Un siglo de sumas trigonométricas en teoría de números

Fernando Chamizo

5 de mayo de 2005

1. Introducción

Se pueden dar numerosos ejemplos, no todos analíticos, de la importancia de las sumas de senos y cosenos en teoría de números. He aquí dos de ellos que se derivan rápidamente del análisis de Fourier:

1) Para estudiar el promedio de $r(n)$, el número de representaciones como suma de dos cuadrados, se tiene

$$\sum_{n=0}^{N} r(n) = \sum_{\vec{n}\in\mathbb{Z}^2} \phi_N(\vec{n}) = \pi N + \sum_{\vec{n}\neq\vec{0}} \widehat{\phi_N}(\vec{n}) \tag{1}$$

donde ϕ_N es la función característica del círculo de radio $\sqrt{N}$, y se ha aplicado la fórmula de sumación de Poisson. Es bien conocido que $\widehat{\phi_N}$ es una función de Bessel que oscila como una función trigonométrica,

$$\widehat{\phi_N}(\vec{\xi}) = N^{1/4}\sqrt{\frac{2}{\pi}}\frac{\cos(2\pi|\xi|\sqrt{N} - 3\pi/4)}{|\xi|^{3/2}} + O\big(N^{-1/4}|\xi|^{-5/2}\big).$$

2) Para estudiar el promedio de $d(n)$, el número de divisores, deberíamos considerar

$$\sum_{n=1}^{N} d(n) = \sum_{a=1}^{N}\sum_{b\le N/a} 1 = \sum_{a=1}^{N}\big(N/a - \mathrm{Frac}(N/a)\big). \tag{2}$$

Y se puede sustituir el desarrollo de Fourier

$$\mathrm{Frac}(x) = \frac{1}{2} + \frac{1}{\pi}\sum_{m=1}^{\infty}\frac{\mathrm{sen}(2\pi m x)}{m}. \tag{3}$$

En ambos casos hay dificultades que superar inicialmente, relacionadas con los problemas de convergencia causados por la baja regularidad. Por ejemplo, (1) y (3) no son estrictamente igualdades si $\sqrt{N}$ o x son enteros, y la baja velocidad de convergencia de las series provoca que no sean útiles de esta forma. Sin embargo, una vez vencidas estas dificultades hay una equivalencia con un problema de acotación de sumas trigonométricas.

Los métodos con este propósito se han desarrollado y perfeccionado durante casi cien años. Para el no iniciado, muchos trabajos de investigación que los emplean se muestran incomprensibles por el apabullante despliegue técnico. Por ejemplo, el trabajo más reciente de M.N. Huxley [Hu 2] requiere muchas páginas de estimaciones para probar que la contribución de la última serie en (1) es $O(N^{131/416}(\log N)^{2{,}26})$, lo cual es descorazonador teniendo en cuenta 1/3 es el llamado "exponente trivial".

Una notación habitual que se empleará en lo sucesivo es $e(x)$ como abreviatura de $e^{2\pi ix} = \cos(2\pi x) + i\,\mathrm{sen}(2\pi x)$. Las sumas consideradas serán fundamentalmente de la forma

$$S = \sum_{n\le N} e(f(n))$$

para cierta función regular f. Se empleará también, la notación "$\ll$" como equivalente a la "O" de Landau, esto es, menor salvo una constante (no siempre absoluta).

2. El método de Weyl

En 1916 Weyl [We] abordó el problema de la equidistribución de ciertas sucesiones $\{a_n\}$ en $[0,1]$. La equidistribución significa que

$$\lim_{N\to\infty} \frac{f(a_1) + f(a_2) + \cdots + f(a_N)}{N} = \int_0^1 f$$

para cualquier f regular. Gracias al análisis de Fourier, es suficiente considerar el caso $f(x) = e(mx)$ con $m \in \mathbb{Z}^+$. Weyl se interesó por la sucesión $a_n = \mathrm{Frac}\big(P(n)\big)$ donde $P(n)$ es un polinomio cuyo coeficiente principal es irracional. Para simplificar, tómese $P(n) = \alpha n^k$, $\alpha \notin \mathbb{Q}$.

La equidistribución, por tanto, en este caso equivale a probar

$$S := \sum_{n\le N} e(\alpha n^k) = o(N)$$

donde no se exige la uniformidad de la cota en m (de hecho no es posible que se cumpla).

La clave del método de Weyl es que desarrollando el cuadrado del módulo de S, se pasa a una suma que tiene como fase (argumento de las exponenciales) los incrementos de las fases iniciales. No hay que minusvalorar esta idea tan simple. El gran éxito de las exponenciales complejas frente a otros posibles armónicos es que sólo para ellas se conoce este truco para manipular las frecuencias.

En el caso $k = 2$, $m = 1$, se tiene

$$\begin{aligned} |S|^2 &= \sum_{-N<r\le N} \sum_{-r<n\le N-r} e\big(\alpha((n+r)^2 - n^2)\big) \le \sum_{-N<r\le N} \Big| \sum_{-r<n\le N-r} e(2\alpha nr)\Big| \\ &\ll N + \sum_{r\le N} \text{mín}\,\big(N, |\csc(2\pi\alpha r)|\big). \end{aligned}$$

Si α fuera racional, $\alpha = a/q$, la contribución de la suma estaría acotada por $N+q+q/2+q/3+\cdots+(q-1)/q$ repetido $O(N/q+1)$ veces; es decir, $O(N^2q^{-1}+(N+q)\log q)$.

Por el teorema de Dirichlet de aproximación diofántica, para cada $\alpha \notin \mathbb{Q}$ existen infinitos a/q irreducibles con $|\alpha - a/q| < q^{-2}$. Una variación de α de orden q^{-2} no puede causar grandes cambios en la estimación anterior porque $\|2\alpha r\|^{-1}$ no llega a oscilar en cada bloque de longitud $O(q)$. Por tanto se concluye,

$$|\alpha - a/q| < q^{-2} \ \Rightarrow\ S \ll Nq^{-1/2} + (N^{1/2} + q^{1/2}) \log^{1/2} q.$$

De aquí

$$\limsup_{N\to\infty} \frac{|S|}{N} \le q^{-1/2},$$

y como q es arbitrariamente grande, $|S| = o(N)$ y $a_n = \text{Frac}(\alpha n^2)$ está equidistribuida.

Al tratar el caso de grado tres, desarrollando $|S|^2$, $(n+r)^3 - n^3$ lleva a un polinomio de segundo grado y una aplicación de la desigualdad de Cauchy-Schwarz permite enlazar con los razonamientos anteriores. En general, un polinomio de grado k requiere $k-2$ aplicaciones de la desigualdad de Cauchy-Schwarz antes de llegar a un polinomio de segundo grado que necesita un cuadrado más. El resultado que se puede obtener de esta manera es:

Theorem 2.1 *Sea P un polinomio de grado k con coeficiente principal $\alpha \in \mathbb{R}$ tal que $|\alpha - a/q| < q^{-2}$ para cierta fracción irreducible a/q; entonces*

$$\sum_{n\le N} e\big(P(n)\big) \ll N^{1+\epsilon}(q^{-1} + N^{-1} + qN^{-k})^{2^{1-k}}$$

para todo $\epsilon > 0$.

Este resultado está lejos de ser óptimo, sobre todo cuando k es moderadamente grande; en ese caso el método de Vinogradov es más poderoso. Hay mejoras para exponentes bajos en [He].

Es posible generalizar el método para tratar sumas $\sum e(f(n))$ con f bajo ciertas condiciones de regularidad. Para ello se aplica esencialmente el Teorema 2.1 después de aproximar f por uno de sus polinomio de Taylor y tratando el error mediante sumación por partes. En cualquier caso, el método de van der Corput se muestra más versátil.

3. El método de van der Corput

En 1921 J.G. van der Corput [Co] diseñó un nuevo método para estimar sumas trigonométricas que más adelante, en manos de E. Phillips, dio lugar a la teoría de pares de exponentes. En comparación con los métodos de Weyl y de Vinogradov tiene una flexibilidad mayor y no da preponderancia a las fases polinómicas. Desde el punto de vista actual se puede considerar, en pocas palabras, como la combinación de una variante del método de Weyl con la fórmula de sumación de Poisson. Esta última lleva a estimar algunas integrales. No es difícil desarrollar alguna intuición al respecto mediante aproximaciones lineales o cuadráticas de las fases.

La onda $g(t) = e(\nu t)$ tiene frecuencia ν porque oscila ν veces por cada unidad de tiempo t. De igual forma, a la onda "anarmónica" $e(f(t))$ en cada instante t se le debe asociar la frecuencia $f'(t)$, y realmente habría $f'(t)$ oscilaciones en una unidad de tiempo si f' no variase demasiado. Pudiera ser que $f'(t)$ se anulase para $t = t_0$, lo que significa que la onda no oscila cerca de t_0, se parecería a $e\big(f(t_0) + f''(t_0)(t - t_0)^2/2\big)$.

Se cumple

$$\Big|\int_a^b e(mt)\,dt\Big| \le \frac{1}{\pi m} \quad \text{y} \quad \int_{-\infty}^{\infty} e(A + \frac{B}{2}t^2)\,dt = \frac{e(A+1/8)}{\sqrt{B}} \quad \text{si } B > 0.$$

Por la analogía anterior se pueden probar fórmulas similares para $e(f(t))$. Por ejemplo, se tiene el lema de van der Corput: Si $f \in C^1([a,b])$ es convexa,

$$\Big|\int_a^b e(f(t))\,dt\Big| \le \frac{1}{\pi f'(a)}. \tag{4}$$

Por otra parte, si $f \in C^4([a,b])$ es convexa y alcanza un punto crítico en x_0, entonces

$$\int_a^b e(f(t))\,dt = \frac{e(f(t_0)+1/8)}{\sqrt{f''(t_0)}} + \texttt{error} \tag{5}$$

donde el error está controlado si las derivadas tercera y cuarta de f se comportan razonablemente bien. La convexidad no es esencial (conjugando se pasa al caso cóncavo) pero sí un signo en la derivada segunda.

Se pueden obtener resultados más finos si se introducen regularizaciones con funciones de soporte compacto (el análogo regular de (5) es lo que se llama *lema* *de fase estacionaria*). En la mayoría de las aplicaciones tales regularizaciones se pueden suponer mediante particiones de la unidad, no obstante la teoría se suele plantear sin ellas.

Si formalmente se aplica la fórmula de sumación de Poisson a $\sum e(f(n))$ se llega a integrales de la forma $\int e(f(t)-mt)\,dt$ que gracias a (4) son pequeñas si m está separado de la imagen de f'. Este argumento no es aplicable literalmente por la falta de convergencia (nótese que (4) llevaría a $\sum m^{-1}$) pero las dificultades técnicas se pueden rodear y llegar a que para cualquier función $f\in C^1$ convexa con $\alpha = f'(a)$ y $\beta = f'(b)$ se verifica

$$\sum_{a\le n\le b} e(f(n)) = \sum_{\alpha-1<m<\beta+1} \int_a^b e(f(t)-mt)\,dt + O\big(\log(2+\beta-\alpha)\big). \tag{6}$$

Las integrales que han subsistido no pueden tratarse con (4) porque $f(t)-mt$ puede tener puntos estacionarios, pero éste es el terreno en el que (5) es efectivo. Con cierto control sobre cuatro derivadas se llega a

Proceso B.

$$\sum_{a\le n\le b} e(f(n)) = \sum_{\alpha-1<m<\beta+1} \frac{e(f(x_m)-mx_m+1/8)}{\sqrt{f''(x_m)}} + \texttt{error}$$

donde x_m es el punto crítico de $f(t)-mt$ en $[a,b]$.

Un corolario que puede probarse independientemente, y de ahí que requiera condiciones menos fuertes es:

Theorem 3.1 *Sea $f\in C^2([a,b])$ convexa con $b-a=N\in\mathbb{Z}^+$ y $\lambda_2 \ll f'' \ll \lambda_2$, entonces*

$$\sum_{a\le n\le b} e(f(n)) \ll N\lambda_2^{1/2} + \lambda_2^{-1/2}.$$

Nótese que $(f'(b)-f'(a)+1)\lambda_2^{-1/2} \ll (\lambda_2 N+1)\lambda_2^{-1/2}$.

El Proceso B se combina con una variante más útil del argumento usado en el método de Weyl: en vez de elevar al cuadrado directamente, se agrupan los términos en bloques de cierta longitud H y así con la desigualdad de Cauchy-Schwarz sólo aparecerán incrementos de términos próximos, que son más fáciles de controlar. Concretamente, se usa

$$|S| = \Big|\sum_{a\le n\le b} e(f(n))\Big| = \Big|\frac{1}{H}\sum_n \sum_{m\in I_n} e(f(m+n))\Big| \le \frac{1}{H}\sum_{a-H\le n\le b-1}\Big|\sum_{m\in I_n} e(f(m+n))\Big|$$

con $I_n = [1, H] \cap [a-n, b-n] \cap \mathbb{Z}$. Y al aplicar Cauchy-Schwarz y separar los términos diagonales se sigue

$$\Big|\sum_{a\le n\le b} e(f(n))\Big|^2 \ll \frac{N^2}{H} + \frac{N}{H}\sum_{1\le r<H}\Big|\sum_{a\le n\le b-r} e(f(n+r)-f(n))\Big|$$

donde $N = b - a$.

Éste es el llamado Proceso A. Siguiendo [Mo] es posible aislar lo que realmente se emplea en el método de van der Corput de la siguiente forma:

PROCESO A. *Sea* $f_r(n) = f(n+r) - f(n)$ *y sean* $H \le b - a = N$, $H, N \in \mathbb{Z}^+$; *entonces*

$$\sum_{r=1}^{H}\Big|\sum_{a\le n\le b-r} e(f_r(n))\Big| \le N \;\Rightarrow\; \sum_{a\le n\le b} e(f(n)) \ll H^{-1/2}N.$$

3.1. La teoría de pares de exponentes

Los procesos A y B pueden aplicarse de manera repetida para mejorar estimaciones. Para traducir esto en un teorema general, es necesario precisar el tamaño de todas las derivadas. La teoría de pares de exponentes se restringe a aquellas funciones tales que tanto ellas como sus inversas cumplan que la derivada $k+1$-ésima sea como la k-ésima divida por la longitud del intervalo donde están definidas (esto viene sugerido por el teorema del valor medio). Por ejemplo, la teoría de pares de exponentes se aplica a $f(x) = \lambda/x$ definida sobre cualquier intervalo diádico.

Dada una función en las condiciones anteriores, se denomina D al tamaño de la derivada y N a la longitud del intervalo donde está definida (de forma que $f^{k)}$ es comparable a D/N^{k-1}). La dificultad para estimar la suma $\sum_n e(f(n))$ es que tenga muchos términos (N grande) o que oscile mucho (D grande). Se supondrá $D > 1$, porque en otro caso (6) es suficiente. Cabe esperar que las acotaciones dependan, por tanto, de potencias de D y N. Se dice que (p, q) es un *par de exponentes* si se cumple la acotación

$$\sum_n e(f(n)) \ll D^p N^q$$

para las funciones de la clase antes considerada.

Ahora es posible traducir de manera elegante los procesos antes mencionados. Si (p, q) es un par de exponentes, con la notación del Proceso A

$$\sum_{r\le H}\Big|\sum_n e(f_r(n))\Big| \le H(HD/N)^p N^q$$

que coincide con N para $H = D^{-p/(p+1)}N^{(1+p-q)/(p+1)}$, y por tanto el Proceso A se puede interpretar como:

$$\boxed{(p,q) \text{ par de exponentes} \Rightarrow A(p,q) = \big(\frac{p}{2p+2}, \frac{p+q+1}{2p+2}\big) \text{ par de exponentes}}$$

Por otra parte, el Proceso B permite pasar de una suma trigonométrica a otra "dual" donde el número de términos es comparable a D. Un cálculo prueba que si g es la función inversa de f', entonces la derivada de $f(g(t)) - tg(t)$ es $-g$; por consiguiente la derivada de las fases en el Proceso B es comparable a N. En definitiva, en la suma dual D y N intercambian sus papeles. Dado un par de exponentes (p,q), después de sacar el factor $(f'')^{-1/2}$ sumando por partes, se obtiene que el segundo miembro está acotado por $(D/N)^{-1/2}N^pD^q$, lo que permite escribir el Proceso B como:

$$\boxed{(p,q) \text{ par de exponentes} \Rightarrow B(p,q) = \big(q - \frac{1}{2}, p + \frac{1}{2}\big) \text{ par de exponentes}}$$

Iterando las funciones A y B se pueden crear infinitos pares de exponentes a partir del trivial $(0,1)$. Por ejemplo $B(0,1) = (1/2, 1/2)$, que es esencialmente el Teorema 3.1, $AB(0,1) = (1/6, 2/3)$, $BA^2B(0,1) = (2/7, 4/7)$.

Como ejemplo de la versatilidad del método de pares de exponentes, considérese (2). En principio el estudio del error (la parte oscilatoria) en la aproximación asintótica de $\sum d(n)$ lleva al estudio de sumas del tipo

$$\sum_{m=1}^{\infty} \sum_{a\le N} \frac{\operatorname{sen}(2\pi mN/a)}{m},$$

pero la simetría entre a y b permite suponer $a \le b \le N/a$ y pasar a una suma más corta en la que a sólo llega hasta $\sqrt{N}$. Por otro lado, al truncar la serie (3) hasta M, el error "típico" cometido es M^{-1}, con lo que el término de error depende de

$$E = \sum_{m\le M} \frac{1}{m} \big| \sum_n e(mN/n) \big| + M^{-1}N^{1/2}$$

donde n recorre algún subintervalo de $[1, \sqrt{N}]$. Si (p,q) es un par de exponentes (con $1 - p + q/2 > 0$)

$$E \ll \big(MN/(\sqrt{N})^2\big)^p (\sqrt{N})^q + M^{-1}N^{1/2} \ll M^pN^{q/2} + M^{-1}N^{1/2},$$

que eligiendo $M = N^{(1-q)/(2p+2)}$ produce

$$E \ll N^{(p+q)/(2p+2)}.$$

El par trivial $(0,1)$ da lugar a $E \ll N^{1/2}$, que se sigue de argumentos geométricos, y $(p,q) = (1/2,1/2)$ prueba $E \ll N^{1/3}$, que es el exponente "trivial" aplicando análisis armónico (fórmula de sumación de Poisson). Empleando $BA^3B(0,1) = (11/30, 8/15)$ se consigue $E \ll N^{27/82}$. Existe un algoritmo debido a S.W. Graham [Gr-Ko] para calcular pares de exponentes óptimos. En este caso, prueba que no es posible llegar muy lejos, porque el límite de lo que se puede obtener es $E \ll N^{0{,}329021\dots}$, mientras que $27/82 = 0{,}329268\dots$; en definitiva, se recortan poco más de cuatro milésimas a $1/3$.

La intuición probabilista sugiere que si verdaderamente hay oscilación ($D > 1$) los sumandos $e(f(n))$ deberían comportarse esencialmente como variables aleatorias independientes y cabe esperar una cancelación como la raíz cuadrada del número de términos. Precisamente, se conjetura que $(\epsilon, 1/2+\epsilon)$ es un par de exponentes para cualquier $\epsilon > 0$, lo que probaría varias conjeturas en teoría de números (hay ejemplos que muestran que ϵ no se puede suprimir).

Otras conjeturas están relacionadas con la estimación de sumas multidimensionales. No se ha conseguido crear una teoría completa de pares de exponentes ni siquiera en el caso bidimensional [Gr-Ko], [Ko]. La razón es que el proceso A lleva a considerar incrementos del tipo $f(m+r_1, n+r_2) - f(m,n)$ que pueden no dar lugar a una función "convexa" (el hessiano se podría anular), lo que impide la aplicación del Proceso B. Los métodos multidimensionales nacieron para funciones concretas [Ti], pero incluso para ellas este problema es inevitable. La conjetura natural, no obstante, es que en una suma en dos variables se pueda conseguir simultáneamente cancelación en ambas duplicando el poder de los métodos unidimensionales. Es decir, si (p,q) es un par de exponentes, se espera que

$$\sum_m \sum_n e(f(m,n)) \ll D_1^p M^q \cdot D_2^p N^q$$

donde D_1 y D_2 miden el tamaño de las derivadas parciales.

4. El método de Vinogradov

La mayor parte de la actividad matemática de I.M. Vinogradov está relacionada con la estimación de sumas trigonométricas, por ello no es de extrañar que lo que se llama hoy método de Vinogradov haya sufrido una evolución desde sus primeros artículos al respecto en 1935 [Vi]. En todas las variantes uno debe acotar integrales del tipo

$$J_{l,k}(N,\vec{\lambda}) = \int_0^1 \cdots \int_0^1 \Big| \sum_{n\le N} e(\beta_1 n + \beta_2 n^2 + \cdots + \beta_k n^k) \Big| e(\vec{\beta}\cdot\vec{\lambda})\, d\beta_1 \cdots d\beta_k$$

con $\vec{\lambda} \in \mathbb{Z}^k$, que representan el número de soluciones enteras de

$$(7) \qquad \begin{cases} n_1 + \cdots + n_l - (n_{l+1} + \cdots + n_{2l}) = \lambda_1 \\ n_1^2 + \cdots + n_l^2 - (n_{l+1}^2 + \cdots + n_{2l}^2) = \lambda_2 \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ n_1^k + \cdots + n_l^k - (n_{l+1}^k + \cdots + n_{2l}^k) = \lambda_k \end{cases}$$

con $1 \le n_j \le N$.

Se suele abreviar $J_{l,k}(N, \vec{0})$ por $J_{l,k}(N)$. La representación integral implica inmediatamente

$$(8) \qquad J_{l,k}(N, \vec{\lambda}) \le J_{l,k}(N)$$

lo cual no parece en absoluto evidente usando 7.

Al igual que el método de Weyl, el de Vinogradov originalmente estaba diseñado para fases polinómicas, pero se extiende a otras funciones con un argumento de aproximación. Es posible dar una interpretación "moderna" del método en pocas palabras: En la suma $\sum e(\alpha n^k)$ las frecuencias n^k no tienen un comportamiento uniforme, presentan grandes saltos. Elevando a una potencia grande, se consigue la uniformidad a costa de pagar con un coeficiente que depende del número de representaciones como suma de k-potencias. Vinogradov ordenó los cálculos de modo que aparecieran muchas de estas sumas, y entonces la idea de la gran criba se aplica, permitiendo extraer cancelación controlando la independencia de estas sumas y el tamaño de los coeficientes.

Una descripción más precisa es la siguiente:

Sea $S = \sum_{n \le N} e(P(n))$ con $P(n) = \alpha_k n^k + \alpha_1 n$ la suma que se desea acotar, y sean $\beta_j(m)$ definidos mediante

$$P(n+m) - P(m) = \beta_k(m) n^k + \beta_{k-1}(m) n^{k-1} + \cdots + \beta_1(m) n.$$

En particular $\beta_k(m) = \alpha_k$ y $\beta_{k-1}(m) = k\alpha_k m + \alpha_{k-1}$. La creación de una suma doble se consigue repitiendo y desplazando la suma original

$$|S| \ll \frac{1}{M} \sum_{m \le M} \Big| \sum_{n \le N} e(P(n+m)) \Big| + M = \frac{1}{M} \sum_{m \le M} \Big| \sum_{n \le N} e(P(n+m) - P(m)) \Big| + M.$$

Con la desigualdad de Hölder con exponente $2l$ se llega a

$$\sum_{m \le M} \Big| \sum_{n \le N} \Big|^{2l} = \sum_{m \le M} \sum_{\lambda_1, \dots, \lambda_k} J_{l,k}(N, \vec{\lambda}) e\big(\beta_k(m)\lambda_k + \beta_{k-1}(m)\lambda_{k-1} + \cdots + \beta_1(m)\lambda_1\big).$$

El término $\beta_k(m)\lambda_k$ realmente no varía con m, y si $\vec{\lambda}_*$ es como $\vec{\lambda}$ pero sin la última coordenada, se tiene

$$\Big|\sum_{\lambda_k} J_{l,k}(N,\vec{\lambda})e(\beta_k(m)\lambda_k)\Big| \le \sum_{\lambda_k} J_{l,k}(N,\vec{\lambda}) = J_{l,k-1}(N,\vec{\lambda}_*).$$

Aplicando la desigualdad de Cauchy-Schwarz y (8), todo se reduce a acotar $J_{l,k-1}(N)$ y la suma

$$\sum_{\lambda_1,\dots,\lambda_{k-1}} \Big|\sum_{m\le M} e\big(\beta_{k-1}(m)\lambda_{k-1}+\cdots+\beta_1(m)\lambda_1\big)\Big|^2$$

que una vez abierto el cuadrado conduce a sumas con fases lineales en los λ_j, lo que lleva a tener algún control sobre las propiedades de aproximación diofántica de los coeficientes de P (típicamente sólo del principal).

En las exposiciones habituales, al transformar este argumento en una cota explícita para S en términos de $J_{l,k-1}(N)$ se especifican ciertos rangos. En [Mo] hay una acotación sin hipótesis adicionales.

Theorem 4.1 *Sea $P(n)=\alpha_k n^k+\cdots+\alpha_1 n$ con $\alpha_k - a/q| < q^{-2}$ para cierta fracción irreducible a/q, entonces para cada $l\in\mathbb{Z}^+$,*

$$\sum_{n\le N} e(P(n)) \ll (kl^k)^{\frac{1}{2l}} N \left(\frac{J_{l,k-1}(3N)}{N^{2l-k(k-1)/2}}\right)^{\frac{1}{2l}} \big(\frac{1}{q}+\frac{\log q}{N}+\frac{q\log q}{N^k}\big)^{\frac{1}{2l}}.$$

El teorema del valor medio de Vinogradov permite mantener bajo control la fracción que contiene a $J_{l,k-1}(3N)$ cuando $l\gg k^2\log k$, por tanto, comparando con el Teorema 2.1 se tiene que el exponente 2^{1-k} se puede reemplazar por $C/(k^2\log k)$. Es decir, el exponente que indica el "ahorro" frente a la estimación trivial, pasa de tener decaimiento exponencial a potencial en el grado. La gran diferencia, por consiguiente, es notoria cuando k y l son grandes y por tanto la ganancia en el exponente de N es necesariamente pequeña. Por ello, cuando se aplica a fases más generales que los polinomios, la ventaja es apreciable sólo en los casos en los que importa mucho la dependencia en las derivadas (relacionadas con la posible elección de q). Por ejemplo, al hallar regiones libres de ceros hay que enfrentarse a sumas parciales de ζ del tipo

$$\sum_{n\le t}\frac{1}{n^{1+it}} = \sum_{n\le t}\frac{1}{n}\, e\big(-\frac{t}{2\pi}\log n\big), \qquad t>2.$$

La estimación trivial es $O(\log t)$. Después de sumar por partes, si sólo se aplicase un par de exponentes fijado no trivial (p,q), se llegaría a

$$\sum_{n\le t}\frac{1}{n^2}(t/n)^p n^q \ll t^p,$$

que es peor que $O(\log t)$.

Con el método de Vinogradov se consigue remplazar t^p por una función de creciento menor. Evidentemente también el método de van der Corput puede conseguir algo parecido tomando una sucesión de pares de exponentes que tiendan al trivial, pero con el de Vinogradov se consigue de alguna forma que el decaimiento de p a cero sea más rápido. Con las mejores versiones, se consigue

$$\sum_{n\le N} n^{-it} \ll N t^{-C(\log N/\log t)^3} \tag{9}$$

para cierta constante $C>0$ y $N\le t$. De aquí se puede deducir $\zeta(1+it)=O(\log^{2/3} t)$ y la mejor región libre de ceros (sin mejorar desde 1958).

4.1. El teorema del valor medio de Vinogradov

Recuérdese que para que el método de Vinogradov sea operativo, se necesita una acotación no trivial para $J_{l,k}(N)$, esto es, para el número de soluciones de (7) cuando $\vec{\lambda}=\vec{0}$.

Como hay unas $\left(N^{1/j}\right)^j = N$ formas de elegir un vector en $[1,N]^j$ formado por j-potencias, cada número debería tener un número esencialmente constante de representaciones de la forma $n_1^j+n_2^j+\dots+n_j^j$. Esto indicaría que la ecuación j-ésima de (7) establece j restricciones (se podrían recuperar j varibles conociendo las otras $2l-j$). El número de variables a escoger libremente serían, según esta heurísitca,

$$\text{todas las variables} - \sum \text{restricciones} = 2l - \sum_{j=1}^{k} j = 2l - \frac{k(k+1)}{2}.$$

Por otra parte, incluso si este número fuera negativo, se tienen las soluciones triviales $n_j=n_{j+l}$ que dependen de l variables libres.

Obviamente esto está muy lejos de ser una demostración pero motiva la conjetura

$$J_{l,k}(N) \ll N^{2l-k(k+1)/2+\epsilon} + N^{l+\epsilon}$$

para todo $\epsilon>0$ y donde la constante "$\ll$" depende de ϵ, k y l.

Sorprendentemente si k^2/l es moderadamente pequeño, se puede probar un resultado muy similar a la conjetura.

Theorem 4.2 (Teorema del valor medio de Vinogradov) *Sean $l,k\in\mathbb{Z}^+$ y $\delta=e^{-l/k^2}$, entonces*

$$J_{l,k}(N) \ll N^{2l-(1-\delta)k(k+1)/2}$$

donde la constante "$\ll$" depende de k y l.

La manera de probar este resultado es muy ingeniosa. En primer lugar se estudia el número de soluciones del sistema de congruencias

$$\begin{array}{rcll} n_1 + n_2 \cdots + n_k & \equiv & \lambda_1 & \pmod{p} \\ n_1^2 + n_2^2 \cdots + n_k^2 & \equiv & \lambda_2 & \pmod{p^2} \\ \ldots \quad \ldots \quad \ldots & & \ldots & \\ n_1^k + n_2^2 \cdots + n_k^k & \equiv & \lambda_k & \pmod{p^k} \end{array}$$

Resulta que este problema "local" es bastante asequible.

Si p es un primo grande, con ciertos argumentos elementales basados en la representación integral, se prueba que todo lo que hay que considerar es (7) con $\lambda = \vec{0}$ en el caso en que $n_1, n_2, \ldots, n_k$ son incongruentes módulo p, $n_{l+1}, n_{l+2}, \ldots, n_{l+k}$ gozan de la misma propiedad, y el resto de las varables son congruentes a un mismo número r. Una propiedad fundamental de (7) con $\lambda = \vec{0}$ es que permanece invariante por traslaciones $\vec{n} \mapsto \vec{n} + \vec{v}$ si $\vec{v}$ es un vector entero con todas sus coordenadas iguales. Con ello se puede suprimir r y llegar a un sistema donde las ecuaciones son de la forma

$$\sum_{i=1}^{k} (n_i^j - n_{l+i}^j) + p^j \sum_{i=k+1}^{l} (n_i^j - n_{l+i}^j) = 0.$$

Por tanto, dados $n_{l+1}, n_{l+2}, \ldots, n_{l+k}$, se sigue que $n_1, n_2, \ldots, n_k$ son soluciones de un sistema de congruencias como el antes considerado, y una vez contadas estas soluciones, se obtiene algo como (7) con otros rangos y $l-k$ pares de variables. Este proceso establece una fórmula que acota $J_{l,k}$ en términos de $J_{l-k,k}$. Para enceder la inducción se emplea $J_{l,k}(N) \le k!N^{2l-k}$ que se sigue fijando todas las variables de (7) excepto las k primeras.

5. El método de Hardy-Littlewood discreto

Cuando parecía que las plusmarcas en las acotaciones de las sumas trigonométricas de muchos problemas clásicos pasaban por diseñar versiones multidimensionales del método de van der Corput para funciones particulares, E. Bomberi y H. Iwaniec [Bo-Iw] asombraron en 1986 a los especialistas con un artículo que contenía nuevas ideas combinadas con el espíritu de los métodos anteriores. Más tarde, M.N. Huxley y N. Watt [Hu-Wa] generalizaron el argumento probando que de él se deducía el par de exponentes $(9/56+\epsilon, 37/56+\epsilon)$ para cualquier $\epsilon > 0$, que está fuera del alcance de la teoría de van der Corput.

En sucesivos trabajos, una variante del método resultó idónea para tratar problemas de puntos del retículo bidimensionales. Como se requiere una división de la suma en "arcos mayores" (en los que f' se aproxima por un racional de denominador pequeño) y "arcos menores"(su complementario), se le ha dado en llamar "método de Hardy-Littlewood discreto".

En realidad, aunque hay ideas básicas comunes, también hay grandes diferencias entre el artículo original (usado para acotar la función ζ en la línea crítica) y la variante empleada en problemas de puntos del retículo. En el primero son cruciales las sumas de Gauss y sus propiedades, mientras que en el segundo no son relevantes.

Las líneas principales en el artículo original son las siguientes:

Se comienza como en la variante de van der Corput del método de Weyl,

$$\Big|\sum_{a\le n\le b} e(f(n))\Big| \le \frac{1}{H}\sum_{a-H\le n\le b-1}\Big|\sum_{m\in I_n} e(f(m+n))\Big|$$

Si f''' es pequeña (lo cual se puede suponer porque en otro caso el par de exponentes que se prueba no sería útil) se puede aproximar $f(x+n)-f(n)$ por su polinomio de Taylor de tercer grado y entender el término cúbico como una perturbación. Además se busca una fracción a/c que aproxime bien a $f''(n)/2$ y a partir de ella se halla b tal que b/c aproxime lo mejor posible a $f'(n)$. Con todo esto, la sumación en n pasa a ser en las fracciones a/c, y los términos de error dependen de la bondad de la aproximación (en último término del tamaño del denominador). Despreciando estos errores, hay que estimar sumas de la forma

$$\sum_{a,c}\Big|\sum_m e\Big(\frac{am^2+bm}{c}+\mu m^3\Big)\Big|. \tag{10}$$

La fórmula de sumación de Poisson en progresiones aritméticas afirma que

$$\sum_{m\equiv d \pmod c} g(m) = c^{-1}\sum_m e(dm/c)\widehat{g}(m/c).$$

Por otra parte, si $g(t)=e(\mu t^3)$, por (5), $\widehat{g}(\xi)$ debe oscilar como $e(-\widetilde{\mu}^{-1/2}\xi^{3/2})$ donde $\widetilde{\mu}$ y μ son iguales salvo multiplicar por una constante. DEspués de dividir en progresiones aritméticas módulo c en la suma interior de (10), esta fórmula de sumación lleva a

$$\sum_{a,c}\Big|\sum_m G(a,b+m;c)e(-\widetilde{\mu}^{-1/2}m^{3/2}/c^{3/2})\Big| \quad \text{donde} \quad G(a,k;c)=\sum_{l=1}^{c} e\Big(\frac{al^2+kl}{c}\Big).$$

El "signo" de $G(a,b+m;c)$ cuando m varía tiene un comportamiento conocido, por ejemplo, para c impar

$$G(a,b+m;c)=e\Big(-\frac{\overline{a}}{c}(b+m)^2\Big)G(a,0;c)$$

donde $\overline{a}$ es el inverso de a módulo c, y el módulo de $G(a,0;c)$ es esencialmente $\sqrt{c}$. Con lo cual se tiene algo del tipo

$$\sum_{a,c}\Big|\sum_{m} e\Big(-\frac{\overline{a}}{c}(b+m)^2-\widetilde{\mu}^{-1/2}m^{3/2}/c^{3/2}\Big)\Big|.$$

Aparentemente estas sumas son intratables por su contenido aritmético, y realmente así ocurre con cada suma interior induviual, pero se puede proceder de forma parecida a la del método de Vinogradov. Después de elevar a cierta potencia para crear uniformidad, incluso con coeficientes artiméticos es posible encontrar cancelación si hay cierta independencia en las sumas. Esto requiere un teorema que estudie el espaciamiento de $\overline{a}/c$ en ciertos rangos, combinado con una especie de teorema del valor medio de Vinogradov con pocos sumandos y tres ecuaciones, correspondientes a los valores de m elevados a 1, 2 y 3/2.

En la versión empleada en los problemas de puntos del retículo, la aparición de términos conteniendo $\overline{a}/c$ proviene de que en estos problemas aparecen sumas del tipo

$$\sum_{h}\sum_{n} e\big(hf(n)-h\frac{an}{c}\big)$$

que al aplicar la fórmula de sumación de Poisson a la suma interior, llevan a

$$\sum_{h}\sum_{n\equiv ah \pmod{c}}\int e\big(hf(x)-\frac{nx}{c}\big)\,dx$$

y al invertir el orden de sumación, h recorre los congruentes con $\overline{a}n$ módulo c. Con argumentos relacionados con los de [Bo-Iw] (pero no similares) se llega también a problemas del mismo tipo relativos al espaciamiento de $\overline{a}/c$ y a ciertas analogías del teorema del valor medio de Vinogradov.

6. ¿Dónde aprender más?

El método de Weyl queda comúnmente superado por otros métodos. No obstante hay buenas explicaciones de lo que se puede conseguir en relación con el método del círculo en [Va]. En un contexto más general también se trata en [Iw-Ko].

El método de van der Corput, con algunas incursiones en el caso bidimensional, está magníficamente expuesto en [Gr-Ko]. Una exposición más breve, aun así muy completa, del caso unidimensional constituye la mayor parte del capítulo 3 de [Mo]. En [Iv] las explicaciones son también buenas pero las hipótesis requeridas para aplicar la teoría de pares de exponentes no parecen ser todo lo fuertes que debieran.

Hay buenas descripciones del método de Vinogradov en muchos libros, por ejemplo en [El], [Mo] y [Va], pero la de [Iw-Ko] está explicada con una profundidad, claridad y concisión difícilmente igualables, sobre todo teniendo en cuenta que trata la versión más poderosa del método.

En la monografía [Hu 1] se pueden aprender todos los detalles relacionados con el método de Hardy-Littlewood discreto. Una descripción completa de la prueba del par de exponentes $(9/56+\epsilon, 37/56+\epsilon)$ constituye el último capítulo de [Gr-Ko].

Referencias

[Bo-Iw] E. Bombieri; H. Iwaniec. *On the order of* $\zeta(1/2+it)$. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 13 (1986), no. 3, 449–472.

[Co] J.G. van der Corput, *Zahlentheoretische abschatzungen*, Math. Ann. 84 (1921), 53-79.

[Da] H. Davenport, *Multiplicative number theory*, Second edition. Revised by H.L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980.

[El] W.J. Ellison, *Les nombres premiers*. En collaboration avec Michel Mendès France. Hermann, Paris, 1975.

[Gr-Ko] S.W. Graham; G. Kolesnik, *van der Corput's method of exponential* sums. London Mathematical Society Lecture Note Series, 126. Cambridge University Press, Cambridge, 1991.

[Ha-Li] G. H. Hardy and J. E. Littlewood, *Some problems in diophantine approximation II.* Acta Mathematica **37** (1914), 194–238.

[He] D. R. Heath-Brown, *Weyl's inequality, Hua's inequality, and Waring's problem.* J. London Math. Soc. (2) **38** (1988), no. 2, 216–230.

[Hö] L. Hörmander, *The Analysis of Linear Partial Differential Operators I*, Springer-Verlag Berlin Heidelberg 1983.

[Hu 1] M.N. Huxley, *Area, Lattice Points, and Exponential Sums* London Mathematical Society Monographs 13. Oxford University Press 1996.

[Hu 2] M.N. Huxley, *Exponential sums and lattice points* III Proc. London Math. Soc. (3) **87** (2003), 591–609.

[Hu-Wa] M.N. Huxley; N. Watt, *Exponential sums and the Riemann zeta function.* Proc. London Math. Soc. (3) 57 (1988), no. 1, 1–24.

[Iv] A. Ivić, *The Riemann Zeta-function*, John Wiley & sons 1985.

[Iw-Ko] H. Iwaniec, E. Kowalski, *Analytic number theory*, Colloquium Publications **53**, American Mathematical Society 2004.

[Ko] G. Kolesnik, *On the estimation of multiple exponential sums.* Recent progress in analytic number theory, Vol. 1 (Durham, 1979), pp. 231–246, Academic Press, 1981.

[Mo] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, 84. American Mathematical Society, Providence, RI, 1994.

[Ti] E.C. Titchmarsh, *The lattice-points in a circle*, Proc. London Math. Soc. (2) **38** (1934), 96–115.

[Va] R. C. Vaughan, *The Hardy-Littlewood method*, Second edition. Cambridge Tracts in Mathematics, 125. Cambridge University Press, Cambridge, 1997.

[Vi] I.M. Vinogradov, *On Weyl's sums*, Math. Sbornik **42**, (1935), 521–530.

[We] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math Ann. **77**, (1916), 313–352.