1. El teorema de los números primos

1.1. Un poco de historia

Hay veces que por una extraña y armónica conjunción de la sencillez, la belleza y la relevancia, una fórmula simple sostiene los cimientos de una compleja teoría. Esto es lo que ocurre en el estudio de la distribución de los primos con la *identidad de Euler*

$$\boxed{\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}}$$

donde $s > 1$ y p recorre los primos. La demostración se reduce al teorema fundamental de la aritmética (descomposición única en primos) después de notar que el segundo miembro es $\prod(1 + p^{-s} + p^{-2s} + p^{-3s} + \ldots)$.

Esta sencilla fórmula es muy importante porque relaciona los números naturales, que conocemos bien, con los número primos, que conforman una sucesión muy caótica. Euler utilizó su identidad para probar la infinitud de los primos notando que el primer miembro diverge cuando $s \to 1^+$. Lo bueno de esta prueba frente a la usual, es que admite cierta cuantificación del crecimiento de los primos. Por ejemplo, si alguien afirmase que a partir de cierto número gigantesco hay siempre a lo más un número primo entre cada par de cuadrados consecutivos, podríamos ver la falsedad de tal afirmación deduciendo de la identidad de Euler

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \text{cte} \prod_{k=1}^{\infty} \left(1 - \frac{1}{k^2}\right)^{-1}.$$

Lo cual lleva a una contradicción cuando $s \to 1^+$ porque $\prod(1 - k^{-2})^{-1} < \infty$.

Una cuestión básica en el estudio de la distribución de los primos es la densidad que tienen en los naturales. Se puede probar por métodos elementales, pero ingeniosos, que $\pi(x) = o(x)$ donde

$$\pi(x) = \sum_{p \leq x} 1 = |\{p \leq x \,:\, p \text{ es primo}\}|.$$

Así pues la densidad tiende a cero. La pregunta natural es si se puede afinar más. Gauss conjeturó (de manera un poco imprecisa, basándose en resultados numéricos) el *teorema de los números primos*, afirmando que

$$\pi(x) \sim Li(x) \qquad \text{con} \quad Li(x) = \int_2^x \frac{dt}{\log t}.$$

De los trabajos de Chebychev en 1849/50 (véase [**Sm**]) se deduce que $C_1 Li(x) < \pi(x) < C_2 Li(x)$ para ciertas constantes C_1 y C_2. Chebychev controló con precisión suficiente estas constantes (en realidad para $x/\log x$ en lugar de $Li(x)$) para probar el *postulado de Bertrand* (entre un número natural y su doble siempre hay un primo).

La gran obra maestra en la distribución de los primos es la brevísima memoria que escribió Riemann en 1860 (hay una traducción en [**Ed**]). En ella utilizó técnicas de Variable Compleja para despejar $\pi(x)$ a partir de la identidad de Euler en términos de una extensión compleja del primer miembro. Con ello obtuvo una fórmula para $\pi(x)$ cuyo primer término era $Li(x)$.

Por poco exigente que uno sea con el rigor, no se puede decir que Riemann probase el teorema de los números primos porque en su memoria enuncia varias propiedades que no demuestra (véase [**Da**] §3), e incluso no está nada claro que en su fórmula para $\pi(x)$ el término $Li(x)$ domine sobre el resto, ni siquiera está claro que tenga sentido por algunos problemas de convergencia.

A pesar de su insuficiencia, la memoria de Riemann marcó el camino para demostrar el teorema de los números primos y fue la clave para que treinta y seis años después, en 1896, de la Vallée Poussin y Hadamard consiguieran independientemente una demostración completa. Es históricamente poco correcto decir que estas pruebas fueran consecuencia necesaria del desarrollo de la Variable Compleja. Más bien al contrario, parte de la Variable Compleja se desarrolló más rápido gracias a la búsqueda de una prueba del teorema de los números primos.

En 1949 Selberg [**Se**] y Erdős sorprendieron al colectivo matemático encontrando una demostración "elemental" (pero no sencilla) del teorema de los números primos. También hay pruebas que están más cerca del Análisis Real que del Complejo [**Dy-Mc**], sin embargo, desde Riemann está claro que si uno quiere estudiar el error en el teorema de los números primos, $\pi(x) - Li(x)$, necesariamente debe enfrentarse a los misteriosos ceros de cierta función compleja. El resultado óptimo se obtendría resolviendo la *hipótesis de Riemann*, la cual sigue sin probarse a pesar del empeño dedicado a ello durante más de 140 años.

1.2. Diversas formas del teorema de los números primos

Es fácil comprobar (por L'Hopital) que el *logaritmo integral*, $Li(x)$, satisface $Li(x) \sim x/\log x$, por lo cual el teorema de los números primos aparece en la mayoría de los textos enunciado como $\pi(x) \sim x/\log x$. Sin embargo hay razones teóricas para escribir $Li(x)$ ya que en cierto sentido da la mejor aproximación posible y se sabe positivamente que aproxima mejor que $x/\log x$. El que confíe más en los datos que en la teoría puede

observar la siguiente tabla:

	$\pi(x)/Li(x)$	$\pi(x)/(x/\log x)$
$x = 10^4$	$0'986$	$1'132$
$x = 10^6$	$0'9983$	$1'084$
$x = 10^8$	$0'99987$	$1'061$
$x = 10^{10}$	$0'9999932$	$1'048$

Es evidente que la aproximación de $\pi(x)$ por $x/\log x$ es muy pobre.

La pregunta ingenua de cuál es el n-ésimo primo p_n sugiere encontrar aproximaciones no sólo para $\pi(x)$ sino también para p_n. De todos modos, por razones técnicas el teorema de los números primos no se suele probar usando directamente $\pi(x)$ o p_n sino a través de una función bastante antinatural introducida por Chebychev y definida como

$$\psi(x) = \sum_{n \le x} \Lambda(n) \qquad \text{con} \quad \Lambda(n) = \begin{cases} \log p & \text{si } n = p^k,\ p \text{ primo } k \in \mathbb{Z}^+ \\ 0 & \text{en otro caso} \end{cases}$$

La relación entre estas funciones y las diferentes formas del teorema de los números primos están contenidas en el enunciado y la prueba del siguiente resultado:

Lema 1.1 . *Las siguiente afirmaciones son equivalentes*

a) $\pi(x) \sim Li(x)$, *b)* $\pi(x) \sim x/\log x$, *c)* $p_n \sim n \log n$, *d)* $\psi(x) \sim x$.

DEM.: Ya hemos mencionado que *a)* $\Leftrightarrow$ *b)*. Claramente $\pi(p_n) = n$, así pues *b)* implica $p_n/\log p_n \sim n$ y tomando logaritmos $\log p_n \sim n$. Multiplicando estas relaciones se obtiene *c)*. El recíproco se prueba en las mismas líneas: $p_n \le x < p_{n+1}$, *c)* $\Rightarrow p_n \sim x$.

Es fácil ver que $\pi(x) = \sum_{n \le x} \Lambda(n)/\log n + O(x^{1/2}\log x)$. De hecho con un poco de esfuerzo se puede reducir el error a $O(x^{1/2})$. Del Lema de Abel se deduce por tanto $\pi(x) = \psi(x)/\log x + \int_2^x (\psi(t) - t)/(t \log^2 t)\, dt + O(x^{1/2})$, o equivalentemente

$$\pi(x) = Li(x) + \frac{\psi(x) - x}{\log x} + \int_2^x \frac{\psi(t) - t}{t \log^2 t}\, dt + O(x^{1/2}) \tag{1.1}$$

que inmediatamente prueba *d)* $\Rightarrow$ *a)*. Si se parte de $\psi(x) = \sum_{n \le x} (\pi(n) - \pi(n-1)) \log n + O(x^{1/2}\log^2 x)$, un argumento similar prueba *b)* $\Rightarrow$ *d)*. ■

La fórmula (1.1) muestra la relevancia del logaritmo integral si partimos de buenas estimaciones de $\psi(x) - x$. Concretamente, si $\psi(x) = x + O(E(x))$ para cierta E creciente, entonces $\pi(x) = Li(x) + O(E(x)/\log x)$. Si, como probaremos, $E(x) = o(x/\log x)$ entonces

la fórmula $Li(x) - x/\log x \sim x/\log^2 x$ implica $\pi(x) - x/\log x \sim x/\log^2 x$, lo que explica la pobreza de la aproximación $x/\log x$. Este razonamiento es en cierta manera condicional, porque no está claro que $\psi(x)$ sea la función natural a considerar y $\psi(x) - x$ el error a estimar. La razón última es la estrecha relación entre $\sum n^{-s}$ y $\psi(x)$.

1.3. Un ejemplo de Cálculo I que se complica

En esta sección vamos a comenzar divagando a través de un problema aparentemente de Cálculo I, para después mostrar por analogía algunos pasos fundamentales en la demostración del teorema de los números primos. Puede que sea un mal truco explicar lo fácil por lo difícil, pero también puede que, como dijo un filósofo, el conocimiento se adquiera a través de metáforas.

Cuando miramos las tablas que reparten las academias a los alumnos de Selectividad, vemos que casi todas las series de Taylor que aparecen tienen una un aspecto sencillo. Una excepción viene dada por la función $f(x) = \tan x$ cuya serie de Taylor alrededor de $x = 0$ es

$$x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \frac{17}{315}x^7 + \frac{62}{2835}x^9 + \dots$$

Cualquiera sabe que los coeficientes impares n-ésimos, c_n, responden a la fórmula $c_n = f^{(2n-1)}(0)/(2n-1)!$ (los pares son trivialmente nulos) y, en principio, hallar los c_n es un problema de Cálculo I, ya que a fin de cuentas sólo implica derivadas en una variable. Los c_n forman una sucesión que aparentemente tiende a cero pero que por lo demás es muy caótica (no parece haber una fórmula computacionalmente sencilla para calcular cada término). Por ello vamos a rebajar el problema de Cálculo I y nos contentaremos con aproximar los c_n en vez de evaluarlos.

La gran dificultad está en que no parece fácil calcular c_n haciendo $2n-1$ derivadas una detrás de otra. Sería conveniente disponer de una fórmula mágica para despejar el coeficiente n-ésimo usando Cálculo Diferencial *menos elevado*. Dicha fórmula mágica (o una de ellas) es la fórmula integral de Cauchy que permite expresar una derivada de cualquier orden como una integral simple. Eso sí, hay que conceder el empleo de números complejos:

$$c_n = \frac{f^{(2n-1)}(0)}{(2n-1)!} = \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz$$

donde $C_R = \{z : |z| = R\}$ con $R < \pi/2$ para trabajar en un dominio en el que $\tan z$ sea holomorfa. Si R es pequeño, el integrando crece en módulo y la integral es difícil de estimar porque requiere el estudio de la cancelación de grandes cantidades oscilatorias. Llevar R más allá de $\pi/2$ es ventajoso porque se reduce el tamaño del integrando. A cambio hay que pagar con los residuos de algunas singularidades. Por ejemplo, si $\pi/2 < R < 3\pi/2$, C_R encierra los polos de $\tan z$ en $z = \pm\pi/2$ con residuo 1 y se tiene

$$c_n = \frac{2}{(\pi/2)^{2n}} + \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz.$$

Es fácil ver que la integral es de orden inferior al término anterior, de modo que esto prueba

$$c_n \sim 2(2/\pi)^{2n}.$$

Si queremos aproximaciones mejores todavía, podemos tomar un R mayor para hacer menor la integral y pagando con nuevos residuos. Si, por ejemplo, $3\pi/2 < R < 5\pi/2$, entonces

$$c_n = \frac{2}{(\pi/2)^{2n}} + \frac{2}{(3\pi/2)^{2n}} + \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz.$$

De modo que $2(2/\pi)^{2n}(1 + 3^{-2n})$ es una aproximación todavía. En una tabla:

	$c_n/A_1(n)$	$c_n/A_2(n)$
$n = 1$	$1'2337006$	$1'1103305$
$n = 2$	$1'0146780$	$1'0023039$
$n = 3$	$1'0014471$	$1'0000752$
$n = 4$	$1'0001552$	$1'0000028$
$n = 5$	$1'0000170$	$1'0000001$

donde $A_1(n) = 2(2/\pi)^{2n}$ y $A_2(n) = 2(2/\pi)^{2n}(1 + 3^{-2n})$.

Utilizando repetidamente esta idea se puede dar una fórmula para c_n con la aproximación que deseemos, y en el límite se obtendrá una fórmula exacta si admitimos series infinitas. A saber:

$$c_n = 2(2/\pi)^{2n}(1 + 3^{-2n} + 5^{-2n} + 7^{-2n} + \ldots).$$

Repasemos los puntos principales en el ejemplo anterior:

Hemos partido de la expresión $\tan x = x + x^3/3 + 2x^5/15 + \ldots$ (válida sólo en cierto rango de valores) y queríamos despejar los coeficientes del segundo miembro que son desconocidos a diferencia del primer miembro que es una función familiar que aparece en

las calculadoras de bolsillo. Para ello hemos considerado $f(z) = \tan z$ como una función de variable compleja y hemos usado una fórmula mágica con una integral compleja para despejar los coeficientes, después hemos transformado el dominio de integración llevándolo a un lugar donde las estimaciones de la integral son sencillas, y finalmente nos hemos percatado de que en el límite podríamos tener una fórmula exacta, aunque no del todo satisfactoria desde el punto de vista computacional por la aparición de sumas infinitas.

Todas estas ideas se pueden aplicar, con muchísimas complicaciones técnicas, en la demostración del teorema de los números primos. Nuestro problema consiste ahora en despejar los primos, en realidad $\psi(x)$, del segundo miembro de la identidad de Euler. Para ello extenderemos la definición del primer miembro a una función de variable compleja, la *función ζ de Riemann*. Después aplicaremos una fórmula mágica para despejar $\psi(x)$ en términos de dicha función. La parte más delicada viene cuando queremos mover el dominio de integración al lugar donde tenemos buenas estimaciones. El problema es que hay que atravesar cierta región desconocida y sobre todo que está la hipótesis de Riemann, todavía sin probar, que nos permitiría controlar los residuos que aparecen. Hasta que alguien la demuestre, debemos dar un rodeo para evitar nuestro desconocimiento. Incluso sin la hipótesis de Riemann se pueden obtener fórmulas "explícitas" para $\pi(x)$ o $\psi(x)$ si se admiten series infinitas que involucran los residuos desconocidos. Estas fórmulas son de escaso interés computacional, pero en forma truncada y con algunas propiedades de los residuos, son suficiente como para concluir el teorema de los números primos. De alguna forma esto es como decir que en el ejemplo anterior $c_n \sim 2(2/\pi)^{2n}$ porque los términos que faltan para tener la igualdad son de orden inferior.

1.4. La extensión meromorfa y la ecuación funcional

Con el propósito de comenzar a seguir el esquema trazado anteriormente, vamos a definir una función $\zeta = \zeta(s)$, (la *función ζ de Riemann*) que es meromorfa en $\mathbb{C}$ y que coincide con el primer miembro de la identidad de Euler cuando $\operatorname{Re} s > 1$. Por las propiedades básicas de las funciones meromorfas, si tal función existe es única.

En vez de dar construcciones más directas (por ejemplo, no es difícil ver que $\zeta(s) = (1-2^{1-s})^{-1}\sum(-1)^{n+1}n^{-s}$ es la extensión meromorfa en $\operatorname{Re} s > 0$, y con el Lema de Abel se pueden dar extensiones sucesivas [**El**]), seguiremos el razonamiento original de Riemann, obteniendo por el mismo precio la extensión deseada y una relación de simetría entre $\zeta(s)$ y $\zeta(1-s)$ llamada la *ecuación funcional* por antonomasia (en [**Ti**] hay otras pruebas diferentes de la de Riemann, algunas muy breves). Tal ecuación funcional es muy interesante, porque traducirá nuestro buen conocimiento de ζ en $\operatorname{Re} s > 1$ en un conocimiento similar en $\operatorname{Re} s < 0$. A la *terra incognita* que queda entremedias, $0 \le \operatorname{Re} s \le 1$, se le llama *banda crítica*.

La ecuación funcional es tan notable que merece la pena alguna ensoñación para motivar su existencia. Podemos hacerla creíble si pensamos que desde el punto de vista de las distribuciones la transformada de Fourier de $|x|^{-s}$ es $|x|^{s-1}$ con ciertos factores [**Li**]. De modo que si creemos con fe ciega en la fórmula de sumación de Poisson se debería tener $\sum n^{-s} = \text{factores} \sum n^{-(1-s)}$. Claramente esta igualdad no puede entenderse de la forma habitual ya que el término $n = 0$ da problemas y, para el resto de los términos, si la serie de la derecha converge la de la izquierda diverge, y viceversa. Pero cabe esperar que si evitamos el problema en $n = 0$ con algún tipo de "renormalización" todo funcione reemplazando la serie que diverge por la extensión dada por la función ζ. Como curiosidad se puede mencionar que antes de ser "descubierto", Ramanujan envió a un matemático (a través de un tercero) la fórmula $1 + 2 + 3 + 4 + 5 + \ldots = -1/12$ que corresponde a lo que se obtendría con la ecuación funcional. Obviamente el matemático dijo con buen criterio que había que tener mucho cuidado con las series divergentes [**Be**].

Riemann partió de la definición de la función Gamma en $s/2$, $\Gamma(s/2) = \int_0^\infty t^{s/2-1} e^{-t}\, dt$ para probar tras el cambio de variable $t \mapsto \pi n^2 t$ que si $\operatorname{Re} s > 1$

$$\pi^{-s/2}\Gamma(s/2)\sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} \int_0^\infty t^{s/2-1} e^{-\pi n^2 t}\, dt$$

o equivalentemente

$$\pi^{-s/2}\Gamma(s/2)\sum_{n=1}^{\infty} n^{-s} = \frac{1}{2}\int_0^\infty t^{s/2-1}(\theta(t) - 1)\, dt \qquad \text{donde} \quad \theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}.$$

Lo que hemos ganado es que se puede aplicar la fórmula de Poisson en sentido clásico a $\theta(t)$ dentro de la integral. Con ello esencialmente t pasará a $1/t$ y por tanto la parte de la integral $\int_0^1$ se transformará en $\int_1^\infty$. Esto es interesante para llevar a cabo la extensión ya que la divergencia de $\int_0^1 t^{s/2-1} t^{-1/2} dt$ para $\operatorname{Re} s < 1$ es la responsable de que no podamos extender el segundo miembro. Con esta idea en mente separamos el rango de integración y utilizamos Poisson en la forma $\theta(t) = t^{-1/2}\theta(1/t)$, con ello el segundo miembro es (para $\operatorname{Re} s > 1$)

$$\frac{1}{2}\int_0^1 + \frac{1}{2}\int_1^\infty = \frac{1}{2}\int_0^1 t^{s/2-1}(t^{-1/2}\theta(1/t) - 1)\, dt + \frac{1}{2}\int_1^\infty t^{s/2-1}(\theta(t) - 1)\, dt.$$

Con el cambio $t \mapsto 1/t$ en la primera integral y algunos cambios cosméticos, se llega a que para $\operatorname{Re} s > 1$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s(s-1)} + \frac{1}{2}\int_1^\infty (t^{s/2-1} + t^{-1/2-s/2})(\theta(t) - 1)\, dt \tag{1.2}$$

Ahora la integral tiene sentido para todo $s \in \mathbb{C}$ y como $\Gamma(s/2)$ no se anula, la función ζ así definida (que coincide con $\sum n^{-s}$ en $\operatorname{Re} s > 1$) es meromorfa en $\mathbb{C}$ y holomorfa en $\mathbb{C} - \{0, 1\}$. Usando que $\lim_{s\to 0} s\Gamma(s/2) = 2$ y $\Gamma(1/2) = \pi^{1/2}$, se deduce que ζ es de hecho meromorfa en $\mathbb{C}$ con un único polo en $s = 1$ de residuo 1. Además la invariancia del segundo miembro de (1.2) al cambiar s por $1 - s$ prueba la *ecuación funcional*

$$\boxed{\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).}$$

A partir de las propiedades básicas de la función Γ se sigue que ζ tiene ceros simples en $s = -2, -4, -6, \ldots$ Estos ceros son los llamados *ceros triviales*. Sabiendo que $\sum n^{-s} \neq 0$ en $\operatorname{Re} s > 1$, es fácil deducir que si hay otros ceros deben estar en la banda crítica $0 \leq \operatorname{Re} s \leq 1$. Se pueden calcular otros valores especiales como $\zeta(-1) = -1/12$ que corresponde a la identidad no rigurosa de Ramanujan. A propósito, nótese que la fórmula obtenida para los coeficientes de Taylor de la tangente implica $\zeta(2n) = c_n \pi^{2n}/(2(2^{2n} - 1))$ para $n \in \mathbb{Z}^+$. No se conocen fórmulas similares para $\zeta(2n + 1)$.

1.5. Fórmulas mágicas y productos infinitos: el poder de la variable compleja

Con diversas variantes de la fórmula integral de Cauchy es posible despejar a partir de ζ y por medio de la identidad de Euler funciones como $\pi(x)$ (esto es lo que hizo Riemann) o la función característica de los primos. Sin embargo los resultados obtenidos son un poco aparatosos y técnicamente es mucho más ventajoso tratar con la función $\psi(x)$ que lleva a fórmulas más limpias.

Tomando logaritmos en la identidad de Euler y derivando, es fácil probar (utilícese $(1 - x)^{-1} = 1 + x + x^2 + \ldots$) para $\operatorname{Re} s > 1$

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

(Nótese que la convergencia en $\operatorname{Re} s > 1$ implica, como habíamos mencionado, que $\sum n^{-s} \neq 0$ en dicha región). Si encontrásemos una fórmula mágica que aplicase n^{-s} en 1 si $n \leq x$ y en 0 si $n > x$, obtendríamos $\psi(x)$. Esta fórmula mágica vuelve a ser la fórmula integral de Cauchy pero en un caso un poco especial.

Proposición 1.2 . *Sea $c > 1$ y sea la línea vertical $L = \{\operatorname{Re} s = c\}$, entonces*

$$\frac{1}{2\pi i} \int_L \frac{t^s}{s}\, ds = \begin{cases} 0 & \text{si } 0 < t < 1 \\ 1 & \text{si } t > 1 \end{cases}$$

DEM.: El caso $0 < t < 1$ se obtiene considerando $\lim_{N\to\infty} \int_{\partial R_N} t^s s^{-1} ds$ con R_N el rectángulo $\{-N < \operatorname{Re} s < c\} \cap \{|\operatorname{Im} s| < N\}$. El otro caso es similar pero considerando el simétrico de R_N por L. ■

De modo que con L como antes, si $x > 1$ no es entero

$$\boxed{\psi(x) = \frac{1}{2\pi i} \int_L -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s}\, ds} \tag{1.3}$$

Una vez que tenemos la fórmula mágica nos gustaría llevar la línea de integración lo más lejos posible a la izquierda para aprovechar el decaimiento exponencial de x^s cuando $\operatorname{Re} s \to -\infty$, pero teniendo buen cuidado de esquivar los ceros triviales. El gran problema es que para ello debemos pagar con los residuos correspondientes a los ceros no triviales de ζ, los que están en $0 \le \operatorname{Re} s \le 1$, cuya localización no se conoce. De ahí surgirán casi todas las dificultades.

Para tomar resuello veamos cómo la Variable Compleja es tan poderosa que permite relacionar la función $-\zeta'/\zeta$ con los ceros de ζ. A pesar de nuestro desconocimiento de ambos objetos en la banda crítica, esperamos obtener alguna ganancia de esta relación.

Aplicaremos la teoría de funciones de orden finito de Hadamard [**Ci-Co**], quien la creó especialmente para aplicarla a ζ. Resumimos aquí los puntos principales:

Si P es un polinomio no constante, evidentemente se puede factorizar como $P(z) = A\prod(1 - z/z_n))$ donde z_n son sus raíces y $A = P(0)$. Podríamos sospechar que lo mismo ocurre con otras funciones enteras, por ejemplo que se cumple $\cos z = \prod(1 - z/z_n)$ para $z_n = n\pi + \pi/2$, los ceros de $\cos z$. Hay problemas de convergencia, pero esta fórmula es cierta si entendemos el producto infinito como límite de $\prod_{n\le N}(1 - z/z_n)$. Sin embargo algo falla en general en este esquema porque la función e^z no tiene ceros y no es constante. La teoría de Hadamard dice que todo funciona bien si nos restringimos a funciones que no crezcan demasiado, permitimos que A sea una función exponencial, y escribimos algunos factores artificiales no nulos para conseguir la convergencia absoluta. La teoría es bastante general, pero aquí sólo emplearemos un resultado específico en este sentido:

Teorema 1.3 . *Sea f una función entera no nula tal que para cada $\epsilon > 0$ verifica $|f(z)| = O\big(e^{|z|^{1+\epsilon}}\big)$. Entonces se cumple la igualdad*

$$f(z) = e^{A+Bz} \prod (1 - z/z_n) e^{z/z_n}$$

donde A y B son constantes y z_n son los ceros de f. Además $\sum |z_n|^{-1-\epsilon} < \infty$ y por tanto el producto converge absolutamente.

Es interesante reescribir el primer miembro de la ecuación funcional de una forma

bonita que dé lugar a una función entera. Exactamente se define

$$\xi(s) = \frac{1}{2} s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Nótese que $\xi(s) = \xi(1-s)$. De (1.2) se puede deducir que $|\xi(s)| = O\big(e^{C|s|\log|s|}\big)$ para cierta constante $C > 0$ cuando $|s| \to \infty$ (por la simetría de ξ basta considerar el caso $\operatorname{Re} s \geq 1/2$). Al aplicar el teorema anterior se tiene

$$\boxed{\xi(s) = e^{A+Bs}\prod(1 - s/\rho)e^{s/\rho}}$$

donde el producto es sobre todos los ceros ρ no triviales de ζ, esto es $0 \leq \operatorname{Re} s \leq 1$. Tomando logaritmos y derivando se sigue

$$\boxed{\frac{\zeta'(s)}{\zeta(s)} = C - \frac{1}{s-1} - \frac{1}{2}\frac{\Gamma'(s/2+1)}{\Gamma(s/2+1)} + \sum_{\rho}\Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big)} \tag{1.4}$$

donde C es una constante que se puede evaluar exactamente [**Da**] pero que no tiene relevancia para demostrar el teorema de los números primos.

1.6. La fórmula explícita

La integral en (1.3) tiene una particularidad que puede dar lugar a muchos problemas técnicos, y es que está al borde de la no convergencia. Si vamos a llevar L a una zona donde $-\zeta/\zeta$ es muy poco conocida cabe la posibilidad de que nos tengamos que enfrentar a una integral divergente. Por ello es mejor "cortar" desde el principio la línea L dejando sólo el segmento $L_T = L \cap \{|\operatorname{Im} s| \leq T\}$. Como es natural, si T es grande la aproximación es buena. De hecho se cumple

$$\psi(x) = \frac{1}{2\pi i}\int_{L_T} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds + O\Big(\frac{x^c}{T(c-1)} + \frac{x}{T}\log^2 x\Big) \tag{1.5}$$

para $x > 1$ no entero (la constante "O" depende de la distancia de x al entero más cercano). Dejaremos esto como un detalle a probar más adelante.

Elegiremos desde ahora $c = 1 + 1/\log x$ para que el término de error se reduzca a $O(xT^{-1}\log^2 x)$.

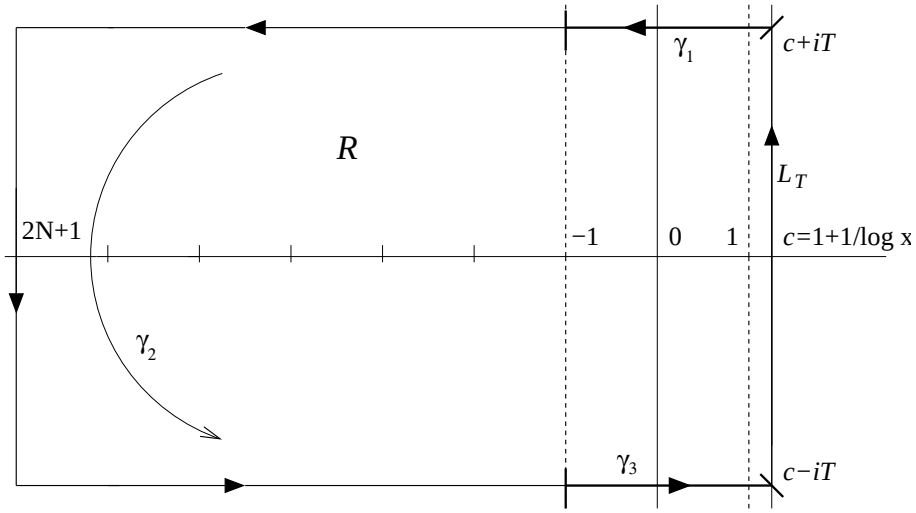
El siguiente paso es aplicar el teorema de los residuos al contorno ∂R donde R es el

rectángulo que tiene a L_T como uno de sus lados y a $-(2N+1)\pm iT$ como vértices opuestos con $N \in \mathbb{Z}^+$ y $N > T \geq 2$.

En la línea quebrada $\partial R \cap \{\mathrm{Re} \leq -1\}$ se tiene $|\zeta'(s)/\zeta(s)| = O(\log|s|)$. Este segundo detalle no es difícil de probar con la ecuación funcional.

Como no sabemos exactamente dónde están los ceros de ζ en la banda crítica, no hay esperanza de estimar para un T dado ζ'/ζ en el trozo restante de $\partial R - L_T$. Todo lo que vamos a afirmar es que siempre podemos mover T a lo más una unidad, es decir, cambiar T por $T+\delta$, $0 \leq \delta \leq 1$, de manera que $|\zeta'(s)/\zeta(s)| = O(\log^2 T)$ en $\partial R \cap \{-1 \leq \mathrm{Re}\, s \leq c\}$. Éste es el detalle más sutil.

En un dibujo:



y las acotaciones que hemos dado por supuesto son:

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log|s|) \quad \text{en } \gamma_2, \qquad \frac{\zeta'(s)}{\zeta(s)} = O(\log^2 T) \quad \text{en } \gamma_1 \cup \gamma_3 \quad \text{(quizá moviendo } T\text{)}.$$

Con estas acotaciones y aplicando el teorema de los residuos a (1.5) con $f(s) = -x^s\zeta'(s)/(s\zeta(s))$, se obtiene:

$$\psi(x) = \sum_{s\in R} \mathrm{Res}(f,s) + O\Big(\int_{\gamma_1\cup\gamma_2\cup\gamma_3} |f| + \frac{x}{T}\log^2 x\Big) = \sum_{s\in R} \mathrm{Res}(f,s) + O\big(\frac{x}{T}\log^2(xT)\big).$$

La función f tiene polos en $s=1$, en $s=0$, en los ceros triviales $s=-2n$ y en los ceros no triviales $s=\rho$. Los residuos son respectivamente x, $-\zeta'(0)/\zeta(0)$, $x^{-2n}/(2n)$ y

$-x^\rho/\rho$. De modo que para x como antes ($x > 1$ y no entero), se tiene

$$\psi(x) = x - \frac{\zeta'(0)}{\zeta(0)} + \frac{1}{2}\sum_{n\le N}\frac{x^{-2n}}{n} - \sum_{|\rho|<T}\frac{x^\rho}{\rho} + O\big(\frac{x}{T}\log^2(xT)\big). \tag{1.6}$$

Permitiendo $T \to \infty$ se deduce la fórmula inútil pero exacta

$$\psi(x) = x - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log(1-x^{-2}) - \sum_\rho \frac{x^\rho}{\rho}$$

donde la suma se debe entender como límite de $\sum_{|\rho|<T}$, no converge absolutamente. Curiosamente se llama *fórmula explícita* a la fórmula anterior.

Mucho más interesante es la fórmula truncada (1.6). Nótese que $\psi(x)$ en los enteros puede "saltar" a lo más $O(\log x)$, así pues añadiendo este término a (1.6) se tiene una fórmula válida uniformemente para x, sin necesidad de imponer que no sea entero. De modo que para $x \ge 2$

$$\psi(x) = x - \sum_{|\rho|<T}\frac{x^\rho}{\rho} + O\big(\frac{x}{T}\log^2(xT) + \log x\big). \tag{1.7}$$

Podemos elegir cualquier $T \ge 2$, pero si lo tomamos pequeño entonces el error es demasiado grande como para probar el teorema de los números primos. Por otra parte, la obligación de tomar T grande lleva al difícil problema de la distribución de los ceros ρ.

Veamos ahora un esbozo de los detalles.

El primero tenía que ver con la aproximación de $\int_L$ por $\int_{L_T}$. Para $0 < t < 1$ se tiene $\int_{L-L_T} t^s/s\,ds = -\int_{L_+} + \int_{L_-}$ donde $L_\pm$ es la semirrecta que une $c \pm iT$ con $+\infty \pm iT$. De donde

$$\int_{L-L_T}\frac{t^s}{s}\,ds = O\big(\frac{t^c}{T|\log t|}\big).$$

Para $t > 1$ se obtiene en su lugar $O(t^c)$ en el segundo miembro. Para comprobarlo basta emplear que $\int_{L-L_T} = -\int_C$ donde C es el arco de circunferencia en $\operatorname{Re} s < c$ centrado en en origen que une $c - iT$ con $c + iT$.

La fórmula mágica (1.3) se puede escribir como

$$\psi(x) = \frac{1}{2\pi i}\int_{L_T} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds + \frac{1}{2\pi i}\sum_n \Lambda(n)\int_{L-L_T}\frac{(x/n)^s}{s}\,ds.$$

Sustituyendo las acotaciones anteriores con $t = x/n$, después de un poco de trabajo se llega a (1.5).

El segundo detalle se puede completar tomando derivadas logarítmicas en la ecuación funcional. Gracias a la simetría la cota trivial $|\zeta'(s)/\zeta(s)| \leq$cte en $\operatorname{Re} s \geq 2$ se transforma en la deseada, $|\zeta'(s)/\zeta(s)| = O(\log|s|)$ en $\operatorname{Re} s \leq -1$, empleando $\Gamma'(s)/\Gamma(s) = O(\log|s|)$.

El último detalle es tan ingenioso que en justicia no merece tal apelativo. Si en (1.4) escribimos $s = 2 + iT$ y tomamos partes reales se tiene

$$1 \gg -\log T + \sum_\rho \operatorname{Re}\left(\frac{1}{2+iT-\rho} + \frac{1}{\rho}\right).$$

Después de calcular la parte real (recuérdese que $0 \leq \operatorname{Re}\rho \leq 1$) se sigue $\log T \gg \sum(1 + (T - \operatorname{Im}\rho)^2)^{-1}$ y de aquí que sólo hay $O(\log T)$ ceros con $T \leq \operatorname{Im}\rho \leq T+1$. Por tanto quizá cambiando T por $T + \delta$, $0 \leq \delta \leq 1$, se puede suponer que hay una distancia $d \gg 1/\log T$ de cada cero de ζ a la horizontal $\operatorname{Im} s = T$.

Si ahora en (1.4) sustituimos $s = \sigma + iT$ con $-1 \leq \sigma \leq 2$ y restamos lo obtenido al sustituir $s = 2 + iT$, se sigue

$$\frac{\zeta'(\sigma+iT)}{\zeta(\sigma+iT)} \ll \log T + \sum_\rho \left|\frac{1}{\sigma+iT-\rho} - \frac{1}{2+iT-\rho}\right|.$$

Los $O(\log T)$ sumandos correspondientes a $|T - \operatorname{Im}\rho| \leq 1$ contribuyen $O(\log^2 T)$ en total por la condición de la distancia. La contribución de los correspondientes a $|T - \operatorname{Im}\rho| > 1$ es menor sin más que emplear la acotación para $\sum(1 + (T - \operatorname{Im}\rho)^2)^{-1}$.

1.7. ¿Qué podemos probar con la hipótesis de Riemann?

Antes de adscribirnos a las ventajas del que nos prometen ser el mejor de los mundos posibles, vamos a comprobar que realmente lo es.

La fórmula

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{s}{s-1} + s\int_1^\infty (\psi(x) - x)x^{-s-1}dx,$$

que se deduce con el Lema de Abel, prueba directamente que $\psi(x) = x + o(x)$ implica necesariamente $\lim_{\sigma\to 1^+} |\zeta'(\sigma + it)/\zeta(\sigma + it)| < \infty$ para todo $t \neq 0$. Es decir, si hubiera algún cero en $\mathrm{Re}\, s = 1$, el teorema de los números primos no sería cierto. De la misma forma, la existencia de un solo cero en $\mathrm{Re}\, s = \sigma_0$ es incompatible con $\psi(x) = x + o(x^{\sigma_0})$, como sugiere (1.7).

Según esto, el error más pequeño en el teorema de los números primos se obtendría si todos los ceros no triviales tuviesen la parte real lo menor posible. Por otro lado, la ecuación funcional implica que si ρ es un cero no trivial entonces $1 - \rho$ también lo es. De forma que para que el supremo de las partes reales de los ceros no triviales sea lo menor posible todas ellas deben ser $1/2$. Quizá fuera este argumento, o simplemente la evidencia numérica [**Ed**] lo que llevo a Riemann a formular su hipótesis, cuyo enunciado es:

HIPÓTESIS DE RIEMANN: *Todos los ceros no triviales de la función ζ están en la línea crítica $Re\, s = 1/2$.*

Que los ceros de una función meromorfa se coloquen todos en fila india es algo tan singular que debería ser fácil de probar si es cierto, o de refutar si hay un contraejemplo. Sin embargo han pasado más de 140 años desde que Riemann hizo su conjetura y no sólo no se ha probado sino que no se ha logrado estrechar ni un ápice la banda crítica en la que viven los ceros. Es decir, no se conoce nigún $\epsilon > 0$ tal que todos los ceros no triviales pertenezcan a una *banda crítica reducida*, $\epsilon < \mathrm{Re}\, s < 1 - \epsilon$.

De todas maneras no está de más imaginar cuál es la mejor situación y ver al menos las consecuencias más inmediatas. Si se cumpliera la hipótesis de Riemann, tomando $T = x^{1/2}$ en (1.7) se tiene (recuérdese que hay $O(\log N)$ ceros con $N \leq |\rho| \leq N + 1$)

$$\psi(x) = x + O(x^{1/2}\log^2 x).$$

Esto se traduce en

$$\pi(x) = Li(x) + O(x^{1/2}\log x).$$

Se conoce que el factor $\log^2 x$ no se puede suprimir totalmente en la primera fórmula [**El**] ya que los límites superior e inferior de $(\psi(x) - x)/\sqrt{x}$ son $+\infty$ y $-\infty$. De ello se puede deducir que $Li(x)$ es la aproximación óptima de $\pi(x)$ si no admitimos términos oscilatorios.

Aparte de la optimización del término de error, conocer la hipótesis de Riemann de antemano permitiría reducciones importantes en la demostración del teorema de los números primos. Así como la prueba de muchos resultados condicionales de la Teoría de Números que dependen de ella.

1.8. ¿Qué podemos probar sin la hipótesis de Riemann?

Como ya hemos mencionado, no se sabe probar la ausencia de ceros en ninguna bandita del tipo $1-\epsilon < \operatorname{Re} s < 1$. Todo lo que se sabe al respecto [**Iv**], y con mucho esfuerzo, es que si existiera una sucesión de ceros no triviales $\rho_n = \sigma_n + it_n$ con $\sigma_n \to 1$, entonces $\log|t_n|$ a la larga superaría a cierta potencia negativa de $1-\sigma_n$. El resultado que veremos aquí es el clásico (no el mejor posible) y permite acotar la suma en (1.7) por el término principal multiplicado por un factor que tiende lentamente a cero; lo cual prueba el teorema de los números primos.

En primer lugar nótese que, por un argumento de continuidad en (1.4), intuitivamente si existiera un cero no trivial $\sigma_n + it_n$ muy cerca de $\operatorname{Re} s = 1$ entonces para $\sigma \to 1^+$ se tendría que $-\zeta'(\sigma+it_n)/\zeta(\sigma+it_n)$ tiene parte real muy grande y negativa. En ese caso, $\zeta'(s)/\zeta(s) = \sum \Lambda(n)n^{-s}$ sugiere que $\cos(t_n \log p)$ toma muchas veces valores negativos. Entonces, recíprocamente, $\cos(2t_n \log p)$ debe tomar muchas veces valores positivos y $-\zeta'(\sigma+2it_n)/\zeta(\sigma+2it_n)$ debe tener parte real grande y positiva. Controlando el tamaño de esta última cantidad controlaremos la cercanía del posible cero a la línea $\operatorname{Re} s = 1$. Lo más ingenioso, a la par que simple, es la manera de cuantificar los tamaños relativos al evaluar en $\sigma + it_n$ y en $\sigma + 2it_n$. Se emplea para ello la sencilla desigualdad trigonométrica

$$3 + \cos(2\alpha) \geq -4\cos\alpha \qquad \forall \alpha \in \mathbb{R}.$$

Susituyendo $\alpha = t_n \log p$ y sumando con coeficientes adecuados se tiene, para $\sigma > 1$,

$$-3\frac{\zeta'(\sigma)}{\zeta(\sigma)} - \operatorname{Re}\frac{\zeta'(\sigma+2it_n)}{\zeta(\sigma+2it_n)} \geq 4\operatorname{Re}\frac{\zeta'(\sigma+it_n)}{\zeta(\sigma+it_n)}$$

De (1.4), cuando $\sigma > 1$ está suficientemente cercano a 1 se cumple $-\zeta'(\sigma)/\zeta(\sigma) < (\sigma-1)^{-1} + \text{cte}$, y además las desigualdades

$$-\operatorname{Re}\frac{\zeta'(\sigma+2it_n)}{\zeta(\sigma+2it_n)} < \text{cte}\ \log(|t_n|+2) \quad \text{y} \quad -\operatorname{Re}\frac{\zeta'(\sigma+it_n)}{\zeta(\sigma+it_n)} < \text{cte}\ \log(|t_n|+2) - \frac{1}{\sigma-\sigma_n}.$$

Para probarlas utilícese (1.4), $\Gamma'(s)/\Gamma(s) = O(\log|s|)$ y que $\operatorname{Re}\left((s-\rho)^{-1} + \rho^{-1}\right) > 0$ para $\operatorname{Re} s > 1$. Sustituyendo se obtiene

$$3/(\sigma-1) + \text{cte}\log(|t_n|+2) \geq 4/(\sigma-\sigma_n).$$

Tomando $\sigma = 1 + \epsilon/\log(|t_n|+2)$ con ϵ pequeño se sigue que $\sigma_n \leq 1 - \text{cte}/\log(|t_n|+2)$ para cierta constante positiva. O dicho de otro modo, existe una constante $C > 0$ tal que

la región $s = \sigma + it$ con

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

está libre de ceros.

La *región libre de ceros* anterior, en conjunción con que hay $O(\log N)$ ceros con $N \leq |\rho| \leq N+1$ permite estimar la suma de (1.7) como

$$\sum_{|\rho|<T} \left| \frac{x^\rho}{\rho} \right| \ll \sum_{N<T} \log N \frac{x^{1-C/\log T}}{N} \ll x^{1-C/\log T} \log^2 T.$$

Finalmente tomando $T = e^{\sqrt{\log x}}$ y haciendo limpieza de los términos de orden inferior se concluye

$$\boxed{\psi(x) = x + O\big(xe^{-K\sqrt{\log x}}\big)}$$

para cierta constante positiva K (en [**El**], $K = 1/15$). Esto está muy lejos de lo que se obtendría con la hipótesis de Riemann pero prueba en particular que $(\psi(x) - x)/x$ tiende a cero más rápido que cualquier potencia negativa de $\log x$. Lo mejor que se ha conseguido hasta la fecha, tras los profundos trabajos de Vinogradov y Korobov [**Iv**], es reemplazar en el exponente de la fórmula anterior $\sqrt{\log x}$ por $\log^\alpha x$ para cualquier $\alpha < 3/5$.

1.9. Primos en progresiones aritméticas

Por último vamos a considerar la distribución de los primos en una progresión aritmética $\{an + b\}$ con $a, b \in \mathbb{Z}^+$ coprimos entre sí (en otro caso la progresión contiene a lo más un primo). Para cada a fijo se cumple $\mathbb{Z} = \{an+0\} \cup \{an+1\} \cup \ldots \cup \{an+(a-1)\}$ con n recorriendo $\mathbb{Z}$. De estas progresiones, $\{an+b\}$, hay $\phi(a)$ con b coprimo con a. Parece natural suponer que no hay ninguna de ellas privilegiada, de modo que todas contienen la misma proporción de primos. Esto sugiere el *teorema de los números primos en progresiones aritméticas*, que afirma

$$\pi(x; a, b) \sim \frac{1}{\phi(a)} Li(x) \qquad \text{con} \quad \pi(x; a, b) = \sum_{\substack{p \equiv b \pmod a \\ p \leq x}} 1$$

Por ejemplo, si $a = 5$ todos los primos mayores que 5 son de la forma $5n+1$, $5n+2$, $5n+3$ o $5n+4$. Por tanto cabe esperar que la cuarta parte de los primos sean de la forma $5n+2$, esto es, $\pi(x; 5, 2) \sim \frac{1}{4} Li(x)$.

Si tratamos de adaptar la demostración del teorema de los números primos usual al caso de progresiones aritméticas, una primera dificultad es que el análogo natural de la identidad de Euler no es cierto. En nuestro caso $\sum(5n+2)^{-s} \neq \prod(1-p^{-s})^{-1}$ con $p \equiv 2 \ (mod\ 5)$; la razón es simplemente que 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.

Un ejemplo que nos puede dar alguna luz es tratar de extraer los términos con grado en cierta progresión geométrica a partir de una serie de Taylor conocida, como la de $e^x = 1 + x/1! + x^2/2! + x^3/3! + \ldots$. Seleccionar los de grado par o impar es sencillo y da lugar a las funciones trigonómetricas hiperbólicas:

$$1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots = \frac{1}{2}(e^x + e^{-x}) = \cosh x, \quad \frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots = \frac{1}{2}(e^x - e^{-x}) = \operatorname{senh} x.$$

Si nos queremos restringir a los múltiplos de cuatro, la expresión es más complicada:

$$1 + \frac{x^4}{4!} + \frac{x^8}{8!} + \ldots = \frac{1}{4}(e^x + e^{ix} + e^{-x} + e^{-ix}) = \frac{\cosh x + \cos x}{2}.$$

Pero nos da la clave para entender que lo necesario para obtener los múltiplos de a es introducir como coeficientes raíces de la unidad teniendo en cuenta que la suma de todas ellas es nula. Así pues (recuérdese la notación $e(t) = e^{2\pi i t}$)

$$1 + \frac{x^a}{a!} + \frac{x^{2a}}{(2a)!} + \frac{x^{3a}}{(3a)!} + \ldots = \frac{1}{a}\sum_{k=0}^{a-1} e^{x\, e(k/a)} \qquad \text{para} \quad a \in \mathbb{Z}^+.$$

Si quisiéramos, por ejemplo, seleccionar los congruentes con 2 módulo 5, o en general módulo a, bastaría "adelantar" la suma en dos unidades:

$$\frac{x^2}{2!} + \frac{x^{a+2}}{(a+2)!} + \frac{x^{2a+2}}{(2a+2)!} + \frac{x^{3a+2}}{(3a+2)!} + \ldots = \frac{1}{a}\sum_{k=0}^{a-1} e(-2/a) e^{x\, e(k/a)}.$$

Una vez vistos estos ejemplos volvamos al problema con la identidad de Euler. Para que una función $f : \mathbb{Z}^+ \to \mathbb{C}$ dé lugar a una identidad como la de Euler:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \Big(1 - \frac{f(p)}{p^s}\Big)^{-1},$$

debe ser completamente multiplicativa (es decir, $f(mn) = f(m)f(n), \ \ \forall n, m \in \mathbb{Z}^+$). Lo

que haremos será elegir f que tome valores entre las raíces de la unidad de manera que nos permita seleccionar progresiones aritméticas como antes. Primeramente nótese que como estamos interesados sólo en el caso en que a y b son coprimos es natural definir $f(n) = 0$ cuando n y a tienen divisores propios comunes porque $n = ak + b$, $\mathrm{mcd}(n, a) > 1 \Rightarrow \mathrm{mcd}(a, b) > 1$. Para el resto de los valores de n queremos que $f(n)$ sea una raíz de la unidad y que, en general, f sea una función multiplicativa y periódica de periodo a. Todos estos requerimientos se pueden completar de forma elegante considerando los *caracteres módulo a*, es decir, los homomorfismos $\chi : \mathbb{Z}_a^* \longrightarrow (\mathbb{C} - \{0\}, \cdot)$ donde $\mathbb{Z}_a^*$ es el grupo (multiplicativo) de unidades del anillo $\mathbb{Z}_a$. No es difícil probar que las únicas funciones con las propiedades anteriores son de la forma

$$f(n) = \begin{cases} 0 & \text{si } \mathrm{mcd}(n, a) > 1 \\ \chi(\overline{n}) & \text{si } \overline{n} \in \mathbb{Z}_a^* \end{cases}$$

donde χ es un carácter módulo a. Nótese que $\chi(\overline{n})$ es una raíz de la unidad para $\overline{n} \in \mathbb{Z}_a^*$ porque

$$(\chi(\overline{n}))^{|\mathbb{Z}_a^*|} = \chi(\overline{n}^{|\mathbb{Z}_a^*|}) = \chi(\overline{1}) = 1.$$

En el grupo $\mathbb{Z}_a^*$ (y en general en todos los abelianos cuando se extiende la definición) los caracteres forman un grupo con la multiplicación isomorfo al de partida. De algún modo conforman un dual del grupo que lo representa fielmente. 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

que 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 $\chi_3 = \chi_1^3$).

No es difícil definir constructivamente los caracteres [**Da**], [**El**] en términos de raíces primitivas de la unidad en $\mathbb{Z}_{p^k}^*$ con $p^k | a$ pero no será de interés aquí. Con el abuso de notación obvio, se suele denotar igual a los caracteres χ que a las funciones f asociadas. Conviniendo en ello, y después de lo dicho anteriormente las funciones que reemplazan a la función ζ en el contexto de los primos en progresiones aritméticas, son las *funciones L de Dirichlet* definidas como

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

Estas funciones satisfacen para $\operatorname{Re} s > 1$

$$L(s,\chi) = \prod_p \big(1 - \frac{\chi(p)}{p^s}\big)^{-1} \quad \text{y} \quad -\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \Lambda(n)\frac{\chi(n)}{n^s}.$$

Variando χ podemos seleccionar los primos en cierta progresión aritmética jugando, como antes, con las raíces de la unidad. Por ejemplo, con los caracteres de la tabla anterior se tiene

$$\sum_{\substack{n\equiv 1 \pmod 5 \\ n\le x}} \frac{\Lambda(n)}{n^s} = -\frac{1}{4}\sum_{j=0}^{4} \frac{L'(s,\chi_j)}{L(s,\chi_j)} \quad \text{y} \quad \sum_{\substack{n\equiv 2 \pmod 5 \\ n\le x}} \frac{\Lambda(n)}{n^s} = -\frac{1}{4}\sum_{j=0}^{4} \overline{\chi}_j(2)\frac{L'(s,\chi_j)}{L(s,\chi_j)}.$$

En general se puede aplicar la "fórmula mágica" como en el teorema de los números primos y probar que

$$\psi(x;a,b) = \sum_{\substack{n\equiv b \pmod a \\ n\le x}} \Lambda(n) = -\frac{1}{\phi(a)}\sum_{\chi} \frac{\overline{\chi}(b)}{2\pi i}\int_{L_T} \frac{L'(s,\chi)}{L(s,\chi)}\frac{x^s}{s}\,ds + \text{Error}$$

donde χ recorre todos los caracteres módulo a (nótese que $\phi(a) = |\mathbb{Z}_a^*|$ es el número de estos caracteres) y Error$= O(x^c/(T(c-1)) + xT^{-1}\log^2 x)$.

Cuando uno llega a este punto ya está cansado y tiende a decir que se procede de forma similar a como se hizo en el teorema de los números primos. Sin embargo esto no es realmente así, hay varias dificultades técnicas y teóricas. Entre las dificultades más notables está la prueba de que $L'(s,\chi)/L(s,\chi)$ sólo tiene un polo en $s = 1$ si χ es constantemente uno (naturalmente, en los coprimos con a); lo cual requiere demostrar que para el resto de los caracteres se cumple $L(1,\chi) \neq 0$. Nótese que si damos esto por supuesto, la prueba de Euler se puede adaptar para deducir el *Teorema de Dirichlet* que afirma que $\{an + b\}$ contiene infinitos primos. Otra dificultad aparece al estudiar la uniformidad en a de las regiones libres de ceros de $L'(s,\chi)/L(s,\chi)$. Este problema viene motivado porque en muchas aplicaciones se necesita que $\pi(x;a,b) \sim \frac{1}{\phi(a)}Li(x)$ siga siendo cierto si a es una función de x que no crece demasiado. Hoy en día sólo se sabe tratar el caso en que a es extremadamente pequeño en comparación con x, debido a que no se conoce la ausencia de ciertos ceros reales de $L(s,\chi)$ llamados *ceros de Siegel* [**Da**], [**El**]. Por otra parte, la generalización de la hipótesis de Riemann a las funciones L, si fuera cierta, implicaría $\pi(x;a,b) \sim \frac{1}{\phi(a)}Li(x)$ para $a = a(x) = O(x^{1/2-\epsilon})$ cualquiera que sea $\epsilon > 0$. Nuestro conocimiento actual con respecto a esta *hipótesis de Riemann generalizada* es todavía mucho más precario que con respecto a la hipótesis original.