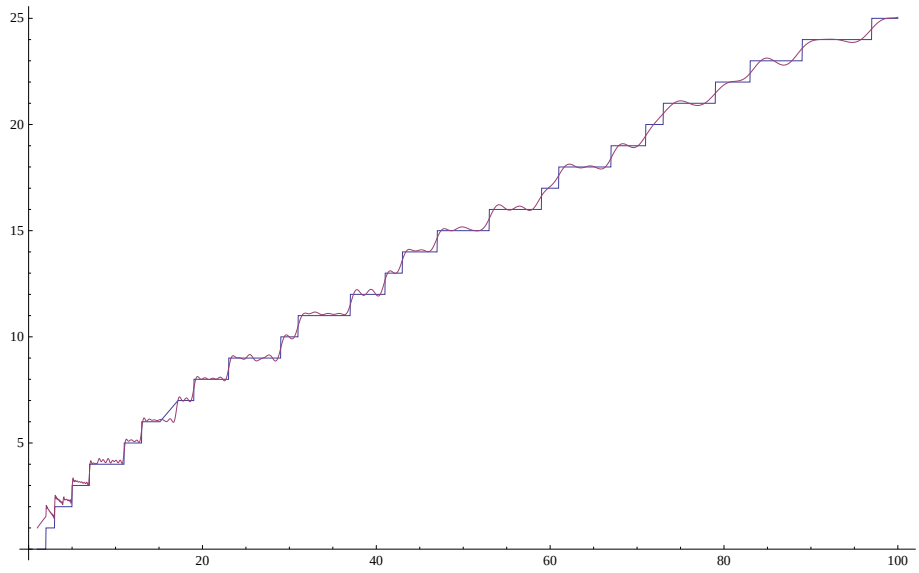
On s'amaguen els nombres primers?



Els zeros de ζ saben on s'amaguen els nombres primers...

Autor: Craig

Curs 2011 / 2012

Índex

Índex de figures

Índex de taules

Capítol 1

Introducció

Quan vaig començar a estudiar batxillerat a l'INS Santa Eugènia el curs 2010/2011, la tutora ens va parlar sobre una assignatura que es deia treball de recerca. Pel que explicava, no semblava una assignatura normal, amb un professor a classe i tots els alumnes escoltant. L'assignatura consistia a escollir un tema i fer una recerca sobre una pregunta inicial que en dèiem hipòtesi. Calia doncs, escollir un tema, fer-nos una pregunta i, amb l'ajut d'un tutor, intentar respondre la hipòtesi inicial que ens havíem plantejat. Però abans de plantejar cap hipòtesi, ens havíem de plantejar quin tema volíem tractar.

Vaig triar un treball de recerca centrat en un tema matemàtic perquè em cau molt bé el professor de matemàtiques que he tingut durant els cursos de batxillerat. També perquè m'agraden molt les matemàtiques. De fet, un dels meus objectius en acabar el batxillerat seria, precisament, estudiar matemàtiques a la universitat. Hi ha hagut altres factors que han influït en l'elecció d'un tema matemàtic per al meu treball de recerca. Per exemple, jo fa dos anys que vaig arribar a Catalunya i encara tinc alguns problemes amb la llengua. Escollint un tema matemàtic he pogut centrar-me més en les idees que s'hi presentaven. Però això va ser només al principi. Finalment he hagut d'escriure el treball i no ha estat gens fàcil, ni per a mi ni per al meu tutor, amb qui he passat moltes hores redactant el treball que ara teniu a les mans.

Inicialment vaig pensar que en un tema matemàtic hi hauria menys paraules complicades d'entendre amb el vocabulari que tinc assolit fins ara. A més, el llenguatge i els signes matemàtics són entesos arreu del món. Vaig pensar que seria més fàcil per a mi. Vaig parlar amb el meu professor de matemàtiques i ell em va plantejar tres temes per fer el treball de recerca: alguna qüestió relacionada amb els nombres primers; fer una ampliació dels nombres complexos; o estudiar el comportament de les òrbites dels satèl·lits al voltant de la Terra.

Finalment, vaig triar un tema relacionat amb els nombres primers. En una segona reunió amb el meu tutor vam plantejar l'objectiu d'aquest treball, que és el d'intentar respondre la pregunta següent:

> *" Quants nombres primers hi ha sota d'un nombre donat?"*

Per poder respondre aquesta pregunta vaig haver de preparar-me matemàticament. Les matemàtiques que aprenem als cursos de batxillerat no són prou especialitzades per respondre la hipòtesi plantejada. Tècnicament parlant, es tracta d'una qüestió d'una branca de les

matemàtiques anomenada *teoria analítica de nombres*. És una assignatura que s'estudia en els cursos superiors de la llicenciatura en matemàtiques. Però, com que les qüestions que pretén resoldre estan relacionades amb els nombres naturals, he pogut endinsar-me una mica en el tema. Aquesta preparació matemàtica es va traduir a fer classes de matemàtiques durant el mes de juliol amb el meu tutor, que m'anava plantejant problemes que jo havia de resoldre. Durant els mesos següents vaig anar recollint i processant informació que al final he hagut de *garbellar* (paraula que he après en la redacció d'aquest treball), ordenar i escriure.

A proposta del meu tutor, el Sr. Berenguer Sabadell, vaig decidir redactar el treball amb un processador de textos pensat expressament per a la redacció i composició de textos científics, LaTeX. Això va complicar el meu aprenentatge atès que, a banda d'aprendre les matemàtiques necessàries per poder fer el treball, també vaig haver d'aprendre a utilitzar LaTeX. Després d'un inici difícil, he anat entenent com treballar amb LaTeX i ara puc assegurar que l'escriptura de fórmules i expressions matemàtiques és més senzill amb aquest processador. A més, he pogut comprovar com la majoria dels llibres i documents que he consultat també estan escrits amb LaTeX. Aquest aprenentatge també em serà útil a l'hora d'enfrontar-me amb els meus estudis universitaris.

1.1 Metodologia del treball

El mètode utilitzat per escriure un treball científic no és lineal. No es treballa mai començant pel principi i seguint de manera seqüencial fins arribar al final. S'han d'anar escrivint algunes parts, deixar-ne d'altres per més endavant i, finalment, ordenar-ho tot i escriure-ho ben escrit. El treball que teniu a les mans es composa dels següents capítols:

- Un primer capítol on s'expliquen les eines matemàtiques elementals de la teoria de nombres. En aquest capítol es defineixen conceptes elementals i s'enuncien resultats fonamentals per a l'estudi de les qüestions relacionades amb els nombres primers. Hi ha un apartat d'una eina especial que no s'explica a batxillerat: les congruències. Per escriure aquesta part he consultat, principalment, les fonts [1], [4],[6], [10] i [11].

- El següent capítol és el propi del tema de recerca. S'hi fa una exposició històrica de la qüestió de la quantitat de nombres primers. A continuació s'exposen els resultats que he pogut anar obtenint a partir de les meves recerques. Les fonts consultades per redactar aquest capítol han estat [1], [3], [5], [6], [7], [8], [9] i [11].

  El capítol acaba amb una part pràctica, utilitzant el programa *Mathematica*© . Per poder-la fer he necessitat consultar detalladament [2] i [12]

- A les conclusions explico les reflexions finals que he pogut fer en acabar el treball. N'hi ha de dos tipus: unes, més matemàtiques, on explico què he après matemàticament parlant i com està actualment la qüestió que jo em vaig plantejar a l'inici del treball; unes altres, més personals, sobre com he canviat com alumna i persona i el que he après de manera genèrica.

Espero que la lectura d'aquest treball us ajudi a estimar els nombres primers com me'ls ha fet estimar a mi durant l'elaboració del que teniu entre mans.

Capítol 2

Eines matemàtiques

2.1 Introducció

Aquest capítol està estructurat en dues seccions.

En la primera secció s'expliquen les eines matemàtiques elementals de la teoria de nombres tals com la divisibilitat, el màxim comú divisor i els nombres primers i compostos. El resultat principal d'aquesta primera secció és *Teorema Fonamental de l'Aritmètica* que demostra que tot nombre enter més gran que 1 es pot descomposar com a producte de factors primers de manera única, llevat de l'ordre dels factors. Per acabar la secció s'exposen tres aplicacions dels conceptes presentats: com calcular quants divisors té un nombre; com calcular tots els divisors d'un nombre; i com calcular de manera eficient el màxim comú divisor de dos nombres (*Algoritme d'Euclides*).

En la segona secció introduïm els conceptes fonamentals de la *teoria de congruències* o *aritmètica modular*. Aquestes eines foren introduïdes per C.F.Gauss (1777-1855) i simplifiquen d'una manera notable molts problemes relatius a la divisibilitat dels enters. Els resultats principals d'aquesta segona secció són la *Congruència de Fermat* i la seva generalització, la *Congruència d'Euler*.

Durant aquest capítol utilitzarem la notació matemàtica clàssica. El conjunt dels nombres naturals el representarem amb la lletra $\mathbb{N}$ i el conjunt dels nombres enters el representarem amb la lletra $\mathbb{Z}$. És a dir,

$$\mathbb{N} = \{1, 2, 3, \dots\}$$
$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

Normalment designarem els nombres enters amb les lletres llatines a, b, c,... i també amb les lletres n, m,... però reservarem les lletres p, q i r per designar nombres primers. Si en necessitem més de tres, utilitzarem subíndexs: p_1, p_2, etc.

Per fer més entenedors tots els conceptes que es presenten, després de cada definició o teorema, mostrarem un petit exemple numèric del que s'acaba de definir o enunciar.

Per demostrar algunes propietats d'aquest capítol utilitzarem la següent propietat dels nombres naturals.

Principi d'inducció matemàtica

Si Q és un conjunt de nombres naturals tals que:

1. $1 \in Q$
2. $n \in Q \quad \Rightarrow \quad n+1 \in Q$

Aleshores, tot $n \geq 1$ pertany a Q (és a dir, $Q = \mathbb{N}$)

Aquest principi ens assegura que tot subconjunt Q de $\mathbb{N}$ complint les propietats següents:

- L'1 pertany a aquest subconjunt.
- Suposant que un cert element n pertany a Q, aleshores el següent element, $n+1$, també hi pertany

Aleshores, aquest subconjunt Q ha de ser tot el conjunt $\mathbb{N}$. Quan suposem que la propietat que volem demostrar és certa per a l'element n, diem que *apliquem la hipòtesi d'inducció* (H.I.).

Veiem amb un exemple com podem utilitzar aquest principi per demostrar certes propietats dels nombres naturals.

Exemple. Demostrem la igualtat $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$

1. Comprovem primer que la igualtat és certa per a $n = 1$

$$1 = \frac{1 \cdot (1+1)}{2} = 1 \quad \surd$$

2. Suposem que la propietat és certa fins a un cert n. Volem demostrar que la propietat també ho és per al proper nombre, $n+1$. És a dir, en llenguatge matemàtic,

$$\text{Si} \quad 1+2+3+\cdots+n = \frac{n(n+1)}{2} \quad \overset{?}{\Rightarrow} \quad 1+2+3+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2}$$

Però

$$\underbrace{1+2+3+\cdots+n}_{\text{Per H.I.}} + (n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2}+1\right) = \frac{(n+1)(n+2)}{2}$$

Per tant, els elements n de $\mathbb{N}$ pels quals la igualtat és certa són, precisament, tots els elements de $\mathbb{N}$. Així doncs, per calcular la suma dels 100 primers nombres naturals, només cal fer un petit càlcul[1]:

$$1 + 2 + 3 + \cdots + 100 = \frac{100 \cdot 101}{2} = 5050$$

[1] S'explica que C.F. Gauss raonà aquest càlcul a l'edat de 9 anys. El seu professor proposà la suma als alumnes per tenir-los entretinguts una bona estona. Al cap de pocs segons Gauss exclamà *"Ligget se'!"* (Ja està!), deixant admirat al seu professor.

2.2 Divisibilitat

Definició 2.2.1 (Divisibilitat)
Diem que d **divideix** *n, i escrivim $d \mid n$, si $n = c \cdot d$ per a un cert $c \in \mathbb{Z}$. Diem també que n és* **múltiple** *de d, que d és un* **divisor** *de n, o que d és un* **factor** *de n. Si d no divideix a n escrivim $d \not| n$.*

Exemple.

- 4 és un divisor de 20 atès que $20 = 4 \cdot 5$. Escrivim $4|20$. Evidentment 5 també és divisor de 20, i 20 és múltiple de 4 i 5.
- Tots els divisors de 20 són: 1, 2, 4, 5, 10 i 20.
- 2 no és divisor d'11, ni de cap nombre senar. És a dir, $2 \not| 2k+1$ per a $k \in \mathbb{Z}$

Teorema 2.2.1
La divisibilitat estableix una relació entre nombres enters amb les següents propietats elementals:

(a)	$n \mid n$	*(propietat reflexiva)*
(b)	$d \mid n \quad i \quad n \mid m \quad \Rightarrow \quad d \mid m$	*(propietat transitiva)*
(c)	$d \mid n \quad i \quad d \mid m \quad \Rightarrow \quad d \mid (an + bm)$	*(propietat lineal)*
(d)	$d \mid n \quad \Rightarrow \quad ad \mid an$	*(propietat multiplicativa)*
(e)	$ad \mid an \quad i \quad a \neq 0 \quad \Rightarrow \quad d \mid n$	*(propietat de simplificació)*
(f)	$1 \mid n$ *(1 divideix a tots els enters)*	
(g)	$n \mid 0$ *(cada enter divideix a zero)*	
(h)	$0 \mid n \quad \Rightarrow \quad n = 0$ *(el zero només divideix a zero)*	
(i)	$d \mid n \quad i \quad n \neq 0 \quad \Rightarrow \quad \lvert d\rvert \leq \lvert n\rvert$	*(propietat de comparació)*
(j)	$d \mid n \quad i \quad n \mid d \quad \Rightarrow \quad \lvert d\rvert = \lvert n\rvert.$	
(k)	$d \mid n \quad i \quad d \neq 0 \quad \Rightarrow \quad (n/d)\lvert n.$	

Totes aquestes propietats són de fàcil demostració. Com a exemple, demostrem la propietat lineal.

$$\left.\begin{array}{lllll} d|n & \Rightarrow & n = c_1 d & \Rightarrow & an = ac_1 d = k_1 d \\ d|m & \Rightarrow & m = c_2 d & \Rightarrow & bm = bc_2 d = k_2 d \end{array}\right\} \Rightarrow an + bm = (k_1 + k_2)d \quad \Rightarrow \quad d|an + bm$$

Un altre concepte important de divisibilitat és el del **màxim comú divisor** de dos nombres.

Definició 2.2.2 (Màxim comú divisor, mcd)
Si un d divideix dos nombres enters a i b, aleshores d s'anomena divisor comú *de a i b. Així, 1 és un divisor comú de tot parell d'enters a i b. Donats dos enters qualssevol existirà sempre un divisor comú que serà el més gran de tots els divisors comuns. Aquest nombre s'anomena* màxim comú divisor *d'aquests dos nombres. Escrivim*

$$\text{mcd}(a, b) = d$$

Si dos nombres compleixen $\text{mcd}(a, b) = 1$ *diem que són* primers entre si *o* coprimers.

Exemple.

- $a = 16$ i $b = 40 \quad \Rightarrow \quad \text{mcd}(16, 40) = 8$
- $a = 15$ i $b = 31 \quad \Rightarrow \quad \text{mcd}(15, 31) = 1$ (15 i 31 són coprimers).
- $a = 32$ i $b = 79 \quad \Rightarrow \quad \text{mcd}(32, 79) = 1$ (32 i 79 són coprimers).

Teorema 2.2.2
El màxim comú divisor compleix les següents propietats:

(a) mcd*(a,b)*=mcd*(b,a)* *(propietat commutativa)*

(b) mcd*(a,*mcd*(b,c))*=mcd*(*mcd*(a,b),a)* *(propietat associativa)*

(c) mcd*(ac,bc)=c* mcd*(a,b)* *(propietat distributiva)*

(d) mcd*(a,1)*=mcd*(1,a)=1*

Teorema 2.2.3 (Lema d'Euclides)
Si $a \mid bc$ i si mcd*(a,b)=1, aleshores $a \mid c$.*

Exemple. $7 \mid 42$ i mcd(7,3)=1, per tant $7 \mid 14$.

Definició 2.2.3 (Nombre primer i nombre compost)
Un nombre enter n s'anomena primer si $n > 1$ i els únics divisors possibles de n són 1 i n. Si n no és primer s'anomena compost.

Exemple. Els nombres primers inferiors a 100 són:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 i 97.

Teorema 2.2.4
Cada nombre enter $n > 1$ o és primer o és producte de nombres primers.

Demostració.
Utilitzem inducció sobre n. El teorema és clar per $n = 2$. Suposem que és cert per a cada enter $< n$. Aleshores si n no és primer té un un divisor $d \neq 1$, $d \neq n$. Per tant $n = cd$, i $c \neq n$. Aleshores, tant c com d són $< n$ i > 1, de manera que cada un d'ells és producte de nombres primers, i per tant n també ho és.

□

El següent teorema és un dels resultats més remarcables de la teoria de nombres, tant per la importància del resultat com per la "bellesa matemàtica" de la demostració.

Teorema 2.2.5 (Euclides)
Existeix una infinitat de nombres primers.

Demostració.

Suposem que només existeixen un nombre finit de primers, per exemple p_1, p_2, ..., p_n. Sigui $N = 1+p_1p_2 \dots p_n$. Com que $N > 1$, pel teorema anterior, o N és primer o és compost. Però N no és primer atès que N és més gran que cada un dels p_i, i hem suposat que no n'hi ha més. Però cap p_i divideix a N. Si $p_i \mid N$ aleshores p_i dividiria la diferència $N - p_1p_2 \dots p_n = 1$ (això per la propietat lineal de la divisibilitat). Però això no pot ser perquè cada p_i és més gran que 1.

□

Un primer aspecte remarcable d'aquesta demostració és l'ús que fa de l'*"argument per contradicció"*. La demostració comença suposant que hi ha un darrer nombre primer. Això és, es comença admetent el contrari d'allò que es pretén demostrar i fent un seguit de raonaments matemàtics correctes, s'obté una contradicció, una impossibilitat. Aquesta contradicció és que 1 sigui divisible per un nombre primer més gran que 1. La conclusió final de la demostració és que la suposició inicial havia de ser falsa: el conjunt dels nombres primers no pot ser finit. Ha de ser infinit.

Un segon aspecte de la demostració és subtil i sol ser malinterpretat. La demostració no prova, com molta gent sol confondre, que N és un nombre primer. Es pot comprovar que el nombre N construït d'aquesta manera és primer per a n =1, 2, 3, 4 i 5. En efecte, tenim els nombres

$$\begin{aligned}
n = 1 &\quad\Rightarrow\quad N = p_1 + 1 = 2 + 1 = 3 \qquad \text{és primer.}\\
n = 2 &\quad\Rightarrow\quad N = p_1p_2 + 1 = 2 \cdot 3 + 1 = 7 \qquad \text{és primer.}\\
n = 3 &\quad\Rightarrow\quad N = p_1p_2p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31 \qquad \text{és primer.}\\
n = 4 &\quad\Rightarrow\quad N = p_1p_2p_3p_4 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \qquad \text{és primer.}\\
n = 5 &\quad\Rightarrow\quad N = p_1p_2p_3p_4p_5 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \qquad \text{és primer.}
\end{aligned}$$

En canvi, si fem $n = 6$ obtenim $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$, que és un nombre compost. El que passa ara és que els factors primers de 30 031 són més grans que el "suposat" màxim primer $p_6 = 13$. Els nombres primers de la forma $N = p_1p_2 \dots p_n + 1$ s'anomenen *primers primerals*

Un darrer comentari. Aquest teorema és molt important i té molta transcendència en la història de les matemàtiques. Hom podria pensar que la llista de nombres primers és finita, que n'hi ha un que és el més gran de tots. Si avancem en la llista dels nombres naturals observarem que els nombres primers són cada vegada més difícils de trobar, que els forats numèrics entre nombres primers es van fent més i més grans. Això és així perquè, com més gran és un nombre, menys possibilitats té de ser primer atès que hi ha molts més candidats a poder-lo dividir. Una simple observació d'aquest fet és que hi ha 25 nombres primers entre 1 i 100, mentre que n'hi ha 168 entre 1 i 1000. En termes de proporció, un 25% dels nombres entre 1 i 100 són primers i la proporció de nombres primers baixa fins al 16.8% entre 1 i 1000.

Teorema 2.2.6
Si un primer p no divideix a a, aleshores $\text{mcd}(p, a) = 1$.

Demostració.
Sigui $d = \text{mcd}(p, a)$. Aleshores $d \mid p$, per tant o $d = 1$ o $d = p$. Però $d \mid a$, per tant $d \neq p$ atès que $p \nmid a$. Com a consequència $d = 1$.
□

Exemple. $8 \nmid 19$, aleshores $\text{mcd}(8, 19) = 1$.

Teorema 2.2.7
Si un primer p divideix a ab, aleshores $p \mid a$ o $p \mid b$. En general, si un primer p divideix a un producte $a_1 ... a_n$, aleshores p divideix a un, com a mínim, dels factors.

Demostració.
Suposem que $p \mid ab$ i que $p \nmid a$. Veiem que $p \mid b$. Segons el teorema anterior, $\text{mcd}(p, a) = 1$. I segons el lema d'Euclides, $p \mid b$.

Per demostrar l'afirmació més general s'utilitza inducció sobre n, nombres de factors.
□

El següent teorema és un dels resultats més importants de la divisibilitat.

Teorema 2.2.8 (Teorema Fonamental de l'Aritmètica)
Cada enter $n > 1$ es pot representar com a producte de factors primers de manera única, llevat de l'ordre dels factors.

Exemple. 18 només es pot escriue com $2 \cdot 3 \cdot 3$ i amb dos 3 i un 2 només podem fer el 18.

Demostració.
Utilitzem inducció sobre n. El teorema és cert per $n = 2$. Suposem, aleshores, que és cert per a tot enter més gran que 1 i més petit que n. Volem veure que és cert també per a n. Si n és primer no cal demostrar res. Per tant, suposem que n és compost i que admet dues descomposicions, que són

$$n = p_1 p_2 \ \ldots \ p_s = q_1 q_2 \ \ldots \ q_t \tag{2.1}$$

Volem demostrar que $s = t$ i que cada p_i és igual a algun q_j. Atès que p_1 divideix el producte $q_1 \cdot q_2 \ \ldots \ q_t$ ha de dividir a un, com a mínim, dels factors q. Ordenem els factors $q_1, q_2, \ldots, q_t$ de manera que $p_1 \mid q_1$. Aleshores $p_1 = q_1$ ja que p_1 i q_1 són primers. Per tant,

$$\frac{n}{p_1} = p_2 \ \ldots \ p_s = q_2 \ \ldots \ q_t$$

Atès que n és compost, $s > 1$ i $t > 1$. Aleshores $1 < \dfrac{n}{p_1} < n$. La hipòtesi d'inducció ens diu que les dues descomposicions de $\dfrac{n}{p_1}$ són idèntiques, prescindint de l'ordre dels factors. Per tant $s = t$ i les dues descomposicions de (2.1) són també idèntiques, si prescidim de l'ordre dels factors.
□

Nota: En la descomposició d'un enter n, un cert primer p pot apàreixer més d'una vegada. Si els factors primers diferents de n són $p_1, \ldots, p_r$, i si p_i apareix a_i vegades com a factor, escriurem:

$$n = p_1^{a_1} \ldots p_r^{a_r} = \prod_{i=1}^{r} p_i^{a_i} \tag{2.2}$$

(el símbol $\prod$ s'anomena *productori* i significa que hem de fer el producte de les expressions contigües, variant l'índex i des de 1 fins a r)

Aquesta expressió s'anomena descomposició de n en factors primers. També és possible expressar el nombre 1 d'aquesta manera amb cada un dels exponents a_i igual a 0.

2.2.1 Eines de divisibilitat

1. Càlcul de la quantitat de divisors que té un nombre

La descomposició de n en factors primers ens permet calcular la quantitat de divisors de n. Sigui $\text{div}(n)$ la funció que ens dóna el número total de divisors de n. El següent teorema ens explica com calcular $\text{div}(n)$.

Teorema 2.2.9
La quantitat de divisors d'un nombre n es calcula a partir de (2.2)

$$n = \prod_{i=1}^{r} p_i^{a_i} \quad \Rightarrow \quad div(n) = \prod_{i=1}^{r} (a_i + 1)$$

Exemple.

(a) $n = 41 = 41^1 \quad \Rightarrow \quad$ div(41)=1+1=2. Com que 41 és un nombre primer, només té dos divisors: 1 i 41.

(b) $n = 3240 = 2^3 \cdot 3^4 \cdot 5 \quad \Rightarrow \quad$ div(3240)=(3+1)(4+1)(1+1)=40

Demostració.

- Observem, en primer lloc que si $n = p$ és un nombre primer, només té 2 divisors: 1 i p. En aquest cas $n = p \quad \Rightarrow \quad a = 1$ i, efectivament, $\text{div}(p)=(1+1)=2$.
- Si n és la potència d'un nombre primer, $n = p^k$, aleshores els únics divisors de n són 1, p, p^2, ..., p^k, és a dir, n té $k+1$ divisors. En aquest cas $n = p^k \quad \Rightarrow \quad a = k$ i, efectivament, $\text{div}(n)=k+1$.
- Si n és el producte de dues potències de nombres primers, $n = p^k \cdot q^r$, aleshores cada un dels $k+1$ divisors de la forma p^l, amb l variant des de 0 fins a k (solem escriure $l = 0 \div k$), pot combinar amb cada un dels $r+1$ divisors de la forma q^s, amb $s = 0 \div r$. Per tant, tenim $(k+1) \cdot (r+1)$ divisors. Efectivament

$$n = p^k \cdot q^r \quad \Rightarrow \quad \text{div}(n) = (k+1)(r+1)$$

- En el cas més general, si $n = \prod_{i=1}^{k} p_i^{a_i}$, cada terme de la forma $p_l^{a_l}$ participa amb $(a_l + 1)$ divisors que, combinant-se entre ells, ens dóna l'expressió

$$\text{div}(n) = (a_1 + 1)(a_2 + 1)...(a_k + 1) = \prod_{i=1}^{k}(a_i + 1)$$

□

2. Càlcul de tots els divisors d'un nombre

Per calcular tots els divisors d'un cert n ens cal saber combinar tots els possibles productes que podem aconseguir amb els factors de la seva descomposició en factors primers.

Si $n = \prod_{i=1}^{k} p_i^{a_i}$, aleshores qualsevol divisor d de n és de la forma $d = \prod_{i=1}^{k} p_i^{b_i}$ on cada b_i varia entre 0 i a_i ($b_i = 0 \div a_i$). Per exemple, si volem calcular els 6 divisors de $n = 12 = 2^2 \cdot 3$ ens cal considerar totes les possibles combinacions $2^k \cdot 3^l$ on k =0, 1, 2 i $l = 0, 1$. Aquestes 6 possibles combinacions són:

$$\begin{array}{lll} 2^0 \cdot 3^0 = 1 & 2^1 \cdot 3^0 = 2 & 2^2 \cdot 3^0 = 4 \\ 2^0 \cdot 3^1 = 3 & 2^1 \cdot 3^1 = 6 & 2^2 \cdot 3^1 = 12 \end{array}$$

Si n és relativament petit, o la seva descomposició en factors primers té pocs factors, aleshores és fàcil calcular tots els possibles divisors de n. Però si n és relativament gran, o en la seva descomposició en factors primers n'apareixen més de dos, resulta més convenient confeccionar una *taula de divisors*. Veiem amb un exemple com es construeix una taula de divisors.

Considerem $n = 448448 = 2^6 \cdot 7^2 \cdot 11 \cdot 13 \quad \Rightarrow \quad \text{div}(448448) = 7 \cdot 3 \cdot 2 \cdot 2 = 84$. És a dir, 448448 té 84 divisors. El primer que fem és buscar els divisors de 448448 que són exactament potència d'un nombre primer. Aquests divisors els tenim agrupats en 4 famílies diferents:

$$\begin{array}{ll} 2^6 : & 2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 32,\ 2^6 = 64 \\ 7^2 : & 7^0 = 1,\ 7^1 = 7,\ 7^2 = 49 \\ 11^1 : & 11^0 = 1,\ 11^1 = 11 \\ 13^1 : & 13^0 = 1,\ 13^1 = 13 \end{array}$$

La taula 2.2.1 mostra com es poden calcular la resta de divisors del 448448. Col·loquem en la primera columna de la taula els divisors de la família més llarga (en el nostre cas, 2^6) i en la primera fila els divisors de la segona família més llarga (en el nostre cas, 7^2). El divisor 1 és comú a les dues famílies i, per tant, l'escrivim només una vegada. Sempre que acabem d'escriure una família farem una línia vertical de separació. Quan vulguem introduir una nova família (en el nostre cas, 11^1 i 13^1) multiplicarem tots els

elements de la família, excepte 1, per tots els nombres de la primera fila fins a l'última línia vertical. És a dir, quan introduïm la família 11^1 – que té els membres 1 i 11 – multiplicarem 11 per 1, 3, 9 i farem una línia vertical. D'aquesta manera la primera fila haurà augmentat fins a 6 termes. El 13 l'haurem de multiplicar per tots aquests 6 termes, doblant-se la dimensió horitzontal de la taula que passarà de 6 a 12 elements. Observem que les dimensions de la taula són $7 \times 12 = 84$ coincidint amb la quantitat total de divisors de 448448. Acabarem calculant els divisors fent el producte cartesià fila per columna. Si ho hem fet bé, a l'extrem inferior dret ens ha de sortir $n = 448448$.

Taula 2.1: Els 84 divisors de $n = 448448$.

1	7	49	11	77	539	13	637	91	143	1001	7007
2	14	98	22	154	1078	26	1274	182	286	2002	14014
4	28	196	44	308	2156	52	2548	364	572	4004	28028
8	56	392	28	616	4312	104	5096	728	1144	8008	56056
16	112	784	176	1232	8624	208	10192	1456	2288	16016	112112
32	224	1568	352	2464	17248	416	20384	2912	4576	32032	224224
64	448	3136	704	4928	34496	832	40768	5824	9152	64064	448448

3. Càlcul del màxim comú divisor de dos nombres

Normalment calculem $\mathrm{mcd}(a, b)$ a partir de les descomposions en factors primers de a i b. Si $a = \prod_{i=1}^{r} p_i^{a_i}$ i $b = \prod_{j=1}^{s} p_j^{b_j}$ aleshores, $\mathrm{mcd}(a,b) = \prod_{k=1}^{t} p_k^{c_k}$ on p_k és una base comuna de les descomposicions d'a i b i prenem c_k com l'exponent mínim de a_k i b_k.

Exemple.

$$\left.\begin{aligned} a &= 1428 = 2^2 \cdot 3 \cdot 7 \cdot 17 \\ b &= 11560 = 2^3 \cdot 5 \cdot 17^2 \end{aligned}\right\} \quad \Rightarrow \quad \mathrm{mcd} = (1428, 11560) = 2^2 \cdot 17 = 68$$

El càlcul anterior és un mètode pràctic per calcular $\mathrm{mcd}(a, b)$ quan es coneixen les descomposicions en factors primers de a i b. Tanmateix, obtenir aquestes descomposicions en factors primers pot comportar considerables càlculs i seria desitjable disposar d'un procediment que impliqués menys esforços. Existeix un procediment útil conegut amb el nom d'*algoritme d'Euclides*, que no requereix les descomposicions en factors primers de a i b. Aquest procediment es basa en divisions successives i fa ús del teorema següent:

Teorema 2.2.10 (de la divisió entera)
Donats dos enters a i b amb $b > 0$, existeix un únic parell d'enters q i r tals que

$$a = bq + r \qquad \text{amb } 0 \leq r < b$$

A més a més, $r = 0$ si, i només si, $b \mid a$. En aquest cas, diem que la divisió és exacta.

Observació. És important notar que en el teorema anterior es compleixen 2 condicions: $a = bq + r$ i $0 \leq r < b$. Per exemple, $23 = 7 \cdot 2 + 9$ no seria correcte atès que $9 > 7$. La divisió entera correcta en aquest cas és $23 = 7 \cdot 3 + 2$.

Teorema 2.2.11 (Algoritme d'Euclides)
Siguin dos enters positius a i b, de manera que $b \nmid a$. Escrivim $r_0 = a$, $r_1 = b$, i apliquem repetidament l'algoritme de divisió entera obtenint un conjunt de residus r_2, r_3,...r_n, r_{n+1} definits successivament per les relacions:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2\,, & 0 < r_2 < r_1\,,\\
r_1 &= r_2 q_2 + r_3\,, & 0 < r_3 < r_2\,,\\
&\vdots & \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n\,, & 0 < r_n < r_{n-1}\,,\\
r_{n-1} &= r_n q_n + r_{n+1}\,, & r_{n+1} = 0\,.
\end{aligned}$$

Aleshores r_n, l'últim residu no nul d'aquest procés, és el $\mathrm{mcd}(a,b)$.

Demostració.

Existeix un moment en què $r_{n+1} = 0$ atès que els r_i són decreixents i positius. L'última relació, $r_{n-1} = r_n q_n$ demostra que $r_n \,|\, r_{n-1}$. L'anterior a l'última prova que $r_n \,|\, r_{n-2}$. En efecte:

$$\left.\begin{aligned} r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n \end{aligned}\right\} \quad \Rightarrow \quad r_{n-2} = r_n(q_n \cdot q_{n-1} + 1) \quad \Rightarrow \quad r_n \,|\, r_{n-2}$$

Per inducció veiem que r_n divideix a cada r_i. En particular $r_n \,|\, r_1 = b$ i $r_n \,|\, r_0 = a$, per tant r_n és un divisor comú de a i b. Ara sigui d un altre divisor comú de a i b. La definició de r_2 prova que $d \,|\, r_2$. En efecte, si $d \,|\, a$ $(a = k_1 d)$ i $d \,|\, b$ $(b = k_2 d)$, la relació $a = bq_1 + r_2$ es pot escriure com:

$$k_1 d = k_2 d q_1 + r_2 \quad \Rightarrow \quad r_2 = d(k_1 - k_2 q_1) \quad \Rightarrow \quad d | r_2$$

La relació que segueix prova que $d \,|\, r_3$. Per inducció, d divideix a cada r_i. Per tant $d \,|\, r_n$. És a dir, r_n és el més gran dels divisors comuns de a i b. Això és $r_n = \mathrm{mcd}(a,b)$.

□

Per facilitar el càlcul del $\mathrm{mcd}(a,b)$, s'acostumen a posar els diversos nombres que intervenen a l'algoritme en la forma següent:

$$\begin{array}{cccccccc}
 & q_1 & q_2 & \dots & q_{k+1} & q_{k+2} & q_{k+3} & \\
a & b & r_1 & \dots & r_k & r_{k+1} & r_{k+2} & 0
\end{array} \qquad r_{k+2} = \mathrm{mcd}(a,b)$$

Exemple. Calculem el mcd de 48697 i 8550.

	5	1	2	3	1	1	19	
48697	8550	5947	2603	741	380	361	19	0

Per tant, mcd(48697, 8550)=19.

2.3 Congruències

En aquesta secció exposem els conceptes bàsics d'una eina fonamental en la teoria de nombres que fou introduïda per C.F. Gauss i que simplifica notablament molts conceptes i problemes relacionats amb la divisibilitat. S'anomena *teoria de congruències* o *aritmètica modular*. Un cop presentats els aspectes més fonamentals d'aquesta teoria, demostrarem alguns resultats bàsics que serien de difícil demostració només amb les eines elementals exposades fins ara.

Definició 2.3.1 (Nombres congruents mòdul m)
Donats enters a, b, m amb $m > 0$, diem que a i b són congruents mòdul m si, i només si, $a - b = km$, $k \in \mathbb{N}$, i escrivim:

$$a \equiv b \pmod{m}$$

En altres paraules, la congruencia $a \equiv b \pmod{m}$ equival a la relació de divisibilitat

$$m \mid a - b \qquad \text{(és a dir, } a - b \text{ és un múltiple de } m)$$

En particular, $a \equiv 0 \pmod{m}$ si, i només si, $m \mid a$. Per tant $a \equiv b \pmod{m}$ si, i només si, $a - b \equiv 0 \pmod{m}$. Si $m \nmid (a - b)$ escrivim $a \not\equiv b \pmod{m}$ i diem que a i b són *incongruents* mòdul m.

Exemple.

- 8 i 12 són congruents mòdul 4. Escrivim $8 \equiv 12 \pmod{4}$ o $12 \equiv 8 \pmod{4}$
- 17 i 29 són congruents mòdul 1, 2, 3, 4, 6 i 12.
- n és parell si, i només si, $n \equiv 0 \pmod{2}$.
- n és senar si, i només si $n \equiv 1 \pmod{2}$.
- $a \equiv b \pmod{1}$ per a cada a i b.

Un cop fixat $m > 0$, tenim repartit el conjunt $\mathbb{Z}$ en m grups diferents que s'anomenen *classes residuals*. Aquest nom prové del fet que si $a \equiv b \pmod{m}$, aleshores a i b tenen el mateix residu quan fem la divisió entera per m. Al conjunt resultant d'agrupar els nombres enters en classes residuals se l'anomena un $\mathbb{Z}$-mòdul i es representa per $\mathbb{Z}/m$

Exemple. $17 \equiv 29 \pmod{12}$. Fent la divisió entera, $17 = 12 \cdot 1 + 5$ i $29 = 12 \cdot 2 + 5$. En ambdós casos el residu a l'hora de dividir per 12 és 5. Per tant, 17 i 29 pertanyen a la mateixa classe a $\mathbb{Z}/12$

Com que els possibles residus a l'hora de dividir per m són 0, 1, 2, ...,$m - 1$, tenim els nombres enters classificats en m classes. Les classes sovint es noten com $\bar{0}$, $\bar{1}$, $\bar{2}$, ... $\overline{m-1}$. Es té el costum d'escollir com a representant de la classe el valor comprès entre 0 i $m - 1$.

Exemple. En l'exemple anterior, tant el 17 com el 29 pertanyen a la classe del 5. Escrivim $17 \in \bar{5}$ i $29 \in \bar{5}$ a $\mathbb{Z}/12$

Teorema 2.3.1
Les congruències estableixen una relació entre nombres enters amb les propietats següents:

(a) $a \equiv a \pmod m$ *(reflexivitat)*

(b) $a \equiv b \pmod m \quad \Rightarrow \quad b \equiv a \pmod m$ *(simetria)*

(c) $a \equiv b \pmod m \quad i \quad b \equiv c \pmod m \quad \Rightarrow \quad a \equiv c \pmod m$ *(transitivitat)*

(d) $a \equiv b \pmod m \quad i \quad c \equiv d \pmod m \quad \Rightarrow \quad a + c \equiv b + d \pmod m$

(e) $a \equiv b \pmod m \quad i \quad c \equiv d \pmod m \quad \Rightarrow \quad ac \equiv bd \pmod m$

(f) $a \equiv b \pmod m \quad i \quad c \in \mathbb{Z} \quad \Rightarrow \quad ac \equiv bc \pmod m$

(g) $a \equiv b \pmod m \quad i \quad d \mid m \quad \Rightarrow \quad a \equiv b \pmod d \quad i \quad a \equiv b \pmod{m/d}$

(h) $ac \equiv bc \pmod m \quad i \quad \mathrm{mcd}(c, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod m$

Amb les tres primeres propietats, diem que les congruències són *relacions d'equivalència*

Exemple. Veiem com funcionen algunes d'aquestes propietats.

(d) $\left.\begin{array}{l} 17 \equiv 8 \pmod 3 \\ 23 \equiv 20 \pmod 3 \end{array}\right\} \quad \Rightarrow \quad 40 \equiv 28 \pmod 3 \quad \Leftrightarrow \quad 40 - 28 = 12 = 4 \cdot 3$

(e) $\left.\begin{array}{l} 22 \equiv 8 \pmod 7 \\ 24 \equiv -4 \pmod 7 \end{array}\right\} \quad \Rightarrow \quad 528 \equiv -32 \pmod 7 \quad \Leftrightarrow \quad 528 - (-32) = 560 = 80 \cdot 7$

(f) $\left.\begin{array}{l} 34 \equiv 25 \pmod 3 \\ c = 7 \end{array}\right\} \quad \Rightarrow \quad 238 \equiv 175 \pmod 3 \quad \Leftrightarrow \quad 238 - 175 = 63 = 21 \cdot 3$

(g) $\left.\begin{array}{l} 17 \equiv 9 \pmod 8 \\ 4 \mid 8 \end{array}\right\} \quad \Rightarrow \quad 17 \equiv 9 \pmod 4 \text{ i } 43 \equiv 13 \pmod 2$

(h) $\left.\begin{array}{l} 65 \cdot 3 \equiv 23 \cdot 3 \pmod 7 \\ \mathrm{mcd}(3, 7) = 1 \end{array}\right\} \quad \Rightarrow \quad 65 \equiv 23 \pmod 7$

Observació. En aquesta darrera propietat, (h), és important notar el fet necessari que $\mathrm{mcd}(c, m) = 1$. En efecte, si això no es compleix, en simplificar la congruència pot ser que els dos nombres resultants no siguin congruents mòdul m. Per exemple,

$$38 = 19 \cdot 2 \equiv 20 = 10 \cdot 2 \pmod 6 \qquad \text{però} \qquad 19 \not\equiv 10 \pmod 6$$

Demostració.

Demostrarem només algunes propietats. Totes es dedueixen ràpidament de les propietats de divisibilitat (veure teorema 2.2.1).

(a) $m|a - a \quad \Rightarrow \quad m|0.$

(b) Si $m|(a - b)$ aleshores $m|(b - a)$.

(c) Si $m|(a-b)$ i $m|(b-c)$ aleshores $m|(a-b)+(b-c) = m|(a-c)$.

(e)
$$\left.\begin{array}{rcl} a \equiv b \pmod m & \Rightarrow & a = b + mk \\ c \equiv d \pmod m & \Rightarrow & c = d + ml \end{array}\right\} \quad \Rightarrow \quad ac = (b+mk)(d+ml)$$

$$\Rightarrow \quad ac = bd + bml + dmk + m^2kl \quad \Rightarrow \quad ac = bd + m\underbrace{(bl + dk + mkl)}_{K}$$

$$\Rightarrow \quad ac = bd + m \cdot K \quad \Rightarrow \quad ac \equiv bd \pmod m$$

(f) $a \equiv b \pmod m \quad \Rightarrow \quad a = b + mk.$

Sigui $c \in \mathbb{N}$. Multipliquem per c ambdós membres:

$$ac = (b+mk)c \quad \Rightarrow \quad ac = bc + mkc \quad \Rightarrow \quad ac = bc + ml \quad \Rightarrow \quad ac \equiv bc \pmod m$$

(g)
$$\left.\begin{array}{rcl} a \equiv b \pmod m & \Rightarrow & a = b + mk \\ \text{Si } d \,|\, m & \Rightarrow & m = dl \end{array}\right\} \quad \Rightarrow \quad a = b + dlk = b + dK$$

Per tant, $a \equiv b \pmod d$. Per altra banda,

$$a = b + dlk = b + lM \quad \Rightarrow \quad a \equiv b \pmod{m/d}$$

(h) $ac \equiv bc \pmod m \quad \Rightarrow \quad ac = bc + mk \quad \Rightarrow \quad c(a-b) = mk$

Però $\text{mcd}(c, m) = 1 \quad \Rightarrow \quad m|(a-b) \quad \Rightarrow \quad a \equiv b \pmod m$

□

Ara donarem alguns exemples que il·lustren utilitat de les congruències.

Exemple. *Criteri de divisibilitat per 9.* Un nombre enter $n > 0$ és divisible per 9 si, i només si, la suma dels dígits de la seva expressió decimal és divisible per 9. En efecte, si els dígits d'n en la seva expressió decimal són d_0, d_1, d_2, ...,d_k, aleshores

$$n = d_0 + 10d_1 + 100d_2 + \cdots + 10^k d_k = \sum_{l=0}^{k} a_l \cdot 10^l$$

Atès que

$$10 \equiv 1\,, \quad 100 \equiv 1\,, \quad \ldots \quad 10^k \equiv 1 \pmod 9$$

utilitzant les propietats (d) i (e) del teorema anterior,

$$n \equiv d_0 + d_1 + d_2 + \cdots + d_k \pmod 9$$

Observem que aquestes congruències també són vàlides mòdul 3. Aleshores, n serà divisible per 3 si, i només si, la suma dels seus dígits és divisible per 3.

Exemple. Els *nombres de Fermat* es defineixen com $F_n = 2^{2^n} + 1$. Els cinc primers nombres de Fermat són nombres primers i corresponen als valors:

$$F_0 = 3\,, \quad F_1 = 5\,, \quad F_2 = 17\,, \quad F_3 = 257\,, \quad F_4 = 65537$$

Amb l'ús de les congruències podem veure que F_5 és divisible per 641 sense haver de calcular explícitament el valor de F_5. Per fer-ho, considerem les potències 2^{2^n} mòdul 641. Tenim:

$$2^2 = 4\,, \quad 2^4 = 16\,, \quad 2^8 = 256\,, \quad 2^{16} = 65536 \equiv 154 \pmod{641}$$

Per tant,

$$2^{32} \equiv 154^2 = 23716 \equiv 640 \equiv -1 \pmod{641}$$

És a dir, $F_5 = 2^{32} + 1 \equiv 0 \pmod{641} \quad \Rightarrow \quad F_5$ és compost[2].

A continuació presentem dos resultats molt importants de la teoria de congruències.

2.3.1 Congruències de Fermat i Euler

Pierre de Fermat (1601-1665) fou un advocat francès apassionat per les matemàtiques i, especialment, per la teoria de nombres. Durant la seva vida va plantejar i resoldre molts problemes relacionats amb nombres primers i conceptes més complicats[3].

Fermat va observar el següent fet:

> *" Per a tot enter a i tot primer p, $a^p - a$ és un múltiple de p."*

Escrivim $a^p - a = a(a^{p-1} - 1)$. Si a és un múltiple de p, aleshores és clar que $a(a^{p-1} - 1)$ és també un múltiple de p. Però si p no divideix a a aleshores, aplicant el Lema d'Euclides (2.2.3), p ha de dividir $a^{p-1} - 1$. Aquesta afirmació es coneix amb el nom de *congruència de Fermat* i normalment s'enuncia utilitzant el llenguatge de les congruències.

Teorema 2.3.2 (Congruència de Fermat)
Si p és un nombre primer i a un enter qualsevol tal que $\mathrm{mcd}(a, p) = 1$, *aleshores es compleix*

$$a^{p-1} \equiv 1 \pmod{p} \tag{2.3}$$

Exemple.

1. $a = 4$ i $p = 5$, aleshores

$$4^{5-1} = 4^4 = 256 \quad \Rightarrow \quad 256 \equiv 1 \pmod{5}\,, \quad 256 = 5 \cdot 51 + 1$$

2. $a = 7$ i $p = 11$, aleshores

$$7^{10} = 282475249 \quad \Rightarrow \quad 282475249 \equiv 1 \pmod{11}\,, \quad 282475249 = 11 \cdot 25679568 + 1$$

[2]Fermat va conjecturar que tots els nombres de la forma $2^{2^n} + 1$ eren primers. Això es compleix per a n =0, 1, 2, 3 i 4. Fou Euler que descomposà $F_5 = 641 \cdot 6700417$. Des d'aleshores no s'ha trobat cap més nombre de Fermat primer. Els nombres de Fermat estan relacionats amb els polígons regulars construïbles amb regle i compàs.

[3]Un dels problemes més famosos és el *Darrer Teorema de Fermat* que afirma el següent:

L'equació $\quad x^n + y^n = z^n\,, \quad n \geq 3 \quad$ no té solucions a $\mathbb{Z} \quad$ llevat de les trivials

Aquest teorema va resistir 350 anys els intents de demostració per parts dels millors matemàtics del moment. Finalment, Andrew Wiles (1953) va donar una demostració definitiva els anys 1994 / 1995.

Observació. Si p no és un nombre primer, (2.3) no és cert. Per exemple,
$a = 2$ i $p = 6$, $2^5 = 32 \not\equiv 1 \pmod 6$, atès que $32 \equiv 2 \pmod 6$

Demostració.

Considerem els nombres 1, 2, 3,..., $p-1$. Com que p és primer, cadascun d'ells pertany a una classe residual mòdul p diferent, atès que són tots els possibles residus, llevat del 0, que podem obtenir en dividir un enter qualsevol per p.

Considerem ara els nombres

$$a \cdot 1, a \cdot 2, a \cdot 3, ..., a \cdot (p-1)$$

Ara també, cadascun d'aquests nombres pertany a una classe residual mòdul p diferent. Si no fos així, passaria

$$a \cdot k \equiv a \cdot l \pmod p \quad \Rightarrow \quad a \cdot k - a \cdot l \equiv 0 \pmod p \quad \Rightarrow \quad a \cdot (k-l) \equiv 0 \pmod p$$

Però com que $p \not| a$ (atès que mcd(a,p)=1), caldria que $p \mid k-l$ (aplicant el Lema d'Euclides 2.2.3) i, per tant, $k \equiv l \pmod p$, en contra del que hem dit a l'inici de la demostració.

Així doncs, cada un dels elements de la forma $a \cdot k$ serà congruent (de la mateixa classe) amb un dels nombres 1, 2, 3, ..., $p-1$.

$$a \cdot k \equiv l \pmod p$$

per a uns certs k i l complint $1 \leq l \leq p-1$ i $1 \leq k \leq p-1$. Aplicant $p-1$ vegades la propietat (e) del teorema 2.3.1,

$$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \ldots a \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod p$$
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$$

Però, com que mcd$(p,(p-1)!) = 1$, aplicant la propietat (h) del teorema 2.3.1,

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

□

Observació. Hom podria caure en la temptació de pensar que la congruència de Fermat és una prova per detectar nombres primers. Això no és cert. Existeixen nombres N compostos que compleixen la congruència de Fermat. Aquests nombres s'anomenen *nombres de Carmichael*. El més petit d'ells és el 561.

La congruència de Fermat sí que serveix per detectar nombres compostos. És a dir, si un N senar no compleix (2.3), segur que és compost. Per exemple, si $N = 323$ i prenem $a = 2$,

$$a^{322} \equiv 157 \not\equiv 1 \pmod{323} \quad \Rightarrow \quad N = 323 \quad \text{compost.} \qquad (323 = 17 \cdot 19)$$

Si el mòdul que considerem a la congruència de Fermat no és un nombre primer, no podem assegurar que es compleixi (2.3). Per exemple, si prenem $p = 6$ i $a = 5$, és clar que mcd(5,6)=1 però

$$a^{p-1} = 5^5 = 3125 \equiv 5 \pmod 6, \qquad 3126 \text{ és parell i divisible per 3.}$$

Taula 2.2: Els primers valors de la funció $\varphi(n)$.

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Això és degut que si p no és primer sempre es complirà $\text{mcd}(p,(p-1)!) = p \neq 1$ i, per tant, no podrem simplificar la congruència. En el cas anterior ($p = 6$ i $a = 5$) es compleix $\text{mcd}(6,120) = 6 \neq 1$

Observem, però, que si p no és primer sí que pot existir un nombre $k < p$ complint la congruència de Fermat. Pensem, per exemple en $p = 15$ i $a = 7$, mcd(7,15)=1. Atès que 15 no és primer, és clar que no es complirà la congruència de Fermat. En efecte,

$$7^{15-1} = 7^{14} = (-2)^{14} = 16384 \equiv 4 \pmod{15}$$

Però, en canvi, es compleix

$$7^8 = 5764801 \equiv 1 \pmod{15}$$

Volem donar un significat a l'exponent de la congruència de Fermat. És clar que, si p és primer, l'exponent es correspon amb $p-1$. Però si p no és primer, com el cas de 15, cal buscar una funció que relacioni el 8 amb el 15. Si pensem amb els nombres inferiors a 15 i coprimers amb ell mateix, n'hi ha exactament 8: 1, 2, 4, 7, 8, 11, 13 i 14. Aquesta propietat fou observada per Leonhard Euler (1707-1783) i ell mateix la demostrà convertint-se en la *congruència d'Euler*. Abans d'enunciar-la, però, ens cal introduir la funció φ (phi) d'Euler[4].

Definició 2.3.2 (Funció φ d'Euler)

$$\forall\, n \in \mathbb{N}\,, \quad \varphi(n) := \sharp\,\{1 \leq a \leq n-1 \,|\, \text{mcd}(a,n) = 1\} \tag{2.4}$$

És a dir, $\varphi(n)$ compta quants nombres per sota d'n són coprimers amb ell mateix. La taula 2.2 mostra els primers valors de la funció $\varphi(n)$.

Teorema 2.3.3 (Congruència d'Euler)
Si m, $a \in \mathbb{N}$, $m > 1$ i mcd*(a,m)=1, aleshores*

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{2.5}$$

Observació. Atès que si p és primer, aleshores $\varphi(p) = p-1$, podem considerar la congruència de Fermat com un cas particular de la congruència d'Euler.

Demostració.

Siguin b_1, b_2, ..., $b_{\varphi(n)}$ tots els nombres naturals coprimers amb m i menors que m. Aquests nombres són incongruents dos a dos mòdul m. Com que $\text{mcd}(a,m)$=1, els nombres

$$a \cdot b_1\,, \quad a \cdot b_2\,, \quad \ldots a \cdot b_{\varphi(m)}$$

[4]També anomenada *funció indicatriu* d'Euler.

seran també incongruents dos a dos mòdul m, i cadascun d'ells congruent amb un, i només un, dels b_1, b_2, ..., $b_{\varphi(n)}$. Per tant,

$$a \cdot b_1 \cdot a \cdot b_2 \cdots a \cdot b_{\varphi(m)} \equiv b_1 \cdot b_2 \cdots b_{\varphi(m)} \pmod{m}$$

És a dir,

$$a^{\varphi(m)}(b_1 \cdot b_2 \cdot \cdots \cdot b_{\varphi(m)}) \equiv b_1 \cdot b_2 \cdot \cdots \cdot b_{\varphi(m)} \pmod{m}$$

Com que cada b_i és coprimer amb m, es pot simplificar la congruència, quedant

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

□

Teorema 2.3.4 (Propietats de $\varphi(n)$)
La funció φ d'Euler compleix les propietats següents:

1. $\varphi(p) = p - 1 \qquad \forall\, p$ *primer.*
2. $\varphi(p^\alpha) = p^{\alpha-1}(p-1) \qquad \forall\, p$ *primer,* $\alpha > 1$, $\alpha \in \mathbb{N}$.
3. $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) \qquad \forall\, p, q,$ *amb* $\mathrm{mcd}(p, q) =!$.
4. $a|b \quad \Rightarrow \quad \varphi(a)|\varphi(b)$.
5. $\varphi(n)$ *és parell per a* $n \geq 3$. *Si* n *té* r *factors primers diferents,* $2^r|\varphi(n)$

Demostració.

1. Trivial.
2. Els nombres menors que p^α i que són coprimers amb p^α són els nombres compresos entre 1 i p^α que no són múltiples de p. Com que de múltiples de p n'hi ha $p^{\alpha-1}$ d'aquí resulta que:
$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Les altres demostracions són més complicades i no disposem de les eines necessàries per fer-les. Direm però, que es dedueixen a partir d'una fórmula producte per a $\varphi(n)$:

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

□

Observació. La congruència d'Euler afirma que si $\mathrm{mcd}(a, m) = 1$ és $a^{\varphi(m)} \equiv 1 \pmod{m}$. Però pot passar que per a alguns nombres a existeixin nombres k menors que $\varphi(m)$ tals que $a^k \equiv 1 \pmod{m}$. Per exemple, hem vist abans que $7^8 \equiv 1 \pmod{15}$. Però també es compleix $7^4 \equiv 1 \pmod{15}$. És clar que, en cas d'existir, k ha de ser un divisor de $\varphi(m)$.

Acabarem el capítol utilitzant les congruències per demostrar que existeixen infinits nombres primers amb determinades estructures. Abans hem vist la infinitud dels nombres primers, demostrat per Euclides. Llevat del 2, tots els altres nombres primers són nombres senars, $2k + 1$. Els nombres senars es poden agrupar en dues famílies:

- Els de la forma $N = 4k + 1$ o, equivalentment, els $N \equiv 1 \pmod 4$.
- Els de la forma $N = 4n + 3$ o $N \equiv 3 \pmod 4$ o $N \equiv -1 \pmod 4$

Sembla lícit demanar quina família conté més primers. Podria ser que dels infinits nombres primers senars una quantitat finita fos del tipus $4k + 1$ i tota la resta de l'altre tipus. O al revés. Però això no és així i mirarem de demostrar-ho.

Teorema 2.3.5

1. *Existeixen infinits nombres primers del tipus* $4k + 3$
2. *Existeixen infinits nombres primers del tipus* $4k + 1$

Demostració.

1. Per veure que existeixen infinits nombres primers del tipus $4k + 3 = 4k - 1$ seguirem un procés semblant al de la demostració d'Euclides. Comencem suposant que a partir d'un cert primer en endavant tots els primers són de la forma $4k+1$. Sigui P el primer més gran de la forma $4k - 1$. Construïm el nombre

$$N = 4 \cdot 3 \cdot 5 \cdots P - 1$$

   El producte $3 \cdot 5 \cdots P$ conté tots el primers senars $\leq P$ com a factors. Com que N és de la forma $4n - 1$, no pot ser primer atès que $N > P$. Cap primer $\leq P$ divideix a N. Si ho fes, aleshores dividiria la seva diferència, que és 1. Absurd! Per tant, tots els factors primers de N són més grans que P. Però no és possible que tots aquests factors siguin de la froma $4k + 1$ atès que el producte de dos nombres del tipus $4k + 1$ és un altre nombre del mateix tipus. En efecte,

$$(4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1 = 4K + 1$$

   Per tant, algun dels factors primers de N ha de ser del tipus $4k - 1$. Això suposa una contradicció que només pot provenir del fet de considerar finit el conjunt dels nombres primers del tipus $4k - 1$

2. Sigui $N \in \mathbb{N}$, $N > 1$. Demostrarem que existeix un primer $p > N$ tal que $p \equiv 1 \pmod 4$. Considerem

$$m = (N!)^2 + 1$$

   Observem que m és senar. Sigui p el menor divisor primer de m, que és més gran que N, ja que tot nombre menor o igual que N divideix $N!$. Com que p divideix m

$$p \,|\, (N!)^2 + 1 \quad \Rightarrow \quad (N!)^2 \equiv -1 \pmod p$$

   Si elevem a la potència $(p-1)/2$ els dos membres d'aquesta darrera congruència obtenim

$$(N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p$$

   Com que $\text{mcd}(p, N!) = 1$, segons la congruència de Fermat,

$$(N!)^{p-1} \equiv 1 \pmod p \quad \Rightarrow \quad (-1)^{(p-1)/2} \equiv 1 \pmod p$$

Si $(p-1)/2$ fos senar, aleshores passaria

$$-1 \equiv 1 \pmod{p} \quad \Rightarrow \quad p = 2 \quad \text{impossible, atès que } m \text{ és senar}$$

Per tant, $(p-1)/2$ ha de ser parell. És a dir,

$$\frac{p-1}{2} = 2k \quad \Rightarrow \quad p = 4k+1$$

Acabem de demostrar que, per a tot enter $N > 1$, existeix un nombre primer $p > N$ tal que $p \equiv 1 \pmod{4}$. En conseqüència, existeixen una infinitat de nombres primers del tipus $4k+1$

□

Podem trobar raonaments semblants als anteriors per adaptar-los a nombres primers d'estructures com ara $5k-1$, $8k-1$, $8k-3$ i $8k+3$. Aquesta qüestió es pot reformular des del llenguatge de les progressions aritmètiques i fer la següent pregunta: quants nombres primers trobem en la progressió aritmètica $5k-1$? O en la $8k-3$?

La resposta a aquesta pregunta d'aparença simple no és fàcil. De fet, encara no s'ha trobat una demostració elemental d'aquest fet. La primera demostració general d'aquest fet es produí l'any 1837 en una famosa memòria publicada per Peter-Gustav Lejeune Dirichlet[5]. Per aconseguir el seu objectiu, Dirichlet utilitzà uns potents mètodes analítics inaugurant el que avui en dia coneixem com a *Teoria Analítica de Nombres*, una branca de les Matemàtiques que barreja els conceptes de l'aritmètica amb les eines del càlcul diferencial i integral.

Teorema 2.3.6 (Teorema de la progressió aritmètica de Dirichlet)
Si el $\mathrm{mcd}(a,b) = 1$ *aleshores la progressió aritmètica*

$$a \cdot n + b \qquad n = 0,\ 1,\ 2,\ ...$$

conté infinits nombres primers

Exemple. Com que mcd(17, 12)=1, existeixen infinits nombres primers d'estructura $17k+12$ i infinits primers d'estructura $12k+17$. En altres paraules,

Existeixen infinits primers p tals que $p \equiv 12 \pmod{17}$ (29, 131, 199, ...)

Existeixen infinits primers p tals que $p \equiv 17 \pmod{12}$ (29, 41, 53, 89, ...)

[5]Dirichlet, P. G. Lejeune. *"Beweis des Satzes, dass jede unbegrentze arithmetische Progression, deren erstes Glied un Differenz ganze Zahlen ohne gemeinschlaftichen Factor sind, unendliche viele Primzahlen enthält"* (Demostració del teorema de que tota progressió aritmètica, el terme general de la qual és format per dos enters sense cap factor comú, conté un nombre infinit de primers) Abhand. Akademic Wiss. Berlin, Werke I (1837).

Capítol 3

Distribució de primers

3.1 Introducció

Al capítol anterior hem vist, entre altres resultats, que existeixen infinits nombres primers i que aquests són fonamentals per escriure qualsevol nombre natural (el *Teorema Fonamental de l'Aritmètica*, 2.2.8). També hem comprovat i demostrat que existeixen infinits nombres primers seguint determinades estructures concretes com ara $4n+1$, $4n-1$ o $8n+3$, on n és qualsevol nombre natural. El *Teorema de Dirichlet*, (2.3.6) generalitza aquest resultat i posa en evidència la dificultat de trobar alguna manera de clasificar, detectar o buscar una regularitat o una fòrmula per localitzar nombres primers.

Els nombres primers presenten una dualitat en el seu comportament que els fa molt i molt interessants perquè, d'una banda, ens diuen una cosa i, de l'altra, justament el contrari. En la lliçó inaugural de la universitat de Bonn l'any 1975, Don Zagier (1951) il·lustrà meravellosament aquesta dualitat:

> *" Hi ha dos fets sobre la distribució dels nombres primers que espero us sorprenguin d'una manera tan aclaparadora que restin permanentment gravats en els vostres cors. El primer fet és que, malgrat la seva definició simple i el seu paper com a blocs de construcció dels nombres naturals, els nombres primers creixen com la mala herba entre els nombres naturals, obeïnt cap altra llei que no sigui la de l'atzar, i ningú no pot predir on brollarà el proper nombre primer. El segon fet és encara més sorprenent perquè justament diu el contrari: que els nombres primers mostren una regularitat impressionant, que hi ha unes lleis que regeixen el seu comportament i que els nombres primers obeeixen aquestes lleis amb una precisió gairebé militar."*

Quan parlem de nombres primers ens interessen, sobretot, tres qüestions:

1. Donat un nombre natural n, saber si és, o no, primer.
2. Fixat un n, dir quants nombres primers hi ha per sota n.
3. Si p_n és l'n-èsim nombre primer, qui és p_{n+1}.

Aquestes tres qüestions tenen una resposta fàcil si ens movem en intervals relativament petits. Amb unes poques divisions podem determinar que 3967 és primer i que 2047 no ho és pas. Tampoc no costa gaire calcular que hi ha exactament 95 nombres primers per sota el 500 i que després del 331, que és el 67è nombre primer, el següent nombre primer que trobem és el 337. Però quan comencem a moure'ns en magnituds més grans, respondre les tres qüestions anteriors pot complicar-se de manera espectacular. És primer el nombre 715 613 967 845 963 213? Quants primers trobem per sota 10^{23}? Quin és el primer número 10^{100}? I si aquestes quantitats ens semblen grosses, no són res comparades amb les dimensions que podem treballar a mesura que ens endinsem en els nombres naturals.

Respondre aquestes tres qüestions quan els nombres amb els quals treballem són grossos és un dels objectes d'estudi d'una branca de les Matemàtiques anomenada *teoria analítica de nombres*, que lliga els conceptes i idees més elementals de l'aritmètica clàssica amb les sofisticades eines del càlcul diferencial i integral en variable complexa.

El nivell del treball que aquí es presenta impedeix un estudi molt elaborat dels resultats als quals s'ha arribat en aquest camp. Malgrat tot, podem fer una petita introducció de la filosofia que adoptem quan ens enfrontem amb les qüestions relacionades amb els nombres primers. També farem una breu exposició dels resultats més importants (la majoria dels quals enunciarem sense demostració per manca de tenir les eines necessàries) i quina repercusió tenen en el desenvolupament actual de les matemàtiques.

De les tres qüestions abans comentades, en aquest capítol ens centrarem en les dues darreres. Primer farem una breu exposició històrica del problema. En la següent secció presentarem resultats importats sobre la distribució de primers. Finalitzarem el capítol amb una secció on analitzarem amb l'ajut de l'ordinador la certesa d'un dels problemes, sense demostració encara, més important de les matemàtiques: la hipòtesi de Riemann.

3.2 La distribució de primers al llarg de la història

Hem comentat diverses vegades la infinitud dels nombres primers. Un cop entès i acceptat aquest fet, voldríem intentar trobar alguna pauta en el seu comportament. Si confeccionem una taula de nombres primers observarem que la seva distribució és molt irregular. Històricament la primera taula de nombres primers la va construir el matemàtic grec Eratòstenes (276-194 a.C.). El seu mètode, conegut com a *Garbell d'Eratòstenes*, consisteix en eliminar sistemàticament els nombres compostos fins que només ens queden els nombres primers. El mètode comença amb una taula on hi tenim escrits tots els nombres naturals més grans o igual que 2 fins a un cert valor donat, per exemple $x = 100$. El primer garbell selecciona el 2 com a nombre primer i elimina tots els seus múltiples, que són els nombres parells. Després d'aquest garbell el primer nombre no eliminat, el 3, resulta ser el següent nombre primer. El segon garbell elimina tots els múltiples de 3 que hi ha a la taula. Alguns nombres, com el 6, s'hauran eliminat dues vegades en ser múltiples de 2 i de 3. Un cop finalitzat el segon garbell, el primer nombre no eliminat, el 5, resulta ser el següent nombre primer. El mètode continua eliminant, en un tercer garbell, tots els múltiples de 5, deixant el 7 com el següent nombre primer després del 5. Repetint el procés, anem eliminant els múltiples del darrer nombre seleccionat com a nombre primer deixant en la taula només els nombres primers (veure Taula 3.1. Els nombres primers s'han marcat en negreta).

Taula 3.1: El garbell d'Eratòstenes per a $x = 100$.

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

Quan confeccionem taules més i més grans, observem grans espais entre nombres primers. Aquest fet té una justificació natural: com més gran és un nombre, més possibilitats té de ser compost en haver-hi més nombres primers que el poden dividir. Per exemple, el nombre primer 370 261 ve seguit de 111 nombres compostos. No existeix cap nombre primer entre 20 831 323 i 20 831 533. La família dels nombres primers presenta forats arbitràriament grans. Per exemple, si volem 100 nombres consecutius compostos, considerem els nombres entre 1 i 101 i els multipliquem entre sí. Aquest número és divisible per cada un dels nombres entre 1 i 101, en tenir-los com a factors. Si prenem qualsevol nombre N entre 2 i 101, el nombre

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots 100 \cdot 101 + N$$

és divisible per N i, per tant, no és primer. D'aquesta manera hem pogut construir un forat de 100 números consecutius compostos .

Per altra banda, les mateixes taules mostren que es presenten reiteradament nombres primers consecutius (entesos com a nombres senars, és clar) com ara el 3 i el 5, el 347 i el 349 o el $76 \cdot 3^{139} - 1$ i el $76 \cdot 3^{139} + 1$, uns nombres de 69 xifres en notació decimal. Els nombres primers que, com aquests, difereixen en 2 s'anomenen *primers bessons*. Hi ha uns 1 000 parells de primers bessons per sota del 100 000 i uns 8 000 per sota d'1 000 000. Molts matemàtics creuen que existeixen infinites parelles de primers bessons, però fins ara ningú no ha estat capaç de demostrar-ho.

Una de les raons de la irregularitat en la distribució dels nombres primers és el fet que no existeixi, o no s'hagi trobat, una fórmula prou senzilla que produeixi tots els nombres primers. Per exemple, l'expressió

$$x^2 - x + 41$$

produeix un nombre primer per a $x = 0, 1, 2, ..., 40$, mentre que l'expressió

$$x^2 - 79x + 1601$$

ens genera un nombre primer per a $x = 0, 1, 2, ..., 79$. Aquestes expressions i d'altres semblants foren trobades per Leonhard Euler (1707-1783). Però fou el seu amic Christian Goldbach (1690-1764) el qui demostrà, el 1752, que malgrat utilitzem potències cúbiques o superiors, cap expressió polinòmica en x a coeficients enters mai no pot generar un nombre

primer per a tot valor de x. Euler fou un dels primers matemàtics que s'interessà per buscar regularitats en el conjunt dels nombres primers. I si bé obtingué alguns resultats importants, ell mateix es mostrà vençut per la complexitat i la irregularitat dels nombres primers. Referint-se a ells, Euler digué:

> *" Els matemàtics han intentat en va fins el dia d'avui descobrir una mica d'ordre en la successió dels nombres primers, i tenim raons per creure que és un misteri on la ment humana no hi podrà penetrar mai."*

Després dels intents infructuosos d'Euler cal anar fins a finals del segle XVIII. Independentment Carl Friedrich Gauss (1777-1855) i Adrien-Marie Legendre (1752-1833) canvien d'orientació la pregunta de com determinar primers i s'interessen per la distribució dels nombres primers en el conjunt dels nombres naturals. Bàsicament es tracta d'estudiar el comportament de la funció que compta els nombres primers inferiors o iguals a x, coneguda com a $\pi(x)$[1].

$$\pi(x) := \sharp\{\ 1 < p \leq x \ /\ p \text{ primer}\}$$

La taula 3.2 ens mostra els primers valors de la funció $\pi(x)$.

Taula 3.2: Els primers valors de la funció $\pi(x)$.

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\pi(x)$	1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	7	7	8

Es tracta d'una funció esglaonada, constant a trossos, que en cada primer té una discontinuïtat de salt en què augmenta en una unitat, tal com es pot veure representada a les figures 3.1 i 3.2. Malgrat que el seu comportament és impredictible en intervals curts, quan s'observa des de prou lluny, es comporta d'una manera sorprenentment regular. Per adonar-nos d'aquest fet només cal observar les figures 3.3 i 3.4.

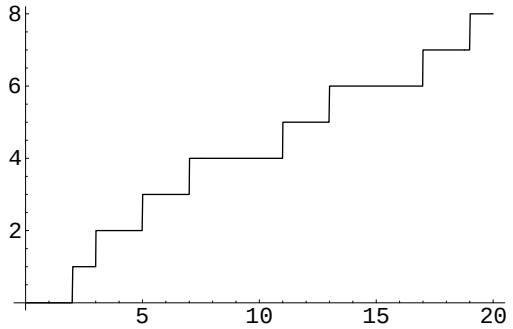


Figura 3.1: $\pi(x)$ a l'interval $[0, 20]$

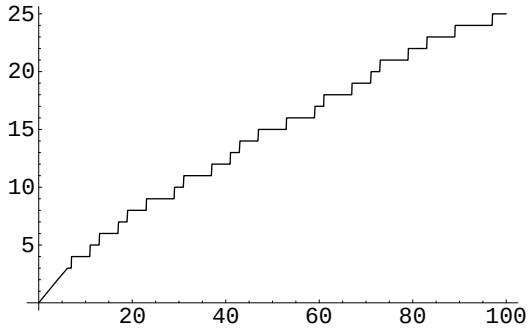


Figura 3.2: $\pi(x)$ a l'interval $[0, 100]$

[1]Evidentment, cal no confondre la funció $\pi(x)$ amb la constant π. Aquesta notació, desafortunada segons alguns matemàtics, la debem al matemàtic alemany Edmund Landau (1877-1938) que la introdueix en el seu *"Handbuch der Lehre von der Verteilung der Primzahlen"* (1909).

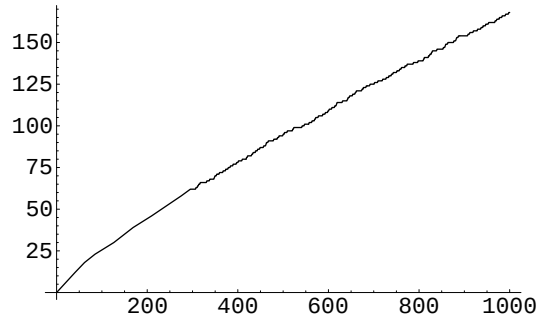


Figura 3.3: $\pi(x)$ a l'interval $[0, 1\,000]$

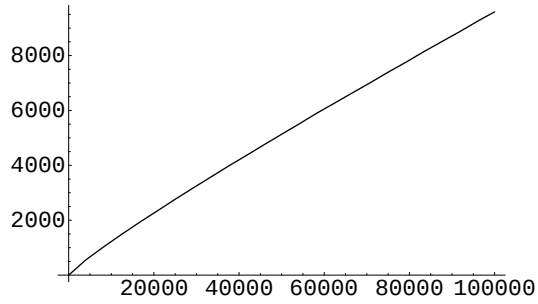


Figura 3.4: $\pi(x)$ a l'interval $[0, 100\,000]$

Històricament sembla que va ser Gauss la primera persona que es va interessar per la distribució dels nombres primers. L'anècdota explica que, pel seu quinzè aniversari, li van regalar una "calculadora" de l'època, és a dir, un llibre amb taules de logaritmes. Com a complement, aquest llibre tenia en un apèndix una llista de nombres primers inferiors a 1 000 000. Amb la seva capacitat innata d'observació, Gauss fou capaç de relacionar els logaritmes naturals i la funció $\pi(x)$. Però no publicà mai res referent al tema. Al llarg de la seva vida Gauss dedicava estones mortes a completar la taula de nombres primers, fins que arribà als 3 000 000, per corroborar la seva aproximació que es basava en el logaritme integral, $\mathrm{Li}(x)$, funció introduïda per ell mateix i que ell defineix com[2]

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t} \tag{3.1}$$

Paral·lelament, Legendre també estudiava la distribució dels primers i, seguint mètodes completament diferents als de Gauss, l'any 1798 conjecturà que la funció

$$F(x) = \frac{x}{\ln x - 1.08366} \tag{3.2}$$

aproximava d'una manera força bona la funció $\pi(x)$. La seva proposta, empírica, es fonamentava en les dades de què es disposava en aquell moment. El 1849, en una carta de Gauss dirigida al seu amic i astrònom Johann Encke, li confessa els resultats que havia obtingut de jove, arran d'un article publicat per Legendre on s'exposava la seva famosa aproximació. En aquells moments es creà una certa tensió entre els dos matemàtics que reclamaven la millor aproximació i l'originalitat de llurs treballs. A la taula 3.3 podem comparar ambdues aproximacions i els errors que produeixen (en %) les aproximacions de Gauss i de Legendre. Actualment sabem que, si bé la proposta de Legendre proporciona una bona aproximació de $\pi(x)$ quan x es inferior a 10^6, més endavant deixa de fer-ho i l'aproximació donada per Gauss sempre serà millor que la de Legendre a mida que x es va fent gran. Les figures 3.5 i 3.6 mostren els comportaments de les aproximacions de Legendre i Gauss respecte a la funció $\pi(x)$ quan $x \in [2, 1000]$.

[2]Actualment es defineix el logaritme integral com la funció

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\ln t}$$

on la integral impròpia s'ha d'interpretar com el valor principal de Cauchy per evitar la singularitat en $t = 1$. Aquesta funció difereix de la Gauss en una constant que es pot calcular i que val 1,04516...

Taula 3.3: Aproximacions de Legendre ($F(x)$) i Gauss ($\mathrm{Li}(x)$) respecte $\pi(x)$.

x	$\pi(x)$	$F(x)$	error $F(x)$	$\mathrm{Li}(x)$	error $\mathrm{Li}(x)$
10^2	25	28.3945	3.39449	30.1261	5.12614
10^3	168	171.692	0.369164	177.61	0.960966
10^4	1229	1230.47	0.0146932	1246.14	0.171372
10^5	9592	9588.13	−0.00387283	9629.81	0.037809
10^6	78498	78541.3	0.00433275	78627.5	0.0129549
10^7	664579	665126.	0.00547427	664918.	0.00339405
10^8	5761455	5.7679×10^6	0.00644897	5.76221×10^6	0.000754375
10^9	50847534	5.09167×10^7	0.00692071	5.08492×10^7	0.000170096
10^{10}	455052511	4.55737×10^8	0.00684262	4.55056×10^8	0.0000310359
10^{11}	4118054813	4.12455×10^9	0.00649402	4.11807×10^9	0.0000115876

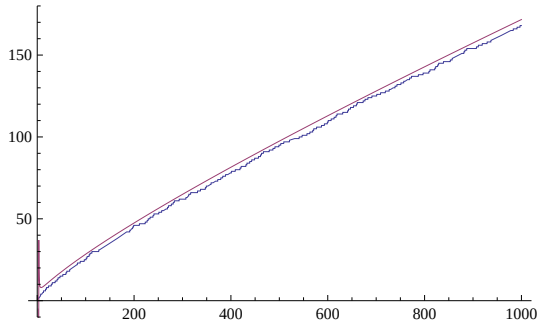


Figura 3.5: $\pi(x)$ *versus* $F(x)$ (Legendre).

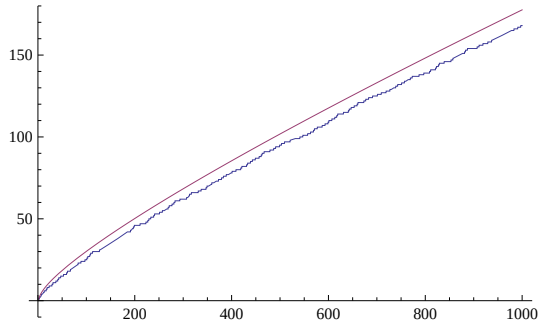


Figura 3.6: $\pi(x)$ *versus* $\mathrm{Li}(x)$ (Gauss).

Tant Gauss com Legendre, a partir de les observacions de les taules, van proposar independentment que, per a x gran, el quocient

$$\frac{\pi(x)\ln(x)}{x} \tag{3.3}$$

era proper a 1 i varen conjecturar que aquest quocient tendia a 1 quan x tendia cap a infinit. Però cap dels dos no va ser capaç de demostrar-ho. El problema de determinar la certesa, o no, d'aquesta afirmació va atreure les millors ments matemàtiques d'Europa durant gairebé 100 anys.

L'any 1851 el matemàtic rus Pafnuti Txebixev (1821-1894) va donar un pas endavant molt important en demostrar que *si* el quocient (3.3) tenia límit, aleshores el seu valor hauria de ser igual a 1. Més concretament, va demostrar que existeixen dues constants C_1 i C_2 tals que, si $x \to \infty$,

$$C_1\frac{\pi(x)\ln(x)}{x} \;\leq\; 1 \;\leq C_2\frac{\pi(x)\ln(x)}{x} \tag{3.4}$$

i va calcular aproximadament els valors $C_1 = 0.9219\ldots$ i $C_2 = 1.10555\ldots$. Tanmateix, va ser incapaç de demostrar que el quocient (3.3) *tenia* límit. Les tècniques que utilitzà per demostrar aquest resultat encara es basaven en les anomenades tècniques elementals.

Un pas conceptualment important el donà l'any 1837 Peter Gustav L. Dirichlet (1805-1859) per demostrar l'existència de primers en successions aritmètiques arbitràries (*teorema de Dirichlet*, 2.3.6). Per demostrar aquest teorema, Dirichlet utilitzà un conjunt de tècniques que pocs anys abans havia començat a introduir A. L. Cauchy (1789-1857). Aquestes noves eines abandonen el "confortable" món dels nombres naturals i llurs propietats, per endinsar-se en les funcions complexes de variable complexa. Aquesta nova branca matemàtica, que uneix els conceptes més elementals de l'aritmètica amb els potents mètodes de l'anàlisi complexa, es coneix sota el nom de *teoria analítica de nombres*.

Més tard, l'any 1859, Georg Bernhard Riemann (1826-1866) presentà una memòria de vuit planes que ha esdevingut un dels escrits matemàtics més importants de la història. En el seu treball *"Über die Anzahl der Primzahlen unter einer gegebenen Grösse"* ("Sobre la magnitud de primers per sota d'una quantitat donada") Riemann relacionarà la distribució dels nombres primers amb una determinada funció extesa a tot el pla complex $\mathbb{C}$ gràcies a una eina anomenada *continuació analítica*. Aquesta funció es coneix des d'aleshores amb el nom de *funció zeta de Riemann*, $\zeta(s)$, i es defineix a partir de la suma infinita

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{3.5}$$

on $s = \sigma + i\,t$ representa un nombre complex. En aquesta famosa memòria Riemann desenvolupa tota la seva creativitat per trobar una expressió que dóna **exactament** la quantitat de nombres primers que hi ha per sota d'un cert x donat. Aquesta expressió és

$$\pi(x) = J(x) - \frac{1}{2}J(x^{1/2}) - \frac{1}{3}J(x^{1/3}) - \frac{1}{5}J(x^{1/5}) + \frac{1}{6}J(x^{1/6}) + \cdots + \frac{\mu(n)}{n}J(x^{1/n}) + \cdots \tag{3.6}$$

on $\mu(n)$ és la *funció de Möbius*[3] definida com

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ és divisible per un primer al quadrat} \\ 1 & \text{si } n \text{ és producte d'un nombre parell de primers diferents} \\ -1 & \text{si } n \text{ és producte d'un nombre senar de primers diferents} \end{cases} \tag{3.7}$$

La sèrie (3.6) és una sèrie finita un cop tenim x fixat i s'ha de combinar amb el càlcul de la funció $J(x)$:

$$J(x) = \mathrm{Li}(x) - \sum_{\Im(\rho)>0} [\mathrm{Li}(x^{\rho}) + \mathrm{Li}(x^{1-\rho})] - \ln 2 + \int_x^{\infty} \frac{dt}{t(t^2-1)\ln t}\,, \quad x > 1 \tag{3.8}$$

La memòria de Riemann és important per plantejar dues qüestions que avui en dia encara no han estat resoltes, malgrat s'han intentat demostrar per les eines més potents de les que disposa les matemàtiques actualment. Una de les qüestions es coneix amb el nom d'*hipòtesi de Riemann* i, possiblement, és un dels problemes no resolts més famosos de les matemàtiques. En calcular l'expressió de la funció $J(x)$, Riemann es veu obligat a estudiar com estan distribuïts en el pla complex $\mathbb{C}$ els valors complexos ρ que anul·len la funció zeta, és a dir, els valors que compleixen $\zeta(\rho) = 0$, responsables de controlar el terme oscil·lant

$$\sum_{\Im(\rho)>0} [\mathrm{Li}(x^{\rho}) + \mathrm{Li}(x^{1-\rho})]$$

[3]En honor a Ferdinand Möbius (1790-1868), professor de Riemann a la universitat de Götingen.

Taula 3.4: Els quinze primers zeros de $\zeta(s)$, $s = \frac{1}{2} + i\,\alpha$, calculats per Gram (1903).

$\alpha_1 = 14.134\ 725$	$\alpha_6 = 37.586\ 176$	$\alpha_{11} = 52.8$
$\alpha_2 = 21.022\ 040$	$\alpha_7 = 40.918\ 720$	$\alpha_{12} = 56.4$
$\alpha_3 = 25.010\ 856$	$\alpha_8 = 43.327\ 073$	$\alpha_{13} = 59.4$
$\alpha_4 = 30.424\ 878$	$\alpha_9 = 48.005\ 150$	$\alpha_{14} = 61.0$
$\alpha_5 = 32.935\ 057$	$\alpha_{10} = 49.773\ 832$	$\alpha_{15} = 65.0$

Riemann se n'adona que hi ha dos tipus diferents de zeros: els que s'anomenen *zeros trivials*, perfectament detectats i que tenen l'estructura $-2n$ amb $n \in \mathbb{N}$; i uns altres, que no ho són gens de trivials, i que, després de calcular-ne uns quants, conjectura que tots tenen una particularitat comuna: la seva part real val $\frac{1}{2}$, és a dir, tots es col·loquen perfectament alineats sobre la recta del pla complex $s = \frac{1}{2}$ (que s'anomena *recta crítica*). Aquesta afirmació és la *hipòtesi de Riemann*. Fora de la recta $s = \frac{1}{2}$, la funció $\zeta(s)$ no val mai zero (figures 3.7 i 3.8 i taula 3.4). L'altra qüestió no resolta per Riemann, i que encara ningú no ha estat capaç tampoc de demostrar, és l'estimació que fa Riemann de la quantitat de zeros no trivials continguts en un segment del pla complex.

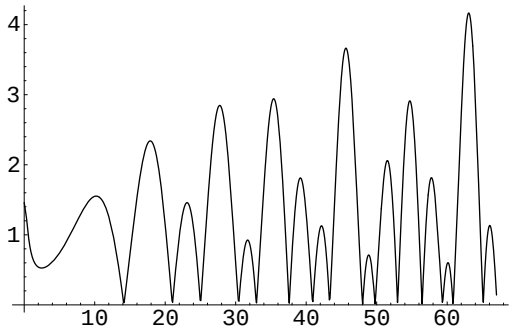


Figura 3.7: $|\zeta(1/2 + i\,t)|$, $t \in [0, 70]$.

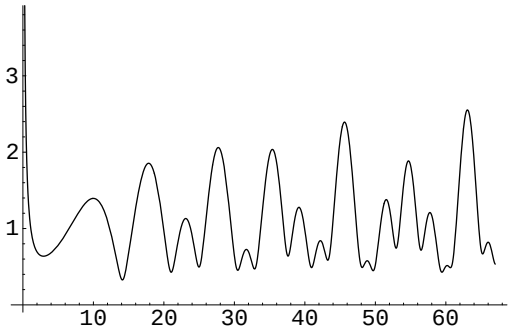


Figura 3.8: $|\zeta(1 + i\,t)|$, $t \in [0, 70]$.

Malauradament Riemann morí jove, abans dels 40 anys, i no es dedicà mai més a l'estudi dels nombres primers. La seva memòria passà a l'oblit durant més de 35 anys però retornà a l'actualitat matemàtica quan, el 1896, Jacques Hadamard (1865-1963) i Charles de la Vallée Poussin (1866-1962) demostraren, independentment un de l'altre, que el quocient (3.3) tendeix a 1 quan $x \to \infty$. És el que es coneix amb el nom del *teorema del nombre primer*

Teorema 3.2.1 (Teorema del nombre primer)

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1$$

Per poder demostrar aquest teorema, Hadamard i de la Vallée Poussin, aprofitaren totes les eines introduïdes per Riemann al voltant de la funció $\zeta(s)$. Aleshores es començà a copsar la importància de l'escrit de Riemann i la necessitat d'entendre i de demostrar tots i cada

un dels passos que el conduïren a calcular l'expressió (3.6). Primerament fou Von Mangoldt (1854-1925) qui s'enfrontà al difícil estil d'escriure matemàtiques de Riemann, on al lector li costa distingir si l'afirmació que es fa, i que no es demostra, és un simple exercici de càlcul o bé és una qüestió més complicada.

Sigui com sigui, la hipòtesi de Riemann continua avui dia sense demostració. Des de la seva formulació, milers de matemàtics, entre els quals els millors del seu moment, s'hi han enfrontat sense trobar-ne una resposta satisfactòria. Entre aquests cal destacar els noms de Godfrey Hardy, John E. Littlewood, Srinavasa Ramanujan, Carl Ludwig Siegel, Atle Selberg, André Weil, Alexandre Grothendieck, Peter Sarnak i Enrico Bombieri. Els resultats més positius als quals s'ha arribat fins ara podrien ser: la demostració de l'existència d'infinits zeros de la funció zeta a la recta crítica (Littlewood, 1915); i la demostració que els 2/5 de la totalitat dels zeros de la funció zeta es troben sobre la recta crítica. Paral·lelament, s'han anat demostrant resultats que depenen de la certesa de la hipòtesi. Per això mai no se l'ha considerat una conjectura. Actualment, amb les noves tecnologies i l'ajut dels ordinadors s'han pogut calcular milions de zeros de la funció zeta i cap d'ells no s'ha separat el més mínim de la recta crítica, tal com va predir Riemann. Tanmateix, la comunitat matemàtica internacional considera aquest fet només com un punt a favor de la hipòtesi. En teoria de nombres es diu que la comprovació d'uns quants casos (encara que siguin milions de casos) no representen en si mateix una demostració.

3.3 Resultats matemàtics

En aquesta secció presentem els resultats propis del treball de recerca. Hem agrupat aquests resultats en dos tipus diferents de grups: uns resultats aproximen, o donen fites mínimes, del valor de la funció $\pi(x)$; uns altres, aproximen el valor de l'n-èsim nombre primer p_n. Al llarg de la secció raonarem que, si el *teorema del nombre primer* és cert[4], aproximar el valor de $\pi(n)$ equival a aproximar el valor de p_n, per a x gran. Començarem pels resultats que aproximen $\pi(x)$.

Una mirada més atenta a l'argument d'Euclides que demostra la infinitud de nombres primers, ens permet una primera (i molt pobra!) fita inferior del valor de $\pi(x)$. El nombre $P_n = 1 + p_1 p_2 \cdots p_n$ construït a partir dels n primers nombres primers, pot o pot no ser primer. Sigui p_{n+1} el divisor més petit del nombre P_n. Aleshores, podem sobreestimar p_{n+1} d'una manera molt barroera com:

$$p_{n+1} \leq P_n = 1 + p_1 p_2 \cdots p_n \leq 2 p_1 p_2 \cdots p_n$$

Aplicant de manera reiterada la darrera desigualtat, obtenim:

$$\begin{aligned} p_1 = 2 \quad &\Rightarrow \quad p_2 \leq 2p_1 = 2 \cdot 2 = 2^2 = 2^{2^1} \\ &\Rightarrow \quad p_3 \leq 2p_1p_2 = 2 \cdot 2 \cdot 2^2 = 2^4 = 2^{2^2} \\ &\Rightarrow \quad p_4 \leq 2p_1p_2p_3 = 2 \cdot 2 \cdot 2^2 \cdot 2^4 = 2^8 = 2^{2^3} \\ &\cdots \\ &\Rightarrow \quad p_{n+1} \leq 2^{2^n} \end{aligned}$$

[4] L'afirmació del *TNP* és certa però, atès el nivell del treball, no podem demostrar-la.

D'aquesta manera hem obtingut una estimació per al valor de l'$n+1$-èsim nombre primer, p_{n+1}. Atès que, per a tot valor de $k = 1, 2, ...,n$ es compleix la desigualtat $p_k < p_{n+1}$, aleshores per a cada p_k amb $k = 1 \div n$ es compleix $p_k \leq 2^{2^n}$. Com que $\pi(x)$ ens dóna la quantitat de nombres primers inferiors a x, si fem $x = 2^{2^n}$, com a mínim hi haurà $n + 1$ nombres primers i, per tant, es complirà la desigualtat:

$$\pi(2^{2^n}) \geq n + 1$$

Prenem logaritmes en base 2 a l'expressió $x = 2^{2^n}$.

$$\log_2 x = \log_2 2^{2^n} = 2^n \log_2 2 = 2^n \quad \Rightarrow \quad \log_2 \log_2 x = \log_2 2^n = n \log_2 2 = n$$

Per tant, $n = \log_2 \log_2 x$ i obtenim una fita inferior (i molt dolenta) de $\pi(x)$.

$$\pi(x) \geq \log_2 \log_2 x + 1 > \log_2 \log_2 x$$

D'aquesta manera, obtenim la primera desigualtat que ens relaciona $\pi(x)$ amb els logaritmes.

$$\pi(x) > \log_2 \log_2 x \tag{3.9}$$

Podem millorar els resultats treballant una mica més. Per fer-ho, utilitzarem les funcions factorial [5], $n!$, i part entera[6], $\lfloor x \rfloor$. Amb aquestes funcions podem comptabilitzar amb la contribució de cada factor primer p_r en la descomposició de $n!$. Per exemple,

$$13! = 6\ 227\ 020\ 800 = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$$

És a dir, $p_1 = 2$ apareix 10 vegades, $p_2 = 3$ apareix 5 vegades, etc. Diem que l'exponent total del 2 en la descomposició de 13! és 10. El nostre objectiu és calcular $\mathrm{E}_{p_r}(n!)$, l'exponent total del nombre primer p_r en la descomposició de $n!$.

Observem en primer lloc que, donat un primer $p < n$, tenim justament $\lfloor n/p \rfloor$ nombres enters inferiors a n que són divisibles per p. Aleshores, p apareix en la descomposició de $n!$ precisament $\lfloor n/p \rfloor$ vegades. És a dir, si $n = 100$ i $p = 7$, tenim $\lfloor 100/7 \rfloor = 14$ nombres inferiors a 100 divisibles per 7 (7,14, 21, 28, ..., 98) i en la descomposició de 100! tindrem, com a mínim., el factor 7^{14}.

De la mateixa manera, p^2 apareix en la descomposició de $n!$ precisament $\left\lfloor n/p^2 \right\rfloor$ vegades, p^3 apareix $\left\lfloor n/p^3 \right\rfloor$ vegades i així successivament fins que p^k apareix $\left\lfloor n/p^k \right\rfloor$ vegades, on $p^{k+1} > n$. L'exponent total de p en la descomposició de $n!$, $\mathrm{E}_p(n!)$, es pot expressar com:

$$\mathrm{E}_p(n!) = \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor , \tag{3.10}$$

on els termes de la sèrie anterior són zero per $r \geq k + 1$ i, per tant, la sèrie (3.10) té suma finita.

[5] Es defineix el factorial de n com el producte $n! = n \cdot (n-1) \cdots 2 \cdot 1$ i $0! = 1$

[6] Es defineix la part entera de x, $\lfloor x \rfloor$, com l'enter més gran inferior, o igual, a x. Per exemple, $\lfloor \sqrt{2} \rfloor = 1$, $\lfloor -\pi \rfloor = -4$ i $\lfloor n \rfloor = n$ per a tot $n \in \mathbb{Z}$.

Seguint amb l'exemple anterior, l'exponent total de $p_4 = 7$ en la descomposició de 100! és la suma finita

$$\mathrm{E}_7(100!) = \left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{7^2} \right\rfloor + \left\lfloor \frac{100}{7^3} \right\rfloor + \cdots = 14 + 2 + 0 + 0 + \cdots = 16$$

Si calculem l'exponent total per a cada nombre primer inferior a 100, obtindrem la descomposició en factors primers de 100!. Atès que $\sqrt{100} = 10$, els nombres primers més grans que 10, contribuiran només amb el terme $\lfloor 100/p \rfloor$. Això passarà des de $p_5 = 11$ fins a $p_{25} = 97$. Per als altres nombres primers, la contribució serà més alta.

$$\begin{aligned}
p_1 = 2 : \quad &\Rightarrow \quad \mathrm{E}_2(100!) = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor = 97 \\
p_2 = 3 : \quad &\Rightarrow \quad \mathrm{E}_3(100!) = \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{9} \right\rfloor + \left\lfloor \frac{100}{27} \right\rfloor + \left\lfloor \frac{100}{81} \right\rfloor = 48 \\
p_3 = 5 : \quad &\Rightarrow \quad \mathrm{E}_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 24 \\
p_4 = 7 : \quad &\Rightarrow \quad \mathrm{E}_7(100!) = \left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{49} \right\rfloor = 16 \\
p_5 = 11 : \quad &\Rightarrow \quad \mathrm{E}_{11}(100!) = \left\lfloor \frac{100}{11} \right\rfloor = 9 \\
&\cdots \\
p_{25} = 97 : \quad &\Rightarrow \quad \mathrm{E}_{97}(100!) = \left\lfloor \frac{100}{97} \right\rfloor = 1
\end{aligned}$$

Ara podem escriure la descomposició factorial de $n!$ com

$$n! = \prod_{p \le n} p^{\mathrm{E}_p(n!)} = \prod_{p \le n} p^{\sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor} \tag{3.11}$$

El resultat anterior fou utilitzat per Legendre per obtenir una estimació de $\pi(x)$. El càlcul es basa en el següent fet:

$$\mathrm{E}_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots,$$

on aquesta sèrie és finita. Podem trobar una fita superior de $\mathrm{E}_p(n!)$ prescindint de la funció $\lfloor\ \rfloor$, obtenint una sèrie geomètrica de raó $1/p$, que és fàcilment sumable fins a l'infinit atès que $0 < 1/p < 1$.

$$\mathrm{E}_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \frac{n}{p} \cdot \frac{1}{1 - 1/p} = \frac{n}{p-1}$$

Aquesta darrera expressió ens diu que $p^{\mathrm{E}_p(n!)} < p^{n/(p-1)}$. Atès que, per a cada nombre $n \ge 2$ es compleix $n \le 2^{n-1}$, obtenim que

$$p^{\mathrm{E}_p(n!)} < p^{n/(p-1)} < (2^{p-1})^{n/(p-1)} = 2^n$$

És a dir, $p^{\mathrm{E}_p(n!)} < 2^n$. Cada factor de l'expressió (3.11) es pot fitar per aquesta desigualtat

$$n! = \prod_{p \le n} p^{\mathrm{E}_p(n!)} < \prod_{p \le n} 2^n$$

Però aquest darrer productori té tants factors com nombres primers hi ha per sota de n. És a dir, té $\pi(n)$ factors. Per tant,

$$n! < \underbrace{2^n \cdot 2^n \cdots 2^n}_{\pi(n)} \quad \Rightarrow \quad n! < (2^n)^{\pi(n)} = 2^{n\pi(n)}$$

Prenent logaritmes en base 2 en aquesta darrera expressió,

$$\log_2 n! < \log_2 2^{n\pi(n)} \quad \Rightarrow \quad \pi(n) > \frac{\log_2 n!}{n}$$

Aquesta darrera desigualtat la podem avaluar per a n gran utilitzant la *fórmula d'Stirling*[7]

$$\log_2 n! \approx \log_2 \left(n^n \, e^{-n} \sqrt{2\pi n} \right) \approx \log_2 n^n + \log_2 e^{-n} + \log_2 \sqrt{2\pi n}$$
$$\log n! \approx n \log_2 n - n \log_2 e + \log_2 \sqrt{2\pi n}$$

Quan $n \to \infty$, el terme $\log_2 \sqrt{2\pi n}$ es pot menysprear respecte als altres dos. Per tant,

$$\Rightarrow \quad \log_2 n! \approx n \log_2 \frac{n}{e}, \quad n \to \infty$$

Finalment, per a n gran ($n \to \infty$), obtenim l'estimació:

$$\pi(n) > \frac{1}{n} \log_2 n! \quad \Rightarrow \quad \pi(n) \approx \log_2 \frac{n}{e} \tag{3.12}$$

A la taula 3.5 comparem les estimacions obtingudes a (3.9) i (3.12) amb el valor exacte de $\pi(x)$.

Daniel Meissel(1826-1895) utilitzà el garbell d'Eratòstenes (taula 3.1) i eines de combinatòria per calcular el valor exacte de $\pi(x)$ per a valors baixos de x. En aquest cas hem d'entendre l'adjectiu baix comparant x amb el cardinal de $\mathbb{N}$, que és infinit, atès que Meissel arribà a calcular exactament $\pi(10^8)$ (1870) i s'equivocà de 56 termes en el valor exacte de $\pi(10^9)$ (1885). El mètode es basa en el principi d'inclusió-exclusió i en l'ús de la funció part entera de x, $\lfloor x \rfloor$.

Suposem fixat un enter x i que tenim accés a la llista de nombres primers inferiors o iguals a $\sqrt{x}$: 2, 3, 5, ...,p_k amb $p_k \le \sqrt{x}$. El primer garbell, el garbell per $p_1 = 2$ eliminarà $\left\lfloor \frac{x}{2} \right\rfloor$ nombres deixant $x - \left\lfloor \frac{x}{2} \right\rfloor$ nombres. El segon garbell, el garbell per $p_2 = 3$ eliminarà els múltiples de 3 i també els múltiples de 6, que ja els havíem eliminat en el garbell de $p_1 = 2$. Per tant, utilitzant el principi d'inclusió-exclusió, ens quedaran

$$x - \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x}{2 \cdot 3} \right\rfloor = x - \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x}{6} \right\rfloor \qquad \text{nombres}$$

[7] S'utilitza per avaluar $n!$ quan $n \to \infty$: $\quad n! \approx n^n \, e^{-n} \sqrt{2\pi n}$

Taula 3.5: Comparació de $\pi(x)$ amb les estimacions (3.9) i (3.12).

n	$\pi(n)$	$\log_2 \log_2 n$	$\frac{1}{n}\log_2 n!$
10^6	78 498	4.32	18.49
10^7	664 579	4.54	21.81
10^8	5 761 455	4.73	25.1
10^9	50 847 534	4.9	28.5
10^{10}	455 052 511	5.05	31.8
10^{11}	4 118 054 813	5.2	35.1
10^{12}	37 607 912 018	5.32	38.4
10^{13}	346 065 536 839	5.43	41.7

Podem continuar el raonament amb el tercer garbell per a $p_3 = 5$. Ara haurem de compensar els múltiples de $2 \cdot 3 \cdot 5$ que els haurem eliminat més d'una vegada. Aplicant directament el principi d'inclusió-exclusió, ens quedaran

$$x - \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor - \left\lfloor \frac{x}{5} \right\rfloor + \left\lfloor \frac{x}{2\cdot 3} \right\rfloor + \left\lfloor \frac{x}{2\cdot 5} \right\rfloor + \left\lfloor \frac{x}{3\cdot 5} \right\rfloor - \left\lfloor \frac{x}{2\cdot 3\cdot 5} \right\rfloor \qquad \text{nombres}$$

I així aniríem continuant fins arribar a p_k, que és el primer més gran tal que $p_k \leq \sqrt{x}$. Si hem començat la llista per 1, ens hem deixat aquest nombre i tots els nombres primers entre $\sqrt{x}$ i x. És a dir, el nombre que hauríem calculat seria $\pi(x) - \pi(\sqrt{x}) + 1$. Aïllant $\pi(x)$ d'aquesta darrera igualtat podem escriure, per tant:

$$\begin{aligned} \pi(x) = x + \pi(\sqrt{x}) - 1 &- \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor - \left\lfloor \frac{x}{5} \right\rfloor - \cdots \\ &+ \left\lfloor \frac{x}{2\cdot 3} \right\rfloor + \left\lfloor \frac{x}{2\cdot 5} \right\rfloor + \left\lfloor \frac{x}{3\cdot 5} \right\rfloor + \cdots \\ &- \left\lfloor \frac{x}{2\cdot 3\cdot 5} \right\rfloor - \cdots \end{aligned} \tag{3.13}$$

Podem aplicar el mètode anterior per veure com calculem exactament la quantitat de nombres primers que hi ha per sota $n = 100$, sabent que per sota la seva arrel quadrada, 10, n'hi ha 4: 2, 3, 5 i 7. En aquest cas l'expressió (3.13) pren la forma

$$\begin{aligned} \pi(100) = 100 + \pi(\sqrt{100}) - 1 &- \left\lfloor \frac{100}{2} \right\rfloor - \left\lfloor \frac{100}{3} \right\rfloor - \left\lfloor \frac{100}{5} \right\rfloor - \left\lfloor \frac{100}{7} \right\rfloor \\ &+ \left\lfloor \frac{100}{2\cdot 3} \right\rfloor + \left\lfloor \frac{100}{2\cdot 5} \right\rfloor + \left\lfloor \frac{100}{2\cdot 7} \right\rfloor + \left\lfloor \frac{100}{3\cdot 5} \right\rfloor + \left\lfloor \frac{100}{3\cdot 7} \right\rfloor + \left\lfloor \frac{100}{5\cdot 7} \right\rfloor \\ &- \left\lfloor \frac{100}{2\cdot 3\cdot 5} \right\rfloor - \left\lfloor \frac{100}{2\cdot 3\cdot 7} \right\rfloor - \left\lfloor \frac{100}{2\cdot 5\cdot 7} \right\rfloor - \left\lfloor \frac{100}{3\cdot 5\cdot 7} \right\rfloor \\ &+ \left\lfloor \frac{100}{2\cdot 3\cdot 5\cdot 7} \right\rfloor \end{aligned}$$

Si calculem el valor numèric d'aquesta darrera expressió obtenim el resultat conegut, però sorprenent, de la quantitat de nombres primers que hi ha per sota $x = 100$.

$$\pi(100) = 100 - 4 - 1 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 = 25$$

Si som una mica menys precisos, podem anar una mica més lluny i arribar a un primer resultat que té connotacions futures molt importants. Per fer-ho, deixem de banda la funció part entera, $\lfloor x \rfloor$, i la duplicació dels nombres eliminats en els successius garbells. Aleshores, podem dir que la meitat dels nombres des d'1 fins a x són divisibles per dos, deixant-ne $\left(1 - \frac{1}{2}\right) x$. Que d'aquests, una tercera part seran divisibles per 3, deixant-ne ara $\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) x$. Que d'aquests, aproximadament, una cinquena part seran divisibles per 5, deixant-ne $\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) x$, etc. Si aquest procés el repetim per a tots els nombres primers $\leq \sqrt{x}$, tenim que la quantitat de nombres no eliminats, això és $\pi(x)$, és aproximadament

$$\pi(x) \approx \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) x \tag{3.14}$$

L'error que provoquem amb totes aquestes aproximacions va creixent a mida que x es va fent gran. Però ens condueix a un resultat prou notable. L'expressió (3.14) està íntimament relacionada amb una expressió que va trobar Franz C. J.Mertens (1840-1927):

$$e^{\gamma} = \lim_{n \to \infty} \frac{1}{\ln n} \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right)^{-1}$$

on γ és l'anomenada *constant d'Euler*[8]

Si prescindim del límit, podem reorganitzar la igualtat de Mertens com:

$$\prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) \approx \frac{e^{-\gamma}}{\ln n}$$

per a n gran. Si fem $n = \sqrt{x}$ obtenim l'aproximació

$$\pi(x) \approx \frac{e^{-\gamma} x}{\ln \sqrt{x}} = 2e^{-\gamma} \frac{x}{\ln x}, \qquad \text{per a } x \text{ gran}$$

[8]En alguns llibres s'anomena constant d'Euler-Mascheroni. Es defineix com

$$\gamma = \lim_{n \to \infty} 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n} - \ln n = \lim_{n \to \infty} \left(\sum_{k=1}^{n} \frac{1}{k} \right) - \ln n \approx 0.577\,215\,664\,901\,532\,860 \ldots$$

Aquesta constant, de la qual encara no s'ha determinat la seva irracionalitat, sorgeix de manera natural en estudiar la sèrie harmònica discreta H_n

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

La natura de γ fou estudiada seriosament per primera vegada per L.Euler i apareix en múltiples qüestions de la teoria analítica de nombres relacionades amb l'estudi dels nombres primers.

Taula 3.6: Valors comparats de $\pi(x)$ amb $M(x) = 2e^{-\gamma}\frac{x}{\ln x}$

	10^4	10^8	10^{12}
$\pi(x)$	1229	5 761 455	37 607 912 018
$M(x)$	1219.19	6 095 968.88	40 639 792 587.55
error	0.798%	5.48%	7.46%

Per primera vegada apareix la important expressió $\dfrac{x}{\ln x}$ relacionada amb la funció $\pi(x)$. La taula 3.6 compara els valors obtinguts amb aquesta nova aproximació.

Amb l'aparició per primera vegada de la funció $\dfrac{x}{\ln x}$ relacionada amb la funció $\pi(x)$ és normal demanar-se quina és, o quines són, les millors aproximacions que podem tenir de la funció $\pi(x)$. Al primer terc del segle XIX hi hagué, com s'ha comentat en la secció anterior (3.2), una tensa discussió entre Gauss i Legendre defensant, cadascun d'ells, la seva aproximació de $\pi(x)$ com a millor. Tanmateix, podem veure que ambdues expressions són equivalents i que, a la llarga, la millor aproximació per a $x \to \infty$ la donarà l'expressió $\dfrac{x}{\ln x}$, com ens assegura el *teorema del nombre primer (TNP)*. Veiem ara, però, que les aproximacions de Gauss i Legendre són equivalents.

Anomenem ε_x a l'error comès en aproximar $\pi(x)$ per una funció $f(x)$. És a dir, escrivim $\pi(x) = f(x) + \varepsilon_x$. Aleshores,

$$\frac{\pi(x)}{f(x)} = 1 + \frac{\varepsilon_x}{f(x)}$$

Si ens concentrem en el comportament asimptòtic de $\pi(x)$ (i.e. quan $x \to \infty$) esperem, evidentment, que el terme de l'error relatiu tendeixi a zero.

$$\lim_{x\to\infty} \frac{\varepsilon_x}{f(x)} = 0 \quad \Rightarrow \quad \lim_{x\to\infty} \frac{\pi(x)}{f(x)} = 1$$

És usual representar aquest darrer comportament amb la notació $\pi(x) \sim f(x)$.

És perfectament clar que, per a qualsevol constant k, si el límits següents existeixen,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} \quad \text{i} \quad \lim_{x\to\infty} \frac{\pi(x)}{x/(\ln x + k)}$$

han de ser iguals. En efecte,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(\ln x + k)} = \lim_{x\to\infty} \frac{\pi(x)(\ln x + k)}{x} = \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} + \lim_{x\to\infty} \frac{k\pi(x)}{x} = \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x}$$

atès que $\pi(x)$ és molt més petit que x i, per tant, $\lim\limits_{x\to\infty} \dfrac{k\pi(x)}{x} = 0$. Aquest fet ens implica que totes les expresions

$$\pi(x) \sim \frac{x}{\ln x} \qquad \pi(x) \sim \frac{x}{\ln x - 1.08366}$$

$$\pi(x) \sim \frac{x}{\ln x + 1} \qquad \pi(x) \sim \frac{x}{\ln x - e^{\pi}}$$

són equivalents en aquest sentit. Per tant, el resultat de Legendre no contradiu el *TNP*. Que les expressions del *TNP* i l'aproximació de Gauss, el logaritme integral, són equivalents, requereix una mica més de feina

$$\pi(x) \sim \frac{\pi(x)}{x/\ln x} \qquad \text{i} \qquad \pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

Per veure-ho, ens cal assumir que:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Aleshores,

$$\lim_{x\to\infty} \frac{\pi(x)}{\int_2^x \frac{dt}{\ln t}} = \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} \cdot \frac{x/\ln x}{\int_2^x \frac{dt}{\ln t}} = 1 \cdot \lim_{x\to\infty} \frac{x/\ln x}{\int_2^x \frac{dt}{\ln t}}$$

Calculem aquest darrer límit amb l'ajut de la *regla de l'Hôpital*

$$\lim_{x\to\infty} \frac{(\ln x - 1)/\ln^2 x}{1/\ln x} = \lim_{x\to\infty} \left(\frac{\ln x - 1}{\ln^2 x} \cdot \ln x \right) = \lim_{x\to\infty} \frac{\ln x - 1}{\ln x} = 1$$

Per tant, ara som en condicions d'enunciar formalment el *teorema del nombre primer*

Teorema 3.3.1 (Teorema del Nombre Primer)
La quantitat de nombres primers per sota d'un cert nombre donat x, $\pi(x)$, satisfà la relació asimptòtica

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

La demostració d'aquest teorema escapa al nivell d'aquest treball. Fou demostrat simultàniament per Jacques Hadamard i Charles de la Vallée-Poussin el 1896 i les eines utilitzades en la seva demostració són molt, però molt elaborades. Tècnicament es tracta de demostrar que la funció zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

extesa a tot el pla complex per continuació analítica, llevat d'un pol simple a $s = 1$, no té zeros no trivials a la recta $s = 1$. Per reflexió es demostra que la funció $\zeta(s)$ tampoc té zeros no trivials a la recta $s = 0$.

Cinquanta anys més tard, el 1949, Paul Erdös (1913-1996) i Atle Selberg (1917-2007) publicaren[9] una demostració del *TNP* anomenada *elemental*. En aquest cas, però, l'adjectiu elemental només fa referència al fet que no s'utilitzà la sofisticada maquinària de les funcions en variable complexa. És, des de qualsevol punt de vista, una demostració difícil i elaborada.

[9]Erdös, P. *"On a new method in elementary number theory wich leads to an elementary proof of the prime number theorem"*, Proc. Nat. Academy Scientific, vol. 35, pp 374-384, USA-1949.

Selberg A. *"An elementary proof of the prime number theorem"*, Annals of Mathematics, vol 50-2, pp 305-313, USA-1949

Tot i que la demostració del *TNP* és inabastable per aquest treball, establirem a continuació una desigualtat molt més feble però que, en qualsevol cas, ens indica que la funció $\pi(x)$ està relacionada amb la funció $\dfrac{x}{\ln x}$. Abans d'enunciar-la, però, ens cal demostrar uns lemes preliminars.

Lema 3.3.1
Per a tot nombre natural $n \geq 1$ es compleix

$$2^n \leq \binom{2n}{n} < 4^n \tag{3.15}$$

on $\binom{2n}{n} = \dfrac{(2n)!}{n!\,n!}$ *és el nombre combinatori* C_n^{2n}.

Demostració.
Demostrarem cada desigualtat per separat.

1. La primera desigualtat es demostra per inducció.

   1.1. Comprovem primer el cas $n = 1$. En efecte,

   $$2 \leq \binom{2}{1} = 2$$

   1.2. Suposem certa la desigualtat per a n. Volem veure la desigualtat per a $n+1$.

   $$2^n \leq \binom{2n}{n} \quad \overset{?}{\Rightarrow} \quad 2^{n+1} \leq \binom{2(n+1)}{n+1}$$

   L'expressió $\binom{2(n+1)}{n+1}$ es pot escriure com

   $$\binom{2(n+1)}{n+1} = \frac{(2n+2)!}{(n+1)!\,(n+1)!} = \frac{(2n+2)(2n+1)(2n)!}{(n+1)!\,(n+1)!} = \frac{2(2n+1)(2n)!}{n!\,(n+1)!}$$

   Aleshores, emprant la hipòtesi d'inducció,

   $$2^{n+1} = 2 \cdot 2^n \leq 2\binom{2n}{n} = \frac{2\,(2n)!}{n!\,n!} \leq \frac{2(2n+1)(2n)!}{n!\,(n+1)!}$$

   atès que $1 < \dfrac{2n+1}{n+1}$ per a $n \geq 1$

2. La segona desigualtat es demostra aplicant el *binomi de Newton*[10]

   $$\binom{2n}{n} < \sum_{k=0}^{2n} \binom{2n}{k} = (1+1)^{2n} = 4^n$$

[10] Per a tot $n \in \mathbb{N}$ es compleix: $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

□

Lema 3.3.2
Si $\sigma > 0$ i $x \geq 1$, la funció $f(x) = \dfrac{\ln x}{x^\sigma}$ té un màxim absolut quan $x = e^{1/\sigma}$

Demostració.

Derivem respecte x la funció $f(x)$: $\quad \Rightarrow \quad f'(x) = \dfrac{1 - \sigma \ln x}{x^{1+\sigma}}$

Igualem $f'(x) = 0$: $\quad \Leftrightarrow \quad 1 - \sigma \ln x = 0 \quad \Leftrightarrow \quad x = e^{1/\sigma}$

Atès que: $\left\{ \begin{array}{l} \lim\limits_{x \to -1^+} \dfrac{\ln x}{x^\sigma} = 0 \\ \lim\limits_{x \to +\infty} \dfrac{\ln x}{x^\sigma} = 0 \end{array} \right\}$; i que: $\left\{ \begin{array}{l} x \in (1, e^{1/\sigma}) \Rightarrow f'(x) > 0 \Rightarrow f(x) \ \nearrow \\ x \in (e^{1/\sigma}, +\infty) \Rightarrow f'(x) < 0 \Rightarrow f(x) \ \searrow \end{array} \right\}$

Aleshores, $f(x)$ té un màxim absolut en $x = e^{1/\sigma}$ i $f\left(e^{1/\sigma}\right) = \dfrac{1}{\sigma e}$

La figura 3.9 ens mostra el comportament de $f(x)$.

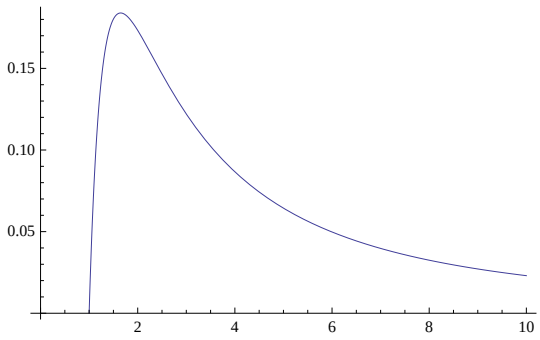


Figura 3.9: Representació de la funció $f(x) = x^{-\sigma} \ln x$, $\sigma > 0$, $x \geq 1$

□

Lema 3.3.3

$$\ln 2 + \frac{1}{2e} < 1$$

Demostració.

$$\ln 2 + \frac{1}{2e} < 1 \quad \Leftrightarrow \quad \ln 2 < 1 - \frac{1}{2e} \quad \Leftrightarrow \quad \ln 2 < \frac{2e - 1}{2e}$$

Per demostrar aquesta darrera desigualtat, demostrarem

$$\ln 2 < \frac{4}{5} < \frac{2e - 1}{2e}$$

Pel que fa a la primera desigualtat:

$$\ln 2 < \frac{4}{5} \quad \Leftrightarrow \quad 5 \ln 2 < 4 \quad \Leftrightarrow \quad \ln 32 < \ln e^4$$

Per tant, cal veure que $32 < e^4$. Atès que $\frac{5}{2} < e$, això implica $32 < \frac{625}{16} < e^4$.

Pel que fa a la segona desigualtat:

$$\frac{4}{5} < \frac{2e-1}{2e} \quad \Leftrightarrow \quad 5 < 2e \quad \Leftrightarrow \quad \frac{5}{2} < e$$

□

Lema 3.3.4
Si $x \geq 1$ aleshores $\ln x \leq \frac{2}{e}\sqrt{x}$

Demostració.

Considerem la funció $f(x) = \frac{2}{e}\sqrt{x} - \ln x$. Observem que $f(1) = \frac{2}{e} > 0$ i que

$$f'(x) = \frac{1}{e\sqrt{x}} - \frac{1}{x} \quad \Rightarrow \quad f'(x) = 0 \quad \Leftrightarrow \quad x = e^2$$

Atès que: $\left.\begin{array}{c} x \in (1, e^2) \Rightarrow f'(x) < 0 \Rightarrow f(x) \searrow \\ x \in (e^2, \infty) \Rightarrow f'(x) > 0 \Rightarrow f(x) \nearrow \end{array}\right\} \quad \Rightarrow \quad x = e^2$ és un mínim de $f(x)$.

A més, $f(e^2) = 0$ i $\lim_{x\to\infty} f(x) = +\infty$. Per tant, $f(x) \geq 0 \quad \Rightarrow \quad \ln x \leq \frac{2}{e}\sqrt{x}$

□

El següent teorema demostra que $n/\ln n$ és del mateix ordre de magnitud que $\pi(n)$.

Teorema 3.3.2
Per a tot enter $n \geq 2$ es compleix

$$\frac{1}{6}\frac{n}{\ln n} \; < \; \pi(n) \; < \; 6\frac{n}{\ln n} \tag{3.16}$$

Demostració.

Demostrarem en primer lloc la primera desigualtat, $\frac{1}{6}\frac{n}{\ln n} < \pi(n)$

Segons el lema 3.3.1

$$2^n < \frac{(2n)!}{n!n!} < 4^n$$

Prenem logaritmes neperians en aquesta darrera desigualtat:

$$n \ln 2 < \ln((2n)!) - 2\ln(n!) < n \ln 4 \tag{3.17}$$

Recordem les expressions (3.11) i (3.10)

$$n! = \prod_{p \leq n} p^{\mathrm{E}_p(n!)} \quad \text{on} \quad \mathrm{E}_p(n!) = \sum_{m=1}^{\infty} \left\lfloor \frac{n}{p^n} \right\rfloor$$

Aquesta darrera suma és finita atès que, si $n < p^m$, aleshores $\left\lfloor \frac{n}{p^m} \right\rfloor = 0$. És a dir,

$$n < p^m \quad \Rightarrow \quad \ln n < m \ln p \quad \Rightarrow \quad \frac{\ln n}{\ln p} < m$$

Per tant, els valors de m que cal sumar són entre 1 i $\left\lfloor \dfrac{\ln n}{\ln p} \right\rfloor$.

$$\mathrm{E}_p(n!) = \sum_{m=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^m} \right\rfloor$$

Prenem de nou logaritmes a l'expressió (3.11)

$$\ln(n!) = \sum_{p \leq n} \mathrm{E}_p(n!) \ln p = \sum_{p \leq n} \sum_{m=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^m} \right\rfloor$$

Aleshores, el $\ln((2n)!)$ s'expressa com:

$$\ln((2n)!) = \sum_{p \leq 2n} \mathrm{E}_p(2n)! \ln p = \sum_{p \leq 2n} \sum_{m=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} \left\lfloor \frac{2n}{p^m} \right\rfloor$$

Per tant, utilitzant el fet que $\lfloor 2x \rfloor - 2 \lfloor x \rfloor = 0$, si $x \in \mathbb{N}$, i $\lfloor 2x \rfloor - 2 \lfloor x \rfloor = 1$, si $x \notin \mathbb{N}$, podem fitar la diferència

$$\ln((2n)!) - \ln(n!) = \sum_{p \leq 2n} \sum_{m=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} \left(\left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right) \ln p < \sum_{p \leq 2n} \left(\sum_{m=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} 1 \right) \ln p \qquad (3.18)$$

Per tant,

$$\ln((2n)!) - \ln(n!) < \sum_{p \leq 2n} \left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor \ln p < \sum_{p \leq 2n} \frac{\ln 2n}{\ln p} \cdot \ln p = \sum_{p \leq 2n} \ln 2n = \pi(2n) \ln 2n$$

Ara podem escriure (3.17) com

$$n \ln 2 < \ln((2n)!) - 2 \ln n! < \pi(2n) \ln 2n$$

Per tant,

$$\frac{n \ln 2}{\ln 2n} < \pi(2n) \qquad (3.19)$$

Observant el fet que:

$$e < 4 \quad \Rightarrow \quad e^{1/2} < 2 \quad \Rightarrow \quad \frac{1}{2} < \ln 2 \quad \Rightarrow \quad \frac{1}{4} < \frac{\ln 2}{2}$$

podem fitar l'expressió (3.19) com:

$$\frac{2n \ln 2}{2 \ln(2n)} < \pi(2n) \quad \Rightarrow \quad \frac{1}{4} \cdot \frac{2n}{\ln 2n} < \pi(2n) \qquad (3.20)$$

Hem obtingut una fita inferior de $\pi(x)$ per a valors d'x enters parells, $x = 2n$. En el cas que x sigui un nombre senar, $x = 2n+1$, podem obtenir una fita inferior de $\pi(x)$ emprant el fet que la funció $\ln x$ és estrictament creixent així com la desigualtat

$$\frac{2n}{2n+1} > \frac{2}{3}, \qquad \forall\, n \geq 1$$

En efecte,

$$\pi(2n+1) > \pi(2n) > \frac{1}{4}\cdot\frac{2n}{\ln 2n} > \frac{1}{4}\cdot\frac{2n}{2n+1}\cdot\frac{2n+1}{\ln(2n+1)} > \frac{1}{6}\cdot\frac{2n+1}{\ln(2n+1)} \tag{3.21}$$

Hem obtingut dues fitacions: una pels parells (3.20) i una pels senars (3.21). Ajuntant les dues, prenem la més restrictiva. Per tant, tenim demostrada la primera desigualtat:

$$\frac{1}{6}\frac{n}{\ln n} < \pi(n) \quad \forall n \geq 2$$

Ara hem de demostrar l'altra desigualtat, $\pi(n) < 6\dfrac{n}{\ln n}$. Per fer-ho, separem de l'expressió (3.18) els termes que corresponen a $m = 1$. La resta de termes són positius. Per tant,

$$\begin{aligned}
\ln((2n)!) - \ln(n!) &= \sum_{p\leq 2n}\sum_{m=1}^{\left\lfloor \frac{\ln 2n}{\ln p}\right\rfloor}\left(\left\lfloor\frac{2n}{p^m}\right\rfloor - 2\left\lfloor\frac{n}{p^m}\right\rfloor\right)\ln p \\
&= \sum_{p\leq 2n}\left\{\left\lfloor\frac{2n}{p}\right\rfloor - 2\left\lfloor\frac{n}{p}\right\rfloor + \sum_{m=2}^{\left\lfloor \frac{\ln 2n}{\ln p}\right\rfloor}\left(\left\lfloor\frac{2n}{p^m}\right\rfloor - 2\left\lfloor\frac{n}{p^m}\right\rfloor\right)\right\}\ln p \\
\Rightarrow \quad \ln((2n)!) - 2\ln(n!) &\geq \sum_{p\leq 2n}\left(\left\lfloor\frac{2n}{p}\right\rfloor - 2\left\lfloor\frac{n}{p}\right\rfloor\right)\ln p
\end{aligned}$$

Si p és primer i $n < p \leq 2n$, aleshores $\left\lfloor\dfrac{2n}{p}\right\rfloor - 2\left\lfloor\dfrac{n}{p}\right\rfloor = 1$. És a dir,

$$\ln((2n)!) - 2\ln(n!) \leq \sum_{n<p\leq 2n}\ln p = \vartheta(2n) - \vartheta(n)$$

on $\vartheta(n)$ és la *funció theta de Txebixev*[11]

Per tant, segons (3.17),

$$\vartheta(2n) - \vartheta(n) < n\ln 4$$

[11] La funció ϑ (theta) de Txebixev es defineix per a tot $x > 0$ com:

$$\vartheta(x) = \sum_{p\leq x}\ln p$$

on p recorre tots els primers $\leq x$. La següent taula mostra els primers valors de $\vartheta(x)$.

x	1	2	3	4	5	6	7	8	9	10
$\vartheta(x)$	0	$\ln 2$	$\ln 6$	$\ln 6$	$\ln 30$	$\ln 30$	$\ln 210$	$\ln 210$	$\ln 210$	$\ln 210$

En particular, si $n = 2^k$ és una potència de 2,

$$\vartheta(2^{k+1}) - \vartheta(2^k) < 2^k \ln 4 = 2^{k+1} \ln 2$$

Si sumem per a $k = 0, 1, 2, ...,r$

$$\sum_{k=0}^{r} \Big(\vartheta(2^{k+1}) - \vartheta(2^k)\Big) < \sum_{k=0}^{r} \Big(2^{k+1} \ln 2\Big)$$

El primer membre és una *sèrie telescòpica*[12]

$$\begin{aligned}\sum_{k=0}^{r} \Big(\vartheta(2^{k+1}) - \vartheta(2^k)\Big) &= \cancel{\vartheta(2)} - \vartheta(1) + \cancel{\vartheta(3)} - \cancel{\vartheta(2)} + \cdots + \vartheta(2^{r+1}) - \cancel{\vartheta(2^r)} \\ &= \vartheta(2^{r+1}) - \vartheta(1) = \vartheta(2^{r+1})\end{aligned}$$

El segon membre és una sèrie geomètrica de raó 2. Per tant,

$$\sum_{k=0}^{r} \Big(2^{k+1} \ln 2\Big) = \ln 2 \sum_{k=0}^{r} 2^{k+1} = \ln 2 \cdot \frac{2 - 2^{r+2}}{1-2} = (2^{r+2} - 2) \ln 2 < 2^{r+2} \ln 2$$

Per tant, obtenim la desigualtat

$$\vartheta(2^{r+1}) < 2^{r+2} \ln 2$$

Ara escollim r de manera que $2^r < n < 2^{r+1} \quad \Rightarrow \quad 2^{r+2} < 4n < 2^{r+3}$. Aleshores,

$$\vartheta(n) \leq \vartheta(2^{r+1}) < 2^{r+2} \ln 2 \leq 4n \ln 2$$

Considerem ara $0 < \alpha < 1$. Aleshores,

$$\left.\begin{aligned}\pi(n) &= \sum_{p \leq n} 1 \\ \pi(n^\alpha) &= \sum_{p \leq n^\alpha} 1\end{aligned}\right\} \Rightarrow \pi(n) - \pi(n^\alpha) = \sum_{n^\alpha < p \leq n} 1 \Rightarrow (\pi(n) - \pi(n^\alpha)) \ln n^\alpha = \sum_{n^\alpha < p \leq n} \ln n^\alpha$$

En aquest darrer sumatori, $\ln n^\alpha$ és el terme més petit. Per tant,

$$(\pi(n) - \pi(n^\alpha)) \ln n^\alpha < \sum_{n^\alpha < p \leq n} \ln p \leq \vartheta(n) < 4n \ln 2$$

És a dir, hem arribat a que

$$\begin{aligned}&\pi(n) < \frac{4n \ln 2}{\alpha \ln n} + \pi(n^\alpha) < \frac{4n \ln 2}{\alpha \ln n} + n^\alpha \\ \Rightarrow \quad &\pi(n) < \frac{n}{\ln n} \left(\frac{4 \ln 2}{\alpha} + \frac{\ln n}{n^{1-\alpha}}\right)\end{aligned}$$

[12] És una sèrie on termes consecutius es van cancel·lant de manera que la seva suma es redueix a la diferència entre el darrer terme i el primer.

Si $\alpha = 2/3 \quad \Rightarrow \quad \dfrac{\ln n}{n^{1-\alpha}} = \dfrac{\ln n}{n^{1/3}}$. Considerem $f(x) = \dfrac{\ln x}{x^{1/3}}$. Segons el lema 3.3.2,

$$\frac{\ln x}{x^{1/3}} \leq \frac{3}{e} \qquad \text{si } x \geq 1$$

Aprofitant el lema 3.3.3 obtenim finalment la desigualtat desitjada,

$$\pi(n) < \frac{n}{\ln n}\left(\frac{4\ln 2}{2/3} + \frac{3}{e}\right) = 6\frac{n}{\ln n}\left(\ln 2 + \frac{1}{2e}\right)$$
$$\Rightarrow \quad \pi(n) < 6\frac{n}{\ln n}$$

□

Aplicant aquest teorema podem establir fites inferiors i superiors de la mida de l'n-èsim nombre primer, p_n.

Teorema 3.3.3
Per a $n \geq 1$, l'n-èsim nombre primer p_n satisfà les desigualtats

$$\frac{1}{6}\, n\, \ln n \;<\; p_n \;<\; 12\left(\, \ln n + n\, \ln\frac{12}{e}\right) \tag{3.22}$$

Demostració.
Si $k = p_n$ aleshores $k \geq 2$ i $\pi(k) = n$. De (3.16) obtenim

$$n = \pi(k) < 6\frac{k}{\ln k} = 6\frac{p_n}{\ln p_n}$$

Per tant, atès que $p_n > n$,

$$p_n > \frac{1}{6} n \ln p_n > \frac{1}{6} n \ln n$$

Hem demostrat, doncs, la fita inferior. Per obtenir la fita superior, tornem a (3.16) i escrivim

$$n = \pi(k) > \frac{1}{6}\frac{k}{\ln k} = \frac{1}{6}\frac{p_n}{\ln p_n}$$

d'on obtenim

$$p_n < 6n \ln p_n \tag{3.23}$$

Atès que $\ln x \leq \dfrac{2}{e}\sqrt{x}$ si $x \geq 1$, (lema 3.3.4) tenim que

$$\ln p_n \leq \frac{2}{e}\sqrt{p_n}$$

Per tant, (3.23) s'escriu com

$$\sqrt{p_n} < \frac{12}{e} n$$

Aleshores, prenent logaritmes,

$$\frac{1}{2}\ln p_n < \ln n + \ln\frac{12}{e}$$

Aquesta darrera desigualtat substituïda a (3.23) ens dóna

$$p_n < 6n\left(2\ln n + 2\ln\frac{12}{e}\right)$$

que és la fita superior de (3.22)

□

Exemple: Si fem $n = 1000$, aleshores el teorema ens diu que $1152 \leq p_{1000} \leq 90631$. La desigualtat és certa, atès que $p_{1000} = 7919$, encara que sigui una mica barroera.

Recordem que en la introducció d'aquest capítol exposàvem que les qüestions importants relacionades amb els nombres primers eren tres:

- Quants nombres primers hi ha per sota d'un nombre donat?
- Qui és l'n-èsim nombre primer, p_n?
- Com saber si un nombre donat n és, o no, primer?

Aquest darrer teorema ens indica que, de fet, les tres qüestions anteriors es redueixen a dues perquè estimar el valor de $\pi(n)$ és equivalent a fer una estimació del valor de p_n. En efecte, si el *TNP* és cert podem deduir que:

$$\begin{aligned}\lim_{n\to\infty}\frac{\pi(n)}{n/\ln n} = 1 \quad &\Rightarrow \quad \lim_{n\to\infty}\ln\left(\frac{\pi(n)}{n/\ln n}\right) = \ln 1 = 0\\ &\Rightarrow \quad \lim_{n\to\infty}\left(\ln\pi(n) - \ln n + \ln\ln n\right) = 0\\ &\Rightarrow \quad \lim_{n\to\infty}\left(\ln n\left(\frac{\ln\pi(n)}{\ln n} + \frac{\ln\ln n}{\ln n} - 1\right)\right) = 0\end{aligned}$$

Atès que la funció $\ln n$ és no fitada quan $n \to \infty$, aleshores

$$\lim_{n\to\infty}\left(\frac{\ln\pi(n)}{\ln n} + \frac{\ln\ln n}{\ln n} - 1\right) = 0$$

Com que $\lim_{n\to\infty}\dfrac{\ln\ln n}{\ln n} = 0$ (fent un canvi de variable $t = \ln n$ i aplicant la regla de l'Hôpital) tenim que

$$\lim_{n\to\infty}\frac{\pi(n)}{\ln n} = 1$$

Per tant,

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\ln n}\cdot\lim_{n\to\infty}\frac{\ln\pi(n)}{\ln n} = \lim_{n\to\infty}\frac{\pi(n)\ln\pi(n)}{n} = 1$$

Si en aquesta darrera igualtat canviem n per l'n-èsim primer, p_n, aleshores la quantitat de nombres primers per sota p_n és, evidentment, n. És a dir, $\pi(p_n) = n$. L'anterior desigualtat ens condueix a:

$$\lim_{n\to\infty}\frac{n\ln n}{p_n} = 1 \quad \Rightarrow \quad p_n \sim n\ln n \tag{3.24}$$

Acabem d'obtenir, a partir d'estudiar el comportament asimptòtic de $\pi(n)$, un comportament asimptòtic del valor de p_n. En un article publicat el 1967 Rosser i Schoenfeld van demostrar el resultat molt més elaborat

$$n\left(\ln n + \ln\ln n - \frac{3}{2}\right) \;<\; p_n \;<\; n\left(\ln n + \ln\ln n - \frac{1}{2}\right) \qquad \text{per } n \geq 20 \tag{3.25}$$

Un argument molt més delicat estableix que

$$p_n \sim n(\ln n + \ln\ln n - 1) \tag{3.26}$$

Els resultats obtinguts a (3.24), (3.25) i (3.26) ens permeten localitzar els intervals on cal buscar l'n-èsim nombre primer. Per exemple, segons (3.25) cal buscar el primer número un milió, $p_{1000000}$, entre els valors 14 941 302 i 15 941 302. Segons (3.26), $p_{1000000} \sim 15\,441\,302$. Els resultats concorden de manera espectacular amb la realitat atès que $p_{1000000} = 15\,485\,863$.

Seguint aquesta darrera línia, la de fitar l'n-èsim nombre primer, demostrarem una propietat curiosa del número 30 que ens permetrà fitar el valor de l'$n+1$-èsim nombre primer, p_{n+1}, en funció dels anteriors nombres primers.

Observem, en primer lloc, que de tots els números inferiors al 10, el 3, el 7 i el 9 són coprimers amb el 10, és a dir,

$$\mathrm{mcd}(3,10) = \mathrm{mcd}(7,10) = \mathrm{mcd}(9,10) = 1$$

Malgrat que el 9 és coprimer amb el 10, el 9 no és ell mateix primer, atès que $9 = 3^2$. En el cas del 12, la situació és una mica diferent. Entre els números de l'1 a l'11, els que són coprimers amb el 12 són, ells mateixos, nombres primers. Parlem del 5, el 7 i l'11. És fàcil veure que aquesta propietat del 12 és compartida pels nombres 3, 4, 6, 8, 12, 18, 24, 30. Doncs bé , el 30 és el nombre més gran tal que tots els nombres inferiors i coprimers amb el 30, són ells mateixos nombres primers. En efecte,

$$A = \{\, n < 30 \,/\, \mathrm{mcd}(n,30) = 1\} = \{7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29\}$$

(tots els elements del conjunt A són nombres primers.)

Veiem per què passa això. Si intentem buscar un nombre amb aquesta propietat, diem-li N, ens adonarem fàcilment que de 4 en endavant N ha de ser divisible per 2. Si fos senar, mcd(N,4)=1 i ja no es compliria la propietat en ser el 4 un compost. Anàlogament, si $N > 9$, ha de ser divisible per 3, altrament es compliria mcd(N,9)=1. Com que en aquest cas també N és divisible per 2, obtenim que N és divisible per 6. Podem, doncs, construir una taula amb aquesta informació.

$$\begin{array}{lcl}
N > 4 & \Rightarrow & 2 \mid N \\
N > 9 & \Rightarrow & 2\cdot 3 \mid N \quad \Rightarrow \quad 6 \mid N \\
N > 25 & \Rightarrow & 2\cdot 3\cdot 5 \mid N \quad \Rightarrow \quad 30 \mid N \\
N > 49 & \Rightarrow & 2\cdot 3\cdot 5\cdot 7 \mid N \quad \Rightarrow \quad 210 \mid N \\
N > 121 & \Rightarrow & 2\cdot 3\cdot 5\cdot 7\cdot 11 \mid N \quad \Rightarrow \quad 2310 \mid N
\end{array}$$

Entre 4 i 9 els únics valors possibles de N són 4, 6 i 8; entre 9 i 25, els valors admesos corresponen a 12, 18 i 24; entre 25 i 49 l'únic número possible és el 30 (el següent múltiple,

60, ja supera 49); entre 49 i 121 ja no hi ha cap possibilitat atès que $210 > 121$. Observem doncs que, a partir d'ara, aquesta desigualtat sempre es mantindrà:

$$13^2 < 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$
$$17^2 < 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$$
$$19^2 < \text{etc...}$$

impedint que puguem trobar un nombre $N > 30$ que compleixi la propietat enunciada. Per tant, $N = 30$ és el nombre més gran tal que els nombres inferiors i coprimers amb ell són, ells mateixos, primers. Però per poder assegurar aquest fet ens cal demostrar que per a qualsevol primer es compleix:

$$p_{n+1}{}^2 < p_1 \cdot p_2 \cdots p_n \quad \Rightarrow \quad p_{n+1} < \sqrt{p_1 \cdot p_2 \cdots p_n} \qquad \forall\, n \geq 4$$

La demostració d'Euclides (2.2.5) demostra que

$$p_{n+1} < p_1 \cdot p_2 \cdots p_n$$

i el que volem demostrar és encara més restrictiu. Cal observar, però, que la fita donada per a p_{n+1} no és molt bona i la discrepància augmenta en dimensió a mesura que n es fa gran. En efecte, si $n = 5$, $p = 11$ i $p_6 < \sqrt{2310} \approx 48$. Però $p_6 = 13$, i 13 queda lluny de 48.

Enunciem, doncs, el següent teorema[13].

Teorema 3.3.4 (Desigualtat de Bonse)

$$\forall n \geq 4 \qquad p_{n+1} < \sqrt{p_1 \cdot p_2 \cdots p_n}$$

Demostració.

Sigui p_n i $k < n$. Considerem els k primers nombres primers p_1, p_2, ..., p_k i construïm els p_k nombres següents:

- $M_1 = p_1 \cdot p_2 \cdots p_{k-1} \cdot 1 - 1$
- $M_2 = p_1 \cdot p_2 \cdots p_{k-1} \cdot 2 - 1$
- $M_3 = p_1 \cdot p_2 \cdots p_{k-1} \cdot 3 - 1$
- $\vdots$
- $M_{p_k} = p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k - 1$

Constatem els següents fets:

1. Cap de les expressions M_1, M_2, ..., M_{p_k} és divisible per cap dels primers p_1, p_2, ..., p_{k-1} atès que cap p_l divideix a 1 en ser $p_l > 1$ ($l = 1 \div k - 1$)

[13] Publicat el 1907 als *Archiv der Mathematik und Physik*, núm. 3, sota el títol *"Über eine bekannte Eigenschaft der Zahl 30 und ihre Verallgemeinerung"* (sobre una propietat important del número 30 i la seva generalització)

2. Com a màxim, una d'aquestes expressions és divisible per p_k. Si ho fossin dues, per exemple

$$\left.\begin{array}{l} p_k \mid p_1 \cdots p_{k-1} \cdot x - 1 \\ p_k \mid p_1 \cdots p_{k-1} \cdot y - 1 \end{array}\right\} \quad \Rightarrow \quad p_k \mid p_1 \cdots p_{k-1} \cdot (x - y)$$

Utilitzant el Lema d'Euclides (2.2.3)

$$p_k \nmid p_1 \cdot p_2 \cdots p_{k-1} \quad \Rightarrow \quad p_k \mid (x - y)$$

Però x i y són algun dels nombres 1, 2, ..., p_k i la seva màxima diferència és $p_k - 1$ inferior a p_k i , per tant, $p_k \nmid (x - y)$.

3. Anàlogament podem demostrar que, com a màxim, una de les M_l ($l = 1 \div p_k$) és divisible per p_{k+1}, una com a màxim és divisible per p_{k+2}, una com a màxim per p_{k+3}, ..., una com a màxim per p_n.

Ara bé, si hi ha menys nombres p_k, p_{k+1}, ..., p_n que expressions M_1, M_2, ..., M_{p_k}, és a dir, si

$$n - k + 1 \ < \ p_k$$

aleshores, com a mínim, una de les M_l no és divisible per cap dels p_k, p_{k+1}, ..., p_n. Designem per M_h aquesta expressió particular. Com que, per construcció, M_h no és divisible per p_1, p_2, ..., p_{k-1} ajuntant els dos fets obtenim que M_h no és divisible per cap dels nombres $p_1, p_2, ...p_n$.

Ara continuem com en la demostració d'Euclides. O bé M_h és primer o bé és compost. Si és compost, aleshores existeix un p primer tal que $M_h = p \cdot d$ i $p > p_n$. El següent primer després de p_n és p_{n+1}. De manera que $p_{n+1} \leq p$. Per altra banda, $p \mid M_h \quad \Rightarrow \quad p \leq M_h$. L'expressió més gran de les M_h és M_{p_k} de manera que

$$p_{n+1} \leq M_{p_k} = p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k - 1 < p_1 \cdot p_2 \cdots p_k$$

Resumint els nostres resultants, hem arribat al fet que

$$p_{n+1} < p_1 \cdot p_2 \cdots p_k \qquad \text{sempre que } n - k + 1 < p_k.$$

Exemplifiquem numèricament el resultat al qual hem arribat. Prenem $n = 5$ i $k = 2$. Els 5 primers nombres primers són $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ i $p_5 = 11$. El grup $p_k, ..., p_n$ és format per 3, 5, 7 i 11. És a dir, $n - k + 1 = 5 - 2 + 1 = 4$ elements. Però 4 no és més petit que $p_k = 3$. Per tant, no es complirà la condició. En efecte, $p_6 = 13 \ > \ 2 \cdot 3 = p_1 \cdot p_2$. Però si fem $k = 3$, aleshores $p_k = 5$ i $n - k + 1 = 5 - 3 + 1 = 3 < 5 = p_k$. En aquest cas es compleix. $p_6 = 13 < 2 \cdot 3 \cdot 5 = p_1 \cdot p_2 \cdot p_3$. Ara, evidentment, si $k > 3$ la desigualtat es continua mantenint i considerem que, per a $n = 5$, el k òptim és $k = 3$.

El següent pas consisteix a demostrar que si prenem el k òptim per a cada n complint $n - k + 1 < p_k$, aleshores

$$p_1 \cdot p_2 \cdots p_k < p_{k+1} \cdots p_n \tag{3.27}$$

Comprovem fàcilment que la condició (3.27) es compleix per a $n = 5$ i $k = 3$:

$$p_1 \cdot p_2 \cdot p_3 \;=\; 2 \cdot 3 \cdot 5 \;<\; 7 \cdot 11 = p_4 \cdot p_5$$

Per demostrar que (3.27) continua essent vàlida en augmentar k, estudiem com varia aquest valor òptim de k en funció de n. Si canviem $n = 5$ per $n = 6$ introduïm un nou primer $p_6 = 13$. Però k continua valent 3 atès que

$$n - k + 1 = 6 - 3 + 1 = 4 < 5 = p_3 \quad \text{i} \quad p_1 \cdot p_2 \cdot p_3 = 2 \cdot 3 \cdot 5 < 7 \cdot 11 \cdot 13 = p_4 \cdot p_5 \cdot p_6$$

Quan canviem $n = 6$ per $n = 7$ la situació és diferent. Ara la condició $n - k + 1 < p_k$ no és compleix si $k = 3$. En efecte,

$$7 - 3 + 1 = 5 \geq 5 = p_3$$

Per tant, en passar de $n = 6$ a $n = 7$, el valor de k òptim canvia de 3 a 4.

$$7 - 4 + 1 = 4 < 7 = p_4 \qquad \text{i} \qquad 2 \cdot 3 \cdot 5 \cdot 7 \;<\; 11 \cdot 13 \cdot 17$$

Com que s'ha fet un salt de 2 xifres, de $p_3 = 5$ a $p_4 = 7$, la desigualtat es mantindrà per a 2 valors més de n, $n = 8$ i $n = 9$. Quan $n = 10$, tornem a tenir la mateixa situació que en passar de $n = 6$ a $n = 7$. En efecte, per $n = 10$, $k = 4$ no serveix atès que

$$n - k + 1 = 10 - 4 + 1 = 7 \geq p_4 = 7$$

Per tant, ens cal prendre $k = 5$ i $p_5 = 11$. Ara es compleix que

$$n - k + 1 = 10 - 5 + 1 = 6 < p_5 = 11$$

Però com que ara hem fet un salt de 4 unitats per passar de $p_4 = 7$ a $p_5 = 11$, la desigualtat es mantindrà per a 4 valors més. És a dir, fins a $n = 14$. La taula 3.7 mostra en negreta quin és el valor de p_k que cal prendre a mesura que augmentem el valor de n.

Cada vegada que canviem n per $n + 1$ p_k augmenta com a mínim 2 unitats, permetent que el nou valor de k es mantingui, com a mínim, els 3 següents valors de n. Si passa que el valor de p_k augmenta més de 2 unitats, el valor de k es mantindrà per a més valors de n.

Ara veiem com es manté la desigualtat

$$p_1 \cdots p_k < p_{k+1} \cdots p_n$$

Si $n = 5$ és cert que

$$2 \cdot 3 \cdot 5 < 7 \cdot 11 \tag{3.28}$$

Si $n = 6$, $k = 3$ i també és cert que $2 \cdot 3 \cdot 5 < 7 \cdot 11 \cdot 13$ atès que el segon membre de (3.28) ha augmentat. Quan $n = 7$ passem $p_4 = 7$ al primer membre i ara cal veure

$$2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 13 \cdot 17$$

Podríem realitzar efectivament el càlcul però no ens cal. Observem que de (3.28),

$$2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 11 \quad \Rightarrow \quad 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7 < 7 \cdot 11 \cdot 13 \cdot 17 \quad \Rightarrow \quad 2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 13 \cdot 17 \tag{3.29}$$

Taula 3.7: Valor òptim de k en funció de n

n	p_1,...,p_n	k
5	2, 3, **5**, 7, 11	3
6	2, 3, **5**, 7, 11, 13	3
7	2, 3, 5, **7**, 11, 13, 17	4
8	2, 3, 5, **7**, 11, 13, 17, 19	4
9	2, 3, 5, **7**, 11, 13, 17, 19, 23	4
10	2, 3, 5, 7, **11**, 13, 17, 19, 23, 29	5
11	2, 3, 5, 7, **11**, 13, 17, 19, 23, 29, 31	5
12	2, 3, 5, 7, **11**, 13, 17, 19, 23, 29, 31, 37	5
13	2, 3, 5, 7, **11**, 13, 17, 19, 23, 29, 31, 37, 41	5
14	2, 3, 5, 7, **11**, 13, 17, 19, 23, 29, 31, 37, 41, 43	5
15	2, 3, 5, 7, 11, **13**, 17, 19, 23, 29, 31, 37, 41, 43, 47	6

La desigualtat es mantindrà per als valors consecutius de $n = 8$ i $n = 9$ en augmentar el 2n membre de (3.29).

$$n = 8 : \qquad 2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 13 \cdot 17 \cdot 19$$
$$n = 9 : \qquad 2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$

Quan $n = 10$, caldria comprovar que

$$2 \cdot 3 \cdot 5 \cdot 7 < 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$

fet que és clarament evident.

Per tant, la desigualtat $p_1 \cdot p_2 \cdots p_k \ < \ p_{k+1} \cdots p_n$ es manté per a $n = 5, 6...$ Multipliquem els 2 membres d'aquesta darrera expressió per $p_1 \cdots p_k$

$$(p_1 \cdots p_k)^2 \ < \ p_1 \cdots p_n \quad \Rightarrow \quad p_1 \cdots p_k \ < \ \sqrt{p_1 \cdots p_n}$$

Però segons (3.27), $p_{n+1} \ < \ p_1 \cdot p_k$. Per tant, finalment, arribem al resultat desitjat

$$p_{n+1} \ < \ \sqrt{p_1 \cdots p_n}$$

□

Aquesta demostració la devem al matemàtic H.Bonse. De fet, Bonse millorà el seu resultat i demostrà, per mètodes similars que, l'$n + 1$-èsim primer,

$$p_{n+1} \ < \ \sqrt[3]{p_1 \cdots p_n}$$

Més endavant, Hans Rademacher (1892-1969) i Otto Toeplitz (1881-1940) milloraren la desigualtat de Bonse arribant a l'expressió

$$p_{n+1} \ < \ \sqrt[7]{p_1 \cdots p_n} \qquad \text{si } n \geq 114$$

3.4 $\pi(x)$ i els zeros de $\zeta(s)$

El resultat més important del treball presentat per Riemann el 1859 és una fórmula explícita que dóna de manera exacta la quantitat de nombres primers que hi ha per sota de x. És a dir, troba una expressió per a la funció $\pi(x)$.

Durant el procés per trobar aquesta expressió, Riemann ha de suposar que els zeros de la funció ζ compleixen una certa estructura. És el que es coneix com la *hipòtesi de Riemann* (veure 3.2). Suposada certa aquesta hipòtesi, podem calcular de manera exacta el valor de $\pi(x)$.

En aquesta secció utilitzarem el programa *Mathematica*© per comprovar gràficament i numèricament que l'expressió donada per Riemann sembla ser correcta. El dia que es demostri la hipòtesi de Riemann[14], podrem assegurar que tal expressió és correcta.

Sembla que els nombres primers van apareixent de manera aleatòria. La funció $\pi(x)$ és una funció esgraonada que s'incrementa una unitat cada vegada que troba un nombre primer. Però observada a gran escala, s'hi presenta una certa regularitat (veure figures 3.3 i 3.4). Intentarem il·lustrar com, a partir dels zeros de la funció zeta, trobem una funció que s'aproxima al comportament irregular de $\pi(x)$.

En el seu treball, Riemann proposa una nova funció per comptar primers.

$$\mathrm{Ri}(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}) \tag{3.30}$$

on $\mu(n)$ és la funció de Möbius (3.7), i $\mathrm{Li}(x)$ és el logaritme integral introduït per Gauss (3.1). *Mathematica*© té definida directament la funció $\mathrm{Ri}(x)$. Així, podem comprovar com de bona és l'aproximació donada per Riemann.

```
In[1]:=  N[RiemannR[1000]]
Out[1]:=  168.359
```

Sabem que $\pi(1000) = 168$. Per tant, a grans trets, $\mathrm{Ri}(x)$ és una bona aproximació de $\pi(x)$. De fet, és la millor quan la comparem amb les de Legendre i Gauss (veure figura 3.30 i comparar-la amb 3.5 i 3.6[15]).

Tanmateix, $\mathrm{Ri}(x)$ no segueix detalladament el comportament de $\pi(x)$. És a dir, no fa els salts discontinus que presenta $\pi(x)$, quan x és primer, i tampoc es manté constant quan $\pi(x)$ ho fa. Malgrat tot, si afegim a la funció $\mathrm{Ri}(x)$ un terme corrector que conté els zeros de la funció zeta de Riemann, s'esdevé un fet sorprenent: la nova funció intenta imitar els salts i les irregularitats de de $\pi(x)$. Quan x és un primer, aquesta nova funció creix aproximadament 1 a prop de x. És com si, aquesta funció pogués reconèixer quan x és un nombre primer. I quan

[14] Actualment encara està per demostrar, tot i que es tenen forts indicis numèrics de que la hipòtesi és certa. Malgrat aquests indicis, la comunitat matemàtica internacional espera encara una demostració rigorosa de la hipòtesi de Riemann. El *Clay Mathematical Institute* ha inclòs la hipòtesi de Riemann en la llista dels set problemes del mil·leni, amb una dotació d'1 000 000 $ per a la persona – o equip de persones – que demostri la hipòtesi. Tanmateix, el principal premi que rebrà qui demostri la HR serà el reconeixement matemàic mundial i immortal.

[15] Aquesta figura l'hem fet amb la comanda de *Mathematica*©

```
Plot[{ PrimePi[x], RiemannR[x]}, {x, 1, 300}]
```

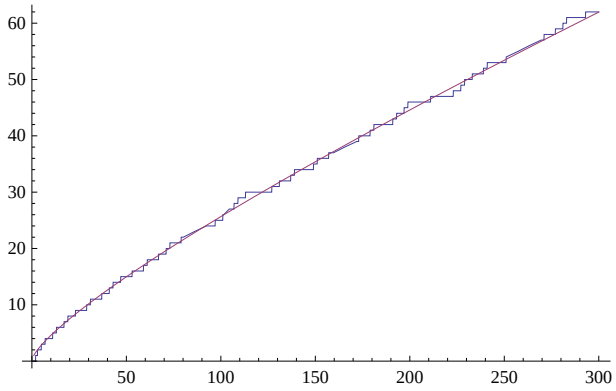


Figura 3.10: Funcions $\pi(x)$ i $\mathrm{Ri}(x)$ (Riemann), $x \in [1, 300]$.

tenim un forat entre primers , aquesta nova funció tendeix a mantenir-se constant, imitant de nou el comportament de $\pi(x)$. Podem pensar que els zeros de la funció zeta determinen quins nombres naturals són primers i quins no. Podem mostrar aquesta comportament amb l'ajut de *Mathematica*© . L'expressió que troba Riemann per al càlcul de $\pi(x)$ és:

$$\pi(x) = \mathrm{Ri}(x) + \sum_{n=1}^{\infty} \frac{\mu(n)}{n} f(x^{1/n}) \tag{3.31}$$

on

$$f(x) = -2\Re\left(\sum_{k=1}^{\infty} \mathrm{Ei}\left(\rho_k \ln(x)\right)\right) + \int_x^{\infty} \frac{dt}{t(t^2-1)\ln t} - \ln 2 \tag{3.32}$$

on ρ_k és el k-èsim zero no trivial de la funció $\zeta(s)$ i $\mathrm{Ei}(z)$ és la funció generalitzada del logaritme integral

$$\mathrm{Ei}(z) = \int_{-z}^{\infty} \frac{e^{-t}}{t}\, dt \tag{3.33}$$

Com que totes les funcions que hem comentat estan definides a *Mathematica*© , no ens hem de preocupar com calcular-les. El que hem de dissenyar és una estratègia que ens permeti poder veure com els zeros de la funció zeta prediuen la distribució dels nombres primers. El punt clau és entendre que el sumatori (3.31) és finit atès que el nombre primer més petit és el 2. És a dir, només cal sumar els termes que compleixen

$$2 < x^{1/n} \quad \Leftrightarrow \quad \frac{\ln 2}{\ln x} < \frac{1}{n} \quad \Leftrightarrow \quad n < \frac{\ln 2}{\ln x} \tag{3.34}$$

Una altra qüestió important és decidir quants zeros no trivials, ρ_k sumem. És clar que el sumatori de (3.32) té infinits termes[16]. És sabut que l'aportació més important la fan els primers zeros. Per no alentir massa l'execució, considerarem com a màxim els 200 primers zeros no trivials que, donada la seva simetria respecte l'eix real, són , de fet, 400 zeros.

Finalment, prescindirem dels terme integral i del $\ln 2$ de (3.32) per fer l'execució més ràpida. La supressió d'aquest dos termes no afecten significativament la imatge final que volem buscar per visualitzar la importància dels zeros no trivials de $\zeta(s)$.

[16] G.H. Hardy va demostrar (1914) que els valors no trivials de $\zeta(s) = 0$ són infinits.

Les comandes específiques que necessitem de *Mathematica*© són les següents:

1. `RiemannR[x]` → és la funció $\mathrm{Ri}(x)$ abans comentada (3.10).
2. `Sum[f[k], {k,1,n} ]` → és la comanda que correspon al sumatori de la funció $f(k)$ pels valors de k compresos entre 1 i n.
3. `MoebiusMu[n]` → és la funció de Möbius $\mu(n)$.
4. `LogIntegral[x]` → és la funció logaritme integral, $\mathrm{Li}(x) = \displaystyle\int_0^x \frac{dt}{\ln t}$
5. `ExpIntegralEi[x]` → és la funció $\mathrm{Ei}(x)$ abans comentada (3.33).
6. `ZetaZero[k]` → és el k-èsim zero no trivial, amb la part imaginària positiva, de la funció $\zeta(s)$.
7. `Log[x]` → és la funció logaritme natural, $\ln x$
8. `Plot[{f[x], g[x]}, {x, x_0, x_1}]` → és la comanda que permet dibuixar simultàniament $f(x)$ i $g(x)$ a l'interval $[x_0, x_1]$.
9. `PrimePi[x]` → és la funció $\pi(x)$.

Farem, primerament, una comprovació numèrica de l'aproximació de la quantitat de nombres primers que hi ha per sota de x amb la funció proposada per Riemann. És a dir, definirem amb *Mathematica*© la funció correctora $f(x)$ de (3.32) amb tots els termes. Considerem, inicialment, els 100 primers zeros no trivials de la funció $\zeta(s)$. Atès que els zeros ρ_k apareixen simètricament respecte l'eix real, multipliquem per 2 el terme de les ρ_k.

```
In[1]:=  f[x_]:=-2Re[Sum[ExpIntegralEi[ZetaZero[k] Log[x]], {k, 1, 100}]]+
          Integrate[1/t/(t^2-1)/Log[t], {t, x, Infinity }]-Log[2]
```

Després definim la funció `pi[x]` que és la funció que aproxima $\pi(x)$. Recordem que, segons (3.34), només ens cal sumar els valors $x = 1 \div (\ln x)/(\ln 2)$.

```
In[2]:=  pi[x_]:= RiemannR[x] +
          Sum[MoebiusMu[n] f[x^ (1/n)]/n, {n, 1, Log[x]/Log[2]}]
```

Aquesta funció, prenent inicialment 100 zeros, s'aproxima al valor de x molt millor que totes les altres aproximacios fins aleshores proposades. En efecte,

```
In[3]:=  PrimePi[10^ 6]
Out[3]:=  78498
In[4]:=  pi[10^ 6]
Out[4]:=  78502.4
```

A la taula 3.8 es poden veure els valors de $\pi(x)$ quan $x = 10^n$ fins a $n = 17$ comparats amb les aproximacions del Teorema del Nombre Primer, *TNP* $(x \ln x)$, Gauss $(\mathrm{Li}(x))$ i Riemann $(\mathrm{Ri}(x))$. Podem comprovar com l'error provocat per l'aproximació de Riemann és molt inferior als provocats per les altres aproximacions. També és interessant observar que tant les aproximacions donades pel *TNP* i la de Gauss sempre superen el valor de $\pi(x)$ mentre

Taula 3.8: Valors de $\pi(x)$ per a $x = 10^n$, $n = 3 \div 17$, comparats amb $x \ln x$, $\mathrm{Li}(x)$ i $\mathrm{Ri}(x)$.

n	$\pi(x)$	$\pi(x) - x/\ln x$	$\pi(x) - \mathrm{Li}(x)$	$\pi(x) - \mathrm{Ri}(x)$
3	168	23	9	0
4	1229	143	16	-2
5	9592	906	37	-5
6	78498	6116	129	4
7	664579	44158	338	88
8	5761455	332774	753	97
9	50847534	2592592	1700	-79
10	455052511	20758029	3103	-1828
11	4118054813	169923159	11587	-2318
12	37607912018	1416705193	38262	-1476
13	346065536839	11992858452	108970	-5733
14	3204941750802	102838308636	314889	-19200
15	29844570422669	891604962452	1052617	73218
16	279238341033925	7804289844393	3214632	327052
17	2623557157654233	68883734693928	7956590	-598255

que la de Riemann va alternant les seves prediccions. El rècord actual que hem pogut trobar correspon al valor $x = 10^{23}$ i els valors són:

$$\begin{aligned} \pi(x) &= 1\ 925\ 320\ 391\ 606\ 818\ 006\ 727 \\ \pi(x) - x/\ln x &= 37\ 083\ 513\ 766\ 592\ 905\ 216 \\ \pi(x) - \mathrm{Li}(x) &= 7\ 236\ 222\ 976 \\ \pi(x) - \mathrm{Ri}(x) &= 1\ 019\ 262\ 049 \end{aligned}$$

Ara voldríem mostrar gràficament com els zeros no trivials de la funció $\zeta(s)$ de Riemann aproximen de manera sorprenent $\pi(x)$. El primer que fem és redefinir la funció correctora $f(x)$. Només ens cal prendre l'aportació dels zeros ρ_k per accelerar l'execució. També ens cal redefinir de nou la funció `pi[x]`.

```
In[5]:=  f[x_]:=-2Re[Sum[ExpIntegralEi[ZetaZero[k] Log[x]], {k, 1, 100}]]
In[6]:=  pi[x_]:= RiemannR[x] +
          Sum[MoebiusMu[n] f[x^ (1/n)]/n, {n, 1, Log[x]/Log[2]}]
```

Podem demanar ara a *Mathematica*© que ens dibuixi les dues funcions a l'interval [1, 100]. El resultat es pot veure a la figura 3.11

```
In[7]:=  Plot[{ PrimePi[x], pi[x]}, {x, 1, 100}]
Out[7]:=  - graphics -
```

Tal com hem definit les funcions, podem veure com, a mesura que prenem més zeros ρ_k, la funció `pi[x]` s'aproxima més i més a la funció $\pi(x)$. Considerem l'interval [10,30] on la funció $\pi(x)$ presenta fins a 6 salts, en $x = 11$, 13, 17, 19, 23 i 29. A la figura 3.12 podem veure la funció $\pi(x)$ aproximada per la funció $\mathrm{Ri}(x)$ sense tenir en compte cap terme corrector. A la figura 3.13 podem veure la primera aproximació de $\pi(x)$ considerant la primera parella de zeros no trivials de $\zeta(s)$,

$$\rho_1 = 0.5 + 14.134725141734693790457251983 6i \qquad \text{i} \qquad \rho_{-1} = \bar{\rho}_1$$

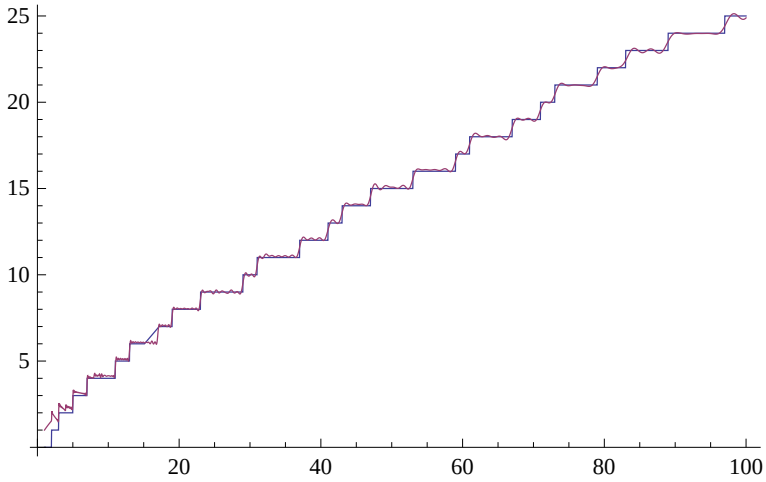


Figura 3.11: La funció $\pi(x)$ i com els 100 primers zeros ρ_k de $\zeta(s)$ l'aproximen.

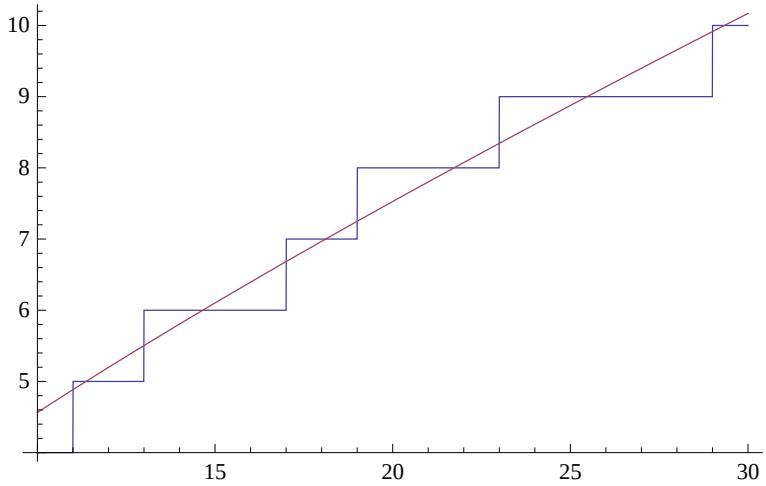


Figura 3.12: Les funcions $\pi(x)$ i $\mathrm{Ri}(x)$ sense cap terme corrector.

A les figures 3.14, 3.15 i 3.16 podem veure les successives aproximacions prenent 10, 50 i 100 zeros no trivials respectivament. El resultat és espectacular.

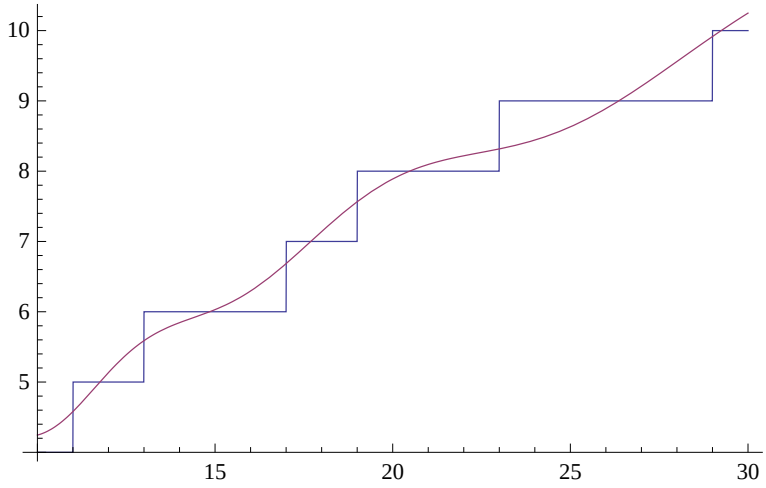


Figura 3.13: Les funcions $\pi(x)$ i `pi[x]`, $x \in [10, 30]$, considerant ρ_1 i $\bar{\rho}_{-1}$.

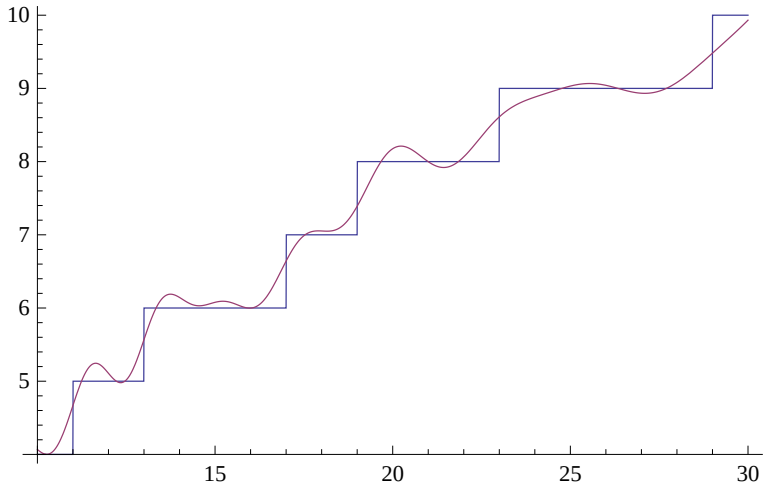


Figura 3.14: Les funcions $\pi(x)$ i `pi[x]`, $x \in [10, 30]$, considerant ρ_k i $\bar{\rho}_{-k}$, $k = 1 \div 10$.

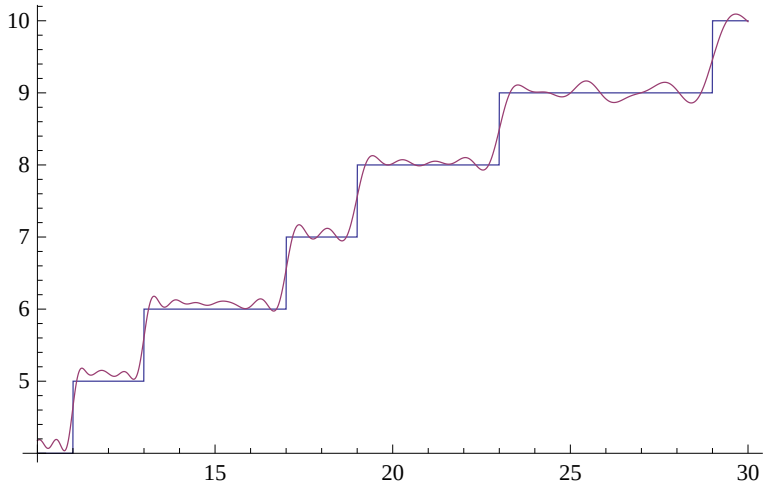


Figura 3.15: Les funcions $\pi(x)$ i `pi[x]`, $x \in [10, 30]$, considerant ρ_k i $\bar{\rho}_{-k}$, $k = 1 \div 50$.

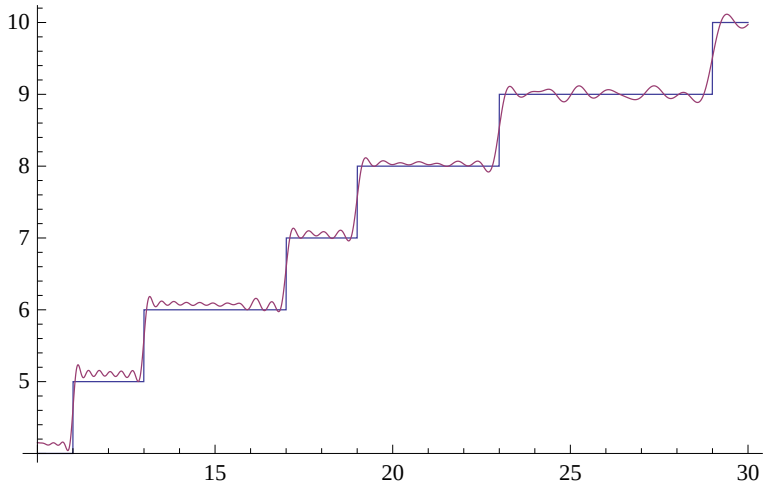


Figura 3.16: Les funcions $\pi(x)$ i `pi[x]`, $x \in [10, 30]$, considerant ρ_k i $\bar{\rho}_{-k}$, $k = 1 \div 100$.

Capítol 4

Conclusions

Per poder escriure aquestes conclusions he fet un llarg camí. El vaig començar el mes de maig de 2011.

Aleshores no sabia gaire coses sobre el tema. Sabia el que havia après a la Xina abans de venir a Catalunya. Allà treballem molt les matemàtiques cada dia, sobretot àlgebra i geometria. Els nombres primers i les seves propietats les vaig aprendre quan fèiem àlgebra. Però només em van explicar les propietats més elementals i ens van fer resoldre molts problemes.

En canvi, fent el treball de recerca he après moltes coses dels nombres primers que no sabia. També he après i he entès algunes de les demostracions més importants relacionades als nombres primers. M'ha sorprès, d'una banda, la seva irregularitat. En el procés del treball de recerca em vaig adonar de la dificultat de cercar el següent nombre primer un cop en sabem un. També vaig aprendre que la pregunta inicial que em va formular el meu tutor – quants nombres primers hi ha per sota d'un nombre donat? – té una resposta difícil i que encara avui no s'ha entès completament. Però per altra banda, els nombres primers presenten una regularitat sorprenent. Podem aproximar el seu comportament per funcions que ens són conegudes. Això m'ha sorprès molt perquè a l'inici del treball em pensava que era impossible descobrir una funció que imités tan bé el comportament dels nombres primers. Però encara hi ha molts problemes amb els nombres primers que no s'han resolt.

En aquest treball he arribat a estudiar dos tipus de resultats sobre la pregunta inicial que em feia. Primer, he trobat fites mínimes i màximes de la funció $\pi(x)$ que compta primers. Aquests resultats, que ara poden semblar poc precisos, van costar molt de demostrar a finals del segle XIX. Molts matemàtics s'hi van barallar i no van saber trobar-ne la resposta. Per a mi, poder entendre alguna d'aquestes fitacions ha estat molt important. Els altres resultats donen fites per a trobar nombres primers. Tot i que semblaven dues preguntes inicialment diferents, vaig poder entendre que, finalment, la resposta és comuna i que respondre quants nombres primers hi ha per sota d'un donat és equivalent a respondre quan trobarem el proper nombre primer.

El que m'ha sorprès més del treball ha estat com un valors molt concrets, els zeros de la funció zeta de Riemann – $\zeta(s)$ –, poden conèixer quins nombres naturals són primers i quins no. Les imatges que vaig aconseguir amb l'ajut de *Mathematica*© em van sorprendre i em van fer entendre moltes coses que fins al moment no havia entès. També em van fer comprendre que encara no entenem perfectament quin és el comportament dels nombres primers.

Si les matemàtiques que he hagut d'estudiar per fer el treball han estat difícils, encara ho ha estat més redactar el treball. Puc dir que m'he passat tantes, o més hores, redactant el treball que entenent el que he escrit. En aquest punt, el meu tutor, en Berenguer, ha estat d'una gran ajuda. M'ha fet treballar molt i hem passat moltes hores junts aprenent. Però jo sé que ho feia pel meu bé. I li vull fer saber que li estic molt agraïda. No he trobat mai cap professor – ni aquí ni a la Xina – que es dediqui tant als alumnes. Ell s'estima molt les matemàtiques i en transmet el seu amor als alumnes. És molt bon professor i molt bona persona.

En el procés d'aquest treball també he crescut com a persona. He après a ser pacient, a tornar a mirar una demostració quan no l'entenia. En definitiva, he après molt de tot i no em sap greu haver treballat durant tant temps per fer aquest treball.

Bibliografia

[1] Apostol, Tom M. *"Introduccíon a la Teoría analítica de números"*. Editorial Reverté. Barcelona, 1980.

[2] Blachman, Nancy. *"Mathematica. Un enfoque práctico"*. Ed. Ariel. Barcelona, 1993.

[3] Cairns, Grant. *"Els nombres primers poden tenir més protagonisme a secundària?"*. Butlletí de la Societat Catalana de Matemàtiques. Institut d'Estudis Catalans. Vol.20, núm.2, pp.75-89. Barcelona, 2006.

[4] Dunham, William. *"Euler. El maestro de todos los matemáticos"*. Editorial Nivola. Madrid, 2000.

[5] Edwards, H.M. *"Riemann's Zeta Function"*. Dover Edition. Mineola, N.Y. 2001

[6] Havil, Julian. *"Gamma. Exploring Euler's constant"*. Princeton University Press. New Jersey, 2003.

[7] Lang, Serge. *"El placer estético de las matemáticas"*. Alianza Editorial. Madrid, 1992.

[8] Quer, Jordi. *"La funció ζ de Riemann"*. Butlletí de la Societat Catalana de Matemàtiques. Institut d'Estudis Catalans. Vol.22, núm.2, pp.197-228. Barcelona, 2007.

[9] Rademacher, Hans i Toeplitz, Otto. *"Números y figuras"*. Alianza Editorial. Madrid, 1970.

[10] Pascual, Griselda. *"Sessions de preparació per a l'Olimpíada Matemàtica. Artmètica"*. Societat Catalana de Matemàtiques. Institut d'Estudis Catalans. Barcelona, 2001.

[11] Travesa, Artur. *"Aritmètica"*. Edicions Universitat de Barcelona. Barcelona, 1998.

[12] Wolfram, Stephen. *"Mathematica. A System for Doing Mathematics by Computer"*. Addison-Weseley Publishing Co., Redwood City, California, 1991.