Butlletí de la Societat Catalana de Matemàtiques
Vol. 33, núm. 1, 2018. Pàg. 57–80. DOI: 10.2436/20.2002.01.80

Els primers, desvelats

Xavier Xarles

Resum: L'objectiu principal de l'article és introduir de manera informal un punt de vista probabilístic en la distribució dels números primers, que podria explicar per què algunes de les conjectures més conegudes sobre els primers són certes. També presentem algunes idees que expliquen per què aquesta aproximació reflecteix en certa manera l'autèntica distribució dels primers. Pel camí introduïm alguns dels resultats més recents sobre els primers deguts a Green, Tao, Zhang i Polymath.

Paraules clau: primers, funció zeta, ènuples primeres, pseudoaleatori, conjectura de Goldbach, conjectura de De Polignac, teorema de Zhang.

Classificació MSC2010: 11-02, 11A41, 11P32.

1 Introducció

Els números primers es troben entre els objectes matemàtics més simples i més estudiats. Però, alhora, encara romanen coberts per un vel de misteri. Sembla difícil conciliar el fet que siguin un objecte tan elemental i alhora tan esmunyedís com per estar poblat de multitud de conjectures.

En aquest breu article voldria explicar que, de fet, coneixem molt bé els números primers, que podem donar molts detalls sobre la seva distribució i decidir amb molta aproximació quants números primers hi ha complint una propietat determinada, encara que sovint no sabem com demostrar les nostres afirmacions (que, d'altra banda, podem verificar numèricament). Dit d'una altra manera, coneixem molt bé l'estructura subjacent del conjunt dels números primers, tot i que de vegades no en tenim demostracions formalment correctes.

Aquest article es basa en la lliçó inaugural del curs acadèmic 2017–2018 dels graus de matemàtiques, física i matemàtiques, estadística aplicada i estadística aplicada i sociologia de la Universitat Autònoma de Barcelona, impartida per l'autor.

El punt clau, i alhora sorprenent, és la naturalesa aparentment aleatòria dels números primers, tot i estar perfectament determinats. Diem que els números primers tenen una distribució pseudoaleatòria: es distribueixen de la mateixa manera que ho farien números escollits a l'atzar seguint unes restriccions bàsiques elementals.

Exposarem breument un model aleatori (essencialment degut a Harald Cramer), explicant l'heurística que el justifica, i en deduirem conjectures degudes a Hardy i a Littlewood. Al final parlarem dels avenços recents en la demostració d'alguns d'aquests resultats.

Potser pot sorprendre al lector que digui que hi ha matemàtics que coneixen molt bé algun fenomen del qual no tenen una demostració; sembla que això xoqui amb la idea molt estesa que els matemàtics no ens creiem res que no estigui rigorosament demostrat. Però la majoria de matemàtics professionals que conec (no tots!) creu en la veracitat de les conjectures més populars i més profundes, i no perquè algunes s'hagin comprovat numèricament (tot i que això també hi ajuda), sinó perquè són conseqüència de certes hipòtesis molt profundes que hom veu com a naturals, segurament boniques en un cert sentit de la paraula, difícil d'explicar però molt vívid, i que alhora expliquen resultats coneguts i els donen un sentit.

Exordi

Tot i dedicar-me a l'aritmètica des que vaig començar la tesi (o potser un parell d'anys abans), els números primers no han estat mai uns objectes en els quals pensés gaire. De fet, durant molts anys de la meva recerca, els números primers eren tan sols una lletra, habitualment p, a vegades q, sovint ℓ, que sortia arreu en els articles i llibres que llegia, i en els problemes en què treballava. Una anècdota famosa d'Alexander Grothendieck il·lustra força bé la meva relació d'aleshores amb els números primers. La llegenda explica que en una conversa amb un altre matemàtic, durant la qual Grothendieck utilitzava tota l'estona un número primer p indeterminat, l'interlocutor li va demanar si podia agafar un número primer particular. Grothendieck li va preguntar si es referia a un número primer concret, i després va dir: «D'acord, agafa el 57».[1]

La meva relació amb els primers, però, va anar canviant per diversos motius. Primer, gràcies al Seminari de Teoria de Nombres de Barcelona (UB-UAB-UPC), en el qual l'any 2005 vàrem estudiar els mètodes de garbell, i en concret la demostració del teorema de Chen. Amb l'ajuda de Jorge Jiménez i Fernando Chamizo vaig poder entendre força millor d'on sortia la conjectura explícita dels números primers bessons. També he de mencionar Andrew Granville, tant pels seus articles de divulgació com pels diversos missatges intercanviats al llarg dels anys.

En segon lloc, i segurament degut a la publicació de la meva lliçó inaugural sobre la conjectura ABC, vaig començar a rebre missatges o fins i tot visites

1 Aquest l'anomenen el *primer de Grothendieck*.

al despatx de persones (des d'aficionats fins a matemàtics més professionals) que em feien preguntes sobre números primers, m'explicaven resultats que havien obtingut o m'enviaven escrits amb mètodes o demostracions. A partir de fer consultes, de llegir articles i de pensar-hi sovint em vaig fer una idea força bona de què se sabia fer a la pràctica amb els números primers, i alhora de què sabia realment la gent del meu voltant.

2 Quants primers hi ha?

Un dels resultats clàssics de les matemàtiques amb una demostració més coneguda i popular és probablement[2] degut a Euclides [6]. És, sense cap dubte, una de les primeres demostracions realment interessants que hom veu quan comença a estudiar matemàtiques.

TEOREMA 2.1. *Hi ha infinits números primers.*

Per cert, sovint s'explica la idea equivocada que Euclides va demostrar el seu teorema per reducció a l'absurd. Però, de fet, el que va demostrar és que, donat qualsevol conjunt finit fixat de números primers, hi ha un número primer (calculable!) no contingut en el conjunt fixat.

Tot i que hom podria pensar que el resultat d'Euclides respon del tot a la pregunta de quants números primers hi ha, de fet no ens dona cap indicació sobre com es distribueixen els primers. Per exemple, no respon a la pregunta de quants números primers realment hi ha amb, posem, 1000 xifres decimals. Si bé és cert que es pot extreure de la demostració una fita inferior per al nombre de primers inferiors a un número donat x, la que s'obté d'aquesta manera està molt lluny de la realitat. Es va haver d'esperar a Legendre, que el 1797 va conjecturar que hi havia aproximadament $n/(\log(n) + A)$ números primers inferiors a n, per a certa constant A (que ell va estimar en $A = -1.083\,66$ d'acord amb unes taules de primers que tenia).[3] De fet, Gauss ja havia conjecturat uns anys abans, el 1792, quan tenia setze anys,[4] un resultat anàleg però amb $A = 0$.

Sembla que Gauss va deduir la seva conjectura estudiant taules de primers de 1000 en 1000 (per tal de suavitzar els «errors experimentals») fins a deduir que la probabilitat que un número menor que n sigui primer és asimptòticament $1/\log(n)$. Així ho descriu a la carta escrita al seu alumne J. F. Encke la nit de Nadal del 1849, en què explica com va fer aquesta extrapolació (vegeu la figura 1).

2 El primer testimoni escrit del teorema que tenim és seu, però els elements d'Euclides recollien molts dels resultats de matemàtiques coneguts fins aquell moment i no podem descartar que l'autor original sigui un altre.

3 Usaré log per a denotar el logaritme neperià.

4 Agraeixo a J. Girbau que m'ajudés a confirmar aquest fet.

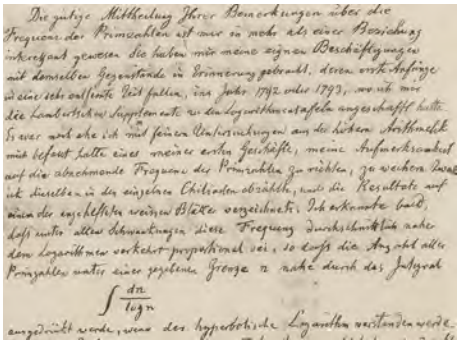


FIGURA 1: Extracte de la carta de Gauss a Encke.

Aquesta conjectura va ser demostrada simultàniament i de manera independent per Jacques Hadamard [11] i Charles-Jean de la Vallée Poussin [4] l'any 1896, basant-se en les idees introduïdes per P. L. Txebixev[5] i sobretot en les de G. F. B. Riemann.

TEOREMA DELS NÚMEROS PRIMERS. *Si denotem per $\pi(x)$ la quantitat de números primers menors o iguals que x, amb $x \geq 2$, aleshores*

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

La notació $f(x) \sim g(x)$ per a funcions de variable real voldrà dir que

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

tot i que la interpretarem dient que $f(x)$ i $g(x)$ són, per a x grans, aproximadament iguals.

Podem interpretar aquest resultat com una estimació aproximada de la probabilitat que un número enter sigui primer. Aquesta estimació és més exacta a mesura que el número n es fa més gran. Ho posaré en forma de principi.

PRINCIPI 2.2. *La probabilitat que un enter entre 1 i n sigui primer és aproximadament $\frac{1}{\log(n)}$.*

3 Els números primers i la funció zeta

La demostració més habitual del teorema dels números primers passa per veure primer que la funció zeta de Riemann, definida per una suma infinita,

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

5 Sí, és el mateix que va demostrar la desigualtat de Txebixev en probabilitat.

on $s \in \mathbb{C}$ és un número complex amb part real > 1 (per tal que la suma sigui convergent), es pot estendre a una funció a tots els complexos a excepció de l'1, i no té cap zero amb part real igual a 1. Que la funció es pot estendre a tots els complexos ho va demostrar el mateix Riemann, que alhora va fer la hipòtesi (o conjectura) que tots els zeros amb part real positiva tenen la part real igual a $1/2$ (la famosíssima hipòtesi de Riemann).

Per tal de comprendre, ni que sigui de manera intuïtiva, com pot ser que la quantitat de números primers tingui alguna relació amb la localització dels zeros d'aquesta funció complexa, el que farem primer és simplificar l'afirmació del teorema dels números primers. Si en lloc de comptar els números primers fins a x, els comptem però ara a cada primer p li assignem el pes $\log(p)$, aleshores obtenim la funció

$$\Theta(x) := \sum_{p \leq x} \log(p),$$

que s'anomena la funció Θ de Txebixev. El que ens diu el teorema aleshores és que la gràfica de la funció $\Theta(x)$ és com la recta $y = x$, o sigui $\Theta(x) \sim x$.

Ara, quina relació hi ha entre que $\Theta(x) \sim x$ i la posició dels zeros de la funció zeta? Doncs justament això és el que va descobrir Riemann amb la seva famosa fórmula explícita (que no va ser demostrada rigorosament fins més endavant, el 1895, per von Mangoldt). Per a poder escriure-la correctament necessitem modificar lleugerament la funció $\Theta(x)$, de manera que no canviarà el seu comportament a l'infinit, però es tornarà una mica més llisa.

Modificarem la funció Θ de Txebixev en dos passos: primer posant el pes $\log(p)$ no només als números primers p, sinó també a les seves potències p^n; obtenim la funció

$$\Psi(x) := \sum_{p^n \leq x} \log(p)$$

(on el sumatori es mou entre els primers p i els enters $n \geq 1$), anomenada la Ψ de Txebixev. Seguidament, en canviarem el valor en els punts on hi ha un salt (les potències dels primers p^n), posant com a valor el valor mitjà del salt: per tant, definim $\Psi_0(x) := \Psi(x)$ si x no és igual a p^n, on p és primer i $n \geq 1$ enter, i $\Psi_0(p^n) := \Psi(p^n) - 1/2 \log(p)$. És fàcil veure (de veritat!) que $\Theta(x) \sim \Psi_0(x)$.

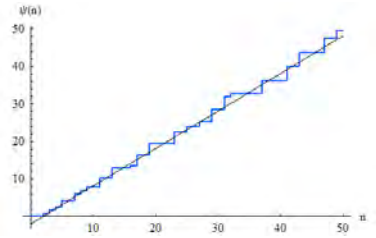


FIGURA 2: La Ψ de Txebixev.

Ara, la fórmula explícita de Riemann ens diu que

$$\Psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \log(2\pi) - \tfrac{1}{2}\log(1 - x^{-2}),$$

on el sumatori és sobre els zeros ρ de la funció zeta de Riemann amb part real positiva (també dits *zeros no trivials*). Observeu que $\log(2\pi) = \frac{\zeta'(0)}{\zeta(0)}$, cosa que d'alguna manera justifica l'aparició d'aquest número a la fórmula.

El punt clau de la demostració del teorema dels números primers és veure que tots els zeros amb part real positiva de la funció zeta de Riemann tenen la part real menor que 1. De fet, si sabéssim que tots els zeros no trivials tenen part real igual a $1/2$, aleshores deduiríem que

$$\sum_\rho \frac{x^\rho}{\rho} = O(\sqrt{x}\log(x))$$

i, per tant, que

$$|\Psi_0(x) - x| = O(\sqrt{x}\log(x)),$$

cosa que ens diu quin és l'error que fem quan aproximem la funció $\Psi_0(x)$ per x. De la mateixa manera, la certesa de la hipòtesi de Riemann ens donaria una fita molt bona de l'error fet en aproximar $\pi(x)$ per $x/\log(x)$.

Ara bé, d'on surt la fórmula explícita? Doncs surt essencialment d'expressar la funció zeta de Riemann com a producte de dues maneres diferents: com a producte sobre els primers, per una banda (el producte d'Euler), i com a producte sobre els seus zeros, per l'altra (el producte de Weierstrass). En aplicar la derivada logarítmica als dos costats de la igualtat, obtenim dues fórmules per a $\zeta(s)/\zeta'(s)$, i la identitat que resulta ja conté la informació buscada, però ens cal extreure-la. Per fer-ho integrem contra la funció x^s/s i hi apliquem el teorema dels residus de Cauchy.

Per exemple, la funció $\frac{1}{2}\log(1 - x^{-2})$ surt dels altres zeros de la funció zeta (els zeros trivials), que són els enters parells negatius, ja que

$$\tfrac{1}{2}\log(1 - x^{-2}) = \sum_{n=1}^{\infty} \frac{x^{-2n}}{-2n},$$

així que la fórmula explícita de fet es pot escriure com

$$\Psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)},$$

on ara ρ es mou dins de *tots* els zeros de la funció ζ, i la x correspon a considerar x^ξ/ξ, on ξ es mou dins de tots els pols de ζ (que només n'hi ha un, i és $\xi = 1$).

En podeu trobar molts més detalls i una informació molt exhaustiva en l'article de J. Quer del 2007 publicat al *Butlletí de la Societat Catalana de Matemàtiques* [17].

4 Conjectures amb números primers

Tots sabem que hi ha multitud de conjectures sobre números primers, i algunes són, de fet, de les més famoses de les matemàtiques. N'explicarem algunes, tot i córrer el risc d'avorrir el lector.

No he sabut trobar el nom de la persona que va formular la primera conjectura.[6] En l'argot de l'ofici diem que és «folklore», en el mateix sentit que diem que cert conte o certa cançó ho són quan no sabem qui en va ser l'autor original.

CONJECTURA DELS PRIMERS BESSONS. *Hi ha infinits primers p tals que $p+2$ és primer.*

Els parells de números primers p i q tal que $q = p+2$ s'anomenen *primers bessons*. Per exemple, les parelles de primers bessons inferiors a 100 són

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

CONJECTURA DE GOLDBACH. *Tot número enter parell ≥ 4 és suma de dos números primers.*

Goldbach va conjecturar en una carta a Euler el 1742 que tot número enter (positiu) era suma de com a molt tres números primers (tot i que ell considerava el número 1 com a número primer). Euler mateix va dir «que tot número parell és suma de dos números primers ho considero un teorema totalment cert, tot i que no el puc demostrar».

La conjectura següent és una generalització natural de la conjectura dels primers bessons feta per De Polignac el 1849.

CONJECTURA DE DE POLIGNAC. *Donat un número parell n, hi ha infinits números primers p tal que $p+n$ és també primer.*

Observeu que la condició que n sigui parell és necessària, ja que si n és senar i p és primer senar, aleshores $p+n$ és parell i no pot ser primer.

Per exemple, per a $n = 4$ les parelles obtingudes amb $p \leq 100$ són

$$(3,7),\ (7,11),\ (13,17),\ (19,23),\ (37,41),\ (43,47),\ (67,71),\ (79,83),\ (97,101),$$

i per a $n = 6$ (els anomenats *primers «sexy»*) n'hi ha força més:

$$(5,11),\ (7,13),\ (11,17),\ (13,19),\ (17,23),\ (23,29),\ (31,37),\ (37,43),$$
$$(41,47),\ (47,53),\ (53,59),\ (61,67),\ (67,73),\ (73,79),\ (83,89),\ (97,103).$$

Explicarem aquest fenomen aparentment sorprenent més endavant.

La conjectura següent és atribuïda a Legendre.

CONJECTURA DE LEGENDRE. *Per a tot número enter $n \geq 2$, hi ha algun número primer p tal que $n^2 < p < (n+1)^2$.*

6 Tot i que sembla que el primer a utilitzar el nom de *primers bessons* va ser P. Stäckel el 1916, A. De Polignac ja havia afirmat la seva conjectura més general el 1849 [5].

Hom pot veure que, de fet, no només és certa per a algun primer, sinó que ho és per a molts. Per exemple, si $n = 100$, hi ha 1228 números primers entre 100^2 i 101^2. Sembla curiós que, tot i que a la pràctica esperem un nombre creixent de primers entre n^2 i $(n+1)^2$, siguem incapaços de demostrar que n'hi ha almenys un!

Finalment, en una llista que va fer Landau el 1912 dels problemes inatacables hi apareix la conjectura següent:

CONJECTURA DELS PRIMERS VORA QUADRATS. *Hi ha infinits números primers de la forma $n^2 + 1$, per a n un enter (parell).*

Per exemple, fins a 10 000 hi ha els primers vora quadrats següents: 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101 i 8837.

Veurem com moltes d'aquestes conjectures estan íntimament relacionades, i que, de fet, són conseqüència natural de la hipòtesi que diu que els números primers estan distribuïts com si fossin números aleatoris sota unes certes restriccions.

5 Tenir conjectures no vol dir no saber res: els casos coneguts

A part de molts resultats numèrics que en certa manera podrien reafirmar les conjectures anteriors, tenim també resultats teòrics obtinguts ens els darrers anys que s'hi aproximen força.

Per exemple, sabem que la conjectura dels primers bessons (i la de De Polignac) és certa si permetem no només números primers, sinó números que són producte de com a molt dos primers (anomenats a vegades *quasiprimers*).

TEOREMA 5.1 (CHEN). *Per a tot número parell n, hi ha infinits números primers p tal que $p + n$ és primer o producte de dos primers.*

En el mateix article [2] es prova que la conjectura de Goldbach és certa per a números prou grans (molt grans!) si a més es permet que un dels dos números sigui quasiprimer. Podeu veure també el volum corresponent del 19è Seminari de Teoria de Nombres de Barcelona [10].

TEOREMA 5.2 (CHEN). *Tot número parell prou gran és suma d'un número primer i un número que és primer o producte de dos primers.*

El mateix Chen va demostrar l'any 1975 a [3] la conjectura de Legendre per a quasiprimers en lloc de primers. Utilitzant un argument similar, H. Iwaniec va demostrar que hi ha infinits quasiprimers vora quadrats [13].

També sabem que la conseqüència següent de la conjectura de Goldbach (que, de fet, s'anomenava la *conjectura dèbil de Goldbach*) és certa.

TEOREMA 5.3 (VINOGRADOV, HELFGOTT). *Tot número senar (> 5) és suma de tres números primers.*

El teorema va ser demostrat per I. M. Vinogradov [19] el 1937 per a un número senar més gran que un número explícit enorme (massa gran per a permetre la comprovació numèrica del teorema per als números més petits),[7] i, després de millores substancials en els mètodes, H. Helfgott, un matemàtic peruà, el va poder provar per a tots els números l'any 2013.

Finalment destaco el teorema recent de Y. Zhang, que va anunciar el 2013, i va ser millorat substancialment per Maynard i Polymath. A les últimes seccions discutiré aquest últim resultat, i explicaré algunes anècdotes al seu voltant.

TEOREMA 5.4 (ZHANG, MAYNARD, POLYMATH). *La conjectura de De Polignac és certa per a algun* $2 \leq n \leq 246$.

6 Tenir conjectures no vol dir no saber res: les conjectures quantitatives

Tot i que es podria pensar que no podem demostrar que hi ha infinits primers bessons perquè són força escassos, o que no sabem la conjectura de Goldbach perquè els números parells són suma de dos primers de poques maneres, de fet (sembla que) tot el contrari és cert: hi ha moltes solucions en ambdós casos.

L'any 1923, G. H. Hardy i J. E. Littlewood van conjecturar, basant-se en una anàlisi heurística de la distribució de primers, fórmules aproximades per al nombre de primers bessons inferiors o iguals a x [12].

G. H. Hardy i J. E. Littlewood.

CONJECTURA 6.1. *Si denotem per* $\pi_2(x)$ *la quantitat de números primers bessons més petits que* x*, aleshores*

$$\pi_2(x) \sim 2\,\Pi_2\,\frac{x}{(\ln x)^2},$$

7 Que un alumne seu va calcular com $3^{3^{15}}$.

on

$$\Pi_2 := \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) = 0.660\,161\,8158\ldots$$

La constant Π_2 s'anomena la *constant dels primers bessons de Hardy-Littlewood*.

De la mateixa manera, van conjecturar de quantes formes es pot escriure un número parell com a suma de dos números primers.

CONJECTURA 6.2. *Si denotem per $G_2(n)$ la quantitat de parelles de números primers (p,q) tals que $n = p + q$, on n és un número parell, aleshores*

$$G_2(n) \sim 2\,\Pi_2 \left(\prod_{p|n;\, p\geq 3} \frac{p-1}{p-2}\right) \frac{n}{(\ln n)^2}.$$

Observeu que a la conjectura hi apareix altra vegada la constant Π_2.

De fet, hi ha versions quantitatives de la conjectura de De Polignac, que comentarem més avall, així com de les altres conjectures, en les quals no hi entrarem.

La pregunta clau és: podem donar una explicació unificada de totes aquestes conjectures, i alhora explicar per què són plausibles?

Veurem que és perfectament possible fer-ho partint d'una suposició molt natural: els números primers es comporten com a números aleatoris seguint un model determinat.

7 L'heurística dels primers

Analitzarem la fórmula conjecturada per Hardy i Littlewood per al nombre de primers bessons.

Partim del teorema dels números primers, que justifica que la probabilitat que un número entre 1 i n sigui primer és «aproximadament» igual a $1/\log(n)$.

La idea és que si el fet que p sigui primer és independent del fet que $p+2$ sigui primer, la probabilitat que p i $p+2$ siguin primers alhora ha de ser el producte de les probabilitats respectives, i, per tant, $1/(\ln(n))^2$ per als números enters a l'interval $[1,n]$.

Però no són independents, ja que si p és primer, $p+2$ és senar, i, per tant, és més probable que sigui primer. De la mateixa manera, si $p = 3m+1$ és primer, aleshores $p+2$ no és primer, ja que 3 el divideix.

Per poder treure'n una fórmula, el que farem és un model «aleatori» més aproximat, que dependrà d'un enter w «petit», i un cop en tinguem conseqüències farem el límit quan w creix.

Per exemple, el model amb $w = 2$ consisteix a dir que la probabilitat que un número n sigui primer és 0 si n és parell, i $2/\log(n)$ si n és senar (donat que un número primer més gran que 2 mai és parell).

El model per a un w general és el següent: direm que la probabilitat que un número n sigui primer és 0 si és divisible per un primer $p \leq w$, i és

$$\prod_{p \leq w} \left(1 - \frac{1}{p}\right)^{-1} \frac{1}{\log(n)}$$

en altre cas.

Ara calcularem el nombre de primers bessons en aquest model depenent de w, sota la hipòtesi d'independència mencionada abans. Obtenim

$$2 \prod_{p \leq w,\, p \neq 2} \left(1 - \frac{1}{p}\right)^{-2} \frac{p-2}{p} \frac{n}{\log(n)^2},$$

on el factor 2 és degut al fet que si p és primer, aleshores $p+2$ és senar, i el factor $\frac{p-2}{p}$ és degut al fet que si tenim p números consecutius, només $p-2$ poden ser el primer més gran d'una parella de primers bessons (ja que els que són congruents amb 0 o amb 2 mòdul p no ho poden ser). Fixeu-vos ara que en fer el límit quan w va a infinit obtenim

$$2 \prod_{p \neq 2} \left(1 - \frac{1}{p}\right)^{-2} \frac{p-2}{p} = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) = 2\Pi_2$$

i, per tant, la fórmula de la conjectura.

Una altra interpretació, potser més senzilla, és la següent: donat que els esdeveniments que p sigui primer i que $p+2$ sigui primer no són independents, hem d'afegir-hi un factor de correcció, tenint en compte la divisibilitat mòdul primers q «petits». La probabilitat que q divideixi un enter n és $1/q$; per tant, la probabilitat que no ho faci és $1 - 1/q$. Per tant, la probabilitat que dos enters escollits a l'atzar no siguin divisibles per a q és $(1 - 1/q)^2$. Ara, la probabilitat que q no divideixi ni p ni $p+2$ és la probabilitat que $p \not\equiv 0, -2 \pmod{q}$, que és, per a un número a l'atzar, igual a $1 - 2/q$ si $q > 2$, i $1/2$ si $q = 2$. Per tant, el factor de correcció que cal posar per a $q = 2$ és

$$\frac{\frac{1}{2}}{(1 - \frac{1}{2})^2} = 2$$

i per a $q > 2$ de

$$\frac{1 - \frac{2}{q}}{(1 - \frac{1}{q})^2} = 1 - \frac{1}{(q-1)^2}.$$

La divisibilitat per primers diferents són clarament condicions independents (pel teorema xinès de les restes), així que cal prendre el producte dels factors de correcció. Finalment, hi ha el problema de fins a quins primers petits cal considerar, però *no importa*, ja que el producte dels factors de correcció per a tots els primers «grans» és molt proper a 1 i no altera el resultat.

8 Un exemple: la conjectura de De Polignac quantitativa

Com que segurament l'argument heurístic anterior no us ha deixat del tot convençuts (he fet el que he pogut per a transmetre la idea en poques paraules), intentaré explicar-vos un argument similar però més senzill que relaciona la conjectura dels primers bessons amb la de De Polignac per a un número parell n qualsevol. Primer descriurem una conseqüència de certes conjectures de Hardy i Littlewood més generals que les conjectures 6.1 i 6.2.

CONJECTURA 8.1. *Donat un número parell qualsevol n, denotem per $\pi_n(x)$ el nombre de primers $p \leq x$ tal que $p+n$ és primer. Aleshores*

$$\pi_n(x) \sim \left(\prod_{q|n} \frac{q-1}{q-2}\right) \pi_2(x),$$

on q es mou dins dels primers senars que divideixen n.

Per exemple, la conjectura ens diria que $\pi_2(x)$ i $\pi_4(x)$ són (aproximadament) iguals, i en canvi $\pi_6(x)$ és el doble de $\pi_2(x)$, i, per tant, hi ha el doble de primers tals que $p+6$ és primer que de primers tals que $p+2$ és primer.

La conjectura la podem comprovar per a alguns valors de n. Per exemple, $\pi_2(100) = 8$, $\pi_4(100) = 9$ i $\pi_6(100) = 17$. I $\pi_2(1000) = 35$, $\pi_4(1000) = 42$ i $\pi_6(1000) = 74$. D'altra banda, això no ens explica per què $\pi_2(x)$ i $\pi_4(x)$ són aproximadament iguals, però $\pi_6(x)$ és aproximadament el doble.

Un argument heurístic que ho justifica és el següent: si a és un número a l'atzar, aleshores 3 té probabilitat $2/3$ de dividir a o $a+2$, però només $1/3$ de dividir a o $a+6$, per tant, el segon parell té el doble de probabilitat d'estar format per dos primers.

El mateix tipus d'argument justifica la conjectura en general.

9 Els primers són pseudoaleatoris

És clar que els números primers no són aleatoris en cap sentit de la paraula: estan perfectament determinats! Què volem dir, per tant, quan diem que són pseudoaleatoris? Volem dir, per exemple, que els podem descriure utilitzant models aleatoris, i obtenir respostes que s'ajusten prou bé a la realitat a preguntes que ens podem formular.

Per exemple, si sabéssim que els primers es distribueixen aleatòriament amb densitat al voltant de x igual $1/\log(x)$ (que és una altra manera de parlar de la probabilitat de ser primer), aleshores un càlcul elemental (que no farem) ens donaria que la fórmula dels números primers més petits o iguals a x esdevé

$$\pi(x) = \int_1^x \frac{dt}{\log(t)} + O(\sqrt{x}\log(x)),$$

on el segon terme «d'error» ens diu que l'error que fem en aproximar una funció per l'altre és més petit que una constant per a $\sqrt{x}\log(x)$.

Doncs resulta que aquesta fórmula, deduïda de la suposició que els primers segueixen una distribució aleatòria, és, de fet, com ja hem comentat abans, equivalent a la hipòtesi de Riemann.

Algú podria pensar que sembla poc plausible que si triem números aleatòriament acabarem tenint prou números molt a prop entre ells (que és el que ens diu la conjectura dels primers bessons), però tot probabilista expert sap que això és una intuïció falsa! Si hom escull prou números a l'atzar, hi ha una probabilitat força alta que alguns acabin sent propers entre si. L'únic que cal tenir en compte és que els primers no poden estar «massa a prop», ja que no poden estar a distància 1 (o senar), per motius aritmètics.

Una altra manera d'entendre per què els primers es comporten com a números aleatoris amb certes restriccions és dir que, de fet, coneixem totes les restriccions que hi ha, i que no hi ha conspiracions ocultes entre ells.

Per exemple, imaginem que fos cert que els números primers prou grans sempre acabessin en 1 en base 3 (o sigui, fossin congruents amb 1 mòdul 3). Aleshores la conjectura dels primers bessons no podria ser certa, ja que en cap parella de primers bessons p i $p+2$ poden ser els dos números congruents amb 1 mòdul 3. Però resulta que sabem que aquesta hipòtesi és falsa! De fet, sabem que és falsa en tota base: hi ha infinits primers acabats en la xifra $b < a$ en base a sempre que no hi hagi cap número que divideixi a i b alhora. Aquest és un teorema degut a Dirichlet que comentarem més endavant (vegeu el teorema 12.2), i que de fet diu que a més els primers es distribueixen de manera equiprobable per a cada a en totes les possibles terminacions b primeres amb a. Per exemple, tenim que una quarta part (aproximadament) dels primers acaben en 1, una altra en 3, una altra en 5 i una última en 7.

Podem interpretar que, de fet, Vinogradov [19] va poder demostrar el seu teorema gràcies al fet que l'ús de l'anàlisi de Fourier i el mètode del cercle (degut a Hardy i Littlewood, però aparentment basat en una idea de Ramanujan)[8] li permeté provar que no hi havia altres conspiracions que poguessin fer falsa la conjectura dèbil (o ternària) de Goldbach. Això és el que ara per ara som incapaços de fer en el cas de la conjectura (binària) de Goldbach.

10 De fet, podem demostrar que els primers gairebé ho són, de pseudoaleatoris

L'abril de l'any 2004, Ben Green i Terence Tao van enviar a l'arxiu de preprints `arxiv` un article en què es demostrava una conjectura plantejada feia més de 230 anys sobre els números primers [9]. El seu resultat era que hi ha successions de números primers arbitràriament llargues en progressió aritmètica.

Per exemple, que n'hi ha de llargada 3 és fàcil: 3, 5 i 7 (amb raó 2). I de llargada 4 també: 5, 11, 17, 23 amb raó 6, que de fet es pot allargar un pas més amb 29. De llargada 10 hi ha 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 amb raó 210. La successió aritmètica de primers explícita més llarga que es coneix té longitud 26.

8 Podeu veure la pel·lícula *L'home que coneixia l'infinit* en què s'explica amb detall les relacions entre ells.

El que varen demostrar Green i Tao és que, tot i que no les sabem trobar explícitament, n'hi ha de llargada tan gran com vulguem. I per provar-ho varen veure que els primers es poden aproximar força bé per conjunts pseudoaleatoris.

La demostració de Green i Tao començava estenent el famós resultat de Szemerédi sobre progressions aritmètiques. Recordem que la densitat (superior) d'un subconjunt A dels números naturals $\mathbb{N}$ està definida per

$$\delta(A) := \limsup_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N}.$$

TEOREMA 10.1 (SZEMERÉDI). *Si un subconjunt $A \subset \mathbb{N}$ dels números naturals té densitat superior $\delta(A) > 0$, aleshores A conté successions aritmètiques arbitràriament llargues.*

Ens agradaria poder aplicar el teorema al conjunt dels números primers, però resulta que aquest conjunt té densitat 0.

La idea és veure ara que els subconjunts dels naturals que, tot i tenir densitat 0, tenen un comportament (pseudo)aleatori, també compleixen el teorema anterior.

En general, podem definir la densitat relativa de $A \subset S \subset \mathbb{N}$ com

$$\delta_S(A) := \limsup_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{|S \cap \{1,\dots,N\}|}.$$

El teorema relatiu de Szemerédi que varen demostrar Green i Tao diu el mateix, però ara per a conjunts pseudoaleatoris.

TEOREMA 10.2. *Si $S \subset \mathbb{N}$ satisfà una condició de pseudoaleatorietat determinada, aleshores tot subconjunt $A \subset S$ amb $\delta_S(A) > 0$ conté successions aritmètiques arbitràriament llargues.*

Aquest resultat, com podeu veure, no fa referència als números primers. De fet, el que es tracta de veure és que el conjunt A es pot aproximar en un cert sentit per un conjunt $\tilde{A}$ de $\mathbb{N}$ amb densitat positiva, de tal manera que el nombre de progressions aritmètiques en A i en $\tilde{A}$ són iguals excepte per un factor de normalització controlat.

Per tal de demostrar el resultat que volien respecte dels números primers, a Green i a Tao ja sols els quedava construir un conjunt pseudoaleatori (en el sentit del teorema anterior) de números «gairebé primers», de manera que contingués els números primers amb densitat positiva.[9] Aquest conjunt es construeix començant per ampliar adequadament els primers per tal que no hi hagi les restriccions aritmètiques que hem trobat abans, com ara que tot primer $\neq 2$ és senar. O sigui, trobant un conjunt que es distribueixi de manera prou uniforme mòdul n per a tot n, però que alhora contingui els números

9 De fet, el conjunt que consideren està directament relacionat amb els quasiprimers, o sigui productes d'un o dos primers.

primers amb densitat positiva. I després cal ampliar-lo una mica més per tal de complir la condició necessària del teorema. Per ser més precisos, el que es fa és treballar no amb conjunts, sinó amb conjunts amb pesos, cosa que simplifica la demostració. No explicarem aquí aquesta construcció, que s'ha anat simplificant en els darrers anys.

De fet, Tao i Ziegler, l'any 2008, varen millorar notablement el teorema 10.2 [18], demostrant que per a tot $k \geq 1$ i tota col·lecció de polinomis $P_1(x), \ldots, P_k(x) \in \mathbb{Z}[x]$ amb coeficients enters i sense terme constant (o sigui que $P_1(0) = \cdots = P_k(0) = 0$), hi ha infinits enters m i $n \geq 1$ de manera que els números $m + P_i(n)$ per a $i = 1$ fins a k són tots primers. El cas del teorema de Green-Tao correspon a prendre els polinomis $P_i(x) = (i-1)x$. Noteu que la condició sobre el terme constant no hauria de ser essencial, sinó una de menys restrictiva que explorarem a la secció següent, i aquí justament és on rau el punt feble (per dir-ho d'alguna manera) del resultat. Per exemple, l'enunciat del teorema de Tao i Ziegler amb $k = 2$ i els polinomis $P_1(x) = 0$ i $P_2(x) = 2$ (que no compleixen les seves hipòtesis) és la conjectura dels primers bessons.

11 Constel·lacions de primers

Si mireu taules de primers, veureu que de tant en tant apareixen primers consecutius amb unitats 1, 3, 7 i 9. Per exemple, 11, 13, 17 i 19; 101, 103, 107 i 109, i 191, 193, 197 i 199. Aquests són exemples de constel·lacions de primers de diàmetre 4.

Així com hem vist que per tal que hi hagi infinits primers p tal que $p+n$ sigui primer ens cal que n sigui parell, també ens podem preguntar quin tipus de condicions naturals hi ha sobre una llista d'enters $0 \leq n_1 < n_2 < \cdots < n_d$ per tal que hi pugui haver infinits números enters x tals que $x + n_i$ siguin primers per a tot $i \in \{1, \ldots, d\}$. Això correspondria a entendre quines condicions s'han de verificar per tal que un resultat equivalent al de Tao i Ziegler de la secció anterior, però ara per a polinomis constants, pugui ser cert.

El punt clau que cal observar, que generalitza el fet que si n és senar, aleshores del parell p, $p + n$, n'hi ha un que és multiple de 2, és el següent: si hi ha un número primer q tal que q divideix $(m + n_1) \cdots (m + n_d)$ per a tot $m \in \mathbb{Z}$, aleshores no hi pot haver infinits enters x amb $x + n_i$ primer per a tot i, ja que almenys un serà divisible per q. Un tal número primer q l'anomenarem una *obstrucció al patró*

$$0 \leq n_1 < n_2 < \cdots < n_d.$$

Per exemple, no hi pot haver infinits primers p tal que $p + 2$ i $p + 4$ siguin ambdós primers. De fet, només n'hi ha un: $p = 3$, amb $p + 2 = 5$ i $p + 4 = 7$. Això és degut al fet que 3 sempre divideix $m(m + 2)(m + 4)$ per a tot $m \in \mathbb{Z}$; o sigui que 3 és una obstrucció per al patró $0 < 2 < 4$. En canvi, no hi ha cap número primer q que divideixi $f(n) := n(n + 2)(n + 6)$ per a tot n, fet que podem comprovar fàcilment, ja que $f(1) = 21$ i $f(2) = 2^6$, que són primers entre ells.

Un patró

$$0 \leq n_1 < n_2 < \cdots < n_d$$

que no tingui cap obstrucció q és un candidat possible a trobar infinits enters x tals que $x + n_i$ és primer per a tot i, o, dit d'una altra manera, que hi hagi infinites dàtuples de primers seguint el patró donat. I, efectivament, això és el que prediu l'heurística i el model aleatori. Aquesta conjectura va ser formulada per Dickson el 1904.

CONJECTURA DE LES ÈNUPLES PRIMERES. *Donat un patró* $0 \leq n_1 < n_2 < \cdots < n_d$ *sense obstruccions, hi ha infinits enters* $x \geq 1$ *tals que* $x + n_i$ *és primer per a tot* $i = 1, \ldots, d$.

Dit d'una altra manera, el conjunt de valors enters que generen primers seguint un patró donat és infinit. Si definim

$$\mathcal{P}_{n_1<n_2<\cdots<n_d} := \{x \in \mathbb{Z}_{\geq 1} : x + n_i \text{ és primer per a tot } i \in \{1, \ldots, d\}\},$$

aleshores la conjectura ens diu que $\mathcal{P}_{n_1<n_2<\cdots<n_d}$ és un conjunt infinit. De fet, com abans, hi ha una conjectura explícita que ens determina de manera asimptòtica quants elements tindria $\mathcal{P}_{n_1<n_2<\cdots<n_d}$ fins a un y donat (això ho veurem a la propera secció).

Observeu també que ens podem reduir a considerar els patrons amb $n_1 = 0$, i aleshores el que busquem són números primers tals que $p + n_i$ és primer per a tot $i = 2, \ldots, d$, o sigui que el conjunt anterior és un subconjunt dels números primers.

Donat un patró $0 = n_1 < \cdots < n_d$, ens podem preguntar per a un d fixat quin és el n_d més petit de manera que obtinguem un patró sense obstruccions. Per exemple, si $d = 2$ el patró més petit és $0 < 2$, i si $d = 3$, tenim dos patrons $0 < 2 < 6$ i $0 < 4 < 6$ amb $n_3 = 6$. Una *constel·lació de primers* de diàmetre d és un patró sense obstruccions de diàmetre d amb n_d mínim. Per posar-ne un exemple més, una constel·lació amb diàmetre 4 té patró $0 < 2 < 6 < 8$ (que ens donarien els exemples anteriors de primers consecutius acabats en 1, 3, 7 i 9), i una de diàmetre 5 és $0 < 4 < 6 < 10 < 12$. Es pot veure que per a tot $d \geq 3$ hi ha més d'una constel·lació de diàmetre d.

La conjectura anterior no està demostrada per a cap patró sense obstruccions, però el resultat de Zhang, que veurem més endavant (teorema 13.2), dona una aproximació a aquesta conjectura: a partir d'un cert valor de d explícit, si en lloc de demanar que hi hagi d primers només demanem que n'hi hagi 2, aleshores el conjunt corresponent conté infinits enters.

12 La hipòtesi H

Hom pot generalitzar de manera natural la conjectura de Dickson prenent polinomis irreductibles amb coeficients enters qualssevol (en lloc dels polinomis de grau 1 de la forma $x + a$ de l'enunciat), cosa que s'anomena també la *hipòtesi H de Schinzel* (amb la versió explícita de Bateman i Horn).

CONJECTURA 12.1 (HIPÒTESI H). *Siguin $f_1(x), \dots, f_m(x) \in \mathbb{Z}[x]$ polinomis irreductibles amb coeficients enters i coeficient de grau màxim positiu. Suposem que no hi ha cap número primer p tal que p divideixi $f_1(n) \cdots f_m(n)$ per a tot $n \in \mathbb{Z}$ (anomenada la condició de Bunyakovsky). Aleshores hi ha infinits números enters n tals que $f_i(n)$ és primer per a tot $i = 1, \dots, m$.*

Més encara, tenim que

$$|\{1 \le n \le x : f_i(n) \text{ és primer per a tot } i \in \{1, \dots, m\}\}| \sim \frac{C}{D} \frac{x}{\log^m(x)},$$

on C i D són les constants explícites següents; D és el producte dels graus dels polinomis $f_i(x)$, i

$$C := \prod_p \frac{1 - \frac{N(p)}{p}}{(1 - \frac{1}{p})^m},$$

on $N(p)$ denota el nombre de solucions mòdul p de

$$\prod_{j=1}^{m} f_j(n) \equiv 0 \pmod{p},$$

i p es mou dins del conjunt de números primers.

No és completament evident, però es pot demostrar fàcilment que la condició de Bunyakovsky implica justament que la constant C és estrictament positiva. Observeu que si no es compleix la condició de Bunyakovsky, aleshores hi ha algun primer p tal que $N(p) = p$, i, per tant, $C = 0$ ja que és un producte (infinit) on un dels termes val 0.

El cas més simple de tots, quan només hi ha un polinomi (o sigui, $m = 1$), i el seu grau és 1 (o sigui, $D = 1$), és de fet el del teorema de Dirichlet que veurem tot seguit. En efecte, si $f(x) = ax + b$, amb a i $b \in \mathbb{Z}$, la condició de Bunyakovsky esdevé la condició que el màxim comú divisor de a i b és 1 (són primers entre ells). Els primers que són de la forma $f(x)$ per a $x \in \mathbb{Z}$ són els primers congruents amb b mòdul a. Finalment, $N(p)$ és igual a 1 si p no divideix a, i igual a 0 si p divideix a. El teorema de Dirichlet va ser la primera aplicació profunda de les tècniques analítiques per a demostrar un resultat aritmètic.

TEOREMA 12.2 (DIRICHLET). *Siguin $a > 1$ i $b \in \mathbb{Z}$ enters primers entre ells. Aleshores*

$$\sharp\{1 \le n \le x : an + b \text{ és primer}\} \sim \prod_{p|a} \left(1 - \frac{1}{p}\right)^{-1} \frac{x}{\log(x)},$$

on el producte és sobre els primers diferents que divideixen a. Equivalentment, en la seva forma més habitual,

$$\sharp\{1 \le n \le x : n \text{ és primer i } n \equiv b \pmod{a}\} = \frac{1}{\varphi(a)} \frac{x}{\log(x)},$$

on φ denota la funció d'Euler.

Recordem que la funció d'Euler

$$\varphi(a) = \sharp\{m : 1 \leq m \leq a \text{ i } a \text{ i } m \text{ són coprimers}\}$$

compleix la fórmula del producte

$$\varphi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right),$$

cosa que demostra l'equivalència del teorema de Dirichlet per un simple canvi d'escala.

Voldria mencionar que hi ha una versió d'aquesta conjectura encara més general per tal d'incloure el cas de més d'una variable, i també per a incloure conjectures com la de Goldbach.

Aquesta versió inclou conjectures com la de Sophie Germain que afirma que hi ha infinits parells de primers p i $2p + 1$ (un resultat no provat per ara), l'afirmació que hi ha infinits primers en successió aritmètica de llargada d fixada (el resultat de Green i Tao que hem explicat a la darrera secció), o altres resultats que les generalitzen, com els de Tao i Ziegler que ja hem comentat, i també moltes de les conjectures que hem posat a la secció 5.

Per exemple, la hipòtesi H quan $m = 1$, i només tenim un polinomi, inclou el cas dels primers vora quadrats (o sigui, de la forma $n^2 + 1$), però també molts d'altres. Observeu que no hi ha primers de la forma $n^2 - 1$ (a excepció del 3), ja que $n^2 - 1 = (n - 1)(n + 1)$ no és irreductible, i no pot ser primer excepte si $n - 1 = 1$. Tampoc hi ha infinits primers de la forma $n^2 + n + 2$, tot i ser irreductible, ja que 2 sempre divideix $n^2 + n + 2$.

13 El teorema de Zhang

Retornem a l'últim resultat demostrat relatiu a aquestes conjectures, en què es prova la conjectura de De Polignac per a algun valor de n parell «petit» (inferior a 70 milions en primera instància, inferior a 246 recentment). Reescriurem aquest teorema de la manera següent, potser més entenedora.

TEOREMA 13.1. *Hi ha una constant K ($K = 70\,000\,000$ per a Zhang, $K = 246$ per a Maynard i Polymath) de manera que hi ha infinits primers p tals que el primer següent q compleix $q \leq p + K$.*

Aquest teorema va ser demostrat per Yitang Zhang el 2013 (va ser anunciat el 17 d'abril del 2013). Aquest matemàtic té una història certament excepcional. Nascut l'any 1955 a la Xina, va anar a fer la tesi als Estats Units d'Amèrica, concretament a la Universitat de Purdue, l'any 1985 (any en què va publicar el seu primer article basat en resultats del seu treball de màster a la Xina). Després de set anys va finalitzar la tesi i no va poder trobar feina de matemàtic. Va haver de treballar en un restaurant de menjar ràpid, fins i tot dormint al cotxe. Finalment va trobar feina de professor ajudant a la Universitat de New Hampshire. Quan va fer el seu anunci l'any 2013 només tenia dos articles publicats, el segon l'any 2001, i tenia cinquanta-vuit anys.

Yitang Zhang.

El que és més sorprenent és que la demostració de Zhang no era una idea nova i totalment revolucionària, sinó que era una millora molt tècnica i molt fina dels últims resultats en el camp, els quals Zhang va entendre a la perfecció. O sigui que, tot i no publicar res, havia estat llegint i entenent en detall el que s'estava fent per tal de poder utilitzar-ho i millorar-ho. Tot i això, la seva millora aconseguia un fet fonamental i que fins aleshores es creia fora de l'abast: poder provar l'existència d'una constant K com la de l'enunciat del seu teorema. Fins aleshores els resultats obtinguts eren amb una funció K depenent de la mida del primer p.

Un altre fet excepcional de la demostració de Zhang és que estava perfectament i clarament redactada, i que ell mateix la va poder explicar detalladament davant d'experts. Això va provocar que un mes després de l'anunci l'article [20] ja estigués acceptat en una de les revistes més importants de matemàtiques: *Annals of Mathematics*.

Un cop va aparèixer l'article es va posar en marxa un equip en línia per a portar les tècniques que havia introduït al límit per tal de rebaixar el valor de la constant K que Zhang havia obtingut. Eren la vuitena encarnació del projecte Polymath, un experiment per a intentar aplicar les tècniques col·laboratives massives, similars a les dels projectes de codi obert que es donen en el món del programari, al món de la matemàtica acadèmica. Els projectes Polymath (`http://polymathprojects.org/`) funcionen a partir d'una proposta de diversos experts d'un problema que creuen que es pot intentar resoldre col·laborativament, que seguidament es planteja en detall al blog d'un dels promotors.[10] És en els comentaris a aquest post on tothom (tu també pots!) va fent propostes, posant resultats parcials, explicant idees. El promotor després va resumint el més significatiu del que s'ha dit fins aleshores en un altre post, i així fins a arribar a un resultat prou satisfactori. Si s'hi arriba, aleshores s'escriu un article signat sota el pseudònim D. H. J. Polymath [16].

Després que el projecte Polymath obtingués en un primer moment una millora substancial de la constant obtinguda per Zhang, James Maynard, un matemàtic que havia acabat la tesi recentment en tècniques de garbell (que

10 Que en el cas del Polymath 8 va ser T. Tao, que ja ha sortit a l'article diverses vegades.

són les tècniques utilitzades per Zhang per a demostrar el seu teorema) es va adonar que podia redemostrar el teorema a partir de resultats previs que Zhang no havia considerat. Aquesta nova demostració, obtinguda el novembre del 2013, portava a una millora considerable del resultat (de fins a $K = 600$), i fins i tot del resultat millorat del Polymath. Així que el projecte Polymath 8 va reiniciar-se utilitzant ara les noves idees de Maynard fins a obtenir el valor de $K = 246$.

De fet, el que demostra Zhang, i després refina Maynard, és un teorema molt més general en la direcció de la conjectura de les ènuples primeres.

TEOREMA 13.2 (ZHANG, MAYNARD, POLYMATH). *Existeix un enter k (k=3 500 000 per a Zhang, $k = 50$ per a Maynard i Polymath) de manera que per a tot patró $(n_1, \dots, n_k)$ sense obstruccions hi ha infinits enters $x \geq 1$ per als quals com a mínim 2 dels enters $x + n_i$ per a $i = 1, \dots, k$ són primers.*

Observeu que la conjectura de les ènuples primeres afirmaria que per a tot k hi ha infinits enters x tals que hi ha com a mínim k primers entre els enters $x + n_i$ per a $i = 1, \dots, k$.

Per a poder deduir el teorema 13.1 a partir d'aquest sols cal trobar quina és la constel·lació de primers més petita amb diàmetre k. I resulta que la més petita per a $k = 50$ va de 0 a 246, i una és[11]

0, 4, 6, 16, 30, 34, 36, 46, 48, 58, 60, 64, 70, 78, 84, 88, 90, 94, 100, 106,
108, 114, 118, 126, 130, 136, 144, 148, 150, 156, 160, 168, 174, 178, 184,
190, 196, 198, 204, 210, 214, 216, 220, 226, 228, 234, 238, 240, 244, 246.

Hom podria pensar que ara ja és una qüestió tècnica arribar a millorar el teorema 13.1 fins a obtenir el valor de $K = 2$, cosa que ens donaria la conjectura dels primers bessons (i amb quasi tota seguretat, la de De Polignac, fins i tot la quantitativa, i altres conjectures més generals). Però, de fet, hi ha una dificultat profunda en els mètodes utilitzats, com hi és en els resultats de Chen o en els de Vinogradov. Els experts l'anomenen la *barrera de la paritat*, i, per exemple, en el cas que ens ocupa, faria que com a molt es pugui obtenir el valor de $K = 6$, que correspon al valor $k = 3$ en el teorema anterior. El problema de la paritat implica en el nostre cas que els mètodes actuals no poden distingir $k = 3$ i $k = 2$.

14 Conspiracions aparents

L'11 de març del 2016, dos experts en primers força coneguts, R. J. Lemke Oliver i K. Soundararajan, varen fer públic al servidor `arxiv` un article en què mostraven dades numèriques aparentment sorprenents de biaixos inesperats en la distribució dels números primers [14]. Per exemple, varen comprovar que

11 No n'hi ha tan sols una d'aquesta llargada!

de tots els primers acabats en 1 (en base 10) fins a cent milions, el primer que el segueix acaba en 3 per a uns 7 milions i mig, un nombre similar acaba en 7, però sols uns 5 milions i mig acaben en 9 i uns 4 milions i mig acaben en 1. El mateix fenomen passa amb les altres terminacions, i de fet en totes les bases. Dit d'una altra manera, tot i que el teorema de Dirichlet ens diu que la probabilitat que un primer acabi en 1, en 3, en 7 o en 9 és la mateixa, ells varen comprovar que si un primer acaba en 1 és molt més probable que el següent primer acabi en 3 (o en 7, o en 9) que en 1.

Anteriorment ja s'havien trobat d'altres biaixos sorprenents, tot i que no tan espectaculars, com l'anomenat *biaix de Txebixev*: si mirem la quantitat de primers inferiors a un enter x, per a la majoria de x hi ha més primers congruents amb 3 mòdul 4 que congruents amb 1 mòdul 4 (mireu [8] per a una introducció molt detallada i accessible al fenomen). El mateix passa quan es compten els primers segons el seu valor mòdul 3, o de manera similar amb qualsevol altre mòdul: fixat un enter n, normalment[12] hi ha menys primers fins a x que són quadrats mòdul n que no que no ho són.

En una primera instància hom podria pensar que aquests fenòmens revelen una conspiració que rebatria la naturalesa pseudoaleatòria dels números primers. Però els mateixos autors demostren en l'article [14] que això no és cert: de fet, el model aleatori que hem presentat anteriorment prediu aquest comportament, fins i tot numèricament i amb molt bona aproximació. Encara més, els mateixos autors expliquen que varen tenir la idea d'estudiar aquest comportament en escoltar una conferència sobre un fenomen molt ben conegut en probabilitat. El que els va sorprendre és que fos tan evident numèricament.

El problema de probabilitat que els va motivar és el següent. Tenim dues persones, X i Y, que juguen al joc següent: cadascú va tirant una moneda (perfecta) fins que surti o bé una cara i després una creu per a X, o bé dues cares seguides per a Y. El primer que obtingui el que busca, guanya. Donat que un cop ha sortit una cara, la tirada següent o bé surt cara o bé creu amb la mateixa probabilitat, hom podria pensar que els dos tenen la mateixa probabilitat de guanyar. Però això és incorrecte! Resulta que X trigarà de mitjana unes 4 tirades a obtenir el que busca, mentre que Y necessitarà de mitjana 6 tirades. Podeu jugar una estona a casa per tal de veure el fenomen en acció, o bé mirar de fer-ne els càlculs precisos vosaltres mateixos.

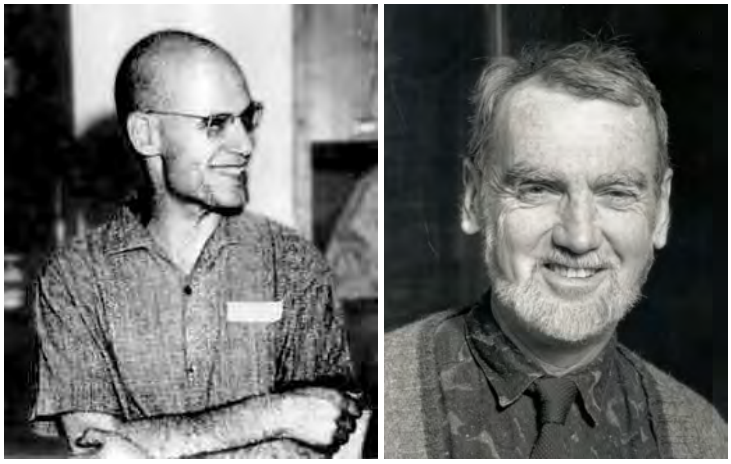
En resum: fins ara, tot i la descoberta de nous comportaments detectats experimentalment sobre la distribució dels números primers, que en una primera instància semblaven indicar un possible error en els models aleatoris dels primers, al final resulta que es poden entendre justament gràcies a la seva naturalesa aleatòria, i els fenòmens es poden comprovar utilitzant idees provinents de la teoria de la probabilitat. Potser el fet que en primera instància ens sorprengui als que treballem en aritmètica deu ser per la nostra escassa intuïció probabilista.

12 Però no sempre. De fet, un argument degut a Littlewood demostra que hi ha infinits valors de x per als quals això no és cert.

15 Saber no és només tenir-ne una demostració

En aquest article he volgut reflexionar, amb un exemple pràctic, sobre les preguntes següents: quin sentit té tenir una teoria matemàtica conjectural? Conté informació realment útil per a un matemàtic? Són, de fet, matemàtiques?

No conec en detall la situació en camps de la matemàtica diferents de l'aritmètica, entesa en un sentit molt ampli, on sé del cert que durant els darrers cent anys han aparegut una pila de teories conjecturals que han servit i serveixen de guia per a molts dels desenvolupaments i resultats més importants. Per exemple, les diverses teories que especulen sobre les analogies entre cossos de números i cossos de funcions sobre un cos finit, subjacents tant en l'esquema de la prova de les conjectures de Weil per Weil i Grothendieck, com fins i tot en la teoria recent dels perfectoides de Scholze. O la teoria (o teories) dels motius de Grothendieck (vegeu [15] per a una introducció breu a la idea subjacent a la teoria dels motius).[13] O en el programa grandiós de Langlands (podeu consultar l'article de Gelbart [7], que, tot i ser de fa uns quants anys, és una bona introducció a algunes de les seves idees, o els dos volums del 12è Seminari de Teoria de Nombres de Barcelona (UB-UAB-UPC) [1] per a una introducció molt més detallada). Totes aquestes teories estan completament interrelacionades, i hi ha un marc que les engloba. De fet, les formulacions recents del programa de Langlands utilitzen la teoria conjectural dels motius.



Alexander Grothendieck i Robert Langlands.

Aquestes teories conjecturals són útils en molts sentits. Primer, de manera pràctica, permeten respondre conjecturalment moltes preguntes i, per tant, preveure quin pot ser el resultat buscat per tal de després intentar demostrar-lo «correctament». No només això, també poden servir de guia en l'obtenció d'aquesta demostració. D'alguna manera són un patró, tal com ho són algunes

13 En el mateix volum hi ha una biografia molt detallada de la vida agitada de Grothendieck.

parts de la física per a certs camps de les matemàtiques. Però per a mi l'objectiu més important de les teories és el d'explicar resultats coneguts i conjectures prèvies, que ens portin a una comprensió més profunda dels problemes i ens mostrin una explicació de les relacions aparents entre resultats distints i a vegades molt allunyats entre ells.

És aquest darrer motiu la raó profunda de l'existència de les diverses teories. Al cap i a la fi, els matemàtics no només volem ser capaços de fer càlculs molt difícils —com sovint els no matemàtics creuen— o de demostrar o estudiar determinats resultats —com sovint ens demanen des d'altres ciències, i segurament és l'únic pel que se'ns avaluarà. També volem comprendre, cada cop amb més profunditat, la realitat (matemàtica), com ho vol un físic, o qualsevol altre científic. I és en aquest sentit que les explicacions donades per les teories conjecturals poden arribar a ser molt més satisfactòries i fins i tot més útils, tot i no ser completament exactes o no estar formalment demostrades, que els resultats establerts purs i durs.

Agraïments

Vull agrair a W. Pitsch haver-me proposat fer la lliçó inaugural que em va induir finalment a escriure l'article, a F. Bars i a E. Nart les innumerables converses sobre aritmètica durant molts anys, a J. Verdera les nombroses correccions, i a M. Masdeu les converses sobre alguns del protagonistes de l'article i comentaris fets a una primera versió de l'article. I a C. Balaguer tantes coses que no puc ni enumerar.

Referències

[1] Bayer, P.; Travesa, A. (ed.). «Representacions automorfes de GL(2)». *Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)*, 2 i 3 (1997).

[2] Chen, J. R. «On the representation of a larger even integer as the sum of a prime and the product of at most two primes». *Sci. Sinica*, 16 (1973), 157–176.

[3] Chen, J. R. «On the distribution of almost primes in an interval». *Sci. Sinica*, 18 (5) (1975), 611–627.

[4] de la Vallée Poussin, Ch.-J. *Recherches analytiques sur la théorie des nombres premiers*. Brussel·les: Hayez, Académie Royale de Belgique, 1897.

[5] de Polignac, A. *Recherches nouvelles sur les nombres premiers*. París: Bachelier, 1851.

[6] Euclides. *The Elements*, circa 300 ac.

[7] Gelbart, S. «An elementary introduction to the Langlands program». *Bull. Amer. Math. Soc. (N.S.)*, 10 (2) (1984), 177–219.

[8] Granville, A.; Martin, G. «Prime number races». *Amer. Math. Monthly*, 113 (1) (2006), 1–33.

[9] Green, B.; Tao, T. «The primes contain arbitrarily long arithmetic progressions». *Ann. of Math. (2)*, 167 (2) (2008), 481–547.

[10] Guàrdia, J.; Jiménez, J. (ed.). «Mètodes de garbell». *Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)*, 13 (2005).

[11] Hadamard, J. «Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques». *Bull. Soc. Math. France*, 24 (1896), 199–220.

[12] Hardy, G. H.; Littlewood, J. E. «Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes». *Acta Math.*, 44 (1) (1923), 1–70.

[13] Iwaniec, H. «Almost-primes represented by quadratic polynomials». *Invent. Math.*, 47 (2) (1978), 171–188.

[14] Lemke Oliver, R. J.; Soundararajan, K. «Unexpected biases in the distribution of consecutive primes». *Proc. Natl. Acad. Sci. USA*, 113 (31) (2016), E4446–E4454.

[15] Mazur, B. «What is ... a motive?». *Notices Amer. Math. Soc.*, 51 (10) (2004), 1214–1216.

[16] Polymath, D. H. J. «Variants of the Selberg sieve, and bounded intervals containing many primes». *Res. Math. Sci.*, 1 (2014), art. 12, 83 p.

[17] Quer, J. «La funció ζ de Riemann». *Butlletí de la Societat Catalana de Matemàtiques*, 22 (2) (2007), 197–228.

[18] Tao, T.; Ziegler, T. «The primes contain arbitrarily long polynomial progressions». *Acta Math.*, 201 (2) (2008), 213–305.

[19] Vinogradow, I. M. «Representation of an odd number as a sum of three primes». *Dokl. Akad. Nauk SSSR*, 15 (1937), 169–172.

[20] Zhang, Y. «Bounded gaps between primes». *Ann. of Math. (2)*, 179 (3) (2014), 1121–1174.

Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona, Catalonia
xarles@mat.uab.cat