Ideas sobre gran criba y el tamaño del menor no residuo cuadrático

Elena Cristóbal

Seminario de teoría de números de UB, UAB y UPC

29 de enero de 2007

· ¿Por qué gran criba?

En teoría de números muchas veces aparecen sumas de sumas trigonométricas con coeficientes aritméticos:

$$\sum_p e(f(p)) \quad \text{se expresa} \quad \sum_t \sum_r e(f(rt))a_t b_r,$$

donde, $e(t) = e^{2\pi i t}$.

Se podría pensar que la solución está en pasar el problema a los coeficientes utilizando que la primera suma es muy parecida a

$$\sum_{n \leq x} \frac{\Lambda(n)e(f(n))}{\log n}.$$

Esto no arregla las cosas.

IDEA: Cuando tenemos sumas con los mismos coeficientes y con las fases independientes en cierto sentido es imposible que los coeficientes se alíen para que no haya cancelación.

Esta idea es tan poderosa que incluso sirve para obtener cancelación en $\sum_{p \leq x} e(f(p))$ una vez que está escrita como suma de varias sumas.

· Un poco de historia:

Vinogradov

$\downarrow$

Con el principio de inclusión-exclusión
expresó sumas trigonométricas sobre
primos como formas bilineales

$\downarrow$

logró estimarlas

$\downarrow$ $\leftarrow$ Método del círculo

¡ Demostró el problema ternario de Golbach !

$\downarrow$

Si $N \geq C$ es impar entonces $N = p_1 + p_2 + p_3$,

siendo p_1, p_2 y p_3 números primos

· Introducción a la acotación de sumas bilineales

- Los instrumentos más versátiles de la teoría analítica de números son:

las ***sumas bilineales***

$$\downarrow$$

$$\Psi(\alpha,\beta)=\sum_m\sum_n \alpha_m\beta_n\phi(m,n),$$

donde $\alpha=(\alpha_m)$ y $\beta=(\beta_n)$ son vectores finitos de números complejos y

$$\Phi=(\phi(m,n))$$

es una matriz compleja.
En notación matricial $\Psi(\alpha,\beta)=\alpha^t\Phi\beta$.

Objetivo: acotar $\Psi(\alpha,\beta)$ independientemente de α y β una vez conocida la matriz Φ.

Cancelación en $\Psi(\alpha, \beta)$

$\downarrow$

propiedades Φ

$\downarrow$

casi-ortogonalidad.

Para estimar $\Psi(\alpha, \beta) \longrightarrow$ Cauchy-Schwarz.

Antes debemos elegir la variable que colocamos en la suma exterior y la de la suma interior.

$$|\Psi(\alpha, \beta)|^2 = |\sum_m \alpha_m \sum_n \beta_n \phi(m, n)|^2$$

$$\leq \|\alpha\|^2 \sum_m |\sum_n \beta_n \phi(m, n)|^2.$$

Observación: Hemos separado los coeficientes α_m desconocidos.

Para acotar el segundo término de la desigualdad anterior desarrollamos el cuadrado e intercambiamos el orden de sumación:

$$\sum_m |\sum_n \beta_n \phi(m,n)|^2 =$$

$$= \sum_{n_1}\sum_{n_2} \beta_{n_1}\bar{\beta}_{n_2} \sum_m \phi(m,n_1)\bar{\phi}(m,n_2).$$

- ¿Hay cancelación en la última suma?

  En los términos diagonales Φ, $(n_1 = n_2)$,

  $$\downarrow$$

  $$\sum_m |\phi(m,n)|^2,$$

  ¡no existe ningún tipo de cancelación!

- ¿Qué esperamos entonces?

  ¡Mucha cancelación en $\sum_m \phi(m,n_1)\bar{\phi}(m,n_2)$!

- La cancelación en

$$\sum_m \phi(m, n_1)\bar{\phi}(m, n_2)$$

es debida a la independencia de las variaciones de signo en $\phi(m, n_1), \phi(m, n_2)$.

- Por tanto nuestro salvavidas para la acotación es que los términos diagonales (donde no hay cancelación) son más pequeños que la suma total y en el resto de términos esperamos cancelación.

- *Observaciones*

  - Cómo acotar la suma anterior depende de la casi-ortogonalidad de las columnas de Φ.

  - La acotación puede hacerse directamente o transformando la suma $\longrightarrow$ Poisson

  - Una estimación trivial de la suma obtenida después de aplicar la fórmula espectral produce una estimación no trivial en la suma original.

□ El hecho de que no tengamos que asumir nada con respecto a los vectores α y β es esencial ya que en la práctica son objetos bastante complejos.

□ Los intentos de utilizar la estructura específica de estos vectores suelen llevar de nuevo a la situación de partida.

□ Es muy importante elegir convenientemente las variables del sumatorio exterior e interior antes de aplicar Cauchy-Schwarz.

- *Observación* No es necesario considerar $\phi(m, n)$ como función en los enteros. Puede ser una función con racionales, caracteres... La notación utilizada hasta ahora sólo es un modelo.

- Podemos repetir el razonamiento anterior en la otra variable.

- Este intercambio de variables es la esencia del siguiente principio.

- ***Principio de dualidad***: Si para cualesquiera números complejos β_n se tiene

$$\sum_m |\sum_n \beta_n \phi(m,n)|^2 \leq \Delta \|\beta\|^2$$

entonces para cualesquiera números complejos α_m se tiene

$$\sum_n |\sum_m \alpha_m \phi(m,n)|^2 \leq \Delta \|\alpha\|^2,$$

siendo Δ el mismo en las dos desigualdades.

· Nociones generales sobre gran criba desde el Álgebra Lineal:

$$\{\vec{u}_1, \ldots \vec{u}_d\} \longrightarrow \text{base ortonormal de } \mathbb{C}^d$$

$$\vec{a} \cdot \vec{u}_1, \ldots \vec{a} \cdot \vec{u}_d \longrightarrow \text{coordenadas de } \vec{a}$$

Por Pitágoras,

$$|\vec{a} \cdot \vec{u}_1|^2 + \ldots + |\vec{a} \cdot \vec{u}_r|^2 \leq \|a\|^2 \qquad (1)$$

para cualquier $r \leq d$, con igualdad si $r = d$.

(Desigualdad de Bessel)

$\vec{a} \longrightarrow$ coordenadas $a_n \in \mathbb{C}$

$\vec{u}_j \longrightarrow$ vector oscilatorio normalizado

$\downarrow$

coordenadas $\longrightarrow e(f(j,n))$

- Con la desigualdad de Bessel,

¿podríamos esperar estimar la suma de muchas sumas trigonométricas como la siguiente?

$$\sum_j |\sum_n a_n e(f(j,n))|^2$$

$$\downarrow$$

sería mucha casualidad que los u_j con la f requerida fueran ortonormales

- El "enemigo" a evitar es que los u_j apunten en la misma dirección $\longrightarrow$ desigualdad (1) falsa,

- Desde el punto de vista de las sumas trigonométricas la conclusión que buscamos es:

casi-ortogonalidad $\Rightarrow$ cancelación

- Si definimos una matriz B cuyas columnas sean los vectores $\vec{u}_1 \ldots \vec{u}_r$

$$\downarrow$$

$$(1) \text{ equivale a } \|\vec{a}^t B\|^2 \leq \|\vec{a}\|^2$$

$$\downarrow$$

Aplicando Cauchy-Schwarz podemos obtener una desigualdad para ciertas formas bilineales:

$$|\vec{a}^t B \vec{c}|^2 \leq \|\vec{a}\|^2 \|\vec{c}\|^2$$

- En el caso anterior B tiene todas sus columnas ortonormales. Con una base cualquiera la desigualdad anterior se "estropea" en función de lo lejos que estén las columnas de B de ser ortonormales. Se cumple

$$|\vec{a}^t B \vec{c}|^2 \leq \Delta(B) \|\vec{a}\|^2 \|\vec{c}\|^2$$

siendo $\Delta(B) = \text{máx}_j \sum_{k=1}^{r} |\langle \overrightarrow{b_j}, \overrightarrow{b_k} \rangle|$ y $\overrightarrow{b_l}$ las columnas de B con $l = 1..r$.

- Si $\vec{c}^t = \vec{a}^t B \longrightarrow \|\vec{a}^t B\|^2 \leq \Delta(B) \|\vec{a}\|^2$

· Gran criba:

- Consideremos una suma de sumas trigonométricas,

$$\sum_r |\sum_{n=1}^{N} a_n e(\alpha_r n)|^2 \text{ con } \alpha_r \in \mathbb{R}.$$

- Buscamos una cota:

  Si los α_r son muy parecidos (módulo 1) se repite muchas veces la misma suma y no obtendremos una cota no trivial.

- Supongamos, por tanto, que los α_r están bien espaciados módulo 1, es decir,

  $\|\alpha_r - \alpha_s\| \geq \delta \quad$ si $r \neq s$ para cualquier $\delta > 0$.

- El número de puntos distintos α_r es $\leq \delta^{-1}$.

- Bajo estas hipótesis el mejor resultado posible es el siguiente teorema:

Teorema 1 *(Selberg)*:

Para cualquier conjunto de puntos α_r como los anteriores y para cualesquiera $a_n \in \mathbb{C}$ con $n \leq N$, se tiene

$$\sum_r |\sum_{n=1}^{N} a_n e(\alpha_r n)|^2 \leq (\delta^{-1} + N)\|a\|^2$$

- Argumento heurístico:

  Por el principio de dualidad basta demostrar que

  $$\sum_{n=1}^{N} |\sum_r \gamma_r e(\alpha_r n)|^2 \leq C(\delta^{-1} + N)\|\gamma\|^2$$

  donde $\gamma_r \in \mathbb{C}$.

  Desarrollando el cuadrado,

  $$\sum_r \sum_s \gamma_r \bar{\gamma}_s \sum_{n=1}^{N} e((\alpha_r - \alpha_s)n)$$

$$\cdot \text{Si} \quad r = s \longrightarrow \sum_{n=1}^{N} e((\alpha_r - \alpha_s)n) \leq N$$

(n$^{\text{o}}$ términos, acotación trivial).

$\cdot$Si $r \neq s$ como los α_r están δ-espaciados

$$\downarrow$$

$$\sum_{n<N} e(\delta n) \ll \delta^{-1} \quad \text{(N.Dirichlet)}$$

- ¡Hemos obtenido $(N + \delta^{-1})$!

- Finalmente aplicando la desigualdad, aritmético-geométrica, $2|\gamma_r \gamma_s| \leq |\gamma_r|^2 + |\gamma_s|^2$, llegamos al resultado requerido.

- Apliquemos gran criba con $\longrightarrow \ \alpha_r = a/q$

  $1 \leq q \leq Q$ y $(a,q) = 1 \Longrightarrow$ puntos δ-espaciados

  Si $\frac{a}{q} \neq \frac{a'}{q'} \Longrightarrow \|\frac{a}{q} - \frac{a'}{q'}\| \geq \frac{1}{Q^2} \longrightarrow \delta = Q^{-2}$

- El teorema 1 funciona y se tiene,

  Teorema 2

  Para cualesquiera $a_n \in \mathbb{C}$ con $n \leq N$,

$$\sum_{q \leq Q} \sum_{\substack{a \pmod q \\ (a,q)=1}} |\sum_{n=1}^{N} a_n e(\frac{a}{q} n)|^2 \leq (Q^2 + N)\|a\|^2.$$

Sobre el menor no residuo cuadrático

- Es un problema natural preguntarse por el menor no residuo cuadrático

- Esperamos que no sea muy grande
  - ¿Cuál es el menor no residuo módulo 101?
    Es 2, pequeño $\longrightarrow$ se cumple lo esperado

- Sea $q(p)$ el menor no residuo cuadrático mod p
  $\downarrow$
  es primo

- Con un argumento ingenioso $\longrightarrow q(p) < \sqrt{p}+1$,

$$\text{Sea } m \in [p, p+q(p)) \text{ con } q(p)|m$$

$$\Downarrow$$

$$\frac{m}{q(p)} \text{ es no residuo}$$

$$\left(\frac{m/q(p)}{p}\right) = \frac{(m/p)}{(q(p)/p)} = \frac{((m-p)/p)}{(q(p)/p)} = \frac{1}{-1} = -1$$

Supongamos ahora que $q(p) \geq \sqrt{p}+1$,

$$\frac{m}{q(p)} \leq \frac{p+q(p)-1}{q(p)} \leq \frac{p+\sqrt{p}}{\sqrt{p}+1} < \sqrt{p}+1 \leq q(p)$$

$$\Downarrow$$

contradicción

Algunas cotas para el menor no residuo residuo cuadrático

- De la hipótesis de Riemann generalizada

  se deduciría la conjetura $\longrightarrow$ $q(p) \ll_\varepsilon p^\varepsilon$

- En sumas cortas de caracteres aparece $q(p)$:

$$\sum_{n<q(p)} \left(\frac{n}{p}\right) = q(p) - 1$$

cotas no triviales para sumas de caracteres

$\downarrow$

cotas para $q(p)$

· La mejor estimación que se conoce, no mejorada desde 1962

$\downarrow$

$$q(p) \ll_\varepsilon p^{1/(4\sqrt{e})+\varepsilon} \qquad \text{(Burgess)}$$

Teorema de Linnik

Sea $\varepsilon > 0$. El número de primos $p \leq N$ tal que $q(p) > N^{\varepsilon}$ está acotado por una constante que sólo depende de ε.

- Para probar el teorema hay que aplicar gran criba en problemas de criba:

  Sean:

  $\cdot\ \mathcal{M} \longrightarrow$ conjunto finito de enteros

  $\cdot\ \mathcal{P} \longrightarrow$ conjunto finito de primos

  $\cdot\ \Omega_p \longrightarrow$ conjunto de clases $(\mathrm{mod}\ p)\ \forall p \in \mathcal{P}$

  $\downarrow$

  conjunto a cribar

- $(\mathcal{M}, \mathcal{P}, \Omega)$ definen $\longrightarrow$ un problema de criba

  Objetivo: estimar el cardinal de:

$$\mathcal{S}(\mathcal{M}, \mathcal{P}, \Omega) = \{m \in \mathcal{M} \ : \ m \notin \Omega_p \ \forall p \in \mathcal{P}\}$$

- De forma más general, para una sucesión arbitraria de números complejos $a = (a_n)$ consideramos:

$$Z = \sum_{n \in \mathcal{S}(\mathcal{M},\mathcal{P},\Omega)} a_n$$

$$\downarrow$$

Buscamos cota para Z
en términos de la norma-l_2 de a.

$$\downarrow$$

Nos la da un resultado que se obtiene
a partir del teorema 2 de gran criba:

Teorema 3
Supongamos que $\mathcal{M} \subset [1, N]$ y que $\Omega_p \neq \mathbb{Z}_p$, es decir, $\omega(p) = |\Omega_p| < p \; \forall \; p \in \mathcal{P}$. Entonces

$$|Z|^2 \leq \frac{N + Q^2}{H} \|a\|^2$$

para cualquier $Q \geq 1$, donde

$$H = \sum_{q \leq Q, \mu(q) \neq 0} h(q)$$

siendo $h(q)$ una función multiplicativa con soporte en los enteros libres de cuadrados con divisores primos en $\mathcal{P}$ tal que

$$h(p) = \frac{\omega(p)}{p - \omega(p)}$$

En particular, tomando a_n como la función característica de $\mathcal{S}(\mathcal{M}, \mathcal{P}, \Omega)$, se tiene

$$S \leq \frac{N + Q^2}{H}$$

donde $\quad S = \displaystyle\sum_{\mathcal{S}(\mathcal{M},\mathcal{P},\Omega)} 1, \quad$ cardinal de $\mathcal{S}(\mathcal{M}, \mathcal{P}, \Omega)$.

Volvamos al enunciado del teorema para para continuar con la prueba.

Teorema 4 (*Linnik*).

Sea $\varepsilon > 0$. El número de primos $p \leq N$ tal que $q(p) > N^{\varepsilon}$ está acotado por una constante que sólo depende de ε.

Demostración

Sea X_ε el n° de primos $p \leq \sqrt{N}$ con $q(p) > N^{\varepsilon}$

$\downarrow$

buscamos una cota en términos de ε

Para hallarla consideremos el siguiente problema de criba:

- $\mathcal{M} = \{1, \ldots, N\}$
- $\mathcal{P} = \{p \leq \sqrt{N} \ : \ \left(\frac{n}{p}\right) = 1 \text{ ó } 0 \ \forall n \leq N^{\varepsilon}\}$
- $\Omega_p = \{\nu \pmod p \ : \ \left(\frac{\nu}{p}\right) = -1\}.$

$\Downarrow$

$\omega(p) = \frac{1}{2}(p-1)$ y $h(p) = \frac{p-1}{p+1}$

$\Downarrow$

$h(p) \geq \frac{1}{3}$

$\cdot\ \mathcal{S}(\mathcal{M},\mathcal{P},\Omega)=\{m\leq N|\ \left(\frac{m}{p}\right)=0 \text{ ó } 1\ \forall p\in\mathcal{P}\}$

$\cdot\ \mathcal{Z}_\varepsilon=\{n\leq N|\ p\nmid n \text{ si } p>N^\varepsilon\}$

$\cdot\ \mathcal{Z}_\varepsilon\subset\mathcal{S}(\mathcal{M},\mathcal{P},\Omega)$:

$$n\in\mathcal{Z}_\varepsilon\Longrightarrow n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\dots p_k^{\alpha_k} \text{ con } p_j\leq N^\varepsilon$$

$$\text{en particular } \left(\frac{p_j}{p}\right)=0 \text{ ó } 1\ \forall p\in\mathcal{P}$$

$$\Downarrow$$

$$\left(\frac{n}{p}\right)=0 \text{ ó } 1\ \forall p\in\mathcal{P}\Longrightarrow n\in\mathcal{S}(\mathcal{M},\mathcal{P},\Omega)$$

$$\text{teorema 3}$$

$$\left(S \leq \tfrac{N+Q^2}{H}\right)$$

$$\downarrow$$

$$\text{Si } Q = \sqrt{N} \Longrightarrow \; Z_\varepsilon = |\mathcal{Z}_\varepsilon| \leq 2NH^{-1}$$

$$\text{Combinando con} \longrightarrow \frac{1}{3}X_\varepsilon \leq \sum_{\substack{p \leq \sqrt{N} \\ q(p) \geq N^\varepsilon}} h(p) \leq H$$

$$\Downarrow$$

$$X_\varepsilon Z_\varepsilon \leq 6N$$

Queda acotar inferiormente $Z\varepsilon$:

$$\text{Se cuentan en } Z\varepsilon \; \longrightarrow \; n = mp_1p_2 \ldots p_k \leq N$$

$$\downarrow$$

$$Z\varepsilon \gg N$$

Por tanto $X_\varepsilon \ll 1$ y el teorema de Linnik queda demostrado.