2.3. Primos en progresiones aritméticas

Teorema de Dirichlet. Un ejemplo. Caracteres de Dirichlet. Relaciones de ortogonalidad. Funciones L.

Desde Euclides sabemos que hay infinitos primos. Cabe preguntarse si la abundancia de primos se conserva cuando nos restringimos a ciertos subconjuntos de $\mathbb{Z}^+$. En relación con esto, se conjetura que si $P \in \mathbb{Z}[x]$ es irreducible entonces $\{P(n) : n \in \mathbb{Z}^+\}$ contiene infinitos primos excepto en los casos triviales en que lo prohíben las condiciones de congruencia o de signo (por ejemplo, $n^2 + n + 2$ es siempre par o $-n^3 + 2023$ es a la larga negativo). Esta conjetura, solo está probada para polinomios de grado 1. El mayor avance en el caso de grado dos es un conocido resultado de Iwaniec [24] que afirma que, eliminando los casos triviales, un polinomio cuadrático alcanza infinitas veces valores con a lo más dos factores primos. Nadie sabe cómo separar los primos de los que tienen dos factores primos en ningún caso. Por ejemplo, es un antiguo problema abierto saber si hay infinitos primos de la forma $n^2 + 1$.

El caso de grado 1 está recogido en el siguiente resultado al que dedicaremos toda la sección. Según algunos autores, la teoría analítica de números nació cuando P.G.L. Dirichlet lo demostró. Gran parte de la idea es buscar una modificación de la sencilla prueba analítica de Euler de la infinitud de los primos.

▶ **Teorema 2.3.1** (Teorema de Dirichlet)**.** *Dados $a \in \mathbb{Z}$ y $q \in \mathbb{Z}^+$ coprimos, hay infinitos primos en la progresión aritmética $\{qn + a\}_{n=1}^{\infty}$.*

Evidentemente, $\gcd(a, q)$ divide a $qn + a$ por tanto la condición de que sean coprimos es necesaria.

Para ilustrar las ideas principales involucradas en la demostración, veremos primero un caso particular:

Proposición 2.3.2. *Hay infinitos primos que acaban en 1, es decir, que cumplen $p \equiv 1$ (10).*

Una ligera modificación de la prueba permite obtener que, en general, hay infinitos primos que acaban en cualquier cifra impar distinta de 5.

Para empezar, es tentador escribir un análogo de (2.2) con la serie $\sum(10n + 1)^{-s}$ en lugar de $\zeta(s)$ pero tal cosa no funciona porque aunque un número entero acabe en 1, sus factores primos pueden no hacerlo, por ejemplo $221 = 13 \cdot 17$. Para forzar un producto de Euler necesitamos introducir funciones multiplicativas que capturen la condición de congruencia y cuya serie de Dirichlet sea razonable.

Demostración. Sabemos que $10 = 2 \cdot 5$ tiene raíces primitivas, por la Proposición 1.2.10, de hecho $g = 3$ es una de ellas. Esto significa que obtenemos cada una de las $\varphi(10) = 4$ clases de $(\mathbb{Z}/10\mathbb{Z})^*$, concretamente,

$$g^0 \equiv 1 \ (10), \qquad g^1 \equiv 3 \ (10), \qquad g^3 \equiv 7 \ (10), \qquad g^2 \equiv 9 \ (10).$$

llamemos $f : (\mathbb{Z}/10\mathbb{Z})^* \longrightarrow \mathbb{Z}/4\mathbb{Z}$ a la función que a cada una de estas clases le asigna su exponente, es decir, $g^{f(n)} \equiv n \ (10)$ para $\gcd(n, 10) = 1$ donde, como siempre, identificamos enteros y sus clases. Introduzcamos las series de Dirichlet L_0, L_1, L_2 y L_3 dadas por

$$L_j(s) = \sum_{n=1}^{\infty} \frac{\chi_j(n)}{n^s} \qquad \text{con} \qquad \chi_j(n) = \begin{cases} e^{2\pi i j f(n)/4} & \text{si } \gcd(n, 10) = 1, \\ 0 & \text{si } \gcd(n, 10) \neq 1. \end{cases}$$

Hay dos hechos fundamentales y sencillos acerca de las funciones χ_j. El primero es que son completamente multiplicativas, lo que se sigue fácilmente de $g^{f(n)+f(m)} \equiv nm \equiv g^{f(nm)}$. El segundo es que

$$\chi_0(n) + \chi_1(n) + \chi_2(n) + \chi_3(n) = \begin{cases} 4 & \text{si } n \equiv 1 \ (10), \\ 0 & \text{si } n \not\equiv 1 \ (10). \end{cases} \tag{2.9}$$

Si $\gcd(n, 10) \neq 1$ es trivial y si $\gcd(n, 10) = 1$ lo único que estamos diciendo es que $\sum_{j=0}^{3} \xi^j = 0$ si ξ es una raíz cuarta o cuadrada de la unidad excepto para $\xi = 1$.

Recordando el comentario que sigue a (2.3), por ser χ_j completamente multiplicativa, L_j admite un producto de Euler de la forma

$$L_j(s) = \prod_p \big(1 - \chi_j(p)p^{-s}\big)^{-1}.$$

Para $|z| < 1/2$ se tiene $\log(1-z) = z + O(z^2)$, por Taylor. Así pues, teniendo en cuenta (2.9), para $s > 1$ real obtenemos

$$\sum_{j=0}^{3} \log L_j(s) = \sum_{p \equiv 1 \ (10)} \frac{4}{p^s} + O(1). \tag{2.10}$$

Como $\chi_0(n) = 1$ si n y 10 son coprimos y 0 en el resto,

$$\lim_{s \to 1^+} L_0(s) \geq \lim_{s \to 1^+} \sum_{k=0}^{\infty} \frac{1}{(10k+1)^s} = \infty. \tag{2.11}$$

Por otro lado, tomando 10 términos en las sumas que definen $L_2(s)$ y $L_1(s) = \overline{L_3(s)}$, se tiene

$$L_2(1) = 0{,}63 + \epsilon_1 \qquad \text{y} \qquad \Re\big(L_3(1)\big) = 0{,}88 + \epsilon_2$$

con $|\epsilon_1|, |\epsilon_2| < 1/10$. Esta cota proviene de que las series son alternadas, con una pequeña trasposición de sus términos, y el error es menor que el primer término despreciado [47, p.600]. Por tanto $L_1(1)L_2(1)L_3(1)$ es un número real positivo y, teniendo en cuenta (2.11), de (2.10) con $s \to 1^+$ se deduce que hay infinitos primos que acaban en 1, de hecho que la suma de sus inversos diverge.

Un comentario final es que la prueba sería similar para otra cifra admisible k, es decir, $\gcd(k, 10) = 1$, considerando en (2.10) $\sum_j \overline{\chi_j(k)} L_j(s)$. □

El primer paso para extender la prueba de la Proposición 2.3.2 de cara a demostrar el Teorema 2.3.1 es generalizar las funciones χ_j. Dado un grupo abeliano finito G, un *carácter* χ es un homomorfismo $\chi : G \longrightarrow \{|z| = 1\}$. El caso más representativo es $G = C_N$, el grupo cíclico de N elementos. Si identificamos sus elementos con clases de congruencia módulo N, un carácter queda condicionado por el valor que toma en 1, que debe ser una raíz N-ésima de la unidad. Es, entonces, fácil ver que hay exactamente N caracteres χ_k, $0 \leq k < N$, dados por $\chi_k(n) = e^{2\pi i k n/N}$. El primero, χ_0, es trivial y se cumplen las relaciones

$$\sum_{k=0}^{N-1} \chi_k(a) = \begin{cases} N & \text{si } N|a, \\ 0 & \text{si } N \nmid a, \end{cases} \qquad \sum_{a=0}^{N-1} \chi_k(a) = \begin{cases} N & \text{si } k = 0, \\ 0 & \text{si } k \neq 0, \end{cases}$$

donde en la primera relación fijamos a y en la segunda fijamos k.

Si G no fuera cíclico, por ejemplo $G = C_N \times C_M$, los elementos del grupo son (n, m) y los caracteres $\chi_{k_1}(n)\chi_{k_2}(m)$ con lo cual habría NM de ellos y si los numeramos $X_0, \ldots, X_{NM-1}$ se siguen cumpliendo las relaciones anteriores. Inductivamente, así construirímos los caracteres de cualquier G abeliano finito y veríamos que hay $|G|$ de ellos y que se cumplen las fórmulas anteriores con $N = |G|$.

Apliquemos esto al grupo $(\mathbb{Z}/q\mathbb{Z})^*$ con $q \in \mathbb{Z}_{\geq 2}$ y extendamos la definición al anillo $\mathbb{Z}/q\mathbb{Z}$ asignando $\chi(n) = 0$ si $\gcd(n, q) \neq 1$, esto es, si n no es invertible. El resultado no es estrictamente un carácter en el sentido de la teoría de grupos (porque $\mathbb{Z}/q\mathbb{Z}$ no es un grupo con el producto), pero se llama a estos objetos *caracteres de Dirichlet* módulo q. Como solo añadimos ceros a la definición, las relaciones anteriores se deben cumplir con $N = |(\mathbb{Z}/q\mathbb{Z})^*| = \varphi(q)$. Es decir,

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi(q) & \text{si } a \equiv 1 \ (q), \\ 0 & \text{si } a \not\equiv 1 \ (q), \end{cases} \qquad \sum_{a=1}^{q} \chi(a) = \begin{cases} \varphi(q) & \text{si } \chi = \chi_0, \\ 0 & \text{si } \chi \neq \chi_0. \end{cases} \tag{2.12}$$

Estas fórmulas se conocen como *relaciones de ortogonalidad*. En la primera, el cambio de $N \mid a$ a $a \equiv 1 \ (q)$, se debe al cambio de la operación aditiva por la multiplicativa. El elemento neutro en C_N es 0 con la suma y 1 lo es

en $(\mathbb{Z}/q\mathbb{Z})^*$ con el producto. Aquí $\chi_0(n) = 1$ si $\gcd(n,q) = 1$ y $\chi_0(n) = 0$ si $\gcd(n,q) \neq 1$ es lo que se llama el *carácter principal*, aunque parecería más acertado llamarle carácter trivial. Seguramente la notación procede de que suele estar asociado a las mayores contribuciones.

Si recordamos lo que era un homomorfismo, otra forma de ver los caracteres de Dirichlet es como funciones completamente multiplicativas de periodo q tales que se anulan en lo valores no coprimos con q.

Se puede dar una construcción explícita de ellos en términos de raíces primitivas. Solo lo haremos para $q > 2$ primo porque el resto de los casos, sobre todo si hay potencias de dos, se complica. Si g es una raíz primitiva módulo q, entonces los caracteres son $\chi_k(n) = e^{2\pi i k\ell/(q-1)}$ para $n \equiv g^\ell \ (q)$ completando la definición con $\chi_k(n) = 0$ si $q \mid n$. En términos de grupos, lo que ocurre es que $\ell \mapsto g^\ell$ induce un isomorfismo $(\mathbb{Z}/(q-1)\mathbb{Z}, +) \cong (\mathbb{Z}/q\mathbb{Z})^*$.

A cada carácter de Dirichlet χ se le asigna su serie de Dirichlet $L(s,\chi)$, que es la generalización de las $L_j(s)$ y tiene un producto de Euler similar,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad L(s,\chi) = \prod_p \big(1 - \chi(p)p^{-s}\big)^{-1}.$$

A diferencia de lo que ocurre con la función ζ, para $\chi \neq \chi_0$ la serie de Dirichlet $L(s,\chi)$ converge en $\Re(s) > 0$. La prueba consiste en escribir la suma como

$$\Big(\frac{1}{1^s} - \frac{1}{2^s}\Big)\chi(1) + \Big(\frac{1}{2^s} - \frac{1}{3^s}\Big)\big(\chi(1)+\chi(2)\big) + \Big(\frac{1}{3^s} - \frac{1}{4^s}\Big)\big(\chi(1)+\chi(2)+\chi(3)\big) + \dots$$

y notar que $\sum_{n=1}^{N} \chi(n)$ está acotada porque, según (2.12), da cero cuando N es un múltiplo de q. La convergencia se sigue de la de $\sum \big|n^{-s} - (n+1)^{-s}\big|$, que está asegurada en $\Re(s) > 0$ porque los sumandos son $O\big(|s|n^{-Re(s)-1}\big)$. La holomorfía de $L(s,\chi)$ en esta región de convergencia es consecuencia del teorema de Morera.

Una vez que tenemos definidas las funciones $L(s,\chi)$, el principal problema para adaptar la prueba de la Proposición 2.3.2 y obtener el Teorema 2.3.1 es que las aproximaciones numéricas que hicimos de $L_j(1)$ tomando unos pocos términos no está claro que tengan una analogía. Lo fundamental es que $L(1,\chi)$ no se anule cuando $\chi \neq \chi_0$ para que no haya una cancelación de infinitos en el análogo de (2.10). En cierto modo, el Teorema 2.3.6 es "fácil" a no ser que ocurra la casualidad de que una función L se anule en $s = 1$. Esa casualidad parece demasiado rara, sin embargo probar que no ocurre es una parte fundamental de la prueba y lo que originariamente llevó más esfuerzo a Dirichlet para probar su teorema. El problema de ir más allá de la no anulación dando cotas inferiores adecuadas en $s = 1$ es uno de los más importantes en teoría analítica de números. En suma, el siguiente resultado

es un lema para obtener el Teorema 2.3.6, pero dada su relevancia es justo elevar su categoría.

Teorema 2.3.3. *Para cualquier carácter $\chi \neq \chi_0$ se tiene $L(1,\chi) \neq 0$.*

También usaremos dos resultados auxiliares de menos entidad:

Lema 2.3.4. *Para $\Re(s) > 1$ y χ un carácter de Dirichlet se cumple*

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

Lema 2.3.5 (Lema de Landau)**.** *Sea f una función aritmética no negativa y supongamos que $\sigma_c = \inf\{\sigma \in \mathbb{R} : D_f(\sigma) \text{ converge}\}$ no es $\pm\infty$, entonces $D_f(s)$ no admite una extensión holomorfa en un entorno de σ_c.*

Esto suena bastante lógico: si la serie de Dirichlet deja de converger es que hay algún tipo de singularidad. No obstante, no es obvio y sería falso si se permitiera que f tomase valores positivos y negativos. A σ_c se le llama *abcisa de convergencia*.

Vamos a deducir el Teorema de Dirichlet de un resultado más fuerte:

Teorema 2.3.6. *Dados $a \in \mathbb{Z}$ y $q \in \mathbb{Z}^+$ coprimos, se cumple*

$$\sum_{\substack{n=1 \\ n\equiv a \ (q)}}^{\infty} \frac{\Lambda(n)}{n^s} \sim \frac{1}{\varphi(q)(s-1)} \qquad \textit{para} \quad s \to 1^+.$$

Dando por supuestos los resultados auxiliares anteriores la prueba es breve.

Demostración. Por las relaciones de ortogonalidad (2.12) y el Lema 2.3.4, el sumatorio del enunciado es

$$\frac{1}{\varphi(q)} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \sum_{\chi} \overline{\chi}(a)\chi(n) = -\frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\frac{L'(s,\chi)}{L(s,\chi)} \tag{2.13}$$

Sabemos que $L(s,\chi_0)$ tiene un polo de orden 1 en $s = 1$, por tanto se cumple $-L'(s,\chi)/L(s,\chi) \sim (s-1)^{-1}$ si $\chi = \chi_0$ mientras que para $\chi \neq \chi_0$ no hay singularidad ya que $L(s,\chi)$ es holomorfa en $\Re(s) > 0$ y $L(1,\chi) \neq 0$, por el Teorema 2.3.3. □

La deducción del Teorema de Dirichlet a partir del Teorema 2.3.6 no es totalmente inmediata pero sí rutinaria.

Demostración del Teorema 2.3.1. Para $s > 1$ real

$$0 \leq \sum_{\substack{n=1 \\ n\equiv a \ (q)}}^{\infty} \frac{\Lambda(n)}{n^s} - \sum_{p\equiv a \ (q)}^{\infty} \frac{\log p}{p^s} \leq \sum_{k=2}^{\infty}\sum_{p} \frac{\log p}{p^k} \leq \sum_{n=2}^{\infty} \frac{\log n}{n^2(1-1/n)}$$

donde en el último paso se han reemplazado primero los primos por los elementos de $\mathbb{Z}_{\geq 2}$ (que son más) y después se ha sumado en k. La última serie converge y por el Teorema 2.3.6 la suma de de $p^{-s}\log p$ sobre $p \equiv a \ (p)$ debe tender a infinito cuando $s \to 1^+$. □

Solo resta probar los resultados auxiliares que habíamos dejado atrás.

Demostración del Lema 2.3.4. Sea $f(n) = \chi(n)\Lambda(n)$. Se tiene

$$(\chi * f)(n) = \sum_{d|n} \chi(d)\Lambda(n)\chi(n/d) = \chi(n)\sum_{d|n}\Lambda(n) = \chi(n)\log n,$$

donde se ha usado (2.7). Por la Proposición 2.1.2, $D_{\chi\log}(s) = D_{\chi\Lambda}(s)L(s,\chi)$ y se deduce el resultado. □

Demostración del Lema 2.3.5. Sin pérdida de generalidad se puede suponer $\sigma_c = 0$ porque siempre es posible redefinir $f(n)$ como $g(n)n^{\sigma_c}$.

Si $\sum f(n)/n^s$ converge para $s = \sigma$, también lo hace para $s = \sigma + it$ (por convergencia absoluta), así pues la convergencia de $D_f(s)$ está asegurada en $\Re(s) > 0$ y lo hace a una función holomorfa por el teorema de Morera. Procedemos por reducción al absurdo. Si existiera una extensión holomorfa en un entorno del origen, tendríamos, para algún $\epsilon > 0$, una F holomorfa definida en el círculo $|s-1| < 1+\epsilon$ que coincide con $D_f(s)$ en la parte con $\Re(s) > 0$. Un resultado básico de variable compleja afirma que las funciones holomorfas son analíticas, esto es, iguales a su desarrollo de Taylor. Si hacemos tal desarrollo en $s = 1$ y lo evaluamos en $\sigma \in (-\epsilon, 0]$ se sigue que las series

$$\sum_{k=0}^{\infty} \frac{F^{(k)}(1)}{k!}(\sigma-1)^k = \sum_{k=0}^{\infty} \frac{D_f^{(k)}(1)}{k!}(\sigma-1)^k = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{f(n)(\log n)^k}{k!n}(1-\sigma)^k$$

convergen a $F(\sigma)$. Al ser la serie doble de términos positivos, no hay problema en intercambiar el orden de sumación (por el teorema de Fubini para series) y obtener que también converge

$$\sum_{n=1}^{\infty} \frac{f(n)}{n}\sum_{k=0}^{\infty} \frac{(\log n)^k}{k!}(1-\sigma)^k = \sum_{n=1}^{\infty} \frac{f(n)}{n}e^{(1-\sigma)\log n} = \sum_{n=1}^{\infty} \frac{f(n)}{n^\sigma}.$$

La convergencia de esta última serie contradice $\sigma_c = 0$ porque σ es arbitrario en $(-\epsilon, 0]$. □

Demostración del Teorema 2.3.3. Por las relaciones de ortogonalidad, o tomando $a = 1$ en (2.13),

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

Sabemos que el término $\chi = \chi_0$ en la suma es $-(s-1)^{-1}$. Si $L(1,\chi) = 0$ para $\chi \neq \chi_0$ se tiene $L(s,\chi) \sim K(s-1)^k$ con $K \neq 0$, $k \in \mathbb{Z}^+$, por tanto $L'(s,\chi)/L(s,\chi) \sim k(s-1)^{-1}$. Como el sumatorio del segundo miembro es no negativo para $s > 1$, no puede haber dos caracteres con $L(1,\chi) = 0$ ni uno con multiplicidad de cero mayor que 1, ya que eso haría que el sumatorio del primer miembro fuera positivo cuando $s \to 1^+$. Esto excluye a todos los caracteres complejos, ya que $L(1,\chi) = 0$ implica $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$.

Si $\chi \neq \chi_0$ es real, para cada n se tiene $\chi(n) \in \{0, 1, -1\}$, porque $\chi(n)$ es cero o una raíz de la unidad. Sea $c = 1 * \chi$. Un cálculo sencillo muestra que $c(p^\alpha) \geq 1$ si α es par y $c(p^\alpha) \geq 0$ si α es impar. Por la Proposición 2.1.2, sabemos

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

La abcisa de convergencia de esta última serie de Dirichlet cumple $\sigma_c \geq 1/2$ porque $\sum_{n=1}^{\infty} c(n)/n^{1/2} \geq \sum_{k=1}^{\infty} c(k^2)/k \geq \sum_{k=1}^{\infty} 1/k$ que diverge. Si $L(1,\chi) = 0$, el primer término no tendría singularidades en $\Re(s) > 0$ y esto contradice el Lema 2.3.5. □

Para el lector ávido de más teoría analítica de números, uno de los clásicos modernos es [11]. Debido a su concisión hay que leerlo con bastante detenimiento. No obstante, es muy recomendable. Más reciente y con una visión más amplia es [27]. El libro [38] contiene una interesante colección de problemas. Dentro de la bibliografía en español, una referencia destacable (difícil de encontrar fuera de las bibliotecas locales) es [5].