UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS
DIVISION DE ESTUDIOS DE POSGRADO

ECUACIONES TENSAS Y NO TENSAS

T E S I S

QUE PARA OBTENER EL GRADO ACADEMICO DE

DOCTOR EN CIENCIAS

(MATEMATICAS)

P R E S E N T A

BERNARDO LLANO PEREZ

DIRECTOR DE TESIS: MAT. VICTOR NEUMANN-LARA
DR. JORGE LUIS AROCHA PEREZ

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

"El matemático es perfecto sólo en la medida en que sea un ser perfecto, en la medida en que perciba la belleza de la verdad; sólo entonces será su trabajo trascendente, transparente, comprensible, puro, claro, atractivo e inclusive, elegante."

J. W. Goethe

A mi familia

AGRADECIMIENTOS

Llegue mi sincera gratitud a todos los que de una forma u otra me han apoyado en el tiempo que duró la realización de este trabajo. Agradezco de corazón a mis maestros, Víctor y Arocha, sus enseñanzas, su paciencia, su confianza y, sobre todas las cosas, su amistad; a mis amigos y colegas de Cuba y de México, su solidaridad y ayuda desinteresadas en los momentos difíciles y los momentos buenos que me han hecho pasar; a mi ya aumentada familia cubano-mexicana por todo el amor y el cariño ofrecido sin límites. De igual forma, doy gracias a la Universidad de la que he recibido apoyo, sin el cual, no hubiera sido posible conseguir esta meta, muy en particular, al Instituto de Matemáticas y a sus directores (gracias, Raymundo y Luis), por las facilidades, por el espacio tan apropiado que brinda para la creación matemática y especialmente por el calor humano que me hace sentir cada día.

Todo es bueno al final.

Contenido

1 Introducción **2**

2 De la tensión en hipergráficas a los teoremas de adición **6**
2.1 Tensión en hipergráficas 6
2.2 Teoremas de adición en la teoría de los números: definiciones y resultados clásicos 8
2.3 Caracterización de los pares $A, B \subseteq \mathbb{Z}_p$ con la propiedad $|A+B| = |A|+|B|$ 12
2.4 Caracterización de los pares $A, B \subseteq \mathbb{Z}_p$ con la propiedad $|A+B| = |A|+|B|+1$ 20

3 Las ecuaciones tensas y no tensas de tipo $x+y \equiv cz \bmod p$ **28**
3.1 El problema general 28
3.2 Clasificación de la ecuaciones no tensas con $b=1$ y $p>7$ . . . 30
3.3 Análisis del Caso 1: $|A+B| = |A|+|B|-1$ 33
3.4 Análisis del Caso 2: $|A+B| = |A|+|B|$ 52
3.5 El teorema de clasificación 55

4 Las ecuaciones tensas y no tensas de tipo $x+by \equiv cz \bmod p$ **56**
4.1 El problema y casos de análisis 56
4.2 El análisis de casos 60
4.3 El teorema de clasificación 76

Capítulo 1

Introducción

Los orígenes del estudio del número heterocromático de hipergráficas y de la definición y desarrollo del concepto de hipergráficas uniformes tensas se remonta al problema de la inconexión acíclica de digráficas. En [NL] se introduce la noción de inconexión acíclica de una digráfica $D = (V, A)$, como el máximo número de componentes (débiles) que pueden obtenerse al omitir un conjunto acíclico de flechas de D. Denotaremos a este número por $\overrightarrow{\omega}(D)$ y de define $\overrightarrow{\omega^+}(D) = \overrightarrow{\omega}(D) + 1$.

Alternativamente, $\overrightarrow{\omega^+}(D)$ puede definirse como el mínimo número de colores tal que toda coloración efectiva de los vértices de D con ese número de colores, produce algún ciclo dirigido de forma tal que toda flecha del mismo tiene sus dos extremos coloreados de distinto color.

En diversos torneos T (digráficas completas sin flechas múltiples ni lazos) para los cuales $\overrightarrow{\omega}(T) = 2$, se cumple la propiedad adicional de que si se colorean sus vértices efectivamente con 3 colores ($\overrightarrow{\omega^+}(T) = 3$), entonces aparece un triángulo cíclicamente orientado tricromático. Esto conduce naturalmente a preguntarse por el mínimo número de 3-aristas en una 3-gráfica H que tenga la propiedad de que toda coloración efectiva con exactamente 3 colores, tenga alguna terna heterocromática, esto es, la tensión en 3-gráficas, desarrollada en [ABN1] y [ABN2].

En el primer artículo de los mencionados con anterioridad, se dan las definiciones del número heterocromático de una hipergráfica $H = (V, E)$ y de las hipergráficas uniformes tensas, que en lo adelante se llamarán k-gráficas (todas sus hiperaristas tienen exactamente k vértices). Se estudian los lla-

mados 3-árboles (3-gráficas minimales en el sentido de que si quitamos una terna, dejan de ser tensas). Es útil destacar que la definición de hipergráfica tensa es una generalización natural de la conexidad de las gráficas (que son 2-gráficas en el sentido expuesto). Los 3-árboles son igualmente una extensión del concepto de árboles ya conocidos. Sin embargo, mientras los árboles tienen la misma cantidad de aristas para un número fijo de vértices, los 3-árboles (y en general los k-árboles, $k \geq 3$) pueden tener diferente cantidad de ternas para un mismo número de vértices (esto es, las propiedades matroidales de los árboles se pierden para $k \geq 3$).

Estos hechos conllevan a plantearse el estudio de los 3-árboles con un mínimo número de ternas. En el trabajo referido se construye una familia infinita de 3-árboles minimales para todo número primo p tal que el número de vértices es $n = (p-1)/2$ y el número de aristas es $n(n-2)/3$. Igualmente, se conjetura que para toda n, existe un 3-árbol con $\lceil n(n-2)/3 \rceil$ aristas.

En la construcción de la familia descrita de 3-árboles minimales, se demuestra un hecho que constituye la principal motivación de este trabajo. En especial, se prueba que para todo coloreo con exactamente 3 colores de $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ (el grupo multiplicativo del campo finito de los residuos módulo un número primo p) existe una solución de la ecuación $x + y = z$ con colores diferentes (véase la proposición 3.1 de [ABN1]).

De aquí se desprende el planteamiento natural del mismo problema para ecuaciones de tipo $ax + by = cz$, donde $a, b, c \in \mathbb{Z}_p^*$, o sea, ¿para qué coeficientes a, b, c la ecuación anterior cumple la propiedad enunciada? A las ecuaciones que tienen esta característica se les llamará tensas (a ellas se asocia una 3-gráfica de modo natural que puede ser tensa o no), en otro caso se llamará no tensa. Con esta terminología, el problema se traduce en clasificar las ecuaciones del tipo dado en tensas y no tensas.

La proposición 3.1 referida es, en cierto sentido, la versión anti-Ramsey de un teorema de Schur de 1916 (véanse [Shu] y [Gra]). Este teorema expresa que si coloreamos a $\mathbb{N}$ (el conjunto de los números naturales) con un número finito de colores, entonces existe una solución de la ecuación $x + y = z$ con x, y, z del mismo color (solución monocromática). Esto es equivalente a decir que si $\mathbb{N}$ se parte en un número finito de subconjuntos, es decir,

$$\mathbb{N} = A_1 \mid A_2 \mid \ldots \mid A_r,$$

entonces existe $j \in \{1, 2, \ldots, r\}$ tal que $x, y, z \in A_j$ y $x + y = z$. Como dato histórico, es interesante mencionar que el artículo de Schur estuvo motivado

La referencia [Man2] resulta apropiada para consultar detalles y aplicaciones de los teoremas de adición en la teoría de los números y en la teoría de grupos. En el capítulo 2 se da un panorama de todo lo expuesto más arriba y se demuestran dos nuevos teoremas de adición necesarios para resolver el problema en cuestión. Estos dos teoremas caracterizan los pares de subconjuntos $A, B \subseteq \mathbb{Z}_p$ tales que

(i) $|A+B| = |A| + |B|$ y

(ii) $|A+B| = |A| + |B| + 1$.

Como en el teorema de Vosper, se da la estructura de los conjuntos que resulta relativamente sencilla de manipular: en la mayoría de los casos se trata de progresiones aritméticas o uniones de progresiones aritméticas con la misma diferencia.

Sentadas las bases para la clasificación de las ecuaciones, en los capítulos 3 y 4 se procede a demostrar cuáles ecuaciones son no tensas. Además se prueba que las ecuaciones resultantes son únicas y por tanto, las que restan son tensas. Las ecuaciones se han dividido en dos tipos para facilitar la exposición. Además, las líneas de razonamiento para ambos casos difieren un poco. El proceso de clasificación se basa en la aplicación del Lema Básico (lema 2.1 de [ABN1] que caracteriza a las k-gráficas tensas) y esto conduce al análisis de todas las particiones en exactamente 3 partes de $\mathbb{Z}_p^*$. Es conocido que el número de estas particiones es del orden de 3^{p-1}. Luego, es necesario acotar la cantidad de particiones a analizar y esto se lleva a cabo con ayuda de la cardinalidad de las partes y de la suma de pares de ellas. Con esto, se reducen considerablemente los casos en cuestión. Con la utilización del teorema de Vosper y de los dos resultados demostrados en el capítulo 2, el problema se convierte en un análisis exhaustivo de casos posibles que provienen de las condiciones de los teoremas mencionados.

En las últimas secciones de los capítulos se resume la clasificación y se exponen algunos resultados derivados del proceso de demostración.

Una lista amplia de referencias bibliográficas de los temas tratados cierra este trabajo, donde confluyen notablemente la teoría de hipergráficas, la teoría de los números y los teoremas de adición. Un problema se resuelve y como siempre, otros nuevos comienzan a perfilarse en el horizonte.

Capítulo 1

Introducción

Los orígenes del estudio del número heterocromático de hipergráficas y de la definición y desarrollo del concepto de hipergráficas uniformes tensas se remonta al problema de la inconexión acíclica de digráficas. En [NL] se introduce la noción de inconexión acíclica de una digráfica $D = (V, A)$, como el máximo número de componentes (débiles) que pueden obtenerse al omitir un conjunto acíclico de flechas de D. Denotaremos a este número por $\overrightarrow{\omega}(D)$ y de define $\overrightarrow{\omega^+}(D) = \overrightarrow{\omega}(D) + 1$.

Alternativamente, $\overrightarrow{\omega^+}(D)$ puede definirse como el mínimo número de colores tal que toda coloración efectiva de los vértices de D con ese número de colores, produce algún ciclo dirigido de forma tal que toda flecha del mismo tiene sus dos extremos coloreados de distinto color.

En diversos torneos T (digráficas completas sin flechas múltiples ni lazos) para los cuales $\overrightarrow{\omega}(T) = 2$, se cumple la propiedad adicional de que si se colorean sus vértices efectivamente con 3 colores ($\overrightarrow{\omega^+}(T) = 3$), entonces aparece un triángulo cíclicamente orientado tricromático. Esto conduce naturalmente a preguntarse por el mínimo número de 3-aristas en una 3-gráfica H que tenga la propiedad de que toda coloración efectiva con exactamente 3 colores, tenga alguna terna heterocromática, esto es, la tensión en 3-gráficas, desarrollada en [ABN1] y [ABN2].

En el primer artículo de los mencionados con anterioridad, se dan las definiciones del número heterocromático de una hipergráfica $H = (V, E)$ y de las hipergráficas uniformes tensas, que en lo adelante se llamarán k-gráficas (todas sus hiperaristas tienen exactamente k vértices). Se estudian los lla-

mados 3-árboles (3-gráficas minimales en el sentido de que si quitamos una terna, dejan de ser tensas). Es útil destacar que la definición de hipergráfica tensa es una generalización natural de la conexidad de las gráficas (que son 2-gráficas en el sentido expuesto). Los 3-árboles son igualmente una extensión del concepto de árboles ya conocidos. Sin embargo, mientras los árboles tienen la misma cantidad de aristas para un número fijo de vértices, los 3-árboles (y en general los k-árboles, $k \geq 3$) pueden tener diferente cantidad de ternas para un mismo número de vértices (esto es, las propiedades matroidales de los árboles se pierden para $k \geq 3$).

Estos hechos conllevan a plantearse el estudio de los 3-árboles con un mínimo número de ternas. En el trabajo referido se construye una familia infinita de 3-árboles minimales para todo número primo p tal que el número de vértices es $n = (p-1)/2$ y el número de aristas es $n(n-2)/3$. Igualmente, se conjetura que para toda n, existe un 3-árbol con $\lceil n(n-2)/3 \rceil$ aristas.

En la construcción de la familia descrita de 3-árboles minimales, se demuestra un hecho que constituye la principal motivación de este trabajo. En especial, se prueba que para todo coloreo con exactamente 3 colores de $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$ (el grupo multiplicativo del campo finito de los residuos módulo un número primo p) existe una solución de la ecuación $x + y = z$ con colores diferentes (véase la proposición 3.1 de [ABN1]).

De aquí se desprende el planteamiento natural del mismo problema para ecuaciones de tipo $ax + by = cz$, donde $a, b, c \in \mathbb{Z}_p^*$, o sea, ¿para qué coeficientes a, b, c la ecuación anterior cumple la propiedad enunciada? A las ecuaciones que tienen esta característica se les llamará tensas (a ellas se asocia una 3-gráfica de modo natural que puede ser tensa o no), en otro caso se llamará no tensa. Con esta terminología, el problema se traduce en clasificar las ecuaciones del tipo dado en tensas y no tensas.

La proposición 3.1 referida es, en cierto sentido, la versión anti-Ramsey de un teorema de Schur de 1916 (véanse [Shu] y [Gra]). Este teorema expresa que si coloreamos a $\mathbb{N}$ (el conjunto de los números naturales) con un número finito de colores, entonces existe una solución de la ecuación $x + y = z$ con x, y, z del mismo color (solución monocromática). Esto es equivalente a decir que si $\mathbb{N}$ se parte en un número finito de subconjuntos, es decir,

$$\mathbb{N} = A_1 \mid A_2 \mid \ldots \mid A_r,$$

entonces existe $j \in \{1, 2, \ldots, r\}$ tal que $x, y, z \in A_j$ y $x + y = z$. Como dato histórico, es interesante mencionar que el artículo de Schur estuvo motivado

por el último teorema de Fermat. En particular, probó de manera más sencilla, y con ayuda del teorema mencionado anteriormente, un resultado de Dickson (véanse [Dic1] y [Dic2]): para toda m , si p es un primo suficientemente grande ($p > m!e$, donde e denota la base de los logaritmos naturales), entonces la ecuación $x^m + y^m \equiv z^m \bmod p$ tiene solución.

Por su parte Rado, [Rad1] en 1933 generalizó el teorema de Schur. En su tesis doctoral demostró lo siguiente. Sea la ecuación

$$\sum_{i=1}^{n} c_i x_i = 0, \quad c_i \in \mathbb{Z}.$$

Entonces, para toda partición del conjunto de los números naturales $\mathbb{N}$ en exactamente r partes, existen $x_1, x_2, ..., x_n$ que satisfacen la ecuación y están en una de las partes si y sólo si existe $\{c_{i_1}, c_{i_2}, ..., c_{i_l}\} \subseteq \{c_1, c_2, ..., c_n\}$ tal que

$$\sum_{j=1}^{l} c_{i_j} = 0.$$

Es fácil ver que el teorema de Schur es consecuencia del de Rado, si ponemos la ecuación $x + y = z$ como $x_1 + x_2 - x_3 = 0$. Los trabajos de Rado fueron generalizados con amplitud, para más detalles consúltense [Rad2] y [Deu].

Luego, el problema que nos concierne puede igualmente considerarse, en algún sentido, como la versión anti-Ramsey del Teorema de Rado para tres variables.

Para la clasificación de las ecuaciones se usan las técnicas de los teoremas de adición en la teoría de los números que constituye un área ya clásica de las matemáticas y que ha sido aplicada a diversos problemas combinatorios. De hecho, el primer teorema de adición se debe a A. Cauchy [Cau] y data de 1813. Probó que si $A, B \subseteq \mathbb{Z}_p$, entonces

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

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

El resultado fue redescubierto por H. Davenport en 1935 [Dav1] y desde entonces se conoce como el teorema de Cauchy-Davenport. Igualmente, se usa el resultado de Vosper [Vos1], [Vos2], que caracteriza los pares de conjuntos para los cuales se cumple la igualdad en el teorema de Cauchy-Davenport.

La referencia [Man2] resulta apropiada para consultar detalles y aplicaciones de los teoremas de adición en la teoría de los números y en la teoría de grupos. En el capítulo 2 se da un panorama de todo lo expuesto más arriba y se demuestran dos nuevos teoremas de adición necesarios para resolver el problema en cuestión. Estos dos teoremas caracterizan los pares de subconjuntos $A, B \subseteq \mathbb{Z}_p$ tales que

(i) $|A+B| = |A| + |B|$ y

(ii) $|A+B| = |A| + |B| + 1$.

Como en el teorema de Vosper, se da la estructura de los conjuntos que resulta relativamente sencilla de manipular: en la mayoría de los casos se trata de progresiones aritméticas o uniones de progresiones aritméticas con la misma diferencia.

Sentadas las bases para la clasificación de las ecuaciones, en los capítulos 3 y 4 se procede a demostrar cuáles ecuaciones son no tensas. Además se prueba que las ecuaciones resultantes son únicas y por tanto, las que restan son tensas. Las ecuaciones se han dividido en dos tipos para facilitar la exposición. Además, las líneas de razonamiento para ambos casos difieren un poco. El proceso de clasificación se basa en la aplicación del Lema Básico (lema 2.1 de [ABN1] que caracteriza a las k-gráficas tensas) y esto conduce al análisis de todas las particiones en exactamente 3 partes de $\mathbb{Z}_p^*$. Es conocido que el número de estas particiones es del orden de 3^{p-1}. Luego, es necesario acotar la cantidad de particiones a analizar y esto se lleva a cabo con ayuda de la cardinalidad de las partes y de la suma de pares de ellas. Con esto, se reducen considerablemente los casos en cuestión. Con la utilización del teorema de Vosper y de los dos resultados demostrados en el capítulo 2, el problema se convierte en un análisis exhaustivo de casos posibles que provienen de las condiciones de los teoremas mencionados.

En las últimas secciones de los capítulos se resume la clasificación y se exponen algunos resultados derivados del proceso de demostración.

Una lista amplia de referencias bibliográficas de los temas tratados cierra este trabajo, donde confluyen notablemente la teoría de hipergráficas, la teoría de los números y los teoremas de adición. Un problema se resuelve y como siempre, otros nuevos comienzan a perfilarse en el horizonte.

Capítulo 2

De la tensión en hipergráficas a los teoremas de adición

En la primera parte de este capítulo, se resumen algunos de los resultados más relevantes de la tensión de hipergráficas necesarios para este trabajo. En la segunda, se exponen algunos de los teoremas de adición conocidos (útiles en los siguientes capítulos) y se demuestran dos nuevos teoremas de este tipo que serán usados en la clasificación de las ecuaciones que nos ocupan.

2.1 Tensión en hipergráficas

Sea $H = (V, E)$ una hipergráfica, donde V denota el conjunto de vértices y E el conjunto de las hiperaristas, definido como una familia arbitraria de subconjuntos de los vértices. Una *3-gráfica* es una hipergráfica para la cual todas sus hiperaristas tienen exactamente 3 vértices. A las hiperaristas de una 3-gráfica se les llaman ternas. Así, una 2-gráfica es una gráfica en el sentido usual.

En [ABN1] y [ABN2] se introduce la definición de hipergráfica tensa y se demuestran los primeros resultados, algunos de los cuales se exhiben a continuación. Para la terminología usada de teoría de gráficas véase [Har].

Una *coloración* de una 3-gráfica $H = (V, E)$ es una función sobreyectiva $f : V \to \{0, 1, 2\}$ (de forma equivalente, una coloración de una 3-gráfica es una partición no degenerada del conjunto de vértices en tres partes). Al codominio de la función f se le llama *conjunto de colores*. Una 3-gráfica H es *tensa* si y sólo si para cualquier coloración de sus vértices con exactamente 3

colores, existe al menos una terna heterocromática, o sea, para toda función sobreyectiva $f : V \to \{0,1,2\}$, existe $e \in E$ tal que $f(e) = \{0,1,2\}$. Así, la tensión de 3-gráficas generaliza la conexidad de gráficas, que se obtiene si se sustituye 3 por 2 en la definición anterior.

Sea $H = (V, E)$ una 3-gráfica y $\emptyset \neq X \subseteq V$. Se llama *traza de* X a la gráfica $Tr(X) = (V \setminus X, E_X)$, donde

$$E_X = \{\{v,w\} \subseteq V \setminus X \mid \exists x \in X, \{v,w,x\} \in E\}.$$

Lema 2.1 (Arocha, Bracho, Neumann-Lara) *$H = (V, E)$ es una 3-gráfica tensa si y sólo si para todo $\emptyset \neq X \subseteq V$, $Tr(X)$ es una gráfica conexa. (Además, es suficiente considerar los conjuntos X de cardinalidad a lo más $\lfloor n/3 \rfloor$, donde $n = |V|$).*

Del lema anterior, se observa que probar la tensión de una 3-gráfica H requiere la comprobación de la conexidad de todas sus trazas. Inversamente, para demostrar que H no es tensa, basta con exhibir una partición en 2 partes de la gráfica $Tr(X)$ que la desconecte. Esta partición conjuntamente con X resulta ser una coloración de H sin ternas heterocromáticas.

Un 3-*árbol* se define como una 3-gráfica $H = (V, E)$ tensa, tal que para toda $e \in E$, la 3-gráfica $H \setminus e = (V, E \setminus \{e\})$ no es tensa. Una 3-*cadena* se define como una 3-gráfica tal que para todo $v \in V$, $Tr(v)$ es una cadena.

Es preciso observar que en el caso de las gráficas conexas, todos los árboles con n vértices tienen $n-1$ aristas, o sea los árboles generadores de una gráfica forman las bases de un matroide. En el caso de las 3-gráficas, esto no ocurre y se tienen 3-árboles con n vértices con distinto número de ternas. En [ABN1] se estudia la cardinalidad mínima φ_n de un 3-árbol con n vértices y se conjetura que para cualquier n, $\varphi_n = \lceil n(n-2)/3 \rceil$. Igualmente, se da una familia infinita de 3-árboles de cardinalidad mínima que de hecho son 3-cadenas. Para la construcción de esta familia infinita, se demostró la siguiente proposición, que constituye una de las principales motivaciones del presente trabajo. Este resultado comienza los intentos para tratar de clasificar las ecuaciones con 3 variables sobre el grupo multiplicativo del campo finito de los restos módulo p (número primo), en tensas y no tensas.

Sean p un número primo y $\mathbb{Z}_p = \{0,1,...,p-1\}$ el campo finito con p elementos. $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ denota el grupo multiplicativo de $\mathbb{Z}_p$.

Proposición 2.1 (Arocha, Bracho, Neumann-Lara) *Para toda coloración de $\mathbb{Z}_p^*$ con 3 colores, existe una solución de la ecuación $x + y = z$ con colores diferentes (esto es, la ecuación $x + y \equiv z \bmod p$ es tensa para todo primo p).*

La demostración de este resultado es ingeniosa, sin embargo las ideas utilizadas resultan aplicables sólo para este caso especial de ecuaciones. Se requieren otras técnicas para lograr clasificar el resto de las ecuaciones.

Para más detalles en esta temática se recomiendan las referencias citadas anteriormente.

2.2 Teoremas de adición en la teoría de los números: definiciones y resultados clásicos

Los teoremas de adición aparecieron primeramente en la solución de problemas de la teoría de los números y posteriormente se extendieron a la teoría de grupos y semigrupos (para citar sólo algunos, consúltense [Cau], [Dav1], [Cho], [She], [Sha], [Kem], [Ols1], [Man3]). Son conocidos muchos teoremas sobre la suma de conjuntos, algunos son generalizaciones del famoso teorema de Cauchy-Davenport, otros se refieren al conocido problema de Erdös, Ginzburg y Ziv [EGZ], [Ols3], [BEL], a los conjuntos libres de sumas maximales [Yap1], [Yap2], [RP1], o a los problemas de densidad de conjuntos de números enteros. De la misma forma, ha habido progresos interesantes al resolver problemas de la teoría de digráficas (en especial, los relativos al estudio de átomos en digráficas y a las digráficas de Cayley), que en algunos casos, han conllevado a la prueba de nuevos teoremas de adición o a la generalización de otros ya conocidos en la literatura (por ejemplo, véanse [Ham1], [HLlS], [Ham2], [Ham4]). Esta temática cuenta con una extensa literatura, una referencia apropiada para adentrarse en la teoría es el libro de Mann [Man2]. La monografía [Str] es adecuada también para tener un panorama de la relación de los teoremas de adición con otros problemas. En general, el objetivo de esta teoría es dar una descripción de la suma de dos conjuntos en términos de ciertas propiedades de los sumandos (por ejemplo, la cardinalidad o la medida de los conjuntos).

En lo que sigue, $\mathbb{Z}_p$ y $\mathbb{Z}_m$ denotarán el grupo aditivo de restos módulo p (número primo) y m (número natural) respectivamente. Sea G un grupo abeliano finito. Se denota por $|A|$ a la cardinalidad del conjunto A y por $\overline{A}$ el complemento del conjunto A. Si $\emptyset \neq A, B \subseteq G$, entonces la suma de estos dos subconjuntos de elementos de un grupo se define como

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

Se definen los conjuntos

$$\begin{aligned} A - B &= A + (-B), \\ -A &= \{-a \mid a \in A\} \quad y \\ tA &= \{ta \mid a \in A\}, \ t \in \mathbb{Z}_p. \end{aligned}$$

Por brevedad, se usarán las notaciones $A \pm c = A \pm \{c\}$, $A \cup c = A \cup \{c\}$, $A \cap c = A \cap \{c\}$ y $A \setminus c = A \setminus \{c\}$.

Se dice que $\emptyset \neq A \subseteq \mathbb{Z}_p$ está en *progresión aritmética* si existen $a, d \in \mathbb{Z}_p$, $d \neq 0$ tales que

$$A = \{a + id \mid 0 \leq i \leq |A| - 1\}.$$

Uno de los teoremas de adición más sencillos se presenta a continuación.

Teorema 2.1 (Mann) *Sean $A, B \subseteq G$. Entonces*

$$G = A + B \ \acute{o} \ |G| \geq |A| + |B|.$$

El primer teorema de adición conocido fue demostrado por Cauchy [Cau] en 1813.

Teorema 2.2 (Cauchy) *Sean $\emptyset \neq A, B \subseteq \mathbb{Z}_p$. Entonces*

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

Equivalentemente, este teorema expresa que

$$A + B = \mathbb{Z}_p \ \acute{o} \ |A + B| \geq |A| + |B| - 1.$$

Cauchy aplicó su resultado para demostrar que todo residuo módulo p se puede representar como la suma de dos residuos cuadráticos, esto es, que toda congruencia $x^2 + y^2 \equiv r \bmod p$ tiene solución para todo $r \in \mathbb{Z}_p^*$.

El mismo resultado de Cauchy fue demostrado independientemente por Davenport [Dav1] en 1935 y desde entonces se conoce como el teorema de Cauchy-Davenport (TCD en lo adelante). En 1953, Mann [Man1] publicó la demostración de un teorema que generaliza el TCD y otros resultados obtenidos con anterioridad por Kneser [Kne1] y Chowla [Cho].

Teorema 2.3 (Mann) *Sean* $\emptyset \neq A, B \subseteq G$. *Si* $c \in G$ *y* $c \notin A+B$, *entonces existen* $B^* \subset G$ *y* H *subgrupo propio de* G *tales que:*

(i) $B \subseteq B^* \subset G$,

(ii) $\overline{A+B^*} = c+H$ *y*

(iii) $|A+B^*| - |A+B| = |B^*| - |B|$.

Corolario 2.1 (Mann) *Si para todo subgrupo propio* H *de* G *se cumple que* $|A+H| \geq |A|+|H|-1$, *entonces para todo* $B \subset G$ *tal que* $G \neq A+B$ *se cumple que* $|A+B| \geq |A|+|B|-1$. *(Si* $G = \mathbb{Z}_p$, *entonces obtenemos el TCD.)*

Corolario 2.2 (Chowla) *Sean* $G = \mathbb{Z}_m$, $A = \{0\} \cup \{a \mid \mathrm{mcd}(a,m) = 1\}$ *y* $B \subseteq G$. *Si* $A+B \neq G$, *entonces* $|A+B| \geq |A|+|B|-1$.

Por otra parte, Vosper [Vos1], [Vos2] en 1956, obtuvo una caracterización de todos los pares de subconjuntos $A, B \subseteq \mathbb{Z}_p$, para los cuales se cumple la igualdad en el TCD, o sea, cuando $|A+B| = \min\{p, |A|+|B|-1\}$. Estos pares de conjuntos fueron denominados por Vosper, *pares críticos.*

Teorema 2.4 (Vosper) *Sean* $\emptyset \neq A, B \subseteq \mathbb{Z}_p$. *Entonces*

$$|A+B| = \min\{p, |A|+|B|-1\}$$

si y sólo si A *y* B *satisfacen una de las siguientes condiciones:*

(i) $|A|+|B| > p$,

(ii) $\min\{|A|, |B|\} = 1$,

(iii) $\overline{B} = c - A$ *para algún* $c \in \mathbb{Z}_p$,

(iv) A y B están en progresión aritmética con la misma diferencia, o sea, existen $a, b, d \in \mathbb{Z}_p$ tales que

$$A = \{a + id \mid 0 \leq i \leq |A| - 1\} \quad y \quad B = \{b + id \mid 0 \leq i \leq |B| - 1\}.$$

Observemos que las condiciones del teorema de Vosper no son excluyentes. Igualmente, la condición (iii) es equivalente a que $|A + B| = p-1$ y $\overline{B} = c-A$, donde $c \notin A + B$.

Para la prueba de los resultados de la siguiente sección, son necesarias algunas definiciones y propiedades de los subconjuntos de $\mathbb{Z}_p$. Primeramente, para todos los conjuntos $\emptyset \neq A, B, C, D \subseteq \mathbb{Z}_p$ se tienen las siguientes propiedades [Vos1]:

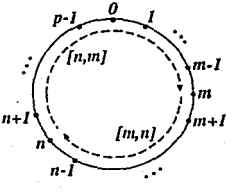
$$\text{Si } A - B = C - D, \text{ entonces } A \cap B = \emptyset \Leftrightarrow C \cap D = \emptyset$$

y como consecuencia

$$\begin{array}{rcl} (A + B) \cap C = \emptyset & \Leftrightarrow & A \cap (C - B) = \emptyset \text{ y} \\ (A - B) \cap (C + D) = \emptyset & \Leftrightarrow & (A - C) \cap (B + D) = \emptyset. \end{array} \tag{2.1}$$

Obsérvese que $A - B = C \Rightarrow A \subseteq B + C$, sin embargo no necesariamente se tiene la implicación de que $A = B+C$. Por ejemplo, si $p = 11$, $A = \{0, 2, 3\}$ y $B = \{3, 4\}$, entonces $C = \{0, 7, 8, 9, 10\}$ y $B + C = \{0, 1, 2, 3, 4, 10\}$.

En lo adelante, se identificarán los elementos de $\mathbb{Z}_p$ con el conjunto de números enteros $\{0, 1, ..., p-1\}$. Un *intervalo de* $\mathbb{Z}_p$ que se denota por $[m, n]$, para $m, n \in \mathbb{Z}_p$, se define como el conjunto$[m, n] = \{m, m + 1, ..., n\}$, donde las sumas se toman módulo p. Para completar la definición, se toma el intervalo $[n, m]$ como el conjunto $[n, m] = \{n, n + 1, ..., m\}$ módulo p. La siguiente figura ilustra esta definición.



Por convención, el intervalo vacío, denotado por $\emptyset$, es aquel que no contiene elementos y $\mathbb{Z}_p = [0, p-1]$. El intervalo $[m, m]$ que contiene sólo al elemento m se denota por $[m]$. Obsérvese que cualquier subconjunto no vacío de $\mathbb{Z}_p$ es una unión de intervalos. Dos intervalos $[m_1, n_1]$ y $[m_2, n_2]$ son *consecutivos* si $m_2 = n_1 + 1$ ó $n_2 = m_1 - 1$.

Se llaman *huecos* (gaps en la literatura) de un conjunto $A \subseteq \mathbb{Z}_p$ a los intervalos de $\overline{A}$. Si $[p-1, 0] \subseteq [m, n]$, entonces se escribirá

$$[m, n] = [m, p-1] \cup [0, n].$$

2.3 Caracterización de los pares $A, B \subseteq \mathbb{Z}_p$ con la propiedad $|A + B| = |A| + |B|$

A continuación se dará una caracterización de todos aquellos pares de conjuntos $\emptyset \neq A, B \subseteq \mathbb{Z}_p$ para los cuales se cumple que $|A + B| = |A| + |B|$. Para probar el teorema correspondiente se requieren los siguientes lemas previos. Recordemos que (A, B) es un par crítico si cumple la igualdad en el TCD.

Lema 2.2 *Sean $\emptyset \neq A, B \subseteq \mathbb{Z}_p$, entonces $|A + B| < |A| + |B|$ si y sólo si (A, B) es un par crítico.*

Demostración. Supongamos que $|A + B| < |A| + |B|$, por el TCD se tiene que

$$\min\{p, |A| + |B| - 1\} \leq |A + B| \leq |A| + |B| - 1.$$

Analicemos dos casos:
CASO 1: $p \leq |A| + |B| - 1 \Leftrightarrow |A| + |B| > p = |A + B|$ y esto es equivalente a la condición (i) del teorema 2.4.
CASO 2: $p > |A| + |B| - 1 \Leftrightarrow |A + B| = |A| + |B| - 1 < p$ y esto se cumple si alguna de las condiciones (ii), (iii) o (iv) se satisface. ∎

De este lema se puede concluir que (A, B) no es un par crítico si y sólo si $|A + B| \geq |A| + |B|$. Para lo que resta de esta sección supongamos que se cumple esta desigualdad, es decir, que asumiremos las siguientes condiciones:

$$|A| + |B| \leq p, \tag{2.2}$$

$$\min\{|A|, |B|\} \geq 2, \tag{2.3}$$

$$\overline{B} \neq c - A \text{ para todo } c \in \mathbb{Z}_p \text{ y} \tag{2.4}$$

A y B no están en progresión aritmética con la misma diferencia. (2.5)

Sea A un conjunto en progresión aritmética y $|A| = l$, es decir,

$$A = \{a + id \mid 0 \leq i \leq l-1\} \ (a, d \in \mathbb{Z}_p, d \neq 0),$$

entonces podemos suponer que $a = 0$ y $d = 1$ ya que el conjunto $A' = \frac{1}{d}(A - a)$ satisface que $|A| = |A'|$. De esta forma podemos escribir $A = [0, l-1]$.

Lema 2.3 *Sean $\emptyset \neq A, B \subseteq \mathbb{Z}_p$, A es una progresión aritmética, $|A| = l \geq 2$ y B cumple que:*

(i) $0 \in B$,

(ii) B *tiene al menos 2 huecos y*

(iii) el número de intervalos de B es $j \geq 2$.

Entonces, si todos los huecos de B tienen longitud $\leq l-1$, excepto uno que tiene longitud $\geq l$, se cumple que

$$|A + B| \geq |A| + |B| + j - 2.$$

Demostración. B puede escribirse como

$$B = \bigcup_{i=0}^{j-1} [s_i, t_i - 1],$$

donde $j \geq 2$, $s_0 = 0$, $s_i \geq t_{i-1} + 1$ $(i \in [1, j-1])$ y $t_{j-1} \leq p - 1$, además

$$|B| = \sum_{i=0}^{j-1} (t_i - s_i) = \sum_{i=0}^{j-1} t_i - \sum_{i=1}^{j-1} s_i$$

y los huecos de B están dados por

$$\overline{B} = \bigcup_{i=0}^{j-2} [t_i, s_{i+1} - 1] \cup [t_{j-1}, p-1].$$

Usando esta notación se tiene que

$$A + B = \bigcup_{i=0}^{j-1} [s_i, l + t_i - 2].$$

Sabemos que B tiene un hueco de longitud $\geq l$ y el resto de los huecos de longitud $\leq l - 1$. Ante todo, se probará que se puede suponer que el hueco de longitud $\geq l$ es $[t_{j-1}, p - 1]$. En caso contrario, si $\|[t_i, s_{i+1} - 1]\| \geq l$ para algún $i \in [0, j-2]$, definamos un conjunto B' tal que $\overline{B'} = \overline{B} + p - s_{i+1}$. Si $0 \notin B'$, entonces $s'_0 \neq 0$ y definimos $B'' = B' - s'_0$. En cualquier caso B' y B'' cumplen las condiciones del lema, su hueco de longitud $\geq l$ está al final y además $|B| = |B'| = |B''|$ y

$$|A + B| = |A + B'| = |A + B''|,$$

por lo que demostrar el lema para B es equivalente a demostrarlo para B' o B''. Así se tiene que

$$s_{i+1} - t_i \leq l - 1 \Leftrightarrow s_{i+1} \leq l + t_i - 1 \text{ (para todo } i \in [0, j-2]) \text{ y}$$

$$p - t_{j-1} \geq l \Leftrightarrow l + t_{j-1} - 2 \leq p - 2,$$

de donde se obtiene que

$$A + B = [0, l + t_{j-1} - 2] \text{ y } |A + B| = l + t_{j-1} - 1.$$

Por otra parte, como $s_0 = 0$ y $s_i \geq t_{i-1} + 1$ $(i \in [1, j-1])$, entonces

$$\sum_{i=1}^{j-1} s_i \geq \sum_{i=0}^{j-2} t_i + j - 1. \tag{2.6}$$

Consideremos la siguiente diferencia:

$$\begin{aligned} |A + B| - (|A| + |B|) &= l + t_{j-1} - 1 - l + \sum_{i=1}^{j-1} s_i - \sum_{i=0}^{j-1} t_i \\ &= \sum_{i=1}^{j-1} s_i - \sum_{i=0}^{j-2} t_i - 1 \geq j - 2, \end{aligned}$$

si hacemos uso de la desigualdad (2.6). ∎

Del lema anterior, hacemos las siguientes observaciones:

(i) Si $j = 2$, entonces $|A + B| \geq |A| + |B|$.

(ii) Si $j = 3$, entonces $|A + B| \geq |A| + |B| + 1$.

Decimos que $A \subseteq \mathbb{Z}_p$ es una *progresión casi aritmética* si A es una progresión aritmética a la que le falta un elemento distinto del primero y el último, es decir:

$$A = \{a + id \mid 0 \leq i \leq j - 1\} \cup \{a + id \mid j + 1 \leq i \leq |A| - 1\},$$

para $j \in [1, |A| - 2]$.

En [Vos1] se prueba que con las suposiciones de que $\min\{|A|, |B|\} \geq 2$, $|A| + |B| < p$ y (A, B) es un par crítico, si A está en progresión aritmética, entonces B y $A + B$ están en progresión aritmética con la misma diferencia (véase el lema 3, p. 203). El recíproco no es cierto como se ve en el siguiente ejemplo.

Sean $p = 13$, $A = [0, 2]$ y $B = [2, 4] \cup [6, 8]$. Entonces, su suma es $A+B = [2, 10]$ que está en progresión aritmética y el complemento de la suma es la progresión aritmética $\overline{A + B} = [0, 1] \cup [11, 12]$. Por tanto, considerando el lema 2.2, en la condición (iii) del siguiente teorema es necesario asumir que A no está en progresión aritmética.

Teorema 2.5 *Sean $\emptyset \neq A, B \subseteq \mathbb{Z}_p$ y supongamos que*

$$|A + B| \geq |A| + |B|. \tag{2.7}$$

Entonces

$$|A + B| = |A| + |B| \tag{2.8}$$

si y sólo si A y B satisfacen una de las siguientes condiciones:

(i) $|A| + |B| = p$,

(ii) $\overline{B} = (c - A) \cup t$ *para* $c \notin A + B$ *y algún* $t \in \mathbb{Z}_p$,

(iii) $\overline{B} = \overline{A + B} - A$ *y A no está en progresión aritmética,*

(iv) $A = \{a, a + d\}$ *y B es la unión de dos progresiones aritméticas con diferencia d, donde* $a, d \in \mathbb{Z}_p$.

(v) A y B están en progresión aritmética y casi aritmética respectivamente, con la misma diferencia.

Demostración.

I. SUFICIENCIA. Se probará que cada una de las condiciones (i)-(v) implica la igualdad (2.8).

(i)⇒(2.8) Evidente.

(ii)⇒(2.8) Suponiendo que la condición (ii) se cumple, entonces

$$\begin{aligned} p-|B| &= \left|\overline{B}\right| = |(c-A)\cup t| \le |c-A|+1 \\ &\approx |A|+1 \Leftrightarrow |A|+|B| \ge p-1. \end{aligned} \tag{2.9}$$

Por otra parte

$$\begin{aligned} B\cap((c-A)\cup t)=\emptyset &\Leftrightarrow (B\cap(c-A))\cup(B\cap t)=\emptyset \\ &\Leftrightarrow (B\cap(c-A))=\emptyset \end{aligned} \tag{2.10}$$

ya que $t \notin B$. Luego (2.10) es equivalente a

$$(A+B)\cap c=\emptyset \Rightarrow |A+B| \le p-1. \tag{2.11}$$

Tomando en cuenta (2.7), (2.9) y (2.11) se obtiene que en

$$p-1 \ge |A+B| \ge |A|+|B| \ge p-1,$$

se cumple la igualdad y se tiene (2.8).

(iii)⇒(2.8) Supongamos que la condición (iii) se verifica, entonces tenemos que $\left|\overline{A+B}\right| \ge 2$ (en otro caso, si $\left|\overline{A+B}\right| = 1 \Leftrightarrow \overline{A+B} = \{c\}$, entonces $\overline{B} = c-A$ que contradice (2.4)) y

$$\left|\overline{B}\right| = \left|\overline{A+B}-A\right| \ge \left|\overline{A+B}\right| + |A|,$$

porque A no está en progresión aritmética. Si en la expresión anterior se cumple la desigualdad estricta, entonces $|A+B| > |A|+|B|$, luego se tiene que

$$\left|\overline{B}\right| = \left|\overline{A+B}-A\right| = \left|\overline{A+B}\right| + |A| \Leftrightarrow |A+B| = |A|+|B|.$$

(iv)⇒(2.8) Sin perder generalidad, podemos suponer que

$$A=[0,1] \text{ y } B=[0,r-1]\cup[s,t-1],$$

donde $r \geq 1$, $r+1 \leq s \leq t-1$, $t \leq p-1$ y $|B| = r-s+t$. Entonces $A+B = [0,r] \cup [s,t]$ y $|A+B| = r+1+t-s+1 = |A|+|B|$.

(v)⇒(2.8) Como A y B están en progresión aritmética y casi aritmética respectivamente, entonces podemos suponer que

$$A = [0, l-1] \text{ con } |A| = l \geq 2 \text{ y}$$

$$B = [0, r-1] \cup [r+1, t-1],\ |B| = t-1 \text{ y } r \in [1, t-2],\ t \geq 3.$$

Luego

$$A+B = [0, l+r-2] \cup [r+1, l+t-2].$$

Como $l \geq 2$ y $r \in [1, t-2]$, entonces

$$A+B = [0, l+t-2] \text{ y } |A+B| = l+t-1 = |A|+|B|.$$

II. NECESIDAD. Supongamos que

$$|A+B| = |A|+|B|. \tag{2.12}$$

1. Si $|A+B| = p$, entonces evidentemente $|A|+|B| = p$, condición (i) del teorema.

2. Supongamos entonces que

   (i) $|A+B| \leq p-1 \Leftrightarrow \left|\overline{A+B}\right| \geq 1$ y

   (ii) B no está en progresión aritmética.

   Consideremos dos casos.

   2.1. CASO: *A no* está en progresión aritmética.
   Como

   $$(A+B) \cap \overline{A+B} = \emptyset \Leftrightarrow B \cap \left(\overline{A+B} - A\right) = \emptyset \Leftrightarrow \overline{B} \supseteq \overline{A+B} - A,$$

   entonces

   $$\left|\overline{B}\right| \geq \left|\overline{A+B} - A\right|. \tag{2.13}$$

2.1.1. SUBCASO: Si $|\overline{A+B}| = 1$, entonces $\overline{A+B} = \{c\}$ $(c \in \mathbb{Z}_p)$, $\overline{B} \supseteq c - A$ y $|\overline{B}| \geq |c - A| = |A|$. Como no se cumple la igualdad (véase (2.4)), se tiene que

$$\overline{B} \supset c - A \Rightarrow |\overline{B}| \geq |c - A| + 1 = |A| + 1.$$

Luego

$$\begin{aligned} |A+B| &= p - |\overline{A+B}| = p - 1 - |A| + |A| \\ &\geq p - |\overline{B}| + |A| = |A| + |B|. \end{aligned}$$

En la desigualdad anterior se cumple la igualdad. Así,

$$\overline{B} = (c - A) \cup t \text{ para algún } t \in \mathbb{Z}_p$$

y se cumple la condición (ii).

2.1.2. SUBCASO: Si $|\overline{A+B}| \geq 2$, entonces usando (2.13)

$$\begin{aligned} |A| + |B| &= |A| + p - |\overline{B}| \leq |A| + p - |\overline{A+B} - A| \\ &\leq |A| + p - |\overline{A+B}| - |A| = |A+B|, \end{aligned}$$

donde para la segunda desigualdad, suponemos que A no está en progresión aritmética. En la expresión anterior se cumple la igualdad y por tanto $|\overline{B}| = |\overline{A+B} - A|$. Como $\overline{B} \supseteq \overline{A+B} - A$, entonces se cumple la condición (iii).

2.2. CASO: A está en progresión aritmética. Se analizarán los intervalos de B. Por el lema 2.3 (véase la observación (i) después del lema), es suficiente considerar solamente el caso en que B tiene exactamente 2 intervalos. Sin perder generalidad podemos suponer que

$$A = [0, l-1], \ |A| = l \geq 2 \text{ y}$$
$$B = [0, r-1] \cup [s, t-1], \ |B| = r - s + t,$$

donde $r \geq 1$, $r+1 \leq s \leq t-1$ y $t \leq p-1$. Los huecos de B están dados entonces por

$$\overline{B} = [r, s-1] \cup [t, p-1]$$

y la suma de A y B es

$$A + B = [0, l + r - 2] \cup [s, l + t - 2]. \tag{2.14}$$

Analicemos los siguientes subcasos:

2.2.1. SUBCASO: Los dos huecos de B tienen longitud $\leq l-1$, es decir,

$$s-r \leq l-1 \Leftrightarrow s \leq l+r-1 \ \text{y} \ p-t \leq l-1 \Leftrightarrow l+t-1 \geq p.$$

Entonces $A+B=\mathbb{Z}_p$, que es una contradicción con la suposición de que $|A+B| \leq p-1$.

2.2.2. SUBCASO: Los dos huecos de B tienen longitud $> l$. Entonces

$$\begin{array}{rcl} s-r \geq l & \Leftrightarrow & s \geq l+r \ \text{y} \\ p-t \geq l & \Leftrightarrow & l+t \leq p. \end{array}$$

Por tanto en (2.14) los intervalos son disjuntos y esto implica que

$$\begin{array}{rcl} |A+B| & = & |[0,l+r-2]|+|[s,l+t-2]| \\ & = & l+r-1+l+t-1-s \\ & = & 2l+r-s+t-2. \end{array}$$

Como se cumple (2.12) se tiene que

$$2l+r-s+t-2=l+r-s+t \Leftrightarrow l=2$$

y se cumple la condición (iv).

2.2.3. SUBCASO: Uno de los huecos de B tiene longitud $\leq l-1$ y el otro es de longitud $\geq l$. Nuevamente, podemos suponer, sin perder generalidad (véase la demostración del lema 2.3) que

$$s-r \leq l-1 \Leftrightarrow s \leq l+r-1 \ \text{y} \ p-t \geq l \Leftrightarrow l+t \leq p.$$

De este modo, en (2.14) los intervalos se intersectan o son consecutivos, así

$$A+B=[0,l+t-2] \ \text{y} \ |A+B|=l+t-1.$$

Como se verifica (2.12) entonces

$$l+t-1=l+r-s+t \Leftrightarrow s=r+1$$

y esto significa que B es una progresión casi aritmética. Se cumple la condición (v). ■

Obsérvese que las condiciones (i)-(v) del teorema no son excluyentes.

2.4 Caracterización de los pares $A, B \subseteq \mathbb{Z}_p$ con la propiedad $|A+B| = |A| + |B| + 1$

En lo que sigue se caracterizan los pares de conjuntos $\emptyset \neq A, B \subseteq \mathbb{Z}_p$ tales que $|A+B| = |A|+|B|+1$. Haremos uso de algunos de los lemas probados en la sección anterior. Para comenzar supondremos que $|A+B| \geq |A|+|B|+1$, esto es no se cumplen las condiciones (i)-(v) del teorema 2.5:

$$|A| + |B| \leq p - 1, \tag{2.15}$$

$$\overline{B} \neq (c - A) \cup t \text{ para todo } t \in \mathbb{Z}_p, \tag{2.16}$$

$$\overline{B} \neq \overline{A+B} - A \text{ para todos } A, B \subseteq \mathbb{Z}_p, \tag{2.17}$$

$$|A| \geq 3 \text{ o } B \text{ no es unión de dos progresiones aritméticas y} \tag{2.18}$$

$$A \text{ y } B \text{ no están en progresión aritmética y casi aritmética respectivamente, con la misma diferencia.} \tag{2.19}$$

Teorema 2.6 *Sean $\emptyset \neq A, B \subseteq \mathbb{Z}_p$ y supongamos que*

$$|A+B| \geq |A| + |B| + 1. \tag{2.20}$$

Entonces

$$|A+B| = |A| + |B| + 1 \tag{2.21}$$

si y sólo si A y B satisfacen una de las siguientes condiciones:

(i) $|A| + |B| = p - 1$,

(ii) $\overline{B} = (c - A) \cup \{t_1, t_2\}$ *para* $c \notin A + B$ *y* $t_1, t_2 \in \mathbb{Z}_p$ *tales que* $t_1 \neq t_2$,

(iii) $\overline{B} = \left(\overline{A+B} - A\right) \cup t$ *para algún* $t \in \mathbb{Z}_p$ *y A no está en progresión aritmética,*

(iv) $A = \{a, a+d, a+2d\}$ *y B es la unión de dos progresiones aritméticas con diferencia d, donde* $a, d \in \mathbb{Z}_p$,

(v) $A = \{a, a+d\}$ *y B es la unión de tres progresiones aritméticas con diferencia d, donde* $a, d \in \mathbb{Z}_p$,

(vi) A está en progresión aritmética con diferencia d y B es la unión de dos o tres progresiones aritméticas con diferencia d tal que

$$B = \{b + id \mid 0 \le i \le r-1\} \cup \{b + id \mid r+2 \le i \le s-1\},$$

donde $r \le s+1$ *y* $s \le p-2$, *ó*

$$B = \{b + id \mid 0 \le i \le r-1\} \cup \{b + id \mid r+1 \le i \le t-1\} \cup \{b + id \mid t+1 \le i \le v-1\},$$

donde $r \le t-2$, $t \le v-2$ *y* $v \le p-2$.

Demostración.

I. SUFICIENCIA. Se probará que cada una de las condiciones (i)-(vi) implica la igualdad (2.21).

(i)⇒(2.21) Evidente.

(ii)⇒(2.21) Supongamos que la condición (ii) se cumple, entonces

$$\begin{aligned} p - |B| &= \left|\overline{B}\right| = |(c-A) \cup \{t_1, t_2\}| \le |c-A| + 2 \\ &= |A| + 2 \Leftrightarrow |A| + |B| \ge p - 2. \end{aligned} \tag{2.22}$$

Por otra parte,

$$\begin{aligned} B \cap ((c-A) \cup \{t_1, t_2\}) = \emptyset \quad &\Leftrightarrow \quad (B \cap (c-A)) \cup (B \cap \{t_1, t_2\}) = \emptyset \\ &\Leftrightarrow \quad B \cap (c-A) = \emptyset \end{aligned} \tag{2.23}$$

ya que $t_1, t_2 \notin B$. Luego (2.23) es equivalente a que

$$(A+B) \cap c = \emptyset \Rightarrow |A+B| \le p-1. \tag{2.24}$$

Tomando en cuenta (2.20), (2.22) y (2.24) se tiene que

$$p - 1 \ge |A+B| \ge |A| + |B| + 1 \ge p - 1,$$

se cumple la igualdad y se cumple (2.21).

(iii)⇒(2.21) Si la condición (iii) se verifica, entonces se tiene que $\left|\overline{A+B}\right| \ge 2$ (en otro caso, si $\left|\overline{A+B}\right| = 1 \Leftrightarrow \overline{A+B} = \{c\}$, entonces $\overline{B} = (c-A) \cup t$, que contradice (2.16)) y

$$\left|\overline{B}\right| = \left|\left(\overline{A+B} - A\right) \cup t\right| = \left|\overline{A+B} - A\right| + 1 \ge \left|\overline{A+B}\right| + |A| + 1$$

porque $t \notin \overline{A+B}-A$ y A no está en progresión aritmética. Si en la expresión anterior se cumple la desigualdad estricta, entonces $|A+B| > |A|+|B|+1$, luego se tiene que

$$\left|\overline{B}\right| = \left|\left(\overline{A+B}-A\right)\cup t\right| = \left|\overline{A+B}\right|+|A|+1 \Leftrightarrow |A+B| = |A|+|B|+1.$$

(iv)⇒(2.21) Sin perder generalidad, podemos suponer que

$$A = [0,2] \text{ y } B = [0,r-1]\cup[s,t-1],$$

donde $r \geq 1$, $r+2 \leq s \leq t-1$, $t \leq p-1$, $|A| = 3$ y $|B| = r-s+t$. Entonces

$$A+B = [0,r+1]\cup[s,t+1] \text{ y } |A+B| = r+2+t-s+2 = |A|+|B|+1.$$

(v)⇒(2.21) Como en el caso anterior, podemos suponer que

$$A = [0,1] \text{ y } B = [0,r-1]\cup[s,t-1]\cup[u,v-1],$$

donde $r \geq 1$, $r+1 \leq s \leq t-1$, $t+1 \leq u \leq v-1 \leq p-2$ y $|B| = r-s+t-u+v$. Entonces

$$A+B = [0,r]\cup[s,t]\cup[u,v] \text{ y}$$

$$|A+B| = r+1+t-s+1+v-u+1 = |A|+|B|+1.$$

(vi)⇒(2.21) Nuevamente, se puede asumir, sin perder generalidad que

$$A = [0,l-1] \text{ con } l \geq 3 \text{ y } |A| = l \text{ y}$$

$$B = [0,r-1]\cup[r+2,t-1],$$

donde $r \geq 1$, $r+2 \leq t-1 \leq p-2$ y $|B| = t-2$ ó

$$B = [0,r-1]\cup[r+1,t-1]\cup[t+1,v-1],$$

con $r \geq 1$, $r+1 \leq t-1$, $t+1 \leq v-1 \leq p-2$ y $|B| = v-2$. Entonces, en el primer caso

$$A+B = [0,l+r-2]\cup[r+2,l+t-2] = [0,l+t-2]$$

debido a que $l \geq 3$ y así los dos intervalos de A son consecutivos o se intersectan. Luego

$$|A+B| = l+t-1 = |A|+|B|+1.$$

En el segundo caso,

$$A+B=[0,l+r-2]\cup[r+1,l+t-2]\cup[t+1,l+v-2]=[0,l+v-2]$$

ya que $l\geq 3$ y consecuentemente, los intervalos de A se intersectan. Entonces

$$|A+B|=l+v-1=|A|+|B|+1.$$

II. NECESIDAD. Supongamos que

$$|A+B|=|A|+|B|+1. \tag{2.25}$$

1. Si $|A+B|=p$, entonces fácilmente se tiene que $|A|+|B|=p-1$, la condición (i) del teorema.

2. Supongamos entonces que

   (i) $|A+B|\leq p-1 \Leftrightarrow \left|\overline{A+B}\right|\geq 1$ y

   (ii) B no está en progresión aritmética.

   Consideremos dos casos.

   2.1. CASO: A no está en progresión aritmética.
   Como

   $$(A+B)\cap\overline{A+B}=\emptyset \Leftrightarrow B\cap\left(\overline{A+B}-A\right)=\emptyset \Leftrightarrow \overline{B}\supseteq\overline{A+B}-A \text{ y}$$

   se cumple la condición (2.17), entonces

   $$\overline{B}\supset\overline{A+B}-A \Rightarrow \left|\overline{B}\right|\geq\left|\overline{A+B}-A\right|+1. \tag{2.26}$$

   2.1.1. SUBCASO: Si $\left|\overline{A+B}\right|=1$, entonces $\overline{A+B}=\{c\}$ $(c\in\mathbb{Z}_p)$, $\overline{B}\supset c-A$ y $\left|\overline{B}\right|\geq|c-A|+1$. Por (2.16), no se cumple la igualdad en la expresión anterior. Por tanto

   $$\left|\overline{B}\right|\geq|c-A|+2=|A|+2.$$

   Luego

   $$\begin{aligned}|A+B| &= p-\left|\overline{A+B}\right|=p-1-|A|+|A|\\ &\geq p-\left|\overline{B}\right|+1+|A|=|A|+|B|+1.\end{aligned}$$

En la desigualdad anterior se tiene la igualdad y entonces

$$\overline{B} = (c - A) \cup \{t_1, t_2\}$$

para ciertos $t_1, t_2 \in \mathbb{Z}_p$ tales que $t_1 \neq t_2$ y $t_1, t_2 \notin c - A \Leftrightarrow c - t_1, c - t_2 \notin A$. Se cumple la condición (ii).

2.1.2. SUBCASO: Si $\left|\overline{A+B}\right| \geq 2$, entonces tomando en cuenta (2.26) se tiene que

$$\begin{aligned} |A| + |B| + 1 &= |A| + 1 + p - \left|\overline{B}\right| \\ &\leq |A| + p - \left|\overline{A+B} - A\right| \\ &\leq |A| + p - \left|\overline{A+B}\right| - |A| = |A+B|, \end{aligned}$$

donde para la segunda desigualdad usamos el hecho de que A no está en progresión aritmética. Nuevamente se cumple la igualdad, así $\left|\overline{B}\right| = \left|\overline{A+B} - A\right| + 1$. Como $\overline{B} \supset \overline{A+B} - A$, entonces

$$\overline{B} = \left(\overline{A+B} - A\right) \cup t$$

para algún $t \in \mathbb{Z}_p$, se verifica la condición (iii).

2.2. CASO: A está en progresión aritmética. Analizaremos los intervalos de B. Por el lema 2.3 (véanse las observaciones que están a continuación del mismo) es suficiente considerar solamente los casos en que B tiene exactamente 2 o 3 intervalos.

2.2.1. SUBCASO. B tiene exactamente 2 intervalos. Sin perder generalidad, supongamos que

$$A = [0, l-1], \ |A| = l \geq 2 \ \text{y}$$

$$B = [0, r-1] \cup [s, t-1], \ |B| = r - s + t,$$

donde $r \geq 1$, $r + 1 \leq s \leq t - 1 \leq p - 2$. Así los huecos de B están dados por

$$\overline{B} = [r, s-1] \cup [t, p-1]$$

y la suma de A y B es

$$A + B = [0, l + r - 2] \cup [s, l + t - 2]. \qquad (2.27)$$

Veamos todas las posibilidades para los huecos de B.

2.2.1.1. Los dos huecos de B tienen longitud $\leq l-1$, es decir, $s-r \leq l-1 \Leftrightarrow s \leq l+r-1$ y $p-t \leq l-1 \Leftrightarrow l+t-1 \geq p$. Entonces $A+B=\mathbb{Z}_p$, que contradice la suposición de que $|A+B| \leq p-1$.

2.2.1.2. Los dos huecos de B tienen longitud $> l$. Entonces

$$s-r \geq l \Leftrightarrow s \geq l+r \text{ y } p-t \geq l \Leftrightarrow l+t \leq p.$$

Luego en (2.27) los intervalos son disjuntos y se tiene que

$$\begin{aligned} |A+B| &= |[0,l+r-2]| + |[s,l+t-2]| \\ &= l+r-1+l+t-1-s \\ &= 2l+r-s+t-2. \end{aligned}$$

Usando (2.25) se tiene que

$$2l+r-s+t-2 = l+r-s+t+1 \Leftrightarrow l=3$$

y se cumple la condición (iv).

2.2.1.3. Uno de los huecos de B tiene longitud $\leq l-1$ y el otro es de longitud $\geq l$. Podemos suponer, sin perder generalidad (véase la demostración del lema 2.3) que

$$s-r \leq l-1 \Leftrightarrow s \leq l+r-1 \text{ y } p-t \geq l \Leftrightarrow l+t \leq p.$$

De este modo,en (2.27) los intervalos se intersectan o son consecutivos, así

$$A+B=[0,l+t-2] \text{ y } |A+B| = l+t-1.$$

Como se verifica (2.25) entonces

$$l+t-1 = l+r-s+t+1 \Leftrightarrow s = r+2$$

y esto significa que B es de la forma descrita en la primera parte de la condición (vi) del teorema.

2.2.2. SUBCASO. B tiene exactamente 3 intervalos. Igual que anteriormente, podemos suponer que

$$A=[0,l-1], \ |A| = l \geq 2 \text{ y}$$

$B = [0, r-1] \cup [s, t-1] \cup [u, v-1]$, $|B| = r - s + t - u + v$,

donde $r \geq 1$, $r+1 \leq s \leq t-1$ y $t+1 \leq u \leq v-1 \leq p-2$. Así los huecos de B están dados por

$$\overline{B} = [r, s-1] \cup [t, u-1] \cup [v, p-1]$$

y la suma de A y B es

$$A + B = [0, l+r-2] \cup [s, l+t-2] \cup [u, l+v-2]. \quad (2.28)$$

Veamos todas las posibilidades para los huecos de B.

2.2.2.1. Los tres huecos de B tienen longitud $\leq l-1$, entonces procediendo de manera similar a 2.2.1.1, $A + B = \mathbb{Z}_p$, contradicción.

2.2.2.2. Los tres huecos de B tienen longitud $\geq l$, entonces

$$\left\{ \begin{array}{c} s-r \geq l \\ u-t \geq l \\ p-v \geq l \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} s \geq l+r \\ u \geq l+t \\ l+v \leq p \end{array} \right\}.$$

Por tanto, en (2.28) todos los intervalos son disjuntos y así la suma de A y B es

$$\begin{aligned} |A+B| &= l+r-1+l+t-1-s+l+v-1-u \\ &= 3l+r-s+t-u+v-3. \end{aligned}$$

Usando (2.25), se obtiene que

$$3l+r-s+t-u+v-3 = l+r-s+t-u+v+1 \Leftrightarrow l = 2$$

y entonces se cumple la condición (v).

2.2.2.3. Dos de los huecos de B tienen longitud $\geq l$ y el otro tiene longitud $\leq l-1$. Si hacemos uso de los argumentos descritos en la demostración del lema 2.3, entonces, podemos suponer que

$$\left\{ \begin{array}{c} s-r \leq l-1 \\ u-t \geq l \\ p-v \geq l \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} s \leq l+r-1 \\ u \geq l+t \\ l+v \leq p \end{array} \right\}.$$

Acorde a lo anterior, en (2.28), los dos primeros intervalos son consecutivos o se intersectan, así

$$A+B=[0,l+t-2]\cup[u,l+v-2] \text{ y}$$

$$|A+B|=l+t-1+l+v-1-u=2l+t-u+v-2.$$

Como se cumple (2.25), se tiene que

$$2l+t-u+v-2=l+r-s+t-u+v+1 \Leftrightarrow l=r-s+3.$$

Pero $r+1\leq s \Rightarrow l\geq 2$, así $l=2$ y $s=r+1$, se cumple la condición (v).

2.2.2.4. Dos de los huecos de B tienen longitud $\leq l$ y el otro tiene longitud $\geq l$. Por las mismas razones expuestas en 2.2.2.3, podemos suponer que

$$\left\{\begin{array}{c} s-r\leq l-1 \\ u-t\leq l-1 \\ p-v\geq l \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} s\leq l+r-1 \\ u\leq l+t-1 \\ l+v\leq p \end{array}\right\}.$$

Entonces en la suma (2.28) los intervalos son consecutivos o se intersectan dos a dos, excepto el primero y el último y se tiene que

$$A+B=[0,l+v-2] \text{ y } |A+B|=l+v-1.$$

Por (2.25),

$$l+v-1=l+r-s+t-u+v+1 \Leftrightarrow s-r+u-t=2.$$

Pero

$$\left\{\begin{array}{c} r+1\leq s \\ t+1\leq u \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} s-r\geq 1 \\ u-t\geq 1 \end{array}\right\} \Leftrightarrow s-r+u-t\geq 2.$$

Como se cumple la igualdad, $s=r+1$ y $u=t+1$. Luego, B tiene la estructura descrita en la segunda parte de la condición (vi). ■

Capítulo 3

Las ecuaciones tensas y no tensas de tipo $x + y \equiv cz \bmod p$

El objetivo principal de este capítulo es dar la clasificación de las ecuaciones no tensas de tipo $x+y \equiv cz \bmod p$. Para ello, se usarán las técnicas expuestas en el capítulo anterior.

3.1 El problema general

Sea $\mathbb{Z}_p^*$ el grupo multiplicativo del campo finito $\mathbb{Z}_p$ de los residuos módulo $p > 3$, donde p denota un número primo y consideremos la ecuación en tres variables

$$ax + by \equiv cz \bmod p, \quad a, b, c \in \mathbb{Z}_p^*.$$

En la ecuación anterior, podemos poner $a \equiv 1 \bmod p$, multiplicando por el inverso de a (lo mismo puede hacerse con b y c). Así, consideremos la ecuación

$$x + by \equiv cz \bmod p. \tag{3.1}$$

A esta ecuación le asociamos una 3-gráfica $H_{b,c} = (V, E)$, tal que su conjunto de vértices es $V = \mathbb{Z}_p^*$ y el conjunto de ternas está dado por

$$E = \{\{x, y, z\} \mid x + by \equiv cz \bmod p\}.$$

Diremos que la ecuación (3.1) es *tensa* si su 3-gráfica asociada $H_{b,c}$ es tensa y *no tensa* en otro caso. De forma equivalente, la ecuación (3.1) es tensa si y sólo si de cualquier forma que se parta el conjunto $\mathbb{Z}_p^*$ en tres partes,

entonces existen x, y, z, uno en cada parte, tal que la ecuación dada se satisface. Hacemos notar que el grupo de automorfismos de $H_{b,c}$ es transitivo en vértices y de aquí se tiene que las trazas de conjuntos de un elemento son todas isomorfas como gráficas.

El problema entonces se puede plantear de la siguiente forma: ¿Para cuáles b y c la ecuación (3.1) es tensa (respectivamente, no tensa)? Este problema se resolverá en dos partes. En el capítulo presente analizaremos el caso en que $b \equiv 1 \bmod p$ y en el siguiente el caso más general.

En lo que sigue, se clasificarán todas las ecuaciones no tensas del tipo $x + y \equiv cz \bmod p$.

De aquí en adelante usaremos la siguiente convención. Expresaremos el hecho de que $a \equiv b \bmod p$, simplemente como $a = b$, siempre que el contexto lo permita. Si no ocurriera esto, se especificará en el momento dado.

Haremos uso de algunas herramientas de la teoría de los números que pueden consultarse, por ejemplo, en [NZM] o [HW]. Un entero a se llama *residuo cuadrático* módulo p si la congruencia $w^2 \equiv a \bmod p$ tiene solución. Hay exactamente $\frac{p-1}{2}$ residuos cuadráticos y el conjunto de ellos forman el mayor subgrupo propio de $\mathbb{Z}_p^*$. Para $p \geq 3$ se define el *símbolo de Legendre*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } a \text{ es un residuo cuadrático} \\ -1, & \text{si } a \text{ no es residuo cuadrático} \\ 0, & \text{si } p \mid a. \end{cases}$$

Se dice que $a \in \mathbb{Z}_p$ es una *raíz primitiva* si a es generador del grupo $\mathbb{Z}_p^*$, en notación $\langle a \rangle = \mathbb{Z}_p^*$.

La congruencia general de segundo grado

$$ax^2 + bx + c \equiv 0 \bmod p,$$

donde $p \nmid a$ es equivalente a que $(2ax + b)^2 \equiv b^2 - 4ac \bmod p$ y tiene solución si y sólo si $\left(\frac{b^2-4ac}{p}\right) = 1$. Si tiene solución, entonces tiene exactamente dos.

Se denotará una partición de un conjunto finito S ($|S| \geq n$, $n \in \mathbb{N}$) en n partes no vacías $S_1, S_2, ..., S_n$ como $S = S_1 \mid S_2 \mid ... \mid S_n$.

Los casos en que $p = 5, 7$ se tratan de manera especial, debido a que los respectivos grupos multiplicativos tienen muy pocos elementos y así las ecuaciones se comportan de manera particular. Consideremos la ecuación

$$x + y = cz, \; c \in \mathbb{Z}_5^* \text{ ó } \mathbb{Z}_7^*.$$

Usando el lema 2.1, se prueban con cálculos sencillos las siguientes proposiciones:

Proposición 3.1 *Si $p = 5$, entonces todas las ecuaciones no tensas son:*

(i) $x + y + z = 0$ *y*

(ii) $x + y + 2z = 0$.

Para ambas ecuaciones, la partición $1 \mid 2 \mid 3,4$ sirve como ejemplo de que son no tensas, en particular $Tr(1) = \overline{K_3}$, la gráfica totalmente desconexa.

Proposición 3.2 *Si $p = 7$, entonces todas las ecuaciones no tensas son:*

(i) $x + y + z = 0$,

(ii) $x + y + 2z = 0$,

(iii) $x + y + 3z = 0$ *y*

(iv) $x + y + 4z = 0$.

Similarmente, las siguientes particiones de $\mathbb{Z}_7^*$ son ejemplos de que las ecuaciones son no tensas:

(i) $1 \mid 3 \mid 2,4,5,6$,

(ii) $1 \mid 2,3,4,5 \mid 6$,

(iii) $1 \mid 2,5,6 \mid 3,4$ y

(iv) $1 \mid 2,5 \mid 3,4,6$.

3.2 Clasificación de la ecuaciones no tensas con $b = 1$ y $p > 7$

Sea la ecuación

$$x + y = cz,\ c \in \mathbb{Z}_p^*,\ p > 7.$$

Por el lema 2.1, esta ecuación es no tensa si y sólo si existe $\mathbb{Z}_p^* = A \mid B \mid C$ tal que

$$\left\{ \begin{array}{l} (A+B) \cap cC = \emptyset \\ (A+C) \cap cB = \emptyset \\ (B+C) \cap cA = \emptyset \end{array} \right\}. \tag{3.2}$$

Observemos que para todo $c \in \mathbb{Z}_p^*$, la partición $cA \mid cB \mid cC$ satisface (3.2). Luego podemos suponer, sin perder generalidad que $|A| \leq |B|$ y $|A| \leq |C|$ y además que $a \in A$ (si $a \notin A$, entonces existen $b \in \mathbb{Z}_p^*$ y $a' \in A$ tales que $a'b = a$ y la partición $bA \mid bB \mid bC$ tiene al elemento a en su primera parte).

El número de particiones a analizar es extremadamente grande, crece exponencialmente a medida que p se hace mayor. Dado este hecho, acotaremos el número de particiones. Así (3.2) es equivalente a

$$\left\{ \begin{array}{l} A+B \subseteq \overline{cC} = cA \cup cB \cup 0 \\ A+C \subseteq \overline{cB} = cA \cup cC \cup 0 \\ B+C \subseteq \overline{cA} = cB \cup cC \cup 0 \end{array} \right\}. \tag{3.3}$$

Se incluye el 0 porque pueden existir $a \in A$ y $b \in B$ tales que $a+b = 0$ y similarmente para los otros dos pares de conjuntos. Usando que $cA \mid cB \mid cC$ es una partición de $\mathbb{Z}_p^*$, que $|cA| = |A|$, $|cB| = |B|$, $|cC| = |C|$ y el TCD, (3.3) implica que

$$\left\{ \begin{array}{l} |A|+|B|-1 \leq |A+B| \leq |A|+|B|+1 \\ |A|+|C|-1 \leq |A+C| \leq |A|+|C|+1 \\ |B|+|C|-1 \leq |B+C| \leq |B|+|C|+1 \end{array} \right\}.$$

Luego las partes A, B, C que satisfacen (3.2) cumplen las siguientes igualdades:

$$\left\{ \begin{array}{l} |A+B| = |A|+|B|+i \\ |A+C| = |A|+|C|+i \\ |B+C| = |B|+|C|+i \end{array} \right\} \text{ para } i \in \{-1, 0, 1\}.$$

La estructura de los pares de conjuntos que satisfacen las igualdades anteriores está caracterizada en los teoremas de Vosper 2.4, 2.5 y 2.6.

Las consideraciones hechas con anterioridad nos llevan al siguiente análisis de casos que se realiza tomando en cuenta las condiciones de los teoremas mencionados.

1. $|A+B| = |A|+|B|-1$.

1.1. $|B+C| = |B| + |C| - 1$.

1.1.1. $|A| = |B| = 1$.

1.1.2. $|A| = 1$, B y C están en progresión aritmética con la misma diferencia ($|B|, |C| \geq 2$).

1.1.3. A, B y C están en progresión aritmética con la misma diferencia ($|A|, |B|, |C| \geq 2$).

Observemos que en el teorema (2.4), la condición (i) no se cumple porque $|A| + |B| + |C| = p - 1$. De igual forma, la condición (iii) implica que $|A| + |B| = p$, que no es posible (ocurre lo mismo para B y C). Es fácil darse cuenta al revisar con detenimiento las condiciones (ii) y (iv) que los casos anteriores son los únicos posibles.

1.2. $|B+C| = |B| + |C|$.

1.2.1. $|A| = 1$, $\overline{C} = \overline{B+C} - B$.

1.2.2. $|A| = 1$ ó A en progresión aritmética con diferencia d, $B = \{b, b+d\}$ y C es la unión de dos progresiones aritméticas con diferencia d.

1.2.3. $|A| = 1$ ó A en progresión aritmética con diferencia d, B y C están en progresión aritmética y casi aritmética respectivamente, con la misma diferencia d.

Nótese que las condiciones (i) y (ii) del teorema (2.5) no son posibles; la primera trivialmente (ver caso anterior), la segunda implica que la suma $|A| + |B| = p - 1$. La combinación de las condiciones que deben cumplirse para (A, B) y (B, C) se reducen a las posibilidades anteriores. En especial, en el caso 1.2.1 A no puede ser una progresión aritmética, porque entonces B estaría en progresión (casos 1.2.2 y 1.2.3).

1.3. $|B+C| = |B| + |C| + 1$.

1.3.1. $|A| = 1$, $\overline{B} = (d - C) \cup \{t_1, t_2\}$ para $d \notin B + C$ y $t_1, t_2 \in \mathbb{Z}_p^*$ tales que $t_1 \neq t_2$.

1.3.2. $|A| = 1$ ó A en progresión aritmética con diferencia d, B es una progresión aritmética con tres elementos y diferencia d, esto es, $B = \{b, b+d, b+2d\}$ y C es la unión de dos progresiones aritméticas con diferencia d.

1.3.3. $|A| = 1$ ó A en progresión aritmética con diferencia d, $B = \{b, b+d\}$ y C es la unión de tres progresiones aritméticas con diferencia d.

1.3.4. $|A| = 1$, B en progresión aritmética con diferencia d y C es la unión de dos o tres progresiones aritméticas con diferencia d (de la forma descrita en la condición (vi) del teorema 2.6).

Es fácil ver que las condiciones (i) y (iii) del teorema 2.6 no son posibles; la (i) evidentemente, la (iii) porque

$$|A| = 1 \Leftrightarrow |B| + |C| = p - 2 \Leftrightarrow |B + C| = p - 1 \Leftrightarrow \left|\overline{B + C}\right| = 1,$$

pero $\left|\overline{B + C}\right| \geq 2$ (véase la demostración del teorema 2.6, suficiencia, (iii)$\Rightarrow$(2.21)). En particular, en los casos 1.3.1 y1.3.4. A no puede ser una progresión aritmética porque $|B + C| = p - 2$ para la primera situación y $|A| = 1, 2$ para la segunda, que ya se analizó en los puntos anteriores.

2. $|A + B| = |A| + |B|$.

2.1. $|B + C| = |B| + |C|$.

La inspección de las condiciones del teorema 2.5 muestra que (i) y (ii) no son posibles (véase 1.2.3). Igualmente, las condiciones (iv) y (v) tampoco se verifican para una partición del tipo que nos ocupa. Solamente es necesario tomar en cuenta (iii) y se demuestra que tampoco es posible.

2.2. $|B + C| = |B| + |C| + 1$.

Como en el punto anterior, una simple inspección a los teoremas 2.5 y 2.6 nos lleva a que la única posibilidad es la condición (iii) en ambos teoremas. La combinación de las condiciones restantes es imposible.

3. $|A + B| = |A| + |B| + 1$ y $|B + C| = |B| + |C| + 1$.

Similar al caso 2.2.

3.3 Análisis del Caso 1: $|A + B| = |A| + |B| - 1$

1.1. $|B + C| = |B| + |C| - 1$.

1.1.1. $|A| = |B| = 1$.

Sean $A = \{1\}$, $B = \{t\}$, $C = \mathbb{Z}_p^* \setminus \{1, t\}$, $t \neq 1$. Entonces, usando las relaciones (2.1), (3.2) es equivalente a

$$\left\{ \begin{array}{c} (1+t) \cap cC = \emptyset \\ (1+C) \cap ct = \emptyset \\ (t+C) \cap c = \emptyset \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} (1+t)/c \cap C = \emptyset \\ (ct-1) \cap C = \emptyset \\ (c-t) \cap C = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \frac{1+t}{c}, ct-1, c-t \notin C \Leftrightarrow \frac{1+t}{c}, ct-1, c-t \in \{0,1,t\}.$$

Denotaremos $\alpha = \frac{1+t}{c}$, $\beta = ct-1$ y $\gamma = c-t$. Veamos todas las posibilidades.

(1) $\alpha = 0 \Leftrightarrow t = -1 \Rightarrow \left\{ \begin{array}{c} \beta = -c-1 \\ \gamma = c+1 \end{array} \right\} \Leftrightarrow \beta = -\gamma$. Entonces,

a) $\beta = 0 \Leftrightarrow \gamma = 0 \Leftrightarrow c = -1$.

b) $\beta = 1 \Leftrightarrow \gamma = -1 \Leftrightarrow c = -2$.

c) $\beta = -1 \Leftrightarrow \gamma = 1 \Leftrightarrow c = 0 \notin \mathbb{Z}_p^*$, contradicción.

De a) y b) obtenemos:

Proposición 3.3 *Las siguientes ecuaciones son no tensas para todo primo $p > 7$:*

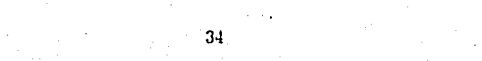
(i) $x + y + z = 0$ *y*

(ii) $x + y + 2z = 0$.

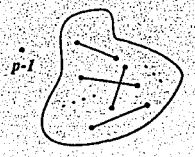
Observemos que para ambas ecuaciones, la partición obtenida es

$$1 \mid -1 \mid \mathbb{Z}_p^* \setminus \{1, -1\}.$$

La siguiente figura muestra la $Tr(1)$ de la 3-gráfica asociada a la ecuación $x + y + z = 0$ para todo primo p.



A continuación, se ilustra la $Tr(1)$ de la ecuación $x+y+2z=0$ para todo primo p.



(2) $\alpha = 1 \Leftrightarrow \frac{1+t}{c} = 1 \Leftrightarrow t = c-1 \Rightarrow \left\{ \begin{array}{l} \beta = c^2-c-1 \\ \gamma = 1 \end{array} \right\}$. Entonces,

a) $\beta = 0 \Leftrightarrow c^2-c-1 \equiv 0 \bmod p \Leftrightarrow (2c-1)^2 \equiv 5 \bmod p \Leftrightarrow \left(\frac{5}{p}\right) = 1$ $\Leftrightarrow p \equiv \pm 1 \bmod 10$. Denotando por $\pm\sqrt{5}$ a las soluciones de la ecuación $w^2 \equiv 5 \bmod p$, se tiene que

$$c = \frac{1 \pm \sqrt{5}}{2} \Rightarrow t = \frac{-1 \pm \sqrt{5}}{2}.$$

b) $\beta = 1 \Leftrightarrow c^2-c-1 = 1 \Leftrightarrow c^2-c-2 = 0 \Leftrightarrow (c+1)(c-2) = 0 \Leftrightarrow$ $c = -1$ ó $c = 2$. Si $c = -1 \Rightarrow t = -2$. Si $c = 2 \Rightarrow t = 1$ que contradice que $t \neq 1$.

c) $\beta = t \Leftrightarrow \beta = c-1 \Leftrightarrow c(c-2) = 0 \Leftrightarrow c = 0$ ó $c = 2$. Ambas son imposibles (véanse (1)c) y (2)b)).

Luego de a) tenemos:

Proposición 3.4 *Si* $p \equiv \pm 1 \bmod 10$, *entonces las ecuaciones*

$$x+y = \frac{1 \pm \sqrt{5}}{2} z$$

son no tensas.

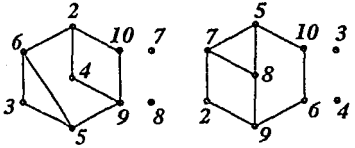
La partición obtenida es

$$1 \left| \frac{-1 \pm \sqrt{5}}{2} \right| \mathbb{Z}_p^* \setminus \left\{ 1, \frac{-1 \pm \sqrt{5}}{2} \right\}.$$

Ejemplo 3.1 *Para* $p = 11$, $\sqrt{5} = 4$ y $-\sqrt{5} = 7$. *Las ecuaciones* $x + y = 8z$ y $x + y = 4z$ *no son tensas y las particiones son*

$$1 \mid 7 \mid \mathbb{Z}_{11}^{*} \setminus \{7\} \quad y \quad 1 \mid 3 \mid \mathbb{Z}_{11}^{*} \setminus \{3\}.$$

La figura que se presenta a continuación, muestra la $Tr(1)$ del par de ecuaciones del ejemplo 3.1 (la de la izquierda para $c = 8$ y la de la derecha para $c = 4$).



De b) obtenemos la ecuación (i) de la proposición 3.3 con la partición $1 \mid -2 \mid \mathbb{Z}_{p}^{*} \setminus \{1, -2\}$.

(3) $\alpha = t \Leftrightarrow \frac{1+t}{c} = t \Leftrightarrow t = \frac{1}{c-1}$ $(c \neq 1) \Rightarrow \left\{ \begin{array}{l} \beta = \frac{1}{c-1} \Rightarrow \beta = t \\ \gamma = \frac{c^2-c-1}{c-1} \end{array} \right\}$. Entonces

a) $\beta = 0 \Leftrightarrow c = 1$, imposible, $c \neq 1$.
$\gamma = 0 \Leftrightarrow c^2 - c - 1 = 0$, que es el caso (2)a).

b) $\beta = 1 \Leftrightarrow c = 2$, imposible, caso (2)b).
$\gamma = 1 \Leftrightarrow c(c-2) = 0$, imposible, caso (2)c).

c) $\gamma = t \Leftrightarrow c^2 - c - 2 = 0 \Leftrightarrow c = -1$ ó $c = 2$. $c = 2$ es imposible y $c = -1 \Rightarrow t = -1/2$.

De c) obtenemos nuevamente la ecuación (i) de la proposición 3.3 con la partición $1 \mid -1/2 \mid \mathbb{Z}_{p}^{*} \setminus \{1, -1/2\}$.

1.1.2. $|A| = 1$, B y C están en progresión aritmética con la misma diferencia ($|B|, |C| \geq 2$).

En este caso (y algunos otros que siguen) haremos uso de un lema probado por Olson y Mann en [MO].

Lema 3.1 (Mann,Olson) *Sea* $A = \{a + id \mid 0 \leq i \leq k\} \subset \mathbb{Z}_p$, *tal que* $1 \leq k \leq p-3$. *Si* $A = \{a' + id' \mid 0 \leq i \leq k\}$, *entonces se cumple que* $d \equiv \pm d' \bmod p$.

Podemos suponer que

$$A = [k],\ B = [1, k-1],\ C = [k+1, p-1], \tag{3.4}$$

(donde $3 \leq k \leq p-3$) en el caso más general. Si $A = [1]$, entonces tenemos $B = [2, k]$ y $C = [k+1, p-1]$ $(3 \leq k \leq p-3)$ que se resuelve exactamente como el caso más general. Si $A = [2]$, entonces es fácil ver que B y C no pueden escribirse como progresiones aritméticas con diferencia 1. Así, es suficiente remitirnos al planteamiento hecho en (3.4). Con A, B y C definidas de esta forma

$$\begin{array}{rcl} A+B & = & [k+1, 2k-1], \\ A+C & = & [2k+1, k-1] \text{ y} \\ B+C & = & [k+2, k-2]. \end{array}$$

y (3.2) es entonces equivalente a

$$\left\{ \begin{array}{r} [k+1, 2k-1] \cap c[k+1, p-1] = \emptyset \\ [2k+1, k-1] \cap c[1, k-1] = \emptyset \\ [k+2, k-2] \cap ck = \emptyset \end{array} \right\} \tag{3.5}$$

$$\Leftrightarrow \left\{ \begin{array}{c} c[k+1, p-1] \subseteq \overline{[k+1, 2k-1]} = [2k, k] \\ c[1, k-1] \subseteq \overline{[2k+1, k-1]} = [k, 2k] \\ ck \in \overline{[k+2, k-2]} = \{k-1, k, k+1\} \end{array} \right\}. \tag{3.6}$$

Se tiene que

$$p - 4 \geq |[k+1, p-1]| = p - k - 1 \geq 2 \text{ y } |[2k, k]| = p - k,$$

$$p - 4 \geq |[1, k-1]| = k - 1 \geq 2 \text{ y } |[k, 2k]| = k + 1,$$

y las dos primeras contenciones de (3.6) nos dicen que una progresión aritmética con diferencia c es una subprogresión de otra progresión con diferencia 1. Se cumplen las condiciones del lema 3.1 y por lo tanto, $c = \pm 1$. Es evidente que si $c = 1$, entonces en (3.5) ninguna de las tres intersecciones es vacía. Si $c = -1$, entonces

$$-k \in \{k-1, k, k+1\} \Leftrightarrow k \in \{1/2, 0, -1/2\},$$

pero $k \neq 0$. Luego, obtenemos nuevamente la proposición 3.3 con las particiones

$$\begin{array}{llll} A = \left\{\frac{p+1}{2}\right\} & B = \left[1, \frac{p-1}{2}\right], & C = \left[\frac{p-3}{2}, p-1\right] & y \\ A = \left\{\frac{p-1}{2}\right\} & B = \left[1, \frac{p-3}{2}\right], & C = \left[\frac{p+1}{2}, p-1\right]. & \end{array}$$

1.1.3. A, B y C están en progresión aritmética con la misma diferencia ($|A|, |B|, |C| \geq 2$).

Entonces, es fácil ver que podemos suponer

$$A = [1,k],\ B = [k+1,l],\ C = [l+1,p-1],$$

con la condición de que $2 \leq k \leq l-2 \leq p-5$ y se tiene que

$$\begin{array}{rcl} A+B & = & [k+2,k+l], \\ A+C & = & [l+2,k-1] \ \text{y} \\ B+C & = & [k+l+2,l-1]. \end{array}$$

Luego (3.2) es equivalente a

$$\left\{\begin{array}{c} [k+2,k+l] \cap c[l+1,p-1] = \emptyset \\ [l+2,k-1] \cap c[k+1,l] = \emptyset \\ [k+l+2,l-1] \cap c[1,k] = \emptyset \end{array}\right\} \tag{3.7}$$

$$\Leftrightarrow \left\{\begin{array}{c} c[l+1,p-1] \subseteq \overline{[k+2,k+l]} = [k+l+1,k+1] \\ c[k+1,l] \subseteq \overline{[l+2,k-1]} = [k,l-1] \\ c[1,k] \subseteq \overline{[k+l+2,l-1]} = [l,k+l+1] \end{array}\right\}.$$

Como en el caso 1.1.2, se tienen las condiciones del lema 3.1 y por lo tanto $c = \pm 1$. Se repite el análisis ya descrito y se comprueba que $c \neq 1$ (por ejemplo, si $c = 1$, la segunda intersección de (3.7) no se cumple) y que $c = -1$, se cumple la proposición 3.3 con las particiones que cumplen (3.7).

1.2. $|B+C| = |B| + |C|$.

1.2.1. $|A| = 1$, $\overline{C} = \overline{B+C} - B$ y B no está en progresión aritmética.

Como $|A| = 1$, entonces $|B+C| = |B| + |C| = p-2 \Leftrightarrow \left|\overline{B+C}\right| = 2$. Por tanto, $\overline{B+C}$ está en progresión aritmética (ya que un conjunto

con dos elementos siempre está en progresión aritmética) y podemos suponer que

$$\overline{B+C} = [0,1] \text{ y } A = [1].$$

Como $\left|\overline{B+C} - B\right| = \left|\overline{B+C}\right| + |B|$ (véase la demostración del teorema 2.5, parte (iii)$\Rightarrow$ (2.8)) y $\left|\overline{B+C}\right| = 2$, entonces por la condición (iv) del mismo teorema, $-B$ es una unión de dos progresiones aritméticas con diferencia 1 y nuevamente se puede suponer que

$$B = [2, l-1] \cup [m, n-1],$$

donde $3 \leq l+1 \leq m \leq n-1 \leq p-1$. Así

$$\begin{aligned} \overline{C} &= \overline{B+C} - B = [0,1] - ([2,l-1] \cup [m,n-1]) \\ &= [0,1] + ([p-n+1, p-m] \cup [p-l+1, p-2]) \\ &= [p-n+1, p-m+1] \cup [p-l+1, p-1] \end{aligned}$$

$$\Leftrightarrow C = [0, p-n] \cup [p-m+2, p-l].$$

Pero $0 \in C$ y $A = [1] \subset C$, que es una contradicción porque A, B y C son una partición de $\mathbb{Z}_p^*$.

1.2.2. $|A| = 1$ ó A en progresión aritmética con diferencia d, $B = \{b, b+d\}$ y C es la unión de dos progresiones aritméticas con diferencia d.

Sin perder generalidad, podemos suponer que

a) $A = [1]$, $B = [k, k+1]$ y $C = [2, k-1] \cup [k+2, p-1]$ tal que $3 \leq k \leq p-3$ ó

b) $A = [1, k]$, $B = [l, l+1]$ y $C = [k+1, l-1] \cup [l+2, p-1]$ tal que $2 \leq k \leq l-2 \leq p-5$.

Para el caso a) se tiene que

$$\begin{aligned} A+B &= [k+1, k+2], \\ A+C &= [3,k] \cup [k+3, p-1] \cup [0] \text{ y} \\ B+C &= [k+2, 2k] \cup [2k+2, k]. \end{aligned}$$

Luego (3.2) es equivalente a que

$$\left\{ \begin{array}{r} [k+1, k+2] \cap c([2,k-1] \cup [k+2, p-1]) = \emptyset \\ ([3,k] \cup [k+3, p-1] \cup [0]) \cap c[k, k+1] = \emptyset \\ ([k+2, 2k] \cup [2k+2, k]) \cap c = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{c} c([2,k-1]\cup[k+2,p-1]) \subseteq \overline{[k+1,k+2]} \\ = [0,k]\cup[k+3,p-1] \\ c[k,k+1] \subseteq \overline{[3,k]\cup[k+3,p-1]\cup[0]} = [1,2]\cup[k+1,k+2] \\ c \in \overline{[k+2,2k]\cup[2k+2,k]} = [k+1]\cup[2k+1] \end{array} \right\}.$$

De la primera relación de lo anterior se tiene que

$$|[2,k-1]| = k-2 \text{ y } |[k+2,p-1]| = p-k-2,$$

$$|[0,k]| = k+1 \text{ y } |[k+3,p-1]| = p-k-3.$$

La contención es posible si y sólo si

$$c[2,k-1] \subseteq [k+3,p-1] \text{ y } c[k+2,p-1] \subseteq [0,k],$$

es decir,

$$k-2 \leq p-k-3 \Leftrightarrow k \leq \frac{p-1}{2} \text{ y}$$

$$p-k-2 \leq k+1 \Leftrightarrow k \geq \frac{p-3}{2}$$

y esto es equivalente a que $\frac{p-3}{2} \leq k \leq \frac{p-1}{2}$ (k puede tomar dos valores).

Si $k = \frac{p-3}{2}$, entonces de la segunda relación se tiene que

$$c\left[\frac{p-3}{2}, \frac{p-1}{2}\right] \subset [1,2] \cup \left[\frac{p-1}{2}, \frac{p+1}{2}\right],$$

que es imposible para cualquier $c \in \mathbb{Z}_p^*$.

Si $k = \frac{p-1}{2}$, entonces de la segunda relación se obtiene que

$$c\left[\frac{p-1}{2}, \frac{p+1}{2}\right] \subset [1,2] \cup \left[\frac{p+1}{2}, \frac{p+3}{2}\right],$$

que también es imposible para toda $c \in \mathbb{Z}_p^*$.

Para el caso b) hay dos posibilidades: $k = 2$ y $k \geq 3$.

Si $k = 2$, entonces

$$A = [1,2],\ B = [l,l+1] \text{ y } C = [3,l-1]\cup[l+2,p-1].$$

Por otra parte,

$$\begin{array}{lcl} A+B & = & [l+1,l+3], \\ A+C & = & [4,l+1]\cup[l+3,p-1]\cup[0,1] \text{ y} \\ B+C & = & [l+3,2l]\cup[2l+2,l]. \end{array}$$

Entonces (3.2) es equivalente a que

$$\left\{\begin{array}{c}[l+1,l+3]\cap c([3,l-1]\cup[l+2,p-1])=\emptyset\\ ([4,l+1]\cup[l+3,p-1]\cup[0,1))\cap c[l,l+1]=\emptyset\\ ([l+3,2l]\cup[2l+2,l])\cap c[1,2]=\emptyset\end{array}\right\}$$

$$\Leftrightarrow\left\{\begin{array}{c}c([3,l-1]\cup[l+2,p-1])\subseteq\overline{[l+1,l+3]}\\ =[0,l]\cup[l+4,p-1]\\ c[l,l+1]\subseteq\overline{[4,l+1]\cup[l+3,p-1]\cup[0,1]}=[2,3]\cup[l+2]\\ c[1,2]\subseteq\overline{[l+3,2l]\cup[2l+2,l]}=[l+1,l+2]\cup[2l+1]\end{array}\right\}.$$

De la tercera relación se obtiene que

$$c=l+1\ \text{ y }\ 2c=l+2\Leftrightarrow l=0,$$

que es imposible porque $l\geq 4$. Por lo tanto, se tiene que

$$c=l+2\ \text{ y }\ 2c=l+1\Leftrightarrow l=p-3$$

y luego, la segunda relación se transforma en

$$c[p-3,p-2]\subseteq[2,3]\cup[p-1]\Leftrightarrow c=-1$$

y nuevamente obtenemos la proposición 3.3 con las particiones que satisfacen el sistema anterior de relaciones.

Si $k\geq 3$, entonces

$$\begin{array}{rcl}A+B&=&[l+1,k+l+1],\\ A+C&=&[k+2,k-1]\ \text{ y}\\ B+C&=&[k+l+1,2l]\cup[2l+2,l].\end{array}$$

En este caso (3.2) se convierte en

$$\left\{\begin{array}{c}[l+1,k+l+1]\cap c([k+1,l-1]\cup[l+2,p-1])=\emptyset\\ [k+2,k-1]\cap c[l,l+1]=\emptyset\\ ([k+l+1,2l]\cup[2l+2,l])\cap c[1,k]=\emptyset\end{array}\right\}$$

$$\Leftrightarrow\left\{\begin{array}{c}c([k+1,l-1]\cup[l+2,p-1])\subseteq\overline{[l+1,k+l+1]}\\ =[k+l+2,l]\\ c[l,l+1]\subseteq\overline{[k+2,k-1]}=[k,k+1]\\ c[1,k]\subseteq\overline{[k+l+1,2l]\cup[2l+2,l]}=[2l+1]\cup[l+1,k+l]\end{array}\right\}.$$

De la segunda relación tenemos dos posibilidades. Si

$$\left\{\begin{array}{c} cl = k \\ c(l+1) = k+1 \end{array}\right\} \Leftrightarrow k = l,$$

entonces el sistema anterior se transforma en

$$\left\{\begin{array}{c} c([l+1, l-1] \cup [l+2, p-1]) \subseteq [2l+2, l] \\ c[l, l+1] = [l, l+1] \\ c[1, l] \subseteq [l+1, 2l+1] \end{array}\right\}.$$

Luego, de la segunda relación se tiene que $c = 1$ y con esto la primera relación es imposible. Si, por otra parte,

$$\left\{\begin{array}{c} cl = k+1 \\ c(l+1) = k \end{array}\right\} \Leftrightarrow k = p-1-l,$$

entonces

$$\left\{\begin{array}{c} c([p-l, l-1] \cup [l+2, p-1]) \subseteq [1, l] \\ c[l, l+1] = [p-1-l, p-l] \\ c[1, p-1-l] \subseteq [2l+1, p-1] \end{array}\right\}.$$

Luego, de la segunda relación se tiene que $l = \frac{p-1}{2}$ y así la primera relación se convierte en

$$c\left(\left[\frac{p-3}{2}, \frac{p+1}{2}\right] \cup \left[\frac{p+3}{2}, p-1\right]\right) \subseteq \left[1, \frac{p-1}{2}\right]$$

que evidentemente es imposible para cualquier $c \in \mathbb{Z}_p^*$.

1.2.3. $|A| = 1$ ó A en progresión aritmética con diferencia d, B y C están en progresión aritmética y casi aritmética respectivamente, con la misma diferencia d.

Es fácil ver que si $|A| = 1$, entonces hay dos posibilidades

a) $A = [2]$, $B = [3, k]$ y $C = [k+1, p-1] \cup [1]$ tal que $5 \leq k \leq p-2$ y

b) $A = [l]$, $B = [1, k]$ y $C = [k+1, l-1] \cup [l+1, p-1]$ tal que $3 \leq k \leq l-2 \leq p-4$.

Para el caso a)

$$\begin{aligned} A+B &= [5,k+2], \\ A+C &= [k+3,p-1]\cup[0,1]\cup[3] \ \text{ y} \\ B+C &= [k+4,p-1]\cup[0,k+1]. \end{aligned}$$

Entonces

$$\left\{ \begin{array}{c} [5,k+2]\cap c([k+1,p-1]\cup[1]) = \emptyset \\ ([k+3,p-1]\cup[0,1]\cup[3])\cap c[3,k] = \emptyset \\ ([k+4,p-1]\cup[0,k+1])\cap 2c = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{c} c([k+1,p-1]\cup[1]) \subseteq \overline{[5,k+2]} = [k+3,p-1]\cup[0,4] \\ c[3,k] \subseteq \overline{[k+3,p-1]\cup[0,1]\cup[3]} = [2]\cup[4,k+2] \\ 2c \in \overline{[k+4,p-1]\cup[0,k+1]} = [k+2,k+3] \end{array} \right\}.$$

Como

$$\begin{aligned} p-k &= |[k+1,p-1]\cup[1]| \\ &\leq |[k+3,p-1]\cup[0,4]| = p-k+2 \end{aligned}$$

y la contención de la primera relación del sistema anterior muestra que hay dos progresiones aritméticas con diferencia c contenidas en una progresión de diferencia 1, entonces se cumplen las condiciones del lema 3.1 y así $c = \pm 1$. Se ve sin dificultad que si $c = 1$, entonces la segunda relación del sistema anterior es imposible. Si $c = -1$, entonces se tiene que

$$\left\{ \begin{array}{c} [1,p-k-1]\cup[p-1] \subseteq [0,4]\cup[k+3,p-1] \\ [p-k,p-3] \subseteq [2]\cup[4,k+2] \\ -2 \in [k+2,k+3] \end{array} \right\}.$$

De la tercera relación se tiene que $k = p-4$ ó $k = p-5$ y para ambas posibilidades las relaciones anteriores se cumplen. Se tiene la proposición 3.3 otra vez.

Para el caso b)

$$\begin{aligned} A+B &= [l+1,k+l], \\ A+C &= [0,l-1]\cup[k+l+1,2l-1]\cup[2l+1,p-1] \ \text{ y} \\ B+C &= [0,k-1]\cup[k+2,p-1]. \end{aligned}$$

Entonces

$$\left\{\begin{array}{c} [l+1,k+l]\cap c([k+1,l-1]\cup[l+1,p-1])=\emptyset \\ ([0,l-1]\cup[k+l+1,2l-1]\cup[2l+1,p-1])\cap c[1,k]=\emptyset \\ ([0,k-1]\cup[k+2,p-1])\cap cl=\emptyset \end{array}\right\}$$

$$\Leftrightarrow \left\{\begin{array}{c} c([k+1,l-1]\cup[l+1,p-1])\subseteq\overline{[l+1,k+l]} \\ =[0,l]\cup[k+l+1,p-1] \\ c[1,k]\subseteq\overline{[0,l-1]\cup[k+l+1,2l-1]\cup[2l+1,p-1]} \\ =[l,k+l]\cup[2l] \\ cl\in\overline{[0,k-1]\cup[k+2,p-1]}=[k,k+1] \end{array}\right\}. \quad (3.8)$$

Como

$$\begin{array}{rcl} p-k-2 & = & |[k+1,l-1]\cup[l+1,p-1]| \\ & \leq & |[0,l]\cup[k+l+1,p-1]|=p-k \end{array}$$

y la primera contención de (3.8) indica que dos progresiones aritméticas con diferencia c son subprogresiones de otra con diferencia 1, se cumplen las condiciones del lema 3.1 y por lo tanto $c=\pm 1$. Si $c=1$, entonces la segunda relación de (3.8) es imposible. Si $c=-1$, entonces

$$\left\{\begin{array}{c} [1,p-l-1]\cup[p-l+1,p-k-1]\subseteq[0,l]\cup[k+l+1,p-1] \\ [p-k,p-1]\subseteq[l,k+l]\cup[2l] \\ -l\in[k,k+1] \end{array}\right\}$$

y estas relaciones se cumplen para $k=p-l$ ó $k=p-l-1$. Así se tiene nuevamente la proposición 3.3.

Si A está en progresión aritmética, entonces no es difícil ver que podemos suponer que

$$A=[k,l]\,,\ B=[l+1,m]\ \text{ y }\ C=[m+1,p-1]\cup[1,k-1]\,,$$

donde $3\leq k+1\leq l$ y $l+2\leq m\leq p-2$. Luego

$$\begin{array}{rcl} A+B & = & [k+l+1,l+m]\,, \\ A+C & = & [0,k+l-1]\cup[k+m+1,p-1] \text{ y} \\ B+C & = & [0,k+m-1]\cup[l+m+2,p-1]\,. \end{array}$$

Entonces se tiene que

$$\left\{\begin{array}{c} [k+l+1,l+m]\cap c([m+1,p-1]\cup[1,k-1])=\emptyset \\ ([0,k+l-1]\cup[k+m+1,p-1])\cap c[l+1,m]=\emptyset \\ ([0,k+m-1]\cup[l+m+2,p-1])\cap c[k,l]=\emptyset \end{array}\right\}$$

$$\Leftrightarrow \left\{ \begin{array}{c} c([m+1,p-1]\cup[1,k-1]) \subseteq \overline{[k+l+1,l+m]} \\ = [l+m+1,p-1]\cup[0,k+l] \\ c[l+1,m] \subseteq \overline{[0,k+l-1]\cup[k+m+1,p-1]} \\ = [k+l,k+m] \\ c[k,l] \subseteq \overline{[0,k+m-1]\cup[l+m+2,p-1]} \\ = [k+m,l+m+1] \end{array} \right\}.$$

Siguiendo el procedimiento descrito anteriormente y aplicando el lema 3.1 se obtiene nuevamente la proposición 3.3.

1.3. $|B+C| = |B| + |C| + 1$.

1.3.1. $|A| = 1$, $\overline{B} = (d-C)\cup\{t_1,t_2\}$ para $d \notin B+C$ y $t_1,t_2 \in \mathbb{Z}_p^*$ tales que $t_1 \neq t_2$.

Sea $A = \{c-1\}$, $c \neq 1$. Entonces

$$\overline{B} = (d-C)\cup\{t_1,t_2\} = C\cup\{0,c-1\}.$$

Como $t_1,t_2 \notin d-C \Leftrightarrow d-t_1, d-t_2 \notin C$, luego

$$\overline{B} = d-(C\cup\{d-t_1,d-t_2\}) = C\cup\{0,c-1\}$$

$$\Leftrightarrow d-\overline{B} = C\cup\{d-t_1,d-t_2\} = d-(C\cup\{0,c-1\}).$$

Por otra parte, $t_1,t_2 \notin B \Leftrightarrow t_1,t_2 \in C\cup\{0,c-1\}$. La relación anterior muestra también que $d-t_1, d-t_2 \notin B$. Esto es equivalente a que $d-t_1 = 0$ y $d-t_2 = c-1 \Leftrightarrow t_1 = d$ y $t_2 = d-c+1$. Entonces

$$\begin{array}{rcl} d-(C\cup\{0,c-1\}) & = & C\cup\{0,c-1\} \text{ y} \\ d-B & = & B. \end{array} \qquad (3.9)$$

O sea, B y $C\cup\{0,c-1\}$ están formados por pares de elementos que suman d. Así (3.2) se escribe como

$$\left\{ \begin{array}{c} (c-1+B)\cap cC = \emptyset \\ (c-1+C)\cap cB = \emptyset \\ (B+C)\cap c(c-1) = \emptyset \end{array} \right\}. \qquad (3.10)$$

Como $|B+C| = p-1$ (véase el caso (ii) del teorema 2.6 y su demostración) y $d, c(c-1) \notin B+C$, entonces

$$d = c(c-1). \qquad (3.11)$$

Sean $A' = A-1 = \{c-2\}$, $B' = B-1$ y $C' = C-1$. Evidentemente, $\mathbb{Z}_p \setminus \{-1\} = c-2 \mid B' \mid C'$. Nótese que (ver (3.9))

$$\begin{aligned} d-2-B' &= B' \text{ y} \\ d-2-(C' \cup \{c-2,-1\}) &= C' \cup \{c-2,-1\}. \end{aligned} \tag{3.12}$$

Con estas definiciones, (3.10) es equivalente a

$$\left\{ \begin{array}{r} (c+B') \cap (cC'+c) = \emptyset \\ (c+C') \cap (cB'+c) = \emptyset \\ (B'+C'+2) \cap c(c-1) = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{r} B' \cap cC' = \emptyset \\ C' \cap cB' = \emptyset \\ (B'+C') \cap c^2 - c - 2 = \emptyset \end{array} \right\}. \tag{3.13}$$

El elemento $-1/c$ no está en B' ó no está en C' y por lo tanto podemos suponer que $-1/c \notin B' \Rightarrow -1 \notin cB'$. Entonces, de la segunda relación de (3.13) se tiene que

$$cB' \subset \overline{C'} = B' \cup \{c-2,-1\}$$

y por lo anterior esto implica que

$$cB' \subset B' \cup \{c-2\}. \tag{3.14}$$

Se tiene el siguiente

Lema 3.2 *Si se cumple (3.14), entonces*

(i) $cB' = B'$, *si* $c-2 \notin cB'$ *ó*

(ii) $c(B' \cup \{c-2\}) = B' \cup \{c-2\}$, *si* $c-2 \in cB'$.

Demostración. La primera afirmación es evidente. Para probar la segunda, sea $B' = \{b_1, b_2, ..., b_r\}$, $2 \leq r \leq p-4$ ($|A'| = 1, |B'|, |C'| \geq 2$ y $|A'| + |B'| + |C'| = p-1$). Como $c-2 \in cB'$, entonces existe $b_i \in B'$ $(1 \leq i \leq r)$ tal que $cb_i = c-2 \Leftrightarrow b_i = \frac{c-2}{c}$. Sin perder generalidad, podemos suponer que $i = 1$. Entonces existe $b_2 \in B'$ tal que $cb_2 = \frac{c-2}{c} \Leftrightarrow b_2 = \frac{c-2}{c^2}$. Siguiendo este procedimiento, llegamos a que existe $b_{n-1} \in B'$ tal que $cb_{n-1} = \frac{c-2}{c^{n-2}} \Leftrightarrow b_{n-1} = \frac{c-2}{c^{n-1}}$, $n-1 \leq r$ y

$c^n = 1$ (es decir $\langle c\rangle = \{1, c, c^2, ..., c^{n-1}\}$ y c no es raíz primitiva, porque de lo contrario, $\langle c\rangle = \mathbb{Z}_p^*$). Así

$$\begin{aligned} B' &= \left\{\tfrac{c-2}{c}, \tfrac{c-2}{c^2}, ..., \tfrac{c-2}{c^{n-1}}, b_n, b_{n+1}, ..., b_r\right\} \\ &= \{c(c-2), c^2(c-2), ..., c^{n-1}(c-2), b_n, b_{n+1}, ..., b_r\} \\ &\subset cB' \cup c\{c-2\}, \end{aligned}$$

donde $c\{b_n, b_{n+1}, ..., b_r\} = \{b_n, b_{n+1}, ..., b_r\}$ (nótese que este conjunto puede ser vacío). Como $c-2 \notin B'$, entonces $b_{n-1} = c(c-2) \notin cB'$ y $b_{n-1} \in B'$. Luego

$$\begin{aligned} B' \cup \{c-2\} &\subseteq cB' \cup c\{c-2\} \text{ y} \\ cB' \cup c\{c-2\} &\subseteq B' \cup \{c-2\}, \end{aligned}$$

por lo tanto, se tiene la igualdad. ∎

Lema 3.3 *Si $A \subset \mathbb{Z}_p^*$ y $g \in \mathbb{Z}_p^*$ (g no es raíz primitiva), entonces $gA = A$ si y sólo si A es una unión de clases laterales módulo el subgrupo generado por g, $\langle g\rangle$.*

Demostración. $gA = A \Leftrightarrow \langle g\rangle A = A \Leftrightarrow A = \bigcup_{a\in A} \langle g\rangle a.$ ∎

Obsérvese que si $A \subset \mathbb{Z}_p$, entonces $gA = A$ si y sólo si $A \setminus \{0\}$ es una unión de clases laterales módulo $\langle g\rangle$. Es bien conocido además (véase, por ejemplo [NZM]) que si g no es una raíz primitiva, entonces

$$\sum_{g\in\langle g\rangle} g \equiv 0 \bmod p$$

y como consecuencia inmediata, si $A \subset \mathbb{Z}_p^*$ es una unión de clases laterales módulo $\langle g\rangle$, entonces

$$\sum_{a\in A} a \equiv 0 \bmod p.$$

El lema 3.2 abre dos posibilidades:

CASO 1: $cB' = B'$ (y $c(C' \cup \{c-2, -1\}) = C' \cup \{c-2, -1\}$). Esta condición es equivalente a que B' es una unión de clases laterales módulo $\langle c\rangle$ y por lo tanto

$$\sum_{b'\in B'} b' \equiv 0 \bmod p.$$

Por (3.12), $d-2-B'=B'$ y de aquí

$$0 \equiv \sum_{b' \in B'} b' \equiv \sum_{b' \in B'} (d-2-b') \equiv |B'|\,(d-2) \bmod p \Leftrightarrow d-2=0.$$

Así las relaciones (3.12) se convierten en

$$\begin{aligned} -B' &= B' \text{ y} \\ -(C' \cup \{c-2,-1\}) &= C' \cup \{c-2,-1\}. \end{aligned}$$

Por otra parte de (3.11) y (3.12) se tiene que

$$c^2-c-2-B'=B'.$$

Así

$$\left\{ \begin{array}{r} -B'=B' \\ c^2-c-2-B'=B' \end{array} \right\}$$

y entonces $c^2-c-2=0 \Leftrightarrow c=-1$ ó $c=2$.

Si $c=-1$, obtenemos nuevamente la proposición 3.3. En este caso, las particiones que ilustran que esta ecuación no es tensa son

$$\mathbb{Z}_p \setminus \{-1\} = -3 \mid B' \mid C',$$

donde B' y C' están formados por pares de elementos que suman 0 y $1,3 \in C'$. Esto es, $\mathbb{Z}_p^* = -2 \mid B \mid C$, donde B y C están formados por pares que suman 1 y $2 \in C$.

Si $c=2$, entonces $-B'=B'$ y $2B'=B'$ que es equivalente a que la clase lateral $\{2,-2\}$, denotada por $\widehat{2}$, no genera al grupo cociente $\mathbb{Z}_p^*/\{1,-1\}$ (recordemos que $\{1,-1\}$ es subgrupo propio de $\mathbb{Z}_p^*$ para todo primo p). Así se tiene la siguiente

Proposición 3.5 *La ecuación*

$$x+y=2z$$

es no tensa para todo primo p tal que $\langle\widehat{2}\rangle \neq \mathbb{Z}_p^*/\{1,-1\}$.

En este caso, una partición que ilustra la no tensión sería

$$1 \mid \langle 2\rangle + 1 \mid \mathbb{Z}_p^* \setminus \{1, \langle 2\rangle + 1\}.$$

Los primeros números primos ($p < 300$) para los que $\langle 2\rangle \neq \mathbb{Z}_p^* / \{1, -1\}$ son

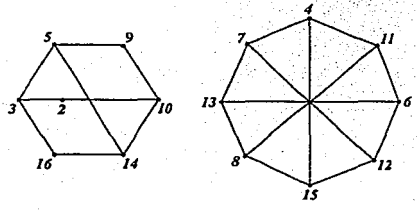
$$17, 31, 41, 43, 73, 89, 97, 109, 113, 127, 137, 151, 157, 193,$$
$$223, 229, 233, 241, 251, 257, 277, 281, 283.$$

Es un problema abierto caracterizar estos primos.

Ejemplo 3.2 *Para $p = 17$, la ecuación $x + y = 2z$ es no tensa con la partición*

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

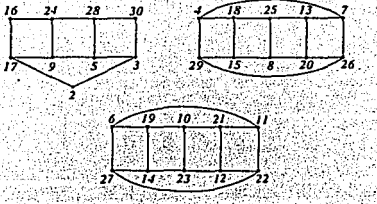
La siguiente figura ilustra la $Tr(1)$ de la ecuación $x + y = 2z$ para $p = 17$.



Ejemplo 3.3 *Para $p = 31$, la ecuación $x + y = 2z$ es no tensa con la partición $1 \mid S \mid \mathbb{Z}_{31}^* \setminus S$, donde*

$$S = \{2, 3, 5, 9, 16, 17, 24, 28, 30\}.$$

A continuación, se muestra la $Tr(1)$ de la ecuación $x + y = 2z$ para $p = 31$.



CASO 2: $c(B' \cup \{c-2\}) = B' \cup \{c-2\}$ (y $c(C' \cup \{-1\}) = C' \cup \{-1\}$). Esta condición es equivqlente a que $B' \cup \{c-2\}$ es una unión de clases laterales módulo $\langle c \rangle$ y por lo tanto

$$\sum_{b' \in B'} b' + c - 2 \equiv 0 \bmod p.$$

Por (3.12), $d - 2 - B' = B'$ y de aquí

$$\begin{array}{rrcl} & \sum_{b' \in B'} (d-2-b') & \equiv & \sum_{b' \in B'} b' \bmod p \\ \Leftrightarrow & |B'|(d-2) & \equiv & 2\sum_{b' \in B'} b' \equiv 2(2-c) \bmod p \\ \Leftrightarrow & d & \equiv & \frac{4-2c}{|B'|} + 2 \bmod p. \end{array}$$

Entonces las relaciones (3.12) son

$$\begin{array}{rcl} \frac{4-2c}{|B'|} - B' & = & B' \text{ y} \\ \frac{4-2c}{|B'|} - (C' \cup \{c-2, -1\}) & = & C' \cup \{c-2, -1\}. \end{array}$$

Así, se tiene que

$$\left\{ \begin{array}{c} \frac{4-2c}{|B'|} - B' = B' \\ c^2 - c - 2 - B' = B' \end{array} \right\}$$

y

$$\frac{4-2c}{|B'|} \equiv c^2 - c - 2 \bmod p \Leftrightarrow c = 2 \text{ ó } c = -1 - \frac{2}{|B'|}.$$

Si $c = 2$, entonces obtenemos la proposición 3.5. Si $c = -1 - \frac{2}{|B'|}$, entonces

$$\frac{4-2c}{|B'|} = \frac{6|B'|+4}{|B'|^2} \text{ y } c^2 - c - 2 = \frac{6|B'|+4-|B'|^2}{|B'|^2}$$

$$\Leftrightarrow |B'| \equiv 0 \bmod p \Leftrightarrow B' = \emptyset \text{ ó } \mathbb{Z}_p,$$

que es una contradicción.

Para concluir, si $c = 1$, entonces poniendo $A = \{1\}$, (3.2) se escribe como

$$\left\{ \begin{array}{c} (1+B) \cap C = \emptyset \\ (1+C) \cap B = \emptyset \\ (B+C) \cap \{1\} = \emptyset \end{array} \right\}.$$

Como $1 \notin B + C$ y $|B| + |C| = p - 2$, entonces $d = 1$. Como antes, se tiene que $1 - B = B$. Sustituyendo esta igualdad en la segunda relación del sistema anterior, se tiene que

$$(1+C) \cap (1-B) = \emptyset \Leftrightarrow (B+C) \cap \{0\} = \emptyset$$

y así,

$$0, 1 \notin B + C \Leftrightarrow |B + C| = p - 2 \Leftrightarrow |B| + |C| = p - 3,$$

que es una contradicción.

1.3.2. $|A| = 1$ ó A en prog. aritmética con diferencia d, $B = \{b, b+d, b+2d\}$ y C es la unión de dos progresiones aritméticas con diferencia d.

Sin perder generalidad, podemos suponer que

a) $A = [1]$, $B = [k, k+2]$ y $C = [2, k-1] \cup [k+3, p-1]$ tal que $3 \leq k \leq p-4$ ó

b) $A = [1, k]$, $B = [l, l+2]$ y $C = [k+1, l-1] \cup [l+3, p-1]$ tal que $2 \leq k \leq l-2 \leq p-6$.

Este caso se resuelve siguiendo exactamente el procedimiento de 1.2.2.

1.3.3. $|A| = 1$ ó A en progresión aritmética con diferencia d, $B = \{b, b+d\}$ y C es la unión de tres progresiones aritméticas con diferencia d.

Como antes, podemos suponer sin perder generalidad que

a) $A = [k]$, $B = [l.l+1]$ y $C = [1, k-1] \cup [k+1, l-1] \cup [l+2, p-1]$ tal que $2 \leq k \leq l-2 \leq p-5$ ó

b) $A = [k, l]$, $B = [m, m+1]$ y $C = [1, k-1] \cup [l+1, m-1] \cup [m+2, p-1]$ tal que $2 \leq k \leq l-1 \leq m-3 \leq p-7$.

El caso a) se resuelve similarmente al 1.2.3 b). El caso b) sigue otra vez el procedimiento de 1.2.3 para cuando A está en progresión aritmética.

1.3.4. $|A| = 1$, B en progresión aritmética con diferencia d y C es la unión de dos o tres progresiones aritméticas con diferencia d (de la forma descrita en la condición (vi) del teorema 2.6).

Se pueden dar dos casos que, sin perder generalidad, podemos suponer que son:

a) $A = [p-1]$, $B = [k,l]$ y $C = [1,k-1] \cup [l+1, p-2]$ tal que $2 \leq k \leq l-2 \leq p-5$.

b) $A = [k]$, $B = [l,m]$ y $C = [1,k-1] \cup [k+1, l-1] \cup [m+1, p-1]$ tal que $2 \leq k \leq l-2$ y $l+2 \leq m \leq p-2$,

que se resuelven de manera análoga a como se procede en los casos 1.2.2 y 1.2.3.

Los casos anteriores 1.3.2, 1.3.3 y 1.3.4 resultan ser imposibles en ocasiones y en otras obtenemos que la única posiblidad es que $c = -1$ y nuevamente se tiene la proposición 3.3 con otras particiones que muestran la no tensión. Los cálculos y los argumentos (en especial, el uso del lema 3.1) son exactamente análogos a los descritos en el análisis de los subcasos de 1.2.

3.4 Análisis del Caso 2: $|A+B| = |A| + |B|$

2.1. $|B+C| = |B| + |C|$.

La situación a analizar es: $\overline{B} = \overline{A+B} - A$, A y B no están en progresión aritmética.

Se tiene que $\overline{B} = A \cup C \cup \{0\}$, entonces $0 \in \overline{B}$ y existe $x \in \overline{A+B} \cap A$ tal que $x \neq 0$ ($x \in A \subset \mathbb{Z}_p^*$) y $0 = x - x$. Como $x \notin A+B$, entonces para todo $a \in A$ se cumple que $x - a \in A \cup C \cup \{0\}$ y de aquí se implica que

$$x - (A \cup C \cup \{0\}) = A \cup C \cup \{0\}.$$

Usando el hecho de que $A \cap B \cap C = \emptyset$, podemos concluir también que se verifica $x - B = B$. De la misma forma, $x \notin A+B$ lleva a que para

todo $b \in B$, $x - b \in B \cup C$ (se excluye el 0 porque $x \notin B$) y entonces

$$\begin{aligned} x-(B\cup C) &= B\cup C \text{ y} \\ x-(A\cup\{0\}) &= A\cup\{0\}. \end{aligned}$$

De todo lo anterior se concluye que

$$\left\{\begin{array}{c} x-(A\cup\{0\}) = A\cup\{0\} \\ x-B = B \\ x-C = C \end{array}\right\}. \tag{3.15}$$

Por lo tanto $x \notin (A+B)\cup(A+C)\cup(B+C) \Leftrightarrow x \in \overline{A+B}\cap\overline{A+C}\cap\overline{B+C}$. Por otra parte, (3.2) es equivalente a que

$$\left\{\begin{array}{l} A+B \subseteq \overline{cC} \\ A+C \subseteq \overline{cB} \\ B+C \subseteq \overline{cA} \end{array}\right\}. \tag{3.16}$$

Como $|A+B| = |A|+|B|$ y $\left|\overline{cC}\right| = |A|+|B|+1$, entonces $A+B = \overline{cC}\setminus y$, con $y \in \overline{cC}$. De manera similar, $B+C = \overline{cA}\setminus z$, con $z \in \overline{cA}$. Así se tiene que $\overline{A+B} = cC\cup y$ y $\overline{B+C} = cA\cup z$.

Si $|A+C| = |A|+|C|$, entonces análogamente, $\overline{A+C} = cB\cup w$, con $w \in \overline{cB}$. En este caso,

$$x \in (cC\cup y)\cap(cB\cup w)\cap(cA\cup z).$$

Si $x \in cC$, entonces $x = w = z \in cC$. Supongamos que $y \in A$. Como $y \notin A+B$, repitiendo el proceso anterior se llega a que

$$\left\{\begin{array}{c} y-(A\cup\{0\}) = A\cup\{0\} \\ y-B = B \\ y-C = C \end{array}\right\}$$

y así $x-B = B = y-B$ y $x-C = C = y-C \Leftrightarrow x = y$, que es una contradicción ($x \in cC$, $y \in \overline{cC}$). Si $y \in B$ ó $y \in C$, este mismo análisis lleva a la conclusión de que $x = y$. Repitiendo un razonamiento análogo, llegamos a la misma contradicción si $x \in cB$ ó $x \in cA$.

Si $|A+C| = |A|+|C|+1$, entonces $\overline{A+C} = cB$ y de esto se tiene que

$$x \in (cC\cup y)\cap cB\cap(cA\cup z).$$

Esto es posible si y sólo si $x = y = z \in cB$. Seleccionemos $t \in \overline{A+C}$ tal que $t \neq x$. Este elemento t existe, porque $|\overline{A+C}| \geq 2$ (véase la condición (iii) del teorema 2.5 y su demostración). Nuevamente aplicamos el procedimiento descrito para t en A, B, C para llegar a la contradicción $x = t$.

Obsérvese que en este caso, se ha demostrado que no existe partición $\mathbb{Z}_p^* = A \mid B \mid C$ tal que

a) $|A+B| = |A| + |B|$,
b) $|B+C| = |B| + |C|$ y
c) $\overline{B} = \overline{A+B} - A$.

2.2. $|B+C| = |B| + |C| + 1$.

Analizaremos la condición (iii) del teorema 2.5 para A y B, o sea, $\overline{B} = \overline{A+B} - A$ y A no está en progresión aritmética. Siguiendo el mismo proceso que en el caso 2.1, existe $0 \neq x \in \overline{A+B} \cap A$, tal que $\overline{B} \ni 0 = x - x$, entonces se cumplen las igualdades (3.15) y se concluye que $x \in \overline{A+B} \cap \overline{A+C} \cap \overline{B+C}$. Como $|A+B| = |A| + |B|$, entonces por las mismas razones que antes, $\overline{A+B} = cC \cup y$, con $y \in c\overline{C}$. De la misma forma, $|B+C| = |B| + |C| + 1$ nos conduce a que $\overline{B+C} = cA$. Podemos suponer que $|A+C| = |A| + |C| + 1$ (si $|A+C| = |A| + |C|$, se tendría el caso anterior ya analizado) y así, $\overline{A+C} = cB$. Luego

$$x \in (cC \cup y) \cap cB \cap cA = \emptyset,$$

que es una contradicción.

En conclusión, no existe partición $\mathbb{Z}_p^* = A \mid B \mid C$ tal que

a) $|A+B| = |A| + |B|$,
b) $|B+C| = |B| + |C| + 1$ y
c) $\overline{B} = \overline{A+B} - A$.

3. $|A+B| = |A| + |B| + 1$ y $|B+C| = |B| + |C| + 1$.

3.5 El teorema de clasificación

De las proposiciones 3.1-3.5 se tiene el siguiente

Teorema 3.1 *Las ecuaciones*

$$x + y = cz$$

son tensas para todo $c \in \mathbb{Z}_p^*$, $p \geq 5$, *con las siguientes excepciones que son todas las ecuaciones no tensas:*

(i) $c = p-1, p-2$ *para todo* $p \geq 5$.

(ii) $c = 3, 4$ *para* $p = 7$.

(iii) $c = \frac{1 \pm \sqrt{5}}{2}$ *para todo* $p \equiv 1, 9 \bmod 10$, *donde* $\pm\sqrt{5}$ *denotan las soluciones de la ecuación* $w^2 \equiv 5 \bmod p$.

(iv) $c = 2$ *para todo primo* p *tal que* $\langle \overline{2} \rangle \neq \mathbb{Z}_p^* / \{1, -1\}$.

En general, podemos concluir que salvo pocas excepciones, la mayoría de la ecuaciones del tipo que nos ocupa son tensas. En paraticular, para cada primo p se tienen $p-1$ ecuaciones de este tipo. Si denotamos por $S(p)$ al número de ecuaciones tensas para un primo p dado, entonces

$$p - 3 \leq S(p) \leq p - 6.$$

Obsérvese que este teorema generaliza la proposición 2.1.

Finalmente, del análisis de casos de las secciones anteriores podemos asegurar el hecho de que para que una ecuación $x + y = cz$ sea no tensa es necesario y suficiente analizar las particiones de $\mathbb{Z}_p^*$ con una de las partes de cardinalidad 1. Esto, en el lenguaje de 3-gráficas, significa que una ecuación es no tensa si y sólo si la traza de un elemento no es conexa. Como sabemos que el grupo de automorfismos de la 3-gráfica asociada es transitivo en vértices y que esto implica que todas las trazas de conjuntos de un elemento son isomorfas como gráficas, entonces la no tensión de ecuaciones se reduce a analizar $Tr(1)$. Así tenemos el siguiente

Teorema 3.2 *La ecuación* $x + y = cz$, $c \in \mathbb{Z}_p^*$ *es tensa si y sólo si* $Tr(1)$ *de su 3-gráfica asociada es conexa.*

Capítulo 4

Las ecuaciones tensas y no tensas de tipo $x + by \equiv cz \bmod p$

En el capítulo presente se concluye la clasificación de las ecuaciones de tipo $x + by \equiv cz \bmod p$, con $b \neq 1$, en tensas y no tensas.

4.1 El problema y casos de análisis

En el capítulo anterior se presentó la clasificación de las ecuaciones cuando $b = 1$. Sea entonces $\mathbb{Z}_p^*$ el grupo multiplicativo del campo finito de los residuos módulo un primo $p > 3$ y consideremos la ecuación

$$x + by = cz,$$

donde $b, c \in \mathbb{Z}_p^*$, $b \neq 1$, $c \neq -1$, $bc \neq 1$ y $\frac{b}{c} \neq -1$ (estas condiciones para b y c excluyen las ecuaciones $x + y = cz$, analizadas en el capítulo 2). Se clasificarán las ecuaciones del tipo anterior en tensas y no tensas.

Para ello, necesitaremos la siguiente definición de la teoría de los números y que pueden consultarse en los textos recomendados en la bibliografía. Un entero a se llama *residuo de orden* k si la congruencia $w^k \equiv a \bmod p$ tiene solución, donde k es un divisor de $p-1$. El conjunto de los residuos de orden k forman un subgrupo de orden $\frac{p-1}{k}$. Obsérvese que si a y -1 son residuos de orden k, entonces $-a$ también es un residuo de orden k.

Es fácil observar que tras cálculos relativamente sencillos, para $p = 5, 7$ todas las ecuaciones del tipo en análisis son tensas, luego nos remitiremos al caso en que $p > 7$.

Por el lema 2.1, esta ecuación es no tensa si y sólo si existe una partición $\mathbb{Z}_p^* = A \mid B \mid C$ tal que

$$\left\{\begin{array}{l}(A+bB)\cap cC=\emptyset\\(A+bC)\cap cB=\emptyset\\(B+bA)\cap cC=\emptyset\\(B+bC)\cap cA=\emptyset\\(C+bA)\cap cB=\emptyset\\(C+bB)\cap cA=\emptyset\end{array}\right\}. \tag{4.1}$$

De la misma forma como se hizo en el capítulo anterior y para acotar el número de particiones a analizar, se tiene que (4.1) es equivalente a que

$$\left\{\begin{array}{l}A+bB\subseteq\overline{cC}=cA\cup cB\cup 0\\A+bC\subseteq\overline{cB}=cA\cup cC\cup 0\\B+bA\subseteq\overline{cC}=cA\cup cB\cup 0\\B+bC\subseteq\overline{cA}=cB\cup cC\cup 0\\C+bA\subseteq\overline{cB}=cA\cup cC\cup 0\\C+bB\subseteq\overline{cA}=cB\cup cC\cup 0\end{array}\right\}$$

y usando el hecho de que A, B, C forman una partición y el TCD, lo anterior implica que

$$\left\{\begin{array}{l}|A|+|B|-1\leq|A+bB|\leq|A|+|B|+1\\|A|+|C|-1\leq|A+bC|\leq|A|+|C|+1\\|B|+|A|-1\leq|B+bA|\leq|B|+|A|+1\\|B|+|C|-1\leq|B+bC|\leq|B|+|C|+1\\|C|+|A|-1\leq|C+bA|\leq|C|+|A|+1\\|C|+|B|-1\leq|C+bB|\leq|C|+|B|+1\end{array}\right\}. \tag{4.2}$$

Entonces las partes A, B, C que satisfacen (4.1), cumplen las siguientes igualdades:

$$|X+bY|=|X|+|Y|+i,$$

donde $X, Y \in \{A, B, C\}$, $X \neq Y$ e $i \in \{-1, 0, 1\}$. La estructura de los pares de conjuntos (X, bY) que satisfacen las igualdades anteriores está caracterizada en los teoremas 2.4, 2.5 y 2.6. Con base en estos teoremas, hacemos el mismo análisis de casos que se describe en el capítulo anterior (véanse la página 31 y siguientes). Para el tipo de ecuaciones que se analizan, no todos estos casos son posibles. El siguiente lema, consecuencia del lema 3.1, es de utilidad para detectar los casos que no se pueden dar.

Lema 4.1 *Sean* $\mathbb{Z}_p^* = A \mid B \mid C$ *y* $d, e, f \in \mathbb{Z}_p^*$. *Si*

(i) $|A| = 1$ *ó* A *es una progresión aritmética con diferencia* d,

(ii) B *es una progresión aritmética con diferencia* e *(*$|B| \geq 2$*) y*

(iii) C *es una progresión aritmética, una progresión casi aritmética o la unión de dos otras progresiones aritméticas con diferencia* f *descritas la condición (vi) del teorema 2.6.*

entonces $d = e = f$.

Demostración.
Sean

$$A = \{a + id \mid i = 0, 1, ..., k-1\}, \quad |A| = k \geq 1,$$
$$B = \{b + ie \mid i = 0, 1, ..., l-1\}, \quad |B| = l \geq 2.$$

Entonces $A = \left(\overline{B} \cap \overline{C}\right) \setminus \{0\}$ (el complemento tomado en $\mathbb{Z}_p$) y así la intersección de los complementos de B y C excluyendo al 0 es una progresión aritmética con diferencia d. Como $1 \leq k < p-3$, se tienen las condiciones del lema 3.1 y por lo tanto $d = \pm e$, $d = \pm f$ y $e = \pm f$, de donde se concluye que $d = e = f$. ∎

El lema expresa que si tenemos una partición de $\mathbb{Z}_p^*$ en tres partes, tal que dos de las partes están en progresión aritmética y la tercera es una progresión aritmética, casi aritmética o una unión de progresiones aritméticas, entonces todas estas progresiones tienen la misma diferencia.

Con estas bases, veamos qué casos son posibles para las ecuaciones del tipo que nos ocupan, tomando como referencia los casos analizados en el capítulo 2 (página 31 y siguientes).

Para los casos 1.1.2, 1.1.3, 1.2.2, 1.2.3, 1.3.2, 1.3.3 y 1.3.4, escribiremos (4.1) de la siguiente forma equivalente

$$\left\{ \begin{array}{l} \left(\frac{1}{c}A + \frac{b}{c}B\right) \cap C = \emptyset \\ \left(\frac{1}{c}A + \frac{b}{c}C\right) \cap B = \emptyset \\ \left(\frac{1}{c}B + \frac{b}{c}A\right) \cap C = \emptyset \\ \left(\frac{1}{c}B + \frac{b}{c}C\right) \cap A = \emptyset \\ \left(\frac{1}{c}C + \frac{b}{c}A\right) \cap B = \emptyset \\ \left(\frac{1}{c}C + \frac{b}{c}B\right) \cap A = \emptyset \end{array} \right\}$$

y de aquí se implica que (similarmente a como obtuvimos (4.2))

$$\left\{\begin{array}{l} |A|+|B|-1 \leq \left|\frac{1}{c}A+\frac{b}{c}B\right| \leq |A|+|B|+1 \\ |A|+|C|-1 \leq \left|\frac{1}{c}A+\frac{b}{c}C\right| \leq |A|+|C|+1 \\ |B|+|A|-1 \leq \left|\frac{1}{c}B+\frac{b}{c}A\right| \leq |B|+|A|+1 \\ |B|+|C|-1 \leq \left|\frac{1}{c}B+\frac{b}{c}C\right| \leq |B|+|C|+1 \\ |C|+|A|-1 \leq \left|\frac{1}{c}C+\frac{b}{c}A\right| \leq |C|+|A|+1 \\ |C|+|B|-1 \leq \left|\frac{1}{c}C+\frac{b}{c}B\right| \leq |C|+|B|+1 \end{array}\right\}.$$

Entonces, para cualesquiera pares $\left(\frac{1}{c}X, \frac{b}{c}Y\right)$ y $\left(\frac{1}{c}Y, \frac{b}{c}Z\right)$ tales que $X, Y, Z \in \{A, B, C\}$, $X \neq Y \neq Z$ y que cumplan las condiciones de los casos 1.1.2, 1.1.3, 1.2.2, 1.2.3, 1.3.2, 1.3.3 y 1.3.4 (por ejemplo, el caso 1.1.3 para $X = A, Y = B, Z = C$, sería $\frac{1}{c}A$, $\frac{b}{c}B$, $\frac{1}{c}B$ y $\frac{b}{c}C$ en progresión aritmética con la misma diferencia), se aplica el lema 4.1 y se tiene que $\frac{1}{c} = \frac{b}{c} \Leftrightarrow b = 1$, que es una contradicción con $b \neq 1$.

Se hará uso de la siguiente observación: $\overline{aC} = a\overline{C}$ para todo $a \in \mathbb{Z}_p^*$ y $\mathbb{Z}_p^* = A \mid B \mid C$ porque $\overline{aC} = aA \cup aB \cup 0 = a(A \cup B \cup 0) = a\overline{C}$, donde el complemento se toma en $\mathbb{Z}_p$.

Luego los casos a analizar serán:

1. $|A + bB| = |A| + |B| - 1$.

1.1. $|B + bC| = |B| + |C| - 1$ y $|A| = |B| = 1$.

1.2. $|B + bC| = |B| + |C|$, $|A| = 1$ y $b\overline{C} = \overline{B + bC} - B$.

1.3. $|B + bC| = |B| + |C| + 1$, $|A| = 1$, $\overline{B} = (d - bC) \cup \{t_1, t_2\}$ para algún $d \notin B + bC$ y $t_1, t_2 \in \mathbb{Z}_p^*$ tales que $t_1 \neq t_2$.

2. $|A + bB| = |A| + |B|$.

2.1. $|B + bC| = |B| + |C|$ y la condición (iii) del teorema 2.5 para ambos pares.

2.2. $|B + bC| = |B| + |C| + 1$, la condición (iii) del teorema 2.5 para el par (A, bB) y la condición (iii) del teorema 2.6 para (B, bC).

3. $|A + bB| = |A| + |B| + 1$ y $|B + bC| = |B| + |C| + 1$ (similar al caso 2.2).

Este mismo análisis se haría para todas las combinaciones posibles de los pares (A, bB) y (bA, B) por una parte y (B, bC) y (bB, C) por la otra, pero los resultados son los mismos en todos los casos. Luego, es suficiente analizar solamente los propuestos anteriormente.

4.2 El análisis de casos

1. $|A + bB| = |A| + |B| - 1$.

1.1. $|B + bC| = |B| + |C| - 1$ y $|A| = |B| = 1$.

Sean $A = \{1\}$, $B = \{t\}$, $C = \mathbb{Z}_p^* \setminus \{1, t\}$, $t \neq 1$. Entonces, usando las relaciones (2.1), (4.1) es equivalente a

$$\left\{ \begin{array}{c} (1+bt) \cap cC = \emptyset \\ (1+bC) \cap ct = \emptyset \\ (t+b) \cap cC = \emptyset \\ (t+bC) \cap c = \emptyset \\ (C+b) \cap ct = \emptyset \\ (C+bt) \cap c = \emptyset \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} \frac{1+bt}{c} \cap C = \emptyset \\ \frac{ct-1}{b} \cap C = \emptyset \\ \frac{t+b}{c} \cap C = \emptyset \\ \frac{c-t}{b} \cap C = \emptyset \\ (ct-b) \cap C = \emptyset \\ (c-bt) \cap C = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \frac{1+bt}{c}, \frac{ct-1}{b}, \frac{t+b}{c}, \frac{c-t}{b}, ct-b, c-bt \notin C$$

$$\Leftrightarrow \frac{1+bt}{c}, \frac{ct-1}{b}, \frac{t+b}{c}, \frac{c-t}{b}, ct-b, c-bt \in \{0, 1, t\}. \qquad (4.3)$$

Usaremos las siguientes notaciones: $\alpha = \frac{1+bt}{c}$, $\beta = \frac{ct-1}{b}$, $\gamma = \frac{t+b}{c}$, $\delta = \frac{c-t}{b}$, $\varepsilon = ct - b$ y $\varphi = c - bt$. La aplicación del principio de Dirichlet a (4.3) permite concluir que al menos dos elementos del conjunto $\{\alpha, \beta, \gamma, \delta, \varepsilon, \varphi\}$ tienen el mismo valor en el conjunto $\{0, 1, t\}$. Luego, se verán todas estas posibilidades y que de todas ellas se obtienen contradicciones, es decir, para el caso que nos ocupa, es imposible encontrar ecuaciones no tensas con partición del tipo $1 \mid t \mid \mathbb{Z}_p^* \setminus \{1, t\}$.

(1) $\alpha = \beta = 0$. Entonces

$$\left\{ \begin{array}{c} \frac{1+bt}{c} = 0 \Leftrightarrow t = -\frac{1}{b} \\ \frac{ct-1}{b} = 0 \Leftrightarrow t = \frac{1}{c} \end{array} \right\} \Leftrightarrow b = -c,$$

contradicción con que $b \neq -c$.

(2) $\alpha = \beta = 1$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 1 \Leftrightarrow t = \frac{c-1}{b} \\ \frac{ct-1}{b} = 1 \Leftrightarrow t = \frac{b+1}{c} \end{array}\right\} \Leftrightarrow \begin{array}{l} \frac{c-1}{b} = \frac{b+1}{c} \\ \Leftrightarrow \ c^2 - c - b^2 - b \equiv 0 \bmod p \\ \Leftrightarrow \ (2c-1)^2 \equiv (2b+1)^2 \bmod p \\ \Leftrightarrow \ 2c - 1 = \pm(2b+1) \\ \Leftrightarrow \ c = b+1 \ \text{ó} \ c = -b. \end{array}$$

Si $c = b+1 \Rightarrow t = 1$, contradicción, $t \neq 1$. El otro caso contradice que $b \neq -c$.

(3) $\alpha = \beta = t$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = t \Leftrightarrow t = \frac{1}{c-b} \\ \frac{ct-1}{b} = t \Leftrightarrow t = \frac{1}{c-b} \end{array}\right\} \ (b \neq c) \tag{4.4}$$

Volviendo a aplicar el principio de Dirichlet, al menos dos elementos del conjunto $\{\gamma, \delta, \varepsilon, \varphi\}$ toman el mismo valor en el conjunto $\left\{0, 1, \frac{1}{c-b}\right\}$.

a) $\gamma = \delta = 0$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 0 \Leftrightarrow t = -b \\ \frac{c-t}{b} = 0 \Leftrightarrow t = c \end{array}\right\} \Leftrightarrow b = -c \text{ (véase caso (1))}.$$

b) $\gamma = \delta = 1$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 1 \Leftrightarrow t = c - b \\ \frac{c-t}{b} = 1 \Leftrightarrow t = c - b \end{array}\right\}.$$

Tomando en cuenta (4.4), se tiene que

$$\frac{1}{c-b} = c - b \Leftrightarrow (c-b)^2 = 1 \Leftrightarrow c - b = \pm 1.$$

Si $c = b+1 \Rightarrow t = 1$, contradicción, $t \neq 1$. Si $c = b-1 \Rightarrow t = -1$ y entonces

$$\left.\begin{array}{l} \varepsilon = -2b+1 \\ \varphi = 2b-1 \end{array}\right\} \Leftrightarrow \varepsilon = -\varphi \in \{0, 1, -1\} \text{ y}$$

$\varepsilon = 0 \Leftrightarrow \varphi = 0 \Leftrightarrow b = \frac{1}{2} \Leftrightarrow c = -\frac{1}{2}$, contradicción, $b \neq -c$.
$\varepsilon = 1 \Leftrightarrow \varphi = -1 \Leftrightarrow b = 0$, contradicción, $b \neq 0$.
$\varepsilon = -1 \Leftrightarrow \varphi = 1 \Leftrightarrow b = 1$, contradicción, $b \neq 1$.

c) $\gamma = \delta = t$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = t \Leftrightarrow t = \frac{b}{c-1} \\ \frac{c}{t-b} = t \Leftrightarrow t = \frac{c}{b+1} \end{array}\right\} \Leftrightarrow \frac{b}{c-1} = \frac{c}{b+1} \text{ (véase caso (2)).}$$

d) $\gamma = \varepsilon = 0$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 0 \Leftrightarrow t = -b \\ ct - b = 0 \Leftrightarrow t = \frac{b}{c} \end{array}\right\} \Leftrightarrow -b = \frac{b}{c} \Leftrightarrow c = -1,$$

contradicción, $c \neq -1$.

e) $\gamma = \varepsilon = 1$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 1 \Leftrightarrow t = c - b \\ ct - b = 1 \Leftrightarrow t = \frac{b+1}{c} \end{array}\right\} \Leftrightarrow \begin{array}{l} c - b = \frac{b+1}{c} \\ \Leftrightarrow \quad c^2 - bc - b - 1 \equiv 0 \bmod p \\ \Leftrightarrow \quad (2c-b)^2 \equiv (b+2)^2 \bmod p \\ \Leftrightarrow \quad c = b+1 \text{ ó } c = 1. \end{array}$$

Si $c = b+1 \Rightarrow t = 1$, contradicción, $t \neq 1$ y $c = 1 \Rightarrow b = 0$, contradicción, $b \neq 0$.

f) $\gamma = \varepsilon = t$. Entonces

$$\left\{\begin{array}{l} \frac{t+b}{c} = t \Leftrightarrow t = \frac{b}{c-1} \\ ct - b = t \Leftrightarrow t = \frac{b}{c-1} \end{array}\right\}.$$

Tomando en cuenta (4.4)

$$\frac{1}{c-b} = \frac{b}{c-1} \Leftrightarrow b^2 - bc + c - 1 \equiv 0 \bmod p$$

(véase el caso (3h)).

g) $\gamma = \varphi = 0$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 0 \Leftrightarrow t = -b \\ c - bt = 0 \Leftrightarrow t = \frac{c}{b} \end{array}\right\} \Leftrightarrow -b = \frac{c}{b} \Leftrightarrow c = -b^2$$

y sustituyendo en (4.4), $t = -\frac{1}{b^2+b}$. Con estos valores para c y t se tiene que

$$\varepsilon = -\frac{b^2}{b+1} \in \left\{0, 1, -\frac{1}{b^2+b}\right\}.$$

$\varepsilon = 0 \Leftrightarrow b^2 = 0 \Leftrightarrow b = 0$, contradicción, $b \neq 0$.
$\varepsilon = 1 \Leftrightarrow b^2 + b + 1 \equiv 0 \bmod p \Leftrightarrow (2b+1)^2 \equiv -3 \bmod p \Leftrightarrow -3$ es resto cuadrático módulo p. En ese caso, denotando por $\pm\sqrt{-3}$ las soluciones de la ecuación $w^2 \equiv -3 \bmod p$, se tiene que

$$b = \frac{-1 \pm \sqrt{-3}}{2} \Leftrightarrow c = \frac{1 \pm \sqrt{-3}}{2} \Leftrightarrow t = 1,$$

contradicción, $t \neq 1$.
$\varepsilon = -\frac{1}{b^2+b} \Leftrightarrow b^3 = 1 \Leftrightarrow b^3 - 1 = 0 \Leftrightarrow (b-1)(b^2+b+1) = 0$, pero $b \neq 1$ y $b^2 + b + 1 = 0$ es el caso visto anteriormente.
Este mismo análisis se haría para δ, pero no es necesario porque con los valores de c y t se obtiene $\varepsilon \notin \left\{0, 1, -\frac{1}{b^2+b}\right\}$.

h) $\gamma = \varphi = 1$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = 1 \Leftrightarrow t = c - b \\ c - bt = 1 \Leftrightarrow t = \frac{c-1}{b} \end{array}\right\} \Leftrightarrow c - b = \tfrac{c-1}{b}$$
$$\Leftrightarrow \quad b^2 - bc + c - 1 \equiv 0 \bmod p \Leftrightarrow (2b-c)^2 \equiv (c-2)^2 \bmod p$$
$$\Leftrightarrow \quad b = c - 1 \text{ ó } b = 1.$$

Pero $b \neq 1$ y $b = c - 1 \Rightarrow t = 1$, contradicción, $t \neq 1$.

i) $\gamma = \varphi = t$. Entonces

$$\left.\begin{array}{l} \frac{t+b}{c} = t \Leftrightarrow t = \frac{b}{c-1} \\ c - bt = t \Leftrightarrow t = \frac{c}{b+1} \end{array}\right\} \text{ (véase caso (2)).}$$

j) $\delta = \varepsilon = 0$. Entonces

$$\left.\begin{array}{l} \frac{c-t}{b} = 0 \Leftrightarrow t = c \\ ct - b = 0 \Leftrightarrow t = \frac{b}{c} \end{array}\right\} \Leftrightarrow c = \frac{b}{c} \Leftrightarrow c^2 = b \text{ (similar a (3g).}$$

k) $\delta = \varepsilon = 1$. Entonces

$$\left.\begin{array}{l} \frac{c-t}{b} = 1 \Leftrightarrow t = c - b \\ ct - b = 1 \Leftrightarrow t = \frac{b+1}{c} \end{array}\right\} \text{ (véase caso (3e)).}$$

l) $\delta = \varepsilon = t$. Entonces

$$\left.\begin{array}{l} \frac{c-t}{b} = t \Leftrightarrow t = \frac{c}{b+1} \\ ct - b = t \Leftrightarrow t = \frac{b}{c-1} \end{array}\right\} \text{ (véase caso (2)).}$$

m) $\delta = \varphi = 0$. Entonces

$$\left\{ \begin{array}{l} \frac{c-t}{b} = 0 \Leftrightarrow t = c \\ c - bt = 0 \Leftrightarrow t = \frac{c}{b} \end{array} \right\} \Leftrightarrow \frac{1}{c} = \frac{b}{c} \Leftrightarrow b = 1,$$

contradicción, $b \neq 1$.

n) $\delta = \varphi = 1$. Entonces

$$\left\{ \begin{array}{l} \frac{c-t}{b} = 1 \Leftrightarrow t = c - b \\ c - bt = 1 \Leftrightarrow t = \frac{c-1}{b} \end{array} \right\} \text{ (véase caso (3h)).}$$

o) $\delta = \varphi = t$. Entonces

$$\left\{ \begin{array}{l} \frac{c-t}{b} = t \Leftrightarrow t = \frac{c}{b+1} \\ c - bt = t \Leftrightarrow t = \frac{c}{b+1} \end{array} \right\}.$$

Tomando en cuenta (4.4),

$$\frac{1}{c-b} = \frac{c}{b+1} \Leftrightarrow c^2 - bc - b - 1 \equiv 0 \bmod p$$

(véase caso (3e)).

p) $\varepsilon = \varphi = 0$. Entonces

$$\left\{ \begin{array}{l} ct - b = 0 \Leftrightarrow t = \frac{b}{c} \\ c - bt = 0 \Leftrightarrow t = \frac{c}{b} \end{array} \right\} \Leftrightarrow b^2 = c^2 \Leftrightarrow b = c \text{ ó } b = -c.$$

Si $b = c \Rightarrow t = 1$, contradicción, $t \neq 1$ y se cumple que $b \neq -c$.

q) $\varepsilon = \varphi = 1$. Entonces

$$\left\{ \begin{array}{l} ct - b = 1 \Leftrightarrow t = \frac{b+1}{c} \\ c - bt = 1 \Leftrightarrow t = \frac{c-1}{b} \end{array} \right\} \text{ (véase caso (2)).}$$

r) $\varepsilon = \varphi = t$. Entonces

$$\left\{ \begin{array}{l} ct - b = t \Leftrightarrow t = \frac{b}{c-1} \\ c - bt = t \Leftrightarrow t = \frac{c}{b+1} \end{array} \right\} \text{ (véase caso (2)).}$$

(4) $\alpha = \gamma = 0$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 0 \Leftrightarrow t = -\frac{1}{b} \\ \frac{t+b}{c} = 0 \Leftrightarrow t = -b \end{array}\right\} \Leftrightarrow b^2 = 1 \Leftrightarrow b = 1 \text{ ó } b = -1.$$

Pero $b \neq 1$ y $b = -1 \Rightarrow t = 1$, contradicción, $t \neq 1$.

(5) $\alpha = \gamma = 1$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 1 \Leftrightarrow t = \frac{c-1}{b} \\ \frac{t+b}{c} = 1 \Leftrightarrow t = c - b \end{array}\right\} \text{ (véase caso (3h)).}$$

(6) $\alpha = \gamma = t$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = t \Leftrightarrow t = \frac{1}{c-b} \\ \frac{t+b}{c} = t \Leftrightarrow t = \frac{b}{c-1} \end{array}\right\} \Leftrightarrow \frac{1}{c-b} = \frac{b}{c-1}$$

$$\Leftrightarrow \quad b^2 - bc + c - 1 \equiv 0 \bmod p \text{ (que es el caso (3h)).}$$

(7) $\alpha = \delta = 0$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 0 \Leftrightarrow t = -\frac{1}{b} \\ \frac{c-t}{b} = 0 \Leftrightarrow t = c \end{array}\right\} \Leftrightarrow -\frac{1}{b} = c \Leftrightarrow bc = -1.$$

Se hace un análisis similar al caso (3) y se ve que ninguna de las posibilidades se da.

(8) $\alpha = \delta = 1$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 1 \Leftrightarrow t = \frac{c-1}{b} \\ \frac{c-t}{b} = 1 \Leftrightarrow t = c - b \end{array}\right\} \text{ (que es el caso (3h)).}$$

(9) $\alpha = \delta = t$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = t \Leftrightarrow t = \frac{1}{c-b} \\ \frac{c-t}{b} = t \Leftrightarrow t = \frac{c}{b+1} \end{array}\right\} \Leftrightarrow \frac{1}{c-b} = \frac{c}{b+1}$$

$$\Leftrightarrow \quad c^2 - bc - b - 1 \equiv 0 \bmod p \text{ (véase caso (3e)).}$$

(10) $\alpha = \varepsilon = 0$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 0 \Leftrightarrow t = -\frac{1}{b} \\ ct - b = 0 \Leftrightarrow t = \frac{b}{c} \end{array}\right\} \Leftrightarrow -\frac{1}{b} = \frac{b}{c} \Leftrightarrow b^2 = -c.$$

Similar a (3g).

(11) $\alpha = \varepsilon = 1$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 1 \Leftrightarrow t = \frac{c-1}{b} \\ ct - b = 1 \Leftrightarrow t = \frac{b+1}{c} \end{array}\right\} \Leftrightarrow \frac{c-1}{b} = \frac{b+1}{c}$$
$$\Leftrightarrow \quad c^2 - c - b^2 - b \equiv 0 \bmod p \text{ (véase el caso (2)).}$$

(12) $\alpha = \varepsilon = t$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = t \Leftrightarrow t = \frac{1}{c-b} \\ ct - b = t \Leftrightarrow t = \frac{b}{c-1} \end{array}\right\} \Leftrightarrow \frac{1}{c-b} = \frac{b}{c-1}$$
$$\Leftrightarrow \quad b^2 - bc + c - 1 \equiv 0 \bmod p \text{ (véase el caso (3h)).}$$

(13) $\alpha = \varphi = 0$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 0 \Leftrightarrow t = -\frac{1}{b} \\ c - bt = 0 \Leftrightarrow t = \frac{c}{b} \end{array}\right\}. \text{ (véase caso (3d)).}$$

(14) $\alpha = \varphi = 1$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = 1 \Leftrightarrow t = \frac{c-1}{b} \\ c - bt = 1 \Leftrightarrow t = \frac{c-1}{b} \end{array}\right\}$$

que lleva a un análisis similar al caso (3).

(15) $\alpha = \varphi = t$. Entonces

$$\left.\begin{array}{l} \frac{1+bt}{c} = t \Leftrightarrow t = \frac{1}{c-b} \\ c - bt = t \Leftrightarrow t = \frac{c}{b+1} \end{array}\right\} \Leftrightarrow \frac{1}{c-b} = \frac{c}{b+1} \text{ (véase caso (3e)).}$$

(16) $\beta = \gamma = 0$. Entonces

$$\left.\begin{array}{l} \frac{ct-1}{b} = 0 \Leftrightarrow t = \frac{1}{c} \\ \frac{t+b}{c} = 0 \Leftrightarrow t = -b \end{array}\right\} \text{ (véase caso (7)).}$$

(17) $\beta = \gamma = 1$. Entonces

$$\left.\begin{array}{l} \frac{ct-1}{b} = 1 \Leftrightarrow t = \frac{b+1}{c} \\ \frac{t+b}{c} = 1 \Leftrightarrow t = c - b \end{array}\right\} \text{ (véase caso (3e)).}$$

(18) $\beta = \gamma = t$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = t \Leftrightarrow t = \frac{1}{c-b} \\ \frac{t+b}{c} = t \Leftrightarrow t = \frac{b}{c-1} \end{array} \right\} \text{ (que es el caso (12)).}$$

(19) $\beta = \delta = 0$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = 0 \Leftrightarrow t = \frac{1}{c} \\ \frac{c-t}{b} = 0 \Leftrightarrow t = c \end{array} \right\} \Leftrightarrow \frac{1}{c} = c \Leftrightarrow c^2 = 1 \Leftrightarrow c = 1 \text{ ó } c = -1.$$

Si $c = 1 \Rightarrow t = 1$, contradicción, $t \neq 1$ y se cumple que $c \neq -1$.

(20) $\beta = \delta = 1$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = 1 \Leftrightarrow t = \frac{b+1}{c} \\ \frac{c-t}{b} = 1 \Leftrightarrow t = c - b \end{array} \right\} \text{ (que es el caso (3e)).}$$

(21) $\beta = \delta = t$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = t \Leftrightarrow t = \frac{1}{c-b} \\ \frac{c-t}{b} = t \Leftrightarrow t = \frac{c}{b+1} \end{array} \right\} \text{ (que es el caso (15)).}$$

(22) $\beta = \varepsilon = 0$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = 0 \Leftrightarrow t = \frac{1}{c} \\ ct - b = 0 \Leftrightarrow t = \frac{b}{c} \end{array} \right\} \text{ (véase caso (3m)).}$$

(23) $\beta = \varepsilon = 1$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = 1 \Leftrightarrow t = \frac{b+1}{c} \\ ct - b = 1 \Leftrightarrow t = \frac{b+1}{c} \end{array} \right\}$$

que conduce a un análisis análogo al caso (3).

(24) $\beta = \varepsilon = t$. Entonces

$$\left\{ \begin{array}{l} \frac{ct-1}{b} = t \Leftrightarrow t = \frac{1}{c-b} \\ ct - b = t \Leftrightarrow t = \frac{b}{c-1} \end{array} \right\} \text{ (que es el caso (6)).}$$

(25) $\beta = \varphi = 0$. Entonces

$$\left.\begin{array}{l} \frac{ct-1}{b} = 0 \Leftrightarrow t = \frac{1}{c} \\ c - bt = 0 \Leftrightarrow t = \frac{c}{b} \end{array}\right\} \Leftrightarrow \frac{1}{c} = \frac{c}{b} \Leftrightarrow c^2 = b$$

(similar al caso (3g)).

(26) $\beta = \varphi = 1$. Entonces

$$\left.\begin{array}{l} \frac{ct-1}{b} = 1 \Leftrightarrow t = \frac{b+1}{c} \\ c - bt = 1 \Leftrightarrow t = \frac{c-1}{b} \end{array}\right\} \text{(que es el caso (2)).}$$

(27) $\beta = \varphi = t$. Entonces

$$\left.\begin{array}{l} \frac{ct-1}{b} = t \Leftrightarrow t = \frac{1}{c-b} \\ c - bt = t \Leftrightarrow t = \frac{c}{b+1} \end{array}\right\} \text{(que es el caso (15)).}$$

(28) $\gamma = \delta = 0$ (véase caso (3a)).

(29) $\gamma = \delta = 1$ (véase caso (3b)).

(30) $\gamma = \delta = t$ (véase caso (3c)).

(31) $\gamma = \varepsilon = 0$ (véase caso (3d)).

(32) $\gamma = \varepsilon = 1$ (véase caso (3e)).

(33) $\gamma = \varepsilon = t$ (véase caso (3f)).

(34) $\gamma = \varphi = 0$ (véase caso (3g)).

(35) $\gamma = \varphi = 1$ (véase caso (3h)).

(36) $\gamma = \varphi = t$ (véase caso (3i)).

(37) $\delta = \varepsilon = 0$ (véase caso (3j)).

(38) $\delta = \varepsilon = 1$ (véase caso (3k)).

(39) $\delta = \varepsilon = t$ (véase caso (3l)).

(40) $\delta = \varphi = 0$ (véase caso (3m)).

(4.1) $\delta = \varphi = 1$ (véase caso (3n)).

(4.2) $\delta = \varphi = t$ (véase caso (3o)).

(4.3) $\varepsilon = \varphi = 0$ (véase caso (3p)).

(4.4) $\varepsilon = \varphi = 1$ (véase caso (3q)).

(4.5) $\varepsilon = \varphi = t$ (véase caso (3r)).

1.2. $|B + bC| = |B| + |C|$, $|A| = 1$ y $\overline{bC} = \overline{B + bC} - B$.

Se resuelve análogamente al caso 1.2.1 del capítulo 2 (se hace uso del lema 4.1).

1.3. $|B + bC| = |B| + |C| + 1$, $|A| = 1$, $\overline{B} = (d - bC) \cup \{t_1, t_2\}$ para algún $d \notin B + bC$ y $t_1, t_2 \in \mathbf{Z}_n^*$ tales que $t_1 \neq t_2$.

Sea $A = \{c - b\}$, $c \neq b$. Entonces

$$\overline{B} = (d - bC) \cup \{t_1, t_2\} = C \cup \{0, c - b\}.$$

Como $t_1, t_2 \notin d - bC \Leftrightarrow d - t_1, d - t_2 \notin bC$, luego

$$\overline{B} = d - (bC \cup \{d - t_1, d - t_2\}) = C \cup \{0, c - b\}$$

$$\Leftrightarrow d - \overline{B} = bC \cup \{d - t_1, d - t_2\} = d - (C \cup \{0, c - b\}).$$

Por otra parte, $t_1, t_2 \notin B \Leftrightarrow t_1, t_2 \in C \cup \{0, c - b\}$. La igualdad anterior muestra también que $d - t_1, d - t_2 \notin B$. Esto es equivalente a que $t_1 = d$ y $t_2 = d - c + b$. Entonces

$$\begin{aligned} d - (bC \cup \{0, c - b\}) &= C \cup \{0, c - b\} \quad \text{y} \\ d - B &= B. \end{aligned} \tag{4.5}$$

Con esto, (4.1) se escribe como

$$\left\{ \begin{array}{r} (c - b + B) \cap cC = \emptyset \\ (c - b + C) \cap cB = \emptyset \\ (B + bc - b^2) \cap cC = \emptyset \\ (B + bC) \cap (c^2 - bc) = \emptyset \\ (C + bc - b^2) \cap cB = \emptyset \\ (C + bB) \cap (c^2 - bc) = \emptyset \end{array} \right\}. \tag{4.6}$$

Como $|B + bC| = p - 1$ (véase la condición (ii) del teorema 2.6 y su demostración) y $d, c^2 - bc \notin B + bC$, entonces

$$d = c^2 - bc. \tag{4.7}$$

Sean $A' = A-1 = \{c - b - 1\}$, $B' = B-1$ y $C' = C-1$. Evidentemente, $\mathbf{Z}_p \setminus \{-1\} = \mathbf{c}-b-1 \mid B' \mid C'$. Con estas definiciones, (4.5) se transforma en

$$\begin{aligned} d - 2 - ((bC' + b) \cup \{c - b - 1, -1\}) &= C' \cup \{c - b - 1, -1\} \text{ y} \\ d - 2 - B' &= B'. \end{aligned} \tag{4.8}$$

y (4.6) es equivalente a

$$\left\{ \begin{array}{l} (c - b + bB' + b) \cap (cC' + c) = \emptyset \\ (c - b + bC' + b) \cap (cB' + c) = \emptyset \\ (B' + 1 + bc - c^2) \cap (cC' + c) = \emptyset \\ (B' + 1 + bC' + b) \cap (c^2 - bc) = \emptyset \\ (C' + 1 + bc - c^2) \cap (cB' + c) = \emptyset \\ (C' + 1 + bB' + b) \cap (c^2 - bc) = \emptyset \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{r} B' \cap \frac{c}{b} C' = \emptyset \\ C' \cap \frac{c}{b} B' = \emptyset \\ B' \cap (cC' + c - 1 - bc + b^2) = \emptyset \\ C' \cap (cB' + c - 1 - bc + b^2) = \emptyset \\ (B' + bC') \cap (c^2 - bc - b - 1) = \emptyset \\ (C' + bB') \cap (c^2 - bc - b - 1) = \emptyset \end{array} \right\}. \tag{4.9}$$

El elemento $-b/c$ no está en B' o no está en C' y por lo tanto podemos suponer que $-b/c \notin B' \Rightarrow -1 \notin \frac{c}{b} B'$. Entonces la segunda relación de (4.9) es equivalente a que

$$\frac{c}{b} B' \subset \overline{C'} = B' \cup \{c - b - 1, -1\}$$

y por lo anterior, esto implica que

$$\frac{c}{b} B' \subset B' \cup \{c - b - 1\}. \tag{4.10}$$

Se tiene el siguiente

Lema 4.2 *Si se cumple (4.10), entonces*

(i) $\frac{c}{b}B' = B'$, *si* $c-b-1 \notin \frac{c}{b}B'$, *ó*

(ii) $\frac{c}{b}(B' \cup \{c-b-1\}) = B' \cup \{c-b-1\}$, *si* $c-b-1 \in \frac{c}{b}B'$.

La demostración de este lema es exactamente igual a la del lema 3.2 correspondiente al capítulo anterior. Este lema abre dos posibilidades:

CASO 1: $\frac{c}{b}B' = B'$, esto es, B' es una unión de clases laterales módulo $\langle \frac{c}{b} \rangle$ (véase el lema 3.3) y entonces

$$\sum_{b' \in B'} b' \equiv 0 \bmod p.$$

Como sabemos que $d-2-B' = B'$, esto es equivalente con que $d-2 = 0$ y entonces las relaciones (4.8) serán

$$\begin{aligned} -((bC'+b) \cup \{c-b-1,-1\}) &= C' \cup \{c-b-1,-1\} \ \ y \\ -B' &= B'. \end{aligned}$$

Por otra parte,

$$\frac{c}{b}B' = B' \Leftrightarrow cB' = bB' \Leftrightarrow \langle c \rangle B' = \langle b \rangle B' \Leftrightarrow \bigcup_{b' \in B'} b' \langle c \rangle = \bigcup_{b' \in B'} b' \langle b \rangle$$

y de aquí se tiene que B' es también una unión de clases laterales módulo $\langle b \rangle$ y $\langle c \rangle$, o sea,

$$bB' = cB' = B' = \frac{c}{b}B' \Leftrightarrow \langle b, c \rangle B' = B'.$$

Como $-B' = B'$, entonces $-1 \in \langle \frac{c}{b} \rangle \subseteq \langle b, c \rangle$ y así $-cB' = B'$. Usando estos hechos, la sexta relación de (4.9) es equivalente a que

$$\begin{aligned} & (C' + B') \cap (c^2 - bc - b - 1) = \emptyset \\ \Leftrightarrow \quad & (bC' + bB') \cap b(c^2 - bc - b - 1) = \emptyset \end{aligned}$$

$$\Leftrightarrow (B' + bC') \cap b\left(c^2 - bc - b - 1\right) = \emptyset. \qquad (4.11)$$

Como $|B' + bC'| = |B + bC| = p - 1$, entonces de la quinta relación de (4.9) y de (4.11) se tiene que

$$c^2 - bc - b - 1, b\left(c^2 - bc - b - 1\right) \notin B' + bC'$$

y esto es equivalente a que

$$\begin{aligned} & c^2 - bc - b - 1 \equiv b(c^2 - bc - b - 1) \bmod p \\ \Leftrightarrow \quad & (b-1)(c^2 - bc - b - 1) \equiv 0 \bmod p \\ \Leftrightarrow \quad & (b-1)(c+1)(c-b-1) \equiv 0 \bmod p \\ \Leftrightarrow \quad & b = 1 \text{ ó } c = -1 \text{ ó } c = b+1. \end{aligned}$$

Los csos en que $b = 1$ y $c = -1$ son imposibles. Luego, $\langle b, c\rangle = \langle b, b+1\rangle$ y como $-1 \in \langle b, c\rangle$, entonces se tiene que

$$\{1, b, b+1, -b, -b-1, -1\} \subseteq \langle b, b+1\rangle.$$

Si $\{1, b, b+1, -b, -b-1, -1\} = \langle b, b+1\rangle$, entonces $\mathbb{Z}_p^*$ contiene un subgrupo de orden 6, esto es $p \equiv 1 \bmod 6$ y por lo tanto $p \equiv 1 \bmod 3$. En el subgrupo de orden 6 está contenido el subgrupo de orden 3 y se cumple que $b^2 \equiv -b-1 \bmod p$ (se recuerda que si g no es raíz primitiva, entonces $\sum_{g\in\langle g\rangle} g \equiv 0 \bmod p$). Así se tiene la siguiente

Proposición 4.1 *Si $p \equiv 1 \bmod 3$ y $\{1, b, b^2\}$ es el subgrupo de orden 3 de $\mathbb{Z}_p^*$, entonces la ecuación*

$$x + by + b^2 z = 0$$

es no tensa.

La partición que se obtiene en este caso es

$$1 \mid 2, b+1, b+2, -b+1, -b \mid \mathbb{Z}_p^* \setminus \{2, b+1, b+2, -b+1, -b\}.$$

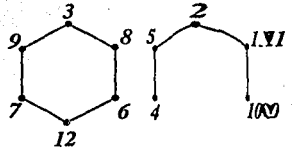
Ejemplo 4.1 *Para $p = 13$ la ecuación $x + 3y + 9z = 0$ es no tensa,*

$$\langle 3, 4\rangle = \{1, 3, 4, 9, 10, 12\}$$

que son los residuos cuadráticos y la partición en este caso es

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

La figura que sigue ilustra la $Tr(1)$ de la 3-gráfica asociada a la ecuación $x + 3y + 9z = 0$ con $p = 13$.



Ejemplo 4.2 *Para $p = 19$ la ecuación $x + 7y + 11z = 0$ es no tensa,*

$$\langle 7, 8\rangle = \{1, 7, 8, 11, 12, 18\}$$

que son los residuos cúbicos y la partición en este caso es

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

Si $\{1, b, b+1, -b, -b-1, -1\} \subset \langle b, b+1\rangle$, entonces es válida la siguiente

Proposición 4.2 *Si b, $b+1$ y -1 son residuos de orden $k \geq 2$, entonces las ecuaciones*

$$x + by = (b+1)z$$

son no tensas.

La partición para este caso es

$$1 \mid \langle b, b+1\rangle + 1 \mid \mathbb{Z}_p^* \setminus \{\langle b, b+1\rangle - 1\}.$$

Ejemplo 4.3 *Para $p = 29$ (que es el menor primo para el cual se cumple la proposición anterior), el subgrupo de los residuos cuadráticos es*

$$R_2 = \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}.$$

Se tiene que

$$\begin{array}{rcl} \{1,4,5,24,25,28\} & \subset & R_2, \\ \{1,5,6,23,24,28\} & \subset & R_2, \\ \{1,6,7,22,23,28\} & \subset & R_2 \end{array}$$

y por lo tanto, las ecuaciones $x+4y=5z$, $x+5y=6z$ *y* $x+6y=7z$ *no son tensas. Para todas ellas, la partición es*

$$1 \mid R_2+1 \mid \mathbb{Z}_{29}^* \setminus \{R_2+1\}.$$

Ejemplo 4.4 *Para* $p=67$, *el subgrupo de los residuos cúbicos es*

$$\{1,3,5,8,9,14,15,22,24,25,27,40,42,43,45,52,53,58,59,62,64,66\}$$

que se denota por R_3. *Se tiene que*

$$\begin{array}{rcl} \{1,8,9,58,59,66\} & \subset & R_3, \\ \{1,14,15,52,53,66\} & \subset & R_3, \\ \{1,24,25,42,43,66\} & \subset & R_3 \end{array}$$

y por lo tanto las ecuaciones $x+8y=9z$, $x+14y=15z$ *y* $x+24y=25z$ *no son tensas. Para todas ellas, la partición es*

$$1 \mid R_3+1 \mid \mathbb{Z}_{67}^* \setminus \{R_3+1\}.$$

CASO 2: $\frac{c}{b}(B' \cup \{c-b-1\}) = B' \cup \{c-b-1\}$, o sea $B' \cup \{c-b-1\}$ es una unión de clases laterales módulo $\langle \frac{c}{b} \rangle$ y por lo tanto

$$\sum_{b' \in B'} b' + c - b - 1 \equiv 0 \bmod p.$$

Por (4.8), $d-2-B' = B'$ y de aquí

$$\begin{array}{rcl} \sum_{b' \in B'} (d-2-b') & \equiv & \sum_{b' \in B'} b' \bmod p \\ \Leftrightarrow \quad |B'|\,(d-2) & \equiv & 2\sum_{b' \in B'} b' \equiv 2(b-c+1) \bmod p \\ \Leftrightarrow \quad d & \equiv & \frac{2b-2c+2}{|B'|} + 2 \bmod p \end{array}$$

Como $d = c^2 - bc$ (véase (4.7), entonces

$$\frac{2b-2c+2}{|B'|} \equiv c^2 - bc - 2 \bmod p \Leftrightarrow b = 1 \text{ y } c = 2,$$

que resulta imposible porque $b \neq 1$.

Por útimo, si $b = c$, sea $A = \{b\}$. Entonces (4.1) se escribe como

$$\left\{\begin{array}{l}(b+bB)\cap bC = \emptyset\\ (b+bC)\cap bB = \emptyset\\ (B+b^2)\cap bC = \emptyset\\ (C+b^2)\cap bB = \emptyset\\ (B+bC)\cap b^2 = \emptyset\\ (C+bB)\cap b^2 = \emptyset\end{array}\right\}. \tag{4.12}$$

De la quinta relación de (4.12) se tiene que $b^2 \notin B+bC$, además sabemos que $d \notin B+bC$ y $|B+bC| = p-1$, así $d = b^2$. Como antes, $d - B = B$. Por otra parte, si $b^2 \notin B+bC$, entonces para todo $b' \in B$ se cumple que $b^2 - b' \in bA \cup bC \cup \{0\}$ y de aquí se tiene que

$$\begin{array}{rcl} b^2 - (bA \cup bC \cup \{0\}) & = & bA \cup bC \cup \{0\} \\ \Leftrightarrow \quad b - (A \cup C \cup \{0\}) & = & A \cup C \cup \{0\}. \end{array}$$

Como los conjuntos A, B, C son una partición, entonces $b - B = B$. Así

$$b^2 - B = B = b - B \Leftrightarrow b^2 = b \Leftrightarrow b = 0 \text{ ó } b = 1,$$

que no es posible.

2. $|A+bB| = |A| + |B|$.

2.1. $|B+bC| = |B| + |C|$ y la condición (iii) del teorema 2.5 para ambos pares.

Supongamos que $b\overline{B} = \overline{A+bB} - A$, A y bB no están en progresión aritmética. Se tiene que $b\overline{B} = bA \cup bC \cup \{0\}$, entonces $0 \in b\overline{B}$ y existe $x \in \overline{A+bB} \cap A$ tal que $x \neq 0$ y $0 = x - x$. Como $x \notin A+bB$, entonces para todo $a \in A$ se cumple que $x - a \in bA \cup bC \cup \{0\}$, esto es,

$$x - (bA \cup bC \cup \{0\}) = bA \cup bC \cup \{0\}.$$

Como A, B, C forman una partición (y por lo tanto bA, bB, bC también), entonces se tiene que $x - bB = bB$. De la misma forma, $x \notin A+bB$ conduce a que para todo $b' \in bB$ se verifica que $x - b' \in B \cup C \cup \{0\}$ y de aquí

$$\begin{array}{rcl} x - (B \cup C \cup \{0\}) & = & B \cup C \cup \{0\} \text{ y} \\ x - A & = & A. \end{array}$$

Por otra parte, $|A+bB| = |A|+|B|$ y $c\overline{C} = |A|+|B|+1$, junto con la primera relación de (4.1) implican que $A+bB = c\overline{C} \setminus y$ con $y \in c\overline{C}$. Como $x \notin A+bB$, entonces $x \in cC \cup y$. Si $x \in cC$, entonces de la tercera relación de (4.1) se tiene que $x \notin B+bA$. Luego para todo $a' \in bA$, $x-a' \in A \cup C \cup \{0\}$, esto es,

$$\begin{aligned} x-(A\cup C\cup\{0\}) &= A\cup C\cup\{0\} \text{ y} \\ x-B &= B, \end{aligned}$$

pero $x-bB = bB \Leftrightarrow \frac{x}{b}-B = B = x-B \Leftrightarrow x = \frac{x}{b} \Leftrightarrow b = 1$, que es una contradicción, pues se supuso que $b \neq 1$. Si $x = y \in B+bA$, entonces seleccionemos un $z \notin B+bA$. Como antes, llegamos a que

$$\begin{aligned} z-(A\cup C\cup\{0\}) &= A\cup C\cup\{0\} \text{ y} \\ z-B &= B, \end{aligned}$$

y de aquí $x = z$ que es una contradicción.

2.2. $|B+bC| = |B|+|C|+1$, la condición (iii) del teorema 2.5 para el par (A, bB) y la condición (iii) del teorema 2.6 para (B, bC).

Funciona el argumento anterior exactamente. Nótese que no se usó en ningún momento la condición (iii) del teorema 2.5 para B y bC.

4.3 El teorema de clasificación

De las proposiciones 4.1 y 4.2 se tiene el siguiente

Teorema 4.1 *Las ecuaciones*

$$x+by = cz,$$

son tensas para todo $b, c \in \mathbb{Z}_p^*$, $p > 7$, donde $b \neq 1$, $c \neq -1$, $bc \neq 1$ y $\frac{b}{c} \neq -1$, con las siguientes excepciones que son todas las ecuaciones no tensas:

(i) $x+by+b^2z = 0$ para todo $p \equiv 1 \bmod 3$, donde $\{1, b, b^2\}$ es el subgrupo de orden 3 de $\mathbb{Z}_p^*$.

(ii) $x+by = (b+1)z$ para todo primo p tal que b, $b+1$ y -1 son residuos de orden $k \geq 2$ y k divide a $p-1$.

Para este tipo de ecuaciones, sólo sabemos que las no tensas descritas en (i) del teorema anterior son únicas para cada primo p (ya que los subgrupos de $\mathbb{Z}_p^*$ son únicos). La cantidad de ecuaciones del caso (ii) constituye un problema aún sin resolver, aunque se puede conjeturar que son "relativamente pocas" respecto al número de todas las ecuaciones posibles para cada primo p.

Por último, para estas ecuaciones es válido nuevamente el teorema 3.2 dados los resultados del análisis de casos de la sección anterior.

Bibliografía

[ABN1] J. L. AROCHA, J. BRACHO, V. NEUMANN-LARA, On the minimum size of tight hypergraphs, *J. Graph Theory* **16**, No. 4 (1992), 319-326.

[ABN2] J. L. AROCHA, J. BRACHO, V. NEUMANN-LARA, Tight and untight triangulations of surfaces by complete graphs, *J. Combin. Theory Ser B* **63**, No.2 (1995), 185-199.

[BEL] A. BIALOSTOCKI, P. ERDÖS, H. LEFMANN, Monochromatic and zero-sum sets of nondecreasing diameter, *Discrete Math.* **137** (1995) 19-34.

[Cau] A. CAUCHY, Recherche sur les nombres, *J. Ecole Polytechn.* **9** (1813) 99-106.

[Cho] I. CHOWLA, A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem, *Proc. Indian Acad. Sci.* **2** (1935) 242-243.

[Dav1] H. DAVENPORT, On the addition of residue classes, *J. London Math. Soc.* **10** (1935) 30-32.

[Dav2] H. DAVENPORT, A historical note, *J. London Math. Soc.* **22** (1947) 100-101.

[Deu] W. A. DEUBER, Developments based on Rado's Dissertation "Studien zur Kombinatorik", Preprint 89-101, Universität Bielefeld, 1989.

[Dic1] L. E. DICKSON, On the congruence $x^n + y^n + z^n \equiv o \bmod p$, *J. fur reine und angew. Mathematik* **135** (1909) 134-141.

[Dic2] L. E. DICKSON, Lower limit for the number ot sets of solutions of $x^e + y^e + z^e \equiv o \bmod p$, *J. fur reine und angew. Mathematik* **135** (1909) 181-188.

[EGZ] P. ERDÖS, A. GINZBURG, A. ZIV, Theorem in the additive number theory, *Bull. Res. Counc. Isr. Sect. F* **10** (1961) 41-43.

[Gra] R. L. GRAHAM, "Rudiments of Ramsey Theory", AMS, Providence, RI (1981).

[GRS] R. L. GRAHAM, B. L. ROTHSCHILD, J. H. SPENCER, "Ramsey Theory", Wiley- Interscience Series in Math., J. Wiley&Sons, NY-Chichester-Brisbane-Toronto, 1980.

[Ham1] Y. O. HAMIDOUNE, A note on the addition of residues, *Graphs and Combin.* 6 (1990) 147-152.

[Ham2] Y. O. HAMIDOUNE, On the subsets product in finite groups, *Europ. J. Combin.* 12 (1991) 211-221.

[Ham3] Y. O. HAMIDOUNE, A generalization of an addition theorem of Shatrowsky, *Europ. J. Combin.* 13 (1992) 249-255.

[Ham4] Y. O. HAMIDOUNE, The representation of some integers as a subset sum, *Bull. London Math. Soc.* **26** (1994) 557-563.

[HLlS] Y. O. HAMIDOUNE, A. S. LLADO, O. SERRA, Vosperian and superconnected abelian Cayley digraphs, *Graphs and Combin.* 7 (1991) 143-152.

[Har] F. HARARY, "Graph Theory", Addison-Wesley, Reading, 1969.

[HW] G. H. HARDY, E. M. WRIGHT, "An Introducction to the Theory of Numbers", 5th ed., Clarendon Press, Oxford, 1979.

[Kem] J. H. B. KEMPERMAN, On small sumsets in an abelian group, *Acta Math.* **103** (1960) 63-88.

[Kne1] M. KNESER, Abschätzung der asymptotischen dichte von Summenmengen, *Math. Z.* **58** (1953) 459-484.

[Lov] L. LOVÁSZ, Topological and algebraic methods in graph theory, in "Graph theory and related topics", Proceedings of Conference in Honour of W. T. Tutte (Waterloo, Ontario, 1977), Academic Press, New York (1979) 1-14.

[Man1] H. B. MANN, An addition theorem for sets of elements of abelian groups, *Proc. Amer. Math. Soc.* 4 (1953) 423.

[Man2] H. B. MANN, "Addition theorems: the addition theorems of group theory and number theory", Interscience tracts in pure and applied mathematics, No.18, John Wiley & Sons, New York, 1965.

[Man3] H. B. MANN, Additive group theory - A progress report, *Bull. Amer. Math. Soc.* 79, No. 6 (1973) 1069-1075.

[MO] H. B. MANN, J. E. OLSON, Sums of sets in the elementary abelian group of type (p, p), *J. Combin. Theory* 2 (1967) 275-284.

[NL] V. NEUMANN-LARA, The acyclic disconnection of a digraph (en preparación).

[NZM] I. NIVEN, H. S. ZUCKERMAN, H. L. MONTGOMERY, "An Introduction to the Theory of Numbers", 5th ed., J. Wiley & Sons, New York, 1991.

[Ols1] J. E. OLSON, An addition theorem modulo p, *J. Combin. Theory* 5 (1968) 45-52.

[Ols2] J. E. OLSON, Sums of sets of group elements, *Acta Arith.* 28 (1975) 147-156.

[Ols3] J. E. OLSON, On a combinatorial problem of Erdös, Ginzburg and Ziv, *J. Number Theory* 8 (1976) 52-57.

[Ols4] J. E. OLSON, On the sum of two sets in a group, *J. Number Theory* 18 (1984) 110-120.

[Pil] S. S. PILLAI, Generalization of a theorem of Davenport on the addition of residue classes, *Proc. Indian Acad. Sci.* (1937) 179-180.

[Rad1] R. RADO, Studien zur Kombinatorik, *Math. Z.* 36 (1933) 424-480.

[Rad2] R. RADO, Note on combinatorial analysis, *Proc. London Math. Soc.* **48** (1945) 122-160.

[RP1] A. H. RHEMTULLA, A. PENFOLD STREET, Maximal sum-free sets in finite abelian groups, *Bull. Austral. Math. Soc.* **2** (1970) 289-297.

[RP2] A. H. RHEMTULLA, A. PENFOLD STREET, Maximal sum-free sets in elementary abelian p-groups, *Canad. Math. Bull.* **14** (1971) 73-80.

[Shu] I. SCHUR, Über die Kongruenz $x^m + y^m \equiv z^m \bmod p$, *Jber. Deutsche Math. Verein.* **25** (1916) 114-116.

[Sha] L. SHATROWSKY, A new generalization of the Davenport's-Pillai's theorem on the addition of residue classes, *C. R. (Dokl.) Acad. Sci. USSR* **XLV** (1944) 315-317.

[She] J. C. SHEPHERDSON, On the addition of elements of a sequence, *J. London Math. Soc.* **22** (1947) 85-88.

[Str] A. PENFOLD STREET, "Sum-free sets", in "Combinatorics", Lecture Notes in Math. **292**, Springer-Verlag, Berlin/Heidelberg/New York, 1972.

[Vos1] A. G. VOSPER, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* **31** (1956) 200-205.

[Vos2] A. G. VOSPER, Addendum to "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956) 280-282.

[Yap1] H. P. YAP, Maximal sum-free sets of group elements, *J. London Math. Soc.* **44** (1969) 131-136.

[Yap2] H. P. YAP, Structure of maximal sum-free sets in C_p, *Acta Arith.* **17** (1970) 29-35.