Caracteres de Dirichlet y sus funciones L

Índice de contenidos

1 Primos en progresiones aritméticas (I)

El objetivo de esta sección es presentar el motivo (idea) central en la demostración del *Teorema de Dirichlet* acerca de primos en progresiones aritméticas. La exposición es un resumen de [Dav80, Ch. 1] con algunas omisiones (adicionales).

1.1 La función ζ

Dado un número *real* $s > 1$, la serie

$$\sum_{n \geq 1} n^{-s} \tag{1}$$

converge.[1] De esta manera, queda definida una función cuyo valor en $s > 1$ está dado por (1); denotamos esta función por $\zeta(s)$. Dado que, para cada $n \geq 1$, $n^{-s} \leq n^{-s_0}$, si $s \geq s_0$, la serie (1) converge uniformemente en semirectas $s \geq s_0$, $s_0 > 1$.

La función $\zeta(s)$ se puede expresar como un producto infinito indexado sobre los primos:

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \ . \tag{2}$$

La expresión (2) es válida para todo $s > 1$ (real, en principio).[2] La función $\zeta(s)$ no se anula en $s > 1$, por ser una sumatoria de términos positivos (no vacía y convergente).

[1] Dada una sucesión decreciente de números reales no negativos, $a_1 \geq a_2 \geq \cdots \geq 0$, la serie $\sum_{n \geq 1} a_n$ converge, si y sólo si la serie $\sum_{k \geq 0} 2^k a_{2^k}$ converge; este es el *criterio de Cauchy*. En este caso, si $s > 0$ es real y $a_n = n^{-s}$,

$$\sum_{k \geq 0} 2^k a_{2^k} = \sum_{k \geq 0} 2^{(1-s)\,k} \ .$$

Ésta es una serie geométrica de razón 2^{1-s}, que converge exactamente en el caso $s > 1$.

[2] El producto $\prod_p$ se debe interpretar como el límite $\lim_{x \to \infty} \prod_{p \leq x}$, donde los productos se realizan sobre los primos menores que x. Dado un primo p y un número real $s > 1$, $0 < p^{-s} < 1$ y

$$\frac{1}{1 - p^{-s}} = \sum_{m \geq 0} \frac{1}{p^{ms}} \ .$$

Dado $x \geq 1$, se cumple que

$$\sum_{n \leq x} n^{-s} \leq \sum_{n \,:\, p^+(n) \leq x} n^{-s} = \prod_{p \leq x} (1 - p^{-s})^{-1} \leq \sum_{n \geq 1} n^{-s} \ ,$$

donde $p^+(n)$ denota el primo más grande que divide a n (o 1, si $n = 1$). La expresión (2) queda justificada por la convergencia de la suma parcial $\sum_{n \leq x}$ con $x \to \infty$.

Aplicando la función logaritmo a la igualdad (2), dado que es una función continua,[3]

$$\mathsf{log}\,\zeta(s) \;=\; \sum_p \sum_{m\geq 1} m^{-1}\, p^{-ms} \;.$$

Ahora, $\zeta(s)$ tiende a $+\infty$ con $s \to 1^+$,[4] con lo cual, $\mathsf{log}\,\zeta(s)$ tiende a $+\infty$, también. Pero, por otro lado,

$$\sum_p \sum_{m\geq 2} m^{-1}\, p^{-ms} \;<\; \sum_p \sum_{m\geq 2} p^{-m} \;=\; \sum_p \frac{1}{p\,(p-1)} \;<\; 1 \;.$$

De esto se deduce que el término restante,

$$\sum_p p^{-s}$$

debe diverger con $s \to 1^+$. En particular, existen infinitos primos; la cantidad de primos es tal que hace que la serie diverja.

1.2 Caracteres

Sea q un primo distinto de 2. Si bien puede ser un poco artificial, fijamos una raíz prmitiva módulo q; para cada entero n coprimo con q, sea $\nu(n)$ el entero positivo (bien definido módulo $q-1$) que verifica

$$g^{\nu(n)} \;\equiv\; n \quad (\mathsf{mod}\, q) \;.$$

Si, ahora, $\omega \in \mathbb{C}$ cumple

$$\omega^{q-1} \;=\; 1 \;,$$

la expresión $\omega^{\nu(n)}$ determina unívocamente, para cada n coprimo con q, un número complejo. Definimos, entonces, una función $\mathbb{Z} \to \mathbb{C}$ por

$$n \;\mapsto\; \begin{cases} \omega^{\nu(n)} \;, & \text{si } \;(n,q) = 1 \;, \\ 0 \;, & \text{si } \;(n,q) > 1 \;. \end{cases}$$

Hay, precisamente, $q-1$ funciones de este tipo; una por cada raíz $(q-1)$-ésima de la unidad.[5] Cada una de ellas es periódica y multiplicativa. Variando ω, asociamos, a cada $n \in \mathbb{Z}$, un vector en $\mathbb{C}^{q-1}$:

$$\hat{n} \;=\; \begin{cases} (\omega^{\nu(n)})_\omega \;, & \text{si } \;(n,q) = 1 \;, \\ 0 \;, & \text{si } \;(n,q) > 1 \;. \end{cases}$$

[3] La función $-\mathsf{log}(1-x)$ es analítica (de variable real) en el intervalo $(-1,1)$ y, en consecuencia, admite un desarrollo en serie de potencias: $\sum_{m\geq 1} m^{-1}\, x^m$. Si $s > 1$ y $p > 1$, entonces $p^{-s} \in (0,1)$ y

$$-\mathsf{log}(1-p^{-s}) \;=\; \sum_{m\geq 1} m^{-1}\, p^{-ms} \;.$$

[4] Para todo $s > 1$, $\zeta(s) \geq \sum_{n\leq x} n^{-s}$. Tomando límite inferior $s \to 1^+$, $\liminf_{s\to 1^+} \zeta(s) \geq \sum_{n\leq x} n^{-1}$. Pero la suma de los recíprocos de los enteros positivos diverge.

[5] No asumimos que ω sea una raíz primitiva, es decir, de orden exactamente $q-1$.

Estos vectores son ortogonales con respecto al producto interno usual de $\mathbb{C}^n$: si $a, n \in \mathbb{Z}$ son coprimos con q, entonces[6]

$$\langle \hat{a} \mid \hat{n} \rangle \;=\; \sum_{\omega} \omega^{-\nu(a)}\, \omega^{\nu(n)} \;=\; \begin{cases} q-1\ , & \text{si } n \equiv a \,(\mathsf{mod}\, q)\ , \\ 0\ , & \text{si no.} \end{cases} \tag{3}$$

Los caracteres de Dirichlet son funciones $\mathbb{Z} \to \mathbb{C}$ que poseen propiedades análogas.

1.3 Funciones L

A cada ω le asociamos una serie de similar a (1): para cada número *real* $s > 1$, la serie

$$\sum_{\substack{n \geq 1 \\ n \not\equiv 0\,(\mathsf{mod}\, q)}} \omega^{\nu(n)}\, n^{-s} \tag{4}$$

converge y define una función que llamamos *función* L asociada a ω y denotamos $L_\omega(s)$. Dado que $|\omega^k| = 1$, para toda ω y todo k, la convergencia de (4) se deduce de la convergencia de (1). En particular, la serie (4) converge uniformemente en $s \geq s_0$, si $s_0 > 1$. Al igual que $\zeta(s)$, la función $L_\omega(s)$ se puede expresar como un producto infinito sobre primos:[7]

$$L_\omega(s) \;=\; \prod_{p \neq q} (1 - \omega^{\nu(p)}\, p^{-s})^{-1}\ . \tag{5}$$

---

[6] Por un lado, la función ν cumple que $\nu(a) \equiv \nu(n)\,(\mathsf{mod}\, q-1)$m si y sólo si $a \equiv n\,(\mathsf{mod}\, q)$. Por otro, dado $k \in \mathbb{Z}$, la suma $\sum_\omega \omega^k$ es igual a $q-1$, si $q-1$ divide a k, y a 0, si no. Esto es consecuencia de que el subconjunto $\{\omega \in \mathbb{C} : \omega^{q-1} = 1\}$ es un subgrupo de $\mathbb{C}^\times$. Sea $\tilde{\omega}$ una de las posibles ω. Entonces

$$\tilde{\omega}^k \sum_\omega \omega^k \;=\; \sum_\omega (\tilde{\omega}\,\omega)^k \;=\; \sum_\omega \omega^k\ .$$

Si k no es múltiplo de $q-1$, existe $\tilde{\omega}$ tal que $\tilde{\omega}^k \neq 1$ (por ejemplo, una raíz primitiva de la unidad de orden $q-1$), de lo que se deduce que la suma sobre ω debe ser igual a 0; si, en cambio, $q-1 \div k$, entonces $\omega^k = 1$, para toda ω y la suma da $q-1$.

[7] Por un lado, como para $s > 1$ la serie converge absolutamente, podemos sumar en cualquier orden. Por otro, el término general es totalmente multiplicativo, con lo cual

$$\sum_{\substack{n\,:\,p^+(n) \leq x \\ n \not\equiv 0\,(\mathsf{mod}\, q)}} \omega^{\nu(n)}\, n^{-s} \;=\; \prod_{\substack{p \leq x \\ p \neq q}} (1 - \omega^{\nu(p)}\, p^{-s})^{-1}\ .$$

Cuando $x \to \infty$, el lado izquierdo converge a $L_\omega(s)$, mientras que el lado derecho converge al producto sobre los primos distintos de q.

La expresión (5) es válida para $s > 1$. Aplicando la función logaritmo, ahora como función de variable compleja,[8]

$$\log L_\omega(s) \;=\; \sum_{p\neq q} \sum_{m\geq 1} m^{-1}\, \omega^{\nu(p^m)}\, p^{-ms} \;.$$

Fijamos $a \in \mathbb{Z}$ coprimo con q. Sumando sobre ω, de (3), deducimos

$$\frac{1}{q-1} \sum_{\omega} \omega^{-\nu(a)} \log L_\omega(s) \;=\; \sum_{p^m \equiv a \,(\mathsf{mod}\, q)} m^{-1}\, p^{-ms} \;.$$

La sumatoria es una sumatoria doble, sobre los primos, p, y sobre los enteros positivos, m, que cumplen $p^m \equiv a\,(\mathsf{mod}\, q)$. El orden de la sumatoria es indistinto, porque la convergencia es absoluta, y el resultado es el valor del lado izquierdo.[9] Si sumamos sobre $m \geq 2$,

$$\sum_{\substack{p^m \equiv a \,(\mathsf{mod}\, q)\\ m\geq 2}} m^{-1}\, p^{-ms} \;\leq\; \sum_{p} \sum_{m\geq 2} m^{-1}\, p^{-ms} \;<\; 1 \;.$$

En consecuencia,

$$\frac{1}{q-1} \sum_{\omega} \omega^{-\nu(a)} \log L_\omega(s) \;=\; \sum_{p \equiv a \,(\mathsf{mod}\, q)} p^{-s} \;+\; O\,(1) \;. \tag{6}$$

De esta manera, si el lado izquierdo de (6) tiende a ∞ con $s \to 1^+$, los primos $p \equiv a$ módulo q no podrán ser una cantidad finita.

---

[8] Si definimos $l_\omega(s) := \sum_{p\neq q} \sum_{m\geq 1} m^{-1}\, \omega^{\nu(p^m)}\, p^{-ms}$, entonces, para $s > 1$,

$$\log L_\omega(s) \;=\; l_\omega(s) \;+\; 2\,\pi\, i\, k(s) \;,$$

donde $k(s) \in \mathbb{Z}$ depende de s. Pero $L_\omega(s)$ y $l_\omega(s)$ son funciones continuas y $k(s)$ es discreta. En consecuencia, $k(s)$ es constante. Con $s \to +\infty$, $L_\omega(s)$ tiende a 1 y $\log L_\omega(s)$ tiende a 0. Como también $l_\omega(s)$ tiende a 0, debe ser $k(s) = 0$ y $\log L_\omega(s) = l_\omega(s)$ para $s > 1$.

[9] Por un lado,

$$\sum_{p\neq q} \sum_{m\geq 1} \left| m^{-1}\, \omega^{\nu(p^m)}\, p^{-ms} \right| \;\leq\; \log \zeta(s) \;.$$

Por otro,

$$\sum_{p^m \equiv a \,(\mathsf{mod}\, q)} m^{-1}\, p^{-ms} \;\leq\; \sum_{p\neq q} \sum_{m\geq 1} m^{-1}\, p^{-ms} \;.$$

Pero, fijado $a \in \mathbb{Z}$, $(a, q) = 1$,

$$n \;\mapsto\; \frac{1}{q-1}\, \langle \hat{a} \mid \hat{n} \rangle$$

coincide con la función característica del subconjunto $\{n \in \mathbb{Z} \;:\; n \equiv a\,(\mathsf{mod}\, q)\}$. Entonces, sumando sobre primos $p \neq q$,

$$\begin{aligned}(q-1) \sum_{p^m \equiv a \,(\mathsf{mod}\, q)} m^{-1}\, p^{-ms} \;&=\; \sum_{p\neq q} \sum_{m\geq 1} \langle \hat{a} \mid \widehat{p^m} \rangle\, m^{-1}\, p^{-ms} \;=\; \sum_{p\neq q} \sum_{m\geq 1} \sum_{\omega} \omega^{-\nu(a)}\, \omega^{\nu(p^m)}\, m^{-1}\, p^{-ms} \\ &=\; \sum_{\omega} \omega^{-\nu(a)} \log L_\omega(s) \;.\end{aligned}$$

1.4 El valor en $s = 1$

El objetivo de esta sección es demostrar que, para cada entero a coprimo con q,

$$\sum_{\omega} \omega^{\nu(a)} \log L_\omega(s) \tag{7}$$

diverge si $s \to 1^+$. Vamos a describir el comportamiento de cada serie L_ω por separado, cerca de $s = 1$, para luego concluir algo acerca de la combinación (7). Sin embargo, vale la pena aclarar que sus comportamientos no son independientes; dado que

$$\sum_{p^m \equiv a \, (\mathrm{mod}\, q)} m^{-1} p^{-ms} \geq 0 \; ,$$

se deduce, especializando en $a = 1$, que

$$\prod_{\omega} L_\omega(s) \geq 1 \; ,$$

para todo $s > 1$.

El caso $\omega = 1$ Consideramos, primero, el caso $\omega = 1$. La serie asociada $L_1(s)$ es igual a:

$$L_1(s) = \sum_{\substack{n \geq 1 \\ (n,q)=1}} n^{-s} = (1 - q^{-s})\, \zeta(s) \; .$$

En particular, comparte con la función ζ su comportamiento asintótico con $s \to 1^+$:

$$\lim_{s \to 1^+} L_1(s) = +\infty \; .$$

De esta manera, si buscamos demostrar que (6) diverge, será suficiente probar que $\log L_\omega(s)$ están acotadas (inferiormente) cerca de $s = 1$ para toda $\omega \neq 1$, es decir, existen $\epsilon > 0$ y $\delta > 0$ tales que

$$\left| L_\omega(s) \right| \geq \epsilon \; , \tag{8}$$

si $1 < s < 1 + \delta$ y $\omega \neq 1$. Para deducir (8), será, a su vez, útil tener una cota sobre el orden de crecimiento de $L_1(s)$. Dado que[10]

$$\zeta(s) = \frac{s}{s-1} + s \int_1^\infty \frac{\{t\}}{t^s} \frac{dt}{t} \; ,$$

se puede comprobar que existe una constante $A = A(q) > 0$, independiente de s, tal que,[11]

$$L_1(s) \leq \frac{A}{s-1} \; ,$$

si $1 < s < 2$.

[10] Se puede comprobar haciendo integración o sumatoria por partes, o, también, usando la fórmula sumatoria de Euler.

[11] Notar que $L_1(s) \leq (1 - q^{-2})\, \zeta(s)$, si $1 < s < 2$.

El caso $\omega \neq 1$ Si $\omega \neq 1$, entonces la serie $L_\omega(s)$ converge para todo $s > 0$. La convergencia es uniformemente en semirectas $s \geq s_0 > 0$.[12] De esto se deduce, en primer lugar, que $L_\omega(s)$ es una función continua en $s > 0$, con lo cual (8) equivale a

$$L_\omega(1) \neq 0 \tag{9}$$

y, en segundo lugar, que $L_\omega(s)$ está acotada en un entorno de $s = 1$. Por otro lado, podemos derivar cada término de la serie $L_\omega(s)$ y concluir que

$$L'_\omega(s) = - \sum_{\substack{n \geq 1 \\ n \not\equiv 0 \,(\mathsf{mod}\, q)}} \omega^{\nu(n)} \, (\log n) \, n^{-s} \ ,$$

si $s > 0$; es decir, la función $L_\omega(s)$ es derivable en $s > 0$ y su derivada es también una serie de Dirichlet. Además, la función $L'_\omega(s)$ es continua en $s > 0$.[13] En particular, $L_\omega(s)$ está acotada cerca de $s = 1$ y existe una constante $A = A(q, \omega) > 0$ tal que, si $s > 1$,[14]

$$\big| L_\omega(s) - L_\omega(1) \big| \leq (s-1)\, A \ . \tag{10}$$

De hecho, como la cantidad de ω es finita, podemos elegir A independiente de ω, también.

Lamentablemente, este aspecto puramente analítico de las funciones L_ω sólo servirá para concluir (9) para $\omega \in \mathbb{C} \smallsetminus \mathbb{R}$. Notemos que el único caso en que $\omega \in \mathbb{R}$ y $\omega \neq 1$ es $\omega = -1$.

El caso $\omega \in \mathbb{C} \smallsetminus \mathbb{R}$ En este caso, si $\omega^{q-1} = 1$, entonces $\bar{\omega}^{q-1} = 1$ y $\bar{\omega} \neq \omega$. Por continuidad,

$$L_{\bar{\omega}}(s) = \overline{L_\omega(s)} \ ,$$

para todo $s > 0$. En consecuencia, si asumimos que $L_\omega(1) = 0$, entonces $L_{\bar{\omega}}(1) = 0$, también. Pero, entonces, por (10), $L_\omega(s) \leq (s-1)\, A$ y $L_{\bar{\omega}}(s) \leq (s-1)\, A$ en un entorno de $s = 1$. La situación sería, entonces, la siguiente:

- $L_1(s) \geq \frac{A}{s-1}$ para cierta constante $A > 0$,
- $|L_{\omega_1}(s)| = O\,(1)$, para toda $\omega_1 \neq 1$ y
- $L_\omega(s) = O\,(s-1)$ y $L_{\bar{\omega}}(s) = O\,(s-1)$.

Esto no es compatible con (7), pues el límite $s \to 1^+$ del producto $L_1(s) \prod_{\omega_1 \neq 1} L_{\omega_1}(s)$ sería cero.[15] La base de la contradicción (?) está en que $\omega \neq \bar{\omega}$ y en conocer el comportamiento asintótico de L_1, L_ω y $L_{\bar{\omega}}$ cerca de $s = 1$. En particular, $\omega = -1$, sólo lograría que el producto de las series L esté acotado superiormente.

[12] Las sumas parciales $\sum_{k=1}^{N} \omega^{\nu(k)}$ están acotadas y $\frac{1}{n^s}$ decrece a 0 con n, si (y sólo si) $s > 0$; *criterio de Dirichlet*.

[13] Usar la convergencia uniforme en semirectas de la serie derivada; criterio de Dirichlet.

[14] El argumento anterior muestra que hay una cota válida cerca de 1, pero, en realidad, $L_\omega(s)$ también está acotada con $s \to +\infty$.

[15] El orden de ceros de L_ω y de $L_{\bar{\omega}}$ en $s = 1$ revierten el orden del polo de L_1.

El caso $\omega = -1$ Si $(n,q) > 1$, el coeficiente de $L_\omega(s)$ en n es cero. Si $(n,q) = 1$, en el caso en que $\omega = -1$, se cumple que

$$\omega^{\nu(n)} = (-1)^{\nu(n)} = \left(\frac{n}{q}\right) .$$

Escribimos $L(s)$ en lugar de $L_{-1}(s)$. La serie asociada a -1 es, entonces, igual a:

$$L(s) = \sum_{n\geq 1} \left(\frac{n}{q}\right) n^{-s} .$$

El primer objetivo será encontrar una *fórmula cerrada* para $L(s)$, es decir, una expresión equivalente que se pueda evaluar sin la necesidad de tomar un límite; específicamente, expresaremos $L(s)$ como una suma finita. A partir de esta fórmula cerrada, se verá que $L(1) \neq 0$.

Dado $n \in \mathbb{Z}$, sea $G(n)$ la *suma de Gauss*

$$G(n) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e(mn/q) ,$$

donde $e(x) = e^{2\pi i\, x}$. Se verifica que

$$G(n) = \left(\frac{n}{q}\right) G(1) ,$$

para todo $n \in \mathbb{Z}$.[16] Si definimos $G := G(1)$, entonces podemos reescribir $L(s)$ de la siguiente manera:[17]

$$L(s) = \frac{1}{G} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \sum_{n\geq 1} \frac{1}{n^s}\, e(mn/q) .$$

Tenemos una suma finita por fuera. Hallaremos una expresión equivalente para la sumatoria interna; nos interesa el caso $s = 1$.

Si $|z| \leq 1$, $z \neq 1$, entonces, usando la rama principal del logaritmo,[18]

$$-\mathsf{log}(1-z) = \sum_{n\geq 1} \frac{1}{n}\, z^n .$$

[16] Si $n \not\equiv 0 \,(\mathsf{mod}\, q)$, entonces $G(n) = (n/q)\ G(1)$, haciendo un cambio de variables $m' \equiv mn$; si $n \equiv 0 \,(\mathsf{mod}\, q)$, entonces $(n/q) = 0$ pero, en general,

$$\sum_{m=1}^{q-1} \left(\frac{m}{q}\right) = 0 .$$

[17] Estamos asumiendo que $G \neq 0$.

[18] Serie de Taylor en $z = 0$.

Se puede ver que el argumento $\mathsf{arg}(1-z)$ está en el rango $\left[\frac{-\pi}{2}, \frac{\pi}{2}\right]$; si $z = e^{i\theta}$, con $\theta \in (0, 2\pi)$, entonces[19]

$$\mathsf{arg}(1-z) \;=\; \frac{\theta - \pi}{2} \;.$$

Además, $|1-z| = 2\,\mathsf{sen}(\theta/2)$. En consecuencia,

$$\sum_{n\geq 1} \frac{1}{n}\, e^{in\theta} \;=\; -\mathsf{log}\big(2\,\mathsf{sen}(\theta/2)\big) \;-\; i\,\frac{\theta-\pi}{2} \;.$$

En definitiva, el valor de L en $s=1$ se puede expresar de la siguiente manera:

$$L(1) \;=\; -\frac{1}{G} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \left[\mathsf{log}\left(2\,\mathsf{sen}\,\frac{\pi m}{q}\right) \;+\; i\left(\frac{\pi m}{q} - \frac{\pi}{2}\right)\right] . \tag{11}$$

Si bien la expresión del lado derecho de (11) involucra una parte real y una parte imaginaria, sabemos, porque $(m/q) \in \mathbb{R}$, que $L(1)$ es un número *real*.

Para terminar, separamos en dos casos: o bien $q \equiv 1$, o bien $q \equiv 3$ módulo 4. La constante G se descompone en su argumento y valor absoluto. El argumento de G depende, únicamente, de la clase de q módulo 4.

El caso $q \equiv 3 \,(\mathsf{mod}\, 4)$ En este caso, $G = i\sqrt{q}$. Como $L(1)$ es real,[20] debe ser igual a[21]

$$L(1) \;=\; -\frac{\pi}{q^{3/2}} \sum_{m=1}^{q-1} m \left(\frac{m}{q}\right) .$$

Ahora, para ver que esta suma no es cero, como $q \equiv 3 \,(\mathsf{mod}\, 4)$,

$$\sum_{m=1}^{q-1} m \left(\frac{m}{q}\right) \;\equiv\; \sum_{m=1}^{q-1} m \;=\; \frac{(q-1)\,q}{2} \;\equiv\; 1 \quad (\mathsf{mod}\, 2) \;.$$

[19] Hacer un dibujo.

[20] Independientemente –en cierto sentido– de esta observación, se puede comprobar que la suma de los términos que involucran el logaritmo da cero como resultado: por un lado, $(-1/q) = -1$, con lo que $(q-m/q) = -(m/q)$, por otro, $\mathsf{sen}(\pi - \theta) = \mathsf{sen}(\theta)$, entonces

$$\left(\frac{m}{q}\right) \mathsf{log}\big(2\,\mathsf{sen}\big(\pi m/q\big)\big) \;+\; \left(\frac{q-m}{q}\right) \mathsf{log}\big(2\,\mathsf{sen}\big(\pi(q-n)/q\big)\big) \;=\; \pm\,\mathsf{log}\left(\frac{\mathsf{sen}\big(\pi m/q\big)}{\mathsf{sen}\big(\pi - (\pi m/q)\big)}\right) \;=\; 0 \;.$$

[21] Usando que $\sum_{m=1}^{q-1} (m/q) = 0$: no es necesario asumir que $q \equiv 3$ para esto, es suficiente que el símbolo de Legendre es sobre $\{\pm 1\}$; en este caso, podemos elegir $(-1/q) = -1$. Entonces,

$$\left(\frac{-1}{q}\right) \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) = \sum_{m=1}^{q-1} \left(\frac{-m}{q}\right) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) .$$

Pero, entonces, como $(-1/q) \neq 1$, la suma debe ser igual a cero.

$\mathsf{El\ caso}\ q \equiv 1\,(\mathsf{mod}\,4)$ Ahora, $G = \sqrt{q}$, con lo cual, dado que $L(1)$ es real, de (11) sólo debe sobrevivir la suma de los logaritmos.[22]

$$L(1) \;=\; -\frac{1}{\sqrt{q}} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \mathsf{log}\big(2\,\mathsf{sen}\big(\pi m/q\big)\big) \;=\; \frac{\mathsf{log}\,Q}{\sqrt{q}}\;,$$

donde Q es igual a

$$Q \;=\; \frac{\prod_N \,\mathsf{sen}\big(\pi N/q\big)}{\prod_R \,\mathsf{sen}\big(\pi R/q\big)}\;,$$

donde R recorre los residuos y N recorre los no residuos módulo q. Veamos que $Q \neq 1$.

Notamos, para empezar, que

$$\begin{aligned}\prod_A \big(1 - \mathsf{exp}\big(\tfrac{2\pi A}{q}\big)\big) \;&=\; \prod_A \mathsf{exp}\big(\tfrac{\pi A}{q}\big)\,\big(-2i\,\mathsf{sen}\big(\pi A/q\big)\big)\\ &=\; (-2i)^{\frac{q-1}{2}}\,\mathsf{exp}\Big(\tfrac{\pi}{q}\sum_A A\Big)\prod_A \mathsf{sen}\big(\pi A/q\big)\;,\end{aligned}$$

con A igual “R” o “N”. Pero[23]

$$\sum_A A \;=\; \frac{(q-1)\,q}{4}\;.$$

Más allá del valor –no nulo–, la suma da el mismo resultado para residuos que para no residuos. Entonces,

$$Q \;=\; \frac{\prod_N \,\big(1 - \mathsf{exp}\big(\frac{2\pi N}{1}\big)\big)}{\prod_R \,\big(1 - \mathsf{exp}\big(\frac{2\pi R}{q}\big)\big)}\;.$$

Para concluir, recurrimos al siguiente resultado: existen polinomios con coeficientes enteros $Y(X)$ y $Z(X)$ tales que

$$\begin{aligned}\prod_R \big(X - \mathsf{exp}\big(\tfrac{2\pi R}{q}\big)\big) \;&=\; \tfrac{1}{2}\big(Y(X) - \sqrt{q}\,Z(X)\big) \quad \text{y}\\ \prod_N \big(X - \mathsf{exp}\big(\tfrac{2\pi N}{q}\big)\big) \;&=\; \tfrac{1}{2}\big(Y(X) + \sqrt{q}\,Z(X)\big)\;.\end{aligned} \tag{12}$$

---

[22] Como antes, es posible probar que los otros términos suman cero: usando que $(-m/q) = (m/q)$,

$$\sum_{m=1}^{q-1} m\left(\frac{m}{q}\right) \;=\; q\sum_{m=1}^{\frac{q-1}{2}}\left(\frac{m}{q}\right) \;=\; \frac{q}{2}\sum_{m=1}^{q-1}\left(\frac{m}{q}\right) \;=\; 0\;.$$

Del término del medio, se deduce que, si $q \equiv 1$, entonces en el intervalo $\big[\!\big[1,\,\frac{q-1}{2}\big]\!\big]$ la cantidad de residuos y de no residuos es igual.

[23] Los elementos A y $q-A$ son ambos residuos o ambos no residuos, pues $(-1/q) = 1$. Pero la cantidad de residuos es igual a la cantidad de no residuos, no sólo en $[\![1, q-1]\!]$, sino también en $\big[\!\big[1,\,\frac{q-1}{2}\big]\!\big]$ y, por lo tanto, en $\big[\!\big[\frac{q-1}{2}, q-1\big]\!\big]$. Entonces, la cantidad de residuos, así como la de no residuos, es igual a $\frac{q-1}{2}$

$$\sum_A A \;=\; q\sum_A \;=\; q\sum_{A\in[\![1,\frac{q-1}{2}]\!]} 1 \;=\; \frac{(q-1)\,q}{4}\;.$$

En particular,

$$\tfrac{1}{4}\left(Y(X)^2 \,-\, q\,Z(X)^2\right) \;=\; \prod_{m=1}^{q-1}\left(X - \mathsf{exp}\left(\tfrac{2\pi m}{q}\right)\right) \;=\; \frac{X^q - 1}{X - 1}\ .$$

Evaluando en $X = 1$ y definiendo $y = Y(1)$ y $z = Z(1)$,

$$Q \;=\; \frac{y + \sqrt{q}\,z}{y - \sqrt{q}\,z}\ ,$$

donde $z \neq 0$, pues, en particular, satisface[24]

$$y^2 \,-\, q\,z^2 \;=\; 4q\ .$$

---X---

CAPÍTULOS 2 Y 3 DE [Dav80] COMO EJERCICIOS, AL IGUAL QUE LAS NOTAS AL PIE Y PARTES DEL PRIMER CAPÍTULO QUE QUEDARON SIN MENCIONAR.

---X---

2 Los caracteres de Dirichlet

2.1 Funciones periódicas

Definición 2.1. Sea $q > 1$ un entero positivo, distinto de 1. Un *carácter de Dirichlet módulo q* es una función $\chi : \mathbb{Z} \to \mathbb{C}$ con las siguientes propiedades:

(i) es completamente multiplicativa, es decir, dados $m, n \in \mathbb{Z}$, $\chi(mn) = \chi(m)\chi(n)$,

(ii) tiene período q, es decir, para todo $n \in \mathbb{Z}$, $\chi(n + q) = \chi(n)$,

(iii) si $(n, q) > 1$, entonces $\chi(n) = 0$,

(iv) no es la función cero, es decir, $\chi(n) \neq 0$ para algún $n \in \mathbb{Z}$.

La condición (ii) implica que un carácter de Dirichlet está determinado por sus valores en un conjunto de representantes de enteros módulo q. Más aun, por (iii), un carácter de Dirichlet módulo q está determinado unívocamente por la función inducida en un sistema de representantes de enteros módulo q coprimos con q. Es decir, podemos pensar en un carácter de Dirichlet como una función $U\,(q) \to \mathbb{C}$ extendida por 0 a $\mathbb{Z}/q\mathbb{Z}$ y periódicamente a $\mathbb{Z}$. La condición (i) implica que

$$\chi(1)^2 \;=\; \chi(1)\ ,$$

es decir, como $\chi(1)$ debe ser un número complejo, $\chi(1) = 0$ o bien $\chi(1) = 1$.[25] En conjunto con (iv), se deduce que $\chi(1) \neq 0$. En definitiva, los caracteres de Dirichlet

[24] El valor de $z = Z(1)$ no es cero, pues q es primo y $4q$ no es un cuadrado perfecto.

[25] Aquí, análisis.

módulo q están en correspondencia con los morfismos de monoides *multiplicativos* $\mathbb{Z} \to \mathbb{C}$[26] que se factorizan por el cociente de anillos $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ y que queda determinado por la restricción a $U(q) \to \mathbb{C}$ definida por la inclusión $U(q) \subseteq \mathbb{Z}/q\mathbb{Z}$.[27]

Engañosamente, si $\chi : U(q) \to \mathbb{C}^\times$ es morfismo *de grupos*, entonces, componiendo con la inclusión $\mathbb{C}^\times \subseteq \mathbb{C}$ y extendiendo a $\mathbb{Z}/q\mathbb{Z}$, por 0, y luego a $\mathbb{Z}$, periódicamente, queda determinado un carácter de Dirichlet módulo q. Es decir, hay una inclusión

$$\mathsf{Hom}\big(U(q), \mathbb{C}^\times\big) \hookrightarrow \left\{ \begin{array}{c} \text{caracteres de Dirichlet} \\ \text{módulo } q \end{array} \right\} . \tag{13}$$

Más engañosamente aun, esta inclusión es una biyección. Para poder dar una descripción explícita de los caracteres de Dirichlet, adaptamos la idea de § 1.2: combinar raíces (complejas) de la unidad con una noción de índice. Empezamos con q una potencia de un primo, para luego definir caracteres de módulo arbitrario.

Sea p un primo distinto de 2 y sea $q = p^\alpha$ una potencia del primo p. Existen raíces primitivas módulo q; fijada g, una raíz primitiva módulo q, podemos definir $\nu(n)$ como el entero positivo, definido módulo $\varphi(q) = p^{\alpha-1}(p-1)$, que verifica

$$g^{\nu(n)} \equiv n \pmod{q} .$$

Si, ahora, $\omega \in \mathbb{C}$ cumple

$$\omega^{\varphi(q)} = 1 ,$$

la expresión $\omega^{\nu(n)}$ determina unívocamente, para cada n comprimo con q, un número complejo. Definimos, entonces, una función $\chi : \mathbb{Z} \to \mathbb{C}$ por

$$n \mapsto \begin{cases} \omega^{\nu(n)} , & \text{si } (n,q) = 1 , \\ 0 , & \text{si } (n,q) > 1. \end{cases} \tag{14}$$

Observación 2.2. Cada raíz de la unidad $\omega \in \mathbb{C}$ que satisface $\omega^{\varphi(q)} = 1$ tiene asociada una función $\chi = \chi_\omega$, por (14). Cada una de estas funciones es un carácter de Dirichlet módulo q y las funciones asociadas a cada ω son distintas; hemos definido, fijando una raíz primitiva g módulo q, $\varphi(q)$ caracteres de Dirichlet módulo q distintos. Eligiendo otra raíz g el resultado hubiese sido el mismo, es decir, como conjunto, las mismas funciones, pero indexadas ("indexadas", no "ordenadas"). Dado que en $\mathbb{C}$ existen exactamente $\varphi(q)$ raíces de la unidad de orden divisor de $\varphi(q)$, es decir, soluciones de la ecuación $z^{\varphi(q)} = 1$, y que las funciones χ_ω son todas distintas (evaluando en $n = g$, por ejemplo), deducimos que éstas funciones son todos los caracteres que se pueden definir de esta manera, a partir de una raíz de la unidad.

[26] Que son, en particular, funciones no nulas, pues la imagen de $1_\mathbb{Z}$ es $1_\mathbb{C}$, por ser morfismo de monoides.
[27] La inclusión $U(q) \subseteq \mathbb{Z}/q\mathbb{Z}$ es morfismo de monoides y la restricción $U(q) \to \mathbb{C}$, en consecuencia, también.

Si $q = 2^\alpha$, no siempre existen raíces primitivas módulo q. Si $\alpha = 1, 2$, $q = 2, 4$ y $U(q)$ es un grupo cíclico de orden $1, 2$. El único carácter módulo 2 que se puede definir a partir de un morfismo de grupos es el trivial:

$$n \mapsto \begin{cases} 1\ , & \text{si } n \text{ es impar y} \\ 0\ , & \text{si } 2 \mid n, \end{cases} \tag{15}$$

que corresponde a elegir la raíz de la unidad de orden 1, $1 \in \mathbb{C}$ y aplicar la definición (14), con $g = 1$; módulo 4, hay dos posibilidades: si $\omega^2 = 1$, entonces $\omega \in \{-1, 1\}$ y, como en (14), con $g = 3$, tenemos las dos funciones

$$n \mapsto \begin{cases} \omega^{\nu(n)}\ , & \text{si } n \text{ es impar y} \\ 0\ , & \text{si } 2 \mid n. \end{cases} \tag{16}$$

Si, en cambio, $\alpha \geq 3$, entonces $U(2^\alpha)$ ya no es un grupo cíclico. Sin embargo, todo elemento se puede expresar como

$$(-1)^\nu\, 5^{\nu'}\ .$$

El valor de ν está determinado módulo 2 y, el de ν', módulo $2^{\alpha-2} = \frac{\varphi(2^\alpha)}{2}$, el orden de 5 en $U(2^\alpha)$. Elegimos, entonces, $\omega, \omega' \in \mathbb{C}$ tales que

$$\omega^2 = 1 \quad \text{y} \quad (\omega')^{2^{\alpha-2}} = 1$$

y definimos

$$n \mapsto \begin{cases} \omega^{\nu(n)}\, (\omega')^{\nu'(n)}\ , & \text{si } n \text{ es impar y} \\ 0\ , & \text{si } 2 \mid n. \end{cases} \tag{17}$$

Observación 2.3. En cada caso, (15), (16) y (17), la cantidad de caracteres producidos es igual a $\varphi(2^\alpha)$.

En general, si $q = 2^\alpha\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ es la factorización de q como producto de primos a potencias, definimos caracteres de Dirichlet módulo q por

$$n \mapsto \chi(n; 2^\alpha)\, \chi(n; p_1^{\alpha_1}) \cdots \chi(n; p_s^{\alpha_s})\ , \tag{18}$$

donde $\chi(n; 2^\alpha)$ es un carácter de Dirichlet módulo 2^α dado por (15), por (16) o por (17), dependiendo de α, y $\chi(n; p_i^{\alpha_i})$ es un carácter de Dirichlet módulo $p_i^{\alpha_i}$ definido por (14).

Teorema 2.4. *Sea $q > 1$ un entero positivo distinto de 1 y sea $q = 2^\alpha\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ su factorización como producto de primos a potencias. Las funciones $\mathbb{Z} \to \mathbb{C}$ definidas por* (18) *son caracteres de Dirichlet módulo q. Cada $\chi(n; 2^\alpha)$ se puede elegir de $\varphi(2^\alpha)$ maneras distintas y, cada $\chi(n; p_i^{\alpha_i})$, de $\varphi(p_i^{\alpha_i})$ maneras distintas. Más aun, todas estas elecciones, que son tantas como $\varphi(q) = \varphi(2^\alpha)\, \varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s})$, dan lugar a funciones aritméticas distintas, todas ellas inducidas por morfismos de grupos $U(q) \to \mathbb{C}^\times$. Recíprocamente, todo morfismo de grupos $U(q) \to \mathbb{C}^\times$ determina un carácter de Dirichlet del tipo* (18).

Demostración. En primer lugar, *todo* carácter de Dirchlet módulo q determina un morfismo $U(q) \to \mathbb{C}^\times$ y, recíprocamente, todo morfismo así determina unívocamente un carácter de Dirichlet módulo q. Esta afirmación es la inclusión (13). Ahora bien, para cada primo (par o impar) p, los caracteres de Dirichlet $\chi(n;p^\beta)$ inducen $\varphi(p^\beta)$ morfismos de grupos $U\left(p^\beta\right) \to \mathbb{C}^\times$ distintos. Por otro lado, para p impar o $p=2$ y $\alpha = 1,2$, el grupo $U(p^\alpha)$ es cíclico, generado por una cierta raíz primitiva g, y, entonces, todo morfismo $U(p^\alpha) \to \mathbb{C}^\times$, tiene que ser de la forma $n \mapsto \omega^{\nu(n)}$, donde $g^{\nu(n)} = n$, para alguna raíz de la unidad ω de orden divisor de $p^{\alpha-1}(p-1)$; para $p=2$, como $U(2^\alpha)$ es el producto directo del subgrupo generado por -1 con el subgrupo generado por 5, todo morfismo $U(2^\alpha) \to \mathbb{C}^\times$ es de la forma $n \mapsto \omega^{\nu(n)}\,(\omega')^{\nu'(n)}$, donde $(-1)^{\nu(n)}\,5^{\nu'(n)} = n$, para ω raíz de orden divisor de 2 y ω' raíz de orden divisor de $2^{\alpha-2}$. En general, por el Teorema chino del resto, existe un isomorfismo de anillos

$$\mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/2^\alpha\mathbb{Z} \times \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}\ ,$$

el cual induce un isomorfismo de grupos entre los grupos de unidades

$$U(q) \simeq U(2^\alpha) \times U(p_1^{\alpha_1}) \times U(p_s^{\alpha_s})\ .$$

Como $\mathbb{C}^\times$ es un grupo abeliano, el isomorfismo anterior induce una *biyección* entre los *conjuntos* de morfismos:[28]

$$\mathsf{Hom}\big(U(q), \mathbb{C}^\times\big) \simeq \mathsf{Hom}\big(U(2^\alpha), \mathbb{C}^\times\big) \times \mathsf{Hom}\big(U(p_1^{\alpha_1}), \mathbb{C}^\times\big) \times \cdots \times \mathsf{Hom}\big(U(p_s^{\alpha_s}), \mathbb{C}^\times\big)\ .$$

En particular, las funciones (18) son todas distintas, ya que dos elecciones de $\chi(n;p^\beta)$ dan lugar a funciones distintas en alguno de los factores. Que son caracteres de Dirichlet se deduce de que los $\chi(n;p^\beta)$ lo son. $\square$

Llamemos *caracteres conocidos* a los caracteres de Dirichlet del tipo (18). Entonces, una conclusión del Teorema 2.4 es que los caracteres conocidos son exactamente la imagen de la inclusión (13). Hay, en total, $\varphi(q)$ caracteres conocidos módulo q

2.2 El monoide de caracteres de Dirichlet

Observación 2.5. El producto de dos caracteres de Dirichlet es un carácter: dadas dos funciones $\chi, \chi' : \mathbb{Z} \to \mathbb{C}$ el producto, es decir, la función

$$(\chi\,\chi')(n) = \chi(n)\,\chi'(n)\ ,$$

está definido. Si χ y χ' son (completamente) multiplicativas, entonces $\chi\,\chi'$ también; si son periódicas de períodos q y q', entonces $\chi\,\chi'$ es periódica de período $[q,q']$, al menos. Si χ y χ' verifican $\chi(n) = 0$ para $(n,q) > 1$ y $\chi'(n) = 0$ para $(n,q') > 1$, entonces el producto verifica $(\chi\,\chi')(n) = 0$ para $(n,qq') > 1$, al menos. Si $\chi(1) = \chi'(1) = 1$, como fuere el caso si fueren caracteres de Dirichlet, entonces $(\chi\,\chi')(1) = 1$, también. El producto de dos caracteres de Dirichlet módulo q es, además, un carácter de Dirichlet módulo q.

[28] Además, los conjuntos de morfismos tienen estructura de grupo (abeliano), pues $\mathbb{C}^\times$ es grupo abeliano y esta biyección es un isomorfismo de grupos (abelianos) para dicha estructura.

Definición 2.6. Dados caracteres de Dirichlet $\chi, \chi' : \mathbb{Z} \to \mathbb{C}$ el *producto* de χ con χ' es el carácter de Dirichlet determinado por la expresión (**??**).

De entre todos los caracteres de Dirichlet módulo q posibles, hay uno especial: el *carácter trivial*.

Definición 2.7. El *carácter de Dirichlet principal (o trivial) módulo* q es la función

$$n \mapsto \begin{cases} 1\,, & \text{si } (n,q) = 1 \text{ y} \\ 0\,, & \text{si } (n,q) > 1. \end{cases} \tag{19}$$

Observación 2.8. El carácter principal es uno de los caracteres conocidos: si $q = p^{\beta}$, entonces corresponde a la elección de raíz de la unidad $\omega = 1$ (y $\omega' = 1$ también, si $p = 2$ y $\beta \geq 3$). En general, el carácter principal módulo q coincide con la (única) elección de caracteres $\chi(n; p^{\beta})$ principales (módulo cada una de las potencias de primo que dividen exactamente a q).

Observación 2.9. El carácter principal módulo q es especial, porque, entre otras cosas tiene la siguiente propiedad: si χ_0 denota el carácter principal módulo q y χ es cualquier otro carácter de Dirichlet módulo q, entonces, en tanto funciones $\mathbb{Z} \to \mathbb{C}$

$$\chi\,\chi_0 \,=\, \chi_0\,\chi \,=\, \chi\,.$$

Es decir, el carácter principal módulo q es un neutro para el producto de caracteres de Dirichlet módulo q.

Observación 2.10. Si $\chi : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet módulo q, definimos una nueva función por

$$n \mapsto \begin{cases} \chi(n)^{-1}\,, & \text{si } \chi(n) \neq 0 \text{ y} \\ 0\,, & \text{si } \chi(n) = 0. \end{cases} \tag{20}$$

Esta nueva función es un carácter de Dirichlet módulo q; si supiésemos que $\chi(n) = 0$ implica $(n,q) > 1$, entonces sería inverso de χ con respecto al producto de caracteres de Dirichlet módulo q y al carácter principal, χ_0, como neutro.

Observación 2.11. El conjunto de caracteres de Dirichlet módulo q es, en principio, sólo un monoide con respecto al producto de caracteres módulo q; el elemento neutro es el carácter principal módulo q. Sin embargo, los caracteres conocidos constituyen un submonoide que es, además, un grupo. Para módulo $q = p^{\alpha}$,[29] el producto de caracteres de Dirichlet conocidos χ y χ' módulo p^{α}, correspondientes a raíces ω y ω', es igual al carácter módulo p^{α} conocido que corresponde a elegir la raíz de la unidad $\omega\,\omega'$, producto de las raíces correspondientes. Análogamente, el inverso (20) de un carácter conocido χ, correspondiente una raíz ω, es igual al carácter conocido que corresponde a elegir la raíz conjugada $\bar{\omega}$. Dicho de otra manera, la inclusión del (conjunto subyacente al) grupo $\mathsf{Hom}\big(U\,(q)\,,\mathbb{C}^{\times}\big)$ en el (conjunto subyacente al) monoide de caracteres de Dirichlet es morfismo de monoides y su imagen, el submonoide conformado por los caracteres conocidos, es un grupo.

[29] p impar; el caso $p = 2$ es similar.

Todo carácter conocido módulo q se puede expresar de manera única (salvo orden de los factores) como producto de caracteres conocidos módulo las potencias de primos que aparecen en la factorización de q, con un carácter por primo. El producto de caracteres conocidos es un carácter conocido y, si ambos factores tienen módulo q, el producto tendrá módulo q. Para cada q, hay un carácter trivial módulo q, que es un carácter conocido. Este carácter es neutro para el producto de caracteres de Dirichlet módulo q. El carácter de Dirichlet asociado por (20) a un carácter conocido es un carácter conocido, con igual módulo, y es su inverso en el grupo de caracteres conocidos módulo q.

2.3 Pairing

En esta sección reescribimos la definición de los caracteres conocidos en términos de la exponencial. Esto corresponde a ordenar de alguna manera las distintas raíces de la unidad que aparecen en la definición de los caracteres conocidos $\chi(n; p^\alpha)$ módulo potencias de primos.

Si $\omega \in \mathbb{C}$ cumple $\omega^N = 1$, entonces

$$\omega \;=\; e(m/N) \;,$$

donde $e(x) = e^{2\pi i x}$. Las raíces de la unidad de orden divisor de N están en correspondencia con los enteros módulo N vía la exponencial; a un entero m le corresponde la raíz $e(m/N)$. En particular, si $q = p^\alpha$ (p impar, o $p = 2$ y $\alpha = 1, 2$), g es una raíz primitiva módulo q y $\chi(n; p^\alpha)$ es un carácter conocido módulo p^α, entonces, para $n \equiv g^\nu \pmod{q}$ coprimo con q,

$$\chi(n; p^\alpha) \;=\; e\!\left(\frac{m\nu}{\varphi(p^\alpha)}\right) \;;$$

si $q = 2^\alpha$ y $\alpha \geq 3$, entonces, para $n \equiv (-1)^\nu\, 5^{\nu'} \pmod{2^\alpha}$ impar,

$$\chi(n; 2^\alpha) \;=\; e\!\left(\frac{m\nu}{2} + \frac{m'\nu'}{2^{\alpha-2}}\right) \,.$$

Si $q = 2^\alpha\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, fijamos, para cada i una raíz primitiva g_i módulo $p_i^{\alpha_i}$. Si $(n, q) = 1$ y[30] $n \equiv (-1)^{\nu_0} 5^{\nu_0'} \pmod{2^\alpha}$ y $n \equiv g^{\nu_i} \pmod{p_i^{\alpha_i}}$, entonces todo carácter conocido módulo q es igual a

$$\chi(n) \;=\; e\!\left(\frac{m_0\nu_0}{2} + \frac{m_0'\nu_0'}{2^{\alpha-2}} + \frac{m_1\nu_1}{\varphi(p_1^{\alpha_1})} + \cdots + \frac{m_s\nu_s}{\varphi(p_s^{\alpha_s})}\right) \,, \tag{21}$$

para ciertos enteros m_0, m_0', m_1, ..., m_s, unívocamente determinados módulo 2, $2^{\alpha-2}$ y $\varphi(p_i^{\alpha_i})$, respectivamente.

Teorema 2.12. *Sea $q > 1$ un entero positivo distinto de 1 y sea $q = 2^\alpha\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ su factorización como producto de primos a potencias. Para cada i, sea g_i una raíz primitiva módulo $p_i^{\alpha_i}$ Los caracteres de Dirichlet módulo q conocidos están en biyección con las secuencias de enteros*

$$(m_0,\, m_0',\, m_1,\, \ldots,\, m_s) \;\in\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/\varphi(p_1^{\alpha_1})\mathbb{Z} \times \,\cdots\, \times \mathbb{Z}/\varphi(p_s^{\alpha_s})\mathbb{Z} \;.$$

[30] Aprovechamos para mencionar que la siguiente manera de expresar enteros módulo 2^α es consistente para todo $\alpha \geq 1$.

2.4 Caracteres primitivos

3 Las funciones L

4 La conexión con formas cuadráticas binarias

En esta sección, deducimos una fórmula para el valor $L(1,\chi_d)$, donde $\chi_d = (d/\cdot)$, el símbolo de Kronecker en d, es uno de los caracteres reales principales; en particular, suponemos que d es un discriminante fundamental y, por lo tanto, que todas las formas cuadráticas binarias de discriminante d son primitivas. La fórmula relaciona el valor $L(1,\chi_d)$ con el número de clases de formas de discriminante d, $\mathsf{h}(d)$. La idea consiste en "calcular" el número de representaciones (primarias) por formas de discriminante d de dos maneras distintas.

4.1 El número de representaciones

Definición 4.1. Un *discriminante* es un entero d tal que $d \equiv 0, 1 \,(\mathsf{mod}\, 4)$.

Definición 4.2. Si $n \in \mathbb{Z}$ y F es una forma cuadrática, el *número de representaciones de n por la forma F* es:

$$\mathsf{R}(n,F) \;:=\; \begin{cases} \#\big\{(x,y)\in\mathbb{Z}^2 \;:\; F(x,y)=n\big\}\ , & \text{si } d<0\ ,\\ \#\big\{(x,y)\in\mathbb{Z}^2 \;:\; F(x,y)=n\ ,\ 1<\frac{x-\bar\theta\, y}{x-\theta\, y}\le \epsilon^2\ ,\ x-\theta\, y>0\big\}\ , & \text{si } d<0\ . \end{cases}$$

Si d es un discriminante, el *número de representaciones de n por formas de discriminante d* es

$$\mathsf{R}(n) \;=\; \mathsf{R}(n,d) \;:=\; \sum_{[F]}{}' \mathsf{R}(n,F)\ ,$$

donde la suma se realiza sobre un conjunto de representantes de las clases de equivalencia de formas *primitivas* de discriminante d.

Observación 4.3. Si $d<0$, $\mathsf{R}(n,F)$ cuenta todas las posibles representaciones de n por la forma F; este número es finito. Si $d>0$, entonces imponemos una condición que garantice que el número sea finito.

Observación 4.4. El número de representaciones $\mathsf{R}(n)$ *sólo incluye las representaciones por formas primitivas.* Además, la suma que lo define se realiza sobre un conjunto de representantes de dichas formas con respecto a la relación de equivalencia por la acción del grupo modular $\mathsf{SL}_2(\mathbb{Z})$.

Definición 4.5. El *estabilizador de F* (o *grupo de autometrías de F*, o. . .) es el subgrupo de $\mathsf{SL}_2(\mathbb{Z})$ conformado por las matrices $\gamma \in \mathsf{SL}_2(\mathbb{Z})$ tales que $F\cdot\gamma = F$.

Observación 4.6. Si d es un discriminante y F es una forma *primitiva* de discriminante d, entonces su estabilizador está en correspondencia con las soluciones a la ecuación:

$$u^2 \,-\, d\,v^2 \;=\; 4\ , \tag{22}$$

con $u, v \in \mathbb{Z}$. En particular, *sólo depende de d.* Si $d < 0$ el conjunto de soluciones tiene cardinal $w \in \{2, 4, 6\}$, donde

$$w \;=\; w(d) \;:=\; \begin{cases} 4\ , & \text{si } d = -1\ , \\ 2\ , & \text{si } d = -2\ , \\ 6\ , & \text{si } d = -3\ , \\ 4\ , & \text{si } d = -4\ , \\ 2\ , & \text{si } d < -4\ . \end{cases}$$

Si $d > 0$, el cardinal del conjunto solución es infinito.

Definición 4.7. Dos representaciones $F(x_1, y_1) = n$ y $F(x_2, y_2) = n$ son *equivalentes*, si existe γ en el estabilizador de F tal que $\gamma \left[\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right]$.

Observación 4.8. Si $d < 0$, el número de representaciones $\mathsf{R}(n, F)$ incluye representaciones que son equivalentes. Si $d > 0$, se demuestra que las representaciones que cuenta son todas inequivalentes. Esto tiene sentido, porque, como el estabilizador es, en estos casos, de orden infinito, cada representación $F(x, y) = n$ da lugar a infinitas soluciones distintas (pero equivalentes en el sentido de la Definición 4.7).

Teorema 4.9. *Si $n > 0$ es un entero positivo y d es un discriminante coprimo con n, entonces*

$$\mathsf{R}(n) \;=\; \begin{cases} w \sum_{k|n} \left(\dfrac{d}{k}\right)\ , & si\ d < 0\ , \\ \sum_{k|n} \left(\dfrac{d}{k}\right)\ , & si\ d > 0\ . \end{cases}$$

Teorema 4.10. *Si d es un discriminante y $N > 1$,*

$$\frac{1}{N} \sum_{\substack{n=1 \\ (n:d)=1}}^{N} \mathsf{R}(n) \;=\; w\, \frac{\varphi(|d|)}{|d|} \sum_{m \le \sqrt{N}} \frac{1}{m} \left(\frac{d}{m}\right) \;+\; O\left(N^{-1/2}\right)\ .$$

Demostración. Por el Teorema 4.9, sumando sobre n y descomponiendo $n = m_1 m_2$,

$$w^{-1} \sum_{\substack{n=1 \\ (n:d)=1}}^{N} \mathsf{R}(n) \;=\; \sum_{\substack{m_1 m_2 \le N \\ (m_1 m_2 : d)=1}} \left(\frac{d}{m_1}\right)\ . \tag{23}$$

Como $m_1 m_2 \le N$, (23) la separamos en una suma con $m_1 \le \sqrt{N}$ y otra con $m_2 \le \sqrt{N}$. Usando que $(d/m_1) = 0$, si $(m_1 : d) > 1$, deducimos que

$$\sum_{\substack{m_1 m_2 \le N \\ (m_1 m_2 : d)=1}} \left(\frac{d}{m_1}\right) = \sum_{m_1 \le \sqrt{N}} \left(\frac{d}{m_1}\right) \sum_{\substack{m_2 \le N/m_1 \\ (m_2 : d)=1}} 1 \;+\; \sum_{\substack{m_2 < \sqrt{N} \\ (m_2 : d)=1}} \;\sum_{\sqrt{N} < m_1 \le \sqrt{N}} \left(\frac{d}{m_1}\right)\ .$$

Ahora,[31]

$$\sum_{\substack{m_2\le N/m_1\\(m_2:d)=1}} 1 \;=\; \frac{N}{m_1}\,\frac{\varphi(|d|)}{|d|} \;+\; O\left(\varphi(|d|)\right)\ ,$$

y, por lo tanto,

$$\sum_{m_1\le\sqrt{N}} \left(\frac{d}{m_1}\right) \sum_{\substack{m_2\le N/m_1\\(m_2:d)=1}} 1 \;=\; N\,\frac{\varphi(|d|)}{|d|} \sum_{m_1\le\sqrt{N}} \frac{1}{m_1}\left(\frac{d}{m_1}\right) \;+\; O\left(\sqrt{N}\right)\ ;$$

como, en esta cuenta, d está fijo, $O\left(\varphi(|d|)\right)$ es $O\left(1\right)$. Por otro lado, $(d/\cdot)$ no es el carácter principal módulo $|d|$,

$$\sum_{\sqrt{N}<m_1\le N/m_2} \left(\frac{d}{m_1}\right) \;=\; O\left(1\right)$$

(la suma está acotada), con lo cual,

$$\sum_{\substack{m_2<\sqrt{N}\\(m_2:d)=1}} \ \sum_{\sqrt{N}<m_1\le N/m_2} \left(\frac{d}{m_1}\right) \;=\; O\left(\sqrt{N}\right)\ .$$

En definitiva,

$$w^{-1}\sum_{\substack{n=1\\(n:d)=1}}^{N} \mathsf{R}(n) \;=\; N\,\frac{\varphi(|d|)}{|d|}\sum_{m\le\sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right) \;+\; O\left(\sqrt{N}\right)\ .$$

□

---

[31] Si $\left\lfloor \frac{N}{m_1}\right\rfloor = q\,|d| + r\ (0\le r<|d|)$, entonces

$$\sum_{\substack{m_2\le N/m_1\\(m_2:d)=1}} 1 \;=\; q\,\varphi(|d|) \;+\; \sum_{\substack{q\,|d|<m_2\le N/m_1\\(m_2:d)=1}} 1\ .$$

Pero

$$\sum_{\substack{q\,|d|<m_2\le N/m_1\\(m_2:d)=1}} 1 \;=\; \sum_{\substack{m_2=1\\(m_2:d)=1}}^{r} 1 \;\le\; \varphi(|d|)\ .$$

Entonces, usando que $q - \frac{N}{m_1}\,\frac{1}{|d|} \le \frac{r}{|d|} < 1$, vemos que

$$\sum_{\substack{m_2\le N/m_1\\(m_2:d)=1}} 1 \;-\; \frac{N}{m_1}\,\frac{\varphi(|d|)}{|d|} \;<\; 2\,\varphi(|d|)\ .$$

Teorema 4.11. *Si d es un discriminante,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1\\(n:d)=1}}^{N} \mathsf{R}(n) \;=\; w\, \frac{\varphi(|d|)}{|d|} \sum_{m\geq 1} \frac{1}{m} \left(\frac{d}{m}\right) \,.$$

Demostración. Se deduce del Teorema 4.10 y del Lema 4.12. □

Lema 4.12. *Si d es un discriminante y $N > 1$,*

$$\sum_{m>\sqrt{N}} \frac{1}{m} \left(\frac{d}{m}\right) \;=\; O\left(N^{-1/2}\right) \,.$$

Definición 4.13. Un discriminante d es *fundamental*, si

- $d \equiv 0 \,(\mathsf{mod}\, 4)$ y $d = 4m$, donde $m \equiv 2, 3 \,(\mathsf{mod}\, 4)$ y libre de cuadrados, o
- $d \equiv 1 \,(\mathsf{mod}\, 4)$ y libre de cuadrados.

Lema 4.14. *Un discriminante d es fundamental, si y sólo si toda forma cuadrática de discriminante d es primitiva.*

Ejemplo 4.15. Los disriminantes $d = -1$ y $d = -2$ no son fundamentales; los discriminantes $d = -3$, $d = -4$ y $d = -8$ sí lo son. El discriminante 5 es fundamental, pero 20 no lo es. El discriminante 2 no es un discriminante, pero 8 sí lo es y es fundamental.

Observación 4.16. En particular, si d es un discriminante fundamental, el número de clases de formas primitivas de discriminante d es igual al número de clases y el estabilizador de toda forma de discriminante d está en biyección con las soluciones a la ecuación (22). Además, el número de representaciones de un entero n por formas de discriminante d es, efectivamente, la cantidad de representaciones (inequivalentes, si $d > 0$) de n por un conjunto de representantes de las formas de discriminante d; la condición de primitividad se cumple automáticamente.

4.2 La cantidad de puntos encerrados

En la sección § 4.1, conectamos el valor $L(1, \chi_d)$ con el comportamiento asintótico del promedio del número de representaciones $\mathsf{R}(n)$ (primarias, si $d > 0$) por formas primitivas de discriminante d, con $n \geq 1$ coprimo con el discriminante d.

$$\begin{tikzcd}
\text{primos en progresiones aritméticas} \arrow[d, "\sum_{p\equiv a\,(m)} \frac{1}{p}"] & \\
\text{funciones L de caracteres} \arrow[r, dashed, "L(1,\chi)\approx\mathsf{R}(n)"] & \text{formas cuadráticas}
\end{tikzcd}$$

En esta sección, deducimos la relación con el número de clases de formas de discriminante d. Esencialmente, si estudiamos el comportamiento asintótico del número de representaciones para cada clase por separado, veremos que el resultado es independiente de la clase.

Sea d un discriminante (no necesariamente fundamental) y sea $F = \{a, b, c\}$ una forma *primitiva* de discriminante d; si $d < 0$, suponemos que $a > 0$. La hipótesis de primitividad la necesitaremos, por eso la hacemos explícita. Sea $\mathsf{R}(n, F)$ el número de representaciones (primarias, si $d > 0$) de un entero positivo n por la forma F. Veremos que el límite

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n:d)=1}}^{N} \mathsf{R}(n, F) \tag{24}$$

es igual para todas las clases.

Observación 4.17. Si d es fundamental y si sumamos sobre un conjunto de representantes de las clases,

$$\mathsf{R}(n) \;=\; \sum_{[F]} \mathsf{R}(n, F) \;.$$

En particular, si $M(d)$ denota el límite (24), entonces

$$\mathsf{h}(d)\, M(d) \;=\; w(d)\, \frac{\varphi(|d|)}{|d|}\, L(1, \chi_d) \;.$$

El valor de la sumatoria

$$\sum_{\substack{n=1 \\ (n:d)=1}}^{N} \mathsf{R}(n, F) \tag{25}$$

es igual al de la cantidad de puntos $(x, y) \in \mathbb{Z}^2$ que verifican:

(i) $(F(x, y) : d) = 1$ y

(ii) $0 < F(x, y) \leq N$;

si $d > 0$, como contamos representaciones *primarias*, pedimos, además, que el par (x, y) cumpla:

(iii) $1 \leq \frac{x-\bar{\theta}\, y}{x-\theta\, y} < \epsilon^2$ y

(iv) $x - \theta\, y > 0$,

donde

$$\theta \;=\; \frac{-b + \sqrt{d}}{2a} \qquad , \qquad \bar{\theta} \;=\; \frac{-b - \sqrt{d}}{2a} \qquad \text{y} \qquad \epsilon \;=\; \frac{u_0 + \sqrt{d}\, v_0}{2}$$

es la solución fundamental a la ecuación $u^2 - d\, v^2 = 4$. A los fines de esta sección, ϵ es sólo una constante y θ y $\bar{\theta}$ hacen que

$$F(x, y) \;=\; a \left(x - \theta\, y\right) \left(x - \bar{\theta}\, y\right) \;.$$

La condición (ii) define una figura en el plano: una elipse, si $d < 0$, o una hipérbola, si $d > 0$; si $d > 0$, la condición (iii) define un sector de la hipérbola y la (iv) determina uno de los cuadrantes, una de las dos componentes conexas de la hipérbola. Definimos

$$A(\sqrt{N}) \;=\; \begin{cases} \{(x,y) \in \mathbb{R}^2 \,:\, \text{(ii)}\} \quad , & \text{si } d < 0 \ , \\ \{(x,y) \in \mathbb{R}^2 \,:\, \text{(ii) , (iii) y (iv)}\} \quad , & \text{si } d > 0 \ . \end{cases} \tag{26}$$

La condición (i), por otro lado, es una condición aritmétca que nos distingue algunos puntos de la región delimitada y sólo depende de la clase de x y de y módulo $|d|$.

Lema 4.18. *Si $F = \{a,b,c\}$ es una forma primitiva de discriminante d, entonces*

$$\#\{(x,y) \in \mathbb{Z}^2 \,:\, 0 \le x, y < |d| \ , \ (F(x,y) : d) = 1\} \;=\; |d|\,\varphi(|d|) \ .$$

Los puntos que cuenta la expresión (25) los podemos subdividir de acuerdo a congruencia módulo $|d|$, de manera que nos gustaría saber (aproximadamente) cuántos puntos $(x,y) \in \mathbb{Z}^2$ verifican las condiciones (ii) –y (iii) y (iv) (si $d > 0$)– y, además,

$$x \;\equiv\; x_0 \,(\mathsf{mod}\,|d|) \qquad \text{y} \qquad y \;\equiv\; y_0 \,(\mathsf{mod}\,|d|) \ ,$$

para cada elección de (x_0, y_0). Es decir, buscaremos estimar el cardinal del conjunto

$$A(\sqrt{N}) \,\cap\, \Big((x_0,y_0) + d\,\mathbb{Z}^2\Big) \ . \tag{27}$$

Podemos suponer que (x_0, y_0) tiene coordenadas en el rango $0 \le x_0, y_0 < |d|$.

Si sólo nos interesa saber a qué tiende el cardinal del conjunto (27), podemos ver que, con $N \to \infty$, se habrá de parecer al área de la figura $A(\sqrt{N})$.

Lema 4.19. *Si $(x_0, y_0) \in \mathbb{Z}^2$ y $A(\sqrt{N}) \subset \mathbb{R}^2$ es el subconjunto del plano definido por* (26)*, entonces*

$$\#\Big[A(\sqrt{N}) \,\cap\, \Big((x_0,y_0) + d\,\mathbb{Z}^2\Big)\Big] \;\sim\; \tfrac{|A(\sqrt{N})|}{|d|^2} \ .$$

Equivalentemente,

$$\lim_{N\to\infty} \frac{1}{N}\,\#\Big[A(\sqrt{N}) \,\cap\, \Big((x_0,y_0) + d\,\mathbb{Z}^2\Big)\Big] \;=\; \tfrac{|A(1)|}{|d|^2} \ .$$

Pero, en realidad, es posible estimar la *diferencia.*

Lema 4.20. *Si $(x_0, y_0) \in \mathbb{Z}^2$ y $A(\sqrt{N}) \subset \mathbb{R}^2$ es el subconjunto del plano definido en* (26)*, entonces*

$$\#\Big[A(\sqrt{N}) \,\cap\, \Big((x_0,y_0) + d\,\mathbb{Z}^2\Big)\Big] \;=\; \tfrac{|A(\sqrt{N})|}{|d|^2} \;+\; O\left(\sqrt{N}\right) \ .$$

Juntando el Lema 4.18 con el Lema 4.19, deducimos el siguiente resultado.

Teorema 4.21. *Dado un discriminante d y una forma primitiva F de discriminante d,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1\\(n:d)=1}} \mathsf{R}(n,F) \;=\; \frac{\varphi(|d|)}{|d|}\,\frac{r}{|d|^{1/2}}\;,$$

donde $r = r(d) > 0$ es la constante

$$r(d) \;=\; \begin{cases} 2\pi\;, & si\ d<0\;,\\ \log\epsilon\;, & si\ d>0\;. \end{cases}$$

Demostración. Del Lema 4.18 y del Lema 4.19,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1\\(n:d)=1}} \mathsf{R}(n,F) \;=\; |d|\,\varphi(|d|)\,\tfrac{|A(1)|}{|d|^2}\;.$$

Sólo resta calcular el área $|A(1)|$. Pero[32]

$$|A(1)| \;=\; \begin{cases} \frac{2\pi}{|d|^{1/2}}\;, & \text{si } d<0\;,\\ \frac{\log\epsilon}{d^{1/2}}\;, & \text{si } d>0\;. \end{cases}$$

□

4.3 Algunas demostraciones

Demostraciones de la sección 4.1

Lema 4.22. *Si d es un discriminante y $N>1$,*

$$\sum_{m>\sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right) \;=\; O\left(N^{-1/2}\right)\;.$$

Demostración. Definimos $a_m = (d/m)$, $f(t)=1/t$ y $A(t) = \sum_{m\le t} a_m$. Entonces, por Partes,

$$\sum_{y<m\le x} \frac{1}{m}\left(\frac{d}{m}\right) \;=\; A(x)\,f(x) \;-\; A(y)\,f(y) \;-\; \int_y^x A(t)\,f'(t)\,dt\;. \tag{28}$$

Como (d/m) no es el carácter principal módulo $|d|$, $A(t) = O(1)$, es decir, $A(t)\le C$, para cierta constante C (que dependerá de d). Entonces, (28) está acotada por

$$C\left(\frac{1}{x}+\frac{1}{y}+\int_y^x \frac{dt}{t^2}\right) \;=\; \frac{2\,C}{y}\;.$$

□

[32] En [Dav80, Ch. 6], está el cálculo del área de $A(\sqrt{N})$ para $N>1$, que luego es comparada con el promedio de los números de representaciones.

Lema 4.23. *Un discriminante d es fundamental, si y sólo si toda forma cuadrática de discriminante d es primitiva.*

Demostración. Sea $\{a, b, c\}$ una forma de discriminante d. Si $g \mid (a : b : c)$, entonces $g^2 \mid d$. Supongamos que $g > 1$. Si $d \equiv 1 \pmod 4$, como no es libre de cuadrados, no es fundamental; si $d \equiv 0 \pmod 4$ con $d = 4m$ y m libre de cuadrados, como $g^2 \mid d$, vale $g = 2$ y $4m = b^2 - 4ac = 4\,(b'^2 - 4a'c')$, con lo que $m \equiv 0, 1 \pmod 4$ y d no es fundamental.

Supongamos, ahora, que $d = 4m$ no es fundamental. Entonces,

- si m no es libre de cuadrados y $f > 1$ es tal que $f^2 \mid m$, la forma $\left\{1, 0, -\frac{m}{f^2}\right\}$ tiene discriminante $4\frac{m}{f^2}$ y la forma $\left\{f, 0, -\frac{m}{f}\right\}$ no es primitiva y tiene discriminante d;
- si $m \equiv 0 \pmod 4$, la forma $\left\{1, 0, -\frac{m}{4}\right\}$ tiene discriminante m y la forma $\left\{2, 0, -\frac{m}{2}\right\}$ no es primitiva y tiene discriminante d;
- si $m \equiv 1 \pmod 4$, la forma $\left\{1, 1, \frac{1-m}{4}\right\}$ tiene discriminante m y la forma $\left\{2, 2, \frac{1-m}{2}\right\}$ no es primitiva y tiene discriminante d.

Supongamos que $d \equiv 1 \pmod 4$ no es fundamental. Entonces, no es libre de cuadrados y existe $g > 1$ tal que $g^2 \mid d$. Si $d = g^2 d'$, como d es impar, $d \equiv d' \pmod 4$. La forma $\left\{1, 1, \frac{1-d'}{4}\right\}$ tiene discriminante d' (y, además, es primitiva). La forma $\left\{g, g, g\,\frac{1-d'}{4}\right\}$ no es primitiva y tiene discriminante d. □

Demostraciones de la sección 4.2 A continuación demostramos los resultados de la sección 4.2. Lo haremos más o menos general.

Sea $F : \mathbb{R}^2 \to \mathbb{R}$ la función

$$F(x, y) \;=\; a\,x^2 \;+\; b\,xy \;+\; c\,y^2 \;,$$

donde $a, b, c \in \mathbb{Z}$, definida por la forma cuadrática correspondiente de discriminante $d = b^2 - 4ac$, no un cuadrado. Dado $\rho > 0$, definimos el subconjunto $A(\rho) \subset \mathbb{R}^2$ del plano por

$$A(\rho) \;=\; \left\{(x, y) \in \mathbb{R}^2 \;:\; 0 < F(x, y) \le \rho^2 \;,\; I\right\} \;, \tag{29}$$

donde I es una familia de condiciones adicionales en (x, y) que no cambian aunque cambiemos (x, y) por $(x/\lambda, y/\lambda)$ (o sea, homogéneas de grado 0) y que garantizan que $A(\rho)$ sea compacto (por ejemplo, las condiciones (iii) y (iv)).

Sean $(x_0, y_0) \in \mathbb{R}^2$ un punto del plano y $l > 0$. Definimos

$$B \;=\; \left\{(x_0 + l\,m, y_0 + l\,n) \;:\; m, n \in \mathbb{Z}\right\} \;=\; (x_0, y_0) \;+\; l\,\mathbb{Z}^2 \;. \tag{30}$$

Los puntos de B son los centros de cuadrados de lado l que teselan el plano, empezando por el cuadrado centrado en (x_0, y_0). Denotamos por Q el conjunto de dichos cuadrados. Si $\rho > 0$, definimos

$$B(\rho) \;=\; \left\{(x, y) \in B \;:\; F(x, y) \le \rho^2\right\} \;=\; B \,\cap\, A(\rho) \;. \tag{31}$$

Denotamos por $Q(\rho)$ el conjunto de aquellos cuadrados de Q cuyo centro pertenece a la figura $A(\rho)$, o sea, a $B(\rho)$. Dado que cada cuadrado del conjunto Q tiene área l^2, la cantidad de puntos en $B(\rho)$ es

$$\#B(\rho) \;=\; \#Q(\rho) \;=\; \frac{1}{l^2}\,\left|\bigcup Q(\rho)\right| \;.$$

Lema 4.24. *Sea $A(\rho)$ definida por* (29) *y sea $B(\rho)$ definida por* (31)*. Entonces,*

$$\lim_{\rho\to\infty}\, \tfrac{1}{\rho^2}\,\#B(\rho) \;=\; \tfrac{1}{l^2}\,|A(1)| \;.$$

Demostración. El área de la unión de los cuadrados de $Q(\rho)$ aproxima el área de $A(\rho)$ y, en particular, $B(\rho)$ y $A(\rho)/l^2$ deberían ser iguales asintóticamente. Para precisar esta afirmación, hacemos un cambio de variables, dividiendo por ρ las coordenadas y, en lugar de comparar $B(\rho)$ con $A(\rho)$ para $\rho > 0$ variable y tendiendo a ∞, comparamos

$$\tfrac{1}{\rho}\,B(\rho) \;=\; \tfrac{1}{\rho}\,B\,\cap\,A(1) \;=\; \Big(\big(\tfrac{x_0}{\rho},\tfrac{y_0}{\rho}\big) \;+\; \tfrac{l}{\rho}\,\mathbb{Z}^2\Big)\,\cap\,A(1)$$

con $A(1)$. Figura fija y retículo variable. Los puntos del retículo $\frac{1}{\rho}\,B$ son los centros de cuadrados de lado l/ρ que teselan el plano, empezando por el cuadrado de centro $(\frac{x_0}{\rho},\frac{y_0}{\rho})$. Si llamamos $Q'(\rho)$ al conjunto de estos nuevos cuadrados (de lado tendiendo a 0 con ρ), entonces

$$\tfrac{l^2}{\rho^2}\,\#B(\rho) \;=\; \tfrac{l^2}{\rho^2}\,\#\tfrac{1}{\rho}\,B(\rho) \;=\; \tfrac{l^2}{\rho^2}\,\#Q'(\rho) \;=\; \left|\bigcup Q'(\rho)\right| \;\xrightarrow[\rho\to\infty]{}\; A(1) \;.$$

□

Lema 4.25. *Sea $A(\rho)$ definida por* (29) *y sea $B(\rho)$ definida por* (31)*. Entonces,*

$$\#B(\rho) \;=\; \tfrac{|A(\rho)|}{l^2} \;+\; O\left(\rho\right) \;.$$

Demostración. Estimaremos $\#B(\rho)$ hallando $\delta > 0$ tal que

$$A(\rho-\delta)\;\subset\;\bigcup Q(\rho)\;\subset\;A(\rho+\delta)\;.$$

Para lograr esto, relacionaremos el valor $F(x,y)$ en un punto con el valor $F(x+h,y+k)$ en un punto cercano (la idea es hacer que el vector (h,k) varíe a lo largo del borde de un cuadrado centrado en $(0,0)$):

$$F(x+h,y+k) \;=\; F(x,y) \;+\; 2\left(a\,xh + \tfrac{b}{2}\,(xk+yh) + c\,yk\right) \;+\; F(h,k)\;.$$

Supongamos que $F(x,y) \le \rho^2$. Entonces,

$$F(x+h,y+k) \;\le\; \rho^2 \;+\; \rho\,f(x/\rho,y/\rho) \;+\; F(h,k)\;,$$

donde

$$f(\xi,\upsilon) \;=\; 2\left(a\,\xi h + \tfrac{b}{2}\,(\xi k+\upsilon h) + c\upsilon k\right) \;=\; 2\,\begin{bmatrix}\xi & \upsilon\end{bmatrix}\begin{bmatrix}a & b/2\\ b/2 & c\end{bmatrix}\begin{bmatrix}h\\ k\end{bmatrix}\;.$$

Notamos que $(\xi, \upsilon) = (x/\rho, y/\rho) \in A(1)$. Si logramos acotar f en $A(1)$ y $F(h,k)$ de manera independiente de (x,y), obtendremos una fórmula asintótica (alguna). La función f depende del vector (h,k). De todas maneras, el máximo de f en $A(1)$ se alcanza en el borde de $A(1)$, es decir, en un par (ξ, υ) que cumple que $F(\xi, \upsilon) = 1$. El máximo se alcanzará en un punto en donde el gradiente de f y el gradiente de F sean proporcionales. El gradiente de f es

$$\nabla f(\xi, \upsilon) = \begin{bmatrix} 2\,ah + bk \\ bh + 2\,ck \end{bmatrix} = 2 \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} h \\ k \end{bmatrix}$$

y el gradiente de F es

$$\nabla F(\xi, \upsilon) = 2 \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} \xi \\ \upsilon \end{bmatrix} .$$

Entonces $(\xi, \upsilon) = \lambda\,(h,k)$ para cierto $\lambda \neq 0$. El valor de λ es el que garantiza que (ξ, υ) pertenezca al borde de $A(1)$, o sea $F(\lambda\,h, \lambda\,k) = 1$. Es decir,

$$\lambda^2 = \frac{1}{\sqrt{|F(h,k)|}} .$$

En particular, en $A(1)$,

$$f(\xi, \upsilon) \leq f(\lambda\,h, \lambda\,k) = 2 \begin{bmatrix} \lambda\,h & \lambda\,k \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} h \\ k \end{bmatrix} = 2\,\lambda\,F(h,k) .$$

En definitiva,

$$F(x+h, y+k) \leq \rho^2 + 2\,\lambda\,F(h,k) + F(h,k) = \big(\rho + \sqrt{|F(h,k)|}\big)^2 .$$

Como $(x,y) \in B(\rho)$ es el centro de uno de los cuadrados en $Q(\rho)$, sus vértices son $(x+h, y+k)$, donde (h,k) pertenece al conjunto

$$C := \big\{(l/2, \pm l/2), (-l/2, \pm l/2)\big\} .$$

Si elegimos

$$\Delta := \max\big\{|F(h,k)| \,:\, (h,k) \in C\big\} ,$$

entonces,

$$F(x+h, y+k) \leq \big(\rho + \Delta\big)^2 .$$

Esto implica que

$$\bigcup Q(\rho) \subset A(\rho + \Delta) .$$

Notemos que Δ no depende de ρ, sólo de F. Entonces, $F(x,y) \leq \rho^2$ implica $F(x+h, y+k) \leq \big(\rho+\Delta\big)^2$. Pero, también, $F(x+h, y+k) > \rho^2$ implica $F(x,y) > \big(\rho - \Delta\big)^2$. Con lo cual,[33]

$$A(\rho - \Delta) \subset \bigcup Q(\rho) \subset A(\rho + \Delta) .$$

$\square$

[33] La inclusión que faltaba: los cuadrados de $Q(\rho)$ que estaban completamente contenidos en $A(\rho)$ siguen siendo considerados en $Q(\rho - \Delta)$ y los que cortaban el borde de $A(\rho)$ quedan completamente afuera de $A(\rho - \Delta)$.

5 Primos en progresiones aritméticas (II)

6 Las sumas de Gauss

Referencias

[Apo76] T. M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts Math. Springer, Cham, 1976.

[Dav80] H. Davenport. *Multiplicative Number Theory*. 2nd. ed. Vol. 74. Grad. Texts Math. Springer, Cham, 1980.

[Lan99] E. Landau. *Elementary Number Theory*. Reprint of the 1966 2nd edition. Providence, RI: American Mathematical Society (AMS), 1999.