SUMAS DE CARACTERES
y aplicaciones en cuerpos primos

Ana Zumalacárregui
a.zumalacarregui@unsw.edu.au

6 de julio de 2016

Índice

**

Las sumas exponenciales y las sumas de caracteres han sido objeto central en la teoría analítica y combinatoria de números. Contamos con muchos ejemplos de problemas clásicos que se han atacado mediante las técnicas en sumas exponenciales: la Conjetura ternaria de Golbach (Vinogradov, Helfgott), el problema de Waring (Hardy, Littlewood, Vaughan, Vinogradov, Wooley), la distribución de los números primos (Ford, Hardy, Korobov, Linnik), así como muchas otras cuestiones.

Las aplicaciones de estas técnicas son muy amplias y representan un área muy activa de investigación a día de hoy. En este curso introductorio discutiremos teoría básica de caracteres en cuerpos primos y demostraremos algunos resultados clásicos en sumas de caracteres así como una serie de aplicaciones directas, alguna de ellas relativamente reciente.

El curso pretende ser un primer acercamiento a la teoría de sumas de caracteres, pero ha sido mi objetivo demostrar al lector que incluso a partir de resultados muy básicos se pueden obtener resultados muy potentes y novedosos, como lo fué la cota de Garaev [5] para el problema de suma-producto en cuerpos finitos que se discutirá en la última sección.

Muchos de los teoremas presentados se pueden generalizar a cuerpos finitos sin mucha dificultad. Para el lector interesado tanto [7] como [10] son buenas referencias. También [6] es una buena referencia en español para una primera toma de contacto con estas técnicas. Un gran libro para estudiar sumas de caracteres más en profundidad es [8].

Notación:

De ahora en adelante denotaremos por $\mathbf{e}(x) := e^{2\pi i x}$ y para un entero positivo n definimos $\mathbf{e}_n(x) := \mathbf{e}(\frac{x}{n}) = e^{2\pi i x/n}$. Nótese que para todo $x, y \in \mathbb{R}$ y entero positivo n se tiene

$$\mathbf{e}\left(x+y\right) = \mathbf{e}\left(x\right)\mathbf{e}\left(y\right) \quad \text{y} \quad \mathbf{e}_n\left(x+y\right) = \mathbf{e}_n\left(x\right)\mathbf{e}_n\left(y\right).$$

Para un anillo R (o cuerpo[1]) denotaremos por $R^\times$ al grupo de unidades o el conjunto de elementos invertibles en R, dependiendo del contexto. Durante todo el curso G denotará un grupo abeliano finito.

El grupo cíclico de n elementos será denotado por $\mathbb{Z}_n$ y lo identificaremos -salvo que se especifique de otro modo- por las clases residuales $\{0, 1, \ldots, n-1\}$.

A lo largo del texto p denotará un número pimo y $\mathbb{F}_p$ denotará el cuerpo de p elementos. En muchas ocasiones identificaremos los elementos en $\mathbb{F}_p$ con sus correspondientes residuos en $\{0, 1, \ldots, p-1\}$. Recordemos que $\mathbb{F}_p$ contiene dos grupos, respecto de las operaciones suma y producto,

$$(\mathbb{F}_p, +) \cong \mathbb{Z}_p \qquad \text{y} \qquad (\mathbb{F}_p^\times, \cdot) \cong \mathbb{Z}_{p-1}.$$

El grupo de unidades $\mathbb{F}_p^\times$ es cíclico y denotaremos por g a su generador (que no tiene por qué ser único), también llamado raíz primitiva.

Para cantidades f, g diremos que $f = O(g)$, o bien $f \ll g$, si existe una constante absoluta C tal que $f \leq Cg$.

1. Caracteres

Sea G un grupo abeliano finito (que denotaremos multiplicativamente) de order $|G|$ y elemento identidad 1_G. Un *caracter* χ de G es un homomorfismo de G en el grupo multiplicativo de los números complejos $\mathbb{C}^\times$. Es decir $\chi : G \to \mathbb{C}^\times$ con

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2), \tag{1}$$

para cualesquiera elementos $g_i \in G$. En particular, como

$$\chi(1_G) = \chi(1_G \cdot 1_G) = \chi(1_G) \cdot \chi(1_G),$$

entonces necesariamente $\chi(1_G) = 1$.

Entre los caracteres de G existe el llamado caracter *trivial*, denotado por χ_0, que es definido por $\chi(g) = 1$ para cada $g \in G$: el resto de caracteres se conocen como no triviales.

Lema 1. *Sea χ un caracter de un grupo G. Entonces, para todo $g \in G$*

I) $(\chi(g))^{|G|} = 1$.

II) $\chi(g^{-1}) = \overline{\chi(g)}$, *donde $\overline{x}$ denota el conjungado complejo de $x \in \mathbb{C}$.*

Demostración. Ejercicio para el lector.

Ejemplo 2. *Si G es el grupo cíclico de order n y sea g un generador de G. Para un entero dado j, $0 \leq j \leq n-1$, la función*

$$\chi_j\big(g^k\big) = \mathbf{e}_n(jk), \quad k = 0, 1, \ldots, n-1,$$

define un caracter de G. Dados $x, y \in G$ tenemos que $x = g^t$, $y = g^s$ para dos enteros $0 \leq s, t \leq n-1$, de modo que

$$\chi_j(xy) = \chi\big(g^{s+t}\big) = \mathbf{e}_n(j(s+t)) = \mathbf{e}_n(js)\mathbf{e}_n(jt) = \chi\big(g^s\big)\chi\big(g^t\big) = \chi_j(x)\chi_j(y).$$

Nótese que $\chi_0 \equiv 1$ coincide con el caracter trivial.

[1]Este curso fue dictado en Colombia, donde a los cuerpos (del francés 'corps') se los denomina *campos* (del inglés 'fields'). A lo largo del texto he intentado ser consistente y usaré la notación Española, a la que estoy habituada.

Proposición 3. *El conjunto $\widehat{G}$ de caracteres de G forma un grupo abeliano con respecto a la operación $\cdot$ dada por*

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g) \quad \text{para cada } g \in G.$$

Demostración. Ejercicio para el lector.

Teorema 4. *Sea H un subgrupo de G, un grupo abeliano finito, y sea ψ un caracter de H. Entonces ψ puede extenderse a un caracter de G:*

$$\text{i.e. existe un caracter } \chi \in \widehat{G} \text{ con } \chi(h) = \psi(h) \text{ para todo } h \in H.$$

Dem. Sin pérdida de generalidad podemos suponer que H es un subgrupo propio de G. Para un elemento $a \in G \setminus H$ sea H_1 el subgrupo generado por H y a. Denotaremos por m al mínimo entero tal que $a^k \in H$, entonces para todo $g \in H_1$ existe una representación única de la forma

$$g = a^k h, \quad \text{donde } k \in \{0, 1, \ldots, m-1\} \text{ y } h \in H.$$

Podemos definir la función $\psi_1 : H_1 \to \mathbb{C}^\times$ por $\psi_1(g) = \omega^k \psi(h)$ con ω un número complejo que satisface

$$\omega^m = \psi(a^m). \tag{2}$$

Veamos ahora que ψ_1 es un caracter en H_1, cuya restricción a H es precisamente ψ. Se sigue de la definición de ψ_1 que $\psi_1(h) = \psi(h)$ para cada $h \in H$.

Sea $g_1 = a^k h_1, g_2 = a^s h_2 \in H_1$, entonces $g_1 g_2 = a^{k+s} h_1 h_2$. Si $k + s < m$ entonces

$$\psi_1(g_1 g_2) = \omega^{k+s}\psi(h_1 h_2) = \omega^k \psi(h_1)\omega^s \psi(h_2) = \psi_1(g_1)\psi_1(g_2),$$

si $k + s \geq m$, entonces dado que $a^m \in H$ se tiene

$$\psi_1(g_1 g_2) = \omega^{k+s-m}\psi(h_1 h_2 a^m) = \omega^{k+s-m}\psi(a^m)\psi(h_1 h_2) = \omega^{k+s}\psi(h_1 h_2) = \psi_1(g_1)\psi_1(g_2)$$

a partir de (2).

Si $H_1 = G$ entonces hemos construido el caracter ψ_1 que buscábamos. En otro caso, siempre podemos repetir este proceso para un nuevo elemento $b \in G \setminus H_1$ y en un número finito de pasos -dado que nuestro G es finito- este algoritmo finaliza y para cierta iteración tendremos $H_t = G$. □

Claramente la extensión de ψ no es única: las distintas elecciones de ω en (2) dan lugar a caracteres distintos en G.

Corolario 5. *Para cualquier $h \neq 1_G$, existe un caracter χ en G para el cual $\chi(h) \neq 1$.*

Demostración. Sea H el subgrupo de G generado por h, que es cíclico de orden m para algún $m \geq 2$. Se sigue del Ejemplo 2 que

$$\psi(h^k) = \mathbf{e}_m(k)$$

define un caracter en H con $\psi(h) = \mathbf{e}_m(1) = e^{2\pi i/m} \neq 1$ (puesto que $m \geq 2$). Del Teorema 4 se sigue que ψ puede extenderse a un caracter en G.

□

El resultado anterior implica que el grupo de caracteres $\widehat{G}$ discrimina entre elementos distintos del grupo: si $g_1 \neq g_2$ en G entonces ha de existir un caracter $\chi \in \widehat{G}$ con $\chi(g_1) \neq \chi(g_2)$.

Teorema 6 (Ortogonalidad de los caracteres)**.** *Sea G un grupo abeliano finito. Entonces, para cada $\chi \in \widehat{G}$*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{de otro modo.} \end{cases} \tag{3}$$

Y para cada $g \in G$ se tiene

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |\widehat{G}| & \text{if } g = 1_E, \\ 0 & \text{de otro modo.} \end{cases} \tag{4}$$

Demostración. Claramente, si $\chi = \chi_0$ la igualdad en (3) se cumple. Asumamos que $\chi \neq \chi_0$. Como χ es no trivial, entonces por el Corolario 5 existe un elemento $h \in G$ con $\chi(h) \neq 1$. entonces

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

porque si g recorre G, también lo hace hg. Entonces tenemos

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0,$$

que de hecho implica (3), dado que $\chi(h) \neq 1$.

Para la segunda parte, de nuevo asumiremos que $g \neq 1_G$, ya que de otro modo el resultado es trivial. Nótese que la función $\widehat{g}(\chi) = \chi(g)$ es un caracter para el grupo $\widehat{G}$, ya que para cualesquiera dos caracteres $\chi_1, \chi_2 \in \widehat{G}$ se tiene

$$g(\chi_1 \cdot \chi_2) = (\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g) = g(\chi_1)g(\chi_2).$$

Este caracter es no trivial puesto que $g \neq 1_G$, por tanto se sigue del Corolario 5 existe un caracter $\chi \in \widehat{G}$ con $\widehat{g}(\chi) = \chi(g) \neq 1$.

Por tanto, la igualdad en (4) se sigue de (3) aplicada al grupo $\widehat{G}$:

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \widehat{g}(\chi) = 0.$$

□

En la demostración anterior, se prueba de forma indirecta que $\widehat{\widehat{G}} = G$.

Corolario 7. *Sea G un grupo abeliano finito. Entonces $|\widehat{G}| = |G|$.*

Demostración. Se sigue de las propiedades de ortogonalidad de los caracteres que

$$|G| = \sum_{g \in G} \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) = |\widehat{G}|.$$

□

$$- \star -$$

Como ya comentamos anteriormente, en un cuerpo primo $\mathbb{F}_p$ existen dos grupos abelianos finitos: el grupo aditivo $(\mathbb{F}_p, +)$ y el grupo multiplicativo $(\mathbb{F}_p^\times, \cdot)$. En este contexto, denominaremos a dichos caracteres los *caracteres multiplicativos* y *caracteres aditivos* de $\mathbb{F}_p$. De ahora en adelante los caracteres aditivos serán denotados por la letra griega φ mientras que la letra χ se reservará para caracteres multiplicativos.

1.1. Caracteres aditivos

Sea p la característica de $\mathbb{F}_p$. El grupo aditivo $(\mathbb{F}_p, +) \cong \mathbb{Z}_p$ es cíclico y está generado por el elemento 1 (unidad multiplicativa en $\mathbb{F}_p$).

La función φ_1 definida por

$$\varphi_1(c) = \mathbf{e}_p(c) = e^{2\pi i c/p} \quad \text{para todo } c \in \mathbb{F}_p \tag{5}$$

es un caracter en el grupo aditivo de $\mathbb{F}_p$, puesto que $\mathbf{e}_p(a+b) = \mathbf{e}_p(a)\,\mathbf{e}_p(b)$ para cada $a, b \in \mathbb{F}_p$. Además φ_1 es un caracter no trivial. Al caracter definido en (5) se llamará *caracter aditivo canónico* en $\mathbb{F}_p$.

Como veremos a continuación los caracteres de $\mathbb{F}_p$ pueden expresarse en términos de φ_1.

Teorema 8. *Para un $b \in \mathbb{F}_p$ dado, la función φ_b dada por $\varphi_b(c) := \varphi_1(cb)$ para cada $c \in \mathbb{F}_p$ es un caracter aditivo de $\mathbb{F}_p$. Además, cada caracter aditivo de $\mathbb{F}_p$ tiene una representación de esta forma.*

Demostración. Para cada $c_1, c_2 \in \mathbb{F}_p$ se tiene,

$$\varphi_b(c_1 + c_2) = \varphi_1(bc_1 + bc_2) = \varphi_1(bc_1)\varphi_1(bc_2) = \varphi_b(c_1)\varphi_b(c_2),$$

lo que demuestra la primera parte del resultado. Como φ_1 es un caracter no trivial, para cada $a, b \in \mathbb{F}_p$, $a \neq b$, tenemos

$$\frac{\varphi_a(c)}{\varphi_b(c)} = \frac{\varphi_1(ac)}{\varphi_1(bc)} = \varphi_1((a-b)c) \neq 1,$$

para cierto $c \in \mathbb{F}_p$, y así φ_a y φ_b son caracteres distintos. Se sigue del Corolario 7 que $\mathbb{F}_p$ tiene exactamente p characters, de modo que la lista de caracteres queda completada. □

Tomando $b = 0$ en (5) se obtiene el caracter trivial $\varphi_0(c) = \varphi_1(0 \cdot c) = \varphi_1(0) = 1$ para cada $c \in \mathbb{F}_p$. Con esta caracterización en mente es claro que $G = (\mathbb{Z}_p, +) \cong \widehat{G}$, mediante el isomorfismo $a \mapsto \varphi_a = \varphi_1^a$.

1.2. Caracteres multiplicativos

Los caracteres del grupo multiplicativo $\mathbb{F}_p^\times$ de $\mathbb{F}_p$ son llamados *caracteres multiplicativos* de $\mathbb{F}_p$. Como $\mathbb{F}_p^\times$ es un grupo cíclico de orden $p-1$ sus caracteres pueden obtenerse de manera sencilla.

Teorema 9. *Sea g una raíz primitiva de $\mathbb{F}_p$. Para cada $j = 0, 1, \ldots, p-2$ la función χ_j dada por*

$$\chi_j\left(g^k\right) = \mathbf{e}_{p-1}(jk) = e^{2\pi ijk/(p-1)} \quad \text{para} \quad k = 0, 1, \ldots, p-2 \tag{6}$$

define un caracter multiplicativo de $\mathbb{F}_p$. Además, todo caracter multiplicativo de $\mathbb{F}_p$ tiene una representación como esa.

Demostración. La demostración es análoga a la del Teorema 8. □

Se sigue de la definición de χ_j que el grupo de caracteres multiplicativos de $\mathbb{F}_p$ es cíclico de orden $p-1$ con elemento unidad χ_0, ya que de hecho

$$\chi_j \equiv \chi_1^j,$$

por definición. Además, para cada j coprimo con $p-1$ el elemento g^j es nuevamente una raíz primitiva de $\mathbb{F}_p$. Por tanto, el caracter χ_j también es generador del grupo de caracteres multiplicativos:

$$\widehat{G} \cong \widehat{(\mathbb{F}_p^\times, \cdot)}$$

mediante el isomorfismo $j \mapsto \chi_j$.

Ejemplo 10. *Símbolo de Legendre: consideremos, para un cuerpo primo dado $\mathbb{F}_p$ de característica impar, el caracter definido en (6) para $j = (p-1)/2$. Es decir,*

$$\chi_{(p-1)/2}(g^c) = \mathbf{e}_{p-1}(c(p-1)/2) = e^{\pi ic}.$$

El caracter $\chi_{(p-1)/2}$ es conocido como caracter cuadrático de $\mathbb{F}_p$ y coincide con el conocido como símbolo de Legendre, habitualmente denotado por $\left(\frac{\cdot}{p}\right)$, y satisface para $x \in \mathbb{F}_p^\times$

$$\chi_{(p-1)/2}(x) = \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ es un cuadrado en } \mathbb{F}_p^\times, \\ -1 & \text{de otro modo.} \end{cases}$$

Se conoce como caracter cuadrático porque es el único caracter χ de $\mathbb{F}_p^\times$ con $\chi^2 \equiv \chi_0$.

Será conveniente para algunas aplicaciones extender los caracteres multiplicativos en $\mathbb{F}_p^\times$ al cuerpo completo imponiendo $\chi(0) = 0$. Esta extensión es compatible con la estructura de caracter: $\chi(c \cdot 0) = \chi(c)\chi(0)$ para todo $c \in \mathbb{F}_p$.

Además con esta nueva definición tenemos que

$$\sum_{c \in \mathbb{F}_p} \chi(c) = \begin{cases} p-1 & \text{si } \chi \text{ es trivial,} \\ 0 & \text{de otro modo.} \end{cases} \tag{7}$$

Veamos ahora alguna propiedad del caracter cuadrático.

Teorema 11 (Euler)**.** *Sea p un primo. Para todo $n \in \mathbb{F}_p$ se tiene*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p},$$

donde $\left(\frac{\cdot}{p}\right)$ denota el símbolo de Legendre.

Demostración. Claramente la identidad se tiene para $n \equiv 0 \pmod{p}$, de modo que podemos asumir que $n \not\equiv 0 \pmod{p}$. En primer lugar, nótese que si $n = m^2$ para algún m, entonces

$$n^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}.$$

Como $\mathbb{F}_p^\times$ es cíclico de orden $p-1$, con una raíz primitiva g, el conjunto de cuadrados

$$\{n \in \mathbb{F}_p^\times : n = m^2 \text{ para algún } m \in \mathbb{F}_p^\times\} = \{g^2, g^4, g^6, \ldots, g^{p-1}\}$$

tiene exactamente $\frac{p-1}{2}$ elementos. Además, la ecuación $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ tiene a lo sumo $\frac{p-1}{2}$ soluciones distintas, así que estas son todas.

Por último, nótese que para todo n se tiene que $\left(n^{\frac{p-1}{2}}\right)^2 = n^{p-1} \equiv 1 \pmod{p}$, lo que implica que para no-residuos cuadráticos

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

que concluye la demostración □

2. Sumas de caracteres

Para la mayoría de las aplicaciones nos interesaremos por el comportamiento de sumas de la forma:

$$\sum_{a \in A} \psi(f(a)), \tag{8}$$

donde $A \subseteq \mathbb{F}_p$ es un conjunto (una variedad, un conjunto de Sidon, el sonjunto de soluciones a cierta ecuación, etc.), ψ un caracter (aditivo o multiplicativo) en $\mathbb{F}_p$ y f es alguna función interesante en $\mathbb{F}_p$ (generalmente un polinomio). Siempre que $A = \mathbb{F}_p$, diremos que la suma es *completa* y de otro modo diremos que es una suma *incompleta*.

En algunos casos –los menos– se obtienen fórmulas cerradas para el valor de ciertas sumas de caracteres. En general sólo podemos esperar obtener cotas no triviales para la cantidad en (8): *i.e.* cualquier cota superior mejor que

$$\left|\sum_{a \in A} \psi(f(a))\right| \leq \sum_{a \in A} \left|\psi(f(a))\right| = |A|.$$

El objetivo de nuestro estudio será encontrar cotas de la forma:

$$\left|\sum_{a \in A} \psi(f(a))\right| \leq \Delta |A|$$

donde o bien $\Delta < 1$ es una constante o bien, en los mejores casos, $\Delta = \Delta(|A|)$ es una cantidad que tiende a cero cuando $|A|$, p tienden a infinito.

2.1. Sumas completas

El siguiente resultado, que se obtiene a partir de la ortogonalidad de los caracteres, sugiere que las sumas de caracteres pueden emplearse para contar soluciones a ciertas congruencias.

Corolario 12. *Sean ψ_a, ψ_b dos caracteres aditivos en $\mathbb{F}_p$. Entonces,*

$$\frac{1}{p}\sum_{c\in\mathbb{F}_p}\psi_a(c)\overline{\psi_b(c)} = \begin{cases} 1 & si\ a=b, \\ 0 & si\ a\neq b \end{cases}$$

Además, sumando sobre todos los caracteres aditivos, tenemos que

$$\frac{1}{p}\sum_{\psi}\psi(c)\overline{\psi(d)} = \begin{cases} 1 & si\ c=d, \\ 0 & si\ c\neq d. \end{cases}$$

Demostración. Nótese que el caracter $\psi_a \cdot \overline{\psi_b} = \psi_a \cdot \psi_{-b} = \psi_0$ si y sólo si $a = b$ y que para cualquier caracter ψ tenemos que $\psi(c)\overline{\psi(d)} = \psi(c-d)$ si ψ es aditivo. El resultado se sigue ahora del Teorema 6 y las observaciones previas. □

En particular, para cualquier función f se tiene que:

$$\frac{1}{p}\sum_{a\in\mathbb{F}_p}\psi_a(f(c))\overline{\psi_a(d)} = \begin{cases} 0 & \text{si } f(c)\neq d \\ 1 & \text{si } f(c)=d, \end{cases}$$

lo que implica que

$$\#\{c : f(c)=d\} = \frac{1}{p}\sum_{c\in\mathbb{F}_p}\sum_{a\in F_p}\psi_a(f(c))\overline{\psi_a(d)}. \tag{9}$$

Nótese que el resultado análogo se obtiene para caracteres multiplicativos ajustando la constante en la suma y análogamente uno obtiene:

$$\#\{c : f(c)=d\} = \frac{1}{p-1}\sum_{c\in\mathbb{F}_p}\sum_{a=0}^{p-2}\chi_a(f(c))\overline{\chi_a(d)}. \tag{10}$$

Las ecuaciones (9) y (10) pueden emplearse para codificar muchos problemas y, una vez expresados en términos de sumas de caracteres, explotar las técnicas que se discutirán en las siguientes secciones.

2.2. Sumas incompletas

El primer ejemplo no trivial de una cota general para sumas de caracteres incompletas en cuerpos primos se presenta a continuación. En este caso el conjunto A en (8) es un intervalo modulo p.

Proposición 13. *Para un primo p y un entero $0 \leq N \leq p-1$*

$$\sum_{\varphi}\left|\sum_{x=0}^{N-1}\varphi(x)\right| = O\left(p\log p\right),$$

donde la suma se toma sobre todos los caracteres aditivos de $\mathbb{F}_p$.

Nótese que la cota trivial en 13 es precisamente pN, que significa que el resultado es no trivial siempre que N sea mayor que $\log p$.

Demostración. Recordemos que todos los caracteres aditivos en $\mathbb{F}_p$ son de la forma $\varphi_a(x) = e^{2\pi iax/p}$ para algún $a \in \mathbb{F}_p$. Por tanto, siempre que $a \neq 0$ la suma

$$\sum_{x=0}^{N}\varphi_a(x) = \mathbf{e}_p(a)^0 + \mathbf{e}_p(a) + \mathbf{e}_p(a)^2 + \cdots + \mathbf{e}_p(a)^{N-1}$$

es una progresión geométrica de razón $\mathbf{e}_p(a) \neq 1$, ya que $\varphi_a \neq \varphi_0$. Por tanto

$$\left| \sum_{x=0}^{N-1} \varphi(x) \right| = \left| \frac{\mathbf{e}_p(a)^N - 1}{\mathbf{e}_p(a) - 1} \right| \leq \frac{2}{|\mathbf{e}_p(a) - 1|}. \tag{11}$$

Dado que

$$|\mathbf{e}_p(a) - 1| = |\exp(\pi i a/p) - \exp(-\pi i a/p)| = 2|\sin(\pi a/p)|,$$

y

$$|\sin(\pi a/p)| = |\sin(\pi(p-a)/p)| \geq \frac{2\,\text{mín}\{a, p-a\}}{p}$$

pues $\sin(\alpha) \geq 2\alpha/\pi$ para $0 \leq \alpha \leq \pi/2$. Incluyendo estas estimaciones en (11) se tiene para φ_a, $a \neq 0$,

$$\left| \sum_{x=0}^{N-1} \varphi_a(x) \right| \leq \frac{p}{2\,\text{mín}\{a, p-a\}}.$$

Para el caracter trivial se tiene

$$\varphi_0(0) + \varphi_0(1) + \cdots + \varphi_0(N-1) = N \leq p - 1.$$

Sumando sobre todos los caracteres obtenemos el resultado deseado

$$\sum_{a=0}^{p-1} \left| \sum_{x=0}^{N-1} \varphi_a(x) \right| \leq N + \sum_{a=1}^{p-1} \frac{p}{2\,\text{mín}\{a, p-a\}} \leq N + \sum_{a=1}^{(p-1)/2} \frac{p}{a} = O(p \log p).$$

□

A continuación obtendremos una estimación no trivial para conjuntos mucho más generales. Para cualquier número complejo $x \in \mathbb{C}^\times$ se tiene $|x|^2 = x \cdot \overline{x}$. Entonces, para cualquier caracter aditivo φ y cualquier conjunto $\mathcal{X}$ de $\mathbb{F}_p$ se tiene:

$$\left| \sum_{a \in \mathcal{X}} \varphi(a) \right|^2 = \left(\overline{\sum_{a \in \mathcal{X}} \varphi(a)} \right) \cdot \left(\sum_{b \in \mathcal{X}} \varphi(b) \right) = \sum_{a,b \in \mathcal{X}} \varphi(b-a). \tag{12}$$

Dados $\mathcal{X}$ e $\mathcal{Y}$ subconjuntos arbritrarios de $\mathbb{F}_p$, para un caracter aditivo dado φ definiremos la suma

$$W_\varphi = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \varphi(xy).$$

De forma trivial se obtiene la cota $|W_\varphi| \leq |\mathcal{X}||\mathcal{Y}|$ y la igualdad se alcanza para $\varphi = \varphi_0$ el caracter trivial. El siguiente resultado mejora la cota trivial incluso para conjuntos muy poco densos, siempre y cuando $|\mathcal{X}||\mathcal{Y}| \geq p$.

Teorema 14. *Para cualesquiera subconjuntos $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$, se tiene*

$$\max_{\varphi \neq \varphi_0} |W_\varphi| \leq (|\mathcal{X}||\mathcal{Y}|p)^{1/2}.$$

Demostración. Claramente

$$|W_\varphi| = \left| \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \varphi(xy) \right| \leq \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \varphi(xy) \right|.$$

A partir de la desigualdad de Cauchy-Schwarz[2] se tiene que

$$|W_\varphi|^2 \leq |\mathcal{X}| \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \varphi(xy) \right|^2 \leq |\mathcal{X}| \sum_{x \in \mathbb{F}_p} \left| \sum_{y \in \mathcal{Y}} \varphi(xy) \right|^2.$$

[2]Para cualesquiera $2n$ números complejos $x_1, y_1, \ldots, x_n, y_n$ se tiene $|\sum_{i=1}^n x_i \overline{y_i}|^2 \leq \sum_{i=1}^n |x_i|^2 \sum_{i=1}^n |y_i|^2$.

Se sigue de (12) que

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{y\in\mathcal{Y}}\varphi(xy)\right|^2=\sum_{x\in\mathbb{F}_p}\sum_{y_1,y_2\in\mathcal{Y}}\varphi(x(y_1-y_2))=\sum_{y_1,y_2\in\mathcal{Y}}\sum_{x\in\mathbb{F}_p}\varphi(x(y_1-y_2)).$$

A partir del Teorema 8 y de (4) se tiene

$$\sum_{x\in\mathbb{F}_p}\varphi(x(y_1-y_2))=\sum_{\psi}\psi(y_1-y_2)=\begin{cases}p & \text{si } y_1=y_2,\\ 0 & \text{en otro caso.}\end{cases}$$

De donde se sigue

$$|W_\varphi|^2\le|\mathcal{X}||\mathcal{Y}|p.$$

□

3. Algunos ejemplos famosos

3.1. Sumas de Gauss

Para un caracter aditivo φ de $\mathbb{F}_p$ y χ uno multiplicativo, se define la suma de Gauss $G(\varphi,\chi)$ como

$$G(\varphi,\chi):=\sum_{c\in\mathbb{F}_p}\varphi(c)\chi(c).$$

El valor absoluto de $G(\varphi,\chi)$ está trivialmente acotado por $p-1$ (puesto que $\chi(0)=0$ para todo χ). La igualdad se alcanza en el caso $\varphi=\varphi_0$ y $\chi=\chi_0$, pero en la mayoría de casos esta cantidad es considerablemente menor.

Nótese que se sigue de (7) que $G(\varphi_0,\chi)=0$, si $\chi\neq\chi_0$, y de (3) que

$$G(\varphi,\chi_0)=\sum_{c\in\mathbb{F}_p^\times}\varphi(c)=\sum_{c\in\mathbb{F}_p}\varphi(c)-\varphi(0)=-1,$$

si $\varphi\neq\varphi_0$. Sin embargo, cuando los caracteres son ambos no triviales, el la suma resulta es más interesante.

Teorema 15. *Sea φ un caracter aditivo y χ uno multiplicativo en $\mathbb{F}_p$. Si $\varphi\neq\varphi_0$ y $\chi\neq\chi_0$, entonces*

$$|G(\varphi,\chi)|=p^{1/2}.$$

Demostración.

$$|G(\varphi,\chi)|^2=\overline{G(\varphi,\chi)}G(\varphi,\chi)=\sum_{b\in\mathbb{F}_p^\times}\sum_{a\in\mathbb{F}_p^\times}\overline{\varphi(b)}\,\overline{\chi(b)}\,\varphi(a)\,\chi(a)=\sum_{b\in\mathbb{F}_p^\times}\sum_{a\in\mathbb{F}_p^\times}\varphi(a-b)\chi(ab^{-1}).$$

En la suma interior haremos la sustitución $ab^{-1}=c$, y por tanto $a-b=b(c-1)$. Entonces

$$\begin{aligned}|G(\varphi,\chi)|^2&=\sum_{b\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times}\varphi(b(c-1))\chi(c)\\&=\sum_{c\in\mathbb{F}_p^\times}\chi(c)\left(\sum_{b\in\mathbb{F}_p}\varphi(b(c-1))-\varphi(0)\right)=\sum_{c\in\mathbb{F}_p^\times}\chi(c)\sum_{b\in\mathbb{F}_p}\varphi(b(c-1)),\end{aligned}\tag{13}$$

dado que del Teorema 6 se sigue que $\sum_{c\in\mathbb{F}_p^\times}\chi(c)\varphi(0)=0$. Del mismo resultado se sigue que la suma

$$\sum_{b\in\mathbb{F}_p}\varphi(b(c-1))=\begin{cases}p & \text{if } c=1,\\ 0 & \text{if } c\neq1.\end{cases}$$

Incluyendo la igualdad anterior en (13) se obtiene $|G(\varphi,\chi)|^2=\chi(1)p=p$. □

Las sumas de Gauss, tal y como las hemos definido anteriormente, tienen distintas aplicaciones conectando caracteres aditivos y multiplicativos y en ocasiones nos permiten estimar ciertas sumas exponenciales.

Corolario 16. *Para cualquier primo $p \geq 3$ y un entero a con $\gcd(a,p) = 1$, se tiene*

$$\Big|\sum_{x=0}^{p-1} \mathbf{e}_p(ax^2)\Big| = p^{1/2}.$$

Demostración. Sea $\left(\frac{\cdot}{p}\right)$ el símbolo de Legendre descrito en el Ejemplo 10 y recordemos que $\mathbf{e}_p(ac) = \varphi_a(c)$ es un caracter aditivo no trivial cuando $\gcd(a,p) = 1$.

Nótese que la cantidad $\left(\left(\frac{c}{p}\right)+1\right) \in \{0,1,2\}$ cuenta el número de soluciones a $x^2 \equiv c \pmod p$, para cualquier $c \in \mathbb{F}_p$. Entonces

$$\sum_{x=0}^{p-1} \mathbf{e}_p(ax^2) = \sum_{c\in\mathbb{F}_p} \varphi_a(c)\left(\left(\tfrac{c}{p}\right)+1\right) = G\big(\varphi, \left(\tfrac{\cdot}{p}\right)\big) + \sum_{c\in\mathbb{F}_p} \varphi_a(c) = G\big(\varphi_a, \left(\tfrac{\cdot}{p}\right)\big),$$

ya que a partir de (3) se sigue que $\sum_{c\in\mathbb{F}_p} \varphi_a(c) = 0$ siempre y cuando $\gcd(a,p) = 1$. El resultado se sigue del Teorema 15. □

3.2. Sumas de Jacobi

Para dos caracteres multiplicativos χ, ψ en $\mathbb{F}_p$, la *suma de Jacobi* asociada a ψ y χ queda definida por

$$J(\psi,\chi) := \sum_{c\in\mathbb{F}_p} \chi(c)\psi(1-c) = \sum_{x+y=1} \chi(x)\psi(y).$$

Esta sumas pueden, sorprendentemente, ser expresables en términos de sumas de Gauss.

Teorema 17. *Sean χ y ψ dos caracteres multiplicativos no triviales en $\mathbb{F}_p$ tales que $(\chi\psi) \neq \chi_0$. Entonces para cualquier caracter aditivo φ no trivial se tiene*

$$J(\chi,\psi) = \frac{G(\varphi,\chi)G(\varphi,\psi)}{G(\varphi,\chi\psi)}.$$

Demostración. En primer lugar nótese que el denominador $G(\varphi,\chi\psi) \neq 0$ por hipótesis. Por tanto a partir de las definiciones se tiene

$$\begin{aligned} J(\chi,\psi)G(\varphi,\chi\psi) &= \sum_{x\in\mathbb{F}_p} \chi(x)\psi(1-x) \sum_{y\in\mathbb{F}_p^\times} \chi(y)\psi(y)\varphi(y) \\ &= \sum_{x\in\mathbb{F}_p} \sum_{y\in\mathbb{F}_p^\times} \chi(xy)\psi((1-x)y)\varphi(y). \end{aligned}$$

Recordemos que extendimos los caracteres multiplicativos a $\mathbb{F}_p$ tras imponer $\chi(0) = \psi(0) = 0$, entonces podemos restringir la suma a $x \neq \{0,1\}$. Para $u = xy$ y $v = y - xy$, tenemos un cambio de variable biyectivo de $(x,y) \in \big(\mathbb{F}_p \setminus \{0,1\}\big) \times \mathbb{F}_p^\times$ a

$$\{(u,v) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times : u+v \neq 0\}.$$

ya que a partir de u, v podemos recuperar x e y como $y = u+v, x = u/(u+v)$. Así se tiene

$$\begin{aligned} J(\chi,\psi)G(\varphi,\chi\psi) &= \sum_{\substack{u,v\in\mathbb{F}_p^\times \\ u+v\neq 0}} \chi(u)\psi(v)\varphi(u+v) \\ &= \Big(\sum_{u\in\mathbb{F}_p^\times} \chi(u)\varphi(u)\Big)\Big(\sum_{v\in\mathbb{F}_p^\times} \psi(v)\varphi(v)\Big) - \sum_{u\in\mathbb{F}_p^\times} \chi(u)\psi(-u) \\ &= G(\varphi,\chi)G(\varphi,\psi) - \psi(-1)\sum_{u\in\mathbb{F}_p^\times} (\chi\psi)(u) \\ &= G(\varphi,\chi)G(\varphi,\psi), \end{aligned}$$

ya que por el Teorema 6 se tiene

$$\sum_{u\in\mathbb{F}_p^\times}(\chi\psi)(u)=0$$

dado que $\chi\psi$ es un caracter no trivial por hipótesis. □

Corolario 18. *Sean χ y ψ dos caracteres multiplicativos no triviales en $\mathbb{F}_p$ tales que $(\chi\psi)\neq\chi_0$. Entonces,*

$$|J(\chi,\psi)|=p^{1/2}.$$

Demostración. Se sigue del Teorema 15 que para cualesquiera caracteres no triviales φ,χ (aditivos y multiplicativos) se tiene $|G(\varphi,\chi)|=p^{1/2}$. El resultado se sigue del Teorema 17. □

3.3. Sumas de Kloosterman

Para dos caracteres aditivos en $\mathbb{F}_p$, definimos la *suma de Kloosterman* $K(\varphi,\psi)$ asociada como

$$K(\varphi,\psi):=\sum_{c\in\mathbb{F}_p^\times}\varphi(c)\psi(c^{-1})=\sum_{xy\equiv 1(p)}\varphi(x)\psi(y). \tag{14}$$

Nótese que $K(\varphi,\psi)$ es siempre un número real, puesto que

$$\overline{K(\varphi,\psi)}=\sum_{c\in\mathbb{F}_p^\times}\overline{\varphi(c)\psi(c^{-1})}=\sum_{c\in\mathbb{F}_p^\times}\varphi(-c)\psi(-c^{-1})=\sum_{d\in\mathbb{F}_p^\times}\varphi(d)\psi(d^{-1})=K(\varphi,\psi),$$

tras realizar el cambio de variable $d=-c$.

Para cada $b\in\mathbb{F}_p^\times$ tenemos que

$$K(\varphi,\psi)=K(\varphi_b,\psi_{b^{-1}}) \tag{15}$$

donde $\varphi_b(x)=\varphi(bx)$ y $\psi_{b^{-1}}(x)=\psi(b^{-1}x)$.

Teorema 19 (Kloosterman)**.** *Sean φ,ψ dos caracteres aditivos no triviales en $\mathbb{F}_p$. Entonces*

$$|K(\varphi,\psi)|<2p^{3/4}.$$

La idea tras de la prueba de este resultado se basa en intentar entender las sumas de Kloosterman globalmente, en vez de individualmente. Más concretamente, la idea es utilizar el siguiente hecho: si somos capaces de probar que para los momentos $k-$ésimos

$$M_k=\sum_{\varphi,psi\neq\varphi_0}|K(\varphi,\psi)|^{2k}\leq M$$

para $k\geq 1$ y algún $M\geq 0$, entonces para cada par φ,ψ podemos deducir de (15) que

$$(p-1)|K(\varphi,\psi)|^{2k}=\sum_{b\in\mathbb{F}_p^\times}|K(\varphi_b,\psi_{b^{-1}})|^{2k}\leq M,$$

y por tanto

$$|K(\varphi,\psi)|\leq\left(\frac{M}{p-1}\right)^{1/2k}. \tag{16}$$

Ahora, para cada $k\geq 1$ tenemos

$$M_k=\sum_{\varphi,\psi}|K(\varphi,\psi)|^{2k}-2\sum_{\varphi\neq\varphi_0}|K(\varphi,\varphi_0)|^{2k}-|K(\varphi_0,\varphi_0)|^{2k}$$

y se sigue del Corolario 12 que $K(\varphi,\varphi_0)=-1$ para todo $\varphi\neq\varphi_0$. Por tanto

$$M_k=\sum_{\varphi,\psi}|K(\varphi,\psi)|^{2k}-2(p-1)-(p-1)^{2k}.$$

Para probar el Teorema 19 necesitaremos el siguiente resultado auxiliar.

Proposición 20. *Los primeros momentos normalizados para las sumas de Kloosterman son*

$$\frac{M_0}{(p-1)^2} = 1, \quad \frac{M_1}{(p-1)^2} = \frac{p^2-p-1}{p-1}, \quad \frac{M_2}{(p-1)^2} = \frac{2p^3-3p^2-3p-1}{(p-1)}.$$

Demostración. La igualdad de M_0 es trivial, de modo que comenzaremos con M_1. De nuevo, se sigue de (12) que

$$\begin{aligned} M_1 &= \sum_{\varphi,\psi} |K(\varphi,\psi)|^2 - 2(p-1) - (p-1)^2 \\ &= \sum_{\varphi,\psi} \sum_{c,d\in\mathbb{F}_p^\times} \varphi(c-d)\psi(c^{-1}-d^{-1}) - 2(p-1) - (p-1)^2 \\ &= \sum_{c,d\neq 0} \Big(\sum_{\varphi} \varphi(c-d)\Big)\Big(\sum_{\psi} \psi(c^{-1}-d^{-1})\Big) - 2(p-1) - (p-1)^2 \\ &= p^2(p-1) - 2(p-1) - (p-1)^2 = (p-1)\big(p^2-p-1\big) \end{aligned}$$

puesto que

$$\Big(\sum_{\varphi} \varphi(c-d)\Big)\Big(\sum_{\psi} \psi(c^{-1}-d^{-1})\Big) = \begin{cases} p^2 & \text{si } c=d \\ 0 & \text{de otro modo.} \end{cases}$$

Ahora analizaremos la fórmula de M_2. Nótese que

$$\begin{aligned} M_2 &= \sum_{\varphi,\psi} \sum_{a,b,c,d,\in\mathbb{F}_p^\times} \varphi(a+c-b-d)\psi(a^{-1}+c^{-1}-b^{-1}-d^{-1}) - 2(p-1) - (p-1)^4 \\ &= \sum_{a,b,c,d,\in\mathbb{F}_p^\times} \Big(\sum_{\varphi} \varphi(a+c-b-d)\Big)\Big(\sum_{\psi} \psi(a^{-1}+c^{-1}-b^{-1}-d^{-1})\Big) - 2(p-1) - (p-1)^4. \end{aligned}$$

De nuevo, por la ortogonalidad de los caracteres, tenemos que el producto de sumas

$$\Big(\sum_{\varphi} \varphi(a+c-b-d)\Big)\Big(\sum_{\psi} \psi(a^{-1}+c^{-1}-b^{-1}-d^{-1})\Big)$$

es p^2 si la cuádrupla $a,b,c,d \in \mathbb{F}_p^\times$ satisface

$$\begin{cases} a+c = b+d \\ \frac{1}{a}+\frac{1}{c} = \frac{1}{b}+\frac{1}{d} \end{cases} \tag{17}$$

y cero en otro caso. Ahora deberemos contar el número de soluciones a (17):

1. Claramente si $\{a,c\} = \{b,d\}$ la cuádrupla (a,b,c,d) satisface (17). Hay exactamente $2(p-1)^2-(p-1)$ de estas.

2. Si $a=-c$, entonces $a+c=b+d=0$ y tenemos $(p-1)^2$ de estas parejas:

   $$(x,y,-x,-y) \quad x,y\in\mathbb{F}_p^\times$$

   pero $2(p-1)$ de ellas estan incluídas en el caso anterior (aquellas de la forma $(x,x,-x-x)$ y $(x,-x,-x,x)$ para aglún $x\in\mathbb{F}_p^\times$). Entonces, debemos añadir $(p-1)^2-2(p-1)$ a la cuenta final.

3. Supongamos que (a,b,c,d) es una solución no contada anteriormente: $a+c\neq 0$ y $\{a,c\}\neq\{b,d\}$. Entonces se sigue de (17) que

   $$\begin{aligned} a+c &= b+d, \\ bd(a+c) &= ac(b+d). \end{aligned}$$

   Sustituyendo a nos queda

   $$bd(b+d) = c(b+d-c)(b+d)$$

   y por tanto $bd = c(b+d-c)$. Esto implica que $b(d-c) = c(d-c)$, que contradice el hecho de que $c\neq b,d$ por hipótesis.

Por tanto, el número total de parejas que satisfacen (17) es precisamente $3(p-1)^2 - 3(p-1)$. Entonces,

$$M_2 = p^2(3(p-1)^2 - 3(p-1)) - 2(p-1) - (p-1)^4 = (p-1)\big(2p^3 - 3p^2 - 3p - 1\big).$$

□

Demostración del Teorema 19. Se sigue de (16) y la Proposición 20 que

$$\big|K(\varphi,\psi)\big| \leq \big((p-1)M_2\big)^{1/4} = \big(2p^3 - (3p^2+3p+1)\big)^{1/4} < 2p^{3/4}$$

para cada pareja de caracteres no triviales φ, ψ. □

La mejor cota conocida, que no probaremos aquí, fue obtenida por Weil mediante argumentos de geometría algebraica relacionados con el estudio de las funciones zeta para variedades algebraicas en cuerpos primos.

Teorema 21 (Weil)**.** *Sea p un número primo y φ, ψ dos caracteres aditivos no triviales. Entonces*

$$|K(\varphi,\psi)| \leq 2\sqrt{p}.$$

El resultado de Weil es en cierto sentido óptimo, tal y como indica el siguiente resultado.

Corolario 22. *Para al menos una pareja de caracteres aditivos no triviales φ, ψ, se tiene*

$$|K(\varphi,\psi)| > \sqrt{2p-2}.$$

Demostración. De la definición de las cantidades M_1, M_2 se sigue que

$$M_2 \leq \big(\max_{\varphi,\psi\neq\varphi_0} |K(\varphi,\psi)|^2\big) M_1,$$

y entonces existe al menos una pareja φ, ψ para la cual

$$|K(\varphi,\psi)|^2 \geq \frac{M_2}{M_1} = \frac{2p^3 - 3p^2 - 3p - 1}{p^2 - p - 1} > 2p - 2,$$

de la Proposición 20. □

3.4. Cota de Pólya-Vinogradov

El siguiente resultado es otro ejemplo de una suma incompleta. Podría entenderse tanto como el análogo multiplicativo de la Proposición 13 o como una truncación de la suma de Gauss $G(\varphi_0, \chi)$.

Teorema 23 (Pólya-Vinogradov)**.** *Para todo entero N, $1 \leq N \leq p-1$ y un caracter multiplicativo no trivial dado χ se tiene*

$$\sum_{x=1}^{N} \chi(x) = O\left(p^{1/2}\log p\right).$$

Demostración. Dado un elemento $a \in \mathbb{F}_p$ denotemos por $S(a)$ la siguiente suma de Gauss

$$S(a) = G(\varphi_a, \chi\big) = \sum_{c=1}^{p-1} \varphi_a(c)\chi(c).$$

Se sigue del Teorema 15 que $|S(a)| = p^{1/2}$ si $a \neq 0$ y de la ortogonalidad de los caracteres $S(0) = 0$.

Utilizando el Corolario 12 obtenemos

$$\begin{aligned}\left|\sum_{c=1}^{N}\chi(c)\right| &= \left|\sum_{c=1}^{p-1}\chi(c)\left(\frac{1}{p}\sum_{a\in\mathbb{F}_p}\sum_{d=1}^{N}\varphi_a(x-y)\right)\right| \\ &= \frac{1}{p}\left|\sum_{a\in\mathbb{F}_p}S(a)\sum_{d=1}^{N}\varphi_a(-y)\right| \\ &\leq \frac{1}{p}\sum_{a\in\mathbb{F}_p}|S(a)|\left|\sum_{d=1}^{N}\varphi_a(-y)\right| \\ &= \frac{p^{1/2}}{p}\sum_{a\in\mathbb{F}_p}\left|\sum_{d=1}^{N}\varphi_a(-y)\right| = O\big(p^{1/2}\log p\big)\end{aligned}$$

puesto que la Proposición 13 implica

$$\sum_{a\in\mathbb{F}_p}\left|\sum_{d=1}^{N}\varphi_a(-y)\right| = \sum_{b\in\mathbb{F}_p}\left|\sum_{d=1}^{N}\varphi_b(y)\right| = O(p\log p)$$

haciendo el cambio de variable $a=-b$. □

3.5. Cotas de Weil

Dado φ un caracter aditivo no trivial de $\mathbb{F}_p$ y $f\in\mathbb{F}_p[x]$ un polinomio de grado positivo. Consideraremos las sumas de la forma

$$\sum_{c\in\mathbb{F}_p}\varphi(f(c)),$$

que en ocasiones son llamadas sumas de Weil.

Obsérvese que si $f(x)=ax+b$, entonces las sumas pueden estimarse de forma sencilla a partir de las relaciones de ortogonalidad. También, si f es un polinomio cuadrático estas sumas pueden expresarse en términos de las sumas de Gauss estudiadas en la Sección 3.1 tras completar cuadrados en $\mathbb{F}_p$.

Para un polinomio general André Weil demostró, a partir de resultados profundos de geometría algebraica, el siguiente resultado.

Teorema 24. *Sea $f\in\mathbb{F}_p[x]$ un polinomio de grado $d\geq 1$ con $\gcd(d,p)=1$ u sea ψ un caracter aditivo no trivial de $\mathbb{F}_p$. Entonces*

$$\left|\sum_{x\in\mathbb{F}_p}\psi(f(x))\right| \leq (d-1)p^{1/2}.$$

La misma cota se obtiene para caracteres multiplicativos.

Teorema 25. *Sea χ un caracter multiplicativo no trivial de $\mathbb{F}_p$ de orden m y sea $f\in\mathbb{F}_p[x]$ un polinomio mónico de grado $d\geq 1$ que no es una potencia m-ésima de un polinomio. Entonces,*

$$\left|\sum_{x\in\mathbb{F}_p}\chi(f(x))\right| \leq (d-1)p^{1/2}.$$

Podemos utilizar el resultado de Weil para probar la siguiente cota para el número de soluciones a ecuaciones en cuerpos finitos.

Corolario 26. *Sea $m\in\mathbb{N}$ y $f\in\mathbb{F}_p[x]$ un polinomio mónico de grado $d\geq 1$ tal que $y^t-f(x)$ es absolutamente irreducible, donde $t=\gcd(m,p-1)$. Entonces el número de soluciones a $y^m=f(x)$ en $\mathbb{F}_p$ es*

$$|N-p| \leq (t-1)(d-1)p^{1/2}.$$

Demostración. Nótese que para cualquier m dado y cualquier caracter multiplicativo ψ

$$\sum_{y\in\mathbb{F}_p}\psi(y^m)=\sum_{y\in\mathbb{F}_p}\psi^m(y)=\begin{cases}p & \text{si } \psi^m=\chi_0,\\ 0 & \text{en otro caso,}\end{cases}$$

y $\psi^m=\chi_0$ si y sólo si el orden de ψ divide a m. De hecho, si $t=\gcd(m,p-1)$ y χ es un caracter multiplicativo de orden t, entonces los únicos caracteres de orden dividiendo a m son precisamente

$$\chi,\chi^2,\dots,\chi^{t-1},\chi^t=\chi_0.$$

Por tanto,

$$N=\frac{1}{p}\sum_{\psi}\sum_{x\in\mathbb{F}_p}\psi(f(x))=\sum_{j=0}^{t-1}\sum_{x\in\mathbb{F}_p}\chi^j(f(x)).$$

Separando la contribución de $j=0$ del resto y aplicando el Teorema 25 tenemos que

$$|N-p|\le\sum_{j=1}^{t-1}\Big|\sum_{x\in\mathbb{F}_p}\chi^j(f(x))\Big|\le(t-1)(d-1)p^{1/2}.$$

□

4. Aplicaciones

A continuación presentaremos una serie de aplicaciones directas de los resultados que hemos presentado, que ilustran varias estrategias clásicas aplicadas a distintos problemas en teoría de números.

4.1. Primos suma de cuadrados

El siguiente resultado se le atribuye a Fermat, que sin embargo no dejó demostración alguna. La primera demostración conocida se debe a Euler, bastante complicada y basada en argumentos de descenso infinito. Se conocen demostraciones muy variadas que emplean la factorización de enteros Gaussianos, fracciones continuas, formas cuadráticas o incluso el teorema de Minkowski.

Aquí incluimos una demostración simple a partir de sumas de Jacobi que puede encontrarse en [7, Cap. 8].

Teorema 27 (Fermat)**.** *Sea p un primo tal que $p\equiv 1 \pmod 4$. Entonces existen enteros a,b tales que*

$$p=a^2+b^2.$$

Demostración. Puesto que $p\equiv 1 \pmod 4$, entonces existe un paracter multiplicativo de orden 4 en $\mathbb{F}_p$, denotado por $\chi_{\frac{p-1}{4}}$.

Nótese que dicho caracter toma valores en las cuartas raíces de la unidad en $\mathbb{C}$. Es decir: $\chi_{(p-1)/4}(x)\in\{1,-1,i,-i\}$ para todo $x\in\mathbb{F}_p^\times$.

Por tanto, dado que el caracter cuadrático sólo toma valores en $\{1,-1\}$, la suma de Jacobi

$$J\big(\big(\tfrac{\cdot}{p}\big),\chi_{(p-1)/4}\big)=\sum_{x+y\equiv 1\,(p)}\big(\tfrac{x}{p}\big)\chi_{(p-1)/4}(y)=a+bi,$$

para ciertos $a,b\in\mathbb{Z}$.

Se sigue del Corolario 18 que

$$\big|J\big(\big(\tfrac{\cdot}{p}\big),\chi_{\frac{(p-1)}{4}}\big)\big|^2=a^2+b^2=p.$$

□

4.2. El mínimo residuo no-cuadrático

En $\mathbb{F}_p$ hay exactamente $\frac{p+1}{2}$ residuos cuadráticos (incluyendo el 0) y $\frac{p-1}{2}$ residuos no cuadráticos. Si ordenamos los residuos $\{0, 1, 2, ..., p-1\}$ entonces $0, 1$ o 4 son siempre cuadrados y por ejemplo $2 \equiv 3^2 \pmod 7$ o $3 \equiv 4^2 \pmod{13}$. Incluso si consideramos $p = 18191$ el primer residuo no cuadrático es 29 y de hecho sólo hay 19 residuos no cuadráticos menores que 100:

$$\{29, 31, 37, 41, 47, 53, 58, 59, 62, 71, 73, 74, 79, 82, 87, 89, 93, 94, 97\}.$$

Con un simple ejercicio de programación uno parece poder encontrar con cierta facilidad primos para los que los primeros n residuos sean todos cuadrados, sin embargo ¿existe algún primo p para el que todos los residuos cuadráticos sean números consecutivos? La respuesta a esta pregunta es no, pero de hecho vamos a dar una respuesta mucho más contundente obteniendo cotas superiores para el menor residuo no cuadrático n_0.

Teorema 28 (Vinogradov)**.** *Sea p un primo. El mínimo residuo no cuadrático n_0 satisface*

$$n_0 \ll p^{1/2} \log p.$$

Demostración. El número de residuos cuadráticos en $[1, N]$ puede expresarse como

$$\#\{\square\text{'s en } [1, N]\} = \frac{1}{2} \sum_{c=1}^{N} \Big(1 + \Big(\frac{c}{p}\Big)\Big)$$

puesto que, como ya vimos en la prueva del Corolario 16, $\big(1 + \big(\frac{c}{p}\big)\big)$ cuenta el número de soluciones a $x^2 \equiv c \pmod p$.

De modo que

$$\left|\#\{\square\text{'s en } [1, N]\} - \frac{N}{2}\right| = \sum_{x=1}^{N} \Big(\frac{x}{p}\Big) = O\big(p^{1/2} \log p\big), \tag{18}$$

por el Teorema 23.

En particular, esto implica que si n_0 denota el mínimo residuo no cuadrático en $[1, p-1]$, entonces por definición de n_0 se tiene que $\#\{\square\text{'s en } [1, n_0]\} = n_0 - 1$. Por tanto

$$n_0 = \#\{\square\text{'s en } [1, N]\} + 1 = \frac{n_0}{2} + O\big(p^{1/2} \log p\big)$$

lo que concluye la demostración. □

A pesar de que la demostración anterior es aparentemente sencilla, ha sido la mejor cota conocida durante mucho tiempo. No fue hasta las mejoras de Burgess para ciertas sumas de caracteres que se consiguió mejorar el resultado de Vinogradov obteniendo

$$n_p \ll_\epsilon p^{1/(4+\sqrt{e})+\epsilon}.$$

Sin embargo se conjetura que el mínimo residuo cuadrático aparece bastante antes, más concretamente para todo $\epsilon > 0$ se cree que

$$n_p \ll_\epsilon \log p^{1+\epsilon}.$$

Para el lector interesado, en [1] los autores utilizan una nueva estrategia para atacar el problema y prueban condicionalmente $n_p \ll \log p^{1,4}$.

4.3. Distribución puntos en la hipérbola modular

Consideremos la hipérbola modular

$$H = \{(x, y) \in \mathbb{F}_p^2 : xy \equiv 1 \pmod p\}.$$

El hecho de que exista mucha cancelación entre los términos en las sumas de Kloosterman

$$K(\varphi_a, \varphi_b) = \sum_{(x,y)\in H} e^{2\pi i(ax+by)/p}$$

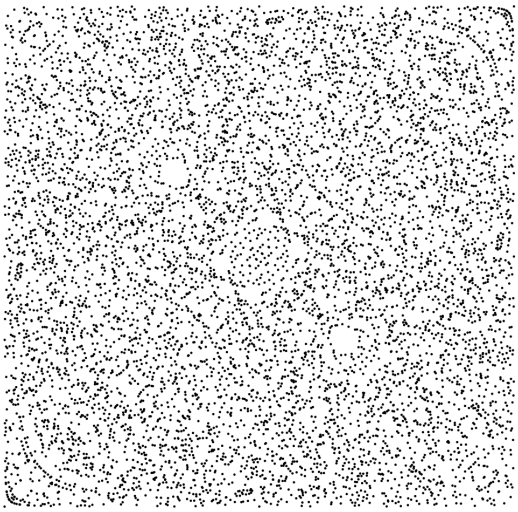
nos hace sospechar que los puntos en H deberían estar *armoniosamente distribuídos* en $\mathbb{F}_p^2$.

Estudiaremos cómo los puntos en H se distribuyen en cajas $B = [h+1, h+N] \times [t+1, t+M]$.

Teorema 29. *El número de puntos de la hipérbola H con coordenadas en una caja B cumple*

$$|H \cap B| = \frac{|B|}{p} + O\big(p^{1/2} \log^2 p\big).$$

Recordemos que la cota trivial en este caso es $|B|^{1/2}$, ya que para cada $x \in [h+1, h+N]$ existe a lo sumo un punto en la hipérbola y lo mismo sucede para cada $y \in [t+1, t+M]$. De hecho, si $|B| = o(p \log^4 p)$ la cota obtenido es peor que la trivial y si $|B| \gg p^{3/2} \log^2 p$ entonces el resultado anterior nos da la asintótica $|H \cap B| \sim |B|/p$.



Puntos en la hipérbola $xy \equiv 1 \pmod{7843}$

Tal y como parece en la figura anterior, los puntos en esta ecuación se encuentran *equidistribuidos* en los residuos $[0, p-1] \times [0, p-1]$: aunque claramente se aprecia en la figura las simetrías propias de la ecuación, si nos fijamos en una región cualquiera (una caja, por ejemplo) entonces el número de puntos con coordenadas en dicha región coincide con el número esperado.

Demostración. Recordemos que a partir de la fórmula (10) podemos codificar el número de puntos en la hipérbola con coordenadas en una caja $B = [h+1, h+N] \times [t+1, t+M]$ de la siguiente forma

$$\begin{aligned} |H \cap B| &= \frac{1}{p^2} \sum_{\varphi, \eta} \sum_{xy \equiv 1 \,(p)} \sum_{u=h+1}^{h+N} \varphi(x)\overline{\varphi(u)} \sum_{v=t+1}^{h+M} \eta(y)\overline{\eta(v)} \\ &= \frac{|H||B|}{p^2} + \frac{1}{p^2} \sum_{(\varphi,\eta) \neq (\varphi_0,\varphi_0)} \sum_{xy \equiv 1 \,(p)} \sum_{u=h+1}^{h+N} \varphi(x)\overline{\varphi(u)} \sum_{v=t+1}^{h+M} \eta(y)\overline{\eta(v)} \qquad (19) \end{aligned}$$

donde la última suma en (19) se toma sobre parejas de caracteres aditivos $(\varphi, \eta) \neq (\varphi_0, \varphi_0)$ en $\mathbb{F}_p$, aunque sí puede incluir parejas en las que uno de ellos es trivial.

Así, teniendo en cuenta que las sumas de Kloosterman se pueden reescribir como

$$K(\varphi, \eta) = \sum_{xy \equiv 1 \,(p)} \varphi(x)\eta(y)$$

reordenando la suma en (19) se tiene

$$\begin{aligned}\left||H\cap B|-\frac{|H||B|}{p^2}\right| &= \frac{1}{p^2}\left|\sum_{(\varphi,\eta)\neq(\varphi_0,\varphi_0)} K(\varphi,\eta)\Big(\sum_{u=h+1}^{h+N}\overline{\varphi(u)}\Big)\Big(\sum_{v=t+1}^{h+M}\overline{\eta(v)}\Big)\right| \\ &\leq \frac{\max\left|K(\varphi,\eta)\right|}{p^2}\sum_{\varphi}\left|\sum_{u=h+1}^{h+N}\overline{\varphi(u)}\right|\sum_{\eta}\left|\sum_{v=t+1}^{h+M}\overline{\eta(v)}\right| \\ &\ll p^{1/2}\log^2 p \end{aligned} \tag{20}$$

puesto que del Teorema 21 se sigue que $|K(\varphi,\eta)|\leq 2p^{1/2}$ y de la Proposición 13

$$\sum_{\varphi}\left|\sum_{u=h+1}^{h+N}\overline{\varphi(u)}\right|\ll p\log p$$

(y de igual modo para la suma en η). Teniendo en cuenta que $|H|=p-1$ se tiene a partir de (20) que

$$|H\cap B|=\frac{|B|}{p}-\frac{|B|}{p^2}+O\big(p^{1/2}\log^2 p\big)$$

lo que concluye la demostración, dado que por definición $|B|\leq p^2$. □

Nótese que utilizando las cotas en la sección 3.5 se pueden obtener, siguiendo las líneas de la demostración anterior, resultados análogos para ecuaciones más variadas. Para ver una discusión general sobre la aplicación de esta estrategia en conjuntos más generales, así como para una mejora del término de error consúltense [3].

4.4. Fenómeno suma-producto en cuerpos primos

Para un conjunto finito de enteros $A\subseteq\mathbb{Z}$, podemos definir sus conjuntos suma y producto

$$\begin{aligned}A+A&=\{n\in\mathbb{Z}:\ n=a+a' \text{ con } a,a'\in A\},\\ A\cdot A&=\{n\in\mathbb{Z}:\ n=aa' \text{ con } a,a'\in A\}.\end{aligned}$$

Si A es una progresión aritmética entonces es sencillo comprobar que $|A+A|=2|A|-1$; de hecho el reverso es cierto también. De manera análoga, A es una progresión geométrica si y sólo si $|A\cdot A|=2|A|-1$.

En 1983, Erdős y Szemerédi que para conjuntos de enteros el conjunto suma y conjunto producto no podían ser grandes al mismo tiempo. Más concretamente.

Conjetura 30 (Erdős-Szemerédi)**.** *Para todo conjunto $A\subseteq\mathbb{Z}$ finito y para $\epsilon>0$,*

$$\max\big(|A+A|,|A\cdot A|\big)\gg_\epsilon |A|^{2-\epsilon}.$$

Los propios Erdős y Szemerédi [4] probaron que existe $\delta>0$ tal que para todo $A\subseteq\mathbb{Z}$

$$\max\big(|A+A|,|A\cdot A|\big)\gg |A|^{1+\delta}.$$

La mejor cota se debe a Solymosi [9], que en 2009 demostró que uno era capaz de tomar $\delta<1/3$.

En este caso nos vamos a centrar en el problema análogo en cuerpos primos. En $\mathbb{F}_p$ el problema es un poco distinto: en particular, si A es un conjunto muy grande (por ejemplo $p-100$) entonces no puede crecer mucho ni bajo adición ni multiplicación, ya que está restringido por el cardinal del cuerpo ambiente.

Para poder demostrar cualquier fenómeno suma-producto en un cuerpo finito, hace falta suponer que el cardinal de A no sea del mismo orden que p. El primer resultado en esta dirección es relativamente reciente [2].

Teorema 31 (Bourgain-Katz-Tao)**.** *Sea p un primo. Para todo $\delta>0$ existe un $\varepsilon=\varepsilon(\delta)>0$ tal que para todo $A\subseteq\mathbb{F}_p$ con $p^\delta<|A|<p^{1-\delta}$ se tiene*

$$\max\big(|A+A|,|A\cdot A|\big)\gg |A|^{1+\varepsilon}.$$

Poco después, Bourgain y Konyagin quitaron la condición $|A| > p^\delta$. No daremos los detalles de la prueba (que es larga y técnica), pero sin embargo probaremos otro resultado debido a Garaev [5] que mejora el anterior en ciertos rangos del tamaño de A. Por suerte para nosotros la demostración de Garaev sólo emplea sumas de caracteres y es sorprendentemente sencilla.

Teorema 32 (Garaev)**.** *Sea p un primo y $A \subseteq \mathbb{F}_p$, entonces*

$$\max\big(|A+A|, |A\cdot A|\big) \gg \min\left(\sqrt{|A|p}, \frac{|A|^2}{\sqrt{p}}\right).$$

Nótese que el resultado es peor que trivial si $|A| \leq p^{1/2}$, pero de hecho es óptimo para todo $|A| > p^{2/3}$.

Demostración. Sin pérdida de generalidad podemos asumir que $0 \notin A$. Definimos el conjunto

$$J = \{(x, a_1, a_2, y) \in (A\cdot A)\times A\times A\times (A+A) : xa_1^{-1} + a_2 = y\},$$

y observamos que para todo $(a_1, a_2, a_3) \in A^3$ se tiene que $(a_1a_3, a_1, a_2, a_3 + a_2) \in J$, de donde $|J| \geq |A|^3$.

Así

$$\begin{aligned} |A|^3 \leq |J| &= \frac{1}{p}\sum_{b=0}^{p-1}\sum_{x\in AA}\sum_{a_1,a_2\in A}\sum_{y\in A+A}\varphi_b\big(xa_1^{-1}+a_2-y\big) \\ &\leq \frac{|A\cdot A||A|^2|A+A|}{p} + \frac{1}{p}\sum_{b=1}^{p-1}\Big|\sum_{x\in AA}\sum_{a_1\in A}\varphi_b\big(xa_1^{-1}\big)\Big|\Big|\sum_{a_2\in A}\sum_{y\in A+A}\varphi_b(a_2-y)\Big|. \quad (21) \end{aligned}$$

Se sigue del Teorema 14 que

$$\max_{\varphi\neq\varphi_0}\Big|\sum_{x\in AA}\sum_{a_1\in A}\varphi(xa_1^{-1})\Big| \leq \sqrt{p|A||A\cdot A|},$$

y para la segunda suma en (21) utilizando la desigualdad de Cauchy-Schwarz se obtiene

$$\Big|\sum_{a_2\in A}\sum_{y\in A+A}\varphi_b(a_2-y)\Big| \leq \Big(\sum_{a_2\in A}\varphi_b(a_2)^2\Big)^{1/2}\Big(\sum_{y\in A+A}\varphi_b(-y)^2\Big)^{1/2} \leq \sqrt{|A||A+A|}.$$

Combinando estas estimaciones con (21) se tiene

$$|A| \leq \frac{|A\cdot A||A+A|}{p} + \frac{\sqrt{p\,|A\cdot A||A+A|}}{|A|}$$

de donde se obtiene que

$$|A+A||A\cdot A| \gg \min\big(|A|\,p, |A|^4/p\big).$$

□

Referencias

[1] J. Bober y L. Goldmakher, Pólya-Vinogradov and the least quadratic nonresidue. `arXiv: 1311.7556`

[2] J. Bourgain, N. Katz y T. Tao, A sum-product estimate in finite fields and applications. *Geom. Funct. Anal.* **14** (2004), no. 1, 27–57.

[3] J. Cilleruelo y A. Zumalacarregui, Saving the logarithmic factor in the error term estimates of some congruence problems, *preprint.*

[4] P. Erdős y E. Szemerédi, On sums and products of integers. *Studies in pure mathematics*, 213–218, Birkhäuser, Basel, 1983.

[5] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **136** (2008), no. 8, 2735–2739.

[6] M. Z. Garaev, Sumas trigonometricas y congruencias aditivas, Gac. R. Soc. Mat. Esp. **12** (2009), no. 1, 129–143.

[7] K. Ireland y M. Rosen, *A classical introduction to modern number theory.* Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[8] H. Iwaniek y E. Kowalski, *Analytic number theory.* American Mathematical Society, Providence, RI, 2004.

[9] J. Solymosi, Bounding multiplicative energy by the sumset, *Adv. in Math.* **222** (2009), 402–408.

[10] R. Lidl y H. Niederreiter, *Finite fields.* Encyclopedia of Mathematics and its Applications, 20. Addison-Wesley Publishing Company, Reading, MA, 1983.