Sumando primos ¿hay tres sin dos?

autor R. Tesoro, tutor F. Chamizo

Departamento de Matemáticas

Universidad Autónoma de Madrid

30 de septiembre de 2011

Sumando primos

Teorema (Vinogradov)

Todo número impar suficientemente grande se puede escribir como suma de tres primos.

Por ejemplo:

$$11 = 3 + 3 + 5$$

$$19 = 5 + 7 + 7$$

Sumando primos

Teorema (Vinogradov)

Todo número impar suficientemente grande se puede escribir como suma de tres primos.

Por ejemplo:

$$11 = 3 + 3 + 5$$

$$19 = 5 + 7 + 7$$

Conjetura (Goldbach)

Todo número par mayor que 2 se puede escribir como suma de dos primos.

Por ejemplo:

$$8 = 3 + 5$$

$$18 = 5 + 13 = 7 + 11$$

Resumen histórico

- 1742, Goldbach y Euler intercambian comentarios sobre este problema. También lo mencionan Descartes (1596–1650) y Waring (en una obra publicada en 1770), de manera independiente.
- 1923, Hardy y Littlewood prueban el teorema de Vinogradov suponiendo ciertas propiedades, todavía desconocidas, de los ceros de las funciones L.
- 1937, Vinogradov. Todo número impar suficientemente grande se puede escribir como suma de tres primos.
- 1966, Chen. Todo número par suficientemente grande puede escribirse como la suma de un primo más un *casi-primo*.
- 1976, Montgomery y Vaughan. El número de excepciones $E(x)$ a la conjetura de Goldbach es $O(x^{1-c})$ para cierto $c > 0$. Entonces

$$\lim_{x\to\infty} \frac{E(x)}{x} \to 0.$$

Relevancia de la conjetura de Goldbach

- En 1900 compartió con la Hipótesis de Riemann el puesto número 8 entre los 23 problemas propuestos por D. Hilbert.
- Su estudio impulsó durante el siglo XX el llamado método del círculo, que es uno de los más útiles en la Teoría Analítica de Números para tratar *problemas aditivos*.
- Durante un par de años comenzando en marzo de 2000 mereció el premio de un millón de dólares, ofrecido por los editores de la versión inglesa del libro *El tío Petros y la conjetura de Goldbach* de A. Doxiadis.

"Si el problema de Goldbach fuera resuelto probablemente se revelaría algo nuevo acerca de los números primos."
Iwaniec, H. y Kowalski, E. *Analytic Number Theory, p. 4*

Conjetura de Goldbach

Para el *número de representaciones* de N como suma de dos primos: $r_2(N) := \#\{(p_1, p_2) \in \mathcal{P} \times \mathcal{P} \mid N = p_1 + p_2\}$, se conjetura que

$$(1) \qquad \boxed{r_2(N) \sim \frac{N}{(\log N)^2}\, 2C_2 \prod_{\substack{p \mid N \\ p>2}} \left(1 + \frac{1}{p-2}\right) \quad N \text{ par}}$$

Notación

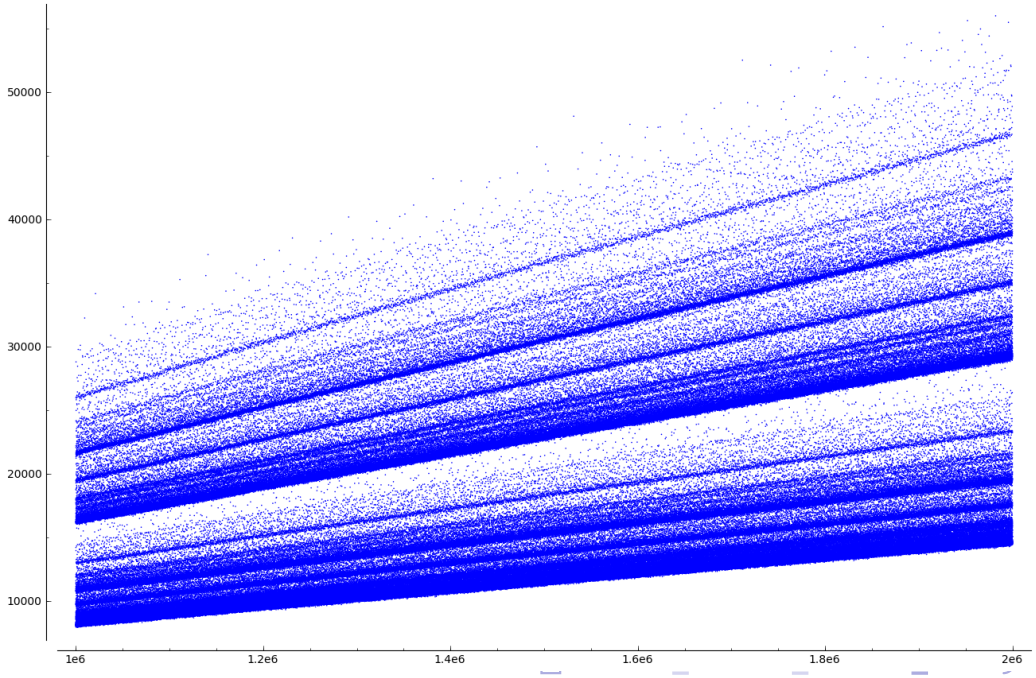
$$\mathcal{P} := \{p\colon p \text{ es primo}\}$$

$$f \sim g \text{ si } \lim_{x\to\infty} f(x)/g(x) = 1.$$

$f = O(g)$ si en el dominio de f

$$\exists\, C > 0 \text{ y } |f(x)| \leq C\,|g(x)|$$

$f \ll g$ significa $f = O(g)$



Teorema de Vinogradov

Para el *número de representaciones* de N como suma de tres primos: $r_3(N) := \#\{(p_1, p_2, p_3) \in \mathcal{P}^3 \mid N = p_1 + p_2 + p_3\}$, se tiene que

$$r_3(N) \sim \frac{N^2}{2\,(\log N)^3}\,\mathfrak{S}_3(N) \quad N \text{ impar} \tag{2}$$

donde $6/\pi^2 < \mathfrak{S}_3(N)$ es la *serie singular* para el problema ternario de Goldbach.

Corolario

Existe c_0 tal que todo entero impar $N \geq c_0$ se puede representar como la suma de tres primos.

Funciones generatrices

Si definimos $F_{\mathcal{P}} : \{z : \ |z| < 1\} \to \mathbb{C}$ como

$$F_{\mathcal{P}}(z) := \sum_{p \in \mathcal{P}} z^p = z^2 + z^3 + z^5 + \cdots ,$$

entonces al elevar al cuadrado

$$\begin{aligned}
[F_{\mathcal{P}}(z)]^2 &= (z^2 + z^3 + z^5 + \cdots)(z^2 + z^3 + z^5 + \cdots) \\
&= 1 \cdot z^{2+2} + 2 \cdot z^{2+3} + 1 \cdot z^{3+3} + 2 \cdot z^{2+5} + \cdots \\
&= r_2(4)\, z^4 + r_2(5)\, z^5 + r_2(6)\, z^6 + \cdots .
\end{aligned}$$

Elevando $F_{\mathcal{P}}$ a k obtenemos una nueva serie de potencias donde el coeficiente de la potencia n-ésima es precisamente $r_k(n)$:

$$[F_{\mathcal{P}}(z)]^k = \sum_{p_1 \in \mathcal{P}} z^{p_1} \times \ldots \times \sum_{p_k \in \mathcal{P}} z^{p_k} = \sum_{n=0}^{\infty} r_k(n) z^n.$$

Expresión como integral

Cambiamos coordenadas $z = \rho\, e^{2\pi i x}$ y truncamos $f_N(x) := F_{\mathcal{P}_N}(1 \cdot e(x))$, donde denotamos $\mathcal{P}_N := \mathcal{P} \cap [1, N]$ y $e(x) := e^{2\pi i x}$. Entonces

$$[f_N(x)]^k := \left(\sum_{p \in \mathcal{P}_N} [e(x)]^p \right)^k = \sum_{n=1}^{kN} r_k(n; N)\, e(nx).$$

siendo $r_k(n; N) := \#\{(p_1, \ldots, p_k) \in \mathcal{P}_N^k \mid n = p_1 + \ldots + p_k\}$.
Recordando la propiedad

$$\int_0^1 e(mx)\, \mathrm{d}x = \begin{cases} 1 & \text{si } m = 0, \\ 0 & \text{en otro caso} \end{cases} \qquad m \in \mathbb{Z},$$

y notando que $p_1 + \ldots + p_k = n \leq N$ implica $p_i \in \mathcal{P}_N$ entonces

$$n \leq N \quad \Rightarrow \quad r_k(n) = r_k(n; N) = \int_0^1 [f_N(x)]^k e(-nx)\, \mathrm{d}x.$$

Arcos mayores y menores

El método del círculo permite "reducir" nuestro problema i.e. calcular

$$r_k(n) := \#\left\{(p_1, \ldots, p_k) \in \mathcal{P}^k \mid n = p_1 + \ldots + p_k\right\}$$

al de estimar la siguiente integral:

$$r_k(n) = \int_0^1 \Big[\sum_{\substack{p \in \mathcal{P} \\ p \leq N}} e(px)\Big]^k e(-nx)\, \mathrm{d}x \quad \text{cuando } n \leq N.$$

El paso siguiente es partir el intervalo en arcos mayores $\mathcal{M}$ y arcos menores $\mathfrak{m} = [0,1] \setminus \mathcal{M}$ y analizar por separado las dos integrales para $n = N$:

$$r_k(N) = \int_{\mathcal{M}} [f_N(x)]^k e(-Nx)\, \mathrm{d}x + \int_{\mathfrak{m}} [f_N(x)]^k e(-Nx)\, \mathrm{d}x.$$

Resumen del método del círculo para problemas aditivos

El *objeto del deseo* es afirmar que $r_{k;\mathcal{A}}(N) > 0$, donde $\mathcal{A} \subset \mathbb{N}$.

1. Se encuentra la expresión integral $r_{k;\mathcal{A}}(N) = \int_0^1 [f_N(x)]^k e(-Nx)\, \mathrm{d}x$.
2. Se parte en dos $[0,1] = \mathcal{M} \cup \mathfrak{m}$ para estudiar por separado la integral.
   - Cada arco mayor $\mathcal{M}_{a/q}$ es un intervalo alrededor de un racional a/q con denominador pequeño.

Resumen del método del círculo para problemas aditivos

El *objeto del deseo* es afirmar que $r_{k;\mathcal{A}}(N) > 0$, donde $\mathcal{A} \subset \mathbb{N}$.

1. Se encuentra la expresión integral $r_{k;\mathcal{A}}(N) = \int_0^1 [f_N(x)]^k e(-Nx)\, \mathrm{d}x$.
2. Se parte en dos $[0,1] = \mathcal{M} \cup \mathfrak{m}$ para estudiar por separado la integral.
   - Cada arco mayor $\mathcal{M}_{a/q}$ es un intervalo alrededor de un racional a/q con denominador pequeño.
3. En los arcos mayores $\mathcal{M}$ *se extrae información de las singularidades*:
   - se espera que los valores de f_N en $\mathcal{M}$ sean grandes debido que $e(\mathcal{M})$ está cerca de los puntos singulares de $F_{\mathcal{A}} := \sum_{a \in \mathcal{A}} z^a$.
   - se encuentra una función parecida a $(f_N)^k$ y fácil de integrar.

   Al integrar se tiene una contribución con cota inferior > 0.

Resumen del método del círculo para problemas aditivos

El *objeto del deseo* es afirmar que $r_{k;\mathcal{A}}(N) > 0$, donde $\mathcal{A} \subset \mathbb{N}$.

1. Se encuentra la expresión integral $r_{k;\mathcal{A}}(N) = \int_0^1 [f_N(x)]^k e(-Nx)\,\mathrm{d}x$.
2. Se parte en dos $[0,1] = \mathcal{M} \cup \mathfrak{m}$ para estudiar por separado la integral.
   - Cada arco mayor $\mathcal{M}_{a/q}$ es un intervalo alrededor de un racional a/q con denominador pequeño.
3. En los arcos mayores $\mathcal{M}$ *se extrae información de las singularidades*:
   - se espera que los valores de f_N en $\mathcal{M}$ sean grandes debido que $e(\mathcal{M})$ está cerca de los puntos singulares de $F_{\mathcal{A}} := \sum_{a\in\mathcal{A}} z^a$.
   - se encuentra una función parecida a $(f_N)^k$ y fácil de integrar.

   Al integrar se tiene una contribución con cota inferior > 0.
4. Se comprueba que cuando $N \to \infty$, la contribución de $\mathfrak{m}$ es de un orden de magnitud menor que la de $\mathcal{M}$. (**El paso más difícil**)

Si hay éxito se tendrá que para N suficientemente grande $r_{k;\mathcal{A}}(N) > 0$.

Distribución de los primos en progresiones aritméticas

$$\forall\ p, p' \in \mathcal{P},\ \text{si } p \equiv p' \pmod{d} \implies e\left(\frac{a}{q}\,p\right) = e\left(\frac{a}{q}\,p'\right)\ \forall\ a/q \in \mathbb{Q},$$

por esto la suma oscilatoria evaluada en el racional a/q es

$$f_N\left(\frac{a}{q}\right) = \sum_{p\in\mathcal{P}\ ,\, p\leq N} e\left(\frac{a}{q}\,p\right) = \sum_{1\leq i\leq M} \pi(N; r_i, q)\ e\left(\frac{a}{q}\,r_i\right),$$

en donde $\pi(N; r_i, q)$ cuenta los elementos de $\mathcal{P}$ menores o iguales que N cuyo residuo módulo q es r_i. **Es esperable que $f_N(a/q)$ sea más grande cuanto más pequeño es** q. Cuando $a/q \in [0, 1]$ es irreducible entonces

$$\pi(x; a, q) \sim \frac{1}{\phi(q)}\,\pi(x),$$

donde $\phi(q)$ es la cantidad de números menores q que y coprimos con q y $\pi(x) = \#\{p \leq x\colon p \text{ primo }\}$.

Pequeños grandes arcos en las sumas de primos

Los racionales con denominador pequeño sostienen a los arcos mayores $\mathcal{M}$. Concretamente: fijados N y $0 < B \in \mathbb{R}$ denotamos $Q := (\log N)^B$. Sea el intervalo

$$\mathcal{M}_{a/q} := \left\{ x \in [0,1] : \left| x - \frac{a}{q} \right| < \frac{Q}{N} \right\} \qquad q \leq Q,$$

($\mathcal{M}_{1/1}$ tiene una definición particular). Los arcos mayores para las representaciones con sumas de primos son:

$$\mathcal{M} := \bigcup_{1 \leq q \leq Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathcal{M}_{a/q}.$$

Nótese que $\mathcal{M}$ depende de N y de B. Su medida de Lebesgue tiende a 0.

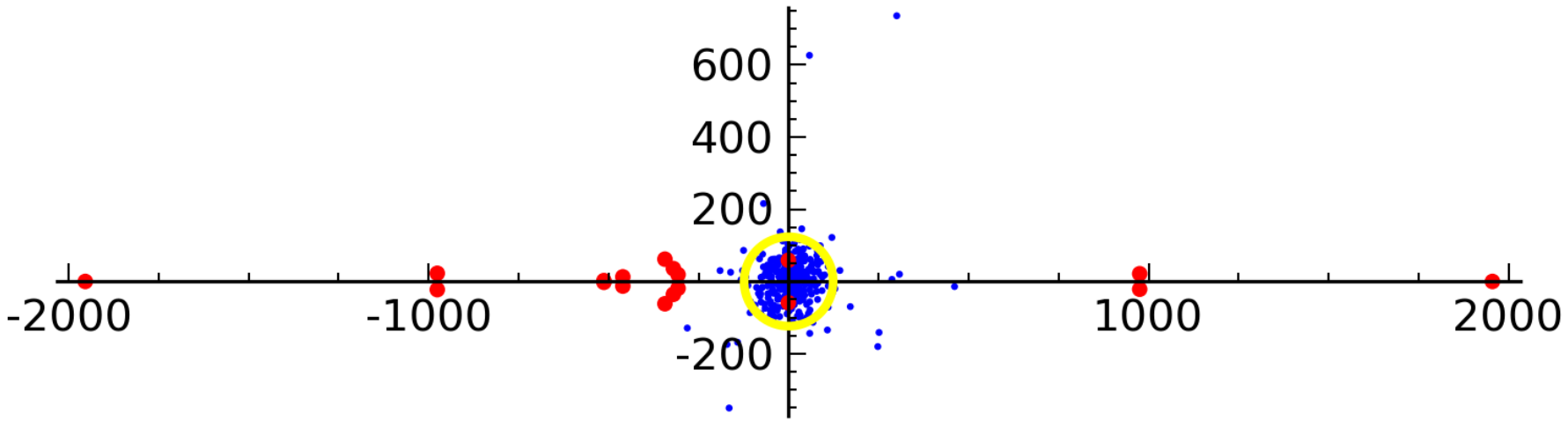


Imagen de $F_N(x) := \sum_{p \leq N} \log p \cdot e(px)$ con $N = 2011$.

- Muestra pseudo-aleatoria de más de 300 números complejos $F_N(a/q)$, $a/q \in [0, 1]$.
- En rojo los arcos mayores: $F_N(a/q)$ con $a/q \in \mathcal{M}$ (nota: $N = 2011, B = 1$).
- En azul los arcos menores: $F_N(a/q)$ con $a/q \in \mathfrak{m}$.
- En amarillo se muestra la circunferencia de radio $\sqrt{N \log N}$ centrada en el origen.

(Preparado con SAGE www.sagemath.org)

Contribución de los arcos mayores

Proposición

En el conjunto de los arcos mayores $\mathcal{M}$ se cumple que para todo $k \geq 2$

$$\int_{\mathcal{M}} \left[\sum_{p \leq N} \log p \; e(px)\right]^k e(-Nx)\, \mathrm{d}x = \mathfrak{S}_k(N) \frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^{B-1}}\right)$$

donde

$$\mathfrak{S}_k(N) = \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right) \quad \prod_{p \nmid N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right)$$

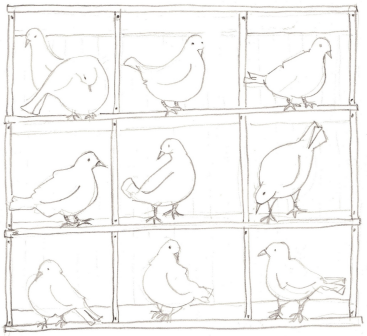
se denomina la serie singular para la representación de N como suma de k primos.

Acotación de Vinogradov

Cuando $|x - a/q| \leq 1/q^2$ con $(a, q) = 1$ entonces (Vinogradov, 1934):

$$\sum_{p \leq N} e(px) \ll q^{1/2} N^{1/2} + q^{-1/2} N + N\, e^{-\frac{1}{2}\sqrt{\log N}}.$$

Hoy se demuestra casi lo mismo con menos esfuerzo



$$\sum_{p \leq N} \log p\; e(px) \ll \left(q^{1/2} N^{1/2} + q^{-1/2} N + N^{4/5} \right) (\log N)^3.$$

Con esto se consigue controlar la contribución de los arcos menores $\mathfrak{m}$:

Proposición

$$\int_{\mathfrak{m}} \left[\sum_{p \leq N} \log p\; e(px) \right]^k e(-Nx)\, \mathrm{d}x = O\left(\frac{N^{k-1}}{(\log N)^{(B/2)-4}} \right) \qquad \forall\, k > 2.$$

Teorema (Vinogradov)

Cuando N y k tienen la misma paridad tenemos la estimación

$$r_k(N) = \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!\,(\log N)^k}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right) \qquad k > 2,$$

donde $\mathfrak{S}_k(N)$ es la serie singular para la representación de N como suma de k primos.

Teorema (Vinogradov)

Cuando N y k tienen la misma paridad tenemos la estimación

$$r_k(N) = \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!\,(\log N)^k}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right) \qquad k > 2,$$

donde $\mathfrak{S}_k(N)$ es la serie singular para la representación de N como suma de k primos.

Teorema (Chudakov, van der Corput, Estermann)

Denotamos la cantidad de excepciones a la conjetura de Goldbach por

$$E(x) := \#\{2n \leq x \mid r_2(2n) = 0\}.$$

Se tiene

$$E(x) = O\left(\frac{x}{(\log x)^A}\right) \qquad \forall\, A > 0,$$

En consecuencia $\lim_{x\to\infty} E(x)/x \to 0$.

La dificultad de rebajar la plausible cota

$$f_N(x) := \sum_{p \leq N} e(px) \ll \sqrt{\pi(N)} \sim \sqrt{\frac{N}{\log N}} \quad \text{para "la mayoría de"} \ x \in \mathfrak{m}.$$

es consistente con la *filosofía de la cancelación de la raíz cuadrada*.
Contando con ella tendríamos

$$\left| \int_{\mathfrak{m}} [f_N(x)]^2 e(-Nx) \, \mathrm{d}x \right| = O\left(\int_{\mathfrak{m}} \frac{N}{\log N} \, \mathrm{d}x \right) = O\left(\frac{N}{\log N} \right).$$

Usando esto último en el problema binario ($k = 2$)

$$r_2(N) = \mathfrak{S}_2(N) \, \frac{N}{(\log N)^2} + Err_{\mathcal{M}}(N) + \int_{\mathfrak{m}} [f_N(x)]^2 e(-Nx) \, \mathrm{d}x,$$

la presunta estimación no funciona

$$r_2(N) = \mathfrak{S}_2(N) \, \frac{N}{(\log N)^2} \left(1 + O\left(\frac{\log N}{\mathfrak{S}_2(N)} \right) \right).$$

Para calibrar lo que falta hasta la conjetura de Goldbach, imaginemos caer presos de un fuerte espejismo

Si en los arcos menores $\mathfrak{m}$ se cumpliera que

$$\sum_{p \leq N} e(px) \ll \sqrt{\frac{N}{\log N}} \frac{1}{(\log N)^{\frac{1}{2}+\delta}} \qquad \text{para algún } \delta > 0$$

esto implicaría

$$r_2(N) = \mathfrak{S}_2(N) \frac{N}{(\log N)^2} \left(1 + O\left(\frac{1}{\mathfrak{S}_2(N) (\log N)^{2\delta}}\right)\right).$$

¡El fallo es por un factor del orden de $(\log N)^{\frac{1}{2}+\delta}$!

Para más detalles

El trabajo completo se puede consultar en PDF en

`http://web.uam.es/personal_pdi/ciencias/fchamizo/posgrado/posgrado.html`

En las últimas páginas se recoge la lista de bibliografía y otras referencias.

Para copias de la fe de erratas del trabajo y de esta presentación:

`http://dl.dropbox.com/u/256172/RafaelTesoro_TrabajofdMaster_Erratas.pdf`

`http://dl.dropbox.com/u/256172/RafaelTesoro_Present-TdfM.pdf`

Gracias