UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO CONJUNTO EN CIENCIAS MATEMÁTICAS UNAM-UMSNH

SUMA Y PRODUCTO DE CONJUNTOS Y ESTIMACIONES DE SUMAS TRIGONOMÉTRICAS DE GAUSS

T E S I S

QUE PARA OPTAR POR EL GRADO DE MAESTRO EN CIENCIAS

PRESENTA:

JOSÉ HERNÁNDEZ SANTIAGO

ASESOR: DR. MOUBARIZ GARAEV

CENTRO DE CIENCIAS MATEMÁTICAS UNAM

MÉXICO, D. F. — MAYO DE 2013.

Índice general

Agradecimientos III

INTRODUCCIÓN IV

Capítulo 1. Sumas trigonométricas racionales 1

Capítulo 2. Elementos de combinatoria aditiva 13

Capítulo 3. Estimaciones de suma-producto en $\mathbb{F}_p$ 35

Capítulo 4. Aplicaciones a sumas trigonométricas 50

Bibliografía 62

Agradecimientos

Al CONACYT, por la beca que me concedió para realizar estudios de maestría en el Posgrado Conjunto en Ciencias Matemáticas UNAM-UMSNH.

Al Centro de Ciencias Matemáticas UNAM, por todas las facilidades que me brindó desde mi primer semana como estudiante de maestría: espacio de trabajo, acceso a su sala de cómputo y acceso ilimitado a su acervo (en este punto, extiendo un agradecimiento especial a la Lic. Lidia González por la prontitud con la cual respondió a cada una de mis peticiones).

Al Dr. Moubariz Garaev, por haber fungido como mi asesor durante mis estudios de maestría y por la paciencia que mostró hacia mi persona durante todo este tiempo.

Al Dr. Eugenio Balanzario, por las conversaciones que tuvimos.

A los doctores Eugenio Balanzario, Víctor C. García y Daniel Pellicer por haber participado en la revisión de esta tesis y por todas las correciones y sugerencias que hicieron con la intención de que el trabajo quedara más depurado.

INTRODUCCIÓN

El tema principal de este trabajo son las sumas trigonométricas de Gauss y su estimación mediante resultados de combinatoria aditiva. En combinatoria aditiva se estudian propiedades combinatorias de objetos algebraicos (grupos, anillos, campos). Ben J. Green apunta en [**18**] que, aunque resulta un tanto difícil especificar lo que el tema es en sí, hay un punto de vista sobre el que gradualmente se empieza a consensuar: "... additive combinatorics is the study of *approximate mathematical structures* such as approximate groups, rings, fields, polynomials and homomorphisms. It is interested in what the right definitions of these approximate structures are, what can be said about them, and what applications this has to other parts of mathematics.". La combinatoria aditiva es un área en la que ha habido avances importantes motivados por investigaciones relacionadas con el teorema de Szemerédi sobre progresiones aritméticas en subconjuntos de $\mathbb{N}$ con densidad superior positiva, el teorema de Green y Tao sobre progresiones aritméticas arbitrariamente largas de números primos y el fenómeno de suma-producto. Dada la particular relevancia que tendrá el fenónemo de suma-producto en este trabajo, daremos a continuación algunos detalles sobre el mismo.

Sea A un subconjunto no vacío de los números enteros. El conjunto suma de A se define como $A+A := \{a+b : (a,b) \in A \times A\}$. El conjunto producto de A se define de manera similar, $AA := \{ab : (a,b) \in A \times A\}$. Si A es finito entonces

$$2|A| - 1 \leqslant |A+A| \leqslant \frac{1}{2}(|A|^2 + |A|)$$

y

$$2|A| - 1 \leqslant |AA| \leqslant \frac{1}{2}(|A|^2 + |A|).$$

El conjunto producto AA tiene cardinalidad mínima cuando A es una progresión geométrica, pero en ese caso el conjunto suma $A+A$ tiene cardinalidad máxima. Por otro lado, el conjunto suma $A+A$ tiene cardinalidad mínima cuando A es una progresión aritmética, esto es $|A+A| = 2|A|-1$. No obstante en este caso el cardinal del conjunto producto AA es grande. De hecho es sabido, de [**10**] por ejemplo, que si $A = \{1,\dots,n\}$ entonces $|AA|$ es casi del orden $|A|^2$.

Aun cuando los elementos de un subconjunto arbitrario de $\mathbb{Z}$ no están necesariamente en progresión aritmética o progresión geométrica, resulta natural cuestionarse si existe algún A finito y no vacío tal que tanto $|A+A|$ como $|AA|$ sean pequeños. Este problema, conocido ahora como problema de suma-producto para subconjuntos de $\mathbb{Z}$, apareció por vez primera en 1983 en el trabajo de Erdös y Szemerédi [**9**]. Ellos demostraron que existe una constante positiva c tal que para cualquier subconjunto finito y no vacío de enteros A se cumple que alguno de los conjuntos $A+A$ y AA tiene cardinalidad mayor o igual a $|A|^{1+c}$. Erdös y Szemerédi conjeturaron que para cada $\epsilon > 0$ existe $c := c(\epsilon) > 0$ tal que

$$\max\{|A+A|, |AA|\} \geqslant c|A|^{2-\epsilon}.$$

Al momento, el mejor resultado que se tiene se debe a Solymosi [**31**]:

$$\max\{|A+A|, |AA|\} \geqslant c|A|^{4/3-\epsilon}.$$

Terence Tao menciona en [**32**] que el problema de obtener un análogo en[1] $\mathbb{F}_p$ del resultado de Erdös y Szemerédi fue planteado en 1999 por Wolff (con cierta restricción adicional sobre $|A|$). Los métodos conocidos en ese momento no funcionaban sobre campos finitos; para resolverlo hacía falta introducir nuevas ideas. La pregunta de Wolff surgió en relación con el análogo del problema de Kakeya sobre campos finitos. La solución del análogo en $\mathbb{F}_p$ de la estimación de suma-producto se atribuye al trabajo de Bourgain, Katz y Tao [**6**] de 2004 (en el rango $p^\epsilon \leqslant |A| \leqslant p^{1-\epsilon}$) y al de Bourgain, Glibichuk y Konyagin [**5**] de 2006 (en el rango completo $1 \leqslant |A| \leqslant p^{1-\epsilon}$). En 2007 Garaev [**11, 13**] introdujo nuevas herramientas que dieron lugar a estimaciones óptimas para subconjuntos relativamente grandes de $\mathbb{F}_p$ y estimaciones explícitas para subconjuntos de cualquier cardinal. La estimación de Garaev sería generalizada posteriormente por Katz y Shen [**23**] a cualquier campo finito.

La estimación de suma-producto y sus variantes han encontrado numerosas aplicaciones en varias áreas de las matemáticas. Un ejemplo particularmente digno de mención se da en el trabajo de Helfgott [**21**] donde se prueba que si A es un conjunto de generadores de $\mathrm{SL}_2(\mathbb{F}_p)$ entonces el diámetro de la gráfica de Cayley $\Gamma(\mathrm{SL}_2(\mathbb{F}_p), A)$ no excede a $c_1(\log p)^{c_2}$, donde c_1 y c_2 son constantes absolutas. Helfgott obtendría después en [**22**] un análogo del resultado anterior para $\mathrm{SL}_3(\mathbb{F}_p)$. Otra aplicación notable se da en la estimación de sumas de caracteres sobre conjuntos especiales; un referente en este sentido sería el trabajo de Chang en [**8**]. Es de mencionar también que a través de estimaciones de suma-producto, Bourgain resolvió en [**2**] una serie de problemas relacionados con ciencias de la computación .

[1] A lo largo de la tesis, $\mathbb{F}_p$ denotará al único campo que tiene por orden el número primo p. Identificaremos a sus elementos con los elementos del conjunto $\{0, 1, 2, \ldots, p-1\}$. Con $\mathbb{F}_p^*$ denotaremos a los elementos distintos de cero de $\mathbb{F}_p$. $\mathbb{F}_p^*$, bajo el producto de $\mathbb{F}_p$, es un grupo al cual se le conoce como *el grupo multiplicativo* de $\mathbb{F}_p$.

En la presente tesis nos dedicaremos a la estimación de suma-producto y a una de sus aplicaciones más espectaculares: la estimación de sumas trigonométricas. La aplicación de la estimación de suma-producto a sumas trigonométricas apareció por vez primera en Bourgain, Glibichuk y Konyagin [**5**]. Posteriormente los resultados de [**5**] fueron mejorados en trabajos de Bourgain [**3**], Bourgain y Garaev [**4**] y Garaev [**15**].

La tesis se basa en [**15**] y consta de cuatro capítulos. En el capítulo 1 se empieza por recapitular los resultados clásicos sobre sumas de Gauss. Después se muestra cómo el problema de su estimación se relaciona con la estimación de sumas trigonométricas multilineales y con la estimación de suma-producto sobre $\mathbb{F}_p$.

En el capítulo 2 se introducen las nociones de combinatoria aditiva necesarias para probar los resultados que devienen en estimaciones no triviales para sumas de Gauss de grados superiores. Entre las nociones y resultados principales que se abordan en este capítulo se encuentran: la desigualdad triangular de Ruzsa, las gráficas de Plünnecke y sus propiedades básicas, la desigualdad de Plünnecke, la desigualdad de Ruzsa-Plünnecke, la versión de Bourgain-Garaev de la estimación de Balog-Szemerédi-Gowers y las relaciones entre las energías aditivas y multiplicativas de conjuntos y las estimaciones de suma-producto.

El capítulo 3 inicia con la solución al problema de la estimación de suma-producto en $\mathbb{F}_p$. Antes de establecer el teorema en toda su generalidad, se presenta un resultado de Garaev que implica a la estimación de suma-producto sobre subconjuntos de $\mathbb{F}_p$ de cardinal relativamente grande. En este capítulo se demuestra también una versión explícita de la estimación de suma-producto de Bourgain para conjuntos diferentes.

En el capítulo 4 se aborda la estimación de sumas trigonométricas multilineales. Es en este apartado donde confluyen los esfuerzos de los capítulos 2 y 3. El resultado central aquí es una versión de la estimación de Bourgain, Glibichuk y Konyagin de sumas trigonómetricas multilineales. Puesto que el interés básico es la obtención de estimaciones no triviales para sumas de Gauss de grados superiores, mostramos cómo éstas pueden derivarse a partir de la versión obtenida de la estimación de Bourgain, Glibichuk y Konyagin.

La notación en el trabajo es estándard. Usamos los símbolos de Vinogradov $\ll$ y $\gg$ con su denotación usual: si $a \geqslant 0$ y f, g son funciones con dominio $[a,\infty)$, escribimos $f(x) \ll g(x)$ para $x \geqslant x_0$ siempre que existan constantes $C > 0$ y $x_0 \geqslant a$ tales que $|f(x)| \leqslant Cg(x)$ para todo $x \geqslant x_0$. La constante implicada C puede depender en ocasiones de otros parámetros cuya naturaleza será clara del contexto. Por otro lado, $f(x) = o(g(x))$ cuando $x \to \infty$ indica que para cada $\epsilon > 0$ existe $x_0 := x_0(\epsilon)$ tal que $|f(x)| < \epsilon g(x)$ para $x \geqslant x_0$.

Capítulo 1

Sumas trigonométricas racionales

Sea m un número entero mayor o igual a 2. Una *suma trigonométrica racional* es una suma de la forma

$$\sum_{n=1}^{N} e^{2\pi i \frac{x_n}{m}} \tag{1}$$

donde $x_1, x_2, \ldots, x_N$ son números enteros. Una cota trivial para el módulo de una suma trigonométrica como la anterior es N. Una problemática recurrente en teoría de números es la determinación de estimaciones no triviales para estas sumas.

Las sumas trigonométricas racionales son una herramienta básica para resolver ciertas clases de problemas en teoría de números pero tienen también aplicaciones en otras partes de las matemáticas. A continuación se presenta un ejemplo de la relación entre la estimación de sumas trigonométricas racionales y el estudio de congruencias aditivas. El lema puede encontrarse ya en [**34**], uno de los primeros escritos de I. M. Vinogradov.

Lema 1.1. *Sean $m \geqslant 2$ entero y u, v números que recorren los sistemas de enteros*

$$u = u_1, \ldots, u_N; \qquad v = v_1, v_2, \ldots, v_M.$$

Supongamos que

$$\max_{1 \leqslant \lambda \leqslant m-1} \left| \sum_{u} e^{2\pi i \frac{\lambda u}{m}} \right| \leqslant R \qquad \text{y} \qquad \sum_{\lambda=1}^{m-1} \left| \sum_{v} e^{2\pi i \frac{\lambda v}{m}} \right| \leqslant D.$$

Entonces el número de soluciones J a la congruencia

$$u_x \equiv v_y \pmod{m}, \quad 1 \leqslant x \leqslant N, \quad 1 \leqslant y \leqslant M$$

se puede representar en la forma

$$J = \frac{NM}{m}\left(1 + \theta \frac{RD}{NM}\right)$$

para algún $\theta \in [-1, 1]$.

Prueba. El punto de partida de la demostración es la siguiente identidad elemental:

$$\sum_{\lambda=0}^{m-1} e^{2\pi i \frac{\lambda x}{m}} = \begin{cases} m & \text{si } x \equiv 0 \pmod{m}, \\ 0 & \text{en otro caso.} \end{cases} \tag{2}$$

De esto se sigue que

$$\frac{1}{m}\sum_{\lambda=0}^{m-1} e^{2\pi i \frac{\lambda(u-v)}{m}} = \begin{cases} 1 & \text{si } u \equiv v \pmod{m}, \\ 0 & \text{en otro caso.} \end{cases}$$

Sumando esta identidad sobre $u = u_1, u_2, \ldots, u_N$ y $v = v_1, v_2 \ldots, v_M$ tenemos

$$\begin{aligned} J &= \sum_u \sum_v \frac{1}{m} \sum_{\lambda=0}^{m-1} e^{2\pi i \lambda \frac{(u-v)}{m}} \\ &= \frac{1}{m} \sum_{\lambda=0}^{m-1} \sum_u \sum_v e^{2\pi i \lambda \frac{(u-v)}{m}}. \end{aligned}$$

Separando el término $\lambda = 0$ se obtiene

$$J = \frac{NM}{m} + E \tag{3}$$

donde

$$E = \frac{1}{m} \sum_{\lambda=1}^{m-1} \left(\sum_u e^{2\pi i \frac{\lambda u}{m}} \right) \left(\sum_v e^{-2\pi i \frac{\lambda v}{m}} \right).$$

Por las hipótesis

$$\begin{aligned} |E| &\leqslant \frac{1}{m} \sum_{\lambda=1}^{m-1} \left| \sum_u e^{2\pi i \lambda u/m} \right| \left| \sum_v e^{2\pi i \lambda v/m} \right| \\ &\leqslant \frac{R}{m} \sum_{\lambda=1}^{m-1} \left| \sum_v e^{2\pi i \lambda v/m} \right| \\ &\leqslant \frac{RD}{m} \end{aligned}$$

Luego, para algún $\theta \in [-1, 1]$ se cumple que $E = \frac{\theta RD}{m}$. El aserto es consecuencia de esto último y (3).

□

Así, si se cuenta con estimaciones de sumas trigonométricas como en la hipótesis del lema entonces se pueden derivar fórmulas asintóticas para el número de soluciones de las respectivas congruencias aditivas.

Una de las estimaciones más simples de sumas trigonométricas es la estimación de sumas bilineales: si p es un número primo y a es un entero coprimo con p entonces para cualesquiera subconjuntos X y Y de $\mathbb{F}_p$ se cumple que

$$W := \sum_{x\in X}\left|\sum_{y\in Y} e^{2\pi i\frac{axy}{p}}\right| \leqslant (p|X||Y|)^{1/2}. \tag{4}$$

Para probarla basta con aplicar la desigualdad de Cauchy-Schwarz[1] a la suma sobre la variable x y extender después la suma al sistema completo de residuos. En efecto,

$$W^2 \leqslant |X|\sum_{x=0}^{p-1}\left|\sum_{y\in Y} e^{2\pi i\frac{axy}{p}}\right|^2 = |X|\sum_{y_1\in Y}\sum_{y_2\in Y}\sum_{x=0}^{p-1} e^{2\pi i\frac{ax(y_1-y_2)}{p}} = p|X||Y|.$$

La estimación en (4) aparece como ejercicio en el libro de Vinogradov [**35**] incluso en una forma más general. A pesar de que su demostración es más bien simple, la estimación de sumas bilineales se aplica en el estudio de varias congruencias aditivas. Cabe mencionar también que si los cardinales de X y Y son por lo menos del orden $p^{1/2+\epsilon}$ entonces la estimación en (4) es no trivial.

Una familia particular de sumas trigonométricas racionales son las sumas de Weyl:

$$S(Q) := \sum_{x=1}^{N} e^{2\pi i Q(x)}$$

donde $Q(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0$ es un polinomio de coeficientes racionales. Se puede suponer que $\alpha_0 = 0$ ya que el término constante no influye en la determinación del módulo de la suma. Además, si el grado de $Q(x)$ es n se dice que la suma $S(Q)$ es de grado n. Dentro de las sumas de Weyl racionales de grado 2, las sumas de la forma

$$S(a,m) := \sum_{x=1}^{N} e^{2\pi i\frac{ax^2}{m}},$$

donde $a \in \mathbb{Z}_m^*$, juegan un papel prominente. Se sabe, por ejemplo, que la sexta prueba de Gauss de la ley de reciprocidad cuadrática inicia con la introducción de la suma

$$G := \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i$$

[1]Si $(a_1,a_2,\ldots,a_n),(b_1,b_2,\ldots,b_n) \in \mathbb{R}^n$ entonces $\left(\sum_{i=1}^n a_i b_i\right)^2 \leqslant \left(\sum_{i=1}^n a_i^2\right)\left(\sum_{i=1}^n b_i^2\right)$. Haremos uso de esta desigualdad en varias puntos del presente trabajo. Notar que al momento de aplicar la desigualdad de Cauchy-Schwarz podría ser necesario considerar el caso en que $a_1 = a_2 = \ldots = a_n = 1$.

donde p es un primo impar, ζ es una raíz primitiva p-ésima de la unidad y

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p|n \\ 1 & \text{si } p \nmid n \text{ y } n \text{ es resto cuadrático módulo } p \\ -1 & \text{si } p \nmid n \text{ y } n \text{ es resto no cuadrático módulo } p \end{cases}$$

es el símbolo de Legendre.

Es importante añadir que el tratamiento de la ley de reciprocidad cuadrática por medio de sumas como las que definen a G es uno de los más susceptibles de generalización. Por el momento no damos más detalles al respecto y sólo agregamos que las sumas del tipo $\sum_{i=1}^{p-1}(\frac{i}{p})\zeta^i$ se conocen como *sumas de Gauss* (el símbolo de Legendre se puede reemplazar por cualquier carácter de Dirichlet[2] módulo p). En particular, si p es primo no es difícil mostrar, hoy en día, que $G = \pm\sqrt{p}$ si $p \equiv 1 \pmod 4$ y $G = \pm i\sqrt{p}$ si $p \equiv 3 \pmod 4$. Empero, es sabido (ver [**1**], pág. 108) que la determinación del signo correcto de G fue un problema que ocupó a Gauss por aproximadamente cuatro años. De hecho, de acuerdo con K. Ireland y M. Rosen[3]: "The conjecture that the plus sign holds in each case was made by Gauss and recorded in his diary in May 1801. It was not until four years later that he found a proof. On August 30, 1805 Gauss recorded in his diary that a proof [of] the 'very elegant theorem mentioned in 1801' had finally been achieved. He wrote to his friend W. Olbers on September 3, 1805 that seldom had a week passed for four years that he had not tried in vain to prove his conjecture. Finally according to Gauss 'Wie der Blitz einschlägt, hat sich das Räthsel gelöst...' (as lightning strikes was the puzzle solved).". Volveremos a este punto más tarde; por ahora, preferimos poner de manifiesto la relación entre la suma de Gauss G y la suma $S(a,p) = \sum_{x=1}^{p} e^{2\pi i \frac{ax^2}{p}}$ para p un primo impar y a un número natural coprimo con p.

Si x varia entre 1 y $p-1$, entonces x^2 recorre dos veces al conjunto de restos cuadráticos módulo p. Luego, al tenerse que

$$1 + \left(\frac{x}{p}\right) = \begin{cases} 2 & \text{si } x \text{ es resto cuadrático módulo } p \\ 0 & \text{si } x \text{ es resto no cuadrático módulo } p \end{cases}$$

se sigue que

$$S(a,p) = \sum_{x=1}^{p} e^{2\pi i \frac{ax^2}{p}} = 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{ax^2}{p}} = 1 + \sum_{x=1}^{p-1} \left[1 + \left(\frac{x}{p}\right)\right] e^{2\pi i \frac{ax}{p}}.$$

[2]Un carácter χ de $\mathbb{F}_p^*$ es un homomorfismo de este grupo en $\mathbb{C}^* := \mathbb{C}\backslash\{0\}$. Un carácter χ de $\mathbb{F}_p^*$ induce una función $f_\chi : \mathbb{Z} \to \mathbb{C}$ de la siguiente manera: $f_\chi(n) = 0$ siempre que $p|n$ y si $p \nmid n$ entonces $f_\chi(n) = \chi([n])$, donde $[n]$ denota la clase de congruencia módulo p a la que pertenece n. Finalmente, un carácter de Dirichlet módulo p es una función inducida por algún carácter del grupo $\mathbb{F}_p^*$.

[3]K. Ireland y M. Rosen, *A classical introduction to modern number theory* (Second Edition). Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1990, pág. 73.

Por otro lado,

$$\begin{aligned} 1+\sum_{x=1}^{p-1}\left[1+\left(\frac{x}{p}\right)\right]e^{2\pi i\frac{ax}{p}} &= \sum_{x=0}^{p-1}e^{2\pi i\frac{ax}{p}}+\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{ax}{p}} \\ &= \left(\frac{a}{p}\right)G \end{aligned}$$

y por tanto

$$S(a,p)=\left(\frac{a}{p}\right)G. \tag{5}$$

En vista de la igualdad anterior resulta razonable que en lo sucesivo se ocupe la denominación *suma de Gauss* para referirnos tanto a $S(a,p)$ como a G.

A diferencia de lo que pasa con las sumas racionales de grado 2, la identidad en (2) indica que la sumas trigonométricas racionales de grado uno se pueden determinar muy fácilmente. En cambio, el primer resultado relevante en torno a las sumas $S(a,q)$, para a y q coprimos entre sí, será la determinación de su módulo.

Proposición 1.2. *Para $q>1$ y a coprimo con q se cumple que*

$$|S(a,q)|=\begin{cases}\sqrt{q} & \text{si } q\equiv 1 \pmod 2,\\ \sqrt{2q} & \text{si } q\equiv 0 \pmod 4,\\ 0 & \text{si } q\equiv 2 \pmod 4.\end{cases}$$

Prueba. Recordemos que si z es un número complejo entonces $|z|^2 = z\cdot\overline{z}$, donde $\overline{z}$ es el conjugado de z. En particular, si $z:=\sum_{x=0}^{q-1}e^{2\pi i\frac{ax^2}{q}}$ entonces $\overline{z}=\sum_{x=0}^{q-1}e^{-2\pi i\frac{ax^2}{q}}$ y por lo tanto

$$\begin{aligned} \left|\sum_{x=0}^{q-1}e^{2\pi i\frac{ax^2}{q}}\right|^2 &= \sum_{y=0}^{q-1}e^{2\pi i\frac{-ay^2}{q}}\sum_{x=0}^{q-1}e^{2\pi i\frac{ax^2}{q}} \\ &= \sum_{y=0}^{q-1}e^{2\pi i\frac{-ay^2}{q}}\sum_{x=0}^{q-1}e^{2\pi i\frac{a(x+y)^2}{q}} \\ &= \sum_{x=0}^{q-1}e^{2\pi i\frac{ax^2}{q}}\sum_{y=0}^{q-1}e^{2\pi i\frac{2axy}{q}}. \end{aligned}$$

Si q es impar entonces, por la identidad en (2), la suma sobre y sólo es diferente de 0 cuando $x=0$. Por consiguiente, en este caso se tiene que $|S(a,q)|^2=q$. Si q es par entonces, nuevamente por la identidad en (2), la suma interior es diferente de cero cuando $q|2x$. Puesto que $x\in\{0,\ldots,q-1\}$,

la condición $q|2x$ sólo se cumple cuando $x = 0$ ó $x = \frac{q}{2}$. Así

$$|S(a,q)|^2 = (1 + e^{2\pi i \frac{aq}{4}})q = (1 + e^{\pi i \frac{q}{2}})q = \begin{cases} 2q & \text{si } q \equiv 0 \pmod 4, \\ 0 & \text{si } q \equiv 2 \pmod 4. \end{cases}$$

□

En el estudio de las sumas de Gauss $S(a,m)$, el caso principal ocurre cuando m es un número primo. Dentro de este caso, la identidad en (5) nos indica que puede suponerse además que $a = 1$.

Una generalización natural a las sumas cuadráticas de Gauss $S(a,m)$ son las sumas trigonométricas racionales

$$S_n(a,p) := \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^n}{p}}$$

donde a y p son coprimos y $n > 2$. A estas sumas nos referiremos en lo sucesivo como *sumas de Gauss de grados superiores*. A diferencia de lo que ocurre cuando $n = 2$, en los casos en que $n > 2$ no se tienen resultados simples sobre la evaluación de $S_n(1,p)$. Por ejemplo, para $n = 3$ y p un primo congruente con 1 módulo 3, se sabe que la suma $\sum_{x=1}^{p} e^{2\pi i \frac{x^3}{p}}$ es un número real (ver [**1**], pág. 114). De este hecho y de una estimación que se probará más adelante en este capítulo se sigue que

$$-2\sqrt{p} \leqslant \sum_{x=1}^{p} e^{2\pi i \frac{x^3}{p}} \leqslant 2\sqrt{p}$$

y por consiguiente

$$\sum_{x=1}^{p} e^{2\pi i \frac{x^3}{p}} = 2p^{1/2} \cos \vartheta_p$$

para algún $\vartheta_p \in [0,\pi]$. De acuerdo con el artículo de R. C. Vaughan en [**36**], cómputos efectuados por von Neumann y Goldstine y por Emma Lehmer, sugirieron en aquellos días que los ϑ_p estaban distribuidos de un modo más bien errático. La sospecha fue confirmada en 1978 por R. Heath-Brown y S. J. Patterson al demostrar que los ϑ_p están uniformemente distribuidos en $[0,\pi]$; el artículo relevante aquí es [**20**]. De esto se desprende en particular que ϑ_p toma infinitos valores distintos. En consecuencia, bajo las condiciones impuestas sobre p, se concluye que no hay una fórmula simple para $S_3(1,p)$. Por otro lado, es relativamente sencillo dar estimaciones no triviales para los módulos de las sumas $S_n(a,p)$.

Proposición 1.3. *Sea p número primo y a un entero tal que $(a,p) = 1$. Se cumple entonces que $|S_n(a,p)| \leqslant n\sqrt{p}$.*

Prueba. Tenemos por un lado que

$$\begin{aligned}\sum_{\lambda=0}^{p-1}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2 &= p\cdot|\{(x,y):0\leqslant x,y\leqslant p-1 \text{ y } x^n\equiv y^n \pmod p\}|\\ &\leqslant p^2\cdot n. \qquad (6)\end{aligned}$$

Para establecer la desigualdad se fija $Y\in\{0,\ldots,p-1\}$ y se aplica a la congruencia

$$x^n\equiv Y^n \pmod p$$

el teorema de Lagrange sobre el número de soluciones a una congruencia con módulo primo. La prueba de la igualdad es como sigue

$$\begin{aligned}\sum_{\lambda=0}^{p-1}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2 &= \sum_{\lambda=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}e^{2\pi i\frac{a\lambda(x^n-y^n)}{p}}\\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{\lambda=0}^{p-1}e^{2\pi i\frac{a\lambda(x^n-y^n)}{p}}\\ &= \sum_{\substack{0\leqslant x,y\leqslant p-1\\ x^n\equiv y^n \pmod p}}p\\ &= p\cdot|\{(x,y):x^n\equiv y^n \pmod p, 0\leqslant x,y\leqslant p-1\}|.\end{aligned}$$

Probaremos a continuación que

$$\sum_{\lambda=1}^{p-1}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2\geqslant\frac{(p-1)}{n}|S_n(a,p)|^2. \qquad (7)$$

Como

$$A:=\{\lambda:1\leqslant\lambda\leqslant p-1 \text{ y } \lambda\equiv u^n \pmod p \text{ para algún } u=u_\lambda\}$$

tiene cardinal mayor o igual a $\frac{p-1}{n}$ y para cada $u\in\{1,\ldots,p-1\}$ se cumple que

$$\sum_{x=0}^{p-1}e^{2\pi i\frac{au^nx^n}{p}}=\sum_{x=0}^{p-1}e^{2\pi i\frac{a(ux)^n}{p}}=S_n(a,p),$$

concluimos que

$$\begin{aligned}\sum_{\lambda=1}^{p-1}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2 &\geqslant \sum_{\lambda\in A}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2\\ &= \sum_{\lambda\in A}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{au_\lambda^n x^n}{p}}\right|^2\\ &= \sum_{\lambda\in A}|S_n(a,p)|^2\\ &\geqslant \frac{(p-1)}{n}|S_n(a,p)|^2\end{aligned}$$

tal como se había anunciado. De (6) y (7) se desprende que

$$\begin{aligned}p^2\cdot n &\geqslant p^2+\sum_{\lambda=1}^{p-1}\left|\sum_{x=0}^{p-1}e^{2\pi i\frac{a\lambda x^n}{p}}\right|^2\\ &\geqslant |S_n(a,p)|^2\left(1+\frac{p-1}{n}\right)\\ &\geqslant |S_n(a,p)|^2\cdot\frac{p}{n}\end{aligned}$$

y la prueba termina.

□

Sea p un número primo y $d = (n, p-1)$. Afirmamos que $S_n(a,p) = S_d(a,p)$. En efecto, si g es una raíz primitiva[4] módulo p y $d = nu + (p-1)v$, entonces

$$\begin{aligned} S_d(a,p) &= 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{a}{p} x^d} \\ &= 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{a}{p} g^{xd}} \\ &= 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{a}{p} g^{xnu + x(p-1)v}} \\ &= 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{a}{p} (g^{xu})^n} \\ &= S_n(a,p). \end{aligned}$$

Vamos a derivar ahora una mejora a la estimación en la proposición **1.3**. Denotemos con $t_n(m)$ al número de soluciones de la congruencia $x^n \equiv m \pmod{p}$. Se cumple entonces que

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^n}{p}} = \sum_{m=0}^{p-1} t_n(m) e^{2\pi i \frac{am}{p}}$$

Para obtener información sobre $t_n(m)$, sea g nuevamente una raíz primitiva módulo p. Si $m \in \{1, \ldots, p-1\}$, denotemos con μ a su índice módulo p. La ecuación $x^n \equiv m \pmod{p}$ es equivalente entonces a $n \cdot \mathrm{ind}(x) \equiv \mu \pmod{p-1}$ y por consiguiente

$$t_n(m) = \begin{cases} d & \text{si } \mu \equiv 0 \pmod{d}, \\ 0 & \text{si } d \text{ no divide a } \mu. \end{cases}$$

De acuerdo con la identidad en (2) esto último se puede escribir como

$$t_n(m) = \sum_{r=0}^{d-1} e^{2\pi i \frac{r \cdot \mathrm{ind}(m)}{d}}$$

[4]Dado un primo positivo p y $g \in \{1, 2, \ldots, p-1\}$, el pequeño teorema de Fermat asegura que $g^{p-1} \equiv 1 \pmod{p}$. Sea m el menor entero positivo tal que $g^m \equiv 1 \pmod{p}$. Si $m = p-1$ entonces se dice que g es una *raíz primitiva módulo p*. El lector familiarizado con el álgebra notará que una raíz primitiva módulo p no es más que un generador del grupo multiplicativo de $\mathbb{F}_p$. Una idea relacionada con la de raíz primitiva módulo p, es la de *índice módulo p*. Sea g una raíz primitiva módulo p. Si $m \in \{1, 2, \ldots, p-1\}$ entonces existe un único $\mu \in \{1, 2, \ldots, p-1\}$ tal que $m \equiv g^\mu \pmod{p}$. En tal situación decimos que μ es el *índice módulo p* de m (con respecto a la raíz primitiva g). Ciertamente la noción de índice módulo p puede pensarse como un análogo discreto de la función logaritmo.

y por tanto

$$\begin{aligned} S_n(a,p) &= 1+\sum_{m=1}^{p-1}\sum_{r=0}^{d-1} e^{2\pi i\frac{r\cdot \mathrm{ind}(m)}{d}} e^{2\pi i\frac{am}{p}} \\ &= 1+\sum_{r=0}^{d-1}\sum_{m=1}^{p-1} e^{2\pi i\left(\frac{r\cdot \mathrm{ind}(m)}{d}+\frac{am}{p}\right)} \\ &= \sum_{r=1}^{d-1}\sum_{m=1}^{p-1} e^{2\pi i\left(\frac{r\cdot \mathrm{ind}(m)}{d}+\frac{am}{p}\right)}. \end{aligned}$$

Luego, en vista de que

$$\begin{aligned} \left|\sum_{m=1}^{p-1} e^{2\pi i\left(\frac{r\cdot \mathrm{ind}(m)}{d}+\frac{am}{p}\right)}\right|^2 &= \sum_{m_1=1}^{p-1}\sum_{m_2=1}^{p-1} e^{2\pi i\left(\frac{r}{d}(\mathrm{ind}(m_1)-\mathrm{ind}(m_2))+\frac{a(m_1-m_2)}{p}\right)} \\ &= \sum_{m=1}^{p-1}\sum_{m_2=1}^{p-1} e^{2\pi i\left(\frac{r}{d}(\mathrm{ind}(mm_2)-\mathrm{ind}(m_2))+\frac{am_2(m-1)}{p}\right)} \\ &= \sum_{m=1}^{p-1}\sum_{m_2=1}^{p-1} e^{2\pi i\left(\frac{r}{d}\cdot \mathrm{ind}(m)+\frac{am_2(m-1)}{p}\right)} \\ &= \sum_{m=1}^{p-1}\sum_{m_2=0}^{p-1} e^{2\pi i\left(\frac{r}{d}\cdot \mathrm{ind}(m)+\frac{am_2(m-1)}{p}\right)} \\ &= p, \end{aligned}$$

concluimos que

$$|S_n(a,p)| \leqslant (d-1)\sqrt{p} \leqslant (n-1)\sqrt{p}. \tag{8}$$

Esta última estimación es no trivial cuando $n < p^{1/2}$. La obtención de estimaciones no triviales para valores grandes de n ha sido el tema central de varios trabajos. Por ejemplo, Shparlinski, utilizando resultados de [**16**], demostró en [**28**] que

$$|S_n(a,p)| \ll n^{7/12}p^{2/3}.$$

Esta estimación es no trivial cuando n es $\mathrm{o}(p^{4/7})$.

La estimación de Shparlinski fue mejorada por Heath-Brown y Konyagin en [**19**]. Ellos demostraron que

$$|S_n(a,p)| \ll \mathrm{mín}\{n^{5/8}p^{5/8}, n^{3/8}p^{3/4}\}.$$

Esta estimación es no trivial cuando n es $o(p^{2/3})$. Este resultado fue mejorado después por Konyagin en [**24**], quien obtuvo una estimación no trivial para $n \leqslant p^{3/4-\epsilon}$.

Supongamos que $n-1|p$ y consideremos el subconjunto $H := \{x^n \pmod p : 1 \leqslant x \leqslant p-1\}$ de $\mathbb{F}_p^*$. H es un subgrupo de orden $\frac{p-1}{n}$ de $\mathbb{F}_p^*$. Además, cada elemento $h \in H$ puede representarse como una potencia n-ésima de exactamente n formas. Bajo este orden de ideas, la suma de Gauss $S_n(a,p)$ puede escribirse como

$$1 + n\sum_{h\in H} e^{2\pi i\frac{ah}{p}}.$$

En consecuencia, el problema de obtener estimaciones no triviales para $S_n(a,p)$ es equivalente al problema de obtener estimaciones no triviales para la suma

$$S(a,H) := \sum_{x\in H} e^{2\pi i\frac{ax}{p}}.$$

La estimación de Konyagin implica, en particular, una estimación para $S(a,H)$ cuando $|H| > p^{1/4+\epsilon}$. Por otra parte, la suma $S(a,H)$ puede escribirse también como

$$S(a,H) = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \cdots \sum_{x_k\in H} e^{2\pi i\frac{ax_1\cdots x_k}{p}}.$$

En particular, si $k = 2$ tenemos que

$$\begin{aligned}
|S(a,H)|^2 &\leqslant \frac{1}{|H|^2}\left(\sum_{x_1\in H}\left|\sum_{x_2\in H} e^{2\pi i\frac{ax_1x_2}{p}}\right|\right)^2 \\
&\leqslant \frac{1}{|H|}\sum_{x_1\in H}\left|\sum_{x_2\in H} e^{2\pi i\frac{ax_1x_2}{p}}\right|^2 \\
&\leqslant \frac{1}{|H|}\sum_{x=0}^{p-1}\left|\sum_{x_2\in H} e^{2\pi i\frac{ax\cdot x_2}{p}}\right|^2 \\
&= \frac{1}{|H|}\sum_{x_2\in H}\sum_{x_2'\in H}\sum_{x=0}^{p-1} e^{2\pi i\frac{ax(x_2-x_2')}{p}} \\
&= p.
\end{aligned}$$

Lo anterior da una estimación trivial cuando $|H| < p^{1/2}$. Utilizando estimaciones de suma-producto para subconjuntos de $\mathbb{F}_p$ de cardinales pequeños es posible obtener estimaciones nuevas para sumas trigonométricas multilineales, las cuales pueden aplicarse a la estimación de las sumas de Gauss de grados superiores. El primer resultado de esa naturaleza fue obtenido por Bourgain, Glibichuk y Konyagin en [**5**]. Ellos probaron el siguiente teorema: *para cada $\epsilon > 0$, existe $\delta := \delta(\epsilon) > 0$ y un entero positivo $k := k(\epsilon)$ tal que si $X \subseteq F_p$ y $|X| > p^{\epsilon}$ entonces*

$$\max_{(a,p)=1}\left|\sum_{x_1\in X}\cdots\sum_{x_k\in X} e^{2\pi i\frac{ax_1\cdots x_k}{p}}\right| < |X|^k p^{-\delta}.$$

Del teorema anterior se desprende, en particular, que si a es coprimo con p y H es un subgrupo de orden $|H| > p^{\epsilon}$ del grupo multiplicativo $\mathbb{F}_p^*$, entonces existe $\delta := \delta(\epsilon) > 0$ tal que

$$|S(a,H)| < |H|^{1-\delta}.$$

Puesto que $S_n(a,p) = 1 + S(a,H)$, la desigualdad previa indica que para cualquier constante pequeña $\epsilon > 0$, la condición $n < p^{1-\epsilon}$ implica una estimación no trivial para $S_n(a,p)$.

Capítulo 2

Elementos de combinatoria aditiva

§1. La desigualdad triangular de Ruzsa. Uno de los resultados más elementales e importantes en combinatoria aditiva es la siguiente aportación de Imre Ruzsa.

Lema 2.1. *Sean G un grupo y X, Y y Z subconjuntos no vacíos y finitos de G. Se cumple entonces que*

$$|X - Z| \leqslant \frac{|X - Y||Y - Z|}{|Y|}. \tag{9}$$

Prueba. Basta con exhibir una aplicación inyectiva de $Y \times (X - Z)$ en $(X - Y) \times (Y - Z)$. Para tal fin, para cada $u \in X - Z$, fijemos una de las representaciones de u como diferencia de un elemento de X y uno de Z y denotémosla con $x(u) - z(u)$. Así, si $f : Y \times (X - Z) \to (X - Y) \times (Y - Z)$ está dada por

$$(y, u) \quad \mapsto \quad (x(u) - y, y - z(u)),$$

aseguramos que f cumple con el requerimiento deseado. En efecto, si

$$(y_\alpha, u_\alpha), (y, u) \in Y \times (X - Z)$$

son tales que $f((y, u)) = f((y_\alpha, u_\alpha))$ entonces

$$x(u) - y = x(u_\alpha) - y_\alpha \quad \text{y} \quad y - z(u) = y_\alpha - z(u_\alpha)$$

y por consiguiente

$$u = x(u) - z(u) = x(u_\alpha) - z(u_\alpha) = u_\alpha.$$

De esto se sigue a su vez que $y = y_\alpha$ y por lo tanto, $(y, u) = (y_\alpha, u_\alpha)$.

□

A la desigualdad en (9) se le conoce como desigualdad triangular de Ruzsa. Una manera de justificar tal designación es la siguiente: defínase

$$\rho(X, Y) := \log \frac{|X - Y|}{\sqrt{|X||Y|}}.$$

La desigualdad en (9) puede expresarse entonces como

$$\rho(X,Z) \leqslant \rho(X,Y) + \rho(Y,Z).$$

Esto último indica que ρ satisface lo que típicamente se conoce como desigualdad triangular. Como ρ cumple también con la propiedad de simetría, *i.e.*, $\rho(X,Y) = \rho(Y,X)$ para cada (X,Y) en el dominio de ρ, la pregunta sobre si ρ determina o no una métrica es natural. En general, la respuesta a esta cuestión es negativa pues, por ejemplo, si X y Y son singuletes distintos en un grupo G entonces

$$\rho(X,Y) = \log 1 = 0.$$

Otra desigualdad de Ruzsa de tipo *triangular* es

$$|X+Z| \leqslant \frac{|X+Y||Y+Z|}{|Y|}. \tag{10}$$

No obstante, la demostración de ésta es menos simple y no la presentaremos sino hasta el final de la sección tres de este capítulo. Por ahora, lo único que añadiremos es que, como consecuencia de la desigualdad triangular de Ruzsa en (10), se tiene que si A es un subconjunto finito y no vacío de un grupo y $|A-A| < |A|^{1+\epsilon}$, entonces $|A+A| < |A|^{1+2\epsilon}$. Lo anterior indica que los conjuntos con conjuntos de diferencias pequeños tienen también conjuntos suma pequeños. El recíproco de la afirmación anterior también es cierto.

§2. Gráficas de Plünnecke y sus propiedades.[1] Una *gráfica de nivel n* es una gráfica $G = (V,E)$, en la cual el conjunto de vértices V es la unión disjunta de conjuntos $V_0, V_1, \ldots, V_n$ y cada arista[2] $e \in E$ es un par ordenado (v,v') con $v \in V_{i-1}$ y $v' \in V_i$ para algún $i \in \{1,2,\ldots,n\}$. Un *camino* entre el vértice $v_{i-1} \in V_{i-1}$ y el vértice $v_j \in V_j$ es una sucesión de aristas de la forma $(v_{i-1},v_i),(v_i,v_{i+1}),\ldots,(v_{j-1},v_j)$. La $i-$ésima *razón de magnificación* de G se define como

$$D_i(G) := \min_{X \subseteq V_0, X \neq \varnothing} \frac{|\mathrm{im}_i(X)|}{|X|},$$

donde $\mathrm{im}_i(X)$ es el conjunto de vértices $v_i \in V_i$ en los cuales terminan los caminos que inician en vértices de X.

[1] En esta sección seguimos el capítulo siete del libro de M. B. Nathanson [**26**].

[2] Es preciso mencionar que a lo que en este trabajo nos referimos con *arista* en algunos textos se denomina *arista orientada* o *arco* (cf. G. Chartrand y L. Lesniak, *Graphs & digraphs* (Second Edition). The Wadsworth & Brooks/Cole Mathematics Series, 1986, pág. 14.). Una aclaración similar aplica también a la noción de *gráfica producto* que se introduce más adelante. Dadas dos gráficas, hay varias maneras de definir a partir de ellas una *gráfica producto* (cf. R. Hammack, W. Imrich y S. Klavžar, *Handbook of product graphs* (Second Edition). CRC Press, 2011, págs. 34-35.). Algunos autores se refieren al *producto* aquí considerado como *producto por capas*; no obstante, hemos optado en este punto por la nomenclatura en el capítulo relevante de [**26**].

Si $G = (V(G), E(G))$ y $H = (V(H), G(H))$ son gráficas de nivel n con

$$V(G) = \bigsqcup_{i=0}^{n} V_i \quad \text{y} \quad V(H) = \bigsqcup_{i=0}^{n} W_i, \tag{11}$$

entonces la gráfica producto $G \times H$ se define como sigue: el conjunto de vértices de $G \times H$ está dado por

$$V(G \times H) := (V_0 \times W_0) \sqcup (V_1 \times W_1) \sqcup \ldots \sqcup (V_n \times W_n)$$

y el conjunto de aristas por

$$E(G \times H) := \{((v, w), (v', w')) : (v, v') \in E(G), (w, w') \in E(H)\}.$$

En particular, como consecuencia directa de la definición tenemos que el producto de dos gráficas de nivel n es también gráfica de nivel n. Un dato que será relevante a la postre es la relación entre las razones de magnificación de la gráfica $G \times H$ y las razones de magnificación de G y H:

Proposición 2.2. *Si $G = (V(G), E(G))$ y $H = (V(H), G(H))$ son gráficas de nivel n entonces, para cada $i \in \{1, \ldots, n\}$, se cumple que*

$$D_i(G \times H) = D_i(G) D_i(H).$$

Prueba. Probaremos en primer lugar que $D_i(G \times H) \leqslant D_i(G) D_i(H)$. Supongamos que V_0 y W_0 son como en (11) y que $Z \subseteq V_0$ y $Z' \subseteq W_0$ son tales que

$$D_i(G) = \frac{|\mathrm{im}_i(Z)|}{|Z|} \quad \text{y} \quad D_i(H) = \frac{|\mathrm{im}_i(Z')|}{|Z'|}.$$

Como se cumple además que $\mathrm{im}_i(Z \times Z') \subseteq \mathrm{im}_i(Z) \times \mathrm{im}_i(Z')$ se sigue que

$$D_i(G \times H) \leqslant \frac{|\mathrm{im}_i(Z \times Z')|}{|Z \times Z'|} \leqslant \frac{|\mathrm{im}_i(Z)||\mathrm{im}_i(Z')|}{|Z||Z'|} = D_i(G) D_i(H).$$

Para establecer la desigualdad en el otro sentido consideremos un subconjunto X no vacío de $V_0 \times W_0$. Es claro que

$$X = \bigcup_a (\{a\} \times X_a)$$

donde X_a es el conjunto de los $b \in W_0$ tales que $(a, b) \in X$. Así, si en $\mathfrak{X}_i$ recolectamos los pares ordenados $(a, d) \in V_0 \times W_i$ tales que existen $b \in W_0$ y un camino en H entre b y d y además

$(a, b) \in X$, obtenemos que

$$\begin{aligned} |\mathfrak{X}_i| &= \left| \bigcup_a (\{a\} \times \mathrm{im}_i(X_a)) \right| \\ &= \sum_a |\mathrm{im}_i(X_a)| \\ &\geqslant D_i(H) \sum_a |X_a| \\ &= D_i(H)|X|. \end{aligned} \tag{12}$$

Por otra parte, si escribimos a $\mathfrak{X}_i$ como $\bigcup_d (Y_d \times \{d\})$, donde Y_d denota al conjunto de los $c \in V_0$ tales que $(c, d) \in \mathfrak{X}_i$, se tiene que

$$\mathrm{im}_i(X) = \bigcup_d (\mathrm{im}_i(Y_d) \times \{d\}).$$

De esto se sigue que

$$|\mathrm{im}_i(X)| = \sum_d |\mathrm{im}_i(Y_d)| \geqslant D_i(G) \sum_d |Y_d| = D_i(G)|\mathfrak{X}_i|.$$

De (12) y lo obtenido en la línea previa se desprende que

$$|\mathrm{im}_i(X)| \geqslant D_i(G)D_i(H)|X|$$

y la prueba termina.

□

Una *gráfica de Plünnecke de nivel n* es una gráfica $G = (V, E)$ de nivel n que satisface las propiedades adicionales:

A. Si $u, v, w_1, \ldots, w_k \in V$ son tales que $(u, v) \in E$ y $(v, w_j) \in E$ para cada $j \in \{1, \ldots, k\}$, entonces existen k vértices diferentes $v_1, \ldots, v_k$ tales que para cada $j \in \{1, \ldots, k\}$, $(u, v_j) \in E$ y $(v_j, w_j) \in E$.
B. Si $u_1, \ldots, u_k, v, w \in V$ son tales que $(u_j, v) \in E$ para cada $j \in \{1, \ldots, k\}$ y $(v, w) \in E$, entonces existen k vértices diferentes $v_1, \ldots, v_k$ tales que para cada $j \in \{1, \ldots, k\}$, $(u_j, v_j) \in E$ y $(v_j, w) \in E$.

Ejemplos.

1. Uno de los ejemplos más importantes de gráfica de Plünnecke son las *gráficas de adición*, las cuales se construyen como a continuación se indica. Sean A y B subconjuntos no vacíos de un

grupo abeliano (escrito aditivamente). El conjunto de vértices es

$$V := V_0 \cup V_1 \cup \ldots \cup V_n$$

donde

$$V_0 := A \times \{0\}$$

y

$$V_i := (A + iB) \times \{i\} = \{a + b_1 + \ldots + b_i : a \in A, b_j \in B\} \times \{i\}$$

y el conjunto de aristas E está conformado por los pares $(v_j, v_{j+1}) \in V_j \times V_{j+1}$ tales que si $v_j = x_j \times \{j\}$ para algún $x_j \in A + jB$ y $v_{j+1} = x_{j+1} \times \{j+1\}$ para algún $x_{j+1} \in A + (j+1)B$, entonces $x_{j+1} - x_j \in B$. Es claro que la gráfica $G := (V, E)$ es de nivel n. Afirmamos que G es también gráfica de Plünnecke. En efecto, sean

$$u, v, w_1, \ldots, w_k \in V$$

tales que $(u, v) \in E$ y $(v, w_j) \in E$ para cada $j \in \{1, \ldots, k\}$. De las definiciones se sigue que existen $i \in \{0, \ldots, n-2\}$, $x_i \in A + iB$, $x_{i+1} \in A + (i+1)B$ y $x_{i+2}^1, \ldots, x_{i+2}^k \in A + (i+2)B$ tales que

$$u = (x_i, i), \quad v = (x_{i+1}, i+1), \quad w_j = (x_{i+2}^j, i+2)$$

y $x_{i+1} - x_i = b_i \in B$ y $x_{i+2}^j - x_{i+1} = \mathfrak{b}_i^j \in B$. Así, si $v_j := (x_i + \mathfrak{b}_i^j, i+1)$ entonces $v_j \in V_{i+1}$ y tanto (u, v_j) como (v_j, w_j) pertenecen a E. Esto indica que la gráfica G satisface la propiedad A en la definición de gráfica de Plünnecke. Procediendo de manera análoga podemos mostrar que G satisface también la propiedad B. Se colige entonces que la gráfica de adición G es gráfica de Plünnecke.

Dentro de las gráficas de adición distinguimos a las *gráficas de adición independiente*: sea $n \in \mathbb{N}$ y $B := \{b_1, \ldots, b_h\} \subseteq \mathbb{N}$ que satisface la condición adicional que las $\binom{h+n-1}{n}$ sumas

$$b_{j_1} + \ldots + b_{j_n} \quad \text{con} \quad 1 \leqslant j_1 \leqslant \cdots \leqslant j_n \leqslant h$$

son distintas. Denotemos con $I_{h,n}$ a la gráfica de adición de nivel n determinada por $A := \{0\}$ y B. Se cumple entonces que $V_0 = \{0\}$, $V_i = iB$ y para cada $i \in \{1, 2, \ldots, n\}$

$$|V_i| = \binom{h+i-1}{i} = \frac{h(h+1)\cdots(h+i-1)}{i!}.$$

$I_{h,n}$ es gráfica de Plünnecke pues es un caso particular de gráfica de adición. En lo sucesivo nos referiremos a $I_{h,n}$ como gráfica de adición independiente de nivel n en h elementos.

2. Una forma de generar una nueva gráfica de Plünnecke a partir de una gráfica de Plünnecke dada es por *contracción*. Supongamos que $G := (V(G), E(G))$ es una gráfica de Plünnecke de nivel n y que $V(G) := \sqcup_{i=0}^n V_i$. Sean j y k enteros tales que $0 \leqslant j < k \leqslant n$ y X y Y subconjuntos no

vacíos de V_j y V_k, respectivamente, tales que para algún $a \in X$ y $b \in Y$ existe un camino de a a b. Si $V(X,Y)$ es el conjunto de todos los vértices de G que pertenecen a algún camino entre X y Y, hacemos

$$V_i(X,Y) := V(X,Y) \cap V_{i+j}$$

para $i \in \{0,1,\ldots,k-j\}$. (Puesto que existe un camino entre $a \in X$ y $b \in Y$, ninguno de los $V_i(X,Y)$ es vacío.) Así, si denotamos por $G(X,Y)$ a la gráfica con conjunto de vértices

$$V(X,Y) := \bigsqcup_{i=0}^{k-j} V_i(X,Y)$$

y conjunto de aristas

$$E(X,Y) := \{(v,v') \in E(G) : v,v' \in V(X,Y)\}$$

se cumple que $G(X,Y)$ es gráfica de Plünnecke de nivel $k-j$.

Otra manera de generar una gráfica de Plünnecke a partir de una dada es por *inversión*. Sea $G := (V(G),E(G))$ una gráfica de Plünnecke de nivel n. Si $V(G) := \sqcup_{i=0}^{n} V_i$, definamos $V_i^{-1} := V_{n-i}$ para cada $i \in \{0,1,\ldots,n\}$. La *gráfica inversa* G^{-1} de G es la gráfica cuyo conjunto de vértices es $V(G^{-1}) := \sqcup_{i=0}^{n} V_i^{-1}$ y cuyo conjunto de aristas $E(G^{-1})$ se determina a través de la condición siguiente: $(v,v') \in E(G^{-1})$ si y sólo si $(v',v) \in E(G)$. No es difícil convencerse que G^{-1} es una gráfica de Plünnecke de nivel n.

Finalmente, el producto de gráficas de Plünnecke de nivel n también sirve para generar otras gráficas de Plünnecke de nivel n.

□

Un resultado central en la teoría y aplicaciones de las gráficas de Plünnecke es la desigualdad de Plünnecke:

Teorema 2.3. *Sea $G = (V(G),E(G))$ una gráfica de Plünnecke de nivel n. Se cumplen entonces las siguientes desigualdades,*

$$D_1(G) \geqslant D_2(G)^{1/2} \geqslant \cdots \geqslant D_n(G)^{1/n}.$$

Antes de pasar a la prueba del teorema, veamos lo que podríamos derivar a partir de él en el caso que G es la gráfica de adición con conjunto de vértices $V = V_0 \cup V_1 \cup \ldots \cup V_n$ donde $V_0 := A \times \{0\}$ y

$$V_i := (A + iB) \times \{i\} = \{a + b_1 + \ldots + b_i : a \in A, b_j \in B\} \times \{i\}.$$

En este caso tenemos que si $X \subseteq A$ entonces

$$\begin{aligned} \mathrm{im}_i(X \times \{0\}) &= (X + iB) \times \{i\} \\ &= \{x + b_1 + \ldots + b_i : x \in X, b_j \in B\} \times \{i\}. \end{aligned}$$

De le definición de las razones de magnificación se sigue entonces

$$D_i(G) = \min_{X \subseteq A, X \neq \varnothing} \frac{|X + iB|}{|X|}.$$

Esto indica en particular que $D_i(G) \leqslant \frac{|A+iB|}{|A|}$. El teorema **2.3** implicaría entonces que para $k \geqslant i$,

$$\left(\frac{|A + iB|}{|A|}\right)^{1/i} \geqslant \left(\min_{X \subseteq A, X \neq \varnothing} \frac{|X + kB|}{|X|}\right)^{1/k}.$$

Si suponemos que para k fijo, el mínimo en la expresión de la derecha se alcanza cuando $X = X_1 \subseteq A$, obtenemos el siguiente

Corolario 2.4. *Sean A y B dos subconjuntos finitos y no vacíos de un grupo abeliano. Si i y k son números enteros fijos tales $i \leqslant k$, entonces existe un subconjunto no vacío X_1 de A tal que*

$$|X_1 + kB| \leqslant \left(\frac{|A + iB|}{|A|}\right)^{k/i} |X_1|.$$

□

En particular, puesto que $1 \leqslant |X_1| \leqslant |A|$, para $i = 1$ se sigue que

$$|kB| \leqslant \frac{|A + B|^k}{|A|^{k-1}}.$$

Para probar el teorema **2.3** requeriremos de un par de lemas:

Lema 2.5. *Sea $G = (V(G), E(G))$ un gráfica de Plünnecke de nivel n con $V = \sqcup_{i=0}^{n} V_i$. Si $D_n(G) \geqslant 1$ entonces existen $|V_0|$ caminos totalmente disjuntos por pares de V_0 a V_n.*

Prueba. La prueba depende de la siguiente consecuencia del teorema de Menger[3]: si $\mathbf{G} := (V(\mathbf{G}), E(\mathbf{G}))$ es una gráfica dirigida y $X, Y \subseteq V(\mathbf{G})$ son no vacíos y disjuntos entonces el máximo número de caminos totalmente disjuntos[4] por pares de X a Y es igual a la cardinalidad mínima que puede tener un subconjunto de $V(\mathbf{G})$ que separe[5] a X de Y.

Puesto que la tesis del aserto en cuestión es sobre el número m de caminos totalmente disjuntos por pares de V_0 a V_n lo que haremos entonces es obtener información sobre este número a través de un $S \subseteq V(G)$ de cardinalidad m que separe a V_0 de V_n. Se trata de establecer, en específico, que $m = |V_0|$.

Para $v \in V(G)$, denotemos con $i(v)$ al único entero i tal que $v \in V_i$. Sea S un subconjunto de vértices de G que separe a V_0 de V_n y tal que $|S| = m$. Claramente, S se puede escoger tal que la suma

$$\sum_{s \in S} i(s)$$

sea mínima. Afirmamos que en tal caso

$$S \subseteq V_0 \sqcup V_n. \tag{13}$$

Si suponemos que la contención no tiene lugar entonces existe $j \in [1, n-1]$ tal que $S \cap V_j \neq \varnothing$. Supongamos que

$$S \cap V_j = \{s_1, \ldots, s_q\}$$

y que los elementos restantes de S son $s_{q+1}, \ldots, s_m$. Sean $\pi_1, \ldots, \pi_m$ caminos totalmente disjuntos por pares de V_0 a V_n indexados de tal manera que para cada $i \in \{1, \ldots, m\}$, $s_i \in \pi_i$. Puesto que $0 < j < n$, se observa que para cada $i \in \{1, \ldots, q\}$, el vértice s_i tiene, sobre el camino π_i, un vértice

[3]Puesto que hay varias versiones del teorema de Menger en la literatura, es preciso hacer unas aclaraciones sobre la versión a la que nos estamos refiriendo aquí. Sean $G = (V(G), E(G))$ una gráfica dirigida y $a, b \in V(G)$ dos vértices (distintos). Sean $a = v_0, v_1, \ldots, v_k = b$ y $a = w_0, w_1, \ldots, w_l = b$ dos caminos en G del vértice a al vértice b. Se dice que estos caminos son *disjuntos* si $v_i \neq w_j$ para cada $i \in \{1, \ldots, k-1\}$ y $j \in \{1, \ldots, l-1\}$. Un subconjunto S de $V(G)$ *separa al vértice a del vértice b* si cada camino en G de a a b contiene al menos un elemento de S. El teorema de Menger asegura así que si $(a, b) \notin E(G)$ entonces el máximo número de caminos disjuntos por pares entre a y b es igual a la cardinalidad del subconjunto S de $E(G)$ más chico que separa al vértice a del vértice b y que no contiene a a o a b.

[4]Un camino de X a Y es una sucesión de vértices $v_0, v_1, \ldots, v_{k-1}$ tal que $v_0 \in X$, $v_k \in Y$ y $(v_{i-1}, v_i) \in E(G)$ para cada $i \in \{1, \ldots, k\}$. Se dice que dos caminos $v_0, v_1, \ldots, v_k$ y $w_0, w_1, \ldots, w_j$ son *totalmente disjuntos* si $v_i \neq w_j$ para cada $i \in \{0, 1, \ldots, k\}$ y $j \in \{0, 1, \ldots, l\}$.

[5]Un conjunto S de vértices *separa al conjunto X* del conjunto Y si cada camino de X a Y contiene al menos un elemento de S.

predecesor $r_i \in V_{j-1}$ y un vértice sucesor $t_i \in V_{j+1}$. De la minimalidad de la suma $\sum_{s\in S} i(s)$ se sigue que el conjunto de vértices

$$S^* = \{r_1, \ldots, r_q, s_{q+1}, \ldots s_m\}$$

no separa a V_0 de V_n y por ende, existe un camino π^* de V_0 a V_n que no pasa por ningún punto de S^*. Sin embargo, puesto que π^* tiene exactamente un vértice sobre S, existe $i \in \{1, \ldots, q\}$ tal que $s_i \in \pi^*$; supongamos que $i = 1$. Es claro que si r^* es el vértice predecesor de s_1 sobre el camino π^* entonces $r^* \notin \{r_1, \ldots, r_q\}$.

Consideremos ahora los siguientes conjuntos de vértices de G:

$$\begin{aligned} S_q^- &:= \{r_1, \ldots, r_q\} \subseteq V_{j-1}, \\ S_q^* &:= \{r^*, r_1, \ldots, r_q\} \subseteq V_{j-1} \\ S_q &:= \{s_1, \ldots, s_q\} \subseteq V_j, \\ S_q^+ &:= \{t_1, \ldots, t_q\} \subseteq V_{j+1}. \end{aligned}$$

Sabemos que la gráfica $G^* := G(S_q^*, S_q^+)$ es gráfica de Plünnecke de nivel 2. Supongamos que $V(G^*) = V_0^* \sqcup V_1^* \sqcup V_2^*$. Como los vértices r_i, s_i y t_i son contiguos sobre el camino π_i (para cada $i \in \{1, \ldots, q\}$) y los vértices r^*, s_1, t_1 son contiguos sobre el camino π^*, se obtiene que

$$V_2^* = S_q^+, \quad V_1^* \supseteq S_q \quad \text{y} \quad V_0^* = S_q^*.$$

Afirmamos ahora que

$$V_1^* = S_q, \tag{14}$$

esto es, que cada camino sobre G de $S_q^* = \{r^*, r_1, \ldots, r_q\}$ a $S_q^+ = \{t_1, \ldots, t_q\}$ pasa por algún punto de S_q. Supongamos que el camino γ sale de r_i y llega a t_j. Si el vértice intermedio es $s^* \notin \{s_1, \ldots, s_q\}$ entonces hemos dado con un camino sobre la gráfica original G que no pasa por ningún vértice de S: se recorre π_i hasta r_i, después, por el camino γ, se pasa de r_i a s^* y de s^* a t_j; finalmente, se recorre π_j desde t_j hasta el vértice correspondiente en V_n. En el caso que el camino γ principie en r^* y finalice en t_j se procede de manera análoga: se recorre π^* hasta r^*, después, por el camino γ, se pasa de r^* a s^* y de s^* a t_j; finalmente, se recorre π_j desde t_j hasta el vértice correspondiente en V_n. Puesto que $s_i \notin \ pi^*$ para $i \neq 1$, el supuesto $s^* \notin \{s_1, \ldots, s_q\}$ indica que en este caso el camino resultante sobre la gráfica original G también evita a S. En sendos casos, la contradicción obtenida implica que la igualdad en (14) es cierta.

Estamos a punto de terminar la prueba de (13). Denotemos por $d^+(a, G^*)$ al número de vértices $v \in V(G^*)$ tales que $(a, v) \in E(G)$ y por $d^-(a, G^*)$ al número de vértices $v \in V(G^*)$ tales que

$(v,a) \in E(G)$. Dado que (r_i, s_i) y (s_i, t_i) son aristas en la gráfica G^*, la cual es una gráfica de Plünnecke, se tiene que

$$d^+(r_i, G^*) \geqslant d^+(s_i, G^*)$$

y

$$d^-(t_i, G^*) \geqslant d^-(s_i, G^*).$$

Además, puesto que el número de aristas que salen de V_0^* es igual al número de aristas que entran a V_1^* y el número de aristas que salen de V_1^* es igual al número de aristas que entran en V_2^* se desprende que

$$\begin{aligned}
\sum_{i=1}^{q} d^+(r_i, G^*) &\geqslant \sum_{i=1}^{q} d^+(s_i, G^*) \\
&= \sum_{i=1}^{q} d^-(t_i, G^*) \\
&\geqslant \sum_{i=1}^{q} d^-(s_i, G^*) \\
&= d^+(r^*, G^*) + \sum_{i=1}^{q} d^+(r_i, G^*) \\
&\geqslant 1 + \sum_{i=1}^{q} d^+(r_i, G^*),
\end{aligned}$$

lo cual es decididamente absurdo y (13) se sigue.

Mostraremos ahora que lo hecho previamente implica que $|S| = |V_0|$. En efecto, puesto que $|S|$ es igual al máximo número de caminos totalmente disjuntos por pares de V_0 a V_n entonces $|S| \leqslant |V_0|$. Luego, si $V_0 \subseteq S$ entonces $|V_0| \leqslant |S|$ y por consiguiente, $|S| = |V_0|$. En otro caso, $V_0 \backslash S$ es no vacío y al ser S un subconjunto de vértices que separa a V_0 de V_n se sigue que cada camino de G que inicie en $V_0 \backslash S$ debe terminar en $V_n \cap S$. Así

$$1 \leqslant D_n(G) \leqslant \frac{|\mathrm{im}_n(V_0 \backslash S)|}{|V_0 \backslash S|} \leqslant \frac{|V_n \cap S|}{|V_0 \backslash S|}$$

y

$$|S| = |V_0 \cap S| + |V_n \cap S| \geqslant |V_0 \cap S| + |V_0 \backslash S| = |V_0|,$$

de donde se desprende nuevamente que $|S| = |V_0|$.

□

Lema 2.6. *Sea $G = (V(G), E(G))$ una gráfica de Plünnecke de nivel $n \geqslant 2$. Si $D_n(G) \geqslant 1$ entonces $D_i(G) \geqslant 1$ para cada $i \in \{1, \ldots, n\}$.*

Prueba. Sea Z un subconjunto no vacío de V_0 fijo (pero arbitrario). Puesto que $D_n(G) \geqslant 1$, el lema **2.5** asegura la existencia de $|V_0|$ caminos disjuntos de V_0 a V_n. Por consiguiente, hay $|Z|$ caminos disjuntos que emanan de $|Z|$ y

$$|Z| \leqslant |\mathrm{im}_i(Z)|.$$

A su vez esto implica que,

$$D_i(G) = \min_{Z \subseteq A, Z \neq \emptyset} \frac{|\mathrm{im}_i(Z)|}{|Z|} \geqslant 1.$$

□

Prueba del teorema 2.3. Basta con demostrar que para $n \geqslant 2$ fijo (pero arbitrario) y para cada $i \in \{1, \ldots, n\}$, $D_i(G) \geqslant D_n(G)^{i/n}$. En efecto: esta desigualdad implica en particular que $D_{n-1}(G) \geqslant D_n(G)^{(n-1)/n}$; luego, si $n - 1 \geqslant 2$, la desigualdad puede aplicarse a la gráfica de Plünnecke de nivel $n - 1$, G_1, que se obtiene a partir de G al eliminar el conjunto de vértices V_n y las aristas que llegan a un vértice de V_n, y obtendríamos que $D_{n-2}(G) = D_{n-2}(G_1) \geqslant D_{n-1}(G_1)^{(n-2)/(n-1)} = D_{n-1}(G)^{(n-2)/(n-1)}$. Si de G_1 removemos el conjunto de vértices V_{n-1} y las aristas que llegan a un vértice de V_{n-1} obtenemos una gráfica de Plünnecke de nivel $n-2$, G_2, sobre la que se puede volver a aplicar la desigualdad puesta a consideración en un principio (siempre que $n-2 \geqslant 2$). Repitiendo el proceso anterior, tantas veces como sea necesario, se llega en un momento a $D_2(G) \geqslant D_3^{2/3}(G)$ y $D_1(G) \geqslant D_2^{1/2}(G)$.

Dicho lo anterior, distinguimos entre cuatro posibles casos para el número $D_n(G)$: $D_n(G) = 1$, $D_n(G) = 0$, $D_n(G) \in (0, 1)$ ó $D_n(G) > 1$.

Si $D_n(G) = 1$ entonces el lema **2.6** implica que $D_i(G) \geqslant 1 = D_n^{i/n}(G)$. Si $D_n(G) = 0$, el resultado es obvio.

Supongamos que $0 < D_n(G) < 1$. Si $r \in \mathbb{N}$ y $m = 1 + \lfloor (n! D_n(G)^{-r})^{1/n} \rfloor$ se sigue que

$$D_n(G)^r m^n \geqslant n!.$$

Si denotamos con G^r al producto de r copias de la gráfica G e $I_{m,n}$ es la gráfica de adición introducida al final del ejemplo **1**, tenemos que $G^r \times I_{m,n}$ es una gráfica de Plünnecke de nivel n y por lo tanto

$$D_n(G^r \times I_{m,n}) = D_n(G)^r D_n(I_{m,n}) \geqslant \frac{D_n(G)^r m^n}{n!} \geqslant 1.$$

El lema **2.6** nos garantiza entonces que

$$1 \leqslant D_i(G^r \times I_{m,n}) = D_i(G)^r m^i$$

y por tanto

$$m^{-i/r} \leqslant D_i(G).$$

Como $D_n(G) \in (0,1)$, se tiene que

$$(n!D_n(G)^{-r})^{1/n} \leqslant m \leqslant 1 + (n!D_n(G)^{-r})^{1/n} \leqslant 2(n!D_n(G)^{-r})^{1/n}$$

y por consiguiente,

$$\begin{aligned} D_i(G) &\geqslant m^{-i/r} \\ &\geqslant (2(n!D_n(G)^{-r})^{1/n})^{-i/r} \\ &= (2(n!)^{1/n})^{-i/r} D_n(G)^{i/n}. \end{aligned} \tag{15}$$

Puesto que la desigualdad en (15) vale para cada $r \geqslant 1$ y

$$\lim_{r\to\infty} (2(n!)^{1/n})^{-i/r} = 1,$$

concluimos que $D_i(G) \geqslant D_n(G)^{i/n}$ para cada $i \in \{1,\ldots,n\}$.

Consideremos ahora el caso $D_n(G) > 1$. Sea r un entero positivo tal que

$$m := \lfloor D_n(G)^{r/n} \rfloor > 1.$$

Se tiene entonces que

$$2 \leqslant m \leqslant D_n(G)^{r/n} < m+1 < 2m$$

y

$$D_n(G)^r m^{-n} \geqslant 1.$$

Sea $I_{m,n}^{-1}$ la gráfica inversa de $I_{m,n}$. Sus razones de magnificación satisfacen las condiciones

$$D_n(I_{m,n}^{-1}) = |nB|^{-1} = \binom{m+n-1}{n-1}^{-1} \geqslant m^{-n}$$

y

$$D_i(I_{m,n}^{-1}) \leqslant \frac{|(n-i)B|}{|nB|} \leqslant \frac{m^{n-i}}{m^n/n!} = n!m^{-i}.$$

Como en el caso anterior, de

$$D_n(G^r \times I_{m,n}^{-1}) = D_n(G)^r D_n(I_{m,n}^{-1}) \geqslant D_n(G)^r m^{-n} \geqslant 1$$

y el lema **2.6** se obtiene que

$$1 \leqslant D_i(G^r \times I_{m,n}^{-1}) = D_i(G)^r n! m^{-i}.$$

De esto se desprende que

$$\begin{aligned} D_i(G) &\geqslant (n!)^{-1/r} m^{i/r} \\ &> (n!)^{-1/r} \left(\frac{D_n(G)^{r/n}}{2} \right)^{i/r} \\ &= (2^i n!)^{-1/r} D_n(G)^{i/n} \end{aligned}$$

Dado que la desigualdad resultante vale para cada r suficientemente grande, se concluye que $D_i(G) \geqslant D_n(G)^{i/n}$ para cada $i \in \{1, \ldots, n\}$.

□

§3. La desigualdad de Ruzsa-Plünnecke. Una consecuencia notable de la desigualdad de Plünnecke es el siguiente hecho:

Sea $\mathcal{A}$ un subconjunto no vacío de un grupo abeliano. Supongamos que $|\mathcal{A} + \mathcal{A}| \leqslant C|\mathcal{A}|$. Se tiene entonces que $|j\mathcal{A} - \ell\mathcal{A}| \leqslant C^{j+\ell}|\mathcal{A}|$ para cada $(j, \ell) \in \mathbb{N} \times \mathbb{N}$.

Su demostración es sencilla. Sin pérdida de generalidad podemos suponer que $\ell \geqslant j$. Luego, si hacemos $i = 1$, $k = j$ y $A = B = \mathcal{A}$ y apelamos al corolario **2.4**, se obtiene $A' \subseteq \mathcal{A}$ tal que

$$|A' + j\mathcal{A}| \leqslant \left(\frac{|\mathcal{A} + \mathcal{A}|}{|\mathcal{A}|} \right)^j |A'| \leqslant C^j |A'|. \tag{16}$$

Si volvemos a aplicar el corolario **2.4**, pero ahora con las asignaciones $i = j$, $k = \ell$, $A = A'$ y $B = \mathcal{A}$ y atendiendo a lo que aparece en (16), se obtiene $A'' \subseteq A'$ tal que

$$|A'' + \ell\mathcal{A}| \leqslant \left(\frac{|A' + j\mathcal{A}|}{|A'|} \right)^{\frac{\ell}{j}} |A''| \leqslant C^\ell |A''|. \tag{17}$$

De (16), (17) y la desigualdad triangular de Ruzsa se concluye entonces que

$$\begin{aligned} |A''||j\mathcal{A} - \ell\mathcal{A}| &\leqslant |A'' + j\mathcal{A}||A'' + \ell\mathcal{A}| \\ &\leqslant |A' + j\mathcal{A}||A'' + \ell\mathcal{A}| \\ &\leqslant C^{j+\ell}|A'||A''| \\ &\leqslant C^{j+\ell}|\mathcal{A}||A''|. \end{aligned}$$

Cabe mencionar que en 2011 Giorgis Petridis dio con una manera de obtener el resultado anterior sin apelar a la desigualdad de Plünnecke (para más detalles sobre este asunto, consúltese la entrada de título *A new way of proving sumset estimates* en la bitácora en internet de Tim Gowers).

La siguiente versión del corolario **2.4** fue demostrada por Ruzsa en [**27**]. La presentamos ahora pues la utilizaremos ampliamente en lo sucesivo.

Lema 2.7. *Sean $X, B_1, \ldots, B_k$ subconjuntos finitos y no vacíos de un grupo abeliano. Supongamos que $|X| = n$ y que para $i \in \{1, \ldots, k\}$, $|X + B_i| = \alpha_i n$. Existe entonces $X_1 \subseteq X$ tal que*

$$|X_1 + B_1 + \ldots + B_k| \ll \alpha_1 \cdots \alpha_k |X_1|.$$

donde la constante implicada depende de k.

Prueba. Sea R un grupo abeliano que contiene a los conjuntos $X, B_1, \ldots, B_k$. Elíjase

$$M > 10k(|X + B_1| + \ldots + |X + B_k|)$$

y para $j \in \{1, \ldots, k\}$, defínase

$$n_j := \left\lfloor \frac{M}{|X + B_j|} \right\rfloor.$$

Supongamos que para $1 \leqslant i \leqslant k$ y $1 \leqslant j \leqslant n_i$, los enteros m_{ij} son distintos por pares de tal manera que las sumas

$$m_{1j_1} + m_{2j_2} + \ldots + m_{kj_k}$$

son también distintas por pares. Definamos a continuación los conjuntos

$$B_{ij} := B_i \times \{m_{ij}\}, \quad 1 \leqslant i \leqslant k, \quad 1 \leqslant j \leqslant n_i.$$

Claramente, los conjuntos así definidos son disjuntos por pares. Luego, si

$$Y := B_{11} \cup \ldots B_{1n_1} \cup B_{21} \cup \ldots \cup B_{2n_2} \cup \ldots \cup B_{k1} \cup \ldots \cup B_{kn_k},$$

al aplicar el corolario **2.4**, con $i = 1$, a los conjuntos $X \times \{0\}$ y Y, obtenemos un subconjunto $X_1 \times \{0\}$ de $X \times \{0\}$ tal que

$$|X_1 \times \{0\} + kY| \leqslant \frac{|X \times \{0\} + Y|^k}{|X|^k} |X_1|. \tag{18}$$

Por otro lado, de la elección de los enteros m_{ij} se sigue que a distintos vectores $(j_1, \ldots, j_k)$ corresponden distintos conjuntos

$$X_1 \times \{0\} + B_{1j_1} + \ldots + B_{kj_k}.$$

El número de conjuntos de esta forma es entonces

$$n_1 \cdots n_k \geqslant \frac{M^k}{2^k |X + B_1| \ldots |X + B_k|}.$$

Por otro lado, como $|X_1\times\{0\}+B_{1j_1}+\ldots+B_{kj_k}| = |X_1+B_1+\ldots+B_k|$ y cada $X_1\times\{0\}+B_{1j_1}+\ldots+B_{kj_k}$ está contenido en $X_1 \times \{0\} + kY$,

$$\frac{M^k}{2^k|X+B_1|\cdots|X+B_k|}|X_1 + B_1 + \ldots + B_k| \quad \leqslant \quad |X_1 \times \{0\} + kY|. \tag{19}$$

Así, de (18) y (19) y $|X \times \{0\} + Y| \leqslant n_1|X + B_1| + \ldots + n_k|X + B_k| \leqslant kM$ se desprende que

$$\frac{M^k}{2^k|X+B_1|\cdots|X+B_k|}|X_1 + B_1 + \ldots + B_k| \leqslant \left(\frac{kM}{|X|}\right)^k |X_1|.$$

Ergo,

$$|X_1 + B_1 + \ldots + B_k| \leqslant (2k)^k\alpha_1\cdots\alpha_k|X_1|$$

y la prueba culmina.

□

Corolario 2.8. *Sean $X, B_1, \ldots, B_k$ subconjuntos no vacíos y finitos de un grupo abeliano. Se tiene entonces que*

$$|B_1 + \ldots + B_k| \ll \frac{|X + B_1|\cdots|X + B_K|}{|X|^{k-1}}.$$

Prueba. Por el lema recién demostrado, existe $X_1 \subseteq X$ tal que

$$\begin{aligned} |X_1 + B_1 + \ldots + B_k| &\ll \frac{|X + B_1|\cdots|X + B_k|}{|X|^k}|X_1| \\ &= \frac{|X + B_1|\cdots|X + B_k|}{|X|^{k-1}} \cdot \frac{|X_1|}{|X|} \\ &\leqslant \frac{|X + B_1|\cdots|X + B_k|}{|X|^{k-1}}. \end{aligned}$$

El resultado se sigue ahora al notar que $|B_1 + \ldots + B_k| \leqslant |X_1 + B_1 + \ldots + B_k|$.

□

§4. Estimaciones del tipo Balog-Szemerédi-Gowers. Sean $(G, +)$ un grupo, A y B subconjuntos finitos de G y E un subconjunto de $A \times B$. Definamos

$$A \underset{\text{E}}{+} B := \{a + b : (a, b) \in E\} \quad \text{y} \quad A \underset{\text{E}}{-} B := \{a - b : (a, b) \in E\}.$$

La idea básica detrás de las estimaciones del tipo Balog-Szemerédi-Gowers es la siguiente: si A y B tienen cardinales comparables, E es un subconjunto *grande* de $A \times B$ mientras que $A \underset{\text{E}}{+} B$ es *pequeño*, entonces existen subconjuntos *grandes* $A' \subseteq A$ y $B' \subseteq B$ tales que $A' + B'$ es *pequeño*.

En la literatura pueden encontrarse varias estimaciones del tipo Balog-Szemerédi-Gowers. Una de las versiones particularmente convenientes para la estimación de sumas trigonométricas es la propuesta por Bourgain y Garaev en [**4**]:

Proposición 2.9. *Sean A y B subconjuntos finitos de un grupo abeliano (escrito aditivamente). Supongamos que $E \subseteq A \times B$ es tal que $|E| \geqslant |A||B|/K$. Existe entonces $A' \subseteq A$ tal que $|A'| \geqslant 0.1|A|/K$ y*

$$|A \underset{\mathrm{E}}{+} B|^4 \geqslant \frac{|A'-A'||A||B|^2}{10^4K^5} \quad \text{y} \quad |A \underset{\mathrm{E}}{-} B|^4 \geqslant \frac{|A'-A'||A||B|^2}{10^4K^5}.$$

Dado $a \in A$, denotemos con $N(a)$ al conjunto de los $b \in B$ tales que $(a,b) \in E$. Análogamente, dado $b \in B$, denotemos con $N_1(b)$ al conjunto de los $a \in A$ tales que $(a,b) \in E$. En particular, si $b \in N(a)$ entonces $a+b \in A \underset{\mathrm{E}}{+} B$ y $a-b \in A \underset{\mathrm{E}}{-} B$. Para lo que sigue será de ayuda tener en mente que

i) $a \in N_1(b)$ si y sólo si $b \in N(a)$.
ii) $N(a_1) \cap N(a_2) = \{b \in B : a_1 \in N_1(b), a_2 \in N_1(b)\}$.
iii) $\sum_{a\in A} |N(a)| = \sum_{b\in B} |N_1(b)| = |E|$.

La prueba de la proposición **2.9** se basa en el siguiente

Lema 2.10. *Supongamos que para $K \geqslant 1$, existe $E \subseteq A \times B$ tal que $|E| \geqslant |A||B|/K$. Entonces, para cada $\epsilon \in (0,1)$, existe $A' \subseteq A$ de cardinalidad mayor o igual a $|A|/\sqrt{2K}$ tal que la estimación*

$$|N(a_1') \cap N(a_2')| \geqslant \frac{\epsilon}{2K^2}|B|$$

se cumple para al menos $(1-\epsilon)|A'|^2$ elementos de $A' \times A'$.

Prueba. Hagamos

$$\Omega := \left\{(a_1,a_2) \in A \times A : |N(a_1) \cap N(a_2)| < \frac{\epsilon}{2K^2}|B|\right\}.$$

Puesto que

$$\begin{aligned}
\sum_{b\in B} \sum_{\substack{(a_1,a_2)\in\Omega \\ a_1,a_2\in N_1(b)}} 1 &= \sum_{b\in B} \sum_{\substack{(a_1,a_2)\in\Omega \\ b\in N(a_1)\cap N(a_2)}} 1 \\
&= \sum_{(a_1,a_2)\in\Omega} \sum_{\substack{b\in B \\ b\in N(a_1)\cap N(a_2)}} 1 \\
&= \sum_{(a_1,a_2)\in\Omega} |N(a_1) \cap N(a_2)|,
\end{aligned}$$

la desigualdad de Cauchy-Schwarz indica que

$$\begin{aligned}\sum_{b\in B}\left(|N_1(b)|^2-\frac{1}{\epsilon}\sum_{\substack{(a_1,a_2)\in\Omega\\ a_1,a_2\in N_1(b)}}1\right) &\geqslant \frac{1}{|B|}\left(\sum_{b\in B}|N_1(b)|\right)^2\\ &- \frac{1}{\epsilon}\sum_{(a_1,a_2)\in\Omega}|N(a_1)\cap N(a_2)|\\ &\geqslant \frac{|A|^2|B|}{K^2}-\frac{|\Omega||B|}{2K^2}\\ &\geqslant \frac{|A|^2|B|}{2K^2}.\end{aligned}$$

Luego, si

$$|N_1(b)|^2-\frac{1}{\epsilon}\sum_{\substack{(a_1,a_2)\in\Omega\\ a_1,a_2\in N_1(b)}}1$$

alcanza su valor máximo en $b=b_0$ entonces

$$\left(|N_1(b_0)|^2-\frac{1}{\epsilon}\sum_{\substack{(a_1,a_2)\in\Omega\\ a_1,a_2\in N_1(b_0)}}1\right)\geqslant\frac{|A|^2}{2K^2}.$$

Para obtener el resultado en cuestión basta con hacer $A'=N_1(b_0)$. De la última desigualdad se sigue de inmediato que $|A'|\geqslant|A|/\sqrt{2}K$. Para probar la otra parte, notamos que de

$$\begin{aligned}|A'|^2 &\geqslant \frac{|A|^2}{2K^2}+\frac{1}{\epsilon}\sum_{\substack{(a_1,a_2)\in\Omega\\ a_1,a_2\in A'}}1\\ &\geqslant \frac{1}{\epsilon}\sum_{\substack{(a_1',a_2')\in A'\times A'\\ |N(a_1')\cap N(a_2')|<\frac{\epsilon}{2K^2}|B|}}1\end{aligned}$$

se desprende que la estimación

$$|N(a_1')\cap N(a_2')|\geqslant\frac{\epsilon}{2K^2}|B|$$

tiene que cumplirse para al menos

$$(1-\epsilon)|A'|^2$$

elementos de $A' \times A'$ pues, en caso contrario, sería

$$\begin{aligned} |A'|^2 &= \sum_{\substack{(a_1',a_2')\in A'\times A' \\ |N(a_1')\cap N(a_2')|<\frac{\epsilon}{2K^2}|B|}} 1 + \sum_{\substack{(a_1',a_2')\in A'\times A' \\ |N(a_1')\cap N(a_2')|\geqslant\frac{\epsilon}{2K^2}|B|}} 1 \\ &< \epsilon|A'|^2 + (1-\epsilon)|A'|^2 \\ &= |A'|^2. \end{aligned}$$

□

Prueba de la proposición 2.9. Diremos que un par $(a_1, a_2) \in A \times A$ es *bueno* si

$$|N(a_1) \cap N(a_2)| \geqslant 0.05\frac{|B|}{K^2}.$$

Tomemos $\epsilon = 0.1$. De acuerdo con el lema **2.10**, existe $A' \subseteq A$ cuya cardinalidad es mayor o igual a $|A|/\sqrt{2}K$ y tal que $A' \times A'$ contiene al menos $0.9|A'|^2$ pares buenos. Ahora bien, para un $a_1' \in A'$, denotemos con $I_{a_1'}$ al conjunto de elementos $a_2' \in A'$ tales que (a_1', a_2') es un par bueno. Se cumple entonces que

$$\sum_{a'\in A'} |I_{a'}| \geqslant 0.9|A'|^2.$$

Sea A'' el conjunto de los $a'' \in A'$ tales que

$$|I_{a''}| > 0.7|A'|.$$

Así, puesto que

$$0.9|A'|^2 \leqslant \sum_{a'\in A'} |I_{a'}| = \sum_{a\in A''} |I_a| + \sum_{a\in A'-A''} |I_a| \leqslant |A''||A'| + 0.7|A'|^2$$

se colige que $|A''| \geqslant 0.2|A'| \geqslant 0.1|A|/K$. Es suficiente con mostrar ahora que

$$|A \underset{\text{E}}{+} B|^4 \geqslant \frac{|A''-A''||A||B|^2}{10^4K^5} \quad \text{y} \quad |A \underset{\text{E}}{-} B|^4 \geqslant \frac{|A''-A''||A||B|^2}{10^4K^5}.$$

Puesto que para cada par $(a_1'', a_2'') \in A'' \times A''$, los conjuntos $I_{a_1''}$ y $I_{a_2''}$ son subconjuntos de A' con cardinalidad mayor que $0.7|A'|$, el principio de inclusión-exclusión garantiza que

$$|I_{a_1''} \cap I_{a_2''}| \geqslant 0.4|A'| \geqslant 0.1\frac{|A|}{K}.$$

Se tiene también que si $a \in I_{a_1''} \cap I_{a_2''}$, entonces tanto (a, a_1'') como (a, a_2'') son buenos. Por lo tanto,

$$|N(a) \cap N(a_1'')| \geqslant 0.05\frac{|B|}{K^2}, \quad |N(a) \cap N(a_2'')| \geqslant 0.05\frac{|B|}{K^2}.$$

Así, puesto que la identidad

$$a_1'' - a_2'' = (a_1'' + b_1) - (a + b_1) + (a + b_2) - (a_2'' + b_2) \tag{20}$$

vale para cada

$$a \in I_{a_1''} \cap I_{a_2''}, \quad b_1 \in N(a) \cap N(a_1''), \quad b_2 \in N(a) \cap N(a_2'').$$

se sigue que cada elemento de $A'' - A''$ tiene al menos

$$\frac{|A|}{10K} \cdot \frac{5|B|}{(10K)^2} \cdot \frac{5|B|}{(10K)^2}$$

representaciones diferentes de la forma $d_1 - d_2 + d_3 - d_4$, donde $d_i \in A \underset{\text{E}}{+} B$. Como el número de vectores del tipo (d_1, d_2, d_3, d_4) no puede ser mayor que $|A \underset{\text{E}}{+} B|^4$, se concluye que

$$|A \underset{\text{E}}{+} B|^4 \geqslant \frac{|A'' - A''||A||B|^2}{10^4 K^5}.$$

La estimación

$$|A \underset{\text{E}}{-} B|^4 \geqslant \frac{|A'' - A''||A||B|^2}{10^4 K^5}.$$

se obtiene procediendo de manera análoga pero partiendo en cambio de la identidad

$$a_1'' - a_2'' = (a_1'' - b_1) - (a - b_1) + (a - b_2) - (a_2'' - b_2).$$

□

§5. Energías aditiva y multiplicativa. Si $(\mathfrak{G}, +)$ es un grupo y X y Y son subconjuntos de $\mathfrak{G}$, la *energía aditiva* de los conjuntos X y Y se define como

$$E_+(X, Y) := |\{(x_1, x_2, y_1, y_2) \in X^2 \times Y^2 : x_1 + y_1 = x_2 + y_2\}|.$$

Si $(\mathfrak{G}, \cdot)$ es un grupo y X y Y son subconjuntos de $\mathfrak{G}$, la *energía multiplicativa* de X y Y se define de manera similar

$$E_\times(X, Y) = |\{(x_1, x_2, y_1, y_2) \in X^2 \times Y^2 : x_1 \cdot y_1 = x_2 \cdot y_2\}|.$$

Utilizando la desigualdad de Cauchy-Schwarz puede deducirse que

$$|X + Y| \geqslant \frac{|X|^2|Y^2|}{E_+(X, Y)} \quad \text{y} \quad |XY| \geqslant \frac{|X|^2|Y|^2}{E_\times(X, Y)}.$$

En efecto, si denotamos con $I(\lambda)$ al número de soluciones de la ecuación

$$x + y = \lambda, \quad x \in X, \quad y \in Y$$

entonces de

$$\{(x_1, x_2, y_1, y_2) \in X^2 \times Y^2 : x_1 + y_1 = x_2 + y_2\} = \bigsqcup_{\lambda \in X+Y} \{(x, u, y, v) \in X^2 \times Y^2 : x + y = \lambda = u + v\}$$

se desprende que

$$\begin{aligned} E_+(X,Y) &= \sum_{\lambda\in X+Y} I^2(\lambda) \\ &\geqslant \frac{1}{|X+Y|}\left(\sum_{\lambda\in X+Y} I(\lambda)\right)^2 \\ &= \frac{|X|^2|Y|^2}{|X+Y|}. \end{aligned}$$

La estimación inferior para $|XY|$ se obtiene procediendo de modo análogo.

Lema 2.11. *Sean X, Y subconjuntos de $\mathbb{F}_p$. Existe entonces $z \in \mathbb{F}_p$ tal que*

$$|X + zY| \geqslant \frac{1}{2}\,\mín\{|X||Y|, p\}.$$

Prueba. Podemos suponer, sin pérdida de generalidad, que $|Y| \geqslant 2$. Sea I el número de soluciones de la ecuación

$$x_1 + zy_1 = x_2 + zy_2, \quad x_1, x_2 \in X, \quad y_1, y_2 \in Y, \quad z \in \mathbb{F}_p.$$

Si $y_1 = y_2$ entonces $x_1 = x_2$. En este caso obtenemos a lo más $p|X||Y|$ soluciones. Si $y_1 \neq y_2$ entonces cada vector (x_1, x_2, y_1, y_2) determina de manera única al correspondiente z. Por consiguiente,

$$I \leqslant p|X||Y| + |X|^2|Y|^2.$$

En consecuencia, existe $z \in \mathbb{F}_p$ tal que el número de soluciones a la ecuación

$$x_1 + zy_1 = x_2 + zy_2, \quad x_1, x_2 \in X, \quad y_1, y_2 \in Y,$$

es menor o igual a $|X||Y| + |X|^2|Y|^2p^{-1}$.

Si $z = 0$ entonces esta última ecuación tiene $|X||Y|^2$ soluciones. Como $|Y| \geqslant 2$, se sigue que $|X| \geqslant p/2$ y el aserto se tendría. En otro caso, el resultado es consecuencia del hecho que

$$E_+(X, zY) \leqslant |X||Y| + \frac{|X|^2|Y|^2}{p}$$

y de la desigualdad $E_+(X, zY) \geqslant |X|^2|Y|^2/|X + zY|$.

□

El resultado que sigue es consecuencia del artículo [**17**] de Glibichuk y Konyagin.

Lema 2.12. *Sea $A_1 \subseteq \mathbb{F}_p$. Existen $b_1, b_2, b_3, b_4 \in A_1$ tales que*

$$|(b_1 - b_2)A_1 + (b_3 - b_4)A_1 + (b_3 - b_4)A_1| \gg |A_1|^2$$

ó

$$|(b_1 - b_2)A_1 + (b_3 - b_4)A_1| \gg p.$$

Prueba. Podemos suponer que $|A_1| > 1$. Sea

$$\frac{A_1 - A_1}{A_1 - A_1} := \left\{ \frac{a_1 - a_2}{a_3 - a_4} : a_1, a_2, a_3, a_4 \in A_1, a_3 \neq a_4 \right\}.$$

Si

$$\frac{A_1 - A_1}{A_1 - A_1} + 1 \nsubseteq \frac{A_1 - A_1}{A_1 - A_1}$$

entonces existen $b_1, b_2, b_3, b_4 \in A_1$, con $b_3 \neq b_4$, tales que

$$\frac{b_1 - b_2}{b_3 - b_4} + 1 \notin \frac{A_1 - A_1}{A_1 - A_1}.$$

En consecuencia, la aplicación $f : A_1 \times A_1 \to \mathbb{F}_p$ definida como

$$f(u, v) = \left(\frac{b_1 - b_2}{b_3 - b_4} + 1 \right) u + v$$

es inyectiva y por ende

$$\left| \left(\frac{b_1 - b_2}{b_3 - b_4} + 1 \right) A_1 + A_1 \right| = |A_1|^2.$$

Si, por el contrario,

$$\frac{A_1 - A_1}{A_1 - A_1} + 1 \subseteq \frac{A_1 - A_1}{A_1 - A_1}$$

entonces es evidente que

$$\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p.$$

El lema **2.11** asegura entonces la existencia de

$$z \in \frac{A_1 - A_1}{A_1 - A_1}$$

tal que

$$|A_1 + zA_1| \geqslant \frac{1}{2} \min\{p, |A_1|^2\}.$$

Así, para algún $(b_1, b_2, b_3, b_4) \in A_1^4$ se tiene que

$$|(b_1 - b_2)A_1 + (b_3 - b_4)A_1| \geqslant \frac{1}{2} \min\{p, |A_1|^2\}.$$

De esto último se sigue que

$$|(b_1 - b_2)A_1 + (b_3 - b_4)A_1| \geqslant \frac{p}{2}$$

ó

$$|(b_1 - b_2)A_1 + (b_3 - b_4)A_1| \geqslant \frac{1}{2}|A_1|^2$$

y la prueba termina.

□

La conclusión del lema anterior pudo haberse formulado de una manera diferente; no obstante, la formulación hecha será particularmente conveniente para la aplicación que se le tiene contemplada.

Capítulo 3

Estimaciones de suma-producto en $\mathbb{F}_p$

Como se ha mencionado en la introducción, el problema de suma-producto en $\mathbb{F}_p$ fue resuelto en trabajos de Bourgain, Katz y Tao y Bourgain, Glibichuk y Konyagin. Ellos probaron el siguiente teorema, al que se le conoce hoy en día como la estimación de suma-producto en campos de orden primo.

Teorema 3.1. *Para cualquier $\epsilon > 0$ existe $\delta = \delta(\epsilon) > 0$ tal que si $A \subseteq \mathbb{F}_p$ y $|A| < p^{1-\epsilon}$, entonces*

$$\max\{|A+A|, |AA|\} \geqslant |A|^{1+\delta}.$$

En las hipótesis del teorema el requerimiento que $|A|$ sea menor que $p^{1-\epsilon}$ es esencial pues si $|A|$ es cercano a p entonces tanto $|A+A|$ como $|AA|$ tienen orden cercano a $|A|$.

En la prueba del teorema **3.1** utilizaremos algunos de los principales resultados del capítulo anterior. Sin embargo, antes de abordarla presentaremos una estimación de suma-producto debida a Garaev que implica al teorema **3.1** cuando $|A| > p^{1/2+\epsilon}$.

Proposición 3.2. *Para cualquier subconjunto no vacío A de $\mathbb{F}_p$ se tiene que*

$$\max\{|A+A|, |AA|\} > c \min\left\{\frac{|A|^2}{p^{1/2}}, p^{1/2}|A|^{1/2}\right\}$$

donde c es una constante absoluta positiva.

Prueba. Podemos suponer, sin pérdida de generalidad, que $0 \notin A$. Consideremos entonces la ecuación

$$xa_1^{-1} + a_2 = y, \quad (x, a_1, a_2, y) \in (AA) \times A \times A \times (A+A). \tag{21}$$

Para cada $(a_1, a_2, a_3) \in A \times A \times A$, la tupla

$$(a_1a_3, a_1, a_2, a_3 + a_2) \in (AA) \times A \times A \times (A+A)$$

es solución de (21). Además, puesto que a tercias diferentes (a_1, a_2, a_3) corresponden soluciones diferentes $(a_1a_3, a_1, a_2, a_3 + a_2)$, el número J de soluciones a la ecuación (21) es mayor o igual a

$|A|^3$. Por otra parte, si expresamos a J por medio del procedimiento usual obtenemos que

$$\begin{aligned} |A|^3 &\leqslant J = \frac{1}{p}\sum_{n=0}^{p-1}\sum_{x\in AA}\sum_{a_1\in A}\sum_{a_2\in A}\sum_{y\in A+A} e^{2\pi i\frac{n(xa_1^{-1}+a_2-y)}{p}} \\ &\leqslant \frac{|AA||A|^2|A+A|}{p} \\ &+ \frac{1}{p}\sum_{n=1}^{p-1}\left|\sum_{x\in AA}\sum_{a_1\in A} e^{2\pi i\frac{nxa_1^{-1}}{p}}\right|\left|\sum_{a_2\in A}\sum_{y\in A+A} e^{2\pi i\frac{n(a_2-y)}{p}}\right|. \end{aligned}$$

Por otra parte, para $n\in\{1,\ldots,p-1\}$ se cumple que

$$\begin{aligned} \left|\sum_{x\in AA}\sum_{a_1\in A} e^{2\pi i\frac{nxa_1^{-1}}{p}}\right|^2 &\leqslant |AA|\sum_{x\in AA}\left|\sum_{a_1\in A} e^{2\pi i\frac{nxa_1^{-1}}{p}}\right|^2 \\ &\leqslant |AA|\sum_{a_1\in A}\sum_{a_2\in A}\sum_{x=0}^{p-1} e^{2\pi i\frac{nx(a_1^{-1}-a_2^{-1})}{p}} \\ &= p|A||AA|. \end{aligned}$$

Por consiguiente

$$\begin{aligned} |A|^3 &\leqslant \frac{|AA||A|^2|A+A|}{p} + \frac{\sqrt{p|AA||A|}}{p}\sum_{n=0}^{p-1}\left|\sum_{a_2\in A} e^{2\pi i\frac{na_2}{p}}\right|\left|\sum_{y\in A+A} e^{2\pi i\frac{ny}{p}}\right| \\ &\leqslant \frac{|AA||A|^2|A+A|}{p} + \sqrt{p|AA||A|}\sqrt{|A||A+A|}. \end{aligned}$$

El resultado se obtiene al notar que las desigualdades de arriba implican que si $M := \max\{|A+A|, |AA|\}$ entonces

$$|A|^2 \leqslant \frac{M^2|A|}{p} + \sqrt{p}M.$$

□

Notemos que en el caso $|A| > p^{2/3}$, la proposición **3.2** implica la estimación $\max\{|A+A|, |AA|\} \gg p^{1/2}|A|^{1/2}$. Por otro lado, un ejemplo de Chang-Garaev indica que para cualquier entero $N\in[1,p]$ existe un subconjunto $A\subseteq\mathbb{F}_p$ de cardinalidad $|A| = N$ tal que

$$\max\{|A+A|, |AA|\} \ll p^{1/2}|A|^{1/2}.$$

En otras palabras, la proposición **3.2** implica una estimación óptima (en la formulación general) para subconjuntos de cardinalidad grande. Posteriormente Solymosi [**29, 30**] encontró una demostración de la proposición **3.2** utilizando métodos de la teoría espectral de gráficas.

Prueba de la proposición 3.1. En vista de la proposición **3.2**, es suficiente con ocuparnos del caso en que $|A| < p^{1/2}$. Además, podemos dar por hecho que $|A|^2 \geqslant 10|AA|\log|A|$ y que $0 \notin A$. Notemos que

$$E_\times(A,A) = \sum_{a\in A}\sum_{b\in A}|aA \cap bA|$$

y que existe $b_0 \in A$ tal que

$$\sum_{a\in A}|aA \cap b_0A| \geqslant \frac{E_\times(A,A)}{|A|}.$$

Al distribuir las cantidades $|aA \cap b_0A|$ en los intervalos $[2^{j-1}, 2^j)$, aseguramos la existencia de un número $N \geqslant 1$ y un subconjunto $A_1 \subseteq A$ tal que

$$N \leqslant |aA \cap b_0A| < 2N \tag{22}$$

vale para cada $a \in A_1$ y

$$N|A_1| \geqslant \frac{E_\times(A,A)}{5|A|\log|A|}. \tag{23}$$

En vista que $N \leqslant |A|$ y $|A_1| \leqslant |A|$, la desigualdad en (23) implica que

$$N \geqslant \frac{E_\times(A,A)}{5|A|^2\log|A|}, \tag{24}$$

$$|A_1| \geqslant \frac{E_\times(A,A)}{5|A|^2\log|A|}. \tag{25}$$

Puesto que $E_\times(A,A) \geqslant |A|^4|AA|^{-1}$ se tiene que $|A_1| > 1$. De la desigualdad triangular de Ruzsa y la primera desigualdad en (22) se colige que

$$\begin{aligned} |aA \pm b_0A| &\leqslant \frac{|aA + (aA \cap b_0A)||(aA \cap b_0A) + b_0A|}{|aA \cap b_0A|} \\ &\leqslant \frac{|A+A|^2}{N}. \end{aligned} \tag{26}$$

Como $A_1 \subseteq A$, el lema **2.12** asegura la existencia de $b_1, b_2, b_3, b_4 \in A_1$ tales que

$$|(b_1 - b_2)A + (b_3 - b_4)A + (b_3 - b_4)A| \gg |A_1|^2.$$

Al aplicar el corolario **2.8** con $k = 3$ y

$$X = B_1 = B_2 = (b_3 - b_4)A, \quad B_3 = (b_1 - b_2)A$$

obtenemos

$$|A_1|^2 \ll \frac{|A+A|^2|(b_1 - b_2)A + (b_3 - b_4)A|}{|A|^2}. \tag{27}$$

Si aplicamos nuevamente el corolario **2.8** pero ahora con $k = 4$ y

$$X = b_0A, \quad B_1 = b_3A, \quad B_2 = -b_4A, \quad B_3 = b_1A, \quad B_4 = -b_2A,$$

llegamos a que

$$|(b_1 - b_2)A + (b_3 - b_4)A| \ll \frac{|b_0A + b_3A||b_0A - b_4A||b_0A + b_1A||b_0A - b_2A|}{|A|^3}.$$

Aplicando la desigualdad en (26) a la expresión en el lado derecho de desigualdad previa y tomando en cuenta (27), obtenemos

$$|A + A|^{10} \gg |A_1|^2|A|^5N^4.$$

De (23), (24) y (25) se sigue entonces que

$$|A + A|^{10} \gg \frac{E_\times(A, A)^4}{|A|}(\log |A|)^{-4}.$$

Puesto que $E_\times(A, A) \geqslant |A|^4|AA|^{-1}$, concluimos que

$$|A + A|^{10}|AA|^4 \gg |A|^{15}(\log |A|)^{-4}.$$

□

§2. Una estimación de suma-producto para conjuntos diferentes. El siguiente resultado es una versión explícita de Garaev a una estimación de suma-producto de Bourgain para conjuntos diferentes. Este resultado jugará un papel clave en el capítulo siguiente al momento de efectuar estimaciones de sumas trigonométricas.

Teorema 3.3. *Sean $A, B \subseteq \mathbb{F}_p^*$ y $L := \min\{|B|, p|A|^{-1}\}$. Se tiene entonces que*

$$|A - A|^2\frac{|A|^2|B|^2}{E_\times(A, B)} \gg |A|^3L^{1/9}(\log L)^{-1}.$$

Antes de establecer el resultado, probaremos un par de lemas.

Lema 3.4. *Sean X e Y subconjuntos de $\mathbb{F}_p^*$ cardinal mayor o igual a 2. Supongamos que existe $z_0 \in \mathbb{F}_p^*$ y $K \in (0, \infty)$ tal que*

$$|yX + z_0X| \leqslant K|X|$$

vale para cada $y \in Y$. Afirmamos entonces que existen $(x_1, x_2) \in X^2$ y $(y_1, y_2) \in Y^2$ tales que

$$|(x_1 - x_2)Y + (y_1 - y_2)X + (y_1 - y_2)X| \geqslant \frac{|X||Y|}{4K}$$

ó

$$|(x_1 - x_2)Y + (y_1 - y_2)X| \geqslant \frac{p}{2}.$$

Prueba. Podemos suponer que $|X| \geqslant 2K$ y $|Y| \geqslant 2K$ pues, en otro caso, el resultado se obtiene fácilmente (por ejemplo, $|X| < 2K$ implica que $\frac{|X||Y|}{4K} < \frac{|Y|}{2} \leqslant |(x_1-x_2)Y+(y_1-y_2)X+(y_1-y_2)X|$ siempre que x_1 y x_2 son elementos distintos de X y y_1 y y_2 son elementos distintos de Y). Luego, en vista de la condición $|yX + z_0X| \leqslant K|X|$ podemos afirmar que

$$|\{(z_0x, z_0x_1, yx_2, yx_3) \in (z_0X)^2 \times (yX)^2 : z_0x + yx_2 = z_0x_1 + yx_3\}|$$

es mayor o igual a

$$\frac{|z_0X|^2|yX|^2}{|yX + z_0X|} \geqslant \frac{|X|^3}{K}$$

para cada $y \in Y$. En consecuencia, el número de soluciones de la ecuación

$$z_0x + yx_2 = z_0x_1 + yx_3 \quad \text{con} \quad (x, x_1, x_2, x_3, y) \in X^4 \times Y$$

es, por muy poco, $|X|^3|Y|/K$. La restricción adicional $x_2 = x_3$ implicaría $x = x_1$ y, por tanto, no más de $|X|^2|Y| \leqslant |X|^3|Y|/(2K)$ soluciones. Luego, si para $(x_1, x_2, x_3) \in X^3$ con $x_2 \neq x_3$ denotamos con $S(x, x_1, x_2, x_3, y)$ al número de soluciones de $z_0x + yx_2 = z_0x_1 + yx_3$ tenemos que

$$\begin{aligned}
\frac{|X|^3|Y|}{K} &\leqslant \sum_{\substack{(x,x_1,x_2,x_3,y)\in X^4\times Y\\ z_0x+yx_2=z_0x_1+yx_3}} 1 \\
&= \sum_{\substack{(x,x_1,x_2,x_3,y)\in X^4\times Y\\ x_2=x_3\\ z_0x+yx_2=z_0x_1+yx_3}} 1 + \sum_{\substack{(x,x_1,x_2,x_3,y)\in X^4\times Y\\ x_2\neq x_3\\ z_0x+yx_2=z_0x_1+yx_3}} 1
\end{aligned}$$

y por consiguiente

$$\begin{aligned}
\sum_{\substack{(x,x_1,x_2,x_3,y)\in X^4\times Y\\ x_2\neq x_3\\ z_0x+yx_2=z_0x_1+yx_3}} 1 &\geqslant \frac{|X|^3|Y|}{K} - \sum_{\substack{(x,x_1,x_2,x_3,y)\in X^4\times Y\\ x_2=x_3\\ z_0x+yx_2=z_0x_1+yx_3}} 1 \\
&\geqslant \frac{|X|^3|Y|}{K} - \frac{|X|^3|Y|}{2K} \\
&= \frac{|X|^3|Y|}{2K}
\end{aligned}$$

o equivalentemente,

$$\sum_{(x_1,x_2,x_3)\in X^3} S(x, x_1, x_2, x_3, y) \geqslant \frac{|X|^3|Y|}{2K}.$$

De la desigualdad anterior se concluye la existencia de $(x_0, x_0', x_0'') \in X^3$ con $x_0' \neq x_0''$ tal que

$$|z_0(X - x_0) \cap (x_0'' - x_0')Y| \geqslant \frac{|Y|}{2K}.$$

Luego, si $Y_1 := \frac{z_0}{x_0'' - x_0'}(X - x_0) \cap Y$ entonces

$$Y_1 \subseteq Y, \quad \frac{x_0'' - x_0'}{z_0} Y_1 \subseteq X - x_0, \quad |Y_1| \geqslant \frac{|Y|}{2K} \geqslant 1.$$

Surgen entonces dos posibilidades. Si

$$\frac{X - X}{Y_1 - Y_1} \neq \mathbb{F}_p$$

entonces existe $(x_1, x_2, y_1, y_2) \in X^2 \times Y_1^2$ tal que

$$\frac{x_1 - x_2}{y_1 - y_2} + \frac{x_0'' - x_0'}{z_0} \notin \frac{X - X}{Y_1 - Y_1}.$$

De esto se desprende a su vez que

$$\left| \left(\frac{x_1 - x_2}{y_1 - y_2} + \frac{x_0'' - x_0'}{z_0} \right) Y_1 + X \right| = |X||Y_1| \geqslant \frac{|X||Y|}{2K}.$$

Puesto que

$$\frac{x_0'' - x_0'}{z_0} Y_1 \subseteq X - x_0,$$

la prueba termina en este caso. Finalmente, si

$$\frac{X - X}{Y_1 - Y_1} = \mathbb{F}_p$$

el lema **2.11** nos permite afirmar la existencia de $(x_1, x_2, y_1, y_2) \in X^2 \times Y_1^2$ tal que

$$|(x_1 - x_2)Y_1 + (y_1 - y_2)X| \geqslant \frac{1}{2} \min\{|X||Y_1|, p\} \geqslant \frac{1}{2} \min\left\{ \frac{|X||Y|}{2K}, p \right\}$$

con lo cual la prueba culmina.

□

Lema 3.5. *Sean $A, B, C \subseteq \mathbb{F}_p^*$. Se cumple entonces que*

$$|A + C| \frac{|A|^2|B|^2}{E_\times(A, B)} \gg \min\left\{ p|A|, \frac{|A|^2|B||C|}{p} \right\}.$$

En particular, si $|A|(\log |B|)^{1000} \geqslant p$ entonces

$$|A - A| \frac{|A|^2|B|^2}{E_\times(A, B)} \gg p|A|.$$

Prueba. Sea J el número de soluciones a la ecuación

$$abb_1^{-1} + c = x \tag{28}$$

donde $(a, b, b_1, c, x) \in A \times B \times B \times C \times (A + C)$. Claramente, para cada vector $(a, a_1, b, b_1, c) \in A^2 \times B^2 \times C$ con $ab = a_1 b_1$, el vector

$$(a, b, b_1, c, a_1 + c) \in A \times B \times B \times C \times (A + C)$$

es solución de la ecuación (28). Además, puesto que a vectores $(a, a_1, b, b_1, c) \in A^2 \times B^2 \times C$ distintos tales que $ab = a_1 b_1$, corresponden vectores distintos $(a, b, b_1, c, a_1 + c)$, el número de soluciones J satisface que

$$\mathrm{J} \geqslant |C| E_\times(A, B). \tag{29}$$

Expresando a J en términos de sumas trigonométricas y siguiendo nuevamente el procedimiento usual obtenemos que

$$\mathrm{J} \leqslant \frac{|A||B|^2|C||A + C|}{p} + \sqrt{|C||A + C|} \max_{(p,n)=1} W(n)$$

donde

$$W(n) := \left| \sum_{b_1 \in B} \sum_{a \in A} \sum_{b \in B} e^{\frac{2\pi i (nabb_1^{-1})}{p}} \right|.$$

Al aplicar la desigualdad de Cauchy-Schwarz a la suma sobre b_1 se tiene que

$$W^2(n) \leqslant |B| \sum_{t=0}^{p-1} \left| \sum_{a \in A} \sum_{b \in B} e^{\frac{2\pi i (nabt)}{p}} \right|^2 = p|B| E_\times(A, B).$$

De esto y lo hecho previamente se desprende que

$$\mathrm{J} \leqslant \frac{|A||B|^2|C||A + C|}{p} + \sqrt{|C||A + C|} \sqrt{p|B| E_\times(A, B)}.$$

El aserto en cuestión se sigue inmediatamente de la desigualdad anterior y la estimación en (29). En efecto, si

$$M := \max \left\{ \frac{|A||B|^2|C||A + C|}{p}, \sqrt{|C||A + C|} \sqrt{p|B| E_\times(A, B)} \right\}$$

entonces

$$M \gg |C| E_\times(A, B).$$

Esto implica en particular que

$$|A + C| \frac{|A|^2|B|^2}{E_\times(A, B)} \gg p|A|$$

ó

$$|A+C|\frac{|A|^2|B|^2}{E_\times(A,B)} \gg \frac{|A|^2|B||C|}{p}.$$

En cualquier caso,

$$|A+C|\frac{|A|^2|B|^2}{E_\times(A,B)} \gg \text{mín}\left\{p|A|, \frac{|A|^2|B||C|}{p}\right\}$$

lo cual deseabamos demostrar.

□

Prueba del teorema 3.3. Sin pérdida de generalidad podemos suponer que tanto $|A|$ como $|B|$ son mayores que 10. Si $|A|(\log|B|)^{200} \geqslant p$, del lema **3.5** se desprende que

$$|A-A|^2\frac{|A|^2|B|^2}{E_\times(A,B)} \gg p|A|^2$$

y el resultado se tiene en este caso. Supongamos entonces que $p/|A| > (\log|B|)^{200}$. Si Δ es tal que

$$\frac{|A|^2|B|^2}{E_\times(A,B)} = |A|\Delta$$

entonces

$$\sum_{b\in B}\sum_{b'B}|bA\cap b'A| = E_\times(A,B) = \frac{|A||B|^2}{\Delta}.$$

De esto se asegura la existencia de $b_0 \in B$ tal que

$$\sum_{b\in B}|bA\cap b_0A| \geqslant \frac{|A||B|}{\Delta}. \tag{30}$$

Sea

$$B_1 := \left\{b\in B : |bA\cap b_0A| > \frac{|A|}{2\Delta}\right\}. \tag{31}$$

Puesto que

$$\sum_{b\in B_1}|bA\cap b_0A| = \sum_{b\in B}|bA\cap b_0A| - \sum_{b\in B\setminus B_1}|bA\cap b_0A| \geqslant \frac{|A||B|}{2\Delta}, \tag{32}$$

se obtiene que $2|B_1|\Delta \geqslant |B|$. Podemos presuponer entonces que $|B_1| > 10$ pues, en caso contrario, se tendría que $\Delta \gg |B|$ y la prueba terminaría. En efecto, pues si $L = |B|$ entonces de $\log|B| > \log 10$ se desprende que $1/\log 10 > 1/\log|B|$ y por consiguiente,

$$L \gg \frac{L^{1/9}}{\log 10} > \frac{L^{1/9}}{\log L}.$$

En el otro caso, $L = p/|A| > (\log|B|)^{200} > (\log 10)^{200}$ y por tanto,

$$\frac{L^{1/9}}{200\log\log 10} > \frac{L^{1/9}}{\log L}.$$

Así,

$$|B| \geqslant \frac{p}{|A|} \geqslant \left(\frac{p}{|A|}\right)^{1/9} \gg \frac{L^{1/9}}{\log L}.$$

Por otro lado, en la luz de la desigualdad triangular de Ruzsa podemos afirmar que

$$|bA \pm b_0A| \leqslant \frac{|bA-(bA\cap b_0A)||(bA\cap b_0A)-b_0A|}{|bA\cap b_0A|} \leqslant \frac{|A-A|^2}{|bA\cap b_0A|}.$$

De esto y la definición (31) se deduce que para cada $b \in B_1$

$$|bA \pm b_0A| \leqslant \frac{2|A-A|^2\Delta}{|A|}. \tag{33}$$

Para $a \in A$ denotemos con $B_1(a)$ al subconjunto de B_1 tal que $aB_1(a) = aB_1 \cap b_0A$. De (32) se obtiene entonces que

$$\sum_{a\in A}|B_1(a)| = \sum_{a\in A}|aB_1\cap b_0A| = \sum_{b\in B_1}|bA\cap b_0A| \geqslant \frac{|A||B|}{2\Delta}.$$

Al distribuir los números $|B_1(a)|$ en los intervalos binarios $[2^{j-1},2^j)$, colegimos que para algún $A_0 \subseteq A$ y algún $N \geqslant 1$ se cumple que

$$N|A_0| \;\geqslant\; \frac{|A||B|}{8\Delta\log|B|} \tag{34}$$

y

$$N \leqslant |B_1(a)| \;\leqslant\; 2N \qquad \text{para cada } a \in A_0. \tag{35}$$

De esto se sigue, en particular, que

$$N \geqslant \frac{|B|}{8\Delta\log|B|}.$$

Por otra parte, de

$$\begin{aligned}\sum_{(a,a')\in A_0^2}|B_1(a)\cap B_1(a')| &= \sum_{(a,a')\in A_0^2}\sum_{\substack{\lambda\\ \lambda\in B_1(a)\\ \lambda\in B_1(a')}}1\\ &= \sum_{\lambda\in B_1}\left(\sum_{\substack{a\in A_0\\ \lambda\in B_1(a)}}1\right)\left(\sum_{\substack{a'\in A_0\\ \lambda\in B_1(a')}}1\right)\\ &= \sum_{\lambda\in B_1}\left(\sum_{\substack{a\in A_0\\ \lambda\in B_1(a)}}1\right)^2,\end{aligned}$$

la desigualdad de Cauchy-Schwarz y

$$\sum_{\lambda\in B_1}\sum_{\substack{a\in A_0\\ \lambda\in B_1(a)}}1=\sum_{a\in A_0}|B_1(a)|\geqslant N|A_0|$$

se deduce que

$$\sum_{(a,a')\in A_0^2}|B_1(a)\cap B_1(a')|\geqslant\frac{N^2|A_0|^2}{|B_1|}.$$

Nuevamente, al distribuir los números $|B_1(a)\cap B_1(a')|$ en los intervalos binarios se obtienen $G\subseteq A_0\times A_0$ y $M\in[1,\infty)$ tales que

$$M|G|\geqslant\frac{N^2|A_0|^2}{10|B_1|\log|B|}.$$

Se tiene además que para todo $(a,a')\in G$,

$$M\leqslant|B_1(a)\cap B_1(a')|\leqslant 2M.$$

En particular, dado que $|G|\leqslant|A_0|^2$, se cumple que

$$M\geqslant\frac{N^2}{10|B_1|\log|B|}. \tag{36}$$

Ahora bien, si $a\in A_0$ denotemos con $G(a)$ al conjunto de $a'\in A_0$ tales que $(a,a')\in G$. Además, si

$$A_1:=\left\{a\in A_0:|G(a)|>\frac{N^2|A_0|}{20M|B_1|\log|B|}\right\},$$

al tenerse que

$$\sum_{a\in A_0}|G(a)|=|G|\geqslant\frac{N^2|A_0|^2}{10M|B_1|\log|B|}$$

se sigue que

$$|A_1||A_0| \geqslant \sum_{a\in A_1}|G(a)| = \sum_{a\in A_0}|G(a)| - \sum_{a\in A_0\setminus A_1}|G(a)| \geqslant \frac{N^2|A_0|^2}{20M|B_1|\log|B|}$$

y por consiguiente

$$M|A_1| \geqslant \frac{N^2|A_0|}{20|B_1|\log|B|}. \tag{37}$$

Si $|A|^5M^2 \leqslant 10N|A||A-A|^4$, entonces de las desigualdades (36) y (33) se desprende que

$$|A|^4|B|^3 \ll |A-A|^4\Delta^4|B_1|^2\log^5|B|.$$

Como $B_1 \subseteq B$ y $|A-A| \geqslant |A|$, la desigualdad anterior deviene en

$$|A-A|^2\frac{|A|^2|B|^2}{E_\times(A,B)} \geqslant |A|^2|A-A|\Delta \gg |A|^3\frac{|B|^{1/4}}{(\log|B|)^{5/4}}$$

y la prueba finalizaría en este caso. Ergo, podemos suponer en lo que sigue que

$$|A|^5M^2 > 10N|A||A-A|^4\Delta. \tag{38}$$

Sea $a_1 \in A_1$. Estimaremos a continuación $|a_1B_1 \pm b_0G(a_1)|$ para cualquier elección del signo. Sea $\delta \in \{-1,1\}$. Por cada $x \in a_1B_1 + \delta b_0G(a_1)$, fijemos $b \in B_1$ y $a_1' \in G(a_1)$ tales que

$$x = a_1b + \delta b_0a_1'$$

y definamos $B_{11}(x) := B_1(a_1) \cap B_1(a_1')$. Como

$$\begin{aligned}\delta b_0^2A + xB_{11}(x) &\subseteq \delta b_0^2A + ba_1B_1(a_1) + \delta b_0a_1'B_1(a')\\ &\subseteq b_0(bA + \delta b_0A + \delta b_0A),\end{aligned}$$

al aplicar el corolario **2.8** con $k=3$ y $X = -\delta b_0A$ se obtiene que

$$\begin{aligned}|\delta b_0^2A + xB_{11}(x)| &\leqslant |b_0(bA + \delta b_0A + \delta b_0A)|\\ &= |bA + \delta b_0A + \delta b_0A|\\ &\ll \frac{|bA - \delta b_0A||\delta b_0A - \delta b_0A||\delta b_0A - \delta b_0A|}{|-\delta b_0A|^2}\\ &\leqslant \frac{|bA - \delta b_0A||A-A|^2}{|A|^2}.\end{aligned}$$

De esto y la estimación en (33) se desprende inmediatamente que

$$|\delta b_0^2A + xB_{11}(x)| \ll \frac{2|A-A|^4\Delta}{|A|^3}.$$

Luego, para x distinto de cero en $a_1B_1 + \delta b_0G(a_1)$, el número de soluciones de la ecuación

$$b_0^2a' + xb' = b_0^2a'' + xb''$$

donde $(a',a'') \in A^2$ y $(b',b'') \in B_{11}(x) \times B_{11}(x)$ satisface

$$\begin{aligned} E_+(b_0^2A, xB_{11}(x)) &\geqslant \frac{|A|^2M^2}{|\delta b_0^2A + xB_{11}(x)|} \\ &\gg \frac{|A|^2M^2}{\frac{2|A-A|^4\Delta}{|A|^3}} \\ &= \frac{|A|^5M^2}{2|A-A|^4\Delta}. \end{aligned}$$

Puesto que $B_{11}(x) \subseteq B_1(a_1)$, para cada x distinto de cero en $a_1B_1 + \delta b_0G(a_1)$, el número de soluciones de la ecuación

$$b_0^2a' + xb' = b_0^2a'' + xb'', \quad (a',a'') \in A^2 \quad (b',b'') \in B_1(a_1)$$

tambiés es, por lo menos, $|A|^5M^2/(2|A-A|^4\Delta)$. En consecuencia, el número de soluciones de la ecuación

$$b_0^2a' + xb' = b_0^2a'' + xb''$$

donde $(a',a'') \in A^2$, $(b',b'') \in B_1(a_1) \times B_1(a_1)$ y $x \in a_1B_1 + \delta b_0G(a_1)\backslash\{0\}$ es, al menos,

$$\frac{|A|^5M^2}{2|A-A|^4\Delta}(|a_1B_1 + \delta b_0G(a_1)| - 1) \geqslant \frac{|A|^5M^2}{4|A-A|^4\Delta}|a_1B_1 + \delta b_0G(a_1)|.$$

Por otra parte, afirmamos que ésta ecuación tiene a lo más

$$2N|A||a_1B_1 + \delta b_0G(a_1)| + 4N^2|A|^2$$

soluciones: en efecto, el primer término corresponde al caso cuando $b' = b''$ y el segundo término corresponde a las 4-uplas (a',a'',b',b'') donde b' y b'' son distintos. De esto y la conclusión del párrafo anterior se concluye que

$$\frac{|A|^5M^2}{4|A-A|^4\Delta}|a_1B_1 + \delta b_0G(a_1)| \leqslant 2N|A||a_1B_1 + \delta b_0G(a_1)| + 4N^2|A|^2.$$

Al considerar (38) llegamos a que

$$\begin{aligned} |a_1B_1 \pm b_0G(a_1)| &\ll \frac{N^2|A|^2|A-A|^4\Delta}{|A|^5M^2 - 8N|A||A-A|^4\Delta} \\ &\ll \frac{N^2|A|^2|A-A|^4\Delta}{|A|^5M^2} \\ &\ll \frac{N^2|A-A|^4\Delta}{M^2|A|^3} \end{aligned} \tag{39}$$

para cada $a_1 \in A_1$. Por otro lado, de (33) sabemos que para cada $b \in B_1$

$$|bA_1 + b_0A_1| \leqslant \frac{2|A-A|^2\Delta}{|A|} = \frac{2|A-A|^2\Delta}{|A||A_1|}|A_1|.$$

Del lema **3.4** se sigue entonces que existen $(a_1, a_{11}) \in A_1$ y $(b_1, b_{11}) \in B_1$ tales que

$$|(a_1B_1 - a_{11}B_1) + (b_1 - b_{11})A + (b_1 - b_{11})A| \gg \frac{|A_1|^2|B_1||A|}{|A-A|^2\Delta}$$

ó

$$|(a_1B_1 - a_{11}B_1) + (b_1 - b_{11})A| \gg p.$$

En el primer caso inferimos, en la luz del corolario **2.8**, que

$$|(a_1B_1 - a_{11}B_1) - (b_1 - b_{11})A| \gg \frac{|A_1|^2|A|^3|B_1|}{|A-A|^4\Delta}.$$

De esto se obtiene a su vez que

$$|a_1B_1 - a_{11}B_1 - b_1A + b_{11}A| \gg \frac{|A_1|^2|A|^3|B_1|}{|A-A|^4\Delta}.$$

Del corolario **2.8** y la estimación en (33) se desprende que

$$\begin{aligned} |a_1B_1 + b_0A||a_{11}B_1 - b_0A| &\gg \frac{|A_1|^2|A|^6|B_1|}{|A-A|^4\Delta} \cdot \frac{1}{|b_0A - b_1A||b_0A + b_{11}A|} \\ &\gg \frac{|A_1|^2|A|^8|B_1|}{|A-A|^8\Delta^3}. \end{aligned} \tag{40}$$

Aplicaremos ahora la desigualdad triangular de Rusza a los dos factores de la expresión que aparece en el lado izquierdo de (40). Dado que $G(a_1) \subseteq A_1$ se sigue que

$$\begin{aligned} |a_1B_1 + b_0A| &\leqslant \frac{|a_1B_1 + b_0G(a_1)||b_0G(a_1) - b_0A|}{|G(a_1)|} \\ &\leqslant \frac{|a_1B_1 + b_0G(a_1)||b_0A - b_0A|}{|G(a_1)|} \\ &= \frac{|a_1B_1 + b_0G(a_1)||A-A|}{|G(a_1)|}. \end{aligned}$$

Análogamente se deduce que

$$|a_{11}B_1 - b_0A| \leqslant \frac{|a_{11}B_1 - b_0G(a_{11})||A-A|}{|G(a_{11})|}.$$

Al multiplicar las dos estimaciones obtenidas y aplicar (40) se llega a que

$$\frac{|a_1B_1 + b_0G(a_1)|}{|G(a_1)|}\frac{|a_{11}B_1 - b_0G(a_{11})|}{|G(a_{11})|} \gg \frac{|A_1|^2|A|^8|B_1|}{|A-A|^{10}\Delta^3}. \tag{41}$$

Luego, de la definición de A_1 y el hecho que $(a_1, a_{11}) \in A_1^2$ se desprende que

$$|G(a_1)||G_(a_{11})| \gg \frac{N^4|A_0|^2}{M^2|B_1|^2}(\log|B|)^{-2}. \tag{42}$$

De (41) y (42) se sigue inmediatamente que

$$|a_1B_1 + b_0G(a_1)||a_{11}B_1 - b_0G(a_{11})| \gg \frac{N^4|A|^8|A_1|^2|A_0|^2}{M^2|A-A|^{10}|B_1|\Delta^3}(\log|B|)^{-2}.$$

La estimación en (39) nos permite afirmar entonces que

$$\frac{N^4|A-A|^8\Delta^2}{M^4|A|^6} \gg \frac{N^4|A|^8|A_1|^2|A_0|^2}{M^2|A-A|^{10}|B_1|\Delta^3}(\log|B|)^{-2}$$

y por tanto

$$|A-A|^{18}|B_1|\Delta^5 \gg M^2|A|^{14}|A_1|^2|A_0|^2(\log|B|)^{-2}.$$

En vista de las estimaciones en (37) y (34), la estimación en la línea anterior puede reescribirse como

$$\begin{aligned} |A-A|^{18}|B_1|\Delta^5 &\gg (M|A_1|)^2|A_0|^2|A|^{14}(\log|B|)^{-2} \\ &\gg \frac{N^4|A_0|^2}{|B_1|^2\log^2|B|}\cdot\frac{|A_0^2||A|^{14}}{\log^2|B|} \\ &\gg \frac{|A|^{18}|B|^4}{|B_1|^2\Delta^4\log^8|B|} \end{aligned}$$

o bien

$$|A-A|^{18}|B_1|^3\Delta^9 \gg |A|^{18}|B|^4(\log|B|)^{-8}.$$

La veracidad del aserto en cuestión se sigue en este caso del hecho que $B_1 \subseteq B$.

Finalmente, en el caso que

$$|a_1B_1 - a_{11}B_1 + b_1A - b_{11}A| \gg p,$$

el corolario **2.8** y la estimación (33) dan

$$|a_1B_1 + b_0A||a_{11}B_1 - b_0A||A-A|^4\Delta^2 \gg p|A|^5.$$

Procediendo como en la última parte del caso precedente obtenemos que

$$|A-A|^{14}\Delta^4 \gg \frac{p|A|^{13}M^2}{|B_1|^2\log^2|B|}.$$

En vista de las estimaciones en (34) y (36), podemos reescribir la estimación en el renglón anterior como

$$|A-A|^{14}\Delta^8 \gg p|A|^{13}(\log|B|)^{-8}.$$

Multiplicando ambos lados de esta estimación anterior por $|A-A|^2 \geqslant |A|^2$ llegamos a

$$|A-A|^2\frac{|A|^2|B|^2}{E_\times(A,B)} \gg |A|^3\left(\frac{p}{|A|}\right)^{1/8}(\log|B|)^{-1}.$$

Como $p/|A| > (\log |B|)^{200}$, la prueba del teorema concluye.

□

Capítulo 4

Aplicaciones a sumas trigonométricas

Consideraremos por fin el problema de la obtención de estimaciones no triviales para sumas trigonométricas multilineales

$$\sum_{x_1\in X_1}\cdots\sum_{x_{2k-2}\in X_{2k-2}}\sum_{x_{2k-1}\in X_{2k-1}}\sum_{x_{2k}\in X_{2k}} e^{2\pi i\frac{x_1\cdots x_{2k-2}x_{2k-1}x_{2k}}{p}}$$

donde todos los conjuntos X_i tienen *aproximadamente* la misma cardinalidad (digamos que para cada $i\in\{1,\dots,2k\}$, $|X_i|\sim M$). La idea es aplicar la estimación de suma-producto, estimaciones del tipo Balog-Szemerédi-Gowers y la desigualdad de Cauchy-Schwarz para reemplazar la suma sobre dos variables (por ejemplo, sobre x_{2k-1} y x_{2k}) por la suma sobre una variable nueva y_k pero sobre un conjunto Y_k de cardinal $|Y_k|>M^{1+\delta}$ para alguna constante $\delta>0$. El problema original se reduce entonces a la estimación de la suma

$$\sum_{x_1\in X_1}\cdots\sum_{x_{2k-2}\in X_{2k-2}}\sum_{y_k\in Y_k} e^{2\pi i\frac{x_1\cdots x_{2k-2}y_k}{p}}.$$

Al reiterar el proceso, llegamos a una suma de la forma

$$\sum_{y_1\in Y_1}\cdots\sum_{y_k\in Y_k} e^{2\pi i\frac{y_1\cdots y_k}{p}}$$

donde cada uno de los conjuntos Y_i tiene ahora cardinalidad $|Y_i|>M^{1+\delta}$. Suponiendo que k es una potencia de 2, podríamos en principio iterar el proceso suficientes veces hasta obtener una suma bilineal sobre conjuntos *grandes* a la que se puede aplicar la estimación clásica. Presentaremos a continuación una versión más rigorosa de la idea descrita arriba. Sean X y Y subconjuntos de $\mathbb{F}_p^*$ tales que tanto $|X|$ como $|Y|$ son aproximadamente igual a M y $M<p^{1/2}$. Sean $c>0$ una constante pequeña, N un entero positivo tal que $N>p^c$ y $s_1,s_2,\dots,s_N$ una sucesión arbitraria de elementos de $\mathbb{F}_p^*$. Supongamos que la suma

$$\sum_{x\in X}\left|\sum_{y\in Y}\sum_{n=1}^{N} e^{2\pi i\frac{xys_n}{p}}\right|$$

no admite una estimación no trivial: esto es, supongamos que

$$\sum_{x\in X}\left|\sum_{y\in Y}\sum_{n=1}^{N} e^{2\pi i\frac{xys_n}{p}}\right|>M^{2+o(1)}N. \tag{43}$$

Afirmamos entonces que existe un subconjunto Z de $\mathbb{F}_p^*$ y una constante $\delta > 0$ tal que $|Z| > M^{1+\delta}$ y

$$\sum_{z\in Z}\left|\sum_{n=1}^{N} e^{2\pi i\frac{zs_n}{p}}\right| > |Z|^{1+o(1)}N. \tag{44}$$

Supongamos lo contrario, es decir, siempre que vale (44) entonces $|Z| \ll M^{1+o(1)}$. Derivaremos una contradicción a partir de este último supuesto. De (43) es fácil deducir la existencia de $X' \subseteq X$ de cardinalidad $|X'| = M^{1+o(1)}$ tal que

$$\left|\sum_{y\in Y}\sum_{n=1}^{N} e^{2\pi i\frac{xys_n}{p}}\right| > M^{1+o(1)}N \tag{45}$$

para cada $x \in X'$. Tenemos entonces que:

a) De (45) puede deducirse a su vez que existe $E \subseteq X' \times Y$ de cardinalidad $|E| = M^{2+o(1)}$ tal que

$$\left|\sum_{n=1}^{N} e^{2\pi i\frac{xys_n}{p}}\right| > NM^{o(1)}$$

para cada $(x,y) \in E$. De la suposición hecha se desprende entonces que $|X' \underset{\text{E}}{\times} Y| = M^{1+o(1)}$. De la versión multiplicativa de la estimación de Balog-Szemerédi-Gowers se asegura entonces la existencia de $X'' \subseteq X'$ de cardinalidad $M^{1+o(1)}$ tal que $|X''X''| = M^{1+o(1)}$.

b) Por otro lado, al sumar (45) sobre los elementos de X'' obtenemos

$$\sum_{y\in Y}\sum_{n=1}^{N}\left|\sum_{x\in X''}\alpha(x)e^{2\pi i\frac{xys_n}{p}}\right| > M^{2+o(1)}N,$$

donde los $\alpha(x)$ son números complejos de módulo 1. Fijando adecuadamente $y_0 \in Y$ y aplicando la desigualdad de Cauchy-Schwarz sobre la variable n llegamos a que

$$\sum_{x_1,x_2\in X''}\left|\sum_{n=1}^{N} e^{2\pi i\frac{(x_1-x_2)y_0s_n}{p}}\right| > M^{2+o(1)}N.$$

Nuevamente, no es difícil deducir de la estimación previa la existencia de $F \subseteq X'' \times X''$ de cardinalidad $M^{2+o(1)}$ tal que la estimación

$$\left|\sum_{n=1}^{N} e^{2\pi i\frac{(x_1-x_2)y_0s_n}{p}}\right| > M^{o(1)}N$$

vale para cada $(x_1,x_2) \in F$. Por la suposición hecha arriba, $|X'' \underset{\text{E}}{-} X''| = M^{1+o(1)}$. Luego, la versión aditiva de la estimación de Balog-Szemerédi-Gowers implica la existencia de $X''' \subseteq X''$ de

cardinalidad $M^{1+o(1)}$ tal que

$$|X''' + X'''| = M^{1+o(1)}.$$

El argumento termina al notar que las conclusiones obtenidas en a) y b) entran en contradicción con la estimación para

$$\max\{|X''' + X'''|, |X'''X'''|\}$$

que se obtiene a partir de la estimación de suma-producto.

Lema 4.1. *Sea p un primo positivo y a un entero coprimo con p. Se cumple entonces que*[1]

$$\left|\sum_{n=1}^{p}\sum_{m=1}^{p} \nu(n)\rho(m)e_p(anm)\right| \leqslant \sqrt{pNM}$$

donde $\nu(n)$ y $\rho(n)$ son números complejos tales que

$$\sum_{n=1}^{p} |\nu(n)|^2 = N \quad y \quad \sum_{m=1}^{p} |\rho(m)|^2 = M.$$

Prueba. Si hacemos $S := \left|\sum_{n=1}^{p}\sum_{m=1}^{p} \nu(n)\rho(m)e_p(anm)\right|$ entonces de la desigualdad de Cauchy-Schwarz se obtiene que

$$\begin{aligned}
S^2 &\leqslant \left(\sum_{n=1}^{p} |\nu(n)|^2\right)^{1/2} \left(\sum_{n=1}^{p}\left|\sum_{m=1}^{p} \rho(m)e_p(anm)\right|^2\right)^{1/2} \\
&= N^{1/2}\left(\sum_{n=1}^{p}\sum_{m_1=1}^{p}\sum_{m_2=1}^{p} \rho(m_1)e_p(anm_1)\overline{\rho(m_2)e_p(anm_2)}\right)^{1/2} \\
&= N^{1/2}\left(\sum_{m_1=1}^{p}\sum_{m_2=1}^{p} \rho(m_1)\overline{\rho(m_2)}\sum_{n=1}^{p} e_p(an(m_1-m_2))\right)^{1/2} \\
&= N^{1/2}\left(\sum_{m=1}^{p} \rho(m)\overline{\rho(m)}p\right)^{1/2} \\
&= \sqrt{pNM}.
\end{aligned}$$

□

[1] En lo que resta del capítulo escribiremos $e_p(a)$ en lugar de $e^{2\pi i\frac{a}{p}}$.

Lema 4.2. *Sean $X, Y \subseteq \mathbb{F}_p^*$, $s_1, \ldots, s_N \in \mathbb{F}_p^*$ y $\delta > 0$. Suponga además que la desigualdad*

$$\left| \sum_{y \in Y} \sum_{n=1}^{N} e_p(xys_n) \right| \geqslant \delta |Y| N$$

vale para cada $x \in X$. Existe entonces $Z \subseteq \mathbb{F}_p^*$ con

$$|Z| \gg |X||Y|^{1/81} \delta^{28/9} (\log |Y|)^{-1}$$

tal que la desigualdad

$$\left| \sum_{n=1}^{N} e_p(zs_n) \right| \geqslant 0.5\delta^2 N$$

vale para cada $z \in Z$.

Prueba. No es difícil establecer la validez del resultado en el caso que $\delta^2 < 10|X|^{-1}$. En efecto, si fijamos $x_0 \in X$ y definimos

$$Z := \left\{ z \in x_0 Y : \left| \sum_{n=1}^{N} e_p(zs_n) \right| \geqslant 0.5\delta N \right\}$$

entonces $|Z| \geqslant 0.5\delta |Y|$. En consecuencia,

$$|Z| \geqslant |X||Y|\delta^3 \geqslant |X||Y|^{1/81} \delta^{28/9} (\log |Y|)^{-1}$$

y por consiguiente, Z satisface la primera aseveración del lema. La segunda aseveración es una consecuencia directa de la definición de Z. Supongamos entonces que $\delta^2 |X| \geqslant 10$. Notemos que existen números complejos α_x de módulo 1 tales que

$$\sum_{x \in X} \sum_{y \in Y} \sum_{n=1}^{N} \alpha_x e_p(xys_n) \geqslant \delta |X||Y| N.$$

De esto se sigue que para algún $n_0 \in \{1, \ldots, N\}$,

$$\sum_{y \in Y} \left| \sum_{x \in X} \alpha_x e_p(xys_{n_0}) \right| \geqslant \delta |X||Y|.$$

Nótese que como consecuencia de la desigualdad anterior y el lema **4.1** se tiene que $\delta^2 |X||Y| \leqslant p$. Por otro lado, una de las hipótesis nos permite asegurar la existencia de $y_0 \in Y$ tal que

$$\sum_{x \in X} \left| \sum_{n=1}^{N} e_p(xy_0 s_n) \right| \geqslant \delta |X| N.$$

La desigualdad anterior deviene en la desigualdad

$$\sum_{n=1}^{N} \left| \sum_{x \in X} \alpha_x e_p(xy_0 s_n) \right| \geqslant \delta |X| N$$

para algunos números complejos α_x de módulo 1. Al elevar al cuadrado ambos lados de la desigualdad previa y aplicar la desigualdad de Cauchy-Schwarz deducimos que

$$\sum_{x_1\in X}\sum_{x_2\in X}\left|\sum_{n=1}^{N} e_p((x_1-x_2)y_0 s_n)\right| \geqslant \delta^2|X|^2N.$$

Puesto que $\delta^2|X| \geqslant 10$, obtenemos que

$$\sum_{x_1\in X, x_2\in X, x_1\neq x_2}\left|\sum_{n=1}^{N} e_p((x_1-x_2)y_0 s_n)\right| \geqslant 0.9\delta^2|X|^2N.$$

Sea

$$E := \left\{(x_1,x_2)\in X\times X : x_1\neq x_2, \left|\sum_{n=1}^{N} e_p((x_1-x_2)y_0 s_n)\right| \geqslant 0.5\delta^2 N\right\}.$$

Es claro que $|E| \geqslant 0.4\delta^2|X|^2$. Al aplicar la proposición **2.9** con $K = 3\delta^{-2}$, obtenemos un subconjunto $X_1 \subseteq X$ de cardinalidad $|X_1| \geqslant 0.0\overline{3}\delta^2|X|$ tal que

$$|X \underset{\mathrm{E}}{-} X|^4 \gg |X_1 - X_1||X|^3\delta^{10}.$$

Así, al hacer $Z_1 := (X \underset{\mathrm{E}}{-} X)y_0$, obtenemos

$$|Z_1|^4 \gg |X_1 - X_1||X|^3\delta^{10}.$$

Además, para cada $z\in Z_1$ tenemos la estimación

$$\left|\sum_{n=1}^{N} e_p(zs_n)\right| \geqslant 0.5\delta^2 N.$$

A continuación, para $x\in X_1$, definamos

$$Y_x := \left\{y\in Y : \left|\sum_{n=1}^{N} e_p(xys_n)\right| \geqslant 0.5\delta N\right\}.$$

Se cumple que $|Y_x| \geqslant 0.5\delta|Y|$. Sea

$$Z_2 := \{xy : x\in X_1, y\in Y_x\}.$$

Puesto que el número de pares (x,y) con $x\in X_1$ y $y\in Y_x$ es al menos $0.5\delta|X_1||Y|$ mientras que el número de soluciones a la ecuación

$$x_1y_1 = x_2y_2, \quad x_i\in X_1, \quad y_i\in Y_{x_i}$$

no excede a $E_\times(X_1,Y)$, entonces

$$|Z_2| \geqslant \frac{\delta^2|X_1|^2|Y|^2}{4E_\times(X_1,Y)}.$$

Además para cada $z \in Z_2$,

$$\left|\sum_{n=1}^{N} e_p(zs_n)\right| \geqslant 0.5\delta N \geqslant 0.5\delta^2 N.$$

Resta probar entonces que uno de los conjuntos Z_1 ó Z_2 tiene la cardinalidad requerida. Se sigue de las estimaciones hechas sobre $|Z_1|$ y $|Z_2|$ que

$$|Z_1|^8|Z_2| \gg |X_1 - X_1|^2 \frac{|X_1|^2|Y|^2}{E_\times(X_1, Y)}|X|^6\delta^{22}.$$

Tomando en cuenta la estimación de suma-producto para conjuntos diferentes (teorema **3.3**) y el hecho que $|X_1| \geqslant 0.0\overline{3}\delta^2|X|$, obtenemos

$$\begin{aligned} |Z_1|^8|Z_2| &\gg |X|^6|X_1|^3 \operatorname{mín}\left\{|Y|, \frac{p}{|X_1|}\right\}^{1/9} \delta^{22}(\log|Y|)^{-1} \\ &\gg |X|^9 \operatorname{mín}\left\{|Y|, \frac{p}{\delta^2|X|}\right\}^{1/9} \delta^{28}(\log|Y|)^{-1}. \end{aligned}$$

Puesto que $\delta^2 \leqslant p/(|X||Y|)$,

$$|Z_1|^8|Z_2| \gg |X|^9|Y|^{1/9}\delta^{28}(\log|Y|)^{-1}$$

y la prueba culmina.

□

Corolario 4.3. *Sean $X, Y \subseteq \mathbb{F}_p^*$, $s_1, \ldots, s_N \in \mathbb{F}_p^*$ y $\delta > 0$. Suponga además que se tiene la desigualdad*

$$\sum_{x\in X}\left|\sum_{y\in Y}\sum_{n=1}^{N} e_p(xys_n)\right| \geqslant \Delta|X||Y|N.$$

Existe entonces $Z \subseteq \mathbb{F}_p^*$ con

$$|Z| \gg |X||Y|^{1/81}\Delta^{28/9}(\log|Y|)^{-5}$$

tal que

$$\sum_{z\in Z}\left|\sum_{n=1}^{N} e_p(zs_n)\right| \geqslant \frac{\Delta^2}{100(\log|Y|)^2}N|Z|.$$

Prueba. Existe $y_0 \in Y$ tal que

$$\sum_{x\in X}\left|\sum_{n=1}^{N} e_p(xy_0s_n)\right| \geqslant \Delta|X|N.$$

Consecuentemente, si $\Delta < 10|Y|^{-1}$, al hacer $Z = y_0X$, obtenemos lo que se requiere. Por lo tanto podemos suponer que $\Delta \geqslant 10|Y|^{-1}$. Se tiene entonces que

$$\sum_{x\in X}{}' \left|\sum_{y\in Y}\sum_{n=1}^{N} e_p(xys_n)\right| \geqslant 0.9\Delta|X||Y|N,$$

donde el apóstrofe sobre la suma exterior indica que se está sumando sólo sobre aquellos $x \in X$ para los cuales

$$N \leqslant \left|\sum_{y\in Y}\sum_{n=1}^{N} e_p(xys_n)\right| \leqslant |Y|N.$$

El intervalo $[N, |Y|N]$ puede ser embebido en la unión de a lo más $2\log|Y|$ intervalos de la forma $[2^{j-1}N, 2^jN)$, donde $2 \leqslant 2^j \leqslant 2|Y|$. Por lo tanto, existe un subconjunto $X_1 \subseteq X$ y un número $0 < \delta \leqslant 1$ tal que

$$\delta N|Y| \leqslant \left|\sum_{y\in Y}\sum_{n=1}^{N} e_p(xys_n)\right| < 2\delta N|Y|$$

para cada $x \in X_1$. Se cumple además que $\delta|X_1|\log|Y| \geqslant 0.2\Delta|X|$. En particular, $\delta \geqslant 0.2\Delta(\log|Y|)^{-1}$ y $|X_1| \geqslant 0.2\Delta|X|(\log|Y|)^{-1}$. Del lema **4.2** se concluye que existe $Z \subseteq \mathbb{F}_p^*$ de cardinalidad

$$|Z| \gg |X_1||Y|^{1/81}\delta^{28/9}(\log|Y|)^{-1} \gg |X||Y|^{1/81}\Delta^{28/9}(\log|Y|)^{-5}$$

tal que para cada $z \in Z$,

$$\left|\sum_{n=1}^{N} e_p(zs_n)\right| \geqslant 0.5\delta^2N \geqslant \frac{\Delta^2}{100(\log|Y|)^2}N.$$

Sumando esta desigualdad sobre $z \in Z$, termina la prueba.

□

Reemplazando Δ en el corolario **4.3** por $\Delta(\log p)^3$, obtenemos para p suficientemente grande que si $X_1, \ldots, X_n$ son subconjuntos de $\mathbb{F}_p^*$ y

$$\frac{1}{|X_1|\cdots|X_n|(\log p)^3}\sum_{x_1\in X_1}\left|\sum_{x_2\in X_2}\cdots\sum_{x_n\in X_n} e_p(x_1\cdots x_n)\right| \geqslant \Delta,$$

entonces existe $X_\kappa \subseteq \mathbb{F}_p^*$ de cardinalidad

$$|X_\kappa| \geqslant |X_1||X_n|^{1/81}\Delta^{28/9}$$

tal que

$$\frac{1}{|X_\kappa||X_2|\cdots|X_{n-1}|(\log p)^3}\sum_{x_1\in X_\kappa}\left|\sum_{x_2\in X_2}\cdots\sum_{x_n\in X_{n-1}} e_p(x_1\cdots x_{n-1})\right| \geqslant \Delta^2.$$

En particular, después de cada iteración la cota inferior de la suma trigonométrica correspondiente cambia de Δ a Δ^2. Así, después de $(n-2)$ iteraciones obtenemos un conjunto X_1' de cardinalidad

$$|X_1'| \geqslant |X_1|(|X_n|\cdots|X_3|)^{1/81}\Delta^{28/9+2\cdot 28/9+\cdots+2^{n-3}\cdot 28/9}$$

tal que

$$\frac{1}{|X_1'||X_2|(\log p)^3}\sum_{x_1\in X_1'}\left|\sum_{x_2\in X_2} e_p(x_1x_2)\right| \geqslant \Delta^{2^{n-2}}.$$

La última desigualdad y el lema **4.1** indican entonces que

$$\Delta^{2^{n-1}} \leqslant \frac{p}{|X_1'||X_2|}.$$

Por otro lado, suponiendo que $|X_1||X_2|(|X_n\cdots X_3|) > p^{1+c}$ donde $c>0$,

$$|X_1'||X_2| \geqslant |X_1||X_2|(|X_n|\cdots|X_3|)^{1/81}\Delta^{(28/9)(2^{n-2}-1)} \geqslant p^{1+c}\Delta^{(28/9)(2^{n-2}-1)}$$

y por consiguiente

$$\Delta^{2^{n+1}} \leqslant p^{-c}.$$

En particular, si $n \leqslant 1.44\log\log p$, tenemos para p suficientemente grande que

$$(\Delta(\log p)^3)^{2^{n+1}} \leqslant p^{-c}(\log p)^{2^{n+3}} \leqslant p^{-0.9c}.$$

De lo anterior se desprende que

$$\Delta(\log p)^3 \leqslant p^{-0.9c/2^{n+1}}.$$

Hemos probado entonces el siguiente

Teorema 4.4. *Sean $n \in [3, 1.44\log\log p]$ y $c>0$ una constante fija arbitraria. Supongamos que $X_1,\ldots,X_n$ son subconjuntos de $\mathbb{F}_p^*$ que satisfacen la condición*

$$|X_1|\cdot|X_2|\cdot(|X_3|\cdots|X_n|)^{1/81} > p^{1+c}.$$

Se cumple entonces que

$$\left|\sum_{x_1\in X_1}\cdots\sum_{x_n\in X_n} e_p(x_1\cdots x_n)\right| \ll |X_1|\cdots|X_n|p^{-0.45c/2^n}.$$

□

Corolario 4.5. *Sea H un subgrupo de $\mathbb{F}_p^*$ de cardinalidad*

$$|H| > e^{57\log p/\log\log p}.$$

Se tiene entonces que

$$\max_{(a,p)=1} \left| \sum_{x\in H} e^{2\pi i \frac{ax}{p}} \right| = o(|H|)$$

cuando $p \to \infty$.

Prueba. Para p suficientemente grande, $c = 0.001$, $n = \lfloor 1.44 \log\log p \rfloor$ y a coprimo con p, se tiene, en la luz del teorema **4.4**, que

$$\begin{aligned} \left| \sum_{x\in H} e^{2\pi i \frac{ax}{p}} \right| &= \left| \frac{1}{|H|^{n-1}} \sum_{x_1 \in aH} \sum_{x_2 \in H} \cdots \sum_{x_n \in H} e^{2\pi i \frac{x_1 x_2 \cdots x_n}{p}} \right| \\ &\ll |H| p^{-0.45c/2^n} \\ &< |H| e^{-(\log p)^{0.0018}}. \end{aligned}$$

Tiene sentido apelar al teorema anterior pues la hipótesis dada sobre $|H|$ implica que

$$|H|^{160}|H|^n > |H|^{n+1} > |H|^{1.44\log\log p} > e^{82.08 \log p} = p^{82.08} > p^{81(1+c)}.$$

□

Teorema 4.6. *Supongamos que* $X, Y, Z \subseteq \mathbb{F}_p^*$ *son tales que*

$$|X||Y| > cp$$

donde c es una constante positiva. Entonces, para $\epsilon > 0$ *se cumple que*

$$\left| \sum_{x\in X} \sum_{y\in Y} \sum_{z\in Z} e_p(xyz) \right| \ll |X||Y||Z|^{539/540+\epsilon}$$

donde las constantes implicadas dependen únicamente de c y ϵ.

Prueba. Supongamos que

$$\sum_{x\in X} \left| \sum_{y\in Y} \sum_{z\in Z} e_p(xyz) \right| = |X||Y||Z|\Delta.$$

Sin pérdida de generalidad podemos suponer que $\Delta \geqslant 10|Z|^{-1}$. Después, podemos incluir al conjunto de elementos $x \in X$ para los cuales

$$|Y| \leqslant \left| \sum_{y\in Y} \sum_{z\in Z} e_p(xyz) \right| \leqslant |Y||Z|$$

en la unión de a lo más $2\log|Z|$ subconjuntos y encontrar un subconjunto $X_1 \subseteq X$ y un número $\delta \in (0,1]$ tal que

$$\delta|Y||Z| \leqslant \left|\sum_{y\in Y}\sum_{z\in Z} e_p(xyz)\right| < 2\delta|Y||Z| \tag{46}$$

para cada $x \in X_1$. Además $\delta|X_1|\log||Z| \gg \Delta|X|$. De esto se desprende, en particular, que

$$\delta \gg \Delta(\log|Z|)^{-1}, \qquad |X_1| \gg \Delta|X|(\log|Z|)^{-1}. \tag{47}$$

Puesto que

$$\sum_{x\in X_1}\sum_{y\in Y}\left|\sum_{z\in Z} e_p(xyz)\right| \geqslant \delta|X_1||Y||Z|,$$

al fijar adecuadamente $y_0 \in Y$ y aplicar el lema **4.1** obtenemos que $\delta^2|X_1||Z| \leqslant p$. Por otra parte, de (46) es claro que

$$\sum_{x\in X_1}\left|\sum_{y\in Y} e_p(xyz_0)\right| \geqslant \delta|X_1||Y|$$

vale para algún $z_0 \in Z$. Al cambiar el orden de sumación en la desigualdad anterior (e introducir nuevamente coeficientes complejos α_x de módulo 1), la desigualdad de Cauchy-Schwarz nos permite colegir que

$$|Y|\sum_{y\in Y}\sum_{x_1\in X_1}\alpha_{x_1}e_p(x_1yz_0)\sum_{x_2\in X_1}\overline{\alpha_{x_2}e_p(x_2yz_0)} \geqslant \delta^2|X_1|^2|Y|^2.$$

Al cambiar el orden de sumación nuevamente llegamos a que

$$\sum_{(x_1,x_2)\in X_1^2}\left|\sum_{y\in Y} e_p((x_1-x_2)z_0y)\right| \geqslant \delta^2|Y||X_1|^2.$$

Por consiguiente, el conjunto

$$E := \left\{(x_1,x_2)\in X_1^2 : \left|\sum_{y\in Y} e_p((x_1-x_2)z_0y)\right| \geqslant 0.5\delta^2|Y|\right\}$$

tiene cardinalidad

$$|E| \geqslant 0.5\delta^2|X_1|^2.$$

Ahora bien, puesto que la estimación

$$\left|\sum_{y\in Y} e_p(tz_0y)\right|^2 \gg \delta^4|Y|^2$$

vale para cada $t \in X_1 \underset{\mathrm{E}}{-} X_1$, se sigue que

$$\delta^4|Y|^2|X_1 \underset{\mathrm{E}}{-} X_1| \ll \sum_{t\in\mathbb{F}_p}\left|\sum_{y\in Y} e_p(tz_0y)\right|^2 = p|Y|. \tag{48}$$

Al aplicar la proposición **2.9** con $K = 2\delta^{-2}$, se asegura la existencia de $X_1' \subseteq X_1$ de cardinalidad $|X_1'| \gg \delta^2|X_1|$ tal que

$$|X_1 \underset{\mathrm{E}}{-} X_1|^4 \gg |X_1' - X_1'||X_1|^3\delta^{10}.$$

De esto y de la acotación en (48) obtenemos que

$$p^4 \gg |Y|^4|X_1|^3|X_1' - X_1'|\delta^{26}. \tag{49}$$

Por otra parte, sabemos que

$$\sum_{x\in X_1'}\left|\sum_{y\in Y}\sum_{z\in Z} e_p(xyz)\right| \geqslant \delta|X_1'||Y||Z|.$$

De esta desigualdad se sigue a su vez que

$$\sum_{y\in Y}\left|\sum_{x\in X_1'}\sum_{z\in Z} \alpha_x e_p(xyz)\right| \geqslant \delta|X_1'||Y||Z|$$

vale para algunos coeficientes α_x de valor absoluto 1. Al aplicar la desigualdad de Cauchy-Schwarz a la suma sobre la variable y obtenemos que

$$\sum_{y\in Y}\left|\sum_{x\in X_1'}\sum_{z\in Z} \alpha_x e_p(xyz)\right|^2 \geqslant \delta^2|X_1'|^2|Y||Z|^2.$$

y por tanto

$$pE_\times(X_1', Z) \gg \delta^2|X_1'|^2|Y||Z|^2.$$

De (49), la estimación en la línea previa y el teorema **3.3** se desprende que

$$p^9 \gg |Y|^9|X_1|^6\delta^{54}|X_1'|^3 \operatorname{mín}\left\{|Z|, \frac{p}{|X_1'|}\right\}^{1/9}(\log|Z|)^{-1}. \tag{50}$$

Como $|X_1'| \gg \delta^2|X_1|$, la estimación en (50) deviene en

$$p^9 \gg \delta^{60}|Y|^9|X_1|^9 \operatorname{mín}\left\{|Z|, \frac{p}{\delta^2|X_1|}\right\}^{1/9}(\log|Z|)^{-1}.$$

De $\delta^2 \leqslant \dfrac{p}{|X_1||Z|}$, $\delta|X_1|\log|Z| \gg |X|\Delta$ y las estimaciones en (47) se obtiene que

$$\begin{aligned} p^9 &\gg |Y|^9\delta^{60}|X_1|^9|Z|^{1/9}(\log|Z|)^{-1} \\ &= |Y|^9\delta^{51}\delta^9|X_1|^9(\log|Z|)^9(\log|Z|)^{-10}|Z|^{1/9} \\ &\gg |Y|^9\delta^{51}\Delta^9|X|^9(\log|Z|)^{-10}|Z|^{1/9} \\ &\gg (cp)^9\Delta^{51}(\log|Z|)^{-51}\Delta^9(\log|Z|)^{-10}|Z|^{1/9} \end{aligned}$$

y por consiguiente

$$\Delta \ll \frac{(\log|Z|)^{61/60}}{|Z|^{1/540}} \ll |Z|^{-1/540+\epsilon}.$$

□

Bibliografía

[1] B. C. Berndt y R. J. Evans, *The determination of Gauss sums.* Bull. Amer. Math. Soc. **5** (1981), Núm. 2, págs. 107-129.

[2] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications.* Int. J. Number Theory **1** (2005), Núm. 1, págs. 1-32.

[3] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources.* Geom. Funct. Anal. **18** (2009), Núm. 5, págs. 1477-1502.

[4] J. Bourgain y M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields.* Math. Proc. Camb. Phil. Soc. **146** (2009), Núm. 1, págs. 1-21.

[5] J. Bourgain, A. A. Glibichuk y S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order.* J. London Math. Soc. **3** (2006), Núm. 2, págs. 380-398.

[6] J. Bourgain, N. Katz y T. Tao, *A sum-product estimate in finite fields and applications.* Geom. Funct. Anal. **14** (2004), Núm. 1, págs. 27-57.

[7] M.-C. Chang, *Some problems in combinatorial number theory.* Integers **8** (2008), Núm. 2, A1, 11 págs.

[8] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields.* Duke Math. J. **145** (2008), Núm. 3, págs. 409-442.

[9] P. Erdös y E. Szemerédi, *On sums and products of integers.* Studies in Pure Mathematics (1983), págs. 213-218.

[10] K. Ford, *The distribution of integers with a divisor in a given integral.* Ann. of Math. **168** (2008), Núm. 2, págs. 367-433.

[11] M. Z. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$. Int. Math. Res. Not. **11** (2007), 11 págs.

[12] M. Z. Garaev, *A quantified version of Bourgain's sum-product estimate in* $\mathbb{F}_p$ *for subsets of incomparable sizes.* Electron J. Combin. **15** (2008), Núm. 1, 8 págs.

[13] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields.* Proc. Amer. Math. Soc. **136** (2008), Núm. 8, págs. 2735-2739.

[14] M. Z. Garaev, *Sumas trigonométricas y congruencias aditivas.* La Gaceta de la RSME **12** (2009), Núm. 1, págs. 129-143.

[15] M. Z. Garaev, *Sums and products of sets and rational trigonometric sum estimates in prime fields.* Russian Math. Surveys **65** (2010), Núm. 4, págs. 599-658.

[16] A. García y F. Voloch, *Fermat curves over finite fields.* J. Number Theory, **30** (1988), Núm. 3, págs. 345-356.

[17] A. A. Glibichuk y S. V. Konyagin, *Additive properties of product sets in fields of prime order* en Additive Combinatorics, CRM. Proc. Lecture Notes, vol. 43, Amer. Math. Soc. Providence, RI, 2007, págs. 279-286.

[18] B. J. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott, and Sarnak.* Current Events Bulletin of the AMS, 2010, 25 págs.

[19] D. R. Heath-Brown y S. V. Konyagin, *New bounds for Gauss sums derived from k-th powers, and for Heilbronn's exponential sum.* Q. J. Math. **51** (2000), Núm. 2, págs. 221-235.

[20] D. R. Heath-Brown y S. Patterson, *The distribution of Kummer sums at prime arguments.* J. Reine. Angew. Math. **310** (1979), págs. 111-130.

[21] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. of Math. **167** (2008), Núm. 2, págs. 601-623.

[22] H. A. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. J. Eur. Math. Soc. **13** (2011), Núm. 3, págs. 761-851.

[23] N. H. Katz y C.-Y. Shen, *Garaev's inequality in finite fields not of prime order.* Online Journal of Analytic Combinatorics, **3** (2008), Núm. 3.

[24] S. V. Konyagin, *Estimates of trigonometric and Gauss sums over subgroups*. Proceedings of the 4th International Conference "Current problems of number theory and its applications" (Tula 2001), Moscow State University Publishing House, Moscow 2002, págs. 86-114.

[25] N. M. Korobov, *Exponential sums and their applications.* Mathematics and its Applications (Soviet Series), Vol. 80, Kluwer Academic Publishers Group, Dordrecht, 1992.

[26] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets.* Graduate Texts in Mathematics, Vol. 165, Springer-Verlag, New York, 1996.

[27] I. Z. Ruzsa, *An application of graph theory to additive number theory*. Scientia Ser. A. Math. Sci. **3** (1998), págs. 97-109.

[28] I. E. Shparlinski, *Estimates of gaussian sums.* Math. Notes **50** (1991), págs. 740-746.

[29] J. Solymosi, *Sumas contra productos.* La Gaceta de la RSME **12** (2009), Núm. 4, págs. 707-719.

[30] J. Solymosi, *Incidences and the spectra of graphs* en Combinatorial number theory and additive group theory, Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009, págs. 299-314.

[31] J. Solymosi, *Bounding multiplicative energy by the sumset*. Adv. Math. **222** (2009), Núm. 2, págs. 402-408.

[32] T. Tao, *Structure and randomness. Pages from year one of a mathematical blog.* Amer. Math. Soc. Providence, RI, 2008.

[33] T. Tao y V. Vu, *Additive Combinatorics.* Cambridge Studies in Advanced Mathematics, Vol. 105, Cambridge Univ. Press, Cambridge, 2006.

[34] I. M. Vinogradov, *The distribution of indices.* Dokl. Akad. Nauk SSSR **4** (1926), págs. 73-76.

[35] I. M. Vinogradov, *An introduction to the theory of numbers.* Pergamon Press, London & New York, 1955.

[36] R. Wilson y J. Gray (compiladores). *Mathematical Conversations: Selections from*, The Mathematical Intelligencer. Springer-Verlag, New York, 2001.