjecture verification* [en línia]. [Consultat: 7 d'octubre de 2009]. Disponible a Internet: http://www.ieeta.pt/~tos/goldbach.html

[17] Riesel, H. *Prime Numbers and Computer Methods for Factorization*. Birkhauser, 2a. edició, 1994.

[18] Rosen, K.H. *Elementary Number Theory and its Applications*. Addison-Wesley, 3a. edició, 1993.

[19] Wikipedia contributors. *Goldbach's conjecture* [en línia]. [Consultat: 7 d'octubre de 2009]. Disponible a Internet: http://en.wikipedia.org/wiki/Goldbach's_conjecture

[20] Wolfram MathWorld. *How the Zeros of the Zeta Function Predict the Distribution of Primes* [en línia]. [Consultat: 13 d'octubre de 2009]. Disponible a Internet: http://demonstrations.wolfram.com/HowTheZerosOfTheZetaFunctionPredictTheDistributionOfPrimes/

[21] Wolfram MathWorld. *Prime-Generating Polynomial* [en línia]. [Consultat: 7 d'octubre de 2009]. Disponible a Internet: http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html

[22] Zeleny, E. *Goldbach Comet from The Wolfram Demostrations Project* [en línia]. [Consultat: 7 d'octubre de 2009]. Disponible a Internet: http://demonstrations.wolfram.com/GoldbachComet/

Departament de Matemàtica
Escola Politècnica Superior
Universitat de Lleida
joangim@matematica.udl.cat
http://www.matematica.udl.cat/joan-gimbert

Publicat el 17 de novembre de 2009