Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques
Universitat de Barcelona

La conjectura feble de Goldbach. Teorema de Helfgott i verificació numèrica

---

Eduard Roure Perdices

Director: Artur Travesa i Grau
Realitzat a: Departament d'Àlgebra i Geometria. UB

Barcelona, 23 de juny de 2014

Índex

1 Introducció

Abstract

Goldbach's weak conjecture asserts that every odd integer greater than 5 is the sum of three primes. We study that problem and the proof of it presented by H. A. Helfgott and D. Platt. We focus on the circle method. Finally, we describe a computation that confirms Goldbach's weak conjecture up to 10^{28}.

El projecte

La conjectura forta de Goldbach assegura que tot nombre enter parell més gran que 2 pot ser escrit com a suma de dos nombres primers. És fàcil veure que aquesta conjectura implica l'anomenada conjectura feble de Goldbach: tot nombre enter senar més gran que 5 pot ser escrit com a suma d'exactament tres nombres primers.

En aquest treball comentarem l'origen d'aquests problemes, exposarem una cronologia parcial del seu tractament, amb alguns dels resultats més coneguts, i n'enunciarem algunes conseqüències.

Posarem de manifest les idees bàsiques i les tècniques utilitzades en l'estudi de la conjectura feble de Goldbach, centrant-nos en les de la demostració presentada recentment per H. A. Helfgott en col·laboració amb D. Platt, prestant especial atenció al mètode del cercle de Hardy-Littlewood.

Una part força extensa de la tasca realitzada consisteix en una verificació parcial de la conjectura feble de Goldbach fins a 10^{28}, que requereix del càlcul d'uns dos mil cinc-cents milions de nombres primers certificats. Veurem com portar a la pràctica tals càlculs i guardar les dades generades utilitzant els recursos informàtics de què disposem.

Conclusions i valoració personal

Fent servir un símil geomètrico-cartogràfic, aquesta memòria constitueix un mapa a escala planetària de la demostració de la conjectura feble de Goldbach presentada per Helfgott i un mapa a escala continental de la verificació numèrica d'aquesta. Estudis posteriors i més profunds haurien de permetre elaborar mapes de menor escala.

La naturalesa dels nombres primers ens ha portat per molts racons diferents de les Matemàtiques; en no imposar-nos restriccions en la forma de pensar, hem pogut gaudir del viatge i assolir els objectius que ens vam plantejar a l'inici del projecte i anar més enllà, sobretot en el camp de la computació i la manipulació de grans volums de dades numèriques.

Una gran part dels coneixements bàsics que hem hagut de fer servir han estat treballats en les assignatures de Mètodes analítics en teoria de nombres i d'Anàlisi harmònica i teoria del senyal, que són optatives de quart curs del Grau de Matemàtiques. Altres els hem hagut d'aprendre durant el desenvolupant del projecte. S'ha realitzat una tasca de recerca bibliogràfica important, consultant recursos antics i moderns, tant en format digital com en format paper.

A cada instant hem trobat la forma de seguir avançant.

Agraïments

Agraeixo a Artur Travesa i Grau que acceptés ser el tutor d'aquest treball. Li dono les gràcies per totes les hores de feina emprades, pel seu esforç i la seva dedicació, pels coneixements que ha compartit amb mi. Al principi tots necessitem algú que ens guiï; en aquest cas ell ha sigut el meu guia.

Agraeixo a Javier Soria de Diego el seu interès pel projecte i les seves respostes als meus dubtes d'anàlisi de Fourier abstracte, que van permetre iniciar l'estudi del mètode del cercle.

Agraeixo a Jaume Timoneda Salat la seva ajuda en la construcció d'una escala de dos mil cinc-cents milions dos mil nombres primers certificats. Sense ell aquesta tasca no hauria transcendit el món de les idees.

Agraeixo l'ús del clúster Hipatia del laboratori de càlcul científic de la Facultat de Matemàtiques de la Universitat de Barcelona per calcular tal escala.

Agraeixo l'ús de les aules d'informàtica de la Facultat de Matemàtiques, gestionades per Francesc Dantí Espinasa, per realitzar proves preliminars de càlcul de nombres primers.

Vull agrair a José Antonio Arenas Sánchez† el seu suport en els moments difícils.

2 Història

2.1 Origen

En una carta escrita el 7 de juny de 1742 per Christian Goldbach i dirigida a Leonhard Euler, entre altres consideracions, Goldbach va conjecturar que tot nombre més gran que 2 és suma de tres nombres primers. Euler li va respondre que aquesta conjectura es dedueix d'una conjectura que el mateix Goldbach ja li havia comentat anteriorment i que afirma que tot nombre parell és suma de dos nombres primers. Euler va escriure que creia que aquest últim resultat és cert, tot i que no ho va poder demostrar [5].

Tals cartes són l'origen de les conjectures feble i forta de Goldbach, que precisem a continuació.

Conjectura feble de Goldbach. *Tot nombre enter senar, N, $5 < N$, es pot escriure com a suma d'exactament tres nombres primers.*

Conjectura forta de Goldbach. *Tot nombre enter parell, N, $2 < N$, es pot escriure com a suma d'exactament dos nombres primers.*

És clar que la conjectura forta de Goldbach implica la conjectura feble.

2.2 Resultats sobre la conjectura feble de Goldbach

Molts són els resultats encaminats a provar la conjectura feble de Goldbach; en destaquem els següents.

- L'any 1923, Hardy i Littlewood [6] van demostrar, sota la hipòtesi generalitzada de Riemann, que tot nombre enter senar suficientment gran es pot escriure com a suma de tres nombres primers.
- L'any 1937, Vinogradov [25] va ser capaç d'eliminar la dependència de la hipòtesi de Riemann i va demostrar el mateix resultat de forma incondicional.
- L'any 1939, Borodzin, un estudiant de Vinogradov, va aconseguir precisar una fita; concretament, va demostrar que tot nombre enter senar més gran que $C = 3^{3^{15}}$ es pot escriure com a suma de tres nombres primers.
- L'any 1989, Chen i Wang [2], i l'any 2002, Liu i Wang [14], van rebaixar la fita a $C = 3.33 \cdot 10^{43000}$ i $C = 2 \cdot 10^{1346}$, respectivament.
- L'any 1997, Deshouillers, Effinger, te Riele i Zinoviev [4] van demostrar la conjectura feble de Goldbach condicionada a la hipòtesi de Riemann.
- L'any 2013, Helfgott i Platt [11, 10, 9, 12] van demostrar la conjectura feble de Goldbach de forma incondicional.

2.3 La constant de Schnirelman

L'any 1933, Schnirelman [19] va demostrar l'existència d'un nombre enter positiu k tal que tot nombre enter més gran que 1 és suma de com a molt k nombres primers. Al menor k se l'anomenà, posteriorment, constant de Schnirelman.

Notem que la conjectura feble de Goldbach implica que la constant de Schnirelman és menor o igual que 4 i la conjectura forta, que és exactament igual a 3.

Des de llavors s'han obtingut successivament fites, cada cop més fines, per al valor de la constant de Schnirelman.

- L'any 1969, Klimov va aconseguir precisar una fita per a la constant de Schnirelman: $k \leq 6 \cdot 10^9$.
- L'any 1972, Klimov, Pil′tjaĭ i Šeptickaja [13] van demostrar que $k \leq 115$.
- Més tard, Klimov va demostrar que $k \leq 55$.
- L'any 1977, Vaughan [22] i Deshouillers [3] van rebaixar la fita a $k \leq 27$ i $k \leq 26$, respectivament.
- L'any 1983, Riesel i Vaughan [17] van demostrar que $k \leq 19$.
- L'any 1995, Ramaré [16] va demostrar que tot nombre enter parell més gran que 1 és suma de com a molt 6 nombres primers. Això implica que $k \leq 7$.
- L'any 2012, Tao [20] va demostrar que tot nombre enter senar més gran que 1 és suma de com a molt 5 nombres primers. Això implica que $k \leq 6$.
- Els resultats presentats l'any 2013 per Helfgott i Platt [11, 10, 9, 12] impliquen que $k \leq 4$.

3 El mètode del cercle de Hardy-Littlewood

3.1 La gènesi

El mètode del cercle és un paradigma de la teoria analítica de nombres que tracta de l'obtenció d'estimacions de la quantitat de representacions de nombres naturals com a suma d'elements d'un conjunt donat. Sorgeix d'un article de Hardy i Ramanujan [7] on estudien la funció partició i el problema de la representació dels nombres naturals com a suma de quadrats. El mètode ha estat modificat i refinat posteriorment per Hardy i Littlewood, Vinogradov i altres.

En termes generals, donada una funció $R : \mathbb{N} \to \mathbb{N}$ es volen calcular funcions $\mathcal{P} : \mathbb{N} \to \mathbb{C}$ i $\mathcal{E} : \mathbb{N} \to \mathbb{C}$ tals que per a tot nombre natural N se satisfaci que $R(N) = \mathcal{P}(N) + \mathcal{E}(N)$, de manera que $\lim_{N\to\infty} \frac{|\mathcal{E}(N)|}{|\mathcal{P}(N)|} = 0$. La funció $\mathcal{P}$ s'anomena el terme principal i la funció $\mathcal{E}$ s'anomena el terme d'error.

En particular, existeix una constant positiva $\mathcal{C}$ tal que per a tot nombre natural $N > \mathcal{C}$ se satisfà que $|\mathcal{P}(N)| > |\mathcal{E}(N)|$. En conseqüència, per a tot $N > \mathcal{C}$, és $R(N) > 0$.

En aquestes condicions, el valor de $R(N)$ quan N és menor o igual que $\mathcal{C}$ s'ha de determinar a partir de verificacions numèriques exhaustives, sempre que la magnitud de la constant $\mathcal{C}$ ho permeti.

3.2 Integrals i sumes

Sigui $\mathscr{A} = (a_m)_m$ una successió estrictament creixent de nombres enters no negatius i considerem la funció generadora

$$F(z) = \sum_{m=1}^{\infty} z^{a_m},$$

convergent per a $z \in \mathbb{C}$ amb $|z| < 1$.

Per a tot nombre natural $s \geq 1$, els coeficients del desenvolupament de la seva potència s-èsima

$$F(z)^s = \sum_{m_1=1}^{\infty} \cdots \sum_{m_s=1}^{\infty} z^{a_{m_1}+\cdots+a_{m_s}} = \sum_{N=0}^{\infty} R_s(N) z^N,$$

proporcionen el nombre de representacions de N com a suma de s elements de $\mathscr{A}$, $R_s(N)$. Recuperem els coeficients $R_s(N)$ a partir de la fórmula integral de Cauchy.

Proposició 3.2.0.1. *Per a tot cercle $\mathscr{C}$ de centre 0 i radi ρ, $0 < \rho < 1$, és*

$$R_s(N) = \frac{1}{2\pi i} \int_{\mathscr{C}} F(z)^s z^{-N-1} dz. \ \square$$

Per al cas particular del cercle parametritzat com $\mathscr{C} = \{e^{\frac{-1}{N}} e^{2\pi i\alpha} | 0 \leq \alpha < 1\}$, amb $\rho = e^{\frac{-1}{N}}$, i escrivint $e(t) := e^{2\pi i t}$, obtenim que

$$R_s(N) = \int_0^1 \left(\sum_{m=1}^{\infty} e(a_m\alpha) e^{\frac{1}{s} - \frac{a_m}{N}} \right)^s e(-N\alpha) d\alpha.$$

Podem enunciar, doncs, el resultat següent.

Corol·lari 3.2.0.1. *Se satisfà la igualtat*

$$R_s(N) = \int_0^1 S_\eta(\alpha, N)^s e(-N\alpha) d\alpha,$$

on

$$S_\eta(\alpha, x) = \sum_{n=0}^{\infty} \mathbf{1}_{\mathscr{A}}(n) e(n\alpha) \eta\left(\frac{n}{x}\right),$$

essent $x \geq 1$*,* $\eta(t) = e^{\frac{1}{s} - t}$ *i* $\mathbf{1}_{\mathscr{A}}$ *la funció característica del conjunt* $\mathscr{A}$*.* $\square$

Comentari. Tal funció η la van proposar Hardy i Littlewood [6].

Una altra forma d'obtenir una expressió similar per a $R_s(N)$ és considerar la funció

$$f(\alpha) = \sum_{a_m \leq N} e(a_m\alpha),$$

amb $\alpha \in \mathbb{R}$, $0 \leq \alpha < 1$, i la seva potència s-èsima

$$f(\alpha)^s = \sum_{a_{m_1} \leq N} \cdots \sum_{a_{m_s} \leq N} e((a_{m_1} + \cdots + a_{m_s})\alpha) = \sum_{n=0}^{sN} R_s(n, N) e(n\alpha);$$

ara s'obté que $R_s(n, N)$ és el nombre de representacions de n com a suma de s elements de $\mathscr{A}$ menors o iguals que N. Notem que per a tot nombre natural n, $n \leq N$, se satisfà que $R_s(n, N) = R_s(n)$.

La relació d'ortogonalitat

$$\int_0^1 e(h\alpha) d\alpha = \begin{cases} 0, & \text{si } h \neq 0, \\ 1, & \text{si } h = 0, \end{cases}$$

ens permet obtenir que

$$R_s(N) = \int_0^1 f(\alpha)^s e(-N\alpha) d\alpha.$$

Podem enunciar, doncs, el resultat següent.

Corol·lari 3.2.0.2. *Se satisfà la igualtat*

$$R_s(N) = \int_0^1 S_\eta(\alpha, N)^s e(-N\alpha) d\alpha,$$

on

$$S_\eta(\alpha, x) = \sum_{n=0}^{\infty} \mathbf{1}_{\mathscr{A}}(n) e(n\alpha) \eta\left(\frac{n}{x}\right),$$

essent $x \geq 1$ *i* $\eta(t) = \mathbf{1}_{[0,1]}(t)$*.* $\square$

Comentari. Tal funció η la va proposar Vinogradov [24].

3.3 Representacions pesades

En general, el càlcul d'estimacions de $R_s(N)$ és complicat. Per a alguns problemes, és suficient provar que és diferent de zero. En aquests casos podem introduir certes funcions en els càlculs per tal de facilitar la tasca analítica.

Definició. Anomenarem pes a tota funció $\omega : [0, \infty) \to \mathbb{R}$.

Definició. Sigui $\mathscr{A} = (a_m)_m$ una successió estrictament creixent de nombres enters no negatius. Siguin s i N nombres naturals. Siguin $\omega_1, \dots, \omega_s$ pesos i posem $\omega = (\omega_1, \dots, \omega_s)$. Definim

$$R_s^\omega(N) = \sum_{a_{m_1}+\cdots+a_{m_s}=N} \omega_1(a_{m_1}) \cdots \omega_s(a_{m_s}).$$

Observacions.

• Notem que per als pesos trivials, $\omega_1 = \cdots = \omega_s = 1$, reobtenim $R_s(N) = R_s^\omega(N)$.

• Per als pesos $\omega_1(t) = \cdots = \omega_s(t) = e^{\frac{1}{s} - \frac{t}{N}}$ i $\omega_1(t) = \cdots = \omega_s(t) = \mathbf{1}_{[0,1]}(\frac{t}{N})$ també obtenim que $R_s(N) = R_s^\omega(N)$.

• Si existeixen pesos $\omega_1, \dots, \omega_s$ tals que $R_s^\omega(N) \neq 0$, aleshores algun sumand és no nul i per tant existeixen $a_{m_1}, \dots, a_{m_s}$ tals que $a_{m_1} + \cdots + a_{m_s} = N$ i aleshores $R_s(N) > 0$.

Podem obtenir una expressió integral de $R_s^\omega(N)$.

Proposició 3.3.0.2. *Sigui $\mathscr{A} = (a_m)_m$ una successió estrictament creixent de nombres enters no negatius. Siguin s i N nombres naturals. Siguin $\omega_1, \dots, \omega_s : [0, \infty) \to \mathbb{R}$ pesos tals que les sèries*

$$S_{\omega_i}(\alpha) = \sum_{n=0}^{\infty} \mathbf{1}_{\mathscr{A}}(n) \omega_i(n) e(n\alpha)$$

siguin absolutament i uniformement convergents a $[0, 1)$. Aleshores,

$$R_s^\omega(N) = \int_0^1 S_{\omega_1}(\alpha) \cdots S_{\omega_s}(\alpha) e(-N\alpha) d\alpha.$$

Demostració. El producte d'aquestes s sèries és

$$\sum_{n_1=0}^{\infty} \cdots \sum_{n_s=0}^{\infty} \mathbf{1}_{\mathscr{A}}(n_1) \cdots \mathbf{1}_{\mathscr{A}}(n_s) \omega_1(n_1) \cdots \omega_s(n_s) e((n_1 + \cdots + n_s)\alpha),$$

que és igual a

$$\sum_{N=0}^{\infty} R_s^\omega(N) e(N\alpha).$$

Per la relació d'ortogonalitat de les exponencials complexes i la convergència uniforme de les sèries, obtenim que

$$R_s^\omega(N) = \int_0^1 S_{\omega_1}(\alpha) \cdots S_{\omega_s}(\alpha) e(-N\alpha) d\alpha. \ \square$$

3.4 Els arcs

Per tal d'estudiar aquestes integrals s'introdueixen les nocions d'arcs majors i arcs menors.

Utilitzarem la versió següent del teorema d'aproximació diofantina de Dirichlet [8].

Teorema 3.4.0.1. *Sigui α un nombre real. Aleshores, per a tot nombre real X, $X \geq 1$, existeix un nombre racional $\frac{a}{q}$ tal que* $\gcd(a,q) = 1, 1 \leq q \leq X$ *i* $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qX}$. $\square$

Definició. Fixem Q i V nombres reals positius i N un nombre natural diferent de 0. Per a cada nombre racional $\frac{a}{q}$ tal que $1 \leq a \leq q \leq Q$ i $\gcd(a,q) = 1$ definim l'arc major com l'interval

$$\mathfrak{M}(a,q) = \left\{\alpha \in [0,1) : \left|\alpha - \frac{a}{q}\right| \leq \frac{QV}{qN}\right\},$$

el conjunt dels arcs majors

$$\mathfrak{M} = \bigcup_{1 \leq q \leq Q} \bigcup_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \mathfrak{M}(a,q)$$

i el conjunt dels arcs menors

$$\mathfrak{m} = [0,1) \setminus \mathfrak{M}.$$

Observació. Més endavant, N serà un nombre suficientment gran com per fer que els arcs majors siguin disjunts.

Nota. Aquesta definició, tot i ser clàssica, és merament orientativa. A la pràctica, els arcs majors es defineixen segons el problema a estudiar, i en el nostre cas caldrà ajustar-los d'acord amb la paritat dels denominadors.

Així doncs, podem escriure

$$R_s^\omega(N) = \int_{\mathfrak{M}} S_{\omega_1}(\alpha) \cdots S_{\omega_s}(\alpha) e(-N\alpha) d\alpha + \int_{\mathfrak{m}} S_{\omega_1}(\alpha) \cdots S_{\omega_s}(\alpha) e(-N\alpha) d\alpha,$$

i el problema d'estimar $R_s^\omega(N)$ s'ha desglossat en dues parts, l'estudi d'una integral sobre els arcs majors i l'estudi d'una integral sobre els arcs menors.

Tals definicions dels arcs es basen en la idea d'aproximar els nombres reals per nombres racionals amb un error controlat per poder substituir les integrals anteriors per sumes d'expressions més senzilles avaluades sobre nombres racionals afegint-hi un terme d'error suficientment petit.

En general, de la integral sobre els arcs majors se n'obté la part principal $\mathcal{P}$ i un terme que, juntament amb la integral sobre els arcs menors, constitueix la part d'error $\mathcal{E}$. Es pren $\mathcal{C}$ tal que per a tot $N > \mathcal{C}$ se satisfaci la desigualtat $|\mathcal{P}(N)| > |\mathcal{E}(N)|$.

3.5 Aplicació a la conjectura feble de Goldbach

Demostrar la conjectura feble de Goldbach és equivalent a demostrar que per a tot nombre enter senar N més gran que 5, la quantitat de representacions de N com a suma de 3 nombres primers és diferent de zero.

Mantenint les notacions introduïdes en les seccions anteriors, cal veure que per a tot nombre enter senar N més gran que 5, $R_3(N) > 0$, amb $\mathscr{A} = \mathbb{P}$, el conjunt dels nombres naturals primers, notació que mantindrem fins al final del treball.

Amb el mètode del cercle i les representacions pesades, la tasca es redueix a buscar una constant positiva $\mathcal{C}$, uns arcs majors $\mathfrak{M}$, uns arcs menors $\mathfrak{m}$ i tres pesos ω_1, ω_2 i ω_3 tals que per a tot nombre enter senar $N > \mathcal{C}$ se satisfaci que

$$R_3^\omega(N) = \int_{\mathfrak{M}} S_{\omega_1}(\alpha)S_{\omega_2}(\alpha)S_{\omega_3}(\alpha)e(-N\alpha)d\alpha + \int_{\mathfrak{m}} S_{\omega_1}(\alpha)S_{\omega_2}(\alpha)S_{\omega_3}(\alpha)e(-N\alpha)d\alpha,$$

on les sèries

$$S_{\omega_i}(\alpha) = \sum_{n=0}^{\infty} \mathbf{1}_{\mathbb{P}}(n)\omega_i(n)e(n\alpha)$$

són absolutament i uniformement convergents a $[0, 1)$ i

$$\left| \int_{\mathfrak{M}} S_{\omega_1}(\alpha)S_{\omega_2}(\alpha)S_{\omega_3}(\alpha)e(-N\alpha)d\alpha \right| > \left| \int_{\mathfrak{m}} S_{\omega_1}(\alpha)S_{\omega_2}(\alpha)S_{\omega_3}(\alpha)e(-N\alpha)d\alpha \right|.$$

Finalment caldrà estudiar, un per un, tots els nombres enters senars $N \leq \mathcal{C}$ per verificar que es poden escriure com a suma de tres nombres primers.

Observació. Per a les seves aproximacions a la prova de la conjectura, Hardy i Littlewood [6] van prendre $\omega_1(t) = \omega_2(t) = \omega_3(t) = e^{\frac{1}{3}-\frac{t}{N}} \log t$; Vinogradov [25] va prendre $\omega_1(t) = \omega_2(t) = \omega_3(t) = \mathbf{1}_{[0,1]}(\frac{t}{N}) \log t$.

3.6 Teoremes de Helfgott

En els articles [10, 9, 11] presentats per Helfgott, l'eina principal és el mètode del cercle. Podem resumir el seu treball en el teorema següent.

Teorema 3.6.0.2. *Existeixen pesos ω_1, ω_2 i ω_3 tals que per a tot nombre enter senar N més gran que 10^{27} se satisfà la desigualtat*

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ primers senars}}} \omega_1(n_1)\omega_2(n_2)\omega_3(n_3) > 0.$$

D'altra banda, a partir d'una verificació numèrica exhaustiva assistida per ordinador, Helfgott i Platt [12] demostren un resultat que implica el següent.

Teorema 3.6.0.3. *Tot nombre enter senar N més gran que 7 i més petit que 10^{27} es pot escriure com a suma d'exactament tres nombres primers senars.* □

Les demostracions d'aquests dos teoremes proporcionen una demostració completa de la conjectura feble de Goldbach, que discutirem a continuació.

4 La demostració de Helfgott

4.1 El problema

En aquesta secció exposarem un esquema de la demostració del teorema 3.6.0.2, proposada per Helfgott l'any 2013.

Com és habitual, denotarem per L^1 l'espai de Lebesgue de les funcions de valor absolut integrable a $[0, \infty)$, amb norma $|\cdot|_1$, per L^2 l'espai de Lebesgue de les funcions de quadrat integrable a $[0, \infty)$, amb norma $|\cdot|_2$, per L^∞ l'espai de Lebesgue de les funcions acotades gairebé per a tot $x \in [0, \infty)$, amb norma $|\cdot|_\infty$, i per $\mathscr{C}^2$ l'espai de les funcions reals dues vegades derivables amb continuïtat.

Considerarem la identitat següent.

Proposició 4.1.0.3. *Siguin* $\omega_1, \omega_2, \omega_3 : [0, \infty) \to \mathbb{R}$. *Sigui* N *un nombre enter senar. Aleshores,*

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ primers senars}}} \omega_1(n_1)\omega_2(n_2)\omega_3(n_3) = \sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ potències} \\ \text{de primers}}} \omega_1(n_1)\omega_2(n_2)\omega_3(n_3) - \sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2 \text{ o } n_3 \text{ és } 2 \\ \text{o potència no primera} \\ \text{d'un primer}}} \omega_1(n_1)\omega_2(n_2)\omega_3(n_3). \qquad \square$$

Per a demostrar el teorema 3.6.0.2 primer de tot s'estudia el segon sumatori amb l'aplicació del mètode del cercle i posteriorment es dóna una fita convenient del tercer sumatori, basada en certs resultats clàssics [18].

4.2 Els pesos i les etes

Recordem la definició de la funció Λ de von Mangoldt.

Definició. Sigui n un nombre natural. Definim

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n = p^k \text{ per a algun primer } p \text{ i algun enter } k \geq 1, \\ 0, & \text{altrament.} \end{cases}$$

Es defineixen els pesos següents.

Definició. Sigui x un nombre real més gran o igual que 1. Sigui n un nombre natural. Helfgott considera

$$\omega_1^x(n) = \omega_2^x(n) = \Lambda(n)\eta_+\left(\frac{n}{x}\right) \text{ i } \omega_3^x(n) = \Lambda(n)\eta_*\left(\frac{n}{x}\right),$$

on $\eta_+, \eta_* : [0, \infty) \to \mathbb{R}$ són de la forma

$$\eta_+(t) = te^{\frac{-t^2}{2}} \int_0^\infty h\left(\frac{t}{y}\right) \frac{\sin(200 \log y)}{\pi \log y} \frac{dy}{y},$$

amb

$$h(t) = \begin{cases} t^2(2-t)^3 e^{t-\frac{1}{2}}, & \text{si } t \in [0,2], \\ 0, & \text{altrament,} \end{cases}$$

i

$$\eta_*(t) = \int_0^\infty 4\max(\log 2 - |\log(2y)|, 0) \left(\frac{49t}{y}\right)^2 e^{-\frac{1}{2}\left(\frac{49t}{y}\right)^2} \frac{dy}{y}.$$

També considera la funció $\eta_\circ : [0,\infty) \to \mathbb{R}$ definida com

$$\eta_\circ(t) = \begin{cases} t^3(2-t)^3 e^{-\frac{(t-1)^2}{2}}, & \text{si } t \in [0,2], \\ 0, & \text{altrament.} \end{cases}$$

El fet que aquestes funcions siguin explícites permet demostrar, a partir de tècniques analítiques i de càlcul numèric assistit per ordinador, tots els resultats analítics i numèrics que s'exposen a continuació.

Proposició 4.2.0.4. *Se satisfà que $\eta_+ \in \mathscr{C}^2$, $\eta_\circ, \eta_+^{''} \in L^2, \eta_+, \eta_* \in L^1 \cap L^2 \cap L^\infty$, $\eta_\circ$ és tres vegades derivable llevat d'una quantitat finita de punts, $\eta_\circ^{(3)} \in L^1$ i per a tot nombre real $x \geq 1$ les sèries*

$$S_{\eta_+}(\alpha, x) = \sum_{n=0}^{\infty} \Lambda(n) e(n\alpha) \eta_+\left(\frac{n}{x}\right)$$

i

$$S_{\eta_*}(\alpha, x) = \sum_{n=0}^{\infty} \Lambda(n) e(n\alpha) \eta_*\left(\frac{n}{x}\right)$$

són absolutament i uniformement convergents a $[0,1)$. □

Lema 4.2.0.1. *Se satisfan les estimacions següents.*

$$|\eta_+|_1 \leq 1.062319, |\eta_+|_2 \leq 0.800132, |\eta_+|_\infty \leq 1.079955,$$

$$|\eta_*|_1 = \frac{\sqrt{\frac{\pi}{2}}}{49}, |\eta_*|_2^2 \leq \frac{1.77082}{49}, |\eta_*|_\infty \leq 1.414,$$

$$0.8001287 \leq |\eta_\circ|_2 \leq 0.8001288, |\eta_+ - \eta_\circ|_2 \leq 2.42942 \cdot 10^{-6}, \left|\eta_\circ^{(3)}\right|_1 \leq 32.5023. \ \square$$

4.3 El mètode del cercle

En virtut del mètode del cercle, per a tot nombre real $x \geq 1$ se satisfà la igualtat

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ potències} \\ \text{de primers}}} \omega_1^x(n_1)\omega_2^x(n_2)\omega_3^x(n_3) = \int_0^1 S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x) e(-N\alpha)\, d\alpha.$$

Definició. Siguin $\delta_0 = 8$ i $r = 150000$. Sigui N un nombre enter senar i sigui $x = \frac{N}{2+\frac{9}{196\sqrt{2\pi}}}$. Helfgott considera els arcs majors $\mathfrak{M} = \mathfrak{M}_{\delta_0,r}$, on

$$\mathfrak{M}_{\delta_0,r} = \bigcup_{\substack{q\le r\\ q \text{ senar}}} \bigcup_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left(\frac{a}{q} - \frac{\delta_0 r}{2qx}, \frac{a}{q} + \frac{\delta_0 r}{2qx}\right) \cup \bigcup_{\substack{q\le 2r\\ q \text{ parell}}} \bigcup_{\substack{1\le a\le q\\ \gcd(a,q)=1}} \left(\frac{a}{q} - \frac{\delta_0 r}{qx}, \frac{a}{q} + \frac{\delta_0 r}{qx}\right)$$

i els arcs menors $\mathfrak{m} = [0,1) \setminus \mathfrak{M}$.

Observació. Helfgott modifica la definició clàssica dels arcs majors prenent $Q = r$ si q és senar i $Q = 2r$ si q és parell.

Notació. A partir d'ara, llevat que es digui el contrari, N denotarà un nombre enter senar més gran que 10^{27}, $x = \frac{N}{2+\frac{9}{196\sqrt{2\pi}}}$, $\delta_0 = 8$ i $r = 150000$.

4.4 La integral sobre els arcs majors

4.4.1 Definicions i estimacions

Comencem l'estudi de la integral sobre els arcs majors

$$\int_{\mathfrak{M}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x) e(-N\alpha) d\alpha.$$

Definició. Definim el producte

$$C_0 = \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right),$$

on p recorre $\mathbb{P}$.

Observació. Fixat N, el segon producte és convergent i, per tant, C_0 també.

Lema 4.4.1.1. *Se satisfà la desigualtat $C_0 \ge 1.3203236$.* $\square$

Definició. Definim la integral, convergent,

$$C_{\eta_\circ,\eta_*} = \int_0^\infty \int_0^\infty \eta_\circ(t_1)\eta_\circ(t_2)\eta_* \left(\frac{N}{x} - (t_1+t_2)\right) dt_1 dt_2.$$

Aquesta integral proporciona la part principal de la integral sobre els arcs majors.

Lema 4.4.1.2. *Se satisfà la desigualtat $C_0 C_{\eta_\circ,\eta_*} \ge \frac{1.058298}{49}$.* $\square$

A partir d'ara, tractem les diferents parts d'error de la integral sobre els arcs majors.

Recordem que un caràcter de Dirichlet mòdul q, χ, és un morfisme de grups $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$. Considerarem l'extensió $\chi : \mathbb{Z} \to \mathbb{C}$, amb $\chi(n) = 0$ per a tot nombre enter n tal que $\gcd(q,n) \neq 1$.

Siguin χ, χ' dos caràcters de Dirichlet de mòduls q i q', respectivament, tals que $q' \mid q$. Si per a tot nombre enter n tal que $\gcd(q,n)=1$ és $\chi(n)=\chi'(n)$, es diu que χ' indueix χ. Es diu que un caràcter de Dirichlet és primitiu si no és induït per cap caràcter de Dirichlet de mòdul més petit.

Denotarem, com Helfgott, per χ^* l'únic caràcter primitiu de Dirichlet que indueix χ, per χ_T el caràcter primitiu trivial, que val 1 per a tot nombre enter i per χ_0 el caràcter de Dirichlet definit mòdul q que val 1 per a tot nombre enter n tal que $\gcd(q,n)=1$ i 0, altrament.

Definició. Sigui $\delta \geq 0$ un nombre real. Sigui $\eta = \eta_+, \eta_*$. Sigui χ un caràcter de Dirichlet, primitiu o no. Definim

$$S_{\eta,\chi}(\delta,x) = \sum_n \Lambda(n)\chi(n)e(n\delta)\eta\left(\frac{n}{x}\right).$$

Proposició 4.4.1.1. *Sigui χ un caràcter primitiu de Dirichlet mòdul $q \leq 2r$. Aleshores, per a tot nombre real δ tal que $|\delta| \leq \frac{8r}{q}$ se satisfà que*

$$S_{\eta_*,\chi}\left(\frac{\delta}{x},x\right) = \mathbf{1}_{\{1\}}(q)\widehat{\eta_*}(-\delta)x + \mathrm{err}_{\eta_*,\chi}(\delta,x)x,$$

on

$$|\mathrm{err}_{\eta_*,\chi}(\delta,x)| \leq \frac{4.269\cdot 10^{-14}}{q} + \frac{1}{\sqrt{x}}\left(\frac{380600}{\sqrt{q}} + 76\right). \ \square$$

Proposició 4.4.1.2. *Sigui χ un caràcter primitiu de Dirichlet mòdul q, amb $q \leq r$ si q és senar i $q \leq 2r$ si és parell. Aleshores, per a tot nombre real δ tal que $|\delta| \leq \frac{4r}{q}\gcd(q,2)$ se satisfà que*

$$S_{\eta_+,\chi}\left(\frac{\delta}{x},x\right) = \mathbf{1}_{\{1\}}(q)\widehat{\eta_+}(-\delta)x + \mathrm{err}_{\eta_+,\chi}(\delta,x)x,$$

on

$$\left|\mathrm{err}_{\eta_+,\chi}(\delta,x)\right| \leq \frac{6.18\cdot 10^{-12}}{\sqrt{q}} + \frac{1.14\cdot 10^{-10}}{q} + \frac{1}{\sqrt{x}}\left(\frac{499100}{\sqrt{q}} + 52\right). \ \square$$

Notació. Les funcions $\widehat{\eta_*}(\xi) := \int_0^\infty \eta_*(t)e(-t\xi)dt$ i $\widehat{\eta_+}(\xi) := \int_0^\infty \eta_+(t)e(-t\xi)dt$ són les transformades de Fourier de η_* i η_+, respectivament.

Observació. La demostració d'aquestes proposicions es basa en una verificació parcial de la hipòtesi generalitzada de Riemann realitzada a [10].

Definició. Sigui $\eta = \eta_+, \eta_*$. Sigui $q \leq 2r$. Definim

$$E_{\eta,r,\delta_0} = \max_{\substack{\chi \bmod q \\ q \leq \gcd(q,2)r \\ |\delta| \leq \gcd(q,2)\delta_0 \frac{r}{2q}}} \sqrt{q}\cdot|\mathrm{err}_{\eta,\chi^*}(\delta,x)| \ \text{ i } ET_{\eta,s} = \max_{|\delta|\leq s}|\,\mathrm{err}_{\eta,\chi_T}(\delta,x)|.$$

Lema 4.4.1.3. *Se satisfan les desigualtats següents.*

$$ET_{\eta_+,\frac{\delta_0 r}{2}} \leq 1.1377\cdot 10^{-8}, |\,\mathrm{err}_{\eta_*,\chi_T}(0,x)| \leq 1.71973\cdot 10^{-8},$$

$$E_{\eta_+,r,\delta_0} \leq 2.3921\cdot 10^{-8}, E_{\eta_*,r,\delta_0} \leq \frac{1.9075\cdot 10^{-8}}{49}. \ \square$$

Definició. Considerem la integral, convergent,

$$A_{\eta_+} = \frac{1}{x}\int_{\mathfrak{M}} \left|S_{\eta_+}(\alpha, x)\right|^2 d\alpha.$$

Lema 4.4.1.4. *Se satisfà la desigualtat següent.*

$$A_{\eta_+} \leq 8.7806. \ \square$$

Definició. Sigui $\eta = \eta_+, \eta_*$. Definim els termes

$$Z_{\eta,k}(x) = \frac{1}{x}\sum_n \Lambda^k(n)\eta\left(\frac{n}{x}\right),$$

$$LS_\eta(x, r) = \log r \cdot \max_{p\leq r}\sum_{v\geq 1}\eta\left(\frac{p^v}{x}\right)$$

i

$$K_{\eta,r,2} = (1+\sqrt{2r})\frac{(\log x)^2}{x}|\eta|_\infty(2\,|S_\eta(0,x)| + (1+\sqrt{2r})(\log x)^2|\eta|_\infty).$$

Lema 4.4.1.5. *Se satisfan les desigualtats següents.*

$$Z_{\eta_+^2,2}(x) \leq 0.640209x\log x, Z_{\eta_*^2,2}(x) \leq 0.0362\log x,$$

$$LS_{\eta_+}(x,r) \leq 18.57\log x + 28.39, LS_{\eta_*}(x,r) \leq 24.32\log x + 0.57,$$
$$S_{\eta_+}(0,x) \leq 1.063x, K_{\eta_+,r,2} \leq 9.71\cdot 10^{-21}x. \ \square$$

4.4.2 El teorema principal

Notació. Donades funcions f i g, essent g real positiva, escriurem que $f = O^*(g)$ si $|f| \leq g$.

La proposició següent proporciona l'estimació de la integral sobre els arcs majors.

Proposició 4.4.2.1. *La integral sobre els arcs majors*

$$\int_{\mathfrak{M}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha$$

és igual a

$$C_0 C_{\eta_\circ,\eta_*}x^2 + \left(2.82643|\eta_\circ|_2^2(2+\varepsilon_0)\cdot\varepsilon_0 + \frac{4.31004|\eta_\circ|_2^2 + 0.0012\frac{\left|\eta_\circ^{(3)}\right|_1^2}{\delta_0^5}}{r}\right)|\eta_*|_1 x^2$$

$$+ O^*\left(E_{\eta_*,r,\delta_0}A_{\eta_+} + E_{\eta_+,r,\delta_0}\cdot 1.6812(\sqrt{A_{\eta_+}} + 1.6812|\eta_+|_2)|\eta_*|_2\right)x^2$$

$$+ O^*\left(2Z_{\eta_+^2,2}(x)LS_{\eta_*}(x,r)x + 4\sqrt{Z_{\eta_+^2,2}(x)Z_{\eta_*^2,2}(x)}LS_{\eta_+}(x,r)x\right),$$

on $|\eta_+ - \eta_\circ|_2 < \varepsilon_0 |\eta_\circ|_2$*, amb* $\varepsilon_0 > 0$*. A més,*

$$\int_{\mathfrak{M}} \left|S_{\eta_+}(\alpha, x)\right|^2 d\alpha = L_{\eta_+,r,\delta_0} x + O^*\left(5.19\delta_0 x r \left(ET_{\eta_+,\frac{\delta_0 r}{2}}\left(|\eta_+|_1 + \frac{ET_{\eta_+,\frac{\delta_0 r}{2}}}{2}\right)\right)\right)$$
$$+ O^*\left(\delta_0 r (\log 2e^2 r)\left(x E^2_{\eta_+,r,\delta_0} + K_{\eta_+,r,2}\right)\right),$$

on L_{η_+,r,δ_0} *satisfà la desigualtat*

$$L_{\eta_+,r,\delta_0} \leq 2|\eta_+|_2^2 \sum_{\substack{q \leq r \\ q \text{ senar}}} \frac{\mu^2(q)}{\phi(q)}$$

i la igualtat

$$L_{\eta_+,r,\delta_0} = 2|\eta_\circ|_2^2 \sum_{\substack{q \leq r \\ q \text{ senar}}} \frac{\mu^2(q)}{\phi(q)} + O^*(\log r + 1.7)\left(2|\eta_\circ|_2 |\eta_+ - \eta_\circ|_2 + |\eta_+ - \eta_\circ|_2^2\right)$$
$$+ O^*\left(\frac{2\left|\eta_\circ^{(3)}\right|_1^2}{5\pi^6 \delta_0^5}\left(0.64787 + \frac{\log r}{4r} + \frac{0.425}{r}\right)\right).$$

Recordem que N denota un nombre enter senar més gran que 10^{27}, $x = \frac{N}{2 + \frac{9}{196\sqrt{2\pi}}}$, $\delta_0 = 8$ i $r = 150000$.

La demostració d'aquesta proposició requereix l'ús de propietats de les sumes de Gauss i de les funcions μ de Möbius, ϕ d'Euler i Λ de von Mangoldt, eines d'anàlisi matemàtica i d'anàlisi harmònica, com la desigualtat de Cauchy-Schwarz i el teorema de Plancherel i eines de càlcul numèric assistit per ordinador, com el paquet d'aritmètica entera en multiprecisió de Platt. Un esquema de la demostració és el següent:

(a) Descomposició de les sèries S_{η_+}, S_{η_*} amb la utilització de caràcters de Dirichlet; per a $\eta = \eta_+, \eta_*$ s'obté que

$$S_\eta(\alpha, x) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a)\tau(\overline{\chi}) S_{\eta,\chi^*}\left(\frac{\delta}{x}, x\right) + O^*\left(2\sum_{p|q} \log p \sum_{v \geq 1} \eta\left(\frac{p^v}{x}\right)\right),$$

on $\alpha = \frac{a}{q} + \frac{\delta}{x}, q \leq x, \gcd(a, q) = 1$ i $\tau(\chi) = \tau(\chi, 1)$, amb

$$\tau(\chi, n) = \sum_{m \,(\mathrm{mod}\, q)} \chi(m) e\left(\frac{mn}{q}\right).$$

(b) Amb tals descomposicions, obtenció d'una expressió per a $S^2_{\eta_+} S_{\eta_*} e(-N\alpha)$ i identificació del terme principal, corresponent als caràcters $\chi_1 = \chi_2 = \chi_3 = \chi_0$ del triple sumatori que hi apareix.

(c) Integració del terme principal de (b) sobre els arcs majors i separació en dues parts; la part que involucra els termes $\widehat{\eta_*}, \widehat{\eta_+}$ i la que involucra els termes $\mathrm{err}_{\eta,\chi_T}$, procedents de les sèries $S_{\eta,\chi}$.

(d) Aproximació de la sèrie η_+ per $\eta_\circ$ en L^2 amb un cert error ε_0 i càlcul de la primera part distingida en l'apartat (c). Obtenció d'una expressió que depèn de C_0 i $C_{\eta_\circ,\eta_*}$ i una altra que depèn de ε_0.

(e) Acotació de la integral de $\left|S_{\eta_+}\right|^2$ sobre els arcs majors. Apareixen els termes $K_{\eta,r,2}$, E_{η,r,δ_0}, $ET_{\eta,s}$ i L_{η,r,δ_0}.

(f) Acotació de la segona part distingida en l'apartat (c) i dels termes no principals de l'expressió de $S^2_{\eta_+}S_{\eta_*}e(-N\alpha)$ obtinguda en l'apartat (b), que depenen dels termes $\mathrm{err}_{\eta,\chi^*}$, amb la utilització de l'apartat anterior. Apareix el terme A_{η_+}.

(g) Acotació dels errors que apareixen en l'expressió de $S^2_{\eta_+}S_{\eta_*}e(-N\alpha)$ obtinguda en l'apartat (b) deguts a la descomposició per caràcters de les sèries S_{η_+}, S_{η_*}. Apareixen els termes $Z_{\eta,k}$ i LS_η. $\square$

Amb aquest teorema s'obté una expressió de la integral que volem calcular sobre els arcs majors, formada per quatre termes. El primer, la part principal, depèn fortament de N, dels nombres primers i de les funcions $\eta_\circ$ i η_*; el segon és degut a l'error en l'aproximació de η_+ per $\eta_\circ$ en L^2; el tercer és degut a les contribucions de les sèries $S_{\eta,\chi}(\frac{\delta}{x}, x)$ i el quart és degut a la descomposició per caràcters de les sèries S_{η_+}, S_{η_*}. Resta fitar el terme L_{η_+,r,δ_0}.

Lema 4.4.2.1. *Se satisfan les desigualtats següents.*

$$8.70517 \leq L_{\eta_+,r,\delta_0} \leq 8.70531. \ \square$$

Corol·lari 4.4.2.1. *Se satisfà l'estimació següent.*

$$\int_{\mathfrak{M}} S_{\eta_+}(\alpha, x)^2 S_{\eta_*}(\alpha, x) e(-N\alpha) d\alpha = C_0 C_{\eta_\circ,\eta_*} x^2 + O^*(7.881 \cdot 10^{-7} x^2). \ \square$$

El resultat anterior completa la demostració del teorema principal d'aquesta secció.

Teorema 4.4.2.1. *Per a la integral sobre els arcs majors se satisfà la desigualtat següent.*

$$\int_{\mathfrak{M}} S_{\eta_+}(\alpha, x)^2 S_{\eta_*}(\alpha, x) e(-N\alpha) d\alpha \geq \frac{1.058259}{49} x^2. \ \square$$

4.5 La integral sobre els arcs menors

4.5.1 Definicions i estimacions

Ara cal estudiar la integral sobre els arcs menors,

$$\int_{\mathfrak{m}} S_{\eta_+}(\alpha, x)^2 S_{\eta_*}(\alpha, x) e(-N\alpha) d\alpha. \tag{4.1}$$

Com en el cas dels arcs majors, que les funcions amb què es treballa siguin explícites permet demostrar, a partir de tècniques analítiques i de càlcul numèric assistit per ordinador, tots els resultats analítics i numèrics que s'exposen a continuació i que constitueixen l'estudi de la part d'error que proporciona aquesta integral.

Mantenim la notació N per a un nombre enter senar més gran que 10^{27}, $x = \frac{N}{2+\frac{9}{196\sqrt{2\pi}}}$, $\delta_0 = 8$ i $r = 150000$.

Definició. Definim la funció $\varphi : [0, \infty) \to [0, \infty)$ com $\varphi(t) = t^2 e^{-\frac{t^2}{2}}$.

Lema 4.5.1.1. *Se satisfà que* $\varphi \in L^1$ *i* $|\varphi|_1 = \sqrt{\frac{\pi}{2}}$. $\square$

Definició. Definim la integral

$$Z = \int_{\mathfrak{m}} \left|S_{\eta_+}(\alpha, x)\right|^2 |S_{\eta_*}(\alpha, x)| \, d\alpha.$$

Observació. Per fitar superiorment el mòdul de la integral sobre els arcs menors (4.1) és suficient donar una fita superior de Z.

Definició. Definim la sèrie, convergent,

$$S = \sum_{p > \sqrt{x}} (\log p)^2 \eta_+^2 \left(\frac{n}{x}\right),$$

on p recorre $\mathbb{P}$.

Lema 4.5.1.2. *Se satisfà la desigualtat* $S \leq 0.640209 x \log x - 0.021095 x$. $\square$

Definició. Definim la integral

$$J = \int_{\mathfrak{M}} \left|S_{\eta_+}(\alpha, x)\right|^2 d\alpha.$$

Lema 4.5.1.3. *Se satisfà l'estimació* $J = (8.7052 + O^*(0.0754))x$. $\square$

Definició. Sigui $K = \frac{\log(\frac{x}{49})}{2}$. Definim els termes

$$C_{\eta_+,0} = 0.7131 \int_0^\infty \frac{1}{\sqrt{t}} \left(\sup_{u \geq t} \eta_+(u)\right)^2 dt,$$

$$C_{\eta_+,1} = 0.7131 \int_1^\infty \frac{\log t}{\sqrt{t}} \left(\sup_{u \geq t} \eta_+(u)\right)^2 dt,$$

$$C_{\eta_+,2} = 0.51942 |\eta_+|_\infty^2,$$

$$C_{\varphi,2}(K) = -\int_{\frac{1}{K}}^1 \varphi(u) \log u du$$

i

$$C_{\varphi,3}(K) = \frac{1.04488}{|\varphi|_1} \int_0^{\frac{1}{K}} |\varphi(u)| du$$

Lema 4.5.1.4. *Se satisfan les desigualtats següents.*

$$C_{\eta_+,0} \leq 2.3375, C_{\eta_+,1} \leq 0.4494, C_{\eta_+,2} \leq 0.60579,$$

$$C_{\varphi,2}(K) \leq 0.093426, C_{\varphi,3}(K) \leq \frac{0.2779}{K^3}. \ \square$$

Definició. Definim el terme

$$E = ((C_{\eta_+,0} + C_{\eta_+,2})\log x + (2C_{\eta_+,0} + C_{\eta_+,1}))\sqrt{x}.$$

Lema 4.5.1.5. *Se satisfà la desigualtat* $E \leq 8.4031 \cdot 10^{-12}x$. $\square$

Definició. Definim el terme

$$T = C_{\varphi,3}(K)(S - (\sqrt{J} - \sqrt{E})^2).$$

Lema 4.5.1.6. *Se satisfà que* $T \leq 3.5776 \cdot 10^{-4}x$. $\square$

Definició. Sigui $\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right) \approx 0.5772156649$ la constant d'Euler. Definim la funció $\digamma : [3,\infty) \to \mathbb{R}$ com $\digamma(u) = e^{\gamma}\log\log u + \frac{2.50637}{\log\log u}$. En particular, $\digamma(r) \leq 5.42506$.

Definició. Definim els termes

$$R_{x,t} = 0.27125\log\left(1 + \frac{\log(4t)}{2\log\left(\frac{9x^{1/3}}{2.004t}\right)}\right) + 0.41415$$

i

$$L_t = \digamma(t)\left(\log\left(2^{\frac{7}{4}}t^{\frac{13}{4}}\right) + \frac{80}{9}\right) + \log\left(2^{\frac{16}{9}}t^{\frac{80}{9}}\right) + \frac{111}{5}.$$

Lema 4.5.1.7. *Sigui* $r_1 = \frac{3}{8}\left(\frac{x}{49}\right)^{\frac{4}{15}}$. *Se satisfan les desigualtats* $R_{\frac{x}{49},2r} \leq 0.58341$, $R_{\frac{x}{49},2r_1} \leq 0.71215$, $R_{\frac{x}{49K},2r} \leq 0.60295$, $R_{\frac{x}{49K},2r_1} \leq 0.71392$, $L_r \leq 394.316$ *i* $L_{r_1} \leq \left(1.8213\log\left(\frac{x}{49}\right) + 13.49459\right)\log\log\left(\frac{x}{49}\right)$. $\square$

Definició. Definim el terme

$$R_{x,K,\varphi,t} = R_{x,t} + \left(R_{\frac{x}{K},t} - R_{x,t}\right)\frac{C_{\varphi,2}(K)}{|\varphi|_1\log K}.$$

Lema 4.5.1.8. *Se satisfan les desigualtats* $R_{\frac{x}{49},K,\varphi,2r} \leq 0.58385$ *i* $R_{\frac{x}{49},K,\varphi,2r_1} \leq 0.71219$. $\square$

Definició. Definim el terme

$$g_{x,\varphi}(u) = \frac{(R_{x,K,\varphi,2u}\log(2u) + 0.5)\sqrt{\digamma(u)} + 2.5}{\sqrt{2u}} + \frac{L_u}{u} + 3.2K^{\frac{1}{6}}x^{\frac{-1}{6}}.$$

Lema 4.5.1.9. *Se satisfan les desigualtats següents.*

$$g_{\frac{x}{49},\varphi}(r) \leq 0.041014, g_{\frac{x}{49},\varphi}(r_1) \leq \frac{0.30782 \log\left(\frac{x}{49}\right)\sqrt{\log\log\left(\frac{x}{49}\right)}}{\left(\frac{x}{49}\right)^{\frac{2}{15}}}$$

i

$$\int_r^{r_1} \frac{g_{\frac{x}{49},\varphi}(u)}{u} du \leq 0.086918. \ \square$$

Definició. Definim el terme

$$M = g_{\frac{x}{49},\varphi}(r)\left(\frac{\log(r+1)+2.3912}{\log(\sqrt{x})+0.6294}S - (\sqrt{J}-\sqrt{E})^2\right)$$
$$+\left(\frac{2}{\log x + 1.2588}\int_r^{r_1}\frac{g_{\frac{x}{49},\varphi}(u)}{u}du + \left(\frac{7}{15} + \frac{-2.14938+\frac{8}{15}\log 49}{\log x + 1.2588}\right) g_{\frac{x}{49},\varphi}(r_1)\right) S.$$

Lema 4.5.1.10. *Se satisfà la desigualtat* $M \leq 0.77671x$. $\square$

4.5.2 El teorema principal

La proposició següent dóna una fita de la integral sobre els arcs menors i, per tant, de la part d'error que proporciona aquesta integral.

Proposició 4.5.2.1. *Per a la integral*

$$Z = \int_{\mathfrak{m}} \left|S_{\eta_+}(\alpha, x)\right|^2 \left|S_{\eta_*}(\alpha, x)\right| d\alpha$$

se satisfà la desigualtat

$$Z \leq \left(\sqrt{\frac{|\varphi|_1 x}{49}(M+T)} + \sqrt{S_{\eta_*(0,x)}E}\right)^2. \ \square$$

La demostració d'aquesta proposició es basa, d'una banda, en un estudi analític de la sèrie S_{η_*} per obtenir fites de $|S_{\eta_*}|$ sobre els arcs menors [9], de l'altra, en l'aplicació del gran garbell per a nombres primers a la sèrie S_{η_+} per obtenir fites de la norma L^2 de S_{η_+} sobre els arcs majors i, finalment, en càlculs numèrics en multiprecisió assistits per ordinador [11].

Observació. Un gran garbell és, essencialment, una desigualtat que proporciona una versió discreta de la identitat de Plancherel [11].

Resta estimar el terme $S_{\eta_*}(0, x)$.

Lema 4.5.2.1. *Se satisfà l'estimació* $S_{\eta_*}(0,x) = \left(\sqrt{\frac{\pi}{2}} + O^*(1.9075 \cdot 10^{-8})\right)\frac{x}{49}$. $\square$

Corol·lari 4.5.2.1. *Se satisfà la desigualtat* $Z \leq \frac{0.97392}{49}x^2$. $\square$

El resultat anterior completa la demostració del teorema principal d'aquesta secció.

Teorema 4.5.2.1. *Per a la integral sobre els arcs menors se satisfà la desigualtat següent.*

$$\left| \int_{\mathfrak{m}} S_{\eta_+}(\alpha, x)^2 S_{\eta_*}(\alpha, x) e(-N\alpha) d\alpha \right| \leq \frac{0.97392}{49} x^2. \ \square$$

4.6 La contribució de les potències de primers

Resta estimar la contribució de la suma

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1, n_2 \text{ o } n_3 \text{ és } 2 \\ \text{o potència no primera} \\ \text{d'un primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right),$$

que apareix a la proposició 4.1.0.3.

Notem que se satisfà la desigualtat

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1, n_2 \text{ o } n_3 \text{ és parell} \\ \text{o no primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right)$$

$$\leq 3|\eta_+|_\infty^2 |\eta_*|_\infty (\log N) \sum_{\substack{n_1 \leq N \\ n_1 = 2 \text{ o no primer}}} \Lambda(n_1) \sum_{n_2 \leq N} \Lambda(n_2).$$

També se satisfà la desigualtat següent [18].

$$\sum_{\substack{n_1 \leq N \\ n_1 = 2 \text{ o no primer}}} \Lambda(n_1) \sum_{n_2 \leq N} \Lambda(n_2) \leq 1.48169 N^{\frac{3}{2}}.$$

Així doncs, podem enunciar el resultat següent.

Corol·lari 4.6.0.2. *Se satisfà que*

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1, n_2 \text{ o } n_3 \text{ és } 2 \\ \text{o potència no primera} \\ \text{d'un primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right)$$

$$\leq \sum_{\substack{n_1+n_2+n_3=N \\ n_1, n_2 \text{ o } n_3 \text{ és parell} \\ \text{o no primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right)$$

$$\leq 7.3306 N^{\frac{3}{2}} \log N. \ \square$$

4.7 El final de la demostració

És hora de recopilar tots els resultats obtinguts i combinar-los.

Teorema. *Per a tot nombre enter senar $N > 10^{27}$ se satisfan les desigualtats*

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ primers senars}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \geq 0.000422N^2 > 0,$$

amb $x = \frac{N}{2+\frac{9}{196\sqrt{2\pi}}}$.

Demostració. La proposició 4.1.0.3 ens dóna la igualtat

$$\begin{aligned}
&\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ primers senars}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \\
&= \sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ potències} \\ \text{de primers}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \\
&- \sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2 \text{ o } n_3 \text{ és 2} \\ \text{o potència no primera} \\ \text{d'un primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right).
\end{aligned}$$

Per la proposició 3.3.0.2, se satisfà que

$$\begin{aligned}
&\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ potències} \\ \text{de primers}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \\
&= \int_0^1 S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha \\
&= \int_{\mathfrak{M}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha + \int_{\mathfrak{m}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha.
\end{aligned}$$

Pel teorema 4.4.2.1, per a la integral sobre els arcs majors se satisfà la desigualtat

$$\int_{\mathfrak{M}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha \geq \frac{1.058259}{49}x^2.$$

Pel teorema 4.5.2.1, per a la integral sobre els arcs menors se satisfà que

$$\left|\int_{\mathfrak{m}} S_{\eta_+}(\alpha,x)^2 S_{\eta_*}(\alpha,x)e(-N\alpha)d\alpha\right| \leq \frac{0.97392}{49}x^2.$$

Pel corol·lari 4.6.0.2 se satisfà la desigualtat

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2 \text{ o } n_3 \text{ és 2} \\ \text{o potència no primera} \\ \text{d'un primer}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \leq 7.3306N^{\frac{3}{2}}\log N.$$

Així doncs, obtenim que

$$\sum_{\substack{n_1+n_2+n_3=N \\ n_1,n_2,n_3 \text{ primers senars}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right)$$
$$\geq \frac{1.058259}{49}x^2 + O^*\left(\frac{0.97392}{49}x^2\right) - 7.3306N^{\frac{3}{2}}\log N \geq 0.000422N^2 > 0,$$

per ser $x = \frac{N}{2+\frac{9}{196\sqrt{2\pi}}}$ i $N > 10^{27}$. $\square$

Corol·lari. *Tot nombre enter senar $N > 10^{27}$ es pot escriure com a suma d'exactament tres nombres primers senars.* $\square$

5 Verificacions numèriques

5.1 Escales de nombres primers

El teorema de Helfgott assegura que la conjectura feble de Goldbach se satisfà per a tot nombre enter senar més gran que 10^{27}. Però la feina no s'acaba aquí; cal comprovar que la conjectura se satisfà per als nombres enters senars més grans que 5 i menors que 10^{27}.

Considerem la verificació parcial de la conjectura forta de Goldbach fins a $4 \cdot 10^{18}$ realitzada per Oliveira e Silva, Herzog i Pardi [15].

Teorema 5.1.0.2. *Tot nombre enter parell, N, $2 < N \leq 4 \cdot 10^{18}$, es pot escriure com a suma d'exactament dos nombres primers.* $\square$

L'hem feta servir per obtenir una comprovació de la conjectura feble de Goldbach similar a la que han obtingut Helfgott i Platt [12] i que alhora proporciona una verificació independent d'aquest càlcul.

Aquesta comprovació es basa en un resultat que podem escriure de la forma següent.

Teorema 5.1.0.3. *Sigui T un nombre natural més gran o igual que $4 \cdot 10^{18}$ per al qual existeixen un nombre natural $r > 0$ i nombres primers senars $4 < \varpi_0 < \cdots < \varpi_k < \cdots < \varpi_r < T$ tals que per a tot $0 \leq k < r$, $4 < \varpi_{k+1} - \varpi_k \leq 4 \cdot 10^{18} - 4$ i $4 < T - \varpi_r \leq 4 \cdot 10^{18} - 4$. Aleshores, tot nombre enter senar, N, més gran que $\varpi_0 + 4$ i menor que T es pot escriure com a suma d'exactament tres nombres primers senars, essent un d'aquests igual a algun dels ϖ_k.*

Observació. Com que la successió de nombres primers conté llacunes tan grans com vulguem, en particular de longitud més gran que $4 \cdot 10^{18} - 4$, per a l'existència de la successió $(\varpi_k)_k$ el valor de T no pot ser arbitrari. No obstant, veurem que per a $T \leq 10^{28}$ podem trobar successions de nombres primers amb les propietats desitjades.

Demostració. Notem que si un nombre parell més gran que 4 és suma de dos nombres primers, aleshores aquests són senars.

Ara, sigui N un nombre enter senar, $\varpi_0 + 4 < N < T$. Es poden donar diversos casos.

(a) Suposem que existeix $0 < k \leq r$ tal que $N = \varpi_k$, $N = \varpi_k + 2$ o $N = \varpi_k + 4$. Aleshores $4 < N - \varpi_{k-1} \leq 4 \cdot 10^{18} - 4$, $6 < N - \varpi_{k-1} \leq 4 \cdot 10^{18} - 2$ o $8 < N - \varpi_{k-1} \leq 4 \cdot 10^{18}$, respectivament.

(b) Suposem que existeix $0 \leq k < r$ tal que $\varpi_k + 4 < N < \varpi_{k+1}$. Aleshores $4 < N - \varpi_k < \varpi_{k+1} - \varpi_k \leq 4 \cdot 10^{18} - 4$.

(c) Suposem que $\varpi_r + 4 < N < T$. Aleshores $4 < N - \varpi_r < T - \varpi_r \leq 4 \cdot 10^{18} - 4$.

En virtut del teorema 5.1.0.2, en tots els casos existeixen un nombre enter k, $0 \leq k \leq r$, i nombres primers senars p i q tals que $N = p + q + \varpi_k$. $\square$

5.2 Algorítmica

En tenir present el teorema anterior, la tasca pendent es redueix a la construcció d'una escala de nombres primers senars per als quals se satisfacin les condicions especificades.

Tot i que és suficient que l'escala arribi fins a 10^{27}, nosaltres arribem fins a 10^{28}.

Mostrem en pseudocodi l'algoritme que hem fet servir per construir l'escala, i que parteix de considerar $\varpi_0 = 7$ i calcular, per a tot $k > 0$, ϖ_k com l'anterior nombre primer a $\varpi_{k-1} + 4 \cdot 10^{18} - 4$.

Com es habitual, donat un nombre real $x \geq 0$ denotem per $\pi(x)$ la quantitat de nombres primers menors o iguals que x i denotem per p_k el k-èsim nombre natural primer; així, per exemple, $p_{\pi(q+n)}$ és $q + n$ si aquest nombre és primer i és l'anterior nombre primer a $q + n$ si aquest nombre no és primer.

`INICI`

`Pas 1:` `Fer` $q = 7$, $d = 0$, $f = 10^{28}$, $n = 4 \cdot 10^{18} - 4$ `i` $m = 1$.

`Pas 2:` `Si` $q > f$, `acabar.`

`Pas 3:` `Si` $q \leq f$, `guardar` q `i fer` $d = p_{\pi(q+n)} - q$ `i` $m \leftarrow m + 1$.

`Pas 4:` `Si` $d \leq 4$, `error i acabar.`

`Pas 5:` `Si` $d > 4$, `fer` $q \leftarrow q + d$ `i tornar al pas 2.`

`FINAL`

Observació. La construcció només hauria pogut fallar si no existís un nombre primer a distància més gran que 4 i menor que $4 \cdot 10^{18} - 4$ de l'últim nombre primer trobat; això ho controla el pas 4.

Si bé Helfgott i Platt [12] utilitzen certes dreceres matemàtiques i tècniques de computació avançada per realitzar la verificació que ells fan fins a $8.875 \cdot 10^{30}$, nosaltres ho farem amb tècniques elementals. Per arribar a 10^{28} ens cal calcular uns dos mil cinc-cents milions de nombres primers.

Els càlculs involucren nombres de fins a 28 xifres decimals i per dur-los a terme utilitzarem el programari lliure *PARI-GP*.

Algunes proves preliminars fetes en un ordinador de sobretaula concret suggereixen que per construir i guardar la llista completa necessitaríem 10^4 hores de càlcul (més d'un any) i 64GB de memòria.

Per solucionar el problema del temps ens hem plantejat una paral·lelització de la tasca. En comptes de calcular tota l'escala de cop, l'hem calculada a trossos. Partim l'interval $[0, 10^{28})$ en intervals de la forma $[K \times 10^{25}, (K+1) \times 10^{25})$, amb $0 \leq K < 10^3$, i en cadascun d'aquests hi cerquem nombres primers per als quals se satisfacin les condicions especificades en el teorema 5.1.0.3. Cada interval ha estat analitzat en un nucli diferent i al final s'ha comprovat que tots encaixen be, és a dir, que l'escala completa satisfà les condicions desitjades. Per assegurar-nos-en, per a cada interval hem calculat dos nombres primers que no hi pertanyen, un que s'escapa per sota i l'altre que s'escapa per sobre. Per al cas $K = 0$ hem pres $\varpi_0 = 7$.

Per solucionar el problema de la memòria no hem guardat la llista completa, només certs fragments d'informació que han permès recuperar-la fàcilment. Notem que, fixat el valor de ϖ_0, per a tot $k > 0$ podem escriure $\varpi_k = \varpi_{k-1} + 4 \cdot 10^{18} - 4 - \varepsilon_k$. Així doncs, per a cada interval analitzat hem guardat el primer nombre primer escollit i els valors d'ε_k que han anat apareixent. La utilització d'aquest mètode ha permès reduir els 64GB que hauríem necessitat a només 9.4GB (sense comprimir, 2.6GB comprimits en format ZIP).

Per a això cal modificar lleugerament l'algoritme plantejat anteriorment.

`INICI`

`Pas 1:` `Llegir` K `i fer` $d = 0$, $f = (K+1) \times 10^{25}$, $n = 4 \cdot 10^{18} - 4$ `i` $m = 1$.

`Pas 2:` `Si` $K = 0$, `fer` $q = 7$.

`Pas 3:` `Si` $K > 0$, `fer` $q = p_{\pi(K \times 10^{25})}$.

`Pas 4:` `Guardar` q.

`Pas 5:` `Si` $q \geq f$, `acabar`.

`Pas 6:` `Si` $q < f$, `fer` $d = p_{\pi(q+n)} - q$.

`Pas 7:` `Si` $d \leq 4$, `error i acabar`.

`Pas 8:` `Si` $d > 4$, `guardar` $n - d$, `fer` $q \leftarrow q + d$, $m \leftarrow m + 1$ `i tornar al pas` 5.

`FINAL`

5.3 Resultats empírics

Per al càlcul de la llista s'han utilitzat els 640 nuclis del clúster Hipatia a la Facultat de Matemàtiques de la Universitat de Barcelona i 3 nuclis d'un ordinador portàtil amb processador Intel(R) Core(TM) i3. S'han necessitat unes 4470 hores de CPU per calcular-la i 9 hores més per comprovar que tots els trossos d'escala encaixen bé. Per a la comprovació que els 1000 blocs de la llista encaixen bé ha estat suficient l'ús del programari *Mathematica 7.0*.

Per trobar els nombres primers desitjats, els $p_{\pi(q+n)}$, s'ha utilitzat la funció *precprime* de *PARI* i tots ells han estat certificats amb la funció *isprime*. Alguns nombres primers han requerit de molta memòria per ser certificats i ha fet falta executar *PARI-GP* amb un stack de 64MB [1]. Aquest és el cas, per exemple, per al nombre primer 4050332007999999999994861099.

En conclusió, s'han calculat i certificat dos mil cinc-cents milions dos mil nombres primers i podem resumir els càlculs en els resultats següents.

Teorema 5.3.0.4. *Tot nombre enter senar, N, $5 < N < 10^{28}$, es pot escriure com a suma d'exactament tres nombres primers.* □

Corol·lari 5.3.0.3. *Tot nombre enter senar, N, $7 < N < 10^{28}$, es pot escriure com a suma d'exactament tres nombres primers senars.* □

5.4 Més enllà

Tots els nombres primers que formen l'escala que hem calculat han estat certificats i aquesta és la tasca que ha portat més temps. Els certificats generats no s'han guardat per qüestions de memòria tot i que es poden tornar a calcular sense més dificultat que el temps de càlcul, que seria del mateix ordre que el que ha tardat la construcció de la llista completa.

Així doncs, ens hem preguntat si és possible calcular una altra escala de nombres primers de forma que un únic certificat ens serveixi per certificar la primeritat de tots els esglaons. A continuació discutim la resposta, que és afirmativa.

Utilitzem el criteri de primeritat següent [21].

Teorema 5.4.0.5. *Sigui $N > 3$ un nombre enter senar. N és primer si, i només si, existeix un nombre enter g, $2 \leq g \leq N-2$, per al qual se satisfà que $g^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ i que per a tot divisor primer ℓ de $N-1$, $\ell \neq 2$, $g^{\frac{N-1}{\ell}} \not\equiv 1 \pmod{N}$.* □

La solució que proposem és construir una llista de nombres naturals senars ϖ per als quals 2 sigui un element d'ordre multiplicatiu $\varpi - 1$. Tals nombres són primers i $(N, g \in (\mathbb{Z}/N\mathbb{Z})^*, \mathrm{o}(g)) = (\varpi, 2, \varpi - 1)$ constitueix un certificat de primeritat vàlid per a tots ells i no cal calcular-lo de nou.

Per tal d'agilitzar la tasca i descartar nombres que no compleixen les propietats desitjades només analitzarem nombres enters senars N tals que $N \equiv 3 \pmod{8}$ i $2^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Recordem que si N és un nombre primer senar i 2 és arrel primitiva mòdul N, aleshores 2 no és un quadrat mòdul N i per tant, del càlcul del símbol de Jacobi obtenim que $\left(\frac{2}{N}\right) = -1$, d'on $N \equiv \pm 3 \pmod{8}$; i, pel criteri d'Euler, $2^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

El teorema 5.4.0.5 ens permet elaborar l'algoritme següent per construir la nova escala de nombres primers. Com en l'algoritme anterior, es paral·lelitza la tasca i es guarda informació parcial dels nombres primers que es van calculant.

`INICI`

`Pas 1:` Llegir K i fer $d = 0$, $f = (K+1) \times 10^{25}$, $n = 4 \cdot 10^{18} - 8$ i $m = 0$.

`Pas 2:` Si $K = 0$, fer $q = 11$.

`Pas 3:` Si $K > 0$, fer $q = K \times 10^{25} - 5$.

`Pas 4:` Mentre $2^{\frac{q-1}{2}} \not\equiv -1 \pmod{q}$, fer $q \leftarrow q - 8$. Si $m > 0$ i $q \leq p$, error i acabar.

`Pas 5:` Calcular els divisors primers $\ell_1 \leq \cdots \leq \ell_s$ de $q-1$ i fer $i = 2$.

`Pas 6:` Si $i > s$ i $m = 0$, fer $m = 1$, guardar q i anar al pas 13.

`Pas 7:` Si $i > s$ i $m > 0$, anar al pas 10.

`Pas 8:` Si $2^{\frac{q-1}{\ell_i}} \equiv 1 \pmod{q}$, fer $q \leftarrow q - 8$ i tornar al pas 4.

`Pas 9:` Fer $i \leftarrow i + 1$ i tornar al pas 6.

```
Pas 10:   Fer d = q − p.
Pas 11:   Si d ≤ 4, error i acabar.
Pas 12:   Si d > 4, guardar (n−d)/8, fer q = p + d, m ← m + 1.
Pas 13:   Si q ≥ f, acabar.
Pas 14:   Si q < f, fer p = q, q = p + n i tornar al pas 4.
FINAL
```

Observació. El pas 5 és possible perquè els nombres amb què treballem són petits. En general, el problema de la factorització de nombres enters no és trivial, però en aquest cas és factible, ja que tots els nombres que apareixen són menors que 10^{28}.

Observació. De la igualtat $\varpi_k = \varpi_{k-1} + 4 \cdot 10^{18} - 8 - \varepsilon_k$ i del fet que $\varpi_k \equiv \varpi_{k-1} \equiv 3 \pmod 8$ s'obté que $\varepsilon_k \equiv 0 \pmod 8$, així que per a cada nombre primer trobat només guardem $\frac{\varepsilon_k}{8}$. Per exemple, els tres primers nombres primers del primer bloc de la llista són $\varpi_0 = 11, \varpi_1 = 3999999999999999883$ i $\varpi_2 = 7999999999999999811$, i nosaltres guardem els valors $\varpi_0 = 11, \frac{\varepsilon_1}{8} = 15$ i $\frac{\varepsilon_2}{8} = 8$; els tres primers nombres primers de l'últim bloc de la llista són $\varpi_0 = 989999999999999999999999827, \varpi_1 = 990000003999999999999999203$ i $\varpi_2 = 990000007999999999999998899$, i nosaltres guardem els valors $\varpi_0 = 989999999999999999999999827, \frac{\varepsilon_1}{8} = 77$ i $\frac{\varepsilon_2}{8} = 37$. Amb aquest mètode, 1GB de memòria és suficient per emmagatzemar les dades calculades, en comptes dels 7GB que farien falta si guardéssim tots els nombres primers calculats.

En aquest cas prendrem $0 \leq K < 100$ per arribar fins a 10^{27}. Notem que la construcció només hauria pogut fallar si no existís un nombre primer a distància més gran que 4 i menor que $4 \cdot 10^{18} - 8$ de l'últim nombre primer trobat amb les propietats desitjades, i ho detectaríem en els passos 4 i 11 de l'algoritme anterior.

El càlcul de la nova llista s'ha realitzat utilitzant 3 nuclis d'un ordinador portàtil amb processador Intel(R) Core(TM) i3. S'han necessitat unes 796 hores de CPU per calcular-la i una hora més per comprovar que tots els trossos d'escala encaixen be. Tots els càlculs s'ha dut a terme amb el programari *Mathematica 7.0*.

En conclusió, s'han calculat i certificat dos-cents cinquanta milions dos-cents nombres primers i podem resumir els càlculs en els resultats següents.

Teorema 5.4.0.6. *Per a tot nombre enter senar, N, $5 < N < 10^{27}$, existeixen nombres primers p, q i ϖ tals que $N = p + q + \varpi$, $\varpi \equiv 3 \pmod 8$ i 2 és arrel primitiva mòdul ϖ.* □

Corol·lari 5.4.0.4. *Per a tot nombre enter senar, N, $7 < N < 10^{27}$, existeixen nombres primers senars p, q i ϖ tals que $N = p + q + \varpi$, $\varpi \equiv 3 \pmod 8$ i 2 és arrel primitiva mòdul ϖ.* □

5.5 Les dades numèriques

Les dades corresponents a les dues llistes de nombres primers que hem calculat s'adjunten a aquest treball en format DVD. Aquestes es distribueixen en diversos fitxers comprimits en format ZIP.

• `RED_Stairway_To_Heaven_Exp27_I3.zip`,
MD5: `A2AA5085A0614C1592E223BAAB4D41C8`,

• `PARI_Stairway_To_Heaven_Exp28_HIPATIA_I3_(Part1).zip`,
MD5: `D4E7DFB2C7BD7A9848D7E200014B8B4A`,

• `PARI_Stairway_To_Heaven_Exp28_HIPATIA_I3_(Part2).zip`,
MD5: `8F84D72A6E5221A8FDCA0A9EC833F346`,

• `PARI_Stairway_To_Heaven_Exp28_HIPATIA_I3_(Part3).zip`,
MD5: `89EEFF6944E4F7D969AABE4BB6ADA181`,

• `PARI_Stairway_To_Heaven_Exp28_HIPATIA_I3_(Part4).zip`,
MD5: `6F29854FA2BE2AB8255D6E1E748A2F21`,

• `PARI_Stairway_To_Heaven_Exp28_HIPATIA_I3_(Part5).zip`,
MD5: `92514F664AF9190BA7D9F4B0B9D550E7`.

El primer conté els fitxers utilitzats en la verificació parcial de la conjectura feble de Goldbach fins a 10^{27}, els noms dels quals són de la forma `REDLIStairwayToHeavenXXX.txt`, on `XXX` va des de 000 fins a 099. Els altres contenen els fitxers utilitzats en la verificació parcial de la conjectura fins a 10^{28}, els noms dels quals són de la forma `PARIStairwayToHeavenXXX.txt`, on `XXX` va des de 000 fins a 999.

Al DVD també s'hi inclou un document de *Mathematica 7.0* amb instruccions i codis per recuperar els nombres primers a partir dels valors numèrics dels fitxers.

A continuació adjuntem pseudocodis dels algoritmes de recuperació dels nombres primers.

INICI

Pas 1: Llegir $0 \leq K \leq 99$ i fer $n = 4 \cdot 10^{18} - 8$.

Pas 2: Considerar l'expressió de K en base 10, $K = 100C + 10D + U$.

Pas 3: Obrir el fitxer REDLIStairwayToHeavenCDU.txt. Si no existeix, error i acabar.

Pas 4: Llegir q del fitxer i guardar-lo.

Pas 5: Mentre quedin línies al fitxer, llegir e del fitxer i fer $q \leftarrow q + n - 8e$. Guardar q.

Pas 6: Tancar el fitxer i acabar.

FINAL

INICI

Pas 1: Llegir $0 \leq K \leq 999$ i fer $n = 4 \cdot 10^{18} - 4$.

Pas 2: Considerar l'expressió de K en base 10, $K = 100C + 10D + U$.

Pas 3: Obrir el fitxer PARIStairwayToHeavenCDU.txt. Si no existeix, error i acabar.

Pas 4: Llegir q del fitxer i guardar-lo.

Pas 5: Mentre quedin línies al fitxer, llegir e del fitxer i fer $q \leftarrow q + n - e$. Guardar q.

Pas 6: Tancar el fitxer i acabar.

FINAL

Referències

[1] Batut, C.; Belabas, K.; Bernardi, D.; Cohen, H.; Olivier, M.: User's guide to *PARI-GP*, `pari.math.u-bordeaux.fr/pub/pari/manuals/2.3.3/users.pdf`, 2000.

[2] Chen, J. R.; Wang, T. Z.: On the Goldbach problem, *Acta Math. Sinica*, 32(5):702-718, 1989.

[3] Deshouillers, J. M.: Sur la constante de Šnirel′man, *Séminaire Delange-Pisot-Poitou, 17e année: (1975/76), Théorie des nombres: Fac. 2, Exp. No.* G16, pàg. 6, Secrétariat Math., Paris, 1977.

[4] Deshouillers, J. M.; Effinger, G.; te Riele, H.; Zinoviev, D.: A complete Vinogradov 3-primes theorem under the Riemann hypothesis, *Electron. Res. Announc. Amer. Math. Soc.*, 3:99-104, 1997.

[5] Dickson, L. E.: *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., New York, 1966.

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

[7] Hardy, G. H.; Ramanujan, S.: Asymptotic formulae in combinatory analysis, *Proc. Lond. Math. Soc.*, 17:75-115, 1918.

[8] Hardy, G. H.; Wright, E. M.: *An introduction to the theory of numbers*, 5a edició, Oxford University Press, 1979.

[9] Helfgott, H. A.: Minor arcs for Goldbach's problem, `arXiv:1205.5252v4 [math.NT]`, desembre de 2013.

[10] Helfgott, H. A.: Major arcs for Goldbach's problem, `arXiv:1305.2897v4 [math.NT]`, abril de 2014.

[11] Helfgott, H. A.: The ternary Goldbach conjecture is true, `arXiv:1312.7748v2 [math.NT]`, gener de 2014.

[12] Helfgott, H. A.; Platt, D.: Numerical verification of the ternary Goldbach conjecture up to $8.875 \cdot 10^{30}$, `arXiv:1305.3062v2 [math.NT]`, abril de 2014.

[13] Klimov, N. I.; Pil′tjaĭ, G. Z.; Šeptickaja, T. A.: An estimate of the absolute constant in the Goldbach-Šnirel′man problem, *Studies in number theory, No. 4*, pàg. 35-51, Izdat. Saratov. Univ., Saratov, 1972.

[14] Liu, M. C.; Wang, T.: On the Vinogradov bound in the three primes Goldbach conjecture, *Acta Arith.*, 105(2):133-175, 2002.

[15] Oliveira e Silva, T.; Herzog, S.; Pardi, S.: Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$, *Math. Comp.*, 83:2033-2060, 2014.

[16] Ramaré, O.: On Šnirel′man's constant, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, 22(4):645-706, 1995.

[17] Riesel, H.; Vaughan, R. C.: On sums of primes, *Ark. Mat.*, 21(1):46-74, 1983.

[18] Rosser, J. B.; Schoenfeld, L.: Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, 6:64-94, 1962.

[19] Schnirelmann, L.: Über additive Eigenschaften von Zahlen, *Math. Ann.*, 107(1):649-690, 1933.

[20] Tao, T.: Every odd number greater than 1 is the sum of at most five primes, *Math. Comp.*, 83:997-1038, 2014.

[21] Travesa, A.: *Aritmètica*, Col·lecció UB, No. 25, Barcelona, 1998.

[22] Vaughan, R. C.: On the estimation of Schnirelman's constant, *J. Reine Angew. Math.*, 290:93-108, 1977.

[23] Vaughan, R. C.: *The Hardy-Littlewood method*, Cambridge Tracts in Mathematics, No. 125, 2a edició, Cambridge University Press, 1997.

[24] Vinogradov, I. M.: Sur le théorème de Waring, *C. R. Acad. Sci. URSS*, 393-400, 1928.

[25] Vinogradov, I. M.: Representation of an odd number as a sum of three primes, *Dokl. Akad. Nauk. SSSR*, 15:291-294, 1937.