ELS NOMBRES PRIMERS (§)

CARLES SIMÓ
Facultat de Ciències,
Universitat Autònoma de Barcelona

Tothom sap que un nombre primer és aquell que només és divisible per ell mateix i per la unitat. Aquesta simple definició ha donat i donarà lloc a nombroses recerques dels matemàtics per a esbrinar com són i com es comporten els nombres primers. No puc negar que, en la meva vessant de matemàtic experimental, he dedicat estones, tot esperant els resultats d'algun programa, a «jugar amb els primers».

La qüestió primera és quants n'hi ha. Euclides (*Elements*, llibre IX, proposició 20) diu: «Hi ha més nombres primers que qualsevol conjunt de nombres primers». La demostració, ben coneguda, és: Si $p_2,\ldots,p_r$ fossin tots els primers, els nombre que s'obté afegint 1 al producte de tots ells o és primer o tot factor d'ell és més gran que qualsevol dels primers p_i. En ambdós casos tenim un absurd.

Una altra demostració basada en la divergència de

$$\sum_{p_n \in \mathcal{P}} p_n^{-1} \qquad (*)$$

($\mathcal{P}$ = conjunt de tots els primers $= \{p_1 < p_2 < \ldots\}$) és deguda a Euler (1737). Una prova elemental d'aquest fet és (Clarkson, 1966): Si (*) convergeix,

$$\exists\, k \mid \sum_{m>k} p_m^{-1} < 1/2 \ .$$

(§) Conferència feta a l'Institut d'Estudis Catalans el 23 de novembre de 1977.

Sigui Q el producte del k primers nombres primers. Considero $1+nQ$, $n \geq 1$. Tots els divisors primers de $1+nQ$ són més grans que p_k. Llavors tindrem l'absurd següent:

$$\forall\, r > 1,\ \sum_{n=1}^{r} (1+nQ)^{-1} \leq \sum_{t=1}^{\infty} \Big(\sum_{m>k} p_m^{-1} \Big)^t < 1 .$$

Euler digué, de fet, que

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \ldots = \ln(\ln \infty) .$$

La interpretació d'això és:

$$\sum_{p_n \leq x} p_n^{-1} \sim \ln(\ln x) ,$$

que, en efecte, surt del teorema dels nombres primers (t.n.p.) o de la forma multiplicativa de la funció ζ. (Una mica de notació:

$$f(x) \sim g(x) \iff \lim_{x \to \infty} \frac{f(x)}{g(x)} = 1 ;$$

$$\ln_2 x = \ln(\ln x) ; \quad exp_2(x) = exp(exp(x)) ;$$

$$\ln_{k+1} x = \ln(\ln_k x) ; \quad exp_{k+1}(x) = exp(exp_k(x)) .$$

Destaquem que $\ln_2 x$ creix molt lentament:

$$x = 10^6 \implies \ln_2 x = 2.6 ; \quad x = 10^{20} \implies \ln_2 x = 3.8 .$$

Altres funcions que es comporten com $\ln_2 x$ són.

$$\sup_{m \leq x} \frac{m}{\phi(m)} \quad (\phi = \text{indicador d'Euler}) ,$$

o bé el nombre mitjà de factors primers diferents d'un enter.

Hi ha fórmules que donin els primers? La resposta és afirmativa, però sembla que poc útil. Vegem fórmules recurrents. Gandhi diu (1971): coneguts $p_1, \ldots, p_n$, siguin P_n el producte de tots ells. Llavors p_{n+1} és l'únic zero enter t de

$$1 < b^t \Big(\sum_{d \mid P_n} \frac{\mu(d)}{b^d - 1} - \frac{1}{b} \Big) < b$$

on b és un enter qualsevol més gran o igual que 2. Ací la funció μ (de Möbius) es definida per $\mu(n) = 0$ si n conté quadrat; $\mu(n) = (-1)^k$ si n és producte de k primers; $\mu(1) = 1$.

Golomb (1976) generalitzà els resultats de Gandhi així: sigui α una probabilitat sobre

$$\mathbb{Z}_+, \text{ i } \alpha(n) \geqq 0 \ , \ \sum_{n \geqq 1} \alpha(n) = 1 \ ;$$

definim

$$\beta(m) = \sum_{n \geqq 1} \alpha(mn) \ , \qquad \gamma(k) = \sum_{d|n} \mu(d)\beta(d) \ .$$

Llavors si per a tota successió de naturals

$$1 \leqq n_1 < n_2 < n_3 \ \dots \ ,$$

T és un operador tal que

$$T(\sum \alpha(n_i)) = n_1 \ ,$$

tenim

$$p_{n+1} = T(\gamma(P_n) - \alpha(1)) \ .$$

Aplicant això obtenim, per exemple:

$$p_{n+1} = \lim_{s\to\infty} (P_n(s)\zeta(s) - 1)^{-1/s} \ ,$$

on

$$P_n(s) = \prod_{p_i | P_n} (1 - p_i^{-s}) \ , \ \zeta(s) = \sum_{n \geqq 1} n^{-s} \ .$$

Voldríem fórmules més explícites, és clar. Per exemple, que

$$y = a_0 + a_1 x + \dots + a_n x^n$$

anés donant primers en donar a x els valors 0,1,2,... . Si fem

$$y = x^2 + x + 41 \qquad \text{o} \qquad y = x^2 - 79x + 1601$$

obtenim primers per valors de x entre 0 i 40 o bé entre 0 i 79, respectivament. Podem esperar una bona fórmula d'aquest tipus? La resposta és *no*. En efecte si per a $x = \alpha$ surt $y = p$, primer, és immediat que per a $x \equiv \alpha \pmod p$ tenim $y \equiv 0 \pmod p$ i obtindrem forçosament no primers.

Però sí que hi ha fórmules que representen tots els primers. Introduïm algunes definicions: Siguin

$$a \in \mathbb{Z}_+^m , \quad x \in \mathbb{Z}_+^n , \quad P(a,x) \in \mathbb{Z}[a,x] .$$

Pensem en $P(a,x) = 0$ en les variables x. Un conjunt de m-ples *a* es diu diofantí si per a aquests valors $0 = P(a,x)$ té solució.

Un conjunt contingut a $\mathbb{Z}_+{}^m$ es diu llistable si existeix un algorisme que permet de fer-ne una llista (és a dir, tot membre del conjunt sortirà en la llista, potser diverses vegades, i no hi sortirà cap no-membre). Trivialment: diofantí $\Longrightarrow$ llistable. El teorema fonamental, que dóna solució negativa al problema 10 de Hilbert, és (Matijasevic, 1970): llistable $\Longrightarrow$ diofantí.

Tot conjunt diofantí de naturals és representat pels valors positius d'un polinomi (Putnam, 1960):

$$Q(a,x) = (a+1)\{1 - P^2(a,x)\} - 1 .$$

Teorema: Els primers formen conjunt diofantí i això implica que són els únics valors positius de polinomis a coeficients enters quan les variables són naturals. N'han estat donades fórmules amb 24 variables i grau 37, o 21 i 21, o 19 i 29, o 42 i 5, o 12 variables i grau molt alt. En donem aquí una amb 26 variables i grau 25 que usa només 325 símbols:

$$\begin{aligned}(k+2)\,\{1 &- [wz+h+j-q]^2 - [(gk+2g+k+1)(h+j)+h-z]^2 - [16(k+1)^3(k+2)(n+1)^2+1-f]^2 - \\ &- [2n+p+q+z-e]^2 - [e^3(e+2)(a+1)^2+1-o^2]^2 - [(a^2-1)y^2+1-x^2]^2 - \\ &- [16r^2y^4(a^2-1)+1-u^2]^2 - [(a^2-1)l^2+1-m^2]^2 - [ai+k+1-l-i]^2 - \\ &- [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 - [n+l+v-y]^2 - \\ &- [p+l(a-n+1)+b(2an+2a-n^2-2n-2)-m]^2 - [7+pl(a-p)+t(2ap-p^2-1)-pm]^2 - \\ &- [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2\} .\end{aligned}$$

Així, mentre que hi ha una demostració que un nombre és compost que exigeix una única multiplicació (simplement, multiplicant 2 divisors seus «adequats»!), hi ha una demostració que un nombre és primer amb un nombre acotat d'operacions! (34 sumes, 39 restes i 68 multiplicacions). Exercici: Demostreu així que 13 és primer.

Podem preguntar-nos com apareixen els primers. En principi sembla que no segueixin cap llei. Així, mentre que del 101 al 113 n'hi ha 5, el següent no apareix fins al 127; del 1327 saltem al 1347; per contra, entre el 5639 i el 5659 n'hi ha 7. Entre 10^7—100 i 10^7 n'hi ha 9 i entre 10^7 i 10^7+100 només 2. En el primer milió de nombres hi ha més primers que en el segon; en el segon més que en el tercer, etc., però en el milió 32 menys que en el 33. (Per a més irregularitats, vegeu més endavant.)

És fàcil de fer taules de primers. El mètode més eficaç és el del garbell. Un ordenador potent eficientment programat pot tractar milions de nombres per segon. Així és possible d'obtenir tots els primers més petits de 10^{12} en un temps prudencial (centenars d'hores). Més difícil és d'emmagatzemar-los (al voltant de 3.7×10^{10} nombres, la major part de 12 xifres). La fig. 1 mostra una plana d'una llista de primers més petits de 10^7 que ocupa 352 fulls d'impressora.

No creguem, però, que hom només coneix primers fins a 10^{12}. Molts d'altres primers han estat obtinguts en estudiar certes successions d'enters. Euclides, cercant nombres perfectes (que coincideixen amb la suma de llurs divisors propis) diu (*Elements*, llibre IX, proposició 36): Si diversos nombres, començant per la unitat, estan en proporció duplicada i el conjunt de tots és primer, el producte d'aquest conjunt pel darrer és perfecte. En fórmula, si

$$2^p-1 \in \mathcal{P} \ , \quad (2^p-1)\,2^{p-1}$$

és perfecte.

Els nombres del tipus $M_p = 2^p - 1$ foren estudiats per Mersenne el 1644. Euler provà que tot perfecte parell és d'aquest tipus. M_p primer implica p primer. Hom només coneix 24 (§) primers de Mersenne; corresponen a

p = 2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2283,3217,4253, 4423,9689,9941,11213,19937.

El darrer, M_{19937}, és el primer més gran que hom coneix actualment. Fou descobert per Tuckerman el 1971. Té 6002 xifres i el presentem a la fig. 2. Per a p més petit o igual que 257, l'estat actual dels nombres de Mersenne (a

(§) Quan aquesta conferència estava en premsa s'ha descobert la següent: p=21701.

Fig. 1. Una pàgina d'una taula de primers $<10^7$. La taula ocupa 352 fulls d'impressora.

part els primers) és el de la taula 1 (recordem que si n divideix p, llavors M_n divideix M_p).

Diguem de passada que pel que fa a perfectes senars, hom no en coneix cap. Si n'hi ha, cal que siguin més grans de 10^{50}, que algun de llurs factors primers sigui més gran de 100110 i que tinguin 6 factors primers o més (10 o més si no hi és el 3).

Altres nombres curiosos són els de Fermat, $F_p = 2^{2^p} + 1$. Són primers per

$$p = 0,1,2,3,4 \quad (F_p = 3,5,17,257,65537).$$

Fermat digué que tots ho eren. Però Euler, el 1732, provà que $F_5 = 641 \times 6700417$. De fet hom no coneix cap més F_p primer. L'estat actual el tenim a la taula 2.

El primer d'ells del qual no se sap res és F_{17} (fig. 3). Té 39457 xifres. Curiosament se sap que F_{1945} és compost. Com a anècdota diguem que l'expressió decimal d'aquest número és «incalculable amb els mitjans actuals i futurs». En efecte, té unes 9.6×10^{584} xifres. Si prenem com a ordres de magnitud: Radi de l'univers $= 10^{10}$ anys de llum, 1 any de llum $= 10^{16}$ m., radi d'una partícula elemental $= 10^{-15}$m, tenim que a l'univers, hi caben aproximadament

$$10^{3(10+16+15)} = 10^{123} \text{ partícules elementals}$$

Ni portant cada una d'elles una xifra podem somniar d'«escriure» F_{1945}.

Els primers de Fermat intervenen en àlgebra com a corol·lari de la Teoria de Galois, ja que els polígons construïbles amb regle i compàs són els que tenen n costats, on $n = 2^k p_1 \ldots p_r$, amb p_i primer de Fermat. No se sap si hi ha infinits nombres de Mersenne primers, ni infinits compostos, infinits de Fermat primers o infinits compostos.

Per què es poden abordar els M_p, F_p?.

Teorema (Lucas, Lehmer): M_p ($p \neq 2$, primer) primer si i sols si divideix el terme $p - 1$ de la successió $\{s_k\}$, on

$$s_1 = 4, \quad s_k = s_{k-1}^2 - 2 .$$

Cal tenir en compte que s_k creix ràpidament (s_{100} té més de 10^{27} xifres). Llavors definim $\{r_k\}$ així:

$$r_1 = 4 \; ; \; r_{k+1} = r_k^2 - 2 \pmod{M_p} .$$

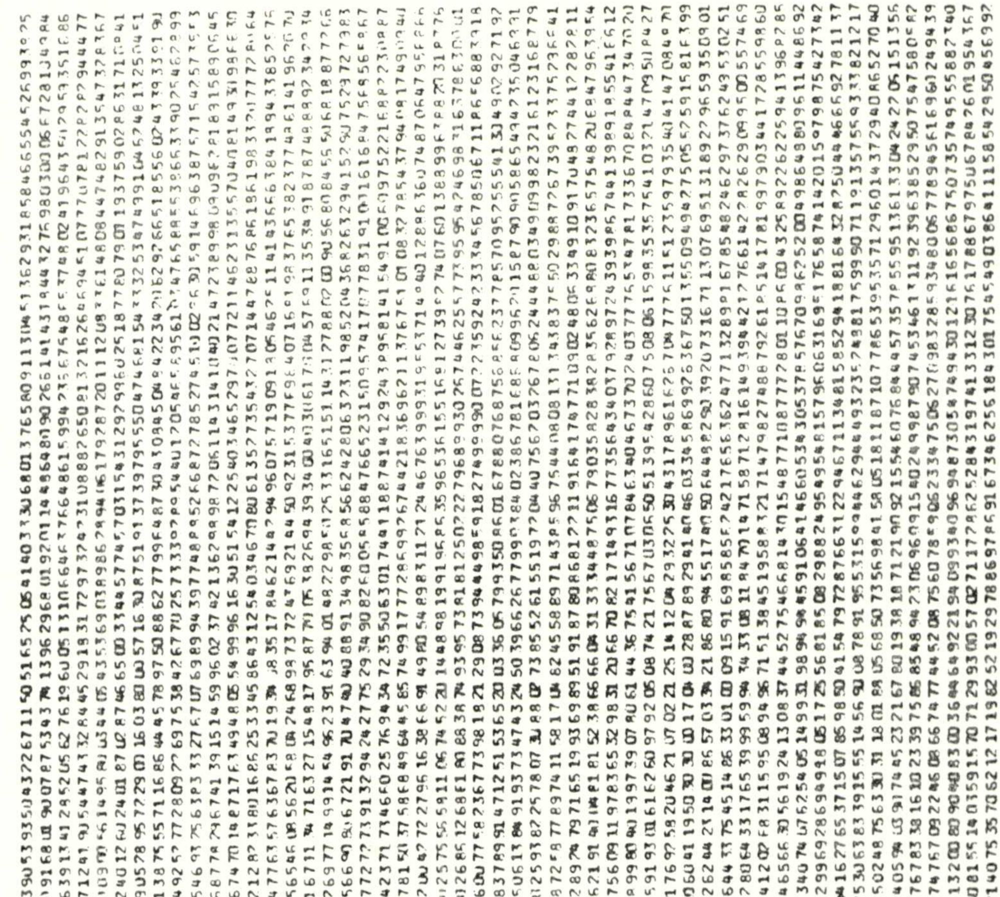


Fig. 2. El nombre primer més gran que es coneix: $M_{19937} = 2^{19937} - 1$.

p	172,179,181,197,233,239	173,191,193,211,223,229,251	199,227,257
M_p	factoritzat del tot	cofactor compost	compost, cap factor conegut

Taula 1 (font Brillhart, Lehmer, Selfridge)

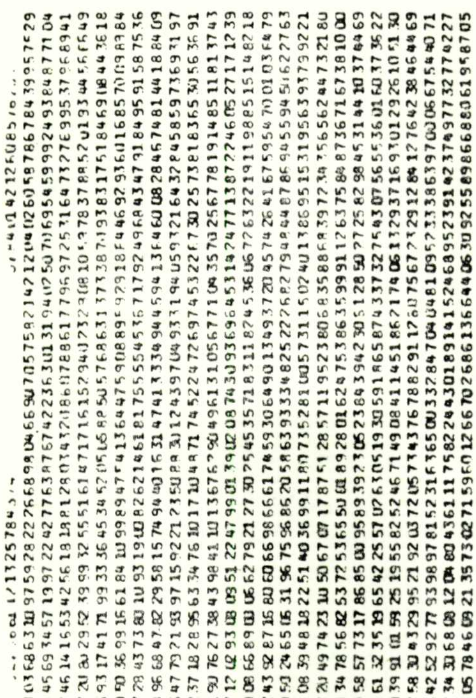
p	$\leqslant 4$	5,6,7	10^+,11,12*,19,30,38	9^+,13,15,16,18,21, 23,25,26,27,32,36, 39,42,52,55,58,63, 73,77,81,117,125, 144,150,207,226, 228,250,267,268, 284,316,452,1945	8,14	17,20,22, 24,28,29, 31, etc.
F_p	primer	factoritzat (2 factors coneguts)	2 ó 4* factors coneguts	compost; es coneix un factor; + = co-factor compost	com-post no es coneix cap factor	?

Taula 2 (font Hallyburton, Brillhart)

x	$\Pi(x)$	$x/\Pi(x)$
10	4	2.5
10^2	25	4.0
10^3	168	6.0
10^4	1229	8.1
10^5	9592	10.4
10^6	78498	12.7
10^7	664579	15.0
10^8	5761455	17.4
10^9	50847534	19.7
10^{10}	455052512	22.0

Taula 3 (font Zagier)

Fig. 3. Primeres i darreres xifres del nombre de Fermat $F_{17}=2^{2}+1$. Ocupa 6 fulls d'l



ssora. És el més petit d'aquests nombres del que no se sap si és primer o compost.

Naturalment

$$M_p | s_{p-1} \iff M_p | r_{p-1} .$$

19937 quadrats de nombres d'unes 6000 xifres permeten de decidir que M_{19937} és primer.
Teorema: Tot divisor primer de F_n per a n més gran que 1 és de la forma $2^{n+2} k+1$.
Per a $n = 8$ s'ha provat fins $k \leq 1542455295$; per a $n = 14$, $k \leq 792008372$, i per a $n = 17$, $k \leq 16777215$.
Teorema (Proth):

$$F_n \in \wp \iff F_n | 3^{(F_n-1)/2} + 1 , \quad n \geq 1 .$$

Pensem, però, que per a F_{17} caldria quadrar i fer mòdul respecte a F_{17}, 131072 nombres d'unes 40000 xifres.

Com se sap que F_{1945} és compost? $2^{1947} k + 1$ és compost per a $k < 5$. Sigui

$$m = 2^{1947} k + 1$$

i $\overline{t}$ la resta de dividir t entre m. Fem

$$r_1 = 4 , \quad r_{k+1} = \overline{r_k^2} .$$

Vegem que

$$m | 2^{2^k} - r_k$$

per inducció. Per a $k = 1$ és cert. Si ho és per a un cert k, tenim

$$m | 2^{2^{k+1}} - r_k^2 \implies m | 2^{2^{k+1}} - r_{k+1} \implies m | F_{1945} - r_{1945} - 1 .$$

Llavors només cal veure si $r_{1945} + 1$ és divisible per m (1944 quadrats i residus de nombres de 587 xifres com a màxim). Certament és divisible si $k = 5 \Rightarrow F_{1945}$ té per divisor menor $5 \times 2^{1947} + 1$. Pel que fa al divisor més gran se cap per a F_m és molt més gran que $m \times 2^m$.

Per a nombres qualssevol no és tan fàcil de trobar-ne els factors (decidir si són primers és relativament més fàcil). Tot mètode (com el trivial) que impliqui $0(\sqrt{n})$ operacions no és considerat com a tal i cal descartar-lo. Calen mètodes $0(n^{1/3})$ o millors.

Els més usats es basen: en representacions de λn ($\lambda = \pm 1,2$) com

$$\lambda n = x^2 - D y^2$$

amb $D = -1, \pm 2, \pm 3, \pm 6, (n,6) = 1$. (D. i E. Lehmer) i 2 representacions de λn d'aquesta forma (sempre existeixen amb λ, D adequats) donen la factorització de n; en representacions en fracció contínua de $\sqrt{n}$ o $\sqrt{kn}$ per a un $k \geq 1$ escaient, mètode que amb un 360/91 factoritza, com a terme mitjà, nombres de 20 xifres en 6 segons i de 40 en 1 hora; en aprofitar factoritzacions completes o parcials de

$$n-1,\ n+1,\ n^2+1,\ n^2 \pm n+1.$$

Sembla que la cota actual és la factorització d'un nombre qualsevol de 50 xifres.Lehmer ha construït dispositius electrònics per a fer certs bucles o garbells en alguns dels mètodes de factorització. L'últim, el SRS—181, pot processar 20 milions de nombres per segon! Un mètode degut a D. Shanks i encara no implementat assegura factorizació en $0(n^{1/4})$ operacions. Existeixen abundants taules de factoritzacions de nombres dels tipus

$$10^p \pm 1 \ ,\ 2^p \pm 1 \ ,\ 2^{2p} \pm 2^p + 1 \ ,\ 2^{2p-1} \pm 2^p + 1 \ ,\ \text{etc.}$$

D'altres qüestions encara no resoltes són per exemple, si hi ha infinits primers del tipus $n^2 + k$, k fix (Bouniakowsky conjecturà que si

$$f(x) = \sum a_i x^i \in \mathbb{Z}[x] \ ,\ \underset{x \in \mathbb{Z}}{\text{m.c.d.}} (f(x)) = N \neq 0$$

llavors $f(x)/N$ és primer per a infinits valors $x \in \mathbb{N}$), o bé si sempre hi ha un primer a (n^2, n^2+n). Se sap que

$$\forall \varepsilon > 0 \ ,\ \exists x_0 \mid \forall x > x_0,\ [x, x+x^{7/12+\varepsilon}] \cap \mathcal{P} \neq \emptyset \ .$$

Més endavant tornarem a aquesta qüestió.

Una classificació molt important dels primers és la relacionada amb l'anomenat últim teorema de Fermat: l'equació diofantina

$$x^n + y^n = z^n$$

no té cap solució ni n és més gran de 2. Evidentment només cal demostrar-ho per a valors de n primers. Kummer, en les seves recerques sobre el problema, introduí les nocions de primers regulars i irregulars, que no detallem. Diguem només que Kummer provà el teorema de Fermat per als primers regulars. Dintre els primers menors de 100, sols 37, 59 i 67 són irregulars. Siguin

$$B_{2n} = \frac{N_{2n}}{D_{2n}}$$

els nombres de Bernoulli (definits més endavant), p un primer més gran de 2. Es diu índex d'irregularitat de p a

$$\mathrm{irr}(p) = \#\{k > 0 \mid 2k \leqq p-3 \text{ i } p \mid D_{2k}\} .$$

Els primers regulars es caracteritzen perquè irr(p) = 0.

Se sap que hi ha infinits primers irregulars, però encara no ha estat demostrat que n'hi hagi infinits de regulars. Les experiències numèriques semblen afavorir la conjectura segons la qual l'índex d'irregularitat segueix una distribució de Poisson de paràmetre 1/2. Per als primers irregulars calen altres procediments per a provar el T. de Fermat. Diguem, però, que en l'actualitat està demostrat que és cert per a tots els primers <100000.

La famosa conjectura de Goldbach: tot parell més gran o igual que 4 és suma de dos primers, encara resta oberta. Ha estat verificada fins a 2^{25}. Se sap que tot nombre prou gran és suma de com a màxim 18 primers. Si n és un senar més gran de $3^{3^{15}}$, podem baixar a 3 primers (Vinogradov, 1937), encara que sembla que això és cert per a tot senar més gran de 5. Per als parells prou grans hom pot escriure $n = p + p_1p_2$ (Chen Jing Run, 1966), amb p_1, p_2, p_3 primers. Hi ha constants efectives, C, $\delta > 0$ tals que

$$E(x) = \#\{n \leqq x,\ n = \dot{2},\ n \notin \mathcal{P} + \mathcal{P}\} \implies E(x) < Cx^{1-\delta}$$

($\#$ = cardinal).

Si $\nu_2(n)$ és el nombre de representacions d'un parell n com a suma de 2 primers, consideracions heurístiques porten a

$$\nu_2(n) \sim A_0 \frac{n}{(\ln n)^2} \prod_{p>2,\, p \mid n} \frac{p-1}{p-2} ,$$

on

$$A_0 = 2 \prod_{p>2} (1-(p-1)^{-2}) .$$

Diguem

$$\nu_r(n) = \sum_{\sum_{i=1}^{r} p_i = n,\, p_i \in \mathcal{P}} 1 .$$

La conjectura de Goldbach s'escriu

$$\nu_2(n) > 0, \forall\, n \in 2\,\mathbf{Z}_{\geq 2} .$$

Un teorema més general que els de Vinogradov és: Si $r \geq 3$, $n \equiv r \pmod 2$, llavors

$$\nu_r(n) = G_r(n) \frac{n^{r-1}}{(\ln n)^r} + O\left(\frac{n^{r-1} \ln_2 n}{(\ln n)^{r+1}}\right) .$$

$G_r(n)$ és una funció aritmètica complicada, però

$$0 < C_1(n) < G_r(n) < C_2(n) < +\infty .$$

Una pregunta no contestada inversa a la de Goldbach és si tot parell és diferència de 2 primers. Però ja sabem que un boig pot fer una pregunta que un milió de savis no podran contestar.

Abans de passar al t.n.p. diguem, per a acabar la miscel·lània, què són els primers truncables. Un primer es diu truncable per la dreta si traient les seves xifres una a una per la dreta sempre tenim primers. Ídem per l'esquerra. Els més llargs en base 10 són 73939133 per la dreta i 35768631264621656 7629137 per l'esquera. Exercici: trobeu-los en d'altres bases.

Després de tot això que hem dit, sembla que els primers surten com volen i que no hi ha llei que pugui dir res sobre ells. Això no és veritat, sinó que a grans trets segueixen fidelment una llei, encara que hi hagi irregularitat en els detalls. Sigui

$$\pi(x) = \#\{p \in \mathcal{P},\ p \leq x\} .$$

Si no ens agrada el salt de π en els primers, podem fer $\pi(p) = \pi(p-\varepsilon) + 1/2$

per $p \in \mathscr{P}$, amb què π queda més simètrica. Per a elaborar taules de π només cal un mètode de garbellar. (En realitat és posible d'obtenir $\pi(x)$ sense calcular directament els primers). La figura 4 mostra part d'una taula de $\pi(x)$ amb pas de la x de 80000.

Si mirem la taula 3, el creixement regular de $x/\pi(x)$ amb un increment de 2.3 quan x es multiplica per 10 fa sospitar una llei com

$$x/\pi(x) \sim ln\, x \; .$$

El primer resultat en aquesta direcció és degut a Chebyshev qui, el 1815, provà que

$$A\,\frac{x}{ln\, x} \leqq \pi(x) \leqq B\,\frac{x}{ln\, x} \qquad \text{si } x > x_0, \quad \text{on} \quad A = A(x_0),\; B = B(x_0)\; .$$

Si $x_0 = 30$, puc agafar

$$A = ln\,\frac{2^{1/2}\,3^{1/3}\,5^{1/5}}{30^{1/30}} = 0.921\;\ldots\;;\; B = \frac{6}{5}A = 1.105\;\ldots\;.$$

Una demostració senzilla amb A i B pitjors és:

$$n^{\pi(2n)-\pi(n)} \leqq \prod_{n<p\leqq 2n} p \leqq \binom{2n}{n} < 2^{2n} \Longrightarrow \pi(2n) - \pi(r) < 1.39\,\frac{n}{ln\, n}\; .$$

Si suposo

$$\pi(n) < 1.7\,\frac{n}{ln\, n}$$

tinc

$$\pi(2n) < 3.09\,\frac{n}{ln\, n} < 1.7\,\frac{2n}{ln\, 2n}$$

si $n > 1020$.

D'altra banda

$$\pi(2n+1) \leqq \pi(2n)+1 < 3.09\,\frac{n}{ln\, n} + 1 \leqq 1.7\,\frac{2n+1}{ln\,(2n+1)}$$

si $n > 1200$. Com que

$$n = 1200 \div 2399 \Longrightarrow \pi(n) < 1.7\,\frac{n}{ln\, n}\; ,$$

la fórmula és vàlida per a tot n més gran o igual que 1200.

Per la cota inferior, sigui

$$p \in \mathcal{P} \,, \quad p^{\nu_p} \,\Big|\, \binom{n}{k} \,, \quad p^{\nu_p+1} \nmid \binom{n}{k}$$

Com que

$$\nu_p = \sum_{i=1}^{[\ln n/\ln p]} \left(\left[\frac{n}{p^i}\right] - \left[\frac{k}{p^i}\right] - \left[\frac{n-k}{p^i}\right] \right)$$

i cada terme de la suma és més petit o igual que 1, $p^{\nu_p} \leq n$. Llavors

$$\binom{n}{k} = \prod_{p \leq n} p^{\nu_p} \leq n^{\pi(n)} \Longrightarrow 2^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n+1)\, n^{\pi(n)} \Longrightarrow$$

$$\Longrightarrow \pi(n) \geq \frac{n \ln 2}{\ln n} - \frac{\ln(n+1)}{\ln n} > \frac{2}{3} \frac{n}{\ln n} \qquad \text{si} \quad n > 200 \,.$$

Es mostra també que

$$p_n > n \ln n, \ \forall n \in N \,, \quad \lim_{n\to\infty} \frac{p_n}{n \ln n} = 1 \,.$$

(Un raonament heurístic envers el t.n. p.: Si f és la densitat i hi ha «independència» entre els diferents primers,

$$f(x) = \prod_{2}^{x} \frac{p-1}{p} \; ; \quad \ln f(x) \simeq - \int_a^x \frac{1}{p} f(p) \,, \quad \text{ja que} \quad \ln \frac{p-1}{p} \simeq - \frac{1}{p}$$

Derivant

$$- \frac{f'}{f} = \frac{f}{x} \Longrightarrow \frac{1}{f} = \ln x \,,$$

com volíem.)

A més de la funció $\pi(x)$, Chebyshev introduí

$$\Pi(x) = \sum_{k \geq 1} \frac{1}{k} \pi(x^{1/k}) = \sum_{p^\nu \leq x} \frac{1}{\nu} \,, \quad \theta(x) = \sum_{p \leq x} \ln p =$$

	99421841	99425586	99429281	99432996	9943672
	99459270	99462932	99466666	99470386	9947410
	99496517	99500247	99503994	99507738	9951150
	99533699	99537433	99541218	99544965	9954863
	99570986	99574710	99578450	99582155	9958594
π(202968E4) =	99608336	99612074	99615782	99619492	9962316
	99645589	99649310	99653025	99656726	9966045
	99682970	99686553	99690321	99694061	9969781
	99720250	99723948	99727721	99731471	9973519
	99757623	99761366	99765074	99768786	9977254
	99794952	99798702	99802426	99806152	9980996
	99832482	99836261	99840042	99843723	9984749
	99869784	99873576	99877206	99880929	9988465
	99907068	99910819	99914481	99918214	9992194
	99944328	99948063	99951745	99955514	9995919
π(203768E4) =	99981595	99985302	99989073	99992746	9999642
	100018818	100022546	100026345	100030038	10003377
	100056265	100060002	100063755	100067515	10007120
	100093551	100097313	100101049	100104727	10010844
	100130822	100134520	100138333	100141992	10014570
	100168011	100171776	100175525	100179195	10018288
	100205243	100209004	100212701	100216384	10022013
	100242717	100246493	100250230	100254003	10025770
	100280052	100283817	100287592	100291302	10029500
	100317419	100321154	100324883	100328624	10033235
π(204568E4) =	100354858	100358588	100362314	100366046	10036971
	100392045	100395821	100399616	100403293	10040708
	100429493	100433174	100436927	100440614	10044435
	100466656	100470317	100474087	100477841	10048156
	100503972	100507754	100511450	100515174	10051885

Fig. 4. Part d'una taula de valors de la func

99440506	99444234	99448036	99451775	99455491	
99477848	99481599	99485379	99489101	99492818	
99515162	99518913	99522645	99526358	99529988	
99552388	99556077	99559804	99563479	99567249	
99589653	99593362	99597068	99600815	99604543	
99626889	99630632	99634361	99638086	99641821	$= \pi(2030400000)$
99664236	99668092	99671810	99675485	99679228	
99701507	99705254	99709010	99712753	99716564	
99738986	99742744	99746442	99750206	99753934	
99776246	99779953	99783730	99787435	99791227	
99813692	99817459	99821229	99825009	99828768	
99851236	99854917	99858675	99862430	99866076	
99888419	99892183	99895921	99899574	99903285	
99925664	99929401	99933142	99936851	99940553	
99962961	99966604	99970314	99974079	99977844	
00000237	100003974	100007677	100011441	100015163	$= \pi(2038400000)$
00037568	100041289	100045028	100048740	100052522	
00074907	100078643	100082416	100086166	100089871	
00112187	100115932	100119666	100123389	100127139	
00149482	100153159	100156885	100160571	100164291	
00186570	100190331	100194024	100197711	100201460	
00223982	100227774	100231494	100235231	100238964	
00261441	100265111	100268848	100272571	100276311	
00298780	100302526	100306266	100309986	100313677	
00336100	100339781	100343596	100347349	100351073	
00373460	100377178	100380907	100384667	100388339	$= \pi(2046400000)$
00410782	100414476	100418207	100421938	100425741	
00448043	100451812	100455510	100459223	100462916	
00485307	100489055	100492800	100496483	100500207	
00522603	100526371	100530126	100533904	100537667	

a intervals de 80000 números.

ln del producte de tots els primers més petits o iguals que x, i

$$\psi(x) = \sum_{k \geq 1} \theta(x^{1/k}) =$$

ln del m.c.m. de tots els nombres més petits o iguals que x.

Si certament x/ln x aproxima $\pi(x)$ i, de fet l'error relatiu tendeix a zero si x tendeix a l'infinit, Gauss, intuint que la «densitat de primers» prop del valor x és 1/ln x, digué que π era més ben representada pel logaritme integral

$$Li(x) = f_0^x \frac{dt}{ln\ t} \qquad \left(f_0^x = \lim_{\varepsilon \to 0} \left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^x \right)\right)$$

valor principal de Cauchy. Si dibuixem $\pi(x)$ i Li (x) per $x \leq 10^6$ és impossible de distingir l'una gràfica de l'altra a simple vista, ja que la diferència màxima és de l'ordre de 130 per $x \simeq 10^6$. Tenim

$$Li(x) = \gamma + ln_2 x + \sum_{n \geq 1} \frac{(ln\ x)^n}{n \cdot n!}$$

si $x > 1$. γ és la constant d'Euler-Mascheroni =

$$= \lim_{n \to \infty} \left(\sum_{k \geq 1} \frac{1}{k} - ln\,n \right) = .5772156649 \ \ldots \ .$$

Encara que és més difícil de calcular que π(que es coneix amb 2^{25} bits), hom té ja γ amb més de 20000 decimals.

Una millor aproximació s'obté posant

$$Li(x) \sim \Pi(x),$$

d'on

$$\pi(x) \sim \sum_{k \geq 1} \frac{\mu(k)}{k} Li(x^{1/k}) = Li(x) - \frac{1}{2} Li(x^{1/2}) - \frac{1}{3} Li(x^{1/3}) - \frac{1}{5} Li(x^{1/5}) + \frac{1}{6} Li(x^{1/6}) \ldots$$

$$= R(x) \ .$$

com va fer Riemann. La taula 4 mostra la bona coincidència entre $\pi(x)$ i R(x). Les diferències Li—π i R—π presenten oscil·lacions petites (relativament) però

x	π(x)	Li(x)-π(x)	R(x)-π(x)	x	π(x)	Li(x)-π(x)	R(x)-π(x)
10^8	5761455	754	97	$13\cdot10^8$	65228333	2560	563
$2\cdot10^8$	11078937	1038	153	$14\cdot10^8$	69985473	2088	25
$3\cdot10^8$	16252325	1084	30	$15\cdot10^8$	74726528	1580	-546
$4\cdot10^8$	21336326	1052	-141	$16\cdot10^8$	79451833	1876	-312
$5\cdot10^8$	26355867	965	-350	$17\cdot10^8$	84163019	2365	118
$6\cdot10^8$	31324703	1342	-81	$18\cdot10^8$	88862422	1607	-697
$7\cdot10^8$	36252931	1311	-212	$19\cdot10^8$	93547928	2505	146
$8\cdot10^8$	41146179	1683	69	$20\cdot10^8$	98222287	3015	602
$9\cdot10^8$	46009215	2434	734	$21\cdot10^8$	102886526	2738	272
$10\cdot10^8$	50847534	1701	-79	$22\cdot10^8$	107540122	2765	248
$11\cdot10^8$	55662470	1021	-834	$23\cdot10^8$	112184940	1743	-824
$12\cdot10^8$	60454705	2034	106	$24\cdot10^8$	116818447	2672	-57

Taula 4 (font autor)

k	ρ_k
1	$.5+i\cdot14.134725$
2	$.5+i\cdot21.022040$
3	$.5+i\cdot25.010856$
4	$.5+i\cdot30.424878$
5	$.5+i\cdot32.935057$
6	$.5+i\cdot37.586176$
7	$.5+i\cdot40.918720$
8	$.5+i\cdot43.327073$
9	$.5+i\cdot48.005150$
10	$.5+i\cdot49.773832$

Taula 5 (font Edwards)

en principi estranyes (fig. 5). Per contra, Li(x) — R(x) és molt «suau». D'altra banda R és una funció entera en ln x:

$$R(x) = 1 + \sum_{n \geqq 1} \frac{1}{n\zeta(n+1)} \frac{(ln\ x)^n}{n!} ,$$

on ζ és la funció de Riemann.

Diguem que Gauss obtingué la relació Li (x) $\sim \pi(x)$ a partir de l'experiència (calculant ell mateix els primers fins a 3 milions). Riemann fou conduït a $R(x) \simeq \pi(x)$ a partir de l'estudi de la funció ζ , però no demostrà que R fos asimptòtica a $\pi(x)$.

En el seu article bàsic (1859) «Über die Anzahl der Primzahlen unter einer gegebener Grösse» introdueix la funció

$$\zeta(s) = \sum_{n \geqq 1} n^{-s} = \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1} ,$$

bé que aquesta relació fonamental ja havia estat notada per Euler. Simplement

$$\prod_{p \in \mathcal{P}} (1-p^{-s})^{-1} = \prod_{p \in \mathcal{P}} (1+p^{-s}+p^{-2s}+\dots) ,$$

i si

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \text{ llavors } n^{-s}$$

s'obté en agafar els termes en

$$p_1^{-k_1 s} , p_2^{-k_2 s} , \dots$$

en els diferents factors.

De

$$\frac{1}{\zeta(s)} = \prod_{p \in \mathcal{P}} (1-p^{-s})$$

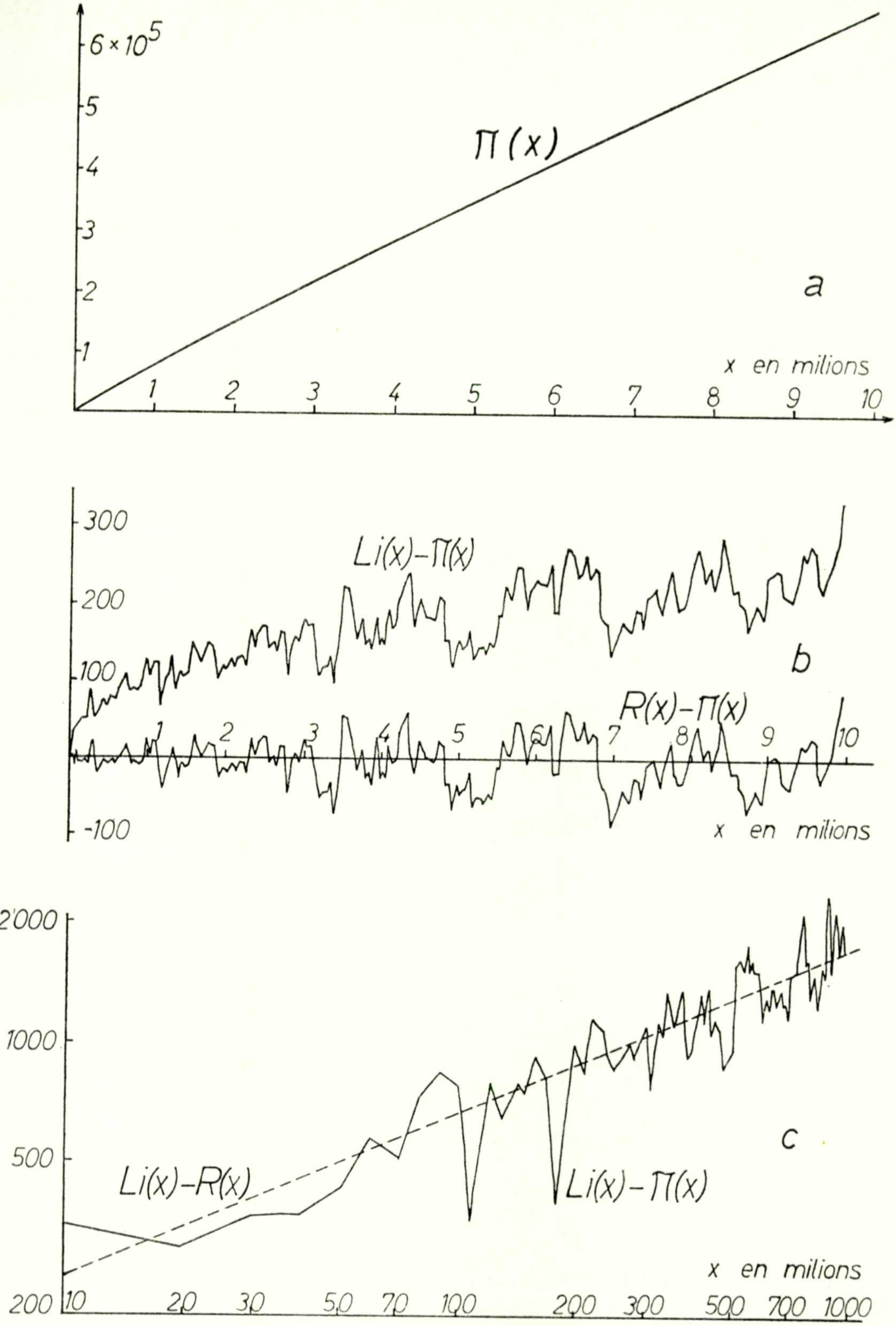


Fig. 5. a) Gràfica de $\pi(x)$. No es distingeixen les irregularitats.
b) Gràfiques de $R(x)—\pi(x)$ i de $Li(x)—\pi(x)$.
c) Gràfiques de $Li(x)—\pi(x)$ i de $Li(x)—R(x)$ en escala logarítmica. (Font : Zagier).

tenim

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} .$$

Com que $\zeta(1) = +\infty$, Euler (1748) tragué d'ací:

$$1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \frac{1}{10} - \frac{1}{11} - \frac{1}{13} + \frac{1}{14} + \frac{1}{15} - \frac{1}{17} - \dots = 0 \quad ,$$

que no és pas evident! La demostració és de Mangoldt (1897).

Mitjançant

$$2 \sin(\pi s) \;\; \Gamma(s) \; \zeta(s) = i \int_{-\infty}^{+\infty} \frac{(-x)^{s-1}}{e^x - 1}$$

s'estén ζ a $\mathbb{C} - \{1\}$.

Diguem que

$$\zeta(2k) = (2\pi)^{2k} \, (-1)^{k+1} \; B_{2k}/2(2k)!$$

on B_{2n} són els nombres de Bernoulli:

$$\frac{x}{e^x - 1} = \sum_{n \geqq 0} \frac{B_n x^n}{n!} .$$

ζ verifica la relació funcional

$$\zeta(s) = \Gamma(1-s) \; (2\pi)^{s-1} \; 2 \sin(\tfrac{\pi s}{2}) \; \zeta(1-s) .$$

És clar que $\zeta(s)$ no té zeros a Re $s > 1$, perquè

$$\prod_{p} (1-p^{-s})^{-1}$$

és un producte infinit convergent si Re $s > 1$ i cap factor no és zero. A més dels zeros «trivials» $s = -2k$, $k = 1,2,3,\ldots$, tots els altres són $\mathrm{Re}\, s \in [0,1]$.

La funció

$$\xi(s) = \Gamma(1+\tfrac{s}{2})\,(s-1)\,\pi^{-s/2}\,\zeta(s)$$

només té zeros a $\mathrm{Re}\, s \in [0,1]$. Aquesta és l'anomenada banda crítica. La famosa hipòtesi de Riemann (HR) diu que tots els zeros de ξ són a la recta crítica: $\mathrm{Re}\, s = 1/2$. Hardy (1914) provà que $\xi\,(1/2 + it)$, $t \in R$, que pren només valor reals té infinits zeros reals (per parelles: $\pm\, t$). El 1921 Hardy i Littlewood mostren que existeix un A positiu tal que el nombre de zeros a la recta crítica amb $|\mathrm{Im}\, t| < T$ és $> AT$ si T és prou gran. Selberg, el 1942, assegurà que hom pot posat AT 1n T en comptes de AT. Finalment Levinson, el 1974, demostrà que més d'un terç dels zeros cauen en la recta crítica.

La demostració del t.n.p. fou feta independentment per J. Hadamard i Ch. de la Vallée-Poussin el 1896. (Nascuts els anys 1865 i 1866 amb poca diferència, i morts el 1962 ambdós, demostraren el t.n.p. simultàniament).

Aquesta demostració requereix la integració de

$$\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) = \eta(s)$$

en $\mathscr{C}$ (fig. 6). Cal que la regió limitada per $\mathscr{C}$ no tingui zeros, la qual cosa s'aconsegueix veient que hi ha cota inferior de

$$|t|\,\Big|\,\xi(\sigma+it) = 0\ ,$$

i que a $\sigma = 1$ no hi ha zeros. Llavors s'ha de veure que per a tot ε positiu, si T, T_0, x són prou grans, s'acompleix

$$\left|\int_{\mathscr{C}'} \eta(s)\right| < \varepsilon \quad \text{on} \quad \mathscr{C}' = ABCDEFGH\ .$$

Així es mostra que

$$\psi(x) \sim x \quad (\text{o millor,}\ \int_1^x \psi(t)dt \sim x^2/2).$$

Les relacions

$$\pi(x) \sim Li(x)\ ,\ \Pi(x) \sim Li(x)\ ,\ \psi(x) \sim x\ ,\ \theta(x) \sim x$$

són equivalents.

Demostracions «elementals» (sense usar altra cosa sinó combinatòria, àlgebra i anàlisi real) foren donades per Erdös i Selberg el 1949.

Una bonica conseqüencia del t.n.p. és que, donat un natural qualsevol de k xifres, sempre hi ha un primer tal que les seves k primeres xifres són les del natural donat.

Hom demostra (Mangoldt) que

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} + \sum_{n \geqq 1} \frac{x^{-2n}}{n} - ln(2\pi) \quad ,$$

on ρ són els zeros de ξ (presos en l'ordre $|\operatorname{Im} \rho|$ creixent, ja que la sèrie no és absolutament convergent). També s'obté, equivalentment:

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

(exactament!). Notem que x^{ρ} o $R(x^{\rho})$ constitueixen la part oscil·latòria de $\psi(x)$ o de $\pi(x)$.

Si

$$T_k(x) = -\left(R(x^{\rho_k}) + R(x^{\overline{\rho_k}})\right) \quad ,$$

amb els ρ_k ordenats per part imaginària creixent T_k és fortament oscil·latori (vegeu fig. 7). Cada zero $\rho = \sigma + it$ implica la presència dels zeros $\sigma - it$, $1-\sigma \pm it$.

HR implica

$$|\psi(x) - x| < Cx^{1/2}(ln\ x)^2 \quad \text{i} \quad |\pi(x) - Li(x)| < Cx^{1/2}\, ln\ x \ .$$

Un cert recíproc és:

$$HR \Longleftrightarrow \forall\ \varepsilon > 0 \quad \left| \frac{\pi(x) - Li(x)}{Li(x)} \right| < x^{-1/2+\varepsilon} \quad ,$$

per a tot x prou gran.

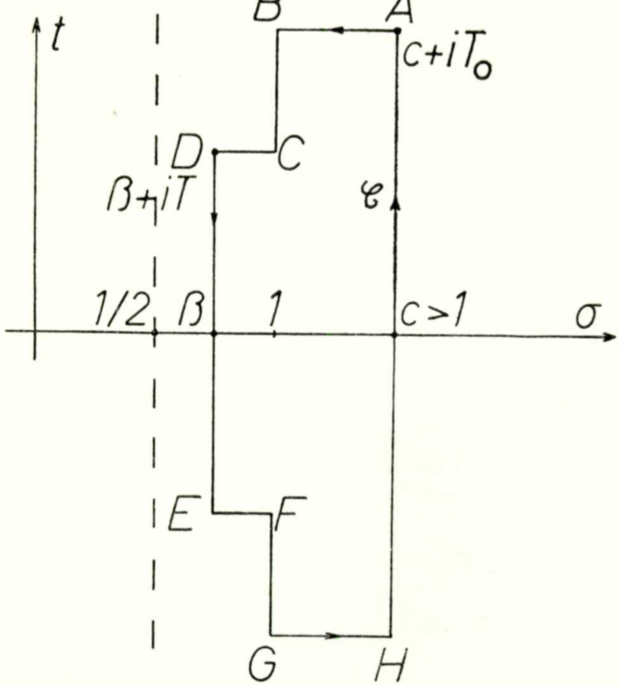


Fig. 6. Corba usada en la demostració del teorema dels nombres primers.

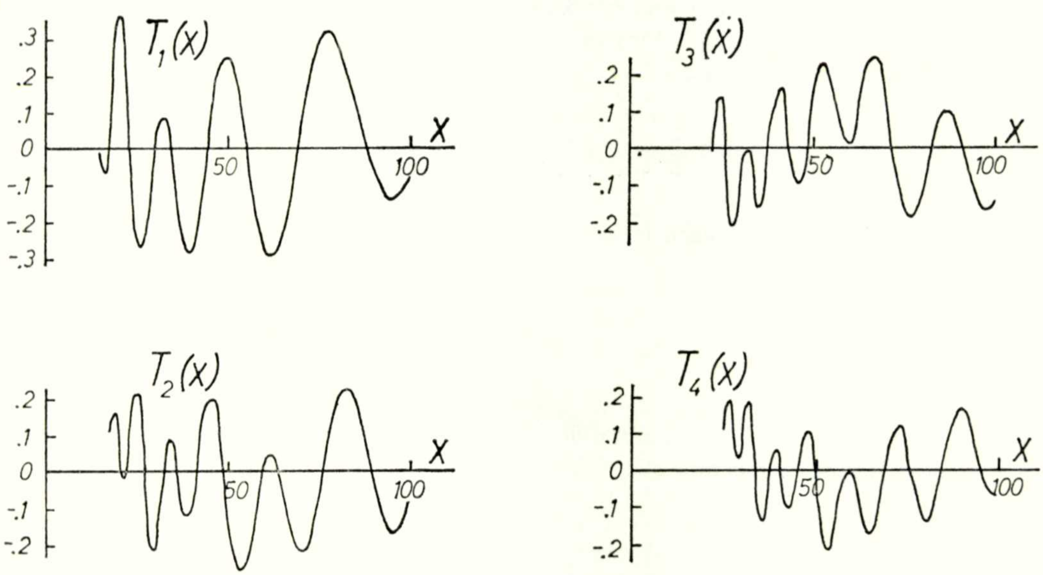


Fig. 7. Termes oscillatoris en la expressió de $\pi(x)$. (Font: Zagier).

Sigui

$$M(x) = \sum_{n<x} \mu(n) \quad ;$$

llavors si

$$\forall\, \varepsilon > 0,\ \lim_{x\to\infty} M(x)\, x^{-1/2-\varepsilon} = 0 \implies HR\ .$$

(Se sap que

$$\forall\, x \geqq 6\ ,\quad |M(x)| < \frac{ax}{(ln\, x)^{\alpha}}$$

on, per exemple, $a = 2.9$, $\alpha = 1$, i que

$$|M(x)| < A\, x\, exp(-\alpha\sqrt{ln\, x}\,)$$

amb A,α explícites).

Un altra propietat equivalent a HR és: Sigui $x \in R_+$. Consideren els trencats $\in [0,1]$ (de Farey) amb denominador natural més petit que x, ordenats de petit a gran, i sigui A(x) el cardinal del conjunt de trencats. (Com a exemple, si x=5.5 surten

$$\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},1 \quad ;$$

A(x) = 10). Si δ_i = ièsim terme de la sèrie — $i/A(x)$, llavors:

$$HR \iff \forall\, \varepsilon > 0\ ,\ \sum_{1}^{A(x)} |\delta_i| = o(x^{1/2+\varepsilon}) \quad \text{quan} \quad x\to\infty\ .$$

Siguin $\{1/2 + it_n\}$ els zeros de ξ en el semiplà superior si és certa HR amb $t_n\uparrow$. Hom conjectura que

$$\underline{\lim}\ \frac{ln(t_{n+1} - t_n)}{ln\, n} \in (-1,0)$$

i potser val —1/3, i que

$$\overline{\lim}\ (t_{n+1} - t_n)\ln t_n = +\infty .$$

Alguns resultats més sobre els zeros són:
Teorema (Bohr-Landau): Per a tot δ positiu, tots els zeros excepte una proporció «infinitesimal» disten menys que δ de Re s = 1/2. ζ no te zeros a

$$\left\{ s = \sigma + it \;\middle|\; |t| \geq 21,\ \sigma \geq 1 - \frac{1}{9.6459 \ln(|t|/17)} \right\}.$$

Destaquem que una regió sense zeros es correspon amb una

$$\phi \mid \psi(x) = x + O(x\, exp(-\phi(x))) .$$

Rosser, Yohe i Schoenfeld han demostrat rigorosament que els 3502500 primers zeros (per banda) de ξ tenen Re = 1/2. Per a ells la part imaginària és menor o igual que 1894438,51... En donem uns quants a la taula 5. Càlculs de Gram, Lehmer, Rosser, Yohe i Schoenfeld, entre d'altres, posen en evidència que ξ té propietats sobre la recta crítica que suggereixen la no certesa de HR. Per exemple, prop del zero número 13.4×10^6 n'hi ha dos de separats per 4.4×10^{-4}. Pel que hom coneix, entre dos extrems consecutius de ξ sobre la recta crítica hi ha un zero, però si per a valors més grans de t entre dos extrems seguits no travessava l'eix, llavors HR seria falsa.

De l'estudi amb detall dels zeros de ζ surten nombroses acotacions dels tipus:

$$\text{Si} \quad x > 10^8 , \quad |\theta(x) - x|, \quad |\psi(x) - x| < .0242269\ x/\ln x \quad .$$

$$x > 1 \implies |\theta(x) - x| \quad |\psi(x) - x| < \eta_k\, x/\ln^k x ,$$

on

$$\eta_2 = 8.7 , \quad \eta_3 \quad 1200, \quad \eta_4 = 1.86*10^7 .$$

Majorant $|\zeta(s)|$ a la banda crítica, tenim

$$\pi(x) - Li(x) = O(x\ exp(-.009 \frac{\ln^{.6} x}{\ln_2^{.2} x})) .$$

Fórmules similars apareixen per a

$$M(x)\,,\quad \Pi(x)\,,\quad \rho(x)\,,\quad \psi(x)\quad .$$

D'ací surten corol·laris com és ara que

$$\{p/q\,,\quad p,q\in \mathcal{P}\}$$

és dens a R_+.

Sigui

$$N(T) = \#\{\text{Zeros de } \xi \text{ amb } t \leq T\}.$$

Hom coneix que

$$N(T) = \frac{T}{2\pi}\left(ln\,\frac{T}{2\pi} - 1\right) + S(T) + \frac{7}{8} + O\left(\frac{1}{T}\right)\quad ,$$

on

$$S(t) = \frac{1}{\pi}\,Arg\,\zeta\left(\frac{1}{2} + it\right)\quad .$$

Hom conjectura

$$S(t) = O\left(\left(\frac{ln\ t}{ln_2 t}\right)^{.5}\right)\quad .$$

Si bé no se sap si és cert

$$|\psi(x) - x| < C\,x^{1/2}\,(ln\ x)^2\ ,$$

sí que tenim una idea de l'oscil·lació de $\psi(x) - x$. Diem

$$f = \Omega_+\, g \quad \text{si}\quad \overline{\lim}\ \frac{f}{g} > 0\ ;\ f = \Omega_-\, g \quad \text{si}\quad \underline{\lim}\ \frac{f}{g} < 0$$

(límits potser no acotats). $\Omega_\pm$ és Ω_+ i Ω_-.

Littlewood demostrà que

$$\psi(x) - x \quad i \quad \theta(x) - x \quad \text{són} \quad \Omega_\pm(\sqrt{x}\ ln_3 x)$$

d'una banda, i d'una altra que

$$\pi(x) - Li(x) \quad i \quad \Pi(x) - Li(x) \quad \text{són} \quad \Omega_\pm\left(\frac{\sqrt{x}}{ln\ x}\ ln_3 x\right)$$

De fet els límits no estan acotats en aquests casos. A més, si

$$x \in [2,T]\,,\quad T \geq exp_5 35\quad ,$$

el nombre de canvis de signe de

$$\pi(x) - Li(x) \quad \text{és} \quad \geqq ln_4 T/e^{35} .$$

Fórmules per al nombre de canvis de signe, de «grans» canvis de signe

$$|\pi(x) - Li(x)| > \frac{1}{100} \frac{\sqrt{x}}{ln\, x} ln_3 x ,$$

de canvis de signe de la mitjana sobre intervals de llargària x/ln_2x, i per a intervals que garanteixen canvi de signe, amb HR o sense, amb constants efectives o sense, han estat donades per Pintz.

Ara bé, tots els exemples donats indiquen que $\pi(x)$ és més petit que Li (x). Així és per a $x < 10^{13}$. Lehman demostrà que entre 1.53×10^{1165} i 1.65×10^{1165} hi ha 10^{500} nombres seguits amb $\pi(x)$ més gran que Li (x). Raonaments de tipus estadístic, concretament la hipòtesi segons la qual

$$(R(x) - \pi(x))\, ln\, x/\sqrt{x}$$

es comporta com una llei normal N (0,.21), (vegeu fig. 8) porten a esperar que $\pi(x)$ és més gran que Li (x) per a algun $x = 0(10^{900})$. Per contra, sembla que no podem esperar canvi de signe abans de 10^{100}.

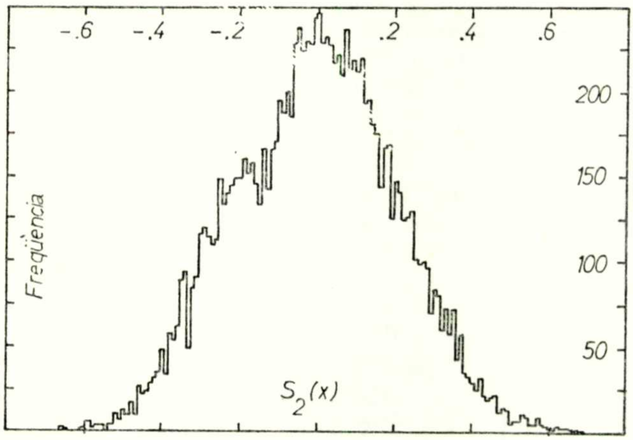


Fig. 8. Distribución estadística de la funció $s_2(x)$ fins a $x = 8 \times 10^{10}$. (Font : Brent).

Malgrat el comportament asimptòtic segons el t.n.p., localment poden haver-hi discrepàncies notables. Així la taula 6 mostra fins a 82 milions en quins blocs d'1 milió de nombres el nombre de primers és més gran que en blocs

milió	Δπ	π	milió	Δπ	π	milió	Δπ	π
1	78498		31	58120		61	55930(+2)	
2	70435		32	57836(-1)		62	55555(-5)	
3	67883		33	57842(+1)		63	55706(+1)(-1)	
4	66330		34	57712		64	55780(+2)	
5	65367		35	57396(-2)		65	55468(-3)	
6	64334		36	57487(+1)		66	55559(+2)(-2)	
7	63799		37	57361(-1)		67	55644(+3)	
8	63129		38	57343(-1)		68	55575(+3)	
9	62712		39	57436(+3)		69	55332(-2)	
10	62090	664579	40	57252	2433654	70	55390(+1)(-1)	4118064
11	61938		41	57102		71	55309(-1)	
12	61543		42	56864(-2)		72	55285(-2)	
13	61192		43	56915(+1)		73	55431(+4)	
14	60825		44	56849(-1)		74	55165(-1)	
15	60627		45	56776(-1)		75	55050(-1)	
16	60426		46	56893(+3)		76	55307(+3)	
17	60184		47	56640		77	54924(-4)	
18	60053		48	56451(-1)		78	55009(-2)(+1)	
19	59683		49	56387(-1)		79	54900(-3)	
20	59557	1270607	50	56603(+2)	3001134	80	54938(+2)(-2)	4669382
21	59336		51	56360		81	55027(+4)	
22	59318		52	56349		82	55021(+4)	
23	58960		53	56209				
24	58901		54	56151				
25	58805		55	55997(-2)				
26	58600		56	56130(+1)				
27	58538		57	56105(+1)				
28	58365		58	55901(-2)				
29	58246		59	55978(+1)				
30	58183	1857859	60	55801(-1)	3562115			

Taula 6 (font autor)

Desenes de milió	$\Delta\Pi$	Π	Desenes de milió	$\Delta\Pi$	Π
201	467612		221	464533(-3)	
202	467063		222	464680(+2)(-2)	
203	466201(-4)		223	464681(+3)(-1)	
204	466708(+1)		224	464455(-3)	
205	466522(+1)		225	464478(+1)(-2)	
206	465920(-5)		226	464362(-2)	
207	466245(+2)(-1)		227	464841(+7)	
208	466068(+1)(-3)		228	464499(+3)	
209	466106(+2)(-1)		229	464156	
210	465794(-3)	102886526	230	464133	112184940
211	466323(+6)		231	463456(-3)	
212	466071(+3)		232	463631(+1)(-1)	
213	464998(-4)		233	463699(+2)	
214	464860(-5)		234	463620(+1)	
215	465831(+3)		235	463131(-3)	
216	465334(+2)(-1)		236	463388(+1)	
217	465180(+2)(-1)		237	463337(+1)	
218	465475(+4)		238	463113(-1)	
219	464656(-4)		239	463186(+2)	
220	464868(+2)	107540122	240	462946	116818447

Taula 7 (font autor)

p	$\pi(p)$	$r_1(p)$	$r_2(p)$	$s_1(p)$	$s_2(p)$
110102617	6308959	239	-446	.4218	-.7871
36917099	2256804	692	260	1.9845	.7456
179845447	10022306	331	-514	.4691	-.7285
11467849447	518601767	8594	3352	1.8589	.7250

Valors grans de $s_2(p)$

Taula 8 (font Brent 1975)

anteriors (el símbol +k indica en quants) o més petit que en blocs següents (i — k indica en quants). Si prenem blocs de 10 milions, la freqüència dels primers va disminuint, però per a $x > 2 \times 10^9$ els blocs de 10 milions ens donen anomalies. No així els de 100 milions (taula 7), etc.

Quant a $R(x) - \pi(x)$, la taula 8 mostra

$$r_2(x) = R(x) - \pi(x), \quad r_1(x) = Li(x) - \pi(x), \quad s_i = r_i \, ln\, x/\sqrt{x}$$

i la taula 9, intervals en els quals r_2 té signe constant. L'amplada creixent dels intervals indica que caldrà refusar la hipòtesi de Shanks:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{2}^{n} s_2(k) = 0 \quad ,$$

ja que sembla que no existeix el límit. Brent proposa

$$\lim \frac{1}{ln\, n} \sum_{2}^{\infty} \frac{s_2(k)}{k} = 0 \quad .$$

Recordem que

$$HR \Longrightarrow s_i = O(ln^2 x) \quad .$$

Preguntes similars respecte a la distribució de primers ens les podem fer per a primers en progressions aritmètiques. Si $(a,k) = 1$ es té que a $\{a + \dot{k}\}$ hi ha infinits primers (Dirichlet). Sigui

$$\pi^k(x) = \#\{p \leq x, \; p \in \mathcal{P}, \; p \equiv a \pmod{k}\} \quad .$$

Llavors

$$\pi^k(x) \sim \frac{\pi(x)}{\phi(k)} \quad .$$

Existeix C_0 positiu, calculable, tal que

$$\inf\left(p \mid p \in \mathcal{P} \cap \{a+\dot{k}\}\right) \leq k^{c_0} \quad , \forall\, k \geq 0, \forall\, a, \quad \text{si } (a,k)=1 \text{ (Linnik)}.(c_0 < 10^4) \quad .$$

Per a acabar, anem una mica al detall dels primers vistos de prop. Poden haver-hi primers molt junts?. Els que disten 2 entre ells es diuen bessons. No se sap si n'hi ha infinits. Bombieri, però, ha demostrat que hi ha infinits primers p tals que $p+2$ té menys de 5 factors primers. Golubew conjecturà l'existència d'un parell de bessons entre n^3 i $(n+1)^3$, per a tot n natural.

A diferència d'allò que passa amb tots els primers, Viggo Brun demostrà que

$$\sum_{p \text{ primer bessó}} \left(\frac{1}{p} + \frac{1}{p+2}\right) < \infty \quad .$$

Hardy i Littlewood conjecturaren que si r és més gran o igual que 1 i n és gran, el nombre de primers p més petits o iguals que n tals que p+2r és el proper primer, és

$$\pi_{2r}(n) \sim A_{r,1}\int_2^n \frac{dx}{(\ln x)^2} \quad ,$$

on

$$A_{r,1} = 2c_2 \prod_{q|r,\, q\in\mathcal{P}-\{2\}} \frac{q-1}{q-2}$$

i c_2 és la dita constant dels bessons:

$$c_2 = \prod_{q\in\mathcal{P}-\{2\}} \frac{1-2/q}{(1-1/q)^2} = .66016 \;\ldots\; .$$

El valor de r pot ésser arbitràriament gran:

$$p_n = \sup\{p \in \mathcal{P} | p \leqq m! + 1\} \Longrightarrow p_{n+1} - p_n \geqq m \; .$$

Malgrat les experiències numèriques i els raonaments heurístics i «estadístics» que donen suport a la conjectura HL, aquesta no ha estat demostrada. Sembla que cal afegir-hi alguns termes (Brent) i escriure

$$\pi_{2r}(n) \sim \int_2^n \sum_{k=1}^{r} A_{r,k}(\ln x)^{-k-1} \quad ,$$

de manera que el terme de HL seria el dominant quan n tendeix a infinit.

Per a nombres entre 10^6 i 10^9 hi ha bon acord entre la distribució teòrica de «forats» de longitud 2,4,6,8,... i la real. Com són alguns dels 50769035 forats, podem veure-ho a la taula 10. Quan n creix, les freqüències més elevades es desplacen cap a r grans.

Tornem als bessons. Els més grans que hom en coneix són $76\times 3^{139} \pm 1$. Tots són de tipus $6k \pm 1$ (excepte (3,5)). Les irregularitats dels primers s'accentuen en els bessons. Per exemple

$$\pi_2(\underbrace{\pi^{-1}(352500)}_{5061919}) - \pi_2(\underbrace{\pi^{-1}(350000)}_{5023307}) = 183 \; .$$

a	b	a/b	min r_2	max r_2
9278	11046	1.191	-6	0
324090	369790	1.141	-33	0
4889994	5530998	1.131	-84	0
34225760	38856760	1.135	0	260
53087472258	58483092228	1.102	-5288	0

Intervals $[a,b]$ amb $r_2(p)$ de signe constant

Taula 9 (font Brent 1975)

r	nombre de forats
1	3416337
2	3416536
3	6076242
4	2689540
5	3477688
6	4460952
7	2460332
8	1843216
9	3346123
10	1821461
11	1567507
12	2364792
13	1118410
14	1218009
15	2176077

Taula 10 (font Brent 1974)

n	$\pi_2(n)$	$r_3(n)$
10^3	35	11
10^6	8169	79
10^9	3224506	802
$2\cdot10^9$	6388041	984
$4\cdot10^9$	11944438	1032
$6\cdot10^9$	17244409	-770
$8\cdot10^9$	22384176	-248
10^{10}	27412679	-1262
$2\cdot10^{10}$	51509099	-4667
$4\cdot10^{10}$	96956707	1869
$6\cdot10^{10}$	140494397	1555
$8\cdot10^{10}$	182855913	-985

Taula 11 (font Brent 1975)

Admetent HL, surt 214. Si

$$r_3(x) = Li_2(x) - \pi_2(x) \quad , \text{ on } \quad Li_2(x) = 2c_2\int_2^x \frac{dt}{ln^2 t} ,$$

tenim la taula 11.

Les oscil·lacions de r_3, són molt llargues:

$$r_3(x) > 0, \ \forall x \in [3 \ , 1.36\cdot 10^6] \cup [1.5\cdot 10^8 \ , 3.06\cdot 10^9] \ ,$$

$$r_3(x) < 0, \ \forall x \in [1.52\cdot 10^6 \ , 3.52\cdot 10^7] \cup [1.19\cdot 10^{10} \ , 2.71\cdot 10^{10}]$$

(vegeu fig. 9). De tota manera fins a 8×10^{10},

$$|r_3(x) \, ln\, x/\sqrt{x}| < 2.3 \quad .$$

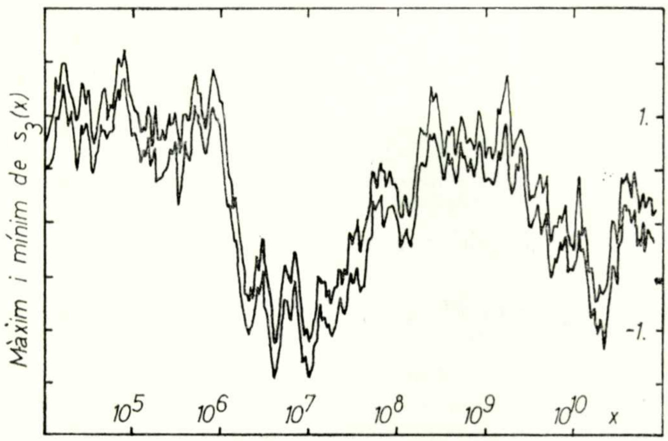


Fig. 9. Oscil·lacions de les discrepàncies en la distribució dels primers bessons: $s_3(x) = (Li_2(x) - \pi_2(x)) ln\ x/\sqrt{x}$. (Font : Brent).

Si admetem HL, la constant dita de Brun

$$\sum_{p \text{ primer bessó}} \frac{1}{p} + \frac{1}{p+2}$$

val $1.9021604 \pm 5\times 10^{-7}$.

Una generalització dels primers poc separats la constitueixen les k-ples, és a dir, conjunts de nombres de la forma

$$n+d_1 , \ n+d_2 , \ldots , \ n+d_k$$

tots ells primers. Sigui

$$\pi_d(N) = \#\{n \leqq N \mid n+d_i \in \mathcal{P},\ i=1 \div k\} \ .$$

Hom conjectura que

$$\pi_d(N) \sim S_d \frac{N}{ln^k N} \ , \quad \text{si} \quad S_d \neq 0, \quad \text{on} \quad S_d = \prod_{p \in \mathcal{P}} \frac{p^{k-1}(p-\nu_d(p))}{(p-1)^k}$$

i $\nu_d(p)$ = nombre de classes mod p ocupades per $d_1, d_2 \ldots, d_k$. Si suposem la conjectura certa uniformement per a

$$1 \leqq d_1 < \ldots < d_k \leqq h$$

pei a cada k, i

$$P_r(h,N) = \#\{n \leqq N \mid \#((n,n+h] \cap \mathcal{P}) = r\} \ ,$$

tenim

$$P_r(h,N) \sim N \frac{e^{-\lambda}\lambda^r}{r!} \quad \text{per } N \to \infty \ , \ h \sim \lambda \, ln \, N \ .$$

Quan al nombre de primers en un interval petit, es demostra que

$$\exists \ c > 0 \mid \text{si} \quad \mu \geqq \lambda \geqq 1, \ \#\{n \leqq N \mid \pi(n+\lambda \, ln \, N) - \pi(n) > \mu\} \leqq N \, e^{-cN/\lambda} \ .$$

Una pregunta natural és com cal triar $d_1 < d_2 < \ldots < d_k$ perquè $S_d \neq 0$ i $d_k - d_1$ sigui el més petit possible. La taula 12 diu com poden estar de compactats els primers, i en presenta exemples. Per exemple, si k = 4, $d_k - d_1$ val 8 com a mínim. D'aquestes quaternes n'hi ha 165 fins a un milió, 295 entre un milió i dos milions i 897 fins a 10 milions. Si p és diferent de 5 i p, p+2, p+6, p+8 són primers, llavors p = 11,101 o 191 (mod 210).

Una conjectura que hom pot fer tenint en compte la convexitat de Li (x) és la de subadditivitat de π:

$$\pi(x+y) \leqq \pi(x) + \pi(y) \ , \ \forall x,y \in N \ .$$

Hensley i Richards han provat, però, que està en contradicció amb la de les k-ples, i sembla que la certa és aquesta. Llavors caldrà obtenir

$$x,y \mid \pi(x+y) > \pi(x) + \pi(y)$$

k	d_k-d_o	d_i	exemples
4	8	0,2,6,8	5,11,101,191,821,1481,1871,...
5	12	0,2,6,8,12	5,11,101,1481,16061,19421,21011,..
		0,4,6,10,12	7,97,1867,3457,5647,15727,16057,..
6	16	0,4,6,10,12,16	7,97,16057,19417,43777,1091257, 1615837,...
7	20	0,2,6,8,12,18,20	11,165701,1068701,11900501, 15760091,18504371,21036131,...
		0,2,8,12,14,18,20	5639,88799,284729,626609,855719, 1146779,6560999,...
8	26	0,2,6,8,12,18,20,26	11,15760091,25658441,...
		0,2,6,12,14,20,24,26	17,1277,113147,2580647,20737877,..
		0,6,8,14,18,20,24,26	88793,284723,855713,1146773, 6560993,...
9	30	0,2,6,8,12,18,20,26,30	11,...
		0,2,6,12,14,20,24,26,30	17,1277,113147,...
		0,4,6,10,16,18,24,28,30	13,113143,...
		0,4,10,12,18,22,24,28,30	88789,855709,...
10	32	0,2,6,8,12,18,20,26,30,32*	
11	36	0,2,6,8,12,18,20,26,30,32,36*	
12	42	0,2,6,8,12,18,20,26,30,32,36,42*	
13	48	0,2,6,8,12,18,20,26,30,32,36,42,48*	
		0,2,8,14,18,20,24,30,32,38,42,44,48*	
		0,2,12,14,18,20,24,30,32,38,42,44,48*	
14	50	0,2,6,8,12,18,20,26,30,32,36,42,48,50*	
15	56	0,2,6,8,12,18,20,26,30,32,36,42,48,50,56*	
		0,2,6,12,14,20,24,26,30,36,42,44,50,54,56*	
16	60	0,2,6,12,14,20,26,30,32,36,42,44,50,54,56, 60*	
17	66	0,2,6,12,14,20,24,26,30,36,42,44,50,54,56, 62,66*	
		0,4,6,10,16,18,24,28,30,34,40,46,48,54,58, 60,66*	
18	70	0,4,6,10,16,18,24,28,30,34,40,46,48,54,58, 60,66,70*	
19	76	0,4,6,10,12,16,24,30,34,40,42,46,52,54,60, 66,70,72,76*	
		0,4,6,10,16,18,24,28,30,34,40,46,48,54,58, 60,66,70,76*	
20	80	0,2,6,8,12,20,26,30,36,38,42,48,50,56,62, 66,68,72,78,80*	
21	84	0,2,8,12,14,18,24,30,32,38,42,44,50,54,60, 68,72,74,78,80,84*	
22	90	0,2,6,8,12,20,26,30,36,38,42,48,50,56,62, 66,68,72,78,80,86,90*	
		0,4,6,10,12,16,24,30,34,40,42,46,52,54,60, 66,70,72,76,82,84,90*	

* = amb cada k-pla de valors d_i (com 0,2,6,8,12,18,20,26,30,32) existeix la simètrica (0,2,6,12,14,20,24,26,30,32)

Taula 12

És immediat de veure que si p és el primer element d'una k-pla minimal,

$$\pi(p+d_k-d_1) = \pi(p) + k \quad .$$

Si $\pi(d_k - d_1)$ és més petit que k i hi ha un tal p, la subadditivitat és falsa. Allò que sí que és cert és que:

$$x \geqq 11 \Longrightarrow \pi(2x) < 2\pi(x) \quad .$$

A l'extrem contrari dels bessons hi ha els primers molt separats. Podem definir la funció g: $\mathbb{N} \to \mathbb{N}$ així:

$$g(r) = \min \{p_k \in \mathcal{P} \mid p_{k+1}-p_k \geqq 2r\} \quad .$$

És monòtona creixent, i la taula 13 ens dóna valors en els quals g salta. Hom conjectura

$$\lim_{x\to\infty} \sup_{p_r \leqq x} \frac{p_{n+1}-p_n}{(ln\, p_n)^2} = 1 \quad .$$

La figura 10 ens diu el valor de

$$\phi = \frac{p_{n+1}-p_n}{(ln\, p_n)^2}$$

per als valors p de la taula anterior. Això en particular implicaria que

$$\forall \varepsilon > 0, \exists N \mid \forall x > N \Longrightarrow [x, x+(1+\varepsilon)\, ln^2 x]$$

té un primer. Se sap (Nicolas, 1969) que per a tot ε positiu, hi ha infinits n tals que

$$p_{n+1} - p_n > (e^\gamma - \varepsilon)\, ln\, p_n \frac{ln_2 p_n \; ln_4 p_n}{ln_3^2 p_n}$$

i que o bé hi ha *a* positiu tal que hi ha infinits primers

$$p_i \mid p_{i+1} - p_i > p_i^a \;,$$

o bé

$$\forall \delta > 1, \; \#\{p_i \leqq x \mid p_{i+1} - p_i \geqq \frac{1}{\delta} e^\gamma\, ln\, x \frac{ln_2 x \; ln_4 x}{ln_3^2 x}\} \geqq x^{1-1/\delta} \quad .$$

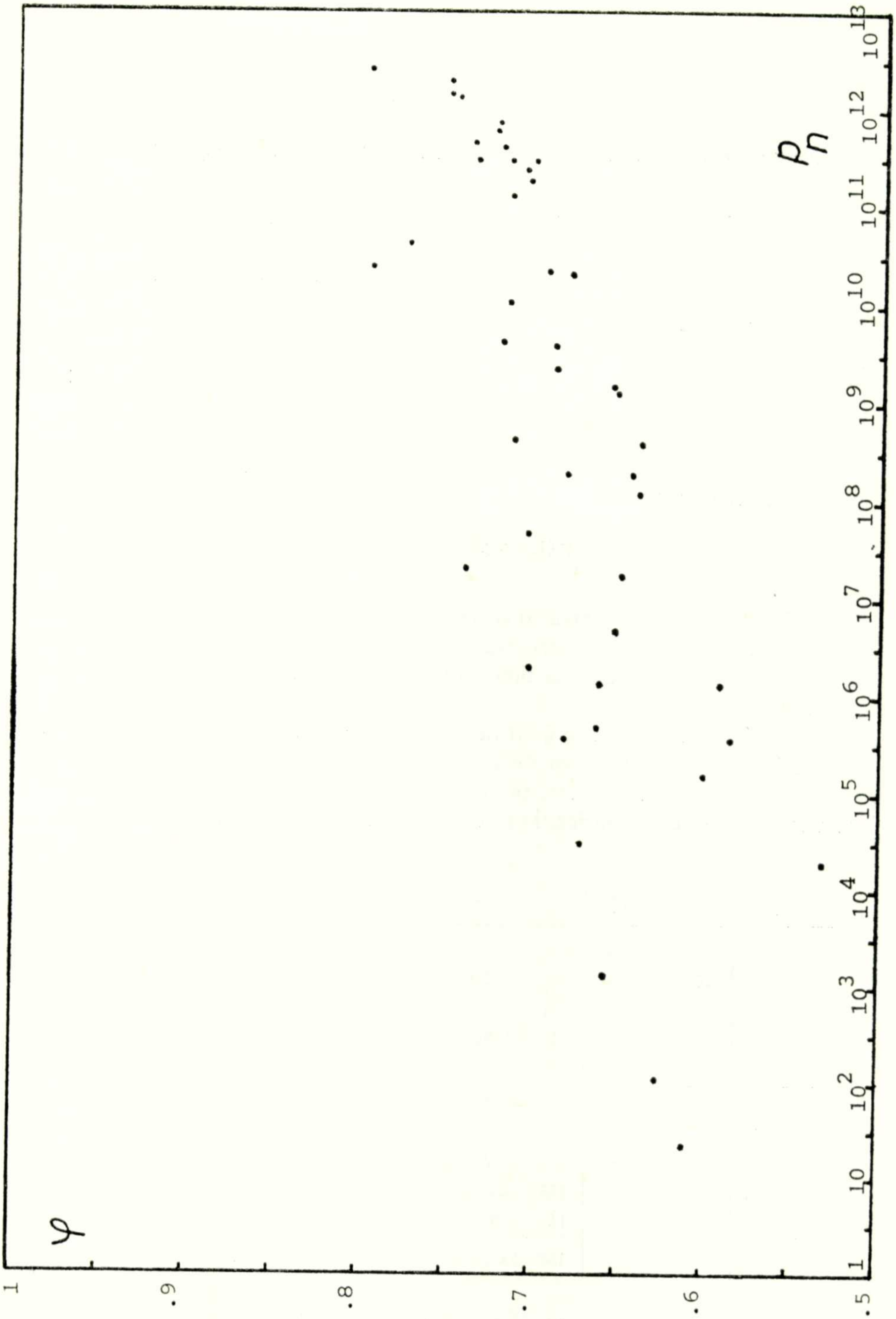


Fig. 10. Valors de la funcio $\varphi=(p_{n+1}-p_n)\ /\ (\ln p_n)^2$ per primers pels que $p_{n+1}-p_n$ és més gran que per tots els anteriors.

D'altres conjectures sobre els primers molt junts o molt separats són:

$$\psi(x+h) - \psi(x) = h + O(h^{1/2} x^{\varepsilon}) \quad \text{per} \quad 1 \leq h \leq x \ .$$

$$\sum_{p_n \leq x,\ p_{n+1}-p_n > \alpha\, ln\, p_n} 1 \sim e^{-\alpha}\pi(x) \quad \text{per} \quad \alpha > 0 \quad \text{fixat.}$$

Si

$$\rho(h) = \overline{\lim}\, (\, \pi(x+h) - \pi(x)) \ ,$$

per a h gran hom tindrà

$$\pi(h) < \rho(h) < \frac{2h}{ln\ h} \ .$$

Una qüestió natural és: Si la distribució dels primers està relacionada amb la funció ζ i, de fet, un coneixement «exacte» de la ζ (zeros, comportament asimptòtic, sumació, etc.) ens dóna tota la informació sobre $\pi(x)$, amb què està relacionada $\pi_d(x)$?.

Hem vist que l'infinit conjunt dels primers té infinits aspectes que atrauen l'atenció dels matemàtics des de fa centúries. Moltes de les coses que hom conjectura semblen raonables, però n'hi ha d'altres que, bé que verificades en unes quantes experiències, hom no veu la raó que en faci plausible la cer-

r	g(r)	r	g(r)	r	g(r)	r	g(r)	r	g(r)
1	3	26	19609	105	20831323	177	4302407359	257	304599508537
2	7	36	31397	110	47326693	191	10726904659	258	416608695821
3	23	43	155921	111	122164747	192	20678048297	266	461690510011
4	89	48	360653	117	189695659	197	22367084959	267	614487453523
7	113	56	370261	124	191912783	228	25056082087	270	738832927927
9	523	57	492113	125	387096133	232	42652618343	291	1346294310749
10	887	59	1349533	141	436273009	234	127976334671	294	1408695493609
11	1129	66	1357201	144	1294268491	237	182226896239	301	1968188556461
17	1327	74	2010733	146	1453168141	243	241160624143	326	2614941710599
18	9551	77	4652353	160	2300942549	245	297501075799		
22	15683	90	17051707	168	3842610773	250	303371455241		

Taula 13 (font Brent 1975 i autor)

tesa. No puc resistir la temptació de cloure amb la conjectura de Gilbreath: Si hom escriu en una fila els primers ordenats, i a sota una altra fila amb les diferències primeres, i a sota una altra amb les diferències de la fila anterior, preses sempre en valor absolut, i hom va construint files així, sempre el primer element de cada fila es + 1!.

REFERÈNCIES

APOSTOL, T. M.: «Introduction to Analytic Number Theory», Springer, 1976.

BÀYER, P.: «El Teorema de Fermat», *Pub. Mat. U.A.B.* 2 (1976), 94-110.

BRENT, R.: «The First Occurrence of Large Gaps between successive Primes», *Math. Comp.* 27 (1973), 959-963.

BRENT, R.: «The Distribution of Small Gaps between successive Primes», *Math. Comp.* 28 (1974), 315-324.

BRENT, R.: «Irregularities in the Distribution of Primes and Twin Primes», *Math. Comp.* 29 (1975), 43-56.

BRILLHART, J., LEHMER, D. H., SELFRIDGE, J. L.: «New Primality Criteria and Factorizations of $2^m \pm 1$», *Math. Comp.* 29 1975), 620-647.

BROWDER, F. E. (Editor): «Mathematical developments arising from Hilbert problems», Proceed. Symp. Pure Math. XXVIII (1976), A.M.S.

Científicos Griegos I, Ed. Aguilar, 1970.

EDWARDS, H. M.: «Riemann's Zeta Function», Academic Press, 1974.

ELLISON, W. J., MÈNDES FRANCE, M.: «Les nombres premiers», Hermann, 1975.

GALLAGHER, P. X.: «On the distribution of primes in short intervals», *Mathematika* 23 (1976), 4-9.

GOLOMB, S W.: «Formulas for the next prime», *Pacific J. of Math.* 63 (1976), 401-404.

HALLYBURTON, J. C., BRILLHART, J.: «Two new factors of Fermat Numbers», *Math. Comp.* 29 (1975), 109-112.

JONES, J. P. et al.: «Diophantine Representation of the set of Primes», *Amer. Math. Monthly* 83 (1976), 449-464.

Journées Arithmétiques de Caen, *Astérisque* 41-42 (1977), S.M.F.

KNUTH, D.: «The Art of Computer Programming II: Seminumerical Algorithms», Addison-Wesley, 1969.

LEHMER, D. H.: «A new Factorization Technique using Quadratic Forms», *Math Comp.* 28 (1974), 625-635.

LEVINSON, N.: «More than one third of zeros of Riemann's Zeta function are on $\sigma = ½$», *Advances Math.* 13 (1974), 383-436.

MORRISON, M. A. BRILLHART, J.: «A Method of factoring and the factorization of F_7», *Math. Comp.* 29 (1975), 183-205.

RIEMANN, B.: «Über die Anzahl der Primzahlen unter einer gegebener Grösse», *Monatber. Preuss. Akad. Wiss. (Berlin)* (1859), 671-680.

ROSSER, J. B., SCHOENFELD, L.: «Sharper Bounds for the Chebyshev functions $\theta(x)$, $\psi(x)$», *Math. Comp.* 29 (1975), 243-269.

SHANKS, D., WRENCH, J. W.: «Brun's constant», *Math. Comp.* 28 (1974), 293-299.

SIERPINSKI, W.: «Elementary Theory of Numbers», Monografie Matematyczne, Tom 42, P.A.N., 1964.

ZAGIER, D.: «The First 50 Million Prime Numbers», *The Math. Intelligencer* 0 (1977), 7-19.