Butlletí de la Societat Catalana de Matemàtiques
Vol. 12, núm. 2, 1997. Pàg. 47–58.

Primers rècord*

Paulo Ribenboim

Resum

La teoria dels nombres primers es pot dividir, aproximadament, en quatre recerques principals: Quants nombres primers hi ha? Com es poden generar? Com es poden reconèixer? Com estan distribuïts els primers entre els nombres naturals? Com a resposta a aquestes preguntes, sorgeixen càlculs que poden ser duts a terme per nombres fins a una certa fita. Aquest article recull les fites més grans assolides fins ara —els nombres primers rècord. Altres preguntes sobre primers i els corresponents rècords es poden trobar a [3] o [4].

A tothom l'encanten els rècords. Ens fascinen i fan volar la nostra imaginació. El famós *Llibre Guinness dels Rècords*, del qual s'ha fet una quantitat sorprenent d'edicions, conté molts successos i fets notables i interessants. Sabíeu, per exemple, que el recorregut més llarg ininterromput en bicicleta el va fer Carlos Vieira, de Leiria, Portugal? Durant el període del 8 al 16 de juny de 1983, va pedalejar durant cent noranta-una hores sense parar i va cobrir una distància de 2 407 km. O sabíeu que la pedra més gran mai treta d'un ésser humà pesava 6,29 kg? La pacient era una dona de vuitanta anys, a Londres, l'any 1952. I, més a la vora de les nostres línies usuals d'interès: Hideaki Tomoyoki, nascut a Yokohama el 1932, va dir de memòria quaranta mil dígits de π, una heroica proesa que va requerir disset hores i vint minuts, amb pauses que sumaren quatre hores en total. Fullejant el *Llibre Guinnes*, hom troba poquíssims rècords científics, i encara menys rècords sobre nombres.

Fa un temps vaig escriure *The Book of Prime Number Records* [3], en el qual parlo de les proeses de certs matemàtics en aquest domini tan descuidat pel *Guinness*. Com es va originar aquest llibre és una història que val la pena explicar. La meva universitat em va demanar que fes una xerrada adreçada als estudiants no graduats, i vaig voler buscar un tema que no sols fos comprensible sinó també interessant.

∗ Aquest article està basat en una conferència que l'autor va pronunciar (en francès) el 25 de març de 1987 a l'École Normale Supérieure de París. Se n'ha publicat una versió en alemany en la revista *Didaktik der Mathematik* i dues versions en anglès a *Nieuw Archief voor Wiskunde* i *The College Mathematics Journal*, respectivament. Ara en publiquem la versió catalana, amb les degudes autoritzacions, per desig exprés de l'autor.

Vaig arribar a la idea de parlar sobre nombres primers rècord, ja que el tema dels rècords és ben popular entre els estudiants, en connexió amb els esports. L'interès dels estudiants va sobrepassar tant les meves previsions que vaig resoldre escriure un text monogràfic basat en aquestes conferències. En aquest procés vaig aprendre tants fets i rècords nous que el breu text que havia planificat anava creixent. Gràcies als col·legues que em van facilitar moltes referències útils, al final vaig ser capaç de completar aquest treball.

Haig de confessar que, quan preparava la conferència, jo no en sabia gaire (realment, en sabia molt poc!), dels teoremes sobre primers i nombres primers rècord. Per a mi tots aquests fets, tot i que prou interessants, estaven desconnectats entre si. Semblava que fossin només teoremes aïllats sobre nombres primers, i no estava clar com podien lligar-se per formar una teoria connexa. Perquè, quan hom vol escriure un llibre, la primera feina que cal fer és donar forma al tema en un tot coherent.

El mètode científic pot ser considerat com un procés de dos passos: primer, observació i experimentació —anàlisi—; llavors, formulació de les regles, teoremes i relacions ordenades entre fets —síntesi. Expressada en aquests termes, la meva feina era presentar una síntesi de les observacions conegudes sobre nombres primers, amb un èmfasi en els rècords assolits. Si el meu treball té alguna originalitat, aquesta rau, sens dubte, en la investigació sistemàtica de la interacció entre teoria i càlcul. Aquesta tasca no necessita justificació si hom té present quin és el paper dels nombres primers en la teoria de nombres. Després de tot, el teorema fonamental de la teoria elemental de nombres diu que tot nombre natural $N > 1$ pot ser expressat d'una forma única (excepte l'ordre dels factors) com a producte de primers. Els nombres primers són la pedra fonamental sobre la qual s'aixeca l'estructura de l'aritmètica.

Ara, com m'ho vaig fer per organitzar la teoria dels nombres primers? Vaig començar plantejant quatre preguntes directes i gens ambigües:

1. Quants nombres primers hi ha?
2. Com podem generar primers?
3. Com podem conèixer si un nombre donat és primer?
4. On estan col·locats els primers?

Com veurem, a partir d'aquestes quatre preguntes, tota la teoria dels nombres primers es desenvolupa de manera natural.

1 Quants nombres primers hi ha?

Com és ben conegut, Euclides en els seus *Elements* prova que existeixen infinits primers, procedint com segueix: suposem que només hi ha un nombre finit de primers. Sigui p el més gran nombre primer i P el producte de tots els primers menors o iguals a p; llavors considerem el nombre P més 1:

$$P + 1 = \left(\prod_{q \leq p} q \right) + 1.$$

Tenim dos casos possibles: (a) $P + 1$ és primer, (b) $P + 1$ no és primer. Però si (a) és cert, $P + 1$ seria un nombre primer més gran que p. I si (b) és cert, cap dels primers $q \leq p$ és un factor primer de $P + 1$, i així els factors primers de $P + 1$ són tots més

grans que p. En tots dos casos, la suposició que existeix un nombre primer p màxim duu a una contradicció. Això demostra que deuen existir infinits nombres primers.

A partir d'aquesta demostració indirecta no podem deduir un mètode per a generar nombres primers, però la demostració ens suscita una pregunta: hi ha infinits primers p tals que el corresponent nombre $P+1$ és també primer? Molts matemàtics han dedicat càlculs a aquesta qüestió.

1 RÈCORD $p = 13\,649$ *és el major primer conegut tal que* $P+1$ *és també primer; aquí,* $P+1$ *té* $5\,862$ *dígits decimals. Va ser trobat per H. Dubner el 1987.*

Hi ha moltes altres demostracions de l'existència d'infinits primers; cadascuna revela altres aspectes interessants del conjunt de tots els nombres primers. Euler va demostrar que la suma dels recíprocs dels nombres primers és divergent:

$$\sum \frac{1}{p} = \infty.$$

A partir d'aquí tornem a veure que no hi pot haver només un nombre finit de primers. La demostració d'Euler es pot trobar en molts llibres elementals de teoria de nombres o anàlisi real, com [1], i permet fer una deducció interessant. Per cada $\epsilon > 0$, no importa com sigui de petit, sabem que

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\epsilon}} < \infty.$$

Per tant, els nombres primers estan més junts en la línia de nombres que els nombres del tipus $n^{\epsilon+1}$. Per exemple, els primers estan més junts que els quadrats n^2, per als quals Euler demostra

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Una altra demostració simple i elegant de l'existència d'infinits primers va ser donada per Pólya, que la va aprendre de Hurwitz. N'hi ha prou de trobar una successió infinita $F_0, F_1, F_2, F_3, \ldots$ de nombres naturals relativament primers dos a dos (és a dir, el màxim comú divisor de cada parella és 1); com que cada F_n té com a mínim un factor primer, llavors hi ha infinits nombres primers. És fàcil provar que la successió de nombres de Fermat $F_n = 2^{2^n} + 1$ té aquesta propietat. Clarament, ni F_n ni F_{n+k}, $(k > 0)$ són divisibles per 2; i si p és un factor primer senar de F_n, llavors $2^{2^n} \equiv -1 \mod p$, d'on $2^{2^{n+k}} = (2^{2^n})^{2^k} \equiv 1 \mod p$. Així, $F_{n+k} \equiv 2 \mod p$, i com que $p > 2$, es dedueix que p no divideix F_{n+k}. Dedicaré més atenció als nombres de Fermat després de la secció següent.

2 Generació de nombres primers

El problema és trobar una «bona» funció $f : \mathbb{N} \longrightarrow \{\textit{nombres primers}\}$. Aquesta funció ha de ser fàcil de calcular i, sobretot, ha de ser representable per funcions prèviament ben conegudes. Hom pot imposar condicions addicionals a aquesta funció, com, per exemple:

(*a*) $f(n)$ és igual al n-èsim nombre primer (en l'ordre natural); això significa una «fórmula» per al n-èsim nombre primer.

(*b*) Per a $m \neq n$, $f(m) \neq f(n)$; això significa una funció que genera primers diferents, però no necessàriament tots els primers.

Hom també pot buscar una funció f definida a $\mathbb{N}$, amb valors enters (pero no necessàriament valors positius), que compleixi això.

(*c*) El conjunt de nombres primers coincideix amb el conjunt de valors positius de la funció. Això és una condició molt més fluixa i que es pot complir de maneres inesperades, com veurem.

Per començar, discutirem les fórmules per als nombres primers. N'hi ha moltes! De fet, quan érem més joves, molts de nosaltres buscàvem —sovint amb èxit— una fórmula per al n-èsim nombre primer. Desgraciadament, totes aquestes fórmules tenen un cosa en comú: expressen el n-èsim nombre primer mitjançant funcions dels anteriors primers que són difícils de calcular. Per tant, aquestes fórmules són inútils de cara a deduir propietats dels nombres primers. De totes maneres, donaré com a il·lustració una d'aquestes fórmules, trobada el 1971. Ho faig en honor del seu descobridor, J. M. Gandhi, un matemàtic que va morir molt jove, i que també treballava en el Darrer Teorema de Fermat.[1]

Per simplificar l'expressió de la fórmula, introduirem la funció de Möbius $\mu : \mathbb{N} \longrightarrow \mathbb{Z}$ donada per

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ és un producte de } r \text{ factors primers diferents} \\ 0 & \text{altrament.} \end{cases}$$

Ara, si p_1, p_2, p_3,... és la successió dels nombres primers en ordre creixent, sigui $P_{n-1} = p_1 p_2 ... p_{n-1}$; la fórmula de Gandhi és

$$p_n = \left[1 - \log_2 \left(-\frac{1}{2} + \sum_{d | P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right],$$

on $\log_2$ indica el logaritme en base 2 i $[x]$ denota, com sempre, el més gran enter menor o igual que el nombre real x. Es pot ben veure la dificultat de calcular p_n usant la fórmula de Gandhi!

Ara esbossem la construcció d'una funció que genera nombres primers. E. M. Wright i G. H. Hardy, en el seu famós llibre [1], demostren que si $\omega = 1,9287800...$ i si

$$f(n) = \left[2^{2^{\cdot^{\cdot^{2^{\omega}}}}} \right] \text{ (amb } n \text{ dosos)}$$

llavors $f(n)$ és primer per a tot $n \geq 1$. Així $f(1) = 3$, $f(2) = 13$, i $f(3) = 16\,381$, però $f(4)$ és una mica difícil de calcular i té quasi cinc mil xifres. També, com que el valor exacte de ω depèn del coneixement dels nombres primers, aquesta fórmula, al cap i a la fi, té poc interès.

Hi ha funcions realment simples que generin nombres primers? No n'hi ha pas, de polinòmiques, a causa del següent resultat negatiu:

2 PROPOSICIÓ *Per a tot* $f \in \mathbb{Z}[X_1, ..., X_m]$ *hi ha infinites m-ples d'enters* $(n_1, ..., n_m)$ *per als quals* $|\, f(n_1, ..., n_m) \,|$ *és un nombre compost.*

1 J. M. Gandhi, nascut el 1933, va morir el 23 de gener de 1982, després d'una operació aparentment inofensiva.

Els resultats negatius similars són abundants.

Bé, aleshores, hi ha polinomis amb una *única* indeterminada per als quals molts valors consecutius són primers? Més precisament: sigui q un nombre primer i plantejem-nos de Trobar un polinomi de grau 1, de fet un polinomi del tipus $f_q(x) = dx + q$, els valors del qual en els nombres $0, 1, ..., q-1$ són tots primers. Llavors f_q genera una successió de q nombres primers en progressió aritmètica amb diferència d i valor inicial q. Per a valors petits de q trobem f_q fàcilment:

q	d	Valors	Valors a 0,1,...,$q-1$
2	1	2	3
3	2	3	5 7
5	6	5	11 17 23 29
7	150	7	157 307 ..... 907.

En canvi, no sé demostrar si això és possible per a tot nombre primer q.

3 RÈCORD *L'any 1986, G. Löh dóna els valors mínims de d per a dos primers:*

Per a $q = 11$ $d = 1\,536\,160\,080$
Per a $q = 13$ $d = 9\,918\,821\,194\,590.$

També podem examinar el problema següent: buscar les successions més llargues de primers en progressió aritmètica.

4 RÈCORD *La successió més llarga coneguda de primers en progressió aritmètica té vint-i-dos termes. El primer terme és* $a = 11\,410\,337\,850\,553$ *i la diferència és* $d = 4\,609\,098\,694\,200$ *(Treball coordinat per P. Pritchard, 1993).*

Euler descobrí polinomis quadràtics per als quals molts valors són primers. Va observar que si q és el primer 2, 3, 5, 11, 17 o 41, llavors els valors $f_q(0), f_q(1), \ldots, f_q(q-2)$ del polinomi $f_q(X) = X^2 + X + q$ són primers. (Evidentment, $f_q(q-1) = q^2$ no és primer i, així, aquesta successió de valors primers consecutius és la millor que hom pot esperar.) Per a $q = 41$ aquesta dóna 40 nombres primers: 41, 43, 47, 53, ..., 1 447, 1 523, 1 601.

La pregunta següent és òbvia: podem trobar primers $q > 41$ per als quals els primers $q-1$ valors del polinomi quadràtic d'Euler són tots primers? Si hi ha infinits valors de q, podrem generar successions arbitràriament llargues de primers! En canvi, el teorema següent ens diu que això no pot ser:

5 TEOREMA *Sigui q un nombre primer. Els enters* $f_q(0), f_q(1), \ldots, f_q(q-2)$ *són tots primers si i només si el cos quadràtic imaginari* $\mathbb{Q}(\sqrt{1-4q})$ *té nombre de classes* 1 *(G. Rabinovitch, 1912).*

(Un cos quadràtic K té nombre de classes 1 si tot enter algebraic de K es pot expressar com a producte de primers de K, i dos representacions només difereixen d'una unitat, i. e., un enter algebraic que és divisor d'1 a K.)

6 TEOREMA *Sigui q un nombre primer. Un cos imaginari quadràtic* $\mathbb{Q}(\sqrt{1-4q})$ *té nombre de classes 1 si i només si* $4q - 1 =$ *7, 11, 19, 43, 67 o 163, és a dir,* $q =$ *2, 3, 5, 11, 17 o 41.*

Els cossos quadràtics imaginaris de nombre de classes 1 van ser determinats l'any 1966 per A. Baker i H. M. Stark, independentment i sense cap dels dubtes que suscitava el treball més antic de Heegner del 1952.

Així s'ha aconseguit el següent rècord immillorable:

7 RÈCORD $q = 41$ *és el nombre primer més gran per al qual els valors* $f_q(0)$, $f_q(1)$, $\ldots$, $f_q(q-2)$ *del polinomi* $f_q(X) = X^2 + X + q$ *són tots primers.*

Cal mencionar que en la solució d'aquest problema d'aparença inofensiva ha calgut utilitzar una teoria força sofisticada. Els detalls són donats en un altre article [2].

Ara tornem a alguns polinomis, els valors positius dels quals coincideixen amb el conjunt de nombres primers. L'increïble fet que tals polinomis existeixen va ser descobert el 1971 per Yu. V. Matijasevič en connexió amb el desè problema de Hilbert. Aquí tenim els rècords, que depenen del nombre d'incògnites n i el grau d del polinomi:

8 RÈCORD

n	d	*Any*
21	21	1971 *Yu. V. Matijasevič (no explícit).*
26	25	1976 *J. P. Jones, D. Sato, H. Wada i D. Wiens.*
42	5	1976 *Jones et al. (no explícit): mínim d.*
10	$\sim 1{,}6 \times 10^{48}$	1978 *Yu. V. Matijasevič (no explícit): mínim n.*

No se sap si els valors mínims de n i d són 10 i 5, respectivament.

3 Reconeixement dels nombres primers

Donat un nombre natural N, és posible determinar amb un nombre finit de càlculs si N és un primer? Sí! N'hi ha prou de dividir N per tots els primers d amb $d^2 < N$. Si la resta sempre és diferent de zero, llavors N és primer. La dificultat d'aquest mètode rau en el fet que un N gran requereix un gran nombre de càlculs. El problema, per tant, és trobar un algorisme A on el nombre de càlculs és acotat per una funció f_A del nombre de dígits de N, així $f_A(N)$ no creix gaire ràpid amb N. Per exemple, si $f_A(N)$ fos una funció polinòmica del nombre de dígits binaris de N, que és $1 + [\log_2(N)]$. Essencialment, aquest nombre és proporcional al logaritme natural $\log N$, ja que $\log_2(N) = \log N / \log 2$.

Aquest problema és obert —nosaltres no sabem si un tal algorisme polinomial existeix. D'una banda, no podem provar la impossibilitat de la seva existència; de l'altra, un tal algorisme encara no s'ha trobat. Els esforços en aquesta direcció han produït diversos algorismes de test de primalitat. Segons el punt de vista, poden classificar-se com segueix:

- Algorismes per a nombres arbitraris.
- Algorismes per a nombres d'un tipus especial.

- Algorismes que estan totalment justificats per teoremes.
- Algorismes que estan basats en conjectures.

- Algorismes deterministes.
- Algorismes probabilístics.

Per tal d'aclarir aquestes nocions, vegem-ne alguns exemples.

Un algorisme aplicable a nombres arbitraris és el de G. L. Miller (1976), la complexitat del qual pot estimar-se només amb l'ajut de la conjectura generalitzada de Riemann. Suposant aquesta conjectura, per a l'algorisme de Miller l'estimació $f_A(N) \leq C(\log N)^5$ és vàlida, on C és una constant positiva. Així aquest és un algorisme, la velocitat de creixement polinomial del qual resta incerta. Per contra, l'algorisme de L. M. Adleman, C. Pomerance, i R. S. Rumely (1983) té completament assegurada l'estimació de complexitat, i el nombre de càlculs d'operacions com una funció del nombre de dígits binaris de N és fitat per $(\log N)^{C \log\log\log N}$, on C és una constant. La complexitat és, per tant, a la pràctica, propera a la polinomial, i aquest algorisme es pot aplicar a un enter arbitrari N.

Aquests dos algorismes són deterministes, diferents dels que descriuré ara. Primer, he d'introduir els anomenats nombres pseudoprimers. Sigui $a > 1$ un enter. Per a tot primer p que no divideix a, el Petit Teorema de Fermat diu que $a^{p-1} \equiv 1 \mod p$. Però és molt possible que un nombre $N > 1$ amb $a^{N-1} \equiv 1 \mod N$ sigui compost —en aquest cas direm que N és *pseudoprimer per la base a*. Per exemple, 341 és el més petit pseudoprimer per la base 2. Tota base a té infinits pseudoprimers. Entre aquests, alguns compleixen una condició de congruència addicional i s'anomenen *pseudoprimers forts per la base a*; també n'hi ha una quantitat infinita.

Un algorisme s'anomena *test probabilístic per a nombres primers* si en aplicar-lo a un nombre N porta, o bé a la conclusió que N és compost, o bé a la conclusió que amb molta probabilitat N és un nombre primer. Entre els tests d'aquest tipus podem incloure els de R. Baillie i S. S. Wagstaff (1980) i M. O. Rabin (1980). En aquests tests hom examina certs «testimonis». Sigui $k > 1$ (per exemple $k = 30$) i siguin $a_1 = 2$, $a_2 = 3$, ..., a_k, primers que serviran com a «testimonis». En el cas que algun testimoni deixi de complir la condició $a_j^{N-1} \equiv 1 \mod N$, aleshores N és, amb tota seguretat, compost. Si, per a tot testimoni a_j, l'anterior congruència és certa (és a dir, si N és pseudoprimer per la base a_j per $j = 1, 2, ..., k$) llavors N és, amb molta probabilitat, un nombre primer. El test de Rabin és semblant, fa servir més congruències restrictives, que condueixen a millors probabilitats. Aquest test porta a la conclusió que N, o és certament compost, o és primer amb probabilitat $1 - (1/4^k)$. Per a $k = 30$, llavors, el test dóna un resultat fals només un cop de cada 10^{18} valors de N. Aquests tests probabilístics són clarament molt fàcils d'aplicar.

Ara tornem al test de nombres primers aplicables a nombres del tipus $N \pm 1$, on molts, si no tots els factors de N, són coneguts. Els tests per a $N + 1$ depenen d'un recíproc feble, degut a Pepin, del Petit Teorema de Fermat, mentre que els de $N - 1$ fan servir la successió de Lucas.

El 1877 Pepin va demostrar que els nombres de Fermat $F_n = 2^{2^n} + 1$ són primers si i només si $3^{(F_n-1)/2} \equiv -1 \mod F_n$. La recerca de primers entre els nombres de Fermat ha produït diversos rècords.

9 RÈCORD *El més gran nombre de Fermat que se sap que és primer és* $F_4 = 65\,537$.

10 RÈCORD F_{11} *és el mes gran nombre de Fermat del qual es coneixen tots els factors primers (R. P. Brent i F. Morain, 1988).*

11 RÈCORD *$F_{23\,471}$ és el més gran nombre de Fermat que se sap que és compost; té el factor* $5 \times 2^{23\,473} + 1$ *(W. Keller, 1984).*

12 RÈCORD *F_{22} és el més petit nombre de Fermat que encara no s'ha demostrat si és primer o compost.*

Per als nombres de Mersenne, $M_q = 2^q - 1$, amb q un primer, hom aplica el test de Lucas (1878): sigui $S_0 = 4, S_{k+1} = S_k^2 - 2$, per $k \geq 0$. Llavors M_q és primer si i només si M_q és un divisor de S_{q-2}. Aquest test ha fet possible descobrir primers molt grans.

13 RÈCORD *Fins ara, es coneixen trenta-tres primers de Mersenne. El primer de Mersenne més gran conegut ara és M_q per $q = 859\,433$, un nombre l'expressió decimal del qual té* $258\,716$ *dígits. Va ser trobat amb un ordinador Cray per D. Slowinski el 1993.*

Els següents primers de Mersenne més petits són M_q per $q = 756\,839$, $q = 216\,091$, i $q = 132\,049$ (tots trobats per Slowinski). A aquests nombres tan grans no se'ls podria pas aplicar el test de nombre primer si no fos per la seva forma especial.

14 RÈCORD *El més gran nombre de Mersenne compost conegut és M_q per $q = 39\,051 \times 2^{6\,001} - 1$ (W. Keller, 1987).*

Durant molts anys —des del 1876, quan E. Lucas va demostrar que M_{127} era primer, fins al 1989— el títol *nombre primer més gran* ha estat sempre atorgat a un nombre primer de Mersenne. Això va tornar a ser cert el 1992, però en els tres anys intermedis van regnar altres campions:

15 RÈCORD *El més gran nombre primer conegut fins ara que no és un primer de Mersenne és* $391\,581 \times 2^{216\,193} - 1$. *Aquest descobriment l'hem d'agrair a sis matemàtics; en ordre alfabètic invers (i per què no?) ells són S. Zarantonello, J. Smith, G. Smith, B. Parady, L. C. Noll i J. Brown.*

4 La distribució dels nombres primers

Fins ara sabem el següent:

1. Hi ha infinits nombres primers.
2. No hi ha cap fórmula raonablement simple per als nombres primers.
3. Hom pot determinar quan un nombre donat és primer, si no és molt gran.

Què podem dir sobre la manera com els nombres primers estan distribuïts entre els nombres naturals? Més amunt he donat ja algun indici en aquesta línia, en connexió amb la demostració d'Euler de l'existència d'infinits primers: els primers estan més junts que, per exemple, els quadrats. Una manera prou simple de discutir la distribució dels nombres primers és comptar el nombre de primers menors que un nombre donat. Per a tot real $x > 0$, sigui $\pi(x) = |\ \{\text{nombres primers} p \mid p \leq x\}\ |$. Així π és la funció que compta els nombres primers. Per tenir una bona idea del comportament de π podem comparar-la amb funcions senzilles. Aquesta aproximació porta a resultats de naturalesa asimptòtica.

Quan només tenia quinze anys, C. F. Gauss va conjecturar, a partir de l'estudi de taules de nombres primers, que

$$\pi(x) \sim \frac{x}{\log x}.$$

És a dir, el límit del quocient

$$\frac{\pi(x)}{x/\log x}$$

quan $x \to \infty$ existeix i val 1. Una formulació equivalent és

$$\pi(x) \sim \int_0^x \frac{dt}{\log t},$$

on $\int$ denota el valor principal de Cauchy. La funció de la dreta s'anomena la integral logarítmica i es denota per Li. L'afirmació de Gauss fou provada el 1896 per J. Hadamard i C. de la Vallée Poussin; prèviament, P. L. Chebyshev va demostrar que el valor del límit, si existia, havia de ser 1.

Aquest teorema està entre els resultats més significatius de la teoria de nombres primers i, per aquesta raó, s'acostuma a anomenar *Teorema dels Nombres Primers*. En canvi, aquest teorema, òbviament, no diu res sobre el valor exacte de $\pi(x)$. Sobre això tenim la famosa fórmula que D. F. E. Meissel va trobar el 1871, que expressa el valor exacte de $\pi(x)$ en termes de $\pi(y)$ per a tot $y \leq x^{2/3}$ i els nombres primers $p \leq x^{1/2}$.

16 RÈCORD *El més gran enter N per al qual $\pi(N)$ ha estat calculat exactament és $N = 10^{17}$ (per M. Deleglise, 1992). El valor és $\pi(10^{17}) = 2\,623\,557\,157\,654\,232$.*

Les diferències

$$\left|\pi(x) - \frac{x}{\log x}\right| \qquad \text{i} \qquad |\pi(x) - Li(x)|$$

no estan acotades quan $x \to \infty$. Avaluar aquests termes d'error tan exactament com sigui possible és d'enorme importància en aplicacions del Teorema dels Nombres Primers. Basant-se en taules, primer es va conjecturar, i després es va provar (J. B. Rosser i L. Schoenfeld, 1962) que, per a tot $x \geq 17$, $x/\log x \leq \pi(x)$. Això és interessant perquè, per contra, la diferència $Li(x) - \pi(x)$ canvia de signe infinits cops, com J. E. Littlewood (1914) va demostrar. El 1933, S. Skewes demostra que la diferència $Li(x) - \pi(x)$ és negativa per cert x_0 amb $x_0 \leq e^{e^{e^{7.7}}}$. De fet, però, aquest canvi de signe té lloc molt abans:

17 RÈCORD *El més petit x_0 per al qual $Li(x) - \pi(x)$ és negatiu és més petit que $6,69 \times 10^{370}$ (H. J. J. te Riele, 1986).*

La funció més important per a l'estudi de la distribució dels primers és la *funció zeta* de Riemann: per a tot nombre complex s amb $Re(s) > 1$, la sèrie $\sum_{n=1}^{\infty} 1/n^s$ és absolutament convergent; també és uniformement convergent en tot semiplà $\{s \mid Re(s) > 1 + \epsilon\}$ per a tot $\epsilon > 0$. La funció ζ així definida es pot estendre per continuació analítica a una funció meromorfa definida en tot el pla complex,

amb un únic pol. El pol és en el punt $s = 1$, té ordre 1, i el residu és 1. Fou l'estudi de les propietats d'aquesta funció el que finalment va proporcionar la demostració del Teorema dels Nombres Primers. La funció ζ té zeros a -2, -4, -6, ..., com pot demostrar-se fàcilment amb l'ajut de l'equació funcional que satisfà ζ. Tots els altres zeros de ζ són nombres complexos $\sigma + it$ (t real) amb $0 < \sigma < 1$.

La hipòtesi de Riemann, que encara no ha estat provada, diu: els zeros no trivials de la funció zeta de Riemann estan collocats a la recta crítica $1/2 + it$ (t real). Sense entrar en detalls, observem només que molts teoremes sobre la distribució dels nombres primers poden ser provats assumint com a certa la hipòtesi de Riemann. És, per tant, d'una importància fonamental determinar els zeros no trivials de ζ. Per motius de simetria, n'hi ha prou de determinar els zeros amb $t > 0$, els quals poden ser enumerats en una successió $\sigma_n + it_n$, on $t_n \leq t_{n+1}$ i en el cas $t_n = t_{n+1}$ necessitem $\sigma_n \leq \sigma_{n+1}$. (Primer cal demostrar que, com a màxim, hi ha un nombre finit de zeros de ζ, per a cada valor de t.)

18 RÈCORD *Per a $n \leq 1\,500\,000\,001$ tots els zeros $\sigma_n + it_n$ de la funció zeta de Riemann es troben a la recta crítica; és a dir, $\sigma_n = 1/2$. Aquests càlculs van ser realitzats el 1986 per J. van de Lune, H. J. J. te Riele, i D.T. Winter.*

19 RÈCORD *El 1974, N. Levinson demostrà que almenys un terç dels zeros de la funció zeta de Riemann són a la recta crítica, i el 1989 J. B. Conrey millorà aquest resultat, reemplaçant $1/3$ per $2/5$.*

Les consideracions anteriors es basen en el comportament asimptòtic de la funció π i en la funció ζ, que és molt útil per a estimar els termes d'error. Podem dir que tracten de l'estimació de π «a l'infinit». A continuació tornem al comportament *local* de π —estimant els intervals entre els nombres primers. Aquí la pregunta fonamental és: coneixent el n-èsim primer p_n, com podem trobar el següent primer p_{n+1}? Així, ens interessem en la successió de diferències $d_n = p_{n+1} - p_n$. És fàcil demostrar que lim sup $d_n = \infty$, és a dir, que existeixen blocs de llargada arbitrària de nombres consecutius compostos. Aquí en tenim un: per a tot N, els N nombres consecutius

$$(N+1)! + 2, (N+1)! + 3, \ldots, (N+1)! + (N+1)$$

són compostos. Alguns matemàtics s'han divertit trobant els blocs més llargs de nombres compostos consecutius entre primers relativament petits —els «forats» més amples entre aquests primers.

20 RÈCORD *L'interval més gran entre nombres primers que ha estat calculat efectivament consisteix en els 863 nombres compostos que segueixen el primer*

$$p = 6\,505\,941\,701\,960\,039$$

(no publicat, comunicat a l'autor el 1993, per S. Weintraub).

La pregunta sobre grans forats entre primers no massa grans es pot fer més exacta. Fixem-nos en la successió d'intervals relatius d_n/p_n. Ja el 1845, J. Bertrand va postular, a partir de l'estudi de taules, que sempre hi ha un primer entre p_n i $2p_n$. Chebyshev va ser el primer a demostrar aquest resultat, el qual es podia escriure en

la forma $p_{n+1} < 2p_n$ o, millor, $d_n/p_n < 1$. Aquest resultat, tot i que és prou divertit, és més dèbil que el que es pot deduir usant el Teorema dels Nombres Primers:

$$\lim_{n\to\infty} \frac{d_n}{p_n} = 0.$$

La teoria d'intervals entre nombres primers ha portat a la conjectura següent: per a tot $\epsilon > 0$ la desigualtat $p_{n+1} < p_n + p_n^{1/2+\epsilon}$ és certa per a tot n prou gran.

21 RÈCORD *El rècord actual, l'últim d'una llarga llista, es deu al treball de C. J. Mozzochi, el 1986:* $p_{n+1} < p_n + p_n^{1/2+11/20-1/384}$.

Què sabem del límit inferior de la successió de diferències d_n? Els dos nombres primers p i p' ($p < p'$) s'anomenen *primers bessons* si $p' - p = 2$. Encara no sabem si hi ha infinits primers bessons o no, és a dir, lim inf $d_n = 2$. La qüestió és delicada. El 1919 V. Brun demostrà que la suma sobre totes les parelles de primers bessons

$$\sum \left(\frac{1}{p} + \frac{1}{p+2} \right) = B < \infty.$$

Es dedueix que, si hi ha infinits primers bessons, com esperem que sigui el cas, estan força dispersos. El 1976, la constant de Brun va ser calculada per R. P. Brent: $B = 1,90216054$.

22 RÈCORD *La parella de primers bessons més gran que es coneix és* $1\,706\,595 \times 2^{11\,235} \pm 1$. *La parella fou descoberta el 1990 per B. K. Parady, J. F. Smith, i S. Zarantonello, que formen part dels «sis d'Amdahl», el mateix grup que posseeix actualment el rècord del primer més gran que no és de Mersenne.*

5 Conclusió

Per tal de no allargar massa aquesta presentació, he hagut de deixar de banda moltes qüestions fascinants, com ara el comportament dels primers en progressió aritmètica, o la conjectura de Goldbach. Per sort, aquests i molts altres fets han estat recollits i àmpliament explicats en un llibre [4] que està esperant ser llegit! Acabaré amb dues curiositats que podeu incloure en el vostre repertori.

Una *repunitat* és un enter del tipus $R_n = 111\ldots1$, amb n dígits decimals iguals a 1. No sabem si hi ha infinites repunitats primeres, però tenim el rècord següent.

23 RÈCORD *H. C. Williams i H. Dubner demostren, el 1986, que* $R_{1\,031}$ *és un nombre primer.*

Només es coneixen quatre repunitats més que són primeres: R_2, R_{19}, R_{23} i R_{317}.

Finalment, ofereixo un darrer rècord notable —però, si voleu saber com i per què va ser trobat, heu de preguntar-ho a H. Dubner, que el va anunciar el 1988.

24 RÈCORD *El més gran nombre primer conegut, els dígits del qual són tots primers és*

$$7\,532 \times \frac{10^{1\,104} - 1}{10^4 - 1} + 1.$$

L'observació i l'estudi dels nombres primers és una activitat fructífera i, ensems, distreta. Els matemàtics hi troben una font de diversió, i això sol ja en justifica la feinada. Arriba un moment que considerem els nombres primers com a amics —amics que ens duen problemes!

Referències

[1] HARDY, G. H., WRIGHT, E. M. *An Introduction to the Theory of Numbers*. 4a ed. Oxford: Clarendon Press, 1960.

[2] RIBENBOIM, P. «Euler's famous prime generating polynomial and the class number of imaginary quadratic fields». *L'Enseignement Mathématique*. 34 (1988), p. 23–42.

[3] RIBENBOIM, P. *The Book of Prime Number Records*. 2a ed. New York: Springer, 1989.

[4] RIBENBOIM, P. *The Little Book of Big Primes*. New York: Springer, 1991.

DEPARTMENT OF MATHEMATICS
QUEEN'S UNIVERSITY
KINGSTON, ONTARIO K7L 3N6
CANADA
mastdept@qucdn.queensu.ca