

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

Eduard Roure Perdices

Facultat de Matemàtiques
Universitat de Barcelona

27 de gener de 2015

Origen

fabus, nicht beschaffen, als wären aber schon mal fälschlich, als
wäre nicht schon länger numerus, was modo in die opera
divisibiles geht, nicht selbst, weil es auf eine conjectura
beruht. In die geht Zahl, welche sich zu einem numerus primis
zusammensetzen, ist an aggregatione ist, wiewol numerorum
primorum, ist, als was will, ist in viderum, mit der 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820,

Figura 1: Carta de Goldbach a Euler del 7 de juny de 1742.

Les conjectures de Goldbach

Conjectura feble

Tot nombre enter senar més gran que 5 es pot escriure com a suma d'exactament tres nombres primers.

Conjectura forta

Tot nombre enter parell més gran que 2 es pot escriure com a suma d'exactament dos nombres primers.

Resultats sobre la conjectura feble de Goldbach

- L'any 1923, Hardy i Littlewood 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 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 $C = 3^{3^{15}} \approx 3.25 \cdot 10^{6846168}$ es pot escriure com a suma de tres nombres primers.
- L'any 1989, Chen i Wang, i l'any 2002, Liu i Wang, van rebaixar la fita a $C = 3.33 \cdot 10^{43000}$ i $C = 2 \cdot 10^{1346}$, respectivament.

Resultats sobre la conjectura feble de Goldbach

- L'any 1997, Deshouillers, Effinger, te Riele i Zinoviev van demostrar la conjectura feble de Goldbach condicionada a la hipòtesi de Riemann.
- L'any 2013, Helfgott i Platt van demostrar la conjectura feble de Goldbach de forma incondicional.

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.

Donada una funció $R : \mathbb{N} \rightarrow \mathbb{N}$, calcular una funció $\mathcal{P} : \mathbb{N} \rightarrow \mathbb{C}$ tal que per a $\mathcal{E} := R - \mathcal{P}$ sigui $\lim_{N \rightarrow \infty} \frac{|\mathcal{E}(N)|}{|\mathcal{P}(N)|} = 0$. En particular, existeix $\mathcal{C} > 0$ tal que $\forall N > \mathcal{C}$ és $R(N) \neq 0$.

Integrals i sumes

Definició

Sigui $\mathcal{A} = (a_m)_m$ una successió estrictament creixent de nombres enters no negatius. Sigui $N \in \mathbb{N}$. Denotarem per $R_s(N)$ el nombre de representacions de N com a suma de s elements de $\mathcal{A}$.

Integrals i sumes

Proposició

Per a cadascuna de les dues funcions $\eta(t) = e^{\frac{1}{s}-t}$ i $\eta(t) = \mathbf{1}_{[0,1]}(t)$ se satisfà la igualtat

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

on

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

essent $x \geq 1$. $\square$

Representacions pesades

Definició

Sigui $\mathcal{A} = (a_m)_m$ una successió estrictament creixent de nombres enters no negatius. Siguin s i N nombres naturals. Siguin $\omega_1, \dots, \omega_s : [0, \infty) \rightarrow \mathbb{R}$ i posem $\omega = (\omega_1, \dots, \omega_s)$. Definim

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

Observació

Si $\omega_i(t) = 1$, $e^{\frac{1}{s} - \frac{t}{N}}$ o $\mathbf{1}_{[0,1]}(\frac{t}{N})$, aleshores és $R_s^\omega(N) = R_s(N)$.

Important

Si existeixen $\omega_1, \dots, \omega_s$ tals que $R_s^\omega(N) \neq 0$, aleshores $R_s(N) > 0$.

Representacions pesades

Proposició

Siguin $\omega_1, \dots, \omega_s : [0, \infty) \rightarrow \mathbb{R}$ tals que les sèries

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

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

Aleshores,

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

Els arcs

Definició

Fixem $Q, V \in \mathbb{R}_+$ i $N \in \mathbb{N}_{>0}$. 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

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

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

- └ El mètode del cercle de Hardy-Littlewood
- └ Aplicació a la conjectura feble de Goldbach

Aplicació a la conjectura feble de Goldbach

Cercar 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:

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

- └ El mètode del cercle de Hardy-Littlewood
- └ Aplicació a la conjectura feble de Goldbach

Aplicació a la conjectura feble de Goldbach

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 $[0, 1)$.

- └ El mètode del cercle de Hardy-Littlewood
- └ Aplicació a la conjectura feble de Goldbach

Aplicació a la conjectura feble de Goldbach

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

- └ El mètode del cercle de Hardy-Littlewood
- └ Aplicació a la conjectura feble de Goldbach

Aplicació a la conjectura feble de Goldbach

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

El treball de Helfgott i Platt

Teorema (Helfgott)

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

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

Teorema (Helfgott i Platt)

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. $\square$

El problema

Proposició

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

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

La funció Λ de von Mangoldt

Definició

Sigui n un nombre natural. Definim

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

La funció Λ de von Mangoldt

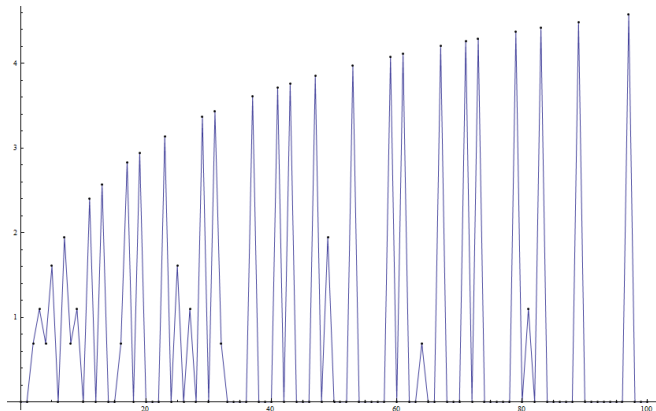


Figura 2: La funció Λ de von Mangoldt.

La funció η_+

Definició

Definim la funció $\eta_+ : [0, \infty) \rightarrow \mathbb{R}$ com

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

amb

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

La funció η_+

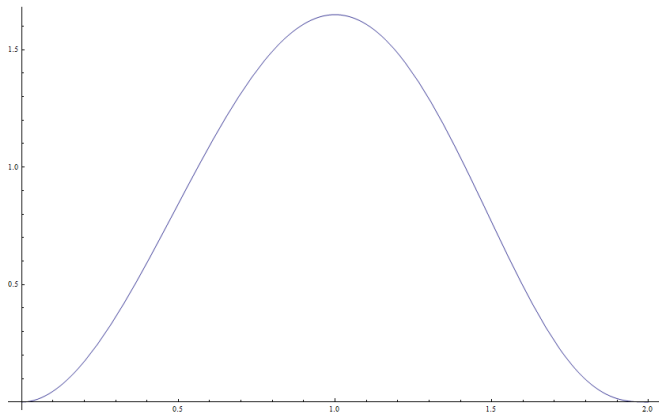


Figura 3: La funció h .

La funció η_+

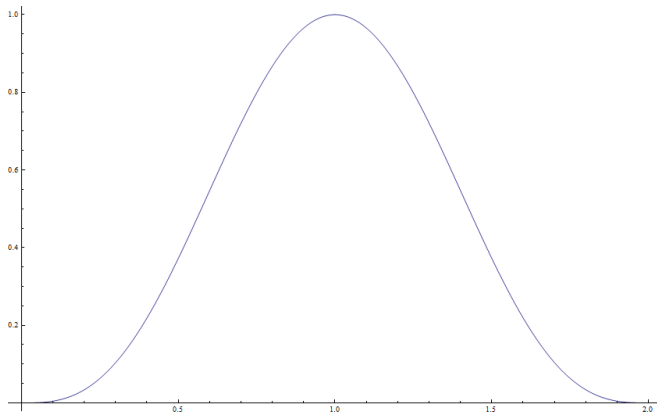


Figura 4: La funció η_+ .

La funció η_o

Definició

Definim la funció $\eta_o : [0, \infty) \rightarrow \mathbb{R}$ com

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

La funció η_o

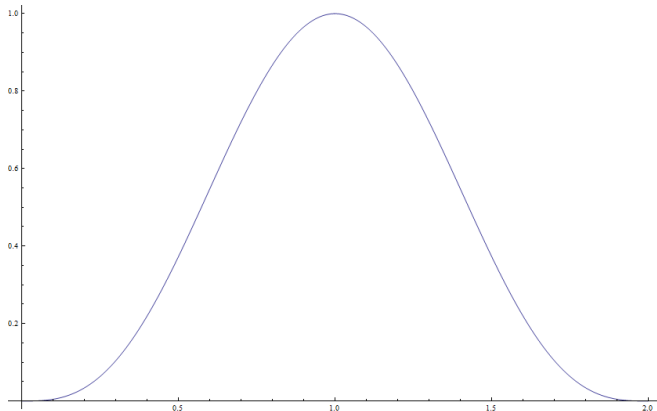


Figura 5: La funció η_o .

La funció η_*

Definició

Definim la funció $\eta_* : [0, \infty) \rightarrow \mathbb{R}$ com

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

La funció η_*

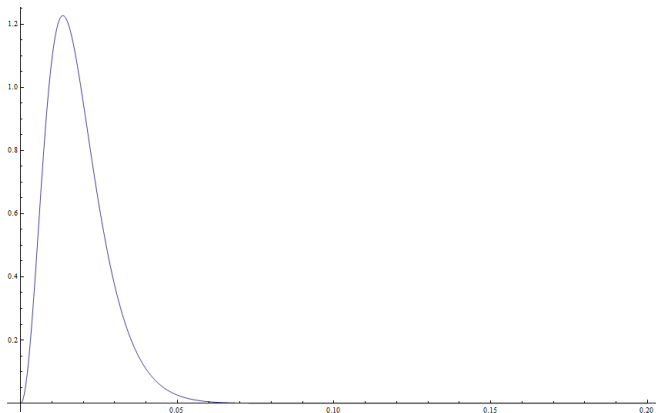


Figura 6: La funció η_* .

Els pesos

Definició

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

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

Els pesos

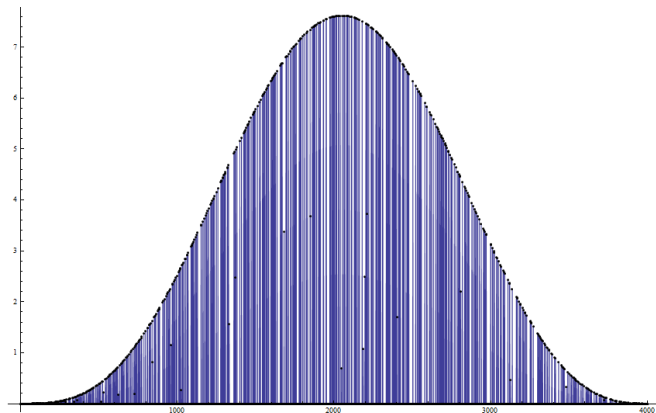


Figura 7: El pes ω_1^{2014} .

Els pesos

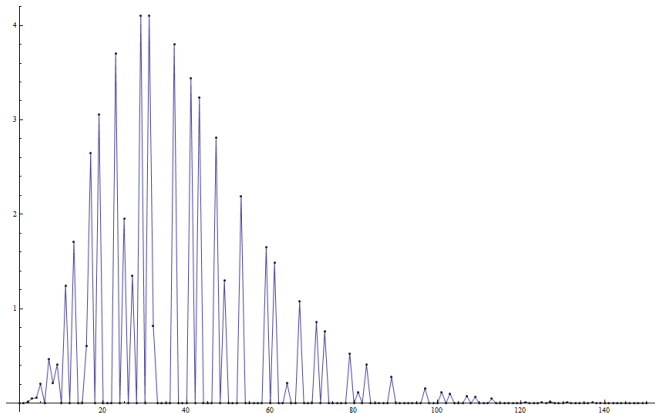


Figura 8: El pes ω_3^{2014} .

Les sèries S_η

Definició

Sigui x un nombre real més gran o igual que 1. Helfgott considera les sèries

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

i

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

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

Les sèries S_η

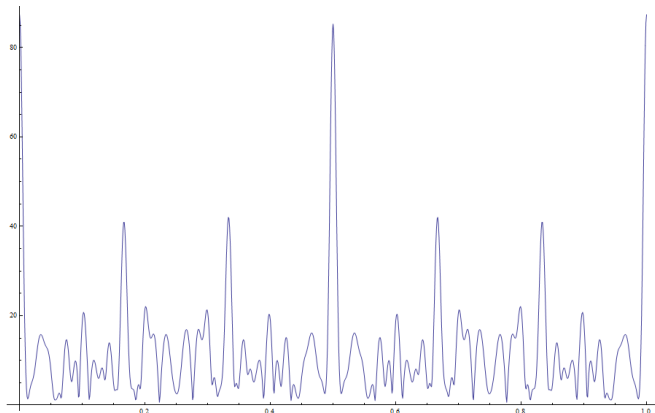


Figura 9: La funció $|S_{\eta_+}(\cdot, 101)|$.

Les sèries S_η

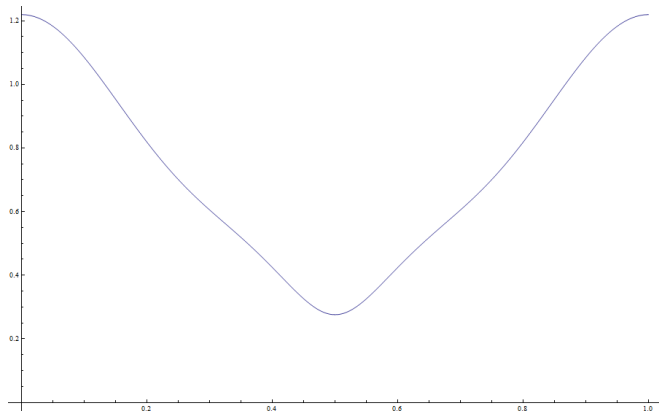


Figura 10: La funció $|S_{\eta_*}(\cdot, 101)|$.

El mètode del cercle

Proposició

Per a tot nombre real $x \geq 1$ se satisfà la igualtat

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

El mètode del cercle

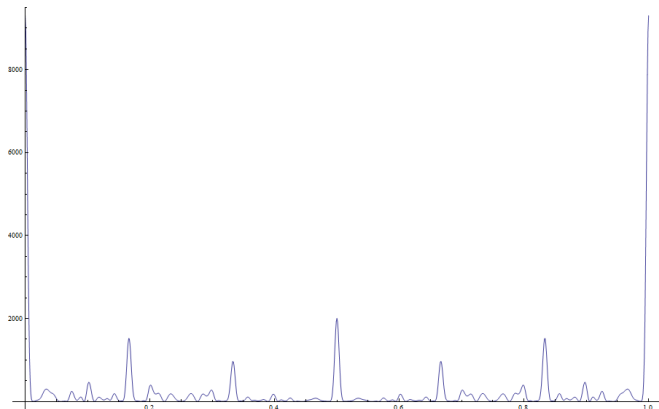


Figura 11: La funció $|S_{\eta_+}(\cdot, 101)^2 S_{\eta_*}(\cdot, 101) e(-204\cdot)|$.

Els arcs de Helfgott

Definició

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

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

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

Els arcs de Helfgott

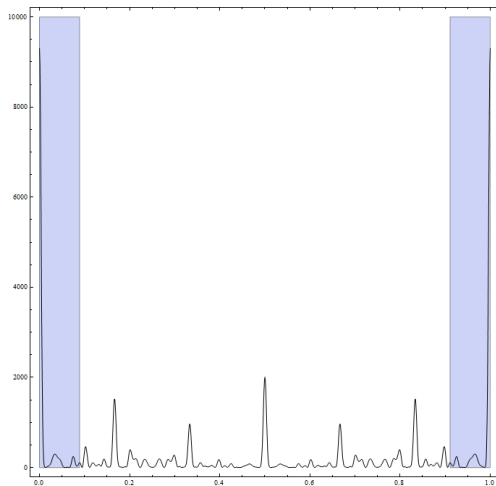


Figura 12: Arcs majors amb denominador 1.

Els arcs de Helfgott

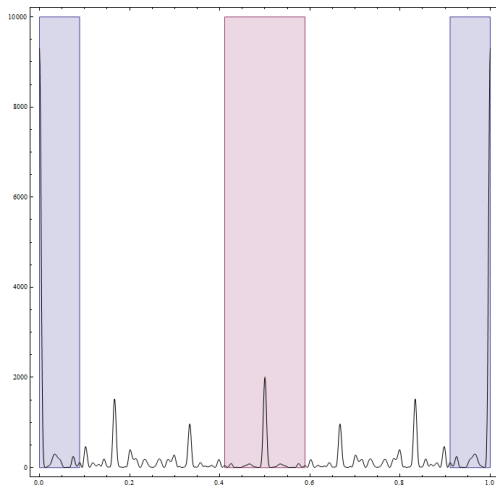


Figura 13: Arcs majors amb denominador menor o igual que 2.

Els arcs de Helfgott

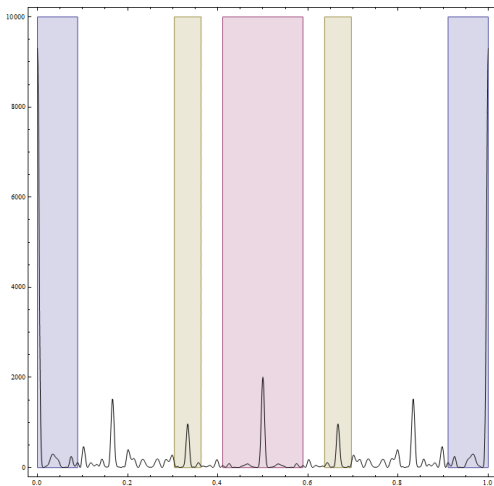


Figura 14: Arcs majors amb denominador menor o igual que 3.

Els arcs de Helfgott

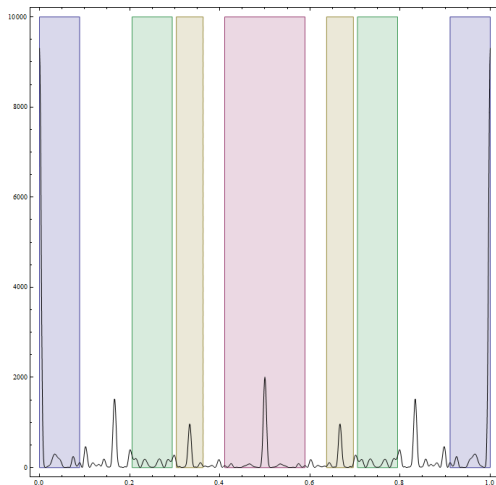


Figura 15: Arcs majors amb denominador menor o igual que 4.

Els arcs de Helfgott

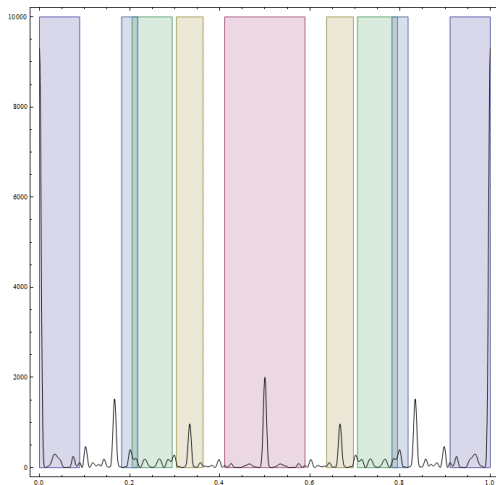


Figura 16: Arcs majors amb denominador menor o igual que 5.

Els arcs de Helfgott

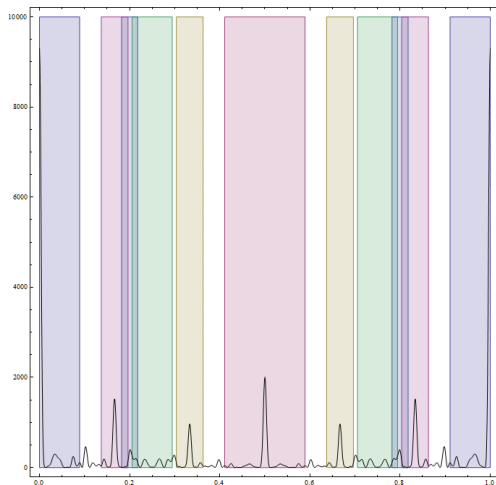


Figura 17: Arcs majors amb denominador menor o igual que 6.

Estudi de la integral sobre els arcs majors

Esquema

- Descomposició de les sèries S_{η_+}, S_{η_*} amb la utilització de caràcters de Dirichlet i obtenció d'una expressió per a $S_{\eta_+}^2 S_{\eta_*} e(-N\cdot)$.
- Identificació i integració del terme principal.
- Integració i acotació dels errors i dels termes no principals.

- └ La demostració de Helfgott
- └ La integral sobre els arcs majors

La contribució dels arcs majors

Teorema

Per a la integral sobre els arcs majors se satisfà la desigualtat

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

Estudi de la integral sobre els arcs menors

Idea

$$\begin{aligned}
 & \left| \int_{\mathfrak{m}} S_{\eta_+}(\alpha, x)^2 S_{\eta_*}(\alpha, x) e(-N\alpha) d\alpha \right| \\
 & \leq \sup_{\alpha \in \mathfrak{m}} |S_{\eta_*}(\alpha, x)| \int_{\mathfrak{m}} |S_{\eta_+}(\alpha, x)|^2 d\alpha \\
 & = \sup_{\alpha \in \mathfrak{m}} |S_{\eta_*}(\alpha, x)| \left(\int_0^1 |S_{\eta_+}(\alpha, x)|^2 d\alpha - \int_{\mathfrak{M}} |S_{\eta_+}(\alpha, x)|^2 d\alpha \right).
 \end{aligned}$$

- └ La demostració de Helfgott
- └ La integral sobre els arcs menors

La contribució dels arcs menors

Teorema

Per a la integral sobre els arcs menors se satisfà la desigualtat

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

La contribució de les potències de primers

Teorema

Se satisfà que

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

El final de la demostració

Teorema

$$\begin{aligned}
 & \sum_{\substack{n_1+n_2+n_3=N \\ n_1, n_2, n_3 \text{ primers senars}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\eta_+\left(\frac{n_1}{x}\right)\eta_+\left(\frac{n_2}{x}\right)\eta_*\left(\frac{n_3}{x}\right) \\
 & \geq \frac{1.058259}{49}x^2 + O^*\left(\frac{0.97392}{49}x^2\right) - 7.3306N^{\frac{3}{2}}\log N \\
 & \geq 0.000422N^2 > 0, \text{ per ser } x = \frac{N}{2 + \frac{9}{196\sqrt{2\pi}}} \text{ i } N > 10^{27}. \square
 \end{aligned}$$

- └ La demostració de Helfgott
- └ El final de la demostració

El final de la demostració

Corol·lari

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

Escales de nombres primers

Teorema (Oliveira e Silva, Herzog, Pardi)

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

Teorema

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 $4 < \varpi_0 < \dots < \varpi_k < \dots < \varpi_r < T$ 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 . $\square$

Algorítmica

Algoritme

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

Comentaris

La tasca

Hem dividit 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 cadascun d'aquests l'hem analitzat per separat. Per al cas $K = 0$ hem pres $\varpi_0 = 7$.

Les dades

Fixat el valor de ϖ_0 , per a tot $k > 0$ podem escriure $\varpi_k = \varpi_{k-1} + 4 \cdot 10^{18} - 4 - \varepsilon_k$. Per a cada interval analitzat hem guardat el primer nombre primer escollit i els valors d' ε_k que han anat apareixent.

Resultats empírics

Recursos utilitzats

- 640 nuclis del clúster Hipatia a la Facultat de Matemàtiques de la Universitat de Barcelona;
- 3 nuclis d'un ordinador portàtil amb processador Intel(R) Core(TM) i3;
- 4480 hores de CPU;
- 9.4GB de memòria;
- programari lliure *PARI-GP*;
- programari *Mathematica 7.0*.

L'Hipatia

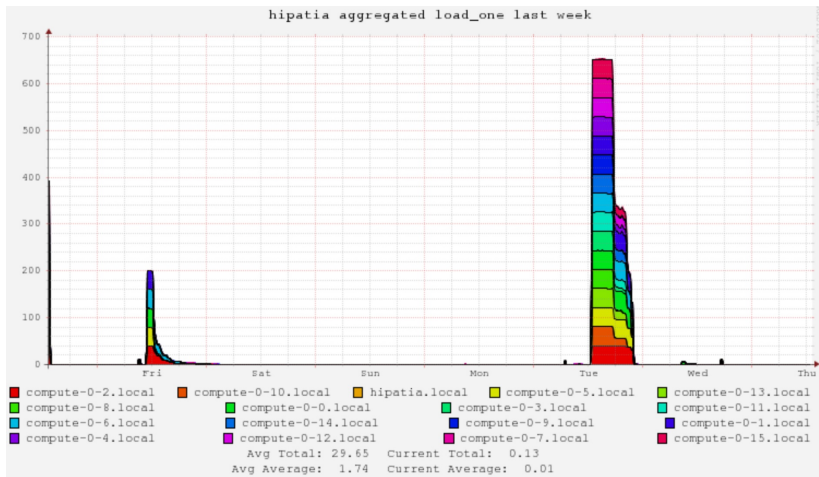


Figura 18: Gràfic de carga de l'Hipatia.

Conclusions

S'han calculat i certificat dos mil cinc-cents milions dos mil (2.500.002.000) nombres primers i podem resumir els càlculs en el resultat següent.

Teorema

Tot nombre enter senar, N , $7 < N < 10^{28}$, es pot escriure com a suma d'exactament tres nombres primers senars. $\square$

Més enllà

Qüestió

És possible calcular una altra escala de nombres primers de forma que un únic certificat de primeritat ens serveixi per certificar la primeritat de tots els esglaons?

Més enllà

Teorema (Criteri de primeritat)

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 $N - 1$, $\ell \neq 2$, és $g^{\frac{N-1}{\ell}} \not\equiv 1 \pmod{N}$. $\square$

Proposta

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 $(N, g \in (\mathbb{Z}/N\mathbb{Z})^*, o(g)) = (\varpi, 2, \varpi - 1)$ constitueix un certificat de primeritat vàlid per a tots ells.

Nova algorítmica

Algoritme 2.0

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 $\ell_1 \leq \dots \leq \ell_s$ 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.

Nova algorítmica

Algoritme 2.0

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 $d \leq 4$, error i acabar.

Pas 12: Si $d > 4$, guardar $\frac{n-d}{8}$, fer $q = p + d$,
 $m \leftarrow m + 1$.

Pas 13: Si $q \geq f$, acabar.

Pas 14: Si $q < f$, fer $p = q$, $q = p + n$ i tornar al pas 4.

FINAL

Comentaris 2.0

La tasca 2.0

Hem dividit l'interval $[0, 10^{27})$ en intervals de la forma $[K \times 10^{25}, (K + 1) \times 10^{25})$, amb $0 \leq K < 100$, i cadascun d'aquests l'hem analitzat per separat. Per al cas $K = 0$ hem pres $\varpi_0 = 11$.

Les dades 2.0

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

Resultats empírics 2.0

Recursos utilitzats 2.0

- 3 nuclis d'un ordinador portàtil amb processador Intel(R) Core(TM) i3;
- 797 hores de CPU;
- programari *Mathematica 7.0*.

Noves conclusions

S'han calculat i certificat dos-cents cinquanta milions dos-cents (250.000.200) nombres primers i podem resumir els càlculs en el resultat següent.

Teorema

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 . $\square$

Exemples

$$10^{27} - 1 = p + q + \varpi, \text{ on}$$

$$p = 31, q = 811284997 \text{ i}$$

$$\varpi = 9999999999999999999188714971$$

$$10^{27} - 1 = p + q + \varpi, \text{ on}$$

$$p = 405641791, q = 405643237 \text{ i}$$

$$\varpi = 9999999999999999999188714971$$

$$\varpi = 999999995999999999188715227$$

