

Los grafos expansores en la teoría de números

Harald Andrés Helfgott
(en colaboración
con Maksym Radziwiłł)

1. Qué son los grafos expansores?
2. Un problema de teoría analítica de números
... y un grafo
3. Resultado principal (e ideas de la prueba)

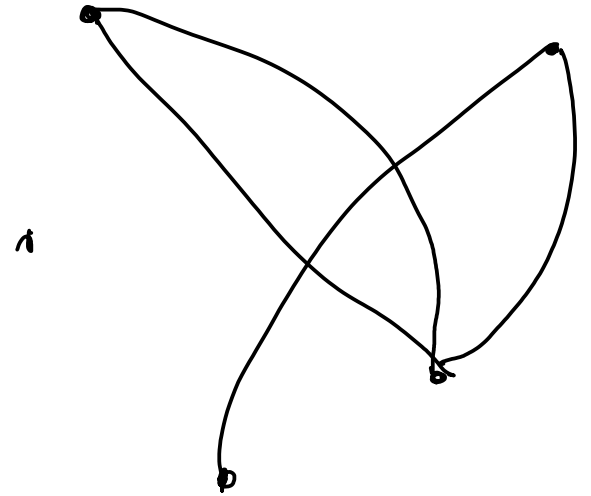
0. Definiciones básicas

Un **grafo** Γ es un par (V, E)

$V =$ conjunto

$E =$ un conjunto de pares $\{v_1, v_2\}, v_1, v_2 \in V$
 $v_1 \neq v_2$

(o, si es dirigido:
 $E \subset V \times V$)



Frontera ∂S de $S \subset V$:

$\partial S := \{v \in S :$

$\exists w \notin S,$
 $\{v, w\} \in E\}$



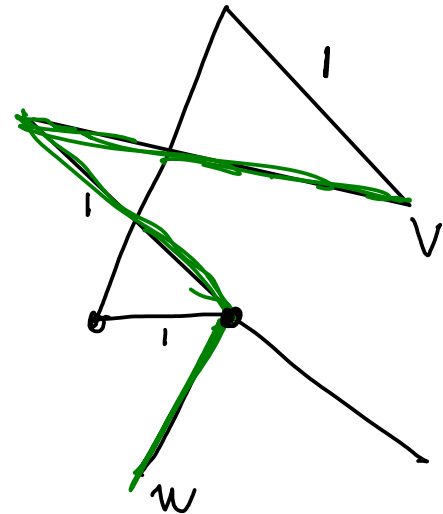
∂S

Distancia en un grafo:

$d(v, w) =$ longitud mínima
entre todos los
caminos de v a w

Grado de un vértice
("valencia")

de aristas
que contienen v



1. Qué es un grafo expensor?

1.1 Definición geométrica

$|S|$ = número de elementos de S

$\epsilon > 0$

Un grafo (V, E) es un ϵ -expensor

si $\forall S \subset V$ $S \neq \emptyset$
 $|S| \leq |V|/2$

$$|\partial S| \geq \epsilon \cdot |S|$$

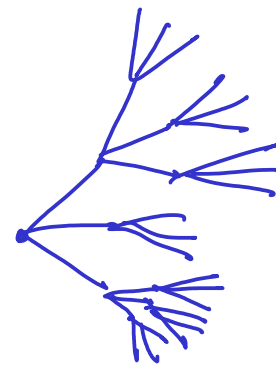
Diámetro $\text{diam}(T)$ de un grafo

$\max_{\substack{v, w \in V \\ v \neq w}} d(v, w)$

Lema (expensivo) Si $T = (V, E)$ es un ϵ -expensor,

$$\text{diam}(T) \leq \frac{C}{\epsilon} \log |V|$$

C un constante



1.2 Definición espectral

Consideremos funciones $f: V \rightarrow \mathbb{C}$

$\Gamma = (V, E)$
grafo
no orientado

un **operador lineal** es una función lineal
de (funciones: $V \rightarrow \mathbb{C}$) a (funciones: $V \rightarrow \mathbb{C}$)

Def El operador lineal **Ad** sobre funciones $f: V \rightarrow \mathbb{C}$
se define por: $(Adf)(v) = \sum_{w: v, w \in E} f(w)$.

El operador **Ad** es **simétrico**: $\langle f, Adg \rangle = \langle Adf, g \rangle$

Recordemos:

Prop Un operador lineal simétrico **A** sobre un espacio de **n** dimensiones
tiene **n** valores propios reales, y **n** autovectores ortogonales

$$\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n$$

$v_1 \quad v_2 \quad \quad \quad v_n$

$$\langle f, g \rangle = \sum_v f(v) \overline{g(v)}$$

$$\langle v_i, v_j \rangle = 0 \quad i \neq j$$

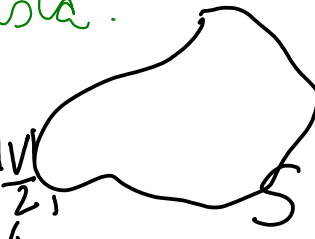
* regular: todos vértices tienen el mismo grado

Def Un grafo regular* de grado d es un ϵ -expansor si $|\lambda| \leq (1-\epsilon)d$

ϵ -expansor (espectral) (bilateral)

para todo autovalor λ , salvo el autovalor $\lambda=d$ asociado a las funciones constantes (y $\lambda=d$ tiene multiplicidad 1)

* pista:



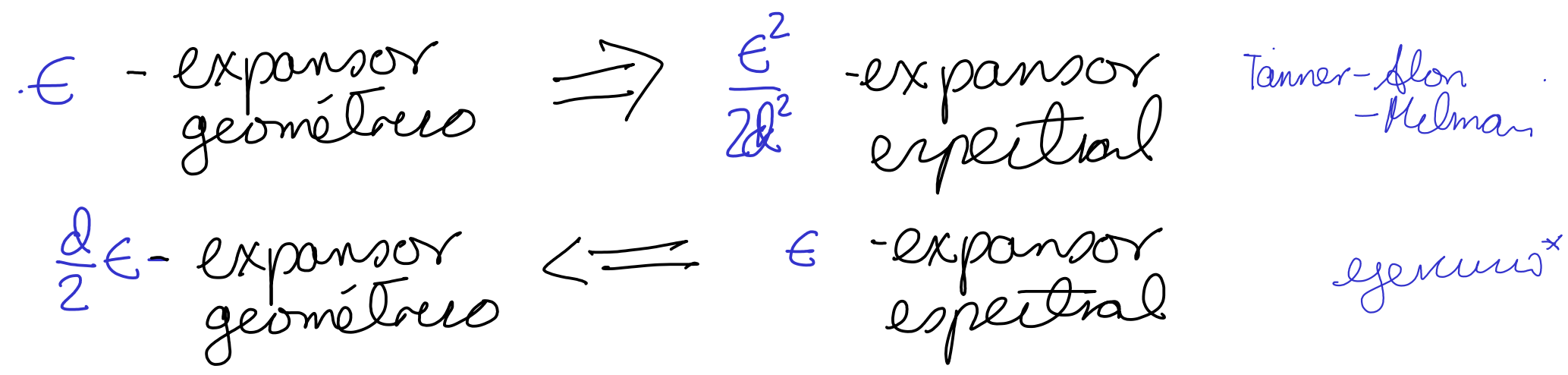
Dado $|S| < \epsilon |V|$

$|S| \leq \frac{|V|}{2}$, $S \neq \emptyset$

construir f $\langle f, \mathbf{1} \rangle = 0$

$\|f\|_2^2 = \langle f, f \rangle = 1$ $\langle f, \mathbf{1} \rangle = 0$

Relación:



Más propiedades de grafos expansores:

Una **caminata aleatoria** de longitud $l \geq \frac{C}{\epsilon} \log |V|$

equidistribuye:

después de l pasos, la ^(en norma l_∞) probabilidad de estar en un vértice v es $\approx \frac{1}{|V|}$

esbozo de argumento:

$$f(v) = \begin{cases} 1 & \text{si } v = v_0 \\ 0 & \text{si no} \end{cases}$$

$$f = \frac{1}{|V|} f_0 + c_1 f_1 + c_2 f_2 + \dots$$

\uparrow
 $= 1$

($v_i =$ autofunciones)

$(\frac{1}{2} A + \frac{1}{2} I)^k f(v) =$ la probabilidad de estar en v después de k pasos

$$= \underbrace{\frac{1}{|V|} v_0 + O((1-\epsilon)^k c_1 f_1) + O((1-\epsilon)^k c_2 f_2) + \dots + O(\epsilon^k)}_{\text{decrece}}$$

\downarrow
domina

Aplicaciones de grafos expansores:

Computación teórica:

Códigos de corrección de errores
Super-concentradores
Derandomización
(Redes de comunicación)

Grupos y geometría:

Teoría computacional de grupos
Crecimiento en los grupos
Conexión con la propiedad (tau)
"Embeddings" de grupos en espacios de Hilbert

Teoría de números

Criba afín
y ahora también...

1. Un problema en teoría analítica de números

Def La función de Liouville $\lambda: \mathbb{Z}^+ \rightarrow \mathbb{C}$

$$\lambda(mn) = \lambda(m)\lambda(n) \quad \forall m, n \in \mathbb{Z}^+$$

$$\lambda(p) = -1$$

$$\frac{1}{x} \sum_{n \leq x} \lambda(n) = o(1) \iff \text{TNP}$$

$$\frac{1}{x} \sum_{n \leq x} \lambda(n)\lambda(n+1) \stackrel{?}{=} o(1) : \begin{array}{l} \text{abierto,} \\ \text{muy} \\ \text{difícil} \end{array}$$

caso grado 2 de una conjetura de Chowla

2015: Matomáki-Radziwiłł

para $H \rightarrow \infty$ cuando $N \rightarrow \infty$

$$\frac{1}{NH} \sum_{x=N+1}^{2N} \left| \sum_{n=x+1}^{x+H} \lambda(n) \right| = o(1) \quad (\dagger)$$

(para $N \rightarrow \infty$)

Tao

(*)

Aquí (*) se reduce únicamente a

(**)

$$\frac{1}{\log x} \sum_{n \leq x} \frac{\lambda(n)\lambda(n+1)}{n} = o(1)$$

para $N \rightarrow \infty$

$$\frac{1}{x^{\mathcal{L}}} \sum_{n \leq x} \sum_{\substack{p \in \mathcal{P} \\ p | n}} \lambda(n)\lambda(n+p) = o(1)$$

donde \mathcal{P} = un conjunto de primos

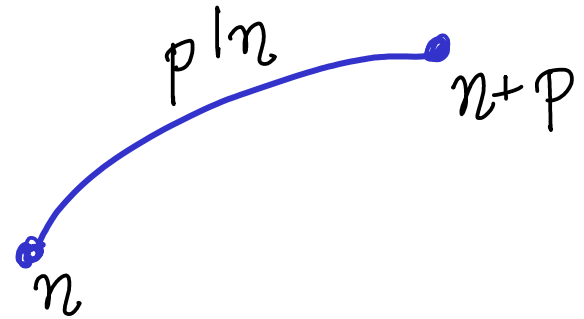
$$\mathcal{L} = \sum_{p \in \mathcal{P}} \frac{1}{p}$$

Lo difícil es reducir (**) a (†)

Un grafo de divisibilidad

$$V = \mathbf{N} = \{N+1, N+2, \dots, 2N\}$$

$$E = \{\{n, n+p\}, n \in \mathbf{N}, n+p \in \mathbf{N}, p \in \mathbf{P}, p|n\}$$



equivalente a grafo considerado en MRT II, Tao

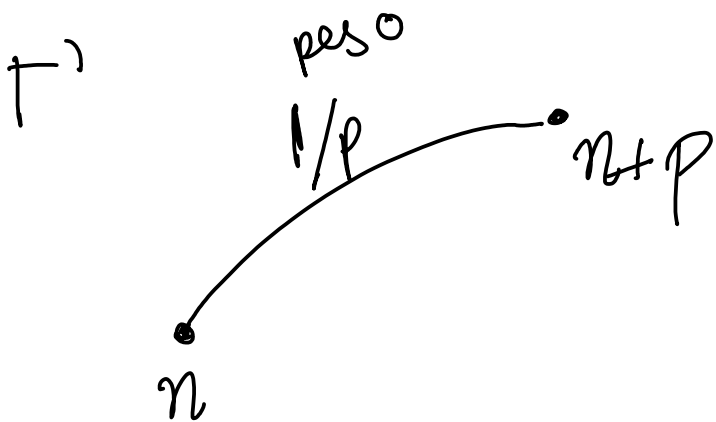
"It may be possible to estimate expressions [...] by establishing some sort of expander graph property." "Unfortunately we were unable to establish such an expansion property, as the [...] standard methods of establishing expansion [do not] work"

Puede Γ ser un expander sin modificaciones?

No: muy local (p pequeño)

- Γ no es regular
- para n primo, el grado del vértice n es 0 ($\mathbf{P} \cap \{1, \dots, N\}$)

meta:
probar expansión local
en casi todos los
puntos



$$A := Ad_T - Ad_{T^*}$$

$$p \in P$$

Es A un expander? (autovalores de A son pequeños)
 aún no: hay vértices de alto grado
 ($n \in \mathbb{N}$ con $\gg \sum_{p \in P} 1/p$ divisores primos)

$$L = \sum_{p \in P} \frac{1}{p}$$

Definiremos un $X \subset \mathbb{N} = \{N+1, \dots, 2N\}$
 t.g. el complemento $\mathbb{N} \setminus X$ es pequeño ($\leq e^{-cL} \cdot N$)

$$(A|_X f) := (A(f|_X))|_X$$

Mostraremos:
 $A|_X$ es un expander fuerte:
 sus autovalores son
 $O(\sqrt{L})$ óptimo
 ("O(Ramanujan)")

Teo. principal Γ, A como digamos, $P \subset [1, H]$ (primos), $\log H \leq \frac{\sqrt{\log N}}{2}$

$\forall C \exists X \subset \mathbb{N}$ con $\geq (1 - e^{-L})N$ elementos $(L = \sum_{p \in P} \frac{1}{p})$

t.g. todo autovector de $A|_X$ es $O(\sqrt{L})$

Corolario: $\frac{1}{\log x} \sum_{n \leq x} \frac{\lambda(n)\lambda(n+1)}{n} = O\left(\frac{1}{\sqrt{\log \log x}}\right)$

comparación: Tao probó $o(1)$

su prueba da

Tao - Teräväinen: $O\left(\frac{1}{(\log \log \log x)^c}\right)$ $c < 1/3$

$O\left(\frac{1}{(\log \log \log \log x)^c}\right)$
(H²-Ukus, AGRAT III)

mejorable
 $c = 1/5$

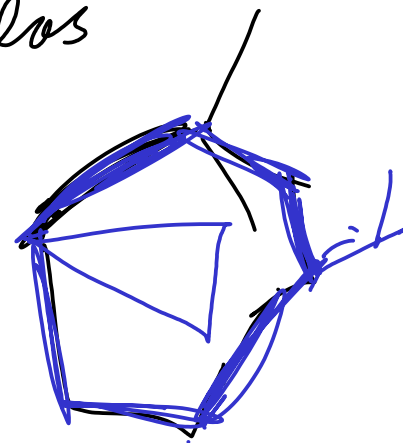
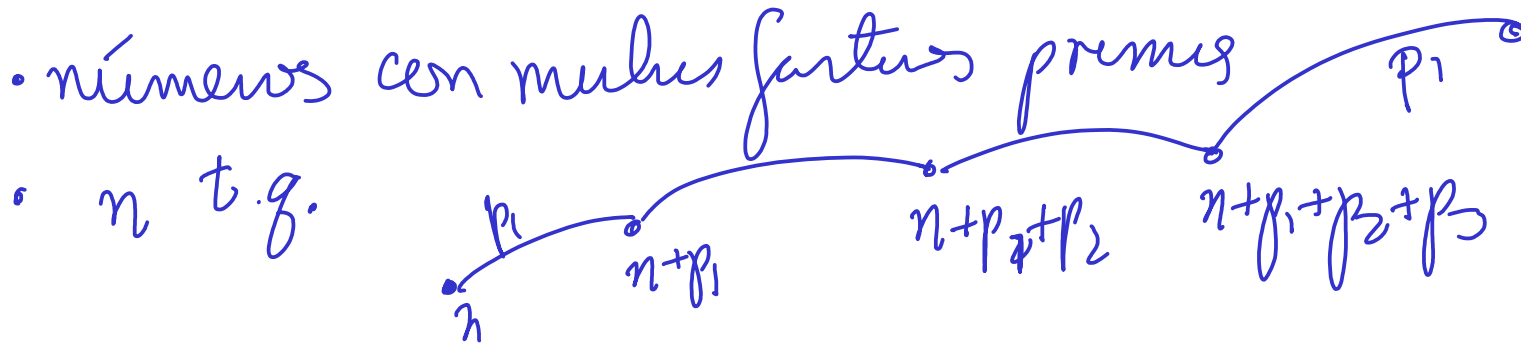
Estrategia de la prueba

0. Si hay un autovalor grande, hay muchos (pues T es "muy local" (+ Hölder))
y entonces $\text{Tr } A^{2k}$ es grande

1. $\sum \lambda = \text{Tr } A = \sum \text{elementos diagonales}$
(matriz)

$\sum \lambda^{2k} = \text{Tr } A^{2k} =$ suma sobre los número de caminatas cerradas

2. Excluimos de X :



de longitud l pequeño

3. Qué es $\text{Tr}(A|X)^{2k}$?

Bueno, qué es $\text{Tr} A^{2k}$?

Correlación para
(completa)

camminatas con muchos "lados" p
(longitudes
de aristas

no repetidos

→ contar camminatas cerradas
con pesos primos no repetidos

Qué es $\text{Tr}(A|X)^{2k}$?

Correlación
imperfecta

Prueba:

- modelo de Kuhnlein
(lema fundamental
de cribas)
- criba no tradicional
(modelos compuestos)

Teorema de "cross-cut" de Rota

El Teorema principal da:

Para $f, g: \mathbb{N} \rightarrow \mathbb{C}$
 $\{N+1, \dots, 2N\}$

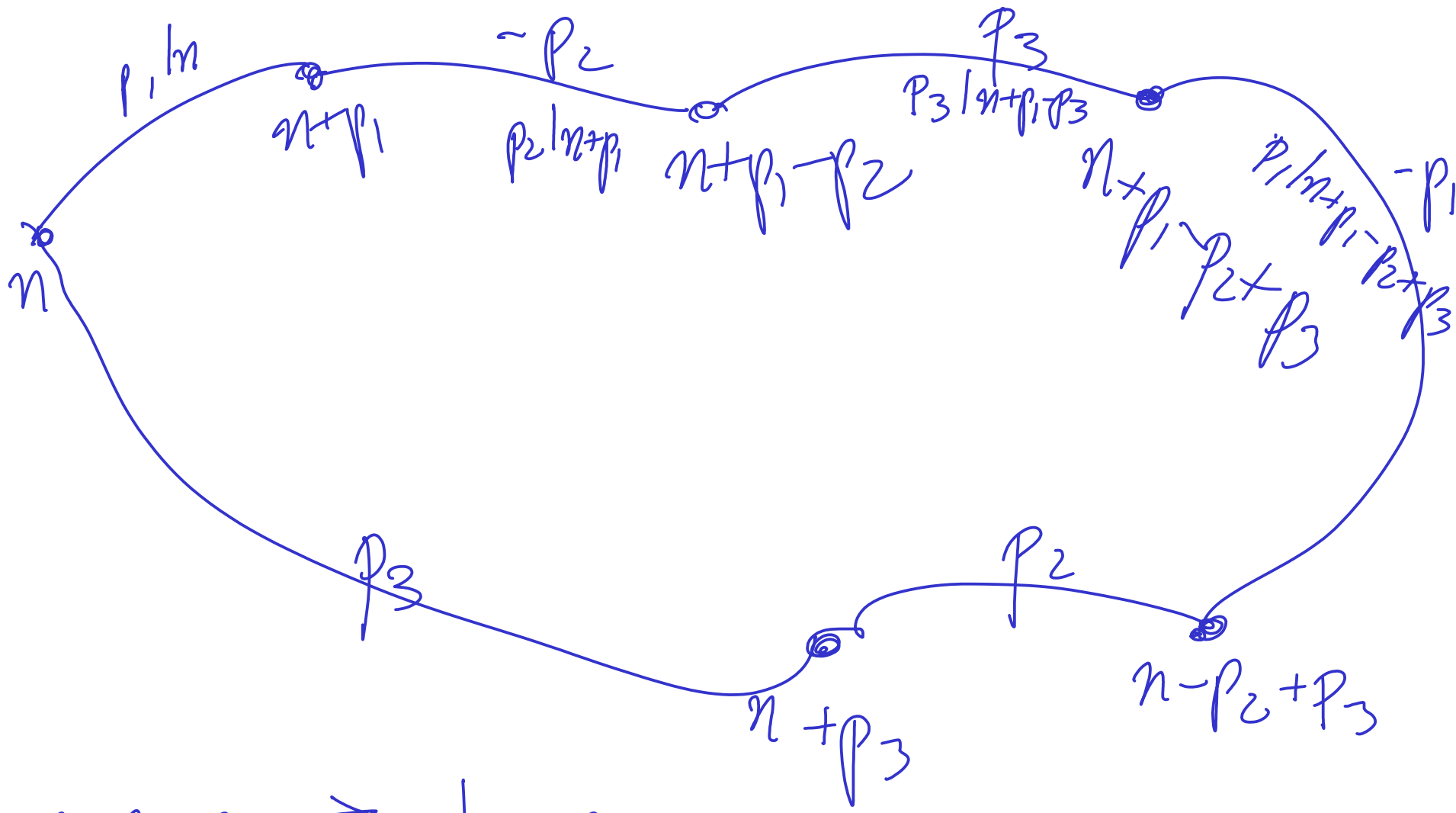
con $|f(n), g(n)| \leq (\log N)^c$

$$\frac{1}{N^2} \left(\sum_{n \in \mathbb{N}} \sum_{\substack{p \in \mathbb{P} \\ p|n}} f(n) \overline{g(n+p)} - \sum_{n \in \mathbb{N}} \sum_{p \in \mathbb{P}} \frac{f(n) \overline{g(n+p)}}{p} \right) = O\left(\frac{1}{\sqrt{N}}\right)$$

\uparrow
 $g(n+p) + g(n-p)$

Suma
que
queremos
conocer

\uparrow para $f, g = \lambda$
se estima
mediante
Matemática
- Hardy-Littlewood



$$p_1 | n$$

$$\wedge p_1 | n + p_1 - p_2 + p_3 \Rightarrow p_1 | p_2 + p_3$$

$p_2 | \dots$
 $p_3 | \dots$

Contar tuplas

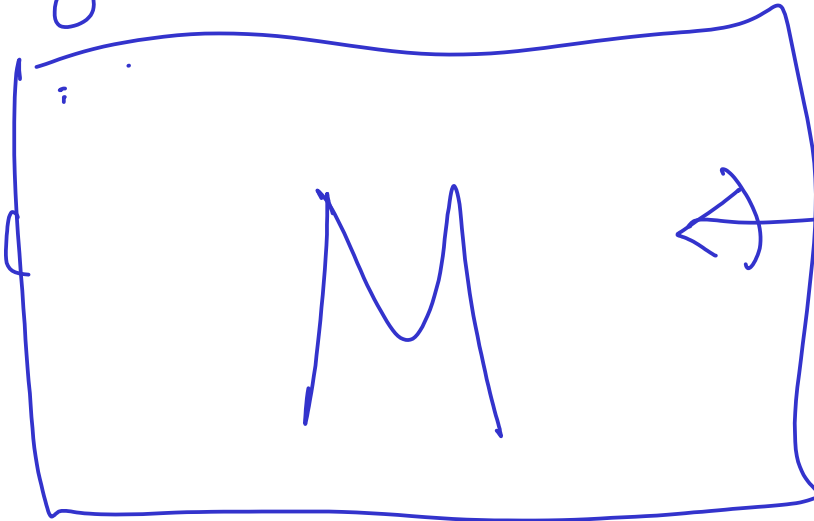
(p_1, \dots, p_k)

que satisfacen condiciones de divisibilidad

M trivial



p_1
 p_2
 p_3
 p_4



combinaciones
lineales de

p_1, \dots, p_k

cuántas
veces aparecen
entre p_i y p_i

geometría
de números
básica

se reduce a:

mostrar que (usualmente)

M tiene una submatriz
con filas y columnas desjuntas y rango
grande

Como se prueba?

grafo $G_n :=$

vértices = clases
de equivalencia
de \sim

n en
 $\{1, \dots, 2k\}$

$i \sim j$ si
el mismo
punto aparece
en los paros
 i y j

arista = $\{[i], [i+1]\}$

todo grafo con
muchos vértices
de grado $\neq 2$ tendrá
un árbol
recubridor
con muchas
hojas

$\{1, 4\}, \{2, 5\}, \{3\}, \{6\}$

induce



Prop Si hay un SCV
con ∂S grande,
existe un submatriz de M con filas y columnas
de rango grande

de M con filas y columnas
de rango grande