Universidad Autónoma de Querétaro

Facultad de Ingeniería

Licenciatura en Matemáticas Aplicadas

Sobre resultados de tipo anti-Ramsey en grupos cíclicos de orden primo p para la ecuación de Schur

TESIS

Que como parte de los requisitos para obtener el grado de

Licenciado en Matemáticas Aplicadas

Presenta:

José David Suárez González

Directora:

Dra. Amanda Montejano Cantoral

Sinodales:

Dra. Amanda Montejano Cantoral
Directora

M. C. Victor Antonio Aguilar Arteaga
Secretario

Mat. Ilán Abraham Gonldfeder Ortiz
Vocal

M. C. Mario Alejandro Huicochea Mason
Vocal

Agradecimientos

Esta tesis representa un parteaguas entre una etapa muy enriquecedora y el camino que el tiempo obliga. En toda la experiencia como universitario y la conclusión del trabajo de tesis, ha habido personas que merecen las gracias porque sin su valiosa aportación no hubiera sido posible este trabajo y hay quienes también las merecen por haber plasmado su huella en mi camino.

Primeramente quiere agradecerle a mis padres, Fernando Súarez y Josefina González, por apoyarme incondicionalmente en todas las decisiones que he tomado tanto en mi vida académica como en mi vida personal, aunque no todas hayan sido de su agrado, pero aún así siempre han estado a mi lado, apoyándome y alentándome para seguir adelante. También por darme la oportunidad de llegar hasta aquí, ya que sin sus consejos, amor y formación posiblemente no hubiera llegado a estar donde estoy.

También quiero agredecerle a mis hermanos Gabriela, Patricia y Fernando por creer en mí y apoyarme cada día a lograr mis objetivos. También por ser grandes hermanos y grandes modelos a seguir; y que además de ser hermanos los considero grandes amigos y confidentes. Gracias por todo queridos hermanos.

A mi asesora Amanda Montejano, por todo el apoyo y paciencia que me brindó durante la realización de este trabajo.
A mis compañeros y amigos de la carrera: Ángel, Cabral, Limón, David y Borre, y en especial a Diego, Valentín, Lupe, Mariana, Mario y Lilí por hacer mis ratos en el áula y fuera de ella más placenteros y también por su apoyo para concluir la carrera.

A mis amigos de toda la vida: Ulises, Winnie, Ilán, Grecia, Checko, Maru, Beto, Luis, Abraham, Jacke, Denya, por su gran amistad que me han brindado durante todo este tiempo. En especial quiero agradecerle a Cindy por ser una gran amiga, por sus grandes consejos que me ha brindado y por todo el apoyo que me ha dado durante todo este tiempo que nos conocemos.

También quiero agradecerle a todas aquellas personas que han pasado por mi vida y con las que he compartido una sonrisa o un trago.

Por último quiero agradecerle al proyecto “PAPIIT IA102013”, al proyecto “CONACYT 219827τ al proyecto “CONACYT 166303”; por su apoyo durante la realización de este trabajo

Índice general

1. Introducción **4**

2. Conceptos básicos **7**
2.1. Coloraciones 7
2.2. Universos aritméticos 10
2.3. Estructuras monocromáticas y heterocromáticas 17

3. Teorías de Ramsey y anti-Ramsey **21**
3.1. La teoría de Ramsey 21
3.2. El teorema de Schur 25
3.3. La teoría anti-Ramsey 28
3.4. El teorema de Schur en la teoría anti-Ramsey 29

4. Teoría anti-Ramsey en otros universos **36**
4.1. Resultados en $\mathbb{N}$ y $\mathbb{Z}_n$ 36
4.2. El grupo abeliano de orden primo: $\mathbb{Z}_p$ 41

5. Teoría aditiva de números versión tríos **43**
5.1. Definiciones 43
5.2. El teorema de Cauchy-Davenport 46
5.3. El teorema de Vosper 57

6. La prueba versión tríos **72**

7. Conclusiones y trabajo a futuro **76**

Capítulo 1

Introducción

Una *k-coloración* de un conjunto X es una partición de dicho conjunto en k subconjuntos; de manera más intuitiva podemos decir que una k-coloración es la asignación de k colores a los elementos de un conjunto, donde a cada elemento se le asigna exactamente un color. Dentro de la teoría de coloraciones existen dos tipos de conjuntos muy especiales: los *conjuntos monocromáticos* —aquellos con todos sus elementos del mismo color—, y *los conjunto heterocromáticos* —aquellos en los cuales todos sus elementos tienen distinto color—.

La *teoría de Ramsey*, llamada así por el matemático Frank P. Ramsey, es un área de las matemáticas que estudia las condiciones bajo las cuales un cierto orden debe aparecer. En pocas palabras, la teoría de Ramsey afirma que, en general, en sistemas lo suficientemente grandes siempre existen subsistemas estructurados. Un ejemplo de ello es el teorema de Schur, que nos afirma que en toda k-coloración del intervalo inicial de números enteros $\{1, 2, ..., n\}$, si n es lo suficientemente grande, siempre podremos encontrar una solución monocromática a la ecuación $x + y = z$ [6, 9].

En contraste con la *teoría de Ramsey* que estudia la existencia de estructuras monocromáticas justificando así que el completo desorden es un imposible, la *teoría anti-Ramsey* estudia la existencia de estructuras heterocromáticas en universos coloreados, motivo por el cual se dice que en la teoría anti-Ramsey se busca demostrar que el perfecto orden es imposible también [4, 5].

En la *teoría anti-Ramsey Aritmética*, por lo general, se busca encontrar la estructura de las coloraciones, de grupos, en donde existan soluciones heterocromáticas a ecuaciones lineales. Un ejemplo de ello es encontrar la estructura de las coloraciones de $\mathbb{Z}_p$ en donde existan soluciones hetero-

cromáticas a la ecuación $x + y = z$. Para determinar la estructura de dichas coloraciones nos es necesario estudiar los conjuntos donde sus elementos satisfacen dicha ecuación, y para ello es más fácil estudiar el conjunto $X + Y$ que los conjuntos X e Y por separado, es decir, resulta factible utilizar como herramienta la *teoría Aditiva de Números.*
La teoría aditiva de números es el área de las matemáticas encargada de estudiar las características del *conjunto suma* de dos o más conjuntos de números. El conjunto suma de dos conjuntos A y B se define como $A+B = \{a + b|a \in A, b \in B\}$. Recientemente en la teoría Aditiva de Números se introdujo el concepto de *trío*, que facilitó el estudio de los conjuntos suma. Tres conjuntos A, B y C se dice que forman un trío si el 0 no pertenece a su conjunto suma, es decir, no pertenece a $A + B + C$. Todos los teoremas clásicos en la teoría aditiva de números se pueden reescribir utilizando este concepto de trío facilitando sus demostraciones [1, 8].

El objetivo principal de esta tesis es encontrar una demostración alterna al teorema que describe las 3-coloraciones de $\mathbb{Z}_p$ donde existen soluciones heterocromáticas a la ecuación $x + y = z$, utilizando como herramienta las nuevas versiones de los teoremas de la teoría de aditiva de números, bajo el concepto de trío.

Este trabajo de tesis está dividido en seis capítulos.

- En el primer capítulo se estudia las propiedades básicas de las coloraciones; las propiedades básicas de $\mathbb{Z}_p$, que es el universo principal a colorear en esta tesis, y por último se introducen las estructuras que se quieren encontrar en las coloraciones.

- En el segundo capítulo se menciona la historia de la teoría de Ramsey así como sus teoremas más importantes. Después se enuncia y se demuestra el t teorema de Schur que fue la principal motivación de este trabajo. Posteriormente se da una breve introducción a la teoría anti-Ramsey y por útimo se contrastan estas dos teorías, mencionando por qué no es posible encontrar un teorema análogo al teorema de Schur en la teoría anti-Ramsey.

- En el tercer capítulo se estudian los teoremas más importantes de la teoría anti-Ramsey aritmética en universos como $\mathbb{Z}_n$, $\mathbb{N}$ e intervalos de los números enteros. Se ve cómo es posible usar los teoremas de la teoría Aditiva de Números como herramienta en la demostración de algunos teoremas de la teoría anti-Ramsey Aritmética.

- En el cuarto capítulo se estudian teoremas importantes de la teoría

Aditiva de Números. Se introduce el concepto de trío; se reformulan dichos teoremas bajo este concepto; se demuestra que estas dos versiones de los teoremas son equivalentes y por último se dan las demostraciones, de algunos de ellos, en la versión trío.

- Finalmente en el quinto capítulo se da la prueba del teorema que nos describe a las 3-coloraciones de $\mathbb{Z}_p$ en donde no existen soluciones heterocromáticas a la ecuación $x + y = z$, empleando los teoremas de la teoría aditiva de números en sus versiones con el concepto de trío.

Capítulo 2

Conceptos básicos

En el presente capítulo exponemos el concepto principal que engloba esta tesis de manera general, así como la estructura algebraica en la que se desarrolla dicho trabajo. El primer término, la coloración, es el concepto esencial del presente trabajo y se entiende intuitivamente como la asignación de múltiples colores a elementos de un conjunto. Por otra parte, se describen las propiedades necesarias de la estructura algebraica que en el desarrollo de este estudio se emplean para obtener los resultados a los que se aspiran. El material contenido en este capítulo fue consultado en el libro "Álgebra moderna: grupos, anillos, campos, teoría de Galois"[2].

2.1. Coloraciones

A continuación se definirá formalmente lo que es una coloración, revelando dos maneras distintas de entender dicho concepto. Además de dar las dos definiciones se verán ejemplos, así como la demostración de la equivalencia entre ellas. Primero veremos las definiciones de partición y función.

Definición 2.1 *Una* partición *de un conjunto X es una familia $\mathcal{P}$ de subconjuntos de X que cumple lo siguiente:*

1. *Si $X_i, X_j \in \mathcal{P}$ entonces $X_i \cap X_j = \emptyset$ para todo $j \neq i$.*
2. *$X_i \neq \emptyset$ para todo $X_i \in \mathcal{P}$.*
3. *$\cup_{i\in\mathcal{I}} X_i = X$.*

Ejemplo 1 *Sea $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Consideremos la partición:*

$$\mathcal{P} = \{\{1, 4, 7, 10\}, \{2, 5, 8, 11\}, \{3, 6, 9, 12\}\}.$$

Equivalentemente, esta partición se puede definir como:

$$\mathcal{P} = \{X_1, X_2, X_3\}$$

donde $X_i = \{a | 1 \leq a \leq 12, a \equiv i \ (mod\ 3)$.

Definición 2.2 *Dados dos conjuntos* X *y* Y, *una* función f *de* X *a* Y *es una regla de correspondencia que asigna a cada elemento de* X *un único elemento de* Y *y se denota por:*

$$f : X \to Y.$$

Al conjunto X *se le conoce como el* dominio *de la función y al conjunto* Y *como el* codominio *de la función. Además, si al elemento* $x \in X$ *le corresponde el elemento* $y \in Y$, *lo denotaremos por* $f(x) = y$.

Ejemplo 2 *Sea* $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ *y* $Y = \{1, 2, 3\}$. *Definimos* $f : X \to Y$ *como*

$$f(x) = \begin{cases} 1 & si\ x \equiv 1\ (mód\ 3), \\ 2 & si\ x \equiv 3\ (m'od\ 3), \\ 3 & si\ x \equiv 0\ (m'od\ 3). \end{cases}$$

Se dice que una función f es *suprayectiva* si para todo elemento y del codominio existe un elemento x del dominio tal que $f(x) = y$, como es el caso del ejemplo 2.

Ahora sí estamos listos para definir el concepto de coloración, primero en términos de particiones y después en términos de funciones.

Definición 2.3 *Sea* X *un conjunto. Una* coloración *de* X *es una partición* $\mathcal{P}$ *de* X. *Si* $|\mathcal{P}| = k$ *entonces diremos que* $\mathcal{P}$ *es una* k-coloración *de* X. *En tal caso:*

$$X = X_1 \cup X_2 \cup \cdots \cup X_k,$$

y a cada X_i, *con* $1 \leq i \leq k$, *se le conoce como la* clase cromática de color i.

Definición 2.4 *Sea* X *un conjunto. Una* k-coloración *de* X *es una función suprayectiva:*

$$c : X \to \{1, 2, ..., k\}.$$

Además, definimos $X_i = c^{-1}(i) = \{x \in X | c(x) = i\}$, *como la* clase cromática *del color* i.

Las definiciones 2.3 y 2.4 son equivalentes. Durante el transcurso de este trabajo de tesis estaremos alternando su uso según sea el caso requerido. Por ejemplo, si la partición del ejemplo 1 y la función del ejemplo 2 son consideradas como 3-coloraciones del conjunto $\{1, 2, ..., 12\}$, podemos ver que obtenemos las mismas clases cromáticas.

Proposición 2.1 *La definición 2.3 y la definición 2.4 son equivalentes.*

Demostración:

Primero demostraremos que una k-coloración según la definición 2.3 (particiones) es una coloración según la definición 2.4 (funciones). Sea $X = A_1 \cup A_2 \cup \cdots \cup A_k$ una k-coloración de X. Definimos $c : X \to \{1, 2, ..., k\}$ como $c(x) = i$ si $x \in A_i$. Notemos que c es una función por el primer punto de la definición de partición (definición 2.1), y c es suprayectiva por el punto 3 de la misma definición.

Ahora demostraremos que una k-coloración según la definición 2.4 (funciones) es una coloración según la definición 2.3 (particiones). Sea $c : X \to \{1, 2, ..., k\}$ una k-coloración de X. Tal como están definidas las clases cromáticas de la función suprayectiva c obtenemos una partición de X.

□

Ejemplo 3 *Sea* $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. *Consideremos la siguiente* 4*-coloración* $c : X \to \{1, 2, 3, 4\}$*:*

$$\begin{gathered} c(1) = c(2) = 1, \\ c(3) = c(4) = 2, \\ c(5) = c(6) = 3, \\ c(7) = c(8) = c(9) = c(10) = 4. \end{gathered}$$

Equivalentemente, $X = X_1 \cup X_2 \cup X_3 \cup X_4$ *donde las clases cromáticas son* $X_1 = \{1, 2\}$, $X_2 = \{3, 4\}$, $X_3 = \{5, 6\}$ *y* $X_4 = \{7, 8, 9, 10\}$.

Para visualizar una coloración como un conjunto coloreado, vamos a pensar que cada número es un color. Por ejemplo, si en las coloraciones dadas en los ejemplos 1 y 2, el 1 es el rojo, el 2 es el azul, el 3 es el verde, las clases cromáticas X_1, X_2 y X_3 corresponden a los conjuntos de rojos, azules y verdes respectivamente, por lo que podemos visualizar tales coloraciones como:

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

y la coloración del ejemplo 3 como:

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Dentro de la teoría de coloraciones hay dos conjuntos muy especiales, con los cuales trabajaremos a lo largo de este trabajo de tesis.

Definición 2.5 *Sea X un conjunto y $Y \subset X$. Dada $X = X_1 \cup X_2 \cup \cdots \cup X_k$ una k-coloración de X, decimos que Y es* monocromático *si $Y \subseteq X_i$ para algún $1 \leq i \leq k$.*

Definición 2.6 *Sea X u conjunto y $Y \subset X$. Dada $X = X_1 \cup X_2 \cup \cdots \cup X_k$ una k-coloración de X, decimos que Y* heterocromático *si $|Y \cap X_i| \leq 1$ para todo $1 \leq i \leq n$.*

Ejemplo 4 *Consideremos el siguiente conjunto coloreado:*

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Los conjuntos $B = \{1, 4, 7\}$ y $C = \{2, 4, 12\}$ son monocromático y heterocromático respectivamente. Notemos que $B = \{1, 4, 7\}$ y $C = \{2, 4, 12\}$,

Entonces un conjunto monocromático tiene todos sus elementos del mismo color, mientras que un conjunto heterocromático es aquel en donde todos sus elementos son de colores distintos. El conjunto $D = \{1, 4, 8, 12\}$ no es ni monocromático ni heterocromático pues $D = \{1, 4, 8, 12\}$.

En el capítulo 3 veremos que la teoría de Ramsey aritmética estudia la existencia de conjuntos monocromáticos en coloraciones de universos aritméticos. En contraste con la teoría anti-Ramsey aritmética que hace lo propio con la existencia de conjuntos heterocromáticos.

En la siguiente sección presentaremos los universos aritméticos que se suelen colorear en las teorías de Ramsey y anti-Ramsey.

2.2. Universos aritméticos

Denotaremos, como es usual, los conjuntos de números naturales y enteros de la siguiente manera:

$$\mathbb{N} = \{1, 2, 3, ...\}.$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}.$$

Además de colorear $\mathbb{N}$ y $\mathbb{Z}$, ha sido de gran interés colorear el intervalo inicial de números enteros:

$$[n] = \{1, 2, ..., n\}.$$

Pero sobre todo, en esta tesis estamos interesados en colorear grupos cíclicos de orden primo. En esta sección daremos los conceptos necesarios para definir lo que es un grupo cíclico de orden primo: $\mathbb{Z}_p$.

En matemáticas uno de los conceptos fundamentales es el concepto de grupo. Un grupo es un conjunto no vacío junto con una operación binaria. Una operación binaria se define formalmente de la siguiente manera.

Definición 2.7 *Sea X un conjunto. Una* operación binaria *es una función $* : X \times X \to X$, donde $X \times X =: \{(a, b) | a \in X, b \in X\}$. La operación binaria se denota por $*$ y $*(a, b)$ se denota por $a * b$.*

Ejemplo 5 *La suma habitual en los enteros es una operación binaria.*

Definición 2.8 *Un* grupo *es una pareja $(G, *)$ donde G es un conjunto no vacío y $*$ es una operación binaria que satisface las siguientes propiedades:*

- Cerradura:

  si $a, b \in G$ entonces $a * b \in G$.

- Asociatividad:

  si $a, b, c \in G$ entonces $a * (b * c) = (a * b) * c$.

- Neutro o identidad:

  existe un elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$.

- Inverso:

  para todo $a \in G$ existe $a^{-1} \in G$ tal que $a * (a^{-1}) = a^{-1} * a = e$.

Además si se cumple la siguiente propiedad, se dice que el grupo es abeliano *o* conmutativo*.*

- Conmutatividad:

  para todo $a, b \in G$ se tiene que $a * b = b * a$.

Ejemplo 6 *Los números enteros junto con la suma habitual forman un grupo abeliano, cuyo elemento neutro es el cero.*

Un grupo de cardinalidad infinita, como en los ejemplos anteriores, se dice que tiene *orden infinito*. Cuando la cardinalidad de un grupo G es finita, entonces diremos que el grupo es de *orden* $|G|$.

En esta tesis, vamos a trabajar principalmente con grupos abelianos. Como es usual cuando se trabaja con grupos abelianos, usaremos la notación aditiva, es decir un grupo será $(G, +)$ con elemento neutro 0. En lo sucesivo usaremos la siguiente notación:

$$na = \underbrace{a + a + a + \cdots + a}_{\text{n veces}}$$

y

$$-na = -(na) = -(\underbrace{a + a + a + \cdots + a}_{\text{n veces}}).$$

Además al grupo $(G, +)$ lo denotaremos simplemente por G.

Definición 2.9 *Se dice que un grupo G es* cíclico *si existe $g \in G$ tal que para todo $a \in G$ existe $n \in \mathbb{Z}$ con $a = ng$. Al elemento g se le conoce como generador del grupo.*

Ejemplo 7 *Los enteros con la suma habitual, $(\mathbb{Z}, +)$, son un grupo cíclico con dos generadores distintos, a saber, 1 y -1.*

Este ejemplo nos dice que el generador no es necesariamente único, y además que existen grupos cíclicos de orden infinito. Más adelante veremos ejemplos de grupos cíclicos de orden finito.

Otra definición importante es la siguiente:

Definición 2.10 *Sea G un grupo abeliano con orden finito. El* orden de un elemento *a en el grupo G se define como el menor entero positivo n tal que $na = 0$, y se denota por $\circ(a) = n$.*

En este trabajo de tesis trabajaremos particularmente con un grupo abeliano muy especial llamado el grupo cíclico de orden n o el grupo de congruencias módulo n. Antes de definirlo daremos los conceptos necesarios. Empezaremos definiendo un concepto muy básico e importante en todas las áreas de las matemáticas

Definición 2.11 *Sea X un conjunto. Una* relación R en X *es un subconjunto de $X \times X$, es decir, es un conjunto formado por parejas ordenadas entre elementos de X. Si la pareja (x, y) pertenece a R, decimos que x* está relacionado con *y. Se dice que una* relación es de equivalencia *si cumple las siguientes propiedades.*

- Reflexividad

  para todo $x \in X$ se tiene que x está relacionado con x.

- Simetría

  para todo $x, y \in X$, si x está relacionado con y, entonces y está relacionado con x

- Transitividad
  para todo $x, y, z \in X$, si x está relacionado con y, y y está relacionado con z, entonces x está relacionado con z.

Además, al conjunto $[x] = \{y \in X |$ x está relacionado con $y\}$ le llamaremos la clase de equivalencia de x

Lo importante de las relaciones de equivalencia es la posibilidad de tratar como "iguales", bajo el criterio de la relación, a los elementos de una misma clase de equivalencia; y esto nos facilita el trabajo ya que en vez de trabajar con todos los elementos de un conjunto, nos reducimos a trabajar simplemente con las clases de equivalencia, que son menos que los elementos y resguardan toda la estructura de interés.

Antes de definir la relación de equivalencia en la que estamos interesados para definir el grupo de congruencias módulo n, presentaremos los conceptos de divisibilidad, números primos, máximo común divisor y primos relativos.

Definición 2.12 *Sean $a, b \in \mathbb{Z}$. Decimos que a* divide a *b, denotado por $a|b$, si existe $h \in \mathbb{Z}$ tal que $ah = b$. Si $a|b$, decimos que a* es divisor de *b o que b* es múltiplo de *a o que a* es factor de *b.*

Hay un conjunto de números que al poseer muy pocos divisores, tienen propiedades únicas muy interesantes y por tanto se vuelven muy importantes. Estos números son los siguientes.

Definición 2.13 *Sea $p \in \mathbb{N}$, $p > 1$. Decimos que p* es número primo *si sus únicos divisores son 1 y p. Si un número no es primo entonces diremos que es un* número compuesto.

Sean $a, b \in \mathbb{Z}$ distintos de 0, denotamos por (a, b) al *máximo común divisor* de a y b. Es fácil ver que el máximo común divisor de dos números siempre existe ya que el 1 divide a todo número.

Definición 2.14 *Decimos que a y b son* primos relativos *si $(a, b) = 1$.*

Ejemplo 8 *El* 2 *y el* 6 *no son primos relativos pues* $(2,6) = 2$. *El* 12 *y el* 18 *no son primos relativos pues* $(12,18) = 6$. *El* 10 *y el* 21 *sí son primos relativos pues* $(10,21) = 1$.

A continuación definiremos la relación de congruencia módulo n, para posteriormente definir el grupo de clases de congruencia módulo n.

Definición 2.15 *Sea n un entero positivo fijo y $a, b \in \mathbb{Z}$. Decimos que a* es congruente con b módulo n *y lo denotamos por: $a \equiv b \pmod{n}$ si $n|(a-b)$.*

Esta relación de congruencia tiene las siguientes propiedades básicas.

Proposición 2.2 *Sea n un entero positivo fijo y $a, b, c, d \in \mathbb{Z}$. Entonces lo siguiente se cumple:*

i) La relación "a es congruente con b módulo n" *es una relación de equivalencia en el conjunto de los números enteros.*

ii) Esta relación de equivalencia tiene exactamente n distintas clases de equivalencia.

iii) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{n}$ y $ac \equiv bd \pmod{n}$.

iv) Si $ab \equiv cd \pmod{n}$ y a es primo relativo con n, entonces $b \equiv c \pmod{n}$.

Demostración:

i) Para demostrar que la relación es reflexiva notemos que para todo n positivo se cumple que $n|0$ y $0 = a - a$, para todo a en los enteros, por lo tanto $a \equiv a \pmod{n}$; luego la relación es reflexiva. Si $a \equiv b \pmod{n}$, entonces $n|(a-b)$ y, por lo tanto, $n|(b-a)$ ya que $(b-a) = -(a-b)$; luego $b \equiv a \pmod{n}$ y por lo tanto la relación es simétrica. Por último, si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $n|(a-b)$ y $n|(b-c)$, de donde $n|((a-b)+(b-c))$, es decir, $n|(a-c)$, esto implica que $a \equiv c \pmod{n}$; luego la relación es transitiva y por lo tanto es de equivalencia.

ii) Sea $a \in \mathbb{Z}$. Denotemos la clase de equivalencia de esta relación a la que pertenece a por $[a]$, y la llamaremos *clase de congruencia* $\pmod{n}$ de a. Dado un entero cualquiera a, sabemos por el algoritmo de la división que $a = qn + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r < n$, de donde obtenemos que $a - r = qn$, entonces $n|(a-r)$, luego $a \equiv r \pmod{n}$.

Pero entonces $a \in [r]$, luego $[a] = [r]$ y por lo tanto hay a lo más n clases de congruencia; a saber, $[0], [1], ..., [n-1]$. Pero estas son distintas entre sí, pues si $[i] = [j]$, con $0 \leq i < j < n$, entonces $n|(j-i)$, lo cual es imposible ya que $0 < j - i < n$. Hay por lo tanto exactamente n distintas clases de congruencia.

iii) Supongamos que $a \equiv b$ (mód n) y $c \equiv d$ (mód n); entonces $n|(a-b)$ y $n|(c-d)$, entonces $n|((a-b)+(c-d))$, que es lo mismo a $n|((a+c)-(b+d))$, y por lo tanto $a+c \equiv b+d$ (mód n). Además $n|((a-b)c+(c-d)b)$ que es lo mismo a $n|(ac-bd)$, luego $ac \equiv bd$ y por lo tanto el tercer apartado queda demostrado.

iv) Observemos finalmente que si $ab \equiv ac$ (mód n), con a primo relativo de n. Como $ab \equiv ac$ (mód n), entonces $n|(ab-ac) = n|a(b-c)$, pero como n y a son primos relativos entonces $n|(b-c)$ y por lo tanto $b \equiv c$ (mód n).

□

Ahora si estamos listos para definir el *grupo de congruencias módulo* n, también conocido como el *grupo cíclico de orden* n. Sea $\mathbb{Z}_n$ el conjunto de las clases de congruencia módulo n, es decir

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}.$$

Dados dos elementos $[i]$ y $[j]$ en $\mathbb{Z}_n$, definimos

$$[i] + [j] = [i + j]$$

Observemos que la operación antes mencionada, está bien definida, es decir, no importa que representantes nos agarremos de cada clase de congruencia, al sumarlos, el resultado siempre será la misma clase de congruencia. Esto se debe al inciso iii) de la proposición anterior.

Proposición 2.3 *El conjunto* $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$ *es un grupo con la suma definida anteriormente. Más aún* $(\mathbb{Z}_n, +)$ *es un grupo abeliano y cíclico, cuyos generadores son aquellas clases de congruencia en donde el representante es primo relativo con* n.

Demostración:

Primero demostraremos que $\mathbb{Z}_n$ es un grupo, por lo tanto tenemos que probar todas las propiedades de un grupo. Empecemos por la cerradura. Sean $[i], [j] \in \mathbb{Z}_n$, entonces $[i]+[j] = [i+j]$. Si $i+j < n$ entonces $[i+j] \in \mathbb{Z}_n$;

si $i + j \geq n$, entonces por el algoritmo de la división tenemos que existen $r, q \in Z$ tal que $i + j = qn + r$ con $0 \leq r < n$, entonces $r \equiv (i + j)$, luego $[r] = [i + j]$ y por lo tanto $[i + j] \in \mathbb{Z}_n$. Ahora probaremos la asociatividad. Sean $[i], [j], [k] \in \mathbb{Z}_n$. Observemos lo siguiente:

$$\begin{aligned}
[i] + ([j] + [k]) &= [i] + ([j + k]) \\
&= [i] + [j + k] \\
&= [i + (j + k)] \\
&= [(i + j) + k] \\
&= [i + j] + [k] \\
[i] + ([j] + [k]) &= ([i] + [j]) + [k].
\end{aligned}$$

Notemos que dentro de los corchetes podemos asociar, conmutar y considerar como ciertas las propiedades de grupo, ya que dentro de ellos estamos trabajando con números enteros y estos forman un grupo.

En $\mathbb{Z}_n$ definimos el elemento identidad como $e = [0]$. Para verificar que $[0]$ es la identidad del grupo tenemos que probar que $[0]+[a] = [a]+[0] = [a]$ para todo $[a] \in \mathbb{Z}_p$. Entones tenemos que:

$$[a] + [0] = [a + 0] = [0 + a] = [0] + [a] = [0 + a] = [a].$$

Comprobemos ahora que todo elemento en $\mathbb{Z}_n$ tiene elemento inverso. Sea $[a] \in \mathbb{Z}_n$. Demostraré que el inverso de $[a]$ es $[n - a]$:

$$\begin{aligned}
[a] + [n - a] =& [a + n - a] \\
& [n - a + a] \\
& [n - a] + [a] \\
& [n - a + a] \\
& [n].
\end{aligned}$$

Pero sabemos que $n \equiv 0$, ya que $n|(n - 0)$; y por lo tanto $[n] = [0]$.

Como se cumplieron todas las propiedades de grupo, entonces $\mathbb{Z}_n$ es un grupo. Al definir el conjunto $\mathbb{Z}_n$ vimos que su orden es n. Ahora probaremos que $\mathbb{Z}_n$ es un grupo abeliano; lo cual es muy fácil. Sean $[i], [j] \in \mathbb{Z}_n$ entonces:

$$[i] + [j] = [i + j] = [j + i] = [j] + [i].$$

$\mathbb{Z}_n$ es un grupo cíclico ya que podemos escribir a todo elemento $[a] \in \mathbb{Z}_n$ como:

$$[a] = [\underbrace{1 + 1 + \cdots + 1}_{a \text{ veces}}] = \underbrace{[1] + [1] + \cdots + [1]}_{a \text{ veces}} = a[1].$$

Con lo cual vemos que [1] es un generador de $\mathbb{Z}_n$.
Sólo nos falta demostrar que si p es primo relativo de n entonces $[p]$ es generador de $\mathbb{Z}_n$. Para probar esto basta demostrar que $\circ([p]) = n$ para todo p primo relativo de n. Podemos deducir facilmente que $\circ([p]) \leq n$. Supongamos que $\circ([p]) < n$. Sea $\circ([p]) = m$, entonces tenemos que $m[p] = 0$, luego $mp \equiv 0$ (mód n). Por lo anterior tenemos que $n|mp$, pero como n y p son primos relativos, entonces $n|m$; lo cual es una contradicción ya que $0 < m < n$. Entonces obtenemos que $\circ([p]) = n$ y por lo tanto $[p]$ genera a $\mathbb{Z}_n$.

□

En esta de tesis trabajaremos principalmente con grupos cíclicos de orden primo, es decir, $\mathbb{Z}_p$. Además, a las clases de congruencias las expresaremos simplemente con su representante positivo más pequeño, así $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$. Notemos que para todo $0 < a < p$, a es primo relativo con p y por lo tanto todo elemento de $\mathbb{Z}_p$ es generador de dicho grupo, entonces podemos fijar dos elementos a, b de $\mathbb{Z}_p$ y escribirlo como $\mathbb{Z}_p = \{a + bi | 0 \leq i \leq p-1\}$.

2.3. Estructuras monocromáticas y heterocromáticas

Una vez que definimos lo que es una coloración y los universos que vamos a colorear, recordemos que lo que nos interesa estudiar es la existencias de estructuras momocromáticas (en la teoría de Ramsey) y estructuras heterocromáticas (en teoría anti-Ramsey). Lo cuál nos lleva a preguntarnos:

¿Qué tipo de estructuras monocromáticas o heterocromáticas queremos encontrar?

Aunque tanto en la teoría de Ramsey como en la teoría anti-Ramsey se trabaja con muy diversas estructuras, en este trabajo de tesis nos enfocaremos principalmente en un tipo de estructura muy especial. Tales estructuras son las soluciones a ecuaciones lineales, que a continuación definimos.

Definición 2.16 *Decimos que*

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_lx_l = b \tag{2.1}$$

es una ecuación lineal *con* l variables*:* $x_1, x_2, ..., x_l$*,* l coeficientes*:* $a_1, a_2, ..., a_l$*, y un* término independiente*:* b*.*

Una solución *de la ecuación 2.1 es un vector* $(s_1, s_2, s_3, ..., s_l)$ *tal que*

$$a_1s_1 + a_2s_2 + a_3s_3 + \cdots + a_ls_l = b.$$

Ejemplo 9 *Consideremos la siguiente ecuación lineal:*

$$3x_1 + 2x_2 - 4x_3 = 5 \tag{2.2}$$

Podemos observar que los vectores $(3, 0, 1)$ *y* $(1, 3, 1)$ *son soluciones de la ecuación 2.2.*

Por lo general, cuando hablamos de soluciones a una ecuación lineal nos referimos a un conjunto y no a un vector.

En el ejemplo anterior podemos ver que tanto el conjunto $\{0, 1, 3\}$ como el conjunto $\{1, 3\}$ son soluciones a la ecuación lineal 2.2.

Definición 2.17 *Un subconjunto* $S \subset \mathbb{Z}$ *con* $|S| \leq l$ *es solución a la ecuación 2.1 si*

$$a_1s_1 + a_2s_2 + \cdots + a_ls_l = b$$

con $s_1, s_2, ..., s_l \in S$*, no necesariamente distintos, y* $\cup_1^l s_i = S$*.*

Si $|S| = 1$ *diremos que* S *es una solución* trivial*.*

Ejemplo 10 *Consideremos la ecuación lineal:*

$$x + y = 2z \tag{2.3}$$

Los conjuntos $\{0, 2, 4\}$ *y* $\{3, 6, 9\}$ *son soluciones a la ecuación 2.3. Los conjuntos* $\{2\}$ *y* $\{10\}$ *son soluciones triviales a la ecuación 2.3. De hecho, podemos notar que para todo* a*, el conjunto* $\{a\}$ *es solución trivial a la ecuación 2.3.*

En el ejemplo anterior podemos observar que en las soluciones a la ecuación 2.3 la diferencia entre dos números consecutivos es constante, es decir, las soluciones son progresiones aritméticas de longitud tres.

Definición 2.18 *Sea* S *subconjunto de* $\mathbb{Z}$*, con* $|S| = k$*. Se dice que* S *es una* progresión aritmética *con* k términos *y* diferencia d *si existe* $s \in \mathbb{Z}$ *tal que*

$$S = \{s + nd | 0 \leq n \leq k - 1\}.$$

Ejemplo 11 *Observemos los siguientes conjuntos:*

1. $\{0, 3, 6, 9\}$ *es una progresión aritmética de diferencia* 3 *y* 4 *términos.*

2. $\{-10, -5, 0\}$ *es una progresión aritmética de diferencia* 5 *y* 3 *términos.*

Las progresiones aritméticas son otra estructura que se estudia mucho en la teoría de Ramsey y en la teoría anti-Ramsey. En este trabajo daremos algunos ejemplos de algunos resultados donde se involucran dichas progresiones aritméticas.

En especial, las progresiones aritméticas con 3 términos son muy estudiadas, ya que, como vimos en el ejemplo 10, las soluciones a la ecuación 2.3 son progresiones aritméticas, y es fácil de ver que toda progresión aritmética con 3 términos es solución a la ecuación 2.3.

Como explicamos en la sección anterior, dada una coloración de $\mathcal{X}$, donde $\mathcal{X}$ es un universo aritmético como $[n], \mathbb{Z}_p$ y $\mathbb{Z}_n$; nos interesa estudiar la existencia de soluciones monocromáticas o heterocromáticas.

Para entender mejor esto veamos el siguiente ejemplo.

Ejemplo 12 *Sea* $c : [10] \to \{R, A, V, N\}$ *una* 4*-coloración de* $[10]$ *definida como sigue:*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

En esta coloración es fácil de ver que no existen soluciones monocromáticas a la ecuación $x + y = z$*, en cambio, el conjunto* $\{4, 6, 10\}$ *es una solución heterocromática a dicha ecuación.*

Ahora consideremos la siguiente 3*-coloración:*

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

podemos ver que en esta coloración el conjunto $\{1, 8, 9\}$ *es una solución monocromática a la ecuación* $x + y = z$*, pero en esta coloración no existen soluciones heterocromáticas a la ecuación antes mencionada.*

En los capítulos posteriores estudiaremos coloraciones en las que no existen estructuras hetecromáticas. A estas coloraciones las llamaremos "libres", pues son libres de estructuras heterocromáticas.

Definición 2.19 *Sea* $\mathcal{X}$ *un universo aritmético y sea* $c : \mathcal{X} \to \{1, 2, ..., k\}$ *una* k*-coloración de* $\mathcal{X}$*. Se dice que* c *es* libre *con respecto a una estructura* C*, si no existen estructuras* C *heterocromáticas.*

Para entender mejor el concepto de "libre"veamos los siguientes ejemplos:

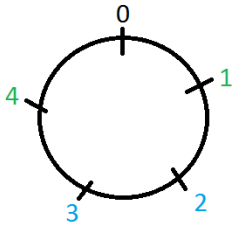
Ejemplo 13 *Consideremos las siguientes coloraciones.*

- *Sea* $c : [10] \to \{R, A, V\}$ *una* 3*-coloración de* [10]*, definida como:*

  $$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

  Esta coloración es libre con respecto a la ecuación $x + y = z$ *ya que no contiene soluciones heterocromáticas de dicha ecuación.*

- *Sea* $c : \mathbb{Z}_5 \to \{A, V, N\}$ *una* 3*-coloración de* $\mathbb{Z}_5$ *definida como:*

  es fácil ver que esta coloración es libre con respecto a $x + y = 2z$*.*

- *Sea* $c : [9] \to \{A, V, N\}$ *una* 3*-coloración de* [9] *definida como:*

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

  Podemos ver que esta coloración es libre con respecto a progresiones aritméticas con 3 *términos, ya que no existen progresiones aritméticas con* 3 *términos heterocromáticas.*

En los capítulos posteriores veremos resultados que nos dirán cuándo una coloración es libre.

Capítulo 3

Teorías de Ramsey y anti-Ramsey

En este capítulo abordaremos dos de las áreas que se tratan en el presente trabajo de tesis. Estas tienen interacción con diversas ramas de las matemáticas y además poseen teoremas muy significativos; estas áreas son: la *teoría de Ramsey* y la *teoría anti-Ramsey*. Veremos cómo fue el nacimiento de cada una de ellas y enunciaremos sus teoremas más importantes. También contrastaremos las dos teorías y veremos las diferencias que existen entre ellas.

En particular, enunciaremos y demostraremos el *teorema de Schur*, resultado central en este trabajo de tesis.

Todo el material que aquí se presenta fue consultado en los libros: "Ramsey Theory on the intergers"[6] y "Ramsey theory: yesterday, today, and tomorrow"[9]; así como en los artículos: "Rainbow arithmetic progressions and anti-Ramsey results"[4] y "Rainbow Ramsey Theory"[5].

3.1. La teoría de Ramsey

La teoría de Ramsey es un fascinante área de las matemáticas con aproximadamente 100 años de edad que tiene intersección no vacía con otras ramas de las matemáticas, como son: la combinatoria, la teoría de números, la geometría, la teoría de gráficas, la topología, la teoría ergódica, y la teoría de la medida, entre otras. En esta tesis nos enfocaremos en problemas relacionados con la combinatoria y la teoría de números. Algunos de los resultados en la Teoría de Ramsey son algunos de los teoremas más bellos de las matemáticas; a pesar de ello, a primera vista parecen ser complicados y

difíciles de seguir, ya que tienden a involucrar muchas variables y a veces tratan con objetos cuyos elementos son conjuntos y a su vez estos conjuntos vuelven a tener elementos que son conjuntos. Sin embargo, cuando el objeto de estudio es el conjunto de los números enteros las cosas se facilitan, como es el caso en esta tesis.

Antes de hablar de la teoría de Ramsey, es necesario mencionar un principio que a primera vista suena innecesario y trivial, pero en la práctica tiene muchas aplicaciones, sobre todo en la teoría de Ramsey, ya que es una herramienta fundamental en sus demostraciones. Este principio se conoce como el principio de las casillas o del palomar y argumenta lo siguiente: si n palomas se acomodan en m nidos, donde $m < n$, entonces al menos un nido tendrá más de una paloma. Formalmente el principio se enuncia de la siguiente manera:

Proposición 3.1 ***(Principio de casillas)***. *Si un conjunto de n elementos es partido en k subconjuntos ajenos a pares, donde $n > k$, entonces al menos un subconjunto de la partición contiene más de un elemento.*

Ejemplo 14 *En una clase de 29 alumnos, hay al menos dos alumnos cuyos nombres empiezan con la misma letra. En este ejemplo nuestras palomas serán las letras iniciales de los nombres, entonces tenemos 29 palomas, y nuestros nidos serán las letras del abecedario, que son 26 nidos, entonces como tenemos más nidos que palomas, un nido tiene al menos dos palomas, es decir, dos nombres al menos empiezan con la misma letra.*

Este principio se puede generalizar como sigue:

Teorema 3.1 ***(Principio de casillas generalizado)***. *Sea S un conjunto con $|S| > mk$, y sea $S = S_1 \cup S_2 \cup \cdots \cup S_k$ una partición de S en k subconjuntos. Entonces existe S_i tal que $|S_i| > m$, con $1 \leq i \leq k$.*

Demostración:

Sea S un conjunto, con $|S| > mk$, y sea $S = S_1 \cup S_2 \cup \cdots \cup S_k$ una partición de S en k conjuntos. Asumamos por contradicción que $|S_i| \leq m$ para todo $1 \leq i \leq k$. Entonces:

$$|S| = \sum_{i=1}^{k} |S_i| \leq mk,$$

lo cual es una contradicción ya que $|S| > mk$, y por lo tanto existe S_i tal que $|S_i| > m$.

□

La teoría de Ramsey se puede percibir como un refinamiento al principio de las casillas, donde no sólo garantizamos un cierto número de elementos en un subconjunto, sino que además garantizamos una cierta relación entre estos elementos.

No existe una "definición universal"de la teoría de Ramsey, pero podemos describirla como el estudio de la preservación de propiedades bajo particiones. O también podemos decir que en la teoría de Ramsey se estudia qué tan grande debe ser un sistema S, para poder garantizar la existencia de cierto subsistema Q monocromático sin importar cómo sea coloreado S.

El primer resultado que se conoce de tipo Ramsey es el *lema del cubo de Hilbert* que enunciaremos en esta sección. Como a este resultado no se le observó nada especial en su tiempo, la teoría de Ramsey no nació en ese momento. El segundo resultado de tipo Ramsey fue el *teorema de Schur*, que se trabajará en esta tesis, demostrado en 1916. Aunque tampoco fue relevante, Schur se dio cuenta de que había descubierto algo impresionante y nuevo así que siguió conjeturando generalizaciones a su teorema. El tercer trabajo que se dio en esta área, que aun no nacía, fue el *teorema de Van der Warden*. Después de los tres trabajos anteriores, la teoría de Ramsey nació por fin gracias a los trabajos de un joven matemático inglés llamado Frank Plumpton Ramsey, véase [9].

Como mencionamos anteriormente el primer resultado tipo Ramsey fue el lema del cubo de Hilbert que apareció en 1892, el autor de este lema fue David Hilbert, prolífico matemático alemán. Hilbert demostró este resultado como herramienta a su estudio de la irreducibilidad de funciones racionales con coeficientes enteros. Para mencionar su lema primero definiremos lo siguiente:

Definición 3.1 *Un conjunto $Q_n(a, x_1, x_2, ..., x_n)$ de enteros es llamado un* cubo n-dimensional afín *si existen $n+1$ enteros positivos $(a, x_1, x_2, ..., x_n)$ tales que:*

$$Q_n(a, x_1, x_2, ..., x_n) = \{a + \textstyle\sum_{i\in F} x_i | \emptyset \neq F \subseteq \{1, 2, 3, ..., n\}\}.$$

Recordemos que para facilitar la escritura denotamos $\{1, 2, 3, ..., n\}$ como $[n]$. Ya que hemos definido lo que es un cubo n-dimensional afín podemos mencionar el primer resultado tipo Ramsey:

Teorema 3.2 ***(Lema del cubo de Hilbert, 1892)***. *Para todo par de enteros positivos k, n existe un entero positivo mínimo $m = H(k, n)$ tal que en toda k-coloración de $[m]$ existe un cubo n-dimensional afín monocromático.*

En otras palabras, el teorema nos dice que para todo número de colores k, si n es suficientemente grande, toda coloración con esos k colores del intervalo de enteros positivos $[n]$ existe un cubo n-dimensional afín monocromático.

El segundo resultado tipo Ramsey, como dijimos anteriormente, fue el teorema de Schur que mostraremos más adelante. En sus trabajos, Schur propuso una conjetura que fue demostrada por el matemático alemán Leendert van der Warden a los 23 años, en 1927. El teorema de Van der Warden, es considerado el tercer resultado tipo Ramsey.

Teorema 3.3 ***(Teorema de Van der Warden, 1927)****. Para todo par de enteros positivos k, l existe un entero positivo mínimo $W = W(k, l)$, tal que para toda k-coloración del conjunto $[W]$ existe una progresión aritmética monocromática con l términos.*

Parecido al lema del cubo de Hilbert, lo que este teorema nos quiere decir es que para todo número de colores k siempre va a existir un intervalo en el cual no importa cómo lo coloreemos con esos k colores, nunca se va a escapar de tener una progresión aritmética con l términos monocromática.

Este teorema fue toda la contribución que hizo Van der Warden a esta aún no nacida teoría. Después de estos tres trabajos vino uno de los orgullos y esperanzas de la universidad de Cambridge: Frank Plumton Ramsey. Ramsey fue un joven matemático inglés, que vivió tan sólo 27 años, cuyas mayores contribuciones fueron a la filosofía, la lógica matemática y la economía. En un trabajo póstumo publicado en 1930, demostró un teorema que fue el nacimiento a la teoría de Ramsey. Este teorema ocupa un lugar único dentro de la teoría de Ramsey ya que es una herramienta muy poderosa. Este teorema también se puede ver como un principio filosófico: "el completo desorden es imposible, toda estructura necesariamente contiene una subestructura ordenada"; por esto mismo es Imperativo llamar al teorema de Ramsey como "Principios de Ramsey"[9]. Este principio tiene dos versiones, una finita y una infinita y se enuncian como sigue:

Teorema 3.4 ***(Principio de Ramsey versión infinita, 1930)****. Para cualesquiera enteros positivos k y r, si la colección de todos los subconjuntos con r elementos de un conjunto infinito S es coloreada con k colores, entonces S contiene un subconjunto infinito S_1, tal que todos los subconjuntos con r elementos de S_1 tienen del mismo color.*

Teorema 3.5 ***(Principio de Ramsey versión finita, 1930)****. Para cualesquiera enteros positivos k, r y n, existe un entero $m_0 = R(k, r, n)$ tal que*

para todo $m \geq m_0$, si la colección de todos los subconjuntos con r elementos de un conjunto S_m con m elementos es coloreada con k colores, entonces S_m contiene un subconjunto S_n con n elementos tal que todos los subconjuntos con r elementos de S_n tienen el mismo color.

A primera vista las dos versiones de este principio son difíciles de digerir, para facilitar su entendimiento veamos una aplicación en su versión infinita, y una aplicación en su versión finita a la teoría de gráficas:

Ejemplo 15 ***(Aplicación de la versión infinita)***. *Sea S un conjunto de carnalidad infinita, entonces cualquier partición de S en k conjuntos tendrá una de las partes de carnalidad infinita.*

En este ejemplo las k partes representan los k colores, y $r = 1$ ya que estamos coloreando elementos, es decir, conjuntos de un sólo elemento.

Ejemplo 16 ***(Aplicación de la versión finita)***. *Para cualesquiera enteros positivos n y k existe un entero positivo mínimo $R = R(n, k)$ tal que toda k-coloración de las aristas de la gráfica completa K_R contiene una subgráfica completa K_n monocromática.*

Como sabemos, las aristas son subconjuntos de dos elementos de los vértices de una gráfica, entonces en el ejemplo anterior $r = 2$.

A continuacuón enunciaremos otro caso particular del principio de Ramsey en su versión finita que se usará en la siguiente sección para demostrar el teorema de Schur.

Proposición 3.2 *Sea k un entero positivo. Existe un entero positivo mínimo $R = R(3, k)$ tal que para toda k-coloración en las aristas de la gráfica completa K_R, existe una subgráfica completa K_3 monocromática.*

3.2. El teorema de Schur

Consideremos la ecuación $z = x + y$. Sabemos que el conjunto de puntos en $\mathbb{R}^3$ que satisfacen tal ecuación es un plano. Sea P el conjunto de puntos en ese plano cuyas coordenadas son números enteros positivos, por ejemplo $(1, 1, 2)$ y $(3, 4, 7)$ (nótese que no necesariamente $x \neq y$). Usando ahora una cantidad finita de colores, coloreamos el conjunto de los números enteros. Para cada $(a, b, c) \in P$ hacemos lo siguiente: si los colores de a, b y c son iguales decimos que (a, b, c) es monocromático, en otro caso marcamos el

punto (a, b, c) con una X. La pregunta es: ¿será posible dar una coloración de los enteros de modo que todos los puntos de P queden marcados con una X? o ¿para toda coloración de los enteros siempre hay un punto monocromático?

Esta pregunta fue contestada por Issai Schur en 1916, en el segundo resultado tipo Ramsey. Schur, al responder esta pregunta, no estaba motivado por la idea de colorear puntos en el plano, su interés más bien era demostrar un teorema que, en su perspectiva, le ayudaría a demostrar una de las más famosas y trabajadas conjeturas de todos los tiempos: "El último teorema de Fermat". El teorema que Schur demostró fue:

Teorema 3.6 ***(I. Schur, 1916)***. *Sea $n \geq 1$. Existe un número primo q tal que para todo primo $p \geq q$ la congruencia $x^n + y^n = z^n$ (mód p) tiene solución en los enteros con $xyz \neq 0$ (mód p).*

Para probar esto, Schur se dio cuenta de que necesitaba un "simple lema, que pertenece más a la combinatoria que a la teoría de números". Dicho lema se conoce actualmente como el teorema de Schur.

Teorema 3.7 ***(Teorema de Schur, 1916)***. *Para todo entero $k \geq 1$, existe un entero positivo mínimo $s = s(k)$, tal que en toda k-coloración de $[s]$ existe una solución monocromática a la ecuación $x + y = z$.*

Demostración:

Por la proposición 3.2 sabemos que para todo k existe n tal que toda k-coloración de las aristas de la gráfica completa K_n existe un triángulo monocromático. Sea K_n la gráfica completa con $V(K_n) = \{1, 2, ..., n\}$. Dada χ una k-coloración cualquiera de $V(K_n) = \{1, 2, ..., n\}$ definiremos una coloración $\chi' : E(K_n) \to \{1, 2, ..., k\}$ de una manera especial: a la arista (ij), con $i < j$, le asignamos el color del vértice $j - i$, es decir $\chi'(ij) = \chi(j - i)$. Sabemos que esta coloración tiene un triángulo monocromático. Sean a, b, c los vértices de este triángulo y sin pérdida de generalidad supongamos que $a < b < c$. Las aristas de este triángulo son $(ab), (bc)$ y (ac), entonces $\chi'(ab) = \chi'(bc) = \chi'(ac)$. Luego,

$$\chi(b - a) = \chi(c - b) = \chi(c - a).$$

Si definimos $x = b - a$, $y = c - b$ y $z = c - a$, entonces:

$$\begin{aligned} x + y &= b - a + c - b \\ x + y &= c - a \\ x + y &= z. \end{aligned}$$

Por lo tanto toda k-coloración de $[n]$ contiene una solución monocromática de $x + y = z$.

□

Definición 3.2 *El número $s(k)$ definido en el teorema de Schur se conoce como el* número de Schur. *Una terna $\{x, y, z\}$ que satisface la ecuación $x + y = z$ se llamará terna de Schur.*

Así, el teorema de Schur nos dice que dado un número de colores k, si el intervalo $[n]$ es suficientemente grande, entonces para cualquier k-coloración de $[n]$ existe una terna de Schur monocromática. Notemos que $s(k)$ está definido como el mínimo entero que satisface esto, y todo $n \geq s(k)$ también lo satisface, ya el intervalo $[s(k)]$ está contenido en el intervalo $[n]$ para todo $n \geq s(k)$, entonces para colorear el intervalo $[n]$ debemos colorear primero el intervalo $[s(k)]$.

Para entender mejor el teorema de Schur encontraremos el número de Schur para $1 \leq k \leq 2$.

- $k = 1$**.** Vamos a colorear con un color, digamos rojo. Entonces hay una sola forma de colorear el intervalo $[n]$, que es coloreando todos los números de rojo. Como $\{1, 1, 2\}$ es una terna de Schur, entonces el intervalo $[2]$ contiene siempre una terna de Schur monocromática, entonces $s(1) \leq 2$. Además, $s(1)$ no puede ser 1 ya que en el intervalo $[1]$ no existen ternas de Schur; por lo tanto $s(1) = 2$.

- $k = 2$**.** Vamos a colorear con dos colores, a saber rojo y azul. Veamos que para la siguiente coloración de $[4]$, no existen ternas de Schur monocromáticas:

  $$\{1, 2, 3, 4\}.$$

  Entonces $s(2) > 4$. Ahora veremos que toda 2-coloración de $[5]$ contiene ternas de Schur monocromáticas. Procederemos por contradicción suponiendo que existe una 2-coloración de $[5]$ sin ternas monocromáticas. Sin pérdida de generalidad supongamos que el 1 es rojo. Como el 1 es rojo entonces el 2 debe ser azul, ya que si fuera rojo tendríamos una terna de Schur roja. El 3 puede ser tanto rojo como azul, pero el 4 debe ser rojo, ya que de lo contrario la terna $\{2, 2, 4\}$ sería monocromática. Entonces, nuestra coloración, hasta el momento, sería:

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

Ahora, el 3 debe ser azul pues en otro caso la terna de Schur $\{1, 3, 4\}$ sería monocromática roja. Finalmente, el 5 no puede ser rojo ya que tendríamos una terna de Schur roja: $\{1, 4, 5\}$ pero tampoco puede ser azul ya que tendríamos una terna de Schur azul: $\{2, 3, 5\}$. Entonces para toda 2-coloración de $[5]$ existen ternas de Schur monocromáticas y por lo tanto $s(2) = 5$.

Encontrar los números de Schur es muy difícil, ya que mientras k crece $s(k)$ crece aún más rápido. Los únicos números de Schur que se conocen, aparte de los exhibidos, son: $s(3) = 14$ y $s(4) = 45$. Las mejores cotas que se conoce del número de Schur son las siguientes:

$$\tfrac{3^r+1}{2} \leq s(r) \leq 3r! - 1.$$

En esta tesis trabajaremos con el teorema de Schur, pero visto desde otro punto de vista.

3.3. La teoría anti-Ramsey

Como vimos en los teorema de la teoría de Ramsey, lo que se busca es encontrar estructuras monocromáticas, pero ¿qué pasa si en vez de buscar estructuras monocromáticas buscamos estructuras heterocromáticas? ¿podremos encontrar teoremas análogos a los mencionados anteriormente?

Estas preguntas se hicieron los matemáticos después de ver como proliferaban los teoremas en la teoría de Ramsey. Estas nuevas preguntas pertenecen a una nueva área llamada *teoría anti-Ramsey*. La teoría anti-Ramsey busca encontrar estructuras heterocromáticas en universos coloreados. Esta nueva corriente matemática es reciente y por lo tanto hay mucho trabajo por hacer en ella, teniendo mayor número de resultados en la parte relacionada con la teoría de gráficas.

Al querer traducir los teoremas clásicos tipo Ramsey a esta nueva corriente, cosas muy distintas ocurren y por lo general no existen versiones análogas de ellos en la teoría anti-Ramsey. Un caso de ello es el teorema de Schur, que en la siguiente sección analizaremos.

Dado que, por lo general, no se pueden traducir de manera directa los resultados de la teoría de Ramsey a la teoría anti-Ramsey, en esta última se busca principalmente encontrar condiciones que deban cumplir las coloraciones para asegurar la existencia de estructuras heterocromáticas.

Un ejemplo de ello, es el siguiente resultado, probado por V. Jungić y R. Radoičić en el año 2003.

Teorema 3.8 ***(V. Jungić y R. Radoičić, 2003)*** *Para toda* 3*-coloración equipartita del intervalo* $[3n]$ *existe una solución heterocromática de la ecuación* $x + y = 2z$*.*

En este caso podemos ver que una condición suficiente para que existan soluciones heterocromáticas de la ecuación $x + y = 2z$, es que las clases cromáticas tengan el mismo número de elementos.

Otro resultado similar es el publicado por J. Fox, M. Mahdian, y R. Radoičić en el año 2004.

Teorema 3.9 ***(J. Fox, M. Mahdian y R. Radoičić, 2004)*** *Para toda* 4*-coloración* $[n] = R \cup G \cup Y \cup B$ *tal que:*

$$min\{|R|, |G|, |Y|, |B|\} > \frac{n+1}{6}$$

existe una solución heterocromática de la ecuación $x + y = w + z$*. Y además esta cota es óptima.*

Al igual que en el teorema anterior, este resultado nos proporciona una condición suficiente para garantizar la existencia de soluciones heterocromáticas de la ecuación en cuestión. Má aún, el teorema nos dice que la cota es óptima. Es decir, que si una clase cromática tiene menos elementos de lo indicado, entonces existe una coloración libre con respecto a la ecuación $x + y = w + z$.

3.4. El teorema de Schur en la teoría anti-Ramsey

Como mencionamos anteriormente en la teoría anti-Ramsey, generalmente, los teoremas de la teoría de Ramsey no tienen análogos, y el teorema de Schur no es la excepción, ya que su versión análoga en esta teoría no es cierto.

Si quisiéramos obtener el teorema de Schur desde la perspectiva de la teoría anti-Ramsey, tendríamos que ver si es posible encontrar un número $s' = s'(k)$ tal que para toda k-coloración de $[s']$ siempre existan ternas de Schur heterocromáticas, es decir, para todo intervalo lo suficientemente grandes nunca habría k-coloraciones libres a la ecuación de Schur. Como queremos encontrar ternas de Schur heterocromáticas, debemos colorear con tres colores o más, ya que con menos cantidad nunca obtendremos ternas heterocromáticas. Un ejemplo claro de que no existe $s'(3)$, es decir, que para tres colores siempre podremos encontrar coloraciones libres a la ecuación de Schur no importando que tan grande sea el intervalo, es el siguiente:

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

En este ejemplo no es posible encontrar una terna de Schur heterocromática pues, para que ésta exista, el 2 debe pertenecer a ella, ya que es el único número azul. Podemos observar, por paridad, que si a cualquier rojo le sumamos el dos obtenemos otro rojo, al igual con los verdes. Entonces por esto es imposible encontrar una terna de Schur heterocromática; y además esta coloraciones se puede extender indefinidamente coloreando los números pares de color verde y los números impares de color rojo. Por lo tanto el teorema de Schur no tiene su versión análoga exacta en esta corriente. Además, como dijimos anteriormente, para todo número de colores, siempre podremos encontrar coloraciones de libres a la ecuación de Schur para intervalos de números de enteros positivos muy grandes. Una prueba de ello es la siguiente proposición.

Proposición 3.3 *Sea* $c : [n] \to \{1, 2, ..., k\}$, *con* $n \geq 2^{k-1}$ *definida como:*

$$c(a) = \begin{cases} i & \text{si } a \equiv 2^{i-1} \text{ (mód } 2^i\text{)}, \\ 1 & \text{en otro caso} \end{cases}$$

entonces c *es libre con respecto a la ecuación de Schur.*

Demostración:

Primero demostraremos que c está bien definida, es decir, todo elemento de $[n]$ se le asigna exactamente un color. Después probaremos que c es libre.

Para demostrar que c está bien definida procederemos por contradicción. Supongamos que existe $a \in [n]$ tal que $c(a) = i$ y $c(a) = j$ con $i \neq j$. Sin pérdida de generalidad supongamos que $i > j$, entonces tenemos dos casos:

- $a \equiv 2^{i-1}$ (mód 2^i) y $a \equiv 2^{j-1}$ (mód 2^j).

  Como $a \equiv 2^{i-1}$ (mód 2^i) y $a \equiv 2^{j-1}$ (mód 2^j) entonces existen $h_1, h_2 \in \mathbb{Z}$ tales que $2^i h_1 = a - 2^{i-1}$ y $2^j h_2 = a - 2^{j-1}$. Como $i > j$ entonces existe $d \geq 0$ tal que $i = j + d$, por consiguiente tenemos que:

$$\begin{aligned} 2^i h_1 + 2^{i-1} &= 2^j h_2 + 2^{j-1} \\ 2^{j+d} h_1 + 2^{(j+d)-1} &= 2^j h_2 + 2^{j-1} \\ 2^{j-1}(2^{d+1} h_1 + 2^d) &= 2^{j-1}(2h_2 + 1) \\ 2^{d+1} h_1 + 2^d &= 2h_2 + 1 \end{aligned}$$

  lo cual nos dice que un número par es igual a un número impar y por ende es una contradicción.

- $a \equiv 2^{i-1}$ (mód 2^i) y $c(a) = 1$

  En este caso podemos ver que $i > 1$ ya que si $i = 1$ entonces $c(a) = 1$. Si a es impar implica que $a \equiv 1$ (mód 2), es decir, $i = 1$. Supongamos que a es par. Para que $c(a) = 1$, necesariamente $a \equiv 2^m$ (mód 2^{m+1}) con $m > k$. Entonces este caso es análogo al anterior, y por lo tanto c está bien definida.

Ahora demostraremos que c es libre. De igual manera procederemos por contradicción.

Supongamos que $\{x, y, z\}$ es una terna de Schur heterocromática, entonces existen i, j, l distintos, tales que $c(x) = i$, $c(y) = j$ y $c(z) = l$, luego $x \equiv 2^{i-1}$ (mód 2^i), $y \equiv 2^{j-1}$ (mód 2^j) y $z \equiv 2^{l-1}$ (mód 2^l). Lo anterior nos implica que existen h_1, h_2, h_3 en $\mathbb{Z}$ tales que $2^i h_1 = x - 2^{i-1}$, $2^j h_2 = y - 2^{j-1}$ y $2^l h_3 = z - 2^{l-1}$. Sin pérdida de generalidad supongamos que $i > j > l$, entonces existen $d_1, d_2 \geq 1$ tales que $i = l + d_1$ y $j = l + d_2$. Entonces tenemos que:

$$\begin{aligned}
x + y &= z \\
(2^i h_1 + 2^{i-1}) + (2^j h_2 + 2^{j-1}) &= 2^l h_3 + 2^{l-1} \\
2^{l+d_1} h_1 + 2^{(l+d_1)-1} + 2^{l+d_2} h_2 + 2^{(l+d_2)-1} &= 2^l h_3 + 2^{l-1} \\
2^{l-1}(2^{d+1} h_1 + 2^{d_1} + 2^{d+1} h_2 + 2^{d_2+1}) &= 2^{l-1}(2h_3 + 1) \\
2^{d+1} h_1 + 2^{d_1} + 2^{d+1} h_2 + 2^{d_2+1} &= 2h_3 + 1
\end{aligned}$$

lo cual nos dice que un número par es igual a un número impar y por ende es una contradicción y por lo tanto c es libre con respecto a la ecuación de Schur.

□

Para ilustrar esta proposición, veamos los siguientes ejemplos.

Ejemplo 17 *Las siguientes coloraciones son libres a la ecuación de Schur.*

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

El no encontrar el equivalente del teorema de Schur en la teoría anti-Ramsey no es el fin del mundo, ya que nos podemos hacer otro tipo de preguntas, como por ejemplo:

1. ¿Cómo es la estructura de las coloraciones libres a la ecuación de Schur?

2. ¿Sucede lo mismo en otros universos algebraicos?

3. ¿Qué pasa con soluciones de otras ecuaciones, además de la de Schur?

Con respecto a la segunda pregunta, nos referimos a estudiar otros universos algebraicos además del intervalo $[n]$, particularmente el conjunto de números naturales $\mathbb{N}$, grupos cíclicos $\mathbb{Z}_n$ o grupos abelianos en general. Con respecto a la tercera pregunta, en esta tesis, nos vamos a limitar a estudiar ecuaciones lineales.

La mayoría de los resultados de tipo anti-Ramsey aritmético que se encuentran en la literatura nos dicen que una característica para que una coloración no sea libre es que tenga todas sus clases cromáticas suficientemente grandes. Por ejemplo, Alekseev y Savchev en 1987 demostraron lo siguiente.

Teorema 3.10 ***(Alekseev y Savchev, 1987)*** *Toda* 3*-colaración equipartita del intervalo* $[3n]$ *contiene soluciones heterocromáticas de la ecuación de Schur.*

Este teorema nos dice que no existen 3-coloraciones de $[3n]$ con $|A| = |B| = |C| = n$ que sean libres. En otras palabras, podemos asegurar la existencia de ternas de Schur heterocromáticas en todas las coloraciones equipartitas , pero ¿necesariamente deben tener las clases cromáticas la misma cardinalidad para asegurar la existencia de ternas de Schur heterocromáticas? es decir ¿se puede relajar la condición equipartita? Esta pregunta fue resuelta en 1990 por Schönheim; quien demostró que no existen coloraciones libres de ternas de Schur con las tres clases cromáticas de cardinalidad mayor que $n/4$.

Teorema 3.11 ***(Schönheim,1990)*** *Para toda* 3*-coloración de* $[n] = R \cup B \cup G$*, tal que:*

$$min\{|R|, |G|, |B|\} > \tfrac{n}{4},$$

existe una terna de Schur heterocromática. Además la cota es óptima

Como podemos ver, esta proposición relajó la condición de que la coloración debe ser equipartita, y no sólo eso, sino que además, como vimos en la sección anterior, al decir que es óptima la cota nos dice que si una clase cromática tiene menos elementos entonces existe una coloración donde

no hay ternas de Schur heterocromáticas. En la siguiente proposición demostraremos que en efecto la cota del teorema 3.11 es óptima. Para ello, exhibiremos coloraciones libres de ternas de Schur heterocromáticas con la cardinalidad de la clase cromática más pequeña igual a $\frac{n}{4}$. Como es usual, para todo $x \in \mathbb{R}$, *el piso* de x, denotado por $\lfloor x \rfloor$, es el entero más grande que es menor que o igual a x, es decir:

$$\lfloor x \rfloor = m\acute{a}x\{k \in \mathbb{Z} | k \leq x\};$$

y *el techo* de x, denotado por $\lceil x \rceil$, es el entero más pequeño que es mayor que o igual a x, es decir:

$$\lceil x \rceil = m\acute{i}n\{k \in \mathbb{Z} | k \geq x\}.$$

Proposición 3.4 *Sea $n \geq 1$ un entero fijo. Existe una 3-coloración de $[n]$ libre con respecto a la ecuación de Schur con clases cromáticas:*

$$|A| = \lceil \tfrac{n}{2} \rceil,\ |B| = \lfloor \tfrac{n}{4} \rfloor,\ |C| = \lfloor \tfrac{n+2}{4} \rfloor$$

Demostración:

Consideremos la siguiente coloración $c : [n] \to \{A, B, C\}$ definida por:

$$c(i) = \begin{cases} A & \text{si } i \text{ es impar,} \\ B & \text{si } i \leq \frac{n}{2} \text{ e } i \text{ es par,} \\ C & \text{si } i > \frac{n}{2} \text{ e } i \text{ es par.} \end{cases}$$

Primero demostraremos que la coloración c es libre de ternas de Schur heterocromáticas, y después demostraremos que sus clases cromáticas tienen las cardinalidades que se indican.

Para demostrar que c es libre, consideramos $\{x, y, z\} \subset [n]$ tal que $x + y = z$. Si z es impar entonces z pertenece a A. Por paridad, tenemos que alguno de x, y es impar y por lo tanto pertenece a A, entonces la terna $\{x, y, z\}$ no puede ser heterocromática. Ahora supongamos que z es par. Por paridad tenemos que ó x, y son pares ó x, y son impares. Si x, y son impares entonces los dos pertenecen a A y por lo tanto la terna $\{x, y, z\}$ no puede ser heterocromática. Si x, y son pares entonces en la terna $\{x, y, z\}$ no hay algún elemento de la clase cromática A y por lo tanto no puede ser heterocromática. Por lo tanto c es libre con respecto a la ecuación de Schur.

Ahora demostraremos que las clases cromáticas de c tienen las cardinalidades que se indican en la proposición.

- $n \equiv 0$ (mód 4).
  En este caso vemos que n es múltiplo de 4. Entonces tenemos que la mitad de los números en el intervalo $[n]$ son impares, luego $|A| = \frac{n}{2} = \lceil \frac{n}{2} \rceil$. Como n es divisible por 4 entonces en el intervalo $[\frac{n}{2}]$ tenemos que la mitad de los números son pares, y por lo tanto $|B| = \frac{n}{4} = \lfloor \frac{n}{4} \rfloor$. Ahora $|C| = [n] - |A| - |B| = n - \frac{n}{2} - \frac{n}{4} = \frac{n}{4}$. Pero $\lfloor \frac{n+2}{4} \rfloor = \lfloor \frac{n}{4} + \frac{2}{4} \rfloor = \frac{n}{4}$.

- $n \equiv 1$ (mód 4).
  En este caso vemos que $n = 4k + 1$, con $k \in \mathbb{Z}$, lo que nos implica que n es impar y también que $n - 1$ es múltiplo de 4. Entonces en el intervalo $[n-1]$ hay $\frac{n-1}{2}$ números impares y como n es impar, entonces en $[n]$ hay $\frac{n-1}{2} + 1 = \frac{n+1}{2}$ números impares. Como $n + 1$ es múltiplo de 2, vemos que $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$, Por lo tanto $|A| = \lceil \frac{n}{2} \rceil$.

  Como n no es múltiplo de 2, entonces $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$. En el intervalo $[\frac{n-1}{2}]$ hay $\frac{n-1}{4}$ números pares. Luego $\lfloor \frac{n}{4} \rfloor = \frac{n-1}{4}$, ya que $n - 1$ es múltiplo de 4. Por lo tanto $|B| = \lfloor \frac{n}{4} \rfloor$.

  Por lo anterior tenemos que $|C| = n - \frac{n+1}{2} - \frac{n-1}{4} = \frac{n-1}{4}$. Como $n + 2$ no es múltiplo de 4, entonces $\lfloor \frac{n+2}{4} \rfloor = \lfloor \frac{n}{4} \rfloor = \frac{n-1}{4}$. Por lo tanto $|C| = \lfloor \frac{n+2}{4} \rfloor$.

- $n \equiv 2$ (mód 4.)
  En este caso tenemos que $n = 4k + 2$, con $k \in \mathbb{Z}$, lo que nos implica que n es múltiplo de 2 pero no de 4. Entonces en el intervalo $[n]$ hay $\frac{n}{2}$ números impares. Luego $\lceil \frac{n}{2} \rceil = \frac{n}{2}$ y por lo tanto $|A| = \lceil \frac{n}{2} \rceil$.

  Como $n = 4k + 2$, entonces $\frac{n}{2} = 2k + 1$, lo que implica que $\frac{n}{2}$ es impar. Como $\frac{n}{2}$ es impar, entonces en el intervalo $[\frac{n}{2}]$ hay $\frac{n-2}{4}$ números pares. Como $n - 2$ es múltiplo de 4, entonces $\lfloor \frac{n}{4} \rfloor = \frac{n-2}{4}$. Por lo tanto $|B| = \lfloor \frac{n}{4} \rfloor$.

  Por lo anterior tenemos que $|C| = n - \frac{n}{2} - \frac{n-2}{4} = \frac{n+2}{4}$. Como $n + 2$ es múltiplo de 4, entonces $\lfloor \frac{n+2}{4} \rfloor = \frac{n+2}{4}$. Por lo tanto $|C| = \lfloor \frac{n+2}{4} \rfloor$.

- $n \equiv 3$ (mód 4.)
  En este caso vemos que $n = 4k + 3$, con $k \in \mathbb{Z}$, por consiguiente n es impar, $n - 1$ es par y $n - 3$ múltiplo de 4. Lo anterior nos implica que en el intervalo $[n - 1]$ hay $\frac{n-1}{2}$ números impares, entonces en $[n]$ hay $\frac{n-1}{2} + 1 = \frac{n+1}{2}$ números impares. Como n no es múltiplo de 2, vemos que $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$, y por lo tanto $|A| = \lceil \frac{n}{2} \rceil$.
  Como n es impar, entonces $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ y por lo tanto en el intervalo $[\frac{n}{2}]$ hay $\lfloor \frac{n-1}{4} \rfloor = \frac{n-3}{4}$ números pares, ya que $n - 1$ es impar. Como $n - 3$ es múltiplo de 4, entonces $\lfloor \frac{n}{4} \rfloor = \frac{n-3}{4}$ y por lo tanto $|A| = \lfloor \frac{n}{4} \rfloor$.

Por lo anterior tenemos que $|C| = n - \frac{n+1}{2} - \frac{n-3}{4} = \frac{n+1}{4}$. Como $n+1$ es múltiplo de 4, entonces $\lfloor \frac{n+2}{4} \rfloor = \frac{n+1}{4}$ y por lo tanto $|C| = \lfloor \frac{n+2}{4} \rfloor$.

□

A continuación damos ejemplos particulares de las coloraciones descritas en la prueba anterior.

Ejemplo 18 *Las siguientes* 3*-coloraciones son libres con respecto a la ecuación de Schur:*

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

Capítulo 4

Teoría anti-Ramsey en otros universos

En el capítulo anterior vimos que los primeros resultados en la teoría anti-Ramsey aritmética se efectuaron en intervalos de enteros positivos, ya que los teoremas importantes en la teoría de Ramsey también fueron estudiados en este tipo de intervalos. Como dijimos en el capítulo anterior es natural e interesante preguntarnos si dichos trabajos se pueden extender a otras estructuras algebraicas, tales como $\mathbb{N}$, $\mathbb{Z}_n$ ó $\mathbb{Z}_p$.

4.1. Resultados en $\mathbb{N}$ y $\mathbb{Z}_n$

En el año 2001, en la sesión de problemas del Seminario de Combinatoria de MIT, Rados Radoicic propuso la siguiente pregunta:

¿Será cierto que toda 3–coloración equipartita del intervalo $[3n]$ contiene una solución heteraocromática a la ecuación $x + y = 2z$?

Como vimos en el capítulo anterior, la respuesta es afirmativa. Sin embargo, antes de ser probado tal resultado, se demostró su versión infinita [4]. Es decir, Jungic, Fox, Mohammad, Nešetril y Radoicic, estudiaron primero la siguiente pregunta:

¿Será cierto que toda 3–coloración equipartita de $\mathbb{N}$ contiene una progresión artitmética de longitud tres heterocromática?

La respuesta a esta pregunta también es afirmativa, es decir, toda 3-coloración equipartita de $\mathbb{N}$ contiene una progresión artitmética de longitud

tres heterocromática. Más aún, los autores probaron un teorema más fuerte. Pero antes de mencionarlo, definiremos el concepto de "densidad"de una clase cromática.

Definición 4.1 *Sea c una k-coloración de $\mathbb{N}$ y A una clase cromática de c. Se dice que A tiene* densidad d *si*

$$\lim_{n\to\infty} \frac{|[n] \cap A|}{n} = d$$

Para entender mejor el concepto de densidad veamos el siguiente ejemplo

Ejemplo 19 *Consideremos la siguientes 3-coloraciones de $\mathbb{N}$:*

$$c(i) = \begin{cases} 1 & si\ a \equiv 1\ (mód\ 3), \\ 2 & si\ a \equiv 3\ (mód\ 3), \\ 3 & si\ a \equiv 0\ (mód\ 3). \end{cases}$$

En esta coloración podemos ver que cada clase cromática representa un tercio de $\mathbb{N}$, es decir, cada clase cromática tiene densidad igual a $\frac{1}{3}$.

ii)

$$c(i) = \begin{cases} 1 & si\ a \equiv 1,2,3\ (mód\ 6), \\ 2 & si\ a \equiv 4,5\ (mód\ 6), \\ 3 & si\ a \equiv 6\ (mód\ 6). \end{cases}$$

En esta coloración podemos ver que la clase cromática X_1 tiene densidad $\frac{1}{2}$, la clase cromática X_2 tiene densidad $\frac{1}{3}$ y por último la clase cromática X_3 tiene densidad $\frac{1}{6}$.

En estos ejemplos podemos observar que cuando nos referimos a densidad, estamos hablando de qué tanta parte de los números naturales estamos metiendo en cada clase cromática.

Ahora sí enunciaremos el teorema, anteriormente mencionado

Teorema 4.1 (Jungic, Fox, Mohammad, Nešetril y Radoicic, 2003) *En toda 3-coloración del conjunto de los número naturales $\mathbb{N}$, cuyas clases cromáticas tienen densidad mayor que $\frac{1}{6}$, existe una solución heterocromática a la ecuación $x + y = 2z$.*

Este teorema es equivalente a decir que si una 3-coloración es libre con respecto a la ecuación $x+y = 2z$, entonces una de sus clases cromática tiene densidad menor o igual a $\frac{1}{6}$.

Notemos que el análogo del teorema no es cierto, es decir, existen 3-coloraciones con soluciones heterecromáticas a la ecuación $x+y=2z$, donde alguna clase cromática tiene densidad menor o igual a $\frac{1}{6}$. Un ejemplo de ello es la segunda coloración del ejemplo 19, ya que $2 \in X_1$, $4 \in X_2$ y $6 \in X_3$. Como corolario al teorema 4.1 se obtiene el siguiente resultado.

Teorema 4.2 *Para toda 3-coloración de $\mathbb{Z}_n = A \cup B \cup C$, con*

$$\text{mín}(|A|, |B|, |C|) > \frac{n}{6}$$

existe una solución heterocromática de la ecuación $x + y = 2z$.

Demostración:

Sea $c : \mathbb{Z}_n \to \{A, B, C\}$ una 3-coloración de Z_n, con $\text{mín}(|A|, |B|, |C|) > \frac{n}{6}$. Definamos una 3-coloración $\overline{c}$ de $\mathbb{N}$ como sigue: $\overline{c}(i) = c(i \pmod n)$. Recordemos que $\mathbb{Z}_n$ es la colección de las clases de equivalencia módulo n, entonces la coloración $\overline{c}$ lo único que está haciendo es coloreando todos los elementos de la clase de congruencia $[i]$ del mismo color. Como la cardinalidad de cada clase cromática en c es mayor a $\frac{n}{6}$, entonces cada clase cromática de $\overline{c}$ tiene densidad mayor a $\frac{1}{6}$.

Por el teorema 4.1, tenemos que en la coloración c existe una solución heterocromática a la ecuación $x+y=2z$. Pero recordemos que la coloración $\overline{c}$ coloreaba todos los elementos de una clase de congruencia módulo n del mismo color, entonces existen $x, y, z \in \mathbb{Z}_n$ pertenecientes a clases cromáticas distintas tales que $x + y = 2z$.

□

Al igual que en los teoremas del capítulo anterior, podemos ver que para asegurar la existencia de soluciones heterocromáticas, las clases cromáticas deben de ser suficientemente grandes. La primera pregunta natural que surgió a partir del teorema anterior fue:

¿Cuándo la condición $\text{mín}(|A|, |B|, |C|) > \frac{n}{6}$ se puede relajar?

Es decir ¿para que valores de n se puede obtener una cota más pequeña? Lo primero que se demostró fue que para n múltiplo de 6 la condición es óptima. La siguiente contrucción muestra que, en efecto, cuando n es múltiplo de 6 la cota es óptima.

Proposición 4.1 *Sea $c : \mathbb{Z}_n \to \{A, B, C\}$ una 3-coloración de $\mathbb{Z}_n$, donde $n \equiv 0$ (mód 6), definida como:*

$$c(i) = \begin{cases} A & \text{si } i \equiv 1, 2, 4, 5 \pmod 6, \\ B & \text{si } i \equiv 3 \pmod 6, \\ C & \text{si } i \equiv 0 \pmod 6. \end{cases}$$

entonces c es una coloración libre con respecto a la ecuación $x + y = 2z$ *y además* $min\{|A|, |B|, |C|\} = \frac{n}{6}$.

Demostración:

Claramente $|A| = \frac{4}{6}$ y $|B| = |C| = \frac{n}{6}$. Demostraremos que c es libre con respecto a la ecuación $x + y = 2z$. Sea $\{x, y, z\} \subset \mathbb{Z}_n$ una solución de $x + y = 2z$.

i) Si $z \in C$, entonces $z \equiv 0$ (mód 6), luego $2z \equiv 0$ (mód 6). Las sumas posibles, módulo 6, entre elementos de A y B nunca nos darán 0, ya que $1+3 \equiv 4$ (mód 6), $2+3 \equiv 5$ (mód 6), $4+3 \equiv 1$ (mód 6), $5+3 \equiv 2$ (mód 6). Por lo tanto en este caso no existe solución heterocromáticas de la ecuación $x + y = 2z$.

ii) $z \in B$.
Como $z \in C$, entonces $z \equiv 3$ (mód 6). luego $2z \equiv 0$ (mód 6). Las sumas posibles, entre un elemento de A y un elemento de C nunca nos darán 0, ya que $1 + 0 = 1$ (mód 6), $2 + 0 = 2$ (mód 6), $4 + 0 = 4$ (mód 6) y $5 + 0 = 0$ (mód 6). Por lo tanto en este caso no existe solución heterocromáticas de la ecuación $x + y = 2z$.

iii) $z \in A$.
Como $z \in C$, entonces $z \equiv 1$ (mód 6), $z \equiv 2$ (mód 6), $z \equiv 4$ (mód 6) ó $z \equiv 5$ (mód 6), luego $2z \equiv 2$ (mód 6), $z \equiv 4$ (mód 6), $z \equiv 2$ (mód 6) ó $2z \equiv 4$ (mód 6). La única suma posible entre un elemento de B y un elemento de C es $0 + 3$, podemos ver que esta suma no nos da ninguna opción factible (mód 6), entonces en este caso no existe solución heterocromáticas de la ecuación $x + y = 2z$a y por lo tanto c es libre con respecto a la ecuación $x + y = 2z$.

□

En la figura **??** se muestran ilustraciones de la coloración descrita anteriormente para los casos de $n = 6$ y $n = 12$.

Cuando n no es múltiplo de 6, se pueden usar las propiedades algebraicas de $\mathbb{Z}_n$ para mejorar el teorema 4.2. Un ejemplo de ello es el siguiente teorema:

Teorema 4.3 (Jungic, Fox, Mohammad, Nešetril y Radoicic, 2003) *Sea n un entero impar y sea q el divisor primo más pequeño de n. Entonces, para toda* 3*-coloración* $\mathbb{Z}_n = A \cup B \cup C$*, con*

$$\text{mín}(|A|, |B|, |C|) > \frac{n}{q},$$

existe una solución heterocromática de la ecuación $x + y = 2z$.

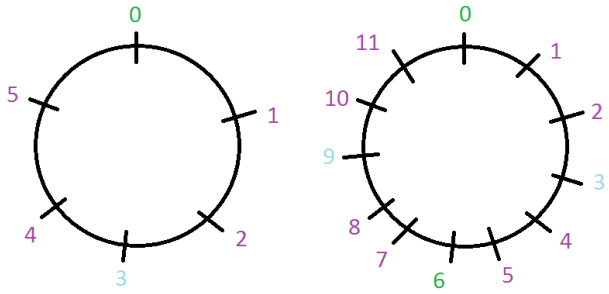


Figura 4.1: $\mathbb{Z}_6$ y $\mathbb{Z}_{12}$

En otras palabras, lo que nos dice este resultado es que, para n impar en los casos en que q (el divisor primo más pequeño de n) sea 3 ó 5, la cota de $\frac{1}{6}$ del teorema 4.2 se puede mejorar. Para facilitar la comprensión de este tipo de resultados veamos la siguiente definición.

Definición 4.2 *Sea n un entero positivo. Definimos $m(n)$ como el mayor entero positivo tal que existe una 3-coloración de $\mathbb{Z}_n = A \cup B \cup C$, con $\min\{|A|, |B|, |C|\} = m(n)$, libre con respecto a la ecuación $x + y = 2z$.*

Utilizando esta notación, lo siguiente es un resumen de lo que hemos visto:

- Teorema 4.2 $\Rightarrow m(n) \leq \frac{n}{6}$ para toda n.
- Proposición 4.1 $\Rightarrow m(n) \geq \frac{n}{6}$ para $n \equiv 0$ (mód 6).
- Teorema 4.2 + Proposición 4.1 $\Rightarrow m(n) = \frac{n}{6}$ para $n \equiv 0$ (mód 6).
- Teorema 4.3 $\Rightarrow m(n) \leq \frac{n}{q}$ para toda n impar, donde q es el divisor primo más pequeño de n.
- Teorema 4.2 + Teorema 4.3 $\Rightarrow m(n) \leq \min\{\frac{n}{6}, \frac{n}{q}\}$ para toda n impar, donde q es el divisor primo más pequeño de n.

El encontrar el valor exacto de $m(n)$ para toda n resultó ser un problema interesante, el lector interesado puede consultar "The structure of rainbow-free colorings for linear equations on three variables in $\mathbb{Z}_p$"[3]. En este trabajo de tesis nos restringiremos al caso en que n es un número primo, es decir, trabajaremos con el grupo abeliano $\mathbb{Z}_p$.

4.2. El grupo abeliano de orden primo: $\mathbb{Z}_p$

Para comenzar, veamos qué nos dice el teorema 4.3 en el caso en que n es un número primo. Observese que si $n = p$ número primo, entonces $q = p$ y $\frac{p}{q} = 1$.

Teorema 4.4 (Jungic, Fox, Mohammad, Nešetril y Radoicic, 2003) *Sea p primo. Entonces, para toda 3-coloración $\mathbb{Z}_p = A \cup B \cup C$, con*

$$\text{mín}(|A|, |B|, |C|) > 1$$

existe una solución heterocromática de la ecuación $x + y = 2z$.

Lo que nos dice el resultado anterior es que en $\mathbb{Z}_p$ las 3-coloraciones libres a la ecuación $x + y = 2z$, si es que existen, deben tener al menos una clase cromática de cardinalidad uno. En otras palabras, $m(p) \leq 1$ para todo p primo.

En la teoría de Ramsey es común que se utilicen como herramienta teoremas clásicos de la *teoría Aditiva de Números.* En la teoría anti-Ramsey, recientemente también se ha demostrado que estas herramientas son muy útiles. En el capítulo siguiente estudiaremos tales herramientas.

Con estas técnicas se probó recientemente un resultado que caracteriza las 3-coloraciones de $\mathbb{Z}_p$ libres con respecto a cualquier ecuación de 3 variables [3] El teorema que nos habla de esto es muy complejo y como en este trabajo de tesis solamente trabajaremos con la ecuación de Schur, no hace falta enunciarlo.

Como trabajaremos con la ecuación de Schur, nos es importante preguntarnos si existe un teorema en $\mathbb{Z}_p$ análogo al teorema de Schur, es decir, ¿será cierto que para cualquier 3-coloración de $\mathbb{Z}_p$ existe una terna de Schur heterocromática? La respuesta a esa pregunta es no; y los siguientes son ejemplos de ello:

Ejemplo 20 *$\mathbb{Z}_7 = A \cup B \cup C$, con $A = \{0\}$, $B = \{1, 2, 5, 6\}$ y $C = \{3, 4\}$ no contiene ternas de Schur heterocromáticas.*

Ejemplo 21 *$\mathbb{Z}_{11} = A \cup B \cup C$, con $A = \{0\}$, $B = \{1, 3, 8, 10\}$ y $C = \{2, 4, 5, 6, 7, 9\}$ no contiene ternas de Schur heterocromáticas.*

Como podemos ver en estos ejemplos, para que no haya ternas de Schur heterocromáticas, necesariamente una clase cromática debe ser muy pequeña, de hecho observemos que en los dos ejemplos anteriores la clase cromática más pequeña siempre es $\{0\}$.

Para saber cómo deben de ser las 3-coloraciones para que existan ternas de Schur heterocromáticas se deben estudiar las coloraciones libres, ya que son éstas las que no nos permiten un teorema análogo al teorema de Schur.

El resultado principal de este trabajo de tesis es el siguiente teorema que nos exhibe la estructura de las clases cromáticas en una 3-coloración de $\mathbb{Z}_p$ libre con respecto a la ecuación de Schur.

Teorema 4.5 *Una 3-coloración de* $\mathbb{Z}_p = A \cup B \cup C$ *es libre si y sólo si* $A = \{0\}$, $B = -B$ *y* $C = -C$

Este resultado es un caso particular de dos teoremas que se encuentran en la literatura [3],[7]. La aportación de este trabajo de tesis será proporcionar una demostración alterna utilizando también los teoremas de la teoría aditiva de números, pero dichos teoremas se abordarán desde la perspectiva de un concepto nuevo que introduciremos en el siguiente capítulo.

Capítulo 5

Teoría aditiva de números versión tríos

En este capítulo abordaremos los elementos necesarios de la teoría aditiva de números que usaremos para demostrar el teorema principal de este trabajo de tesis. Empezaremos por definir el conjunto suma de dos o más conjuntos y demostraremos sus propiedades más elementales. Después definiremos el concepto de trío, el cuál, es el concepto más importante en esta tesis, ya que con él se dará una demostración original del teorema principal. Y finalmente enunciaremos los teoremas clásicos de la teoría aditiva de números; que son el teorema de "Cauchy-Davenportz el teorema de "Vosper". Enunciaremos dichos teoremas en sus versiones clásicas y una nueva versión construida a partir del concepto de trío; veremos que las dos versiones de los teoremas son equivalentes; y por último se demostrarán sólo la versiones trío.
Todo el material contenido en este capítulo fue consultado del artículo "A New Proof of Kemperman's Theorem"[1], y del artículo "Una nueva mirada a cuatro teoremas clásicos en teoría aditiva de números"[8].

5.1. Definiciones

Definición 5.1 *Sea G un grupo y $A_i \subseteq G$, con $1 \leq i \leq n$. Al conjunto $A_1 + A_2 + ... + A_n = \{a_1 + a_2 + ... + a_n \mid a_i \in A_i\}$ se le conoce como el* conjunto suma *de $A_1, A_2, ..., A_n$.*

Ejemplo 22 *Sean $A, B, C \subseteq \mathbb{Z}_7$, $A = \{0, 1\}$, $B = \{2, 3\}$, $C = \{1, 3\}$, entonces $A + B + C = \{3, 4, 5, 6, 0\}$.*

De aquí en adelante trabajaremos sólo con el grupo cíclico $\mathbb{Z}_p$ de orden primo.

Definición 5.2 *Dado $g \in \mathbb{Z}_p$, al conjunto suma $A + \{g\}$ se le denota como $A + g$ y se dice que es una* traslación *de A.*

Ejemplo 23 *Sea $A \subseteq \mathbb{Z}_{11}$ y $g \in \mathbb{Z}_{11}$, con $A = \{1, 2, 3\}$ y $g = 5$, entonces $A + g = \{6, 7, 8\}$.*

Definición 5.3 *Sea $A \subseteq \mathbb{Z}_p$, entonces se define $-A = \{-a \mid a \in A\}$.*

Ejemplo 24 *Sea $A \subseteq \mathbb{Z}_{23}$ $A = \{1, 3, 15, 18\}$ entonces $-A = \{22, 20, 8, 5\}$.*

Como podemos ver en los pasados ejemplos la cardinalidad de A, de $-A$, y de $A + g$ es la misma, así que esa es nuestra primera proposición.

Proposición 5.1 *Sea $A \subseteq \mathbb{Z}_p$ y $g \in \mathbb{Z}_p$, entonces $|A| = |-A| = |A + g|$.*

Demostración:

Demostraré que existe una biyección entre A y $-A$. Sea $\phi : A \longrightarrow -A$ definida como $\phi(a) = -a$. Para confirmar la inyectividad tomamos $x, y \in A$ tales que $\phi(x) = \phi(y)$ entonces:

$$\begin{aligned} -x &= -y \\ x - y &= 0 \\ x + (-y) &= 0 \end{aligned}$$

luego $-y$ es el inverso de x y como los inversos son únicos entonces $x = y$. Para verificar la suprayectividad notemos que, por definición de $-A$, para todo $x \in -A$ existe $-x \in A$ tal que $\phi(-x) = -(-x) = x$. Entonces ϕ es biyectiva y por lo tanto $|A| = |-A|$.

Ahora, demostraré que existe una biyección entre A y $A + g$. Sea $\phi : A \longrightarrow A + g$ definida ahora como $\phi(a) = a + g$. Empezaré a verificar la inyectividad de ϕ. Sean $x, y \in A$ tales que $\phi(x) = \phi(y)$, entonces:

$$\begin{aligned} x + g &= y + g \\ x &= y \end{aligned}$$

La suprayectividad se cumple ya que, por definición de $A+g$, si $z \in A+g$ entonces $z = a+g$ para algún $a \in A$, luego $\phi^{-1}(z) = a$. Entonces concluimos que ϕ es biyectiva y por lo tanto $|A + g| = |A|$

□

A continuación enunciaremos el concepto más importante de este trabajo, con el cual trabajaremos a lo largo de toda la tesis. Este concepto fue introducido en "A New Proof of Kemperman's Theorem"[1], con la finalidad de simplificar el enunciado y la prueba del teorema estructural de Kemperman.

Definición 5.4 *Sean $A, B, C \subseteq \mathbb{Z}_p$ no vacíos, si $0 \notin A + B + C$ diremos que (A, B, C) es un* trío.

Ejemplo 25 *Sea $A, B, C \subset \mathbb{Z}_{11}$ con $A = \{1, 2, 3\}$, $B = \{4, 7, 9\}$ y $C = \{7, 8\}$, entonces $A+B+C = \{1, 4, 6, 2, 5, 7, 3, 8, 9\}$, aquí vemos que (A, B, C) es un trío.*

Ejemplo 26 *Sean $A, B, C \subset \mathbb{Z}_{11}$ con $A = \{1, 2\}$, $B = \{4, 5\}$ y $C = \{3, 4\}$ entonces $A + B + C = \{8, 9, 10, 0\}$, aquí vemos que (A, B, C) no es un trío.*

Un pregunta natural es: ¿Dado un trío, cuál es la relación entre los conjuntos que lo conforman? ó ¿En un trío, puedo expresar un conjunto en términos de los otros dos? La respuesta a estas preguntas nos la da la siguiente proposición.

Proposición 5.2 *Si (A, B, C) es un trío en $\mathbb{Z}_p$ entonces:*

1. $A \subseteq G \setminus -(B + C)$
2. $B \subseteq G \setminus -(A + C)$
3. $C \subseteq G \setminus -(B + A)$

Demostración:

Demostraremos 1 por contradicción. Supongamos que $A \nsubseteq G \setminus -(B+C)$, entonces $A \cap -(C + B) \neq \emptyset$. Sea $a \in A \cap -(B + C)$, entonces el elemento $a \in A$ se puede expresar como $a = -(b+c)$ para algún $-(b+c) \in -(B+C)$ con $b \in B$ y $c \in C$, luego $a = -b - c$ entonces $a + b + c = 0$, lo cual es una contradicción ya que (A, B, C) es un trío. Por lo tanto $A \subseteq G \setminus -(B + C)$. Las demostraciones de 2 y 3 son análogas.

□

En esta tesis nos interesa saber la relación que hay entre la cardinalidad del conjunto y las cardinalidades de los conjuntos sumandos y es por eso que definimos lo siguiente.

Definición 5.5 *Sean $A, B \subset \mathbb{Z}_p$. La* deficiencia *de la pareja (A, B) se define como:*

$$\delta(A,B) = |A| + |B| - |A+B|.$$

Ejemplo 27 *Sean $A, B \subseteq \mathbb{Z}_{17}$ con $A = \{0,1,15,16\}$, $B = \{0,1,7\}$. Entonces $A+B = \{0,1,2,5,6,7,8,15,16\}$, aquí la deficiencia de (A,B) es:*

$$\delta(A,B) = |A| + |B| - |A+B| = 4+3-9$$
$$\delta(A,B) = -2$$

Ejemplo 28 *Sean $A, B \subseteq \mathbb{Z}_{11}$ con $A = \{4\}$, $B = \{0,1,7\}$. Entonces $A+B = \{4,5,0\}$, aquí la deficiencia de (A,B) es de:*

$$\delta(A,B) = |A| + |B| - |A+B| = 1+3-3$$
$$\delta(A,B) = 1$$

En en el ejemplo 6 vemos que, respecto a las cardinalidades, el conjunto suma es mucho más grande que los conjuntos que lo formaron, mientras que en el ejemplo 7 pasa al contrario, el conjunto suma es pequeño conforme a las parejas que lo formaron.

Definición 5.6 *Se dice que (A,B) tiene* suma pequeña *o que es* pareja crítica *si $\delta(A,B) > 0$.*

Como dijimos anteriormente estamos interesados en aquellas ternas de conjuntos (A,B,C) llamadas tríos, y en las cardinalidades de los conjuntos que los conforman. Por esta razón extendemos la definición anterior a tríos, aunque a primera vista no parezcan conectadas las dos definiciones más adelante veremos su relación.

Definición 5.7 *La* deficiencia *de un trío (A,B,C) en $\mathbb{Z}_p$ se define como:*

$$\delta(A,B,C) = |A| + |B| + |C| - p$$

Si $\delta(A,B,C) > 0$ entonces el trío es crítico.

5.2. El teorema de Cauchy-Davenport

Un teorema muy importante en la Teoría Aditiva de Números es el *teorema de Cauchy-Davenport* que nos dice qué tan pequeño puede llegar a ser el conjunto suma de una pareja (A,B) respecto a los conjuntos A y B. El siguiente teorema fue probado originalmente por el famoso matemático Augustin Louis Cauchy (1789 -1857). Posteriormente, el mismo resultado, fue redescubierto por Harold Davenport (1907 - 1969). Actualmente, el teorema se conoce como el teorema de Cauchy-Davenport.

Teorema 5.1 ***(Teorema de Cauchy-Davenport, versión clásica)*** *Sean A y B subconjuntos no vacíos de $\mathbb{Z}_p$, entonces:*

$$|A+B| \geq \text{mín}\{p, |A|+|B|-1\}.$$

Lo que nos dice este teorema es que la carnalidad de un conjunto suma $|A+B|$ es mayor o igual a $|A|+|B|-1$ excepto cuando $A+B$ sea todo $\mathbb{Z}_p$. Para entender esto necesitamos la siguiente proposición.

Proposición 5.3 *Sean $A, B \subseteq \mathbb{Z}_p$. Si $|A|+|B| > p$ entonces $A+B = \mathbb{Z}_p$.*

Demostración:

Es claro que $A+B \subseteq \mathbb{Z}_p$. Para demostrar que $\mathbb{Z}_p \subseteq A+B$ sea $g \in \mathbb{Z}_p$ entonces $|g-A| = |A|$. Como $|A|+|B| > p$ entonces $|g-A|+|B| > p$. Por lo anterior y el principio de las casillas tenemos que $(g-A) \cap B \neq \emptyset$, luego existen $a \in A$ y $b \in B$ tales que $g-a = b$, entonces $g = a+b$. Esto es para todo $g \in \mathbb{Z}_p$, lo cual implica que $\mathbb{Z}_p \subseteq A+B$ y por lo tanto $A+B = \mathbb{Z}_p$.

□

Notemos que el regreso de la proposición no es cierto, es decir, que si el conjunto $A+B = \mathbb{Z}_p$, con A,$B \subset \mathbb{Z}_p$, entonces no necesariamente $|A|+|B| > p$. Un ejemplo de esto es el siguiente:

Ejemplo 29 *Sean A,$B \subset \mathbb{Z}_{11}$ con $A = \{0,1,4,7\}$ y $B = \{0,1,2,3\}$. Podemos ver que $A+B = \mathbb{Z}_{11}$ y $|A|+|B| = 8 < p = 11$.*

Ahora sí, con esta proposición podemos enunciar el *teorema de Cauchy-Davenport* de la siguiente manera:

Teorema 5.2 ***(Teorema de Cauchy-Davenport, versión 2.)*** *Sean A y B subconjuntos no vacíos de $\mathbb{Z}_p$ tales que $|A|+|B| \leq p$, entonces:*

$$|A+B| \geq |A|+|B|-1.$$

Más adelante veremos una versión equivalente a estos teoremam utilizando el concepto de trío y daremos su demostración en ese contexto. Antes de eso veamos la equivalencia entre los teoremas 5.1 y 5.2.

Proposición 5.4 *Los teoremas 5.1 y 5.2 son equivalentes.*

Demostración:

Primero demostraré que el teorema 5.1 implica al teorema 5.2. Sean A, B subconjuntos no vacíos de $\mathbb{Z}_p$ tales que $|A|+|B| \leq p$. Por el teorema 5.1 tenemos que:

$$|A+B| \geq \text{mín}\{p, |A|+|B|-1\}$$

Si el mínimo fuera $|A|+|B|-1$ entonces el teorema 5.2 ya se cumple. Supongamos ahora que el mínimo es p, es decir:

$$\begin{aligned} p &\leq |A|+|B|-1 \\ p+1 &\leq |A|+|B| \\ p &< |A|+|B| \end{aligned}$$

Lo cual es una contradicción ya que por hipótesis $|A|+|B| \leq p$, luego el $\text{mín}\{p, |A|+|B|-1\} = |A|+|B|-1$ y por lo tanto el teorema 5.1 implica al teorema 5.2.

Ahora probaré que el teorema 5.2 implica al teorema 5.1. Sean A, B subconjuntos no vacíos de $\mathbb{Z}_p$. Los conjuntos A, B tienen dos opciones: que la suma de sus cardinalidades sea menor o igual a p, es decir, $|A|+|B| \leq p$, o que la suma de sus cardinalidades exceda a p, es decir, $|A|+|B| > p$. A continuación analizaremos las dos opciones:

- Si $|A|+|B| \leq p$ entones por el teorema 5.2:

$$|A+B| \geq |A|+|B|-1 \tag{5.1}$$

- Si $|A|+|B| > p$ entonces por la proposición 5.3 tenemos que:

$$|A+B| = p \tag{5.2}$$

En ambos casos tenemos que $|A+B| \geq \text{mín}\{|A|+|B|-1, p\}$, luego el teorema 5.1 es consecuencia del teorema 5.2, y por lo tanto los dos teoremas son equivalentes.

□

Si la desigualdad estricta se da, es decir, si $|A+B| > |A|+|B|-1$ obtenemos $|A|+|B|-|A+B| < 1$, entonces $\delta(A,B) < 1$, luego la pareja (A,B) no es crítica, lo cual quiere decir que su suma no es pequeña. Si se cumple la igualdad, es decir, $|A+B| = |A|+|B|-1$, despejando obtenemos $|A|+|B|-|A+B| = 1$, entonces $\delta(A,B) = 1$. De lo anterior inferimos que el teorema de Cauchy-Davenport nos dice que una pareja crítica en $\mathbb{Z}_p$ a lo más puede tener deficiencia 1.

Antes de demostrar el *teorema de Cauchy-Davenport (versión tríos)* necesitamos primero definir el concepto de progresión aritmética y probar dos proposiciones.

Definición 5.8 *Sea $A \subseteq \mathbb{Z}_p$. Se dice que A es una* progresión aritmética *con* diferencia *d y k* términos *si $A = \{a + nd \mid 0 \leq n \leq k-1\}$ con $a \in \mathbb{Z}_p$.*

Ejemplo 30 *Sea $A \subseteq \mathbb{Z}_{13}$, con $A = \{1, 4, 5, 8, 11\}$. A primera vista A no parece una progresión aritmética, pero si reescribimos $A = \{5, 8, 11, 1, 4\}$, vemos que A es una progresión aritmética con diferencia 3 y 5 términos que inicia en 5*

Ejemplo 31 *Sea $A \subseteq \mathbb{Z}_{11}$, con $A = \{0, 2, 4, 7, 9\}$. Si reescribimos a A como $A = \{7, 9, 0, 2, 4\}$, vemos que A es una progresión aritmética con diferencia 2 y 5 términos que inicia en 7*

Proposición 5.5 *Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$. Entonces, para todo $g_1, g_2 \in \mathbb{Z}_p$, $(A + g_1, B + g_2, C - (g_1 + g_2))$ también es un trío en $\mathbb{Z}_p$ con $\delta(A, B, C) = \delta(A + g_1, B + g_2, C - (g_1 + g_2))$.*

Demostración:

Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$. Primero demostraré que $(A + g_1, B + g_2, C - (g_1 + g_2))$ es un trío. Supongamos que no lo es, es decir, existen $a + g_1 \in A + g_1$, $b + g_2 \in B + g_2$ y $c - (g_1 + g_2) \in C - (g_1 + g_2)$ tales que:

$$a + g_1 + b - g_2 + c - g_1 - g_2 = 0$$

luego

$$a + b + c = 0$$

lo cual es una contradicción ya que (A, B, C) es un trío.

Ahora demostraremos que $\delta(A, B, C) = \delta(A + g_1, B + g_2, C - (g_1 + g_2))$. Sabemos que:

$$\begin{aligned} |A| &= |A + g_1|, \\ |B| &= |B + g_2|, \\ |C| &= |C - (g_1 + g_2)|, \end{aligned}$$

entonces:

$$\begin{aligned} \delta(A + g_1, B + g_2, C - (g_1 + g_2)) &= |A + g_1| + |B + g_2| + |C - (g_1 + g_2)| - p \\ &= |A| + |B| + |C| - p \\ &= \delta(A, B, C) \end{aligned}$$

y por lo tanto la deficiencia de los tríos es la misma. □

Antes de continuar, recordemos que para todo a y d en $\mathbb{Z}_p$ se verifica que $\{a + nd : n \in \mathbb{N}\} = \mathbb{Z}_p$.

Proposición 5.6 *Sea (A, B, C) un trío en $\mathbb{Z}_p$, con $2 \leq |A| \leq |B| \leq |C|$. Entonces existen $A', B', C' \subseteq \mathbb{Z}_p$ con $2 \leq |A'| \leq |B'| \leq |C'|$ tales que:*

1. $0 \in A' \cap B'$.
2. $A' \setminus B' \neq \emptyset$.
3. (A', B', C') *es un trío con* $\delta(A, B, C) = \delta(A', B', C')$.

Demostración:

La demostración procederá por casos, considerando las tres posibilidades siguientes: **(1)** $A \cap B \neq \emptyset$ y $A \setminus B \neq \emptyset$; **(2)** $A \cap B \neq \emptyset$ y $A \setminus B = \emptyset$; **(3)** $A \cap B = \emptyset$. A continuación verificamos cada uno de estos casos:

Caso (1) Sean $x \in A \cap B$ y $y \in A \setminus B$ (sabemos que estos elementos existen pues $A \cap B \neq \emptyset$ y $A \setminus B \neq \emptyset$). Definimos:

$$\begin{aligned} A' &= A - x, \\ B' &= B - x, \\ C' &= C + 2x. \end{aligned}$$

Notemos que el punto *1* se cumple pues $x - x = 0 \in A' \cap B'$. El punto *2* se cumple pues $y - x \in A'$ y $y - x \notin B'$. El punto *3* es consecuencia de la proposición 5.5 tomando $g_1 = g_2 = -x$.

Caso (2) En este caso tenemos que $A \subseteq B$. Sean a y b, $a < b$, dos elementos distintos de A (sabemos que existen pues $|A| \geq 2$). Para $d = b - a$ consideramos:

$$A_{a,d} = \{a, a + d, a + 2d, ..., a + nd\}$$

la progresión aritmética más larga contenida en A que comienza en a y tiene diferencia d. Sabemos que $n \geq 1$ pues $a + d = b \in A$. De la misma forma, consideramos:

$$B_{a,d} = \{a, b, a + 2d, ..., a + (n + k)d\}$$

la progresión aritmética más larga, que comienza en a y tiene diferencia d, contenida en B. En este caso sabemos que $k \geq 0$, y dado que $B \neq \mathbb{Z}_p$ entonces $a + (n + k + 1)d \notin B$. Notemos que $A_{a,d} \subseteq B_{a,d}$, $|A_{a,d}| = n + 1$ y $|B_{a,d}| = n + 1 + k$. Definimos:

$$\begin{aligned} A' &= A - a, \\ B' &= B - a - (k + 1)d, \\ C' &= C + 2a + (k + 1)d. \end{aligned}$$

Veamos que el punto *1* se cumple pues $a \in A$ luego $a - a = 0 \in A'$, y $a+(k+1)d \in B$ luego $a+(k+1)d-a-(k+1)d = 0 \in B'$. El punto *2* se cumple pues $nd \in A'$ (ya que $a+nd \in A$) y $nd \notin B'$ (para verificar esto supongamos lo contrario, es decir, supongamos que $nd \in B'$, entonces $nd = b-a-(k+1)d$ para algún $b \in B$, pero despejando obtenemos $b = a + (n + k + 1)d$ lo cual es una contradicción). El punto *3* es consecuencia de la proposición 5.5 tomando $g_1 = -a$ y $g_2 = -a - (k + 1)d$.

Caso (3) $A \cap B = \emptyset$. Como $A \neq \emptyset$ y $B \neq \emptyset$, entonces existen $a \in A$ y $b \in B$. Definiendo $A' = A - a$ y $B' = B - b$ obtenemos que $0 \in A' \cap B'$; de aquí generamos dos nuevos casos: $A' \setminus B' \neq \emptyset$ y $A' \setminus B' = \emptyset$.
Si $A' \setminus B' \neq \emptyset$ llegamos al caso 1 y por lo tanto nuestros conjuntos deseados son:

$$\begin{aligned} A' &= A - a \\ B' &= B - b \\ C' &= C + a + b \end{aligned}$$

Si $A' \setminus B' = \emptyset$ aplicamos el caso 2 a A',B' y obtenemos los siguientes conjuntos:

$$\begin{aligned} A'' &= A' - a' \\ B'' &= B' - a' - (k + 1)d \end{aligned}$$

reescribiendo estos conjuntos en términos de A y B y añadiendo C':

$$\begin{gathered} A'' = A - a - a' \ B'' = B - b - a' - (k + 1)d \\ C' = C + a + b + a' + b' + (k + 1)d \end{gathered}$$

y estos son nuestros conjuntos deseados. □

Ahora sí ya estamos listos para demostrar uno de los teoremas que más usaremos en este trabajo de tesis.

Teorema 5.3 ***(Teorema de Cauchy-Davenport, versión tríos.)*** *Todo trío crítico (A, B, C) en $\mathbb{Z}_p$ satisface $\delta(A, B, C) = 1$.*

Demostración:

Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$ con $|A| \leq |B| \leq |C|$. Se procederá por inducción sobre $|A|$. Supongamos que $|A| = 1$. Como (A, B, C) es crítico entonces $\delta(A, B, C) > 0$, en otras palabras:

$$\begin{aligned} |A| + |B| + |C| - p &> 0 \\ 1 + |B| + |C| - p &\geq 1 \\ |B| + |C| &\geq p \end{aligned}$$

Si $|B| + |C| > p$ entonces, por la proposición 5.3, $B + C = \mathbb{Z}_p$, luego:

$$|B + C| = p \tag{5.3}$$

Por otro lado la proposición 5.2 nos indica que:

$$|A| \leq p - |B + C| \tag{5.4}$$

Sustituyendo 5.3 en 5.4 obtenemos que $|A| \leq 0$ lo cual es una contradicción ya que $|A| = 1$. Entonces $|B| + |C| = p$, por lo tanto $\delta(A, B, C) = |A| = 1$.

Supongamos ahora que $|A| \geq 2$. Por hipótesis de inducción, supongamos también que la proposición es cierta para todo trío (A', B', C') con $|A'| \leq |B'| \leq |C'|$ y $|A'| < |A|$. Además, por la proposición 5.6, podemos suponer sin pérdida de generalidad que $0 \in A \cap B$ y $g \in A \setminus B$. Como 0 está tanto en A como en B entonces la intersección de A y B no es vacía, y como g está en A pero no en B entonces la intersección tampoco es todo A, luego $0 < |A \cap B| < |A|$. Consideremos ahora los conjuntos $A \cap B$ y $A \cup B$. Demostraremos que $(A \cap B, A \cup B, C)$ es un trío crítico para posteriormente aplicar la hipótesis de indución ya que $|A \cap B| < |A|$.

Para demostrar que $(A \cap B, A \cup B, C)$ es un trío basta demostrar que $(A \cap B) + (A \cup B) + C \subseteq A + B + C$. Sea $x \in (A \cap B) + (A \cup B) + C$ entonces $x = a' + b' + c$ con $a' \in A \cap B, b' \in A \cup B, c \in C$. Como $b' \in A \cup B$ entonces $b' \in A$ ó $b' \in B$. Si $b' \in B$ sabemos que $a' \in A$, puesto que $a' \in A \cap B$, entonces $x \in A + B + C$. Si $b' \in A$ sabemos que $a' \in B$, entonces $x \in A + B + C$. Por lo tanto, $(A \cap B) + (A \cup B) + C \subseteq A + B + C$, luego $(A \cap B, A \cup B, C)$ es un trío.

Para probar que $(A \cap B, A \cup B, C)$ es crítico, observemos lo siguiente:

$$\begin{aligned}
\delta(A \cap B, A \cup B, C) &= |A \cap B| + |A \cup B| + |C| - p \\
&= |A \cap B| + |A| + |B| - |A \cap B| + |C| - p \\
&= |A| + |B| + |C| - p \\
&= \delta(A, B, C)
\end{aligned}$$

Como sabemos que (A, B, C) es crítico, entonces $\delta(A, B, C) > 0$ y por lo tanto $\delta(A \cap B, A \cup B, C) > 0$, entonces $(A \cap B, A \cup B, C)$ es un trío crítico. Como mencionamos anteriormente $|A \cap B| < |A|$, entonces aplicando la hipótesis de indución tenemos que $\delta(A \cap B, A \cup B, C) = 1$, luego $\delta(A, B, C) = 1$, y por lo tanto todo trío crítico tiene deficiencia exactamente 1.

□

Una vez demostrado el teorema de Cauchy-Davenport en su versión tríos, veamos que este es equivalente a las versiones anteriormente presentadas.

Proposición 5.7 *El teorema 5.3 y el teorema 5.2 son equivalentes.*

Demostración:

Demostraremos primero que el teorema 5.2 implica al teorema 5.3. Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$. Si $|A| + |B| > p$, por la proposición5.3 obtenemos que $A + B = \mathbb{Z}_p$, lo que implica que $-(A + B) = \mathbb{Z}_p$ y a su vez que $C = \emptyset$, lo cual es una contradicción ya que (A, B, C) es un trío. Entonces tenemos que $|A| + |B| \leq p$, y por lo tanto se cumple la hipótesis del teorema 5.2 que usaremos más adelante.

Como (A, B, C) es un trío crítico entonces $\delta(A, B, C) \geq 1$. Queremos probar que $\delta(A, B, C) = 1$ así que supongamos, por contradicción, que $\delta(A, B, C) > 1$, entonces:

$$|A| + |B| + |C| > p + 1 \tag{5.5}$$

Por la proposición 5.2 tenemos que:

$$|C| \leq p - |A + B| \tag{5.6}$$

Ahora el teorema 5.2 nos dice que:

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

$$|A| + |B| \leq |A + B| + 1 \tag{5.7}$$

Sustituyendo 5.6 y 5.7 en 5.5 obtenemos:

$$\begin{aligned} |A + B| + 1 + p - |A + B| &> p + 1 \\ p + 1 &> p + 1 \end{aligned}$$

lo cual es una contradicción, entonces $\delta(A, B, C) = 1$, que es lo que queríamos demostrar, y por lo tanto el teorema 5.3 es consecuencia del teorema 5.2.

Ahora demostraremos que el teorema 5.3 implica al teorema 5.2. Sean $A, B \subset \mathbb{Z}_p$ tales que $|A| + |B| \leq p$. Definimos $C = \mathbb{Z}_p \setminus -(A + B)$ entonces:

$$|C| = p - |A + B|$$

Observemos que (A, B, C) es un trío, pues de lo contrario tendríamos:

$$\begin{aligned} 0 &= a + b + c \\ c &= -(a + b) \end{aligned}$$

con $a \in A$, $b \in B$ y $c \in C$ lo cual contradice la definición de C.

La deficiencia del trío (A, B, C) está dada por:

$$\begin{aligned}\delta(A,B,C) =& |A| + |B| + |C| - p \\ =& |A| + |B| + p - |A+B| - p \\ =& |A| + |B| - |A+B|\end{aligned}$$

El trío (A, B, C) puede ser crítico o no. Si (A, B, C) es crítico entonces por el teorema 5.3, $\delta(A, B, C) = 1$, luego:

$$\begin{aligned}|A| + |B| - |A+B| &= 1 \\ |A| + |B| - 1 &= |A+B| \\ |A| + |B| - 1 &\leq |A+B|\end{aligned}$$

por lo que el teorema 5.2 se verifica. Si (A, B, C) no es crítico entonces $\delta(A, B, C) \leq 0$, entonces:

$$\begin{aligned}|A| + |B| - |A+B| &\leq 0 \\ |A| + |B| &\leq |A+B| \\ |A| + |B| - 1 &\leq |A+B|\end{aligned}$$

por lo que el teorema 5.2 se cumple.

En consecuencia los dos teoremas son equivalentes.

□

Una vez probado el teorema de Cauchy-Davenport y sus equivalencias, demostraremos tres proposiciones de gran utilidad en el resto del capítulo.

Proposición 5.8 *Sean $A, B \subseteq \mathbb{Z}_p$ no vacíos tales que $|A| + |B| \leq p$. Los siguientes enunciados son equivalentes:*

1. $\delta(A, B) = 1$.
2. $|A + B| = |A| + |B| - 1$.
3. (A, B) *es una pareja crítica.*

Demostración:

(1 ⇒ 2) Supongamos que $\delta(A, B) = 1$. Esto quiere decir que $|A| + |B| - |A + B| = 1$, por lo tanto $|A + B| = |A| + |B| - 1$.

(2 ⇒ 3) Supongamos que $|A + B| = |A| + |B| - 1$, entonces $|A| + |B| - |A + B| = 1$, luego $\delta(A, B) = 1$ y por lo tanto (A, B) es una pareja crítica.

(3 ⇒ 1) Supongamos que (A, B) es una pareja crítica, entonces:

$$|A| + |B| - |A + B| > 0$$
$$|A| + |B| - |A + B| \geq 1$$

$$|A| + |B| - 1 \geq |A + B| \tag{5.8}$$

Por hipótesis tenemos que $|A| + |B| \leq p$, entonces por el teorema 5.2:

$$|A + B| \geq |A| + |B| - 1 \tag{5.9}$$

De las desigualdades 5.8 y 5.9 obtenemos que $|A| + |B| - |A + B| = 1$ y entonces $\delta(A, B) = 1$.

□

Proposición 5.9 *Sea (A, B, C) un trío en $\mathbb{Z}_p$. Los siguientes enunciados son equivalentes:*

1. *$\delta(A, B, C) = 1$*
2. *Para todo $\{X, Y, Z\} = \{A, B, C\}$ tenemos $X = \mathbb{Z}_p \setminus -(Y + Z)$.*
3. *(A, B, C) es crítico.*

Demostración:

(1 ⇒ 2) Sea $\{X, Y, Z\} = \{A, B, C\}$. Supongamos que $\delta(A, B, C) = 1$, entonces:

$$|X| + |Y| + |Z| - p = 1 \tag{5.10}$$

Notemos que $|Y| + |Z| \leq p$ (de lo contrario, sustituyendo $|Y| + |Z| > p$ en (5.10), obtenemos $|X| < 1$, una contradicción). Entonces, podemos usar el teorema 5.2, de donde:

$$|Y + Z| \geq |Y| + |Z| - 1 \tag{5.11}$$

Sustituyendo 5.11 en 5.10 obtenemos:

$$|X| + |Y + Z| + 1 - p \geq 1$$

$$|X| \geq p - |Y + Z| \tag{5.12}$$

Por otro lado, de la proposición 5.2 sabemos que $X \subseteq \mathbb{Z}_p \setminus -(Y + Z)$ y por lo tanto:

$$|X| \leq p - |Y + Z| \tag{5.13}$$

De 5.12 y 5.13 se infiere que $|X| = p - |Y + Z|$, y en consecuencia que $X = \mathbb{Z}_p \setminus -(Y + Z)$.

(2 ⇒ 3) Sea $\{X, Y, Z\} = \{A, B, C\}$. Supongamos que $X = \mathbb{Z}_p \backslash -(Y+Z)$, entonces:

$$|X| = p - |Y + Z| \tag{5.14}$$

Observemos que $|Y|+|Z| \leq p$ (de lo contrario por la proposición 5.3, tenemos que $|Y + Z| = p$ y por lo tanto $|X| = 0$, lo cual es una contradicción ya que por definición de trío $|X| > 0$). Por el teorema 5.2 tenemos que:

$$|Y + Z| \geq |Y| + |Z| - 1 \tag{5.15}$$

sustituyendo 5.15 en 5.14 obtenemos que:

$$|X| \geq p - |Y| + |Z| + 1$$
$$|X| + |Y| + |Z| - p \geq 1$$

$\delta(A, B, C) > 0$ y (A, B, C) es un trío crítico.

(3 ⇒ 1) Supongamos que (A, B, C) es un trío crítico. Por teorema 5.3, $\delta(A, B, C) = 1$.

□

Ahora, lo interesante es que estas dos proposiciones se pueden unir mediante la siguiente proposición.

Proposición 5.10 *Para toda pareja crítica (A, B) existe un conjunto $C \subseteq \mathbb{Z}_p$, tal que (A, B, C) es un trío crítico, y para todo trío crítico (A, B, C) la pareja (X, Y) es crítica, con $X, Y \in \{A, B, C\}$ distintos.*

Demostración:

Primero demostraré la primera parte de la proposición. Sean $A, B \subseteq \mathbb{Z}_p$ una pareja crítica. Definimos a $C = \mathbb{Z}_p \setminus -(A + B)$. Para demostrar que (A, B, C) es un trío supongamos que no lo es, es decir, existen $a \in A, b \in B, c \in C$ tales que $a + b + c = 0$ que es lo mismo que $c = -(a + b)$, es decir, hay un elemento en C que se puede escribir como elemento $-(A + B)$, o en otras palabras, que $C \cap -(A + B) \neq \emptyset$, lo que es una contradicción ya que $C = \mathbb{Z}_p \backslash -(A+B)$. Por lo tanto (A, B, C) es un trío. Ahora para checar que (A, B, C) es crítico notemos que como A, B es una pareja crítica entonces:

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

$$|A| + |B| \geq |A + B| + 1. \tag{5.16}$$

por otro lado $C = \mathbb{Z}_p \setminus -(A + B)$, entonces:

$$|C| = p - |A + B|$$

$$|A+B| = p - |C| \tag{5.17}$$

Sustituyendo 5.17 en 5.16 obtenemos que:

$$\begin{aligned} |A| + |B| &\geq p - |C| + 1 \\ |A| + |B| + |C| - p &\geq 1 \\ \delta(A,B,C) &\geq 1 \\ \delta(A,B,C) &> 0 \end{aligned}$$

Luego el trío (A, B, C) es crítico y ya encontramos nuestro C que necesitábamos.
A continuación demostraremos la segunda parte de la proposición. Supongamos ahora que (A, B, C) es un trío crítico. Por la proposición 5.12, tenemos que eso es equivalente a que $X = \mathbb{Z}_p \setminus -(Y + Z)$, para todo $\{X, Y, Z\} = \{A, B, C\}$. Pasando lo anterior en términos de cardinalidades, obtenemos:

$$|X| = p - |Y + Z| \tag{5.18}$$

por otro lado como (X, Y, Z) es un trío crítico entonces:

$$|X| + |Y| + |Z| - p \geq 1 \tag{5.19}$$

sustituyendo 5.19 en 5.18 obtenemos que:

$$\begin{aligned} p - |Y + Z| + |Y| + |Z| - p &\geq 1 \\ |Y| + |Z| - |Y + Z| &\geq 1 \\ \delta(Y,Z) = |Y| + |Z| - |Y + Z| &\geq 1 \\ \delta(Y,Z) &\geq 1 \\ \delta(Y,Z) &> 0 \end{aligned}$$

Por lo tanto la pareja (Y, Z) es crítica para todo $\{X, Y, Z\} = \{A, B, C\}$.

□

5.3. El teorema de Vosper

Dados dos subconjuntos en $\mathbb{Z}_p$ ya sabemos qué tan pequeño puede ser su conjunto suma. Una pregunta natural es: si sabemos que el conjunto suma de dos conjuntos es pequeño ¿Qué podemos decir de la naturaleza de estos conjuntos? es decir, si el conjunto suma, es pequeño ¿Cómo es la estructura de sus conjuntos sumandos? La respuesta a esta pregunta nos lo da el *teorema de Vosper* probado en 1956.

Al igual que el teorema de Cauchy-Davenport, el teorema de Vosper tiene varias versiones. Primero enunciaremos sus versiones y posteriormente demostraremos que estas son equivalentes. La demostración de las equivalencias no se harán en forma de círculo sino se demostrarán todas a modo de ejercicio y además porque es importante ver la forma en que se conectan una con otra.

Teorema 5.4 ***(Teorema de Vosper, versión clásica)*** *Sean $A, B \in \mathbb{Z}_p$ no vacíos. Si $|A| + |B| = |A + B| + 1$ y $A + B \neq \mathbb{Z}_p$ entonces alguna de las siguientes condiciones se cumple:*

1. *mín $\{|A|, |B|\} = 1$.*
2. *$B = \mathbb{Z}_p \setminus (c - A)$ con $c \in \mathbb{Z}_p$.*
3. *A, B son progresiones aritméticas con la misma diferencia.*

Teorema 5.5 ***(Teorema de Vosper, versión semiclásica)*** *Sean $A, B \subseteq \mathbb{Z}_p$ con $|A|, |B| \geq 2$ y*

$$|A + B| = |A| + |B| - 1 \leq p - 2$$

Entonces A y B son progresiones aritméticas con la misma diferencia.

Teorema 5.6 ***(Teorema de Vosper, versión tríos)*** *Sea (A, B, C) un trío en $\mathbb{Z}_p$. Si (A, B, C) es crítico entonces alguna de las siguientes condiciones se cumple:*

1. *mín$\{|A|, |B|, |C|\} = 1$*
2. *A, B, C son progresiones aritméticas con la misma diferencia.*

Antes de demostrar las equivalencias, es necesario demostrar una proposición más.

Proposición 5.11 *Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$ con A una progresión aritmética de diferencia d. Entonces B y C son progresiones aritméticas de diferencia d.*

Demostración:

Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$, sea A una progresión aritmética con diferencia d y sea $X \in \{B, C\}$. Primero definiremos unos conjuntos que nos serán de mucha utilidad en la demostración: $A' = A \cap (A + d)$ y

$X' = X \cup (X - d)$. Notemos que $A' + X' \subset A + X$, esto se da porque si $x \in A' + X' = (A \cap (A + d)) + (X \cup (X - d))$ entonces $x = a' + b'$ con $a' \in A \cap (A + d)$ y $b' \in (X \cup (X - d)$. Como $b' \in (X \cup (X - d)$ entonces $b' \in X$ ó $b' \in X - d$. Si $b' \in X$ entonces $b' = b$ con $b \in X$. Como $a' \in A \cap (A + d)$ entonces $a' \in A$, luego $x = (b + a) \in X + A$. Si $b' \in X - d$, entonces $b' = b - d$ con $b \in X$. Como $a' \in A \cap (A + d)$ entonces $a' = a + d$ entonces $x = b - d + a + d = b + a$, luego $x \in A + X$ y por lo tanto $A' + X' \subset A + X$. Lo que nos implica que:

$$|A' + X'| \leq |A + X| \tag{5.20}$$

Por otro lado como (A, B, C) es un trío crítico entonces por la proposición 5.10, la pareja (A, X) es crítica y por la proposición 5.7, el ser (A, X) una pareja crítica nos implica que:

$$|A + X| = |A| + |X| - 1 \tag{5.21}$$

sustituyendo la ecuación 5.20 en la ecuación 5.21, obtenemos:

$$|A| + |X| - 1 = |A + X| \geq |A' + X'|$$

$$|A| + |X| - 1 \geq |A' + X'| \tag{5.22}$$

ahora aplicamos el *teorema de Cauchy-Davenport* a la pareja (A', X'):

$$|A' + X'| \geq |A'| + |X'| - 1 \tag{5.23}$$

juntando las ecuaciones 5.22 y 5.23:

$$\begin{aligned} |A| + |X| - 1 &\geq |A'| + |X'| - 1 \\ &= |A \cap (A + d)| + |X \cup (X - d)| - 1 \end{aligned}$$

Como A es una progresión aritmética de diferencia d y $(A + d)$ es una traslación de A, entonces A y $A + d$ se intersectan en todos los elementos de A menos uno, es decir, $A \cap (A + d) = |A| - 1$, luego:

$$\begin{aligned} |A| + |X| &\geq |A \cap (A + d)| + |X \cup (X - d)| \\ &= |A| - 1 + |X \cup (X - d)| \end{aligned}$$

De aquí se concluye que:

$$|X| + 1 \geq |X \cup (X - d)|$$

Luego X es una progresión aritmética de diferencia d. Por lo tanto B, C son progresiones aritméticas de diferencia d.

□

Proposición 5.12 *El teorema 5.4 y el teorema 5.6 son equivalentes.*

Demostración:

Primero demostraremos el teorema 5.4 usando el teorema 5.6. Sean $A, B \in \mathbb{Z}_p$ no vacíos tales que $|A| + |B| = |A + B| + 1$ y $A + B \neq \mathbb{Z}_p$. Por la proposición 5.8, (A, B) es una pareja crítica. Definimos $C = \mathbb{Z}_p \setminus -(A + B)$. Por hipótesis $A + B \neq \mathbb{Z}_p$ entonces $-(A + B) \neq \mathbb{Z}_p$, luego $C \neq \emptyset$. Por la proposición 5.10 resulta que (A, B, C) es un trío crítico, entonces por el teorema 5.6 algunas de las siguientes condiciones se cumple:

1. $\text{mín}\{|A|, |B|, |C|\} = 1$
2. A, B, C son progresiones aritméticas con la misma diferencia.

Supongamos que la primera condición se cumple. Si $\text{mín}\{|A|, |B|, |C|\} = \text{mín}\{|A|, |B|\}$ entonces el $\text{mín}\{|A|, |B|\} = 1$ y por lo tanto llegamos a la primera condición del teorema 5.4. Si $\text{mín}\{|A|, |B|, |C|\} = |C|$ entonces $|C| = 1$, luego $C = \{c\}$. Por la proposición 5.9 sabemos que:

$$\begin{aligned} B &= \mathbb{Z}_p \setminus -(A + c) \\ &= \mathbb{Z}_p \setminus (-A - c) \\ &= \mathbb{Z}_p \setminus (-c - A) \end{aligned}$$

implicando la segunda condición del teorema 5.4.

Supongamos ahora que la segunda condición se cumple, es decir A, B, C son progresiones aritméticas con la misma diferencia. Luego, en particular, A, B son progresiones aritméticas con la misma diferencia y por lo tanto el teorema 5.6 implica al teorema 5.4.

Ahora demostraremos que el teorema 5.4 implica el teorema 5.6.

Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$. Primero checaremos que las dos hípotesis del teorema 5.4 se cumplen. Notemos que como (A, B, C) es crítico entonces por la proposición 5.10: (A, B) es una pareja crítica y por la proposición 5.8: $|A| + |B| = |A + B| + 1$ y por lo tanto la primera condición del teorema se cumple. Para comprobar la segunda hipótesis, veamos que por la proposición 5.9: $\emptyset \neq C = \mathbb{Z}_p \setminus -(A + B)$, entonces $-(A + B) \neq \mathbb{Z}_p$, luego $A + B \neq \mathbb{Z}_p$ y por lo tanto las hipótesis del teorema se cumple. Como se cumplieron las hipótesis podemos aplicar el teorema 5.4 que nos dice que una de las siguientes condiciones se cumple:

1. mín $\{|A|, |B|\} = 1$.

2. $B = \mathbb{Z}_p \setminus c - A$ con $c \in \mathbb{Z}_p$.

3. A, B son progresiones aritméticas con la misma diferencia.

Supongamos que la primera condición se cumple. Sabemos que

$$1 \leq \text{mín}\{|A|, |B|, |C|\} \leq \text{mín}\{|A|, |B|\} = 1,$$

entonces mín$\{|A|, |B|, |C|\} = 1$ y por lo tanto la primera condición del teorema 5.4 nos implica la primera condición del teorema 5.6. Supongamos ahora la segunda segunda condición del teorema 5.4, es decir, $B = \mathbb{Z}_p \setminus (c - A)$ con $c \in \mathbb{Z}_p$. Por la proposición 5.9, $B = \mathbb{Z}_p \setminus -(A + C)$, entonces:

$$\begin{aligned} \mathbb{Z}_p \setminus (c - A) &= \mathbb{Z}_p \setminus -(A + C) \\ c - A &= -(A + C). \end{aligned}$$

Entonces $|A| = |A + C|$ y $|C| = 1$, luego mín$\{|A|, |B|, |C|\} = 1$ y por lo tanto se cumple la primera condición del teorema 5.6.

Por último supongamos la tercera condición del teorema 5.4, es decir, A, B son progresiones aritméticas con diferencia d. Por la proposición 5.11: C es una progresión aritmética con diferencia d. Por lo tanto los dos teoremas son equivalentes. □

Proposición 5.13 *El teorema 5.4 y el teorema 5.5 son equivalentes.*

Demostración:

Primero demostraremos el teorema 5.5 usando el teorema 5.4. Sean $A, B \subseteq \mathbb{Z}_p$ con $|A|, |B| \geq 2$ y $|A + B| = |A| + |B| - 1 \leq p - 2$. Como $|A + B| = |A| + |B| - 1$ entonces por el teorema 5.4 tenemos que alguna de las siguientes condiciones se cumple:

1. mín $\{|A|, |B|\} = 1$.

2. $B = \mathbb{Z}_p \setminus (c - A)$ con $c \in \mathbb{Z}_p$.

3. A, B son progresiones aritméticas con la misma diferencia.

La primera condición no se puede cumplir ya que por hipótesis $|A|, |B| \geq 2$.

Supongamos que la segunda condición se cumple, es decir:

$$\begin{aligned} B = \mathbb{Z}_p \setminus (A - c) \Rightarrow |B| &= p - |A| \\ |B| + |A| &= p \end{aligned}$$

lo cual es una contradicción ya que $|A| + |B| \leq p - 1$. Entonces necesariamente se debe cumplir que A,B son progresiones aritméticas con la misma diferencia y por lo tanto el teorema 5.4 implica al teorema 5.5.

Ahora demostraremos que el teorema 5.5 implica al teorema 5.4. Sean $A, B \in \mathbb{Z}_p$ no vacíos. Supongamos que $|A| + |B| = |A + B| + 1$ y además que $A + B \neq \mathbb{Z}_p$. La demostración se efectuará por casos:

Caso (1) $|A|, |B| \geq 2$ y $|A| + |B| - 1 \leq p - 2$. En este caso vemos que son las hipótesis del teorema 5.5, entonces aplicándolo tenemos que A, B son progresiones aritméticas con la misma diferencia.

Caso (2) ($|A| < 2$,$|B| < 2$) ó $|A|+|B|-1 > p-2$. Este caso lo haré en dos partes: Cuando $|A| < 2$ ó $|B| < 2$. Sin pérdida de generalidad supongamos que el que tiene cardinalidad menor a dos es A. Como $1 \leq |A| < 2$, entonces tenemos que $|A| = 1$, luego mín$\{|A|, |B|\} = 1$ y por lo tanto se cumple la segunda condición del teorema 5.4.
Cuando $|A| + |B| - 1 > p - 2$. Como $|A| + |B| - 1 > p - 2$ entonces:

$$|A| + |B| \geq p \tag{5.24}$$

ahora por hipótesis tenemos que $A + B \neq \mathbb{Z}_p$, entonces aplicando la proposición 5.3 vemos que:

$$|A| + |B| \leq p \tag{5.25}$$

Juntando 5.28 y 5.29 obtenemos que:

$$|A| + |B| = p \Rightarrow |B| = p - |A| \tag{5.26}$$

Por otra parte, como $|A + B| = |A| + |B| - 1$ entonces por la proposición 5.8, tenemos que la pareja (A, B) es crítica y además por la proposición 5.10, existe $C \subseteq \mathbb{Z}_p$ tal que (A, B, C) es un trío crítico. Aplicando ahora la proposición 5.9, vemos que:

$$\begin{aligned} B &= \mathbb{Z}_p \setminus -(C + A) \\ B &= \mathbb{Z}_p \setminus -C - A \\ |B| &= p - | - C - A| \end{aligned}$$

Juntando la ecuación 5.26 con lo anterior:

$$\begin{aligned} p - | - C - A| &= p - |A| \\ | - C - A| &= |A| \end{aligned}$$

entonces $|C| = 1$, lo que nos quiere decir que $B = \mathbb{Z}_p \setminus (c - A)$, luego se cumple la segunda condición del teorema 5.4.
Juntando los resultados de nuestros tres casos llegamos a que si $A, B \in \mathbb{Z}_p$ no vacíos tales que $|A|+|B| = |A+B|-1$ y además que $A+B \neq \mathbb{Z}_p$ entonces una de las siguientes condiciones se cumple:

1. mín$\{|A|, |B|\} = 1$
2. $B = \mathbb{Z}_p \setminus (c - A)$
3. A, B son progresiones aritméticas con la misma diferencia.

Que es lo que queríamos demostrar, entonces el teorema 5.5 implica el teorema 5.4 y por lo tanto los dos teoremas son equivalentes.

□

Proposición 5.14 *El teorema 5.6 y el teorema 5.5 son equivalentes.*

Demostración:

Primero demostraremos el teorema 5.6 usando el teorema 5.5. Sea (A, B, C) un trío en $\mathbb{Z}_p$ tal que $\delta(A, B, C) = 1$, es decir, un trío crítico. Como (A, B, C) es un trío crítico, por la proposición 5.10 tenemos que la pareja (A, B) es crítica y por la proposición 5.8, $|A| + |B| - 1 = |A + B|$. Continuaremos la demostración por casos.

Caso (1) $|A|, |B| \geq 2$ y $|A| + |B| - 1 \leq p - 2$. Este caso son las hipótesis del teorema 5.5, entonces podemos aplicarlo y por lo tanto A, B son progresiones aritméticas con la misma diferencia. Como A, B resultaron ser progresiones aritméticas con la misma diferencia, entonces por la proposición 5.11 tenemos que C también es una progresión aritmética y además con la misma diferencia que A y B, y por lo tanto se cumple la segunda condición del teorema 5.6.

Caso (2) $|A| < 2$,$|B| < 2$ ó $|A| + |B| - 1 > p - 2$. Este caso lo haremos en dos partes. Primero supongamos que $|A| < 2$ ó $|B| < 2$. Sin pérdida de generalidad supongamos que $|A| < 2$, es decir, $|A| = 1$. Como B no es vacío entonces $|B| \geq 1$, luego:

$$min\{|A|, |B|\} = 1 \tag{5.27}$$

Supongamos ahora que $|A| + |B| - 1 > p - 2$. Como $|A| + |B| - 1 > p - 2$ entonces:

$$|A| + |B| \geq p \tag{5.28}$$

ahora por hipótesis tenemos que $A + B \neq \mathbb{Z}_p$, entonces aplicando la proposición 5.3 vemos que:

$$|A| + |B| \leq p \tag{5.29}$$

juntando 5.28 y 5.29 obtenemos que:

$$|A| + |B| = p \tag{5.30}$$

como (A, B, C) es un trío con deficiencia 1, tenemos que:

$$\begin{aligned} \delta(A, B, C) &= 1 \\ |A| + |B| + |C| - p &= 1 \\ |A| + |B| + |C| &= p + 1 \end{aligned}$$

sustituyendo la ecuación 5.30 en la ecuación anterior, obtenemos que:

$$|C| = 1$$

juntando los resultados de las dos partes obtenemos que mín$\{|A|, |B|, |C|\} = 1$ y por lo tanto se cumple la primera condición del teorema 5.6. Entonces vemos por los resultados de nuestros casos que si un trío tiene deficiencia 1 entonces una de las siguientes condiciones se cumple:

1. mín$\{|A|, |B|, |C|\} = 1$
2. A, B, C son progresiones aritméticas con la misma diferencia.

Que es lo que queríamos demostrar, por lo tanto el teorema 5.5 implica al teorema 5.6.

Ahora demostraré el teorema 5.5 usando el teorema 5.6. Sean $A, B \subseteq \mathbb{Z}_p$ con $|A|, |B| \geq 2$ y $|A+B| = |A|+|B|-1 \leq p-2$. Como $|A+B| = |A|+|B|-1$, entonces la pareja (A, B) es crítica. Por la proposición 5.10 tenemos que existe $C \subseteq \mathbb{Z}_p$ tal que (A, B, C) es un trío crítico. Como (A, B, C) es un trío crítico entonces por el teorema 5.6 una de las siguientes condiciones se cumplen:

1. mín$\{|A|, |B|, |C|\} = 1$
2. A, B, C son progresiones aritméticas con la misma diferencia.

Supongamos que la primera condición es cierta. Por hipótesis sabemos que $|A|, |B| \geq 2$, entonces forzosamente $|C| = 1$. Como (A, B, C) es un trío

crítico tenemos que:

$$\begin{aligned} \delta(A,B,C) &= 1 \\ |A|+|B|+|C|-p &= 1 \\ |A|+|B|+1 &= p+1 \\ |A|+|B| &= p \end{aligned}$$

Lo cual es una contradicción ya que por hipótesis $|A|+|B| \leq p-1$, entonces sólo se puede cumplir el segundo caso, es decir, necesariamente A, B, C son progresiones aritmética con la misma diferencia y por lo tanto A, B son progresiones aritméticas con la misma diferencia. Por lo tanto los dos teoremas son equivalentes.

□

Ya demostrado que estas tres versiones del teorema de Vosper son equivalentes entre sí, procederemos a demostrar el teorema en su versión tríos.

Para demostrar el teorema de Vosper en su versión tríos necesitamos definir el concepto de *conjunto de diferencias únicas* y demostrar dos proposiciones, ya que nos apoyaremos fuertemente en ellos.

Definición 5.9 *Sea $A \subseteq \mathbb{Z}_p$. Se dice que A es* un conjunto de diferencias únicas *si las únicas soluciones a la ecuación $a-a' = b-b'$, con $a, a', b, b' \in A$, $a \neq a'$ y $b \neq b'$, son aquellas donde $a = b$ y $a' = b'$.*

Ejemplo 32 *Sea $A \subset \mathbb{Z}_7$, con $A = \{3, 4, 6\}$. En este ejemplo podemos observar que A es un conjunto de diferencias únicas, ya que realizando todas las restas posibles entre elementos diferentes de A vemos que éstas son distintas:*

$$\begin{aligned} 6-3 &= 3 \\ 6-4 &= 2 \\ 4-3 &= 1 \\ 4-6 &= 5 \\ 3-6 &= 4 \\ 3-4 &= 6 \end{aligned}$$

Ejemplo 33 *Sea $A \subset \mathbb{Z}_1 1$, con $A = \{1, 2, 4, 5, 8\}$. En este caso vemos que A no es un conjunto de diferencias únicas ya que $8-5 = 4-1 = 3$.*

Lo que podemos observa en los ejemplos anteriores es que un conjunto de diferencias únicas es aquel conjunto en el cuál las restas entre parejas de elementos distintos, siempre son resultados distintos. Otra observación sobre

este tipo de conjuntos es que son los conjuntos más alejados a ser progresiones aritméticas, ya que en las progresiones aritméticas siempre hay una resta que se repite muchas veces, la diferencia de la progresión aritmética. La siguiente proposición nos dice cómo es la cardinalidad de un conjunto, cuando uno de los conjuntos sumando es un conjunto de diferencias únicas.

Proposición 5.15 *Sean $A, B \subseteq \mathbb{Z}_p$ y supongamos que $k \leq |A| \leq |B|$. Si B es un conjunto de diferencias únicas, entonces $|A+B| \geq k|B| - k(k-1)/2$.*

Demostración:

Sean $A, B \subseteq \mathbb{Z}_p$ tales que $|A| \leq |B|$ y B un conjunto de diferencias únicas; sea $k > 0$ tal que $k \leq |A|$ y sean $a_1, a_2, ..., a_k \in A$. Primero construiremos unos conjuntos, que serán de gran apoyo para la prueba, y posteriormente veremos propiedades importantes de ellos.

Definimos el conjunto $B_i = (B + a_i) \setminus (B + \{a_1, a_2, ..., a_{i-1}\})$, con $1 \leq i \leq k$. Por construcción podemos observar que $B_i \subseteq B + a_i$ y además que $B_i \cap B_j = \emptyset$ para $i \neq j$, es decir, los conjuntos B_i son disjuntos a pares.

Por las observaciones anteriores deducimos que:

$$\begin{aligned} B_1 \cup B_2 \cup ... \cup B_k \subseteq & (B + a_1) \cup (B + a_2) \cup ... \cup (B + a_k) \\ B_1 \cup B_2 \cup ... \cup B_k \subseteq & B + \{a_1, a_2, .., a_k\} \\ |B_1 \cup B_2 \cup ... \cup B_k| \leq & |B + \{a_1, a_2, .., a_k\}| \\ |B_1| + |B_2| + ... + |B_k| \leq & |B + \{a_1, a_2, .., a_k\}| \end{aligned}$$

$$\sum_{i=1}^{k} |B_i| \leq |B + \{a_1, a_2, .., a_k\}| \tag{5.31}$$

A continuación aproximaremos la cardinalidad de cada conjunto B_i. Primero recordemos que $|\bigcup_{k=1}^{n} A_n| \leq \sum_{k=1}^{n} |A_n|$. Ahora tenemos que:

$$\begin{aligned} |B_i| &= |B + a_i| - |(B + a_i) \cap (B + \{a_1, a_2, ..., a_{i-1}\}) \\ &= |B| - |(B + a_i) \cap [(B + a_1) \cup (B + a_2) \cup ... \cup (B + a_{i-1})] \\ &= |B| - |[(B + a_i) \cap (B + a_1)] \cup [(B + a_i) \cap (B + a_2)] \cup ... \cup [(B + a_i) \cap (B + a_{i-1})] \end{aligned}$$

$$|B_i| \leq |B| - (|(B+a_i) \cap (B+a_1)| + |(B+a_i) \cap (B+a_2)| + ... + |(B+a_i) \cap (B+a_{i-1})| \tag{5.32}$$

Ahora veamos que $|(B + a_i) \cap (B + a_j)| \leq 1$, para todo $i \neq j$, lo cual lo demostraremos por contradicción. Supongamos que $|(B+a_i) \cap (B+a_j)| \geq 2$, entonces existen $x, y \in (B+a_i) \cap (B+a_j)$ distintos. Luego $x = b_1 + a_i = b_2 + a_j$

y $y = b_3 + a_1 = b_4 + a_j$, de donde obtenemos que $b_1 - b_2 = a_j - a_i$ y $b_3 - b_4 = a_j - a_i$, luego $b_1 - b_2 = b_3 - b_4$, lo cual es una contradicción ya que B es un conjunto de diferencias únicas, por lo tanto $|(B+a_i) \cap (B+a_j)| \leq 1$. Sustituyendo este resultado en la ecuación 5.32, obtenemos que:

$$|B_i| \leq |B| - (i-1) \tag{5.33}$$

Ahora usaremos las ecuaciones 5.31 y 5.33 para llegar al resultado esperado:

$$\begin{aligned} |A+B| &\geq |B + \{a_1, a_2, ..., a_k\}| \\ &\geq \sum_{i=1}^{k} |B_i| \\ &\geq \sum_{i=1}^{k} (|B| - (i-1)) \\ &\geq \sum_{i=1}^{k} |B| - \sum_{i=1}^{k} (i-1) \\ &\geq k|B| - \frac{k(k-1)}{2} \end{aligned}$$

y por lo tanto:

$$|A+B| \geq k|B| - \tfrac{k(k-1)}{2}$$

Ejemplo 34 *Sean $A, B \subset \mathbb{Z}_7$, con $A = \{3,4,6\}$ y $B = \{1,4\}$. Como vimos en el ejemplo 33 A es un conjunto de diferencias únicas y como $2 = |B| \leq |A|$, entonces podemos aplicar la proposición anterior con $k = 2$, obteniendo:*

$$\begin{aligned} |A+B| &\geq 2 * 3 - 2 * 1/2 \\ |A+B| &\geq 5 \end{aligned}$$

Sabemos que $|A+B| \leq |A| * |B| = 6$.

Ejemplo 35 *Sean $A, B \subset \mathbb{Z}_{11}$, con $A = \{1,3,9\}$ y $B = \{0,1,9\}$, calculando todas las restas posibles entre parejas de A:*

$$\begin{aligned} 9 - 3 &= 6 \\ 9 - 1 &= 8 \\ 3 - 9 &= 5 \\ 3 - 1 &= 2 \\ 1 - 9 &= 3 \\ 1 - 3 &= 9 \end{aligned}$$

de lo anterior, A es un conjunto de diferencias únicas. Tomando a $k = 3$ tenemos que:

$$|A + B| \geq 3 * 3 - 3 * 2/2$$
$$|A + B| \geq 6$$

Proposición 5.16 *Sea $B \in \mathbb{Z}_p$ entonces $|B \cap (B - g)| = |B \cap (B + g)|$*

Demostración:

Para demostar que $|B \cap (B-g)| = |B \cap (B+g)|$, basta demostrar que existe una biyección entre $B \cap (B-g)$ y $B \cap (B+g)$. Sea $\phi : B \cap (B-g) \longrightarrow B \cap (B+g)$ definida como $\phi(x) = x + g$. Primero veré que ϕ está bien definida, es decir, $\phi(x) \in B \cap (B+g)$. Sea $x \in B \cap (B-g)$, entonces $x \in B$ y $x \in (B-g)$. Como $x \in B$ entonces $x + g \in (B + g)$, y como $x \in B - g$ entonces existe $b \in B$ tal que $x = b - g$, $x + g = b - g + g = x$, consecuentemente $\phi(x) \in B \cap (B - g)$ y por lo tanto ϕ está bien definida.
Ahora que ya verificamos que ϕ está bien definida procederemos a demostrar su inyectividad. Sean $x, y \in B \cap (B - g)$ tales que $\phi(x) = \phi(y)$, entonces:

$$x + g = y + g$$
$$x = y$$

Para probar la suprayectividad de ϕ consideremos $y - g$, con $y \in B \cap (B+g)$. Como $y \in B \cap (B + g)$, entonces $y \in B$ y $y \in (B + g)$. Como $y \in B$ entonces $x - g \in (B - g)$, y como $y \in B + g$ entonces existe $b \in B$ tal que $y = b + g$, $y - g = b + g - g = y$, consecuentemente $y - g \in B \cap (B - g)$ y por lo tanto $\phi^{-1}(y) = y - g$. Concluimos pues que ϕ es biyectiva y por lo tanto$|B \cap (B - g)| = |B \cap (B + g)|$.

□

Después de haber demostrado las proposiciones anteriores continuaremos con la demostración del teorema de Vosper versión tríos.

Teroema 6 (Teorema de Vosper, versión tríos) *Sea (A, B, C) un trío en $\mathbb{Z}_p$. Si (A, B, C) es crítico entonces alguna de las siguientes condiciones se cumple:*

1. *mín$\{|A|, |B|, |C|\} = 1$*
2. *A, B, C son progresiones aritméticas con la misma diferencia.*

Demostración:

Sea (A, B, C) un trío crítico en $\mathbb{Z}_p$ y supongamos sin pérdida de generalidad que $|A| \leq |B| \leq |C|$. Supongamos que $|A| = 1$. Como $1 = |A| \leq |B| \leq |C|$ entonces mín$\{|A|, |B|, |C|\} = 1$ y por lo tanto se satisface la primera condición del teorema.

Demostraremos a continuación por inducción sobre $|A|$...., que si $2 \leq |A| \leq |B| \leq |C|$ entonces se satisface la segunda condición del teorema. Supongamos que $|A| = 2$. Como $|A| = 2$, entonces $A = \{a_1, a_2\}$, luego A es una progresión aritmética de tamaño dos y diferencia $a_2 - a_1$. Como A es una progresión aritmética, por la proposición 5.11 tenemos que B y C también son progresiones aritméticas de diferencia $a_2 - a_1$ y por lo tanto se satisface la segunda condición del teorema. Supongamos ahora que $3 \leq |A| \leq |B| \leq |C|$. Por hipótesis de inducción, supongamos también que la proposición es cierta para todo trío (A', B', C') con $|A'| \leq |B'| \leq |C'|$ y $|A'| < |A|$.

A continuación probaremos que ni B ni C pueden ser conjuntos de diferencias únicas. Por contradicción supongamos que B es un conjunto de diferencias únicas. Por la proposición 5.15, con $k = 3$ tenemos:

$$|A + B| \geq 3|B| - 3 \tag{5.34}$$

por hipótesis tenemos que $3 \leq |A| \leq |B| \leq |C|$, entonces:

$$\begin{gathered} |B| \geq 3 \\ |B| + |B| + |B| \geq 3 + |B| + |A| \\ 3|B| - 3 \geq |A| + |B| \end{gathered}$$

juntando lo anterior con la ecuación 5.34:

$$|A + B| \geq |A| + |B|. \tag{5.35}$$

Por otra parte, como (A, B, C) es un trío crítico entonces por la proposición 5.9:

$$|C| = p - |A + B| \tag{5.36}$$

sustituyendo la ecuación 5.35 en la ecuación 5.36 obtenemos:

$$|A| + |B| + |C| \leq p \tag{5.37}$$

lo cuál es una contradicción ya que (A, B, C) es un trío crítico y por lo tanto $|A| + |B| + |C| = p + 1$. Análogamente C no es un conjunto de diferencias únicas.

A continuación definiremos unos nuevos conjuntos, a los cuáles les aplicaremos la hipótesis de inducción. Como B no es un conjunto de diferencias

únicas entonces existe $g \neq 0$ tal que $b_1 - b_1' = b_2 - b_2' = g$, entonces $b_1 = g + b_1'$ y $b_2 = g + b_2'$, lo cuál nos dice que $|B \cap (B+g)| \geq 2$, análogamente como C no es un conjunto de diferencias únicas entonces $|C \cap (C+g)| \geq 2$. A partir de la observación anterior definimos $B' = B \cap (B+g)$, $C' = C \cup (C-g)$, $B'' = B \cup (B-g)$ y $C'' = C \cap (C+g)$. Por construcción $B', C', B'', C'' \neq \emptyset$. Ahora demostraremos que (A, B', C') y (A, B'', C'') son tríos y para ello basta demostrar que $B' + C' \subseteq B + C$ y $B'' + C'' \subseteq B + C$. Sea $b' + c' \in B' + C'$ con $b' \in B \cap (B+g)$ y $c' \in C \cup (C-g)$, entonces $b' \in B$ y $b' \in B+g$, y $c' \in C$ ó $c' \in C - g$. Si $c' \in C$, como $b' \in B$ entonces $b' + c' \in B + C$. Si $c' \in C - g$, como $b' \in B + g$, entonces existen $b \in B$, y $c \in C$ tales que $b' = b + g$ y $c' = c - g$, luego $b' + c' = b + g + c - g = b + c \in B + C$, y por lo tanto $B' + C' \subseteq B + C$. Ahora sólo falta checar que $B'' + C'' \subseteq B + C$. Sea $b'' + c'' \in B'' + C''$ con $b'' \in B \cup (B-g)$ y $c' \in C \cap (C+g)$, entonces $c'' \in C$ y $c'' \in C + g$, y $b'' \in B$ ó $b'' \in B - g$. Si $b'' \in B$, como $c'' \in C$ entonces $b'' + c'' \in B + C$. Si $b'' \in B - g$, como $c'' \in C + g$, entonces existen $b \in B$, y $c \in C$ tales que $b'' = b - g$ y $c'' = c + g$, luego $b'' + c'' = b - g + c + g = b + c \in B + C$, y por lo tanto $B'' + C'' \subseteq B + C$.
Para poder aplicar la hipótesis de inducción sólo nos falta demostrar que (A, B', C') y (A, B'', C'') son tríos críticos, lo cuál haremos a continuación, encontrando la deficiencia de cada trío.

$$\begin{aligned}\delta(A, B', C') + \delta(A, B'', C'') = {} & |A| + |B \cap (B+g)| + |C \cup (C-g)| - p \\ & + |A| + |B \cup (B-g)| + |C \cap (C+g)| - p \\ & = \\ & 2|A| + |B \cap (B+g)| + |B| + |(B-g)| - |B \cup (B+g)| \\ & + |C| + |(C-g)| - |C \cup (C+g)| + |C \cap (C+g)| - 2p\end{aligned}$$

por la proposición 5.1, la proposición 5.16 y además como (A, B, C) es un trío crítico tenemos que:

$$\begin{aligned}\delta(A, B', C') + \delta(A, B'', C'') &= 2|A| + 2|B| + 2|C| - 2p \\ \delta(A, B', C') + \delta(A, B'', C'') &= 2\end{aligned}$$

si $\delta(A, B', C') \leq 0$ entonces por la ecuación anterior $\delta(A, B'', C'') \geq 2$, lo cuál es una contradicción, ya que $\delta(A, B'', C'')$ es a lo más 1, luego $\delta(A, B', C') = 1$ y por lo tanto (A, B', C') y (A, B'', C'') son tríos críticos.
Como $B' = B \cap (B+g)$ entonces B' es un subconjunto propio de B y por lo tanto $|B'| < |B|$, y además como $|B| \geq 2$ entonces podemos aplicar la hipótesis de inducción al trío (A, B', C'), luego A, B', C' satisfacen la segunda condición del teorema. Por anterior a A es una progresión aritmética y

consecuentemente por la proposición 5.11 tenemos que B, C también son progresiones aritméticas con la misma diferencia de A, y por lo tanto si $2 \leq |A| \leq |B| \leq |C|$ entonces A, B, C son progresiones aritméticas con la misma diferencia.

□

Capítulo 6

La prueba versión tríos

En el presente capítulo resolveremos el problema principal de este trabajo de tesis. El cuál consiste en encontrar todas las 3-coloraciones de $\mathbb{Z}_p$ en las que existen soluciones heterocromáticas a la ecuación de Schur usando como herramienta los teoremas clásicos de la teoría aditiva de números en sus versiones trío. Para resolver este problema, caracterizaremos aquellas 3-coloraciones libres a la ecuación de Schur, es decir, caracterizaremos aquellas 3-coloraciones en donde no existen soluciones heterocromáticas a la ecuación de Schur. Para llegar al resultado esperado, empezaremos construyendo unos tríos que se derivan de nuestras coloraciones libres con respecto a la ecuación de Schur; posteriormente demostraremos una proposición que nos será de gran utilidad para probar nuestro teorema objetivo.

Proposición 6.1 *Una 3-coloración $\mathbb{Z}_p = A \cup B \cup C$ es libre con respecto a la ecuación de Schur si y sólo si $(X, Y, -Z)$ es un trío para todo $\{X, Y, Z\} = \{A, B, C\}$.*

Demostración:

Primero demostraremos que si $\mathbb{Z}_p = A \cup B \cup C$ es libre con respecto a la ecuación de Schur entonces $(X, Y, -Z)$ es trío para todo $\{X, Y, Z\} = \{A, B, C\}$.

Sea $\mathbb{Z}_p = A \cup B \cup C$ una 3-coloración libre con respecto a la ecuación de Schur. Entonces:

$$\begin{aligned} a + b &\neq c \\ a + c &\neq b \\ b + c &\neq a \end{aligned}$$

para todo $a \in A$, $b \in B$ y $c \in C$. Lo anterior implica que:

$$a+b-c \neq 0$$
$$a+c-b \neq 0$$
$$b+c-a \neq 0$$

lo cual nos dice que $0 \notin A+B-C$, $0 \notin A+C-B$ y $0 \notin B+C-A$, es decir, $(A,B,-C)$, $(A,C,-B)$ y $(B,C,-A)$ son tríos y por lo tanto para todo $\{X,Y,Z\} = \{A,B,C\}$, $(X,Y,-Z)$ es trío.

Ahora demostraremos que si $(X,Y,-Z)$ es trío, para todo $\{X,Y,Z\} = \{A,B,C\}$, entonces la 3-coloración $\mathbb{Z}_p = A \cup B \cup C$ es libre con respecto a la ecuación de Schur. Procederemos por contradicción.

Sea $\mathbb{Z}_p = A \cup B \cup C$ una coloración no libre tal que para todo $\{X,Y,Z\} = \{A,B,C\}$, $(X,Y,-Z)$ es trío. Como $\mathbb{Z}_p = A \cup B \cup C$ no es libre con respecto a la ecuación de Schur, entonces existen $x \in X$, $y \in Y$ y $z \in Z$, con $\{X,Y,Z\} = \{A,B,C\}$, tales que $x+y=z$; luego $x+y-z=0$, es decir, $0 \in X+Y-Z$. Lo cual es una contradicción ya que $(X,Y,-Z)$ es trío.

□

Ya que construimos estos tríos, que serán de gran utilidad en nuestro teorema principal, continuaremos demostrando unas proposiciones de gran importancia en nuestro resultado esperado.

Proposición 6.2 *Sea $\mathbb{Z}_p = X \cup Y \cup Z$ una partición de $\mathbb{Z}_p$ tal que $0 \in X$ y $(X,Y,-Z)$ es trío. Entonces $(X, Y \cup \{0\}, -Z)$ es trío crítico.*

Demostración:

Sea $\mathbb{Z}_p = X \cup Y \cup Z$ una partición de $\mathbb{Z}_p$ tal que $0 \in X$ y $(X,Y,-Z)$ es trío. Primero demostraremos que $(X, Y \cup \{0\}, -Z)$ es un trío. Supongamos, por contradicción, que $(X, Y \cup \{0\}, -Z)$ no es trío. Entonces $0 \in X + (Y \cup \{0\}) - Z$, es decir, existen $x \in X$, $y \in Y \cup \{0\}$ y $z \in Z$ tales que $x+y-z=0$. Si $y \in Y$ entonces tendríamos una contradicción ya que $(X,Y,-Z)$ es trío. Si $y=0$, entonces $x-z=0$, luego, $x=z$, es decir $x \in X \cap Z$. Lo cual es una contradicción ya que $\mathbb{Z}_p = X \cup Y \cup Z$ es una partición de $\mathbb{Z}_p$. Por lo tanto $(X, Y \cup \{0\}, -Z)$ es trío.

Ahora demostraremos que la deficiencia del trío $(X, Y \cup \{0\}, -Z)$ es 1, es decir, $\delta(X, Y \cup \{0\}, -Z) = 1$. La deficiencia del trío $(X, Y \cup \{0\}, -Z)$ es:

$$\begin{aligned} \delta(X, Y \cup \{0\}, -Z) &= |X| + |Y \cup \{0\}| + |-Z| - p \\ &= |X| + |Y| + 1 + |Z| - p \\ &= p + 1 - p \\ &= 1 \end{aligned}$$

□

Con las dos proposiciones anteriores estamos listos para demostrar el resultado principal en este trabajo de tesis.

Teorema 6.1 *Una 3-coloración $\mathbb{Z}_p = A \cup B \cup C$, con $|A| \leq |B| \leq |C|$, es libre con respecto a la ecuación de Schur si y sólo si $A = \{0\}$, $B = -B$ y $C = -C$.*

Demostración:

Primero demostraremos que si en una 3-coloración de $\mathbb{Z}_p$ las clases cromáticas son tales que $A = \{0\}$, $B = -B$ y $C = -C$, entonces esa coloración es libre con respecto a la ecuación de Schur.

Por contradicción supongamos que $\mathbb{Z}_p = A \cup B \cup C$, con $A = \{0\}$, $B = -B$ y $C = -C$, no es libre con respecto a la ecuación de Schur. Entonces, existen $b \in B$ y $c \in C$ tales que $b + 0 = c$ ó $b + c = 0$. Si $b + 0 = c$, entonces tenemos una contradicción ya que $\mathbb{Z}_p = A \cup B \cup C$ es una partición de $\mathbb{Z}_p$. Si $b + c = 0$, entonces $b = -c$, es decir, $b \in -C$, lo cual es una contradicción ya que $C = -C$ y $\mathbb{Z}_p = A \cup B \cup C$ es una partición de $\mathbb{Z}_p$.

Ahora demostraremos que si una 3-coloración es libre con respecto a la ecuación de Schur entonces sus clases cromáticas son tales que $A = \{0\}$, $B = -B$ y $C = -C$.

Sea $\mathbb{Z}_p = A \cup B \cup C$ una 3-coloración libre con respecto a la ecuación de Schur. Entonces, por la propisición 6.1, $(X, Y, -Z)$ es un trío para todo $\{X, Y, Z\} = \{A, B, C\}$. Sin pérdida de generalidad supongamos que $0 \in X$. Por la proposición 6.2 tenemos que $(X, Y \cup \{0\}, -Z)$ también es trío, y más aún es un trío crítico. Luego, por el teorema de *Vosper* tenemos que mín$\{|X|, |Y \cup \{0\}|, |-Z|\} = 1$ ó $X, Y \cup \{0\}$ y $-Z$ son progresiones aritméticas con la misma diferencia.

- Si mín$(|X|, |Y \cup \{0\}|, |-Z|) = 1$.
  Podemos observar que como $\mathbb{Z}_p = X \cup Y \cup Z$ es una partición de $\mathbb{Z}_p$, entonces $Y \neq \emptyset$ y por lo tanto $|Y \cup \{0\}| \geq 2$. Por lo anterior tenemos que $|X| = 1$ ó $|-Z| = 1$.
  Si $|X| = 1$ tenemos que como $0 \in X$, entonces $X = \{0\}$. En este caso obtenemos que nuestra coloración libre con respecto a la ecuación de Schur tiene la forma $\mathbb{Z}_p = \{0\} \cup Y \cup Z$. Como $\mathbb{Z}_p = \{0\} \cup Y \cup Z$ es libre con respecto a la ecuación de Schur, entonces $y + z \neq 0$, para todo $y \in Y$ y $z \in Z$. Luego tenemos que $y \neq -z$ y $z \neq -y$, para todo $y \in Y$ y $z \in Z$, es decir $Y \cap -Z = \emptyset$ y $Z \cap -Y = \emptyset$. Por lo tanto $A = \{0\}$, $B = -B$ y $C = -C$.
  Si $|Z| = 1$. Como $|Z| = 1$ y $0 \in X$, entonces sea $Z = \{z\}$ con $z \neq 0$,

entonces $-z \in X$ ó $-z \in Y$. Si $-z \in Y$ entonces tenemos una contradicción ya que $\{-z, z, 0\}$ es una terna de Schur heterocromática y $\mathbb{Z}_p = X \cup Y \cup \{z\}$ es libre con respecto a la ecuación de Schur. Sea $-z \in X$. En este caso demostraré que $nz \notin Y$ para todo $n \in \mathbb{Z}$. Como $\mathbb{Z}_p = X \cup Y \cup \{z\}$ es una partición de $\mathbb{Z}_p$, entonces $z \notin Y$. Si $2z \in Y$, entonces tenemos que $\{2z, -z, z\}$ es una terna de Schur heterocromática, lo cual es una contradicción, luego $2z \in X$. Si $-2z \in Y$, entonces tenemos que $\{-2z, z, -z\}$ es una terna de Schur heterocromática, lo cual es una contradicción, luego $-2z \in X$. Si $3z \in Y$, entonces $\{3z, -2z, z\}$ es una terna de Schur heterocromática, por lo tanto $3z \in X$. Si $-3z \in Y$, entonces $\{-3z, z, 2z\}$ es una terna de Schur heterocromática, luego $-3z \in X$. Continuando con este procedimiento llegamos que $nz \notin Y$, para todo $n \in \mathbb{Z}$. Como $\mathbb{Z}_p$ es grupo, donde todo elemento es generador, entonces z genera a $\mathbb{Z}_p$ y por lo tanto $Y = \emptyset$, lo cual es una contradicción ya que $Y \neq \emptyset$. Por lo tanto este caso no se da.

- Si $X, Y \cup \{0\}$ y $-Z$ son progresiones aritméticas con la misma diferencia.
  Por el inciso anterior podemos suponer que $|X|, |Y \cup \{0\}|, |Z| \geq 2$.
  Como $-Z$ es una progresión aritmética, entonces Z es una progresión aritmética con la misma diferencia que $-Z$.
  Como $\mathbb{Z}_p$ es un grupo cíclico, donde cualquier elemento es generador, podemos suponer sin pérdida de generalidad que $X, Y \cup \{0\}$ y Z son progresiones aritméticas con diferencia 1.
  Como $\mathbb{Z}_p = X \cup Y \cup Z$ es una partición de $\mathbb{Z}_p$ forzosamente $X = \{x, x+1, ..., -1, 0\}$ y $Y \cup \{0\} = \{0, 1, ..., -1, y\}$, ó $X = \{0, 1, , ..., x\}$ y $Y \cup \{0\} = \{y, y+1, ..., -1, 0\}$.
  Por lo anterior, tenemos que nuestra 3-coloración libre con respecto a la ecuación de Schur necesariamente tiene la forma $\mathbb{Z}_p = \{0, 1, , ..., x-1, x\} \cup \{x+1, x+2, ..., y-2, y-1\} \cup \{y, y+1, ..., -2, -1\}$ ó la forma $\mathbb{Z}_p = \{1, 2, ..., x-1, x\} \cup \{x+1, x+2, ..., y-2, y-1\} \cup \{y, y+1, .., -1, 0\}$.
  Supongamos que $\mathbb{Z}_p = \{1, 2, ..., x-1, x\} \cup \{x+1, x+2, ..., y-2, y-1\} \cup \{y, y+1, .., -1, 0\}$, en este caso podemos ver que $\{1, x-1, x\}$ es una terna de Schur heterocromá tica, lo cual es una contradicción. El caso $\mathbb{Z}_p = \{0, 1, , ..., x-1, x\} \cup \{x+1, x+2, ..., y-2, y-1\} \cup \{y, y+1, ..., -2, -1\}$ es análogo al enterior.
  Por lo tanto este caso del teorema de *Vosper* no se da.

Por lo tanto si una 3-coloración $\mathbb{Z}_p = A \cup B \cup C$, con $|A| \leq |B| \leq |C|$, es libre con respecto a la ecuación de Schur, entonces $A = \{0\}$, $B = -B$ y $C = -C$. □

Capítulo 7

Conclusiones y trabajo a futuro

Después de estudiar los teoremas clásicos de la teoría aditiva de números para encontrar coloraciones libres con respecto a la ecuación de Schur, se puede concluir brevemente que:

El introducir el concepto de trío en la teoría aditiva de números en los conjuntos suma, es una idea muy original y muy útil ya que facilita la formulación y la demostración del teorema de "Cauchy-Davenporz del teorema de "Vosper".
También dicho concepto, reduce la complejidad de demostrar el teorema principal de esta tesis, ya que al aplicarlo reduce casos a trabajar y nos deja una demostración más limpia.
Como está constituida la demostración del teorema objetivo de este trabajo, seguramente se puede extender la prueba al caso general, es decir, se puede usar la técnica, usada en esta tesis, para encontrar todas las coloraciones libres con respecto a las ecuaciones lineales con tres incognitas: "$a_1x + a_2y + a_3z = b$". EL caso donde $b = 0$, es decir, la ecuación $a_1x + a_2y + a_3z = 0$; constituye un caso muy simple, el cual, intuitivamente, se puede resolver casi de igual manera, como se resolvió en esta tesis el caso de la ecuación de Schur. El caso donde $b \neq 0$, es decir, el caso general, constituye un caso más complejo, pero de igual manera, se podría resolver usando el concepto de trío.

El principal proyecto a futuro es el encontrar todas las coloraciones libres respecto a ecuaciones lineales con tres incógnitas, pero en grupos abelianos

en general. Ya que el usar el concepto de trío podría servir para encontrar un teorema análogo al demostrado en esta tesis.

Bibliografía

[1] Tomas Boothby, Matt DeVos, and Amanda Montejano. A new proof of kemperman's theorem. *arXiv preprint arXiv:1301.0095*, 2013.

[2] Israel N Herstein and Federico Velasco Coba. *Algebra moderna: grupos, anillos, campos, teoría de Galois*. Trillas, 1970.

[3] Mario Huicochea and Amanda Montejano. The structure of rainbow-free colorings for linear equations on three variables in zp. *arXiv preprint arXiv:1502.04413*, 2015.

[4] Veselin Jungic, Jacob Licht, Mohammad Mahdian, Jaroslav Nešetril, and Radoš Radoicic. Rainbow arithmetic progressions and anti-ramsey results. *Combinatorics, Probability and Computing*, 12(5+ 6):599–620, 2003.

[5] Veselin Jungic, Jaroslav Nešetril, and Radoš Radoicic. Rainbow ramsey theory. *Integers: Electronic Journal of Combinatorial Number Theory*, 5(2):A09, 2005.

[6] Bruce M Landman and Aaron Robertson. *Ramsey theory on the integers*, volume 73. American Mathematical Soc., 2014.

[7] Bernardo Llano and Amanda Montejano. Rainbow-free colorings for x+ y= cz in zp. *Discrete Mathematics*, 312(17):2566–2573, 2012.

[8] Amanda Montejano. Una nueva mirada a cuatro teoremas clásicos en teoría aditiva de números. *Miscelánea matemática, revista de divulgación de la SMM*.

[9] Alexander Soifer. *Ramsey theory: yesterday, today, and tomorrow*, volume 285. Springer Science & Business Media, 2010.