# BASES ADITIVAS DE ORDEN DOS PARA GRUPOS ABELIANOS FINITOS

**HELBERT AUGUSTO AGUILAR PRIETO**

**JORGE ARTURO BURBANO SOLARTE**

**NÉSTOR FABIO CERÓN ERAZO**

**Universidad del Cauca**

**Facultad de Ciencias Naturales, Exáctas y de la Educación**

**Departamento de Matemáticas**

**Popayán**

Septiembre, 2009

# BASES ADITIVAS DE ORDEN DOS PARA GRUPOS ABELIANOS FINITOS

**HELBERT AUGUSTO AGUILAR PRIETO**

**JORGE ARTURO BURBANO SOLARTE**

**NÉSTOR FABIO CERÓN ERAZO**

**Trabajo de grado presentado como requisito parcial para optar al título de Matemático**

Dr. CARLOS ALBERTO TRUJILLO SOLARTE

Director

**Universidad del Cauca**

**Facultad de Ciencias Naturales, Exáctas y de la Educación**

**Departamento de Matemáticas**

**Popayán**

Septiembre, 2009

Nota de Aceptación

Dr. Carlos Alberto Trujillo Solarte
Director

Profesor. Diego Fernando Ruiz
Comite de seguimiento

Profesor. Freddy William Bustos
Comite de seguimiento

Popayán, 16 de Septiembre, 2009

# Agradecimientos

Agradecemos a Dios por darnos la fortaleza y la sabiduría para poder culminar con éxito esta etapa de nuestra vida.

A nuestro director Dr Carlos Alberto Trujillo Solarte, por su calidad humana y su colaboración durante el desarrollo de este trabajo de grado. Al comité de seguimiento conformado por los profesores Diego Fernando Ruiz y Freddy William Bustos por sus constantes aportes en beneficio de nuestro trabajo.

A nuestras familias, pues gracias a ellas todo esto ha sido posible, por creer en nosotros y por estar de nuestro lado todos los dias de nuestra vida.

Gracias a los profesores por todo los conocimientos transmitidos, a nuestros amigos y compañeros que de una u otra manera nos acompañaron en el transcurso de nuestra carrera.

HELBERT AUGUSTO AGUILAR PRIETO
JORGE ARTURO BURBANO SOLARTE
NÉSTOR FABIO CERÓN ERAZO

*Universidad del Cauca*
*16 de Septiembre, 2009*

# Tabla de Contenido

**Introducción** vi

**1. Bases Aditivas** **1**

1.1. **Preliminares** . . . . . 1

1.2. **Cotas Inferiores** . . . . . 4

1.3. **Construcción Natural de una Base para $\mathbb{Z}_n$** . . . . . 8

1.4. **Mejoras de la Construcción Natural** . . . . . 9

1.5. **Resultado Central** . . . . . 12

**2. Conjuntos de Sidon.** **15**

2.1. **Definiciones y Resultados Básicos** . . . . . 15

2.2. **Construcciones(Bose, Ruzsa)** . . . . . 19

2.3. **Bases a partir de Conjuntos de Sidon** . . . . . 28

**3. Aplicación y Anexos** **33**

3.1. **Aplicación** . . . . . 33

3.2. **Equivalencias Holomórficas** . . . . . 34

3.3. **Progresiones Aritméticas en Bases** . . . . . 40

3.4. **Otras Funciones Extremas Relacionadas** . . . . . 43

3.5. **Problemas Abiertos** . . . . . 45

3.6. **Tablas** . . . . . 45

**Conclusiones** **61**

**Bibliografía** **62**

# Introducción

Un subconjunto $A$ de un grupo abeliano finito notado aditivamente $(G, +)$ es una base aditiva para $G$, si todo elemento de $G$ puede escribirse como la suma de dos elementos en $A$ no necesariamente distintos, una base estricta para $G$ si todo elemento de $G$ puede escribirse como la suma de dos elementos distintos de $A$ y una base diferencia para $G$ si todo elemento de $G$ puede expresarse como la diferencia de dos elementos en $A$.

Por otro lado $A$ es un conjunto de Sidon para $G$ si todas las sumas de dos elementos de $A$ son distintas, un conjunto de Sidon estricto si todas las sumas de dos elementos distintos son diferentes y un conjunto de Sidon diferencia si todas las diferencias de dos elementos son distintas.

El presente trabajo está basado en las investigaciones que se desarrollan en los artículos de Harri Haanpää, *Minimum Sum and Difference Covers of Abelian Groups* y Mark A. Fitch and Robert E. Jamison, *Minimum Sum Covers of Small Cyclic Groups*, que buscan encontrar el mínimo cardinal de una base para $G$.

El trabajo de grado se encuentra dividido en tres capítulos. El primero muestra cotas inferiores para el cardinal mínimo de una base para $G$, la construcción de una base trivial y las mejoras a dicha construcción. El segundo muestra la construcción de conjuntos de Sidon según R. C. Bose (1942) e I. Ruzsa (1996), además cómo construir bases a partir de estas construcciones. El tercer capítulo muestra una aplicación, tablas para bases obtenidas computacionalmente y algunos problemas abiertos. Finalmente se presentan las conclusiones obtenidas en el desarrollo del trabajo de grado.

# Capítulo 1

# Bases Aditivas

## 1.1. Preliminares

Sean $(G, +)$ un grupo conmutativo finito, notado aditivamente y $A \subseteq G$.

El **conjunto suma** de $A$, que se nota $A + A$, se define como el conjunto de todas las sumas de dos elementos en $A$, es decir

$$A + A := \{x + y : x, y \in A\}.$$

La tabla que representa esta suma se obtiene de la siguiente manera.

Dado $A = \{x_1, x_2, ..., x_n\}$, la entrada $ij$-ésima de la tabla está dada por: $x_i + x_j$. Esto es, si consideramos $n = 3$ entonces

| $+$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|
| $x_1$ | $x_1 + x_1$ | $x_1 + x_2$ | $x_1 + x_3$ |
| $x_2$ | $x_2 + x_1$ | $x_2 + x_2$ | $x_2 + x_3$ |
| $x_3$ | $x_3 + x_1$ | $x_3 + x_2$ | $x_3 + x_3$ |

El conjunto **suma estricta** de $A$, que se nota $A\hat{+}A$, se define como el conjunto de todas las sumas de dos elementos **distintos** en $A$, es decir

$$A\hat{+}A := \{x + y : x, y \in A, x \neq y\}.$$

De igual manera que se obtuvo la tabla para la suma se obtiene para la suma estricta, solo que los elementos de la diagonal principal no cuentan.

**Definición 1.1.1** *$A$ se llama una **base**(aditiva de orden dos) para $G$ si $A + A = G$.*

**Nota.** El orden hace referencia al número de veces que se suma el conjunto $A$.

**Ejemplo 1.1.1** *Sean $G = \mathbb{Z}_{12}$ y $A = \{0, 1, 2, 7, 8, 10\}$. Entonces*

| $+$ | 0 | 1 | 2 | 7 | 8 | 10 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 7 | 8 | 10 |
| 1 | 1 | 2 | 3 | 8 | 9 | 11 |
| 2 | 2 | 3 | 4 | 9 | 10 | 0 |
| 7 | 7 | 8 | 9 | 2 | 3 | 5 |
| 8 | 8 | 9 | 10 | 3 | 4 | 6 |
| 10 | 10 | 11 | 0 | 5 | 6 | 8 |

*Como $A+A=\mathbb{Z}_{12}$, $A$ es una base para $\mathbb{Z}_{12}$.*

De ahora en adelante cuando el conjunto $A$ tenga el elemento cero omitimos la primera fila y debido a la conmutatividad de $G$ la tabla es simétrica, entonces también omitiremos todos los elementos por debajo de la diagonal principal, es decir la tabla anterior se representa de la siguiente manera

| $+$ | 0 | 1 | 2 | 7 | 8 | 10 |
|---|---|---|---|---|---|---|
| | | 2 | 3 | 8 | 9 | 11 |
| | | | 4 | 9 | 10 | 0 |
| | | | | 2 | 3 | 5 |
| | | | | | 4 | 6 |
| | | | | | | 8 |

**Ejemplo 1.1.2** *Sean $G = \mathbb{Z}_{12}$ y $A = \{0, 1, 2\}$ entonces $A + A = \{0, 1, 2, 3, 4\} \neq \mathbb{Z}_{12}$, luego, $A$ no es base para $\mathbb{Z}_{12}$.*

**Definición 1.1.2** *$A$ se llama una **base estricta**(aditiva de orden dos) para $G$ si*

$$A\hat{+}A = G.$$

**Ejemplo 1.1.3** *Sean $G = \mathbb{Z}_{10}$ y $A = \{0, 1, 3, 5, 7, 8\}$. Entonces*

| $+$ | ***0*** | 1 | 3 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| | ***2*** | 4 | 6 | 8 | 9 | |
| | | ***6*** | 8 | 0 | 1 | |
| | | | ***0*** | 2 | 3 | |
| | | | | ***4*** | 5 | |
| | | | | | ***6*** | |

*Se puede ver que* $A\hat{+}A = \mathbb{Z}_{10}$*, con lo que decimos que* $A$ *es base estricta para* $\mathbb{Z}_{10}$*.*

**Ejemplo 1.1.4** *En el Ejemplo 1.1.1 el conjunto* $A$ *no es una base estricta para* $\mathbb{Z}_{12}$*.*

El **Conjunto Diferencia** de $A$, escrito $A - A$, se define como el conjunto de todas las diferencias de dos elementos de $A$, es decir

$$A - A := \{x - y : x, y \in A\}.$$

**Definición 1.1.3** *$A$ es una **Base Diferencia**(de orden dos) para $G$ si, $A - A = G$.*

Análogamente como se obtuvo la tabla para la suma se obtiene para la diferencia.

**Ejemplo 1.1.5** *Sean* $G = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ *y* $A = \{0, 1, 2, 4\}$*. Entonces*

| $-$ | 0 | 1 | 2 | 4 |
|---|---|---|---|---|
| 0 | 0 | 7 | 6 | 4 |
| 1 | 1 | 0 | 7 | 5 |
| 2 | 2 | 1 | 0 | 6 |
| 4 | 4 | 3 | 2 | 0 |

*es decir que* $A - A = G$*, luego* $A$ *es una base diferencia para* $G$*.*

**Ejemplo 1.1.6** *Sean* $G = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ *y* $A = \{0, 2, 4\}$*. Entonces*

| $-$ | 0 | 2 | 4 |
|---|---|---|---|
| 0 | 0 | 6 | 4 |
| 2 | 2 | 0 | 6 |
| 4 | 4 | 2 | 0 |

*es decir que* $A - A = \{0, 2, 4, 6\} \neq \mathbb{Z}_{10}$*, luego* $A$ *no es una base diferencia para* $G$*.*

De las definiciones de suma y suma estricta de $A$ se deduce el siguiente resultado.

**Lema 1.1.1** $A\hat{+}A \subseteq A + A$*.*

**Prueba**

Es claro que $A + A = (A\hat{+}A) \cup \{a + a : a \in A\}$, por lo tanto el resultado se sigue. □

*En relación con estos conceptos nos interesa obtener bases con el menor número de elementos posibles (bases minimales), es decir, se trata de estudiar el comportamiento asintótico de las siguientes funciones*

$$\alpha(G):=\text{mín}\{|A| : A + A = G\},$$

$$\hat{\alpha}(G):=\text{mín}\{|A| : A\hat{+}A = G\},$$

donde $|A|$ hace referencia al cardinal de $A$.

Además nos interesa estudiar la estructura de los conjuntos que logran ese mínimo.

Si $G$ es cíclico de orden $n$ entonces sabemos que $G$ es isomorfo a $\mathbb{Z}_n$ (aditivamente), en este caso notemos $\alpha(G) = \alpha(n)$ y $\hat{\alpha}(G) = \hat{\alpha}(n)$, además las bases las llamamos **bases modulares**.

**Teorema 1.1.1** $\alpha(G) \leq \hat{\alpha}(G)$.

**Prueba**

Sean $T$ y $S$ base y base estricta de $G$ respectivamente tal que $\alpha(G) = |T|$ y $\hat{\alpha}(G) = |S|$. Por Lema 1.1.1 como $S$ es una base estricta, en particular $S$ es una base, pero el cardinal de $T$ es el mínimo cardinal de una base, así $|T| \leq |S|$, es decir $\alpha(G) \leq \hat{\alpha}(G)$. □

## 1.2. Cotas Inferiores

Mediante conteo es fácil obtener una cota inferior para las funciones minimales $\alpha(G)$ y $\hat{\alpha}(G)$.

**Teorema 1.2.1** *Sea $G$ un grupo conmutativo de orden $n$. Si $A$ es una base para $G$ con $k$ elementos, entonces $k(k+1) \geq 2n$.*

**Prueba**

Supongamos que $A$ es una base para $G$, entonces

$$A + A = G,$$

de donde

$$|A + A| = |G| = n.$$

Como $|A| = k$, entonces $A + A$ tiene a lo sumo $\binom{k}{2} + k$ elementos, es decir

$$n = |A + A| \leq \binom{k+1}{2} = \frac{k(k+1)}{2},$$

en consecuencia

$$2n \leq k(k+1). \ \square$$

**Corolario 1.2.1** *La función $\alpha(G)$ satisface la siguiente relación*

$$\liminf_{|G|\to\infty} \frac{\alpha(G)}{\sqrt{|G|}} \geq \sqrt{2}.$$

**Prueba**

Por Teorema 1.2.1, $\alpha(G)$ satisface la relación

$$\begin{aligned}
(\alpha(G)+1)^2 \geq \alpha(G)(\alpha(G)+1) \geq 2n, &\text{ donde } n = |G| \\
\alpha(G)+1 \geq \sqrt{2n}, & \\
\alpha(G) \geq \sqrt{2n} - 1, & \\
\frac{\alpha(G)}{\sqrt{n}} \geq \sqrt{2} - \frac{1}{\sqrt{n}}, &
\end{aligned}$$

luego

$$\liminf_{|G|\to\infty} \frac{\alpha(G)}{\sqrt{|G|}} \geq \sqrt{2}. \ \square$$

**Teorema 1.2.2** *Sea $G$ un grupo conmutativo de orden $n$. Si $A$ es una base estricta para $G$ con $k$ elementos, entonces*

$$k(k-1) \geq 2n.$$

**Prueba**

Supongamos que A es una base estricta para G, entonces

$$A\hat{+}A = G,$$

de donde

$$| \ A\hat{+}A \ | = | \ G \ | = n.$$

Como $|A| = k$, entonces $A\hat{+}A$ tiene a lo sumo $\binom{k}{2}$ elementos, es decir

$$n = |\ A\hat{+}A\ | \leq \binom{k}{2} = \frac{k(k-1)}{2},$$

en consecuencia,

$$2n \leq k(k-1). \ \square$$

**Corolario 1.2.2** *La función $\hat{\alpha}(G)$ satisface la siguiente relación*

$$\liminf_{|G|\to\infty} \frac{\hat{\alpha}(G)}{\sqrt{|G|}} \geq \sqrt{2}.$$

**Prueba**

Por Teorema 1.2.2 $\hat{\alpha}(G)$ satisface la relación

$$\begin{aligned}
(\hat{\alpha}(G))^2 &\geq \hat{\alpha}(G)(\hat{\alpha}(G)-1) \geq 2n, \text{donde } n = |G| \\
\hat{\alpha}(G) &\geq \sqrt{2n}, \\
\hat{\alpha}(G) &\geq \sqrt{2n}, \\
\frac{\hat{\alpha}(G)}{\sqrt{n}} &\geq \sqrt{2},
\end{aligned}$$

luego

$$\liminf_{|G|\to\infty} \frac{\hat{\alpha}(G)}{\sqrt{|G|}} \geq \sqrt{2}. \ \square$$

Los Teoremas 1.2.1 y 1.2.2 nos determinan cotas inferiores para el cardinal de una base para $G$.

En [2] se presenta el siguiente teorema el cual nos muestra cotas inferiores análogas a las de los Teoremas 1.2.1 y 1.2.2.

**Teorema 1.2.3** *Sea* $CI(n) := \left\lceil \frac{1+\sqrt{1+8n}}{2} \right\rceil$. *Entonces para todo grupo abeliano $G$ de orden $n$, se tiene*

*1)* $\alpha(G) \geq CI(n) - 1$.

*2)* $\hat{\alpha}(G) \geq CI(n)$.

**Prueba**

1) Sea $A$ un subconjunto de $G$ de cardinalidad $k$. Entonces $A$ tiene a lo sumo $\binom{k}{2}+k$ sumas distintas. Comparándola con $n$ nos conduce a una condición necesaria sobre el tamaño de $k$ si $A$ es base para $G$

$$\binom{k}{2}+k \geq n,$$

esto conduce a la desigualdad cuadrática en $k$

$$k^2+k-2n \geq 0,$$

completando cuadrados

$$k \geq \frac{\sqrt{8n+1}}{2}-\frac{1}{2},$$

como $\left\lceil x-\frac{1}{2}\right\rceil = \left\lceil x+\frac{1}{2}\right\rceil - 1$, para $x \in \mathbb{Z}^+$ entonces

$$k \geq \left\lceil \frac{1+\sqrt{1+8n}}{2}\right\rceil - 1,$$

luego

$$k \geq CI(n)-1.$$

2) Sea $A$ un subconjunto de $G$ de cardinalidad $k$. Entonces $A$ tiene a lo sumo $\binom{k}{2}$ sumas estrictas distintas. Comparándolas con $n$ nos conduce a una condición necesaria sobre el tamaño de $k$ si $A$ es base estricta para $G$

$$\binom{k}{2} \geq n,$$

esto conduce a la desigualdad cuadrática en $k$

$$k^2-k-2n \geq 0,$$

completando cuadrados

$$k \geq \frac{\sqrt{8n+1}}{2}+\frac{1}{2},$$

es decir

$$k \geq \left\lceil \frac{1+\sqrt{1+8n}}{2} \right\rceil,$$

luego

$$k \geq CI(n).$$

En consecuencia de 1) y 2) el resultado se sigue. □

## 1.3. Construcción Natural de una Base para $\mathbb{Z}_n$

En [2] utilizando representación de enteros base b, se puede obtener una construcción para una base, la cual presentamos en la demostración del siguiente teorema.

**Teorema 1.3.1** *La función $\hat{\alpha}(n)$ satisface la siguiente relación*

$$\hat{\alpha}(n) \leq 2\lceil \sqrt{n}\ \rceil.$$

**Prueba**.

Sean $b = \lceil \sqrt{n}\ \rceil$, y

$$P := \{0, 1, 2, 3, ..., b-1\},$$
$$Q := \{b, 2b, 3b, ..., (b-1)b\}.$$

Si al conjunto $P$ le sumamos cada uno de los elementos de $Q$ obtenemos

$$\begin{aligned} P + \{b\} &= \{b, b+1, b+2, ..., 2b-1\} \\ P + \{2b\} &= \{2b, 2b+1, 2b+2, ..., 3b-1\} \\ &\vdots \\ P + \{(b-2)b\} &= \{b^2-2b, b^2-2b+1, ..., b^2-b-1\} \\ P + \{(b-1)b\} &= \{b^2-b, b^2-b+1, b^2-b+2, ..., b^2-1\}. \end{aligned}$$

Esto significa que las sumas en $P + Q$, que son todas estrictas, producen todos los enteros desde $b$ hasta $b^2 - 1$, es decir $P + Q = [b, b^2 - 1]$.

Por otro lado como $P\hat{+}P = [1, 2b-3]$, entonces $(P\hat{+}P) \cup (P+Q) = [1, b^2-1]$. Además por definición de $b$ tenemos, $[1, n-1] \subseteq [1, b^2-1]$. Finalmente, para obtener el cero como suma estricta se agrega $-1$ al conjunto $P \cup Q$.

Luego $P \cup Q \cup \{-1\}$ es una base estricta para $\mathbb{Z}_n$ con $2b$ elementos y por lo tanto $\hat{\alpha}(n) \leq 2\lceil \sqrt{n} \rceil$. $\square$

El teorema anterior nos determina una cota superior para el mínimo cardinal de una base estricta para $\mathbb{Z}_n$ y la prueba nos proporciona la construcción de una base estricta.

**Nota.** El autor en esta construcción no modula como lo vemos en el siguiente ejemplo.

**Ejemplo 1.3.1** *Sea $n = 56$, entonces $b = 8$ y así*

$$P = \{0, 1, 2, 3, 4, 5, 6, 7\} \text{ y } Q = \{8, 16, 24, 32, 40, 48, 56\}$$

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 16 | 24 | 32 | 40 | 48 | 56 | −1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 17 | 25 | 33 | 41 | 49 | 57 | 0 |
| | | | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 18 | 26 | 34 | 42 | 50 | 58 | 1 |
| | | | | 6 | 7 | 8 | 9 | 10 | 11 | 19 | 27 | 35 | 43 | 51 | 59 | 2 |
| | | | | | 8 | 9 | 10 | 11 | 12 | 20 | 28 | 36 | 44 | 52 | 60 | 3 |
| | | | | | | 10 | 11 | 12 | 13 | 21 | 29 | 37 | 45 | 53 | 61 | 4 |
| | | | | | | | 12 | 13 | 14 | 22 | 30 | 38 | 46 | 54 | 62 | 5 |
| | | | | | | | | 14 | 15 | 23 | 31 | 39 | 47 | 55 | 63 | 6 |
| | | | | | | | | | 16 | 24 | 32 | 40 | 48 | 56 | 64 | 7 |
| | | | | | | | | | | 32 | 40 | 48 | 56 | 64 | 72 | 15 |
| | | | | | | | | | | | 48 | 56 | 64 | 72 | 80 | 23 |
| | | | | | | | | | | | | 64 | 72 | 80 | 88 | 31 |
| | | | | | | | | | | | | | 80 | 88 | 96 | 39 |
| | | | | | | | | | | | | | | 96 | 104 | 47 |
| | | | | | | | | | | | | | | | 112 | 55 |
| | | | | | | | | | | | | | | | | −2 |

*Por lo tanto, $P \cup Q \cup \{-1\}$ nos entrega una base estricta no modular para $\mathbb{Z}_{56}$.*

## 1.4. Mejoras de la Construcción Natural

Considerando los conjuntos $P$ y $Q$ de la la prueba del Teorema 1.3.1 tenemos el siguiente corolario.

**Corolario 1.4.1** *Para $b \geq 3$, si $n$ es tal que $b = \lceil \sqrt{n} \rceil$ entonces $P \cup Q$ es una base estricta módulo $n$.*

**Prueba**

De igual manera que se hizo en la prueba del Teorema 1.3.1 tenemos que

$$(P\hat{+}P) \cup (P+Q) = [1, b^2-1] \text{ y } [1, n-1] \subseteq [1, b^2-1].$$

Finalmente, para mostrar que el cero se obtiene como suma estricta módulo $n$ hacemos el siguiente análisis:

notemos que por definición $b = \lceil \sqrt{n} \rceil$, entonces $\sqrt{n} \leq \lceil \sqrt{n} \rceil = b$, luego $n \leq b^2$.

- Si $n = b^2$, entonces $n = b + (b-1)b = 0(\text{mód } n)$, con $b \neq (b-1)b$ pues $b \geq 3$, es decir que el cero se obtiene en $Q\hat{+}Q$.
- Si $n < b^2$, el cero se obtiene como suma estricta módulo $n$, ya que $n \in [1, b^2-1]$.

Por lo tanto tenemos que $P \cup Q$ es una base estricta módulo $n$ con $2b-1$ elementos. □

Un análisis detallado de la construcción natural nos conduce a mejoras en cuanto al número de elementos de una base estricta lo cual presentamos en los siguientes teoremas.

**Teorema 1.4.1** *Para $b \geq 4$, si $n$ es tal que $b = \lceil \sqrt{n} \rceil$, La función $\hat{\alpha}(n)$ satisface las siguientes relaciones*

*1)* $\hat{\alpha}(n) \leq 2b-2$, *si* $n \in [b^2-2b+2, b^2-b]$.

*2)* $\hat{\alpha}(n) \leq 2b-1$, *si* $n \in [b^2-b+1, b^2]$.

**Prueba**

Notemos que $n \geq b^2-2b+2$, pues $\sqrt{n} > b-1$ de donde $n > b^2-2b+1$.

1) Sean

$$P = \{0, 1, 2, ..., b-1\} \text{ y } Q' = \{b, 2b, ..., (b-2)b\}.$$

De igual manera que se hizo en la prueba del Teorema 1.3.1 tenemos que

$$(P\hat{+}P) \cup (P+Q') = [1, b^2-b-1] \text{ y } [1, n-1] \subseteq [1, b^2-b-1].$$

Finalmente, para mostrar que el cero se obtiene como suma estricta módulo $n$ hacemos el siguiente análisis:

- Si $n = b^2-b$, entonces $n = (b-2)b + b = 0(mod\ n)$, con $b \neq (b-2)b$ pues $b \geq 4$.
- Si $b^2-2b+2 \leq n < b^2-b$, el cero se obtiene como suma estricta módulo $n$, ya que $n \in [1, b^2-b-1]$.

Por lo tanto $P \cup Q'$ es una base estricta para $\mathbb{Z}_n$, con $2b-2$ elementos.

2) Considerando los conjuntos $P$ y $Q$ de la prueba del Teorema 1.3.1 tenemos que la demostración es análoga a la del Corolario 1.4.1.

De 1) y 2) se obtiene lo deseado. □

**Ejemplo 1.4.1** *Sea* $n = 56$*, entonces* $b = 8$ *y así*

$$P = \{0, 1, 2, 3, 4, 5, 6, 7\} \text{ y } Q' = \{8, 16, 24, 32, 40, 48\}$$

| + | ***0*** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 16 | 24 | 32 | 40 | 48 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***2*** | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 17 | 25 | 33 | 41 | 49 | |
| | | ***4*** | 5 | 6 | 7 | 8 | 9 | 10 | 18 | 26 | 34 | 42 | 50 | |
| | | | ***6*** | 7 | 8 | 9 | 10 | 11 | 19 | 27 | 35 | 43 | 51 | |
| | | | | ***8*** | 9 | 10 | 11 | 12 | 20 | 28 | 36 | 44 | 52 | |
| | | | | | ***10*** | 11 | 12 | 13 | 21 | 29 | 37 | 45 | 53 | |
| | | | | | | ***12*** | 13 | 14 | 22 | 30 | 38 | 46 | 54 | |
| | | | | | | | ***14*** | 15 | 23 | 31 | 39 | 47 | 55 | |
| | | | | | | | | ***16*** | 24 | 32 | 40 | 48 | 0 | |
| | | | | | | | | | ***32*** | 40 | 48 | 0 | 8 | |
| | | | | | | | | | | ***48*** | 0 | 8 | 16 | |
| | | | | | | | | | | | ***8*** | 16 | 24 | |
| | | | | | | | | | | | | ***24*** | 32 | |
| | | | | | | | | | | | | | ***40*** | |

*Por lo tanto,* $P \cup Q'$ *nos entrega una base estricta módulo* 56*, con* 14 *elementos.*

**Teorema 1.4.2** *Para* $c \in \mathbb{Z}^+$ *tal que* $c \geq 3$*, la función* $\hat{\alpha}(n)$ *satisface las siguientes relaciones*

*1)* $\hat{\alpha}(n) \leq 2c-2$*, si* $n \in [c^2-c-2, c^2-3]$.

*2)* $\hat{\alpha}(n) \leq 2c-1$*, si* $n \in [c^2-2, c^2+c-3]$.

**Prueba**

1) Sean $P = \{0, 1, 2, 3, ..., c-1\}$ y $Q^* = \{2c-2, 3c-2, ..., (c-1)c-2\}$. Con un argumento igual al del Teorema 1.3.1, las sumas $P + Q^*$ son todas estrictas y producen todos los enteros desde $2c-2$ hasta $c^2-3$, es decir $P + Q^* = [2c-2, c^2-3]$. Por otro

lado $P\hat{+}P = [1, 2c-3]$ entonces $(P\hat{+}P) \cup (P + Q^*) = [1, c^2-3]$. Como por hipótesis $n \in [c^2-c-2, c^2-3] \subset [1, c^2-3]$, entonces el cero lo obtenemos como suma estricta módulo $n$. Por lo tanto $P \cup Q^*$ es base estricta para $\mathbb{Z}_n$ con $2c-2$ elementos.

2) Sean $P = \{0, 1, 2, 3, ..., c-1\}$ y $Q^* = \{2c-2, 3c-2, ..., c^2-2\}$. Con un argumento igual al del Teorema 1.3.1, las sumas $P + Q^*$ son todas estrictas y producen todos los enteros desde $2c-2$ hasta $c^2+c-3$, es decir $P + Q^* = [2c-2, c^2+c-3]$. Por otro lado $P\hat{+}P = [1, 2c-3]$ entonces $(P\hat{+}P) \cup (P + Q^*) = [1, c^2+c-3]$. Como por hipótesis $n \in [c^2-2, c^2+c-3] \subset [1, c^2+c-3]$, entonces el cero lo obtenemos como suma estricta módulo $n$. Por lo tanto $P \cup Q^*$ es base estricta para $\mathbb{Z}_n$ con $2c-1$ elementos. □

**Ejemplo 1.4.2** *Sea $n = 57$, entonces $c = 8$ ya que $n \in [c^2-c-2, c^2-3] = [54, 61]$, así*

$$P = \{0, 1, 2, 3, 4, 5, 6, 7\} \text{ y } Q^* = \{14, 22, 30, 38, 46, 54\}$$

| + | ***0*** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 14 | 22 | 30 | 38 | 46 | 54 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ***2*** | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 15 | 23 | 31 | 39 | 47 | 55 |
| | | ***4*** | 5 | 6 | 7 | 8 | 9 | 10 | 16 | 24 | 32 | 40 | 48 | 56 |
| | | | ***6*** | 7 | 8 | 9 | 10 | 11 | 17 | 25 | 33 | 41 | 49 | 0 |
| | | | | ***8*** | 9 | 10 | 11 | 12 | 18 | 26 | 34 | 42 | 50 | 1 |
| | | | | | ***10*** | 11 | 12 | 13 | 19 | 27 | 35 | 43 | 51 | 2 |
| | | | | | | ***12*** | 13 | 14 | 20 | 28 | 36 | 44 | 52 | 3 |
| | | | | | | | ***14*** | 15 | 21 | 29 | 37 | 45 | 53 | 4 |
| | | | | | | | | ***28*** | 36 | 44 | 52 | 3 | 11 | 19 |
| | | | | | | | | | ***44*** | 52 | 3 | 11 | 19 | 27 |
| | | | | | | | | | | ***3*** | 11 | 19 | 27 | 35 |
| | | | | | | | | | | | ***19*** | 27 | 35 | 43 |
| | | | | | | | | | | | | ***35*** | 43 | ***51*** |

*Por lo tanto, $P \cup Q^*$ nos entrega una base estricta módulo 57, con 14 elementos, a diferencia de la base estricta módulo 57, que entrega la prueba del Teorema 1.4.1 que tiene 15 elementos.*

## 1.5. Resultado Central

**Teorema 1.5.1** *Las funciones $\alpha(n)$ y $\hat{\alpha}(n)$, satisfacen la siguientes relaciones*

*1)* $\sqrt{2} \leq \liminf_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq 2.$

*2)* $\sqrt{2} \leq \liminf_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq 2.$

**Prueba**

1) Por el Corolario 1.2.1 se tiene que

$$\liminf_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \geq \sqrt{2}.$$

Como $\frac{\alpha(n)}{\sqrt{n}}$ es una sucesión de números reales, entonces

$$\liminf_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}}.$$

Resta probar que

$$\limsup_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq 2.$$

Aplicando los resultados del Teorema 1.1.1 y Teorema 1.3.1 obtenemos la relación $\alpha(n) \leq 2\lceil \sqrt{n} \rceil \leq 2(\sqrt{n}+1)$, con lo cual $\frac{\alpha(n)}{\sqrt{n}} \leq 2 + \frac{2}{\sqrt{n}}$. Así

$$\limsup_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq 2,$$

por lo tanto

$$\sqrt{2} \leq \liminf_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\alpha(n)}{\sqrt{n}} \leq 2.$$

2) Por el Corolario 1.2.2 se tiene que

$$\liminf_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \geq \sqrt{2}.$$

Como $\frac{\hat{\alpha}(n)}{\sqrt{n}}$ es una sucesión de números reales, entonces

$$\liminf_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}}.$$

Resta probar que:

$$\limsup_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq 2,$$

aplicando el Teorema 1.3.1 tenemos la siguiente relación $\hat{\alpha}(n) \leq 2\lceil\sqrt{n}\,\rceil \leq 2(\sqrt{n}+1)$, con lo cual $\dfrac{\hat{\alpha}(n)}{\sqrt{n}} \leq 2 + \dfrac{2}{\sqrt{n}}$. Así

$$\limsup_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq 2.$$

Por lo tanto

$$\sqrt{2} \leq \liminf_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{\hat{\alpha}(n)}{\sqrt{n}} \leq 2. \quad \square$$

# Capítulo 2

# Conjuntos de Sidon.

## 2.1. Definiciones y Resultados Básicos

Sean $(G, +)$ un grupo conmutativo finito, notado aditivamente y $A \subseteq G$.

$A$ es un **conjunto de Sidon** en $G$ si todas las sumas de dos elementos de A son distintas. Es decir, si $|A + A| = \binom{|A|+1}{2}$.
Para probar que $A$ es un conjunto de Sidon verificamos que

$$(a + b = c + d) \Rightarrow (a = c \wedge b = d) \vee (a = d \wedge b = c),$$

para todo $a$, $b$, $c$, $d \in A$.

**Ejemplo 2.1.1** *Sean $G = \mathbb{Z}_{25}$ y $A = \{0, 1, 3, 7, 12\}$, entonces $A+A$ se puede representar por la siguiente tabla*

| + | 0 | 1 | 3 | 7 | 12 |
|---|---|---|---|---|---|
| | | 2 | 4 | 8 | 13 |
| | | | 6 | 10 | 15 |
| | | | | 14 | 19 |
| | | | | | 24 |

*se puede notar que los elementos del conjunto suma $A + A$ son todos distintos. Luego $A$ es un conjunto de Sidon en $G$.*

**Ejemplo 2.1.2** *Sean $G = \mathbb{Z}_{17}$ y $A = \{0, 1, 3, 7, 8\}$, entonces $A+A$ se puede representar por la siguiente tabla*

| $+$ | 0 | 1 | 3 | 7 | 8 |
|---|---|---|---|---|---|
| | | 2 | 4 | 8 | 9 |
| | | | 6 | 10 | 11 |
| | | | | 14 | 15 |
| | | | | | 16 |

*se puede notar que el* 8 *se repite dos veces. Por lo tanto A no es un conjunto de Sidon en G.*

$A$ es un **conjunto de Sidon estricto** en $G$ si todas las sumas de dos elementos diferentes de $A$ son distintas. Es decir, $|A\hat{+}A| = \binom{|A|}{2}$.

**Ejemplo 2.1.3** *Sean* $G = \mathbb{Z}_{15}$ *y* $A = \{0, 3, 5, 6, 7\}$*, entonces* $A\hat{+}A$ *se puede representar por la siguiente tabla*

| $\hat{+}$ | ***0*** | 3 | 5 | 6 | 7 |
|---|---|---|---|---|---|
| | | ***6*** | 8 | 9 | 10 |
| | | | ***10*** | 11 | 12 |
| | | | | ***12*** | 13 |
| | | | | | ***14*** |

*se puede notar que todas las sumas de dos elementos diferentes son distintas, luego A es un conjunto de Sidon estricto en G, pero no un conjunto de Sidon ya que se repiten los elementos* $6, 10$ *y* $12$*.*

**Ejemplo 2.1.4** *Sean* $G = \mathbb{Z}_{18}$ *y* $A = \{0, 3, 5, 6, 7, 14\}$*, entonces* $A\hat{+}A$ *se puede representar por la siguiente tabla*

| $\hat{+}$ | ***0*** | 3 | 5 | 6 | 7 | 14 |
|---|---|---|---|---|---|---|
| | | ***6*** | 8 | 9 | 10 | 17 |
| | | | ***10*** | 11 | 12 | 1 |
| | | | | ***12*** | 13 | 2 |
| | | | | | ***14*** | 3 |
| | | | | | | ***10*** |

*se puede notar que el* 3 *se repite dos veces. Por lo tanto A no es un conjunto de Sidon estricto en G.*

$A$ es un **conjunto de Sidon diferencia** en $G$ si todas las diferencias de dos elementos distintos de A son distintas. Es decir, $|(A - A)\backslash\{0\}| = |A|(|A| - 1)$. Para probar que $A$ es un conjunto de Sidon diferencia verificamos que

$$(a - b = c - d \text{ con } a \neq b \wedge c \neq d) \Rightarrow a = c \wedge b = d,$$

para todo $a$, $b$, $c$, $d \in A$.

**Ejemplo 2.1.5** *Sean $G = \mathbb{Z}_{15}$ y $A = \{0, 1, 3, 7\}$, entonces $A - A$ se puede representar por la siguiente tabla*

| $-$ | 0 | 1 | 3 | 7 |
|---|---|---|---|---|
| 0 | 0 | 14 | 12 | 8 |
| 1 | 1 | 0 | 13 | 9 |
| 3 | 3 | 2 | 0 | 11 |
| 7 | 7 | 6 | 4 | 0 |

*se puede notar que todas las diferencias de dos elementos diferentes son distintas, luego $A$ es un conjunto de Sidon diferencia en $G$.*

**Ejemplo 2.1.6** *Sean $G = \mathbb{Z}_{17}$ y $A = \{0, 2, 3, 4, 6, 7\}$, entonces $A - A$ se puede representar por la siguiente tabla*

| $-$ | 0 | 2 | 3 | 4 | 6 | 7 |
|---|---|---|---|---|---|---|
| 0 | 0 | 15 | 14 | 13 | 11 | 10 |
| 2 | 2 | 0 | 16 | 15 | 13 | 12 |
| 3 | 3 | 1 | 0 | 16 | 14 | 13 |
| 4 | 4 | 2 | 1 | 0 | 15 | 14 |
| 6 | 6 | 4 | 3 | 2 | 0 | 16 |
| 7 | 7 | 5 | 4 | 3 | 1 | 0 |

*se puede notar que los números $1, 2, 3, 4, 13, 14, 15, 16$ se repiten. Por lo tanto $A$ no es un conjunto de Sidon diferencia en $G$.*

Los conceptos de conjunto de Sidon y conjunto de Sidon diferencia son equivalentes como muestra el siguiente resultado.

**Teorema 2.1.1** *$A$ es un conjunto de Sidon en $G$ si solo si $A$ es un conjunto de Sidon diferencia.*

**Prueba**

Sean $a, b, c, d \in A$.

($\Rightarrow$) Supongamos que $A$ es un conjunto de Sidon y que $a - d = c - b$ con $a \neq d$ y $c \neq b$; entonces $a + b = c + d$. Pero sabemos que $A$ es un conjunto de Sidon, lo cual implica

que $(a = c,\ b = d)$ o $(a = d,\ b = c)$ y como $a \neq d$ y $c \neq b$, entonces $a = c$ y $b = d$. Por lo tanto $A$ es un conjunto de Sidon diferencia para $G$.

($\Leftarrow$) Supongamos que $A$ es un conjunto de Sidon diferencia y que $a + b = c + d$; luego $a - d = c - b$ con $a \neq d$ lo cual implica que $a = c$, $d = b$. Por lo tanto $A$ es un conjunto de Sidon en $G$. $\square$

De igual manera que se hizo en el Capítulo 1 se puede preguntar por las siguientes funciones extremas que han sido estudiadas en trabajos anteriores. Por este motivo sólo las mencionaremos.

$$\beta(G) := \text{máx}\{|A| : A \textit{ es Sidon en } G\}.$$

$$\hat{\beta}(G) := \text{máx}\{|A| : A \textit{ es Sidon estricto en } G\}.$$

Si $G$ es cíclico de orden $n$ entonces sabemos que $G$ es isomorfo a $\mathbb{Z}_n$ (aditivamente), en este caso notamos $\beta(G) = \beta(n)$ y $\hat{\beta}(G) = \hat{\beta}(n)$.

Mediante conteo es fácil obtener una cota superior para un conjunto de Sidon, la cual presentamos en el siguiente teorema.

**Teorema 2.1.2** *Sea $G$ un grupo de orden $n$. Si $A$ es un conjunto de Sidon en $G$ con $k$ elementos entonces*

$$k(k-1) \leq n - 1.$$

**Prueba**

Supongamos que $A$ es un conjunto de Sidon en $G$, entonces hay $\binom{k}{2}$ subconjuntos de dos elementos $\{a, b\}$. A cada uno de ellos se le asigna dos diferencias distintas $(a - b)$ y $(b - a)$. Por lo tanto hay $2\binom{k}{2}$ diferencias no cero en $A - A$ entonces

$$2\binom{k}{2} + 1 = k(k-1) + 1 = |A - A| \leq n,$$

luego

$$k(k-1) \leq n - 1. \ \square$$

**Corolario 2.1.1** *La función $\beta(n)$ satisface la siguiente relación*

$$\limsup_{n\to\infty} \frac{\beta(n)}{\sqrt{n}} \leq 1.$$

**Prueba**

Por definición de $\beta(n)$ existe un conjunto de Sidon $A \subseteq \mathbb{Z}_n$ tal que $\beta(n) = |A|$. Por Teorema 2.1.2

$$\begin{aligned}(\beta(n)-1)^2 \leq \beta(n)(\beta(n)-1) &\leq n-1,\\ \beta(n) &\leq \sqrt{n-1}+1,\\ \frac{\beta(n)}{\sqrt{n}} &\leq \sqrt{1-\frac{1}{n}}+\frac{1}{\sqrt{n}},\end{aligned}$$

luego

$$\limsup_{n\to\infty} \frac{\beta(n)}{\sqrt{n}} \leq 1. \ \square$$

## 2.2. Construcciones(Bose, Ruzsa)

En esta sección mostraremos como se construyen conjuntos de Sidon para determinados módulos y así encaminarnos hacia la construcción de bases a partir de estos conjuntos.

Recordemos algunos conceptos y resultados básicos de la Teoría de Campos Finitos.

Sean $q$ una potencia prima, $F_q$ el único (salvo isomorfismos) campo finito con $q$ elementos, $F_q^* = F_q \backslash \{0\}$ (grupo multiplicativo) con $|F_q^*| = q-1$ y $\delta$ un generador de $F_q^*$. Luego

$$F_q^* = \langle \delta \rangle = \{\delta, \delta^2, \delta^3, ..., \delta^{q-1} = 1\},$$

es decir, para todo $\alpha \in F_q^*$, existe un único $k \in [1, q-1]$ tal que $\alpha = \delta^k$. Escribimos $k = \log_\delta \alpha$ (logaritmo discreto de $\alpha$ en base $\delta$). Este logaritmo tienes las propiedades de logaritmo real para el producto y el cociente.

Para todo par de enteros $i$, $j$,

$$\delta^i = \delta^j \Leftrightarrow i \equiv j \ (\text{mód } q-1)$$

y para $i, j \in [1, q-1]$

$$\delta^i = \delta^j \Leftrightarrow i = j.$$

**Construcción R.C. Bose (1942)**

En versión actual la construcción de Bose puede escribirse como sigue:

Sea $\theta$ un generador de $F_{q^2}^*$.

1) Consideremos el campo finito $F_q$ y su extensión $F_{q^2}$.

2) Como $\theta$ es un generador de $F_{q^2}^*$, tenemos

$$F_{q^2}^* = \langle\theta\rangle = \{\theta, \theta^2, \theta^3, ..., \theta^{q^2-1} = 1\},$$

con lo que además se concluye que $\theta$ es algebraico de grado 2 sobre $F_q$, es decir el polinomio mónico minimal irreducible de $\theta$ sobre $F_q$ es de grado 2, además $\theta^{q+1}$ genera en $F_{q^2}^*$ un subgrupo de orden $q-1$ el cual debe ser $F_q^*$.

3) Definimos en $F_{q^2}$ el conjunto

$$\theta + F_q = \{\theta + a : a \in F_q\} \subseteq F_{q^2}^*.$$

4) Definimos el conjunto de enteros positivos

$$Bose(q, \theta) = \{\log_\theta(\theta + a) : a \in F_q\}.$$

Es claro que

$$|Bose(q, \theta)| \leq q.$$

**Teorema 2.2.1** *Para toda potencia prima $q$ y todo $\theta$ generador de $F_{q^2}^*$, tenemos que $Bose(q, \theta)$ es un conjunto de Sidon en $\mathbb{Z}_{q^2-1}$ con $q$ elementos.*

**Prueba**

Veamos que $Bose(q, \theta)$ tiene $q$ elementos. Sean $a, b \in F_q$ tales que

$$\log_\theta(\theta + a) = \log_\theta(\theta + b) = k \in [1, q-1],$$

luego

$$\theta^k = \theta + a = \theta + b,$$

entonces $a = b$, por lo tanto $|Bose(q, \theta)| = q$.

Probemos ahora que $Bose(q, \theta)$ es un conjunto de Sidon en $\mathbb{Z}_{q^2-1}$.

Sean $x, y, u, v \in Bose(q, \theta)$ tales que

$$x + y = u + v. \tag{2.1}$$

Por definición de $Bose(q, \theta)$, existen $a, b, c, d \in \mathbb{F}_q$ tales que

$$x = \log_\theta(\theta + a),\ y = \log_\theta(\theta + b),\ u = \log_\theta(\theta + c) \text{ y } v = \log_\theta(\theta + d).$$

luego

$$\begin{aligned} x + y &= \log_\theta(\theta + a) + \log_\theta(\theta + b) \\ &= \log_\theta((\theta + a)(\theta + b)) \end{aligned}$$

y

$$\begin{aligned} u + v &= \log_\theta(\theta + c) + \log_\theta(\theta + d) \\ &= \log_\theta((\theta + c)(\theta + d)), \end{aligned}$$

así de (2.1) tenemos

$$\log_\theta((\theta + a)(\theta + b)) = \log_\theta((\theta + c)(\theta + d))$$

entonces

$$((a + b) - (c + d))\theta + (ab - cd) = 0,$$

como el grado de $\theta$ sobre $\mathbb{F}_q$ es igual a 2, debe tenerse que

$$a + b = c + d \text{ y } ab = cd, \text{ en } \mathbb{F}_q.$$

Sean $s = a + b = c + d$ y $p = ab = cd$, entonces los conjuntos $\{a, b\}$ y $\{c, d\}$ contienen las raíces del polinomio $z^2 - sz + p$ y como estamos en el campo $\mathbb{F}_q$, tenemos que

$$\{a, b\} = \{c, d\},$$

entonces

$$\{\theta + a, \theta + b\} = \{\theta + c, \theta + d\},$$

con lo cual

$$\{x, y\} = \{u, v\}.$$

Por lo tanto $Bose(q, \theta)$ es un conjunto de Sidon en $\mathbb{Z}_{q^2-1}$ con $q$ elementos. □

**Ejemplo 2.2.1** *Sea $q = 5$ y $\theta$ un generador de $F_{25}^*$ el cual es raíz del polinomio mónico irreducible $x^2 + 4x + 2$ sobre $F_5$ . la siguiente tabla muestra las potencias de $\theta$*

| $k$ | $\theta^k$ |
|---|---|
| 1 | $\theta$ |
| 2 | $\theta + 3$ |
| 3 | $4\theta + 3$ |
| 4 | $2\theta + 2$ |
| 5 | $4\theta + 1$ |
| 6 | 2 |
| 7 | $2\theta$ |
| 8 | $2\theta + 1$ |
| 9 | $3\theta + 1$ |
| 10 | $4\theta + 4$ |
| 11 | $3\theta + 2$ |
| 12 | 4 |
| 13 | $4\theta$ |
| 14 | $4\theta + 2$ |
| 15 | $\theta + 2$ |
| 16 | $3\theta + 3$ |
| 17 | $\theta + 4$ |
| 18 | 3 |
| 19 | $3\theta$ |
| 20 | $3\theta + 4$ |
| 21 | $2\theta + 4$ |
| 22 | $\theta + 1$ |
| 23 | $2\theta + 3$ |
| 24 | 1. |

*Como*

$$\theta + F_5 = \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4\}$$

*luego, aplicando logaritmo en base $\theta$ al conjunto anterior tenemos*

$$\{1, 2, 15, 17, 22\} = Bose(5, \theta).$$

**Corolario 2.2.1** *Para toda potencia prima $q$*

$$\beta(q^2 - 1) = q.$$

**Prueba**

Supongamos que existe un conjunto de Sidon $A$ en $\mathbb{Z}_{q^2-1}$ tal que $|A| = k > q$, entonces

$$k(k-1) \geq (q+1)q = q^2 + q > n - 1, \text{ donde } n = q^2 - 1$$

que no es posible ya que por Teorema 2.1.2 $k(k-1) \leq (n-1)$.
Por lo tanto $\beta(q^2 - 1) = q$. □

**Propiedades de** $Bose(q, \theta)$

1) Para todo $x \in Bose(q, \theta)$, se tiene que $x \not\equiv 0(\text{mód } q+1)$.

   **Prueba**

   Como $x \in Bose(q, \theta)$, entonces existe $a \in F_q$ tal que $x = \log_\theta(\theta + a)$, luego $\theta^x = \theta + a$.

   Supongamos que $x \equiv 0(\text{mód } q+1)$, a lo que es equivalentemente $x = t(q+1)$, para algún $t \in \mathbb{Z}^+$, lo cual implica que $\theta^x = (\theta^{q+1})^t \in F_q^*$, ya que $\langle \theta^{q+1} \rangle = F_q^*$. Así $\theta + a \in F_q^*$, lo cual no es posible ya que el grado de $\theta$ sobre $F_q$ es igual a dos. □

2) Para todo $x, y \in Bose(q, \theta)$ con $x \neq y$ se tiene que $x \not\equiv y(\text{mód } q+1)$.

   **Prueba**

   Como $x, y \in Bose(q, \theta)$ entonces existen $a$,$b \in F_q$ tales que:

   $$x = \log_\theta(\theta + a) \text{ y } y = \log_\theta(\theta + b).$$

   Con esto se tiene:

   $$x - y = \log_\theta \left( \frac{\theta + a}{\theta + b} \right)$$
   $$\theta^{x-y} = \frac{\theta + a}{\theta + b}.$$

   Ahora supongamos que $x \equiv y(\text{mód } q+1)$, es decir $x - y = t(q+1)$ para algún $t \in \mathbb{Z}$, de ahí que $\theta^{x-y} = (\theta^{q+1})^t \in F_q^*$, lo cual implica que $\dfrac{\theta + a}{\theta + b} = c \in F_q^*$, esto es $(1-c)\theta + (a - bc) = 0$, lo cual es una contradicción pues el grado de $\theta$ sobre $F_q$ es igual a dos. □

3) Sean $M = \{t(q+1) : t = 1, 2, ..., q-2\}$ y $A = Bose(q, \theta)$. Entonces

$$(A - A)(\text{mód } q^2 - 1) = \mathbb{Z}_{q^2-1} \backslash M.$$

**Prueba**

Como $A$ es un conjunto de Sidon (mód $q^2 - 1$) y $|A| = q$ entonces se tiene que $|A - A| = q(q-1) + 1 = q^2 - q + 1$. Por propiedad 2 sabemos que $(A - A) \cap M = \emptyset$, de ahí que

$$\begin{aligned} |(A - A) \cup M| &= |A - A| + |M| \\ &= (q^2 - q + 1) + (q - 2) \\ &= q^2 - 1. \end{aligned}$$

Luego $(A - A) \cup M = \mathbb{Z}_{q^2-1}$. □

**Construcción I. Ruzsa (1996)**

Sean $p$ un primo, y $g$ una raíz primitiva módulo $p$

$$\langle g \rangle = \{g, g^2, ..., g^{p-1}\} = \mathbb{Z}_p^* = F_p^*.$$

Para cada $i = 1, 2, 3, ..., p-1$ sea $a_i$ es la única solución (módulo $p(p-1)$) del sistema

$$\begin{aligned} x &\equiv i(\text{mód } p-1), \\ x &\equiv g^i(\text{mód } p). \end{aligned}$$

Definamos el conjunto $Ruzsa(p, g) = \{a_i : i = 1, 2, 3, ..., p-1\}$.

**Teorema 2.2.2** *Para todo primo $p$ y todo $g$ generador de $F_p^*$, tenemos que $Ruzsa(p, g)$ es un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$ con $p-1$ elementos.*

**Prueba**

Sean $a_i, a_j, a_k, a_l \in Ruzsa(p, g)$, con $1 \leq i, j, k, l \leq p-1$. Veamos que $Ruzsa(p, g)$ tiene $p-1$ elementos.

Supongamos que $a_i \equiv a_j(\text{mód } p-1)$, entonces

$$i \equiv j(\text{mód } p-1),$$

esto es

$$(p-1)|(i-j),$$

lo cual ocurre solamente cuando $i - j = 0$ puesto que $(1 \leq i, j \leq p-1)$, luego

$$a_i = a_j.$$

Por lo tanto $Ruzsa(p, g)$ tiene $p - 1$ elementos.

Ahora probemos que $Ruzsa(p, g)$ es un conjunto de Sidon módulo $p(p-1)$.

Supongamos que $a_i + a_j \equiv a_k + a_l (\text{mód } p(p-1))$, entonces

$$a_i + a_j \equiv a_k + a_l (\text{mód } p-1),$$
$$a_i + a_j \equiv a_k + a_l (\text{mód } p),$$

por definición de $Ruzsa(p, g)$

$$i + j \equiv k + l (\text{mód } p-1) \tag{2.2}$$
$$g^i + g^j \equiv g^k + g^l (\text{mód } p) \tag{2.3}$$

y de (2.2) tenemos que

$$g^{i+j} \equiv g^{k+l} (\text{mód } p)$$
$$g^i g^j \equiv g^k g^l (\text{mód } p). \tag{2.4}$$

Así, de (2.3) y (2.4) tenemos que

$$g^i + g^j = g^k + g^l \text{ y } g^i g^j = g^k g^l, \text{ en } F_p$$

por un argumento similar al de la prueba de la construcción de $Bose(q, \theta)$, se tiene

$$\{g^i, g^j\} = \{g^k, g^l\},$$

entonces

$$\{i, j\} = \{k, l\}, \text{ por que } (1 \leq i, j, k, l \leq p-1),$$

luego

$$\{a_i, a_j\} = \{a_k, a_l\}.$$

Por lo tanto $Ruzsa(p, g)$ es un conjunto de Sidon en $Z_{p(p-1)}$ con $p - 1$ elementos. □

**Nota.** Como $Ruzsa(p, g) = \{a_i : i = 1, 2, ..., p-1\}$, donde $a_i$ es la única solución del sistema

$$x \equiv i (\text{mód } p-1)$$
$$x \equiv g^i (\text{mód } p),$$

resolviendo este sistema $a_i$ es solución de

$$x \equiv pi - g^i(p-1)(\text{mód } p(p-1)).$$

**Ejemplo 2.2.2** *Sea $p = 5$ y $g = 2$ un generador de $F_5^*$ por la nota anterior*

$$a_i \equiv 5i - 2^i(4)(\text{mód } 20), \text{ para } i = 1, 2, ..., 4,$$

*luego*

$$\begin{aligned} a_1 &\equiv 5 - 8(\text{mód } 20) = 17, \\ a_2 &\equiv 10 - 16(\text{mód } 20) = 14, \\ a_3 &\equiv 15 - 12(\text{mód } 20) = 3, \\ a_4 &\equiv 20 - 4(\text{mód } 20) = 16, \end{aligned}$$

*por lo tanto $Ruzsa(5, 2) = \{3, 14, 16, 17\}$.*

**Corolario 2.2.2** *Para todo primo $p$ tenemos*

$$\beta(p(p-1)) = p - 1.$$

**Prueba**

Supongamos que existe un conjunto de Sidon $A$ en $\mathbb{Z}_{p(p-1)}$ tal que $|A| = k > p - 1$, entonces

$$k(k-1) \geq p(p-1) > n - 1, \text{ donde } n = p(p-1)$$

que no es posible ya que por Teorema 2.1.2

$$k(k-1) \leq (n-1).$$

Por lo tanto $\beta(p^2 - p) = p - 1$. □

**Propiedades de $Ruzsa(p, g)$**

1) Para todo $a \in Ruzsa(p, g)$, $a \not\equiv 0(\text{mód } p)$.

   **Prueba**

   Sea $a \in Ruzsa(p, g)$, luego $a = a_k$ para algún $k \in [1, p-1]$. Por definición de $Ruzsa(p, g)$, $a_k = g^k(\text{mód } p)$ donde $g$ es un generador de $F_p^*$ de ahí que $g^k \neq 0$ para todo $k$, luego $a \not\equiv 0(\text{mód } p)$. □

2) Sean $A = Ruzsa(p, g)$ y $M_p = \{p, 2p, ..., (p-2)p\}$. Entonces $(A - A) \cap M_p = \emptyset$.

**Prueba**

Sea $x \in (A - A) \cap M_p$. Como $x \in (A - A)$,

$$\begin{aligned} x &= a_i - a_j \\ &\equiv (g^i - g^j)(\text{mód } p), \end{aligned} \tag{2.5}$$

por otro lado $x \in M_p$, implica que

$$x \equiv 0(\text{mód } p). \tag{2.6}$$

Luego de (2.5) y (2.6)

$$(g^i - g^j) \equiv 0(\text{mód } p),$$

con lo cual

$$\begin{aligned} g^i &\equiv g^j(\text{mód } p) \\ i &\equiv j(\text{mód } p-1), \end{aligned}$$

pero como $i, j \in [1, p-1]$, debemos tener que $i = j$, entonces $a_i = a_j$. Es decir $x = 0$, lo cual es una contradicción pues $0 \notin M_p$. □

3) Sea $M_{p-1} = \{p-1, 2(p-1), ..., (p-1)(p-1)\}$. Entonces $(A - A) \cap M_{p-1} = \emptyset$.

**Prueba**

Sea $x \in (A - A) \cap M_{p-1}$. Como $x \in (A - A)$,

$$\begin{aligned} x &= a_i - a_j \\ &\equiv (i - j)(\text{mód } p-1), \end{aligned} \tag{2.7}$$

por otro lado $x \in M_{p-1}$, implica que

$$x \equiv 0(\text{mód } p-1). \tag{2.8}$$

Luego de (2.7) y (2.8)

$$(i - j) \equiv 0(\text{mód } p-1),$$

con lo cual

$$i \equiv j(\text{mód } p-1),$$

pero como $i, j \in [1, p-1]$, debemos tener que $i = j$, entonces $a_i = a_j$. Es decir $x = 0$, lo cual es una contradicción pues $0 \notin M_{p-1}$. □

4) $A - A = \mathbb{Z}_{p(p-1)} \backslash (M_p \cup M_{p-1})$.

**Prueba**

Como $A$ es un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$ con $|A| = p-1$, entonces

$$|A - A| = (p-1)(p-2) + 1 = p^2 - 3p + 3.$$

Notemos que $M_p \cap M_{p-1} = \emptyset$, en efecto, sea $x \in M_p \cap M_{p-1}$, entonces $x = pt$ y $x = (p-1)s$, donde $t \in [1, 2, ..., p-2]$ y $s \in [1, 2, ..., p-1]$, lo cual nos lleva a

$$\begin{aligned} pt &= (p-1)s \\ s &= (s-t)p, \end{aligned}$$

que no es posible pues $s$ no es múltiplo de $p$.

Veamos cuántos elementos hacen falta para completar $|\mathbb{Z}_{p(p-1)}|$,

$$p(p-1) - (p^2 - 3p + 3) = 2p - 3.$$

Ahora como $M_p \cap M_{p-1} = \emptyset$, $|M_p| = p-2$ y $|M_{p-1}| = p-1$, tenemos

$$|M_p \cup M_{p-1}| = |M_p| + |M_{p-1}| = 2p - 3.$$

Es decir los $2p-3$ elementos que le faltan a $A-A$ para ser $\mathbb{Z}_{p(p-1)}$, son precisamente los elementos de $M_p \cup M_{p-1}$. Por lo tanto $A - A = \mathbb{Z}_{p(p-1)} \backslash (M_p \cup M_{p-1})$. □

## 2.3. Bases a partir de Conjuntos de Sidon

En esta sección presentamos la construcción de bases a partir de un conjunto de Sidon módulo $q^2 - 1$ y $p(p-1)$, donde $q$ es una potencia prima y $p$ es un primo. Nuestra intención es formar bases con el menor número posible de elementos entonces los conjuntos de Sidon son de gran ayuda puesto que todas las sumas de dos elementos en estos conjuntos son diferentes.

**Teorema 2.3.1** *(Base a partir de un conjunto de Bose). Para toda potencia prima $q > 3$ y todo $\theta$ generador de $F^*_{q^2}$, si $A = Bose(q, \theta)$ y $M = \{t(q+1) : t = 0, 1, ..., q-2\}$ entonces $A \cup M$ es una base estricta módulo $q^2 - 1$ con $2q - 1$ elementos.*

**Prueba**

Sea $x \in A + M$, entonces probemos que $x$ se puede escribir de manera única como un elemento de $A$ y un elemento de $M$.

Supongamos que $x = a + t(q + 1)$ y $x = b + s(q + 1)$, donde $a, b \in A$ y $a \neq b$, luego $a + t(q + 1) = b + s(q + 1)$ entonces $a - b = (s - t)(q + 1) \in A - A$, lo cual no es posible por Propiedad 3 de $Bose(q, \theta)$ entonces debe ser $a = b$ de donde se deduce que $t = s$, esto es en $A+M$ todos los elementos tienen representación única. Además por Propiedad 1 de $Bose(q, \theta)$ tenemos que $A \cap M = \emptyset$ lo que nos lleva a concluir $A + M = A\hat{+}M$.

Por otro lado probemos que $(A + M) \cap (M + M) = \emptyset$. Sea $x \in (A + M) \cap (M + M)$ entonces

$$x = a + t(q + 1) \text{ y } x = s(q + 1),$$

luego

$$\begin{aligned} a + t(q + 1) &= s(q + 1) \\ a &= (s - t)(q + 1) \\ a &\equiv 0(\text{mód } q + 1), \end{aligned}$$

lo cual contradice la Propiedad 1 de $Bose(q, \theta)$, por lo tanto $(A+M)\cap(M+M) = \emptyset$.

Notemos ahora que $|A + M| = q^2 - q$, pues en $A + M$ todos los elementos son distintos y $|A| = q$, $|M| = q - 1$.

Mostremos ahora en dónde están los $q - 1$ elementos restantes de $\mathbb{Z}_{q^2-1}$.

Como $0 \in M$ tenemos

$$(M\backslash\{0\}) = (0\hat{+}M) \subseteq (M + M),$$

como

$$(A + M) \cap (M + M) = \emptyset,$$

en particular

$$(A+M)\cap(M\backslash\{0\})=\emptyset,$$

pero sabemos que $|M\backslash\{0\}|=q-2$ entonces

$$|(A+M)\cup(M\backslash\{0\})|=q^2-2.$$

Por Propiedad 1 de $Bose(q,\theta)$ tenemos que $0\notin(A+M)$ y como $0\notin(M\backslash\{0\})$, luego el cero lo obtenemos de manera estricta como

$$(q-2)(q+1)+(q+1)=q^2-1\equiv 0(\text{mód } q^2-1),$$

donde $(q-2)(q+1)$, $(q+1)\in M$ y $(q-2)(q+1)\neq(q+1)$, pues $q>3$.

Así

$$|(A+M)\cup(M\backslash\{0\})\cup\{0\}|=q^2-1. \tag{2.9}$$

Como $A\cap M=\emptyset$, $|A|=q$ y $|M|=q-1$, tenemos

$$|A\cup M|=2q-1. \tag{2.10}$$

Por lo tanto de (2.9) y (2.10) $A\cup M$ es una base estricta módulo $q^2-1$, con $2q-1$ elementos. □

**Ejemplo 2.3.1** *Sea $q=5$ entonces $\mathbb{Z}_{q^2-1}=\mathbb{Z}_{24}$, por el ejemplo 2.2.1 tenemos que $A=\{1,2,15,17,22\}$ es un conjunto de Sidon y por definición $M=\{0,6,12,18\}$. Afirmamos que $A\cup M$ es base estricta para $\mathbb{Z}_{24}$, en efecto*

| $\hat{+}$ | 1 | 2 | 15 | 17 | 22 | 0 | 6 | 12 | 18 |
|---|---|---|---|---|---|---|---|---|---|
| | ***2*** | 3 | 16 | 18 | 23 | 1 | 7 | 13 | 19 |
| | | ***4*** | 17 | 19 | 0 | 2 | 8 | 14 | 20 |
| | | | ***6*** | 8 | 13 | 15 | 21 | 3 | 9 |
| | | | | ***10*** | 15 | 17 | 23 | 5 | 11 |
| | | | | | ***20*** | 22 | 4 | 10 | 16 |
| | | | | | | ***0*** | 6 | 12 | 18 |
| | | | | | | | ***12*** | 18 | 0 |
| | | | | | | | | ***24*** | 6 |
| | | | | | | | | | ***12*** |

*Por lo tanto $A\cup M$ es una base estricta para $\mathbb{Z}_{24}$ con 9 elementos.*

**Teorema 2.3.2** *(Base a partir de un conjunto de un conjunto de Ruzsa). Para todo primo $p$ y todo $g$ raíz primitiva de $\mathbb{F}_p^*$, si*

$$A = Ruzsa(p, g) \text{ y } M = M_p \cup \{0\},$$

*entonces $A \cup M$ es una base estricta módulo $p(p-1)$ con $2(p-1)$ elementos.*

**Prueba**

Probemos primero que en $A + M$ todos los elementos tienen representación única.

Supongamos que $a + tp = b + sp$ donde $a, b \in A$, $tp, sp \in M$ y $a \neq b$, de ahí que $a - b = (s - t)(p) \in A - A$, lo cual no es posible por Propiedad 2 de $Rusa(p, g)$ entonces debe ser $a = b$ de donde se deduce que $t = s$, esto es en $A + M$ todos los elementos tienen representación única. Además por Propiedad 1 de $Ruzsa(p, g)$ tenemos que $A \cap M = \emptyset$ lo que nos lleva a decir $A + M = A\hat{+}M$.

Por otro lado probemos $(A + M) \cap (M + M) = \emptyset$.

Sea $x \in (A + M) \cap (M + M)$ entonces

$$x = a + tp \text{ y } x = sp,$$

luego

$$\begin{aligned} a + tp &= sp \\ a &= (s - t)p \\ a &\equiv 0(\text{mód } p), \end{aligned}$$

lo cual contradice la Propiedad 1 de $Ruzsa(p, g)$. Por lo tanto $(A+M)\cap(M+M) = \emptyset$.

Notemos ahora que $|A + M| = p^2 - 2p + 1$ pues en $A + M$ todos los elementos son distintos y $|A| = p - 1$, $|M| = p - 1$.

Mostremos en dónde están los $p - 1$ elementos restantes.

Como $0 \in M$ tenemos

$$(M\backslash\{0\}) = (0\hat{+}M) \subseteq (M + M),$$

como

$$(A + M) \cap (M + M) = \emptyset,$$

en particular

$$(A+M)\cap(M\backslash\{0\})=\emptyset,$$

pero sabemos que $|M\backslash\{0\}|=p-2$ entonces

$$|(A+M)\cup(M\backslash\{0\})|=p^2-p-1.$$

Por Propiedad 1 de $Ruzsa(p,g)$ tenemos que $0\notin(A+M)$ y como $0\notin(M\backslash\{0\})$, luego el cero lo obtenemos de manera estricta así

$$(p-2)p+p=p^2-p\equiv 0(\text{mód } p(p-1)),$$

donde $(p-2)p$, $p\in M$ y $(p-2)p\neq p$, pues $p>3$.

Así

$$|(A+M)\cup(M\backslash\{0\})\cup\{0\}|=p(p-1). \tag{2.11}$$

Como $A\cap M=\emptyset$, $|A|=p-1$ y $|M|=p-1$, tenemos

$$|A\cup M|=2(p-1). \tag{2.12}$$

Por lo tanto de (2.11) y (2.12) $A\cup M$ es una base estricta módulo $p(p-1)$, con $2(p-1)$ elementos. □

**Ejemplo 2.3.2** *Sean $p=5$ entonces $\mathbb{Z}_{p^2-p}=\mathbb{Z}_{20}$ y $g=2$ un generador de $\mathbb{Z}_5$, por Ejemplo 2.2.2 tenemos que $A=\{3,14,16,17\}$ es un conjunto de Sidon y por definición $M=\{0,5,10,15\}$. Afirmamos que $A\cup M$ es base estricta para $\mathbb{Z}_{20}$, en efecto*

| $\hat{+}$ | 3 | 14 | 16 | 17 | 0 | 5 | 10 | 15 |
|---|---|---|---|---|---|---|---|---|
| | ***6*** | 17 | 19 | 0 | 3 | 8 | 13 | 18 |
| | | ***8*** | 10 | 11 | 14 | 19 | 4 | 9 |
| | | | ***12*** | 13 | 16 | 1 | 6 | 11 |
| | | | | ***14*** | 17 | 2 | 7 | 12 |
| | | | | | ***0*** | 5 | 10 | 15 |
| | | | | | | ***10*** | 15 | 0 |
| | | | | | | | ***0*** | 5 |
| | | | | | | | | ***10*** |

*Por lo tanto $A\cup M$ es una base estricta para $\mathbb{Z}_{20}$ con 8 elementos.*

# Capítulo 3

# Aplicación y Anexos

## 3.1. Aplicación

Las bases pueden también usarse en una forma interesante para trabajar sobre el problema geométrico de encontrar el mínimo número de puntos en un plano para generar líneas en todas las direcciones posibles. Esto se presenta en el siguiente teorema.

Recordemos que la pendiente $m$ de la recta que pasa por los puntos $P(x_1, y_1)$ y $Q(x_2, y_2)$ $\in F \times F$ se define como

$$m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & \text{si } x_1 \neq x_2, \\ \infty, & \text{si } x_1 = x_2. \end{cases}$$

.

**Teorema 3.1.1** *Sea $F$ un campo de orden finito. Entonces existe un conjunto de $\alpha(F) + 1$ puntos en el plano $F \times F$ sobre $F$ cuyos pares determinan rectas que tienen todas las pendientes posibles incluyendo $\infty$.*

**Prueba**

Sea $S$ una base estricta de cardinalidad mínima del grupo aditivo $(F, +)$. Sea $X$ el conjunto de puntos de la parábola $y = x^2$, es decir

$$X = \{(s, s^2) : s \in S\}.$$

Notemos que la pendiente de la recta que pasa por los puntos $(s, s^2)$ y $(t, t^2)$ es

$$(s^2 - t^2)(s - t)^{-1} = s + t \text{ con } s \neq t,\ s, t \in S.$$

Es decir que el conjunto de pendientes que determina $X$ es $S\hat{+}S = F$, ya que $S$ es base para $F$.

Por otro lado sean $P(x_1, y_1)$, $Q(x_2, y_2) \in F \times F$ luego la pendiente de la recta que une los puntos $P$ y $Q$ es

$$(y_2 - y_1)(x_2 - x_1)^{-1},\ x_2 \neq x_1.$$

Como $F$ es campo entonces $(x_2 - x_1)^{-1}$ y $(y_2 - y_1)(x_2 - x_1)^{-1} \in F$, es decir que todas las pendientes de $F \times F$ están en $F$. Luego $X$ determina toda las posibles pendientes finitas. Para obtener la pendiente infinita, simplemente adjuntamos a $X$, otro punto con la misma $x$-coordenada de algún punto en $X$. Por lo tanto existe un conjunto con $\alpha(F) + 1$ elementos con la condición descrita en el teorema. □

## 3.2. Equivalencias Holomórficas

**Definición 3.2.1** *Una holomorfía de un grupo conmutativo $(G, +)$, es una aplicación de la forma $h(x) := \phi(x) + t$, donde $\phi$ es un automorfismo de $G$ y $t$ algún elemento fijo de $G$.*

**Lema 3.2.1** *Las holomorfías de un grupo conmutativo $(G, +)$, satisfacen las siguientes propiedades.*

*1) Toda holomorfía es una biyección.*

*2) La inversa de una holomorfía es una holomorfía.*

*3) La composición de holomorfías es una holomorfía.*

**Prueba**

1) Veamos que toda holomorfía es una biyección.

- **Inyectividad**
  Supongamos que $h(x_1) = h(x_2)$. Por hipótesis tenemos

  $$h(x_1) = \phi(x_1) + t = \phi(x_2) + t = h(x_2),$$

  y por la existencia del inverso aditivo de $t$ en $G$ se tiene :

  $$\phi(x_1) = \phi(x_2),$$

y como $\phi$ es un automorfismo, se deduce que $x_1 = x_2$. Esto es, $h$ es inyectiva.

- **Sobreyectividad**

  Sea $y \in G$, probemos que existe $x \in G$ tal que $h(x) = y$.

  Como $G$ es grupo, $y - t \in G$ y ademas por ser $\phi$ sobreyectiva, existe $x \in G$ tal que

  $$\phi(x) = y - t,$$

  es decir

  $$h(x) = \phi(x) + t = y,$$

  con lo cual se muestra que $h$ es sobreyectiva

  De lo anterior tenemos que $h$ es biyectiva.

2) Veamos que la inversa de una holomorfía es una holomorfía.

   Sean $h$ una holomorfía definida como $h(x) = \phi(x) + t$ y $g(x) = \phi^{-1}(x) + \phi^{-1}(-t)$, notemos que $g$ así definida es una holomorfía ya que $\phi$ es un automorfismo, ahora afirmamos que $g$ es la inversa de $h$, en efecto

   $$\begin{aligned}(g \circ h)(x) &= g(h(x)) \\ &= g(\phi(x) + t) \\ &= \phi^{-1}(\phi(x) + t) + \phi^{-1}(-t) \\ &= \phi^{-1}(\phi(x)) + \phi^{-1}(t) + \phi^{-1}(-t) \\ &= x + \phi^{-1}(t - t) \\ &= x.\end{aligned}$$

   De igual manera

   $$\begin{aligned}(h \circ g)(x) &= h(g(x)) \\ &= h(\phi^{-1}(x) + \phi^{-1}(-t)) \\ &= \phi(\phi^{-1}(x) + \phi^{-1}(-t))) + t \\ &= \phi(\phi^{-1}(x)) + \phi(\phi^{-1}(-t)) + t \\ &= x.\end{aligned}$$

   Por lo tanto la inversa de una holomorfía es de nuevo una holomorfía.

3) Veamos que la composición de holomorfías es una holomorfía.

Sean $h(x) = \phi(x) + t$ y $g(x) = \lambda(x) + s$ dos holomorfías, entonces

$$\begin{aligned}(h \circ g)(x) &= h(g(x)) \\ &= h(\lambda(x) + s) \\ &= \phi(\lambda(x) + s) + t \\ &= \phi(\lambda(x)) + \phi(s) + t \\ &= \theta(x) + r.\end{aligned}$$

Donde $\theta = (\phi \circ \lambda)$ es un automorfismo, ya que $\phi$ y $\lambda$ son automorfismos y $r = \phi(s)+t$ es un elemento de $G$. Por lo tanto $(h \circ g)$ es una holomorfía. □

**Lema 3.2.2** *Sea $g \in G$ un elemento fijo. Si $A$ es base para $G$ entonces*

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

*es base para $G$.*

**Prueba**

Supongamos que $g \in G$ es un elemento fijo y $A$ una base para $G$ entonces probemos que todo elemento de $G$ se puede escribir como suma de dos elementos de $A + g$.

Sea $x \in G$, entonces como $G$ es grupo

$$x - (g + g) \in G,$$

luego como $A$ es base para $G$,

$$x - (g + g) = a + a', \text{ donde } a, a' \in A,$$

ahora

$$x = a + a' + (g + g),$$

entonces

$$x = (a + g) + (a' + g).$$

Por lo tanto $A + g$ es base para $G$. □

**Teorema 3.2.1** *Toda holomorfía transforma bases (estrictas) en bases (estrictas).*

**Prueba**

Sean $h(x) = \phi(x) + t$ una holomorfía y $A$ una base para $G$. Probemos que $h(A)$ es base para $G$.

Primero probemos que $\phi(A)$ es base para $G$.

Sea $g' \in G$, entonces como $\phi$ es sobreyectiva existe $g \in G$ tal que, $\phi(g) = g'$. Como $g \in G$ y $A$ es base para $G$ entonces $g = a + b$, donde $a, b \in A$, luego

$$\phi(g) = \phi(a + b) = g',$$

en consecuencia como $\phi$ es homomorfismo,

$$\phi(a) + \phi(b) = g', \text{ con } \phi(a),\ \phi(b) \in \phi(A),$$

esto es $\phi(A)$ es una base para $G$.

Ahora, por Lema 3.2.2, $\phi(A) + t$ es base para $G$, y por definición de $h$ tenemos que $h(A)$ es base para $G$. □

**Definición 3.2.2** *Dos bases son equivalentes si existe una holomorfía que transforma una base en la otra.*

Sea $T$ el conjunto de todas las bases para $G$ y consideremos los conjuntos $A$, $B \in T$. Definimos la relación $\sim$ en el conjunto $T$ mediante $A \sim B$ si existe una holomorfía $h$ tal que $h(A) = B$.

**Proposición 3.2.1** *La relación $\sim$ definida anteriormente es de equivalencia.*

**Prueba**

1) **Reflexiva**

   Sea $A$ una base para $G$, tomando $h(x) = x$, que es una holomorfía, se tiene que $h(A) = A$. Luego $\sim$ es reflexiva.

2) **Simétrica**

   Sean $A, B \in T$ y supongamos que $A \sim B$, luego existe una holomorfía $h(x) = \phi(x)+t$ tal que $h(A) = B$, probemos que $B \sim A$.

   Por la parte dos del Lema 3.2.1, existe la holomorfía $h^{-1}$, tal que

   $$\begin{aligned} h^{-1}(B) &= h^{-1}(h(A)) \\ &= A. \end{aligned}$$

   Esto es $h^{-1}(B) = A$. Luego $B \sim A$, es decir $\sim$ es simétrica.

3) **Transitiva**

Supongamos que $A \sim B$ y $B \sim C$, probemos que $A \sim C$.

Como $A \sim B$ y $B \sim C$, luego existen $h$ y $h'$ holomorfías tales que $h(A) = B$ y $h'(B) = C$, por parte tres del Lema 3.2.1, $h^* = (h' \circ h)$ es una holomorfía tal que $h'(h(A)) = C$, esto es existe $h^*$ tal que $h^*(A) = C$, de ahí que $A \sim C$, es decir $\sim$ es transitiva.

Por lo tanto, de 1), 2) y 3) tenemos que $\sim$ es una relación de equivalencia. □

**Lema 3.2.3** *$\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ es un automorfismo, si y sólo si $\varphi(x) = ax$ para algún $a \in \mathbb{Z}_n$ con $mcd(a, n) = 1$.*

**Prueba**

($\Rightarrow$) Veamos que todo automorfismo $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$, es de la forma $\varphi(x) = ax$.

Como $\varphi$ es un automorfismo, entonces $\varphi(mx) = m\varphi(x)$, para $m \in \mathbb{Z}^+ \cup \{0\}$ . Ahora observemos lo siguiente

$$\varphi(x) = \varphi(1x),$$

como $x \in \{0, 1, 2, ..., n-1\}$, en particular $x \in \mathbb{Z}^+ \cup \{0\}$

$$\varphi(x) = x\varphi(1).$$

Sea $\varphi(1) = a$, por lo tanto

$$\varphi(x) = ax.$$

Por otro lado como $\varphi$ es un automorfismo en particular es inyectivo, de ahí que

$$Ker(\varphi) = \{0\},$$

en consecuencia

$$ax \equiv 0(\text{mód } n), \tag{3.1}$$

tiene única solución, la cual es $x = 0$.

Sabemos que $ax \equiv b(\text{mód } n)$ tiene $d$ soluciones incongruentes si y solo si $d|b$, donde $d = mcd(a, n)$.

Como la ecuación (3.1) tiene única solución entonces $d = 1$ es decir $mcd(a, n) = 1$.

($\Leftarrow$) probemos que $\varphi$ es automorfismo

1) Veamos que $\varphi$ es un homomorfismo.

   Sean $x, y \in \mathbb{Z}_n$

$$\begin{aligned}\varphi(x+y) &= a(x+y)\\ &= ax+ay\\ &= \varphi(x)+\varphi(y).\end{aligned}$$

2) Veamos que $\varphi$ es biyectiva.

- **Inyectiva**

$$\begin{aligned}Ker\varphi &= \{x \in \mathbb{Z}_n : \varphi(x) \equiv 0(\text{mód } n)\}\\ &= \{x \in \mathbb{Z}_n : ax \equiv 0(\text{mód } n)\}\\ &= \{x \in \mathbb{Z}_n : a^{-1}ax \equiv a^{-1}0(\text{mód } n)\}\\ &= \{x \in \mathbb{Z}_n : x \equiv 0(\text{mód } n)\},\end{aligned}$$

  luego

$$Ker\varphi = \{0\}.$$

  Por lo tanto $\varphi$ es inyectiva.

- **Sobreyectiva**

  Sea $y \in \mathbb{Z}_n$, probemos que existe $x \in \mathbb{Z}_n$ tal que $\varphi(x) = y$.

  Tomando $x = a^{-1}y$, obtenemos

$$\begin{aligned}\varphi(x) &= \varphi(a^{-1}y)\\ &= a(a^{-1}y)\\ &= y.\end{aligned}$$

  Así $\varphi$ es sobreyectiva.

  De 1) y 2) tenemos que $\varphi$ es un automorfismo. □

Ahora mostremos cuándo podemos asumir que una base contiene al 0 y 1. Note que cualquier conjunto no vacío $A$ en cualquier grupo abeliano $G$ es equivalente vía traslación a un conjunto que contiene al 0, así 0 no es problema. Como los automorfismos en $\mathbb{Z}_n$ son de la forma $\varphi(x) = ax$ donde $a$ y $n$ son primos relativos, las holomorfías en $\mathbb{Z}_n$ vienen dadas como $h(x) = ax + t$.

**Teorema 3.2.2** *Para que $A$ en $\mathbb{Z}_n$ sea equivalente a un conjunto que contiene al 0 y 1, es necesario y suficiente que $A$ contenga dos elementos tal que su diferencia sea prima relativa con $n$.*

**Prueba**

($\Rightarrow$) Supongamos que $h : x \longmapsto ax + t$ transforma $A$ en un conjunto que contiene al 0 y 1 esto es , $au + t = 0$ y $av + t = 1$, donde $u$, $v \in A$. Entonces

$$\begin{aligned} a(v-u) &= (av+t) - (au+t) \\ &= 1 - 0 \\ &= 1, \end{aligned}$$

así $v - u$ es invertible en $\mathbb{Z}_n$. Luego $v - u$ es primo relativo con $n$. (En $\mathbb{Z}_n$ los elementos invertibles son los primos relativos con $n$).

($\Leftarrow$) supongamos que $v - u$ es primo relativo con $n$. Así sea $a$ el inverso de $v - u$ en $\mathbb{Z}_n$. Tomemos $t = -au$ y sea $h$ la holomorfía $h(x) = ax + t$. Entonces $h(u) = au + t = au - au = 0$ y $h(v) = av + t = av - au = a(v - u) = 1$. $\square$

El siguiente resultado se presenta en [2] del cual no se tiene la prueba.

**Observación 3.2.1** *Toda base de $\mathbb{Z}_n$ para $n < 2310$ es equivalente holomórficamente a uno que contiene al a 0 y 1.*

## 3.3. Progresiones Aritméticas en Bases

Esta sección es importante debido a que en una base para $\mathbb{Z}_n$ esta contenida una progresión aritmética, a saber 0 y 1 para $n < 2310$.

Una progresión de longitud $k$ con diferencia $d$ en un grupo conmutativo $(G, +)$ es una secuencia $x_1, x_2, ..., x_k$ tal que $x_{i+1} - x_i = d$ para todo $i$. Los dos resultados siguientes discuten invariantes de progresiones aritméticas bajo la acción de holomorfías.

**Definición 3.3.1** *Sea $G$ un grupo cíclico, se dice que los elementos $x_1, x_2 \in G$, están en la misma órbita de $G$ bajo la acción del grupo de automorfismos de $G$, notado $Aut(G)$, si existe $\phi \in Aut(G)$ tal que $\phi(x_1) = (x_2)$.*

**Teorema 3.3.1** *Una holomorfía envía una progresión aritmética de longitud $k$ con diferencia $d$ en una progresión aritmética de longitud $k$ con diferencia $d^*$, donde $d$ y $d^*$ están en la misma órbita de $G$ bajo la acción del grupo de automorfismos $Aut(G)$.*

**Prueba**

Supongamos que $x_1, x_2, ..., x_k$ es una progresión aritmética de longitud $k$, con diferencia $d$ y $y_i = \phi(x_i) + t$ donde $\phi$ es un automorfismo de $G$, con $t$ un término de traslación constante. Entonces

$$\begin{aligned} y_{i+1} - y_i &= (\phi(x_{i+1}) + t) - (\phi(x_i) + t) \\ &= \phi(x_{i+1}) - \phi(x_i) \\ &= \phi(d). \end{aligned}$$

Luego $d^* = \phi(d)$ es la diferencia constante para los $y_i$. Es decir que $d$ y $d^*$ están en la misma órbita de $G$ bajo la acción de $Aut(G)$. □

**Teorema 3.3.2** *Si $G$ es un grupo cíclico, entonces dos elementos $d$ y $d^*$ están en la misma órbita de $G$ bajo la acción de $Aut(G)$ si, y solo si $d$ y $d^*$ tienen el mismo orden.*

**Prueba**

($\Rightarrow$) Supongamos que $d$ y $d^*$ están en la misma órbita de $G$ bajo la acción de $Aut(G)$, esto es existe $\phi \in Aut(G)$ tal que $\phi(d) = d^*$. Siendo $d$ de orden $m$, probemos que $\phi(d)$ tiene orden $m$. Como $md = e$ y $G$ es aditivo entonces

$$\begin{aligned} e &= \phi(e) \\ &= \phi(md) \\ &= m\phi(d) \\ &= md^*. \end{aligned}$$

Resta probar que $m$ es el menor entero positivo que cumple que $md^* = e$.

Supongamos que existe $t \in \mathbb{Z}^+$ con $t \neq m$ tal que $td^* = e$, entonces

$$\begin{aligned} e &= td^* \\ &= t\phi(d) \\ &= \phi(td), \end{aligned}$$

como $e = \phi(td)$, aplicando $\phi^{-1}$ en ambos lados de la igualdad tenemos

$$e = td,$$

Pero sabemos que el orden de $d$ es $m$ de ahí que $m < t$. Esto es, $m$ es el menor entero tal que $md^* = e$.

($\Leftarrow$) Supongamos que $d$ y $d^*$ tienen orden $m$ y probemos que existe un automorfismo $\phi$ tal que $\phi(d) = d^*$. Sea $G = \mathbb{Z}_n$, donde $n = qm$. El subgrupo $\langle q \rangle$ generado por $q$ es el único subgrupo de $\mathbb{Z}_n$ de orden $m$. Note que los generadores de $\langle q \rangle$ son precisamente los elementos de orden $m$ en $\mathbb{Z}_n$, así todo generador de $\langle q \rangle$ tienen la forma $kq$, $k \in \mathbb{Z}$ donde $mcd(k, m) = 1$. Es decir que existen $k_1$, $k_2 \in \mathbb{Z}$ tales que $d = k_1 q$ y $d^* = k_2 q$.

Luego para probar el resultado necesitamos $\gamma \in Aut(\mathbb{Z}_n)$, tal que $\gamma(q) = kq$, pero sabemos que los automorfismos en $\mathbb{Z}_n$ son de la forma $\gamma(x) = ax$, donde $mcd(a, n) = 1$, es decir estamos buscando un invertible $a$ en $\mathbb{Z}_n$ tal que $aq \equiv kq(\text{mód } n)$. Sea $q = rs$, con $s = mcd(q, m)$ entonces $mcd(r, m) = 1$.Ahora como $r$ y $m$ son primos relativos entonces por el teorema chino de los restos, las congruencias

$$x \equiv k(\text{mód } m) \text{ y } x \equiv 1(\text{mód } r),$$

tienen una solución simultanea, digamos $a$. Afirmamos que $mcd(a, n) = 1$. En efecto,

$n = qm = rsm$, así cualquier primo $p$ que divida a $n$ debe dividir uno de los factores, ya sea $r$, $s$, ó $m$.

1) $p|r$ no es posible, ya que si esto fuera cierto tendríamos que, $a \equiv 1(\text{mód } r)$ implicaría que $a \equiv 1(\text{mód } p)$ y como $p|a$, seria una contradicción puesto que no puede ocurrir simultáneamente que $p|a$ y $p|(a-1)$.

2) $p|s$ no es posible, ya que si esto fuera cierto y como, $s = mcd(q, m)$ implicaría que $p|m$, esto es $a \equiv k(\text{mód } p)$, por otro lado tenemos que $p|a$, por lo tanto $p|k$, lo cual es una contradicción pues si $p|m$ y $p|k$ no se tendría que $mcd(k, m) = 1$.

3) $p|m$ no es posible, ya que si esto fuera cierto y como $a \equiv k(\text{mód } m)$ se tendría que $a \equiv k(\text{mód } p)$, y como por hipótesis $p|a$, tenemos que $p|k$, lo cual es una contradicción pues si $p|m$ y $p|k$ no se tendría que $mcd(k, m) = 1$.

De 1), 2) y 3) tenemos que $mcd(a, n) = 1$, luego $a$ es invertible en $\mathbb{Z}_n$ y así $x \mapsto ax$ es un automorfismo de $\mathbb{Z}_n$. Como $a \equiv k(\text{mód } m)$ tenemos que $a = k + tm$ para algún $t \in \mathbb{Z}$. Aplicando el automorfismo a $q$, tenemos

$$aq = (k + tm)q = kq + tmq = kq + tn = kq(\text{mód } n),$$

como se desea. Lo que se ha probado es que existen automorfismos que me envía a $q$ en $d$ y a $q$ en $d^*$. Luego existe un automorfismo $\phi$ tal que $\phi(d) = d^*$, por lo tanto $d$ y $d^*$ están en la misma orbita. $\square$

El Teorema 3.3.1 muestra que la longitud de la progresión más larga es una invariante holomórfica, y el Teorema 3.3.2 da una forma fácil de distinguir el tipo de holomorfía de una progresión basada en el orden de su diferencia constante.

## 3.4. Otras Funciones Extremas Relacionadas

$\eta(k)$ :=máx{$|G|$: $G$ tiene una base con k elementos}.

$\hat{\eta}(k)$ :=máx{$|G|$: $G$ tiene una base estricta con $k$ elementos}.

$\eta_d(k)$ :=máx{$|G|$: $G$ tiene una base diferencia con $k$ elementos}.

$\zeta(k)$ :=mín{$|G|$: *$G$ tiene un Sidon con $k$ elementos*}.

$\hat{\zeta}(k)$ :=mín{$|G|$: *$G$ tiene un Sidon estricto con $k$ elementos*}.

$\zeta_d(k)$ :=mín{$|G|$: *$G$ tiene un Sidon diferencia con $k$ elementos*}.

En el caso en que $G = \mathbb{Z}_n$, notaremos $\eta(k) = \eta'(k)$, $\hat{\eta}(k) = \hat{\eta}'(k)$, $\eta_d(k) = \eta'_d(k)$, $\zeta(k) = \zeta'(k)$, $\hat{\zeta}(k) = \hat{\zeta}'(k)$ y $\zeta_d(k) = \zeta'_d(k)$.

Las definiciones anteriores nos llevan a plantear los siguientes resultados. Primero presentaremos un corolario del Teorema 2.1.1.

**Corolario 3.4.1** *Por definición, $\zeta_d(k) = \zeta(k)$.*

**Teorema 3.4.1** *Las funciones $\eta(k)$, $\hat{\eta}(k)$, $\eta_d(k)$,$\zeta(k)$, $\hat{\zeta}(k)$, $\zeta_d(k)$ satisfacen las siguientes relaciones*

*1)* $\eta'_d(k) \leq \eta_d(k) \leq k(k-1)+1 \leq \zeta_d(k) \leq \zeta'_d(k)$

*2)* $\eta'(k) \leq \eta(k) \leq \binom{k+1}{2} \leq \zeta(k) \leq \zeta'(k)$

*3)* $\hat{\eta}'(k) \leq \hat{\eta}(k) \leq \binom{k}{2} \leq \hat{\zeta}(k) \leq \hat{\zeta}'(k)$

**Prueba**

1) a. Primero miremos que $\eta_d(k) \leq k(k-1)+1$.

Supongamos que $\eta_d(k) = m = |G|$ entonces $G$ tiene una base diferencia $A$ con $k$ elementos.

Como A es base diferencia entonces $A-A = G$ y $A-A$ tiene a lo sumo $2\binom{k}{2}+1$ elementos de ahí que

$$m = |G| = |A-A| \leq 2\binom{k}{2}+1,$$

por lo tanto

$$\eta_d(k) \leq k(k-1)+1.$$

b. Probemos que $k(k-1)+1 \leq \zeta_d(k)$.

Supongamos que $\zeta_d(k) = l = |G|$, entonces $G$ tiene un Sidon diferencia $A$ con $k$ elementos.

Como $A$ es Sidon diferencia entonces

$$|(A-A)\backslash\{0\}| = |A|(|A|-1) \leq l,$$

es decir

$$|A-A| = |A|(|A|-1)+1 \leq l,$$

como $|A| = k$

$$k(k-1)+1 \leq l = \zeta_d(k).$$

c. Probemos que $\zeta_d(k) \leq \zeta'_d(k)$.

Sean $C$ el conjunto de los cardinales de todos los grupos abelianos que admiten un Sidon diferencia con $k$ elementos y $C'$ el conjunto de los cardinales de todos los $\mathbb{Z}_n$ que admiten un Sidon diferencia con $k$ elementos, de ahí que $C' \subseteq C$ por lo tanto mín$C \leq$ mín $C'$, es decir $\zeta_d(k) \leq \zeta'_d(k)$.

d. Probemos que $\eta'_d(k) \leq \eta_d(k)$

Sean $B$ el conjunto de los cardinales de todos los grupos abelianos que admiten una base diferencia con $k$ elementos y $B'$ el conjunto de los cardinales de todos los $\mathbb{Z}_n$ que admiten una base diferencia con $k$ elementos, de ahí que $B' \subseteq B$, por lo tanto máx$B' \leq$máx $B$ es decir $\eta'_d(k) \leq \eta_d(k)$.

Con este mismo argumento se demuestra 2) y 3). □

## 3.5. Problemas Abiertos

**Problemas Abiertos**

1) ¿Cuántos elementos le faltan a un conjunto de Sidon para ser base?

2) ¿Cuál es el máximo conjunto de Sidon contenido en una base?

3) ¿Cuál es la progresión más larga contenida en una base?

4) ¿Cuántas bases equivalentes holomórficamente hay?

## 3.6. Tablas

**Tabla 1: valores de** $\eta_d(k)$, $\eta'_d(k)$, $\eta(k)$, $\eta'(k)$, $\hat{\eta}(k)$, $\hat{\eta}'(k)$.

| **k** | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\eta_d(k)$ | 3 | 7 | 13 | 21 | 31 | 39 | 57 | 73 | 91 | 95 | 133 | | |
| $\eta'_d(k)$ | 3 | 7 | 13 | 21 | 31 | 39 | 57 | 73 | 91 | 95 | 133 | | |
| $\eta(k)$ | 3 | 5 | 9 | 13 | 19 | 21 | 30 | 36 | 43 | 51 | 64 | 72 | |
| $\eta'(k)$ | 3 | 5 | 9 | 13 | 19 | 21 | 30 | 35 | 43 | 51 | 63 | 67 | |
| $\hat{\eta}(k)$ | | 3 | 6 | 9 | 13 | 20 | 25 | 30 | 36 | 42 | 56 | 64 | 72 |
| $\hat{\eta}'(k)$ | | 3 | 6 | 9 | 13 | 17 | 24 | 30 | 36 | 42 | 56 | 61 | 72 |

**Tabla 2: Bases diferencia que corresponden a los valores de $\eta_d(k)$ y $\eta'_d(k)$.**

| k | G | una base diferencia mínima |
|---|---|---|
| 2 | $\mathbb{Z}_3$ | $\{0,1\}$ |
| 3 | $\mathbb{Z}_7$ | $\{0,1,3\}$ |
| 4 | $\mathbb{Z}_{13}$ | $\{0,1,3,9\}$ |
| 5 | $\mathbb{Z}_{21}$ | $\{0,1,6,8,18\}$ |
| 6 | $\mathbb{Z}_{31}$ | $\{0,1,3,8,12,18\}$ |
| 7 | $\mathbb{Z}_{39}$ | $\{0,1,16,20,22,27,30\}$ |
| 8 | $\mathbb{Z}_{57}$ | $\{0,1,9,11,14,35,39,51\}$ |
| 9 | $\mathbb{Z}_{73}$ | $\{0,1,3,7,15,31,36,54,63\}$ |
| 10 | $\mathbb{Z}_{91}$ | $\{0,1,7,16,27,56,60,68,70,73\}$ |
| 11 | $\mathbb{Z}_{95}$ | $\{0,1,5,8,18,20,29,31,45,61,67\}$ |
| 12 | $\mathbb{Z}_{133}$ | $\{0,1,32,42,44,48,51,59,72,77,97,111\}$ |

**Tabla 3: Bases aditivas que corresponden a los valores $\eta(k)$ o $\eta'(k)$.**

| k | \|G\| | G | un base aditiva mínima |
|---|---|---|---|
| 2 | 3 | $\mathbb{Z}_3$ | $\{0,1\}$ |
| 3 | 5 | $\mathbb{Z}_5$ | $\{0,1,2\}$ |
| 4 | 9 | $\mathbb{Z}_9$ | $\{0,1,3,4\}$ |
| 5 | 13 | $\mathbb{Z}_{13}$ | $\{0,1,2,6,9\}$ |
| 6 | 19 | $\mathbb{Z}_{19}$ | $\{0,1,3,12,14,15\}$ |
| 7 | 21 | $\mathbb{Z}_{21}$ | $\{0,1,3,7,11,15,19\}$ |
| 8 | 30 | $\mathbb{Z}_{30}$ | $\{0,1,3,9,11,12,16,26\}$ |
| 9 | 35 | $\mathbb{Z}_{35}$ | $\{0,1,3,13,15,17,27,29,30\}$ |
| 9 | 36 | $\mathbb{Z}_4 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(1,1,0),$ $(1,2,0),(3,0,2),(3,1,0),(3,2,0)\}$ |
| 10 | 43 | $\mathbb{Z}_{43}$ | $\{0,1,2,3,10,15,21,25,31,36\}$ |
| 11 | 51 | $\mathbb{Z}_{51}$ | $\{0,1,3,7,10,15,18,22,24,25,38\}$ |
| 12 | 63 | $\mathbb{Z}_{63}$ | $\{0,1,3,8,12,18,22,27,29,30,43,50\}$ |
| 12 | 64 | $\mathbb{Z}_8^2$ | $\{(0,0),(0,1),(0,4),(1,0),(1,2),(2,1),(2,2),$ $(2,6),(4,5),(5,0),(5,2),(6,5)\}$ |
| 13 | 67 | $\mathbb{Z}_{67}$ | $\{0,1,2,3,4,,5,6,16,24,33,40,49,57\}$ |
| 13 | 72 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,2,1),(0,2,4),$ $(0,2,7),(0,3,1),(1,0,3),(1,0,8),(1,1,1),$ $(1,2,5),(1,2,6),(1,3,1)\}$ |

**Tabla 4: Bases estrictas correspondiente a los valores $\hat{\eta}(k)$ o $\hat{\eta}'(k)$.**

| **k** | **\|G\|** | **G** | **una base estricta mínima** |
|---|---|---|---|
| 3 | 3 | $\mathbb{Z}_3$ | $\{0,1,2\}$ |
| 4 | 6 | $\mathbb{Z}_6$ | $\{0,1,2,4\}$ |
| 5 | 9 | $\mathbb{Z}_9$ | $\{0,1,3,6\}$ |
| 6 | 13 | $\mathbb{Z}_{13}$ | $\{0,1,2,3,6,10\}$ |
| 7 | 17 | $\mathbb{Z}_{17}$ | $\{0,1,2,3,4,8,13\}$ |
| 7 | 20 | $\mathbb{Z}_2^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,0,3),(0,0,4),$ $(1,0,1),(1,1,1)\}$ |
| 8 | 24 | $\mathbb{Z}_{24}$ | $\{0,1,2,4,8,13,18,22\}$ |
| 8 | 25 | $\mathbb{Z}_5^2$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0),(2,1),(3,2),(4,3)\}$ |
| 9 | 30 | $\mathbb{Z}_{30}$ | $\{0,1,2,6,9,12,16,17,18\}$ |
| 10 | 36 | $\mathbb{Z}_{36}$ | $\{0,1,4,5,7,13,18,23,28,34\}$ |
| 11 | 42 | $\mathbb{Z}_{42}$ | $\{0,1,11,12,18,22,24,27,30,32,36\}$ |
| 12 | 56 | $\mathbb{Z}_{56}$ | $\{0,1,12,15,22,29,32,43,44,48,50,52\}$ |
| 13 | 61 | $\mathbb{Z}_{61}$ | $\{0,1,2,3,4,7,13,21,29,36,44,52,58\}$ |
| 13 | 64 | $\mathbb{Z}_4 \times \mathbb{Z}_{16}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,7),(0,13),$ $(1,0),(1,8),(2,2),(2,10),(3,4),(3,12)\}$ |
| 14 | 72 | $\mathbb{Z}_{72}$ | $\{0,1,2,5,12,30,37,40,41,42,50,56,58,64\}$ |

A continuación presentamos unas tablas que contienen bases y bases estrictas mínimas, para $2 \leq |G| \leq 85$ y $3 \leq |G| \leq 90$ respectivamente, donde $k$ representa el cardinal de la base.

| **k** | **\|G\|** | **G** | **una base mínima** |
|---|---|---|---|
| 2 | 2 | $\mathbb{Z}_2$ | $\{0,1\}$ |
| 2 | 3 | $\mathbb{Z}_3$ | $\{0,1\}$ |
| 3 | 4 | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | $\{(0,0),(0,1),(1,0)\}$ |
| 3 | 4 | $\mathbb{Z}_4$ | $\{0,1,2\}$ |
| 3 | 5 | $\mathbb{Z}_5$ | $\{0,1,2\}$ |
| 4 | 6 | $\mathbb{Z}_2 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2)\}$ |
| 4 | 7 | $\mathbb{Z}_7$ | $\{0,1,2,3\}$ |
| 5 | 8 | $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ | $\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0)\}$ |
| 5 | 8 | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0)\}$ |
| 4 | 8 | $\mathbb{Z}_8$ | $\{0,1,2,5\}$ |
| 4 | 9 | $\mathbb{Z}_3 \times \mathbb{Z}_3$ | $\{(0,0),(0,1),(1,0),(1,1)\}$ |
| 4 | 9 | $\mathbb{Z}_9$ | $\{0,1,3,4\}$ |
| 5 | 10 | $\mathbb{Z}_2 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(1,3)\}$ |
| 5 | 11 | $\mathbb{Z}_{11}$ | $\{0,1,2,3,7\}$ |
| 5 | 12 | $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,2),(1,0,1),(1,1,1)\}$ |
| 5 | 12 | $\mathbb{Z}_4 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,2),(2,1),(3,1)\}$ |
| 5 | 13 | $\mathbb{Z}_{13}$ | $\{0,1,2,6,9\}$ |
| 6 | 14 | $\mathbb{Z}_2 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(1,4)\}$ |
| 6 | 15 | $\mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(1,0),(1,2)\}$ |
| 6 | 16 | $\mathbb{Z}_{16}$ | $\{o,1,2,4,9,14\}$ |
| 6 | 16 | $\mathbb{Z}_2^4$ | $\{(0,0,0,0),(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0),(1,1,1,1)\}$ |
| 6 | 16 | $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,1,1),(1,0,1),(1,1,3)\}$ |
| 7 | 16 | $\mathbb{Z}_2 \times \mathbb{Z}_8$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(1,0),(1,3)\}$ |
| 6 | 16 | $\mathbb{Z}_4 \times \mathbb{Z}_4$ | $\{(0,0),(0,1),(0,2),(1,0),(2,1),(3,2)\}$ |
| 6 | 17 | $\mathbb{Z}_{17}$ | $\{0,1,2,3,8,12\}$ |
| 7 | 18 | $\mathbb{Z}_2 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,1,0),(1,1,1),(1,2,0)\}$ |
| 7 | 18 | $\mathbb{Z}_2 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,5)\}$ |
| 6 | 19 | $\mathbb{Z}_{19}$ | $\{0,1,3,12,14,15\}$ |
| 7 | 20 | $\mathbb{Z}_2^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(1,0,1),(1,1,3),(1,1,4)\}$ |
| 7 | 20 | $\mathbb{Z}_4 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(1,3),(3,0),(3,3)\}$ |
| 7 | 21 | $\mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,3),(1,0),(1,5),(2,4)\}$ |
| 8 | 22 | $\mathbb{Z}_2 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,6)\}$ |
| 8 | 23 | $\mathbb{Z}_{23}$ | $\{0,1,2,3,4,5,11,16\}$ |
| 8 | 24 | $\mathbb{Z}_2^3 \times \mathbb{Z}_3$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),(0,0,1,0),(0,1,0,2),(1,0,0,2),(1,1,1,2)\}$ |
| 8 | 24 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,1,0),(0,3,2),(1,0,0),(1,2,0)\}$ |
| 8 | 24 | $\mathbb{Z}_8 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2),(1,0),(3,0),(5,1),(7,1)\}$ |
| 8 | 25 | $\mathbb{Z}_{25}$ | $\{0,1,2,3,4,5,12,18\}$ |
| 8 | 25 | $\mathbb{Z}_5^2$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0),(2,1),(3,2),(4,3)\}$ |
| 8 | 26 | $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,8),(1,6),(1,10)\}$ |
| 8 | 27 | $\mathbb{Z}_{27}$ | $\{0,1,2,3,8,12,18,22\}$ |
| 8 | 27 | $\mathbb{Z}_3^3$ | $\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$ |
| 8 | 27 | $\mathbb{Z}_3 \times \mathbb{Z}_9$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0),(1,3),(2,4),(2,8)\}$ |

| | | | |
|---|---|---|---|
| 9 | 28 | $\mathbb{Z}_2^2 \times \mathbb{Z}_7$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,6),(1,0,1),(1,1,4),(1,1,5)\}$ |
| 9 | 28 | $\mathbb{Z}_4 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,0),(2,2),(3,4)\}$ |
| 8 | 29 | $\mathbb{Z}_{29}$ | $\{0,1,2,6,7,8,17,20\}$ |
| 8 | 30 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0,0),(1,1,1),(0,0,2),(0,1,1),(0,2,1),(1,0,3),(1,0,4),(1,2,1)\}$ |
| 9 | 31 | $\mathbb{Z}_{31}$ | $\{0,1,2,3,4,5,12,18,24\}$ |
| 9 | 32 | $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,10),(1,2),(1,7),(1,13)\}$ |
| 10 | 32 | $\mathbb{Z}_2^5$ | $\{(0,0,0,0,0),(0,0,0,0,1),(0,0,0,1,0),(0,0,0,1,1),(0,0,1,0,0),(0,0,1,0,1),(0,0,1,1,0),(0,1,0,0,0),(1,0,0,0,0),(1,1,1,1,1)\}$ |
| 10 | 32 | $\mathbb{Z}_2^3 \times \mathbb{Z}_4$ | $\{(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,0,3),(0,0,1,0),(0,0,1,1),(0,0,1,2),(0,1,0,1),(1,0,0,1),(1,1,1,3)\}$ |
| 10 | 32 | $\mathbb{Z}_2^2 \times \mathbb{Z}_8$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,1,0),(0,1,1),(0,1,2),(0,3,1),(1,0,0),(1,2,2)\}$ |
| 9 | 32 | $\mathbb{Z}_{32}$ | $\{0,1,2,3,4,,10,15,21,26\}$ |
| 10 | 32 | $\mathbb{Z}_4 \times \mathbb{Z}_8$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(1,1),(2,3),(3,5)\}$ |
| 9 | 33 | $\mathbb{Z}_3 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,7),(2,3),(2,8)\}$ |
| 9 | 34 | $\mathbb{Z}_2 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,3),(0,12),(0,15),(1,7),(1,8),(1,14)\}$ |
| 9 | 35 | $\mathbb{Z}_5 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(2,3),(2,6),(3,3),(3,6),(4,1)\}$ |
| 10 | 36 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0),(0,1,0,1),(0,0,0,1),(0,0,0,2),(0,0,1,0),(0,0,2,0),(0,1,0,2),(1,0,0,0),(1,1,1,0),(1,1,2,0)\}$ |
| 10 | 36 | $\mathbb{Z}_2^2 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,6),(0,1,2),(1,0,0),(1,0,3),(1,1,6)\}$ |
| 9 | 36 | $\mathbb{Z}_4 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(1,1,0),(1,2,0),(3,0,2),(3,1,0),(3,2,0)\}$ |
| 10 | 36 | $\mathbb{Z}_4 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,5),(2,3),(3,0),(3,4)\}$ |
| 10 | 37 | $\mathbb{Z}_{37}$ | $\{0,1,2,3,4,5,11,18,24,30\}$ |
| 10 | 38 | $\mathbb{Z}_2 \times \mathbb{Z}_{19}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,11),(0,18),(1,8),(1,14)\}$ |
| 10 | 39 | $\mathbb{Z}_3 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,8),(2,4),(2,10)\}$ |
| 10 | 40 | $\mathbb{Z}_2^3 \times \mathbb{Z}_5$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,0,2),(0,1,0,1),(0,1,1,1),(1,0,0,1),(1,0,1,1),(1,1,0,1),(1,1,1,3),(1,1,1,4)\}$ |
| 10 | 40 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times Z_5$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,2,1),(0,3,1),(1,0,1),(1,1,1),(1,2,3),(1,2,4),(1,3,1)\}$ |
| 10 | 40 | $\mathbb{Z}_5 \times \mathbb{Z}_8$ | $\{(0,0),(1,1),(0,1),(0,2),(1,3),(5,0),(5,3),(6,0),(6,1),(6,2)\}$ |
| 10 | 41 | $\mathbb{Z}_{41}$ | $\{0,1,2,3,7,16,18,26,28,37\}$ |
| 10 | 42 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times Z_7$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,4),(0,0,6),(0,1,2),(0,1,3),(0,1,5),(1,0,1),(1,2,1)\}$ |
| 10 | 43 | $\mathbb{Z}_{43}$ | $\{0,1,2,3,10,15,21,25,31,36\}$ |
| 11 | 44 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{11}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,1,8),(1,0,2),(1,0,8),(1,1,4),(1,1,10)\}$ |
| 11 | 44 | $\mathbb{Z}_4 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,7),(1,7),(3,2),(3,7),(3,9)\}$ |
| 11 | 45 | $\mathbb{Z}_3^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,1,0),(0,1,2),(0,2,0),(1,0,1),(1,0,4),(2,1,1),(2,1,4)\}$ |
| 11 | 45 | $\mathbb{Z}_9 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(1,0),(1,2),(2,0),(4,0),(4,3),(6,2),(6,4)\}$ |
| 11 | 46 | $\mathbb{Z}_2 \times \mathbb{Z}_{23}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,10),(0,13),(0,16),(1,2),(1,6),(1,20)\}$ |

| | | | |
|---|---|---|---|
| 11 | 47 | $\mathbb{Z}_{47}$ | $\{0,1,2,3,4,5,13,19,26,33,39\}$ |
| 11 | 48 | $\mathbb{Z}_{16}\times\mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2),(3,0),(5,0),(7,0),(9,1),(11,1),(13,1),(15,0)\}$ |
| 12 | 48 | $\mathbb{Z}_2^4\times\mathbb{Z}_3$ | $\{(0,0,0,0,0),(0,0,0,1,1),(0,0,0,0,1),(0,0,0,0,2),(0,0,0,1,0),$ $(0,0,1,0,0),(0,1,0,0,0),(0,1,1,0,2),(1,0,0,0,0),(1,0,1,0,2),$ $(1,1,0,1,2),(1,1,1,0,0)\}$ |
| 11 | 48 | $\mathbb{Z}_2^2\times\mathbb{Z}_4\times\mathbb{Z}_3$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),(0,0,3,0),(0,1,0,2),$ $(0,1,2,2),(1,0,0,2),(1,0,2,2),(1,1,1,2),(1,1,3,2)\}$ |
| 11 | 48 | $\mathbb{Z}_2\times\mathbb{Z}_8\times\mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,3,0),(0,5,0),(0,7,1),(1,0,0),$ $(1,2,1),(1,4,0),(1,6,1)\}$ |
| 11 | 48 | $\mathbb{Z}_4^2\times\mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,3,0),(1,0,2),(1,2,2),(2,1,2),$ $(2,3,2),(3,0,2),(3,2,2)\}$ |
| 11 | 49 | $\mathbb{Z}_{49}$ | $\{0,1,2,3,4,11,17,24,29,36,42\}$ |
| 11 | 49 | $\mathbb{Z}_7^2$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(1,0),(2,1),(3,1),(4,3),(5,3),(6,4)\}$ |
| 12 | 50 | $\mathbb{Z}_2\times\mathbb{Z}_{25}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,11),(0,18),(1,9),$ $(1,15),(1,21)\}$ |
| 12 | 50 | $\mathbb{Z}_2\times\mathbb{Z}_5^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,0,3),(0,1,0),(0,1,2),(0,4,0),$ $(0,4,3),(1,0,4),(1,2,2),(1,3,3)\}$ |
| 11 | 51 | $\mathbb{Z}_3\times\mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,3),(0,7),(0,15),(1,5),(1,7),(1,8),(1,10),(2,4)\}$ |
| 12 | 52 | $\mathbb{Z}_2^2\times\mathbb{Z}_{13}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),(0,1,9),$ $(1,0,1),(1,0,9),(1,1,6),(1,1,12)\}$ |
| 12 | 52 | $\mathbb{Z}_4\times\mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,6),(2,3),(2,9),(3,3),$ $(3,10)\}$ |
| 12 | 53 | $\mathbb{Z}_{53}$ | $\{0,1,2,3,4,5,7,13,22,29,36,45\}$ |
| 12 | 54 | $Z_2\times\mathbb{Z}_{27}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,12),(0,18),(0,26),(1,8),$ $(1,15),(1,22)\}$ |
| 12 | 54 | $Z_2\times\mathbb{Z}_3^3$ | $\{(0,0,0,0),(1,0,0,1),(0,0,0,1),(0,0,0,2),(0,0,1,0),(0,0,1,1),$ $(0,1,0,0),(0,1,0,1),(0,1,2,1),(0,2,1,1),(1,1,1,0),(1,2,2,2)\}$ |
| 12 | 54 | $\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_9$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,0,3),(0,0,6),(0,1,1),(0,1,5),$ $(0,2,1),(0,2,8),(1,1,7),(1,2,4)\}$ |
| 12 | 55 | $\mathbb{Z}_5\times\mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(1,3),(1,7),(2,9),(3,5),(4,0),(4,2),(4,7)\}$ |
| 12 | 56 | $\mathbb{Z}_2^3\times\mathbb{Z}_7$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,2),(0,0,0,3),(0,0,0,5),(0,0,1,4),(0,1,0,6),$ $(0,1,1,6),(1,0,0,6),(1,0,1,6),(1,1,0,6),(1,1,1,6)\}$ |
| 12 | 56 | $\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_7$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,0,3),(0,0,6),(0,2,1),(0,3,1),(1,0,1),$ $(1,1,1),(1,2,4),(1,2,5),(1,3,1)\}$ |
| 12 | 56 | $\mathbb{Z}_8\times\mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(2,5),(3,1),(4,0),(4,3),(5,2),(6,5),(7,2)\}$ |
| 12 | 57 | $\mathbb{Z}_3\times\mathbb{Z}_{19}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,7),(0,15),(1,9),(1,13),(1,18),(2,4),$ $(2,13)\}$ |
| 13 | 58 | $\mathbb{Z}_2\times\mathbb{Z}_{29}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,14),(0,21),(1,7),$ $(1,14),(1,23)\}$ |
| 12 | 59 | $\mathbb{Z}_{12}$ | $\{0,1,2,3,4,5,14,21,29,35,43,50\}$ |
| 13 | 60 | $\mathbb{Z}_2^2\times\mathbb{Z}_3\times\mathbb{Z}_5$ | $\{(0,0,0,0),(0,1,1,1),(0,0,0,1),(0,0,0,2),(0,0,0,3),(0,0,0,4),(0,1,0,0),$ $(0,1,0,2),(0,1,2,1),(1,0,0,3),(1,0,0,4),(1,0,1,1),(1,0,2,1)\}$ |
| 13 | 60 | $\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_5$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(1,0,0),(1,0,2),$ $(1,0,3),(1,2,1),(3,0,3),(3,1,0),(3,2,0)\}$ |

| | | | |
|---|---|---|---|
| 12 | 61 | $\mathbb{Z}_{61}$ | $\{0, 1, 2, 7, 8, 9, 20, 23, 33, 37, 47, 50\}$ |
| 13 | 62 | $\mathbb{Z}_2 \times \mathbb{Z}_{31}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,10), (0,25), (1,3), (1,9), (1,14), (1,21), (1,26)\}$ |
| 12 | 63 | $\mathbb{Z}_3^2 \times \mathbb{Z}_7$ | $\{(0,0,0), (0,1,1), (0,0,2), (0,0,3), (0,1,5), (0,1,6), (1,0,4), (1,1,4), (1,2,4), (2,0,4), (2,1,4), (2,2,4)\}$ |
| 12 | 63 | $\mathbb{Z}_9 \times Z_7$ | $\{(0,0), (1,1), (0,4), (0,6), (2,1), (3,2), (3,3), (3,5), (4,1), (5,1), (7,1), (8,1)\}$ |
| 13 | 64 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{16}$ | $\{(0,0,0), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,0,7), (0,0,13), (0,1,2), (0,1,10), (1,0,2), (1,0,10), (1,1,6), (1,1,14)\}$ |
| 14 | 64 | $\mathbb{Z}_2^6$ | $\{(0,0,0,0,0,0), (0,0,0,0,0,1), (0,0,0,0,1,0), (0,0,0,0,1,1), (0,0,0,1,0,0), (0,0,0,1,0,1), (0,0,0,1,1,0), (0,0,1,0,0,0), (0,1,0,0,0,0), (0,1,1,0,0,0), (1,0,0,0,0,0), (1,0,1,0,0,0), (1,1,0,0,0,0), (1,1,1,1,1,1)\}$ |
| 14 | 64 | $\mathbb{Z}_2^4 \times \mathbb{Z}_4$ | $\{(0,0,0,0,0), (0,0,0,0,1), (0,0,0,0,2), (0,0,0,0,3), (0,0,0,1,0), (0,0,0,1,1), (0,0,0,1,2), (0,0,1,0,0), (0,1,0,0,0), (0,1,1,0,1), (1,0,0,0,0), (1,0,1,0,1), (1,1,0,1,3), (1,1,1,0,0)\}$ |
| 13 | 64 | $\mathbb{Z}_2^3 \times \mathbb{Z}_8$ | $\{(0,0,0,0), (0,0,0,1), (0,0,0,2), (0,0,0,3), (0,0,0,4), (0,0,1,1), (0,0,1,3), (0,1,0,2), (0,1,1,6), (1,0,0,2), (1,0,1,6), (1,1,0,6), (1,1,1,2)\}$ |
| 14 | 64 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4^2$ | $\{(0,0,0,0), (0,0,0,1), (0,0,0,2), (0,0,0,3), (0,0,1,0), (0,0,1,1), (0,0,1,2), (0,0,3,0), (0,1,0,0), (0,1,2,1), (1,0,0,0), (1,0,2,2), (1,1,1,3), (1,1,3,1)\}$ |
| 13 | 64 | $\mathbb{Z}_2 \times \mathbb{Z}_{32}$ | $\{(0,0), (0,1), (0,2), (0,3), (0,4), (0,12), (0,18), (0,24), (1,2), (1,9), (1,14), (1,22), (1,27)\}$ |
| 13 | 64 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$ | $\{(0,0,0), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,1,0), (0,2,1), (0,2,3), (0,3,4), (1,0,2), (1,1,4), (1,2,6), (1,3,0)\}$ |
| 13 | 64 | $\mathbb{Z}_4 \times \mathbb{Z}_{16}$ | $\{(0,0), (0,1), (0,2), (0,3), (0,4), (0,7), (0,13), (1,0), (1,8), (2,2), (2,10), (3,4), (3,12)\}$ |
| 14 | 64 | $\mathbb{Z}_4^3$ | $\{(0,0,0), (0,0,1), (0,0,2), (0,0,3), (0,1,0), (0,1,1), (0,1,2), (0,3,0), (1,0,0), (1,2,0), (2,1,1), (2,3,1), (3,0,2), (3,2,2)\}$ |
| 13 | 64 | $\mathbb{Z}_{64}$ | $\{0, 1, 2, 4, 5, 12, 20, 26, 33, 37, 42, 50, 56\}$ |
| 12 | 64 | $\mathbb{Z}_8^2$ | $\{(0,0), (0,1), (0,4), (1,0), (1,2), (2,1), (2,2), (2,6), (4,5), (5,0), (5,2), (6,5)\}$ |
| 13 | 65 | $\mathbb{Z}_5 \times \mathbb{Z}_{13}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (1,7), (2,4), (2,9), (3,0), (3,8), (4,3), (4,10)\}$ |
| 13 | 66 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ | $\{(0,0,0), (1,1,1), (0,0,1), (0,0,2), (0,0,3), (0,0,10), (0,1,6), (0,2,7), (1,0,3), (1,0,10), (1,1,7), (1,2,1), (1,2,6)\}$ |
| 13 | 67 | $\mathbb{Z}_{67}$ | $\{0, 1, 2, 3, 4, 5, 6, 16, 24, 33, 40, 49, 57\}$ |
| 14 | 68 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{17}$ | $\{(0,0,0), (0,1,1), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,0,5), (0,0,6), (0,0,16), (0,1,11), (1,0,1), (1,0,11), (1,1,7), (1,1,15)\}$ |
| 14 | 68 | $\mathbb{Z}_4 \times \mathbb{Z}_{17}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,7), (1,9), (2,3), (2,13), (3,6), (3,14)\}$ |
| 14 | 69 | $\mathbb{Z}_3 \times \mathbb{Z}_{23}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,14), (1,8), (1,18), (2,4), (2,12), (2,20)\}$ |
| 14 | 70 | $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ | $\{(0,0,0), (1,1,1), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,1,4), (0,2,2), (0,3,2), (0,4,5), (1,0,2), (1,2,5), (1,3,5), (1,4,4)\}$ |
| 14 | 71 | $\mathbb{Z}_{71}$ | $\{(0), (1), (2), (3), (4), (5), (6), (7), (17), (25), (35), (42), (52), (61)\}$ |

| | | | |
|---|---|---|---|
| 13 | 72 | $\mathbb{Z}_2^3 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0,0),(0,0,1,0,1),(0,0,0,0,1),(0,0,0,0,2),(0,1,0,0,1),$ $(0,1,1,1,0),(0,1,1,2,2),(1,0,0,0,1),(1,0,1,1,1),(1,0,1,2,1),$ $(1,1,0,1,2),(1,1,0,2,0),(1,1,1,0,1)\}$ |
| 13 | 72 | $\mathbb{Z}_2^3 \times \mathbb{Z}_9$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,2),(0,0,1,4),(0,0,1,7),(0,1,0,1),(0,1,1,1),$ $(1,0,0,1),(1,0,1,1),(1,1,0,3),(1,1,0,8),(1,1,1,5),(1,1,1,6)\}$ |
| 13 | 72 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0),(0,1,0,1),(0,0,0,1),(0,0,0,2),(0,2,1,0),(0,2,2,2),$ $(0,3,0,1),(1,0,1,1),(1,0,2,1),(1,1,0,1),(1,2,1,2),(1,2,2,0),(1,3,0,1)\}$ |
| 13 | 72 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,2,1),(0,2,4),(0,2,7),(0,3,1),(1,0,3),$ $(1,0,8),(1,1,1),(1,2,5),(1,2,6),(1,3,1)\}$ |
| 14 | 72 | $\mathbb{Z}_8 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(0,2,1),(0,2,2),$ $(2,1,2),(3,0,1),(4,0,1),(5,0,1),(6,2,0),(7,0,1)\}$ |
| 14 | 72 | $\mathbb{Z}_8 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,8),(2,6),(3,1),(4,4),(4,8),$ $(5,2),(6,6),(7,2)\}$ |
| 14 | 73 | $\mathbb{Z}_{73}$ | $\{0,1,2,3,4,5,6,7,17,26,36,44,54,63\}$ |
| 14 | 74 | $\mathbb{Z}_2 \times \mathbb{Z}_{37}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,4),(0,6),(0,15),(0,24),(0,33),(0,35),$ $(1,10),(1,17),(1,22),(1,29)\}$ |
| 14 | 75 | $\mathbb{Z}_3 \times \mathbb{Z}_{25}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,16),(0,20),(1,14),(1,15),(1,16),$ $(1,17),(1,22),(2,19),(2,23)\}$ |
| 14 | 75 | $\mathbb{Z}_3 \times \mathbb{Z}_5^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(0,3,2),$ $(1,3,2),(1,4,4),(2,1,3),(2,3,0),(2,3,4),(2,4,0),(2,4,3)\}$ |
| 15 | 76 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{19}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),(0,0,6),$ $(0,0,17),(0,0,18),(0,1,12),(1,0,2),(1,0,12),(1,1,6),(1,1,16)\}$ |
| 14 | 76 | $\mathbb{Z}_4 \times \mathbb{Z}_{19}$ | $\{(0,0),(1,1),(0,1),(0,3),(0,4),(0,7),(0,16),(1,12),(1,17),(2,0),$ $(2,4),(3,3),(3,6),(3,11)\}$ |
| 14 | 77 | $\mathbb{Z}_7 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,3),(1,6),(1,10),(2,3),(2,7),(3,0),(3,4),(3,9),$ $(4,7),(4,9),(4,10)\}$ |
| 15 | 78 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{13}$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),(0,1,0),$ $(0,1,6),(0,2,5),(1,0,0),(1,0,5),(1,1,7),(1,2,4),(1,2,11)\}$ |
| 14 | 79 | $\mathbb{Z}_{79}$ | $\{0,1,2,3,9,10,11,12,26,30,43,48,61,65\}$ |
| 14 | 80 | $\mathbb{Z}_{16} \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(2,0),(2,3),(4,3),(5,1),(6,4),(8,2),(8,4),$ $(9,1),(10,1),(10,2),(13,1)\}$ |
| 15 | 80 | $\mathbb{Z}_2^4 \times \mathbb{Z}_5$ | $\{(0,0,0,0,0),(0,0,0,1,1),(0,0,0,0,1),(0,0,0,0,2),(0,0,0,0,3),$ $(0,0,0,0,4),(0,0,0,1,0),(0,0,1,0,2),(0,0,1,0,4),(0,1,0,0,3),$ $(0,1,1,1,3),(1,0,0,0,3),(1,0,1,1,3),(1,1,0,1,3),(1,1,1,0,3)\}$ |
| 15 | 80 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),$ $(0,0,0,3),(0,0,0,4),(0,0,1,0),(0,0,1,2),(0,0,3,0),(0,1,1,1),(0,1,3,4),$ $(1,0,1,1),(1,0,3,4),(1,1,1,4),(1,1,3,1)\}$ |
| 14 | 80 | $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,2,1),(0,3,1),(0,4,0),(0,4,2),(1,0,3),$ $(1,0,4),(1,1,1),(1,3,1),(1,4,3),(1,4,4),(1,6,1)\}$ |
| 15 | 80 | $\mathbb{Z}_4^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,1,0),(0,1,2),$ $(0,3,0),(1,0,1),(1,2,4),(2,1,1),(2,3,4),(3,0,4),(3,2,1)\}$ |
| 15 | 81 | $\mathbb{Z}_3 \times \mathbb{Z}_{27}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,8),(0,15),(0,21),(1,1),(1,10),$ $(1,19),(2,4),(2,13),(2,22)\}$ |

| | | | |
|---|---|---|---|
| 14 | 81 | $\mathbb{Z}_3^4$ | $\{(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,1,0),(0,0,1,1),(0,0,1,2),$ $(0,1,0,0),(0,2,1,0),(1,0,0,0),(1,1,1,0),(1,2,2,1),(2,0,1,1),(2,1,2,2),$ $(2,2,0,1)\}$ |
| 14 | 81 | $\mathbb{Z}_3^2 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,0,1),(0,0,3),(0,0,4),(0,0,6),(0,0,7),(0,1,2),(0,2,2),$ $(1,0,2),(1,1,2),(1,2,5),(2,0,5),(2,1,8),(2,2,5)\}$ |
| 15 | 81 | $\mathbb{Z}_{81}$ | $\{0,1,2,3,4,5,6,7,8,19,29,40,49,60,70\}$ |
| 14 | 81 | $\mathbb{Z}_9^2$ | $\{(0,0),(0,1),(0,2),(0,4),(1,6),(2,4),(4,0),(5,7),(6,0),(6,2),(6,3),$ $(6,4),(7,3),(8,1)\}$ |
| 15 | 82 | $\mathbb{Z}_2 \times \mathbb{Z}_{41}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,15),(0,21),(0,31),$ $(0,40),(1,10),(1,19),(1,27),(1,34)\}$ |
| 15 | 83 | $\mathbb{Z}_{83}$ | $\{0,1,2,3,4,5,6,7,8,20,30,41,50,61,71\}$ |
| 15 | 84 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0,0,0),(0,1,1,1),(0,0,0,1),(0,0,0,2),(0,0,0,3),(0,0,0,6),$ $(0,1,0,3),(0,1,0,6),(0,1,2,1),(1,0,0,1),(1,0,1,4),(1,0,2,5),$ $(1,1,0,1),(1,1,1,5),(1,1,2,4)\}$ |
| 15 | 84 | $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),(0,1,5),(0,2,5),(1,0,0),$ $(1,0,2),(1,2,1),(3,0,1),(3,0,2),(3,0,4),(3,1,3),(3,2,3)\}$ |
| 15 | 85 | $\mathbb{Z}_5 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(1,9),(2,3),(2,10),$ $(3,3),(3,13),(4,5),(4,14)\}$ |

| **k** | **\|G\|** | **G** | **una base estricta mínima** |
|---|---|---|---|
| 3 | 3 | $\mathbb{Z}_3$ | $\{0,1,2\}$ |
| 4 | 4 | $\mathbb{Z}_4$ | $\{0,1,2,3\}$ |
| 4 | 5 | $\mathbb{Z}_5$ | $\{0,1,2,3\}$ |
| 4 | 6 | $\mathbb{Z}_2 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2)\}$ |
| 5 | 7 | $\mathbb{Z}_7$ | $\{0,1,2,3,4\}$ |
| 5 | 8 | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0)\}$ |
| 5 | 8 | $\mathbb{Z}_8$ | $\{0,1,2,3,5\}$ |
| 5 | 9 | $\mathbb{Z}_3^2$ | $\{(0,0),(0,1),(0,2),(1,0),(2,0)\}$ |
| 5 | 9 | $\mathbb{Z}_9$ | $\{0,1,2,3,6\}$ |
| 6 | 10 | $\mathbb{Z}_2 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4)\}$ |
| 6 | 11 | $\mathbb{Z}_{11}$ | $\{0,1,2,3,4,7\}$ |
| 6 | 12 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(1,0,0),(1,1,0)\}$ |
| 6 | 12 | $\mathbb{Z}_4 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2),(2,0),(3,0)\}$ |
| 6 | 13 | $\mathbb{Z}_{13}$ | $\{0,1,2,3,6,10\}$ |
| 7 | 14 | $\mathbb{Z}_2 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(1,3)\}$ |
| 7 | 15 | $\mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(2,0)\}$ |
| 7 | 16 | $\mathbb{Z}_{16}$ | $\{0,1,2,3,4,7,12\}$ |
| 7 | 16 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,1,0),(1,0,0),(1,1,0)\}$ |
| 7 | 16 | $\mathbb{Z}_2 \times \mathbb{Z}_8$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(1,2),(1,6)\}$ |
| 7 | 16 | $\mathbb{Z}_4^2$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0),(2,0),(3,0)\}$ |
| 7 | 17 | $\mathbb{Z}_{17}$ | $\{0,1,2,3,4,8,13\}$ |
| 8 | 18 | $\mathbb{Z}_2 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(0,1,2),(1,1,0)\}$ |
| 8 | 18 | $\mathbb{Z}_2 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,4)\}$ |
| 8 | 19 | $\mathbb{Z}_{19}$ | $\{0,1,2,3,4,5,8,14\}$ |
| 7 | 20 | $\mathbb{Z}_2^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,0,3),(0,0,4),(1,0,1),(1,1,1)\}$ |
| 8 | 20 | $\mathbb{Z}_4 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(2,0),(3,0)\}$ |
| 8 | 21 | $\mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(1,4),(2,2),(2,6)\}$ |
| 8 | 22 | $\mathbb{Z}_2 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,4),(0,9),(1,6),(1,7)\}$ |
| 9 | 23 | $\mathbb{Z}_{23}$ | $\{0,1,2,3,4,5,6,10,17\}$ |
| 8 | 24 | $\mathbb{Z}_2^3 \times \mathbb{Z}_3$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),(0,0,1,0),$ $(0,1,0,2),(1,0,0,2),(1,1,1,2)\}$ |
| 9 | 24 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,1,0),(0,1,2),$ $(0,2,0),(1,0,0),(1,2,0)\}$ |
| 8 | 24 | $\mathbb{Z}_8 \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,2),(2,0),(2,2),(4,1),(5,1),(6,1)\}$ |
| 9 | 25 | $\mathbb{Z}_{25}$ | $\{0,1,2,3,4,5,6,12,19\}$ |
| 8 | 25 | $\mathbb{Z}_5^2$ | $\{(0,0),(0,1),(0,2),(0,3),(1,0),(2,1),(3,2),(4,3)\}$ |
| 9 | 26 | $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,8),$ $(1,4),(1,9)\}$ |
| 9 | 27 | $\mathbb{Z}_{27}$ | $\{0,1,2,3,4,5,10,16,22\}$ |

| | | | |
|---|---|---|---|
| 9 | 27 | $\mathbb{Z}_3^3$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,2,0),(1,0,0),(1,1,1),$ $(2,0,0),(2,2,2)\}$ |
| 9 | 27 | $\mathbb{Z}_3 \times \mathbb{Z}_9$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(1,0),(1,4),(2,0),$ $(2,4)\}$ |
| 9 | 28 | $\mathbb{Z}_2^2 \times \mathbb{Z}7$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,6),$ $(1,0,1),(1,1,4),(1,1,5)\}$ |
| 9 | 28 | $\mathbb{Z}_4 \times \mathbb{Z}_7$ | $\{(0,0),(1,1),(0,1),(0,4),(0,6),(2,2),(2,3),(2,5),$ $(3,1)\}$ |
| 9 | 29 | $\mathbb{Z}_{29}$ | $\{0,1,2,3,5,10,16,22,27\}$ |
| 9 | 30 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,1,1),(0,2,2),(1,0,4),(1,2,2)\}$ |
| 10 | 31 | $\mathbb{Z}_{31}$ | $\{0,1,2,3,4,5,6,11,18,25\}$ |
| 10 | 32 | $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,10),(1,0),$ $(1,5),(1,11)\}$ |
| 10 | 32 | $\mathbb{Z}_2^3 \times \mathbb{Z}_4$ | $\{(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,0,3),(0,0,1,0),$ $(0,1,0,1),(1,0,0,1),(1,1,1,3)\}$ |
| 10 | 32 | $\mathbb{Z}_2^2 \times \mathbb{Z}_8$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),(0,0,6),$ $(0,0,1,1),(0,0,1,2),(0,1,3),(1,0,3),(1,1,7)\}$ |
| 10 | 32 | $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,1,0),(0,1,1),(0,1,2),$ $(0,3,1),(1,0,1),(1,2,3)\}$ |
| 10 | 32 | $\mathbb{Z}_{32}$ | $\{0,1,2,3,4,5,6,12,19,26\}$ |
| 10 | 32 | $\mathbb{Z}_4 \times \mathbb{Z}_8$ | $\{(0,0),(0,1),(0,2),(0,3),(0,5),(1,0),(2,0),(2,2),$ $(2,3),(3,4)\}$ |
| 10 | 33 | $\mathbb{Z}_3 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2)(0,3),(0,4),(0,5),(1,6),$ $(2,4),(2,10)\}$ |
| 10 | 34 | $\mathbb{Z}_2 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1)(0,1),(0,2),(0,3),(0,6),(0,13),(0,16),$ $(1,9),(1,10)\}$ |
| 10 | 35 | $\mathbb{Z}_5 \times \mathbb{Z}_7$ | $\{(0,0),(1,1)(0,1),(0,2),(1,0),(1,2),(2,3),(2,6),$ $(4,3),(4,6)\}$ |
| 10 | 36 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0),(0,1,0,1),(0,0,0,1),(0,0,0,2),$ $(0,0,1,0),(0,0,2,0),(0,1,0,2),(1,0,0,0),(1,1,1,0),(1,1,2,0)\}$ |
| 10 | 36 | $\mathbb{Z}_2^2 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,0,6),(0,1,2),(1,0,0),(1,0,3),(1,1,6)\}$ |
| 10 | 36 | $\mathbb{Z}_4 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,1,0),(1,0,0),$ $(1,2,1),(2,0,2),(2,1,0),(3,0,2),(3,2,1)\}$ |
| 10 | 36 | $\mathbb{Z}_4 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,4),(1,4),(1,5),(2,0),(2,7),$ $(3,5),(3,7)\}$ |
| 11 | 37 | $\mathbb{Z}_{37}$ | $\{0,1,2,3,4,5,6,7,14,22,30\}$ |
| 11 | 38 | $\mathbb{Z}_2 \times \mathbb{Z}_{19}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),$ $(0,12),(1,6),(1,13)\}$ |
| 11 | 39 | $\mathbb{Z}_3 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),$ $(1,7),(2,5),(2,12)\}$ |
| 11 | 40 | $\mathbb{Z}_2^3 \times \mathbb{Z}_5$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),(0,0,0,3),(0,1,0,0),$ $(0,1,1,4),(1,0,0,0),(1,0,1,4),(1,1,0,4),(1,1,1,1),\}$ |

| | | | |
|---|---|---|---|
| 11 | 40 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,2,0),(0,3,2),(1,0,0),(1,1,2),(1,2,4),(1,3,1)\}$ |
| 11 | 40 | $\mathbb{Z}_8 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(2,0),(3,2),(4,4),(5,1),$ $(6,0),(7,2)\}$ |
| 11 | 41 | $\mathbb{Z}_{41}$ | $\{0,1,2,3,4,5,11,18,23,28,35\}$ |
| 11 | 42 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,0,4),(0,0,5),(0,1,1),(0,2,4),(1,0,6),(1,2,4)\}$ |
| 12 | 43 | $\mathbb{Z}43$ | $\{0,1,2,3,4,5,6,7,12,20,28,36\}$ |
| 12 | 44 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{11}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),$ $(0,0,5),(0,0,8),(0,1,4),(1,0,2),(1,0,3),(1,1,8)\}$ |
| 12 | 44 | $\mathbb{Z}_4 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,5),$ $(2,0),(2,6),(3,5),(3,10)\}$ |
| 12 | 45 | $\mathbb{Z}_3^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,1,0),$ $(0,2,0),(0,2,3),(1,0,3),(1,1,4),(2,0,4),(2,2,3)\}$ |
| 12 | 45 | $\mathbb{Z}_9 \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(1,0),(2,0),(2,1),(4,2),$ $(5,4),(7,0),(8,1)\}$ |
| 12 | 46 | $\mathbb{Z}_2 \times \mathbb{Z}_{23}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,10),(0,17),$ $(1,6),(1,10),(1,17)\}$ |
| 12 | 47 | $\mathbb{Z}_{47}$ | $\{0,1,2,3,4,5,6,12,20,27,34,39\}$ |
| 12 | 48 | $\mathbb{Z}_{16} \times \mathbb{Z}_3$ | $\{(0,0),(1,1),(0,1),(0,2),(1,0),(3,0),(5,0),(7,0),(9,1),$ $(11,2),(13,0),(15,2)\}$ |
| 12 | 48 | $\mathbb{Z}_2^4 \times \mathbb{Z}_3$ | $\{(0,0,0,0,0),(0,0,0,1,1),(0,0,0,0,1),(0,0,0,0,2),$ $(0,0,0,1,0),(0,0,1,0,0),(0,1,0,0,0),(0,1,1,0,2),(1,0,0,0,0),$ $(1,0,1,0,2),(1,1,0,1,2),(1,1,1,0,0)\}$ |
| 12 | 48 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),$ $(0,0,1,0),(0,0,2,0),(0,1,0,0),(0,1,3,2),(1,0,0,1),(1,0,2,2),$ $(1,1,0,2),(1,1,2,1)\}$ |
| 12 | 48 | $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,1,0),(0,3,0),$ $(0,5,0),(0,7,2),(1,0,0),(1,2,0),(1,4,1),(1,6,2)\}$ |
| 12 | 48 | $\mathbb{Z}_4^2 \times \mathbb{Z}_3$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,1,0),(0,3,2),(1,0,0),$ $(1,2,0),(2,0,0),(2,2,0),(3,0,2),(3,2,2)\}$ |
| 12 | 49 | $\mathbb{Z}_{49}$ | $\{0,1,2,3,4,5,11,18,23,31,36,43\}$ |
| 12 | 49 | $\mathbb{Z}_7^2$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(1,0),(2,0),(3,1),(4,4),(5,5),$ $(6,5)\}$ |
| 12 | 50 | $\mathbb{Z}_2 \times \mathbb{Z}_{25}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,6),(0,9),(0,19),(0,22),(1,2),$ $(1,12),(1,16)\}$ |
| 13 | 50 | $\mathbb{Z}_2 \times \mathbb{Z}_5^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(1,0,0),(1,0,2),$ $(1,0,3),(1,1,0),(1,2,1),(1,3,2),(1,4,3)\}$ |
| 13 | 51 | $\mathbb{Z}_4 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(0,8),(1,9),$ $(2,7),(2,16)\}$ |
| 12 | 52 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{13}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,6),(0,0,10),$ $(0,1,2),(1,0,0),(1,0,3),(1,1,6),(1,1,10)\}$ |
| 12 | 52 | $\mathbb{Z}_4 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,4),(0,5),(0,6),(1,8),(2,0),(2,6),$ $(3,5),(3,11)\}$ |

| | | | |
|---|---|---|---|
| 12 | 53 | $\mathbb{Z}_{53}$ | $\{0, 1, 2, 3, 6, 11, 18, 25, 31, 38, 45, 50\}$ |
| 13 | 54 | $\mathbb{Z}_2 \times \mathbb{Z}_{27}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,12), (0,20), (1,7), (1,12), (1,20)\}$ |
| 12 | 54 | $\mathbb{Z}_2 \times \mathbb{Z}_3^3$ | $\{(0,0,0,0), (1,0,0,1), (0,0,0,1), (0,0,0,2), (0,0,1,0), (0,0,2,0), (0,1,0,0), (0,1,1,1), (0,2,0,2), (0,2,2,0), (1,1,2,0), (1,2,1,2)\}$ |
| 12 | 54 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ | $\{(0,0,0), (1,0,1), (0,0,1), (0,0,2), (0,0,3), (0,0,6), (0,1,1), (0,1,5), (0,2,1), (0,2,8), (1,1,7), (1,2,4)\}$ |
| 13 | 55 | $\mathbb{Z}_5 \times \mathbb{Z}_{11}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (1,5), (2,1), (2,7), (3,3), (3,8), (4,3), (4,10)\}$ |
| 13 | 56 | $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ | $\{(0,0,0,0), (0,0,1,1), (0,0,0,1), (0,0,0,2), (0,0,0,3), (0,0,0,4), (0,0,0,5), (0,1,0,0), (0,1,1,6), (1,0,0,0), (1,0,1,6), (1,1,0,6), (1,1,1,1)\}$ |
| 12 | 56 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ | $\{(0,0,0), (0,1,1), (0,0,4), (0,0,6), (0,2,2), (0,2,3), (0,2,5), (0,3,1), (1,0,1), (1,1,1), (1,2,1), (1,3,1)\}$ |
| 12 | 56 | $\mathbb{Z}_8 \times \mathbb{Z}_7$ | $\{(0,0), (1,1), (0,4), (0,6), (2,1), (3,1), (4,2), (4,3), (4,5), (5,1), (6,1), (7,1)\}$ |
| 13 | 57 | $\mathbb{Z}_3 \times \mathbb{Z}_{19}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (0,13), (1,8), (1,13), (2,3), (2,11), (2,16)\}$ |
| 13 | 58 | $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{29}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,8), (0,15), (0,18), (0,25), (1,3), (1,12), (1,21)\}$ |
| 13 | 59 | $\mathbb{Z}_{59}$ | $\{0, 1, 2, 3, 4, 7, 14, 23, 31, 33, 39, 48, 55\}$ |
| 13 | 60 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0,0,0), (0,1,1,1), (0,0,0,1), (0,0,0,2), (0,0,1,0), (0,0,1,3), (0,0,2,2), (0,0,2,4), (0,1,2,1), (1,0,1,0), (1,0,2,2), (1,1,1,0), (1,1,2,2)\}$ |
| 13 | 60 | $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ | $\{(0,0,0), (1,1,1), (0,0,1), (0,0,2), (0,0,3), (0,1,4), (1,0,1), (1,2,1), (2,0,3), (2,1,0), (2,1,1), (2,1,2), (2,1,4)\}$ |
| 13 | 61 | $\mathbb{Z}_{61}$ | $\{0, 1, 2, 3, 4, 7, 13, 21, 29, 36, 44, 52, 58\}$ |
| 14 | 62 | $\mathbb{Z}_2 \times \mathbb{Z}_{31}$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,7), (0,14), (0,23), (1,8), (1,14), (1,23)\}$ |
| 14 | 63 | $\mathbb{Z}_3^2 \times \mathbb{Z}_7$ | $\{(0,0,0), (0,1,1), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,0,5), (0,2,0), (1,0,0), (1,1,3), (1,2,5), (2,0,2), (2,1,0), (2,2,6)\}$ |
| 14 | 63 | $\mathbb{Z}_9 \times \mathbb{Z}_7$ | $\{(0,0), (1,1), (0,1), (0,2), (0,3), (0,4), (0,5), (2,0), (3,0), (4,2), (5,3), (6,5), (7,4), (8,4)\}$ |
| 13 | 64 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{16}$ | $\{(0,0,0), (0,0,1), (0,0,2), (0,0,3), (0,0,4), (0,0,7), (0,0,13), (0,1,2), (0,1,10), (1,0,2), (1,0,10), (1,1,6), (1,1,14)\}$ |
| 14 | 64 | $\mathbb{Z}_2^4 \times \mathbb{Z}_4$ | $\{(0,0,0,0,0), (0,0,0,0,1), (0,0,0,0,2), (0,0,0,0,3), (0,0,0,1,0), (0,0,0,1,1), (0,0,0,1,2), (0,0,1,0,0), (0,1,0,0,0), (0,1,1,0,1), (1,0,0,0,0), (1,0,1,0,1), (1,1,0,1,3), (1,1,1,0,0)\}$ |
| 14 | 64 | $\mathbb{Z}_2^3 \times \mathbb{Z}_8$ | $\{(0,0,0,0), (0,0,0,1), (0,0,0,2), (0,0,0,3), (0,0,0,4), (0,0,0,5), (0,0,0,6), (0,0,1,0), (0,1,0,0), (0,1,1,3), (1,0,0,0), (1,0,1,3), (1,1,0,7), (1,1,1,0)\}$ |
| 14 | 64 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4^2$ | $\{(0,0,0,0), (0,0,0,1), (0,0,0,2), (0,0,0,3), (0,0,1,0), (0,0,1,1), (0,0,1,2), (0,0,3,1), (0,1,0,0), (0,1,2,0), (1,0,0,0), (1,0,2,0), (1,1,1,1), (1,1,3,3)\}$ |
| 14 | 64 | $\mathbb{Z}_2 \times \mathbb{Z}_{32}$ | $\{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,7), (0,15), (0,24), (1,8), (1,15), (1,24), (1,31)\}$ |

| | | | |
|---|---|---|---|
| 14 | 64 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),$ $(0,0,6),(0,1,0),(0,2,0),(0,3,6),(1,0,0),(1,1,6),(1,2,7),(1,3,0)\}$ |
| 13 | 64 | $\mathbb{Z}_4 \times \mathbb{Z}_{16}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,7),(0,13),(1,0),(1,8),(2,2),$ $(2,10),(3,4),(3,12)\}$ |
| 14 | 64 | $\mathbb{Z}_4^3$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,1,0),(0,1,1),(0,1,2),(0,3,0),$ $(1,0,0),(1,2,1),(2,1,0),(2,3,1),(3,0,3),(3,2,0)\}$ |
| 14 | 64 | $\mathbb{Z}_{64}$ | $\{0,1,2,3,4,5,6,7,15,24,31,40,4,56\}$ |
| 14 | 64 | $\mathbb{Z}_8^2$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(1,0),(2,0),(3,1),(4,2),$ $(5,5),(6,6),(7,6)\}$ |
| 14 | 65 | $\mathbb{Z}_5 \times \mathbb{Z}_{13}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(1,6),(2,1),(2,8),(3,4),$ $(3,10),(4,4),(4,12)\}$ |
| 14 | 66 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),$ $(0,0,5),(0,0,8),(0,1,6),(0,1,10),(0,2,7),(0,2,9),(1,0,1),(1,2,1)\}$ |
| 14 | 67 | $\mathbb{Z}_{67}$ | $\{0,1,2,3,5,6,7,8,17,27,35,40,48,58\}$ |
| 14 | 68 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{17}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,8),$ $(0,0,13),(0,1,2),(0,1,3),(1,0,0),(1,0,4),(1,1,8),(1,1,13)\}$ |
| 14 | 68 | $\mathbb{Z}_4 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,12),(0,13),(0,14),(0,15),(1,10),$ $(2,3),(2,12),(3,5),(3,14)\}$ |
| 14 | 69 | $\mathbb{Z}_3 \times \mathbb{Z}_{23}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,8),(0,18),(1,5),(1,14),(1,17),$ $(2,2),(2,9),(2,12),(2,21)\}$ |
| 14 | 70 | $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ | $\{(0,0,0),(1,1,1),(0,0,4),(0,0,6),(0,1,1),(0,2,1),$ $(0,3,1),(0,4,1),(1,0,2),(1,0,3),(1,0,5),(1,2,1),(1,3,1),(1,4,1)\}$ |
| 15 | 71 | $\mathbb{Z}_{71}$ | $\{0,1,2,3,4,5,6,7,8,16,26,35,45,54,61\}$ |
| 14 | 72 | $\mathbb{Z}_2^3 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0,0),(0,0,1,0,1),(0,0,0,0,2),(0,0,0,1,0),(0,0,0,1,1),$ $(0,0,1,2,1),(0,0,1,2,2),(0,1,0,2,0),(0,1,1,2,0),(1,0,0,2,0),$ $(1,0,1,2,0),(1,1,0,2,0),(1,1,1,2,0)\}$ |
| 14 | 72 | $\mathbb{Z}_2^3 \times \mathbb{Z}_9$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,2),(0,0,0,3),(0,0,0,4),(0,0,0,5),$ $(0,0,0,7),(0,0,1,6),(0,1,0,8),(0,1,1,8),(1,0,0,8),(1,0,1,8),$ $(1,1,0,8),(1,1,1,8)\}$ |
| 14 | 72 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2$ | $\{(0,0,0,0),(0,1,0,1),(0,0,0,2),(0,0,1,0),(0,0,2,2),$ $(0,2,1,1),(0,2,1,2),(0,2,2,0),(0,2,2,1),(0,3,0,1),(1,0,0,1),$ $(1,1,0,1),(1,2,0,1),(1,3,0,1)\}$ |
| 14 | 72 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,1,1),(0,0,2),(0,0,3),(0,0,4),(0,0,7),$ $(0,0,8),(0,2,5),(0,2,6),(0,3,1),(1,0,1),(1,1,1),(1,2,1),(1,3,1)\}$ |
| 14 | 72 | $\mathbb{Z}_8 \times \mathbb{Z}_3^2$ | $\{(0,0,0),(1,0,1),(0,0,2),(0,1,0),(0,2,2),(2,0,1),(3,0,1),$ $(4,1,1),(4,1,2),(4,2,0),(4,2,1),(5,0,1),(6,0,1),(7,0,1)\}$ |
| 14 | 72 | $\mathbb{Z}_8 \times \mathbb{Z}_9$ | $\{(0,0),(1,1),(0,1),(0,2),(0,4),(1,5),(2,2),(2,4),(2,5),(2,6),$ $(4,3),(5,1),(5,5),(6,3)\}$ |
| 15 | 73 | $\mathbb{Z}_{73}$ | $\{0,1,2,3,4,5,6,7,8,17,27,35,46,54,64\}$ |
| 15 | 74 | $\mathbb{Z}_2 \times \mathbb{Z}_{37}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,14),(0,21),$ $(0,27),(0,36),(1,9),(1,17),(1,25),(1,32)\}$ |
| 15 | 75 | $\mathbb{Z}_3 \times \mathbb{Z}_{25}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),$ $(0,15),(1,11),(1,19),(2,6),(2,13),(2,22)\}$ |
| 15 | 75 | $\mathbb{Z}_3 \times \mathbb{Z}_5^2$ | $\{(0,0,0),(1,0,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(1,1,0),$ $(1,2,0),(1,3,0),(1,4,4),(2,0,0),(2,1,1),(2,2,2),(2,3,3),(2,4,4)\}$ |

| | | | |
|---|---|---|---|
| 15 | 76 | $\mathbb{Z}_2^2 \times \mathbb{Z}_{19}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,0,5),$ $(0,0,9),(0,0,15),(0,1,12),(1,0,1),(1,0,12),(1,1,6),(1,1,16),(1,1,18)\}$ |
| 15 | 76 | $\mathbb{Z}_4 \times \mathbb{Z}_{19}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,4),(0,8),(0,13),(1,15),(2,7),$ $(2,9),(2,10),(2,11),(2,17),(3,1),(3,15)\}$ |
| 15 | 77 | $\mathbb{Z}_7 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,6),(1,0),(1,2),(2,10),(3,5),$ $(3,8),(4,1),(5,5),(5,8),(6,3),(6,10)\}$ |
| 15 | 78 | $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{13}$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,5),(0,0,10),$ $(0,0,12),(0,1,6),(0,1,9),(0,2,6),(0,2,9),(1,0,3),(1,0,12),(1,2,1)\}$ |
| 16 | 79 | $\mathbb{Z}_{79}$ | $\{01,2,3,4,5,6,7,8,9,18,29,39,50,60,68\}$ |
| 15 | 80 | $\mathbb{Z}_{16} \times \mathbb{Z}_5$ | $\{(0,0),(1,1),(0,1),(2,1),(3,4),(4,1),(4,3),(6,0),(8,2),$ $(8,4),(9,1),(10,4),(11,4),(12,0),(12,4)\}$ |
| 15 | 80 | $\mathbb{Z}_2^4 \times \mathbb{Z}_5$ | $\{(0,0,0,0,0),(0,0,0,1,1),(0,0,0,0,1),(0,0,0,0,2),(0,0,0,0,3),$ $(0,0,0,0,4),(0,0,0,1,0),(0,0,1,0,2),(0,0,1,0,4),(0,1,0,0,3),$ $(0,1,1,1,3),(1,0,0,0,3),(1,0,1,1,3),(1,1,0,1,3),(1,1,1,0,3)\}$ |
| 15 | 80 | $\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),$ $(0,0,0,3),(0,0,0,4),(0,0,3,1),(0,1,0,0),(0,1,0,2),(0,1,2,3),$ $(0,1,2,4),(1,0,0,1),(1,0,2,1),(1,1,1,1),(1,1,3,1)\}$ |
| 15 | 80 | $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,3,1),$ $(0,5,1),(0,7,1),(1,0,0),(1,0,2),(1,2,1),(1,4,3),(1,4,4),(1,6,1)\}$ |
| 16 | 80 | $\mathbb{Z}_4^2 \times \mathbb{Z}_5$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),(0,0,4),(0,1,0),(0,1,2),$ $(0,1,3),(0,3,0),(1,0,0),(1,2,0),(2,1,1),(2,3,2),(3,0,2),(3,2,2)\}$ |
| 15 | 81 | $\mathbb{Z}_3 \times \mathbb{Z}_{27}$ | $\{(0,0),(0,1),(0,2),(0,3),(0,9),(0,12),$ $(0,15),(0,18),(0,21),(1,1),(1,6),(1,11),(2,1),(2,20),(2,24)\}$ |
| 15 | 81 | $\mathbb{Z}_3^4$ | $\{(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,1,0),(0,0,1,1),$ $(0,0,1,2),(0,0,2,0),(0,1,0,0),(0,2,1,0),(1,0,0,0),(1,1,1,1),$ $(1,2,2,2),(2,0,1,0),(2,1,2,2),(2,2,0,1)\}$ |
| 15 | 81 | $\mathbb{Z}_3^2 \times \mathbb{Z}_9$ | $\{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,0,4),$ $(0,0,6),(0,0,7),(0,1,0),(0,2,1),(1,0,0),(1,1,4),(1,2,8),$ $(2,0,7),(2,1,5),(2,2,0)\}$ |
| 16 | 81 | $\mathbb{Z}_{81}$ | $\{0,1,2,3,4,5,6,7,8,9,19,30,39,51,60,71\}$ |
| 15 | 81 | $\mathbb{Z}_9^2$ | $\{(0,0),(0,1),(0,2),(0,3),(0,4),(0,6),(0,7),(1,0),(2,1),$ $(3,2),(4,3),(5,7),(6,2),(7,6),(8,4)\}$ |
| 16 | 82 | $\mathbb{Z}_2 \times \mathbb{Z}_{41}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),$ $(0,16),(0,24),(0,31),(1,8),(1,16),(1,25),(1,31)\}$ |
| 16 | 83 | $\mathbb{Z}_{83}$ | $\{0,1,2,3,4,5,6,7,8,17,27,37,46,54,65,72\}$ |
| 16 | 84 | $\mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0,0,0),(0,1,1,1),(0,0,0,1),$ $(0,0,0,2),(0,0,0,3),(0,0,0,4),(0,0,1,5),(0,0,2,0),(0,0,2,3),(0,1,1,2),$ $(0,1,1,3),(0,1,2,2),(1,0,0,4),(1,0,1,0),(1,1,0,4),(1,1,1,0)\}$ |
| 16 | 84 | $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,0,4),(0,1,4),(0,2,0),(1,0,3),(1,2,0),(2,0,2),(2,1,6),(2,2,5),$ $(3,0,1),(3,1,4),(3,2,3)\}$ |
| 16 | 85 | $\mathbb{Z}_5 \times \mathbb{Z}_{17}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(1,8),$ $(2,1),(2,10),(3,6),(3,14),(4,6),(4,16)\}$ |
| 16 | 86 | $\mathbb{Z}_2 \times \mathbb{Z}_{43}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,6),(0,14),(0,21),(0,26),$ $(0,33),(0,41),(1,10),(1,19),(1,28),(1,37)\}$ |

| | | | |
|---|---|---|---|
| 16 | 87 | $\mathbb{Z}_3 \times \mathbb{Z}_{29}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,5),(0,14),(0,24),(1,11),$ $(2,7),(2,9),(2,10),(2,11),(2,12),(2,17),(2,27)\}$ |
| 16 | 88 | $\mathbb{Z}_2^3 \times \mathbb{Z}_{11}$ | $\{(0,0,0,0),(0,0,1,1),(0,0,0,1),(0,0,0,2),(0,0,0,3),$ $(0,0,0,7),(0,0,1,2),(0,1,0,0),(0,1,0,3),(0,1,1,7),(1,0,0,4),$ $(1,0,0,7),(1,0,0,10),(1,1,0,7),(1,1,1,4),(1,1,1,10)\}$ |
| 16 | 88 | $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{11}$ | $\{(0,0,0),(0,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,0,4),(0,0,7),(0,2,6),(0,2,9),(0,3,1),(1,0,1),(1,1,5),(1,1,10),$ $(1,2,1),(1,3,6),(1,3,8)\}$ |
| 16 | 88 | $\mathbb{Z}_8 \times \mathbb{Z}_{11}$ | $\{(0,0),(1,1),(0,1),(0,2),(0,3),(0,4),(0,7),(2,5),(2,10),$ $(3,1),(4,6),(4,9),(5,1),(6,6),(6,8),(7,1)\}$ |
| 16 | 89 | $\mathbb{Z}_{89}$ | $\{0,1,2,3,5,6,7,8,15,25,35,46,5),62,72,82\}$ |
| 16 | 90 | $\mathbb{Z}_2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$ | $\{(0,0,0,0),(1,0,1,1),(0,0,0,1),(0,0,0,2),$ $(0,0,0,3),(0,0,1,0),(0,0,2,4),(1,0,0,0),(1,0,0,3),(1,0,2,2),$ $(1,1,0,4),(1,1,1,4),(1,1,2,4),(1,2,0,4),(1,2,1,4),(1,2,2,4)\}$ |
| 16 | 90 | $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ | $\{(0,0,0),(1,1,1),(0,0,1),(0,0,2),(0,0,3),$ $(0,0,4),(1,0,0),(1,1,4),(1,2,2),(1,3,2),(1,4,4),(1,5,1),(1,6,3),$ $(1,7,3),(1,8,1),(1,8,4)\}$ |

# Conclusiones

1) Se realizó un estudio detallado de los artículos *Minimum Sum and Difference Covers of Abelian Groups*. Harri Haanpää y *Minimum Sum Covers of Small Cyclic Groups*. Mark A. Fitch and Robert E. Jamison, logrando así su fácil entendimiento para posteriores estudios relacionados con el tema.

2) El análisis de la construcción natural de una base para $\mathbb{Z}_n$ presentada en el artículo *Minimum Sum Covers of Small Cyclic Groups*. Mark A. Fitch and Robert E. Jamison, nos permitió encontrar una base modular con un número menor de elementos.

3) Se evidenció la importancia de los conjuntos de Sidon en la construcción de una Base para ciertos valores de $n$.

4) La elaboración de esta monografía nos enseño a investigar, analizar y escribir textos matemáticos, además recordamos conceptos y resultados básicos adquiridos en el transcurso de nuestra carrera.

5) Se abre un camino para trabajos posteriores relacionados con los temas y los problemas abiertos que se identificaron.

# Bibliografía


[1] Harri Haanpää, *Minimun Sum and Difference Covers of Abelian*, Journal of integer Sequences, Vol. 7(2004), Article 04.2.6, Laboratory for Theoretical Computer science, Department of Computer Science and Engineering, Helsinki University of Technology.

[2] Mark A Fitch and Robert E. Jamison, *Minimum Sum covers of Small Cyclic Groups*, Congressus Numerantium 147(2000), 65-81, Departament of Mathematical Science, Clemson University.

[3] S. Gómez, P. Pisso, C. Trujillo, *Conjuntos de Sidon Módulo m y Particiones*, Unicauca Ciencia Vol 7(2002), Departamento de Matemáticas, Universidad del Cauca, Popayán Colombia.

[4] John B. Fraleigh, *Algebra Abstracta*, Addison-Wesley Iberoamericana.