UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Superior d'Enginyeries Industrial,
Aeroespacial i Audiovisual de Terrassa

TREBALL DE FI D' ESTUDIS

Estudi de la hipòtesi de Riemann: nombres primers i aplicacions

Document:
Memòria

Autor/Autora:
Ivet Sala Samarra

Director/Directora - Codirector/Codirectora:
Gisela Pujol

Titulació:
Grau en Enginyeria en Tecnologies Industrials

Convocatòria:
Primavera de 2022

Resum

En aquest treball s'estudia la hipòtesi de Riemann, un problema matemàtic relacionat amb la distribució dels nombres primers i que no ha estat resolt des que el 1859, Bernhard Riemann, un matemàtic alemany, l'anuncià en una memòria escrita de menys de 10 pàgines. Aquesta hipòtesi forma part del selecte grup dels Problemes del mil·lenni, i s'ofereixen 1.000.000 de dòlars a qui pugui verificar-la o negar-la.

En aquest treball es pretén arribar a comprendre com fou plantejada la hipòtesi i en quines circumstàncies, per això s'estudien treballs d'altres matemàtics com ara Gauss o Euler, ja que les seves publicacions contribuïren a què Riemann finalment formulés la famosa hipòtesi, i foren molt importants, ja que sense les aportacions de diversos matemàtics a aquesta ciència, probablement no s'hauria pogut formular la hipòtesi.

Moltíssims matemàtics al llarg de la història han intentat trobar una fórmula *màgica* que generi tots els nombres primers, o vàries fórmules que entre elles els cobreixin tots, però donat que això no fou possible, Gauss començà estudiant la distribució dels nombres primers, doncs no aconseguia trobar-hi un sentit complet, i a partir d'aquí definí una funció que comptaria els nombres primers, i la representació gràfica d'aquesta seria com una escala infinita.

A partir d'aquí, molts matemàtics intentaren trobar una funció que seguís per complet el comportament de la funció $\pi(x)$ que definí Gauss, i a partir d'estudis diversos d'altres matemàtics, hi acabaren intervenint els nombres complexos. A partir d'aquí s'obrí un nou camí que il·luminaria esperances perdudes als matemàtics que ja havien perdut l'esperança respecte la distribució dels nombres primers.

Les relacions que Riemann feu amb els matemàtics que intervindran en aquesta història foren clau, doncs tot plegat resulta irònicament com una recepta d'ingredients aparentment independents que entrellaçats donen lloc a un plat deliciós

Per a poder realitzar aquest treball s'ha seguit l'article de Don Zagier, The first 50 million prime numbers. També s'ha seguit el llibre de Marcus Du Sautoy, La música de los números primos, títol que sorgeix gràcies a la relació d'aquesta hipòtesi amb la sèrie harmònica, i altres articles que també tracten la hipòtesi de Riemann.

S'ha emprat l'eina Maple per a poder representar gràficament les funcions que hi intervenen i poder realitzar càlculs complicats.

Abstract

This paper examines Riemann's hypothesis, a mathematical problem related to the distribution of prime numbers that has not been solved since 1859, when Bernhard Riemann, a German mathematician, announced it in a written memoir of less than 10 pages. This hypothesis is part of the select group of the Millennium problems, and offers 1,000,000 dollars to those who can verify or deny it.

The aim of this paper is to understand how the hypothesis was posed and under what circumstances, so studies of other mathematicians such as Gauss and Euler are studied, as their publications contributed to Riemann finally formulating the famous hypothesis, and they were very important, as without the contributions of various mathematicians to this science, the hypothesis probably would not have been possible.

A great lot of mathematicians all over the history tried to find a magical equation wich generate all the prime numbers, or at least a group of equations, but unfourtunately this has never seemed possible so Gauss began studying the distribution of the first primes, as he could not find a complete meaning, and from there he defined a function that would count the first primes, and the graphical representation of this would be like an infinite scale.

From there, many mathematicians tried to find a function that completely followed the behavior of the π(x), the function defined by Gauss, and based on various studies by other mathematicians, complex names came into play. From here, things get trickier, and this is where the true hope of mathematicians comes in.

Riemann's relationship with the mathematicians who will be involved in this story was very important, as it all ironically turns out to be a recipe for seemingly independent ingredients that, intertwined, result in a delicious creation.

In order to do this work, we followed Don Zagier's article, *The first 50 million prime numbers*. Marcus Du Sautoy's book, *The Music of Prime Numbers*, and other articles dealing with Riemann's hypothesis have also been followed.

The Maple tool has been used to graphically represent the functions involved and to perform complicated calculations

«És molt probable que tots els zeros no trivials de la funció tingan part real igual a 1/2»

Georg Friedrich Bernhard Riemann (1826-1866)

«Si m'adormís durant 500 anys, el primer que faria al despertar
seria preguntar qui ha resolt la hipòtesi de Riemann»

David Hilbert (1862-1943)

«Els encants d'aquesta ciència sublim, les matemàtiques, només
són revelats a aquells que tenen el valor d'aprofunditzar en ella»

Carl Friedrich Gauss (1777-1855)

Índex

Índex de taules

Títol i número de totes les taules per ordre d'aparició en el text.

Índex de figures

Títol i número de tots els gràfics per ordre d'aparició en el text.

Llista d'abreviatures/Glossari

En aquest apartat es comentaran conceptes i glossari que apareixeran al llarg de la memòria.

Funció analítica: és aquella funció que pot expressar-se en forma de sèrie de potències convergent.

Sèrie convergent: una suma de termes successius que tendeix a un nombre concret, és a dir, existeix un límit.

Sèrie divergent: una suma de successions, les sumes parcials de la qual no tendeixen a cap nombre en concret, és a dir, no existeix cap límit i és infinita.

Continuació analítica: la continuació analítica d'una funció és una tècnica que s'usa per a ampliar el domini d'aquesta. La continuació analítica serà una expressió diferent, de manera que es puguin estudiar els punts que no pertanyen al domini de la funció inicial, però amb el mateix comportament que tenia la primera funció en els punts del domini d'aquesta funció inicial.

Funció holomorfa: són funcions que es defineixen sobre un subconjunt del pla complex i són diferenciables en algun entorn d'un punt del seu domini. Una funció pot ser holomorfa exclusivament en algun punt del seu domini, o en tot el seu domini.

Funció meromorfa: són funcions que es defineixen sobre un subconjunt obert (és a dir, un subconjunt en què tots els entorns de cada element, pertanyen al subconjunt, de manera que cap element del subconjunt forma part de la frontera d'aquest) del pla complex i que són diferenciables en tot el pla complex excepte en alguns punts aïllats; els pols de la funció.

Funció entera: una funció entera és una funció que és holomorfa en tot el pla complex.

Pols: els pols d'una funció definida en el pla complex són aquells punts en què la funció tendeix a infinit, per exemple quan el denominador de la funció és nul.

Zero: el zero d'una funció definida en el pla complex es dona quan, essent ***z*** un nombre complex, es compleix que $f(z) = 0$.

Nombre complex: nombre compost per una part real i una part imaginària (acompanyada de la unitat imaginària $i = \sqrt{-1}$).

Teorema Fonamental de l'Aritmètica: afirma que tot nombre enter major que 1 o bé és un nombre primer o bé és un producte únic de nombres primers.

1. Introducció

1.1 Objecte

Mitjançant aquest projecte de recerca, tinc la intenció de poder comprendre la Hipòtesi que Bernhard Riemann va formular al llarg de la seva carrera i que ha causat una gran repercussió a tots els matemàtics que han tractat de demostrar que Riemann tenia raó o no.

És encara en l'actualitat un dels problemes no resolts i forma part del prestigiós recull anomenat "Problemes del milió".

La importància d'aquest problema recau en la comprensió de la distribució dels nombres primers, un camp en el qual els matemàtics encara no han aconseguit posar-hi ordre.

Així doncs, per poder comprendre amb profunditat aquest camp, durem a terme un estudi previ dels descobriments fets al llarg dels anys per alguns dels matemàtics més prestigiosos de la història ([1], [2] i [3]).

Per ultimar el contingut, estudiarem l'aplicació que han tingut els nombres primers al llarg de la història i encara ara.

Així doncs, l'objectiu principal d'aquest treball de fi de grau és la comprensió de la hipòtesi de Riemann, que conjectura com es distribueixen els zeros de la funció Z de Riemann en el pla complex. Com objectius secundaris tenim:

1) Fer l'estudi de l'art dels nombres primers: com es calculen, quants n'hi ha i com es distribueixen en la recta real.

- Estudiar el context històric dels estudis dels nombres primers, així com les circumstàncies respectives i els matemàtics involucrats.
- Pensar en la distribució dels nombres primers.

2) Entendre la funció Z de Riemann, que inclou estudiar la continuació analítica de funcions

- Comprendre el significat d'estendre una funció fora del seu domini real.
- Comprendre els zeros de la funció Z de Riemann
- Comprendre la relació entre la funció Z de Riemann i la sèrie harmònica.

3) Relacionar la funció Z amb els nombres primers

- Saber explicar i comprendre la importància que tindria demostrar la conjectura de Riemann en el camp dels nombres primers
- Comprendre com des la funció Pi (x) Riemann va arribar a la conjectura que duu el seu nom.

4) Estudiar les aplicacions dels nombres primers, centrant-se en la criptografia (generació de codis secrets).

- Comprendre la importància i l'impacte que han tingut els nombres primers en el desenvolupament de la criptografia i entendre en què estan implicats en el nostre dia a dia.
- Ser capaç de generar un programa de criptografia.

1.2 Abast

En aquest treball s'estudiarà:

- Els nombres primers al llarg de la història.
- Algunes de les equacions més famoses generadores d'alguns nombres primers i estudi personal de possibles equacions generadores de nombres primers.
- Projectes vigents en la recerca de nombres primers.
- La funció $\pi(x)$ i la freqüència dels nombres primers.
- La funció Z de Riemann: el desenvolupament teòric que es va seguir per arribar a plantejar la hipòtesi, l'explicació d'aquesta i la seva importància.
- Estudi i generació d'exemples numèrics de la generació de codis secrets.

S'empraran eines de càlcul com Excel, Matlab i Maple.

Aquest treball de recerca no depèn de cap normativa específica.

1.3 Requeriments

Es realitzarà un estudi de la teoria de nombres centrant-se en els nombres primers i la seva relació amb la hipòtesis de Riemann.

1. Es pretén ampliar els coneixements de matemàtiques adquirits durant els estudis universitaris, centrant-se en la teoria de nombres primers i les seves aplicacions.

2. Es farà una ressenya històrica de l'estudi dels nombres primers incloent alguns dels matemàtics més cèlebres com ara Gauss, Legendre, Euler, etc.

3. Es coneixerà el context històric de la hipòtesi de Riemann.

4. S'estudiarà i es comprendrà la Funció Z de Riemann, tot incloent-hi la definició, les propietats i la relació que té amb els nombres primers.

5. Es pretén saber quines teories han sorgit de l'estudi dels intents de la seva demostració, i es coneixeran les aproximacions que s'han fet fins ara.

6. S'hauran estudiat les aplicacions dels nombres primers, centrant-se en la generació de codis secrets i la importància d'aquests.

7. S'estudiarà l'aproximació de la funció π(x), que compta quants nombres primers hi ha menors que x, a partir de l'article de Don Zagier, *The first 50 million prime numbers*.

1.4 Justificació

La necessitat de realitzar aquest projecte sorgeix primerament de la curiositat que he sentit des de sempre pels nombres primers. Són la base de qualsevol nombre, en són els generadors, les partícules indivisibles; i partint de la creença que les matemàtiques són la ciència de l'ordre, els nombres primers semblen ser tot el contrari.

A més a més, els nombres primers tenen una gran aplicació en el desenvolupament de codis per a l'encriptació d'informació. Recentment, la meva tutora, de casualitat es va assabentar que la mateixa xarxa d'Internet de la universitat està encriptada amb el codi RSA, que es basa en la divisibilitat dels nombres i, precisament per això, els nombres primers en prenen un paper molt important en el desenvolupament d'aquest. Així doncs, tot i que la gran majoria ho ignori, els nombres primers estan presents en moltíssims instants del nostre dia a dia.

I bé, la hipòtesi que estudio al llarg d'aquesta memòria, és una de les hipòtesis més famoses en les matemàtiques, i porta més de 150 anys formulada sense resoldre.

Són molts els matemàtics, de talent excepcional per la ciència a què es dediquen, que s'han *barallat* amb la pregunta que Riemann feu, i que han perdut el *combat.* I jo desitjo entendre-la des que en vaig sentir parlar. De ser certa aquesta hipòtesi, per fi es podria posar ordre en el major *desordre* de les matemàtiques: els nombres primers. Seria, segons he pogut entendre, una meravella que Riemann tingués raó sobre les seves sospites.

2 Revisió de l'estat de la qüestió

Actualment la hipòtesi de Riemann segueix sense estar resolta. La meva intenció al començar aquest treball no era resoldre-la, ni acostar-m'hi, tan sols pretenia comprendre-la.

Milers de matemàtics arreu del món s'han barallat amb l'afirmació que feu Riemann, però ningú ha aconseguit afirmar-la o negar-la. Si bé, s'han trobat bilions d'arrels de la funció, totes d'acord amb l'afirmació de Riemann, i encara que molts matemàtics sospiten que el matemàtic Alemany tenia raó, no en tenen la prova irrefusable: la demostració.

En certes ocasions, alguns matemàtics han afirmat a ver-la resolt, han accedit fins i tot a oferir conferències i seminaris, però finalment, mai ha estat la demostració que es buscava.

El 1896, dos matemàtics, independentment l'un de l'altre, demostraren que en la singularitat que presentava la funció $zeta$ en $Re(z) = 1$, no hi havia cap zero.

El 1914, Godfrey Harold Hardy demostrà l'existència d'infinits zeros a la recta crítica, però això no significava que no poguessin existir infinits zeros no trivials en alguna altra recta de la franja crítica. Més tard, juntament amb Littlewood, van proporcionar estimacions de la densitat mitjana dels zeros no trivials damunt la recta crítica.

Encara ara, moltíssims matemàtics investiguen la qüestió, i molts afirmen que faria falta una idea nova per *sortir* del propi problema, tal com intuí Riemann en el seu dia.

3 Metodologia

Els passos que s'han seguit durant la realització d'aquest treball han estat els següents.

Primerament he llegit alguns capítols d'un llibre titulat La música de los números primos, de Marcus Du Sautoy. Aquest llibre m'inspirà a dedicar el meu treball a poder comprendre la hipòtesi de Riemann.

A continuació, la meva tutora em va facilitar un article d'un matemàtic que ha dedicat força temps de recerca als nombres primers i a la famosa Hipòtesi: Don Zagier, i l'article The first 50 million prime numbers. L'article s'ha seguit per a poder realitzar aquest treball, juntament amb altres articles basats en aquest.

Per a poder entendre la hipòtesi he hagut de reposar molt la teoria apresa. Cada vegada que pensava que l'havia entesa, me n'adonava que no del tot. D'aquesta manera, he hagut de llegir molts articles i visualitzar molts vídeos. He hagut d'intentar explicar la hipòtesi a molts companys per tal d'assegurar-me que l'havia entesa i poder respondre les preguntes d'aquests, les quals si no sabia respondre del tot, significava que havia de tornar a llegir els articles amb més deteniment.

S'ha emprat el programari Maple per a poder estudiar gràficament les funcions i poder realitzar càlculs difícils de realitzar amb la calculadora.

S'ha visualitzat vídeos explicatius, d'algunes classes universitàries que tractaven de la matèria corresponent, per a poder comprendre millor la matèria.

4 Desenvolupament de l'estudi de la funció Zeta de Riemann

Per a introduir la teoria estudiada per tal de comprendre la hipòtesi de Riemann, prèviament s'ha posat en context una sèrie de matemàtics que influïren en el desenvolupament d'aquesta, i s'explica les seves aportacions.

També s'expliquen *Els problemes del mil·lenni* i una breu explicació de per què la hipòtesi de Riemann en forma part.

4.1 Els problemes del mil·lenni

Els problemes del mil·lenni són un selecte grup de 7 problemes matemàtics i la resolució d'algun d'ells seria premiada amb 1.000.000 de dòlars per *Clay Mathematics Institute*, una fundació sense ànims de lucre en la qual participen les universitats de Cabridge i Massachusetts per tal de fomentar l'interès per les matemàtiques.

Aquest selecte grup està format pel següent llistat:

1. $P\ versus\ NP$
2. $La\ conjectura\ de\ Hodge$
3. $La\ conjectura\ de\ Poincaré$
4. $La\ hipòtesi\ de\ Riemann$
5. $L'existència\ de\ Yang\ Mills\ i\ del\ salt\ de\ massa$
6. $Les\ equacions\ de\ Navier-Stokes$
7. $La\ conjectura\ de\ Birch\ i\ Swinnerton-Dyer$

Actualment, només un d'aquests problemes ha estat resolt: la conjectura de Poincaré, demostrada per un matemàtic rus: Grigori Yákovlevich Perelmán.

Aquesta llista de problemes s'elaborà anys més tard de que David Hilbert (1862-1943), un matemàtic alemany que dirigí el departament de matemàtiques de Gotinga, elaborés un llistat format per 23 problemes matemàtics no resolts, per a la conferència mundial de les matemàtiques el 1900 a París.

4.2 Els matemàtics i conceptes que es mencionen en aquesta memòria

Al llarg d'aquest estudi es fa menció de molts matemàtics, els quals van influir enormement en el desenvolupament de la Hipòtesi en qüestió. En aquest capítol es té la intenció d'ordenar els matemàtics i els esdeveniments en el temps.

Els matemàtics que seran mencionats a continuació contribuïren en diversos camps de les matemàtiques, de la ciència o d'altres disciplines, però aquest treball se centra en les contribucions d'aquests respecte els nombres primers.

EUCLIDES D'ALEXANDRIA (300 a.C.)

Fou un matemàtic grec conegut avui dia com "El pare de la geometria". Fundà l'escola de matemàtiques de la ciutat i redactà un dels llibres més importants el la història de les matemàtiques, *Elements*.
Contribuï enormement en les matemàtiques, i respecte els nombres primers se'l recorda per demostrar la infinitud d'aquests.

Figura 1. Biografia resumida d'Euclides

Tot i que hi ha historiadors que suggereixen que els nombres primers foren observats molt abans, les primeres nocions matemàtiques que en tenim es remunten a l'antiga Grècia fa més de 2.200, quan Euclides, un matemàtic grec observà que hi havia nombres diferents, i no era capaç de preveure quan en trobaria un altre o si, per contra, deixarien d'haver-n'hi. Aleshores Euclides ho raonà de la següent manera:

Partint de que cada nombre compost, com dicta el Teorema Fonamental de l'Aritmètica, que també estudià el m atemàtic grec, té una composició única de productes de nombres primers; suposem que tenim una llista finita de nombres primers 2, 3, 5, 7, 11, ..., pn dels primers n nombres primers. Si fóssim capaços de trobar el següent nombre primer a aquesta llista, significaria que els nombres primers són infinits, ja que hauríem comprovat que la llista no acabaria mai. Així doncs, tenint en compte l'enunciat del Teorema Fonamental de l'Aritmètica, si multipliquem tots els nombres primers que tenim a la llista $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p_n + 1$ i a aquest se li suma 1 unitat, es pot apreciar que el nombre N resultant no serà divisible per cap nombre primer, dons a l'haver sumat aquesta unitat després de calcular el producte de tots els nombres primers, se'ns ha assegurat que no és divisible per cap nombre primer. Aleshores, si N no és divisible per cap nombre primer, tampoc serà divisible per cap nombre compost, i per tant ens trobarem davant del següent nombre primer de la llista, major que p_n. De manera que, Euclides afirmà l'existència d'infinits nombres primers.

En aquesta demostració, s'han emprat els nombres primerials, que són aquells nombres que resulten del producte de tots els nombres primers més petits o iguals que un nombre fixat p. Aquests nombres es representen #p. De manera que:

$$\#2 = 2$$
$$\#3 = 2 \cdot 3 = 6$$
$$\#5 = 2 \cdot 3 \cdot 5 = 30$$
$$\#7 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$$
$$\#11 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$
$$\#13 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$$
(1)

Aleshores, segons la demostració d'Euclides, si se sumés una unitat a tots aquests primerials, els resultats haurien de ser primers, però:

$$\#2 = 2 + 1 = 3, primer$$
$$\#3 = 2 \cdot 3 = 6 + 1 = 7, primer$$
$$\#5 = 2 \cdot 3 \cdot 5 = 30 + 1 = \ 31, primer$$
$$\#7 = 2 \cdot 3 \cdot 5 \cdot 7 = 210 + 1 = 211, primer$$
$$\#11 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 + 1 = 2311, primer$$
$$\#13 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030 = 30031, és\ compost\ (59 \cdot 509)$$
$$\#17 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 510510 = 510511, és\ compost\ (19 \cdot 97 \cdot 207)$$
(2)

Això es deu a què si $\#p + 1$, és compost, és perquè tots els seus factors són més grans que p, i es confirma la demostració que hi ha infinits nombres primers.
Actualment, es desconeix si hi ha infinits nombres primers de la forma $\#p + 1$.

MARIN MERSENNE (1588-1648)

Marin Mersenne fou un sacerdot, matemàtic i filòsof francès del segle XVII que estudià diversos camps de la teologia i la matemàtica. També fou un músic. En la teoria musical se'l considera molt important en el camp de l'acústica. Fou amic i company d'estudis de Huygens i Descartes.
En la història dels nombres primers, se'l coneix sobretot, pels nombres que duen el seu nom.

Figura 2. Biografía resumida de Mersenne

Mersenne feu enormes contribucions en les matemàtiques, i és especialment recordat pel que fa als nombres primers pels nombres que porten el seu nom. Els nombres de Mersenne, són uns nombres determinats mitjançant una potència positiva de dos menys una unitat:

$$M_n = 2^n - 1 \quad (3)$$

Sent n un nombre natural.
Per exemple,

$n = 1$;
$$M_1 = 2^1 - 1 = 1$$

$n = 2$;
$$M_2 = 2^2 - 1 = 3$$

$n = 3$;
$$M_3 = 2^3 - 1 = 7$$

$n = 4$;
$$M_4 = 2^4 - 1 = 15$$

$n = 5$;
$$M_5 = 2^5 - 1 = 31$$

$n = 6$;
$$M_6 = 2^6 - 1 = 63$$

$n = 7$;
$$M_7 = 2^7 - 1 = 127$$

Fàcilment, s'arriba a la conclusió que tots els nombres de Mersenne seran nombres imparells, doncs totes les potències naturals de 2 són nombres parells, i restant-li una unitat, en resulta un nombre imparell.
També es pot apreciar, que entre un nombre de Mersenne M_n i el seu posterior $M_n + 1$, hi ha $2n$ unitats de diferència.

Mersenne aprecià que entre tots aquests nombres generats, podien trobar-s'hi nombres primers, com ara el 3 ($n = 2$), el 7 ($n = 3$), el 31 ($n = 5$), el 127 ($n = 7$) i demés. Aleshores es fixà amb què el nombre n per a tots aquests nombres primers generats, era també un nombre primer. Després d'estudiar amb més deteniment altres nombres, però, va poder veure que no per a tot n primer, el nombre de Mersenne generat era primer.
Aleshores, la conclusió extreta és que per a tot nombre de Mersenne primer, n serà primer; però no per a tot n primer un nombre primer de Mersenne serà generat.

En l'actualitat, els nombres primers de Mersenne constitueixen els majors nombres primers coneguts fins el moment. El projecte *GIMPS* (1996), "Great Internet Mersenne Prime Search", de computació distribuïda, usa els programes gratuïts *Prime95* i *MPrime* per tal de poder trobar nombres primers que seguissin la fórmula plantejada per Mersenne tants anys endarrere. Actualment, es coneixen 51 nombres primers de Mersenne. Es par-

la de nombres amb més de 24 milions de xifres; concretament, el 7 de desembre de 2018, l'associació *GIMPS*, va trobar el major nombre primer conegut a la història, format per 24.862.048 xifres, de la mà de Patrick Laroche.
El projecte ha estat un èxit, des la seva fundació, s'han trobat un total de 17 nombres primers de Mersenne, i tothom és lliure de prestar el seu ordinador per a què aquest ajudi a calcular nombres primers.

PIERRE FERMAT (1601-1665)

Fou un jurista i matemàtic francès i un dels matemàtics més rellevants de principis del segle XVII, qui treballà pioneramente en camps com ara el càlcul, la geometria analítica i la probabilitat. Tot i això, és molt conegut gràcies a les seves aportacions a la teoria de nombres i els seus teoremes i hipòtesis al respecte.
Anecdòticament, anunciava els seus teoremes sense donar cap mena de justificació, i els matemàtics posteriors, tractaven de demostrar les seves solucions.
Respecte els nombres primers, és recordat gràcies al Teorema de la suma de dos quadrats i al Petit Teorema de Fermat.

Figura 3. Biografia resumida de Fermat

El Teorema de la suma de dos quadrats

Aquest teorema formulat per Fermat el 1640, anuncia que un nombre primer p, és expressable com a suma de quadrats si, i només si,

$$p \equiv 1(mod\ 4) o\ p = 2 \qquad (4)$$

Per exemple, $p = 5, p = 13, p = 17, \dots, per\ tot\ p = 4k + 1$; on k és un nombre natural.

$$Per\ p = 2 \rightarrow 2 = 12 + 12;$$
$$Per\ p = 5 \rightarrow 5 = 12 + 22;$$
$$Per\ p = 9 \rightarrow 9\ no\ és\ un\ nombre\ primer.$$
$$Per\ p = 13 \rightarrow 13 = 32 + 22;$$
$$Per\ p = 17 \rightarrow 17 = 12 + 42;$$

Fermat va anunciar el seu teorema en una carta dirigida a Marin Mersenne datada el 25 de desembre de 1640, raó per la qual coneixem aquest teorema també com a Teorema de Nadal de Fermat.
Fermat no va donar cap demostració del seu teorema i fou Leonhard Euler el primer en donar una demostració formal basada en un descens infinit. Va ser anunciada en una carta escrita a Christian Goldbach el 12 d'abril de 1749.
Altres matemàtics van tractar de demostrar aquest teorema que formulà Fermat, i Lagrange, publicà una demostració el 1775 basada en el seu estudi de formes quadràti-

ques. Aquesta demostració fou simplificada per Gauss al seu llibre Disquisitiones arithmeticae.
Catorze anys més tard, Fermat anuncià, el 25 de setembre de 1654, mitjançant una carta dirigida a Blaise Pascal, els resultats per nombres primers majors que 2:

· Cada nombre primer, que és major en una unitat a un múltiple de 3, és compost per un quadrat i el triple d'un quadrat com ara 7, 13, 19, 31, 37, ...

· Cada nombre primer, que és major en una unitat (1) o en tres unitats (3) a un múltiple de 8, és compost per un quadrat i el doble d'un altre quadrat com ara 11, 17, 19, 41, 43, ...

En aritmètica modular podríem transcriure-ho de la següent manera:

$$p = x^2 + 3 \cdot y^2, p \equiv 1(mod\ 3) \quad (5)$$
$$p = x^2 + 32, p \equiv 1(mod\ 8) o\ p \equiv 3(mod\ 8) \quad (6)$$

El Petit Teorema de Fermat

El 1636, Fermat anunciava l'anomenat Petit Teorema de Fermat, relacionat amb la divisibilitat dels nombres de la següent manera:

$$\text{“}Si\ p\ és\ un\ nombre\ primer, llavors, per\ cada\ nombre\ natural\ a, amb\ a > 0,$$
$$a \equiv p^a\ (mod\ p)\text{”}$$

El que aquest enunciat implica, és que si elevem un nombre a a la p-èssima potència, i al resultat se li resta aquest nombre a, ens resultarà un nombre divisible per p.
Aquest resultat ha estat aplicat en teoria de primeritat i criptografia.

Els nombres de Fermat

Els nombres de Fermat, foren una altra de les moltes aportacions del reconegut matemàtic i jurista a les matemàtiques. Són de la forma següent,

$$F_n = 2^{2^n} + 1, n \in N \quad (7)$$

Els primers nombres primers de Fermat són:

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 65.537$$

Cada un d'ells és primer. Però a l'arribar al nombre F_5, més tard, Leonhard Euler demostrà que no era un nombre primer, ja que el resultat equival al producte de $641 \cdot 6700417$. El 1995 el demostrà un matemàtic britànic: Andrew Wiles.

LEONHARD EULER (1707 -1783)

Fou un matemàtic i físic suís que visqué a Rússia i a Prússia. Euler feu importants descobriments en el camp del càlcul i la teoria de grafs. Feu importants avenços en la teoria de nombres imaginaris, en l'anàlisi matemàtica, astronomia i òptica.
Respecte els nombres matemàtics és recordat gràcies a demostrar l'existència d'infinits nombres primers mitjançant la sèrie harmònica i convertint aquesta en producte de potències de primers, anomenant-se així *el producte d'Euler*. També demostrà hipòtesis d'altres matemàtics com Fermat.

Figura 4. Biografia resumida d'Euler

Euler fou un dels matemàtics més importants. Contribuí en molts camps de les matemàtiques. Com a matemàtic fou molt creatiu i de pensament obert. Feu nombrosos avenços en les matemàtiques i, respecte els nombres primers, els estudià. Més endavant s'explicarà que Euler estudià la sèrie harmònica i la transformà en un producte de potències de nombres primers. A aquest producte se'l coneix com *Producte D'Euler* i fou de gran importància per a què Riemann desenvolupés la famosa Hipòtesi. També treballà en anàlisi matemàtica i els nombres imaginaris, i els seus estudis donaren lloc a molta teoria matemàtica.

ADRIEN MARIE LEGENDRE (1752-1833)

Fou un destacat matemàtic francès que feu importants contribucions a diverses àrees de les matemàtiques com ara l'estadística, la teoria dels nombres, l'àlgebra abstracta i l'anàlisi matemàtica.
Ell escrigué una obra titulada *Essai sur la théorie des nombres*, que inspirà a Riemann. També descobrí que entre la funció logarítmica i la distribució dels nombres primers existia una relació, i aquest millorà la funció que donà Gauss.

Figura 5. Biografia resumida de Legendre

Legendre fou un matemàtic que encara és recordat ara per les seves nombroses aportacions. Quan Riemann tingué 15 anys, llegí la seva obra *Essai sur la théorie des nombres* de manera increïblement ràpida, ja que sentí passió pel que explicava Legendre en aquelles pàgines, i començà a trobar el seu camí en les matemàtiques.

Hi ha discòrdia en el fet de qui descobrí abans la relació entre la distribució dels nombres primers i la funció logarítmica, doncs Gauss assegura que ho feu entre el 1792 i el 1793, mentre que Legendre ho publicà el 1798. De totes maneres, ambdós realitzaren

importants avenços. Adrien Marie feu pública la funció que trobà més pròxima a la funció que distribuïa els nombres primers, i que era força millor que la primera proposta de Gauss. No obstant, Gauss n'acabà trobant una més pròxima encara.

CARL FRIEDRICH GAUSS (1777-1855)

Fou un matemàtic, físic i astrònom alemany, que contribuí en molts àmbits de la ciència: des de magnetisme fins a teoria de nombres. Considerat encara ara el *Príncep de les Matemàtiques*. Des molt petit ja mostrà increïbles aptituds per les matemàtiques, i al ser d'origen molt pobre fou becat per un Duc per poder estudiar. Fou professor i investigador a Gotinga. Respecte els nombres primers en feu nombroses contribucions: com ara definir la funció $\pi(x)$, i la integral $Li(x)$ com a aproximació de la funció.

Figura 6. Biografia resumida de Gauss

Gauss és encara ara considerat un dels millors matemàtics de la història. La seva intuïció, dedicació i capacitat d'anàlisi, han deixat petjada en la física, les matemàtiques, l'estadística i l'astronomia.

Pel que fa als nombres primers, Gauss fou capaç d'observar una relació entre la funció logarítmica i la distribució dels nombres primers. A partir d'aquí obrí un nou camí a la recerca d'aquests, i aquest fet influí molt en el desenvolupament de la hipòtesi de Riemann, tal com es veurà més endavant.

PETER GUSTAV LEJEUNE DIRICHLET (1805-1859)

Fou un matemàtic alemany al qui se li atribueix la definició formal d'una funció. Dirichlet és conegut en part gràcies a les sèries que duen el seu nom i que han estat aplicades en els càlculs de la distribució de la calor i en la investigació de la distribució dels nombres primers. Quan Gauss morí, aquest ocupà la seva càtedra a Gotinga i fou professor.
Pel que fa als nombres primers se li atribueix el fet d'haver innovat alhora de definir les sèries que duen el seu nom, i haver estat creatiu en general.

Figura 7. Biografia resumida de Dirichlet

Tal com s'explicarà més endavant, Riemann tingué la sort de conèixer Dirichlet a Berlín, i quedaren impressionats l'un per l'altre: Riemann, un jove matemàtic molt capaç, i Dirichlet, d'una edat semblant, un matemàtic creatiu, innovador, reivindicatiu i carismàtic.

Riemann quedà sorprès per les sèries que Dirichlet estudià, i també volgué estudiar-les. Més endavant, tornaren a coincidir a Gotinga.

PAFNUTI LVÓVICH CHEBYSHOV (1821-1894)

També conegut com Chebyshev, fou un matemàtic rus. Feu importants aportacions el l'estadística, la probabilitat i la teoria de nombres. Se'l recorda especialment per la desigualtat que duu el seu nom, entre d'altres.
En l'àmbit dels nombres primers contribuí enormement en el desenvolupament de la hipòtesi de Riemann, doncs Chebyshev desenvolupà una ampliació analítiva de la funció zeta, que s'explica més endavant en aquesta memòria.

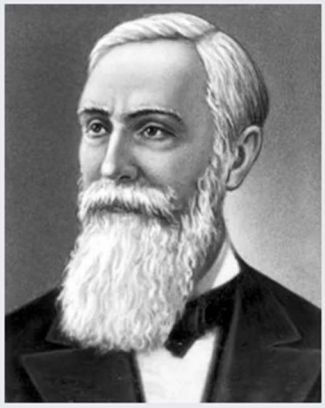

Figura 8. Biografia resumida de Chebyshev

Chebyshev obrí camí a Riemann mitjançant la continuació analítica de funcions, per a poder-les estudiar fora del seu domini mitjançant una funció que es comportés de la manera deguda en els punts en què la funció inicial no ho feia. Riemann prengué els seus estudis com a referència i inspiració i anà molt més enllà. També s'explicarà més endavant, tot i que no s'entrarà el els detalls més analítics d'aquest procés, doncs probablement em falti formació.

GEORG FRIEDRICH BERNHARD RIEMANN (1826-1866)

Riemann fou un matemàtic alemany que realitzà contribucions molt importants en molts àmbits de les matemàtiques com ara l'anàlisi i la geometria diferencials, que serviren per a què Einstein desenvolupés la teoria de la relativitat general.
Es recordat especialment per la hipòtesi que duu el seu nom, i de la qual tracta aquest treball, i per moltes altre aportacions que feu al llarg de la seva vida.
Quan Dirichlet morí, ell ocupà la càtedra que prèviament havia pertangut a Gauss.

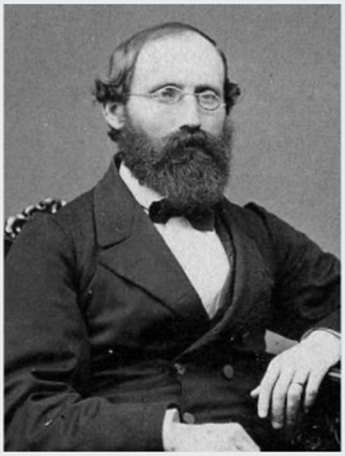

Figura 9. Biografia resumida de Riemann

Riemann, fou un estudiant brillant a qui li agradava refugiar-se en llibres de matemàtiques; especialment en llibres de matemàtiques més aviat conceptuals. Fou així quan un dia, a la biblioteca del seu professor de secundària trobà un llibre d'Adrien Marie Legendre: *la Théorie des nombres (1808)*, on el matemàtic fou l'autor del primer text que registrà l'observació d'un curiós nexe entre la distribució dels nombres primers i la funció logarítmica.

Riemann llegí tot el llibre en menys d'una setmana, i a partir d'aquest, la seva passió per les matemàtiques fou encara més notable.

A l'hora d'entrar a la universitat, les circumstàncies, les quals disgustaren el jove, el portaren a emprendre estudis eclesiàstics a l'única universitat d'Alemanya on s'impartien: a la Universitat de Gotinga.
Fou en aquella mateixa universitat on hi residia aleshores el famosíssim Carl Friedrich Gauss. En aquells moments era el cap del departament d'astronomia, impartia poques classes i aquestes només eren relatives al seu departament. Però tot i així, la presència de Gauss en la mateixa universitat on estudiava, i l'oportunitat de poder assistir a algunes de les seves classes; l'animà per demanar permís al seu pare i posar-se a estudiar matemàtiques. Gauss fou fins i tot el director de tesi de Riemann. Gotinga aviat li semblà petita i d'aquesta manera se n'anà cap al nucli científic en aquell moment: Berlín.

A Berlín va poder estudiar alguns papers de Gauss i va poder assistir a les classes del matemàtic Johann Peter Gustav Lejeune Dirichlet, i com a professor aquest el marcà profundament, i ja es veurà quant.
Allà a Berlín, arribaren traces de la revolució francesa que hi havia aleshores, i amb aquestes hi arribava la revista Comptes rendus en la qual publicava el matemàtic francès Agustin Louis Cauchy, i Riemann trobà aquelles noves idees tan revolucionàries que es quedà encandilat. El que havia captat tota atenció i admiració per Cauchy i Riemann foren els nombres imaginaris.
Més tard, Riemann retornà a Gotinga a presentar la seva tesi, ja que el seu tutor caigué en malaltia i un any més tard de la presentació, Gauss moriria. No obstant, l'anomenat Príncep de les matemàtiques pogué llegir el treball de Bernhard, i quedà profundament sorprès de les innovadores idees que presentà l'alumne.
Quan la càtedra de Gauss quedà lliure degut a la seva mort, fou ocupada per Dirichlet qui, el 1859, quatre anys més tard que Gauss, morí. La càtedra que havien ocupat aquests grans matemàtics, finalment fou per a Riemann.

Bé, ja posada en context la història d'un dels millors matemàtics del segle IXX, s'analitzarà com aquest va arribar a formular una de les hipòtesis que actualment forma part dels Problemes del mil·lenni.

Riemann s'interessà pels nombres primers quan, tal com s'ha mencionat prèviament, quan llegí una obra de Legendre on aquest establia públicament que existia una relació entre el logaritme neperià d'un nombre i la quantitat de nombres primers que es trobaven entre l'1 i aquell nombre. Més endavant es comentarà com Gauss i Legendre, pràcticament alhora, establiren aquesta relació i n'anaren millorant la *troballa* de l'altre.
Fora com fora, Riemann quedà realment encuriosit per aquella relació que mantenia en secret la naturalesa dels nombres, i anys més tard, ens donà la clau que podria obrir la porta a la resposta que posaria ordre entre els primers.

GAUSS

Tot començà a Gotinga, quan Gauss, independentment de Legendre, relacionà la distribució dels nombres primers amb la funció logarítmica de base e.

Anys endarrere, quan Gauss comptava únicament amb 15 anys, va rebre com a regal un llibre que contenia taules de logaritmes i els seus valors corresponents. Aquest llibre, a més a més, contenia un llistat de nombres primers.
Gauss usà els valors dels logaritmes per a realitzar diversos càlculs i estudis, i anà prenent consciència de com funcionaven les funcions logarítmiques.
Fou aleshores quan, contemplant el llistat de nombres primers, no sostingué la idea que aquests es trobessin distribuïts de forma aleatòria entre els nombres naturals, de manera que realitzà tota mena de càlculs i hipòtesis per a treure'n alguna conclusió. Entre aquests, Gauss definí el que coneixem en teoria de nombres com *El teorema dels nombres primers*, i descriu la funció $\pi(x)$, que compta la quantitat de nombres primers que podem trobar entre 1 i x.

4.3 El teorema dels nombres primers

El Teorema dels nombres primers és un enunciat que descriu com estan distribuïts els nombres primers, mitjançant una funció esglaonada que denotem per $\pi(x)$.

La funció es defineix de la següent manera:

$$\pi(x) = \{p \in P, p \leq x\} \tag{8}$$

On $\#A$ significa "el nombre d'elements d'A,
P és el conjunt de nombres primers.
i x és un nombre natural.

L'expressió (8) significa que: tot nombre p que sigui primer i es trobi entre 1 i x, serà comptabilitzat i $\pi(x)$ donarà el valor total de nombres entre 1 i x que pertanyen al conjunt de nombres primers P.

D'aquesta manera;

$$(4) = 2, entre\ l'1\ i\ el\ 4\ trobem\ dos\ nombres\ primers: els\ nombres\ 2\ i\ 3;$$
$$(10) = 4, entre\ l'1\ i\ el\ 10\ trobem\ quatre\ nombres\ primers: els\ nombres\ 2,3,5\ i\ 7;$$
$$(31) = 11, entre\ l'1\ i\ el\ 31\ trobem\ dos\ nombres\ primers: 2,3,5,7,11,13,17,19,23,29,31;$$

Aleshores, la funció $\pi(x)$ és una funció que en certa manera representa la freqüència amb què trobem nombres primers entre l'1 i x.

Gràficament, la representació de la funció $\pi(x)$, és de la següent manera:

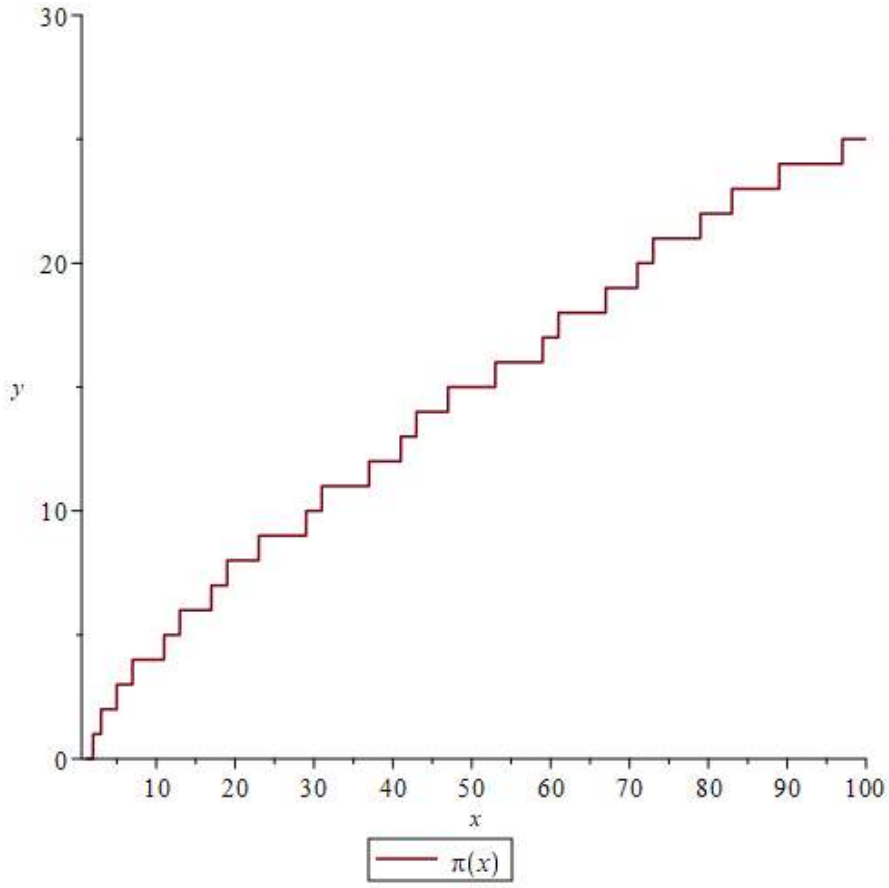

Figura 10. Representació gràfica de $\pi(x)$ en [1, 100]

En la figura 10 es representa la funció $\pi(x)$ per $x = 100$. Es veu com $\pi(100) = 25$, la qual cosa significa que en el primer centenar de nombres naturals hi trobem 25 nombres primers i, equival per tant, a una freqüència d'1 nombre primer cada 4 nombres naturals.
Aleshores, Gauss pensà que si pogués trobar una funció que, sense que ningú hagués de comptar la quantitat de nombres primers, i aquesta pogués tenir el mateix comportament que $\pi(x)$, significaria que es podria saber quants nombres primers hi ha en tot moment i, si fós possible, saber quins nombres són primers o no sense haver de realitzar massa càlculs.
Per el moment es dedicà a estudiar la freqüència amb què apareixen els nombres primers a mesura que prenia nombres més i més grans.

En la següent taula hi podem observar la *funció comptadora de nombres primers* $\pi(x)$ i el resultat corresponent a l'invers de la freqüència amb què es troben nombres primers entre 1 i cada x corresponent.

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10	4	2,5
100	25	4
1.000	168	5,95
10.000	1.229	8,14
100.000	9.592	10,43
1.000.000	78.498	12,74
10.000.000	664.579	15,05
100.000.000	5.761.455	17,36
1.000.000.000	50.847.534	19,66
10.000.000.000	455.052.512	21,98

Taula 1. Comparació entre $\pi(x)$ i $\frac{x}{\pi(x)}$ per a diferents valors de x.

Fou aleshores quan, ja sabent-se pràcticament els valors dels logaritmes de memòria, el jove Gauss observà un fet que, particularment, em resulta preciós.

Estudiant aquesta última columna, es poden provar diverses combinacions d'operacions per extreure'n conclusions i experimentar, però Gauss en traié una que, concretament, canvià per complet la visió del desordre que representaven els nombres primers.
Gauss es fixà en la diferència present entre els nombres d'aquesta tercera columna;

$$
\begin{aligned}
&Entre\ 2{,}5\ i\ 4, hi\ ha\ 1{,}50\ unitats,\\
&Entre\ 5{,}95\ i\ 4, hi\ ha\ 1{,}95\ unitats,\\
&Entre\ 8{,}14\ i\ 5{,}95, hi\ ha\ 2{,}19\ unitats,\\
&Entre\ 10{,}43\ i\ 8{,}14, hi\ ha\ 2{,}29\ \ unitats,\\
&Entre\ 12{,}74\ i\ 10{,}43, hi\ ha\ 2{,}31\ unitats,\\
&Entre\ 15{,}05\ i\ 12{,}74, hi\ ha\ 2{,}31\ unitats,\\
&Entre\ 17{,}36\ i\ 15{,}05, hi\ ha\ 2{,}31\ unitats,\\
&Entre\ 19{,}66\ i\ 17{,}36, hi\ ha\ 2{,}30\ unitats,\\
&Entre\ 21{,}98\ i\ 19{,}66, hi\ ha\ 2{,}32\ unitats,
\end{aligned}
$$

Observant les diferències entre els nombres de la tercera columna, podem veure com, a mesura que va creixent l'interval $[0, x]$, aquesta diferència s'estabilitza aproximadament a les 2,3 unitats.
I Gauss, gràcies al llibre de taules de logaritmes amb el llistat de nombres primers, relacionà ràpidament que;

$$\ln(10) = 2{,}302585093.$$

D'aquesta manera, Gauss trobà que la distribució dels nombres primers estava relacionada amb la funció logarítmica de base e.

A partir d'aquí, els nombres primeres prengueren importància en la curiositat d'un dels millors matemàtics de la història, i aquest començà a buscar funcions i fórmules que encaixessin en la distribució dels nombres primers.

El 1792, proposà una funció matemàtica que conservava un comportament molt semblant al de la funció comptadora de nombres primers, quan el nombre primer en qüestió tendia a l'infinit. Aquesta funció fou la següent:

$$f(x) = \frac{x}{\ln(x)} \tag{9}$$

de manera que;

$$\pi(x) \sim \frac{x}{\ln(x)} \tag{10}$$

Aquest resultat, tal com s'ha mencionat prèviament, l'introduí Gauss, i s'anomena el Teorema dels nombres primers.

No obstant, la diferència entre $\pi(x)$ i $f(x)$ no és nul·la, sinó que el quocient entre ambdues funcions s'aproxima a la unitat.

Si s'escriu de la següent manera, es pot apreciar que la quantitat de nombres primers entre 2 i x, dividida per x, s'aproxima a la funció $\frac{1}{\ln(x)}$ a mesura que el nombre x és major. Recordem que $\ln(x)$és major per a x majors cada vegada.

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln(x)} \tag{11}$$

La comparació gràfica d'aquestes dues funcions es pot apreciar a la representació següent.

Aquesta gràfica està acotada per als primer 100 nombres naturals; i ja hem comentat que a mesura que major és x, millor s'aproxima la funció $f(x)$ a $\pi(x)$.

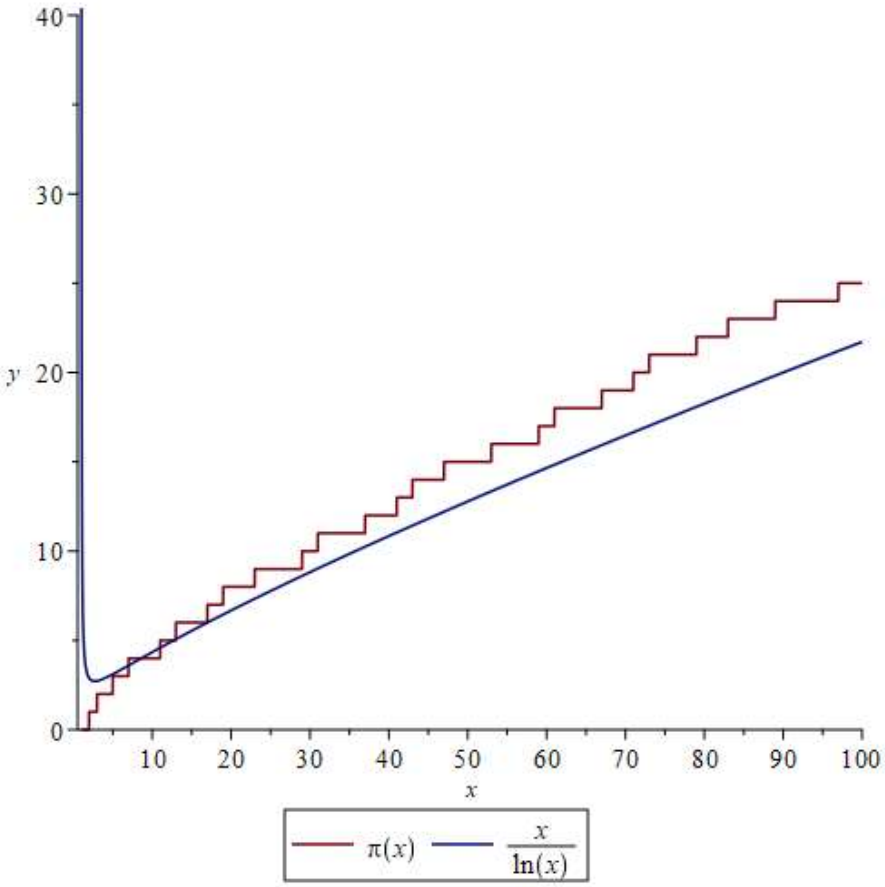

Figura 11. Representació gràfica entre $\pi(x)$ i l'expressió (9) en [0, 100]

És clar que $f(x)$ té un comportament asimptòtic a mesura que x s'aproxima a 1, doncs sabem que la funció logarítmica no té imatge per $x = 1$, i de totes maneres, tampoc existeix un nombre primer natural menor o igual que 1.

Mostrant ambdues funcions ara en un major interval:

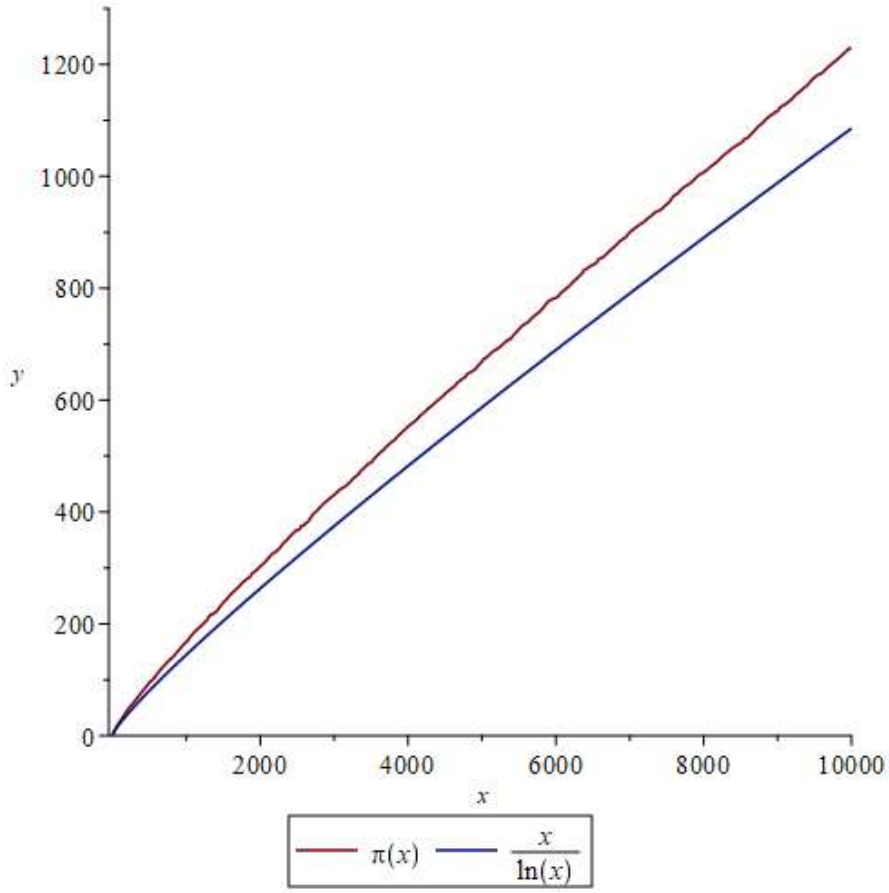

Figura 12. Representació gràfica entre $\pi(x)$ i l'expressió (9) en [0, 10.000]

Es pot apreciar que, no són dues funcions idèntiques, però si més no, tenen un comportament semblant.

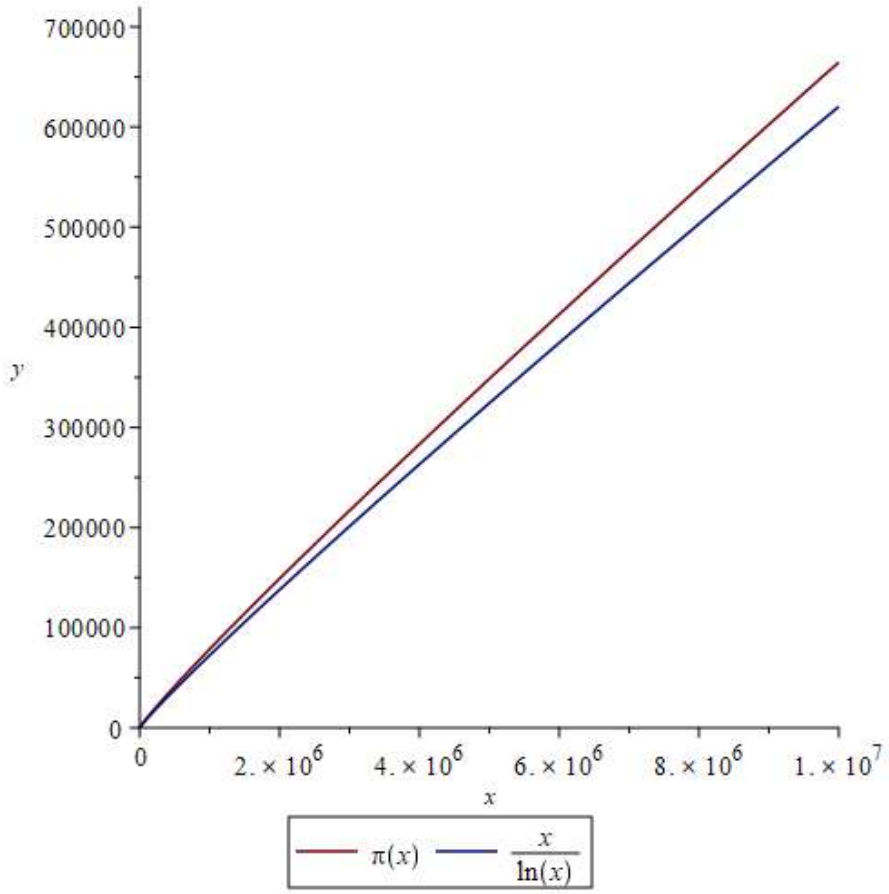

Figura 13. Representació gràfica entre $\pi(x)$ i l'expressió (9) en [0, 10.000.000]

Per a un interval $[0, 10.000.000]$, segueix essent notable la similitud entre ambdues funcions. I cal considerar que el més important és que la distribució dels nombres primers segueixi una tendència relacionada amb el logaritme neperià.

LEGENDRE

Ja s'ha fet menció de que existeix certa discòrdia en el fet de qui va descobrir primerament aquesta relació entre la distribució dels nombres primers i la funció logarítmica, no obstant, es parla de dos dels més meravellosos matemàtics que han existit, així que es tractarà de reconèixer els mèrits per parts iguals en aquest treball.
Així doncs, Adrien Marie Legendre estigué treballant amb els logaritmes i els nombres primers, i a l'apreciar que la funció

$$f(x) = \frac{x}{\ln(x)} \tag{9}$$

presentava discrepàncies amb el resultat que ell pretenia obtenir, en proposà una millora:

$$g(x) = \frac{x}{\ln(x) - 1.08366} \tag{12}$$

Gràficament, i comparant la funció $\pi(x)$, $f(x)$ i $g(x)$ aquesta millora s'aprecia de la següent manera:

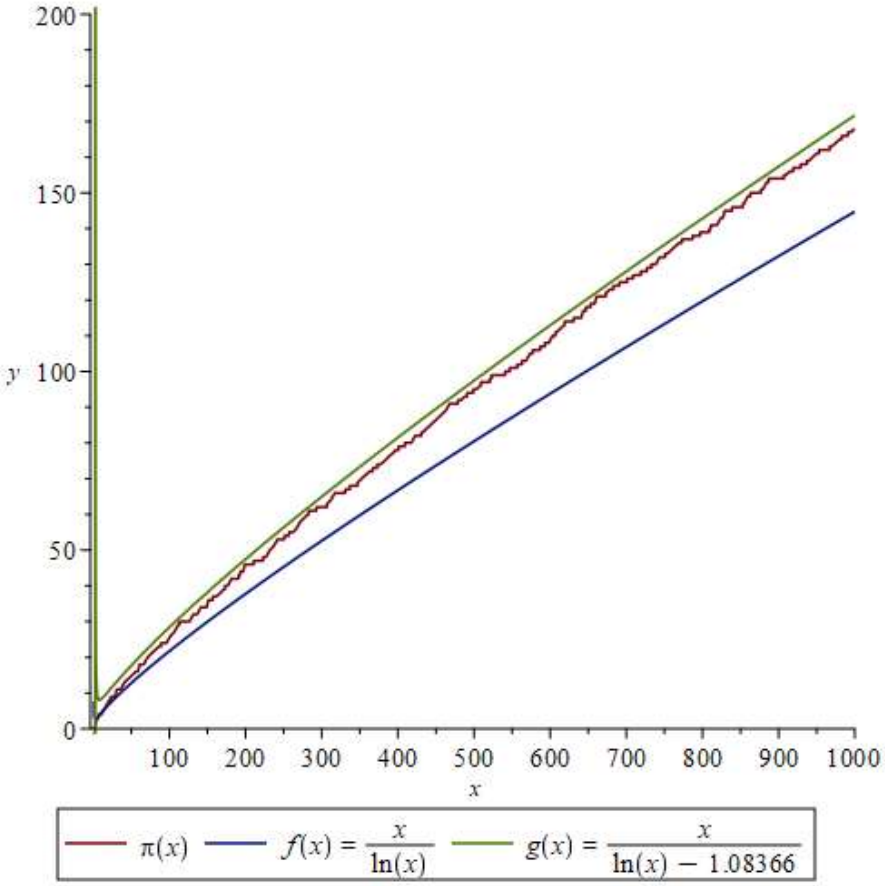

Figura 14. Representació gràfica entre $\pi(x)$, l'expressió (9) i l'expressió (12) en [0, 1.000]

Altra vegada, primerament es mostren les gràfiques en un interval petit. Aparentment, sembla que la millora de Legendre és una proposta encertada.

Si es visualitza el comportament de les tres funcions per a un major interval de nombres:

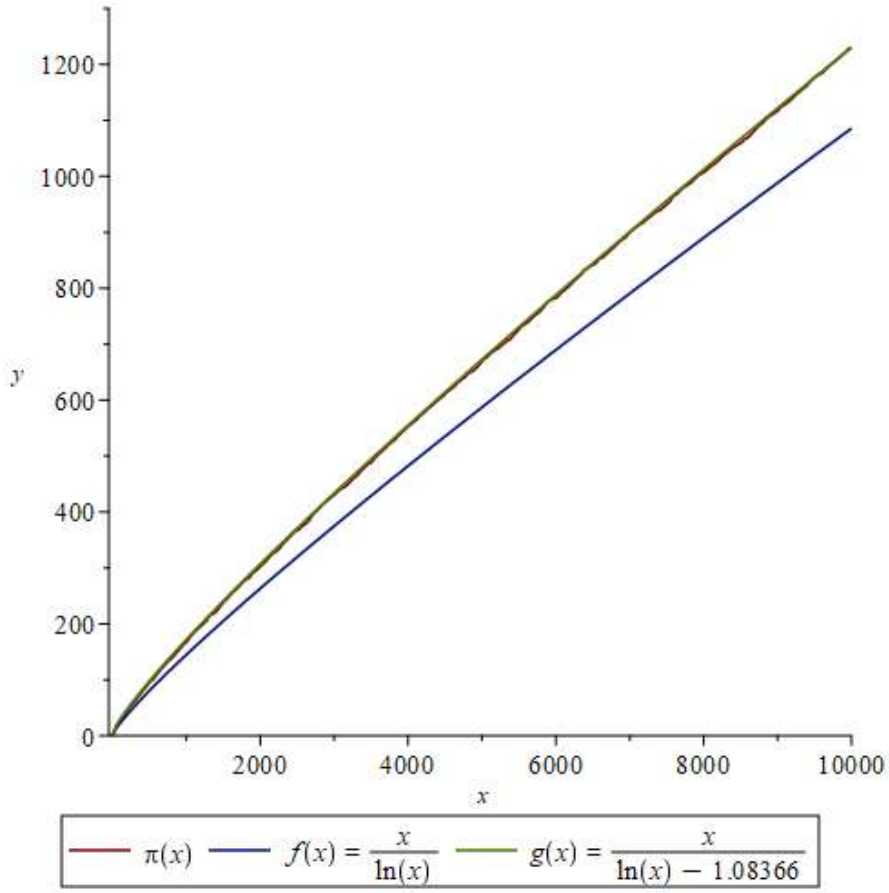

Figura 15. Representació gràfica entre $\pi(x)$, l'expressió (9) i l'expressió (12) en [0, 10.000]

Ara sí que, per a $x = 10.000$ podem veure com realment la millora de Legendre és millor que la proposta inicial del matemàtic alemany.
De fet, si resultà millor fou pel simple fet que aquest emprà el mètode de mínims quadrats per a trobar una constant restant al denominador de manera que la funció s'aproximés millor a $\pi(x)$.
Més endavant es podrà observar, si és la seva voluntat, una sèrie d'estudis que vaig dur a terme al pensar erròniament en un principi, que Legendre proposà aquella constant al equivaldre a una tercera part del nombre π.

GAUSS

Gauss no es conformà amb una aproximació "ben aconseguida" i seguí estudiant els logaritmes.
Partint de la fórmula que proposà prèviament, observà que, sí $\frac{x}{\ln(x)}$ determinava aproximadament la quantitat de nombres primers des de 0 fins a x, i aquesta relació era assimptòticament equivalent a $\pi(x)$, aleshores:

$$\pi(x) \sim \frac{x}{\ln(x)}, \rightarrow \frac{\pi(x)}{x} \sim \frac{1}{\ln(x)} \qquad (9) \text{ i } (10)$$

La traducció d'aquesta relació, és que, si $\pi(x)$ és el nombre aproximat de primers entre 0 i x, i ho dividim per x, aleshores en tenim una aproximació del que representa ser la freqüència amb què apareixen nombres primers en un interval donat i, aleshores, el terme $\frac{1}{\ln(x)}$ també havia d'equivaldre a una aproximació de la freqüència.

En aquesta taula s'observen els termes esmentats i els seus corresponents valors.

x	$\pi(x)$	$\frac{x}{\pi(x)}$	$\frac{1}{\ln(x)}$
10	4	0,4	0,4342944819
100	25	0,25	0,2171472410
1.000	168	0,168	0,2171472410
10.000	1.229	0,1229	0,1447648273
100.000	9.592	0,09592	0,08685889642
1.000.000	78.498	0,078498	0,07238241364

Taula 2. Comparació entre $\pi(x)$, l'expressió (9) i l'expressió (12)

La idea que Gauss tingué fou la següent. En la tercera columna en tenim la freqüència recentment explicada, i a l'última columna en tenim el terme $\frac{1}{\ln(x)}$. Fou així que el matemàtic observà que si sumava aquests termes per a cada x d'un interval donat, el resultat s'aproximava a la funció $\pi(x)$.

D'aquí en sorgí el terme *suma logarítmica*. Que és precisament la suma infinita, per a tot $x > 1$, de la quarta columna de la taula anterior;

$$Ls = \frac{1}{\ln(2)} + \frac{1}{\ln(3)} + \frac{1}{\ln(4)} + \cdots + \frac{1}{\ln(x)} \tag{13}$$

En la taula següent, es comparen el terme Ls (suma logarítmica) i $\pi(x)$.

x	$\pi(x)$	$Ls = \sum_{2}^{n} \frac{1}{\ln(n)}$
10	4	6,137938134
100	25	29,99143756
1.000	168	177,4388002
10.000	1.229	1.245,948278
100.000	9.592	9.629,609202
1.000.000	78.498	78.627,34000

Taula 3. Comparació entre $\pi(x)$ i l'expressió (13

Es pot apreciar que, a mesura que x augmenta, la precisió d'aquesta aproximació també ho fa. I d'aquesta manera sorgí la integral logarítmica, denominada $Li(x)$, que Gauss proposà com a aproximació de la funció $\pi(x)$; doncs la definició d'una integral és precisament un sumatori infinit de funcions avaluades en cada un dels punts del domini d'aquesta funció:

$$Li(x) = \int_{2}^{x} \frac{1}{\ln(t)} dt \tag{14}$$

A continuació es mostren diverses gràfiques per a diferents intervals de nombres naturals, de manera que es podrà apreciar millor la precisió d'aquesta funció en relació amb la distribució dels nombres primers.

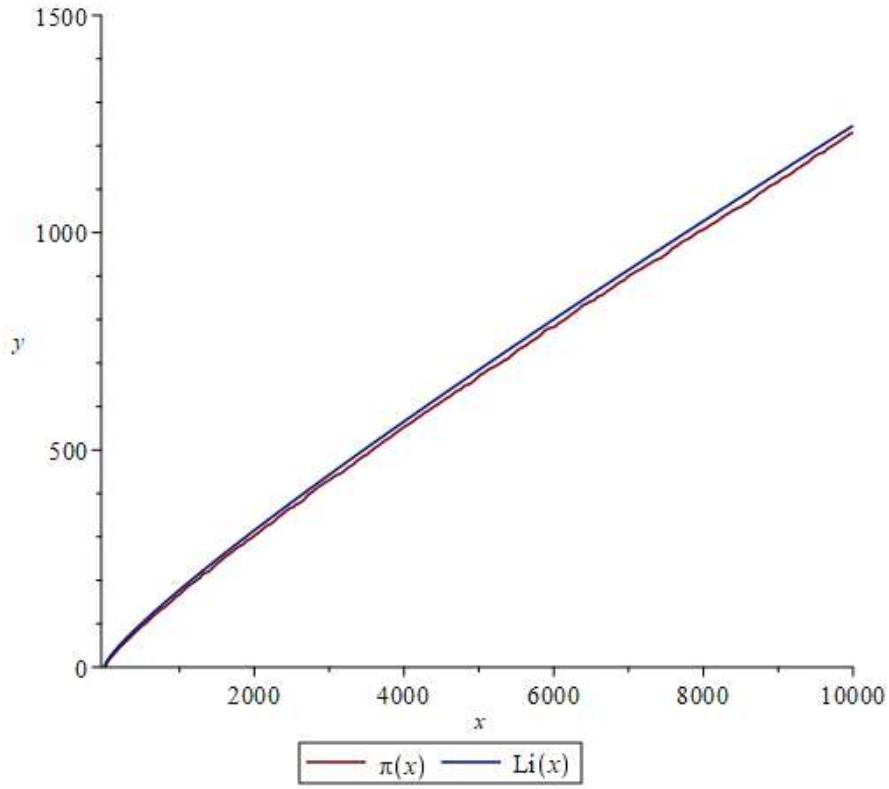

Figura 16. Comparació entre $\pi(x)$ i l'expressió (14) en [0, 10.000]

En aquesta primera representació s'hi troba la funció $\pi(x)$ i la integral logarítmica. Es pot veure com realment tenen un comportament semblant.

Tot i això, es compararan ambdues funcions amb $g(x)$.

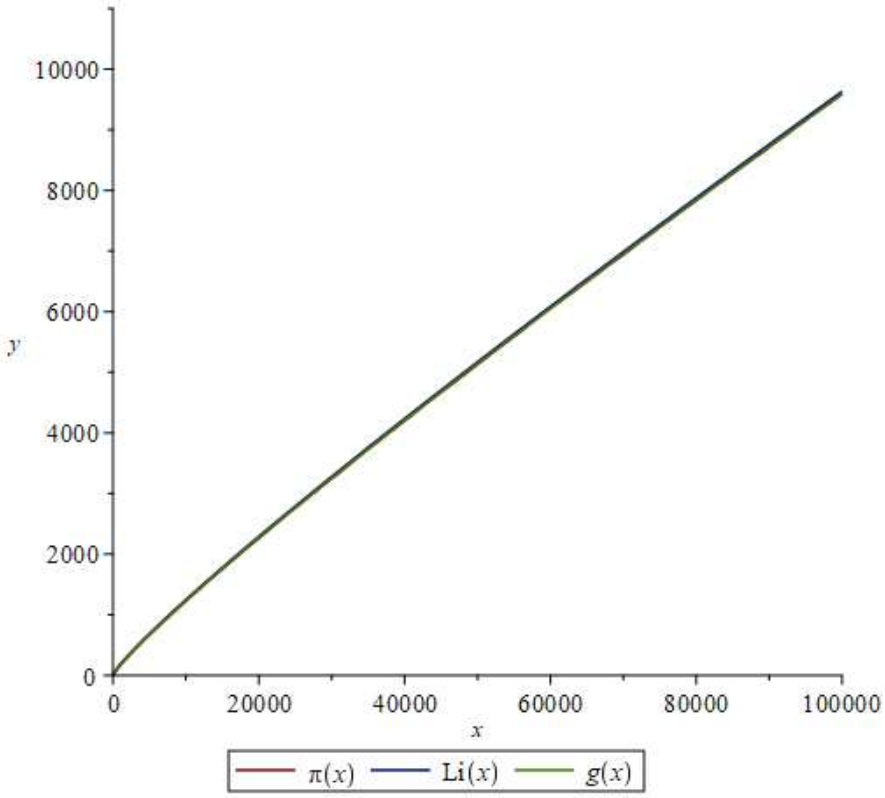

Figura 17. Comparació entre $\pi(x)$ i l'expressió (14) i l'expressió (12) en [0, 100.000]

Les 3 funcions es confonen entre elles i resulta impossible distingir quina de les dues resulta millor aproximació. Es prendrà a continuació un interval menor però de més magnitud.

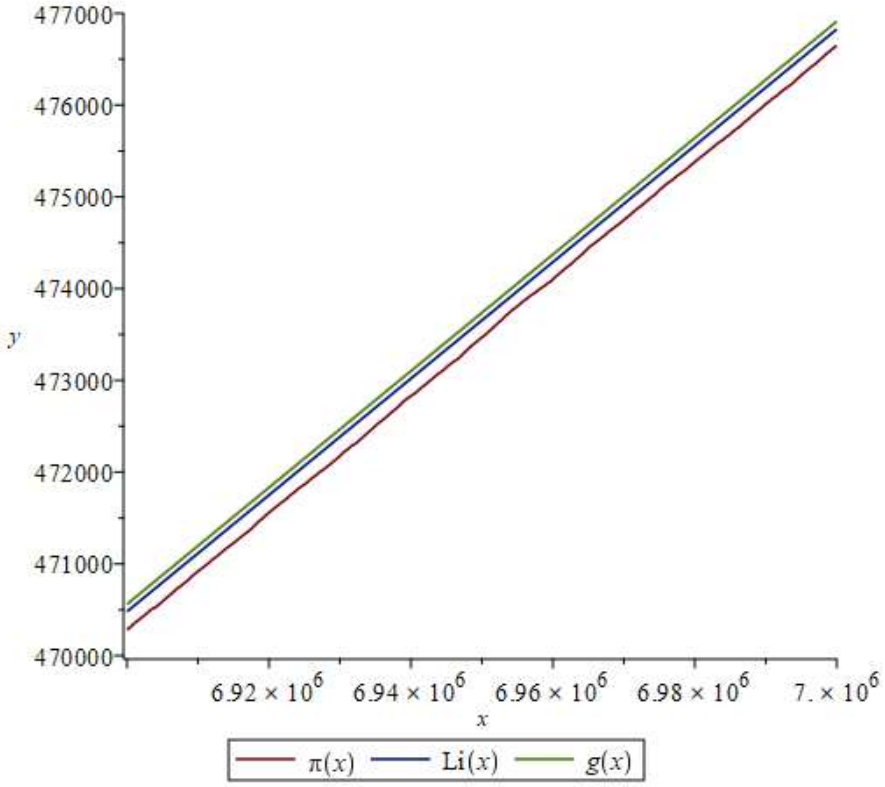

Figura 18. Comparació entre $\pi(x)$ i l'expressió (14) en [0, 1.000.000]

Per a un interval corresponent a $[6.900.000, 7.000.000]$ s'aprecia que tant $g(x)$ com $Li(x)$ són molt bones aproximacions de $\pi(x)$.

La primera aproximació que proposà Gauss, en canvi, està molt lluny de ser realment una bona aproximació per a $\pi(x)$, en comparació amb les dues altres funcions.

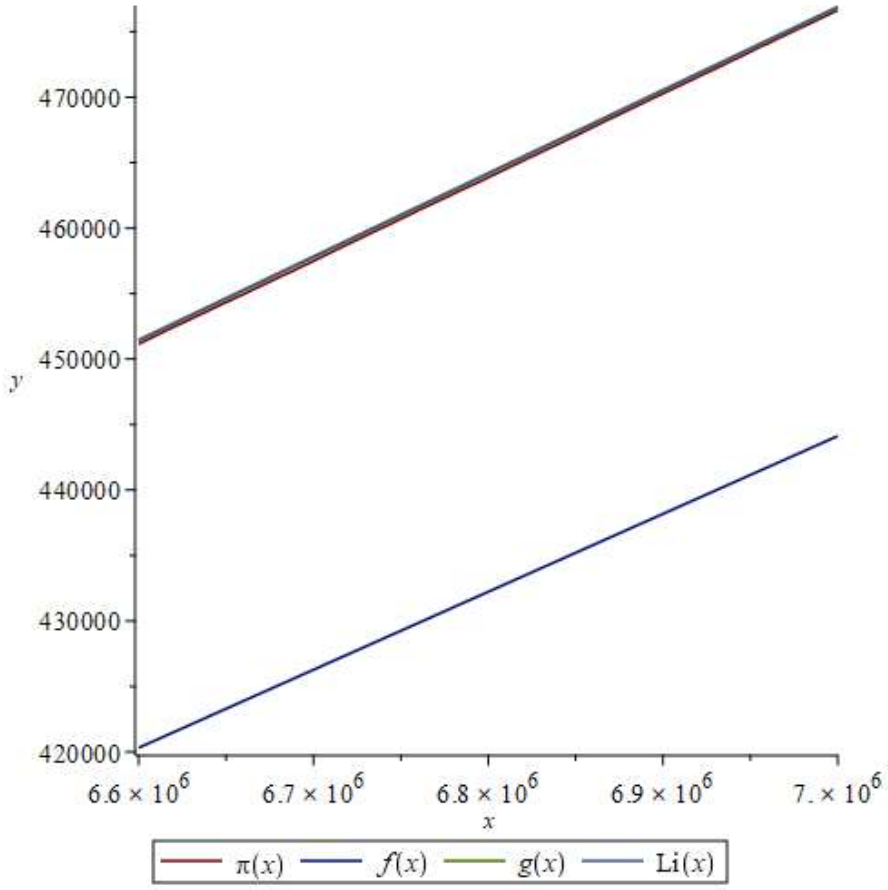

Figura 19. Comparació entre $\pi(x)$ (9), (12) i l'expressió (14) en [0, 1.000.000]

Els matemàtics quedaren realment impressionats davant la precisió de la funció que Gauss acabà deduint gràcies en gran part, a la seva brillant intuïció.

A partir d'aquí, molts matemàtics intentaren arribar a una fórmula que fos encara més precisa. Entre aquests matemàtics, s'hi trobà Riemann.

DIRICHLET

Johann Peter Gustav Lejeune Dirichlet, fou un matemàtic alemany qui nasqué a principis del segle IXX. Fou un home molt carismàtic, i a Riemann li fascinà des d'un principi, quan el conegué a Berlín. Tenia moltes idees, diverses, i les anava estudiant.
Dirichlet també trobava els nombres primers interessants, i seguia els treballs de Gauss. Tan fou així que el 1837 resolgué una hipòtesi que Gauss conjecturà respecte aquests i que era:

$$Siguin\ a, d\ \in N\ tal\ que\ el\ màxim\ comú\ divisor\ entre\ aquests\ sigui\ 1, mcd(a,d) = 1,$$
$$aleshores\ la\ progressió\ aritmètica\ a_n = a + n \cdot d\ conté\ infinits\ nombres\ primers.$$

Això significava que els nombres $a + n \cdot d$ formen una progressió aritmètica en la qual hi ha infinits nombres primers. Dirichlet estava interessat per les sèries i les progressions

aritmètiques. De fet hi ha unes sèries que duen el seu nom en honor al seu treball en aquestes, les Sèries de Dirichlet.

Les Sèries de Dirichlet es defineixen de la següent manera:

$$\sum_{1}^{\infty} \frac{a_n}{n^s} \text{ , on } s \text{ i } a_n \text{ són nombres complexos} \tag{15}$$

Fixant-nos-hi, podem apreciar que, per a $a_n = 1$ i $s = 1$ tenim la famosa sèrie harmònica. La sèrie harmònica, és aquella que suma els inversos dels nombres naturals; és a dir:

$$\sum_{1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}, n \in N \tag{16}$$

La sèrie harmònica, també denotada mitjançant la lletra grega zeta, és una sèrie infinita, i fou demostrat per Nicolás Oresme, considerat un geni francès del segle XIV, que no convergeix per a $s = 1$, és a dir, que tendeix a infinit. Qualsevol fita que es vulgui posar a aquesta sèrie, s'acaba superant mitjançant l'addicció dels infinits termes.
Rep el nom degut a la seva relació amb les longituds d'ona dels successius harmònics d'una corda vibrant.

EULER

Leonhard Euler fou un matemàtic i físic suís, qui també forma part de la privilegiada selecció dels millors matemàtics de la història. Estudià els nombres complexos i els nombres primers. En ambdós camps n'és l'autor de nombrosos i importantíssims enunciats. Per exemple respecte els nombres primers, ell definí la funció $gamma(n)$.
Aquesta funció és:

$$Si\ n\ és\ un\ nombre\ enter\ positiu, aleshores\ gamma(n) es\ defineix\ com\ la\ quantitat\ d'enters\ positius\ menors\ a\ n\ i\ comprimers\ amb\ n.$$

Aquesta funció pren molta importància en el desenvolupament teòric del codi RSA, que s'explicarà en aquesta memòria.

Euler també fou un estudiós de la sèrie harmònica, i emprà la definició d'aquesta per a demostrar, una vegada més, l'existència d'infinits nombres primers. El segle XVIII demostrà que la suma dels inversos dels nombres primers divergia:

$$zeta(n) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} \tag{17}$$

És a dir, que qualsevol fita que es pregués com el nombre més gran a què arribaria la suma, s'acabava superant, ja que per molt petites que siguin les quantitats sumades, *tot suma*.
Tot i això, està demostrat que, per nombres n equivalents a la magnitud de 10^{19}, la suma no arriba a les 4 unitats.

Euler també demostrà que $zeta(2)$, és a dir, que la funció harmònica per a $s = 2$, convergia i en un resultat preciós:

$$zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^3} + \cdots + \frac{1}{n^2} = \frac{\pi^2}{6} \tag{18}$$

De fet està provat que per a tot $s > 1$, la funció $zeta$ convergeix.

Euler també afirmà el que portà a Riemann a admirar tal demostració, i és que Euler demostrà que la suma infinita $zeta(s)$ es podia escriure de la següent manera:

$$\prod_{p \in P} \{(1 - p^{-s})\}^{-1} = \sum_{n=1}^{\infty} n^{-s}, on\ p\ pertany\ al\ conjunt\ de\ nombres\ primers\ P. \tag{19}$$

S'il·lustrarà aquesta propietat mitjançant un exemple numèric. Per exemple, el terme 1/54 es pot escriure mitjançant el producte d'Euler:

$$\frac{1}{54} = \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{3} = \frac{1}{2} \cdot \frac{1}{3^2}$$

Riemann quedà meravellat pels resultats que oferia la funció $zeta$, i per la seva meravellosa transformació en productes que incloïen els primers; tan fou així que actualment té la seva pròpia funció $zeta$: la funció $Zeta\ de\ Riemann$.

La funció $zeta$ havia estat estudiada per a nombres naturals, $zeta(n)$, havia estat estudiada per a nombres reals, $zeta(r)$, i Riemann volgué estudiar-la per a nombres complexos $zeta(s)$.
Riemann veié que, altra vegada, la funció no convergia per a $s = 1$, de manera que, al treballar en el pla complex, pogué ampliar analíticament la funció, de manera que pogués obtenir valors per a $s = 1$.
La continuació analítica d'aquesta funció tindria el comportament de la sèrie $zeta(s)$ per a $s > 1$, però seria diferent en la resta de nombres.

Aleshores, la funció $zeta\ de\ Riemann$, no és ben bé $zeta(s)$, sinó que ho és la continuació analítica d'aquesta.

RIEMANN

Així doncs, el 1747 Riemann se n'anà cap a Berlín, i allà tingué l'oportunitat de conèixer matemàtics com Jacobi, Steiner i Dirichlet, i d'ells aprengué conceptes que més endavant marcarien un abans i un després en el món de les matemàtiques.

Hi ha dos temes que en concret l'influïren molt:

- L'ús que Lejeune Dirichlet en feu de la funció $zeta$ d'Euler per a demostrar el Teorema de Dirichlet per a progressions aritmètiques, ja explicat anteriorment. Juntament amb la transformació de la sèrie de harmònica en el producte d'Euler.
- El desenvolupament de la teoria de variable complexa, que publicà Cauchy en forma de molts articles en una revista francesa anomenada Comptes Rendus, seguint els estudis iniciats per Euler. Riemann, a diferència de molts matemàtics

d'aleshores, quedà realment impressionat amb la nova teoria; n'estava realment segur de que era el futur de les matemàtiques.

El 1749 Riemann tornà a Gotinga per a completar la seva tesi doctoral supervisada per Gauss. En aquell mateix any, Gauss comunicà a un contacte amic seu, Johann Encke, els descobriments que havia fet respecte els nombres primers 57 anys endarrere.

En aquell moment, Riemann no estigué profundament interessat en els nombres primers, però després d'haver presentat la seva tesi doctoral, estigué treballant amb Weber, qui fou físic a la universitat de Gotinga i treballà amb Gauss per a establir una línia telegràfica entre el seu despatx i l'observatori del matemàtic.

El 1754 Riemann presentà la seva tesi doctoral davant de Gauss, qui estava molt malalt. Pogué sentir les idees que Riemann exposà, moltes d'elles relacionades amb la física i la geometria, inspirades a l'haver treballat amb Weber. Gauss pogué veure un talent meravellós i creatiu en el jove matemàtic.

Gauss morí un any més tard, i deixà una vacant a Gotinga que ocuparia Dirichlet.

Ja s'ha comentat que Riemann sentia també admiració per Dirichlet i les seves idees. Pogué aprendre d'ell a Berlín i ara novament en tenia l'oportunitat.

Riemann gaudia estant a la biblioteca, i començà a prendre interès per les hipòtesis que el seu mestre hagué fet públiques; volia poder demostrar les hipòtesis que tant de temps Gauss duia investigant.

Fou així que, Dirichlet, d'un caràcter molt menys introvertit que Riemann, l'animà sovint a passejar amb ell. Compartiren coneixements, idees i inspiracions.

El 1759 Riemann fou nombrat membre de l'Acadèmia de Berlín, i hagué d'escriure una memòria per a formalitzar-ne el seu accés. Aquesta memòria tenia menys de 10 pàgines però contemplava una nova manera de percebre els nombres primers, i marcaria un abans i un després en la història de les matemàtiques.

Veient els estudis de Gauss, Riemann es posà a estudiar la funció $\pi(x)$ i també la integral $Li(x)$. Aleshores afirmà que la probabilitat de que un nombre gran x fos primer podia ser inclús major si no només es comptessin els nombres primers fins x, sinó que també es comptessin els primers fins les potències dels nombres primers:

$$\pi(x)+\frac{1}{2}\pi\left(x^{\frac{1}{2}}\right)+\frac{1}{3}\pi\left(x^{\frac{1}{3}}\right)+\cdots+\frac{1}{n}\pi\left(x^{\frac{1}{n}}\right)\simeq Li(x) \tag{20}$$

O de manera equivalent,

$$\pi(x)+\frac{1}{2}\pi\left(\sqrt{x}\right)+\frac{1}{3}\pi\left(\sqrt[3]{x}\right)+\cdots+\frac{1}{n}\pi\left(\sqrt[n]{x}\right)\simeq Li(x) \tag{21}$$

I usant que $Li(x)\simeq\pi(x)$,

$$\pi(x)\simeq Li(x)-\frac{1}{2}Li\left(\sqrt{x}\right)-\frac{1}{3}Li\left(\sqrt[3]{x}\right)-\cdots-\frac{1}{n}Li\left(\sqrt[n]{x}\right) \tag{22}$$

El coeficient dels termes $Li(\sqrt[n]{x})$ és $\frac{1}{n}$ positiu si n és el producte d'un nombre parell de nombres primers diferents, $\frac{1}{n}$ negatiu si n és el producte d'un nombre imparell de primers diferents, i 0 si n conté factors primers múltiples.
En honor a Riemann, aquesta última sèrie d'operacions que dóna lloc a una millora de l'aproximació a $\pi(x)$, passà a denominar-se $R(x)$;

$$R(x) = Li(x) - \frac{1}{2}Li(\sqrt{x}) - \frac{1}{3}Li(\sqrt[3]{x}) - \cdots - \frac{1}{n}Li(\sqrt[n]{x}) \tag{23}$$

A la següent taula, facilitada en estudis de Don Zagier, es compara la funció $\pi(x)$ amb $R(x)$:

x	$\pi(x)$	$Li(x)$	$Distància\ entre\ \pi(x) cada\ 100.000.000\ nombres$
100.000.000	5.761.455	5.761.552	5.317.482
200.000.000	11.078.937	11.079.090	5.173.388
300.000.000	16.252.325	16.252.355	5.084.001
400.000.000	21.336.326	21.336.185	5.019.541
500.000.000	26.355.867	26.355.517	4.968.836
600.000.000	31.324.703	31.324.622	4.928.228
700.000.000	36.252.931	36.252.719	4.893.248
800.000.000	41.146.179	41.146.248	4.863.770
900.000.000	46.009.215	46.009.949	4.838.319
1.000.000.000	50.847.534	50.847.455	

Taula 4. Comparació entre $\pi(x)$ i l'expressió (14)

M'he pres la llibertat d'afegir-hi l'última columna, en què bàsicament s'aprecia quants nombres primers hi ha cada 100.000.000 nombres naturals més que l'anterior, que és el mateix que feu Gauss en el seu dia, tot i que no m'ha portat a cap observació en especial.

En la teoria matemàtica, $R(x)$ és una funció entera de la funció $\ln(x)$. Les funcions de part entera són funcions que prenen un nombre real i tornen un nombre enter proper, sigui per excés o per defecte, i es pot escriure de la següent manera:

$$R(x) = \sum_{n=1}^{\infty} \frac{1}{n \cdot zeta(n+1)} = \frac{(\ln x)^n}{n!} \tag{24}$$

No s'entrarà en el detall d'explicar teòricament com s'ha arribat a aquesta funció, però s'ha seguit la teoria de la fórmula integral de Cauchy i l'analiticitat de les funcions holomorfes.

Les funcions holomorfes són el principal objecte d'estudi de l'anàlisis complex. Són funcions que es defineixen sobre un subconjunt del pla complex i en algun punt del seu domini són diferenciables. Si només són diferenciables en algun o alguns punts, és diu que la funció és holomorfa allà. Si aquesta funció és diferenciable en tot el seu domini del pla complex, es diu que la funció és holomorfa en el seu domini. Aquesta condició, a diferència de quan una funció és diferenciable al pla real, implica que la funció en qüestió és infinitament diferenciable i pot ser escrita mitjançant una sèrie de Taylor. A més a més, una funció que sigui holomorfa en tot el pla complex rep el nom de funció entera.

Per exemple, si es digués que una funció és holomorfa en un punt a, no només significaria que la funció és diferenciable en aquell punt, sinó que és diferenciable en tot un disc obert centrat en a.

Si la funció fos holomorfa en tots els punts excepte en alguns punts concrets, s'estaria parlant d'una funció meromorfa, i aquests punts en què no seria diferenciable l'expressió, s'anomenarien pols de la funció.

També s'ha de mencionar quan una funció és analítica, doncs es necessitarà aquest coneixement per a poder seguir la memòria del treball. Així doncs, una funció analítica són operacions de derivades infinites en funció d'una variable complexa. Dit d'una altra manera, una funció $f(z)$ és analítica en un punt z_0 si aquesta és derivable en tots els punts d'algun entorn d'aquest punt. D'aquesta manera, una funció analítica en cada un dels punts d'un conjunt S, és analítica en S i, conseqüentment, és holomorfa.

És per això que $R(x)$ és una funció entera de la funció $\ln(x)$, doncs la funció de Riemann és diferenciable en tot el pla complex, i com que la funció logarítmica no és entera, ja que no està definida al pla complex, $R(x)$ n'és una part entera.

CHEBYSHEV

El 1848 Pafnuti Chevyshov, conegut com Chebyshev, fou un matemàtic rus i, entre altres coses, feu públic un estudi mitjançant mètodes analítics de la funció $\pi(x)$, el seu estudi fou el primer realitzat respecte la funció comptadora de nombres primers, mitjançant mètodes analítics.

En aquesta expressió hi apareix la funció Gamma, $gamma(x)$. Gamma és una aplicació que amplia el concepte de factorial als nombres reals i complexos. Recordem que un factorial es calcula de la següent manera:

$$n! = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot 1 \tag{25}$$

Si no es tracta diferent, el factorial no pot ser calculat per tots els nombres reals, i tampoc els complexos; i precisament per això, es va continuar analíticament la funció factorial, ampliant d'aquesta manera el domini de la funció i donant lloc a Gamma. Aquesta notació fou proposada per Adrien-Marie Legendre.

Si la part real del nombre complex és positiva, aleshores la següent integral convergeix de manera absoluta i pot ser extesa a tot el pla complex excepte als enters negatius i a 0:

$$\Gamma(x) = \int_0^e e^{-t} \cdot t^{x-1} dt \tag{26}$$

Si $n \in R+$ aleshores,

$$\Gamma(n) = (n-1)! \tag{27}$$

I, de fet, la funció Gamma es pot expressar mitjançant el producte d'Euler de la següent manera:

$$\Gamma(x) = n! = \prod_{n=1}^{\infty} [\frac{1}{1+\frac{z}{n}} \cdot \left(1+\frac{1}{n}\right)^{z}] \tag{28}$$

Chebyshev prengué logaritmes en la representació de la funció $zeta$ en producte de Euler i n'obtingué la següent expressió:

$$zeta(x) - 1 - \frac{1}{x-1} = \frac{1}{\Gamma(x)} \cdot \int_0^{\infty} \left(\frac{1}{e^t-1} - \frac{1}{t}\right) \cdot e^{-t} \cdot t^{x-1} dt \tag{29}$$

de la qual pogué deduir que si existia una fórmula per a $\pi(x)$ com la següent, havia de donar-se el cas que $a_k = (k-1)!$ per a $1 \leq k \leq r-1$:

$$\pi(N) = \sum_{k=1}^{r-1} \frac{a_k \cdot n}{(\ln N)^k} + O(\frac{N}{(lnN)^r} \tag{30}$$

El terme O davant d'una expressió significa "termes de l'ordre de".

Aquesta fórmula que trobà el matemàtic rus coincidia amb el desenvolupament asimptòtic que Gauss trobà en $Li(x)$.

RIEMANN

En la memòria que escriví per a ser acceptat com a membre de l'Acadèmia de Berlín, el 1759, Riemann estudià les expressions de Gauss, Chebyshev i les seves pròpies.

Ja s'ha comentat que aquest article de Riemann fou breu, però concís.

Riemann tractà els següents punts:

1. L'obtenció de la representació de la integral $zeta(x) = \frac{1}{\Gamma(x)} \cdot \int_0^{\infty} \left(\frac{e^{-t}}{1-e^t}\right) \cdot t^{x-1} dt$ de la funció expressada en forma del producte d'Euler $zeta(z) = \prod_{p \in P} \{(1-p^{-z})\}^{-1} = \sum_{n=1}^{\infty} n^{-z}$, quan $Re(z) > 1$.
2. La prolongació analítica d'aquesta funció a una funció meromorfa, que passaria a anomenar-se *Funció zeta de Riemann* i l'obtenció de les equacions funcionals estàndard i simètriques respecte la recta $x = \frac{1}{2}$, la qual anomenà recta crítica.
   Aquestes equacions serien:

$$zeta(z) = 2^s \cdot \pi^{s-1} \cdot sin\left(\frac{\pi \cdot z}{2}\right) \cdot \Gamma(1-z) \cdot zeta(1-z) \tag{31}$$

i

$$\pi^{-\frac{z}{2}} \cdot \Gamma\left(\frac{z}{2}\right) \cdot zeta(z) = \pi^{\frac{z-1}{2}} \cdot \Gamma\left(\frac{1-z}{2}\right) \cdot zeta(1-z). \tag{32}$$

A partir d'aquestes en va determinar els zeros trivials, que s'explicaran més endavant.

3. La representació integral del logaritme de $zeta(z)$ per a $Re(z) > 1$, que és

$$\frac{1}{z} \cdot \ln\big(zeta(z)\big) = \int_1^{\infty} Li(t)\, t - z - 1 dt, \tag{33}$$

mitjançant la funció

$$Li(x) = \pi(x) + \frac{1}{2} Li\big(\sqrt{x}\big) + \frac{1}{3} Li\big(\sqrt[3]{x}\big) + \cdots + \frac{1}{n} Li\big(\sqrt[n]{x}\big) \tag{34}$$

per la qual aconseguí demostrar que

$$\pi(x) = Li(x) + O\big(\sqrt{x}\big), per\ a\ x > 1. \tag{35}$$

4. Aconseguí expressar $Li(x)$ com una integral complexa que calculà mitjançant el mètode dels residus, localitzats en la singularitat de $\ln(z)$ en $z = 1$. També ho aconseguí per als zeros no trivials de la funció zeta de Riemann.

$$\pi(x) = li(x) - \sum_\rho li(x^\rho) - ln2 \tag{36}$$

El terme $li(x)$ és el logaritme integral de x, i el seu sumatori s'estén a tots els zeros no trivials de la funció zeta de Riemann. El terme x^ρ són els zeros de la funció Zeta de Riemann, de manera que aquests zeros contribueixen a l'aproximació de $\pi(x)$.

La diferència entre $Li(x)$ i $li(x)$ és:

$$li(x) = \int_0^x \frac{dt}{\ln(t)} \ i \quad Li(x) = \int_2^x \frac{dt}{\ln(t)} = li(x) - li(2) \tag{37) i (38}$$

4.4 Anàlisi de la hipòtesi de Riemann

Un cop donada bona part de la teoria, es pot procedir a analitzar per què és tan important i tan famosa aquesta hipòtesi.

Sintetitzant aquesta memòria, s'ha vist com, fruit de petites casualitats que feren que certs matemàtics foren en el lloc adequat en el moment adequat, i es fessin, entre moltes d'altres, les preguntes adequades, Riemann arribà a formular un dels problemes més complicats i bonics en consideració matemàtica.

Gauss, per una banda, estudià la funció $\pi(x)$, i acabà arribant a $Li(x)$. Euler, estudià la funció $zeta$ per a diversos exponents naturals diferents i n'observà també la seva convergencia, a més a més de transformar una serie infinita en un producte infinit relacionat amb els nombres primers. Dirichlet començà a introduir els nombres complexos en l'estudi de sèries. Chebyshev decidí estudiar la funció $\pi(x)$ mitjançant mètodes analítics per a ampliar el domini d'aquesta i poder tractar la funció analíticament.

I amb tot això, Riemann aconseguí relacionar $\pi(x)$ amb els zeros de l'extensió analítica de la funció real $zeta(s)$.

Riemann ho va fer de la següent manera: tingué la pretensió d'estudiar la funció $zeta(s)$ mitjançant el producte d'Euler, però aquesta funció només convergia per a valors de $s > 1$, doncs es mostra en les següents línies:

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

Per a $s = 1$ sabem que és té la serie harmònica, i que aquesta no convergeix mai;

Per a $s = 0$,

$$zeta(0) = \sum_{n=1}^{\infty} n^{-0} = 1 + \frac{1}{2^0} + \frac{1}{3^0} + \cdots + \frac{1}{n^0} = 1 + 1 + 1 + \cdots + 1 = \infty$$

tampoc convergeix;

Per a $s = -1$;

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

tenim la suma infinita dels nombres naturals, de manera que tampoc convergeix. A partir d'aquí, es pot deduir que per a tot $s \leq 1$ tindrem series que tendeixen a l'infinit.

Així doncs, per a valors menors que 1 tampoc podia estudiar el comportament d'aquesta funció. Ell volia estudiar-la sense termes infinits enmig. Aleshores decidí ampliar el domini d'aquesta funció. Ja s'havia provat anteriorment d'ampliar el conjunt de nombres naturals fins als nombres reals, però se seguia sense poder determinar amb profunda certesa el comportament de la funció $zeta$.

Fou aleshores quan, inspirat per matemàtics del seu voltant, com Dirichlet, decidí ampliar el domini i incloure-hi els nombres complexos. No obstant, seguia tenint el mateix problema: per a valors en què la component real era menor o igual que 1, no podia estudiar la funció com ell pretenia. D'aquesta manera, seguint els passos del matemàtic rus, Pafnuti Chebyshev, Riemann continuà analíticament la funció.

Ampliar la funció en qüestió analíticament, significava trobar una funció que, per a valors de $zeta(z)$ amb $z > 1$, essent z un nombre complex, la funció tingués el comportament que tenia la sèrie $zeta\,(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \cdots + \frac{1}{a^z}$ en el pla complex, i que per a les parts reals dels nombres complexos amb $z \leq 1$, aquesta funció convergís.

A hores d'ara, segueix sense semblar fàcil, però ho feu, i trobà la funció exacta, que li permetria estudiar valors de $z < 1$, però en $Re(z) = 1$ hi tindria un pol, doncs la funció tendiria a infinit, i aquest seria l'únic pol. D'entre les dues versions simètriques a la recta crítica $x = \frac{1}{2}$, la versió més famosa n'és la següent (31), i n'examinarem la composició d'aquesta expressió:

$$zeta(z) = 2^s \cdot \pi^{s-1} \cdot sin\left(\frac{\pi \cdot z}{2}\right) \cdot \Gamma(1-z) \cdot zeta(1-z),$$

Està composada per potències del nombre 2 i de π, la funció sinus, la funció gamma, sobre la qual s'ha explicat anteriorment que correspon a la continuació analítica del factorial, i per últim, composada per la mateixa funció zeta de Riemann avaluada en $1 - z$, i aquest últim apunt és molt important.

Tenint present que l'expressió (31) és vàlida com a continuació analítica de l'expressió (17) només per a valors en què la part real $s \leq 1$, validant, per exemple, en $s = -1$, és té $zeta\big(1-(-1)\big) = zeta(2)$, i coneixem aquest valor. Per tot $s < 0$ coneixerem $zeta(1-z)$.

La funció sinus es fa nul·la en 0, π i 2π radians, de manera que sempre que la part real del nostre nombre complex, z sigui un nombre parell, la funció sinus resulta 0. De manera que aquí trobem infinites arrels de la funció. Aquestes es coneixen com zeros trivials.

La funció gamma és una funció meromorfa de $z \in C$ amb pols simples en $z = -n$,

$n = 0, 1, 2, 3, 4, \ldots$, és a dir per cada nombre enter no negatiu. Si apliquem gamma a valors enters positius resulta positiva, però en canvi, si apliquem la seva extensió analítica a un nombre enter negatiu, aquesta té un pol que anul·la el l'efecte de la funció sinusoidal. D'aquesta manera, en els nombres parells enter positius, la funció zeta no s'anul·la, i com que estem parlant de nombres complexos amb part real s menor que 1, $1 - s$ mai serà negatiu, per tant, no tindrem problemes amb la funció gamma.

Riemann hagué trobat infinits zeros trivials, però volia trobar-ne de no trivials. Primerament determinà on s'havien de trobar aquests punts, i arribà a la conclusió que aquesta havien de trobar-se en la franja en què la part real del nombre complex es trobava entre 0 i 1, amb amdós inclosos.

Realment, Riemann desconeixia si allà hi trobaria algun zero, però era l'unic interval on podia haver-n'hi, justament perquè:

- Per nombres amb part real igual a 1, hi teníem una singularitat, i no es podia estudiar bé la funció,
- I com que es desconeixia el valor de $zeta(1)$, no es podia calcular $zeta(0)$, doncs retornant a l'expressió (31), es requeria del valor de $zeta(1-z)$ per a determinar el valor de $zeta(z)$.

Fou d'aquesta manera que sapigué que per $0 < Re(z) < 1$ hi podia haver zeros, i aquests no serien trivials. Així doncs, es posà a calcular punts on l'equació funcional fos 0; i en trobà.

Riemann calculà en total 6 zeros més de la funció, i observà que cada un d'ells tenia part real equivalent a $\frac{1}{2}$.

$$\rho_1 = \frac{1}{2}i \pm 14{,}134725$$
$$\rho_2 = \frac{1}{2}i \pm 21{,}022040$$
$$\rho_3 = \frac{1}{2}i \pm 25{,}010858$$

I fou aleshores quan Riemann formulà la famosíssima hipòtesi en la memòria de 1859, en la qual comentà que bé podria tractar-se d'una casualitat, però feu públiques les seves sospites respecte que tots els zeros no trivials de l'equació funcional de $zeta(z)$ es troben sobre la recta $x = \frac{1}{2}$, la recta crítica.

A partir d'aquí, Riemann ens descobrí un enigma que encara ara no ha estat resolt. Els matemàtics han calculat bilions de zeros no trivials, i absolutament tots cauen damunt la recta crítica. No obstant, ningú ha pogut demostrar que la hipòtesi sigui certa, ja que tampoc s'ha aconseguit provar que no ho sigui: es necessitaria com a mínim un zero no trivial fora d'aquesta recta, i ara per ara tampoc s'ha trobat.

Matemàtics com Hardy, Littlewood, Ramanujan i demés, han estat provant qualsevol afirmació possible respecte la hipòtesi, i de moment només s'ha aconseguit demostrar que tots els zeros no trivials estan com a mínim a una distància ε (essent aquest un nombre molt petit) de la recta crítica.

Si aquesta hipòtesi fos certa, implicaria que els nombres primers realment tenen una estructura, en certa manera ordenada. A més a més de què les arrels de la funció s'inclouen en el càlcul de l'aproximació de $\pi(x)$, i està comprovat que, a mesura que s'inclouen més arrels a l'expressió, més precisa és l'aproximació a $\pi(x)$; i es diu que les arrels fan *ballar* l'aproximació per *tocar* els nombres primers (Figura 25).

D'altra banda, de cara a la recerca de nombres primers per a l'encriptació de missatges, es facilitaria molt la tasca, doncs coneixent els zeros i l'equació funcional, es podrien determinar. Doncs no oblidem que, aquests zeros són punts on l'extensió analítica de la sèrie de potències inverses de nombres naturals s'anul·la, i aquesta sèrie està expressada en forma de producte d'Euler amb els nombres primers, gràcies al Teorema Fonamental de l'Aritmètica.

Per ultimar aquest capítol, s'afegiran representacions gràfiques estudiades mitjançant el programa $Maple$, i que seran d'ajuda al lector per a poder comprendre la matèria tractada.

En la següent imatge s'hi pot apreciar la funció $R(x)$ de Riemann en comparació amb la funció distribució dels nombres primers $\pi(x)$, des de 0 fins a 50.

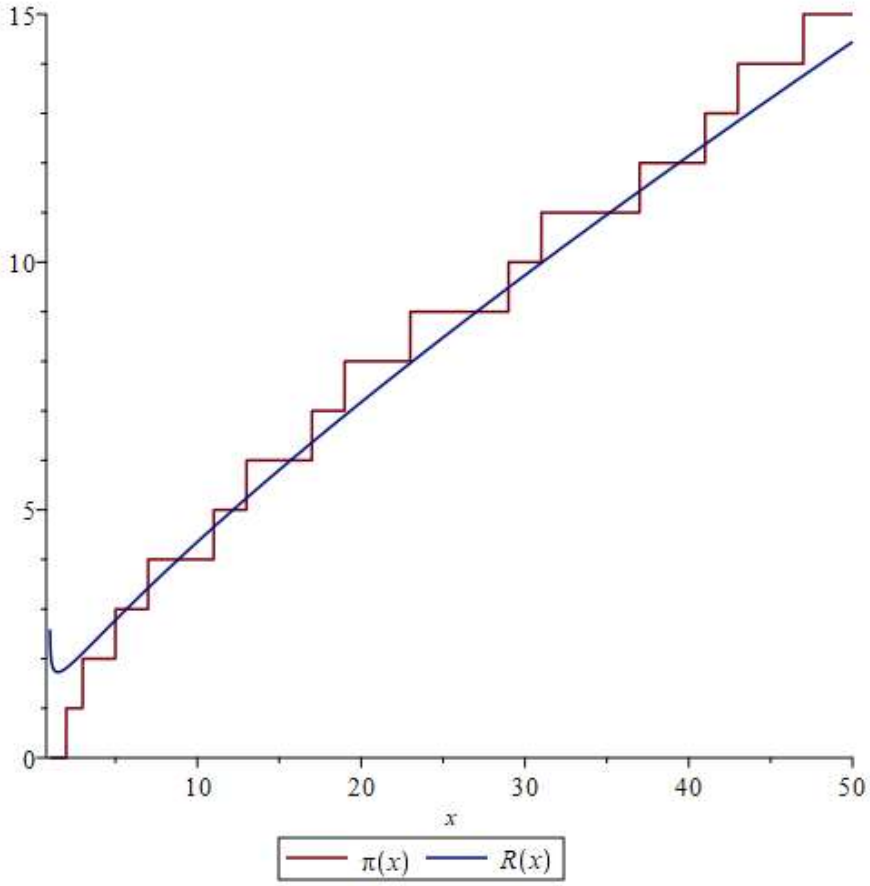

Figura 20. Comparació entre $\pi(x)$ i R(x) en [0, 50]

Gràcies a aquesta gràfica es pot veure que $R(x)$ té una tendència i un comportament adequat i proper al de la funció $\pi(x)$.

En la següent imatge s'ha estudiat, gràficament, l'error que hi ha entre les dues funcions de què es parla, per als primers 1.000 nombres naturals.

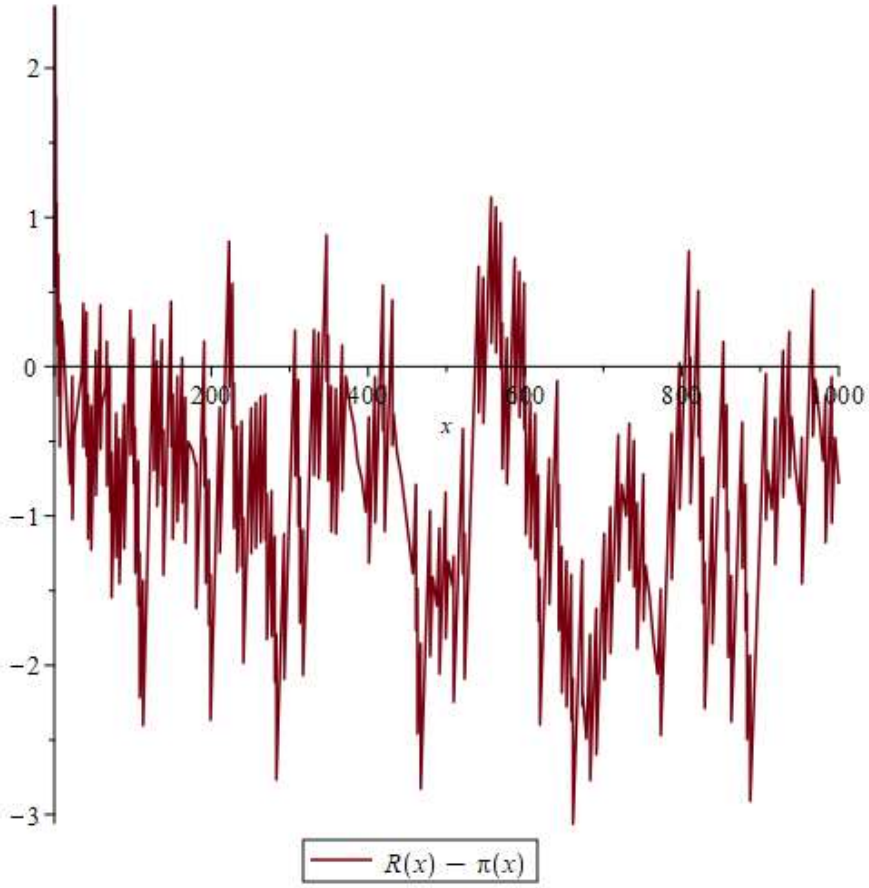

Figura 21. Gràfica d'error entre R(x) i $\pi(x)$ en [0, 1.000]

Observant l'eix vertical s'aprecia que l'error que hi ha entre ambdues funcions és realment petit, de manera que, altra vegada, es confirma que estan relacionades.
I en la següent gràfica hi tenim un resultat interessant el qual he seguit a partir de l'article de Don Zagier. En la següent figura (22) es mostra una aproximació de la funció $\pi(x)$ a partir de $R(x)$:

$$\pi(x) = R(x) - \sum_{arrels} R(x^{\rho}) \tag{39}$$

L'article ens explica que, la k-èssima aproximació a $\pi(x)$ que proporciona aquesta fórmula és la funció:

$$R_k(x) = R(x) + T_1(x) + T_2(x) + \ldots + T_k(x) \tag{40}$$

On els termes $T(x)$ representen la contribució del n-èssim parell d'arrels de la funció zeta. No s'estudien aquestes dues expressions en aquesta memòria, però s'han representat per a poder comprendre'n millor el contingut global de l'estudi dut a terme.

Les següents gràfiques s'han intentat reproduir a *Maple,* però no me n'he acabat de sortir, de manera que es comentaran les gràfiques inserides a l'article de Don Zagier:

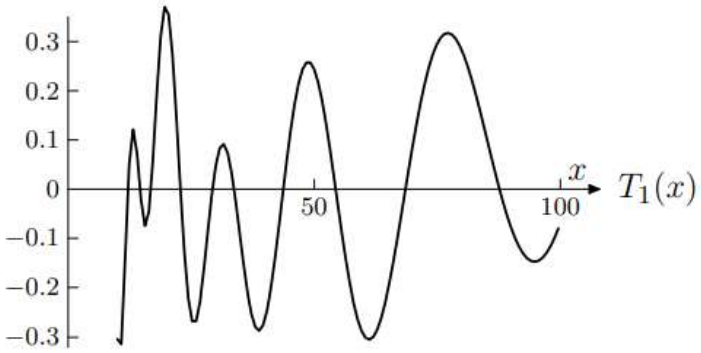

Figura 22. Gràfica de $T_1(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

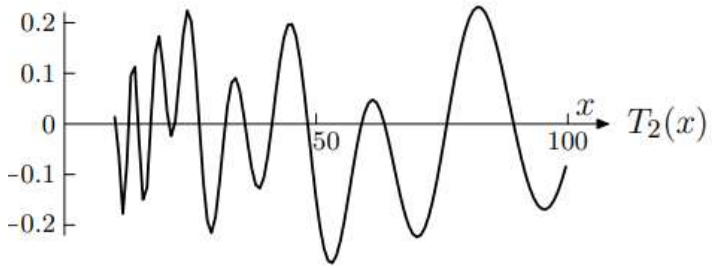

Figura 23. Gràfica de $T_2(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

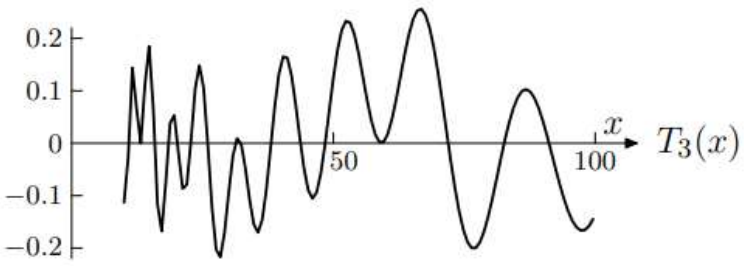

Figura 24. Gràfica de $T_2(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

Aquestes figures representen la contribució del n-èssim parell d'arrels de la funció zeta.

Aleshores, la funció $R_k(x)$, suma tots aquests termes i s'aproxima, per a x cada vegada majors, a $\pi(x)$.

Tal com s'ha mencionat, aquestes arrels contribueixen a què l'expressió (39) sigui una aproximació a $\pi(x)$ quasi bé ***exacta.*** I precisament aquesta és la relació que la hipòtesi de Riemann té respecte els nombres primers. Una relació sovint complicada de comprendre, doncs a mi m'ha costat molt, però preciosa quan es va assimilant.

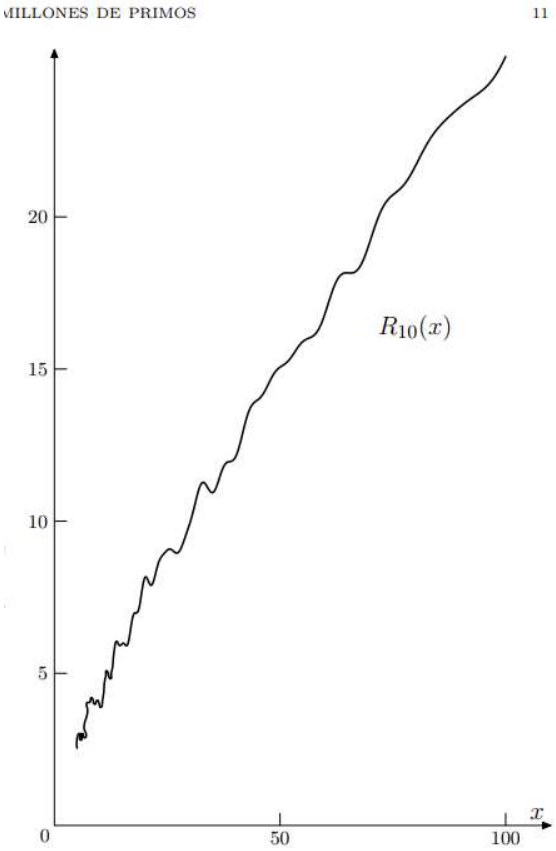

Figura 25. Gràfica de $R_{10}(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

La tendència que té per créixer aquesta funció, hauria de resultar familiar, doncs és realment molt semblant a com es desenvolupa la distribució de nombres primers.

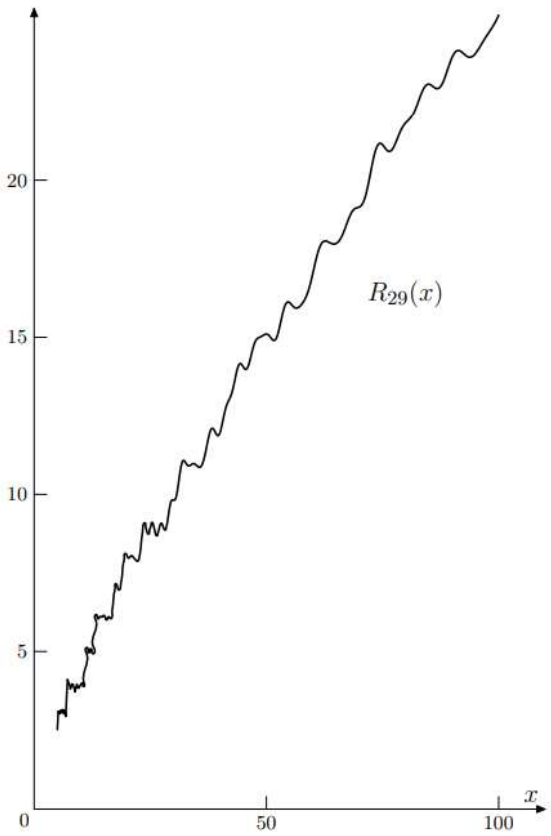

Figura 26. Gràfica de $R_{29}(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

En la figura 26 s'aprecia que, a mesura que prenem més termes $T(x)$, millor s'aproxima a $\pi(x)$, i en podrem veure la comparació a la figura 27.

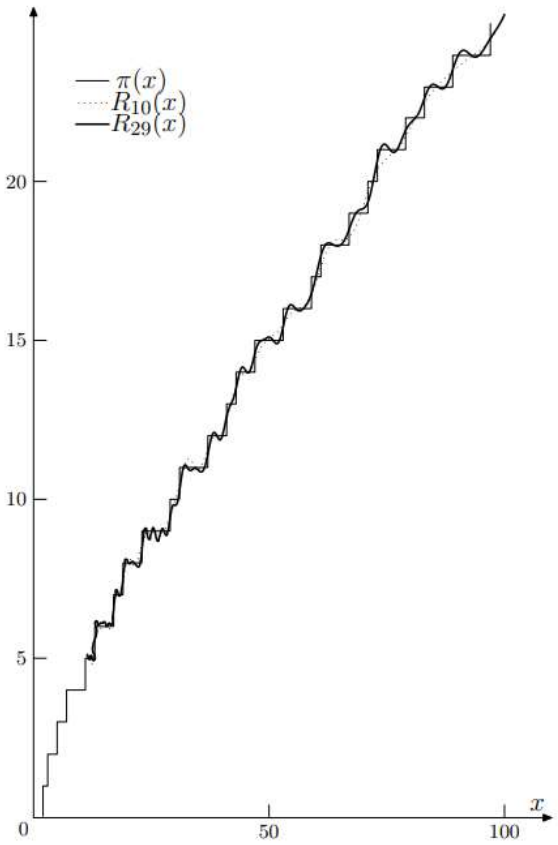

Figura 27. Gràfica de $R_{29}(x), R_{10}(x)$ i $\pi(x)$ en [0, 100] (Font: The first 50 million prime numbers, Don Zagier, febrer de 2003)

L'aproximació que ens proporciona és realment increïble, per a k majors, és a dir, a mesura que més arrels contribueixin en l'expressió, millor s'aproxima a $\pi(x)$.

5 Dels nombres primers a la informació encriptada

Des que en conec la seva existència, els nombres primers sempre m'han fascinat. No he pogut evitar mai d'intentar trobar la lògica i el sentit en ells; mentre que alhora em preguntava si tenien alguna aplicació a part de ser l'objecte dels meus estudis.

I efectivament, tenen aplicació. Molt més rellevant en el nostre dia a dia del que ningú es podria pensar: l'encriptació de missatges.
Si bé sabem que els nombres primers són diferents en propietats dels compostos, també són els nombres primers els que els generen. Són les peces que conformen els nombres.
I amb aquesta senzilla idea és com Ronald Rivest, Adi Shamir i Leonard Adleman van idear el que avui dia coneixem com codi RSA (Rivest-Shamir-Adleman, 20 de setembre de 1983).

Figura 28

Ronald Rivest

Figura 29

Adi Shamir

Figura 30

Leonard Adleman

Els creadors del codi RSA.

En termes de criptografia, el codi RSA és un algorisme criptogràfic de clau pública. Això significa que aquest compta amb dues claus, una clau pública, que pot conèixer tothom, i una clau privada, de la qual només en serà coneixedor el receptor del missatge. Així doncs, la clau pública servirà per encriptar el missatge i la clau privada per desencriptar-lo.
A aquest sistema se'l coneix com algorisme antisimètric, ja que les claus són diferents i, al desencriptar el missatge no s'empren els mateixos passos que durant l'encriptació d'aquest.
El punt fort d'aquest codi és, com es podrà veure a les pròximes línies, que s'haurà de treballar amb la descomposició factorial de nombres, on prenen importància els nombres primers, que seran prou grans com per dificultar aquesta tasca.

Així doncs, el codi RSA funciona de la següent manera. Suposem que un receptor vol rebre missatges. Aleshores, aquest receptor ha de generar dues claus, una clau pública, que servirà per a què els emissors encriptin els missatges en qüestió, i una clau privada amb la qual el receptor podrà desencriptar el missatge codificat.
La clau pública estarà conformada per un mòdul n i un exponent públic e. La clau privada estarà conformada per un exponent privat, d. D'aquesta manera, el receptor distribuirà una clau pública (n, e) als emissors i ell es quedarà amb la clau privada d per a desencriptar-los; i així qualsevol que conegués la clau pública, podria enviar missatges al receptor, però només aquest podria desencriptar-los i conèixer-ne el seu contingut. Ni tan sols els emissors podrien desencriptar els seus missatges si ho desitgessin.

Matemàticament, el que hi ha darrera és el següent procediment:

1. El receptor escull dos nombres primers molt grans: p i q;
2. Calcula $n = p \cdot q$;
3. Es calcula la funció d'Euler de n;

   Per a calcular la funció d'Euler, prèviament la introduirem.
   Sempre que $n \geq 1$, la funció d'Euler, denotada per ϕ, per a n diu la quantitat de nombres enters positius menors que n que són relativament primers amb n, i es definirà de la següent manera:

$$\phi(n) = \{k \in N: k \leq n, mcd\ (k,n) = 1\} \tag{41}$$

   Aleshores, es prova si n és primer si $(n) = n - 1$. Amb aquesta propietat ja podem calcular la funció d'Euler del nostre nombre n.

$$\phi(n) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1) \tag{42}$$

4. El receptor escull un nombre e de manera que aquest es trobi $1 < e < \phi(n)$, i que e sigui coprimer amb ϕ (n). Sovint es pren $n > \frac{n}{2}$.
5. Es realitza el càlcul de l'invers d de e mòdul $\phi\ (n)$, de manera que aquest existeix al ser e i $\phi(n)$ coprimers i queda així:

$$d \cdot e = 1 \quad mod(\phi(n)) \tag{43}$$

6. Aleshores el receptor fa públics n i e i es guarda d per a poder desxifrar els missatges que li siguin enviats. Tampoc fa públics els valors p i q tot i que aquests dos no els haurà d'usar més.
7. Els emissors transformen el missatge M que volen enviar en un nombre enter m. Per a poder convertir el missatge alfanumèric M en un nombre enter, es durà a terme el següent procediment:

   - S'encripta l'enter m mitjançant el càlcul $c = m^e\ mod\ n$ (44)
   - S'envia el terme c al receptor

8. El receptor desencripta c i obté $m = c^d\ mod\ n$ (45)
9. Descodifica m i obté el missatge M

La desencriptació és possible degut al teorema d'Euler, aplicable sota la suposició que m i n són coprimers.
Si $d \cdot e = 1 \quad mod(\phi(n))$ significa que existeix un nombre k pertanyent al grup dels enters, tal que:

$$d \cdot e = 1 + k \cdot \phi(n) \tag{46}$$

Aleshores és té que,

$$c^d = (m^e)^d = m^{e\cdot d} = m^{1+k\cdot\phi(n)} = m\left(m^{\phi(n)}\right)^k \rightarrow$$
$$aplicant\ el\ Teorema\ d'Euler \rightarrow$$
$$m \cdot 1^k = m\ mod\ n$$

(47) i (48)

Suposem que m i n són coprimers, ja que si això no fos així, significaria que m és múltiple dels primers p o q, i això és poc probable.

> I per ultimar-ne l'explicació teòrica, què impediria a un tercer usuari desencriptar els missatges que rep l'emissor i esbrinar-ne el contingut?

Per a què aquest tercer usuari pogués descodificar el missatge M, hauria de desencriptar c, i per això necessitaria conèixer d, i per a aconseguir-ho, prèviament hauria de factoritzar n per a poder conèixer els seus factors p i q. Si aquests dos últims contenen prou dígits, aquesta factorització resultaria difícil en poc temps.
Actualment, les longituds de n rauen en els 2048 dígits binaris o, equivalentment, en 617 dígits decimals, i en aplicacions reals, no es recomana que el factor més petit dels dos tingui menys de 80 dígits, ja que llavors aquest cau dins del rang on els algorismes de factorització basats en corbes el·líptiques són molt eficients i es desxifraria ràpidament el codi. Generalment es recomana que p i q siguin equivalents en grandària, és a dir, aproximadament uns 1024 dígits binaris.

Per a una millor comprensió d'aquest algoritme de codificació, es complementarà l'explicació teòrica amb un exemple senzill.

> Per exemple, suposem que el Josep vol rebre missatges de la seva companya Ivet.
> El Josep escull dos nombres primers, 11 i 23.
> En la pràctica, ja hem mencionat que haurien de ser prou grans, però en aquest exemple, no es complicarà tant.
>
> Un cop escollits, en calcula $n = p \cdot q$; $n = 1123 = 253$.
> Aplicant el Teorema d'Euler, es podrà calcular:
>
> $$\phi(n) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1),$$
>
> i aleshores $\phi(n) = \phi(11) \cdot \phi(23) = (10) \cdot (22) = 220$.
> Ara el Josep escull un nombre e, que sigui coprimer amb $(p-1)$ i $(q-1)$, aleshores aquest nombre haurà de ser coprimer amb 10 i amb 22.
> És important recordar que el terme *coprimer* es refereix a què entre el nombre e, 11 i 22, no hauria d'existir un divisor diferent d'1. Llavors, sabent que els divisors dels nostres nombres són:
>
> 10 → 1, 2, 5 i 10
> 22 → 1, 2, 11 i 22
>
> De manera que, e podria ser, per exemple 3.
> Ara al Josep li pertoca escollir un nombre d, de manera que $e \cdot d \equiv 1\ mod(\phi(n))$, això significa que el producte entre e i d, ha de resultar un nombre que al ser dividit entre 220 tingui residu 1.

Això es podria anar mirant, i hem mencionat que normalment s'escull un nombre entre $n = 253$, i $\frac{n}{2} = 126{,}5$; però si s'anés mirant quins múltiples de 220 més 1 unitat fossin divisibles entre 3, potser es trigaria molta estona.
Així doncs, aquest nombre d el podem calcular mitjançant l'invers multiplicatiu modular, i cal tenir en compte que aquest només existeix si d i 220 són coprimers. Realitzant la sèrie de càlculs pertinents, trobem que l'invers multiplicatiu modular amb mòdul 220 de 3 és 147. Matemàticament, $d = inv(3{,}220) = 147$.
Aleshores, ja tenim la clau pública: $(e, n) = (3, 253)$, i la clau privada: $(d, n) = (147, 253)$.
D'aquesta manera, el xifrat es faria:

$$C = m^e mod(n)$$

I el desxifrat:

$$C^d mod\ n = m$$

Llavors, mitjançant una taula on a cada lletra se li assigna un nombre,

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Taula 5. Taula de valors numèrics assignats a lletres.

Amb això, es xifrarà el missatge m, *PENTAGON*.

P	E	N	T	A	G	O	N
15	4	13	19	0	6	14	13

Taula 6. Taula de resultat.

El xifrat amb clau pública (3, 253):

$$m = 15\ 4\ 13\ 19\ 0\ 6\ 14\ 13$$

$153 = 3.375\ \ mod\ 253 = 86$
$43 = 64\ mod\ 253 = 64$
$133 = 2.197\ mod\ 253 = 173$
$193 = 6.859\ \ mod\ 253 = 28$
$03 = 0\ mod\ 253 = 0$
$63 = 216\ mod\ 253 = 216$
$143 = 2.744\ \ mod\ 253 = 214$
$133 = 2.197\ mod\ 253 = 173$

$$C = 86\ 64\ 173\ 28\ 0\ 216\ 214\ 173$$

C seria el missatge encriptat que rebria el Josep. Aleshores, ell al desxifrar-lo realitzaria les següents operacions:

Desxifrat amb clau privada (147, 253):

$$C = 86\ 64\ 173\ 28\ 0\ 216\ 214\ 173$$

$$86147\ mod\ 253 = 15$$
$$64147\ mod\ 253 = 4$$
$$173147\ mod\ 253 = 13$$
$$28147\ mod\ 253 = 19$$
$$0147\ mod\ 253 = 0$$
$$216147\ mod\ 253 = 6$$
$$214147\ mod\ 253 = 14$$
$$173147\ mod\ 253 = 13$$

$$m = 15\ 4\ 13\ 19\ 0\ 6\ 14\ 13$$

Es pot comprovar que és exactament el missatge inicial que hauria encriptat la Ivet. El Josep, acompanyant-se de les taules de lletres numerades, podria desxifrar el missatge. Aquest procés desconeixent d hauria estat impossible. I cal recordar, que l'ordre de magnitud dels nombres que s'empren el l'actualitat és molt major, i aquí és on recau el què d'aquest mètode i el que fa que sigui complicat de desencriptar a menys que hi intervinguin ordinadors quàntics.

6 Resum del pressupost i/o estudi de viabilitat econòmica

Al llarg de la realització d'aquest estudi, no s'ha requerit de cap inversió econòmica en cap moment, doncs el material emprat ja es posseïa.

Aquest material ha estat:

- Diversa bibliografia que ha estat facilitada per la biblioteca de la Universitat on estudio,
- Un ordinador portàtil amb processador $i7$ per a poder usar els programes informàtics pertinents sense malmetre el software,
- El programari també ha estat facilitat per la Universitat, i ha constat del programa *Maple 2021* i *Matlab*,
- També ha estat necessària una calculadora i una plantilla tipus Excel per a poder realitzar diversos càlculs còmodament,
- Internet.

Així doncs, alhora de realitzar el meu Treball de Fi de Grau no he hagut de realitzar cap inversió econòmica, però val a dir que, avui dia, hi ha molts matemàtics que encara ara es dediquen a l'estudi dels nombres primers, al desenvolupament de sistemes de codificació relacionats amb els nombres primers, el personal del *GIMPS (Great Internet Mersenne Prime Search)* qui compta amb superordinadors, els matemàtics qui estudien encara ara la hipòtesi de Riemann; i si més endavant treballés en algun d'aquests projectes, amb tota probabilitat necessitaria una inversió inicial per a cert material, però en principi, com que el meu estudi ha estat un estudi teòric, en principi no hi ha hagut abast econòmic.

7 Anàlisi i valoració de les implicacions ambientals i socials

Al llarg d'aquest estudi tampoc s'ha tingut un impacte mediambiental significant, doncs ha estat un estudi teòric.

Tot i això he usat l'ordinador durant moltes hores, de manera que aquest estudi n'és responsable de certes quantitats de CO2 emeses, entre d'altres.

En total calculo que he usat l'ordinador un total de 300 hores, dividides entre unes 18 setmanes de treball. També he estat hores llegint llibres, i l'impacte mediambiental d'aquestes hores és positiu.
Segons la Comissió Europea, un ordinador encès durant una hora, emet entre 52 i 234 grans equivalents de CO2, i considerant la mitjana entre aquests, que equival a 143 grams, el càlcul és el següent:

$300\ h \times 0{,}143\ kg = 42{,}9 kg\ de\ CO2$ emesos en les hores de treball amb ordinador considerades.

8 Conclusions

Em considero molt afortunada d'haver tingut l'oportunitat de poder dedicar el meu Treball de Fi de Grau a aprofundir els meus coneixements teòrics en el camp dels nombres primers.

Des que vaig saber que els nombres primers, aparentment, tenen una distribució aleatòria, em vaig sentir totalment encuriosida per aquesta gran incògnita. Tant fou així que vaig dedicar el meu Treball de Recerca de batxillerat també als nombres primers.
Durant l'any de redacció i investigació d'aquest treball, assistia a un programa per a estudiants als quals els agradessin les matemàtiques: Bojos per les matemàtiques.
Fou una oportunitat increïble, 24 classes diferents per a què poguéssim endinsar-nos en el món de les matemàtiques, envoltats d'estudiants apassionats com jo. I aleshores un dia després de classe, vaig veure el professor d'aquell dia amb una carpeta sota el braç i una equació escrita de la qual no n'entenia pràcticament cap terme. Naturalment vaig preguntar-li per l'equació, i ell em respongué que es tractava de l'equació més maca de totes: l'extensió analítica de la funció zeta de Riemann.

A l'haver acabat el Treball de Recerca del batxillerat, no vaig poder evitar haver-me quedat amb les ganes d'entendre la hipòtesi de Riemann: Per què era tan important?, Quina relació tenia amb els nombres primers? Com és que s'ofereixen un milió de dòlars a qui la resolgui?
I precisament ha estat l'oportunitat que he tingut.

Mentre estudiava els llibres i articles pertinents per a poder entendre la matèria necessària, vaig poder adonar-me'n que la Hipòtesi de Riemann arribà a ser formulada, en primer lloc perquè Riemann fou brillant, però en segon lloc, pogué ser concebuda gràcies a una sèrie d'esdeveniments que semblaven precioses casualitats, als meus ulls. Per exemple, el fet que el pare de Riemann tingués pensat per ell uns estudis eclesiàstics, fou clau en la història de les matemàtiques, ja que tal com s'ha mencionat, l'única universitat on s'impartien aquests estudis era a la Universitat de Gottinga, on hi treballava Gauss. A Riemann ja li agradaven les matemàtiques, i en tenia talent, però fou al conèixer Gauss quan tingué clar que volia estudiar-les. Més endavant, Riemann es mudà a Berlín, ja que a Gottinga li semblà poc estimulant, per dir-ho d'alguna manera, i allà conegué molts dels matemàtics que aportaren coneixements a l'enteniment de Riemann i que feren possible la concepció de la hipòtesi. Anys més tard de que passés tot, em semblen *casualitats* i encontres preciosos.

I bé, havent finalitzat aquest treball, reconec que la Figura 27 em sembla absolutament preciosa. Un cop he vist tot el que hi ha darrere, tot el que implica... No he pogut entendre per complet totes les matemàtiques que hi ha darrere l'enunciat de Riemann, però considero que he entès l'essencial, i això fa que admiri meravellada com Riemann donà una aproximació a $\pi(x)$ tan espectacular..., i tan bonica.

He de reconèixer que no ha estat una tasca gens fàcil per mi. En primer lloc, els meus coneixements matemàtics no es trobaven a l'altura dels coneixements necessaris per a entendre la hipòtesi de Riemann, perquè l'objectiu principal d'aquest estudi era poder entendre-la, saber-la explicar i poder pensar-la.
Me n'he adonat que encara em falta camí per a poder arribar a comprendre tot el procés que es va seguir per a arribar a formular aquesta hipòtesi. Però per ara, em sento satisfeta; la qual cosa no significa que acabi aquí la meva recerca. Tinc la intenció de seguir investigant, seguir estudiant, llegint i assistint a classes. Les matemàtiques sempre m'han fascinat, les trobo precioses, i els nombres primers són una gran peça que no puc acabar de comprendre, la curiositat que he sentit envers ells sempre ha estat significant, i mai deixarà de ser-ho.

Com a afegit, he tingut la sort de comptar amb una tutora atenta i entregada, apassionada de les matemàtiques i una gran persona que m'ha ajudat amb tot el que he necessitat.

Per ultimar les meves conclusions respecte aquest treball, el finalitzo satisfeta. M'he desesperat en certs moments quan, per més que rellegís el text, o revizualitzés la classe d'algun matemàtic, no podia entendre la matèria. Quan no podia comprendre com Riemann o Gauss o Dirichlet havien arribat a les conclusions en qüestió, com se'ls havia ocorregut tot allò? I per què jo no era capaç de comprendre ni una sola paraula del que explicaven?
Poc a poc vaig anar veient la llum. I, tot i que tal com he dit, encara em queda molt per aprendre, estic satisfeta de poder explicar què significa la hipòtesis de Riemann, quina importància té, per què no està resolta, i per què és bonica.
A més a més, he pogut experimentar amb el *Maple* i en certa manera he pogut treballar la meva intuïció matemàtica, que és una cosa que sempre he fet per pura diversió, però havent pogut dedicar hores i hores a treballar-hi, m'ha fet feliç, em quedava absorta; i penso que això és el millor que et pot passar durant un treball de recerca.

Tot i això, m'ha quedat una pregunta per respondre, i penso que probablement no tingui cap sentit matemàtic, però de totes maneres, no n'he trobat resposta.

I és que, en l'expressió (31):

$$zeta(z) = 2^s \cdot \pi^{s-1} \cdot sin\left(\frac{\pi \cdot z}{2}\right) \cdot \Gamma(1-z) \cdot zeta(1-z),$$

es necessita $zeta(1-z)$ per a determinar $zeta(z)$, relació que ens permet, per a valors negatius de z, poder calcular $zeta$. I jo m'he preguntat si el fet que la mitjana aritmètica d'ambdós valors resulti ½ ($és\ a\ dir \rightarrow \frac{z+1-z}{2} = \frac{1}{2}$) , té alguna relació amb què en $Re(z) = 1/2$ s'hi trobin tots els zeros no trivials trobats.

Suposo que no hi té res a veure, però m'ha cridat l'atenció aquest fet, i si no hi trobo resposta, probablement em passi part del temps lliure de l'estiu investigant-ho.

9 Referències

[1] Zagier, Don. 1977. “The First 50 Million Prime Numbers.” *The Mathematical Intelligencer* 1(2).

[2] Calderón, Catalina. *La Función Zeta de Riemann*.

[3] Carlos B. *Criptografía, MAPLE y RSA*.

[4] López Pellicer, Manuel. 2012. *Lección Inaugural Del Año Académico 2012-2013 Leída En La Sesión Celebrada El Día 24 de Octubre de 2012 Por El Académico Numerario Excmo. Sr. D. Manuel López Pellicer Sobre El Tema Alrededor de La Hipótesis de Riemann*. Real Academia de Ciencias Exactas, Físicas y Naturales.

[5] Thiziers, Achi Harrisson, Haba T. Zoueu, and Babri Michel. 2019. “Enhanced, Modified and Secured RSA Cryptosystem Based on N Prime Numbers and Offline Storage for Medical Data Transmission via Mobile Phone.” *International Journal of Advanced Computer Science and Applications* 10(10): 353–60.

[6] O’Shea, Donal. 2018. “Prime Numbers and the Reimann Hypothesis.” *Notices of the American Mathematical Society* 65(07).

[7] Ramos Gaytan, Jaime. 2003. 38 Miscelánea Matemática *El Teorema de Los Números Primos*.

[8] Quintilla, Joan Gimbert. 2009. “Amb Els Nombres Primers.” (7).

[9] Gustavo, Carlos X V I et al. 2012. “Sabías Que...”

[10] Aplicat, Amal, and A L E S Corbes. “Índex.”

[11] Alsina, Júlia. “Criptografia: un repte per a les matemàtiques i la física”.

[12] DU SAUTOY, Marcus. “La música de los números primos”. Barcelona: Acantilado, 2007.

[13] Universidad Complutense de Madrid. Meromorfas, Funciones. “Funciones Meromorfas. El Teorema de Los Residuos y Algunas de Sus Consecuencias 1. F.” : 1–5.

[14] Beshenov, Alexey. 2017. “Valores Especiales de La Función Zeta.” : 1–9.

[15] Galia Lisbeth Tantarico Minchola. “Teorema de los Números Primos”. Dic. 2019.

[16] Isant, Pilar Bayer. 2017. “The Riemann Hypothesis: The Great Pending Mathematical Challenge.” *Metode* 2017(8): 35–41.

9.1 Recursos en vídeos

[1] "El patrón de los números primos y la Hipótesis de Riemann": .
https://www.youtube.com/watch?v=cZJv2FKutPU

[2], [3], [4] "La Hipótesis de Riemann y lols números primos":

https://www.youtube.com/watch?v=HbDZj0eX9C0

https://www.youtube.com/watch?v=IwIqZ6hdkf4&t=175s

https://www.youtube.com/watch?v=T4FgqV0F_bY

[5] "Sobre la Hipótesis de Riemann" (Hararec Medina González):
https://www.youtube.com/watch?v=Y1WpLrNTRyg

[6] "La Hipótesis de Riemann, casi un siglo sin demostración o refutación...":
https://www.youtube.com/watch?v=y8ab70BAbXw

[7] "The Riemann Hypothesis, Explained":
https://youtu.be/zlm1aajH6gY

[8] "Visualizing the Riemann Zeta function and analytic continuation":
https://www.youtube.com/watch?v=sD0NjbwqlYw

9.2 Webgrafia

[1] Colaboradores de Wikipedia. *Teorema de los números primos* [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Teorema_de_los_n%C3%BAmeros_primos&oldid=139910570

[2] Colaboradores de Wikipedia. *Extensión analítica* [en línea]. Wikipedia, La enciclopedia libre, 2019 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Extensi%C3%B3n_anal%C3%ADtica&oldid=119543299

[3] Colaboradores de Wikipedia. *Extensión analítica* [en línea]. Wikipedia, La enciclopedia libre, 2019 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Funci%C3%B3n_anal%C3%ADtica&oldid=135923239

[4] Colaboradores de Wikipedia. *Serie convergente* [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Serie_convergente&oldid=138879427

[5] Colaboradores de Wikipedia. *Función zeta de Riemann* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Funci%C3%B3n_zeta_de_Riemann&oldid=141280090

[6] Colaboradores de Wikipedia. *Serie divergente* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Serie_divergente&oldid=144020617

[7] Colaboradores de Wikipedia. *Polo (análisis complejo)* [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 1 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Polo_(an%C3%A1lisis_complejo)&oldid=136617671

[8] Colaboradores de Wikipedia. *Raíz de una función* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Ra%C3%ADz_de_una_funci%C3%B3n&oldid=141020222

[9] Juan Arias de Reyna. "Si la Hipótesis de Riemann es cierta, será por los pelos". BLOG DEL INSTITUTO DE MATEMÁTICAS DE LA UNIVERSIDAD DE SEVILLA. 21 feb 1018.
https://institucional.us.es/blogimus/2018/02/si-la-hipotesis-de-riemann-es-cierta-sera-por-los-pelos/

[10] Colaboradores de Wikipedia. *Producto de Euler* [en línea]. Wikipedia, La enciclopedia libre, 2020 [fecha de consulta: 21 de mayo del 2022]
https://es.wikipedia.org/w/index.php?title=Producto_de_Euler&oldid=129789040

[11] Col·laboradors de la Viquipèdia. *Leonhard Euler* [en línia]. Viquipèdia, l'Enciclopèdia Lliure, 2022 [data de consulta: 5 de juny del 2022]
https://ca.wikipedia.org/w/index.php?title=Leonhard_Euler&oldid=30270213

[12] Colaboradores de Wikipedia. *Carl Friedrich Gauss* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Carl_Friedrich_Gauss&oldid=144100692

[13] Col·laboradors de la Viquipèdia. *Euclides* [en línia]. Viquipèdia, l'Enciclopèdia Lliure, 2022 [data de consulta: 29 de maig del 2022]
https://ca.wikipedia.org/w/index.php?title=Euclides&oldid=30240901

[14] Col·laboradors de la Viquipèdia. *Marin Mersenne* [en línia]. Viquipèdia, l'Enciclopèdia Lliure, 2022 [data de consulta: 23 d' abril del 2022]
https://ca.wikipedia.org/w/index.php?title=Marin_Mersenne&oldid=30088544

[15] Col·laboradors de la Viquipèdia. *Adrien-Marie Legendre* [en línia]. Viquipèdia, l'Enciclopèdia Lliure, 2022 [data de consulta: 2 d' abril del 2022]
https//ca.wikipedia.org/w/index.php?title=Adrien-Marie_Legendre&oldid=29831519

[16] Colaboradores de Wikipedia. *Peter Gustav Lejeune Dirichlet* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Peter_Gustav_Lejeune_Dirichlet&oldid=141315744

[17] Colaboradores de Wikipedia. *Pafnuti Chebyshov* [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 21 de abril del 2022]
https://es.wikipedia.org/w/index.php?title=Pafnuti_Chebyshov&oldid=136665332

[18] Colaboradores de Wikipedia. *Serie armónica (matemática)* [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 21 de junio del 2022]

https://es.wikipedia.org/w/index.php?title=Serie_arm%C3%B3nica_(matem%C3%A1tica)&oldid=136039253

[19] Colaboradores de Wikipedia. *Bernhard Riemann* [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 21 de junio del 2022]
https://es.wikipedia.org/w/index.php?title=Bernhard_Riemann&oldid=143752423

[20] Segura de León, Sergio. Mètode 2017 - 93. "Els problemes del mil·lenni" - Primavera 2017 (última consulta 14 juny 2022)
https://metode.cat/revistes-metode/monografics/els-problemes-del-millenni.html

10 Agraïments

En primer lloc vull agrair a la meva tutora, Gisela Pujol, la confiança que ha tingut en mi des del primer moment; la quantitat de recursos que m'ha proporcionat, la dedicació i la implicació que ha mostrat en mi i el meu projecte des que el vaig escollir; la seva disponibilitat sempre i la reva rapidesa en ajudar-me.

Una de les majors preocupacions que tenia respecte del treball de fi de grau, era tenir un tutor o tutora que no es mostrés compromès amb mi i el meu projecte; doncs tinc companys que no han tingut la mateixa sort que jo, i n'estic molt agraïda.

També volia agrair a la meva parella, qui per Nadal em va regalar el llibre "*La música de los números primos*" de Marcus Du Sautoy, i aquest llibre em va inspirar a buscar poder fer aquest treball.

Volia agrair a la Universitat en general, per disposar d'una biblioteca tan àmplia i que compta amb tota mena de serveis per a què l'estudiantat còmodament puguem rebre llibres que es troben a altres campus, i amb una rapidesa remarcable. Així com per a proporcionar-nos als alumnes tota mena de recursos per a poder treballar amb llicències d'estudiant.

Així doncs, finalitzo aquest grau agraïda amb la Universitat, el professorat, els companys i altres membres no docents els quals ha estat un plaer conèixer.

11 Futurs treballs, perspectiva de futur

Fa cinc anys vaig tenir l'oportunitat de començar el treball de recerca de batxillerat, i aquest tractava dels nombres primers. Els nombres primers són una part de les matemàtiques que fa temps que investigo. M'apassionen. Potser es deu a què són un *problema* sense resoldre, o potser perquè em resulten molt bonics.

Sigui com sigui, espero mai deixar d'investigar els nombres primers i els teoremes i conjectures que els envolten.

Ara per ara, he pogut entendre una hipòtesi, i la importància d'aquesta, que fa temps que tracto de comprendre, però degut a la falta de coneixements mai aconseguia entendre-la, i francament no me'n veia capaç! Com podia jo entendre una hipòtesi que ni tan sols els millors matemàtics que s'hi ha dedicat des de 1859 havien pogut resoldre! Ni se'm passava per la ment, i amb molt d'orgull, ara puc dir que l'he entesa, que sóc capaç d'explicar-la, i que espero poder ser capaç d'arribar a comprendre tota la teoria analítica que hi ha darrere l'expressió (31), ja que vaig intentar comprendre-la, però no en vaig ser capaç: hi havia molts teoremes i propietats que desconeixia, i no podia assimilar-les per complet en 4 mesos.

Així doncs, el meu objectiu de cara al futur és poder arribar des de l'expressió de la funció $zeta$ definida per tots els nombres reals majors que 1, fins a l'extensió analítica d'aquesta. D'aquesta manera n'estic segura que podré comprendre més profundament tota la teoria que enllaça aquesta hipòtesi.