Universidad Nacional Autónoma de México

Facultad de Ciencias

Bases heterocromáticas en Teoría Aditiva de Números

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

PRESENTA:

Mario Guadiana Martínez

TUTORA

Amanda Montejano Cantoral

Ciudad Universitaria, CD. MX. Marzo 2020

1. Datos del alumno
   Guadiana
   Martínez
   Mario
   461 15 41 42 1
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   415058115

2. Datos del tutor
   Dra
   Amanda
   Montejano
   Cantoral

3. Datos del sinodal 1
   Dr
   César
   Hernández
   Cruz

4. Datos del sinodal 2
   Dra
   Adriana
   Hansberg
   Pastor

5. Datos del sinodal 3
   Dra
   Natalia
   Jonard
   Pérez

6. Datos del sinodal 4
   Dra
   Mucuy-Kak del Carmen
   Guevara
   Aguirre

7. Datos del trabajo escrito
   Bases heterocromáticas en Teoría Aditiva de Números
   70 p
   2019

Agradecimientos

Agradezco a toda mi familia, la cual siempre me ha brindado su apoyo en todas las decisiones que he tomado y que gracias a ellos he podido dedicar mi vida completamente a mis estudios académicos, en especial, quiero agradecer a dos miembros de ésta que han sido de vital importancia en mi vida, me refiero a mi madre María Martínez Mendoza que en todo momento ha cuidado tan bien de mí y a mi amiguito Popeye con el cual he mantenido una enorme amistad desde que lo incorporé a nuestro hogar. También doy las gracias a mi tutora Amanda Montejano Cantoral por todo el tiempo invertido en éste trabajo y sin la cual la presente tesis no hubiese sido posible. Asimismo, quiero expresar mi estima por todos mis amigos (cuyos nombres prefiero no mencionar debido a que podría olvidar a alguno de ellos) pues gracias a su amistad mi estadía en esta vida se ha tornado más amena y por último, agradezco profundamente a todas las personas de las cuales he recibido algún tipo de enseñanza pues gracias a ellas he sido capaz de observar nuestro mundo con ojos de contemplador.

Índice general

Capítulo 1

Introducción

En el presente trabajo de tesis estudiaremos dos tipos de resultados a los que llamaremos, respectivamente, *resultados de coloraciones* y *resultados de densidad*. Para comenzar, consideremos un conjunto X y una familia de subconjuntos $\mathcal{F}$ de X, es decir, $\mathcal{F} \subset \mathcal{P}(X)$. Por ejemplo, los siguientes son dos casos que se estudiarán en esta tesis:

(i) $X = \{1, 2, ..., n\}$ y $\mathcal{F}$ es el conjunto de ternas en X que forman una progresión aritmética de longitud tres, es decir,

$$\mathcal{F} = \{\{x, y, z\} \in \mathcal{P}(X) : x + y = 2z, x \neq y\}.$$

(ii) $X = E(K_n)$ es el conjunto de aristas de una gráfica completa de orden n y $\mathcal{F}$ es el conjunto de ternas en X que forman un triángulo en K_n, es decir,

$$\mathcal{F} = \{\{e_1, e_2, e_3\} \in \mathcal{P}(X) : \{e_1, e_2, e_3\} = E(K_3) \text{ para algún } K_3 \subseteq K_n\}.$$

Dado un conjunto X, una *k-coloración* de X es una función $\chi : X \to C$ donde C es un conjunto de colores y $|C| = k$. Dada una coloración χ de X y un subconjunto $Y \subseteq X$, decimos que Y es *monocromático* si la función χ restringida a Y es constante, en otras palabras, si todos los elementos de Y recibieron el mismo color. Dado un conjunto X y una familia de subconjuntos $\mathcal{F}$ de X, los resultados de coloraciones (tipo Ramsey) establecen que si X es suficientemente grande entonces toda k-coloración de X contiene un elemento de $\mathcal{F}$ monocromático; en contraparte, los resultados de densidad establecen que todo subconjunto suficientemente grande de X contiene un miembro de $\mathcal{F}$. Para decir que un subconjunto de X es suficientemente grande, particularmente en el caso en que X sea un conjunto de cardinalidad infinita, usamos el concepto de densidad: si X es finito, la *densidad* de $Y \subseteq X$ se define como el cociente $|Y|/|X|$; si X no es finito, se puede definir el concepto de densidad de distintas maneras; en este trabajo, usaremos la *densidad superior* (Definición 3.25) y la *densidad de Schnirelmann* (Definición 4.4).

La tesis está estructurada de la siguiente manera. En el Capítulo 2, presentaremos las herramientas necesarias para desarrollar el material de los capítulos posteriores. Repasaremos conceptos básicos sobre aritmética, sucesiones y coloraciones. Además, probaremos un caso particular del Teorema de Ramsey (Teorema 2.30) que es el resultado de coloraciones correspondiente al ejemplo (ii) arriba descrito. Así mismo, presentaremos (sin prueba) el Teorema de van der Waerden (Teorema 2.32) que es el resultado de coloraciones correspondiente a $X = \{1, 2, ..., n\}$ y $\mathcal{F}$ el conjunto de subconjuntos de X que forman una progresión aritmética de longitud ℓ. Ambos resultados son fundamentales en la teoría de Ramsey.

En el Capítulo 3 estudiaremos un teorema clásico en teoría combinatoria de números, a saber el Teorema de Roth (Teorema 3.10). El teorema de Roth es el resultado de densidad correspondiente al ejemplo (i) arriba descrito: establece que si $S \subseteq \{1, ..., n\}$ es suficientemente denso entonces S contiene una progresión aritmética de longitud tres. Presentaremos una prueba combinatoria del Teorema de Roth que utiliza dos resultados, el primero de coloraciones (Lema 3.5) y el segundo de densidad (Lema 3.8) referentes a un objeto combinatorio llamado *cubo afín* o *cubo de Hilbert* (Definición 3.1). El Lema 3.5 tiene relevancia histórica pues se reconoce como el primer resultado tipo Ramsey en la literatura y fue probado por David Hilbert en 1892.

En el Capítulo 4 daremos el concepto de *base* (Definición 4.1) y demostraremos el clásico Teorema de Lagrange (Teorema 4.3) que afirma que todo número natural puede ser escrito como la suma de cuatro cuadrados (en otras palabras, el conjunto de números cuadrados es una base de orden cuatro). Además, definiremos la densidad de Schnirelmann (Definición 4.4) y probaremos que si S es suficientemente denso (con esta definición de densidad) en $\mathbb{N}$ entonces S es una base (Teorema 4.10) lo cual es un resultado de tipo densidad.

Aunque, en apariencia, el material de los Capítulos 3 y 4 no está relacionado, en el Capítulo 5 establecemos que sí lo está y presentamos un proyecto de investigación. Dicho proyecto es el que le da el título a la tesis. Dado un resultado de densidad es natural preguntarse cuál es su análogo en versión coloraciones, y dado un resultado de coloraciones en teoría de Ramsey se puede plantear, además, el estudio de su versión heterocromática. De esta manera, proponemos el estudio de *bases heterocromáticas* traduciendo el problema de las bases en teoría aditiva de números (resultados de densidad) a su versión en coloraciones (teoría de Ramsey monocromática) y, posteriormente, a su versión anti-Ramsey (estudio de sub-estructuras heterocromáticas).

Capítulo 2

Preliminares

En este capítulo introduciremos las herramientas matemáticas que utilizaremos en los siguientes capítulos. Presentaremos conceptos básicos sobre aritmética, sucesiones y coloraciones. La mayor parte del material en este capítulo fue consultado en [4, 5, 8].

2.1. Aritmética

En esta sección definiremos lo que es una progresión aritmética finita e introduciremos conceptos básicos de divisibilidad, así como el Teorema Fundamental de la Aritmética 2.5.

Adoptaremos la notación usual en teoría de conjuntos. Denotamos al conjunto de números enteros por $\mathbb{Z}$, al conjunto de números naturales por $\mathbb{N}$ y al conjunto de números reales por $\mathbb{R}$. El cero pertenece al conjunto de los números naturales,

$$\mathbb{N} = \{0, 1, 2, \cdots\},$$

de modo que para referirnos al conjunto de números enteros positivos usaremos

$$\mathbb{Z}^+ = \{1, 2, \cdots\} = \mathbb{N} \setminus \{0\}.$$

Dados $a, b \in \mathbb{Z}$, con $a \leq b$, el intervalo de números enteros entre a y b se denota por

$$[a, b] := \{x \in \mathbb{Z} \mid a \leq x \leq b\}.$$

Definición 2.1. *Una* progresión aritmética *con t términos es un conjunto de enteros de la forma*

$$\{a, a + d, a + 2d, \cdots, a + (t - 1)d\}$$

donde $t \in \mathbb{Z}^+$ *es el* número de términos, $a \in \mathbb{Z}$ *es la* base *de la progresión y* $d \in \mathbb{Z}^+$ *es su* diferencia*. A las progresiones aritméticas con* t *términos comúnmente se les denota por* $AP(t)$*.*

En este trabajo nos interesan particularmente las $AP(3)$, es decir, las progresiones de la forma $\{a, a+d, a+2d\}$. La siguiente es una observación que será de mucha utilidad en el Capítulo 5.

Observación 2.2. *Una progresión aritmética con tres términos* $\{a, a+d, a+2d\}$ *es una solución de la ecuación* $x+y=2z$*, tomando* $x=a, y=a+2d$ *y* $z=a+d$*. Recíprocamente, cada solución no trivial (es decir con* $x \neq y$*) de la ecuación* $x+y=2z$ *es una progresión aritmética de tres términos* $\{x, (x+y)/2, y\}$*.*

Por definición, una progresión aritmética con t términos es un subconjunto finito de $\mathbb{Z}$. Más adelante definiremos lo que es una progresión aritmética infinita, pero antes veremos algunos aspectos de divisibilidad.

Definición 2.3. *Sean* a *y* b *enteros con* $a \neq 0$*. Decimos que* b *es* divisible *por* a *si existe un entero* x *tal que* $b = ax$*. Cuando* b *es divisible por* a *también decimos que* a divide a b *y lo denotamos por* $a \mid b$*. En caso en que* b *no sea divisible por* a *se escribe* $a \nmid b$*.*

Observemos que $a \mid 0$ para todo entero a y $1 \mid b$ para todo entero b.

Definición 2.4. *Se dice que un número entero* $p > 1$ *es un número primo, si* p *es divisible únicamente por él mismo y por la unidad. Si un número* $a > 1$ *no es primo, entonces se dice que es un número compuesto.*

Uno de los teoremas más importantes en la teoría de números es el siguiente.

Teorema 2.5 (Fundamental de la Aritmética)**.** *Todo número natural mayor que* 1 *puede expresarse de forma única como producto de números primos (puede que algunos se repitan).*

Por ejemplo $21\,160 = 2^3 \cdot 5 \cdot 23^2$ y no existe otra factorización en primos de $21\,160$. Ahora introduciremos las congruencias, que son un concepto más sútil en relación a la divisibilidad.

Definición 2.6. *Si un entero* $m \neq 0$ *divide a la diferencia* $a-b$*, se dice que* a *es* congruente con b módulo m *y se escribe* $a \equiv b \pmod{m}$*. Si* $a-b$ *no es divisible por* m*, se dice que* a *no es congruente con* b *módulo* m *y se escribe* $a \not\equiv b \pmod{m}$*.*

Definición 2.7. *Si* $x \equiv y \pmod{m}$ *entonces decimos que* y *es* residuo de x módulo m. *Un conjunto de enteros* $\{x_1, x_2, \cdots, x_m\}$ *es un* sistema completo de residuos módulo m *si para todo entero* y *existe un único* $j \in \{1, ..., m\}$ *tal que* $y \equiv x_j \pmod{m}$*.*

Observemos que un conjunto de enteros $\{x_1, x_2, \cdots, x_m\}$ es un sistema completo de residuos módulo m si y solo si $x_i \not\equiv x_j \pmod{m}$ para todo $x_i \neq x_j$. Por ejemplo, $\{0, 1, 2\}$ es un sistema completo de residuos módulo 3, así como también lo son $\{1, 2, 3\}$, $\{-1, 0, 1\}$ o $\{0, -5, 32\}$. Dado un entero m, existe un número infinito de sistemas completos de residuos módulo m, sin embargo el conjunto $\{1, 2, \cdots, m\}$ se conoce como el sistema completo de residuos principal módulo m.

Definición 2.8. *Sea* A *un conjunto, una relación* $R \subset A \times A$ *se llama de equivalencia si satisface:*

(i) $(a, a) \in R$ *para todo* $a \in A$ *(reflexividad).*

(ii) Si $(a, b) \in R$*, entonces* $(b, a) \in R$ *(simetría).*

(iii) Si $(a, b) \in R$ *y* $(b, c) \in R$*, entonces* $(a, c) \in R$ *(transitividad).*

Dada cualquier relación de equivalencia R, escribiremos

$$a \sim b \quad \text{si} \quad (a, b) \in R.$$

Ejemplo 2.9. *La relación en* $\mathbb{Z}^+$ *dada por* $a \sim b$ *si* $a \equiv b \pmod{m}$ *es de equivalencia.*

Definición 2.10. *Sea* A *un conjunto, una* partición P *de* A *consiste de una familia de subconjuntos de* A *no vacíos* $\{A_i\}_{i \in I}$*, tales que :*

(i) si $A_i \neq A_j$*, entonces* $A_i \cap A_j = \emptyset$,

(ii) $\bigcup_{i \in I} A_i = A$.

Teorema 2.11. *Sea* A *cualquier conjunto y* R *una relación de equivalencia en* $A \times A$*, entonces* R *induce una partición en* A*.*

Este teorema quiere decir que la relación de equivalencia R define subconjuntos ajenos en A llamados *clases de equivalencia*. Dado un elemento $x \in A$, el conjunto dado por todos los elementos relacionados con x definen la clase

$$[x] := \{y \in A : x \sim y\}.$$

Esto nos permite escribir a A como la unión de sus clases de equivalencia.

Ejemplo 2.12. *En el Ejemplo 2.9 tomemos $m = 2$, entonces la relación de equivalencia dada por $a \sim b$ si $a \equiv b$ (mod 2) define la partición en $\mathbb{Z}$ dada por*

$$[0] = \{y \in \mathbb{Z} : y \equiv 0\ (mod\ 2)\} = \{\cdots - 4, -2, 0, 2, 4, \cdots\}$$

y

$$[1] = \{y \in \mathbb{Z} : y \equiv 1\ (mod\ 2)\} = \{\cdots - 3, -1, 1, 3, 5, \cdots\}.$$

Por último, definiremos la suma de conjuntos.

Definición 2.13. *Dados A y B dos subconjuntos de $\mathbb{Z}$, definimos la* suma de Minkowski de A y B *como*

$$A + B := \{a + b : a \in A, b \in B\}.$$

Ejemplo 2.14. *Sean $A, B \subset \mathbb{N}$ con $A = \{n \in \mathbb{N} : n \equiv 0 \pmod 2\} = \{0, 2, 4, 6, 8, \cdots\}$, entonces*

- *$A + B = A$ si y solo si $0 \in B$ y todo elemento de B es un numero par, y*
- *$A + B = \mathbb{N}$ si y solo si $\{0, 1\} \subseteq B$.*

En la Definición 2.13, cuando $B = \{c\}$ (con $c \in \mathbb{Z}$) , al conjunto $A + \{c\} := \{a + c : a \in A\}$ se le conoce como *traslación* de A en c unidades . Observemos que para todo $c \in \mathbb{Z}$ y $A \subset \mathbb{Z}$ se tiene que $|A| = |A + \{c\}|$.

Sean $A \subset \mathbb{Z}$ y $c \in \mathbb{Z}$, definimos los conjuntos $-A := \{-a : a \in A\}$ y $cA := \{ca : a \in A\}$. Es fácil ver por definición que también se cumple que $|-A| = |A|$ y $|cA| = |A|$. Notemos que $A + A \neq 2A$, pues por ejemplo si $A = \{0, 1\}$ tenemos que $A + A = \{0, 1, 2\}$, en cambio $2A = \{0, 2\}$. Por útimo, definimos el conjunto $A - B$ como $A - B := A + (-B)$.

La suma de Minkowski la podemos extender de forma natural a un número cualquiera de conjuntos. Dada la colección $A_1, A_2, \cdots, A_n$ de subconjuntos de $\mathbb{Z}$ definimos el conjunto suma de las n sucesiones como

$$A_1 + \cdots + A_n = \{a_1 + \cdots + a_n : a_1 \in A_1, \cdots, a_n \in A_n, \}.$$

2.2. Sucesiones

En esta sección introduciremos la definición de sucesión y estudiaremos algunos casos especiales de ésta. Para más información sobre sucesiones consultar [8].

Comencemos formalizando el concepto de sucesión de números reales.

Definición 2.15. *Una* sucesión de números reales *es la imagen de una función*

$$a : \mathbb{N} \to \mathbb{R}.$$

Según la Definición 2.15, la sucesión de números reales correspondiente a la función a es el conjunto $\{a(0), a(1), a(2), \cdots\}$. Sin embargo, la notación con subíndices $\{a_0, a_1, a_2, \cdots\}$ donde $a_n := a(n)$, para toda $n \in \mathbb{N}$, se usa con mayor frecuencia. Además, usaremos letras mayúsculas para denotar estas sucesiones, por ejemplo, $A = \{a_n : n \in \mathbb{N}\}$, $B = \{b_n : n \in \mathbb{N}\}$, etc.

Definición 2.16. *Una sucesión $A = \{a_n : n \in \mathbb{N}\}$ es* creciente (*resp.* estrictamente creciente) *si $a_n \leq a_{n+1}$ (resp. $a_n < a_{n+1}$) para todo $n \in \mathbb{N}$ y es* decreciente (*resp.* estrictamente decreciente) *si $a_n \geq a_{n+1}$ (resp. $a_n > a_{n+1}$) para todo $n \in \mathbb{N}$. Todos estos tipos de sucesiones se denominan sucesiones* monótonas.

En este trabajo nos interesa un tipo especial de sucesiones; en primer lugar, vamos a considerar únicamente sucesiones inyectivas (es decir, si $n \neq m$ entonces $a_n \neq a_m$); en segundo lugar, la imagen de las sucesiones que vamos a estudiar siempre será un subconjunto de $\mathbb{N}$. Además, asumiremos que los elementos de la sucesión están ordenados de menor a mayor, es decir, la sucesión es estrictamente creciente. Formalmente, tenemos la siguiente definición.

Definición 2.17. *Una* sucesión natural *es una sucesión $A = \{a_n : n \in \mathbb{N}\}$ tal que $a_n \in \mathbb{N}$ para toda $n \in \mathbb{N}$ y A es estrictamente creciente. Una* sucesión natural con cero *es una sucesión natural $A = \{a_n : n \in \mathbb{N}\}$ tal que $a_0 = 0$.*

Ejemplo 2.18. *Consideremos las siguientes sucesiones:*

- $A = \{n^2 : n \in \mathbb{N}\} = \{0^2, 1^2, 2^2, 3^2, \cdots\} = \{0, 1, 4, 9, \cdots\}$.
- $B = \{2 + 5n : n \in \mathbb{N}\} = \{2 + 5(0), 2 + 5(1), \cdots\} = \{2, 7, 12, 17, \cdots\}$.
- $C = \{3^{n+1} : n \in \mathbb{N}\} = \{3^1, 3^2, 3^3, 3^4, \cdots\} = \{3, 9, 27, 81, \cdots\}$.

Como podemos observar A, B y C son sucesiones naturales, de las cuales la única que contiene al cero es A.

Un tipo particular de sucesiones que nos interesa estudiar es el siguiente.

Definición 2.19. *Una* progresión aritmética infinita *es una sucesión de números naturales tales que la diferencia entre cualesquiera dos términos consecutivos es constante. Al primer elemento de la sucesión a_0 se le llama* base*, y a la cantidad constante $a_{n+1} - a_n = d$ se le llama* diferencia.

En el Ejemplo 2.18 únicamente la sucesión B es una progresión aritmética, cuya base es $a_0 = 2$, y cuya diferencia es $d = 5$, pues

$$b_{n+1} - b_n = (2 + 5(n+1)) - (2 + 5n) = 2 + 5n + 5 - 2 - 5n = 5,$$

para todo $n \in \mathbb{N}$. En general, esto se puede expresar como una relación de recurrencia de la siguiente manera:

$$a_{n+1} - a_n = d$$

luego

$$a_{n+1} = a_n + d,$$

de modo que, si conocemos el primer término a_0 y la diferencia d, se puede calcular el enésimo término de la sucesión mediante la sustitución sucesiva en la relación de recurrencia

$$a_0, (a_0 + d), \underbrace{(\underbrace{a_0 + d}_{a_1} + d)}_{a_2}, \cdots, \underbrace{(\underbrace{a_0 + (n-1)d}_{a_{n-1}} + d)}_{a_n}$$

con lo que se obtiene la siguiente fórmula para el término general a_n con $n \geq 1$, de una progresión aritmética en función de la base a_0 y la diferencia d:

$$a_n = a_0 + nd.$$

Ahora veremos otro tipo especial de sucesiones.

Definición 2.20. *Una* progresión geométrica *es una sucesión de números naturales tales que el cociente entre cualesquiera dos términos consecutivos es constante. A dicha cantidad* $\frac{a_{n+1}}{a_n} = r$ *se le llama* razón*.*

En el Ejemplo 2.18 únicamente la sucesión C es una progresión geométrica cuya razón es $r = 3$, pues

$$\frac{c_{n+1}}{c_n} = \frac{3^{n+2}}{3^{n+1}} = 3$$

para todo $n \in \mathbb{N}$. En general, esto se puede expresar como una relación de recurrencia como sigue:

$$\frac{a_{n+1}}{a_n} = r$$

luego

$$a_{n+1} = a_n r,$$

de modo que, si conocemos el primer término a_0 y la razón r, podemos calcular el enésimo término de la sucesión mediante la sustitución sucesiva en la ecuación de recurrencia

$$a_0, (a_0 r), \underbrace{(\underbrace{(a_0 r)}_{a_1} r)}_{a_2}, \cdots, \underbrace{(\underbrace{(a_0 r^{n-1})}_{a_{n-1}} r)}_{a_n}$$

por lo que el término general de una progresión geométrica está dado por

$$a_n = a_0 r^n.$$

De este modo, la sucesión C del Ejemplo 2.18 se puede expresar como

$$C = \{c_0 \cdot 3^n : n \in \mathbb{N}\} = \{3 \cdot 3^n : n \in \mathbb{N}\} = \{3^{n+1} : n \in \mathbb{N}\}.$$

A partir de dos sucesiones podemos definir una nueva sucesión. Dadas dos sucesiones naturales, $A = \{a_n : n \in \mathbb{N}\}$ y $B = \{b_n : n \in \mathbb{N}\}$, consideramos la sucesión natural $A + B = C$ con $C = \{c_n : n \in \mathbb{N}\}$ que resulta de realizar la suma de Minkowski 2.13 de A y B . Es importante notar que el elemento c_n puede tener varias representaciones, y no necesariamente sucede $c_n = a_i + b_j$ con $i + j = n$.

Ejemplo 2.21. *Sean* $A = \{a_n : n \in \mathbb{N}\}$ *y* $B = \{b_n : n \in \mathbb{N}\}$ *definidas por*

$$a_0 = 0 \text{ y } a_n = 2n - 1 \text{ para todo } n \in \mathbb{Z}^+,$$

$$b_0 = 0 \text{ y } b_n = 3n - 2 \text{ para todo } n \in \mathbb{Z}^+,$$

De modo que, $A = \{0, 1, 3, 5, 7, \cdots\}$ *y* $B = \{0, 1, 4, 7, 10, \cdots\}$. *Es fácil ver que* $A + B = \mathbb{N}$ *pues si* $m = 0$ *entonces* $0 = 0 + 0 \in A + B$. *Ahora si* m *es un número natural impar entonces* $m = 2n - 1$ *con* $n \in \mathbb{Z}^+$ *por lo que* $m = (2n - 1) + 0 \in A + B$. *Por otro lado, si* m *es un entero positivo par entonces* $m = 2n$ *con* $n \in \mathbb{Z}^+$, *luego* $(m - 1) = 2n - 1 \in A$, *por lo que* $m = (m - 1) + 1 \in A + B$. *En este ejemplo se tiene que* $c_5 = 5$ *y* $c_5 = a_1 + b_2 = a_3 + b_0$.

De la misma forma que como lo hicimos con dos sucesiones naturales, dada la colección $A_1, A_2, \cdots, A_n$ de sucesiones naturales podemos definir una nueva sucesión natural $A := A_1 + A_2 + \cdots + A_n = \sum_{i=1}^{n} A_i$.

2.3. Coloraciones

En esta sección daremos la definición de coloración de un conjunto S y la definición de gráfica. Enunciaremos un caso particular del Teorema de Ramsey (1930) para coloraciones de las aristas de una gráfica completa. Además, presentaremos algunos de los teoremas más famosos en la teoría de Ramsey para coloraciones en los números enteros positivos.

La teoría de Ramsey es nombrada así en honor al matemático Frank Plumpton Ramsey (1903-1930) y su homónimo teorema, el cual probó en 1930. Aunque no hay una definición formal de la teoría de Ramsey, podemos decir que es el estudio de la preservación de propiedades bajo particiones de conjuntos. También se dice que el Teorema de Ramsey es una profunda generalización del siguiente principio. El material de esta sección fue extraído de [4].

Principio 2.22 (de las casillas)**.** *Si un conjunto de n elementos es dividido en r subconjuntos ajenos donde $n > r$, entonces al menos uno de los subconjuntos tiene más de un elemento.*

Abajo, presentaremos este mismo principio en el lenguaje de las coloraciones.

Definición 2.23. *Una k-coloración de un conjunto S es una función $\chi : S \to C$ donde $|C| = k$.*

Comúnmente, usaremos $C = \{0, 1, \cdots, k-1\}$ o $C = \{1, 2, \cdots, k\}$. Así, podemos pensar a la coloración χ de un conjunto S como una partición de S en k subconjuntos $S_1, S_2, \cdots, S_k$ asociando al subconjunto S_i con el conjunto $\{x \in S : \chi(x) = i\}$. La siguiente definición se usará con frecuencia.

Definición 2.24. *Dada una coloración χ de S y un subconjunto $Y \subseteq S$, decimos que Y es* monocromático (con respecto a χ) *si la función χ restringida a Y es constante.*

Ejemplo 2.25. *Sea $\chi : \mathbb{Z}^+ \to \{0, 1\}$ definida como $\chi(n) = 0$ si n es par y $\chi(n) = 1$ si n es impar. Entonces χ es una 2-coloración de $\mathbb{Z}^+$ en que cualquier subconjunto de números con la misma paridad es monocromático.*

El principio de las casillas se puede reformular de la siguiente manera.

Principio 2.26 (de las casillas, versión coloraciones)**.** *Dada una r-coloración de un conjunto de n elementos donde $n > r$, entonces al menos dos elementos del conjunto son del mismo color.*

Para mostrar y probar el Teorema de Ramsey (en un caso particular), requerimos las siguientes definiciones.

Definición 2.27. *Una* gráfica $G = (V, E)$ *es un conjunto* V *de elementos, llamados* vértices *junto con un conjunto* E *de pares de vértices, llamados* aristas.

Definición 2.28. *Una* subgráfica $G' = (V', E')$ *de una gráfica* $G = (V, E)$ *es una gráfica tal que* $V' \subseteq V$ *y* $E' \subseteq E$.

Definición 2.29. *La* gráfica completa *con* n *vértices, denotada por* K_n*, es la gráfica en la cual todo par de vértices es una arista.*

A K_3 se le suele llamar *triángulo*. Ahora podemos enunciar un caso particular del teorema de Ramsey que nos interesa.

Teorema 2.30 (Teorema de Ramsey (caso particular), 1930)**.** *Para todo entero* $k \geq 2$*, existe un mínimo entero positivo* $R = R(k)$ *tal que toda* k*-coloración de las aristas de* K_R *contiene un triángulo monocromático.*

Demostración. Procederemos por inducción sobre k. Para $k = 2$ mostremos que $R(2) \leq 6$. Consideremos una 2-coloración (digamos que con los colores azul y rojo) de $E(K_6)$ donde $V(K_6) = \{v_1, \cdots, v_6\}$. Tomemos un vértice cualquiera, digamos v_1. Por el principio de las casillas 2.26 el vértice v_1 tiene (al menos) tres vecinos con aristas del mismo color. Sin pérdida de generalidad supongamos que este color es el rojo y que los tres vecinos son v_2, v_3 y v_4. Ahora, si alguna de las aristas entre los vértices de $N = \{v_2, v_3, v_4\}$ es de color rojo, entonces se forma un triángulo monocromático de color rojo (junto con v_1). Si ninguna de las aristas en N es roja, entonces todas son azules, pero en este caso se forma un trángulo monocromático azul que tiene por vértices al conjunto N. En cualquiera de los dos casos, aparece un triángulo monocromático.

Ahora supongamos que existe $R(k)$ y mostremos que $R(k+1) \leq (k+1)R(k) + 1$. Sea $\ell = (k+1)R(k) + 1$. Consideremos la gráfica completa K_ℓ con $V(K_\ell) = \{v_1, \cdots, v_\ell\}$. Por el principio de las casillas 2.26 el vértice v_1 tiene (al menos) $R(k)$ vecinos con aristas del mismo color, digamos que este color es c_1. Sin pérdida de generalidad supongamos que estos $R(k)$ vecinos son $N = \{v_2, \cdots, v_{R(k)+1}\}$. Ahora consideremos la subgráfica completa $K_{R(k)}$ que tiene por vértices al conjunto N. Si alguna de las aristas entre los vértices de N es de color c_1, entonces tenemos un triángulo monocromático de color c_1 (junto con el vértice v_1). Si ninguna de las aristas en N es de color c_1 entonces $K_{R(k)}$ está coloreada con k colores, pero por hipótesis de inducción $K_{R(k)}$ contiene un triángulo monocromático. Por lo tanto R_ℓ contiene un triángulo monocromático. $\square$

Algo curioso es que el Teorema de Ramsey no fue el primer teorema en la área que se conoce como teoría de Ramsey. Los resultados que generalmente se aceptan como los primeros teoremas de tipo Ramsey se deben, en orden cronológico, a Hilbert (1892), Schur (1916) y Van der Waerden (1927). En la presente tesis estudiaremos dichos resultados.

El siguiente teorema fue probado por Issai Schur (1875-1941) en 1916. Históricamente, el Teorema de Schur es el segundo resultado del tipo Ramsey. Para la demostración del Teorema de Schur haremos uso del Teorema de Ramsey 2.30.

Teorema 2.31 (Schur, 1916)**.** *Para todo $k \in \mathbb{Z}^+$ existe un mínimo entero positivo $S(k)$ tal que toda k-coloración de $[1, S(k)]$ contiene una solución monocromática de la ecuación $x + y = z$.*

Demostración. El Teorema de Ramsey 2.30 nos dice que existe un entero $n = R(k)$ tal que toda k-coloración de K_n contiene un triángulo monocromático. Numeremos los vértices de K_n por $1, 2, \cdots, n$. Sea χ una k-coloración arbitraria de $[1, n-1]$. Ahora coloreamos la arista ij de la gráfica completa K_n por el color $\chi(|j - i|)|$. Por el teorema de Ramsey existe un triángulo monocromático para esta coloración. Un triángulo monocromático bajo esta coloración con vértices $i_1 < i_2 < i_3$ significa que $i_3 - i_2, i_2 - i_1$ y $i_3 - i_1$ tienen el mismo color. Hagamos $x = i_2 - i_1, y = i_3 - i_2$ y $z = i_3 - i_1$, y notemos que $\{x, y, z\}$ es una solución monocromática bajo χ para la ecuación $x + y = z$. Entonces, dado un entero $k \geq 1$ hemos probado que $S(k)$ existe pues $S(k) \leq R(k) - 1$. □

El siguiente teorema, debido a Bartel Leendert van der Waerden (1903-1996), es un resultado muy importante en la teoría de Ramsey. Históricamente, fue el tercer teorema de este tipo, apareciendo después de los resultados de Hilbert (Lema 3.5) y Schur (Teorema 2.31). El Teorema de van der Waerden ha generado muchos resultados en la teoría de Ramsey. Por esta razón, y porque las progresión aritméticas son objetos naturales y simples de gran importancia, se han hecho muchos refinamientos, extensiones y generalizaciones del teorema de van der Waerden.

Teorema 2.32 (van der Waerden 1927)**.** *Para todo $k, \ell \in \mathbb{Z}^+$ existe un mínimo entero postivo $W(k, \ell)$ tal que toda k-coloración de $[1, W(k, \ell)]$ contiene una progresión aritmética monocromática de longitud ℓ.*

La prueba del Teorema de van der Waerden es bastante más complicada que las pruebas de los Teoremas 2.30 y 2.31, por lo que en esta tesis no la daremos. Sin embargo, hacemos notar que, en vista de la Observación 2.2, el teorema de van der Waerden en el caso particular en que $\ell = 3$ se puede reescribir como sigue.

Teorema 2.33 (van der Waerden, caso particular $\ell = 3$, 1927)**.** *Para todo $k \in \mathbb{Z}^+$ existe un mínimo entero positivo $W(k)$ tal que toda k-coloración de $[1, W(k)]$ contiene una solución monocromática de la ecuación $x + y = 2z$ (con $x \neq y$).*

Observemos que los teoremas de Ramsey (Teorema 2.30), Schur (Teorema 2.31) y van der Waerden (Teorema 2.32) son teoremas que afirman la existencia de un mínimo entero positivo pero no dicen nada acerca del valor exacto de este número. En general, es muy difícil determinar dichos números; para hacerlo se deben de probar dos desigualdades, una de las cuales conlleva un ejemplo y la otra una demostración. Para ejemplificarlo, encontraremos el valor exacto de $W(2,3)$ (el mínimo entero positivo que se define en el enunciado del Teorema 2.32). Probaremos que $W(2,3) = 9$, es decir

$$9 \leq W(2,3) \leq 9.$$

La primera desigualdad se infiere de la siguiente proposición.

Proposición 2.34. *Existe una 2-coloración de* $[1,8]$ *sin* $AP(3)$ *monocromática.*

Demostración. Consideremos la siguiente 2-coloración de $[1,8]$,

$$\color{blue}{1}\ \color{red}{2}\ \color{blue}{3}\ \color{red}{4}\ \color{red}{5}\ \color{blue}{6}\ \color{red}{7}\ \color{blue}{8}.$$

Observemos que los posibles subconjuntos de tamaño tres del conjunto de elementos rojos $\{2,4,5,7\}$ son $\{2,4,5\}$, $\{2,4,7\}$, $\{2,5,7\}$ y $\{4,5,7\}$ y ninguno de estos es una $AP(3)$. Igualmente, los posibles subconjuntos de cardinalidad tres del conjunto de elementos azules $\{1,3,6,8\}$ son $\{1,3,6\}$, $\{1,3,8\}$, $\{1,6,8\}$ y $\{3,6,8\}$ y ninguno de estos es una $AP(3)$. Por lo tanto para esta coloración no hay una $AP(3)$ monocromática en $[1,8]$. □

Dado que hemos mostrado la existencia de una 2-coloración del intervalo $[1,8]$ sin $AP(3)$ monocromática, entonces $W(2,3) \geq 9$. A continuación, probaremos que $W(2,3) \leq 9$.

Proposición 2.35. *Toda 2-coloración de* $[1,N]$*, con* $N \geq 9$*, contiene una* $AP(3)$ *monocromática.*

Demostración. Procedamos por contradicción suponiendo que existe una 2-coloración de $[1,9]$ sin $AP(3)$ monocromáticas. Sea $\chi : [1,9] \to \{rojo, azul\}$ dicha 2-coloración.

Afirmación 1. $\chi(3) \neq \chi(5)$, $\chi(5) \neq \chi(7)$ *y* $\chi(4) \neq \chi(6)$.

Para ver esto supongamos, por contradicción, que 3 y 5 son ambos del mismo color, a saber rojo sin pérdida de generalidad

$$1\ 2\ \color{red}{3}\ 4\ \color{red}{5}\ 6\ 7\ 8\ 9.$$

Como $\{1,3,5\}$ es una $AP(3)$ entonces 1 es azul. De la misma manera, como $\{3,4,5\}$ y $\{3,5,7\}$ son progresiones aritméticas de longitud tres entonces 4 y 7 son azules

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9,$$

lo cual no es posible pues $\{1,4,7\}$ es una $AP(3)$ monocromática. Entonces, 3 y 5 son de diferente color. Similarmente, se prueba que tanto 5 y 7 como 4 y 6 no pueden ser ambos del mismo color. $\diamond$

Ahora, supongamos sin pérdida de generalidad que 3 es rojo. Por las restricciones de la Afirmación 1, tenemos dos posibles coloraciones de $\{3,4,5,6,7\}$

(i) 1 2 3 4 5 6 7 8 9

(ii) 1 2 3 4 5 6 7 8 9

Para el caso (i), debido a que $\{2,3,4\}$ es una $AP(3)$ entonces 2 es de color azul. Luego como $\{2,5,8\}$ es una $AP(3)$ se tiene que 8 es rojo, y por $\{1,4,7\}$, 1 es azul. Finalmente por $\{1,5,9\}$, 9 es rojo. Entonces, tenemos

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9.$$

Vemos que $\{7,8,9\}$ es una $AP(3)$ monocromática, lo cual es una contradicción. Ya que el caso (ii) es simétrico a (i), un argumento por simetría nos conduce a que en (ii) también hay una contradicción. Así, toda 2-coloración de $[1,9]$ contiene una $AP(3)$ monocromática.

Finalmente, dada una 2-coloración de $[1,N]$ con $N > 9$, notemos que $[1,9] \subset [1,N]$ contiene una $AP(3)$ monocromática. $\square$

Capítulo 3

Cubos afines y progresiones aritméticas

El objetivo de este capítulo es demostrar el Teorema de Roth (Teorema 3.24), el cual nos dice que si un conjunto $S \subset \mathbb{N}$ tiene densidad positiva entonces S contiene una progresión aritmética de tres términos. El teorema de Roth es el resultado de densidad que le corresponde al Teorema 2.33 (teorema de van der Waerden) en el caso particular $\ell = 3$. Para la prueba del Teorema de Roth usaremos un resultado de densidad referente a ciertos subconjuntos de $\mathbb{N}$ llamados cubos afines (ver Definición 3.1). Estos subconjuntos de $\mathbb{N}$ generalizan el concepto de progresión aritmética y son llamados, en ocasiones, cubos de Hilbert [1]; sin embargo, decidimos no usar ese término en esta tesis para evitar confusiones con los espacios topológicos también conocidos como cubos de Hilbert.

La mayoría del material de este capítulo fue consultado en [1]. La prueba del Teorema de Roth 3.24 que se presenta en [1] cuenta con muchos vacíos argumentales por lo que en el presente trabajo la hemos escrito lo más detalladamente posible, además la Sección 3.2 fue desarrollada por nosotros.

3.1. El lema de Hilbert del cubo afín

En esta sección presentaremos dos resultados, el primero de coloraciones (Lema 3.5) y el segundo de densidad (Lema 3.8) referentes a un objeto combinatorio llamado cubo afín. Comenzaremos definiendo lo que es un d-cubo afín y proporcionando varios ejemplos.

Definición 3.1. *Un* d-cubo afín *es un conjunto de enteros de la forma*

$$Q_d(x_0, x_1, \cdots, x_d) := \left\{ x_0 + \sum_{i \in I} x_i : I \subseteq [1, d] \right\},$$

con $d, x_0, \cdots, x_d \in \mathbb{N}$ *y* $d \geq 1$. *Al conjunto* $\{x_1, \cdots, x_d\}$ *se le llama* conjunto de generadores *del cubo.*

Ejemplo 3.2. *Cualquier conjunto de enteros con dos elementos,* $\{a, b\}$*, es un* 1*-cubo afín. Para comprobar esto, notemos que*

$$Q_1(x_0, x_1) = \left\{ x_0 + \sum_{i \in I} x_i : I \subseteq \{1\} \right\}$$

y como los únicos dos subconjuntos de $\{1\}$ *son el vacío y él mismo, tenemos*

$$Q_1(x_0, x_1) = \left\{ x_0 + \sum_{i \in \emptyset} x_i, x_0 + \sum_{i \in \{1\}} x_i \right\} = \{x_0, x_0 + x_1\},$$

de modo que $\{a, b\} = Q_1(a, b - a)$.

A continuación vamos a analizar cómo son los 2-cubos afines.

Ejemplo 3.3. *Sean* $x_0, x_1, x_2 \in \mathbb{N}$. *Notemos que hay cuatro subconjuntos de* $\{1, 2\}$*, a saber* $\emptyset, \{1\}, \{2\}$ *y* $\{1, 2\}$*, de manera que*

$$Q_2(x_0, x_1, x_2) = \{x_0, x_0 + x_1, x_0 + x_2, x_0 + x_1 + x_2\}.$$

Observemos que un 2*-cubo es una traslación (por* x_0*) del conjunto* $\{0, x_1, x_2, x_1 + x_2\}$*, es decir*

$$Q_2(x_0, x_1, x_2) = \{x_0\} + \{0, x_1, x_2, x_1 + x_2\}.$$

Además,

- *con* $x_2 = 0$*, un* 2*-cubo es un* 1*-cubo afín;*
- *con* $x_1 = x_2$*, un* 2*-cubo afín es una progresión aritmética de tres términos con diferencia* x_1 *y base* x_0.

Más aún, notemos que

$$\begin{aligned} Q_2(x_0,x_1,x_2) &= \{x_0, x_0+x_1, x_0+x_2, x_0+x_1+x_2\} \\ &= \{x_0, x_0+x_1\} \cup \{x_0+x_2, x_0+x_1+x_2\} \\ &= \{x_0, x_0+x_1\} \cup (\{x_0, x_0+x_1\} + \{x_2\}) \\ &= Q_1 \cup (Q_1 + \{x_2\}). \end{aligned}$$

En general, tenemos la siguiente proposición. Usaremos $Q_d = Q_d(x_0, \cdots, x_d)$, y dado un conjunto arbitrario X, a la familia de subconjuntos de X de cardinalidad k lo denotaremos por $\binom{X}{k}$, es decir

$$\binom{X}{k} := \{A \subset X : |A| = k\}.$$

Proposición 3.4. *Sean $d, x_0, \cdots, x_d \in \mathbb{N}$ con $d \geq 1$, entonces*

a) $|Q_d| \leq 2^d$.

b) $Q_d = Q_{d-1} \cup (Q_{d-1} + \{x_d\})$.

c) $Q_d(x_0, x_1, \cdots, x_d) = Q_d(x_0, x_{\sigma(1)}, \cdots, x_{\sigma(d)})$, *donde* $\sigma : \{1, \cdots, d\} \to \{1, \cdots, d\}$ *es una permutación, es decir, en un d-cubo no importa el orden en que coloquemos los generadores.*

d) si $x_{k+1} = x_{k+2} = \cdots = x_d = 0$ *entonces* $Q_d(x_0, x_1, \cdots, x_d) = Q_k(x_0, x_1, \cdots, x_k)$.

e) si $x_1 = x_2 = \cdots = x_d$ *entonces* Q_d *es una progresión aritmética con* $d+1$ *términos, diferencia* x_1 *y base* x_0.

Demostración. Sea Q_d un d-cubo afín.

a) Tenemos que

$$\begin{aligned} |Q_d| =& |\{x_0 + \sum_{i \in I} x_i : I \subseteq [1,d]\}| \\ &= \left| \left\{ x_0 + \sum_{i\in I} x_i : I \subseteq \binom{[1,d]}{0} \right\} \cup \cdots \cup \left\{ x_0 + \sum_{i\in I} x_i : I \subseteq \binom{[1,d]}{d} \right\} \right| \\ &\leq \left| \left\{ x_0 + \sum_{i\in I} x_i : I \subseteq \binom{[1,d]}{0} \right\} \right| + \cdots + \left| \left\{ x_0 + \sum_{i\in I} x_i : I \subseteq \binom{[1,d]}{d} \right\} \right| \\ &= \binom{d}{0} + \binom{d}{1} + \cdots + \binom{d}{d} \\ &= 2^d. \end{aligned}$$

b) Primero mostremos que $Q_d \subseteq Q_{d-1} \cup (Q_{d-1} + \{x_d\})$. Sea $z \in Q_d$, entonces $z = x_0 + \sum_{i \in I} x_i$ con $I \subseteq [1, d]$.

Si $d \notin I$, entonces $I \subseteq [1, d-1]$ por lo que

$$z = x_0 + \sum_{i \in I} x_i \in Q_{d-1}.$$

Si $d \in I$, entonces

$$z = (x_0 + \sum_{i \in I} x_i) = (x_0 + \sum_{i \in I \setminus \{d\}} x_i) + x_d \in (Q_{d-1} + \{x_d\}).$$

Por lo tanto si $z \in Q_d$ tenemos que $z \in Q_{d-1}$ o $z \in (Q_{d-1} + \{x_d\})$, es decir $Q_d \subseteq Q_{d-1} \cup (Q_{d-1} + \{x_d\})$.

Ahora mostremos que $Q_{d-1} \cup (Q_{d-1} + \{x_d\}) \subseteq Q_d$. Sea $y \in Q_{d-1} \cup (Q_{d-1} + \{x_d\})$.

Como y pertenece a una unión de conjuntos, entonces hay dos posibles casos, que $y \in Q_{d-1}$ o $y \in (Q_{d-1} + \{x_d\})$. Si $y \in Q_{d-1}$ entonces $y = x_0 + \sum_{i \in I} x_i$ con $I \subseteq [1, d-1] \subseteq [1, d]$, por lo que $y \in Q_d$. Si $y \in (Q_{d-1} + \{x_d\})$ tenemos que $y = (x_0 + \sum_{i \in I} x_i) + x_d$ con $I \subseteq [1, d-1]$, luego $y = (x_0 + \sum_{i \in I \cup \{d\}} x_i)$ y como $I \cup \{d\} \subseteq [1, d]$ concluimos que $y \in Q_d$. Por lo tanto dado $z \in Q_{d-1}$ tenemos que $z \in (Q_{d-1} + \{x_d\})$,es decir $Q_{d-1} \cup (Q_{d-1} + \{x_d\}) \subseteq Q_d$.

c) Se sigue directamente de la definición de cubo.

d) Por el inciso b) tenemos que $Q_d = Q_{d-1} \cup (Q_{d-1} + \{x_d\})$, por lo que

$$Q_d = Q_{d-1} \cup (Q_{d-1} + \{0\}) = Q_{d-1} \cup Q_{d-1} = Q_{d-1}.$$

Usando de nuevo el inciso b) vemos que $Q_{d-1} = Q_{d-2} \cup (Q_{d-2} + \{x_{d-1}\})$, entonces

$$Q_{d-1} = Q_{d-2} \cup (Q_{d-2} + \{0\}) = Q_{d-2} \cup Q_{d-2} = Q_{d-2}.$$

Repitiendo este proceso con los otros generadores que son iguales a cero concluimos que

$$Q_d = Q_{d-1} = Q_{d-2} = \cdots = Q_k.$$

e) Como

$$\begin{aligned} Q_d &= \{x_0 + \sum_{i \in I} x_i : I \subseteq [1, d]\} \\ &= \left\{ x_0 + \sum_{i \in I} x_i : I \subseteq \binom{[1, d]}{0} \right\} \cup \cdots \cup \left\{ x_0 + \sum_{i \in I} x_i : I \subseteq \binom{[1, d]}{d} \right\} \end{aligned}$$

y por otra parte

$$\left\{ x_0 + \sum_{i \in I} x_i : I \subseteq \binom{[1,d]}{k} \right\} = \{x_0 + kx_1\}$$

para todo $1 \leq k \leq d$. Entonces

$$\begin{aligned} Q_d &= \{x_0\} \cup \{x_0 + x_1\} \cup \cdots \cup \{x_0 + kx_1\} \\ &= \{x_0, x_0 + x_1, \cdots, x_0 + kx_1\}. \end{aligned}$$

□

Ahora estamos listos para demostrar un resultado tipo Ramsey con respecto a la existencia de d-cubos afines monocromáticos en toda coloración del intervalo inicial de números enteros.

Lema 3.5 (Hilbert, 1892)**.** *Para todo* $k, d \in \mathbb{Z}^+$ *existe un mínimo entero* $H(k, d)$ *tal que para toda* k*-coloración de* $[1, H(k, d)]$ *existe un* d*-cubo afín monocromático.*

Demostración. Procederemos por inducción sobre d. Si $d = 1$, por el Ejemplo 3.2, sabemos que todo par de números enteros es un 1-cubo afín; entonces, $H(k, 1) \leq k+1$ pues, por el principio de las casillas (Observación 2.26), para toda k-coloración de $[1, k + 1]$ existen al menos dos números que tienen el mismo color.

Ahora sea $d \geq 2$, supongamos que para toda k existe $H = H(k, d-1)$ tal que para toda k-coloración de $[1, H]$ existe un $(d-1)$-cubo monocromático. A continuación demostraremos que $H(d, k) \leq K$ donde $K := k^H + H$; es decir, demostraremos que para toda k-coloración de $[1, K]$ existe un d-cubo monocromático. Para cada $i \in [1, k^H + 1]$ definimos el intervalo $[i, i + H - 1]$ y observamos que cada uno de estos intervalos (de cardinalidad H) se puede colorear de k^H formas distintas. Como tenemos $k^H + 1$ intervalos, por el principio de las casillas (Observación 2.26), hay dos de ellos, digamos $[i_1, i_1 + H - 1]$ e $[i_2, i_2 + H - 1]$, con $i_1 < i_2$, que están coloreados de la misma manera. Por hipótesis de inducción, existe un $(d-1)$-cubo monocromático $Q_{d-1} \subset [i_1, i_1 + H - 1]$. Para concluir la prueba mostraremos que el conjunto $Q_d := Q_{d-1} \cup (Q_{d-1} + \{i_2 - i_1\})$ es un d-cubo monocromático. Sabemos que Q_d es un d-cubo afín por el inciso $b)$ de la Proposición 3.4, para comprobar que es monocromático notemos que $(Q_{d-1} + \{i_2 - i_1\})$ es la traslación de Q_{d-1} por $i_2 - i_1$ unidades. Entonces, $(Q_{d-1} + \{i_2 - i_1\}) \subset [i_2, i_2 + H - 1]$, pero como Q_{d-1} era monocromático y los intervalos $[i_1, i_1 + H - 1]$ e $[i_2, i_2 + H - 1]$ tienen el mismo patrón de color concluimos que Q_d es monocromático. □

El Lema 3.5 es conocido en la literatura como el lema del cubo de Hilbert y tiene mucha importancia histórica ya que es el primer resultado tipo Ramsey que se conoce; David Hilbert lo probó en 1892 como un lema para demostrar lo que ahora se conoce como teorema de irreductibilidad de Hilbert [6].

Antes de probar el lema del cubo de Hilbert en su versión de densidad (Lema 3.8), requerimos estudiar los siguientes conjuntos: sea $T \subset [1, N]$, para cada $i \in [1, N]$ definimos

$$T_i := \{t \in T : t + i \in T\}.$$

Ejemplo 3.6. *Sea* $N = 10$ *y* $T = \{1, 2, 4, 7, 8\}$*, entonces* $T_1 = \{1, 7\}$*,* $T_2 = \{2\}$*,* $T_3 = \{1, 4\}$*,* $T_4 = \{4\}$*,* $T_5 = \{2\}$*,* $T_6 = \{1, 2\}$*,* $T_7 = \{1\}$*,* $T_8 = \emptyset$*,* $T_9 = \emptyset$*,* $T_{10} = \emptyset$*.*

Notemos que en el Ejemplo 3.6 sucede que $\sum_{i=1}^{10} |T_i| = 10 = \binom{5}{2} = \binom{|T|}{2}$. Observemos que esto sucede en general, es decir, para todo $T \subset [1, N]$,

$$\sum_{i \in [1,N]} |T_i| = \binom{|T|}{2} \tag{3.1}$$

pues $|T_i|$ es igual a la cantidad de parejas $t, t' \in T$ tales que $t' - t = i$, por lo tanto $\sum_{i \in [1,N]} T_i$ es igual a la cantidad de parejas $t, t' \in T$ tales que $t' - t > 0$ y de estas precisamente hay $\binom{|T|}{2}$.

Ahora, utilizaremos la observación anterior para enunciar la siguiente proposición.

Proposición 3.7. *Sea* $N \geq 2$*. Para todo subconjunto* $T \subset [1, N]$ *con* $|T| \geq 2$ *existe* $i \in [1, N]$ *tal que* $|T_i| \geq |T|^2/4N$*.*

Demostración. Por (3.1) y el principio de las casillas, existe $i \in [1, N]$ tal que

$$|T_i| \geq \frac{\binom{|T|}{2}}{N}. \tag{3.2}$$

Por otro lado, si $|T| \geq 2$, tenemos $|T|^2 \geq 2|T|$ luego $\frac{|T|^2}{2} \geq |T|$, por lo que

$$|T|^2 - |T| \geq \frac{|T|^2}{2},$$

y por lo tanto

$$\frac{|T|^2 - |T|}{2N} \geq \frac{|T|^2}{4N}. \tag{3.3}$$

Como

$$\frac{\binom{|T|}{2}}{N} = \frac{|T|(|T| - 1)}{2N} = \frac{|T|^2 - |T|}{2N},$$

concatenando (3.2) y (3.3) obtenemos $|T_i| \geq \frac{|T|^2}{4N}$ que era lo que buscábamos. $\square$

Ahora presentaremos la versión de densidad del Lema 3.5.

Lema 3.8 (Szemerédi, 1969 [7]). *Sean $d, N \in \mathbb{Z}^+$. Todo subconjunto $S \subset [1, N]$ con $|S| \geq 4N^{1-1/2^d}$ contiene un d-cubo afín.*

Demostración. Por la Proposición 3.7 sabemos que existe un $i_1 \in [1, N]$ tal que $|S_{i_1}| \geq |S|^2/4N$. Luego, como $4N^{1-1/2^d} \geq (4N)^{1-1/2^d}$, tenemos

$$|S_{i_1}| \geq \frac{|S|^2}{4N} \geq \frac{(4N^{1-1/2^d})^2}{4N} \geq \frac{((4N)^{1-1/2^d})^2}{4N} = \frac{(4N)^{2-2/2^d}}{4N} = (4N)^{1-1/2^{d-1}}.$$

Consideremos ahora el conjunto S_{i_1}. Por la Proposición 3.7 sabemos, nuevamente, que existe un $i_2 \in [1, N]$ tal que $|(S_{i_1})_{i_2}| \geq |S_{i_1}|^2/4N$, y aplicando el mismo procedimiento llegaremos a que $|(S_{i_1})_{i_2}| \geq (4N)^{1-1/2^{d-2}}$. En general, si escribimos $S_{i_1,i_2} = (S_{i_1})_{i_2}, S_{i_1,i_2,i_3} = (S_{i_1,i_2})_{i_3}$, etc. y repetimos el argumento, obtenemos, para cada $j \in [1, d]$, $S_{i_1,i_2,\cdots,i_j} = (S_{i_1,\cdots,i_{j-1}})_{i_j}$ con $|S_{i_1,\cdots,i_j}| \geq (4N)^{1-1/2^{d-j}}$. Observemos que para $j = d$, $|S_{i_1,\cdots,i_d}| \geq (4N)^{1-1/2^{d-d}} = 1$ y por lo tanto $S_{i_1,\cdots,i_d}$ no es vacío. Sea i_0 cualquier elemento en $S_{i_1,\cdots,i_d}$. Probaremos que el cubo $Q_d(i_0, i_1, \cdots, i_d)$ está contenido en S. En efecto, $i_0 \in S_{i_1,\cdots,i_d}$ significa que $i_0, i_0 + i_d \in S_{i_1,\cdots,i_{d-1}}$, que a la vez implica que $i_0, i_0 + i_{d-1}, i_0 + i_d, i_0 + i_d + i_{d-1} \in S_{i_1,\cdots,i_{d-2}}$, etc. En general vemos que $i_0 + \sum_{j \in I} i_j$ está en S para todo $I \subset [1, d]$. $\square$

Para darnos una idea de lo que dice el Lema 3.8, observemos que $4N^{1-1/2^d} = \frac{4}{N^{1/2^d}}N$, de modo que una proporción de $\frac{4}{N^{1/2^d}}$ es lo que nos garantiza la existencia de un d-cubo en $[1, N]$. Por ejemplo, si $N = 625$ y $d = 2$, el Lema 3.8 nos dice que todo subconjunto $S \subset [1, 625]$ con $|S| \geq 500 = \frac{4}{5}N$ contiene un 2-cubo.

En general, del Lema 3.8 se deduce el siguiente corolario (usaremos $\log = \log_2$, la función logaritmo en base 2).

Corolario 3.9. *Si $N \geq 2^{[\log(4/\delta)]^2}$, entonces cualquier $S \subset [1, N]$ con $|S| \geq \delta N$ contiene un d-cubo afín con $d \geq \frac{1}{4} \log \log N$.*

Demostración. Sea d un entero que esté entre $\frac{1}{4} \log \log N$ y $\frac{1}{2} \log \log N$, es decir $\frac{1}{4} \log \log N \leq d \leq \frac{1}{2} \log \log N$, utilizando la desigualdad de la derecha tenemos $2^d \leq [\log N]^{1/2}$. Por hipótesis tenemos que $N \geq 2^{[\log(4/\delta)]^2}$ entonces

$$2^{[\log N]^{1/2}} \geq 4/\delta,$$

lo cual implica

$$N = 2^{\log N} \geq (4/\delta)^{[\log N]^{1/2}} \geq (4/\delta)^{2^d}.$$

Esto nos da $\delta N \geq 4N^{1-1/2^d}$, y aplicando el Lema 3.8 obtenemos un d-cubo afín con $d \geq \frac{1}{4} \log \log N$. $\square$

Para entender el Cororario 3.9 analicemos el siguiente ejemplo.

Consideremos $\delta = 1/2$. Lo que nos dice el Corolario 3.9 es que, si $N \geq 2^9 = 512$, entonces cualquier $S \subset [1, N]$ con $|S| \geq (1/2)N$ contiene un d-cubo afín con $d \geq \frac{1}{4} \log\log N$. Pero notemos que si tomamos exactamente $N = 2^9 = 512$ entonces lo más que podemos concluir es que S contenga un d-cubo con $d \geq \frac{1}{4} \log\log 2^9 \approx ,7924$, lo cual no muestra nada interesante pues d podría ser incluso igual a uno. Esto quiere decir que debemos tomar un N todavía más grande para que haya la posibilidad de que S contenga cubos de mayor cardinalidad. Veamos qué tan grande debe ser N para tener un valor específico de d. Tomemos $N = 2^{2^{4d'}}$ con $d' \geq 2$, entonces el Corolario 3.9 nos dice que cualquier $S \subset [1, N]$ con $|S| \geq (1/2)(2^{2^{4d'}})$ contiene un d-cubo afín con $d \geq \frac{1}{4} \log\log 2^{2^{4d'}} = d'$. Notemos que si queremos aumentar el tamaño del d-cubo, entonces N crece de manera exponencial.

3.2. Presentación del teorema de Roth

Existen dos versiones del Teorema de Roth que son equivalentes, la versión finita [1] y la versión infinita [9]. En la presente tesis demostraremos la versión finita del Teorema de Roth por un método meramente combinatorio y mostraremos que la versión finita implica la versión infinita.

Teorema 3.10 (Roth versión finita)**.** *Para todo $0 < \delta < 1$ existe un mínimo entero $N_0 = N_0(\delta)$ tal que si $N \geq N_0$, cualquier subconjunto $S \subset [1, N]$ con $|S| \geq \delta N$ contiene una $AP(3)$.*

Por ejemplo, para el valor concreto $\delta = 1/2$ el teorema de Roth nos dice que existe un mínimo entero $N_0(1/2)$ tal que si $N \geq N_0(1/2)$, cualquier subconjunto $S \subset [1, N]$ de cardinalidad mayor o igual que $N/2$, contiene una $AP(3)$.

Antes de dar la prueba del teorema de Roth (en la siguiente sección) mostraremos una forma equivalente de este teorema y probaremos que $N_0(1/2) = 17$. Primero definamos la siguiente función.

Definición 3.11. *Sea $F : \mathbb{Z}^+ \to \mathbb{Z}^+$ definida por*

$$F(N) := \max\{|S| : S \subset [1, N],\ S \ \ sin\ \ AP(3)\}.$$

Observemos que esta función nos daría exactamente el mismo valor si sustituimos el intervalo $[1, N]$ por el intervalo $[a, N + (a - 1)]$ donde $a \in \mathbb{Z}$, es decir , si

$$F_a(N) := \max\{|S| : S \subset [a, N + (a - 1)],\ S \ \ \text{sin}\ \ AP(3)\}$$

entonces $F(N) = F_a(N)$ para toda $N \in \mathbb{Z}^+$. Esto se debe a que las progresiones aritméticas son invariantes bajo traslaciones. Por simplicidad, estaremos trabajando únicamente con la función F pero siempre teniendo en cuenta que es igual a F_a.

De la Definición 3.11 se sigue inmediatamente que $F(1) = 1$ y $F(2) = 2$. En el Ejemplo 3.14 veremos casos más interesantes. Antes, veamos algunas observaciones.

Observación 3.12. *Dado $x \in \mathbb{Z}^+$,*

a) el significado de $x \leq F(N)$ es que existe un conjunto $S \subset [1, N]$ con $|S| = x$ que no contiene $AP(3)$. En consecuencia, para todo $N \in \mathbb{Z}^+$, tenemos que

$$F(N) \leq F(N+1).$$

b) El significado de $F(N) \leq x$ es que todo conjunto $S \subset [1, N]$ con $|S| = x + 1$ contiene una $AP(3)$.

Ahora procedamos a dar una propiedad importante de la función.

Proposición 3.13. *La función $F : \mathbb{Z}^+ \to \mathbb{Z}^+$ es* subaditiva*, es decir, para todo $x_1, x_2 \in \mathbb{Z}^+$ tenemos que*

$$F(x_1 + x_2) \leq F(x_1) + F(x_2).$$

Demostración. Por la definición de F existe un $S \subset [1, x_1+x_2]$ con $|S| = F(x_1+x_2)$ y S sin $AP(3)$. Luego, tenemos que $S = (S \cap [1, x_1]) \cup (S \cap [x_1+1, x_1+x_2])$, por lo tanto $|S| = |S \cap [1, x_1]| + |S \cap [x_1+1, x_1+x_2]|$. Ahora, observemos que $|S \cap [1, x_1]| \leq F(x_1)$ pues de lo contrario tendríamos que $S \cap [1, x_1] \subset S$ contiene una $AP(3)$, es decir, S contiene una $AP(3)$, lo cual es una contradicción. De igual forma tenemos que $|S \cap [x_1+1, x_1+x_2]| \leq F(x_2)$. Por lo tanto $|S| \leq F(x_1) + F(x_2)$. $\square$

En el siguiente ejemplo calcularemos varios valores de F, que más tarde usaremos.

Ejemplo 3.14. *Usaremos la siguiente coloración $\chi : [1, N] \to \{azul, rojo\}$ definida por $\chi(n) = azul$ si $n \notin S$ y $\chi(n) = rojo$ si $n \in S$ para todo $n \in [1, N]$ (los números serán de color negro cuando aún no se decida si pertenecen o no a S).*

- $F(3) = 2$.

  $F(3) \geq 2$ *por el siguiente conjunto de dos elementos sin* $AP(3)$

  $$1\ 2\ 3.$$

  $F(3) \leq 2$ *porque el único subconjunto de tres elementos de $[1, 3]$ es él mismo, y este es una $AP(3)$.*

- $F(4) = 3$.

  $F(4) \geq 3$ por el siguiente conjunto de tres elementos sin $AP(3)$

  $$1\ 2\ 3\ 4.$$

  $F(4) \leq 3$ porque el único subconjunto de cuatro elementos de $[1,4]$ es él mismo y contiene una $AP(3)$.

- $F(5) = 4$.

  $F(5) \geq 4$ por el siguiente conjunto de cuatro elementos sin $AP(3)$

  $$1\ 2\ 3\ 4\ 5.$$

  $F(5) \leq 4$ porque el único subconjunto de cinco elementos de $[1,5]$ es él mismo y contiene una $AP(3)$.

- $F(6) = 4$.

  $F(6) \geq 4$ por la Observación 3.12 inciso a) y el caso anterior.

  $F(6) \leq 4$ por la Proposición 3.13 tomando $x_1 = x_2 = 3$.

- $F(7) = 4$.

  $F(7) \geq 4$ por la Observación 3.12 inciso a) y el caso anterior.

  $F(7) \leq 4$ porque todo subconjunto $S \subset [1,7]$ con $|S| = 5$ contiene una $AP(3)$. Para ver esto, supongamos por contradicción que existe $S \subset [1,7]$ con $|S| = 5$ sin $AP(3)$. Notemos que $7 \in S$ pues $F(6) = 4$, de igual forma, $1 \in S$ pues $F_2(6) = 4$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7.$$

  Luego, $4 \notin S$, de lo contrario $\{1,4,7\} \subset S$ sería una $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7.$$

  Ahora, por el principio de las casillas hay dos elementos de S en el intervalo $[2,3]$ o en $[5,6]$. Sin pérdida de generalidad supongamos que los dos elementos de S están en $[2,3]$. Entonces $\{1,2,3\} \subset S$ es una $AP(3)$ lo cual es una contradicción.

- $F(8) = 4$.

  $F(8) \geq 4$ *por la Observación 3.12 inciso a) y el caso anterior.*

  $F(8) \leq 4$ *porque todo subconjunto* $S \subset [1, 8]$ *con* $|S| = 5$ *contiene una* $AP(3)$. *Para ver esto, supongamos por contradicción que existe* $S \subset [1, 8]$ *con* $|S| = 5$ *sin* $AP(3)$. *Notemos que* $8 \in S$ *pues* $F(7) = 4$, *de igual forma,* $1 \in S$ *pues* $F_2(7) = 4$

  1 2 3 4 5 6 7 8.

  Ahora, por el principio de las casillas hay al menos dos elementos de S *en el intervalo* $[2, 4]$ *o en* $[5, 7]$. *Sin pérdida de generalidad supongamos que los dos elementos de* S *están en* $[2, 4]$.

  - *caso i)* $2, 3 \in S$.

    1 2 3 4 5 6 7 8.

    Notemos que $\{1, 2, 3\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

  - *caso ii)* $2, 4 \in S$.

    1 2 3 4 5 6 7 8.

    notemos que $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\}$ *sería una* $AP(3)$ *en* S, $5 \notin S$ *pues de otro modo* $\{2, 5, 8\}$ *sería una* $AP(3)$ *en* S, $7 \notin S$ *ya que en otro caso* $\{1, 4, 7\}$ *sería una* $AP(3)$ *en* S

    1 2 3 4 5 6 7 8.

    Por lo tanto $6 \in S$

    1 2 3 4 5 6 7 8.

    Notemos que $\{4, 6, 8\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

  - *caso iii)* $3, 4 \in S$.

    1 2 3 4 5 6 7 8.

    notemos que $2 \notin S$ *pues de lo contrario* $\{1, 2, 3\}$ *sería una* $AP(3)$ *en* S, $5 \notin S$ *pues de otro modo* $\{3, 4, 5\}$ *sería una* $AP(3)$ *en* S, $6 \notin S$ *ya que en otro caso* $\{4, 6, 8\}$ *sería una* $AP(3)$ *en* S

    1 2 3 4 5 6 7 8.

    Por lo tanto $7 \in S$

    1 2 3 4 5 6 7 8.

    Notemos que $\{1, 4, 7\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- $F(9) = 5$.

  $F(9) \geq 5$ *por el siguiente conjunto de cinco elementos en* $[1, 9]$ *sin* $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9.$$

  $F(9) \leq 5$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 8$.

- $F(10) = 5$.

  $F(10) \geq 5$ *por la Observación 3.12 inciso a) y el caso anterior.*

  $F(10) \leq 5$ *porque todo subconjunto* $S \subset [1, 10]$ *con* $|S| = 6$ *contiene una* $AP(3)$. *Para ver esto, supongamos por contradicción que existe* $S \subset [1, 10]$ *con* $|S| = 6$ *sin* $AP(3)$. *Como* $F(8) = 4$ *entonces* $9, 10 \in S$, *de la misma forma* $1, 2 \in S$ *pues* $F_3(8) = 4$, *entonces tenemos*

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10$$

  luego $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\}$ *sería una* $AP(3)$, $5 \notin S$ *pues de otro modo* $\{1, 5, 9\}$ *sería una* $AP(3)$, $6 \notin S$ *ya que en otro caso* $\{2, 6, 10\}$ *sería una* $AP(3)$, $8 \notin S$ *ya que de lo contrario* $\{8, 9, 10\}$ *sería una* $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10$$

  por lo tanto $4, 7 \in S$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10$$

  lo cual es una contradicción pues $\{1, 4, 7\}$ *es una* $AP(3)$.

- $F(11) = 6$.

  $F(11) \geq 6$ *por el siguiente conjunto de seis elementos en* $[1, 11]$ *sin* $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11.$$

  $F(11) \leq 6$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 10$.

- $F(12) = 6$.

  $F(12) \geq 6$ *por la Observación 3.12 inciso a) y el caso anterior.*

  $F(12) \leq 6$ *porque todo subconjunto* $S \subset [1, 12]$ *con* $|S| = 7$ *contiene una* $AP(3)$. *Para ver esto, supongamos por contradicción que existe* $S \subset [1, 12]$ *con* $|S| = 7$

sin $AP(3)$*. Como* $F(10) = 5$ *entonces* $11, 12 \in S$ *, de la misma forma,* $1, 2 \in S$ *pues* $F_3(10) = 5$

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12.$$

Luego, $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\} \subset S$ *sería una* $AP(3)$*,* $6 \notin S$ *pues de otro modo* $\{1, 6, 11\} \subset S$ *sería una* $AP(3)$*,* $7 \notin S$ *ya que de otro modo* $\{2, 7, 12\} \subset S$ *sería una* $AP(3)$*,* $10 \notin S$ *ya que de lo contrario de lo contrario* $\{10, 11, 12\} \subset S$ *sería una* $AP(3)$

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12.$$

Ahora nos faltan tres elementos de S *que están en* $[4, 5]$ *y* $[8, 9]$*. Entonces tenemos que dos elementos de* S *están en* $[4, 5]$ *y uno* $[8, 9]$ *, o un elemento de* S *está en* $[4, 5]$ *y dos en* $[8, 9]$*. Sin pérdida de generalidad supongamos que los dos elementos de* S *están en* $[4, 5]$ *y uno* $[8, 9]$

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12.$$

Luego, $8 \notin S$ *pues de lo contrario* $\{2, 5, 8\} \subset S$ *seía una* $AP(3)$*, por lo tanto tenemos que* $9 \in S$

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12.$$

Pero $\{1,5,9\} \subset S$ *es una* $AP(3)$ *, lo cual es una contradicción.*

- $F(13) = 7$

  $F(13) \geq 7$ *por el siguiente conjunto de siete elementos en* $[1, 13]$ *sin* $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13.$$

  $F(13) \leq 7$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 12$*.*

- $F(14) = 8$

  $F(14) \geq 8$ *por el siguiente conjunto de ocho elementos en* $[1, 14]$ *sin* $AP(3)$

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14.$$

  $F(14) \leq 8$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 13$*.*

- $F(15) = 8$

  $F(15) \geq 8$ *por la Observación 3.12 inciso a) y el caso anterior.*

  $F(15) \leq 8$ *por la Proposición 3.13 tomando* $x_1 = 7$ *y* $x_2 = 8$*.*

- $F(16) = 8$

  $F(16) \geq 8$ por la Observación 3.12 inciso a) y el caso anterior.

  $F(16) \leq 8$ por la Proposición 3.13 tomando $x_1 = 8$ y $x_2 = 8$.

- $F(17) = 8$

  $F(17) \geq 8$ por la Observación 3.12 inciso a) y el caso anterior.

  $F(17) \leq 8$ porque todo subconjunto $S \subset [1, 17]$ con $|S| = 9$ contiene una $AP(3)$. Para ver esto, supongamos por contradicción que existe $S \subset [1, 17]$ con $|S| = 9$ sin $AP(3)$. Notemos que $9 \in S$, pues de lo contrario, como $|S| = 9$, por el principio de las casillas en alguno de los intervalos $[1, 8]$ o $[10, 17]$ habría cinco elementos de S y como $F(8) = F_{10}(8) = 4$ tendríamos que S contiene una $AP(3)$, lo cual es una contradicción.

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17.$$

  Entonces, $9 \in S$, $|S \cap [1, 8]| \leq 4$ y $|S \cap [10, 17]| \leq 4$ (porque $F(8) = 4$). Ahora, observemos que $1 \in S$, ya que en otro caso $|S \cap [2, 9]| = 5$ lo cual es una contradicción pues $F_2(8) = 4$. Análogamente, $17 \in S$.

  $$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17.$$

  Entonces $\{1, 9, 17\} \subset S$, lo cual es una contradicción pues $\{1, 9, 17\}$ es una $AP(3)$.

En la siguiente tabla se muestran los valores exatos de $F(N)$ que hemos calculado.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$F(N)$	1	2	2	3	4	4	4	4	5	5	6	6	7	8	8	8	8

Cuadro 3.1: Valores de $F(N)$ calculados en el Ejemplo 3.14.

La función $F(N)$ nos servirá para enunciar la siguiente equivalencia del Teorema 3.10.

Proposición 3.15. *Los siguientes enunciados son equivalentes:*

(1) *Para todo $0 < \delta < 1$ existe un mínimo entero $N_0 = N_0(\delta)$ tal que si $N \geq N_0$, cualquier subconjunto $S \subset [1, N]$ con $|S| \geq \delta N$ contiene una $AP(3)$,*

(2) $\lim\limits_{N \to \infty} \frac{F(N)}{N} = 0.$

Demostración. Primero mostremos que (1) implica (2). Tenemos que mostrar que $\lim_{N\to\infty} \frac{F(N)}{N} = 0$, es decir, para toda $\epsilon > 0$ existe $N_0 \in \mathbb{N}$ tal que si $N \geq N_0$ entonces $F(N)/N < \epsilon$. Sea $\epsilon > 0$, entonces por (1) tenemos que existe $N_0 = N_0(\epsilon)$ tal que si $N \geq N_0$, cualquier subconjunto $S \subset [1, N]$ con $|S| \geq \epsilon N$ contiene una $AP(3)$. Para finalizar mostremos que $F(N) < \epsilon N$. Para esto , supongamos que $F(N) \geq \epsilon N$. Sea $S \subset [1, N]$ con $|S| = F(N) \geq \epsilon N$, entonces S contiene una $AP(3)$, lo cual contradice la definición de F. Por lo tanto $F(N) < \epsilon N$, es decir $F(N)/N < \epsilon$.

Ahora veamos que (2) implica (1). Como $\lim_{N\to\infty} \frac{F(N)}{N} = 0$, tenemos que para toda $\delta > 0$ existe $N_0 \in \mathbb{N}$ tal que si $N \geq N_0$ entonces $F(N)/N < \delta$. Consideremos $S \subset [1, N]$ con $|S| \geq \delta N$. Como $F(N) < \delta N$ y $\delta N \leq |S|$ tenemos que $F(N) < |S|$. Entonces por la defición de F tenemos que $S \subset [1, N]$ contiene una $AP(3)$. $\square$

En la Proposición 3.17, probaremos que $N_0(1/2) = 17$. Notemos que $N_0(1/2) \geq 17$ puesto que $F(16) = 8$ y por lo tanto $F(16)/16 = 1/2$. Para demostrar que $N_0(1/2) \leq 17$, hay que mostrar que a partir de $N = 17$ se tiene $F(N)/N < 1/2$. En el siguiente ejemplo nos dedicaremos a calcular cotas superiores para $F(N)$ con $N \in [18, 33]$.

Ejemplo 3.16. *Recordemos la coloración $\chi : [1, N] \to \{azul, rojo\}$ definida por $\chi(n) = azul$ si $n \notin S$ y $\chi(n) = rojo$ si $n \in S$ para todo $n \in [1, N]$ (los números serán de color negro cuando aún no se decida si pertenecen o no a S).*

- $F(18) \leq 8$ *porque todo subconjunto $S \subset [1, 18]$ con $|S| = 9$ contiene una $AP(3)$. Para ver esto, supongamos por contradicción que existe $S \subset [1, 18]$ con $|S| = 9$ sin $AP(3)$. Como $F(17) = 8$ entonces $18 \in S$, de igual forma, como $F_2(17) = 8$ entonces $1 \in S$.*

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

  Aún nos faltan siete elementos de S que están en $[2, 17]$, entonces por el principio de las casillas hay al menos cuatro elementos de S en el intervalo $[2, 9]$ o hay al menos cuatro elementos de S en el intervalo $[10, 17]$. Sin pérdida de generalidad supongamos que los cuatro elementos están en $[2, 9]$. Como $F(8) = 4$ entonces $9 \in S$.

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

  Luego, $5 \notin S$ pues de lo contrario $\{1, 5, 9\} \subset S$ sería una $AP(3)$, $17 \notin S$ ya que de otro modo $\{1, 9, 17\} \subset S$ sería una $AP(3)$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

- *Caso i) Hay tres elementos de S en* $[2, 4]$.
  Vemos que $\{2, 3, 4\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*
- *Caso ii) Hay tres elementos de S en* $[6, 8]$.
  Observemos que $\{6, 7, 8\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*
- *Caso iii) Hay dos elementos de S en* $[2, 4]$ *y uno en* $[6, 8]$.
  - *Caso iii.1)* $2, 3 \in S$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Vemos que $\{1, 2, 3\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*
  - *Caso iii.2)* $2, 4 \in S$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Luego, $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\} \subset S$ *sería una* $AP(3)$, $6 \notin S$ *pues de otro modo* $\{2, 4, 6\} \subset S$ *sería una* $AP(3)$, $7 \notin S$ *ya que en otro caso* $\{1, 4, 7\} \subset S$ *sería una* $AP(3)$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Por lo tanto $8 \in S$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Luego, $10 \notin S$ *pues de lo contrario* $\{8, 9, 10\} \subset S$ *sería una* $AP(3)$, $14 \notin S$ *pues de otro modo* $\{2, 8, 14\} \subset S$ *sería una* $AP(3)$, $15 \notin S$ *ya que en otro caso* $\{1, 8, 15\} \subset S$ *sería una* $AP(3)$, $16 \notin S$ *ya que de lo contrario* $\{2, 9, 16\} \subset S$ *sería una* $AP(3)$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Por lo tanto $11, 12, 13 \in S$.

    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18.

    Observemos que $\{11, 12, 13\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- *Caso iii.3)* $3, 4 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $6 \notin S$ *pues de lo contrario* $\{3, 6, 9\} \subset S$ *sería una* $AP(3)$*,* $7 \notin S$ *pues de otro modo* $\{1, 4, 7\} \subset S$ *sería una* $AP(3)$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $8 \in S$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $10 \notin S$ *pues de lo contrario* $\{8, 9, 10\} \subset S$ *sería una* $AP(3)$*,* $14 \notin S$ *pues de otro modo* $\{2, 8, 14\} \subset S$ *sería una* $AP(3)$*,* $15 \notin S$ *ya que en otro caso* $\{1, 8, 15\} \subset S$ *sería una* $AP(3)$*,* $16 \notin S$ *ya que de lo contrario* $\{2, 9, 16\} \subset S$ *sería una* $AP(3)$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $11, 12, 13 \in S$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Observemos que $\{11, 12, 13\} \subset S$ *es una* $AP(3)$*, lo cual es una contradicción.*

- *Caso iv) Hay un elemento de* S *en* $[2, 4]$ *y dos en* $[6, 8]$*.*
  - *Caso iv.1)* $6, 7 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $3 \notin S$ *pues de lo contrario* $\{3, 6, 9\} \subset S$ *sería una* $AP(3)$*,* $4 \notin S$ *pues de otro modo* $\{1, 4, 7\} \subset S$ *sería una* $AP(3)$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $2 \in S$*.*

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $10 \notin S$ *pues de lo contrario* $\{2, 6, 10\} \subset S$ *sería una* $AP(3)$*,* $11 \notin S$ *pues de otro modo* $\{7, 9, 11\} \subset S$ *sería una* $AP(3)$*,* $12 \notin S$ *ya* *que en otro caso* $\{2,7,12\} \subset S$ *sería una* $AP(3)$, $16 \notin S$ *ya que de lo contrario* $\{2,9,16\} \subset S$ *sería una* $AP(3)$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $13, 14, 15 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Observemos que $\{13,14,15\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- *Caso iv.2)* $6, 8 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $3 \notin S$ *pues de lo contrario* $\{3,6,9\} \subset S$ *sería una* $AP(3)$, $4 \notin S$ *pues de otro modo* $\{4,6,8\} \subset S$ *sería una* $AP(3)$, $7 \notin S$ *ya que en otro caso* $\{6,7,8\} \subset S$ *sería una* $AP(3)$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $2 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Luego, $10 \notin S$ *pues de lo contrario* $\{8,9,10\} \subset S$ *sería una* $AP(3)$, $12 \notin S$ *pues de otro modo* $\{6,9,12\} \subset S$ *sería una* $AP(3)$, $14 \notin S$ *ya que en otro caso* $\{2,8,14\} \subset S$ *sería una* $AP(3)$, $16 \notin S$ *ya que de lo contrario* $\{2,9,16\} \subset S$ *sería una* $AP(3)$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Por lo tanto $11, 13, 15 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Observemos que $\{11,13,15\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- *Caso iv.3)* $7, 8 \in S$.

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18.$$

Vemos que $\{7,8,9\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- *$F(19) \leq 9$ por la Proposición 3.13 tomando $x_1 = 1$ y $x_2 = 18$.*

- *$F(20) \leq 9$ porque todo subconjunto $S \subset [1, 20]$ con $|S| = 10$ contiene una $AP(3)$. Para ver esto, supongamos por contradicción que existe $S \subset [1, 20]$ con $|S| = 10$ sin $AP(3)$. Como $F(18) = 8$ entonces $19, 20 \in S$, de igual forma, como $F_2(18) = 8$ entonces $1, 2 \in S$.*

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20.

  Luego, $3 \notin S$ pues de lo contrario $\{1, 2, 3\} \subset S$ sería una $AP(3)$, $10 \notin S$ pues de otro modo $\{1, 10, 19\} \subset S$ sería una $AP(3)$, $11 \notin S$ ya que en otro caso $\{2, 11, 20\} \subset S$ sería una $AP(3)$, $18 \notin S$ ya que de lo contrario $\{18, 19, 20\} \subset S$ sería una $AP(3)$.

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20.

  Si en el intervalo $[4, 9]$ hubiera más de tres elementos de S entonces en el intervalo $[1, 9]$ habría más de cinco elementos de S, por lo tanto en $[1, 9]$ habría una $AP(3)$ pues $F(9) = 5$. En cambio, si en $[4, 9]$ hubiera menos de tres elementos de S entonces en el intervalo $[12, 17]$ habría más de tres elementos de S, por lo tanto en $[12, 20]$ habría más de cinco elementos de S, por lo tanto en $[12, 20]$ habría una $AP(3)$ pues $F_{12}(9) = 5$. Entonces en los intervalos $[4, 9]$ y $[12, 17]$ hay tres elementos de S respectivamente. Ahora, $9 \in S$ pues $F(8) = 4$, de igual forma, $12 \in S$ pues $F_{13}(8) = 4$.

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20.

  Luego, $5 \notin S$ pues de lo contrario $\{1, 5, 9\}$ sería una $AP(3)$, $6 \notin S$ pues de otro modo $\{6, 9, 12\}$ sería una $AP(3)$, $7 \notin S$ ya que en otro caso $\{2, 7, 12\}$ sería una $AP(3)$, $14 \notin S$ ya que de lo contrario $\{9, 14, 19\}$ sería una $AP(3)$, $15 \notin S$ pues de otra manera $\{9, 12, 15\}$ sería una $AP(3)$, $16 \notin S$ ya que de otra forma $\{12, 16, 20\}$ sería una $AP(3)$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20.

  Por último tenemos que $4, 9, 13, 17 \in S$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20.

  Observemos que $\{1, 9, 17\} \subset S$ es una $AP(3)$, lo cual es una contradicción.

- *$F(21) \leq 10$ por la Proposición 3.13 tomando $x_1 = 1$ y $x_2 = 20$.*

- $F(22) \leq 10$ *porque todo subconjunto* $S \subset [1, 22]$ *con* $|S| = 11$ *contiene una* $AP(3)$. *Para ver esto, supongamos por contradicción que existe* $S \subset [1, 22]$ *con* $|S| = 11$ *sin* $AP(3)$. *Como* $F(20) = 9$ *entonces* $21, 22 \in S$, *de igual forma, como* $F_3(20) = 9$ *entonces* $1, 2 \in S$.

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22.

  Luego, $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\} \subset S$ *sería una* $AP(3)$, $11 \notin S$ *pues de otro modo* $\{1, 11, 21\} \subset S$ *sería una* $AP(3)$, $12 \notin S$ *ya que en otro caso* $\{2, 12, 22\} \subset S$ *sería una* $AP(3)$, $20 \notin S$ *pues de otra manera* $\{20, 21, 22\} \subset S$ *sería una* $AP(3)$.

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22.

  Por el principio de las casillas, hay al menos cuatro elementos de S *en* $[3, 10]$ *o* $[13, 20]$. *Sin pérdida de generalidad, supongamos que hay al menos cuatro elementos de* S *en* $[3, 10]$, *por lo tanto en el intervalo* $[1, 10]$ *habría más de cinco elementos de* S, *pero esto es una contradicción pues* $F(10) = 5$.

- $F(23) \leq 11$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 22$.

- $F(24) \leq 11$ *porque todo subconjunto* $S \subset [1, 24]$ *con* $|S| = 12$ *contiene una* $AP(3)$. *Para ver esto, supongamos por contradicción que existe* $S \subset [1, 24]$ *con* $|S| = 12$ *sin* $AP(3)$. *Como* $F(22) \leq 10$ *entonces* $23, 24 \in S$, *de la misma manera, como* $F_3(22) \leq 10$ *entonces* $1, 2 \in S$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

  Luego, $3 \notin S$ *pues de lo contrario* $\{1, 2, 3\} \subset S$ *sería una* $AP(3)$, $22 \notin S$ *pues de otro modo* $\{22, 23, 24\} \subset S$ *sería una* $AP(3)$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

  Como $F(20) \leq 9$ *entonces* $21 \in S$, *y como* $F_5(20) \leq 9$ *entonces* $4 \in S$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

  Luego, $6 \notin S$ *pues de lo contrario* $\{2, 4, 6\} \subset S$ *sería una* $AP(3)$, $7 \notin S$ *pues de otro modo* $\{1, 4, 7\} \subset S$ *sería una* $AP(3)$, $18 \notin S$ *ya que en otro caso* $\{18, 21, 24\} \subset S$ *sería una* $AP(3)$, $19 \notin S$ *pues de otra manera* $\{19, 21, 23\} \subset S$ *sería una* $AP(3)$

  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

Como $F(17) = 8$ *entonces* $20 \in S$ *y como* $F_8(17) = 8$ *entonces* $5 \in S$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

Luego, $8 \notin S$ *pues de lo contrario* $\{2,5,8\} \subset S$ *sería una* $AP(3)$,$9 \notin S$ *pues de otro modo* $\{1,5,9\} \subset S$ *sería una* $AP(3)$, $12 \notin S$ *ya que en otro caso* $\{4,12,20\} \subset S$ *sería una* $AP(3)$, $13 \notin S$ *ya que de lo contrario* $\{5,13,21\} \subset S$ *sería una* $AP(3)$, $16 \notin S$ *pues de otra manera* $\{16,20,24\} \subset S$ *sería una* $AP(3)$, $17 \notin S$ *ya que de otra forma* $\{17,20,23\} \subset S$ *sería una* $AP(3)$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

Por lo tanto $10, 11, 14, 15 \in S$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.

Podemos observar que $\{1,11,21\} \subset S$ *es una* $AP(3)$, *lo cual es una contradicción.*

- $F(25) \leq 12$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 24$.
- $F(26) \leq 12$ *por la Proposición 3.13 tomando* $x_1 = 8$ *y* $x_2 = 18$.
- $F(27) \leq 13$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 26$.
- $F(28) \leq 13$ *por la Proposición 3.13 tomando* $x_1 = 8$ *y* $x_2 = 20$.
- $F(29) \leq 14$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 28$.
- $F(30) \leq 14$ *por la Proposición 3.13 tomando* $x_1 = 8$ *y* $x_2 = 22$.
- $F(31) \leq 15$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 30$.
- $F(32) \leq 15$ *por la Proposición 3.13 tomando* $x_1 = 8$ *y* $x_2 = 24$.
- $F(33) \leq 16$ *por la Proposición 3.13 tomando* $x_1 = 1$ *y* $x_2 = 32$.

En la siguiente tabla mostramos las cotas de $F(N)$ que hemos probado.
Ahora sí estamos listos para probar que $N_0(1/2) = 17$.

Proposición 3.17. *Para todo* $N \geq 17$, *se satisface* $F(N)/N < 1/2$.

N	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$F(N) \leq$	8	9	9	10	10	11	11	12	12	13	13	14	14	15	15	16

Cuadro 3.2: Cotas superiores establecidas en el Ejemplo 3.16.

Demostración. Sea $N \geq 17$ expresado como $N = 17q + r$ con $q \geq 0$ y $17 \leq r \leq 33$. Por la subaditividad de F, obtenemos

$$\frac{F(N)}{N} \leq \frac{qF(17) + F(r)}{N} = \frac{qF(17)}{N} + \frac{F(r)}{N} = \frac{17q}{N}\left(\frac{F(17)}{17}\right) + \frac{r}{N}\left(\frac{F(r)}{r}\right),$$

pero sabemos que $F(r)/r < 1/2$ para todo $r \in [17, 33]$ (ver Tablas 3.1 y 3.2) de modo que

$$\frac{17q}{N}\left(\frac{F(17)}{17}\right) + \frac{r}{N}\left(\frac{F(r)}{r}\right) < \frac{17q}{N}\left(\frac{1}{2}\right) + \frac{r}{N}\left(\frac{1}{2}\right) = \frac{17q + r}{N}\left(\frac{1}{2}\right) = \frac{1}{2}$$

y por lo tanto concluimos que si $N \geq 17$, entonces $F(N)/N < 1/2$.

$\square$

3.3. Prueba del teorema de Roth

Antes de dar la prueba general del teorema de Roth, daremos algunas definiciones y enunciaremos proposiciones que nos serán de utilidad.

Definición 3.18. *Sean A y B dos subconjuntos finitos de $\mathbb{N}$. La densidad de A en B está definida por*

$$\delta(A|B) := \frac{|A \cap B|}{|B|}.$$

A continuación enunciaremos una proposición relacionada con la definición anterior.

Proposición 3.19. *Sean A, B subconjuntos finitos de $\mathbb{N}$ tal que $B = B_1 \cup \cdots \cup B_k$ donde B_i son conjuntos ajenos entre sí, entonces:*

(i)

$$\delta(A|B) = \frac{|B_1|}{|B|}\delta(A|B_1) + \cdots + \frac{|B_k|}{|B|}\delta(A|B_k).$$

(ii) Si $\delta(A|B) \geq D$ entonces existe B_i con $i \in [1, k]$ tal que $\delta(A|B_i) \geq D$.

Demostración. (i)

$$\begin{aligned}\delta(A|B) = \frac{|A\cap B|}{|B|} = \frac{|A\cap (B_1\cup\cdots\cup B_k)|}{|B|} &= \frac{|(A\cap B_1)\cup\cdots\cup (A\cap B_k)|}{|B|}\\ &= \frac{|(A\cap B_1)|+\cdots+|(A\cap B_k)|}{|B|}\\ &= \frac{|(A\cap B_1)|}{|B|}+\cdots+\frac{|(A\cap B_k)|}{|B|}\end{aligned}$$

pero por definición tenemos $|B_i|\delta(A|B_i) = |A\cap B_i|$ para todo $i\in[1,k]$, entonces

$$\delta(A|B) = \frac{|B_1|}{|B|}\delta(A|B_1)+\cdots+\frac{|B_k|}{|B|}\delta(A|B_k)$$

como se quería probar.

(ii) Procedamos por contradicción, es decir, supongamos que $\delta(A|B_i) < D$ para todo $i\in[1,k]$. Entonces

$$\begin{aligned}\delta(A|B) &= \frac{|B_1|}{|B|}\delta(A|B_1)+\cdots+\frac{|B_k|}{|B|}\delta(A|B_k) < \frac{|B_1|}{|B|}D+\cdots+\frac{|B_k|}{|B|}D\\ &= \frac{D}{|B|}(|B_1|+\cdots+|B_k|) = \frac{D}{|B|}(|B|) = D,\end{aligned}$$

por lo tanto, $\delta(A|B) < D$ lo cual es una contradicción.

$\square$

Enseguida daremos otras definiciones.

Definición 3.20. *Sea $A\subset\mathbb{N}$, el complemento de A está definido por*

$$A^c := \{x\in\mathbb{N} : x\notin A\}.$$

Definición 3.21. *Sea $A\subset\mathbb{N}$ un conjunto finito y sea $d\in\mathbb{N}$. Decimos que $a\in A$ y $b\in A$ son equivalentes y escribimos $a\sim b$ si existe una progresión aritmética P tal que*

$$P = \{a, a+d,\cdots, a+sd = b\}\subset A \quad o \quad P = \{b, b+d,\cdots, b+sd = a\}\subset A.$$

La Definición 3.21 cumple con lo siguiente.

Proposición 3.22. *Se tiene que:*

(i) La relación "$\sim$" definida en 3.21 es de equivalencia. Las clases de equivalencia son progresiones maximales.

(ii) El total de clases de esquivalencia es $k = |(A + \{d\}) \setminus A|$.

(iii) El complemento de A se divide en a lo más $k + d$ progresiones, es decir,

$$A^c = B_1 \cup \cdots \cup B_L \quad \textit{con} \quad L \leq k + d.$$

Demostración. Procedamos a demostrar cada inciso.

(i) Tenemos que probar que la relación " $\sim$ " es reflexiva, simétrica y transitiva.

- $a \sim a$.
  No hay nada que hacer.
- Si $a \sim b$ entonces $b \sim a$.
  Esto se sigue directamente de la definición de $\sim$.
- Si $a \sim b$ y $b \sim c$ entonces $a \sim c$.
  Como $a \sim b$ entonces existe $P_1 = \{a, a + d, \cdots, a + s_1 d = b\}$ o $P_1 = \{b, b + d, \cdots, b + s_1 d = a\}$, y como $b \sim c$ entonces existe $P_2 = \{b, b + d, \cdots, b + s_2 d = c\}$ o $P_2 = \{c, c + d, \cdots, c + s_2 d = b\}$. Entonces hay que hacer cuatro casos:
  Si tenemos $P_1 = \{a, a+d, \cdots, a+s_1 d = b\}$ y $P_2 = \{b, b+d, \cdots, b+s_2 d = c\}$. Podemos tomar la progresión aritmética

  $$P = P_1 \cup P_2 = \{a, a + d, \cdots, a + s_1 d = b, b + d, \cdots, b + s_2 d = c\}.$$

  Si tenemos $P_1 = \{a, a + d, \cdots, a + s_1 d = b\}$ y $P_2 = \{c, c + d, \cdots, c + s_2 d = b\}$. Sin pérdida de generalidad supongamos que $a < c$. Notemos que $a + s_1 d = c + s_2 d = b$, entonces $c = a + (s_1 - s_2)d$. Como $a < c$ se tiene que $0 < (s_1 - s_2) < s_1$, en consecuencia $c = a + (s_1 - s_2)d \in P_1$. Por lo tanto podemos tomar la progresión aritmética

  $$P = \{a, a + d, \cdots, a + (s_1 - s_2)d = c\}.$$

  Si tenemos $P_1 = \{b, b+d, \cdots, b+s_1 d = a\}$ y $P_2 = \{b, b+d, \cdots, b+s_2 d = c\}$. Sin pérdida de generalidad supongamos que $a < c$. Por lo tanto $a \in P_2$. Entonces podemos tomar la progresión aritmética

  $$P = \{b + s_1 d = a, \cdots, b + s_2 d = c\}.$$

Si tenemos $P_1 = \{b, b+d, \cdots, b+s_1d = a\}$ y $P_2 = \{c, c+d, \cdots, c+s_2d = b\}$. Podemos tomemos la progresión aritmética

$$P = P_2 \cup P_1 = \{c, c+d, \cdots, c+s_2d = b, b+d, \cdots, b+s_1d = a\}.$$

Por lo tanto en todos los casos se cumple que $a \sim c$.

(ii) Por el Teorema 2.11 al conjunto A lo podemos escribir como $A = P_1 \cup P_2 \cdots \cup P_k$ donde $P_1, \cdots, P_k$ son las distintas clases de equivalencia, es decir, A puede ser escrito como la unión de progresiones aritméticas ajenas de diferencia d.

Sea $P_i := \{x_i, x_i+d, \cdots, x_i+s_id = y_i\} \subset A$ para todo $i \in \{1, \cdots, k\}$, entonces $P_i + \{d\} = \{x_i+d, x_i+2d, \cdots, x_i+(s_i+1)d = y_i+d\}$. Es fácil ver que $A + \{d\} = (P_1 + \{d\}) \cup (P_2 + \{d\}) \cdots \cup (P_k + \{d\})$. Ahora notemos que $x_i + (s_i+1)d = (y_i+d) \in P_i + \{d\}$ no pertenece a A para toda $i \in \{1, \cdots, k\}$, pues de lo contrario tendríamos

$$P_i \subset \{x_i, x_i+d, \cdots, x_i+s_id = y_i, x_i+(s_i+1)d = y_i+d\} \subset A$$

lo cual es una contradicción pues P_i es la progresión aritmética más grande que contiene a x_i. Entonces

$$\begin{aligned}
|(A+\{d\}) \setminus A| &= \left|\left(\bigcup_{i=1}^{k}(P_i+\{d\})\right) \setminus A\right| = \left|\left(\bigcup_{i=1}^{k}(P_i+\{d\})\right) \cap A^c\right| \\
&= \left|\bigcup_{i=1}^{k}((P_i+\{d\}) \cap A^c)\right| = \left|\bigcup_{i=1}^{k}((P_i+\{d\}) \setminus A)\right| \\
&= \left|\bigcup_{i=1}^{k}(y_i+d)\right| = |\{y_1+d, y_2+d, \cdots, y_k+d\}| = k.
\end{aligned}$$

(iii) Primero, como A es finito entonces A^c es infinito.

Tenemos que $A^c = B_1 \cup \cdots \cup B_L$, entonces algunos de estos conjuntos B_i con $i \in \{1, 2, \cdots, L\}$ son infinitos. Sin pérdida de generalidad supongamos que $B_1, B_2, \cdots, B_\ell$ son los conjuntos infinitos y $B_{\ell+1}, B_{\ell+2}, \cdots, B_L$ son los finitos.

Afirmación 1. $\ell = d$.

Como todas las B_i con $i \in \{1, \cdots, \ell\}$ son progresiones aritméticas infinitas, las podemos escribir como sigue

$$\begin{gathered}B_1 = \{x_1, x_1 + d, x_1 + 2d, \cdots\} \subset A^c \\ B_2 = \{x_2, x_2 + d, x_2 + 2d, \cdots\} \subset A^c \\ \vdots \\ B_\ell = \{x_\ell, x_\ell + d, x_\ell + 2d, \cdots\} \subset A^c\end{gathered}$$

donde $x_m \neq x_n$ si $m \neq n$ para todo $m, n \in \{1, 2, \cdots, \ell\}$.

Ahora consideremos los residuos r_i de dividir x_i entre d donde $i \in \{1, 2, \cdots, \ell\}$, entonces

$$x_i \equiv r_i \pmod d \quad \text{donde} \quad 0 \leq r_i < d. \tag{3.4}$$

Aquí tenemos que $r_l \neq r_j$ para toda $l, j \in \{1, \cdots, \ell\}$ con $l \neq j$, pues si suponemos que $r_l = r_j$ entonces tendríamos que $x_l \equiv x_j \pmod d$, por lo que $d \mid (x_l - x_j)$, luego $x_l - x_j = sd$ con $s \in \mathbb{Z}^+$, por lo tanto $x_l = x_j + sd$. Esto último quiere decir que $x_l \in B_j$, y como $x_l \in B_l$ entonces $x_l \in B_l \cap B_j$; lo cual es una contradicción pues todos los B_i con $i \in \{1, 2, \cdots, \ell\}$ son ajenos entre sí. Por lo tanto $r_l \neq r_j$ cuando $l \neq j$.

Ahora veamos que no podemos tener que $\ell < d$ y tampoco $\ell > d$.

Primero supongamos que $\ell < d$.

Como tenemos d clases de congruencia módulo d y $\ell < d$ entonces existe r con $0 \leq r < d$ y tal que $r \neq r_i$ para todo $i \in \{1, \cdots, \ell\}$. Consideremos el conjunto

$$Q = \{a \in \mathbb{Z}^+ : a \equiv r \pmod d\} = \{r + sd : s \in \mathbb{Z}^+\}.$$

Vemos que $Q \cap B_i = \emptyset$ para todo $i \in \{1, \cdots, \ell\}$, pues si suponemos que $z \in Q \cap B_i$ entonces como $z \in B_i$ tendríamos que $z = x_i + sd$ para algún $s \in \mathbb{Z}^+$ y como $z \in Q$, entonces

$$x_i + sd \equiv r \pmod d$$

luego

$$x_i \equiv r \pmod d,$$

por lo tanto

$$r_i \equiv r \pmod d,$$

lo cual es una contradicción.

Ahora sea

$$Q' = \{a' \in Q : a' > b \text{ para todo } b \in B_{\ell+1} \cup B_{\ell+2} \cup \cdots \cup B_L\}.$$

Si $a' \in Q'$ tenemos que $a' \notin B_1 \cup \cdots \cup B_\ell$ y $a' \notin B_{\ell+1} \cup \cdots \cup B_L$, entonces $a' \notin B_1 \cup \cdots \cup B_L = A^c$, luego $a' \in A$, por lo tanto $Q' \subset A$, lo cual es una contradicción pues Q' es infinito y A es finito.

Ahora supongamosmos que $\ell > d$. Ya vimos que $r_l \neq r_j$ con $l \neq j$ para todo $l, j \in \{1, \cdots, \ell\}$ en 3.4, esto quiere decir que hay al menos ℓ distintas clases de equivalencia módulo d, lo cual es una contradicción pues únicamente hay d clases de equivalencia módulo d.

Como ℓ no es menor y tampoco mayor que d, entonces tenemos que $d = \ell$. $\diamond$

Por lo tanto $A^c = B_1 \cup B_2 \cup \cdots \cup B_d \cup B_{d+1} \cup \cdots \cup B_L$, donde $B_1, \cdots, B_d$ son d conjuntos infinitos y $B_{d+1}, \cdots, B_L$ son $L - d$ conjuntos finitos.

Sean

$$\begin{gathered}
B_{d+1} = \{x_{d+1}, x_{d+1} + d, \cdots, x_{d+1} + k_1 d = y_{d+1}\} \subset A^c \\
B_{d+2} = \{x_{d+2}, x_{d+2} + d, \cdots, x_{d+2} + k_2 d = y_{d+2}\} \subset A^c \\
\vdots \\
B_L = \{x_L, x_L + d, \cdots, x_L + k_L d = y_L\} \subset A^c.
\end{gathered}$$

Como vimos en la demostración de la Proposición 3.22 punto (ii), el elemento $y_i + d$ con $i \in \{d+1, \cdots, L\}$ no pertenece a A^c, es decir $(y_i + d) \in A$. Ahora consideremos la clase $[y_i + d] = \{z \in A : z \sim (y_i + d)\}$, sabemos que $[y_i + d]$ es una sucesión maximal que contiene a $y_i + d$, obervemos que esta sucesión comienza en $y_i + d$, pues de no ser así tendríamos que $(y_i + d) - d = y_i \in A$, lo cual no es posible pues $y_i \in A^c$ para todo $i \in \{d+1, \cdots, L\}$. Entonces $[y_i + d]$ es una sucesión en A que comienza en $y_i + d$ para toda $i \in \{d+1, \cdots, L\}$. Vemos que $[y_i + d] \neq [y_j + d]$ para todo $i \neq j$ con $i, j \in \{d+1, \cdots, L\}$ pues de lo contrario tendríamos que $y_i + d = y_j + d$, es decir, $y_i = y_j$ lo cual es falso. En conclusión, tenemos una clase de equivalencia $[y_i + d] \subset A$ para todo $i \in \{d+1, \cdots, L\}$, es decir, tenemos al menos $L - d$ clases de equivalencia en A. Es decir, $L - d \leq k$, por lo que $L \leq k + d$.

$\square$

Por último presentaremos el Lema 3.23. Con este lema ya es fácil demostrar el teorema de Roth.

Lema 3.23. *Sea* $0 < \delta < 1$ *y* $N \in \mathbb{N}$ *tal que* $N \geq 2^{2[\log(4/\delta)]^2}$. *Si* $S \subset [1, N]$ *cumple que* $|S| \geq \delta N$ *y* S *no contiene una progresión aritmética de tres términos, entonces existe una progresión aritmética* $P \subset [1, N]$ *tal que* $|P| \geq (\frac{\delta^2}{160}) \log \log N$ *y* $\delta(S|P) \geq \delta + \delta^2/32$.

Demostración. Dividimos $[1, N]$ en cuatro partes $N_i = [(iM + 1, (i + 1)M]$ para $i = \{0, 1, 2, 3\}$ donde $M = \lceil \frac{N}{4} \rceil$ (quizás con la última parte un poco más pequeña $\lceil \frac{N}{4} \rceil - 3 \leq |N_3| \leq \lceil \frac{N}{4} \rceil$). Tenemos que $[1, N] = N_0 \cup \cdots \cup N_3$.

Si suponemos que $\delta(S|N_i) < \delta/2$ para algún $i \in \{0, 1, 2, 3\}$ entonces existe $j \neq i$ tal que $\delta(S|N_j) > \delta + \frac{\delta^2}{32}$. Par ver esto, hacemos lo siguiente.

Por la Proposición 3.19 inciso (i), tenemos que

$$\delta(S|[1, N]) = \frac{|N_i|}{N} \delta(S|N_i) + \frac{|[1, N] \setminus N_i|}{N} \delta(S|([1, N] \setminus N_i)),$$

pero por hipotésis $\delta(S|[1, N]) \geq \delta$, entonces

$$\frac{|N_i|}{N} \delta(S|N_i) + \frac{|[1, N] \setminus N_i|}{N} \delta(S|([1, N] \setminus N_i)) \geq \delta,$$

luego

$$\frac{|[1, N] \setminus N_i|}{N} \delta(S|([1, N] \setminus N_i)) \geq \delta - \frac{|N_i|}{N} \delta(S|N_i)$$

pero como $\delta(S|N_i) < \delta/2$, entonces

$$\begin{aligned} \frac{|[1, N] \setminus N_i|}{N} \delta(S|([1, N] \setminus N_i)) > & \delta - \frac{|N_i|}{N} \cdot \left(\frac{\delta}{2} \right) \\ & = \delta \cdot \left(1 - \frac{|N_i|}{2N} \right) \\ & = \delta \cdot \left(\frac{2|N| - |N_i|}{2N} \right), \end{aligned}$$

después

$$\begin{aligned}\delta\left(S|([1,N]\setminus N_i)\right) &> \delta\cdot\left(\frac{2N-|N_i|}{2N}\right)\cdot\frac{N}{|[1,N]\setminus N_i|}\\ &= \delta\cdot\left(\frac{2N-|N_i|}{2N}\right)\cdot\frac{N}{N-|N_i|}\\ &= \delta\cdot\left(\frac{2N-|N_i|}{2N-2|N_i|}\right)\\ &= \delta\cdot\left(1+\frac{|N_i|}{2N-2|N_i|}\right)\\ &= \delta+\frac{|N_i|}{2N-2|N_i|}\cdot\delta\end{aligned}$$

pero $|N_i|/(2N-2|N_i|) > \delta/32$, entonces

$$\delta\left(S|([1,N]\setminus N_i)\right) > \delta+\frac{\delta^2}{32}.$$

Luego, por Proposición 3.19 inciso (ii) tenemos que existe N_j con $i \neq j$ tal que $\delta(S|N_j) > \delta + \frac{\delta^2}{32}$, por lo tanto el intervalo N_j es una progresión aritmética tal que $|N_j| = \lceil \frac{N}{4} \rceil > (\frac{\delta^2}{160}) \log\log N$ y $\delta(S|N_j) > \delta + \frac{\delta^2}{32}$.

Ahora supongamos que $\delta(S|N_i) \geq \delta/2$ para toda $i \in \{0,1,2,3\}$. Por conveniencia, tomemos el segmento $N_1 = [M+1, 2M]$ y lo dividimos en aproximadamente $(\log\log N)/2$ intervalos de longitud entre $N/(2\log\log N)$ y $N/(\log\log N)$, luego, por la Proposición 3.19 inciso (ii) hay uno de estos intervalos, digamos I, en el cual S tiene una densidad de almenos $\delta/2$.

Luego como $N \geq 2^{2[\log(4/\delta)]^2}$ por hipótesis y $2\log\log N \leq N^{1/2}$ cuando $N \geq 16$, entonces

$$\begin{aligned}|I| \geq N/(2\log\log N) &\geq N/N^{1/2} = N^{1/2}\\ &\geq \left(2^{2[\log(4/\delta)]^2}\right)^{1/2}\\ &= 2^{[\log(4/\delta)]^2}.\end{aligned}$$

Así, si vemos al conjunto $S \cap I$ como subconjunto de I, podemos aplicar el Corolario 3.9 para encontrar un cubo de Hilbert

$$C_k(x_0, x_1, \cdots, x_k) = C \subset S \cap I$$

de dimensión $k \geq (\log\log|I|)/4$ y con $c_1, \cdots, c_k \leq |I| \leq N/(\log\log N)$. Observemos que debido a que $|I| \geq N^{1/2}$ entonces $k \geq (\log\log|I|)/4 \geq (\log\log N^{1/2})/4$ y además como $(\log\log N^{1/2})/4 \geq (\log\log N)/8$ cuando $N \geq 16$, se sigue que $k \geq (\log\log N)/8$.

Ahora sea C_i el cubo con generadores $c_0, \cdots, c_i$ y hagamos

$$D_i = 2C_i - (S \cap [1, M]) = \{2b - h : b \in C_i, h \in S \cap [1, M]\},$$

como $b \in C_i \subset [M+1, 2M]$ y $h \in S \cap [1, M]$ entonces $M+1 \leq 2b-h \leq 4M$ por lo que $D_i \subset [M+1, 4M] \subset [1, N]$. Observemos que cada D_i es ajeno a S, pues si suponemos que $D_i \cap S \neq \emptyset$ se tiene que existe $2b - h \in D_i \cap S$ con $b \in C_i \subset S, h \in S \cap [1, M]$, luego $\{h, b, 2b-h\} \subset S$ es una progresión aritmética de tres términos con diferencia $b - h$, pero esto es una contradiccón pues S es libre de progresiones de este tipo. Por lo tanto $D_i \cap S = \emptyset$.

También vemos que esta colección de conjuntos forma la secuencia

$$D_0 \subset D_1 \cdots \subset D_k \subset [1, N],$$

entonces $(D_{i+1} \setminus D_i) \cap (D_{j+1} \setminus D_j) = \emptyset$ si $i \neq j$. Entonces hay un i tal que $|D_{i+1} \setminus D_i| \leq N/k$, pues si suponemos que $|D_{i+1} \setminus D_i| > N/k$ para toda i, se tiene que

$$\begin{aligned}\sum_{i=0}^{k-1} |D_{i+1} \setminus D_i| &= |D1 \setminus D_0| + |D2 \setminus D_1| + \cdots + |Dk \setminus D_{k-1}| \\ &\geq \underbrace{N/k + \cdots + N/k}_{k-veces} = k(N/k) = N,\end{aligned}$$

pero por otro lado

$$\begin{aligned}\sum_{i=0}^{k-1} |D_{i+1} \setminus D_i| &= (|D_1| - |D_0|) + (|D_2 - |D_1|) + \cdots + (|D_k| - |D_{k-1}|) \\ &= |D_k| - |D_0| < N,\end{aligned}$$

lo cual es una contradicción. Por lo tanto existe i tal que $|D_{i+1} \setminus D_i| \leq N/k$.

Como $D_{i+1} = D_i \cup (D_i + \{2c_{i+1}\})$, tenemos que $|(D_i + \{2c_{i+1}\}) \setminus D_i| \leq N/k$. Haciendo $B = D_i$ y $d = 2c_{i+1}$ tenemos

$$|(B + \{d\}) \setminus B| \leq \frac{N}{k} \leq \frac{N}{(\log\log N)/8} \leq \frac{8N}{\log\log N}.$$

También tenemos que $d \leq 2N/\log\log N$ y

$$|B| \geq |D_0| \geq |S \cap [1, M]| \geq (\delta/2)M = (\delta/8)N,$$

es decir, $\delta(B|[1,N]) \geq \delta/8$.

Sea $A = [1,N] \setminus B = [1,N] \cap B^c$, por la Proposición 3.22 inciso (ii) y (iii) podemos escribir $B^c = P'_1 \cup \cdots \cup P'_\ell$ donde los P'_i son progresiones aritméticas de diferencia d y $\ell \leq d + |(B + \{d\}) \setminus B|$, entonces $A = [1,N] \cap (P'_1 \cup \cdots \cup P'_\ell) = (P'_1 \cap [1,N]) \cup \cdots \cup (P'_\ell \cap [1,N])$. Sea $P_i = P'_i \cup [1,N]$ para toda $i \in \{1, \cdots, \ell\}$, vemos que todas estas P_i son progresiones arítmeticas de diferencia d. Luego,

$$\ell \leq d + |(B + \{d\}) \setminus B| \leq \frac{2N}{\log\log N} + \frac{8N}{\log\log N} = \frac{10N}{\log\log N}.$$

Así, podemos escribir

$$A = P_1 \cup \cdots \cup P_\ell,$$

con $\ell \leq 10N/\log\log N$, donde cada P_i es una progresión aritmética de diferencia d, y todo P_i disjunto.

Como $\delta((A \cup B)|[1,N]) = \delta([1,N]|[1,N]) = 1$ y por otra parte

$$1 = \delta(A \cup B|[1,N]) = |A \cup B|/N = |A|/N + |B|/N = \delta(A|[1,N]) + \delta(B|[1,N]),$$

entonces

$$\delta(A|[1,N]) = 1 - \delta(B|[1,N]) \leq 1 - (\delta/8).$$

Sea $J \subset \{1, \cdots, \ell\}$ el conjunto de índices i para los cuales $|P_i| \geq (\delta^2/160)\log\log N$. Entonces tenemos

$$\sum_{i \notin J} |P_i| \leq \sum_{i \notin J} \frac{\delta^2 \log\log N}{160} \leq \ell \cdot \frac{\delta^2 \log\log N}{160} \leq \frac{10N}{\log\log N} \cdot \frac{\delta^2 \log\log N}{160} \leq \frac{\delta^2}{16} N.$$

Ahora como $B \cap S = \emptyset$ entonces $S \subset A = [1,N] \setminus B$. Luego,

$$A = P_1 \cup \cdots \cup P_\ell = \left(\bigcup_{i \in J} P_i \right) \cup \left(\bigcup_{i \notin J} P_i \right),$$

sea $A_1 = \bigcup_{i \in J} P_i$ y $A_2 = \bigcup_{i \notin J} P_i$, entonces $A = A_1 \cup A_2$.

Como

$$\begin{aligned} S \subset A_2 \cup S &= (A_1 \cup A_2) \cap (S \cup A_2) \quad \text{pues} \quad S \cup A_2 \subset A_1 \cup A_2 \\ &= (A_1 \cap S) \cup A_2 \end{aligned}$$

Esto muestra que $|(A_1 \cap S) \cup A_2| \geq |S|$, luego como $(A_1 \cap S)$ y A_2 son ajenos, entonces $|(A_1 \cap S) \cup A_2| = |A_1 \cap S| + |A_2|$, por lo que $|A_1 \cap S| \geq |S| - |A_2|$.

Así tenemos

$$\begin{aligned}\delta(S|A_1) = \frac{|S\cap A_1|}{|A_1|} \geq \frac{|S\cap(\bigcup_{i\in J}P_i)|}{|A|} &\geq \frac{|S| - |(\bigcup_{i\notin J}P_i)|}{|A|} \\ &\geq \frac{\delta N - \frac{\delta^2}{16}N}{(1-\frac{\delta}{8})N} \geq (\delta - \frac{\delta^2}{16})(1+\frac{\delta}{8}) \\ &\geq \delta + \frac{\delta^2}{32}.\end{aligned}$$

Esto significa que S tiene densidad $\delta + \frac{\delta^2}{32}$ sobre la unión de las progresiones P_i de longitud almenos $(\delta^2 \log\log N)/160$, así por la Proposición 3.19 inciso (ii) hay un P_i con $i \in J \subset \{1,\cdots,\ell\}$ en el que S tiene densidad al menos $\delta + \delta^2/32$ y $|P_i| \geq (\frac{\delta^2}{160})\log\log N$.

□

Teniendo todas las herramientas necesarias, ahora procederemos a demostrar el teorema de Roth.

Teorema 3.24 (Roth)**.** *Para todo* $0 < \delta < 1$ *existe un mínimo entero* $N_0 = N_0(\delta)$ *tal que si* $N \geq N_0$*, cualquier* $S \subset [1, N]$ *con* $|S| \geq \delta N$ *contiene una* $AP(3)$*.*

Demostración. Sea $0 < \delta < 1$. Ahora consideremos N_0 lo suficientemente grande como para que después de iterar la función $f(N_0) = (\delta^2 \log\log N_0)/160$ al menos $32/\delta^2$ veces, comenzando con N_0, todavía tengamos un valor mayor que $2^{2[\log(4/\delta)]^2}$, para que el Lema 3.23 pueda ser aplicado. Ahora demostremos que para todo $N \geq N_0$, cualquier $S \subset [1, N]$ con $|S| \geq \delta N$ contiene una $AP(3)$.

Procedamos por contradicción, es decir, supongamos que existe $N \geq N_0$ tal que hay un $S \subset [1, N]$ con $|S| \geq \delta N$ que no contiene una progresión aritmética de tres términos.

Como N es lo suficientemente grande como para que en primera instancia se cumpla que $N \geq 2^{2[\log(4/\delta)]^2}$ y además tenemos que $S \subset [1, N]$ con $|S| \geq \delta N$ sin $AP(3)$, entonces por el Lema 3.23 existe una progresión aritmética $P_1 \subset [1, N]$ tal que $|P_1| \geq (\frac{\delta^2}{160})\log\log N$ y $\delta(S|P_1) = \delta_1 \geq \delta + \delta^2/32$.

Ahora sea $S_1 = S \cap P_1$. Ya que las progresiones aritméticas se preservan bajo transformaciones afines, podemos identificar P_1 con $[1, |P_1|]$ y S_1 como subconjunto de $[1, |P_1|]$ con densidad $\delta_1 \geq \delta + \frac{\delta^2}{32}$ en P_1. Debido a que S no contiene progresiones aritméticas, entonces S_1 tampoco, además como N es lo suficientemente grande tenemos que $|P_1| \geq (\frac{\delta^2}{160})\log\log N \geq 2^{2[\log(4/\delta)]^2}$, luego $2^{2[\log(4/\delta)]^2} \geq 2^{2[\log(4/\delta_1)]^2}$ pues $\delta_1 \geq \delta$, por lo tanto $|P_1| \geq 2^{2[\log(4/\delta_1)]^2}$ y como $S_1 \subset [1, |P_1|]$ con $|S_1| = \delta_1|P_1|$ entonces podemos volver a aplicar el Lema 3.23 y obtener otra progresión $P_2 \subset [1, |P_1|]$

con $|P_2| \geq (\frac{\delta_1^2}{160}) \log\log |P_1|$ y $S_2 := S_1 \cap P_2$ con $\delta(S_2|P2) = \delta_2 \geq \delta_1 + \frac{\delta_1^2}{32}$. Repitiendo este proceso, obtenemos una secuencia de progresiones P_k y subconjuntos S_k con densidad δ_k en P_k que satisface

$$|P_k| \geq \frac{\delta_{k-1}^2 \log\log(|P_{k-1}|)}{160} \quad \text{y} \quad \delta_k \geq \delta_{k-1} + \frac{\delta_{k-1}^2}{32}.$$

Afirmación 1. $\delta_k \geq \delta + k\frac{\delta^2}{32}$.

Para mostrar esto, procedamos por inducción. Cuando $k = 1$ ya vimos que $\delta_1 \geq \delta + (\delta^2)/32$. Ahora supongamos que $\delta_k \geq \delta + k\frac{\delta^2}{32}$. Luego

$$\begin{aligned}
\delta_{k+1} &\geq \delta_k + \frac{\delta_k^2}{32} \\
&\geq (\delta + k\frac{\delta^2}{32}) + \frac{\left(\delta + k\frac{\delta^2}{32}\right)^2}{32} \\
&= \delta + \frac{\delta^2}{32} + k\frac{\delta^2}{32} + k\frac{\delta^3}{512} + k^2\frac{\delta^4}{32768} \\
&= \delta + (k+1)\frac{\delta^2}{32} + k\frac{\delta^3}{512} + k^2\frac{\delta^4}{32768} \\
&\geq \delta + (k+1)\frac{\delta^2}{32}.
\end{aligned}$$

Quedando demostrada la afirmación. $\diamond$

Así ,después de $k = 32/\delta^2$ iteraciones, tenemos $\delta_k \geq \delta + 1 > 1$, por lo tanto después de un número finito de iteraciones la densidad ha incrementado a un número mayor que 1, lo cual es una contradicción.

$\square$

A continuación definiremos un tipo de densidad que se le puede asociar a una sucesión natural. Esta nos será de utilidad para poder enunciar el teorema de Roth en su versión infinita. Primero recordemos algunas definiciones de Cálculo.

Sea $A = \{a_n : n \in \mathbb{N}\}$ una sucesión acotada de números reales. Definimos

$$\alpha_n = \text{ínf}\{a_k : k \geq n\}$$

y

$$\beta_n = \sup\{a_k : k \geq n\}$$

entonces a cada sucesión $\{a_n\}$ le podemos asociar las sucesiones $\{\alpha_n\}$ y $\{\beta_n\}$, donde es claro que $\alpha_n \leq a_n \leq \beta_n$ para todo $n \in \mathbb{N}$. Es fácil demostrar (ver [8]) que $\{\alpha_n\}$

es monótona creciente y acotada superiormente, mientras que $\{\beta_n\}$ es monótona decreciente y acotada inferiormente. Por lo tanto ambas sucesiones son convergentes.

Al límite de $\{\alpha_n\}$ se le llama *límite inferior* de la sucesión $\{a_n\}$ y se denota por $\liminf\limits_{n\to\infty} a_n$. Análogamente, al límite de $\{\beta_n\}$ se le llama *límite superior* de $\{a_n\}$ y se denota por $\limsup\limits_{n\to\infty} a_n$. Así:

$$\liminf_{n\to\infty} a_n := \lim_{n\to\infty}(\inf\{a_k : k \geq n\})$$

y

$$\limsup_{n\to\infty} a_n := \lim_{n\to\infty}(\sup\{a_k : k \geq n\}).$$

Se puede demostrar (ver [8]) que

$$\lim_{n\to\infty}(\inf\{a_k : k \geq n\}) = \sup_{n\in\mathbb{N}} \inf_{k\geq n} a_k$$

y

$$\lim_{n\to\infty}(\sup\{a_k : k \geq n\}) = \inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k$$

donde

$$\sup_{n\in\mathbb{N}} \inf_{k\geq n} a_k := \sup\{\inf\{a_k : k \geq n\} : n \geq 0\}$$

e

$$\inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k := \inf\{\sup\{a_k : k \geq n\} : n \geq 0\}.$$

Definición 3.25. *Sea A una sucesión natural, la* densidad superior *de A está dada por*

$$\overline{d}(A) := \limsup_{n\to\infty} \frac{A(n)}{n}.$$

Notemos que la *densidad superior* está bien definida pues $a_n = A(n)/n$ es una sucesión acotada, por lo tanto siempre existe su límite superior.

El teorema de Roth puede ser escrito en la siguiente forma equivalente. De hecho, en algunas fuentes ([9, 10]) el teorema de Roth se encuentra escrito de esta manera.

Teorema 3.26 (Roth versión infinita, 1953)**.** *Sea A una sucesión natural con $\overline{d}(A) > 0$, entonces A contiene una progresión aritmética de tres términos.*

En la presente tesis solo mostraremos que la versión finita del Teorema de Roth (Teorema 3.10) implica la versión infinita (Teorema 3.26).

Proposición 3.27. *El teorema de Roth versión finita implica la versión infinita.*

Demostración. Sea A una sucesión natural tal que $\overline{d}(A) = L > 0$. Debemos mostrar que A contiene una $AP(3)$ suponiendo que el Teorema 3.10 se cumple. Sea $\delta = L/2$, entonces por el Teorema 3.10 existe N_0 tal que para todo $N \geq N_0$, cualquier $S \subset [1, N]$ con $|S| \geq (L/2)N$ contiene una $AP(3)$.

Sabemos que $\overline{d}(A) = L > 0$, es decir, $\lim_{n\to\infty}(\sup\{A(k)/k : k \geq n\}) = L > 0$, por definición de límite tenemos que, dado $\epsilon = L/2 > 0$ existe $N_1 \geq 0$ tal que $-\epsilon + L < \sup\{A(k)/k : k \geq n\} < \epsilon + L$ si $n \geq N_1$. Como $\sup\{A(k)/k : k \geq n\} > L/2$ si $n \geq N_1$, entonces existe $k \geq n$ tal que $A(k)/k > L/2$ si $n \geq N_1$. Es decir, existe $k \geq n$ tal que $|A \cap [1, k]| > (L/2)k$ si $n \geq N_1$.

Sea $n = \max\{N_0, N_1\}$, por lo anterior existe $k \geq \max\{N_0, N_1\}$ tal que $|A \cap [1, k]| > (L/2)k$. Luego como $k \geq N_0$ y $A \cap [1, k] \subset [1, k]$ con $|A \cap [1, k]| > (L/2)k$, entonces $A \cap [1, k]$ contiene una $AP(3)$, y por lo tanto A contiene una $AP(3)$.

$\square$

Capítulo 4

Bases y densidad de Schnirelmann

En el Capítulo 2 presentamos la definición de sucesión natural con cero y definimos la operación suma para este tipo de conjuntos. En el presente capítulo trabajaremos con este tipo de sucesiones, definiremos lo que significa que una sucesión natural con cero sea una base y demostraremos el clásico teorema de Lagrange que afirma que todo número natural puede ser escrito como la suma de cuatro cuadrados. Además, definiremos un tipo de densidad para las sucesiones naturales llamada *densidad de Schnirelmann* y probaremos que si A es suficientemente denso en $\mathbb{N}$ entonces A es una base. El material de este capítulo fue consultado en [3].

A continuación presentaremos un concepto con el que estaremos trabajando constantemente por lo que es importante tenerlo siempre en cuenta.

Definición 4.1. *Sea A una sucesión natural con cero, decimos que A es una* base de orden k *si la suma de k copias de A contiene a todos los números naturales, es decir, si se cumple que*

$$\underbrace{A + A + \cdots + A}_{k} = \mathbb{N}.$$

Ejemplo 4.2. *Consideremos las sucesiones naturales del Ejemplo 2.21.*

(1) $A = \{0, 1, 3, 5, \cdots\}$ *es una base de orden* 2.

Tenemos que demostrar que $\mathbb{N} \subseteq A + A$. Sea $n \in \mathbb{N}$, si $n \in A$ entonces $n = n + 0 \in A + A$. Si $n \notin A$, notemos que entre cualesquiera dos elementos consecutivos de A hay un único número que no está en A. Supongamos que n está entre a_m y a_{m+1}, entonces $n = a_m + 1$. Por lo que tenemos $n = a_m + 1 \in A + A$, es decir $\mathbb{N} \subseteq A + A$.

(2) $A = \{0, 1, 4, 7, \cdots\}$ *es una base de orden* 3.

Mostremos que $\mathbb{N} \subseteq A + A + A$. *Sea* $n \in \mathbb{N}$, *si* $n \in A$ *tenemos que* $n = n+0+0 \in A+A+A$. *Si* $n \notin A$, *notemos que entre cualesquiera dos elementos consecutivos de* A *hay únicamente dos elemento que no están en* A. *Supongamos que* n *está entre* a_m *y* a_{m+1}, *entonces* $n = a_m + 1$ *o* $n = a_m + 2$. *Vemos que* $a_m+1+0 \in A+A+A$ *y* $a_m+1+1 \in A+A+A$, *por lo tanto* $\mathbb{N} \subseteq A+A+A$.

Es importante recalcar que cuando trabajemos con bases siempre utilizaremos sucesiones naturales con el cero. Es fundamental que las sucesiones naturales cuenten con este número pues si suponemos que $A = \{a_n \mid n \in \mathbb{N}\}$ es una base de orden k pero A no contiene al cero, entonces por un lado $a_i > 0$ para todo $i \in \mathbb{N}$ y por el otro $0 = x_1 + x_2 + \cdots + x_k$ donde $x_i \in A$ lo cual es una contradicción.

Podemos observar que si A es una base de orden k entonces se tiene que A también es una base de orden $k+1$. Esto se sigue de que al ser A una base de orden k existen $a_1, a_2, \cdots, a_k \in A$ tal que $a_1 + a_2 + \cdots + a_k = n$ para todo $n \in \mathbb{N}$, lo cual se puede escribir como $a_1 + a_2 + \cdots + a_k + 0 = n$ para todo $n \in \mathbb{N}$ con $a_1, a_2, \cdots, a_k, 0 \in A$.

4.1. El Teorema de Lagrange

Muchas veces es difícil determinar si una sucesión natural es una base de un determinado orden k, para ilustrar esto presentaremos el famoso *Teorema de los Cuatro Cuadrados de Lagrange* [2]. Dicho teorema establece que la sucesión de cuadrados, la sucesión A en el Ejemplo 2.18, es una base de orden cuatro. Es fácil ver que la sucesión de los cuadrados no es una base de orden tres, pues el número 7 no puede ser escrito como la suma de tres cuadrados, es decir, la ecuación $x_1^2 + x_2^2 + x_3^2 = 7$ no tiene solución en los números naturales ya que x_1, x_2, x_3 solo pueden tomar los valores $0, 1, 2$, (pues $3^2 > 7$) pero ninguna de las posibles sumas que podemos formar con estos números es igual a 7.

Teorema 4.3 (Teorema de Lagrange, 1770)**.** *Todo número natural puede ser escrito como la suma de cuatro cuadrados.*

Demostración. Primero observamos que

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{4.1}$$

donde

$$\left.\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2 \\ z_4 &= x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2 \end{aligned}\right\} \tag{4.2}$$

Esto quiere decir que el producto de dos números que son suma de cuatro cuadrados también es suma de cuatro cuadrados. Entonces por lo anterior y teniendo en cuenta el Teorema Fundamental de la Aritmética (Teorema 2.5) , basta probar el teorema para números primos. Como $2 = 1^2 + 1^2 + 0^2 + 0^2$, únicamente tendremos en cuenta los primos impares.

Sea p un primo impar. Consideremos los conjuntos

$$A = \{a^2 : a = 0, 1, \cdots, (p-1)/2\} \quad \text{y} \quad B = \{-1 - b^2 : b = 0, 1, \cdots, (p-1)/2\}.$$

Afirmación: En cada uno de estos conjuntos hay $(p+1)/2$ distintas clases de congruencia módulo p.

En otras palabras, todos los elementos de A (respectivamente, de B) son distintos módulo p. Para demostrar esto procedamos por contradicción, primero tomando en cuenta los elementos del conjunto A. Supongamos que existen a_1^2,$a_2^2 \in A$ tal que

$$a_1^2 \equiv a_2^2 \pmod{p},$$

entonces

$$p \mid (a_1^2 - a_2^2).$$

Como p es primo y además $(a_1^2 - a_2^2) = (a_1 + a_2)(a_1 - a_2)$, tenemos que al menos una de las dos opciones se cumple

$$p \mid (a_1 + a_2) \quad \text{o} \quad p \mid (a_1 - a_2).$$

Pero como $0 < a_1 + a_2 \leq p - 1 < p$ y $0 < |a_1 - a_2| \leq (p-1)/2 < p$ obtenemos una contradicción. Por lo tanto A tiene $(p+1)/2$ distintas clases de congruencia módulo p. Análogamente se demuestra para el conjunto B, supongamos que existen $(-1 - b_1^2), (-1 - b_2^2) \in B$ tales que

$$-1 - b_1^2 \equiv -1 - b_2^2 \pmod{p}$$

entonces

$$-b_1^2 \equiv -b_2^2 \pmod{p}$$

luego

$$b_1^2 \equiv b_2^2 \pmod{p}$$

por lo tanto

$$p \mid (b_1^2 - b_2^2).$$

Como p es primo y además $(b_1^2 - b_2^2) = (b_1 + b_2)(b_1 - b_2)$, tenemos que al menos una de las dos opciones se cumple

$$p \mid (b_1 + b_2) \quad \text{o} \quad p \mid (b_1 - b_2).$$

Pero como $0 < b_1 + b_2 \leq p - 1 < p$ y $0 < |b_1 - b_2| \leq (p-1)/2 < p$ obtenemos una contradicción . Por lo tanto B tiene $(p+1)/2$ distintas clases de congruencia módulo p. $\diamond$

Como sólo hay p distintas clases de congruencia módulo p, por el principio de las casillas existen enteros a,b con $a^2 \in A$ y $(-1-b^2) \in B$ tales que

$$a^2 \equiv -1 - b^2 \pmod{p}$$

entonces

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}$$

después

$$p \mid (a^2 + b^2 + 1)$$

por lo tanto existe $n \in \mathbb{Z}^+$ tal que $np = a^2 + b^2 + 1$. Luego

$$\begin{aligned} p \leq np = a^2 + b^2 + 1^2 + 0^2 &\leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{p}\right)^2 + 1 = 2\left(\frac{p-1}{2}\right)^2 + 1 \\ &= \frac{(p-1)^2}{2} + 1 < \frac{p^2}{2} + 1 < p^2 \end{aligned}$$

por lo que $p \leq np < p^2$, entonces $1 \leq n < p$. De acuerdo a lo anterior se tiene que el conjunto

$$C = \{k \in \mathbb{Z} \ : \ 1 \leq k < p \ \text{ y } \ kp \text{ es la suma de cuatro cuadrados } \} \neq \emptyset.$$

Como C es no vacío y acotado por abajo, tiene un elemento mínimo. Sea m este valor. Entonces existen $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ tal que

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad \text{con} \quad 1 \leq m \leq n < p.$$

Ahora debemos demostrar que $m = 1$.

Procedamos por contradicción, es decir, supongamos que $1 < m < p$. Consideremos el conjunto de los números enteros y tales que $-m/2 < y \leq m/2$, observemos que tenemos m números enteros consecutivos en este intervalo, entonces este conjunto es un sistema completo de residuos módulo m, por lo que para cada x_i existe un único y_i con $-m/2 < y_i \leq m/2$ tal que

$$x_i \equiv y_i \pmod{m}$$

entonces

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}$$

luego

$$m \mid (y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

por lo tanto

$$\text{existe } r \in \mathbb{N} \text{ tal que } mr = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Si $r = 0$ tenemos que $0 = y_1^2 + y_2^2 + y_3^2 + y_4^2$, entonces $y_1 = y_2 = y_3 = y_4 = 0$. Por lo tanto

$$0 \equiv x_i \pmod{m} \text{ con } 1 \leq i \leq 4$$

luego

$$m \mid x_i$$

por lo que

$$m^2 \mid x_i^2$$

entonces

$$m^2 \mid x_1^2 + x_2^2 + x_3^2 + x_3^2 = mp$$

después

$$m^2 \mid mp$$

finalmente

$$m \mid p.$$

Lo cual no es posible pues p es primo y $1 < m < p$. Por lo tanto $r \geq 1$ y

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4(m/2)^2 = m^2.$$

Pero $m = r$ si y sólo si m es par y $y_i = m/2$ para $i = 1, 2, 3, 4$. Entonces tenemos que $x_i \equiv m/2 \pmod{m}$, de donde $m \mid (x_i - m/2)$ y de aquí obtenemos que $m \mid (x_i + m/2)$.

Luego como $m \mid (x_i - m/2)$ y $m \mid (x_i + m/2)$ se tiene que $m^2 \mid (x_i^2 - (m/2)^2)$, por lo tanto

$$x_i^2 \equiv (m/2)^2 \pmod{m^2} \quad \text{para toda} \quad 1 \leq i \leq 4,$$

entonces

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv m^2 \equiv 0 (\text{mod } m^2)$$

luego

$$m^2 \mid (x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp)$$

después

$$m^2 \mid mp$$

por lo tanto

$$m \mid p$$

lo cual es una contradicción. Por lo tanto $1 \leq r < m$.

Por la Ecuación (4.1) tenemos que

$$m^2 rp = (mr)(mp) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Luego por la Ecuación (4.2) tenemos que $z_i \equiv 0 \pmod{m}$ para $1 \leq i \leq 4$, entonces $z_i = mw_i$ para algún $w_i \in \mathbb{Z}$, por lo que

$$m^2 rp = m^2(w_1^2 + w_2^2 + w_3^2 + w_4^2) \quad \text{entonces} \quad rp = w_1^2 + w_2^2 + w_3^2 + w_4^2$$

Lo cual contradice que m era mínimo. Por lo tanto $m = 1$ y el número primo p es la suma de cuatro cuadrados. $\square$

Como vimos en el Teorema 4.3, la sucesión de los cuadrados es una base de orden cuatro, más tarde se demostró que la sucesión de los cubos $\{0^3, 1^3, 2^3, \cdots\}$ es una base de orden nueve. Estos hallazgos llevaron a los matemáticos a conjeturar, que para todo número natural n, la sucesión $\{0, 1^n, 2^n, 3^n, \cdots\}$ es una base (donde el orden depende de n). Esta conjetura fue propuesta por el matemático Edward Waring (1736-1798) en el siglo XVIII. El problema resultó ser muy difícil de demostrar, sin embargo en el año 1909 la hipótesis de Waring fue demostrada por David Hilbert (1862-1943) usando herramientas analíticas muy complicadas. Quince años después, nuevas pruebas del teorema de Hilbert fueron publicadas por Godfrey Harold Hardy (1877-1947) y John Edensor Littlewood (1885-1977) en Inglaterra y por Iván Matvéievich Vinográdov (1891-1983) en la URSS. Estas pruebas fueron de nuevo analíticas, pero se diferenciaban de la prueba de Hilbert en que el método de estas era claro y sus conceptos eran simples. De hecho, debido a esto, ambos métodos se convirtieron en poderosas fuentes de nuevos teoremas aritméticos.

En los años posteriores se siguió con la búsqueda de una prueba que sólo hiciera uso de la aritmética elemental y fue hasta el año 1942 cuando el estudiante Soviético Yuri Vladimirovich Linnik (1915-1972) logró encontrarla.

4.2. Densidad de Schnirelmann

Dada una sucesión natural $A = \{a_n : n \in \mathbb{N}\}$ denotamos por $A(n)$ a la cantidad de números en la sucesión que no sobrepasan al entero n (sin contar al cero, en caso de ser A sucesión natural con cero). Formalmente, para $n \in \mathbb{Z}^+$, definimos

$$A(n) := |A \cap [1, n]|.$$

Observemos que, para todo $n \in \mathbb{Z}^+$, $0 \leq A(n) \leq n$, por lo que

$$0 \leq \frac{A(n)}{n} \leq 1. \tag{4.3}$$

Ahora procederemos a dar la definición de densidad de Schnirelmann.

Definición 4.4. *Sea A una sucesión natural. La* densidad de Schnirelmann *de A está dada por*

$$d(A) := \text{ínf}\left\{\frac{A(n)}{n} : n \in \mathbb{Z}^+\right\}.$$

Observemos que esta definición tiene sentido para toda sucesión natural A, pues en consecuencia de (4.3), el conjunto $\{A(n)/n : n \in \mathbb{Z}^+\}$ está acotado inferiormente, y por lo tanto siempre existe su ínfimo.

Para familiarizarnos con la Definición 4.4 demostremos el siguiente resultado.

Proposición 4.5. *Sea $A = \{a_n : n \in \mathbb{N}\}$ una sucesión natural con cero.*

(1) *Si $a_1 > 1$ (es decir, la sucesión A no contiene al número 1) entonces $d(A) = 0$.*

(2) *La sucesión A es el conjunto $\mathbb{N}$ si y solamente si $d(A) = 1$.*

(3) *Si $a_1 = 1$ y $d(A) = 0$, entonces para todo $\epsilon > 0$ existe un número m suficientemente grande tal que $A(m) < \epsilon m$.*

Demostración. Sea A una sucesión natural con cero. Procedamos a probar cada uno de los incisos.

(1) Por (4.3), sabemos que $A(n)/n \geq 0$ para todo $n \in \mathbb{Z}^+$. Por otra parte, $a_1 > 1$ implica $A(1) = 0$, y entonces $A(1)/1 = 0$. Luego, la sucesión de números reales $\{A(n)/n \, : \, n \in \mathbb{Z}^+\}$ alcanza su cota inferior 0 , por lo tanto

$$d(A) = \inf\{A(n)/n : n \in \ \mathbb{Z}^+\} = 0.$$

(2) Supongamos primero que $A = \mathbb{N}$. Entonces, $A(n) = n$ para todo $n \in \mathbb{Z}^+$. Por lo tanto $A(n)/n = 1$ para todo $n \in \mathbb{Z}^+$. Luego, $d(A) = \inf\{A(n)/n : n \in \mathbb{Z}^+\} = 1$.

Supongamos ahora que A es una sucesión natural con cero tal que $d(A) = 1$. Entonces, por definición, se cumple que $1 \leq A(n)/n$ para todo $n \in \mathbb{Z}^+$. Por otro lado, de (4.3) sabemos que $A(n)/n \leq 1$ para todo $n \in \mathbb{Z}^+$. Entonces, $A(n) = n$ para todo $n \in \mathbb{Z}^+$; es decir, para cada $n \in \mathbb{Z}^+$, hay n elementos en A (sin contar al cero) que son mayores o iguales que 1 y menores o iguales que n. La única forma de que esto sea posible es que $a_1 = 1, a_2 = 2, \cdots, a_n = n$ para todo $n \in \mathbb{Z}^+$. De lo cual concluimos que $A = \{0, 1, 2, 3, \cdots\} = \mathbb{N}$.

(3) Observemos primero que como A contiene al 1, entonces $0 < A(n)$ para todo $n \in \mathbb{Z}^+$ por lo que $0 < A(n)/n$ para todo $n \in \mathbb{Z}^+$. Sea $\epsilon > 0$, como $\inf\{A(n)/n : n \in \mathbb{Z}^+\} = 0$ se tiene que ϵ no es cota inferior de $S = \{A(n)/n : n \in \mathbb{Z}^+\}$. Esto quiere decir que existe $s_\epsilon \in S$ tal que $s_\epsilon < \epsilon$. Luego, existe $m \in \mathbb{Z}^+$ tal que $s_\epsilon = \frac{A(m)}{m}$. Entonces, $0 < \frac{A(m)}{m} < \epsilon$ y por lo tanto $A(m) < m\epsilon$.

□

Ahora, veamos algunos ejemplos.

Proposición 4.6. *Sea A una sucesión natural.*

(1) *Si A es la sucesión de los cuadrados perfectos entonces $d(A) = 0$.*

(2) *Si A es una progresión aritmética con término inicial $a_1 = 1$ y diferencia r entonces $d(A) = 1/r$.*

(3) *Si A es una progresión geométrica tal que $a_0 = 0$ y $a_n = ar^{n-1}$ con $n \in \mathbb{Z}^+$ entonces $d(A) = 0$.*

Demostración. Procedamos a probar cada uno de los incisos.

(1) Tenemos que $a_n = n^2$ para todo $n \in \mathbb{N}$, es decir

$$a_0 = 0, \ a_1 = 1, \ a_2 = 4, \ a_3 = 9, \cdots, \ a_k = k^2, \ \cdots$$

Luego

$$A(1) = 1,\ A(4) = 2,\ A(9) = 3,\ \cdots,\ A(k^2) = k,\ \cdots$$

Observemos que $\{A(k^2)/k^2 : k \in \mathbb{Z}^+\}$ es una subsucesión de $\{A(n)/n : n \in \mathbb{Z}^+\}$ que cumple

$$\lim_{k\to\infty} \frac{A(k^2)}{k^2} = \lim_{k\to\infty} \frac{k}{k^2} = \lim_{k\to\infty} \frac{1}{k} = 0,$$

y por lo tanto $\inf\{A(n)/n : n \in \mathbb{N}\} = 0$.

(2) Tenemos que

$$a_1 = 1,\ a_2 = 1 + r,\ a_3 = 1 + 2r,\ a_4 = 1 + 3r,\ \cdots,\ a_{k+1} = 1 + kr,\ \cdots$$

Luego

$$\begin{gathered} A(1) = 1,\ A(2) = 1,\ \cdots,\ A(r) = 1 \\ A(1+r) = 2,\ A(2+r) = 2,\ \cdots,\ A(2r) = 2 \\ A(1+2r) = 3,\ A(2+2r) = 3,\ \cdots,\ A(3r) = 3 \\ \vdots \\ A(1+(k-1)r) = k,\ A(2+(k-1)r) = k,\ \cdots,\ A(kr) = k \\ \vdots \end{gathered}$$

Como

$$\frac{k}{1+(k-1)r} \geq \frac{k}{2+(k-1)r} \geq \cdots \geq \frac{k}{kr} = \frac{1}{r} \quad \text{para toda } k \in \mathbb{Z}^+,$$

entonces

$$\frac{A(1+(k-1)r)}{1+(k-1)r} \geq \frac{A(2+(k-1)r}{2+(k-1)r} \geq ... \geq \frac{A(kr)}{kr} = \frac{1}{r} \quad \text{para toda } k \in \mathbb{Z}^+.$$

Por lo tanto, $\frac{A(n)}{n} \geq \frac{1}{r}$ para toda $n \in \mathbb{Z}^+$. En otras palabras, $1/r$ es cota inferior de la sucesión $\{A(n)/n : n \in \mathbb{Z}^+\}$. Como, además dicha cota inferior se alcanza, entonces $d(A) = 1/r$.

(3) Tenemos que, para todo $n \in \mathbb{Z}^+$, $a_n = ar^{n-1}$ donde $a, r \in \mathbb{Z}^+$ con $r > 1$. Observemos que $a_1 = a$. Si $a > 1$, por la Proposición 4.5 punto (1) se tiene que $d(A) = 0$. Asumamos entonces que $a = 1$, luego

$$a_1 = 1,\ a_2 = r,\ a_3 = r^2,\ \cdots,\ a_k = r^{k-1},\ \cdots$$

y

$$A(1) = 1,\ A(r) = 2,\ A(r^2) = 3,\ \cdots,\ A(r^{k-1}) = k,\ \cdots$$

Es decir

$$A(a_k) = A(r^{k-1}) = k \quad \text{para todo } k \in \mathbb{Z}^+.$$

Observemos que $\{A(r^{k-1})/r^{k-1} : k \in \mathbb{Z}^+\}$ es una subsucesión de $\{A(n)/n : n \in \mathbb{Z}^+\}$ que cumple

$$\lim_{k\to\infty} \frac{A(r^{k-1})}{r^{k-1}} = \lim_{k\to\infty} \frac{k}{r^{k-1}} = 0, \quad \text{pues}\, r > 1.$$

Por lo tanto $\inf\{A(n)/n : n \in \mathbb{N}\} = 0$.

□

4.3. Lema de Schnirelmann

Una vez familiarizados con el concepto de densidad de Schnirelmann, procederemos a presentar el lema de Schnirelmann.

Lema 4.7 (Schnirelmann)**.** *Sean A y B dos sucesiones naturales ambas con el cero, entonces se cumple que*

$$d(A + B) \geq d(A) + d(B) - d(A)d(B). \tag{4.4}$$

Demostración. Sean $d(A) = \alpha$, $d(B) = \beta$, $A + B = C$ y $d(C) = \gamma$. Por definición, el segmento $[1, n]$ contiene $A(n)$ elementos de la sucesión A, y cada uno de ellos también está en la sucesión C (puesto que $0 \in B$). Sean a_k y a_{k+1} dos elementos consecutivos de A. Observemos que entre a_k y a_{k+1} hay $l := a_{k+1} - a_k - 1$ números que no pertenecen a A. Sean

$$a_k + 1, a_k + 2, \cdots, a_k + l = a_{k+1} - 1$$

estos números. Notemos que algunos de estos términos podrían estár en C. Exactamente, los números de la forma $a_k + r$ donde $r \in B$ y $1 \leq r \leq a_{k+1} - a_k - 1 = l$. La cantidad de estos números es igual a la cantidad de números en B que pertenecen al segmento $[1, l]$, es decir, $B(l)$. De lo anterior, concluimos que la cantidad de números de la secuencia C que no sobrepasan a n satisface

$$C(n) \geq A(n) + \sum B(l) \tag{4.5}$$

donde la suma se realiza sobre las longitudes de cada segmento en $[1, n]$ sin elementos de A (incluyendo, si es el caso, el segmento entre 1 y a_1, y el segmento entre $A_{A(n)}$ y n). Por definición, sabemos que $B(l) \geq \beta l$, para todo $l \in \mathbb{Z}^+$, luego (4.5) es equivalente a

$$C(n) \geq A(n) + \sum \beta l = A(n) + \beta \sum l, \tag{4.6}$$

donde $\sum l$ es la suma de las longitudes de todos los intervalos sin elementos de A en el segmento $[1, n]$, es decir $\sum l = n - A(n)$. Luego (4.6) se puede reescribir como

$$C(n) \geq A(n) + \beta(n - A(n)) = A(n) - \beta A(n) + \beta n,$$

y como $A(n) \geq \alpha n$, tenemos que

$$C(n) \geq \alpha n - \beta\alpha n + \beta n = \alpha n(1 - \beta) + \beta n. \tag{4.7}$$

Dividiendo entre n ambos lados de (4.7) obtenemos

$$C(n)/n \geq \alpha(1 - \beta) + \beta = \alpha + \beta - \alpha\beta.$$

como n es un número natural arbitrario se concluye que

$$\gamma \geq \alpha + \beta - \alpha\beta$$

lo cual es equivalente a (4.4). □

La Desigualdad (4.4) puede alcanzarse o no. Ilustremos lo anterior con ejemplos.

Ejemplo 4.8.

- *Sean A y B las sucesiones definidas en el Ejemplo 2.21. Sabemos que $A + B = \mathbb{N}$. Entonces, como $(A + B) = \mathbb{N}$, por definición y la Proposición 4.5 punto* (2) *tenemos que $d(A + B) = 1$. Sabemos además, por la Proposición 4.6 punto* (3) *que $d(A) = 1/2$ y $d(B) = 1/3$, entonces*

  $$d(A) + d(B) - d(A)d(B) = (1/2) + (1/3) - (1/2)(1/3) = 2/3,$$

  por lo que en este caso tenemos desigualdad estricta:

  $$1 = d(A + B) > d(A) + d(B) - d(A)d(B) = 2/3.$$

- *Sea $A = \mathbb{N}$ y B una sucesión arbitraria, se tiene que $A + B = \mathbb{N}$, luego $d(A + B) = 1$ por el segundo punto de la Proposición 4.5, Por otro lado*

  $$d(A) + d(B) - d(A)d(B) = 1 + d(B) - d(B) = 1.$$

  Por lo tanto

  $$d(A + B) = d(A) + d(B) - d(A)d(B).$$

El lema de Schnirelmann se puede generalizar usando inducción matemática. Primero observamos que podemos reescribir la Ecuación (4.4) como

$$1 - d(A+B) \leq (1-d(A))(1-d(B)). \tag{4.8}$$

De esta forma podemos hacer una generalización para una cantidad arbitraria de sumandos.

Lema 4.9 (Schnirelmann generalizado)**.** *Sean $A_1, A_2, ..., A_k$ sucesiones naturales todas con el cero, entonces se cumple que*

$$1 - d(A_1 + A_2 + ... + A_k) \leq \prod_{i=1}^{k}(1-d(A_i)) \tag{4.9}$$

Demostración. Procederemos por inducción sobre k.

Si $k = 2$, por (4.8) tenemos que

$$1 - d(A_1 + A_2) \leq (1-d(A_1))(1-d(A_2)).$$

Ahora supongamos que se cumple para $k = n$, es decir

$$1 - d(A_1 + A_2 + ... + A_n) \leq \prod_{i=1}^{n}(1-d(A_i)).$$

Sea $C = A_1 + A_2 + ... + A_n$, entonces

$$\begin{aligned}
1 - d(A_1 + A_2 + ... + A_{n+1}) &= 1 - d(C + A_{n+1}) \\
&\leq (1-d(C))(1-d(A_{n+1})) \\
&= (1-d(A_1 + A_2 + ... + A_n))(1-d(A_{n+1})) \\
&\leq \left(\prod_{i=1}^{n}(1-d(A_i))\right)(1-d(A_{n+1})) \\
&= \prod_{i=1}^{n+1}(1-d(A_i))
\end{aligned}$$

por lo tanto

$$1 - d(A_1 + A_2 + ... + A_{n+1}) \leq \prod_{i=1}^{n+1}(1-d(A_i)).$$

□

Por último, notemos que la Desigualdad (4.9) se puede escribir de la siguiente forma

$$d(A_1 + A_2 + ... + A_k) \geq 1 - \prod_{i=1}^{k}(1 - d(A_i)). \tag{4.10}$$

En el Otoño de 1931, después de regresar de un viaje al extranjero, Lev Genrikhovich Schnirelmann (1905-1938) le contó a Aleksandr Yakovlevich Khinchin (1894-1959) la conversación que tuvo con Edmund Georg Hermann Landau (1877-1938) en Göttingen, y le contó entre otras cosas, el siguiente hecho: En todos los ejemplos que ellos habían propuesto, era posible reemplazar la desigualdad

$$d(A + B) \geq d(A) + d(B) - d(A)d(B) \tag{4.11}$$

(la cual deducimos en 4.7) por la desigualdad

$$d(A + B) \geq d(A) + d(B). \tag{4.12}$$

Es decir, la densidad de la suma siempre es mayor o igual que la suma de las densidades (con la suposición que $d(A) + d(B) \leq 1$).

Ellos conjeturaron que la Ecuación 4.12 debía ser verdadera, pero sus primeros intentos de probar esta conjetura fueron insuficientes. Pronto se dieron cuenta que de ser cierta, el camino de su prueba sería bastante difícil. En este punto, supongamos que se cumple la Ecuación 4.12, entonces esta ley puede ser generalizada inmediatamente por inducción para un número arbitrario de sumandos, es decir, bajo la suposición que

$$\sum_{i=1}^{k} d(A_i) \leq 1$$

tenemos

$$(\sum_{i=1}^{k} A_i) \geq \sum_{i=1}^{k} d(A_i). \tag{4.13}$$

Este problema atrajo la atención de estudiantes, debido a la simplicidad y elegancia de la Desigualdad 4.12 y al contraste entre su apariencia elemental del problema y la dificultad que aparentó después de los primeros intentos. En 1923, después de muchos meses de trabajo, A. Y. Khinchin logró probar la Ecuación 4.12 para el caso más importante, $d(A) = d(B)$ (este caso es importante porque en la mayoría de problemas concretos todos los sumandos son el mismo). Al mismo tiempo, él también probó la desigualdad general 4.13 bajo la suposición que $d(A_1) = d(A_2) = \cdots = d(A_k)$. Su método para la demostración fue completamente elemental, pero muy complicado, además sus ideas no podían ser usadas para dar la demostración general.

Mientras tanto la publicación de su trabajo atrajo la atención de un gran círculo de estudiantes de todos los países. Muchos resultados insignificantes fueron obtenidos, y una literatura completa surgió debido a esto. Algunos matemáticos llevaron el problema del dominio de los naturales a otros campos. En breve, el problema llegó a ser fascinante e incluso sociedades matemáticas ofrecieron dinero por la solución. No fue hasta 1942 que el joven matemático americano Henry Berthold Mann (1905-2000) resolvió el problema: él encontró una prueba completa de la Ecuación 4.12 (y por lo tanto también de 4.13). Su método fue completamente elemental y estaba relacionado con el trabajo de A. Y. Khinchin, aunque estaba basado en una idea completamente diferente. La prueba es bastante larga y muy complicada. Un año después, en 1943, Emil Artin (1898-1962) y Peter Scherk (1910-1985) publicaron una nueva prueba del mismo teorema. Esta prueba fue considerablemente más corta y clara y aún seguía siendo elemental.

4.4. Consecuencia del lema de Schnirelmann

Con el uso del Lema 4.9 podemos demostrar el siguiente teorema.

Teorema 4.10. *Sea A una sucesión natural con cero. Si $d(A) > 0$ entonces A es una base.*

Para demostrar este resultado necesitamos el siguiente lema.

Lema 4.11. *Sea $n \in \mathbb{Z}^+$, si $A(n) + B(n) > n - 1$ entonces $n \in (A + B)$.*

Demostración. Si n está en A o en B se tiene que n también está en $A + B$.

Ahora supongamos que n no está en A ni en B. Como n no está en A ni en B, se tiene que $A(n) = A(n-1)$ y $B(n) = B(n-1)$, luego por hipótesis tenemos que

$$A(n-1) + B(n-1) = A(n) + B(n) > n - 1.$$

Sean $a_1, a_2, \cdots, a_r$ y $b_1, b_2, \cdots, b_s$ los términos de A y B que están en el segmento $[1, n-1]$ respectivamente, entonces $r = A(n-1)$ y $s = B(n-1)$.

Como $1 \leq b_i \leq n - 1$ con $1 \leq i \leq s$, entonces si multiplicamos por -1 esta desigualdad tenemos

$$1 - n \leq -b_i \leq -1$$

luego, si sumamos n nos queda

$$1 \leq n - b_i \leq n - 1$$

por lo tanto los números

$$a_1, a_2, \cdots, a_r$$
$$n - b_1, n - b_2, \cdots, n - b_s$$

están en el segmento $[1, n-1]$.

Luego, se tiene que al menos un número de la fila de arriba es igual a uno de la fila de abajo, pues de no ser así tendríamos que todos estos números deben de ser distintos y como están en el segmento $[1, n-1]$ se tiene que $s + r \leq n - 1$, pero esto no es posible pues $r + s > n - 1$. Entonces $a_i = n - b_k$, por lo tanto $n = a_i + b_k$, es decir, n pertenece a $A + B$. □

Ahora regresemos a la demostración del Teorema 4.10 .

Demostración del Teorema 4.10: Sea A una sucesión natural con cero tal que $d(A) = \alpha > 0$. Por simplicidad escribiremos A_k en lugar de la suma de k sucesiones, donde cada sucesión es A.

Tenemos por (4.10) que

$$d(A_k) \geq 1 - (1 - \alpha)^k.$$

Luego, como $0 < \alpha \leq 1$ se tiene que $0 \leq 1 - \alpha < 1$, entonces

$$\lim_{k \to \infty} (1 - \alpha)^k = 0.$$

Por lo tanto, para un k suficientemente grande tenemos que $(1 - \alpha)^k < 1/2$, entonces

$$d(A_k) \geq 1 - (1 - \alpha)^k > 1/2$$

y como

$$A_k(n)/n \geq d(A_k) \text{ para todo } n \in \mathbb{Z}^+$$

se tiene que

$$A_k(n)/n > 1/2$$

por lo tanto

$$A_k(n) > n/2 > (n - 1)/2.$$

En consecuencia $A_k(n) + A_k(n) > n - 1$. Aplicando el Lema 4.11 se concluye que n pertenece a $A_k + A_k = A_{2k}$ para todo $n \in \mathbb{Z}^+$. Por lo tanto A es una base de orden $2k$.

□

En la prueba de este teorema podemos inferir que si $d(A) = \alpha > 0$, entonces A es base de orden $2k$ donde k es un entero positivo que cumple $(1-\alpha)^k < 1/2$. Ahora nos preguntamos: para el k más pequeño que cumple la condición anterior, ¿$2k$ es el menor número tal que $A_{2k} = \mathbb{N}$?

Para responder esta pregunta veamos el siguiente ejemplo:

Consideremos $A = \{0, 1, 3, 5, 7, 9, \cdots\}$. Por la Proposición 4.6 punto (3) sabemos que $d(A) = 1/2$, luego tenemos que el entero k más pequeño tal que

$$(1 - 1/2)^k = (1/2)^k < 1/2$$

es $k = 2$, por lo tanto A es una base de orden 4, es decir $A + A + A + A = \mathbb{N}$. Pero por el Ejemplo 4.2 tenemos que A es una base de orden 2. Por lo tanto la respuesta a nuestra pregunta es no.

El Teorema 4.10 llevó a una serie de importantes aplicaciones en los trabajos de L. G. Schniremann. Por ejemplo, él fue el primero en demostrar que la sucesión P formada por la unidad y todos los números primos es una base. Es cierto que la secuencia P tiene densidad cero, como Euler lo había mostrado, así que el Teorema 4.10 no puede ser aplicado directamente . Pero Schnirelmann fue capaz de probar que $P + P$ tiene densidad positiva. Ya que $P + P$ forma una base, se sigue que P también. De esto se sigue que todo número natural, a excepción del número uno, puede ser escrito como la suma de k números primos donde k es lo suficientemente grande.

Capítulo 5

Trabajo a futuro

Aunque parezca que el material de los Capítulos 3 y 4 no tiene conexión, en el presente capítulo encontraremos cierto vínculo. Primero, nos preguntamos ¿cuál es la relación que existe entre la densidad superior (Definición 3.25) y la densidad de Schnirelmann (Definición 4.4)? Claramente, dichos parámetros son diferentes, sin embargo, nuestro interés es acerca de las implicaciones que tiene un conjunto con densidad positiva. En este sentido, resulta que un conjunto de números enteros positivos que contiene a la unidad, tiene densidad superior positiva si y sólo si tiene densidad de Schnirelmann positiva, como se muestra a continuación.

Proposición 5.1. *Sea A una sucesión natural con $1 \in A$. Entonces $d(A) > 0$ si y solo si $\overline{d}(A) > 0$.*

Demostración. La proposición es equivalente a demostrar que $d(A) = 0$ si y solo si $\overline{d}(A) = 0$.

Primero supongamos que $d(A) = 0$. Como $1 \in A$, por la Proposición 4.5 inciso (3) se tiene que

$$\lim_{n\to\infty} \frac{A(n)}{n} = 0$$

luego como

$$\lim_{n\to\infty} \frac{A(n)}{n} = \limsup \frac{A(n)}{n}$$

entonces

$$\overline{d}(A) = 0.$$

Ahora supongamos que $\overline{d}(A) = 0$. Como $\{\frac{A(k)}{k} : k \geq n\} \subset \{\frac{A(i)}{i} : i \in \mathbb{N}\}$ para todo $n \in \mathbb{N}$, entonces $\inf\{\frac{A(i)}{i} : i \in \mathbb{N}\} \leq \inf\{\frac{A(k)}{k} : k \geq n\} \leq \sup\{\frac{A(k)}{k} : k \geq n\}$ para todo $n \in \mathbb{N}$, por lo que ínf $\left\{\frac{A(i)}{i} : i \in \mathbb{N}\right\} \leq \sup\limits_{k \geq n} \frac{A(k)}{k}$ para todo $n \in \mathbb{N}$, luego

$$\text{ínf}\left\{\frac{A(i)}{i} : i \in \mathbb{N}\right\} \leq \inf_{n \in \mathbb{N}} \sup_{k \geq n} \frac{A(k)}{k},$$

es decir $d(A) \leq \overline{d}(A) = 0$. Por lo tanto $d(A) = 0$. □

Notemos que en esta proposición es necesario que la sucesión natural A contenga al 1, pues por ejemplo, si damos la sucesión $A = \{0, 2, 3, 4, 5, \cdots\}$ entonces $d(A) = 0$ pero $\overline{d}(A) = 1$.

De acuerdo a la Proposición 5.1 y la Observación 2.2 podemos escribir el Teorema de Roth versión infinita 3.26 de la siguiente forma.

Teorema 5.2 (Roth). *Sea A una sucesión natural con $1 \in A$. Si $d(A) > 0$ entonces A contiene una solución de la ecuación $x + y = 2z$ (con $x \neq y$).*

En el Capítulo 4 vimos el Teorema 4.10, el cual nos dice que si A tiene densidad positiva entonces A es una base de cierto orden $k \in \mathbb{Z}^+$. Que A sea una base de orden $k \in \mathbb{Z}^+$ quiere decir que

$$\underbrace{A + \cdots + A}_{k-\text{veces}} = \mathbb{N},$$

esto a su vez significa que la ecuación $x_1 + \cdots + x_k = n$ tiene solución en A para todo $n \in \mathbb{N}$. Entonces el Teorema 4.10 lo podemos escribir como sigue.

Teorema 5.3. *Sea A una sucesión natural con cero tal que $d(A) > 0$, entonces existe $k \in \mathbb{Z}^+$ tal que A contiene una solución de la ecuación*

$$x_1 + \cdots + x_k = n \quad \textit{para todo} \quad n \in \mathbb{N}.$$

Notemos que tanto el Teorema 5.2 como el Teorema 5.3 son resultados de tipo densidad, es decir, nos dicen que si A tiene densidad positiva entonces A contiene una solución de cierta ecuación, o cierto conjunto de ecuaciones. En el contexto de la teoría de Ramsey, los trabajos de Richard Rado (1906-1989), quien fue un estudiante de Schur, se plantean precisamente la versión coloraciones de este tipo de problemas (ver [4]).

A lo largo de este trabajo vimos que ciertos resultados de densidad tienen su análogo en versión coloraciones y viceversa, por ejemplo, los Lemas 3.5 y 3.8 concernientes a los d-cubos afines, así como el Teorema de Roth 5.2 implica el Teorema de van der Waerden 2.33 (en el caso particular $\ell = 3$). Debido a estos hechos, es natural preguntarse si cada resultado tipo densidad tiene su análogo en versión coloraciones. Además, dado un resultado de coloraciones, podemos preguntarnos por su versión heterocromática, es decir, estudiar la existencia de estructuras heterocromáticas en toda coloración con cierta densidad en las clases cromáticas (ver [4]).

Por lo tanto, en el proyecto de investigación nos planteamos las siguientes preguntas:

(1) ¿Cuál es la versión de coloración del Teorema 5.3?

(2) ¿Tiene sentido pensar en *bases heterocromáticas*?

(3) ¿Será cierto que existe una versión tipo densidad del teorema de Rado?

Bibliografía

[1] Frank de Zeeuw. *A Course in Arithmetic Ramsey Theory*. 2017, https://pdfs.semanticscholar.org/31ee/80f864362c49382757ce0467afee82dba6ab.pdf

[2] Melvyn Nathanson. *Number Theory: the Classical Bases*. Springer, New York, 1996.

[3] Aleksandr Khinchin. *Three Pearls of Number Theory*. Graylock Press, New York, 1956.

[4] Bruce Landman & Aaron Robertson. *Ramsey Theory on the Integers*. Board, United States of America, 2014.

[5] Ivan Niven & Herbert Zuckerman. *Introducción a la Teoría de los Números*. Limusa, México, 1976.

[6] Mark Villarino, Bill Gasarch & Kenneth Regan. *Hilbert's Proof of His Irreducibility Theorem*. arXiv:1611.06303, 2016.

[7] Endre Szemerédi. *On Sets of Integers Containing no Four Elements in Arithmetic Progression*. Acta Mathematica Academiae Scientiarum Hungarica 20, 89-104, 1969.

[8] Michael Spivak. *Cálculo infinitesimal*. Reverté, México, 1996.

[9] Ronald Graham, Bruce Rothschild & Joel Spencer. *Ramsey Theory*. Wiley, New York, 1990.

[10] Ramdinmawia. *Roth's Theorem on Arithmetic Progressions*. 2011, http://math.univ-lille1.fr/bhowmik/enseignement/Mem_master/memoire_ramdin.pdf