El teorema de Freiman-Ruzsa

Dirigido por Javier Cilleruelo

Espacios pequeños entre primos

Dirigido por Fernando Chamizo

Carlos Vinuesa del Río

2006

Cursos de doctorado

- Principios de análisis matemático (José García-Cuerva)
- Curvas algebraicas y aplicaciones (Adolfo Quirós)
- Procesos estocásticos (José Ramón Berrendero)
- Análisis de Fourier y aplicaciones (Eugenio Hernández)
- Geometría algebraica (Orlando Villamayor)

Trabajos de investigación

- El teorema de Freiman-Ruzsa
  Dirigido por Javier Cilleruelo
- Espacios pequeños entre primos
  Dirigido por Fernando Chamizo

Justificando el tiempo empleado en la presentación...

Una teoría matemática no se puede considerar completa hasta que la hagas tan clara que se la puedas explicar a la gente de la calle.
David Hilbert

Justificando el tiempo empleado en la presentación...

Una teoría matemática no se puede considerar completa hasta que la hagas tan clara que se la puedas explicar a la gente de la calle.
David Hilbert

A los doce años sabía dibujar como Rafael pero necesité toda una vida para poder aprender a pintar como un niño.
Pablo Picasso

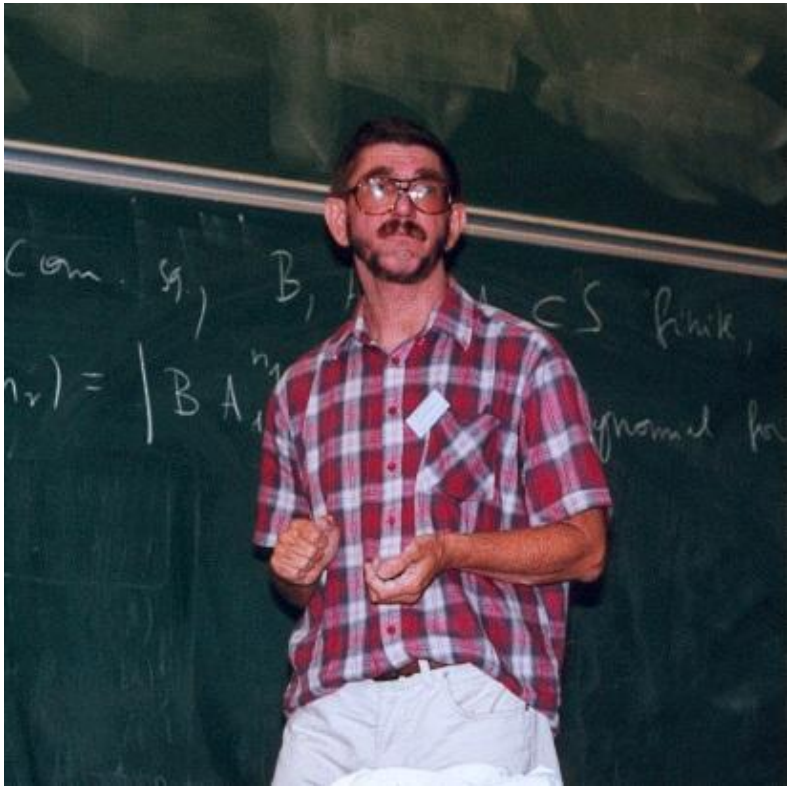
El teorema de Freiman-Ruzsa

Ben Joseph Green

Autor de la referencia básica,
Structure Theory of Set Addition

Gregory A. Freiman

Creador del resultado principal, que da nombre tanto al teorema como al concepto clave de *homomorfismo de Freiman*



Imre Z. Ruzsa

Redescubrió y simplificó el trabajo de Plünnecke, lo que le permitió llegar a su prueba del teorema

Mei-Chu Chang

Autora de los resultados que hacen mejorar el orden de las cotas en el teorema

¿Qué es el conjunto suma?

Dado un subconjunto de los enteros (finito y no vacío),

$$A = \{a_1, a_2, \ldots, a_n\}$$

(suponemos, por simplificar, $a_1 < a_2 < \cdots < a_n$), definimos

Conjunto suma

$$A + A = \{a + a' : a, a' \in A\}$$

Pregunta

¿Cómo de **grande** o **pequeño** puede ser $A + A$?

Grande y pequeño

Números al azar, por favor.

Grande y pequeño

$$7 \quad 25 \quad 49 \quad 85 \quad 100 \quad 113$$

Grande y pequeño

$+$	7	25	49	85	100	113
7						
25						
49						
85						
100						
113						

Grande y pequeño

+	**7**	**25**	**49**	**85**	**100**	**113**
7	14	32	56	92	107	120
25		50	74	110	125	138
49			98	134	149	162
85				170	185	198
100					200	213
113						226

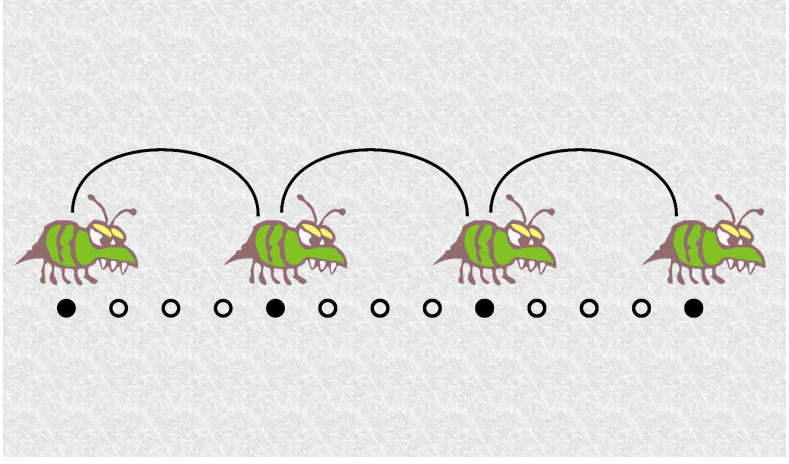
Grande y pequeño

+	**7**	**25**	**49**	**85**	**100**	**113**
7	14	32	56	92	107	120
25		50	74	110	125	138
49			98	134	149	162
85				170	185	198
100					200	213
113						226

Idea

Si tomamos **números al azar**, las sumas son todas o casi todas distintas. Es decir, el conjunto suma es **grande**.

Grande y pequeño



Progresión aritmética, por favor.

Grande y pequeño

$$\mathbf{5} \qquad \mathbf{10} \qquad \mathbf{15} \qquad \mathbf{20} \qquad \mathbf{25} \qquad \mathbf{30}$$

Grande y pequeño

$+$	5	10	15	20	25	30
5						
10						
15						
20						
25						
30						

Grande y pequeño

+	**5**	**10**	**15**	**20**	**25**	**30**
5	10	15	20	25	30	35
10		20	25	30	35	40
15			30	35	40	45
20				40	45	50
25					50	55
30						60

Grande y pequeño

+	**5**	**10**	**15**	**20**	**25**	**30**
5	10	15	20	25	30	35
10		20	25	30	35	40
15			30	35	40	45
20				40	45	50
25					50	55
30						60

Grande y pequeño

$+$	**5**	**10**	**15**	**20**	**25**	**30**
5	10	15	20	25	30	35
10		20	25	30	35	40
15			30	35	40	45
20				40	45	50
25					50	55
30						60

Idea

Si tomamos **progresiones aritméticas**, muchas sumas se repiten. Es decir, el conjunto suma es **pequeño**.

Ejemplos extremos

Pregunta (y respuesta)

¿Cuánto es lo **máximo** que puede valer $|A+A|$?

$$|A+A| \leq \frac{|A|(|A|+1)}{2}$$

$+$	a_1	a_2	$\dots$	a_n
a_1	●	●	●	●
a_2	○	●	●	●
$\dots$	○	○	●	●
a_n	○	○	○	●

Y Gauss dijo cuando era pequeño que $1+2+\cdots+n = \frac{n(n+1)}{2}$.

Ejemplos extremos

Pregunta (y respuesta)

¿Cuánto es lo **mínimo** que puede valer $|A+A|$?

$$|A+A| \geq 2|A| - 1$$

Lema

Sea $A \subseteq \mathbb{Z}$. Entonces $|A+A| \geq 2|A| - 1$, con igualdad si y sólo si A es una **progresión aritmética**.

$+$	a_1	a_2	$\ldots$	a_n
a_1	●	●	●	●
a_2	○	○	○	●
$\ldots$	○	○	○	●
a_n	○	○	○	●

Ejemplos extremos

Ejemplo

Ya sabemos que para todas las progresiones aritméticas el conjunto suma es **pequeño**, de hecho se alcanza la cota inferior.
No es difícil encontrar conjuntos un poco menos estructurados para los que $|A+A|$ siga siendo **pequeño**. Por ejemplo, si nos conformamos con $|A+A| \leq 100|A|$, podemos tomar como A cualquier subconjunto de n elementos de una progresión aritmética, P, de longitud $50n$.

$$|A+A| \leq |P+P| = 100n-1 \leq 100n = 100|A|$$

Ejemplos extremos

Pregunta (muy importante)

En general $|A+A|$ es grande y sólo en casos muy especiales es pequeño. ¿Podemos caracterizar estos pocos casos?

¿Qué es una progresión aritmética generalizada? I

Una generalización natural de las progresiones aritméticas.

Dados $x_0, x \in \mathbb{Z}$ y $m \in \mathbb{Z}_{>0}$, una progresión aritmética es

$$P = \{x_0 + \lambda x \mid 0 \leq \lambda \leq m-1\}$$

Podemos relajar un poco la definición para tener

Dados $x_0 \in \mathbb{Z}$, $\overline{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{Z}^d$ y $m_1, m_2, \ldots m_d \in \mathbb{Z}_{>0}$, una progresión aritmética generalizada de dimensión d es

$$P = \{x_0 + \overline{\lambda} \cdot \overline{x} \mid \overline{\lambda} \in Q\}$$

donde $Q = [0, m_1 - 1] \times [0, m_2 - 1] \times \cdots \times [0, m_d - 1] \cap \mathbb{Z}^d$.

El **volumen** de la progresión es $|Q| = |m_1 m_2 \cdots m_d|$.

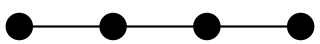
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética (dimensión 1)

Dados $x_0, x_1 \in \mathbb{Z}$ y $m_1 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 \mid 0 \leq \lambda_1 \leq m_1 - 1\}$$

Partimos de un intervalo de longitud $m_1 - 1$



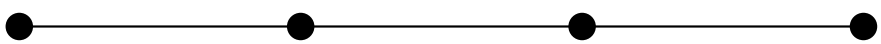
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética (dimensión 1)

Dados $x_0, x_1 \in \mathbb{Z}$ y $m_1 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 \mid 0 \leq \lambda_1 \leq m_1 - 1\}$$

Lo dilatamos por la razón x_1.



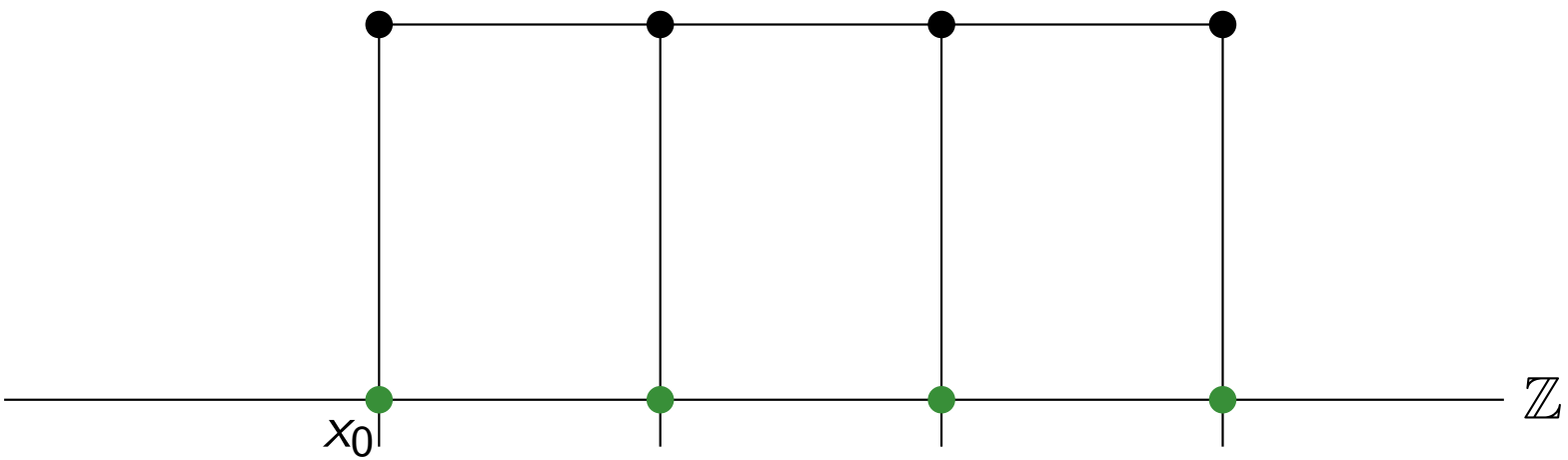
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética (dimensión 1)

Dados $x_0, x_1 \in \mathbb{Z}$ y $m_1 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 \mid 0 \leq \lambda_1 \leq m_1 - 1\}$$

Lo proyectamos sobre $\mathbb{Z}$.



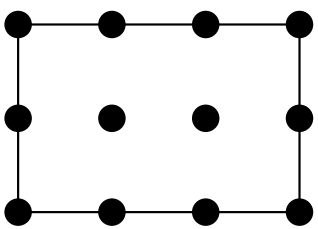
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 2)

Dados $x_0, x_1, x_2 \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 \mid (\lambda_1, \lambda_2) \in [0, m_1 - 1] \times [0, m_2 - 1]\}$$

Partimos de un rectángulo de base $m_1 - 1$ y altura $m_2 - 1$



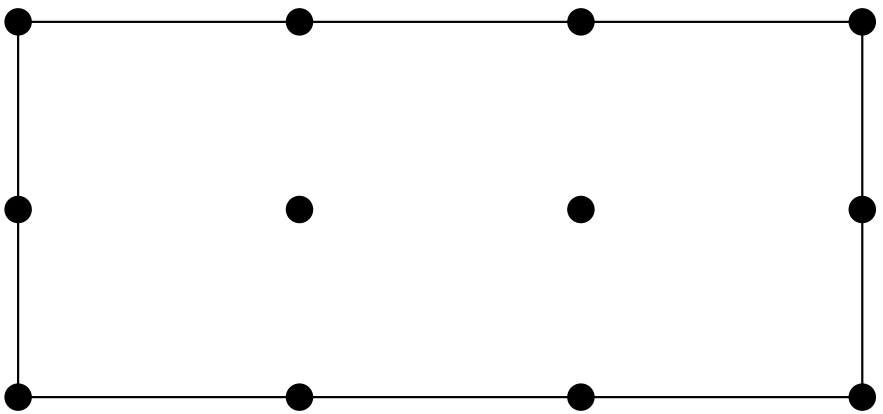
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 2)

Dados $x_0, x_1, x_2 \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 \mid (\lambda_1, \lambda_2) \in [0, m_1 - 1] \times [0, m_2 - 1]\}$$

Lo dilatamos por las razones x_1 y x_2 respectivamente.



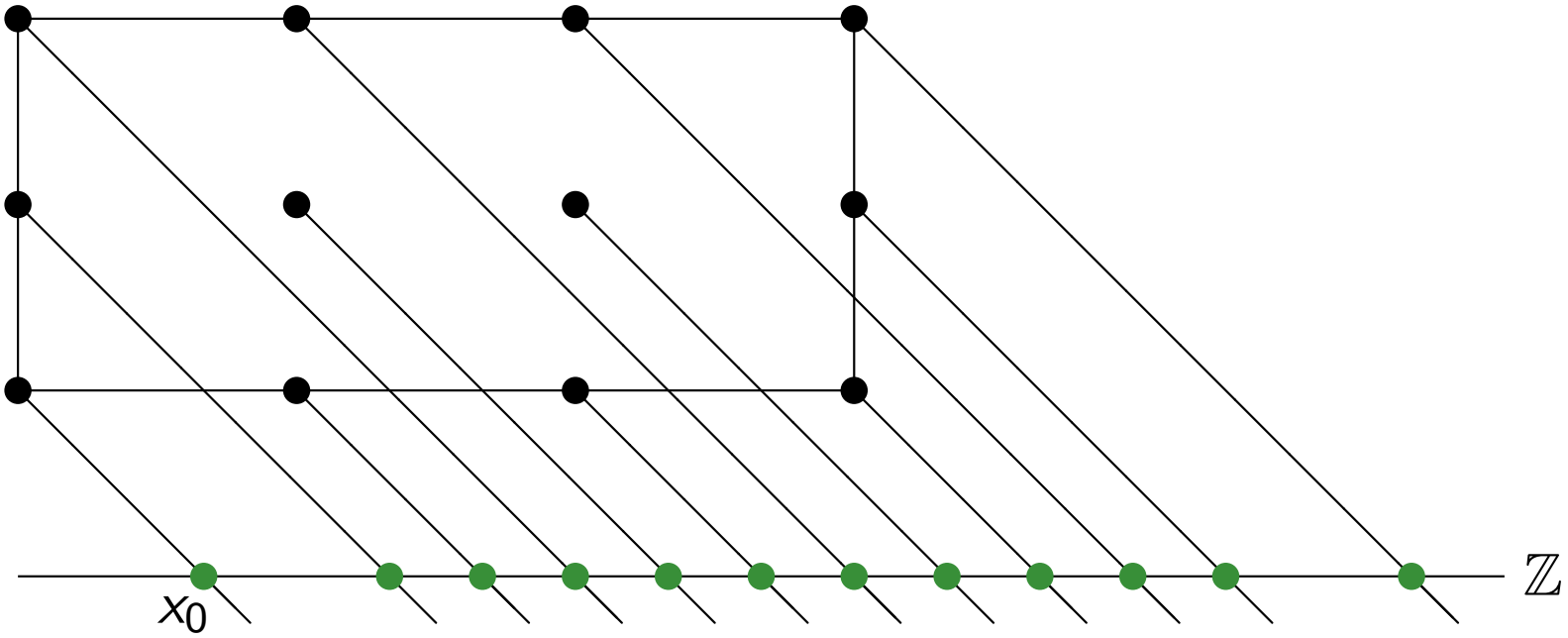
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 2)

Dados $x_0, x_1, x_2 \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 \mid (\lambda_1, \lambda_2) \in [0, m_1 - 1] \times [0, m_2 - 1]\}$$

Lo proyectamos sobre $\mathbb{Z}$.



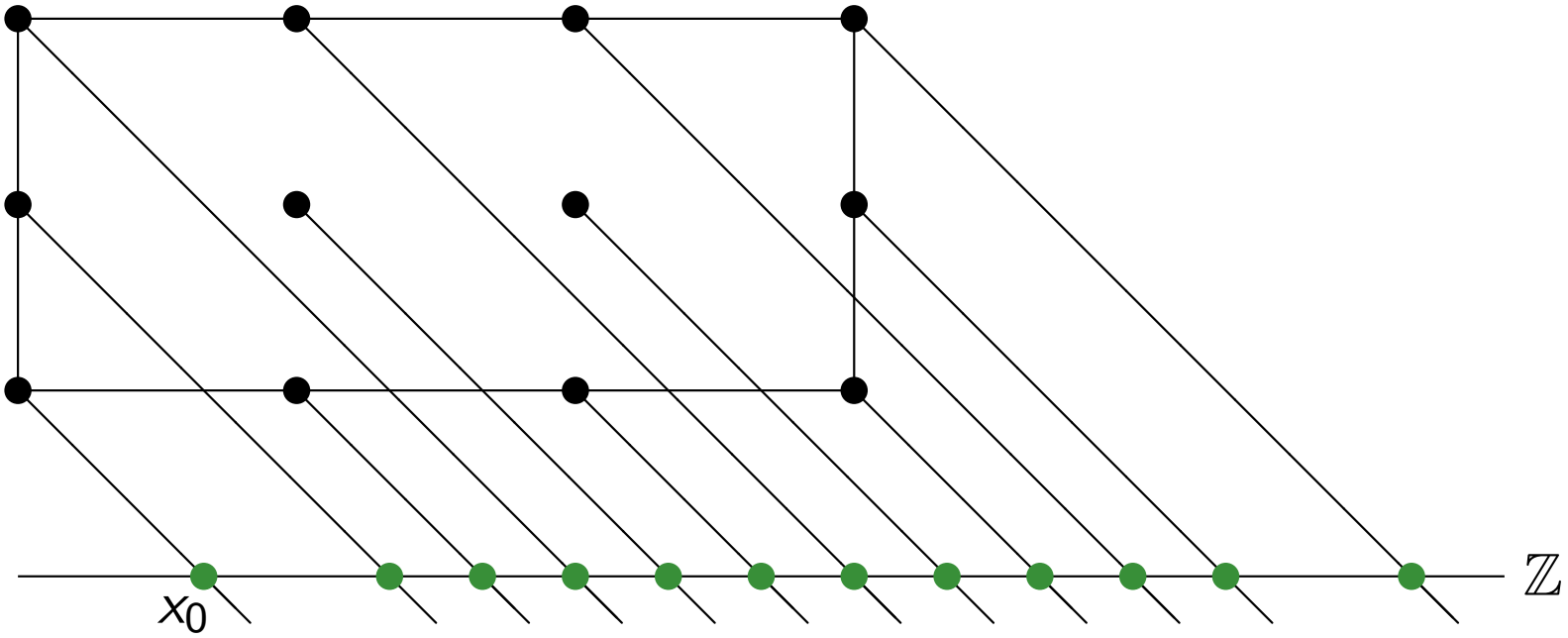
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 2)

Dados $x_0, x_1, x_2 \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 \mid (\lambda_1, \lambda_2) \in [0, m_1 - 1] \times [0, m_2 - 1]\}$$

Proyección con las rectas de pendiente -1, las rectas $x + y =$ constante.



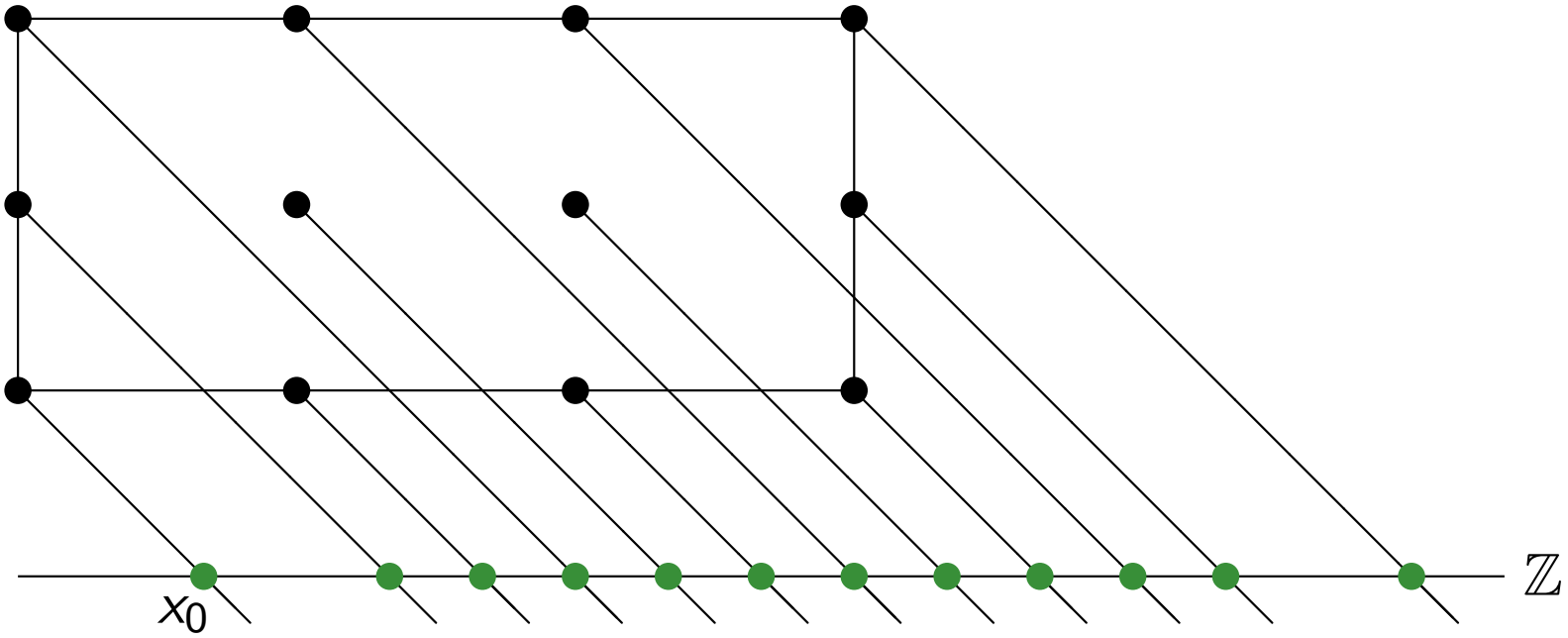
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 2)

Dados $x_0, x_1, x_2 \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 \mid (\lambda_1, \lambda_2) \in [0, m_1 - 1] \times [0, m_2 - 1]\}$$

Si dos puntos de arriba comparten diagonal entonces dan la misma suma abajo.



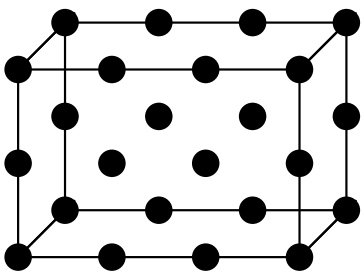
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 3)

Dados $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ y $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \mid (\lambda_1, \lambda_2, \lambda_3) \in [0, m_1 - 1] \times [0, m_2 - 1] \times [0, m_3 - 1]\}$$

Partimos de un prisma de dimensiones $m_1 - 1$, $m_2 - 1$ y $m_3 - 1$



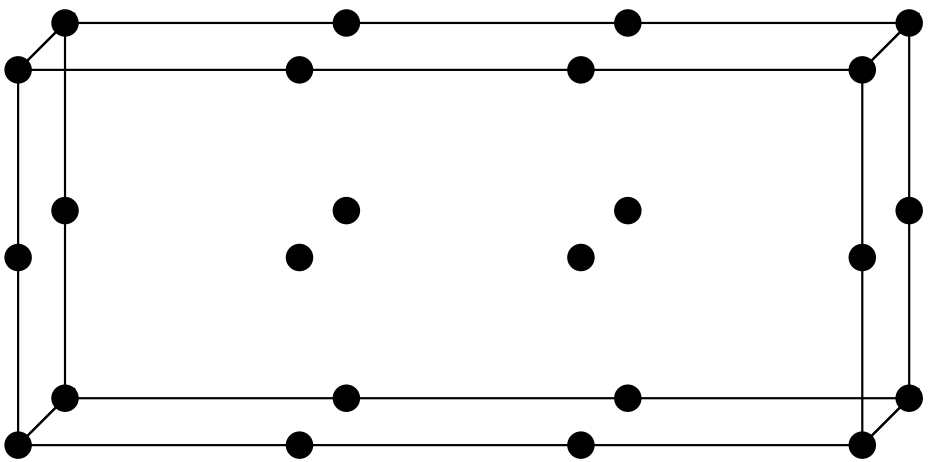
¿Qué es una progresión aritmética generalizada? II

Progresión aritmética generalizada (dimensión 3)

Dados $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ y $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \mid (\lambda_1, \lambda_2, \lambda_3) \in [0, m_1 - 1] \times [0, m_2 - 1] \times [0, m_3 - 1]\}$$

Lo dilatamos por las razones x_1, x_2 y x_3 respectivamente.



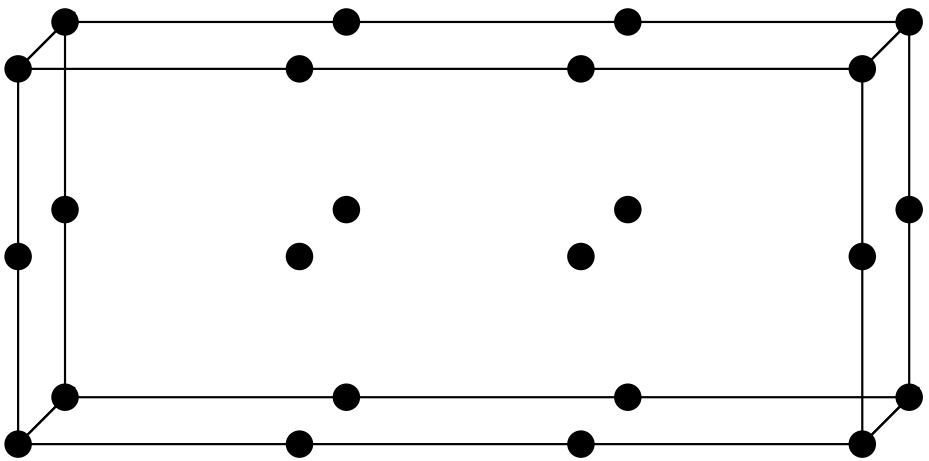
¿Qué es una progresión aritmética generalizada? II

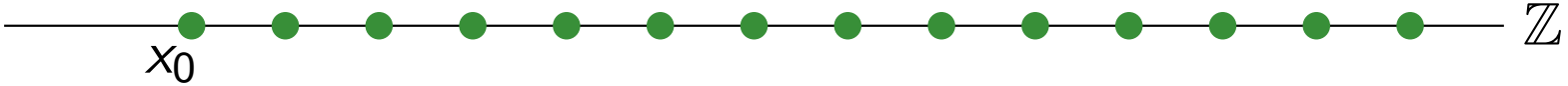
Progresión aritmética generalizada (dimensión 3)

Dados $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ y $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \mid (\lambda_1, \lambda_2, \lambda_3) \in [0, m_1 - 1] \times [0, m_2 - 1] \times [0, m_3 - 1]\}$$

Lo proyectamos sobre $\mathbb{Z}$.





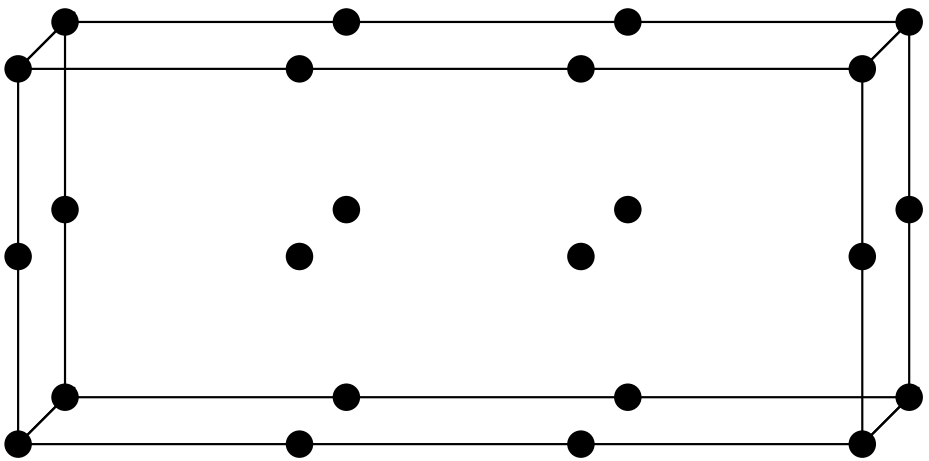
¿Qué es una progresión aritmética generalizada? II

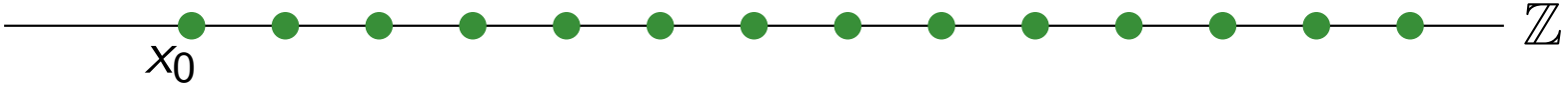
Progresión aritmética generalizada (dimensión 3)

Dados $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ y $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \mid (\lambda_1, \lambda_2, \lambda_3) \in [0, m_1 - 1] \times [0, m_2 - 1] \times [0, m_3 - 1]\}$$

Proyección con los planos $x + y + z =$ constante.





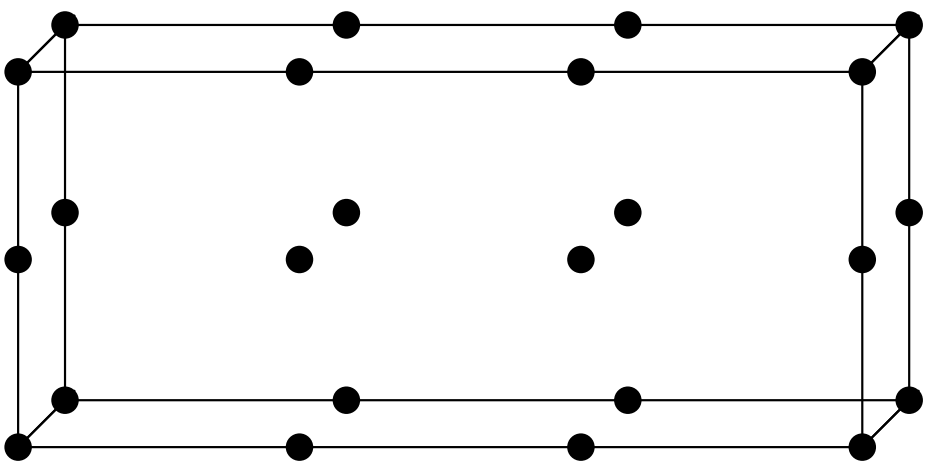
¿Qué es una progresión aritmética generalizada? II

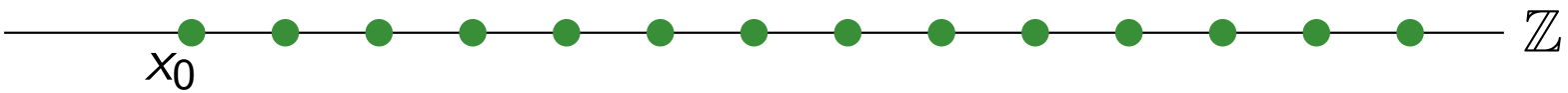
Progresión aritmética generalizada (dimensión 3)

Dados $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ y $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$,

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 \mid (\lambda_1, \lambda_2, \lambda_3) \in [0, m_1 - 1] \times [0, m_2 - 1] \times [0, m_3 - 1]\}$$

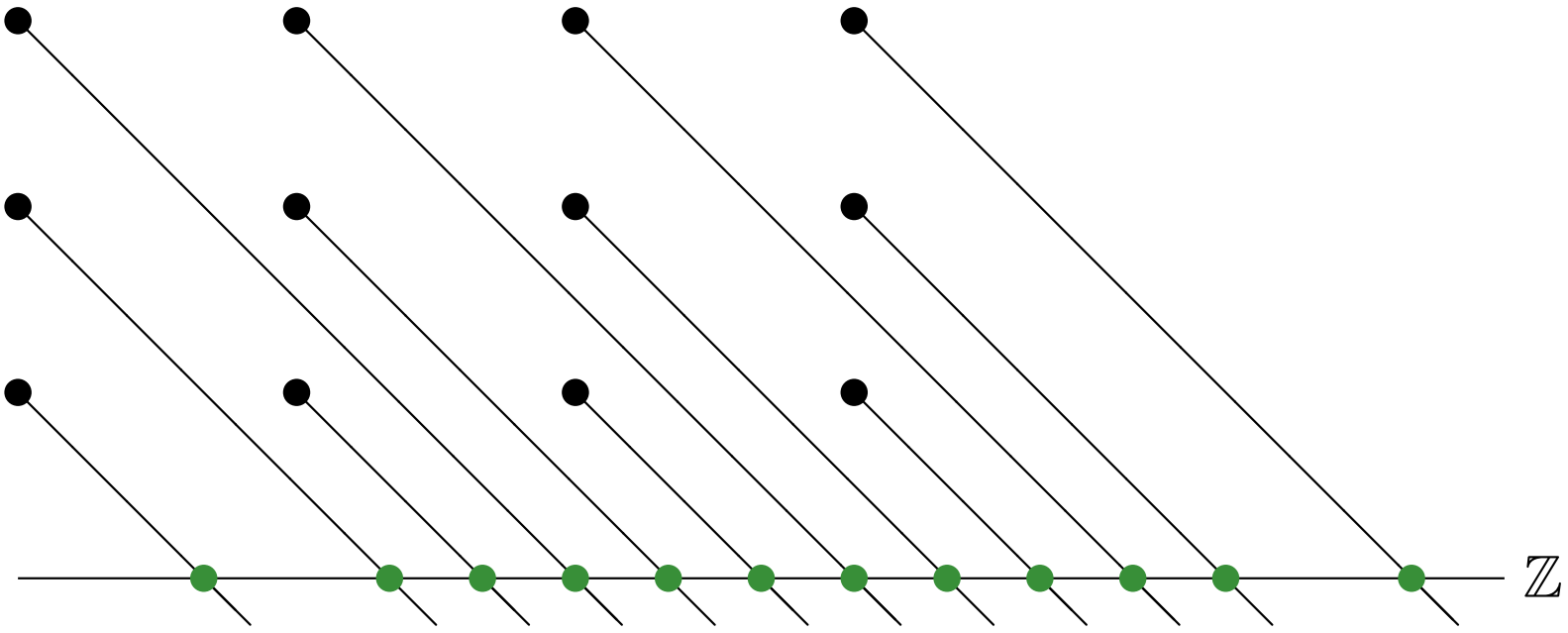
Si dos puntos de arriba comparten plano entonces dan la misma suma abajo.





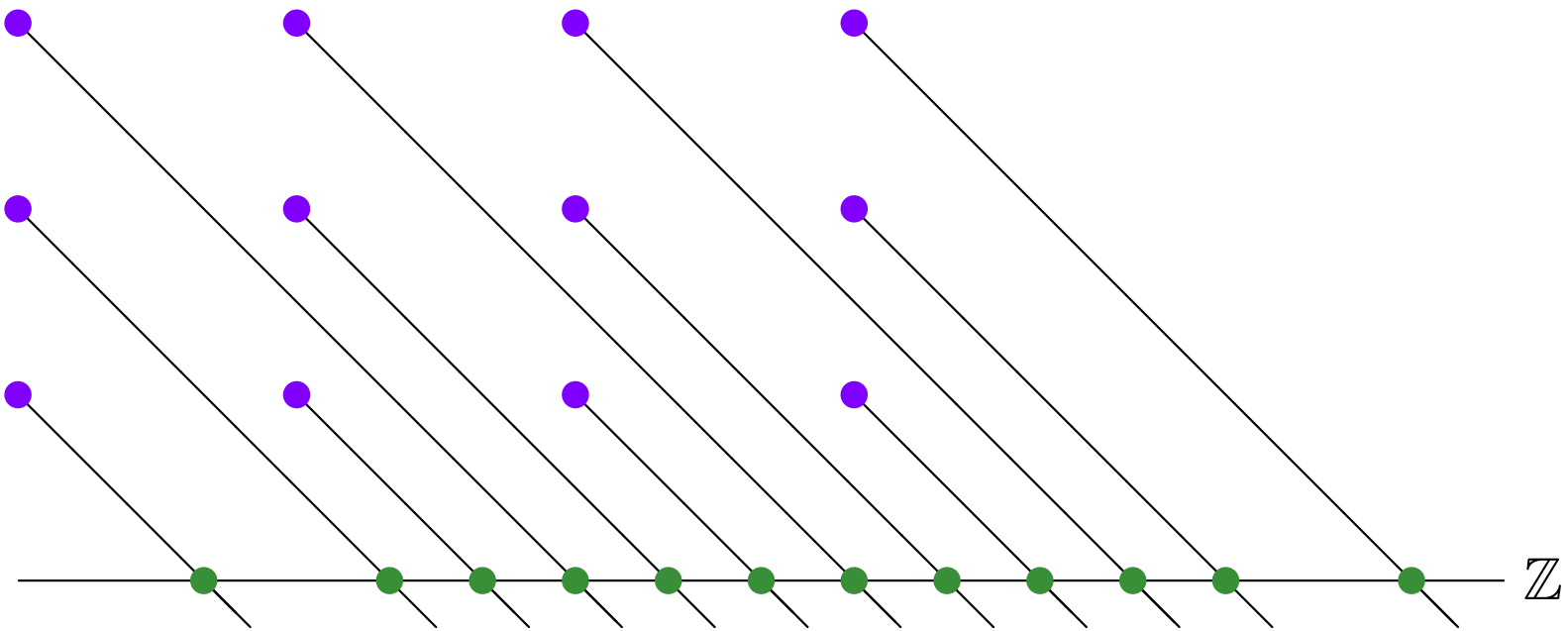
¿Qué es una progresión aritmética generalizada? II

Así que, en general, podemos ver una progresión aritmética generalizada como la imagen de una aplicación de un "prisma d-dimensional" a los enteros.



¿Qué es una progresión aritmética generalizada? II

- El **tamaño** de una progresión aritmética generalizada es su número de elementos.
- El **volumen** de una progresión aritmética generalizada es $m_1 m_2 \cdots m_d$.
- Una progresión aritmética generalizada es **propia** si y sólo si su volumen es igual a su tamaño.



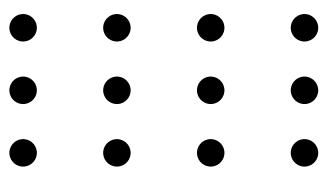
¡Otra vez conjunto suma pequeño!

Observación

Para una **progresión aritmética generalizada** de dimensión d tenemos

$$|P + P| \leq 2^d |P|$$

Geométricamente, el prisma d-dimensional se ve repetido 2^d veces (en realidad un poco menos) para formar el prisma de $|P + P|$:



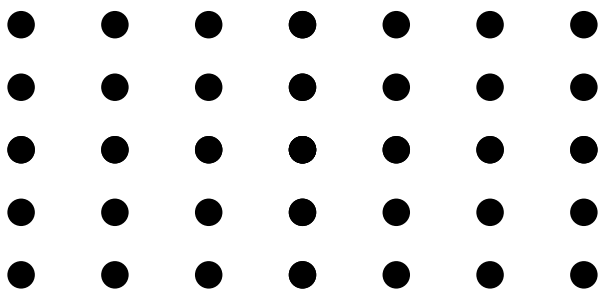
¡Otra vez conjunto suma pequeño!

Observación

Para una **progresión aritmética generalizada** de dimensión d tenemos

$$|P + P| \leq 2^d |P|$$

Geométricamente, el prisma d-dimensional se ve repetido 2^d veces (en realidad un poco menos) para formar el prisma de $|P + P|$:



¡Otra vez conjunto suma pequeño!

Ejemplo

Así que para todas las progresiones aritméticas generalizadas el conjunto suma es **pequeño**.
Al igual que ocurría con las progresiones aritméticas, podemos tomar subconjuntos suficientemente grandes de progresiones aritméticas generalizadas y el conjunto suma seguirá siendo **pequeño**.

¡Otra vez conjunto suma pequeño!

Lo que hemos conseguido

Como una progresión aritmética es obviamente una progresión aritmética generalizada de dimensión 1, lo que hemos probado hasta ahora es que:

Las progresiones aritméticas generalizadas y sus subconjuntos "significativos" (grandes) tienen conjunto suma pequeño.

¿Habrá más ejemplos?

El resultado de Freiman nos dice que las **progresiones aritméticas generalizadas** y sus subconjuntos grandes son los únicos ejemplos en los que el conjunto suma es **pequeño**.

Teorema de Freiman

Sea $A \subseteq \mathbb{Z}$ y supongamos que $|A + A| \leq C|A|$. Entonces A está contenido en una progresión aritmética d-dimensional de tamaño a lo sumo $K|A|$, donde d y K dependen sólo de C.

Obviamente, tanto K como d sólo pueden depender de C, pues si pudieran depender de A el teorema diría una tontería...

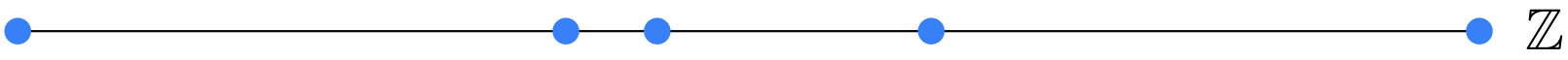
¿Habrá más ejemplos?

El resultado de Freiman nos dice que las **progresiones aritméticas generalizadas** y sus subconjuntos grandes son los únicos ejemplos en los que el conjunto suma es **pequeño**.

Teorema de Freiman

Sea $A \subseteq \mathbb{Z}$ y supongamos que $|A + A| \leq C|A|$. Entonces A está contenido en una progresión aritmética d-dimensional de tamaño a lo sumo $K|A|$, donde d y K dependen sólo de C.

. . . porque, por ejemplo, todo conjunto está contenido en el intervalo que va desde su mínimo a su máximo, que es una progresión aritmética.



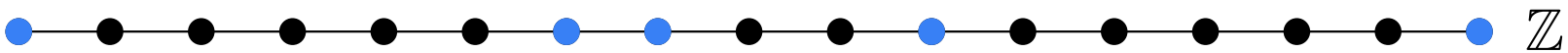
¿Habrá más ejemplos?

El resultado de Freiman nos dice que las **progresiones aritméticas generalizadas** y sus subconjuntos grandes son los únicos ejemplos en los que el conjunto suma es **pequeño**.

Teorema de Freiman

Sea $A \subseteq \mathbb{Z}$ y supongamos que $|A + A| \leq C|A|$. Entonces A está contenido en una progresión aritmética d-dimensional de tamaño a lo sumo $K|A|$, donde d y K dependen sólo de C.

. . . porque, por ejemplo, todo conjunto está contenido en el intervalo que va desde su mínimo a su máximo, que es una progresión aritmética.



¿Habrá más ejemplos?

El resultado de Freiman nos dice que las **progresiones aritméticas generalizadas** y sus subconjuntos grandes son los únicos ejemplos en los que el conjunto suma es **pequeño**.

Teorema de Freiman

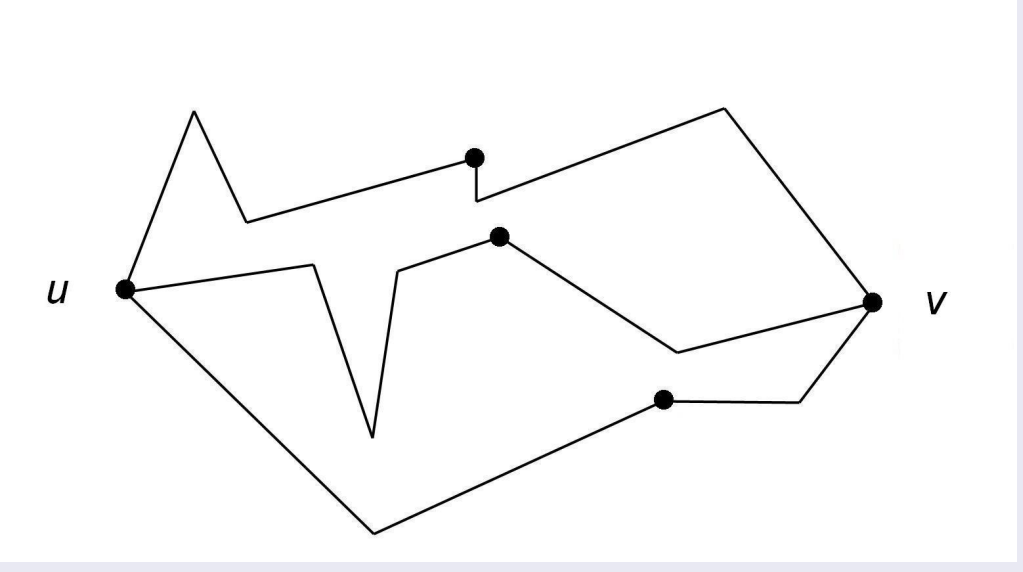
Sea $A \subseteq \mathbb{Z}$ y supongamos que $|A + A| \leq C|A|$. Entonces A está contenido en una progresión aritmética d-dimensional de tamaño a lo sumo $K|A|$, donde d y K dependen sólo de C.

Dicho de otro modo, **si A tiene conjunto suma pequeño, entonces es un subconjunto grande de una progresión aritmética generalizada de dimensión pequeña**.

La desigualdad de Plünnecke

Observación

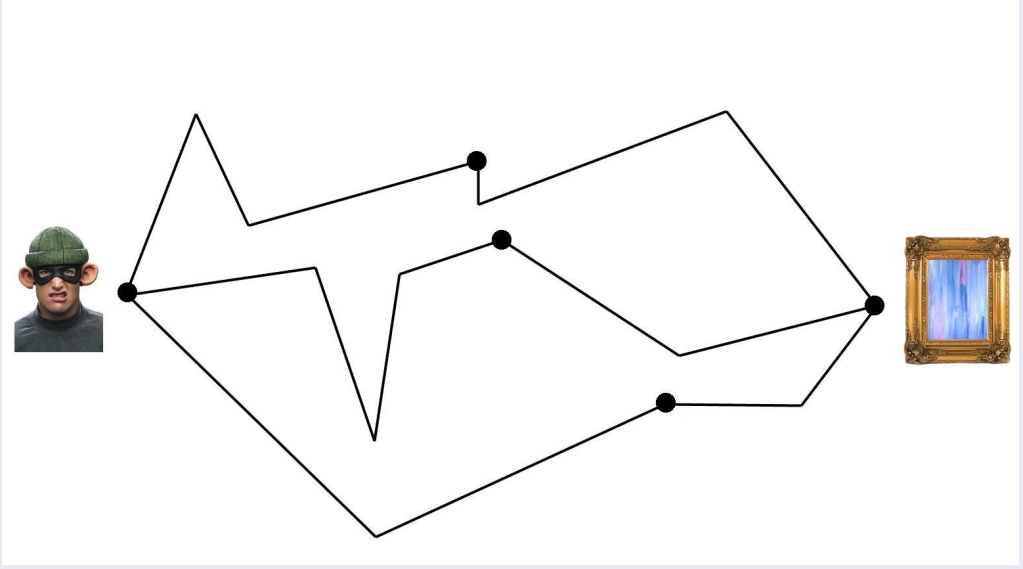
Si u y v son dos vértices no adyacentes en un grafo, entonces: El máximo número de caminos disjuntos de u a v es **menor o igual** que el mínimo número de vértices que hay que quitar para desconectar u de v.



La desigualdad de Plünnecke

Observación

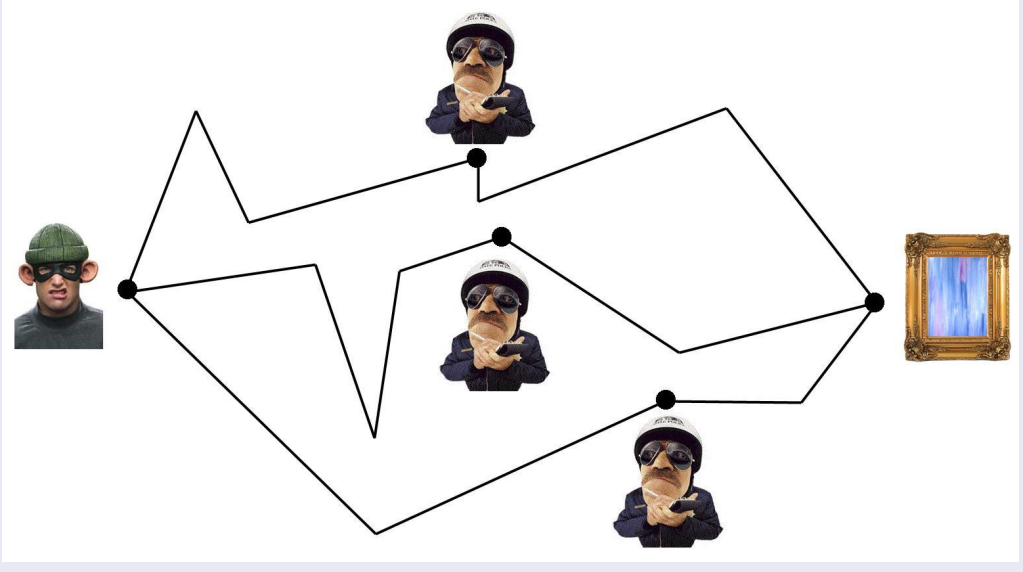
Si u y v son dos vértices no adyacentes en un grafo, entonces: El máximo número de caminos disjuntos de u a v es **menor o igual** que el mínimo número de vértices que hay que quitar para desconectar u de v.



La desigualdad de Plünnecke

Observación

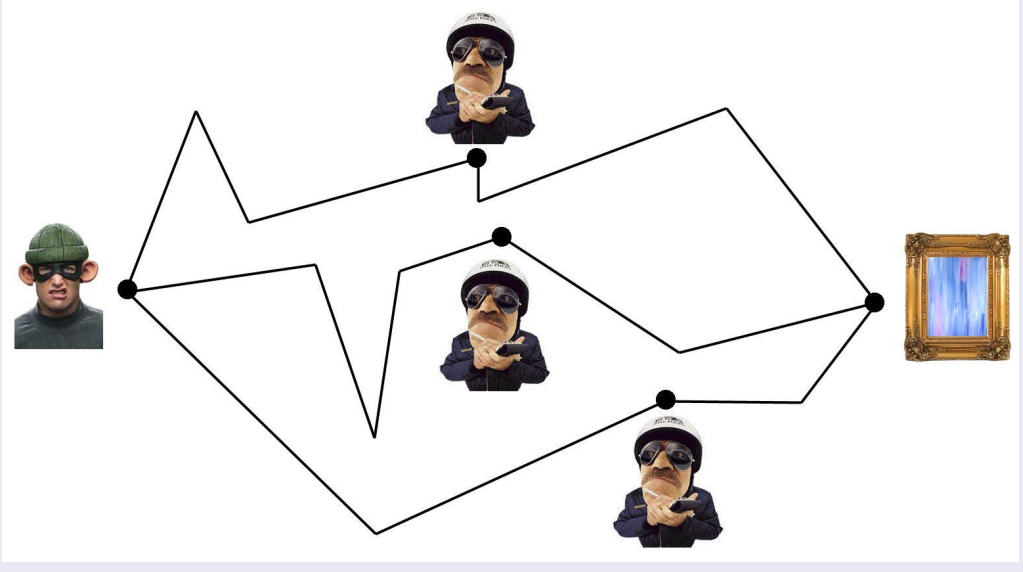
Si u y v son dos vértices no adyacentes en un grafo, entonces: El máximo número de caminos disjuntos de u a v es **menor o igual** que el mínimo número de vértices que hay que quitar para desconectar u de v.



La desigualdad de Plünnecke

Teorema de Menger

Si u y v son dos vértices no adyacentes en un grafo, entonces: El máximo número de caminos disjuntos de u a v es ~~**menor o**~~ **igual** que el mínimo número de vértices que hay que quitar para desconectar u de v.



La desigualdad de Plünnecke

Dados $k, l \in \mathbb{Z}_{\geq 0}$ podemos generalizar el conjunto suma:

$$kA = \{a_1 + \cdots + a_k : a_i \in A\}$$

$$kA - lA = \{a_1 + \cdots + a_k - a'_1 - \cdots - a'_l : a_i, a'_i \in A\}$$

Teorema de Plünnecke-Ruzsa

Si $|A + A| \leq C|A|$ **entonces** $|kA - lA| \leq C^{k+l}|A|$**.**

La desigualdad de Plünnecke se prueba utilizando **teoría de grafos**, en particular el teorema de Menger. Se consideran grafos cuyos vértices son los elementos de ciertos conjuntos suma.

Entornos de Bohr

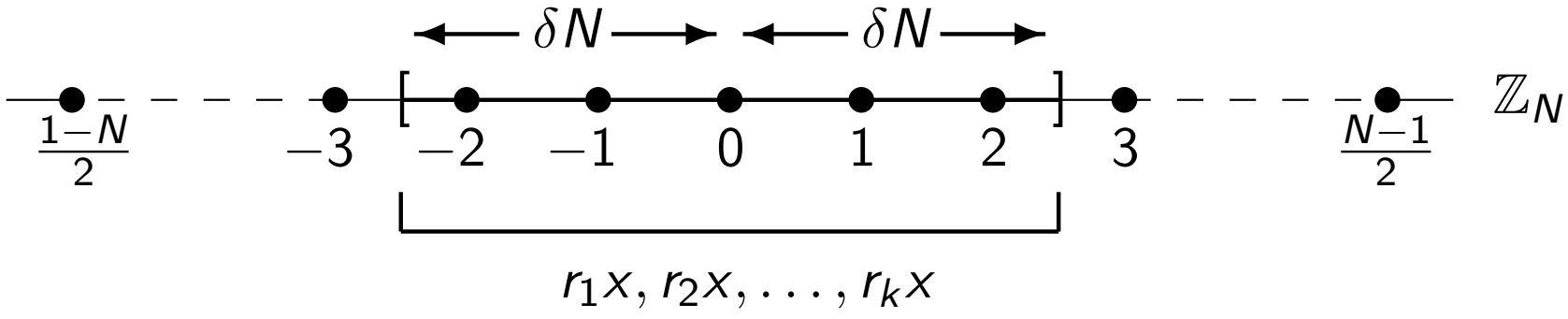
N es un primo impar. Definimos en $\mathbb{Z}_N$ los entornos de Bohr.

Sea $R \subseteq \mathbb{Z}_N$, y sea $\delta > 0$ un número real. El entorno de Bohr $B(R, \delta)$ es el conjunto

$$\left\{ x \in \mathbb{Z}_N \middle| \left\| \frac{rx}{N} \right\| \leq \delta \text{ para todo } r \in R \right\},$$

donde $\|y\|$ representa la distancia de y al entero más cercano.

Si $R = \{r_1, r_2, \ldots, r_k\}$: $x \in B(R, \delta) \iff r_1 x, r_2 x, \ldots, r_k x \in [-\delta N, \delta N]$



Entornos de Bohr

N es un primo impar. Definimos en $\mathbb{Z}_N$ los entornos de Bohr.

Sea $R \subseteq \mathbb{Z}_N$, y sea $\delta > 0$ un número real. El entorno de Bohr $B(R, \delta)$ es el conjunto

$$\left\{ x \in \mathbb{Z}_N \middle| \left\| \frac{rx}{N} \right\| \leq \delta \text{ para todo } r \in R \right\},$$

donde $\|y\|$ representa la distancia de y al entero más cercano.

$$B(R, \delta) = \bigcap_{r \in R} r^{-1}\{-\lfloor \delta N \rfloor, \ldots, -2, -1, 0, 1, 2, \ldots, \lfloor \delta N \rfloor\}$$

Un entorno de Bohr es una intersección de progresiones aritméticas en $\mathbb{Z}_N$ del mismo tamaño que contienen al 0.

La transformada de Fourier discreta

Dada una función $f : \mathbb{Z}_N \to \mathbb{C}$

la **transformada de Fourier discreta** de f es $\hat{f} : \mathbb{Z}_N \to \mathbb{C}$, donde

$$\hat{f}(r) = \sum_{x \in \mathbb{Z}_N} f(x) e^{2\pi i r x / N}$$

para todo $r \in \mathbb{Z}_N$.

Podemos probar igualdades que relacionan **propiedades aditivas** de un conjunto de $\mathbb{Z}_N$ con la **transformada de Fourier** de su función característica.

Chang

Usando este análisis de Fourier discreto podemos probar el siguiente resultado

Teorema

Sea $A \subseteq \mathbb{Z}_N$ un conjunto de cardinal αN y supongamos que $|A+A| \leq C|A|$. Entonces $2A-2A$ contiene algún entorno de Bohr $B(K,\delta)$, donde $|K| \leq 8C\log(1/\alpha)$ y $\delta \geq (160C\log(1/\alpha))^{-1}$.

Cuanto más pequeño es K y más grande es δ, más grande es el entorno de Bohr $B(K,\delta)$. Luego el teorema dice:

Si $A \subseteq \mathbb{Z}_N$ tiene conjunto suma pequeño entonces $2A-2A$ contiene un entorno de Bohr grande (algo grande con estructura).

Tres cosas más

Sabemos que

Si $A \subseteq \mathbb{Z}_N$ tiene conjunto suma pequeño entonces $2A - 2A$ contiene un entorno de Bohr grande.

Tenemos tres problemas, para probar el teorema de Freiman:

- Sabemos que los entornos de Bohr son intersecciones de progresiones aritméticas, pero necesitamos una relación más clara con las progresiones aritméticas generalizadas
- El teorema de Freiman habla de subconjuntos de $\mathbb{Z}$, no de $\mathbb{Z}_N$
- Lo que queremos son conclusiones sobre la estructura de A, no sobre la de $2A - 2A$

Minkowski

Usando resultados sobre retículos (geometría de los números) como el segundo teorema de Minkowski, podemos probar el siguiente teorema, que es el que nos da la relación que buscamos entre los entornos de Bohr y las progresiones aritméticas generalizadas.

Teorema

Sea $R \subseteq \mathbb{Z}_N$ un subconjunto de cardinal k, y sea $\delta \in (0, 1/2)$. Entonces el entorno de Bohr $B(R, \delta)$ contiene una progresión aritmética generalizada propia de dimensión k y tamaño al menos $(\delta/k)^k N$.

Homomorfismos de Freiman

Una función, ϕ, es un k-**homomorfismo de Freiman** si siempre que tengamos

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$$

tenemos

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k}).$$

Un homomorfismo habitual ($\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$) es un homomorfismo de Freiman de todos los órdenes.

Un k-homomorfismo de Freiman es más débil que el homomorfismo habitual, pero conserva las propiedades aditivas hasta k sumandos.

Homomorfismos de Freiman

Si además ϕ tiene una inversa que también es un k-homomorfismo de Freiman entonces ϕ es un k-**isomorfismo de Freiman**.

Empleando el concepto de k-isomorfismo y el resultado de Chang, se prueba el siguiente resultado, que nos permite dar el salto de $\mathbb{Z}_N$ a $\mathbb{Z}$

Teorema (Ruzsa)

Sea $A \subseteq \mathbb{Z}$ tal que $|A+A| \leq C|A|$. Entonces $2A-2A$ contiene una progresión aritmética generalizada propia de dimensión a lo sumo $2^{11}C\log C$ y tamaño al menos $\exp(-2^{17}C(\log C)^2)|A|$.

El teorema de Freiman efectivo

Un último argumento ingenioso de Ruzsa y el uso de la desigualdad de Plünnecke nos dan por fin una versión efectiva del teorema de Freiman

Teorema de Freiman efectivo

Sea $A \subseteq \mathbb{Z}$ tal que $|A+A| \leq C|A|$. Entonces A está contenido en una progresión aritmética generalizada de dimensión a lo sumo $2^{20}C^2(\log C)^2$ y tamaño a lo sumo $\exp(2^{20}C^2(\log C)^2)|A|$.

Bibliografía

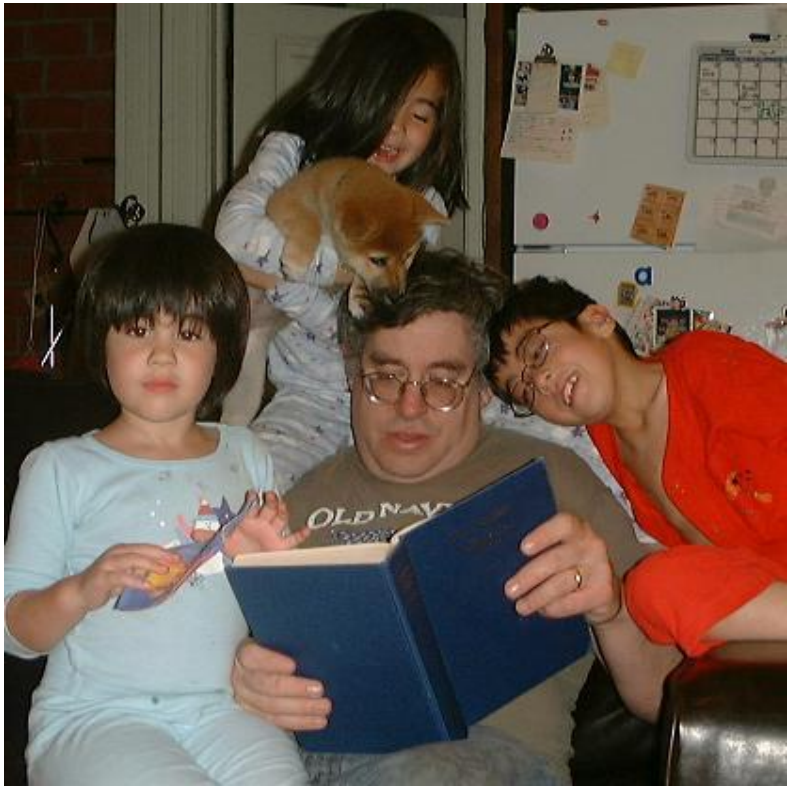

B. J. Green, Structure Theory of Set Addition, ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis. Edimburgh (March 25 - April 5, 2002).


Andrew Granville, Additive Combinatorics (Winter 2005).


Fabio Vicentini, Teoría de Grafos (Apuntes curso 2003).


Imre Z. Ruzsa, An analog of Freiman's theorem in groups (November 1993).

Espacios pequeños entre primos



Daniel Alan Goldston

Los autores del artículo *Small gaps between primes exist*

János Pintz

Los autores del artículo *Small gaps between primes exist*

Cem Yalçın Yıldırım

Los autores del artículo *Small gaps between primes exist*

Kannan Soundararajan

Autor del artículo *Small gaps between prime numbers: The work of Goldston-Pintz-Yıldırım*

Enrico Bombieri

El famoso teorema de Bombieri-Vinogradov será crucial

Si hubiera que resumir el artículo en un titular...

En 2005, Daniel Alan Goldston, János Pintz y Cem Yalçın Yıldırım hicieron un sensacional descubrimiento en el estudio de los números primos

Probaron que hay infinitos números primos para los que el espacio hasta el siguiente primo es tan pequeño como queramos comparado con el espacio medio entre primos consecutivos.

El espacio medio entre primos

Notación

- p denota un número primo
- p_n denota el primo n-ésimo ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...)
- $\pi(x) = |\{p : p \leq x\}|$, o sea, el número de primos menores o iguales que x

El espacio medio entre primos

La historia comienza en 1793. Gauss, que contaba con 16 años de edad, observó, estudiando tablas de los números primos hasta 3 millones, que "el número de primos hasta x es aproximadamente $x/\log x$"

Teorema del número primo
1896 Hadamard-de la Vallée Poussin (zeta de Riemann)
1949 Selberg-Erdös (elemental)

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

El espacio medio entre primos

Teorema del número primo
1896 Hadamard-de la Vallée Poussin (zeta de Riemann)
1949 Selberg-Erdös (elemental)

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

Moraleja

Como hasta x hay más o menos $x/\log x$ primos, si miramos a los primos que están cerca de x el espacio medio entre primos consecutivos es más o menos $\log x$.

Espacios grandes y pequeños

- Pero entre $p = 1.693.182.318.746.371$ y $p + 1.132$ no hay ningún primo y $\log p = 35{,}065\ldots$
- Y $p = 1.000.000.000.061$ y $p + 2$ son primos y no distan como $\log p = 27{,}631\ldots$

Luego

Algunos primos distan más que la media y otros distan menos que la media.

Espacios grandes y pequeños

Uno puede preguntarse si habrá infinitos espacios entre primos consecutivos arbitrariamente más grandes o arbitrariamente más pequeños que el espacio medio.

Esto es, uno puede preguntarse si se cumplen

Espacios entre primos arbitrariamente más grandes que la media

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty$$

Espacios entre primos arbitrariamente más pequeños que la media

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Espacios grandes y pequeños

Uno puede preguntarse si habrá infinitos espacios entre primos consecutivos arbitrariamente más grandes o arbitrariamente más pequeños que el espacio medio.

Esto es, uno puede preguntarse si se cumplen

1930's. Westzynthius, Erdös, Rankin...: sí

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty$$

Espacios entre primos arbitrariamente más pequeños que la media

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Espacios grandes y pequeños

Uno puede preguntarse si habrá infinitos espacios entre primos consecutivos arbitrariamente más grandes o arbitrariamente más pequeños que el espacio medio.

Esto es, uno puede preguntarse si se cumplen

1930's. Westzynthius, Erdös, Rankin...: sí

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty$$

2005. Goldston-Pintz-Yıldırım: sí (nuestro objetivo)

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Reduciendo la constante

El teorema del número primo nos dice que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 1$$

porque el espacio medio entre p_n y p_{n+1} es como $\log p_n$.
¡Si todo el mundo cobrara más que el salario medio entonces el salario medio sería mayor!

Reduciendo la constante

En 1940, Erdös probó que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} < 1.$$

Reduciendo la constante

En 1965, Bombieri y Davenport probaron que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 0,4665\ldots$$

Reduciendo la constante

En 1977, Huxley probó que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 0,4349\ldots$$

Reduciendo la constante

En 1988, Maier probó que

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 0,2484\ldots$$

y esto era lo mejor que se sabía desde entonces. . . hasta el año pasado.
Es decir, después de tantos años, sólo se sabía que había infinitos espacios entre primos que medían aproximadamente $1/4$ del espacio medio, lo que resulta un poco patético si creemos que existen infinitos espacios de longitud 2, como nos dice la conjetura de los primos gemelos.

Reduciendo la constante

En 2005, Goldston, Pintz y Yıldırım dieron un salto cualitativo probando

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Es decir, existen infinitas diferencias arbitrariamente pequeñas en comparación con la diferencia media.

Teorema del número primo e hipótesis de Riemann

Notación

Cuando $\limsup_{x \to a} \frac{|f(x)|}{|g(x)|} = C < \infty$ decimos que

- "$f(x) = O(g(x))$ cuando $x \to a$" (Landau)
- "$f(x) \ll g(x)$ cuando $x \to a$" (Vinogradov)

Es decir $f(x) = O(g(x))$ y $f(x) \ll g(x)$ significan lo mismo, que a la larga f es menor que una constante por g cuando $x \to a$.

Teorema del número primo e hipótesis de Riemann

El teorema del número primo, nos dice más que lo que hemos escrito antes. Concretamente

$$\pi(x) = Li(x) + E(x)$$

donde

- $Li(x)$ es el término principal esperado (es como $x/\log x$)
- dado cualquier $A > 0$ existe una constante $C(A)$ tal que $|E(x)| \leq C(A)\frac{x}{(\log x)^A}$

Si se cumpliera la hipótesis de Riemann, tendríamos la maravillosa fórmula:

$$\pi(x) = Li(x) + O(x^{1/2}\log x)$$

Para primos en progresiones

Dada una progresión aritmética a (mód q) con $(a, q) = 1$

$$\pi(x; a, q) = \frac{Li(x)}{\varphi(q)} + E(x; a, q)$$

donde

- $\pi(x; a, q)$ es el número de primos menores o iguales que x congruentes con a (mód q)
- $\frac{Li(x)}{\varphi(q)}$ es el término principal esperado
- para todo $A > 0$ existe una constante $C(q, A)$ tal que $|E(x; a, q)| \leq C(q, A)\frac{x}{(\log x)^A}$

Importante: la constante depende de q, por lo que el resultado sólo nos sirve si tenemos q fijo y $x \to \infty$. Pero en la mayoría de las aplicaciones, como es nuestro caso, eso no nos vale, necesitamos que q crezca con x.

Para primos en progresiones

Si se cumpliera la hipótesis de Riemann generalizada, tendríamos:

$$\pi(x; a, q) = \frac{Li(x)}{\varphi(q)} + O(x^{1/2} \log x)$$

Esto nos permitiría tener "cotas buenas variando" q en un rango grande (hasta q un poco menor que $x^{1/2}$).
Aunque desafortunadamente no sabemos probar la hipótesis de Riemann, en muchas aplicaciones es suficiente con tener una cota en media para q variando. El profundo resultado de Bombieri y Vionogradov nos da esa estimación en media.

Para primos en progresiones

Teorema de Bombieri-Vinogradov

Para toda constante $A > 0$ existe una constante $B > 0$ tal que

$$\sum_{q \leq \frac{x^{1/2}}{(\log x)^B}} \max_{\substack{a \\ (a,q)=1}} \left| \pi(x; a, q) - \frac{Li(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

En media (incluso cogiendo dentro de cada módulo la progresión aritmética que da lugar al mayor error), si sumamos sobre los módulos en cierto rango, el error medio está todavía bajo control.

Para primos en progresiones

Teorema de Bombieri-Vinogradov

Para toda constante $A > 0$ existe una constante $B > 0$ tal que

$$\sum_{q \leq \frac{x^{1/2}}{(\log x)^B}} \max_{\substack{a \\ (a,q)=1}} \left| \pi(x; a, q) - \frac{Li(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

Además, olvidándonos del poder de $\log x$ frente a x, esto es tan bueno como lo que nos decía la hipótesis de Riemann generalizada, el rango de q llega hasta un poco menos que $x^{1/2}$.

Goldston-Pintz-Yıldırım

Con el teorema de Bombieri-Vinogradov, y usando técnicas clásicas de variable compleja (teorema de Cauchy, teorema de los residuos...) y algunos resultados sobre la función ζ de Riemann, se prueban fórmulas asintóticas que combinadas en un argumento de criba con pesos nos dan el resultado

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

¿Y si...?

Una conjetura clásica nos dice que en el teorema de Bombieri-Vinogradov tendríamos que poder variar q en un rango mayor, hasta un poco menos que x.

Conjetura de Elliott-Halberstam

Dados $\varepsilon > 0$ y $A > 0$

$$\sum_{q \leq x^{1-\varepsilon}} \max_{\substack{a \\ (a,q)=1}} \left| \pi(x; a, q) - \frac{Li(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

¿Y si...?

Pese a lo espectacular del resultado de Goldston, Pintz y Yıldırım, nos puede seguir pareciendo un poco pobre el hecho de que todavía seguimos sin saber si existe una constante d tal que la diferencia $p_{n+1} - p_n \leq d$ para infinitos valores de n. Esperamos que haya infinitas parejas de primos que disten 2 y ¡ni siquiera sabemos que existan infinitas parejas que disten menos que mil millones!

¿Y si...?

Suponiendo cierta la conjetura de Elliott-Halberstam, podemos probar que

$$p_{n+1} - p_n \leq 20$$

para infinitos valores de n.
Esto implicaría inmediatamente que $p_{n+1} - p_n = d$ en infinitas ocasiones para algún d que podría ser 2, 4, 6, 8, 10, 12, 14, 16, 18 o 20. ¿Y si fuera la diferencia 2 la que se repite en infinitas ocasiones? ¡Entonces tendríamos la conjetura de los primos gemelos!

¿Y si. . . ?

Bibliografía


D. A. Goldston - Y. Motohashi - J. Pintz - C. Y. Yildirim, Small gaps between primes exist, Proceedings of the Japan Academy, Series A. Mathematical Sciences, Volume 82, Number 6 (June 2006).


K. Soundararajan, Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım Mathematics ArXiv, NT/0605696v1 (27 May 2006).

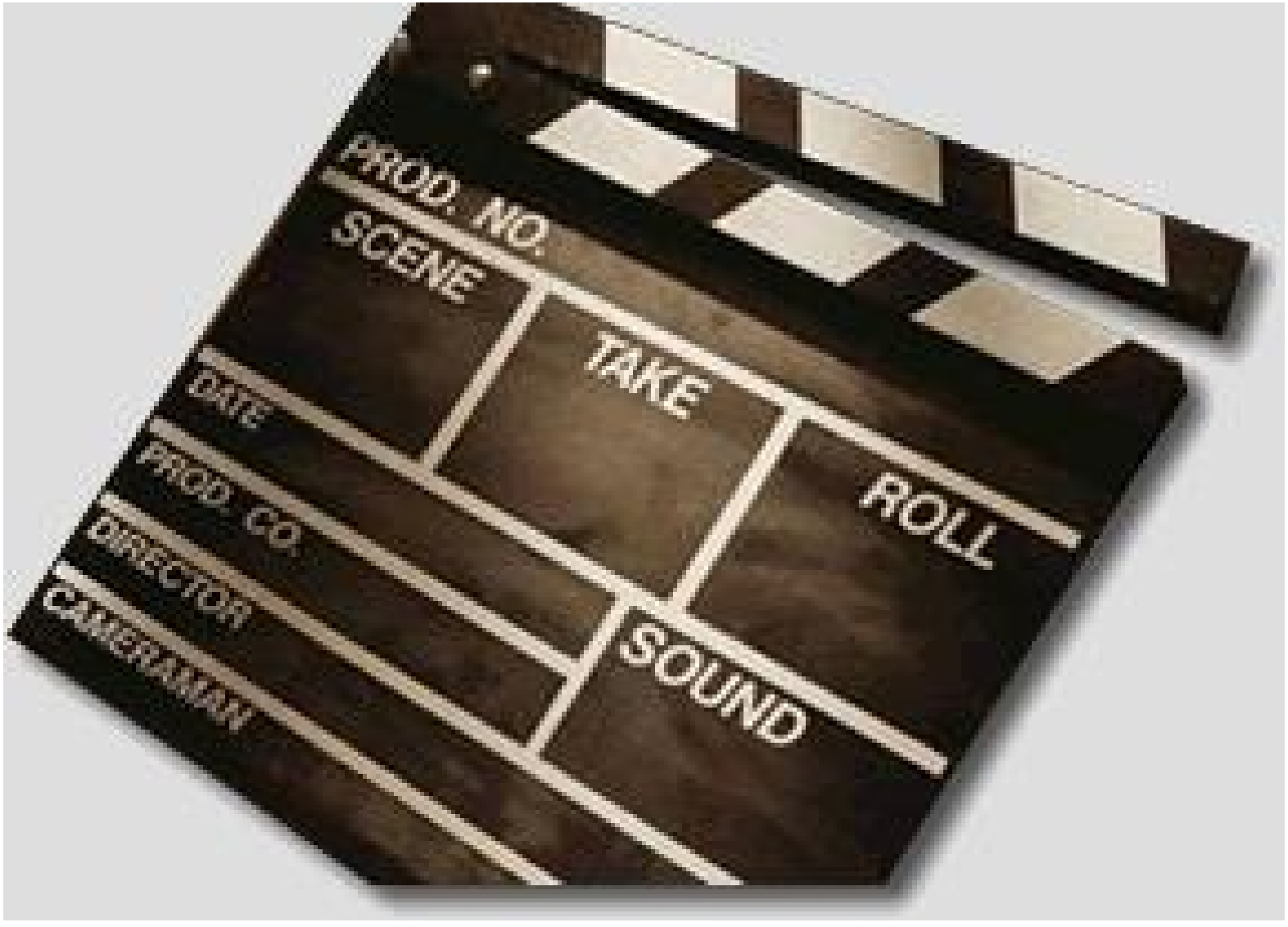

Fernando Chamizo, Temas de teoría de números. Seminario avanzado, Departamento de Matemáticas, UAM (2006).

A Javier y a Fernando...

El educador mediocre habla.
El buen educador explica.
El educador superior demuestra.
El gran educador inspira.
William Arthur Ward

...gracias por inspirarme.

¡Corten!


PROD. NO.
SCENE
TAKE
DATE
ROLL
PROD. CO.
DIRECTOR
SOUND
CAMERAMAN