Capítulo 3

Primos en progresiones aritméticas

3.1. Caracteres y funciones L

Caracteres. Las funciones L de Dirichlet. Caracteres primitivos. Fórmula del número de clases.

Un carácter en un grupo abeliano finito G no es más que un homomorfismo de grupos $\chi : G \longrightarrow (\mathbb{C} - \{0\}, \cdot)$. Como los elementos de G tienen orden finito que divide a $|G|$, Im χ es siempre un subgrupo multiplicativo de las raíces $|G|$-ésimas de la unidad.

Los caracteres, con una definición más general, tienen un puesto destacado en la teoría de representaciones con sus implicaciones en el análisis armónico pero aquí no iremos tan lejos. Lo único que queremos es conjugar dos ideas: 1) Las funciones multiplicativas tienen productos de Euler asociados. 2) Las raíces de la unidad sirven para detectar progresiones aritméticas, por ejemplo $f(n) = q^{-1} \sum_{k=1}^{q} e(k(n-1)/q)$ es la función característica de $\{qn + a\}$.

Estos objetivos tienen un origen humilde en la observación de que $\sum n^{-s} = \prod(1 - p^{-s})^{-1}$ cuando $s \to 1^+$ implica que hay infinitos primos (Euler) mientras que el procedimiento falla si se quiere probar la infinitud de los primos de la forma $5n + 2$ empleando $\sum(5n + 2)^{-s}$. Esta función no tiene un producto de Euler similar al de ζ simplemente porque un número de la forma $5n + 2$ no tiene siempre factores primos de este mismo tipo. Se hace necesaria una manera de seleccionar progresiones aritméticas que sea coherente con una identidad como la de Euler.

Con este propósito consideramos inicialmente los caracteres del grupo $\mathbb{Z}_q^*$, los elementos invertibles de $(\mathbb{Z}/q\mathbb{Z}, \cdot)$, $q > 1$. Los caracteres forman un grupo con la multiplicación isomorfo al de partida. Por ejemplo $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ es un grupo cíclico de orden cuatro ($\mathbb{Z}_5^* = \{\ \overline{2}^0, \overline{2}^1, \overline{2}^3, \overline{2}^2\}$) cuyos caracteres son:

	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
χ_0	1	1	1	1
χ_1	1	i	$-i$	-1
χ_2	1	-1	-1	1
χ_3	1	$-i$	i	-1

y de nuevo forman un grupo cíclico de orden cuatro ($\chi_0 = \chi_1^4$ es la identidad, $\chi_1 = \chi_1^1$, $\chi_2 = \chi_1^2$ y $\chi_3 = \chi_1^3$).

En el primer capítulo, las funciones multiplicativas estaban definidas en $\mathbb{N}$, no en $\mathbb{Z}_q^*$, por tanto es natural redefinir $\chi(n)$ como $\chi(\overline{n})$ si $(n,q)=1$ y despreocuparnos del caso $(n,q)>1$ escribiendo $\chi(n)=0$. Con el abuso de notación obvio, llamaremos caracteres módulo q a las funciones obtenidas de esta forma y no emplearemos más la definición original.

Dicho de otro modo, en estas notas un *carácter módulo q* es una función aritmética multiplicativa de periodo q tal que $\chi(n)=0 \Leftrightarrow (n,q)>1$.

Al carácter trivial módulo q que vale 1 cuando $(n,q)=1$ se le llama *carácter principal* y se le suele denotar con χ_0.

A cada carácter le podemos asociar una *función L de Dirichlet*

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

y la multiplicatividad nos asegura un producto de Euler

$$L(s,\chi)=\prod(1-\chi(p)p^{-s})^{-1}.$$

Por ejemplo, con los caracteres de la tabla anterior

$$L(s,\chi_2)=\prod_{p\equiv 1,4\ (5)}(1-p^{-s})^{-1}\prod_{p\equiv 2,3\ (5)}(1+p^{-s})^{-1}=\prod\left(1-(\frac{p}{5})p^{-s}\right)^{-1}.$$

Veremos más adelante que la última expresión en términos del símbolo de Legendre no es casual cuando χ toma valores reales.

La manera efectiva a través de la cual los caracteres detectan progresiones aritméticas son las llamadas *relaciones de ortogonalidad*[1], gracias a ellas la construcción explícita de los caracteres es poco relevante y no la daremos aquí (véase [Da], [El]).

Proposición 3.1.1 (relaciones de ortogonalidad) *Para un carácter χ módulo q*

$$\sum_{n=1}^{q}\chi(n)=\begin{cases}\phi(q) & si\ \chi=\chi_0\\ 0 & si\ \chi\neq\chi_0\end{cases}$$

Si χ recorre todos los caracteres módulo q

$$\sum_{\chi}\chi(n)=\begin{cases}\phi(q) & si\ n\equiv 1\ (q)\\ 0 & si\ n\not\equiv 1\ (q)\end{cases}$$

Demostración: Supongamos que $\mathbb{Z}_q^*$ es cíclico generado por $\overline{r}$, entonces hay $|\mathbb{Z}_q^*|=\phi(q)$ caracteres determinados por la raíz de la unidad en la que se aplica $\overline{r}$, $\chi_j(r)=e(j/\phi(q))$, $0\leq j<\phi(q)$. Con esto ambas fórmulas se reducen a que la suma de las raíces k-ésimas de la unidad es cero excepto si $k=1$. Si $\mathbb{Z}_q^*$ no es cíclico, basta escribirlo como producto directo de grupos cíclicos (?!). □

[1]Si uno quiere que realmente parezcan de "ortogonalidad", conviene escribir en la primera $n\equiv ab^*$ con $b^*b\equiv 1\ (q)$, así $\chi(n)=\chi(a)\overline{\chi}(b)$, y en la segunda, $\chi=\chi_1\overline{\chi}_2$.

Corolario 3.1.2 *Si q y a son coprimos*

$$\sum_{n\equiv a\ (q)} \frac{\Lambda(n)}{n^s} = -\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \frac{L'(s,\chi)}{L(s,\chi)}$$

donde $\Re s > 1$ y χ recorre los caracteres módulo q.

Demostración: Como en el caso de la función ζ, por derivación logarítmica del producto de Euler

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \Lambda(n) \frac{\chi(n)}{n^s}.$$

Si $aa^* \equiv 1\ (q)$, se cumple $\overline{\chi}(a)\chi(n) = (\chi(a))^{-1}\chi(n) = \chi(a^*n)$ que sumando en χ se anula excepto si $n \equiv a\ (q)$. □

Sumando por partes se tiene la representación integral

$$L(s,\chi) = s \int_1^{\infty} t^{-s-1} \sum_{n\le t} \chi(n)\, dt. \tag{3.1}$$

Como $\sum_{n=1}^{q} \chi(n) = 0$ siempre que $\chi \neq \chi_0$, se tiene que en este caso la suma es de módulo menor que q y por tanto $L(s,\chi)$ tiene una extensión analítica a $\Re s > 0$ con $|L(s,\chi)| < C_\epsilon q$ si $\Re s > \epsilon$.

Si $\chi = \chi_0$ entonces la función L correspondiente se relaciona fácilmente con ζ

$$L(s,\chi_0) = \sum_{(n,q)=1} \frac{1}{n^s} = \prod_{p\not| q} (1-p^{-s})^{-1} = \zeta(s) \prod_{p|q} (1-p^{-s}) \tag{3.2}$$

y por tanto admite una extensión meromorfa en $\mathbb{C}$ con un único polo en $s = 1$ de residuo $\phi(q)/q$.

Si $L(s,\chi)$ es "buena" para $\chi \neq \chi_0$ y $L(s,\chi_0)$ tiene un polo en $s = 1$, parece que con el corolario anterior podríamos aprovechar la fuerza de la singularidad en $s = 1$ copiando la demostración del teorema de los números primos para deducir la asintótica de

$$\psi(x;a,b) = \sum_{\substack{n\equiv a\ (q)\\ n\le x}} \Lambda(n).$$

En parte es así, pero hay un serio escollo y es que aunque $L(s,\chi)$ sea buena cerca de $s = 1$, L'/L no lo sería si L tiene un cero ¡de nuevo los malvados ceros traban el camino directo! Se muestra como un problema ineludible (y difícil) probar $L(1,\chi) \neq 0$. Otro problema relacionado de gran importancia en las aplicaciones es que incluso si $L(1,\chi) \neq 0$, la existencia de ceros cada vez más cercanos a $s = 1$ cuando q aumenta, echarían al traste la uniformidad de los resultados. Volveremos sobre ello más adelante. Por ahora veamos que la prueba analítica debida a Euler de la infinitud de los primos se puede extender al caso de primos en progresión aritmética, una vez establecido el resultado de no anulación.

Teorema 3.1.3 *Para cualquier carácter no principal, χ, se cumple $L(1,\chi)\neq 0$.*

Corolario 3.1.4 *(Dirichlet) Si a y q son coprimos, hay infinitos primos en la progresión aritmética $\{qn+a\}_{n\in\mathbb{N}}$.*

Demostración: Por el Corolario 3.1.2 y el teorema anterior, para $1<s<1+\epsilon$ con ϵ suficientemente pequeño,

$$\sum_{n\equiv a\ (q)}\frac{\Lambda(n)}{n^s}=-\frac{1}{\phi(q)}\frac{L'(s,\chi_0)}{L(s,\chi_0)}+O(1).$$

Teniendo en cuenta (3.2),

$$\sum_{n\equiv a\ (q)}\frac{\Lambda(n)}{n^s}=-\frac{1}{\phi(q)(s-1)}+O(1)$$

y basta tomar $s\to 1^+$. □

Daremos una demostración elemental y breve del Teorema 3.1.3 (esencialmente seguimos [St], véase en [Da] §4 otra prueba). Los razonamientos originales de Dirichlet fueron mucho más complejos pero con interesantes implicaciones que mencionaremos después (en [Da] §1,6 hay un tratamiento más detallado).

Demostración del Teorema 3.1.3: Tomemos $a=1$ en el Corolario 3.1.2. Si $L(1,\chi)=0$ exactamente para k caracteres módulo q contando multiplicidades (los ceros dobles cuentan por dos, etc.), se tiene

$$\sum_{n\equiv 1\ (q)}\frac{\Lambda(n)}{n^s}=-\frac{1-k}{\phi(q)(s-1)}+O(1).$$

Evidentemente el primer miembro es positivo o nulo (todavía no hemos probado incondicionalmente que hay primos en progresiones aritméticas, así que la suma podría ser vacía), por lo tanto a lo más existe un carácter módulo q con $L(1,\chi)=0$ y además el cero, si existe, es simple (tómese $s\to 1^+$). Esto descarta automáticamente los caracteres que toman valores complejos, porque $L(1,\chi)=0\Leftrightarrow L(1,\overline{\chi})=0$.

Supongamos por tanto que $\chi\neq\chi_0$ es un carácter real (Im $\chi\subset\{-1,0,1\}$) y sea $f=1*\chi$. Se tiene $f(p^{2\alpha})\geq 1$ en general $f(p^\beta)\geq 0$ que se extiende a $f\geq 0$ por la multiplicatividad. Con ello

$$1<\sum_{md\leq x}\frac{\chi(d)}{m^{1/2}d^{1/2}}=\sum_{d\leq x^{1/2}}\frac{\chi(d)}{d^{1/2}}\sum_{m\leq x/d}\frac{1}{m^{1/2}}+\sum_{m\leq x^{1/2}}\frac{1}{m^{1/2}}\sum_{x^{1/2}<d\leq x/m}\frac{\chi(d)}{d^{1/2}}$$

donde lo único que se ha hecho es separar los términos con $m\geq d$ y con $m<d$.

Sumando por partes (recuérdese que $\sum_{N<n\leq N+q}\chi(n)=0$)

$$\sum_{m\leq x/d}\frac{1}{m^{1/2}}=2\big(\frac{x}{d}\big)^{1/2}+\mathrm{cte}+O\big(\big(\frac{x}{d}\big)^{-1/2}\big)\qquad\text{y}\qquad\sum_{x^{1/2}<d\leq x/m}\frac{\chi(d)}{d^{1/2}}=O(x^{-1/4}).$$

Sustituyendo

$$1 < 2x^{1/2} \sum_{d \le x^{1/2}} \frac{\chi(d)}{d} + O(1) = 2x^{1/2} L(1,\chi) + O(1)$$

donde se ha sumado por partes para probar que los términos con $d > x^{1/2}$ no contribuyen sustancialmente. Tomando x suficientemente grande se tiene

$$L(1,\chi) > 0$$

para cualquier carácter real no principal. □

Dado un carácter se puede aumentar artificialmente su módulo introduciendo los ceros que sean necesarios. Por ejemplo$\chi(1) = 1$, $\chi(2) = -1$, $\chi(3) = 0$ define un carácter módulo 3 (el único no principal) y se puede extender a otro módulo $105 = 3 \cdot 35$ como

$$\widetilde{\chi}(n) = \begin{cases} \chi(n) & \text{si } (n,105) = 1 \\ 0 & \text{si } (n,105) > 1 \end{cases}$$

Los caracteres que tienen realmente cierto módulo sin estos artificios reciben una denominación especial.

Definición: Se dice que un carácter no principal módulo q, χ, es *primitivo* si no existe ningún carácter λ con módulo menor tal que $\chi(n) = \lambda(n)$ para todo $(n,q) = 1$.

Si χ no es primitivo, siempre existe un λ primitivo con la propiedad indicada en la definición anterior, en este caso el producto de Euler implica

$$L(s,\chi) = L(s,\lambda) \prod_{p|q} (1 - \lambda(p) p^{-s}). \tag{3.3}$$

Así pues el estudio de los ceros en las cercanías de $s = 1$ (y de hecho en todo $\Re s > 0$) puede reducirse al caso de caracteres primitivos. Esto es muy conveniente porque sus funciones L son más manejables.

Si $q = p^\alpha$ con p primo impar, $\mathbb{Z}_{p^\alpha}^*$ es cíclico [Ga] Sec. 3, digamos generado por $\overline{r}$. Los únicos caracteres reales están determinados por $\chi(r) = \pm 1$. Si $\chi(r) = 1$ el carácter es uno siempre que puede y $\chi = \chi_0$, mientras que si $\chi(r) = -1$, es 1 sólo en las potencias pares y por tanto (!?)

$$\chi(n) = \left(\frac{n}{p}\right) = \left(\frac{(-1)^{(p-1)/2} p}{n}\right).$$

Si $p = 2$, sólo son cíclicos $\mathbb{Z}_4^*$ y $\mathbb{Z}_8^*$. Con la extensión de Kronecker del símbolo de Legendre (véase [Da] §5) los caracteres reales no principales para estos módulos pueden escribirse como

$$\left(\frac{-4}{n}\right), \qquad \left(\frac{8}{n}\right) \quad \text{y} \quad \left(\frac{-8}{n}\right).$$

Con ello hemos hallado explícitamente los caracterese primitivos reales (!?)

Lema 3.1.5 *Un carácter primitivo primitivo real χ es de la forma*

$$\chi(n) = \left(\frac{d}{n}\right)$$

donde d es igual a un elemento del conjunto $\{1, -4, 8, -8\}$ quizá multiplicado por factores distintos de la forma $(-1)^{(p-1)/2}p$ (con $p > 2$ primo). El módulo de χ es $|d|$.

La no anulación de $L(1, \chi)$ era "sencilla" para caracteres complejos y según (3.3) y el lema anterior, la parte difícil es equivalente a

$$\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{d}{n}\right) \neq 0.$$

De hecho por la prueba del Teorema 3.1.3, esta cantidad debe ser positiva. ¿Qué misteriosa razón explica que los $+1/n$ ganen siempre a los $-1/n$? ¿no están los signos del símbolo de Legendre distribuidos al azar?

Dirichlet demostró que el valor de dicha serie depende ¡del número de clases del anillo de enteros de $\mathbb{Q}(\sqrt{d})$! Nos limitaremos aquí a mencionar el caso $d < 0$ (si $d > 0$ también participa en la fórmula la llamada "unidad fundamental").

Fórmula del número de Clases (Dirichlet 1840): Sean χ y d como en el lema anterior con $d < 0$. Si $h(d)$ es el *número de clases* de $\mathbb{Q}(\sqrt{d})$) (el orden del grupo de clases de su anillo de enteros) entonces

$$L(1, \chi) = \frac{\pi}{\sqrt{-d}} c_d h(d)$$

donde $c_{-4} = 1/2$, $c_{-3} = 1/3$ y $c_d = 1$ en otro caso.

Por ejemplo, si $d = -4$ el anillo de enteros de $\mathbb{Q}(\sqrt{-4})$ es $\mathbb{Z}[i]$, como allí hay factorización única, $h(-4) = 1$ y se tiene

$$L(1, \chi) = \frac{\pi}{4} \qquad \text{con} \qquad \chi(n) = \left(\frac{-4}{n}\right).$$

La comprobación es sencilla usando $L(1, \chi) = \sum_{k=0}^{\infty} (-1)^k/(2k + 1)$ y el desarrollo en serie de $\arctan x$.

Se puede invertir el proceso para calcular el número de clases de anillos cuadráticos. Así por ejemplo, $\mathbb{Z}[\sqrt{-5}]$ es el anillo de enteros de $\mathbb{Q}(\sqrt{-5}) = \mathbb{Q}(\sqrt{d})$ con $d = -4 \cdot 5$, por tanto el número de clases de $\mathbb{Z}[\sqrt{-5}]$ es

$$h(-20) = \frac{2\sqrt{5}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{-20}{n}\right).$$

Tomando 15 términos no nulos ya se tiene que el valor de la serie está en $[1'3, 1'5]$ y esto es más que suficiente para concluir que el número de clases sólo puede ser dos. Con

algún esfuerzo se puede incluso dar una fórmula cerrada general para $L(1,\chi)$ como suma finita [Da] §6, sin embargo no se conoce una prueba directa de que tal suma es no nula.

Con este procedimiento, $L(1,\chi) \neq 0$ es consecuencia de la (evidente) positividad del número de clases (incluso en el caso $d > 0$ que no hemos considerado). Además preguntas acerca del tamaño del número de clases que tienen una larga historia que se remonta a Gauss [Ga], se traducen en acotaciones más precisas que $L(1,\chi) \neq 0$.

¿Cómo es posible que Gauss y Dirichlet estudiasen el número de clases si Kummer no introdujo los ideales hasta 1843? ¿Qué misterios se ocultan tras la sorprendente fórmula del número de clases? Una breve e incompleta respuesta a estas preguntas es que el número de clases del anillo de enteros de $\mathbb{Q}(\sqrt{d})$ tiene una representación (la definición original, históricamente) en términos de formas cuadráticas. Si se asocia a una forma cuadrática $Q = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$ el ideal $\langle a, (-b + \sqrt{d})/2\rangle$ con $d = b^2 - 4ac$, resulta que la estructura del grupo de clases se refleja en la de las formas cuadráticas de discriminante d y las clases de ideales equivalen a clases de formas cuadráticas que no pueden transformarse unas en otras por cambios de variable enteros invertibles. Así por ejemplo, $Q_1 = x^2+y^2$ y $Q_2 = 5x^2+6xy+2y^2$ son dos formas de discriminante $d = -4$ en la misma clase porque Q_2 se obtiene a partir de Q_1 con el cambio $x \mapsto 2x+y$, $y \mapsto x+y$. Se puede probar (y no es difícil) que todas las formas de discriminante $d = -4$ se pueden transformar en Q_1 y por ello el número de clases para $d = -4$ es 1. En general, para cada discriminante hay un número finito de clases. Por otra parte, la teoría de formas cuadráticas da una fórmula, con símbolos de Legendre, para calcular el número de representaciones de un número por formas de alguna clase. Lo que hizo Dirichlet es emplear que al variar $n \leq N$ cada forma representa más o menos la misma cantidad de números (para d negativo son los puntos dentro de una elipse $ax^2 + bxy + cy^2 \leq N$, aproximadamente $2\pi N/\sqrt{-d}$). Con todo esto se puede relacionar una suma de símbolos de Legendre con una suma sobre clases y de ahí sale la fórmula (véase [Hu] y [Da]).

3.2. Primos en progresión aritmética

El teorema de los números primos en progresiones aritméticas. La ecuación funcional de $L(s,\chi)$. Ceros y término de error. Ceros excepcionales.

Dado q hay $\phi(q)$ números $1 \leq a \leq q$ coprimos con q y parece natural que los primos se equidistribuyan en las $\phi(q)$ sucesiones $\{qn + a\}$ que contienen infinitos de ellos. La cantidad que pretendemos medir es

$$\pi(x; q, a) = \{p \leq x \ : \ p \equiv a \ (q)\}$$

que se complementa con dos funciones ψ, la primera de las cuales ya apareció en la sección anterior

$$\psi(x; a, b) = \sum_{\substack{n \equiv a \ (q) \\ n \leq x}} \Lambda(n) \qquad \text{y} \qquad \psi(x, \chi) = \sum_{n \leq x} \chi(n)\Lambda(n).$$

Teorema 3.2.1 (de los números primos en progresiones aritméticas) *Para a y q coprimos fijados*

$$\pi(x;q,a) \sim \frac{\mathrm{Li}(x)}{\phi(q)}.$$

Sumando por partes, el teorema de los números primos en progresiones aritméticas equivale a

$$\psi(x;q,a) \sim \frac{x}{\phi(q)}.$$

Por otro lado, la fórmula

$$\psi(x;q,a) = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a)\psi(x,\chi) \tag{3.4}$$

donde χ recorre los caracteres módulo q, obtenida de las relaciones de ortogonalidad, permite deducir el teorema de los números primos en progresiones aritméticas a partir de

$$\psi(x,\chi_0) \sim x \qquad \text{y} \qquad \psi(x;\chi) = o(x) \qquad \text{para} \qquad \chi \neq \chi_0.$$

A través de la "fórmula mágica", analoga a la de $\psi(x)$,

$$\psi(x;\chi) = -\frac{1}{2\pi i} \int_L \frac{L'(s,\chi)}{L(s,\chi)} \frac{x^s}{s}\, ds, \tag{3.5}$$

uno podría copiar la definición clásica del teorema de los números primos. En cierta manera esto funciona[2] pero hay que comprobar que algunos puntos son relamente similares. Por otro lado hay un serio problema con la uniformidad en q (que es importante en la aplicaciones) por la posible existencia de ceros reales $1/2 < \rho < 1$ que no tienen equivalente en el caso de la función ζ.

Comencemos probando que también $L(s,\chi)$ satisface una ecuación funcional. Realmente sólo adquiere una forma aceptable cuando χ es un carácter primitivo, la razón última es que sólo para ellos

$$\sum_{n=1}^{q} \chi(\alpha n + \beta) = 0 \tag{3.6}$$

cualesquiera que sean β y $\alpha \not\equiv 0\ (q)$. Para probarlo, si $(q,\alpha) = 1$ basta hacer el cambio $u = \alpha n + \beta$ módulo q, en otro caso tomando $q' = q/(\alpha, q)$ es fácil ver que $\chi(1+q'k)\chi(\alpha n + \beta) = \chi(\alpha(n+n_0)+\beta)$ para cierto n_0, lo que implica que el primer miembro de (3.6) es invariante al multiplicar por $\chi(1+q'k)$ y si esta cantidad fuera constantemente 1 al variar k, χ estaría inducido por un carácter módulo $q' < q$.

Esta propiedad aparece al hallar el desarrollo de Fourier discreto de un carácter, que es necesaria en la deducción de la ecuación funcional.

[2]También en este caso hay demostraciones elementales [Se] o simplificadas [Ne] que de nuevo tienen el inconveniente de que no muestran la verdadera naturaleza del término de error.

Lema 3.2.2 *Si χ es un carácter primitivo módulo q, se cumple*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{k=1}^{q} \overline{\chi}(k) e(nk/q)$$

donde

$$\tau(\chi) = \sum_{k=1}^{q} \chi(k) e(k/q)$$

es la llamada suma de Gauss *y verifica* $|\tau(\chi)| = \sqrt{q}$.

Demostración: Si $(n, q) = 1$, con el cambio de variable (módulo q) $u = nk$ se tiene $\chi(k) = \chi(u)\overline{\chi(n)}$ y la fórmula es inmediata. Si $(n, q) > 1$, $\chi(n) = 0$ y dividiendo la sumación en progresiones aritméticas con diferencia $q/(q, n)$, también el segundo miembro se anula por (3.6).

La prueba de $|\tau(\chi)| = \sqrt{q}$ es truculenta:

$$|\tau(\chi)|^2 = \frac{1}{\phi(q)} \sum_{n=1}^{q} |\chi(n)|^2 |\tau(\chi)|^2 = \frac{1}{\phi(q)} \sum_{n=1}^{q} \left| \sum_{k=1}^{q} \chi(k) e(nk/q) \right|^2.$$

Desarrollando el cuadrado e intercambiando el orden de sumación se deduce $|\tau(\chi)|^2 = q$. □

Proposición 3.2.3 *Sea χ un carácter primitivo módulo q, entonces $L(s, \chi)$ admite una extensión entera. Además, si $\chi(-1) = 1$*

$$(q/\pi)^{s/2} \Gamma(s/2) L(s, \chi) = \epsilon_\chi (q/\pi)^{(1-s)/2} \Gamma((1-s)/2) L(1-s, \overline{\chi}) \qquad \textit{con} \quad \epsilon_\chi = \frac{\tau(\chi)}{\sqrt{q}}$$

y si $\chi(-1) = -1$

$$(q/\pi)^{(s+1)/2} \Gamma((s+1)/2) L(s, \chi) = \epsilon_\chi (q/\pi)^{(2-s)/2} \Gamma((2-s)/2) L(1-s, \overline{\chi}) \qquad \textit{con} \quad \epsilon_\chi = \frac{\tau(\chi)}{i\sqrt{q}}.$$

Demostración: Comencemos como en el caso de la función ζ, partiendo de la definición de la función Γ en $s/2$ para probar

$$\pi^{-s/2} q^{s/2} \Gamma(s/2) \sum_{n=1}^{\infty} \chi(n) n^{-s} = \sum_{n=1}^{\infty} \int_0^\infty t^{s/2-1} \chi(n) e^{-\pi n^2 t/q} \, dt \qquad \text{para} \quad \Re s > 1. \tag{3.7}$$

Si $\chi(-1) = 1$,

$$\sum_{n=1}^{\infty} \chi(n) e^{-\pi n^2 t/q} = \frac{1}{2} \theta(t, \chi) \qquad \text{con} \quad \theta(t, \chi) = \sum_{n=-\infty}^{\infty} \chi(n) e^{-\pi n^2 t/q},$$

donde se ha extendido la definición de χ a $\mathbb{Z}$ usando la periodicidad. Veamos que $\theta(t,\chi)$, como $\theta(t)$, goza de cierta invariancia $t \mapsto 1/t$. Para ello aplicamos el lema anterior y la fórmula de sumación de Poisson

$$\begin{aligned}\theta(t,\chi) = \frac{1}{\tau(\overline{\chi})}\sum_{k=1}^{q}\overline{\chi}(k)\sum_{n=-\infty}^{\infty} e^{-\pi n^2 t/q}e(kn/q) &= \frac{\sqrt{q}}{\tau(\overline{\chi})\sqrt{t}}\sum_{k=1}^{q}\overline{\chi}(k)\sum_{n=-\infty}^{\infty} e^{-\pi q(n+k/q)^2/t} \\ &= \frac{\sqrt{q}}{\tau(\overline{\chi})\sqrt{t}}\theta(t^{-1},\overline{\chi}).\end{aligned}$$

Dividiendo la integración en (3.7) en los intervalos $[0,1]$ y $[1,\infty)$ y usando esta fórmula de transformación en la primera,

$$\pi^{-s/2}q^{s/2}\Gamma(s/2)L(s,\chi) = \frac{\sqrt{q}}{2\tau(\overline{\chi})}\int_1^\infty t^{(-s-1)/2}\theta(t,\overline{\chi})\,dt + \frac{1}{2}\int_1^\infty t^{s/2-1}\theta(t,\chi)\,dt.$$

Esto prueba la extensión entera y también la ecuación funcional porque el segundo miembro es invariante al cambiar $s \mapsto 1-s$, $\chi \mapsto \overline{\chi}$ salvo multiplicación por $\tau(\overline{\chi})/\sqrt{q} = \overline{\tau(\chi)}/\sqrt{q} = \sqrt{q}/\tau(\chi)$.

Si $\chi(-1) = -1$ entonces $\theta(t,\chi) = 0$ y el argumento anterior no funciona. El parche consiste en definir

$$\widetilde{\theta}(t,\chi) = \sum_{n=-\infty}^{\infty} n\chi(n)e^{-\pi n^2 t/q}$$

que satisface

$$\widetilde{\theta}(t,\chi) = \frac{i\sqrt{q}}{t\tau(\overline{\chi})\sqrt{t}}\widetilde{\theta}(t^{-1},\overline{\chi}).$$

Introducir esta nueva n en la definición de $\theta(t,\chi)$ es como multiplicar en (3.7) por n y el paso $n^{-s} \mapsto n^{1-s}$ tiene como efecto que la ecuación funcional aparezca trasladada una unidad (!?) en el resultado final. □

Como en el caso de la función ζ, esta demostración ya nos da alguna información acerca de los ceros.

Corolario 3.2.4 *Sea χ un carácter primitivo, si $\chi(1) = 1$, $L(s,\chi)$ tiene ceros simples en $s = 0, -2, -4, -6\ldots$ y si $\chi(-1) = -1$, $L(s,\chi)$ tiene ceros simples en $s = -1, -3, -5, -7\ldots$. en cualquier caso, aparte de estos ceros llamados* ceros triviales*, el resto están en la banda crítica $0 \le \Re s \le 1$. Además si ρ es un cero no trivial, también lo es $1-\overline{\rho}$.*

La restricción a caracteres primitivos no es demasiado drástica porque gracias a la relación (3.3) la única diferencia es que para caracteres no primitivos aparecen unos pocos ceros con $\Re\rho = 0$ asociados a primos que dividen al módulo.

Con una prueba similar a la de la función ζ, para $\chi \neq \chi_0$ se tiene la expresión

$$\frac{L'(s,\chi)}{L(s,\chi)} = K_\chi - \frac{\Gamma'((s+\delta)/2)}{2\Gamma((s+\delta)/2)} + \sum_\rho\Big(\frac{1}{s-\rho}+\frac{1}{\rho}\Big) \tag{3.8}$$

donde ρ recorre los ceros no triviales de ζ y $\delta = (1-\chi(-1))/2$. De aquí se puede deducir también en este caso que no hay demasiados ceros en bandas horizontales.

Corolario 3.2.5 *El número de ceros no triviales de* $L(s,\chi)$ *en* $T \le \Im\rho \le T+1$ *es* $O(\log(q(|T|+2)))$.

Al aplicar el teorema de los residuos a (3.5) se tiene formalmente una fórmula explícita para $\psi(x,\chi)$ en términos de los ceros de $L(s,\chi)$. si ρ es un cero no trivial, el residuo en $s=\rho$ es $-x^\rho/\rho$. Sin entrar en detalles, para evitar dificultosos problemas de convergencia es conveniente truncar la serie y se puede probar:

Teorema 3.2.6 *Si* χ *es no principal de módulo* q, *para* $T \le x$

$$\psi(x,\chi) = -\sum_{|\Im\rho|<T} \frac{x^\rho - 1}{\rho} + O\big(\frac{x}{T}(\log x)^2\big)$$

uniformemente en $q \le x$.

Observación: Para $\chi = \chi_0$ la expresión es válida sin más que sumar x, que proviene del residuo en $s=1$, o alternativamente se deriva de la fórmula explícita para $\psi(x)$ teniendo en cuenta (3.2).

El -1 que acompaña a x^ρ (y que no aparece en el residuo) es sólo una precaución porque en principio no sabemos si hay muchos ceros cercanos a 0, que provocarían que algunos términos en la serie fueran demasiado grandes. Si nos negamos a escribir este -1 entonces no nos podemos olvidar del residuo en $s=0$, que es K_χ y está relacionado con $\sum(1/\rho + 1/(2-\rho))$, tomando $s=2$ en (3.8), que se compensa (??) con una porción de $-\sum 1/\rho$ cuando ρ es muy pequeño.

A través de este resultado se muestra fundamental entender la distribución de los ceros de las funciones L y esto resulta ser un problema (¡cómo no!) muy difícil.

Lo que soñaríamos es:

Hipótesis de Riemann: *Todos los ceros con* $\Re\rho > 0$ *de cualquier función* $L(s,\chi)$ *cumplen* $\Re\rho = 1/2$.

De los dos últimos resultados resultados se deduce:

Corolario 3.2.7 *Suponiendo la hipótesis de Riemann generalizada, para* $(a,q)=1$ *se cumple*

$$\psi(x;q,a) = \frac{x}{\phi(q)} + O(x^{1/2}(\log x)^2) \qquad y \qquad \pi(x;q,a) = \frac{Li(x)}{\phi(q)} + O(x^{1/2}\log x)$$

uniformemente en q.

Y lo que sabemos probar es bien poco, de hecho algo menos que en el caso de la función ζ si exigimos uniformidad en q.

Proposición 3.2.8 *Existe una constante absoluta (computable) $C > 0$ tal que cualquier $L(s,\chi)$ tiene a lo más un cero en la región*

$$\{\sigma + it \ : \ \sigma > 1 - \frac{C}{\log(q(|t|+2))}\}.$$

Dicho cero, si existe, es real y simple y sólo puede aparecer cuando χ es real y no principal.

Ese cero que se puede colar en la presunta región libre de ceros es el causante de que algunos teoremas dejen de ser "redondos" cuando q varía. Es lógico dar una denominación especial a nuestra frustración.

Definición: Se dice que un cero de $L(s,\chi)$ es un *cero excepcional* si está dentro de la región del teorema anterior.

Obviamente la definición depende del valor de C que no hemos hecho explícito pero éste no será relevante en razonamientos posteriores.

Antes de entrar en la demostración de

Corolario 3.2.9 *Para cualquier carácter χ de módulo q*

$$\psi(x,\chi) = E(x) + O\big(x(\log x)^2 e^{-C(\log x)/(\log q + \sqrt{\log x})}\big)$$

donde $C > 0$ es cierta constante absoluta y $E(x) = x^\beta/\beta$ si hay un cero excepcional de $L(s,\chi)$ en $s = \beta$, $E(x) = x$ si $\chi = \chi_0$ y $E(x) = 0$ en el resto de los casos.

Demostración: Nótese que el resultado es trivial si $q \gg x^\delta$ para algún δ. Si $\rho = \beta + i\gamma$, entonces por la Proposición 3.2.8

$$x^\rho \ll x e^{-C(\log x)/(\log q + \log(|\gamma|+2))}.$$

Escogiendo $T = e^{\sqrt{\log x}}$ en el Teorema 3.2.6 y empleando que hay $O(\log(q(n+2)))$ ceros con $n \le |\gamma| < n+1$, se deduce el resultado. □

Demostración de la Proposición 3.2.8: Siempre podemos suponer, gracias a (3.3), que o bien $\chi = \chi_0$ o bien χ es primitivo. Por (3.2) en el caso $\chi = \chi_0$ no hay nada nuevo que probar. Para el resto, la prueba es muy similar a la de la región libre de ceros para la función ζ, Proposición 1.4.10, empleando

$$-3\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} - \Re\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)} \ge 4\Re\frac{L'(\sigma+it,\chi)}{L(\sigma+it,\chi)} \qquad \text{para } \sigma > 1.$$

Si $\chi \neq \chi_0$, esto es, si χ no es un carácter real, por (3.8) se tiene

$$-\Re\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)} \le C\log(q(|t|+2)) - \Re\sum_\rho \frac{1}{\sigma+2it-\rho} \le C\log(q(|t|+2))$$

ya que tomando s grande, como habíamos mencionado, K_χ compensa a $\sum 1/\rho$ (?!). Con esto se obtiene la región libre de ceros sin ninguna excepción simplemente repitiendo la prueba de la Proposición 1.4.10 cambiando los $|t|+2$ por $q(|t|+2)$. Sin embargo, si $\chi^2=\chi_0$ esta acotación no es en principio cierta porque (3.8) no lo es, habría que emplear la Proposición 1.4.8 en su lugar, teniendo en cuenta (3.2), lo que daría

$$-\Re\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)}\le \Re\frac{1}{\sigma-1+2it}+C\log(q(|t|+2)).$$

Si t no es muy pequeño esto no nos causará ningún problema porque el primer sumando del segundo miembro es despreciable, pero si t es de orden menor que $1/\log q$, entonces el primer término podría acabar con el segundo. En el resto de los casos todo estaría bajo control.

Es decir, hemos probado que si hay ceros en la región del enunciado, χ debe ser real y los posibles ceros cumplen $|\Im\rho|=o(1/\log q)$. Falta probar que a lo más hay uno de estos ceros malos (contando multiplicidades), ello implica que sólo puede ser real ($L(\rho,\chi)=0$ $\Rightarrow L(\overline{\rho},\chi)=0$ si χ es real).

Si hubiera dos ceros malos ρ y ρ' o uno múltiple ($\rho=\rho'$), de nuevo por (3.8)

$$\Re\frac{L'(\sigma+it,\chi)}{L(\sigma+it,\chi)}\ge -C\log(q(|t|+2))+\Re\left(\frac{1}{\sigma+it-\rho}+\frac{1}{\sigma+it-\rho'}\right).$$

si alguno de ellos no fuera real, podemos suponer $\rho'=\overline{\rho}$, y si los dos fueran reales, $\rho'\ge\rho$ (pondríamos $\rho=\rho'$ si el cero es múltiple). En cualquier caso si $\rho=\beta+i\gamma$ con $\gamma\ge 0$, la parte real en la cota inferior anterior para $t=\gamma$ es $(\sigma-\beta)^{-1}+(\sigma-\beta)/((\sigma-\beta)^2+4\gamma^2)$ y la desigualdad original da con estas acotaciones

$$\frac{3}{\sigma-1}+\Re\frac{1}{\sigma-1+2i\gamma}+C\log(q(|\gamma|+2))>\frac{4}{\sigma-\beta}+\frac{4(\sigma-\beta)}{(\sigma-\beta)^2+4\gamma^2}.$$

Si $\gamma<\epsilon/\log q$ con ϵ pequeño, eligiendo $\sigma=1+2\epsilon/\log q$ se llega a una contradicción si $\beta>1-\epsilon/\log q$ (en ese caso $\sigma-\beta<3\epsilon/\log q$). Es decir, hemos probado que existe un ϵ universal tal que $L(s,\chi)$ con χ real y primitivo no tiene más de un cero $\rho=\beta+i\gamma$ con $|\gamma|<\epsilon/\log q$ y $\beta>1-\epsilon/\log q$, entonces se puede ajustar la constante del enunciado para que se cumpla también la segunda parte de la conclusión. □

3.3. El Teorema de Siegel

Enunciado y demostración. El teorema de Siegel-Walfisz

Se puede probar que no hay ceros excepcionales tan cerca de uno como algo comparable a una potencia negativa del módulo. Éste es un resultado importante, el Teorema de Siegel, porque permite domesticar un poco mejor la dependencia en q del error en el teorema de los números primos en progresiones aritméticas.

Teorema 3.3.1 (Teorema de Siegel) *Para cada $\epsilon>0$ existen $C_\epsilon, C'_\epsilon>0$ tales que para todo χ carácter primitivo módulo q se cumple*

$$L(1,\chi)>C_\epsilon q^{-\epsilon}\qquad y\qquad L(\sigma,\chi)>0\quad para\quad \sigma>1-C'_\epsilon q^{-\epsilon}.$$

Observación: Con los conocimientos actuales no se conoce ninguna fórmula que produzca constantes válidas C_ϵ y C'_ϵ a partir de cada valor de ϵ. Se dice que C_ϵ y C'_ϵ son *no efectivas*, lo cual tiene su repercusión negativa en las aplicaciones. La razón última de la no efectividad es que en la demostración se emplea la repulsión de los ceros reales: si hubiera alguno muy cercano a 1 no podría haber más. El desconocimiento acerca de la posible aparición de tal cero causa la incertidumbre en las constantes.

Hay varias pruebas simplificadas del Teorema de Siegel, aquí seguiremos la de Estermann a través de [Da] (véase también la de Goldfeld en el original [Go] o en [Iw-Ko] §5). El peso del argumento recae en la positividad de los coeficientes de la serie de Dirichlet de

$$F(s) = \zeta(s)L(s,\chi)L(s,\widetilde{\chi})L(s,\chi\widetilde{\chi})$$

cuando los caracteres involucrados son reales no principales. Con ello se llega a probar que no puede ser mucho menor en valor absoluto que su aproximación de Laurent de orden -1 en $s=1$

$$G(s) = (s-1)^{-1}L(1,\chi)L(1,\widetilde{\chi})L(1,\chi\widetilde{\chi}).$$

Lema 3.3.2 *Sean χ y $\widetilde{\chi}$ caracteres reales y primitivos con módulos $q \neq \widetilde{q}$, respectivamente. Entonces*

$$F(s) > \frac{1}{2} + C\frac{G(s)}{(q\widetilde{q})^{8(s-1)}} \qquad \textit{para} \qquad \frac{7}{8} < s < 1$$

donde C es una constante positiva, absoluta y efectiva.

Observación: Las constantes $1/2$, 8 y $7/8$ se pueden mejorar con la misma prueba pero su valor es irrelevante en la demostración del teorema.

Demostración: Procediendo como en el caso de la función ζ, con derivadas logarítmicas de los productos de Euler, para $\Re s > 1$

$$-\frac{F'}{F}(s) = \sum \frac{\Lambda(n)}{n^s}\big(1+\chi(n)+\widetilde{\chi}(n)+(\chi\widetilde{\chi})(n)\big) = \sum \frac{\Lambda(n)}{n^s}\big(1+\chi(n)\big)\big(1+\widetilde{\chi}(n)\big).$$

Integrando, $\log F(s)$ se expresa como una serie de Dirichlet de coeficientes positivos y de ahí, $F(s)$ goza de la misma propiedad (!?). Por tanto para $s>1$, donde la serie converge uniformemente sobre compactos, $(-1)^k F^{k)}(s) > 0$. Alrededor de $s=2$ se tendrá un desarrollo de Taylor de la forma

$$F(s) = \sum_{m=0}^{\infty} b_m (2-s)^m \qquad \text{con} \qquad b_m \geq 0$$

válido en $|s-2|<1$, además $b_0 = F(2) > 1$. Lo que impide extender más allá la validez de este desarrollo es el polo en $s=1$, el cual se puede suprimir restando $G(s)$:

$$F(s) - G(s) = \sum_{m=0}^{\infty} c_m (2-s)^m \tag{3.9}$$

con

$$c_m = b_m - L(1,\chi)L(1,\widetilde{\chi})L(1,\chi\widetilde{\chi}) \geq -G(s)(s-1). \tag{3.10}$$

Por (3.1) (véanse los comentarios que siguen) se cumple

$$|F(s)-G(s)| \ll q\cdot\widetilde{q}\cdot q\widetilde{q} = (q\widetilde{q})^2 \qquad \text{en} \quad |s-2| = 3/2$$

(con una constante "$\ll$" efectiva), por tanto

$$c_m = -\frac{1}{2\pi i}\int_{|s-2|=\frac{3}{2}} \frac{F(s)-G(s)}{(2-s)^{m+1}}\,ds \ll (q\widetilde{q})^2\big(\frac{2}{3}\big)^m. \tag{3.11}$$

Descomponiendo la sumación en (3.9) en los rangos $m < M$ y $m \geq M$ y empleando (3.10) en el primero y (3.11) en el segundo,

$$F(s)-G(s) \geq 1 + G(s)\big((2-s)^M - 1\big) - C(q\widetilde{q})^2\big(\frac{2}{3}\big)^M.$$

Eligiendo $M = 8\log(q\widetilde{q}) + c_0$ con c_0 una constante adecuada (para que el último término engulla menos de medio uno), se obtiene el resultado, de hecho algo mejor. □

Demostración del Teorema de Siegel: Supongamos primero que $L(s,\widetilde{\chi})$ nunca tiene un cero real con $1-\epsilon/16 \leq s < 1$ cualquiera que sea $\widetilde{\chi}$ real y primitivo. Entonces la segunda parte del teorema es trivial (con $C'_\epsilon = \epsilon/16$). Para la primera digamos que $q > 3$ (en otro caso la constante se puede ajustar "a mano") y tomemos como $\widetilde{\chi}$ el único carácter no principal módulo 3, entonces $F(1-\epsilon/16) < 0$ porque si $0 < s < 1$ se tiene $\zeta(s) = (1-2^{1-s})^{-1}\sum(-1)^{n+1}n^{-s} < 0$ y $L(1,\chi), L(1,\widetilde{\chi}), L(1,\chi\widetilde{\chi}) > 0$ y estas funciones L no cambian de signo en $[1-\epsilon/16, 1]$ por hipótesis. El lema anterior asegura

$$-G\big(1-\epsilon/16\big) > Cq^{-\epsilon/2}$$

para cierta constante efectiva C. Con la estimación trivial $|\sum_{n\leq t}\chi(m)| \leq t - q[t/q]$ en (3.1) se deduce $L(1,\chi\widetilde{\chi}) \ll \log q$ y $L(1,\widetilde{\chi}) \ll 1$, y sustituyendo en la desigualdad anterior se sigue la primera parte del teorema ($q^{-\epsilon/2}\log q \gg q^{-\epsilon}$) con una constante efectiva.

Si $L(s,\widetilde{\chi})$ con $\widetilde{\chi}$ real y primitivo de módulo $\widetilde{q}$ tuviera un cero real $1-\epsilon/16 \leq \beta < 1$ entonces $F(\beta) = 0$ y copiando el argumento anterior, para $q > \widetilde{q}$

$$-G\big(\beta\big) > (C\widetilde{q}^{-\epsilon/2})q^{-\epsilon/2}.$$

Como $-G\big(1-\epsilon/16\big) > -G\big(\beta\big)$ todo el argumento se repite igualmente, salvo que ahora la constante $C\widetilde{q}^{-\epsilon/2}$ no es computable, ni la que hay que ajustar "a mano" si $q \leq \widetilde{q}$. □

Los ceros reales tienden a huir de los ceros reales, como se ha visto en la prueba anterior y en la propia demostración de la Proposición 3.2.8. Tanto es así que dentro de cada módulo sólo puede haber a lo más uno "malo".

Proposición 3.3.3 *Es posible escoger C en la Proposición 3.2.8 de forma que para cada $q$haya a lo más un carácter χ tal que $L(s,\chi)$ tiene un cero excepcional.*

Demostración: Supongamos que $L(s,\chi_1)$, $L(s,\chi_2)$ tuvieran ceros excepcionales β_1, β_2 con $\chi_1 \neq \chi_2$ caracteres reales no principales módulo q. Vamos a probar que existe una constante positiva K tal que

$$\text{mín}(\beta_1,\beta_2) < 1 - \frac{K}{\log q}, \tag{3.12}$$

lo que implica el resultado. Nos restringiremos al caso en que χ_1 y χ_2 son primitivos porque en otro caso al pasar a los caracteres primitivos χ_1^* y χ_2^* que los inducen, con los argumentos que siguen se llegaría a una desigualdad del tipo (?!) $\text{mín}(\beta_1,\beta_2) < 1 - 2K/\log(q_1^* q_2^*)$ que es más fuerte que (3.12).

Como en la Proposición 3.2.8, se tiene (ahora las partes reales son innecesarias)

$$-\frac{L'(\sigma,\chi_1\chi_2)}{L(\sigma,\chi_1\chi_2)} < C\log q^2 \qquad \text{y} \qquad -\frac{L'(\sigma,\chi_j)}{L(\sigma,\chi_j)} < C\log q - \frac{1}{\sigma-\beta_j}$$

con $j = 1, 2$ y $\sigma > 1$.

En el lema empleado para demostrar el Teorema de Siegel ya habíamos visto que $-F'/F$ es una serie de Dirichlet con coeficientes positivos. Tomemos en nuestro caso $\chi = \chi_1$, $\widetilde{\chi} = \chi_2$ y sustituyamos las cotas anteriores y $-\zeta'(\sigma)/\zeta(\sigma) < 1/(\sigma-1) + C$, entonces

$$\frac{1}{\sigma-1} - \frac{1}{\sigma-\beta_1} - \frac{1}{\sigma-\beta_2} + C\log q > 0.$$

Eligiendo $\sigma = 1 + K/(3\log q)$ con K pequeño se sigue que $\beta_1, \beta_2 \geq 1 - K/\log q$ es imposible, por tanto se cumple (3.12). □

El Teorema de Siegel y el hecho de que hay pocos ceros excepcionales permiten controlar uniformemente el término de error en el teorema de los números primos en progresiones aritméticas a pesar de que este control sea débil y la constante involucrada no efectiva.

Teorema 3.3.4 (de Siegel-Walfisz) *Dado $A > 0$*

$$\pi(x;q,a) = \frac{\text{Li}(x)}{\phi(q)} + O\left(\frac{x}{(\log x)^A}\right)$$

donde la constante O sólo depende de A (de manera no efectiva).

Demostración: Si $q \gg (\log x)^A$ el resultado es trivial porque $\pi(x;q,a) \ll x/q$ y $\phi(q) \gg q/\log q$. Supondremos por tanto $q \ll (\log x)^A$, bajo esta hipótesis el término de error en el Corolario 3.2.9 es $O(x/(\log x)^A)$. Por otro lado, eligiendo ϵ pequeño en el Teorema de Siegel para x suficientemente grande (uniformemente en $q \ll (\log x)^A$)

$$(1 - C_\epsilon q^{-\epsilon})\log x \leq \log x - A\log\log x$$

y $E(x)$ en el Corolario 3.2.9 es también $O(x/(\log x)^A)$ para $\chi \neq \chi_0$. Es decir, hemos probado

$$\psi(x,\chi) = O\left(\frac{x}{(\log x)^A}\right) \quad \text{si } \chi \neq \chi_0 \qquad \text{y} \qquad \psi(x,\chi_0) = x + O\left(\frac{x}{(\log x)^A}\right)$$

y la fórmula (3.4) conduce a $\psi(x;q,a) = x/\phi(q) + O(O(x/(\log x)^A)$ que sumando por partes da el resultado. □

3.4. El Teorema de Bombieri-Vinogradov

Enunciado y significado. Algunas aplicaciones.

Nuestro desconocimiento acerca de los ceros excepcionales y en general sobre la hipótesis de Riemann generalizada reduce bastante el poder del teorema de los números primos en progresiones aritméticas en las aplicaciones que lo requieren. Afortunadamente en ellas no suele aparecer una progresión aritmética particular sino algún tipo de suma sobre muchas de ellas, quizá con coeficientes aritméticos. Es ahí donde entran en juego diversos resultados en media cuando el módulo varía. Uno de los más poderosos[3] es el que da título a esta sección.

Teorema 3.4.1 (Teorema de Bombieri-Vinogradov) *Para cada $A > 0$ existen dos constantes positivas B y C tales que*

$$\sum_{q \leq Q} \max_{(a,q)=1} \left|\pi(x;q,a) - \frac{\mathrm{Li}(x)}{\phi(q)}\right| \leq C \frac{x}{(\log x)^A}$$

donde $Q = x^{1/2}/(\log x)^B$.

A grandes rasgos el teorema indica que si escogemos dentro de cada módulo la progresión aritmética que da lugar al mayor error, al sumar sobre los módulos en cierto rango el error medio está todavía bajo control.

Una interpretación optimista nos puede hacer ver este teorema como un sustituto de la hipótesis de Riemann generalizada, ya que el Corolario 3.2.7 concuerda con el teorema salvo que las potencias ϵ se transmutan en logaritmos.

Una visión pesimista, no del todo justa, nos muestra que para módulos grandes, digamos $Q/2 < q \leq Q$, después de la desigualdad de Brun-Titchmarsh el control que ofrece el teorema apenas arranca una potencia de logaritmo a la estimación trivial (esto no le resta poder al teorema para módulos moderadamente grandes).

Es fácil vender un teorema dándole nombre propio (en este caso dos) y mostrándolo como parejo a la inalcanzable hipótesis de Riemann generalizada, lo cual está bien habida cuenta que las Matemáticas tienen algo de arte, pero también tienen algo de ciencia positiva donde impera la dictadura de los hechos. Así surge la pregunta natural: ¿Cuáles son esas aplicaciones en las que se reclama la presencia del teorema de Bombieri-Vinogradov? Nos centraremos aquí en una que tiene interés histórico (estuvo en el origen de su creación) y que enlaza con el material del capítulo anterior.

Todos conocemos la conjetura de Goldbach, *todo número par mayor que dos es suma de dos primos*, que constituye todavía un problema abierto. digamos que $2N$ es el número par genérico y $r(2N)$ su número de representaciones como suma de dos primos. Por

[3]En realidad hay otra versión algo más fuerte del teorema de Bombieri-Vinogradov añadiendo un nuevo máximo (véase [Da]).

argumentos basados en el método del círculo (o más elementales) se conjetura para N grande un resultado mucho más preciso que el mero $r(2N) > 0$ postulado por Goldbach

$$r(2N) \sim \mathfrak{G}(N)\frac{N}{(\log N)^2} \qquad \text{donde} \qquad \mathfrak{G}(N) = 2\prod_{p\not| 2N}\frac{p(p-2)}{(p-1)^2}\prod_{p|2N}\frac{p}{p-1}.$$

Los dos resultados siguientes están relacionados con esta conjetura y requieren el uso del Teorema de Bombieri-Vinogradov.

Teorema 3.4.2 *Se cumple*

$$r(2N) \leq (4+o(1))\mathfrak{G}(N)\frac{N}{(\log N)^2}.$$

Es decir, a esta cota superior sólo le sobra un factor cuatro. Con vistas a la prueba de la conjetura de Goldbach, evidentemente lo que se reclama es una cota inferior no trivial. Tal resultado se desconoce pero hay algo cercano cambiando un poco el enunciado.

Teorema 3.4.3 *Sea $r^*(2N)$ el número de representaciones de $2N$ como suma de un número primo y otro que a lo más tiene cuatro factores primos, entonces para N mayor que cierta constante (efectiva)*

$$r^*(2N) \geq 0'3\mathfrak{G}(N)\frac{N}{(\log N)^2}.$$

Observación: Empleando una variante del Teorema de Bombieri-Vinogradov y alguna idea novedosa en los métodos de criba, J.-R. Chen probó (véase [Ha-Ri]) que si $r^{**}(2N)$ es como $r^*(2N)$ pero permitiendo que el segundo sumando tenga a lo más dos factores primos, entonces

$$r^{**}(2N) \geq 0'335\mathfrak{G}(N)\frac{N}{(\log N)^2}$$

para N suficientemente grande. Éste es uno de los mayores avances en relación con la conjetura de Goldbach. Aunque no entraremos aquí en ello, con la forma original del Teorema de Bombieri-Vinogradov se puede probar algo similar permitiendo a lo más tres factores primos [He].

Las demostraciones de estos dos teoremas se apoyan en métodos de criba. El conjunto base que se considera es:

$$\mathcal{A} = \{2N - p \ : \ p \text{ es primo } \leq 2N\}.$$

Entonces $A_d = \pi(2N; d, 2N)$ y para $(d, 2N) = 1$ se cumple

$$A_d = X\frac{g(d)}{d} + r_d$$

con $X = \mathrm{Li}(2N)$, $g(d) = d/\phi(d)$ y $r_d = \pi(2N; d, 2N) - \mathrm{Li}(2N)/\phi(d)$. La igualdad se cumple para $(d, 2N) > 1$ con $g(d) = 0$ y $|r_d| \leq 1$ (los primos no tienen demasiados divisores). Las cotas individuales para el error en el teorema de los números primos son muy pobres como para sacar algo de provecho de un esquema de criba y es ahí donde entra el Teorema de Bombieri-Vinogradov.

Demostración del Teorema 3.4.2: Es muy fácil comprobar

$$r(2N) \leq S(\mathcal{A}, z) + z.$$

Empleando la criba de Selberg, Teorema 2.3.3, manipulando el "término principal" como en el Teorema 2.3.4 se tiene suponiendo $\kappa = 1$

$$\begin{aligned} \frac{X}{\sum_{d<z} h(d)} &= C\frac{X}{(\log z)^\kappa} + O\Big(\frac{X}{(\log z)^{\kappa+1}}\Big) \\ &= \frac{\mathrm{Li}(2N)}{\log z} \prod_{p\not| 2N} \big(1 - \frac{1}{p-1}\big)\big(1 - \frac{1}{p}\big)^{-1} \prod_{p|2N} \big(1 - \frac{1}{p}\big)^{-1} = \mathfrak{G}(N)\frac{\mathrm{Li}(2N)}{2\log z}. \end{aligned}$$

Si N tiene un número acotado de factores primos, la hipótesis $\kappa = 1$ está asegurada porque $\sum_{p<z} h(p)\log p = \log z + O(1)$ se sigue de la fórmula de Mertens ya que $h(p)$ es casis siempre $1/(p-2)$. En el caso general hay que quitar muy pocos sumandos y no afecta a la asintótica del término principal (??) con el rango de z que se maneja. Comprobarlo requeriría rehacer en este caso particular simplificaciones como las del Teorema 2.3.4 (véase [He]).

Eligiendo $z = N^{1/4}(\log N)^{-B/2}$ con B grande, como $\mathrm{Li}(x) = (1 + o(1))x/\log x$, se deduce

$$r(2N) \leq (4 + o(1))\mathfrak{G}(N)\frac{N}{(\log N)^2} + \sum_{d<z^2} 3^{\nu(d)}|r_d|$$

y basta demostrar que el sumatorio es $o(N/(\log N)^2)$ con esta elección de z. Por la desigualdad de Cauchy la suma está mayorada por

$$\Big(\sum_{d<z^2} \frac{9^{\nu(d)}}{d}\Big)^{1/2}\Big(\sum_{d<z^2} d|r_d|^2\Big)^{1/2} \ll (\log N)^9\Big(\sum_{d<z^2} |r_d|\Big)^{1/2} \sup_{d<z^2}(d|r_d|)$$

donde se ha acotado la primera suma como en (2.4) del capítulo anterior.

La definición de r_d asegura que para $(d, 2N) = 1$

$$|r_d| \leq \max_{(a,d)=1} \big|\pi(2N; d, a) - \frac{\mathrm{Li}(2N)}{\phi(d)}\big|$$

mientras que para $(d, 2N) > 1$, $|r_d| \leq 1$. En cualquier caso

$$d|r_d| \ll N$$

y por el Teorema de Bombieri-Vinogradov, para B suficientemente grande

$$\sum_{d<z^2} |r_d| \ll \frac{N}{(\log N)^{100}}.$$

Sustituyendo estas dos estimaciones, el término de error en la criba de Selberg está bajo control. □

Demostración del Teorema 3.4.3: Sean

$$D = \frac{N^{1/2}}{(\log N)^B} \qquad \text{y} \qquad z = D^{2\theta} \quad \text{con } 1/5 < \theta < 1/4.$$

Entonces $r^*(2N) \geq S(\mathcal{A}, z)$ para N suficientemente grande porque $z^5 > 2N$ y por tanto ningún elemento que sobreviva a la criba puede tener más de cuatro factores primos. El Teorema de Bombieri-Vinogradov asegura que las hipótesis requeridas sobre el error en el Teorema de Jurkat-Richert son satisfechas con la elección anterior de D y z. La cota inferior es:

$$r^*(2N) \geq \big(f(1/2\theta) + o(1)\big)\mathrm{Li}(2N) \prod_{\substack{p<N^\theta \\ p\not| 2N}} \big(1 - \frac{1}{p-1}\big).$$

Es fácil relacionar el producto con $\mathfrak{G}(N)$

$$\prod_{\substack{p<N^\theta \\ p\not| 2N}} (1 - \frac{1}{p-1}) \geq \prod_{\substack{p<2N \\ p\not| 2N}} \frac{p-2}{p-1} \geq \prod_{p\not| 2N} \frac{p(p-2)}{(p-1)^2} \prod_{\substack{p<2N \\ p\not| 2N}} \frac{p-2}{p} = \frac{1}{2}\mathfrak{G}(N) \prod_{p<2N} \frac{p-1}{p}.$$

Por el Lema 2.1.2

$$r^*(2N) \geq \big(f(1/2\theta) + o(1)\big)\mathfrak{G}(N)\frac{N}{e^\gamma(\log N)^2}.$$

En el rango empleado $f(s) = 2e^\gamma s^{-1}\log(s-1)$ y escogiendo θ algo mayor que $1/5$, por ejemplo $\theta = 0'201$ se consigue una constante válida. □

No daremos aquí la prueba del Teorema de Bombieri-Vinogradov. Inicialmente requería resultados de densidad (algo así como que si consideramos muchas funciones L la mayoría de los ceros están cerca de la línea crítica) pero actualmente se puede hacer sin referencia a este tipo de resultados, empleando desigualdades llamadas de *gran criba*. El nombre es confuso porque en apariencia no tienen nada que ver con la criba y adquirieron tal nombre por su participación al demostrar resultados como los anteriores. Se pueden ver una pruebas completa del Teorema de Bombieri-Vinogradov en [Da] §28 y si se quiere profundizar más en las desigualdades de gran criba y sus aplicaciones una buena referencia es [Iw-Ko] §7.

Para terminar la sección y el capítulo, reflexionemos acerca del término de error en el teorema de los números primos en progresiones aritméticas y su reflejo en resultados en media como el teorema de Bombieri-Vinogradov.

Bajo la hipótesis de Riemann generalizada, el Corolario 3.2.7 da un error $O(x^{1/2+\epsilon})$ que es óptimo para q fijado salvo quizá cambiar x^ϵ por una potencia de logaritmo porque hay ceros en la línea crítica. Sin embargo nada impediría que q nos "ayudase" cuando

es grande porque en ese caso hay menos primos que contar. La conjetura más optimista en este sentido, debida a H.L. Montgomery, es que para cualquier $\epsilon > 0$

$$\pi(x; q, a) = \frac{\mathrm{Li}(x)}{\phi(q)} + O(x^{1/2+\epsilon} q^{-1/2} + 1)$$

sea uniformemente válida en x y q. Obviamente para $q > x$ es trivial. Por otro lado J.B. Friedlander y A. Granville [Fr-Gr] probaron que $\pi(x; q, a) \sim \mathrm{Li}(x)/\phi(q)$ no puede ser cierto para q tan grande como $x/(\log x)^A$, lo cual implica que el rango de validez $q \leq x^{1-\epsilon}$ que da la conjetura anterior para el teorema de los números primos en progresiones aritméticas, es bastante crítico.

Soñar es gratuito pero si no ha habido ningún avance que haya abierto un posible camino hacia la hipótesis de Riemann generalizada, ¿no es ilusorio trabajar sobre conjeturas mucho más fuertes? La experiencia es que muchas de nuestras esperanzas se reflejan en resultados en media (y a decir verdad, tienen su origen en ellos), por tanto quizá en aplicaciones como las anteriores que requieren módulos que varían no es un delirio onírico esperar más que lo que nos ofrece la hipótesis de Riemann generalizada. Un resultado (probado) en esta dirección es el Teorema de Barban-Davenport-Halberstam [Da] §29 que afirma que para cada $A > 0$ existen $B, C > 0$ tales que

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right|^2 \leq C \frac{x}{(\log x)^A}$$

con $Q = x/(\log x)^B$. Nótese que esto es mucho mejor que lo que se derivaría a través del Corolario 3.2.7 de la hipótesis de Riemann generalizada. La pregunta natural es si podemos suprimir el sumatorio interior sin grandes reducciones en el tamaño de Q, más concretamente, si el Teorema de Bombieri-Vinogradov es válido con $Q = x^{1-\epsilon}$. Esto es un problema abierto (una respuesta afirmativa por ejemplo reduciría automáticamente la constante del Teorema 3.4.2 a la mitad). Todavía más, todavía nadie ha llegado a $Q = X^{1/2+\delta}$ para algún $\delta > 0$. El único avance desde que Bombieri y A.I. Vinogradov crearan su teorema ha sido pasar de $Q = x^{1/2}/(\log x)^B$ a $Q = x^{1/2} e^{\log x/(\log\log x)^B}$ [Bo-Fr-Iw], lo cual, a pesar de su profundidad, no parece tener grandes repercusiones.

Bibliografía

[Bo-Fr-Iw] E. Bombieri, J.B. Friedlander, H. Iwaniec. Primes in arithmetic progressions to large moduli. II. Math. Ann. 277 (1987), no. 3, 361–393.

[Da] H. Davenport. Multiplicative number theory (2nd ed.). Graduate texts in Mathematics 74. Springer-Verlag, New York-Berlin, 1980.

[El] W.J. Ellison. Les nombres premiers. En collaboration avec Michel Mendès France. Publications de l'Institut de Mathématique de l'Université de Nancago, No. IX. Actualités Scientifiques et Industrielles, No. 1366. Hermann, Paris, 1975.

[Fr-Gr] J.B. Friedlander, A. Granville. Limitations to the equi-distribution of primes. III. Compositio Math. 81 (1992), no. 1, 19–32.

[Ga] C.F. Gauss. Disquisitiones arithmeticae. Springer-Verlag, New York, 1986.

[Go] D.M. Goldfeld. A simple proof of Siegel's theorem. Proc. Nat. Acad. Sci. U.S.A. 71 (1974), 1055.

[Ha-Ri] H. Halberstam, H.-E. Richert. Sieve methods. London Mathematical Society Monographs, No. 4. Academic Press, London-New York, 1974.

[He] D.R. Heath-Brown. Lectures on sieves. Proceedings of the Session in Analytic Number Theory and Diophantine Equations, Bonner Math. Schriften, 360, Univ. Bonn, Bonn, 2003.

[Hu] L.-K. Hua. Introduction to number theory. Springer-Verlag, Berlin-New York, 1982.

[Iw-Ko] H. Iwaniec, E. Kowalski. Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[Ne] D.J. Newman. Analytic number theory. Graduate Texts in Mathematics, 177. Springer-Verlag, New York, 1998.

[Se] A. Selberg. Collected papers. Vol. I. Springer-Verlag, Berlin, 1989.

[St] J. Steuding. `http://www.uam.es/jorn.steuding/files/seminario0.pdf`