Carlos Ivorra Castillo

TEORÍA ANALÍTICA DE NÚMEROS

¿Por qué los números son hermosos? Es como preguntar por qué la novena sinfonía de Beethoven es hermosa. Si no ves por qué, nadie puede explicártelo. Yo sé que los números son hermosos. Si no lo son, nada lo es.

PAUL ERDŐS

Índice General

Introducción

La teoría de números surge con el estudio de las propiedades aritméticas de los números naturales. Sin embargo, sucede que muchas de esas propiedades requieren para ser demostradas —o incluso a veces, para ser entendidas— técnicas y conceptos matemáticos sofisticados, que requieren adentrarse en las ramas más abstractas de la matemática y que conducen a resultados en los que a menudo es difícil —si no imposible— reconocer hechos sobre números naturales que puedan haberlos motivado.

Por ello existe una tradición de distinguir entre la *teoría de números elemental* (que no emplea más que técnicas aritméticas sencillas), la *teoría algebraica de números* (que emplea técnicas algebraicas más o menos sofisticadas) y la *teoría analítica de números* (que emplea técnicas del análisis matemático). Sin embargo, las fronteras entre ellas son difusas, ya que hay muchos resultados que requieren simultáneamente técnicas algebraicas y analíticas, e incluso dentro de la teoría analítica de números se suele distinguir entre resultados que sólo requieren de técnicas elementales del análisis real (límites, derivadas, etc.) y las que requieren de la teoría de funciones de variable compleja, cuya conexión con los números naturales es, en principio, más lejana.

Así, en mis libros de *Introducción a la teoría algebraica de números* [ITAl] e *Introducción a la teoría analítica de números* [ITAn] probamos resultados a menudo no triviales usando un bagaje teórico minimalista (algebraico y analítico, respectivamente) y, del mismo modo que en mi libro de *Teoría algebraica de números* hemos avanzado en dicha teoría aprovechando la teoría algebraica de mi libro de *Álgebra* [Al] y la teoría analítica de mis libros de *Introducción al cálculo diferencial* [IC] y *Análisis matemático* [An], aquí vamos a avanzar en el estudio de la teoría analítica de números aprovechando, además de los contenidos de estos libros, algunos resultados más profundos de mi libro de *Funciones de variable compleja* [VC]. Ocasionalmente usaremos algún resultado de [TAl].

Insistimos en que las fronteras entre la teoría algebraica y la analítica son difusas. Por ejemplo, en el primer capítulo de este libro combinaremos técnicas algebraicas y analíticas para obtener varias pruebas de trascendencia, es decir, resultados que aseguran que determinados números reales son trascendentes. Podríamos decir que la afirmación "$2^{\sqrt{2}}$ es trascendente" es algebraica (en cuanto que la trascendencia es una propiedad algebraica), pero sucede que la demostración combina técnicas algebraicas y analíticas.

A título orientativo (sin ánimo de ser rigurosos) podríamos decir que los resultados algebraicos sobre números naturales suelen tratarlos "de forma individualizada". Por ejemplo, la ley de reciprocidad cuadrática de Gauss [ITAl 7.1] es un resultado aplicable a cada par de primos impares individuales. Esto contrasta con afirmaciones como la siguiente:

> *La proporción de números libres de cuadrados menores o iguales que un número dado N es aproximadamente $6/\pi^2 \approx 0.6$, y la estimación es más exacta cuanto mayor es N.*

Esta afirmación habla sobre los números libres de cuadrados, pero no dice nada sobre ninguno de ellos en particular. Los resultados analíticos que vamos a obtener en este libro comparten mayoritariamente esta naturaleza "estadística". Vamos a desarrollar esta idea comentando algunos de los resultados de los que nos vamos a ocupar en los capítulos siguientes.

Empezamos considerando un resultado que ya demostramos tanto en [ITAn] como en [TAl], a saber, el teorema de Dirichlet sobre primos en progresiones aritméticas:

> *En toda progresión aritmética $mx + n$, donde m y n son enteros primos entre sí, hay infinitos números primos.*

Se trata de un enunciado puramente algebraico —y con muchas repercusiones en la teoría algebraica de números, como hemos puesto de manifiesto en [ITAl]—, pero con esa componente "global" típicamente analítica y que coincide con el hecho de que no se conoce ninguna demostración puramente algebraica. En 3.27 veremos cómo Euler usó la fórmula [ITAn 8.25]

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

donde p recorre los números primos, para deducir que la serie

$$\sum_p \frac{1}{p}$$

de los inversos de los primos es divergente, lo cual implica en particular que existen infinitos números primos. Obviamente, hay formas mucho más simples de llegar a esta conclusión, pero el interés del razonamiento de Euler es que es generalizable, y fue precisamente generalizando su argumento como Dirichlet llegó a la prueba del teorema que hoy lleva su nombre.

Cuando Kummer descubrió que los anillos de enteros ciclotómicos tienen factorización única ideal, Dirichlet decidió estudiar el análogo a la función dseta de Riemann para los enteros ciclotómicos de orden m, a saber, la función

$$\zeta_m(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre los ideales no nulos del anillo de los enteros ciclotómicos.

En [TAl 4.1] hemos estudiado estas series para cuerpos numéricos arbitrarios. La factorización única ideal implica trivialmente una fórmula análoga a la de Euler:

$$\sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}},$$

donde $\mathfrak{p}$ recorre los primos ciclotómicos (ideales). En su estudio de la función dseta ciclotómica, Dirichlet descubrió lo que hoy se conoce como "caracteres de Dirichlet" [ITAn 7.19] y las "funciones L de Dirichlet" [ITAn 8.33], que son series de Dirichlet "ordinarias" de la forma

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

donde χ es un carácter de Dirichlet, y demostró [TAl 4.26] que la función dseta del cuerpo ciclotómico factoriza como

$$\zeta_m(s) = \prod_{\chi} L(s,\chi),$$

donde χ recorre los $\phi(m)$ caracteres módulo m.

Es fácil probar que las funciones $L(s,\chi)$ se extienden a funciones holomorfas en el semiplano $\mathrm{Re}\, s > 0$ salvo si $\chi = 1$ es el carácter principal, en cuyo caso la extensión existe igualmente, pero la función $L(s,1)$ tiene un polo simple en $s = 1$. Por lo tanto, la función $\zeta_m(s)$ es holomorfa en dicho semiplano salvo quizá en $s = 1$. Decimos "quizá" porque en principio el polo de $L(s,1)$ podría cancelarse si alguna de las demás funciones L cumpliera $L(1,\chi) = 0$. Precisamente, el punto crucial de la prueba es demostrar que esto no sucede, es decir, que si χ es un carácter no principal, entonces $L(1,\chi) \neq 0$. Una vez garantizado este punto, el resto de la prueba es una adaptación sencilla del argumento original de Euler sobre la divergencia de la serie de los inversos de los primos.

Dirichlet demostró que la función $\zeta_m(s)$ tiene ciertamente un polo en $s = 1$ usando la aritmética ideal del cuerpo ciclotómico m-simo (teorema [TAl 4.8]). Esto lo probamos en [TAl 4.8] y es el núcleo de la demostración del teorema de Dirichlet dada en [TAl 4.28], mientras que en [ITAn 7.24] dimos una prueba "elemental", en el sentido de que no usa ningún resultado sobre funciones de variable compleja ni mucho menos de la teoría algebraica de números.

En la sección 3.6 veremos una prueba intermedia, que es mucho más simple y conceptual que la dada en [ITAn] porque usa la teoría de funciones holomorfas, y también mucho más simple que la dada en [TAl] porque evita completamente la teoría algebraica de números. Para que quede claro que es así, hemos incluido en un apéndice al final del capítulo III los pocos resultados (elementales) sobre caracteres de Dirichlet que usamos en la prueba, aunque todos ellos están probados en [ITAn] y generalizados a grupos arbitrarios en mi libro de *Teoría de grupos* [TG]. La prueba de [ITAn] surge a su vez de despojar la prueba que veremos aquí de toda referencia a la teoría de funciones holomorfas, lo cual requiere de bastante ingenio.

Más concretamente, en la demostración que veremos en la sección 3.6 tomaremos el producto precedente de funciones L como definición[1] de $\zeta_m(s)$, con lo que eliminamos de raíz toda alusión a los cuerpos ciclotómicos y su factorización ideal.

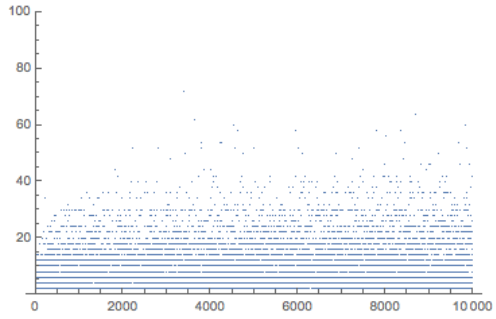
El estudio de los números primos es uno de los temas fundamentales de la teoría de números (tanto algebraica como analítica). La ley de reciprocidad cuadrática, que hemos mencionado antes, es un ejemplo de la clase de afirmaciones que el álgebra puede probar sobre los números primos (aunque también existen demostraciones analíticas). El análisis matemático, por su parte, permite obtener muchos resultados que ponen en evidencia las regularidades ocultas en la apariencia caótica de la distribución de los números primos en el seno de los números naturales. El teorema de Dirichlet es un buen ejemplo de ello, al igual que el postulado de Bertrand o los teoremas de Mertens demostrados también en el capítulo VI de [ITAl], pero hay otro mucho más famoso, que vamos a discutir a continuación.

Llamaremos $\{p_n\}_{n=1}^{\infty}$ a la sucesión de los números primos o, dicho con otras palabras, llamamos p_n al primo n-simo. Sus primeros términos son:

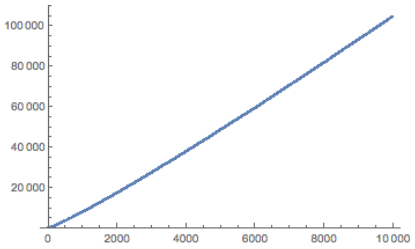
$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, \ldots$$

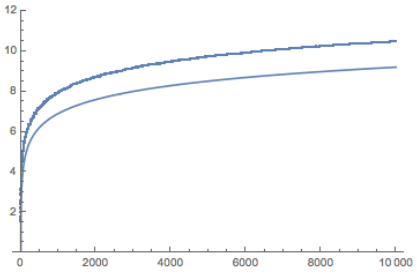
Se trata de una sucesión muy irregular, en el sentido de que no hay forma de predecir exactamente cuándo, al ir enumerando los números naturales, "aparece" el siguiente primo. Puede ocurrir que $p_{n+1} = p_n + 2$ y puede ocurrir que haya que recorrer bastantes números naturales a partir de p_n hasta que aparezca p_{n+1}. La gráfica muestra la sucesión $p_{n+1} - p_n$, y en ella vemos que abundan más las distancias cortas, pero que de vez en cuando se dan también distancias más largas.



[1] En realidad hay una discrepancia entre esta $\zeta_m(s)$ y la función $\zeta_K(s)$ considerada en [TAl], y es que en [TAl 4.23] la función $L(s,\chi)$ se define sustituyendo χ por el carácter primitivo χ_0 que lo induce, y eso hace que la función $L(s,\chi)$ de [TAl] difiera de la que estamos considerando aquí en un número finito de factores $\left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1}$, para primos $p \mid m$, que aparecen en el desarrollo en producto de Euler cuando se emplea χ_0 y valen 1 en nuestro caso, pero dichos factores determinan una función entera que no tiene ni ceros ni polos, por lo que son irrelevantes en la prueba, y eliminarlos es una simplificación más del argumento.



Pese a ello, la sucesión de los números primos presenta una gran regularidad "a gran escala", y muchos resultados de la teoría analítica de números consisten en poner de manifiesto dicha regularidad. Si nos limitamos a representar la sucesión p_n, la imagen resultante es bastante regular, pero esto es engañoso. Lo que sucede es que los saltos de un primo al siguiente son pequeños en relación a la magnitud de los primos, y por ello en la figura no se aprecian las irregularidades. El hecho de que la gráfica parezca recta también es engañoso, ya que se debe a la diferencia de escala entre los ejes. En realidad es una curva cuya pendiente varía lentamente, de modo que si tratáramos de aproximarla por una recta, habría que ir modificando su pendiente a medida que ampliáramos el intervalo representado.



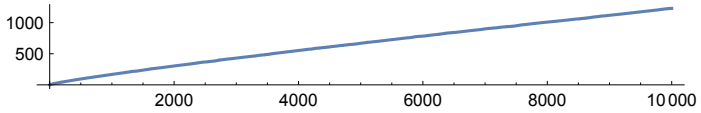
Esto puede verse representando la sucesión p_n/n, que es la pendiente de la recta que une $(0,0)$ con el último par (n,p_n) representado en la gráfica. Como la forma de la gráfica resultante se parece a la de la función $\log x$, hemos representado también esta función (que es la curva inferior). Vemos que, en efecto, la pendiente va variando, pero, por otra parte, encontramos una nueva regularidad, y es el parecido de esta pendiente con la función logaritmo, que no es en absoluto fácil de justificar.

Este parecido está relacionado con una propiedad de la sucesión de los números primos que fue señalada por Gauss. En una carta de 1849 afirmó que ya en 1793 (es decir, a los 16 años) había observado que la densidad del conjunto de los números primos se aproxima a $1/\log x$ para valores grandes de x, y que cada nueva tabla de primos publicada venía a confirmar su conjetura.

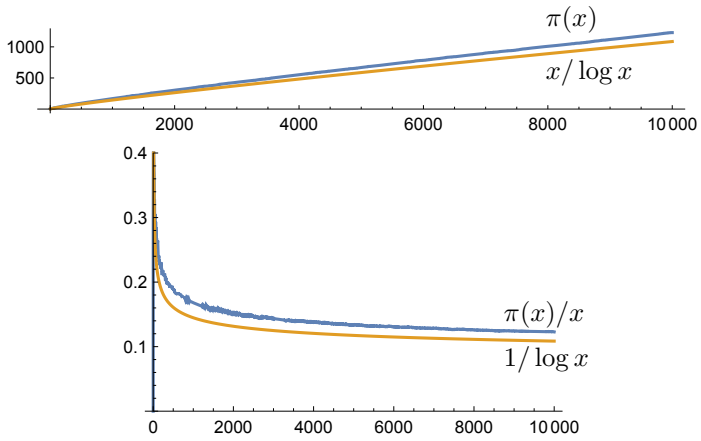
Para formalizar la conjetura de Gauss conviene introducir la función

$$\pi(x) = \sum_{p \leq x} 1$$

que asigna a cada número real x el número de primos menores o iguales que x. He aquí su gráfica:



La densidad de primos en un intervalo $[0,x]$ es $\pi(x)/x$, es decir, el número de primos por unidad de longitud que contiene el intervalo. Según la conjetura de Gauss, esta densidad es aproximadamente $1/\log x$, con lo que a su vez $\pi(x)$ se parecerá a $x/\log x$. Comparemos las gráficas correspondientes:



Vemos que, ciertamente, hay un parecido, si bien no puede interpretarse como que la diferencia entre ambas funciones tiende a 0, pues esto es falso. Lo que se cumple realmente es lo siguiente:

Teorema de los números primos

$$\pi(x) \sim \frac{x}{\log x},$$

donde, en general, la notación $f(x) \sim g(x)$ indica que

$$\lim_{x\to+\infty} \frac{f(x)}{g(x)} = 1.$$

Se dice entonces que las funciones f y g son *asintóticamente equivalentes*. Notemos que esto equivale a que

$$\lim_{x\to+\infty} \frac{f(x)-g(x)}{f(x)} = 0,$$

lo que significa a su vez que el error relativo de aproximar $f(x)$ por $g(x)$ tiende a 0. Discutiremos esta noción con más detalle en la sección 2.2.

Sin embargo, $x/\log x$ no es la función más razonable para aproximar $\pi(x)$. Si de verdad $1/\log x$ aproxima a la densidad de los números primos en cualquier intervalo, a la hora de aproximar el número de primos entre 1 000 y 1 100 será más fiable multiplicar la densidad aproximada $1/\log(1\,100)$ por la longitud del intervalo, o sea, 100, lo cual nos da

$$\frac{100}{\log(1\,100)} = 14.28,$$

en lugar de restar las aproximaciones

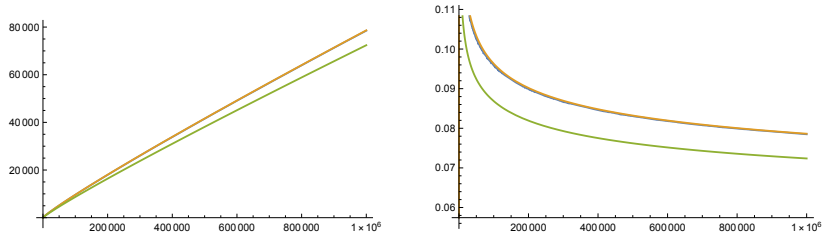
$$\frac{1\,100}{\log(1\,100)} - \frac{1\,000}{\log(1\,000)} = 12.31,$$

pues en este caso usamos la aproximación $1/\log(1\,000)$, que es peor. Efectivamente, hay 16 primos en dicho intervalo.

Más en general, para aproximar el número de primos en un cierto intervalo es más fiable dividirlo en subintervalos pequeños y sumar la aproximación $1/\log x$ en un punto de cada intervalo multiplicada por la longitud de éste. Tomando límites llegamos a la llamada *integral logarítmica*

$$\pi(x) \sim \mathrm{Il}(x) = \int_2^x \frac{dt}{\log t}.$$

Ésta es la aproximación que consideró Gauss. Las gráficas siguientes nos permiten comparar las dos aproximaciones, y vemos que —como era de esperar— la integral logarítmica es mejor:



En la gráfica de la izquierda, la curva superior es la superposición de las funciones $\pi(x)$ e $\mathrm{Il}(x)$, que resultan indistinguibles, mientras que la inferior es $x/\log x$. Similarmente, en la gráfica de la derecha, en la curva superior se superponen $\pi(x)/x$ e $\mathrm{Il}(x)/x$, mientras que la inferior es $1/\log x$. No obstante, cabe recalcar que si las aproximaciones con logaritmos se distinguen claramente de las funciones que pretenden aproximar, ello se debe a que la convergencia de la aproximación es más lenta. Si pudiéramos calcular las gráficas en un intervalo suficientemente grande, las tres curvas serían indistinguibles.

Veamos por último algunos valores numéricos. Gauss trabajó con tablas que llegaban hasta $\pi(3\,000\,000)$. En la tabla de la página siguiente tenemos en el centro $\pi(x)$, a sus lados las aproximaciones $x/\log x$ e $\mathrm{Il}(x)$, el error e para cada una de ellas y el porcentaje de error relativo e_r. La tabla confirma una vez más que la integral logarítmica es una aproximación mucho mejor. Sin embargo, la relación $\pi(x) \sim x/\log x$ es cierta, lo que significa que los errores relativos que muestra la tabla tienden igualmente a 0, aunque haya que tomar valores de x mucho mayores para que se vuelvan realmente despreciables.

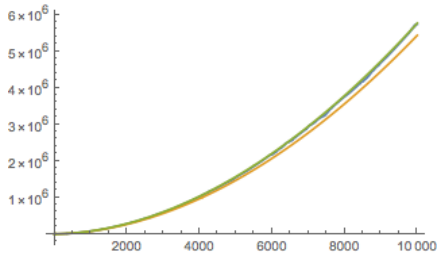
En una memoria de 1859, Riemann dio unas directrices para demostrar el teorema de los números primos, si bien los detalles de su argumento no fueron precisados hasta 1896, cuando aparecieron dos pruebas, una de Jacques Hadamard y otra de Charles Jean de la Vallée-Poussin. Posteriormente se encontraron varias pruebas algo más simples, aunque todas ellas bastante sofisticadas. Selberg y Erdős dieron en 1949 una prueba elemental, en el sentido de que no requería resultados de la teoría de funciones de variable compleja, o análisis funcional en general. Aquí presentaremos una prueba debida a Donald J. Newman de 1980, que sí que usa la teoría de funciones de variable compleja, pero que es muchísimo más simple que cualquier otra prueba conocida.

x	$e_r(\%)$	e	$x/\log x$	$\pi(x)$	$\mathrm{Il}(x)$	e	$e_r(\%)$
10^2	12	3	22	25	29	4	16
10^3	14	23	145	168	176	9	5.4
10^4	12	143	1 086	1 229	1 245	16	1.3
10^5	9.4	906	8 686	9 592	9 628	37	0.39
10^6	7.8	6 115	72 383	78 498	78 626	128	0.16
10^7	6.6	44 158	620 421	664 579	664 917	338	0.05
10^8	5.8	332 773	5 428 682	5 761 455	5 762 208	753	0.013
10^9	5.1	2 592 591	48 254 943	50 847 534	50 849 234	1 700	0.0033
10^{10}	4.6	20 758 030	434 294 482	455 052 512	455 055 613	3 101	0.00068

El teorema de los números primos está relacionado con muchos otros patrones regulares que pueden derivarse de la sucesión de los números primos. Ya hemos señalado uno de ellos, a saber, el parecido de la gráfica de p_n/n con la función $\log x$. Observemos ahora la gráfica de la función[2]

$$\sum_{p\leq x} p,$$

es decir la suma de todos los primos menores o iguales que un número real x dado:

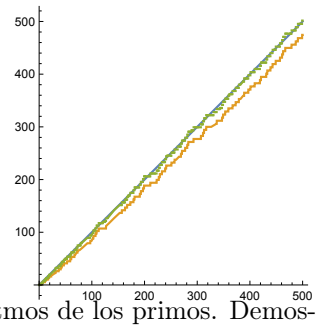


En realidad hemos representado dos funciones más. La segunda es $\mathrm{Il}(x^2)$, cuya gráfica no puede distinguirse en la figura de la de la suma de los primos. La que queda ligeramente por debajo es $\frac{x^2}{2\log x}$. Sucede que para probar que estas dos funciones son asintóticamente equivalentes a la gráfica de la suma de los primos no nos bastará con el teorema de los números primos tal y como lo hemos enunciado, sino que necesitaremos una versión fuerte que estime la diferencia entre $\pi(x)$ e $\mathrm{Il}(x)$.

[2]En lo sucesivo adoptaremos el convenio de que la letra p en un índice de una suma o un producto recorre los números primos.

Veamos por último lo que sucede si, en vez de sumar los primos, sumamos los logaritmos de los primos, es decir, si consideramos la función

$$\vartheta(x) = \sum_{p \le x} \log p.$$



Nuevamente, en la figura hemos representado tres funciones, de las cuales $\vartheta(x)$ es la que queda más abajo. Observemos que los dos ejes están a la misma escala, por lo que esta vez es fácil conjeturar a qué función se aproxima la suma de los logaritmos de los primos. Demostraremos que $\vartheta(x) \sim x$ y, más aún, que esto implica el teorema de los números primos (de hecho, éste es el camino por el que demostraremos el teorema).

Sin embargo, la gráfica contiene una tercera función que apenas se distingue de la diagonal y que resulta ser un refinamiento de ϑ. Es la construida como sigue: dado un número x, por ejemplo $x = 25$, consideramos, no los primos, sino todas las potencias de primo $p^m \le x$, que en este caso son

$$2,\ 3,\ 2^2,\ 5,\ 7,\ 2^3,\ 3^2,\ 11,\ 13,\ 2^4,\ 17,\ 19,\ 23.$$

Ahora eliminamos los exponentes y sumamos los logaritmos de las bases:

$$\log 2 + \log 3 + \log 2 + \log 5 + \log 7 + \log 2 + \log 3 +$$

$$\log 11 + \log 13 + \log 2 + \log 17 + \log 19 + \log 23 = 24.01.$$

Vemos que el resultado aproxima a 25 con un error inferior al 4%. Ésta es la tercera función de la gráfica y vemos en ella que, para valores de x moderadamente grandes, el error de la aproximación se vuelve inferior a nuestra capacidad de discernimiento. Formalmente, la tercera función es

$$\psi(x) = \sum_{n \le x} \Lambda(n),$$

donde Λ es la llamada *función de Mangoldt* [ITAn 7.7], y que viene dada por

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m, \text{ con } m \ge 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Sucede que $\psi(x) \sim x$ y, como vemos, la convergencia es mucho más rápida que la de $\vartheta(x)$. Las funciones ϑ y ψ se conocen como *funciones de Chebyshev,* y las estudiaremos en la sección 3.2. La función de Mangoldt es un ejemplo de las *funciones aritméticas* que estudiamos en la sección [ITAn 7.4] y que abordaremos de nuevo con más detalle en el capítulo II, mientras que en el capítulo III empezaremos a estudiar la distribución de los números primos. En las primeras secciones probaremos algunos resultados elementales, es decir, resultados que pueden probarse sin necesidad de usar el análisis complejo y en la sección 3.5 relacionaremos las funciones aritméticas estudiadas en el capítulo precedente con las series de Dirichlet ya estudiadas en [ITAn] e [IC], lo cual bastará para demostrar el teorema de Dirichlet y el teorema de los números primos en las dos secciones siguientes, y después una versión más precisa del teorema de Dirichlet cuya prueba se basa en el teorema de los números primos.

Se trata de un teorema fácil de conjeturar. Para ello consideremos por ejemplo las cuatro progresiones geométricas de la forma $10x+k$ con $(10,k)=1$, es decir, $k=1,3,7,9$. El teorema de Dirichlet afirma que cada una de ellas contiene infinitos primos. Equivalentemente, es obvio que todo primo distinto de 2 o 5 tiene que terminar en $1,3,5$ o 7 y lo que afirma el teorema es que hay infinitos primos en cada uno de estos cuatro casos. Ahora bien, La tabla siguiente contiene los 23 primos menores que 100 distintos de 2 o 5:

11	31	41	61	71			5	22%
3	13	23	43	53	73	83	7	30%
7	17	37	47	67	97		6	26%
19	29	59	79	89			5	22%

Vemos que están repartidos de forma casi uniforme. Sólo podrían haber estado mejor repartidos si uno de los acabados en 3 hubiera acabado en 1 o en 9. Si consideramos intervalos de primos mayores, el número de primos con cada terminación se aproxima más al 25%:

Hasta	Total	1		3		7		9	
100	23	5	(22%)	7	(30%)	6	(26%)	5	(22%)
1 000	166	40	(24%)	42	(25%)	46	(28%)	38	(23%)
10 000	1 227	306	(24.9%)	310	(25.3%)	308	(25.1%)	303	(24.7%)
100 000	9 590	2 387	(24.9%)	2 402	(25.1%)	2 411	(25.1%)	2 390	(24.9%)

Esto no es casual, sino que se cumple un hecho mucho más general: si $m\geq 2$ y k es un entero primo con m, llamamos $\pi(x)$ al número de primos $p\leq x$ y $\pi_k(x)$ al número de primos $p\leq x$ tales que $p\equiv k \pmod m$. El teorema de Dirichlet sobre primos en progresiones aritméticas equivale a que

$$\lim_{x\to+\infty}\pi_k(x)=+\infty$$

y lo que estamos constatando (y podemos constatar igualmente para cualquier otro valor de m distinto del caso $m=10$ que estamos examinando) es que

$$\lim_{x\to+\infty}\frac{\pi_k(x)}{\pi(x)}=\frac{1}{\phi(m)},$$

donde $\phi(m)$ es la función de Euler que nos da el número de valores posibles de k (en nuestro ejemplo $\phi(10)=4$).

Así pues, no sólo cada progresión aritmética $mx+k$ con $(m,k)=1$ contiene infinitos primos, como afirma el teorema de Dirichlet, sino que se puede constatar que los primos están estadísticamente bien repartidos entre las $\phi(m)$ progresiones correspondientes a un mismo valor de m. Esto es lo que afirma el teorema 3.43.

La prueba original del teorema de los números primos, siguiendo las ideas de Riemann se basaban en una estrecha conexión que existe entre la ahora conocida como función dseta de Riemann y la distribución de los números primos. La función dseta la introdujimos en el capítulo VIII de [ITAn], la estudiamos más

a fondo en el capítulo X de [An] y en el capítulo IV de este libro profundizamos en su estudio. En el capítulo V mostramos la relación entre los ceros de la función dseta y la distribución de los números primos, y en los dos capítulos siguientes demostramos resultados mucho más profundos que aprovechan esta relación. Finalmente, en el capítulo VIII estudiamos varias familias de números compuestos.

Capítulo I

Pruebas de trascendencia

En este primer capítulo presentamos tres resultados notables sobre números trascendentes, ninguno de los cuales será necesario más adelante, salvo por una aplicación del teorema de las seis exponenciales en el capítulo VIII. Cada uno de ellos se apoya en un resultado fundamental de la teoría de las funciones de variable compleja: el teorema de Lindemann-Weierstrass usa el teorema de Cauchy, el teorema de las seis exponenciales usa el principio del módulo máximo, mientras que el teorema de Gelfond-Schneider usa la fórmula integral de Cauchy. (Para otros resultados más elementales véase la sección [ITAn 10.1].)

1.1 El teorema de Lindemann-Weierstrass

En 1873 Hermite demostró la trascendencia del número e. Anteriormente ya se había probado que e no era racional. De hecho, era conocido su desarrollo en fracción continua. En 1882 Lindemann consiguió generalizar el argumento de Hermite y demostró la trascendencia de π. Lindemann afirmó que sus técnicas permitían probar un resultado mucho más general. La primera prueba detallada de este resultado fue publicada por Weierstrass y constituirá el contenido de esta sección, junto con sus consecuencias inmediatas.

Necesitaremos algunos resultados elementales sobre cuerpos numéricos. Recordemos que un cuerpo numérico $K \subset \mathbb{C}$ es una extensión finita de $\mathbb{Q}$ [Al 8.4]. El grado de un cuerpo numérico es su dimensión como $\mathbb{Q}$-espacio vectorial. Si $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son números algebraicos, entonces $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es el menor cuerpo numérico que los contiene, y podemos extenderlo hasta un cuerpo numérico normal K [Al 5.24]. Si K es un cuerpo numérico normal de grado h, esto se traduce en que tiene precisamente h automorfismos [Al 5.36], digamos $\sigma_1, \ldots, \sigma_h$, y un $\alpha \in K$ cumple $\alpha \in \mathbb{Q}$ si y sólo si es fijado por todos ellos [Al 5.32].

Según [Al 5.2], cada $\alpha \in K$ es raíz de un único polinomio mónico irreducible en $\mathbb{Q}[X]$, cuyas raíces (todas ellas simples) son los conjugados de α, es decir, sus imágenes por los automorfismos de K [Al 5.23].

Todo automorfismo σ de K induce un automorfismo $\sigma : K[X] \longrightarrow K[X]$ del anillo de polinomios de K, de modo que un polinomio $p(X) \in K[X]$ queda fijado por σ si y sólo si σ fija a todos sus coeficientes, por lo que $p(X) \in \mathbb{Q}[X]$ si y sólo si es fijado por todos los automorfismos de K.

En cada cuerpo numérico K podemos considerar su anillo de enteros algebraicos [Al 8.5]. Un hecho fundamental sobre ellos es que un $\alpha \in \mathbb{Q}$ es un entero algebraico si y sólo si es un entero ordinario (un entero racional).

Necesitaremos dos resultados auxiliares:

Teorema 1.1 *Sean $f_i(x) \in \mathbb{Z}[x]$, $i = 1, \ldots, r$ polinomios no constantes de grado k_i y, para cada i, sean $\beta_{1i}, \ldots, \beta_{k_i i}$ las raíces de $f_i(x)$. Supongamos que son no nulas. Sean $a_i \in \mathbb{Z}$ para $i = 0, \ldots, r$ tales que $a_0 \neq 0$. Entonces*

$$a_0 + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} e^{\beta_{ki}} \neq 0.$$

Demostración: Supongamos que se cumple la igualdad. Vamos a expresar cada $e^{\beta_{ki}}$ como

$$e^{\beta_{ki}} = \frac{M_{ki} + \epsilon_{ki}}{M_0}, \quad k = 1, \ldots, k_i, \quad i = 1, \ldots, r,$$

donde $M_0 \in \mathbb{Z}$, $M_0 \neq 0$. Entonces, sustituyendo en la igualdad obtendremos que

$$a_0 M_0 + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} + \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} \epsilon_{ki} = 0, \tag{1.1}$$

con $a_0 M_0 \neq 0$.

Vamos a encontrar un primo p tal que $a_0 M_0$ no sea divisible entre p, mientras que la suma

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki}$$

será un número entero múltiplo de p. Por otra parte se cumplirá que

$$\left| \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} \epsilon_{ki} \right| < 1, \tag{1.2}$$

con lo que tendremos una contradicción, pues en (1.1) los dos primeros sumandos son un entero no divisible entre p, luego no nulo, mientras que el tercero tiene módulo menor que 1. Para conseguir todo esto definimos primeramente

$$f(z) = \prod_{i=1}^{r} f_i(z) = b_0 + b_1 z + \cdots + b_N z^N = b_N \prod_{i=1}^{r} \prod_{k=1}^{k_i} (z - \beta_{ki}),$$

donde $N = \sum_{i=1}^{r} k_i$ y $b_0 \neq 0$, ya que las raíces son no nulas. Podemos suponer que $b_N > 0$.

Sea

$$M_0 = \int_0^{+\infty} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz,$$

donde p es un número primo y la integración se realiza sobre el semieje real positivo.

Vamos a probar que la integral es finita y que, si p es suficientemente grande, se trata de un número entero no divisible entre p. Notemos que

$$b_N^{(N-1)p-1} z^{p-1} f^p(z) = b_N^{(N-1)p-1} b_0^p z^{p-1} + \sum_{s=p+1}^{(N+1)p} c_{s-1} z^{s-1},$$

para ciertos coeficientes $c_s \in \mathbb{Z}$, y $b_N b_0 \neq 0$. Por lo tanto

$$\begin{aligned} M_0 &= \frac{b_N^{(N-1)p-1} b_0^p}{(p-1)!} \int_0^{+\infty} z^{p-1} e^{-z}\, dz + \sum_{s=p+1}^{(N+1)p} \frac{c_{s-1}}{(p-1)!} \int_0^{+\infty} z^{s-1} e^{-z}\, dz \\ &= b_N^{(N-1)p-1} b_0^p + \sum_{s=p+1}^{(N+1)p} \frac{(s-1)!}{(p-1)!} c_{s-1} = b_N^{(N-1)p-1} b_0^p + pC, \end{aligned}$$

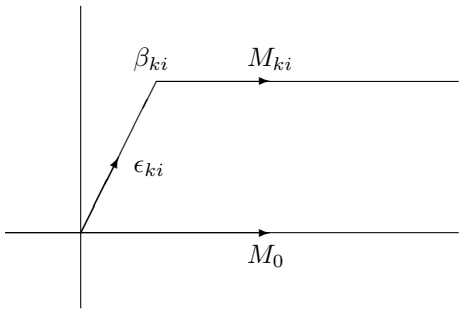
para un cierto $C \in \mathbb{Z}$, donde hemos hecho uso de la identidad de Euler [IC 3.30]

$$n! = \int_0^{+\infty} z^n e^{-z}\, dz.$$

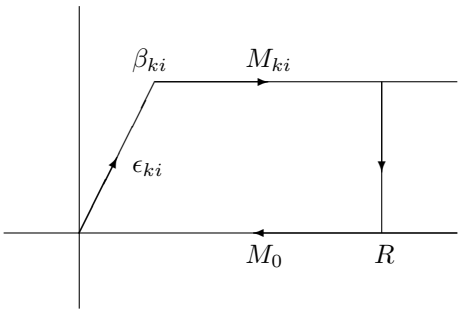
Así, M_0 es entero y si el primo p es mayor que $|a_0|$, b_N, $|b_0|$ entonces $p \nmid a_0 M_0$. Ahora definimos

$$\begin{aligned} M_{ki} &= e^{\beta_{ki}} \int_{\beta_{ki}}^{+\infty} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz, \quad k = 1, \ldots, k_i, \quad i = 1, \ldots, r, \\ \epsilon_{ki} &= e^{\beta_{ki}} \int_0^{\beta_{ki}} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z}}{(p-1)!}\, dz, \quad k = 1, \ldots, k_i, \quad i = 1, \ldots, r, \end{aligned}$$

donde los caminos de integración son los indicados en la figura siguiente:



La finitud de M_{ki} se debe a que, puesto que el integrando es una función entera, por el teorema de Cauchy sabemos que la integral a lo largo de una trayectoria como la de la figura siguiente es nula para todo R suficientemente grande:



Ahora bien, es fácil ver que la integral sobre el segmento vertical tiende a 0 con R, luego la integral que define M_{ki} es finita, y al sumarle la integral que define a ϵ_{ki} da exactamente M_0. Así pues, $M_{ki} + \epsilon_{ki} = e^{\beta_{ki}} M_0$, y tenemos la descomposición buscada.

Si en la definición de M_{ki} descomponemos en factores el polinomio $f(z)$ obtenemos

$$M_{ki} = \int_{\beta_{ki}}^{+\infty} \frac{b_N^{Np-1} z^{p-1} \prod_{j=1}^{r} \prod_{t=1}^{k_j} (z-\beta_{tj})^p e^{-z+\beta_{ki}}}{(p-1)!}\, dz.$$

El camino de integración es $z = u + \beta_{ki}$, luego $dz = du$. Al hacer el cambio la integral se convierte en

$$M_{ki} = \int_0^{+\infty} \frac{b_N^{Np-1} (u+\beta_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (u+\beta_{ki}-\beta_{tj})^p}{(p-1)!}\, du,$$

donde el asterisco en el producto indica que falta el factor $(t,j) = (k,i)$, que hemos extraído como u^p. Podemos redistribuir los coeficientes b^N:

$$M_{ki} = \int_0^{+\infty} \frac{(b_N u + b_N\beta_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + b_N\beta_{ki} - b_N\beta_{tj})^p}{(p-1)!}\, du.$$

Es fácil ver que, puesto que b_N es el coeficiente director de un polinomio cuyas raíces son los β_{ij}, los números $\alpha_{ij} = b_N\beta_{ij}$ son enteros algebraicos. Con esta notación:

$$M_{ki} = \int_0^{+\infty} \frac{(b_N u + \alpha_{ki})^{p-1} u^p e^{-u} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + \alpha_{ki} - \alpha_{tj})^p}{(p-1)!}\, du.$$

Sumando obtenemos que

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} = \int_0^{+\infty} \frac{u^p \Phi(u) e^{-u}}{(p-1)!}\, du,$$

donde

$$\Phi(u) = \sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} (b_N u + \alpha_{ki})^{p-1} \prod_{j=1}^{r} \prod_{t=1}^{k_j}{}^{*} (b_N u + \alpha_{ki} - \alpha_{tj})^p.$$

Si consideramos una cuerpo numérico normal K que contenga a todos los α_{ij}, resulta que un automorfismo de K permuta los números $\alpha_{1i}, \ldots, \alpha_{k_i i}$, y se ve claramente que entonces deja invariante a $\Phi(u)$. Esto significa que $\Phi(u) \in \mathbb{Q}[u]$, y como los α_{ij} son enteros algebraicos, en realidad $\Phi(u) \in \mathbb{Z}[u]$. Digamos que

$$u^p \Phi(u) = \sum_{s=p+1}^{(N+1)p} d_{s-1} u^{s-1}.$$

Entonces

$$\sum_{i=1}^{r} a_i \sum_{k=1}^{k_i} M_{ki} = \sum_{s=p+1}^{(N+1)p} \frac{d_{s-1}}{(p-1)!} \int_0^{+\infty} u^{s-1} e^{-u}\, du = \sum_{s=p+1}^{(N+1)p} d_{s-1} \frac{(s-1)!}{(p-1)!} = pC,$$

para un $C \in \mathbb{Z}$. Sólo queda demostrar (1.2).

Sea R tal que todos los números β_{ij} estén contenidos en el disco de centro 0 y radio R. Llamemos

$$g_{ki} = \max_{|z| \le R} |b_N^{N-2} f(z) e^{-z+\beta_{ki}}|, \quad g = \max_{|z| \le R} |b_N^{N-1} z f(z)|,$$

y sea g_0 el máximo de todos los números g_{ki}. Entonces

$$\begin{aligned} |\epsilon_{ki}| &= \left| \int_0^{\beta_{ki}} \frac{b_N^{(N-1)p-1} z^{p-1} f^p(z) e^{-z+\beta_{ki}}}{(p-1)!}\, dz \right| \\ &\le \frac{1}{(p-1)!} |\beta_{ki}|\, |b_N^{N-2} f(z) e^{-z+\beta_{ki}}|\, |b_N^{N-1} z f(z)|^{p-1} \le g_0 R \frac{g^{p-1}}{(p-1)!}. \end{aligned}$$

Puesto que la última expresión tiende a 0 con p, eligiendo p suficientemente grande podemos garantizar que se cumple (1.2). ∎

El segundo resultado que necesitamos es muy simple:

Teorema 1.2 *Consideremos números* $\sum_{k=1}^{k_i} A_{ki} e^{\alpha_{ki}}$, *donde* $k_i \ge 1$, $i = 1, \ldots, r$, $r \ge 2$, $A_{ki} \in \mathbb{C} \setminus \{0\}$ *y* $\alpha_{1i}, \ldots, \alpha_{k_i i}$ *son números complejos distintos para cada* i. *Si operamos el producto*

$$\prod_{i=1}^{r} \sum_{k=1}^{k_i} A_{ki} e^{\alpha_{ki}} = \sum_{i=1}^{N} B_i e^{\beta_i},$$

donde los exponentes $\beta_1, \ldots, \beta_N$ *son distintos dos a dos (es decir, donde los coeficientes* B_i *se obtienen multiplicando un* A_{ki} *para cada* i *y después sumando todos los productos que acompañan a un mismo exponente), se cumple que alguno de los coeficientes* B_i *es no nulo.*

DEMOSTRACIÓN: Ordenemos los números $\alpha_{1i},\dots,\alpha_{k_i i}$ según el crecimiento de sus partes reales y, en caso de igualdad, según el crecimiento de sus partes imaginarias. Entonces el número $\alpha_{11}+\cdots+\alpha_{1r}$ no puede alcanzarse mediante otra combinación $\alpha_{j_1 1}+\cdots+\alpha_{j_r r}$, pues la parte real de una cualquiera de estas sumas será mayor o igual que la de la primera, y en caso de igualdad la parte imaginaria será mayor. Consecuentemente existe un i de modo que $\beta_i=\alpha_{11}+\cdots+\alpha_{1r}$ y el coeficiente B_i será exactamente $A_{11}\cdots A_{1r}\neq 0$. ∎

Teorema 1.3 (Teorema de Lindemann-Weierstrass) *Si $\alpha_1,\dots,\alpha_n$ son números algebraicos distintos ($n\geq 2$) y $c_1,\dots,c_n$ son números algebraicos no todos nulos, entonces*

$$c_1e^{\alpha_1}+\cdots+c_ne^{\alpha_n}\neq 0.$$

DEMOSTRACIÓN: Supongamos, por el contrario, que

$$c_1e^{\alpha_1}+\cdots+c_ne^{\alpha_n}=0. \tag{1.3}$$

Podemos suponer que todos los coeficientes c_i son no nulos. Multiplicando la ecuación por un número natural suficientemente grande podemos suponer que de hecho son enteros algebraicos. Veremos en primer lugar que también podemos suponer que son enteros racionales.

Sean $c_{i1},\dots,c_{ik_i}$ los conjugados de cada c_i. Entonces

$$\prod_{i_1=1}^{k_1}\cdots\prod_{i_n=1}^{k_n}(c_{1i_1}e^{\alpha_1}+\cdots+c_{ni_n}e^{\alpha_n})=0,$$

pues entre los factores se encuentra (1.3). Operemos el polinomio

$$\prod_{i_1=1}^{k_1}\cdots\prod_{i_n=1}^{k_n}(c_{1i_1}z_1+\cdots+c_{ni_n}z_n)=\sum c_{h_1,\dots,h_n}z_1^{h_1}\cdots z_n^{h_n},$$

donde el último sumatorio se extiende sobre todas las n-tuplas $(h_1,\dots,h_n)$ de números naturales tales que $h_1+\cdots+h_n=N=k_1+\cdots+k_n$.

Si consideramos un cuerpo numérico normal K que contenga a todos los números c_{ij}, resulta que todo automorfismo de K permuta a $c_{i1},\dots,c_{ik_i}$, luego deja invariante a este polinomio, lo que implica que sus coeficientes $c_{h_1,\dots,h_n}$ son números racionales. Como además son enteros algebraicos, tenemos que $c_{h_1,\dots,h_n}\in\mathbb{Z}$.

Sustituimos $z_i=e^{\alpha_i}$ y nos queda

$$\prod_{i_1=1}^{k_1}\cdots\prod_{i_n=1}^{k_n}(c_{1i_1}e^{\alpha_1}+\cdots+c_{ni_n}e^{\alpha_n})=\sum c_{h_1,\dots,h_n}e^{h_1\alpha_1+\cdots+h_n\alpha_n}=\sum_{i=1}^{M}b_ie^{\beta_i},$$

donde los coeficientes b_i son enteros racionales obtenidos sumando los $c_{h_1,\dots,h_n}$ que acompañan a un mismo exponente, es decir, según las hipótesis del teorema anterior, por lo que alguno de ellos es no nulo (y claramente ha de haber al menos dos no nulos). Los números b_i son números algebraicos distintos, luego tenemos una expresión como la original pero con coeficientes enteros.

A partir de ahora suponemos (1.3) con $c_i \in \mathbb{Z}$ y donde $\alpha_1, \ldots, \alpha_n$ son números algebraicos distintos.

Sea $f(x) \in \mathbb{Q}[x]$ el producto de los polinomios mínimos de los números α_i (sin repetir dos veces el mismo factor). Sea $m \geq n$ el grado de f, sean $\gamma_1, \ldots, \gamma_m$ todas las raíces de f. Llamemos $\mu = m(m-1)\ldots(m-n+1)$, al número de n-tuplas posibles $(i_1, \ldots, i_n)$ de números distintos comprendidos entre 1 y m. Entonces

$$\prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = 0,$$

donde el producto recorre las μ citadas n-tuplas. El producto es 0 porque entre sus factores se encuentra (1.3).

Consideremos el polinomio

$$\prod(c_1 z_{i_1} + \cdots + c_n z_{i_n}) = \sum B_{h_1,\ldots,h_m} z_1^{h_1} \cdots z_m^{h_m},$$

donde la suma se extiende sobre las m-tuplas $(h_1, \ldots, h_m)$ de números naturales que suman μ y los coeficientes $B_{h_1,\ldots,h_m}$ son enteros racionales.

La expresión de la izquierda es claramente invariante por permutaciones de las indeterminadas $z_1, \ldots, z_m$, luego los coeficientes $B_{h_1,\ldots,h_m}$ son invariantes por permutaciones de $h_1, \ldots, h_m$. Consecuentemente podemos agrupar así los sumandos:

$$\prod(c_1 z_{i_1} + \cdots + c_n z_{i_n}) = \sum_{k=1}^{r} B_k \sum z_{k_1}^{h_{k1}} \ldots z_{k_m}^{h_{km}},$$

donde r es el número de elementos de un conjunto de m-tuplas $(h_{k1}, \ldots, h_{km})$ de números naturales que suman μ sin que haya dos que se diferencien sólo en el orden, y el segundo sumatorio varía en un conjunto P_k de permutaciones $(k_1, \ldots, k_m)$ de $(1, \ldots, m)$ que dan lugar, sin repeticiones, a todos los monomios posibles $z_{k_1}^{h_{k1}} \ldots z_{k_m}^{h_{km}}$. Sustituimos las indeterminadas por exponenciales y queda

$$\prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = \sum_{k=1}^{r} B_k \sum e^{h_{k1}\gamma_{k_1} + \cdots + h_{km}\gamma_{k_m}} = 0.$$

La definición del conjunto P_k hace que el polinomio

$$\prod\big(x - (h_{k1} z_{k_1} + \cdots + h_{km} z_{k_m})\big)$$

sea invariante por permutaciones de $z_1, \ldots, z_m$, luego

$$F_k(x) = \prod\big(x - (h_{k1}\gamma_{k_1} + \cdots + h_{km}\gamma_{k_m})\big) \in \mathbb{Q}[x].$$

Si llamamos $\gamma_{1k}, \ldots, \gamma_{t_k k}$ a las raíces de $F_k(x)$ (repetidas con su multiplicidad), nuestra ecuación puede escribirse como

$$\prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) = \sum_{k=1}^{r} B_k (e^{\gamma_{1k}} + \cdots + e^{\gamma_{t_k k}}) = 0.$$

Sean $s_i(x) \in \mathbb{Q}[x]$, $i = 1, \ldots, q$ los distintos factores mónicos irreducibles de los polinomios $F_k(x)$. Así cada $F_k(x)$ se expresa como

$$F_k(x) = \prod_{i=1}^{q} s_i^{p_{ik}}(x),$$

para ciertos números naturales p_{ik}.

Sean $\beta_{1i}, \ldots, \beta_{t_i i}$ las raíces de $s_i(x)$ (todas son simples, porque el polinomio es irreducible). Entonces el polinomio $F_k(x)$ tiene p_{ik} veces cada raíz β_{ji}, luego

$$B_k(e^{\gamma_{1k}} + \cdots + e^{\gamma_{t_k k}}) = \sum_{i=1}^{q} p_{ik} B_k(e^{\beta_{1i}} + \cdots + e^{\beta_{t_i i}}).$$

Sumando resulta

$$\begin{aligned} \prod(c_1 e^{\gamma_{i_1}} + \cdots + c_n e^{\gamma_{i_n}}) &= \sum_{k=1}^{r} B_k(e^{\gamma_{1k}} + \cdots + e^{\gamma_{t_k k}}) \\ &= \sum_{i=1}^{q} A_i(e^{\beta_{1i}} + \cdots + e^{\beta_{t_i i}}) = 0, \end{aligned}$$

donde

$$A_i = \sum_{k=1}^{r} p_{ik} B_k \in \mathbb{Z}.$$

Notemos que todos los números β_{ij} son distintos, pues son raíces de polinomios irreducibles distintos. Por construcción, los exponentes β_{ij} son todas las sumas distintas de exponentes γ_{ij} que aparecen al efectuar el producto de la izquierda de la ecuación. Podemos aplicar el teorema anterior y concluir que alguno de los coeficientes A_i es no nulo. Eliminando los nulos podemos suponer que ninguno lo es. En resumen tenemos

$$\sum_{i=1}^{q} A_i(e^{\beta_{1i}} + \cdots + e^{\beta_{t_i i}}) = 0,$$

donde los coeficientes son enteros racionales no nulos y los exponentes de cada sumando son familias de números conjugados correspondientes a polinomios irreducibles distintos $s_i(x)$ de grado t_i. Distinguimos dos casos:

1) Algún $\beta_{ki} = 0$. Pongamos por ejemplo $i = 1$. Esto significa que $s_1(x) = x$, luego además $t_1 = 1$ y la ecuación se reduce a

$$A_1 + \sum_{i=2}^{q} A_i(e^{\beta_{1i}} + \cdots + e^{\beta_{t_i i}}) = 0,$$

donde los exponentes son todos no nulos, y esto contradice al teorema 1.1.

2) Todos los β_{ki} son distintos de 0. Dividimos la ecuación entre $e^{\beta_{k1}}$ para $k = 1, \ldots, t_1$, con lo que obtenemos las ecuaciones

$$\sum_{i=1}^{q} A_i \sum_{t=1}^{t_i} e^{\beta_{ti} - \beta_{k1}} = 0, \quad k = 1, \ldots, t_1.$$

Las sumamos y queda

$$\sum_{i=1}^{q} A_i \sum_{k=1}^{t_1} \sum_{t=1}^{t_i} e^{\beta_{ti}-\beta_{k1}} = 0.$$

En el sumando $i = 1$, los sumandos con $k = t$ valen todos 1. Los separamos:

$$t_1 A_1 + A_1 \sum_{k\neq t} e^{\beta_{ti}-\beta_{k1}} + \sum_{i=2}^{q} A_i \sum_{k=1}^{t_1} \sum_{t=1}^{t_i} e^{\beta_{ti}-\beta_{k1}} = 0,$$

donde en el primer sumatorio k y t varían entre 1 y t_1.

El polinomio

$$g_1(x) = \prod_{k\neq t} \big(x - (\beta_{t1} - \beta_{k1})\big)$$

es invariante por permutaciones de los conjugados β_{k1}, luego sus coeficientes son racionales. Igualmente ocurre con los polinomios

$$g_i(x) = \prod_{k=1}^{t_1} \prod_{t=1}^{t_i} \big(x - (\beta_{ti} - \beta_{k1})\big)$$

para $i = 2, \ldots, q$. Además todos tienen las raíces no nulas.

Llamando $A_0 = t_1 A_1 \neq 0$, $k_1 = t_1(t_1 - 1)$, $k_i = t_1 t_i$ para $i = 2, \ldots, q$ y $\alpha_{1i}, \ldots, \alpha_{k_i i}$ a las raíces de $g_i(x)$, la ecuación se convierte en

$$A_0 + \sum_{i=1}^{q} A_i \sum_{k=1}^{k_i} e^{\alpha_{ki}} = 0,$$

que contradice al teorema 1.1. ∎

Ejercicio: Probar que si $\alpha_1, \ldots, \alpha_n$ son números algebraicos linealmente independientes sobre $\mathbb{Q}$ entonces $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\mathbb{Q}$, es decir, no son raíces de ningún polinomio $P(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ no nulo.

Algunas consecuencias inmediatas son las siguientes:

1. *Si $\alpha \neq 0$ es un número algebraico, entonces e^α es un número trascendente. En particular el número e es trascendente.*

   En efecto, si $c = e^\alpha$ fuera algebraico, tendríamos $e^\alpha - ce^0 = 0$, en contradicción con el teorema de Lindemann-Weierstrass.

2. *El número π es trascendente.*

   Si π fuera algebraico también lo sería $i\pi$, y el número $e^{i\pi} = -1$ sería trascendente.

3. *Si $\alpha \neq 1$ es un número algebraico, entonces $\log \alpha$ es trascendente.*

   Si $\beta = \log \alpha \neq 0$ fuera algebraico, entonces $\alpha = e^\beta$ sería trascendente.

4. *Si $\alpha \neq 0$ es un número algebraico, entonces* $\operatorname{sen}\alpha$, $\cos\alpha$, $\tan\alpha$ *son números trascendentes.*

   Si $\beta = \operatorname{sen}\alpha = (e^{i\alpha} - e^{-i\alpha})/2i$ fuera algebraico, entonces

   $$e^{i\alpha} - e^{-i\alpha} - 2i\beta e^0 = 0,$$

   en contradicción con el teorema de Lindemann-Weierstrass. Igualmente con el coseno.

   Si $\beta = \tan\alpha = (e^{i\alpha} - e^{-i\alpha})/(e^{i\alpha} + e^{-i\alpha})$ fuera algebraico, entonces

   $$(\beta - 1)e^{i\alpha} + (\beta + 1)e^{-i\alpha} = 0,$$

   en contradicción con el teorema de Lindemann-Weierstrass.

Ejercicio: Probar que las funciones arcsen, arccos y arctan toman valores trascendentes sobre números algebraicos (salvo casos triviales).

1.2 El teorema de las seis exponenciales

En esta sección demostraremos una curiosa prueba de trascendencia que no garantiza la trascendencia de ningún número en particular:

Teorema 1.4 (de las seis exponenciales) *Sean x_1, x_2 e y_1, y_2, y_3 dos conjuntos de números complejos linealmente independientes sobre $\mathbb{Q}$. Entonces al menos una de las seis exponenciales*

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_1y_3}, e^{x_2y_1}, e^{x_2y_2}, e^{x_2y_3}$$

es trascendente.

Notemos que la hipótesis es que x_1, x_2 son linealmente independientes, por una parte, y que y_1, y_2, y_3 también lo son, pero no exigimos que los cinco números lo sean conjuntamente.

El hecho de que los exponentes sean productos es fundamental. Por ejemplo, si $p_1, \ldots, p_n$ son primos distintos, se cumple que los números $\log p_1, \ldots, \log p_n$ son linealmente independientes sobre $\mathbb{Q}$, pues en caso contrario existirían números racionales tales que $m_1 \log p_1 + \cdots + m_n \log p_n = 0$, y de hecho podemos suponer que son enteros, pero entonces $p_1^{m_1} \cdots p_n^{m_n} = 1$, y pasando al miembro derecho las potencias con exponente negativo tenemos una contradicción con la factorización única de $\mathbb{Z}$. Sin embargo ninguna de la exponenciales $e^{\log p_1}, \ldots, e^{\log p_n}$ es trascendente.

Una aplicación destacada del teorema se obtiene tomando $x_1 = 1$, $x_2 = \alpha$ irracional, $y_1 = \log p$, $y_2 = \log q$, $y_3 = \log r$, donde p, q, r son tres primos distintos. Entonces concluimos que alguno de los números

$$p, \quad q, \quad r, \quad p^\alpha, \quad q^\alpha, \quad r^\alpha$$

es trascendente. Como los tres primeros no lo son, la conclusión es que, de las infinitas potencias

$$2^\alpha, \quad 3^\alpha, \quad 5^\alpha, \quad 7^\alpha, \ldots$$

a lo sumo dos son algebraicas, mientras que todas las demás son trascendentes. Una ligera variante de interés es la siguiente:

Teorema 1.5 *Si p, q, r son primos distintos y $\alpha \in \mathbb{R}$ cumple que p^α, q^α, r^α son números racionales, entonces $\alpha \in \mathbb{Z}$.*

DEMOSTRACIÓN: Por la discusión precedente α tiene que ser racional, o de lo contrario una de las potencias sería trascendente. Ahora bien, si $\alpha = m/n$, donde la fracción es irreducible, entonces $p^{m/n} = \sqrt[n]{p^m}$ es un número irracional, salvo que $n = 1$, luego $\alpha = m \in \mathbb{Z}$. ∎

La conjetura de las cuatro exponenciales Si en el enunciado del teorema de las seis exponenciales sustituimos y_1, y_2, y_3 por y_1, y_2, tenemos la *conjetura de las cuatro exponenciales,* que, como su nombre indica, no se sabe si es cierta o no. Si es cierta, en el la hipótesis del teorema anterior basta considerar dos potencias en lugar de tres. ∎

Las primeras pruebas del teorema fueron publicadas por S. Lang y K. Ramachandra, si bien un caso particular fue probado por Alaoglu y Erdős en 1944 en un artículo en el que afirmaban que Siegel conocía una prueba.

Vamos a necesitar algunos resultados adicionales sobre cuerpos numéricos. Si K es un cuerpo numérico normal[1] de grado h y $\sigma_1, \ldots, \sigma_h$ son sus automorfismos, podemos definir la norma y la traza [Al 5.39]:

$$\mathrm{N} : K \longrightarrow \mathbb{Q}, \qquad \mathrm{Tr} : K \longrightarrow \mathbb{Q}$$

mediante $\mathrm{N}(\alpha) = \sigma_1(\alpha) \cdots \sigma_h(\alpha)$, $\mathrm{Tr}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_h(\alpha)$. La traza define a su vez una forma bilineal [Al 8.1] $K \times K \longrightarrow \mathbb{Q}$ dada por $(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha\beta)$, de modo que si $\alpha_1, \ldots, \alpha_h$ es una $\mathbb{Q}$-base de K, podemos considerar su base dual $\beta_1, \ldots, \beta_h$, caracterizada por que

$$\mathrm{Tr}(\alpha_i\beta_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Así, si $\alpha = a_1\alpha_1 + \cdots + a_h\alpha_h$ es un elemento arbitrario de K, tenemos que $a_i = \mathrm{Tr}(\alpha\beta_i)$. Definimos $\overline{|\alpha|}$ como el máximo de los módulos de los conjugados de α, y así

$$|a_i| = |\,\mathrm{Tr}(\alpha\beta_i)| \leq h\overline{|\alpha\beta_i|} \leq h\overline{|\beta_i|}\,\overline{|\alpha|}.$$

Fijamos la base $\alpha_1, \ldots, \alpha_h$ con la condición adicional de que sea una entera [Al 8.15], es decir, una base del anillo de los enteros de K como $\mathbb{Z}$-módulo. Así, si llamamos c_K al producto de h por el máximo de los módulos de los conjugados

[1] En realidad la hipótesis de normalidad no es necesaria.

de los elementos de su base dual, tenemos que las coordenadas de un $\alpha \in K$ en dicha base están acotadas por:

$$|a_i| \leq c_K \overline{|\alpha|}.$$

Por último, si $\alpha \in K$ es entero no nulo, todos sus conjugados también lo son, luego también lo es $\mathrm{N}(\alpha)$ y, al ser también un número racional, es un entero racional. Por consiguiente:

$$1 \leq |\,\mathrm{N}(\alpha)| \leq \overline{|\alpha|}^{h-1}|\alpha|. \tag{1.4}$$

Aquí hemos acotado por $\overline{|\alpha|}$ todos los conjugados de α excepto él mismo.

Vamos a necesitar una generalización del siguiente resultado elemental:

Teorema 1.6 (Lema de Siegel) *Sea (a_{jk}) una matriz $M \times N$ con coeficientes enteros racionales tal que $M < N$ y de modo que todos los coeficientes estén acotados en módulo por $A \geq 1$. Entonces el sistema de ecuaciones lineales*

$$a_{j1}x_1 + \cdots + a_{jN}x_N = 0, \quad 1 \leq j \leq M,$$

tiene una solución entera no trivial tal que

$$|x_k| \leq (NA)^{M/(N-M)},$$

para $1 \leq k \leq N$.

Demostración: Para cada N-tupla de enteros racionales $(x_1, \ldots, x_N)$ consideremos la M-tupla de enteros racionales $(y_1, \ldots, y_M)$ dada por

$$y_j = a_{j1}x_1 + \cdots + a_{jN}x_N, \quad 1 \leq j \leq M.$$

Sea $H = \mathrm{E}\big((NA)^{M/(N-M)}\big)$, donde E representa la parte entera. De este modo, $(NA)^{M/(N-M)} < H + 1$, luego $NA < (H+1)^{(N-M)/M}$,

$$NAH + 1 \leq NA(H+1) < (H+1)^{N/M},$$

luego tenemos que $(NAH+1)^M < (H+1)^N$.

Sea $(x_1, \ldots, x_N)$ tal que $0 \leq x_k \leq H$ para $1 \leq k \leq N$. Sea $-B_j$ la suma de los a_{jk} negativos y C_j la suma de los a_{jk} positivos. Entonces

$$B_j + C_j = |a_{j1}| + \cdots + |a_{jN}| \leq NA,$$

y claramente $-B_jH \leq y_j \leq C_jH$.

Ahora bien, el número de N-tuplas $(x_1, \ldots, x_N)$ tales que $0 \leq x_k \leq H$ es $(H+1)^N$, mientras que sus M-tuplas asociadas $(y_1, \ldots, y_M)$ varían en un conjunto de a lo sumo $(C_jH + B_jH + 1)^M \leq (NAH+1)^M < (H+1)^N$ elementos, luego tiene que haber dos N-tuplas distintas con la misma imagen. Su diferencia cumple el teorema. ∎

Ahora generalizamos el resultado para matrices de enteros algebraicos:

Teorema 1.7 *Sea (α_{kl}) una matriz $p \times q$ con coeficientes enteros en un cuerpo numérico K tal que $p < q$ y de modo que $\overline{|\alpha_{kl}|} \leq A$. Entonces el sistema de ecuaciones lineales*

$$\alpha_{k1}\xi_1 + \cdots + \alpha_{kq}\xi_q = 0, \quad 1 \leq k \leq p,$$

tiene una solución entera (en K) no trivial tal que $\overline{|\xi_l|} \leq c(cqA)^{p/(q-p)}$, para $1 \leq l \leq q$, donde c es una constante que depende de K y de una base entera $\beta_1, \ldots, \beta_h$ de K, pero no de la matriz.

DEMOSTRACIÓN: : Para cualquier q-tupla $(\xi_1, \ldots, \xi_q)$ de enteros de K consideremos sus coordenadas

$$\xi_l = x_{l1}\beta_1 + \cdots + x_{lh}\beta_h, \quad 1 \leq l \leq q,$$

donde $x_{l1}, \ldots, x_{lh}$ son enteros racionales.

Sea

$$\alpha_{kl}\beta_r = a_{klr1}\beta_1 + \cdots + a_{klrh}\beta_h, \quad 1 \leq k \leq p,\ 1 \leq l \leq q,\ 1 \leq r \leq h.$$

Entonces

$$\begin{aligned} \sum_{l=1}^{q} \alpha_{kl}\xi_l &= \sum_{l=1}^{q} \alpha_{kl} \sum_{r=1}^{h} x_{lr}\beta_r = \sum_{r=1}^{h} \sum_{l=1}^{q} x_{lr} \sum_{u=1}^{h} a_{klru}\beta_u \\ &= \sum_{u=1}^{h} \Big(\sum_{r=1}^{h} \sum_{l=1}^{q} a_{klru}x_{lr} \Big)\beta_u, \end{aligned}$$

luego $(\xi_1, \ldots, \xi_q)$ será solución del sistema de ecuaciones si y sólo si las coordenadas $(x_{l1}, \ldots, x_{lh})$ son solución del sistema de $M = hp$ ecuaciones con $N = hq$ incógnitas

$$\sum_{r=1}^{h} \sum_{l=1}^{q} a_{klru}x_{lr} = 0, \quad 1 \leq u \leq h, \quad 1 \leq k \leq p.$$

Según hemos observado, existe una constante c' tal que

$$|a_{klru}| \leq c' \overline{|\alpha_{kl}\beta_r|} \leq c' \max_{1 \leq i \leq h} \overline{|\beta_i|} A = c''A.$$

Por el teorema anterior este sistema de ecuaciones tiene una solución entera no trivial tal que

$$|x_{lr}| \leq (hqc''A)^{p/(q-p)}, \quad 1 \leq l \leq q, \quad 1 \leq r \leq h.$$

Los $(\xi_1, \ldots, \xi_q)$ con estas coordenadas son enteros de K no todos nulos que cumplen el sistema de ecuaciones y además

$$\begin{aligned} \overline{|\xi_l|} &\leq |x_{l1}|\,\overline{|\beta_1|} + \cdots + |x_{lh}|\,\overline{|\beta_h|} \leq \max_{1 \leq i \leq h} \overline{|\beta_i|}(|x_{l1}| + \cdots + |x_{lh}|) \\ &\leq hc''(hqc''A)^{p/(q-p)} = c(cqA)^{p/(q-p)}. \end{aligned}$$

■

Finalmente generalizamos el teorema para matrices de números algebraicos, no necesariamente enteros. Si $\alpha_1, \dots, \alpha_n$ son números algebraicos, el conjunto de los enteros algebraicos m tales que $m\alpha_1, \dots, n\alpha_m$ son enteros algebraicos es claramente un ideal no nulo en $\mathbb{Z}$. A su generador positivo d lo llamaremos el *mínimo común denominador* de los números dados.

Teorema 1.8 *Sea (α_{kl}) una matriz $p \times q$ con coeficientes en un cuerpo numérico K tal que $p < q$ y de modo que $\overline{|\alpha_{kl}|} \leq A$. Entonces el sistema de ecuaciones lineales*

$$\alpha_{k1}\xi_1 + \cdots + \alpha_{kq}\xi_q = 0, \quad 1 \leq k \leq p,$$

tiene una solución entera (en K) no trivial tal que $\overline{|\xi_l|} \leq c(cqdA)^{p/(q-p)}$, para $1 \leq l \leq q$, donde d es una cota del mínimo común denominador de los coeficientes de cada ecuación y c es una constante que depende de K y de una base entera $\beta_1, \dots, \beta_h$, pero no de la matriz.

Demostración: Si d_k es el mínimo común denominador de la ecuación k-ésima, la multiplicamos por d_k, con lo que pasa a tener coeficientes enteros algebraicos con $\overline{|d_k\alpha_{kl}|} \leq dA$, y basta aplicar el teorema anterior. ∎

Demostración (del teorema de las seis exponenciales): Supongamos que las seis exponenciales del enunciado son algebraicas y sea K un cuerpo numérico normal que las contenga todas. Sea d el mínimo común denominador de todos ellos. Vamos a considerar una función de la forma

$$F(z) = \sum_{i,j=1}^{r} a_{ij} e^{(ix_1 + jx_2)z},$$

donde los a_{ij} serán enteros de K que vamos a elegir de modo que F se anule en todos los puntos de la forma

$$k_1y_1 + k_2y_2 + k_3y_3, \qquad 1 \leq k_i \leq n,$$

para un cierto n elegido adecuadamente, al igual que r.

Las condiciones $F(k_1y_1 + k_2y_2 + k_3y_3) = 0$ forman un sistema de n^3 ecuaciones lineales con r^2 incógnitas (las a_{ij}). Pretendemos aplicar el teorema anterior, por lo que necesitamos que $r^2 > n^3$. Concretamente, tomaremos $r^2 = (4n)^3$, Notemos que siempre podemos encontrar números que cumplan esto con n arbitrariamente grande. Los coeficientes del sistema de ecuaciones son los números algebraicos

$$(e^{x_1y_1})^{ik_1}(e^{x_1y_2})^{ik_2}(e^{x_1y_3})^{ik_3}(e^{x_2y_1})^{jk_1}(e^{x_2y_2})^{jk_2}(e^{x_2y_3})^{jk_3}$$

cuyo mínimo común denominador está acotado por d^{6rn} y, si e^{c_0} es una cota[2] de los conjugados de las seis exponenciales $e^{x_uy_v}$, entonces los conjugados de los coeficientes están acotados por e^{c_0rn}. Así, el teorema anterior nos da que

[2]En lo sucesivo $c_0, c_1, \dots$ serán constantes independientes de r y n.

existen enteros $a_{ij} \in K$ que hacen que F tenga los ceros requeridos y de modo que

$$\overline{|a_{ij}|} \le C(Cr^2 d^{6rn} e^{c_0 rn})^{n^3/(r^2-n^3)} = C(4Cn^3 d^{6rn} e^{c_0 rn})^{1/63} \le e^{c_1 n^{5/2}}.$$

Detallamos la última desigualdad, si bien en lo sucesivo omitiremos estas comprobaciones rutinarias: Teniendo en cuenta que $r = 8n^{3/2}$, tenemos que

$$\log \overline{|a_{ij}|} \le \log C + \frac{1}{63}\log 4C + 3\log n + 48 \log d\, n^{5/2} + 8c_0\, n^{5/2},$$

es decir,

$$\log \overline{|a_{ij}|} \le C_1 + C_2 \log n + C_3 n^{5/2} = \left(\frac{C_1}{n^{5/2}} + C_2 \frac{\log n}{n^{5/2}} + C_3\right) n^{5/2},$$

y la expresión entre paréntesis tiende a C_3, luego está acotada por una constante c_1.

Como x_1, x_2 son linealmente independientes sobre $\mathbb{Q}$, los coeficientes $ix_1 + jx_2$ son distintos dos a dos, luego el polinomio

$$P(X) = \sum_{i,j=1}^{r} a_{ij} X^{(ix_1+jx_2)}$$

no es idénticamente nulo, luego no puede anularse en todos los números e^z (en todos los números complejos no nulos) luego la función $F(z)$ no puede ser idénticamente nula.

Además F toma valores en K sobre el conjunto $R = \langle y_1, y_2, y_3\rangle_{\mathbb{Z}}$. Este conjunto no puede ser discreto, porque entonces sería un retículo [TAl 3.7] y tendría a lo sumo rango 2 sobre $\mathbb{Z}$, pero tiene rango 3. Por el principio de prolongación analítica F no puede anularse sobre todos los puntos de R.

Sea s el mayor natural tal que $F(k_1y_1 + k_2y_2 + k_3y_3) = 0$ para todos los coeficientes $1 \le k_i \le s$. Por construcción $s \ge n$. Sea $w = k_1y_1 + k_2y_2 + k_3y_3$ tal que $F(w) \ne 0$ con $1 \le k_i \le s+1$, necesariamente con algún $k_i = s+1$. Entonces $d^{6r(s+1)}F(w)$ es entero (y no nulo) en K, luego

$$|\,\mathrm{N}(d^{6r(s+1)}F(w))| \ge 1.$$

Por otra parte,

$$\overline{|F(w)|} \le r^2 e^{c_1 n^{5/2} + c_0(s+1)r} \le e^{c_1 s^{5/2}}.$$

Si h es el grado de K, usando (1.4) obtenemos que

$$1 \le d^{6r(s+1)h}|\,\mathrm{N}(F(w))| \le d^{16hs^{3/2}} e^{c_1(h-1)s^{5/2}}|F(w)| \le e^{c_2 s^{5/2}}|F(w)|.$$

Así $|F(w)| \ge e^{-c_2 s^{5/2}}$, o también

$$\log|F(w)| \ge -c_2 s^{5/2}.$$

Por otro lado,

$$F(w) = \lim_{z\to w} F(z) \prod_{1\le k_1,k_2,k_3\le s} \frac{w-(k_1y_1+k_2y_2+k_3y_3)}{z-(k_1y_1+k_2y_2+k_3y_3)},$$

donde la función del miembro derecho es entera, ya que los polos simples del producto se cancelan con ceros de F. Consideremos el disco de centro 0 y radio $R = s^{3/2}$.

Notemos que $|w| \le 3(s+1)\,\text{máx}\{|y_i|\}$, por lo que, tomando n es suficientemente grande (y, por consiguiente, s también), podemos exigir que $|w| < R$. Más aún, podemos exigir que si $|z| = R$ y $1 \le k_i \le s+1$, entonces

$$|z-(k_1y_1+k_2y_2+k_3y_3)| \ge R/2.$$

Por otra parte, también $|w-(k_1y_1+k_2y_2+k_3y_3)| \le 3(s+1)\,\text{máx}\{|y_i|\}$. Llamemos F_R al máximo de F en $\partial D(0,R)$. Por el principio del módulo máximo, tenemos que $|F(w)|$ está acotado por el supremo de la función del miembro derecho en $\partial D(0,R)$, es decir,

$$|F(w)| \le F_R(c_2 s/s^{3/2})^{s^3} = F_R(c_2/s^{1/2})^{s^3},$$

luego

$$\log|F(w)| \le \log F_R + s^3(\log c_2 - \tfrac{1}{2}\log s).$$

Nos falta estimar F_R, que depende de s:

$$F_R \le r^2 e^{c_1 n^{5/2}} e^{c_3 rR} \le 16n^3 e^{c_1 n^{5/2} + c_3 8 n^{3/2} s^{3/2}} \le e^{c_4 s^3}.$$

En total hemos obtenido que

$$-c_2 s^{5/2} \le c_4 s^3 + s^3 \log c_2 - s^3 \tfrac{1}{2}\log s,$$

luego $s^3 \log s \le c_5 s^3$, o también, $\log s \le c_5$, lo cual es absurdo. ∎

1.3 El teorema de Gelfond-Schneider

Entre los famosos problemas planteados por Hilbert a principios de siglo, el séptimo consistía en determinar el carácter algebraico o trascendente de ciertos números concretos, tales como la constante de Euler. Entre otras cosas Hilbert preguntaba si en general α^β es un número trascendente cuando α y β son números algebraicos, $\alpha \ne 0$, 1 y β es irracional (en los casos exceptuados α^β es obviamente algebraico). Por α^β se entiende $e^{\beta\log\alpha}$, donde $\log\alpha$ es *cualquier* logaritmo complejo de α. Esta parte del séptimo problema fue demostrada independientemente por Gelfond y Schneider en 1934. De este hecho se sigue en particular que los números $2^{\sqrt{2}}$ o $e^\pi = (-1)^{-i}$ son trascendentes.

Teorema 1.9 (Gelfond-Schneider) *Si α y β son números algebraicos tales que $\alpha \ne 0$, 1 y β es irracional, entonces el número α^β es trascendente.*

DEMOSTRACIÓN: Fijemos un valor para $\log\alpha$ y supongamos que $\gamma = e^{\beta\log\alpha}$ es algebraico. Sea K un cuerpo numérico de grado h que contenga a α, β y γ. Sean $m = 2h+2$ y $n = q^2/(2m)$, donde $t = q^2$ es un múltiplo de $2m$.

Notemos que podemos tomar valores para n arbitrariamente grandes en estas condiciones. En lo sucesivo las letras c, c_1, c_2, ... representarán constantes que dependerán de K, de una base entera de K prefijada y de α, β, γ, pero nunca de n.

Sean $\rho_1, \ldots, \rho_t$ los números $(a+b\beta)\log\alpha$, con $1 \le a \le q$, $1 \le b \le q$. Observemos que, como β es irracional, los números 1 y β son linealmente independientes, luego los números $\rho_1, \ldots, \rho_t$ son distintos dos a dos.

Sean $\eta_1, \ldots, \eta_t$ números complejos en K arbitrarios. Consideremos la función entera dada por $R(z) = \eta_1 e^{\rho_1 z} + \cdots + \eta_t e^{\rho_t z}$. Consideremos las mn ecuaciones lineales con $t = 2mn$ incógnitas $(\eta_1, \ldots, \eta_t)$

$$(\log\alpha)^{-k} R^{k)}(l) = 0, \quad 0 \le k \le n-1, \quad 1 \le l \le m.$$

Los coeficientes de la ecuación (k,l) son los números

$$(\log\alpha)^{-k}\rho_i^k e^{\rho_i l} = (\log\alpha)^{-k}\big((a+b\beta)\log\alpha\big)^k e^{l(a+b\beta)\log\alpha} = (a+b\beta)^k \alpha^{al}\gamma^{bl} \in K,$$

con $1 \le l \le m$, $1 \le a, b \le q$, $0 \le k \le n-1$.

Sea c_1 un número natural no nulo tal que $c_1\alpha$, $c_1\beta$ y $c_1\gamma$ sean enteros en K. En cada coeficiente, al desarrollar el binomio $(a+b\beta)^k$ aparecen monomios de α, β y γ con grado a lo sumo

$$k + al + bl \le n - 1 + mq + mq \le n + 4m^2 n = (4m^2+1)n,$$

luego si multiplicamos cualquiera de los coeficientes por $c_1^{4(m^2+1)n} = c_2^n$ obtenemos un entero de K. El módulo de los conjugados de los coeficientes multiplicados por c_2^n es a lo sumo

$$|c_2^n (a+b\beta^{(i)})^k (\alpha^{(i)})^{al} (\gamma^{(i)})^{bl}| \le c_2^n (a+b\overline{|\beta|})^k \,\overline{|\alpha|}^{al}\,\overline{|\gamma|}^{bl}$$

$$\le c_2^n (q+q\overline{|\beta|})^{n-1}\,\overline{|\alpha|}^{mq}\,\overline{|\gamma|}^{mq} \le c_2^n \big(\sqrt{2m}\sqrt{n} + \sqrt{2m}\sqrt{n}\,\overline{|\beta|}\big)^{n-1} \overline{|\alpha|}^{2m^2 n}\,\overline{|\gamma|}^{2m^2 n}$$

$$\le c_2^n \big(\sqrt{2m} + \sqrt{2m}\,\overline{|\beta|}\big)^n \overline{|\alpha|}^{2m^2 n}\,\overline{|\gamma|}^{2m^2 n}\,\sqrt{n}^{\,n-1} = c_3^n\, n^{(n-1)/2}.$$

Podemos aplicar el teorema 1.7, que nos garantiza que $\eta_1, \ldots, \eta_t$ pueden elegirse de modo que sean enteros en K, no todos nulos, satisfagan las $2t$ ecuaciones (multiplicadas o no por c_2^n, da igual) y además

$$\begin{aligned} \overline{|\eta_k|} &\le c(c\,2t\,c_3^n\, n^{(n-1)/2}) \le 2c^2 t\, c_3^n\, n^{(n-1)/2} \\ &\le 4m\,c^2\, n\, c_3^n\, n^{(n-1)/2} \le c_4^n\, n^{(n+1)/2}, \end{aligned} \tag{1.5}$$

para $1 \le k \le t$.

A partir de ahora consideramos la función $R(z)$ para estos $\eta_1, \dots, \eta_t$. En primer lugar, $R(z)$ no puede ser idénticamente nula, pues desarrollándola en serie de Taylor en el origen resultaría entonces que

$$\eta_1\rho_1^k + \cdots + \eta_t\rho_t^k = 0, \quad \text{para } k = 0, 1, 2, 3, \dots$$

pero las t primeras ecuaciones son un sistema de ecuaciones lineales en $\eta_1, \dots, \eta_t$ cuyo determinante es de Vandermonde, luego es no nulo, puesto que $\rho_1, \dots, \rho_t$ son distintos dos a dos. Esto implica que $\eta_1 = \cdots = \eta_t = 0$, lo cual es falso.

En resumen tenemos que la función $R(z)$ es no nula pero tiene sus $n-1$ primeras derivadas nulas en los puntos $l = 1, \dots, m$.

Existe, pues, un natural $r \geq n$ tal que $R^{k)}(l) = 0$ para $0 \leq k \leq r-1$, $1 \leq l \leq m$ y $R^{r)}(l_0) \neq 0$ para un cierto l_0 tal que $1 \leq l_0 \leq m$.

Llamemos $\rho = (\log\alpha)^{-r} R^{r)}(l_0) \neq 0$. El mismo análisis que hemos realizado antes sobre los coeficientes del sistema nos da ahora que $\rho \in K$ y que $c_1^{r+2mq}\rho$ es un entero en K.

Así pues, $1 \leq |\,\mathrm{N}(c_1^{r+2mq}\rho)| = c_1^{h(r+2mq)}|\,\mathrm{N}(\rho)|$, luego

$$|\,\mathrm{N}(\rho)| \geq c_1^{-h(r+2mq)} > c_5^{-r}. \tag{1.6}$$

Por otro lado tenemos que ρ es una suma de t términos, cada uno de los cuales es el producto de un η_k, para el que tenemos la cota (1.5), y de un coeficiente de la forma $(a+b\beta)^r\alpha^{al_0}\gamma^{bl_0}$, cuyos conjugados están acotados por

$$(a+b\overline{|\beta|})^r\,\overline{|\alpha|}^{al_0}\,\overline{|\gamma|}bl_0 \leq (q+q\overline{|\beta|})^r\,\overline{|\alpha|}^{mq}\,\overline{|\gamma|}^{mq} \leq (c_6q)^r c_7^q.$$

Consecuentemente $\overline{|\rho|} \leq t\,c_4^n\,n^{(n+1)/2}(c_6q)^r c_7^q$.

Ahora acotamos $t = q^2 = 2mn \leq 2mr$, $n \leq r$, $q \leq \sqrt{2m}\sqrt{n} \leq \sqrt{2m}\,r^{1/2}$ y llegamos a

$$\overline{|\rho|} \leq 2mr\,c_4^r\,r^{(r+1)/2}\,c_6^r\big(\sqrt{2m}\big)^r r^{r/2} c_7^{2mr} \leq c_8^r\,r^{r+3/2}. \tag{1.7}$$

Vamos a obtener una cota más fina para $|\rho|$. Para ello aplicaremos la fórmula integral de Cauchy a la función

$$S(z) = r!\frac{R(z)}{(z-l_0)^r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r.$$

Puesto que las derivadas de R anteriores al orden r son nulas en $z = 1, \dots, m$, la función S es entera. Además

$$\rho = (\log\alpha)^{-r}R^{r)}(l_0) = (\log\alpha)^{-r}S(l_0) = (\log\alpha)^{-r}\frac{1}{2\pi i}\int_C \frac{S(z)}{z-l_0}\,dz,$$

donde C es la circunferencia $|z| = m(1+r/q)$, que contiene a los números $1, \dots, m$, en particular a l_0. Para los puntos $z \in C$ tenemos las cotas

$$\begin{aligned}
|R(z)| &\leq t\,c_4^n\,n^{(n+1)/2}\exp\big((q+q|\beta|)\,|\log\alpha|\,m(1+r/q)\big)\\
&\leq t\,c_4^n\,n^{(n+1)/2}\,c_9^{r+q} \leq c_{10}^r\,r^{(r+3)/2},\\
|z-k| &\geq |z|-|k| \geq m(1+r/q)-m = mr/q, \quad \text{para } k = 1, \dots, m,
\end{aligned}$$

$$\left|(z-l_0)^{-r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r\right| \leq \left(\frac{q}{mr}\right)^r \prod_{\substack{k=1\\k\neq l_0}}^{m} m^r \left(\frac{q}{mr}\right)^r \leq c_{11}\left(\frac{q}{r}\right)^{mr},$$

$$\begin{aligned}|S(x)| &\leq r!\, c_{10}^r\, r^{(r+3)/2}\, c_{11}^r \left(\frac{q}{r}\right)^{mr}\\ &\leq r^r c_{10}^r\, r^{(r+3)/2} c_{11}^r \big(\sqrt{2m}\,\big)^{mr} r^{-mr/2} = c_{12}^r\, r^{(3r+3-mr)/2}.\end{aligned}$$

Acotando la integral llegamos a que

$$\begin{aligned}|\rho| &\leq \frac{1}{2\pi}|(\log\alpha)^{-r}|2\pi m\left(1+\frac{r}{q}\right) c_{12}^r\, r^{(3r+3-mr)/2}\left(\frac{q}{mr}\right)\\ &= |\log\alpha|^{-r}\left(\frac{q}{r}+1\right) c_{12}^r\, r^{(3r+3-mr)/2} \leq c_{13}^r\, r^{(3r+3-mr)/2}.\end{aligned}$$

Ahora vamos a acotar $|\,\mathrm{N}(\rho)|$, que es el producto de los módulos de los conjugados de ρ, usando la cota anterior para $|\rho|$ y la cota (1.7) para los $h-1$ conjugados restantes. Concretamente

$$|\,\mathrm{N}(\rho)| \leq c_{13}^r r^{(3r+3-mr)/2}(c_8^r r^{r+3/2})^{h-1} = c_{14}^r\, r^{(3r+3-mr)/2+(h-1)(r+3/2)}.$$

Si sustituimos $m = 2h+2$ la expresión se simplifica hasta

$$|\,\mathrm{N}(\rho)| \leq c_{14}^r\, r^{(3h-r)/2}.$$

Pero combinando esto con (1.6) resulta $c_5^{-r} < c_{14}^r\, r^{(3h-r)/2}$, o lo que es lo mismo, $r^{(r-3h)/2} < c_{14}^r\, c_5^r = c_{15}^r$. Tomando logaritmos es fácil llegar a que

$$\left(\frac{1}{2}-\frac{3h}{2r}\right)\log r < \log c_{15}.$$

Hemos probado que esto se cumple para una constante c_{15} y para valores de r arbitrariamente grandes (pues $r \geq n$), pero esto es claramente contradictorio, pues el miembro de la izquierda tiende a $+\infty$ cuando r tiende a $+\infty$. ∎

Por ejemplo, ahora podemos asegurar que un logaritmo $\log_\alpha \beta$ con α, β algebraicos es racional o trascendente, pues si si fuera algebraico irracional entonces $\beta = \alpha^{\log_\alpha \beta}$ sería trascendente. Por ejemplo, es fácil ver que $\log_2 3$ es trascendente, ya que no puede ser un número racional a/b. En tal caso $2^{a/b} = 3$, luego $2^a = 3^b$, lo cual es imposible, con $a, b \neq 0$.

En particular vemos que un número algebraico elevado a un número trascendente puede ser algebraico. Por otra parte, por una mera cuestión de cardinalidad, es claro que α^β tiene que ser trascendente para muchos números trascendentes β.

Capítulo II

Funciones aritméticas

Una parte notable de la teoría analítica de números consiste en estudiar el comportamiento de diversas funciones aritméticas, que no son sino sucesiones $f : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{C}$.

Técnicamente, una función aritmética no es, pues, sino una sucesión de números complejos, pero "psicológicamente" no es lo mismo, pues en una función aritmética los números naturales no son meros índices sin más papel que ordenar los términos de la sucesión, sino que la idea es considerar casos en los que $f(n)$ expresa alguna propiedad del número natural n. Ésta puede ser una propiedad trivial, como en el caso de $N(n) = n$, una propiedad con un contenido aritmético natural, como pueda ser el número de divisores de n, o una propiedad más técnica, como en el caso de la función de Mangoldt que hemos presentado en la introducción, que representará un papel destacado en la prueba del teorema de los números primos y otros muchos resultados. La primera sección es esencialmente la sección [ITAn 7.4].

2.1 El álgebra de las funciones aritméticas

Definición 2.1 Llamaremos $\mathcal{A}$ al conjunto de todas las *funciones aritméticas,* es decir, el conjunto de todas las funciones $f : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{C}$. Es claro que $\mathcal{A}$ tiene estructura de $\mathbb{C}$-espacio vectorial con la suma y el producto dados por

$$(f + g)(n) = f(n) + g(n), \qquad (\alpha f)(n) = \alpha f(n).$$

Además, $\mathcal{A}$ adquiere estructura de $\mathbb{C}$-álgebra con el producto definido puntualmente:

$$(fg)(n) = f(n)g(n).$$

Sin embargo, $\mathcal{A}$ admite una estructura de álgebra mas interesante, que es la que resulta de tomar como producto la *convolución de Dirichlet,* dada por

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Nota El producto de convolución surge de forma natural en el contexto de las series de Dirichlet [ITAn 8.23], pero de momento desarrollaremos la teoría elemental sobre las funciones aritméticas, que no requiere la teoría de funciones de variable compleja, y después mostraremos esta relación. ∎

Es evidente que este producto cumple la propiedad distributiva con la suma puntual, así como que es compatible con el producto por escalares. La expresión alternativa

$$(f * g)(n) = \sum_{n=d_1 d_2} f(d_1)g(d_2)$$

muestra claramente que el producto de convolución es conmutativo, y facilita la prueba de la asociatividad:

$$((f * g) * h)(n) = \sum_{n=d_1 d_2 d_3} f(d_1)g(d_2)h(d_3) = (f * (g * h))(n).$$

Ejemplos de funciones aritméticas Veamos los primeros ejemplos de funciones aritméticas, aunque más adelante introduciremos algunas más:

- Si $\alpha \in \mathbb{C}$, llamaremos c_α a la función constante igual a α. Es claro entonces que la función c_1 es el elemento neutro en $\mathcal{A}$ para el producto puntual. En cambio, no es el elemento neutro para el producto de convolución, sino que, para cualquier función aritmética f:

$$(f * c_1)(n) = \sum_{d|n} f(d).$$

- El elemento neutro en $\mathcal{A}$ para el producto de convolución es la función 1 dada por

$$1(n) = E[1/n] = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

  Aquí, y en lo sucesivo, $E[x]$ representará siempre la parte entera del número real x.

- La *función divisor* es la que a cada número natural n le asigna su número de divisores $d(n)$. Se cumple entonces que $d = c_1 * c_1$, pues

$$d(n) = \sum_{d|n} 1 = \sum_{d|n} c_1(d) = (c_1 * c_1)(n).$$

- La *función de Euler* es la dada por

$$\phi(n) = |\{m \in \mathbb{N} \mid 1 \leq m \leq n,\ (m, n) = 1\}|,$$

  es decir, la que a cada número natural no nulo n le asigna el número de números menores que n primos con n.

- La función N es la dada por $N(n) = n$. Está relacionada con la función de Euler por la igualdad $N = c_1 * \phi$. En efecto, esto equivale a que

$$\sum_{d|n} \phi(n/d) = n,$$

lo cual se prueba sin más que considerar los conjuntos

$$A_d = \{m \in \mathbb{N} \mid 1 \leq m \leq n,\ (m,n) = d\}.$$

Es claro que $\{1,\dots,n\} = \bigcup_{d|n} A_d$, que la unión es disjunta y, teniendo en cuenta que $(m,n) = d$ equivale a $(m/d, n/d) = 1$, concluimos que $|A_d| = \phi(n/d)$.

- La función σ es la dada por $\sigma(n) = \sum_{d|n} d$, es decir, la que a cada número natural no nulo le asigna la suma de sus divisores. Claramente $\sigma = N * c_1$.

■

Todas las funciones que acabamos de definir son multiplicativas, en el sentido siguiente:

Definición 2.2 Una función aritmética f es *multiplicativa* si no es idénticamente nula y además

$$f(mn) = f(m)f(n)$$

para todo par de naturales m y n primos entre sí. Diremos que f es *completamente multiplicativa* si no es idénticamente nula y cumple esta relación para todo par de naturales m y n.

Observemos que toda función multiplicativa cumple $f(1) = 1$, pues

$$f(1) = f(1 \cdot 1) = f(1)f(1),$$

y no puede ser $f(1) = 0$, ya que entonces $f(n) = f(1n) = f(1)f(n) = 0$ y f sería idénticamente nula.

Es inmediato que las funciones c_1, 1 y N son completamente multiplicativas, y el teorema siguiente implica que d, ϕ y σ son multiplicativas, pues cada una de ellas es producto de funciones multiplicativas:

Teorema 2.3 *El producto de funciones aritméticas multiplicativas es de nuevo una función multiplicativa.*

Demostración: Si f y g son multiplicativas entonces

$$(f * g)(1) = f(1)g(1) = 1 \neq 0,$$

luego $f * g$ no es nula. Si m y n son números naturales primos entre sí,

$$(f * g)(mn) = \sum_{d|mn} f(d)g(mn/d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)g(mn/d_1d_2)$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1)g(m/d_1)f(d_2)g(n/d_2) = (f * g)(m)(f * g)(n).$$

Por lo tanto $f * g$ es multiplicativa. ■

Claramente, una función aritmética multiplicativa está determinada por su restricción a las potencias de primo, ya que tiene que cumplir $f(1) = 1$ y

$$f(p_1^{k_1} \cdots p_n^{k_n}) = f(p_1^{k_1}) \cdots f(p_n^{k_n}).$$

Análogamente, una función aritmética completamente multiplicativa está determinada por su restricción a los primos.

Ejemplos A la hora de calcular las tres funciones multiplicativas no completamente multiplicativas que hemos introducido conviene tener presente la forma en que actúan sobre potencias de primo:

- $d(p^n) = n + 1$.

  Es obvio que los divisores de p^n son las potencias $1, p, p^2, \ldots, p^n$.

- $\phi(p^n) = (p-1)p^{n-1} = p^n(1 - 1/p)$.

  En efecto, de los p^n números naturales no nulos menores o iguales que p^n, todos son primos con p^n excepto los múltiplos de p, que son p^{n-1} en total.

- $\sigma(p^n) = \dfrac{p^{n+1} - 1}{p - 1}$.

  Basta tener en cuenta que $\sigma(p^n) = 1 + p + \cdots + p^n$, y aplicar la fórmula para sumar progresiones geométricas.

Es fácil ver que las funciones anteriores no son completamente multiplicativas (por ejemplo, $d(4) = 3 \neq 4 = d(2)d(2)$), por lo que vemos que el producto de funciones completamente multiplicativas no tiene por qué ser completamente multiplicativo.

Recíprocamente, podemos definir una función multiplicativa (completamente multiplicativa) determinándola únicamente sobre potencias de primo (sobre primos). Por ejemplo [ITAn 7.12]:

Definición 2.4 La *función de Möbius* es la función multiplicativa dada por

$$\mu(p^n) = \begin{cases} -1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2. \end{cases}$$

Así, la función de Möbius es nula salvo en los números libres de cuadrados, y sobre éstos vale 1 o -1 según si son divisibles entre un número par o impar de primos. Su interés radica en el teorema siguiente:

Teorema 2.5 *Considerando $\mathcal{A}$ como anillo con el producto de convolución, se cumple:*

1. *Una función aritmética f tiene inversa si y sólo si $f(1) \neq 0$.*
2. *La inversa de una función multiplicativa es una función multiplicativa.*
3. *Si f es una función aritmética completamente multiplicativa entonces $f^{-1} = \mu f$ (donde el producto es el puntual).*

DEMOSTRACIÓN: 1) Si existe f^{-1} entonces

$$f(1)f^{-1}(1) = (f * f^{-1})(1) = 1(1) = 1,$$

luego $f(1) \neq 0$. Recíprocamente, si $f(1) \neq 0$ vamos a definir inductivamente f^{-1}. En primer lugar $f^{-1}(1) = 1/f(1)$, con lo que el razonamiento anterior garantiza que $f(1)f^{-1}(1) = 1(1)$.

Para definir $f^{-1}(n)$ con $n > 1$ observamos que queremos que se cumpla

$$\sum_{d|n} f(d)f^{-1}(n/d) = 0,$$

luego la definición ha de ser

$$f^{-1}(n) = \frac{1}{f(1)} \sum_{1<d|n} f(d)f^{-1}(n/d).$$

Claramente, la función f^{-1} así definida es la inversa de f.

2) Supongamos que f es multiplicativa pero f^{-1} no lo es. Entonces existen números m y n primos entre sí tales que $f^{-1}(mn) \neq f^{-1}(m)f^{-1}(n)$. Podemos tomarlos de modo que mn sea el mínimo posible. Como la función $f * f^{-1} = 1$ es multiplicativa, tenemos que $(f * f^{-1})(mn) = (f * f^{-1})(m)(f * f^{-1})(n)$, o sea,

$$\sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)f^{-1}(mn/d_1d_2) = \sum_{d_1|m} f(d_1)f^{-1}(m/d_1) \sum_{d_2|n} f(d_2)f^{-1}(n/d_2).$$

Ahora bien, por la minimalidad de mn cada sumando de la izquierda es igual a un sumando de la derecha y viceversa, excepto los correspondientes a $d_1 = d_2 = 1$. Pero si cancelamos los sumandos iguales queda simplemente $f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$, contradicción.

3) Hemos de probar que $\mu f * f = 1$. La función de la izquierda es multiplicativa por ser un producto de funciones multiplicativas, luego basta probar que $(\mu f * f)(p^n) = 0$, para todo primo p y todo $n \geq 1$. Ahora bien, como los divisores de p^n son los p^k para $k \leq n$, tenemos

$$\begin{aligned}(\mu f * f)(p^n) &= \sum_{k=0}^{n} \mu(p^k)f(p^k)f(p^{n-k}) = \sum_{k=0}^{n} \mu(p^k)f(p^n) \\ &= \big(\mu(1) + \mu(p)\big)f(p^n) = 0.\end{aligned}$$

∎

Como la función constante c_1 es completamente multiplicativa, el teorema anterior nos da que $\mu = c_1^{-1}$. En particular vemos que la inversa de una función completamente multiplicativa no tiene por qué ser completamente multiplicativa, ya que μ no lo es.

La relación $\mu = c_1^{-1}$ tiene un enunciado alternativo de interés:

Teorema 2.6 (Fórmula de inversión de Möbius) *Si f y g son funciones aritméticas tales que $g(n) = \sum_{d|n} f(d)$, entonces*

$$f(n) = \sum_{d|n} \mu(d)g(n/d).$$

Por ejemplo, de la relación $N = c_1 * \phi$ deducimos ahora que $\phi = \mu * N$, que explícitamente significa que

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Ejemplo En [Al 4.50] demostramos que todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico (lo que en particular implica que existen raíces primitivas módulo todo primo p), para lo cual nos apoyamos en los teoremas de estructura de los grupos abelianos finitos. Vamos a dar una prueba mucho más elemental basada en el teorema anterior y en la observación siguiente:

Si G es un subgrupo de orden q de un cuerpo F y $n \mid q$, el polinomio $x^n - 1$ tiene n raíces distintas en G.

En efecto, considerando congruencias módulo $P = x^n - 1$ en $F[x]$ vemos que

$$x^q - 1 = (x^n)^{q/n} - 1 \equiv 0 \text{ (mód } P),$$

luego $x^q - 1 = (x^n - 1)g(x)$, para cierto polinomio $g(x) \in F[x]$. Si $x^n - 1$ tuviera menos de n raíces distintas en G, entonces $x^q - 1$ tendría menos de q raíces distintas, pero esto es absurdo, porque los q elementos de G son raíces de $x^q - 1$.

Sabiendo esto, llamamos $\bar{\phi}(n)$ al número de elementos de G de orden n y concluimos que, si $n \mid q$,

$$\bar{N}(n) = \sum_{d|n} \bar{\phi}(d) = n,$$

pues los elementos de G orden divisor de n son las raíces de $x^n - 1$. Equivalentemente, tenemos que $\bar{N} = \bar{\phi} * c_1$, luego $\bar{\phi} = \bar{N} * \mu$. Explícitamente, si $n \mid q$,

$$\bar{\phi}(n) = \sum_{d|n} \mu(d)\bar{N}(n/d) = \sum_{d|n} \mu(d)\frac{n}{d} = \phi(n).$$

Así pues, para cada $n \mid q$, resulta que G tiene $\phi(n)$ elementos de orden n y, en particular, tiene $\phi(q) \geq 1$ elementos de orden q. ∎

Veamos un segundo ejemplo de aplicación de la fórmula de inversión:

Teorema 2.7 *El número de polinomios irreducibles de grado n en el cuerpo finito de q elementos es*

$$I_n = \frac{1}{n}\sum_{d|n} \mu(n/d)q^d.$$

Demostración: Sea F el cuerpo finito de q elementos. Entonces el polinomio $x^{q^n} - x$ es el producto de todos los polinomios irreducibles en $F[x]$ de grado $d \mid n$. En efecto, si $p(x) \mid x^{q^n} - x$ es un polinomio irreducible de grado d y α es una raíz en una clausura algebraica de F, entonces α es raíz de $x^{q^n} - x$, pero, por [Al 9.2], las raíces de este polinomio forman el cuerpo de q^n elementos, que tiene grado n sobre F, luego $d = |F(\alpha) : F|$ divide a n.

Recíprocamente, si $p(x)$ es un polinomio irreducible en $F[x]$ de grado $d \mid n$ y α es una de sus raíces, entonces $F(\alpha)$ es el cuerpo de q^d elementos, que, siempre por [Al 9.2], está contenido en el cuerpo de q^n elementos, luego α es raíz de $x^{q^n} - x$, luego $p(x) \mid x^{q^n} - x$.

Sólo falta observar que cada polinomio irreducible aparece sólo una vez como factor de $x^{q^n} - x$, pues la derivada de este polinomio es -1, luego no tiene raíces múltiples.

Por consiguiente, q^n es la suma de los grados de todos los polinomios irreducibles de grado divisor de n, es decir:

$$S(n) = \sum_{d|n} dI_d = q^n.$$

Por la fórmula de inversión,

$$nI_n = \sum_{d|n} \mu(n/d)S(d) = \sum_{d|n} \mu(n/d)q^d.$$

∎

En la última sección presentamos una aplicación más sofisticada de la fórmula de inversión. Probamos ahora un último resultado sobre la función de Möbius:

Teorema 2.8 *Se cumple que*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}.$$

Demostración: Nos apoyamos en que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

En particular esto implica que la serie del enunciado es absolutamente convergente, pues $|\mu(n)| \leq 1$. Por consiguiente, podemos operar las series:

$$\sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \sum_{m,n}^{\infty} \frac{\mu(n)}{(mn)^2} = \sum_{k=1}^{\infty} \sum_{d|k} \frac{\mu(d)}{k^2} = \sum_{k=1}^{\infty} \frac{(\mu * c_1)(k)}{k^2} = 1,$$

donde hemos usado que $(\mu * c_1)(k) = E[1/k]$. ∎

En el álgebra de las funciones aritméticas podemos definir una derivación que surge de forma natural a partir de la relación entre éstas y las series de Dirichlet que de momento estamos evitando:

Definición 2.9 Si $f \in \mathcal{A}$ es una función aritmética, definimos su *derivada* como la función dada por $f'(n) = f(n) \log n$.

Se comprueba sin dificultad que

$$(f+g)' = f' + g', \qquad (f*g)' = f'*g + f*g'.$$

Notemos que $c_1' = \log$ (donde el miembro derecho es la función $n \mapsto \log n$).

Introducimos ahora una función aritmética que tendrá gran importancia en lo sucesivo:

Definición 2.10 Se define la *función de Mangoldt* como la función aritmética dada por

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m,\ m \geq 1 \\ 0 & \text{en otro caso.} \end{cases}$$

Vamos a comprobar la relación siguiente: $\Lambda * c_1 = \log$.

En efecto, si $n = 1$ es claro que $(\Lambda * c_1)(1) = 0 = \log 1$. En otro caso $n = p_1^{k_1} \cdots p_r^{k_r}$ y se cumple

$$(\Lambda * c_1)(n) = \sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \Lambda(p_i^j) = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \log p_i = \sum_{i=1}^{r} k_i \log p_i = \log n.$$

Terminamos esta sección presentando una generalización de la fórmula de inversión de Möbius que necesitaremos más adelante. Para ello generalizamos el concepto de convolución:

Definición 2.11 Si f es una función aritmética y $F :]0, +\infty[\longrightarrow \mathbb{C}$ es una función tal que $F|_{]0,1[} = 0$, definimos

$$(f \circ F)(x) = \sum_{n \leq x} f(n) F(x/n).$$

Observemos que $f \circ F :]0, +\infty[\longrightarrow \mathbb{C}$ también se anula en $]0, 1[$. Se cumple una propiedad asociativa mixta:

$$f \circ (g \circ F) = (f * g) \circ F,$$

donde f y g son funciones aritméticas. En efecto:

$$(f \circ (g \circ F))(x) = \sum_{n \leq x} f(n) \sum_{m \leq x/n} g(m) F(x/mn)$$

$$= \sum_{mn \leq x} f(n) g(m) F(x/mn) = \sum_{k \leq x} \sum_{d|k} f(d) g(k/d) F(x/k)$$

$$\sum_{k \leq x} (f * g)(k) F(x/k) = ((f * g) \circ F)(x).$$

Por otra parte, es claro que $1 \circ F = F$, lo que nos da este teorema de inversión:

Teorema 2.12 (Fórmula de inversión generalizada) *Si f es una función aritmética con inversa f^{-1}, las funciones $F, G :]0, +\infty[\longrightarrow \mathbb{C}$ se anulan en el intervalo $]0, 1[$ y*

$$G(x) = \sum_{n \leq x} f(n)F(x/n),$$

entonces

$$F(x) = \sum_{n \leq x} f^{-1}(n)G(x/n).$$

DEMOSTRACIÓN: La hipótesis es que $G = f \circ F$, luego

$$f^{-1} \circ G = f^{-1} \circ (f \circ F) = (f^{-1} * f) \circ G = 1 \circ F = F.$$

■

En particular:

Teorema 2.13 *Si f es una función aritmética completamente multiplicativa, las funciones $F, G :]0, +\infty[\longrightarrow \mathbb{C}$ se anulan en $]0, 1[$ y*

$$G(x) = \sum_{n \leq x} f(n)F(x/n),$$

entonces

$$F(x) = \sum_{n \leq x} \mu(n)f(n)G(x/n).$$

Veamos un ejemplo:

Teorema 2.14 *El número de fracciones irreducibles $0 < a/b < 1$ con $0 < b \leq n$ viene dado por*

$$f(n) = \frac{1}{2} \sum_{m \leq n} \mu(m)E[n/m](E[n/m] - 1).$$

DEMOSTRACIÓN: Sea $g(n)$ el número de fracciones $0 < a/b < 1$ no necesariamente irreducibles con $0 < b \leq n$. Claramente, $g(n) = n(n-1)/2$, y se cumple que

$$g(n) = \sum_{m \leq n} f(E[n/m]).$$

En efecto, el conjunto de todas las fracciones que cuenta $g(n)$ se divide en clases de equivalencia de fracciones con el mismo representante irreducible. Si $0 < a/b \leq 1$ es una de estas fracciones irreducibles, los números $1 \leq m \leq n$ que cumplen $b \leq E[n/m]$ son los mismos que cumplen $bm \leq n$, es decir, los que dan lugar a fracciones $0 < (am)/(bm) \leq 1$ con $bm \leq n$ cuya fracción irreducible es la dada. En otras palabras, el número de números m tales que $b \leq E[n/m]$ es el cardinal de la clase de a/b.

Por lo tanto, la fracción a/b aparece contada en tantos sumandos de la expresión anterior como elementos tiene su clase de equivalencia, luego la suma cuenta todos los elementos de todas las clases de equivalencia.

Ahora definimos $F(x) = f(E[x])$ y $G(x) = g(E[x])$, de modo que, llamando $n = E[x]$, tenemos que

$$G(x) = g(n) = \sum_{m\le x} f(E[n/m]) = \sum_{m\le x} F(E[x/m]) = \sum_{m\le x} F(x/m),$$

donde hemos usado que $E[n/m] = E[x/m]$. En efecto, es evidente que se cumple $E[n/m] \le E[x/m]$ y, si la desigualdad fuera estricta, tendríamos que

$$n/m < E[n/m] + 1 \le E[x/m] \le x/m,$$

luego $n < m(E[n/m] + 1) \le x$, luego $E[x] + 1 = n + 1 \le x$, contradicción. El teorema anterior nos da que

$$F(x) = \sum_{m\le x} \mu(m)G(x/m),$$

y cuando x es un número natural n obtenemos la fórmula del enunciado. ∎

La función contadora de primos de Riemann Veamos un último ejemplo más sofisticado de una inversión mediante la función de Möbius que no responde a los esquemas que hemos visto.

En la introducción hemos hablado del teorema de los números primos, que permite estimar la función $\pi(x)$ que cuenta el número de primos menores o iguales que un número $x > 0$ dado. Sin embargo, en su estudio del problema, Riemann consideró más conveniente considerar otra función que cuenta los primos más indirectamente:

Definición 2.15 La *función contadora de primos de Riemann* es la dada por

$$\pi^*(x) = \sum_{n\le x} \frac{\Lambda(n)}{\log n} = \sum_{p^m\le x} \frac{1}{m} = \sum_{m=1}^{\infty} \frac{\pi(x^{1/m})}{m}.$$

La última serie es en realidad finita, pues $\pi(x^{1/m}) = 0$ cuando $x^{1/m} < 2$, es decir, cuando $m > \log x/\log 2$. Por lo tanto, no alteramos la suma si limitamos el sumatorio a $m \le \log x/\log 2$, o incluso $m \le \log x$, o simplemente $m \le x$.

Podría objetarse que $\pi^*(x)$ cuente primos, pero es que lo hace indirectamente, en el sentido de que $\pi(x)$ puede calcularse en términos de $\pi^*(x)$:

Teorema 2.16 *Para todo $x > 0$ se cumple*

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \pi^*(x^{1/n}).$$

Demostración: Notemos que, como en el caso de la suma que define a $\pi^*(x)$, la suma del enunciado es finita. Vamos a definir recurrentemente una sucesión de funciones $f_0, f_1, f_2, \ldots$ mediante

$$f_0(x) = \pi^*(x), \qquad f_{k+1}(x) = f_k(x) - \frac{1}{p_{k+1}} f_k(x^{1/p_{k+1}}),$$

donde p_{k+1} es el primo $k+1$-ésimo.

Veamos cuáles son los primeros términos de la sucesión. El primero es

$$f_0(x) = \pi^*(x) = \sum_{m=1}^{\infty} \frac{\pi(x^{1/m})}{m}.$$

A su vez

$$f_1(x) = \pi^*(x) - \frac{1}{2}\pi^*(x^{1/2}) = \sum_{m=1}^{\infty} \frac{\pi(x^{1/m})}{m} - \sum_{m=1}^{\infty} \frac{\pi(x^{1/2m})}{2m}.$$

Así, en el miembro derecho sólo están los términos $\pi(x^{1/m})/m$ correspondientes a índices m impares. A su vez,

$$\frac{1}{3}f_1(x^{1/3}) = \frac{1}{3}\pi^*(x^{1/3}) - \frac{1}{6}\pi^*(x^{1/6}) = \sum_{m=1}^{\infty} \frac{\pi(x^{1/3m})}{3m} - \sum_{m=1}^{\infty} \frac{\pi(x^{1/6m})}{6m},$$

luego

$$\begin{aligned} f_2(x) &= \pi^*(x) - \frac{1}{2}\pi^*(x^{1/2}) - \frac{1}{3}\pi^*(x^{1/3}) + \frac{1}{6}\pi^*(x^{1/6}) \\ &= \sum_{m=1}^{\infty} \frac{\pi(x^{1/m})}{m} - \sum_{m=1}^{\infty} \frac{\pi(x^{1/2m})}{2m} - \sum_{m=1}^{\infty} \frac{\pi(x^{1/3m})}{3m} + \sum_{m=1}^{\infty} \frac{\pi(x^{1/6m})}{6m}. \end{aligned}$$

Vemos que en la primera expresión para $f_2(x)$ aparecen todos los índices m libres de cuadrados divisibles únicamente entre 2 y 3 y el signo es $\mu(m)$, mientras que en la segunda expresión aparecen todos los índices m no divisibles ni entre 2 ni entre 3 (como los múltiplos de 6 se restan dos veces, luego se suman para que sólo sean sustraídos una vez).

Una inducción rutinaria muestra que esto es cierto en general, es decir, que $f_k(x)$ admite una expresión con sumandos $\frac{\mu(m)}{m}\pi^*(x^{1/m})$, donde m recorre todos los números divisibles únicamente entre los primos $p_1, \ldots, p_k$ (libres de cuadrados, si se quiere, porque en caso contrario $\mu(m) = 0$) y también una segunda expresión con sumandos $(1/m)\pi(x^{1/m})$ para todos los índices no divisibles entre ninguno de los primos $p_1, \ldots, p_k$.

Así, cuando k es suficientemente grande, la primera expresión para f_k coincide con el miembro derecho de la fórmula del enunciado (pues todos los sumandos que faltarían por aparecer serían ya nulos) y la segunda expresión se reduce a $\pi(x)$. ∎

2.2 Orden de crecimiento

En lo sucesivo vamos a considerar muchas sucesiones y funciones que tienden a infinito, pero con esto no está dicho todo, sino que podemos tratar de estimar "a qué velocidad" tienden a infinito, comparando su crecimiento con el de otras funciones sencillas cuyo comportamiento podamos considerar bien conocido. Esta comparación puede concretarse de formas distintas. El caso más sencillo en que podemos decir que dos funciones crecen "por igual" es el recogido en la definición siguiente (véase la sección [ITAn 7.2]):

Definición 2.17 Sea X un espacio topológico, $a \in X$ un punto de acumulación de X y $f, g : X \setminus \{a\} \longrightarrow \mathbb{R}$. Diremos que f y g son *asintóticamente equivalentes* en a si existe

$$\lim_{x \to a} \frac{f(x)}{g(x)} = 1.$$

La definición supone en particular que $g(x)$ no se anula en un entorno de a, aunque en la práctica la aplicaremos cuando f y g tiendan a $+\infty$ en a, con lo que esto se cumplirá trivialmente.

Usaremos la notación $f(x) \sim g(x)$ para indicar que las funciones son asintóticamente equivalentes, indicando el punto a si no se sobreentiende por el contexto.

Notemos que la definición equivale a que

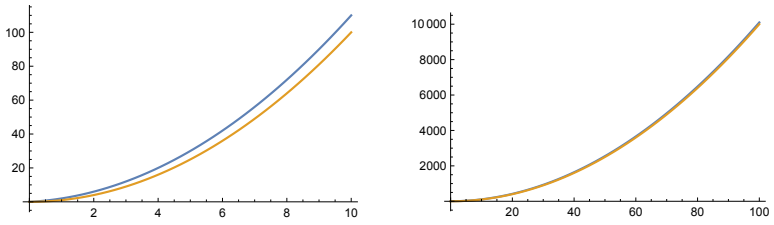
$$\lim_{x \to a} \frac{f(x)}{g(x)} = 1.$$

o también a que

$$\lim_{x \to a} \frac{f(x) - g(x)}{g(x)} = 0, \qquad \lim_{x \to a} \frac{g(x) - f(x)}{f(x)} = 0.$$

Las dos últimas expresiones se interpretan como que el error relativo cometido al aproximar una por la otra (es decir, el error absoluto dividido entre el valor real que queríamos aproximar) tiende a 0.

Ejemplo 1 Se cumple que $x^2 + x \sim x^2$ (en $+\infty$). El error absoluto cometido al aproximar una por la otra tiende a infinito, pero dicho error es cada vez menor en relación al valor que toman ambas funciones.



Esto se pone de manifiesto al comparar las gráficas. En la primera, cuando x varía de 0 a 10, vemos cómo la diferencia entre ambas funciones se hace cada vez mayor, pero en la segunda, al modificar la escala para que las gráficas guarden la misma proporción, esa diferencia, pese a ser cada vez mayor, se vuelve inapreciable. ∎

Ejemplo 2 Consideremos un caso ligeramente más sofisticado. Vamos a estudiar el crecimiento de la función

$$\sum_{n \leq x} n$$

Siempre que empleemos esta notación habrá que entender que n recorre los números naturales no nulos menores o iguales que el número real x. Equivalentemente,

$$\sum_{n\le x} n = \sum_{n=1}^{E[x]} n = \frac{E[x](E[x]+1)}{2}.$$

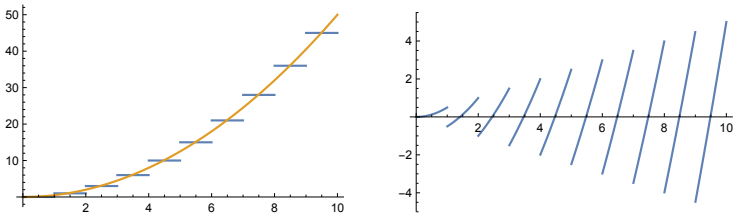
Se cumple entonces que

$$\sum_{n\le x} n \sim \frac{x^2}{2},$$

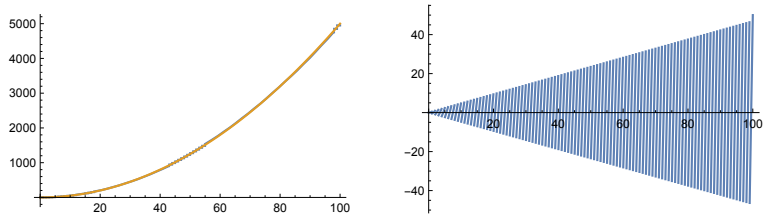
pues

$$\left|\frac{\sum\limits_{n\le x} n}{x^2/2} - 1\right| = \frac{|E[x]^2 + E[x] - x^2|}{x^2} \le \frac{(x - E[x])(x + E[x]) + E[x]}{x^2}$$

$$\le \frac{1(x + x + 1) + x + 1}{x^2} = \frac{3x + 2}{x^2} \to 0.$$



La gráfica de la izquierda muestra las dos funciones y la de la derecha la diferencia entre ambas. Vemos que el error oscila cada vez con más amplitud, y esto se confirma en la gráfica de la derecha siguiente, pero en la gráfica de la izquierda ambas funciones son indistinguibles, pues, aunque las diferencias sean cada vez más grandes, se vuelven despreciables cuando se comparan con la magnitud de cualquiera de las dos funciones:

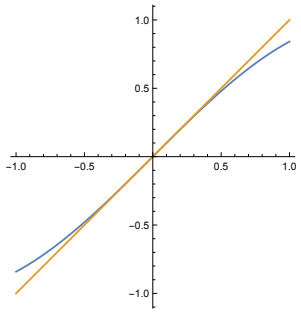


Así pues, $x^2/2$ es una función sencilla que describe bien el crecimiento de las sumas finitas de números naturales. ∎

En los dos ejemplos anteriores hemos comparado dos funciones que tienden a $+\infty$ en $+\infty$. Será el caso más habitual, pero también tiene interés estudiar el modo en que una función tiende a 0 en un punto finito o infinito. Por ejemplo, podemos afirmar que

$$\operatorname{sen} x \sim x \qquad \text{alrededor de } 0.$$

Notemos que si dos funciones cualesquiera tienden a 0 en un punto, el error absoluto que cometemos al aproximar una por otra tiende a 0 en el punto, pero la equivalencia asintótica expresa algo más fuerte, a saber, que las gráficas de las dos funciones resultan indistinguibles incluso a escalas en las que ambas se distinguen de 0. Por ejemplo, la figura muestra las funciones $\operatorname{sen} x$ y x. Si representamos también, digamos, $2x$, su gráfica se distinguiría perfectamente de las otras dos, a pesar de que la diferencia entre todas ellas tiende a 0 en 0.



Una relación un poco más débil que la equivalencia asintótica es la siguiente:

Definición 2.18 Sea X un espacio topológico, $a \in X$ un punto de acumulación de X y $f, g : X \setminus \{a\} \longrightarrow \mathbb{R}$. Diremos que *el crecimiento de f en a es del orden del de g* si existen un entorno U de a en X y una constante $C > 0$ tales que $|f(x)/g(x)| \leq C$ para todo $x \in U \setminus \{a\}$.

Es frecuente usar una notación un tanto abusiva para expresar este hecho, consistente en escribir $O(g(x))$ para referirse a una función arbitraria que crezca como $g(x)$, es decir, una función arbitraria que permanece acotada cuando se divide entre $|g(x)|$.

Ejemplo 1 Hemos dicho que esta definición es más débil que la anterior porque, claramente, si $f(x) \sim g(x)$ entonces el crecimiento de f es del orden del de g (pues la definición se cumple con cualquier constante mayor que 1), y el recíproco no es cierto en general. Sin embargo, con el concepto de orden de crecimiento podemos expresar relaciones más precisas que con el de equivalencia asintótica. Por ejemplo, decir que

$$\sum_{n\leq x} n = O(x^2/2)$$

es más débil que decir que ambas funciones son asintóticamente equivalentes, pues sólo expresa que el cociente está acotado, no que tienda a 1. De hecho, esto es equivalente a

$$\sum_{n\leq x} n = O(x^2),$$

y ya no es cierto que la suma y x^2 sean asintóticamente equivalentes, pero la relación

$$\sum_{n\leq x} n = \frac{x^2}{2} + O(x) \tag{2.1}$$

es más precisa. En efecto, ante todo esta relación es cierta, pues

$$\left|\frac{\sum\limits_{n\le x} n - x^2/2}{x}\right| = \left|\frac{E[x]^2 - x^2 + E[x]) + E[x]}{2x}\right| \le$$

$$\frac{(x - E[x])(x + E[x]) + E[x]}{2x} \le \frac{3x+2}{2x} \to \frac{3}{2},$$

luego el cociente está acotado, y de aquí se deduce a su vez que

$$\frac{\sum\limits_{n\le x} n}{x^2/2} = 1 + O(1/x), \tag{2.2}$$

pues al dividir entre $x^2/2$ una función que permanece acotada al dividirla entre x obtenemos una función que permanece acotada al dividirla entre $2/x$, luego también si la dividimos entre $1/x$.

Vemos que la expresión (2.1) no sólo dice que las dos primeras funciones son asintóticamente equivalentes, sino que nos acota el error absoluto de aproximar una por la otra, y la expresión (2.2) no sólo indica explícitamente que el cociente de la izquierda tiende a 1, sino que nos informa de la rapidez con la que tiende a 1 (al menos tan rápidamente como $1/x$ tiende a 0). ∎

En general, cuando comparamos dos funciones que tienden a $+\infty$, lo que expresa la definición es que $f(x)$ deja de tender a $+\infty$ cuando se la divide entre $g(x)$ o, en otras palabras, que $g(x)$ crece con la rapidez suficiente como para compensar el crecimiento de $f(x)$.

Así, la serie $\sum\limits_{n\le x} n$ tiende a $+\infty$, pero deja de tender a $+\infty$ y permanece acotada cuando se la divide entre x^2, o el error de aproximar dicha serie por $x^2/2$ tiende a $+\infty$, pero deja de tender a $+\infty$ cuando se divide entre x.

Ejemplo 2 Consideremos ahora el caso de una serie convergente. Se cumple que

$$\sum_{n\le x} \frac{1}{2^n} = 1 + O(1/2^x).$$

En efecto, tenemos que

$$\sum_{n\le x} \frac{1}{2^n} = 1 - \frac{1}{2^{E[x]}},$$

luego

$$\left|\frac{\sum\limits_{n\le x} (1/2^n) - 1}{1/2^x}\right| = 2^{x-E[x]} \le 2,$$

pero con la estimación que hemos hecho no sólo sabemos que la serie converge a 1, sino que tenemos información sobre la velocidad con la que converge (al menos tan rápidamente como $1/2^x$ converge a 0). ∎

Ejemplo 3 Considerando la serie de Taylor del seno es fácil ver que, alrededor de 0,

$$\operatorname{sen} x = x - \frac{x^3}{6} + O(x^5), \tag{2.3}$$

lo cual significa, por definición, que el crecimiento de la función $\operatorname{sen} x - x + x^3/6$ es como el de x^5, es decir, que el cociente permanece acotado. De hecho, se cumple que

$$\lim_{x\to 0} \frac{\operatorname{sen} x - x + x^3/6}{x^5} = \frac{1}{5!}.$$

Si dividiéramos entre x^4 el límite sería 0 y si dividiéramos entre x^6 el límite sería infinito, por lo que 5 es "el exponente justo" que da un cociente acotado que no tiende ni a 0 ni a $+\infty$. De (2.3) se sigue inmediatamente que

$$\frac{\operatorname{sen} x}{x} = 1 - \frac{x^2}{6} + O(x^4),$$

pues si dividimos entre x una función que permanece acotada al dividirla entre x^5, obtenemos una función que permanece acotada al dividirla entre x^4, y esto implica a su vez que $\operatorname{sen} x \sim x$, por lo que (2.3) proporciona información más precisa sobre el modo en que $\operatorname{sen} x$ tiende a 0 en $a = 0$. ∎

En lugar de (2.3), podríamos haber escrito

$$\operatorname{sen} x = x - \frac{x^3}{6} + O(x^4),$$

lo cual, aunque es cierto, es menos preciso, porque la función que estamos representando por $O(x^4)$ (que es la misma que en (2.3) representamos por $O(x^5)$, a saber, $\operatorname{sen} x - x + x^3/6$), no sólo es una función que permanece acotada cuando se divide entre x^4, sino que de hecho tiende a 0. Para hacer constar este hecho usaremos una *o* minúscula:

Definición 2.19 Sea X un espacio topológico, $a \in X$ un punto de acumulación de X y $f, g : X \setminus \{a\} \longrightarrow \mathbb{R}$. Diremos que *el crecimiento de f en a es de orden menor que el de g* si existe

$$\lim_{x\to a} \frac{f(x)}{g(x)} = 0.$$

Usaremos la notación $o(g(x))$ para representar cualquier función de orden menor que el de $g(x)$, es decir, una función que dividida entre $g(x)$ tiende a 0 (en un punto a prefijado). En estos términos,

$$\operatorname{sen} x = x - \frac{x^3}{6} + o(x^4).$$

En general, una comparación en términos de $o(g(x))$ es menos fina que otra con O, pues indica que "nos hemos excedido" y estamos comparando con una función $g(x)$ que tiende a su límite más rápidamente que la que tratamos de describir. Así, el polinomio de Taylor de grado 3 de la función seno aproxima a esta función alrededor de 0 con orden exactamente $O(x^5)$, en el sentido de que si ponemos un exponente $\alpha < 5$ en realidad tenemos $o(x^\alpha)$, mientras que si ponemos un exponente mayor el cociente tiende a ∞.

Observaciones He aquí algunos hechos adicionales sobre los conceptos que acabamos de introducir:

- Si $f, g : [a, +\infty[\longrightarrow \mathbb{R}$ son funciones continuas en un intervalo, una relación de tipo $f(x) = O(g(x))$ en $+\infty$ sólo significa que existe una constante $C > 0$ tal que $|f(x)| \leq C|g(x)|$ para valores de x suficientemente grandes, digamos para $x \geq x_0$, pero si $g(x)$ es estrictamente mayor que 0, entonces, como $|f|$ tiene un máximo M en $[a, x_0]$ y g tiene un mínimo $m > 0$ en dicho intervalo, sucede que $|f(x)| \leq (M/m)g(x)$ en $[a, x_0]$, luego cambiando C por el máximo entre C y M/m tenemos que $|f(x)| \leq Cg(x)$ en todo el intervalo $[a, +\infty[$.

- Todos los conceptos que hemos definido aquí valen trivialmente para funciones f con valores complejos si los entendemos aplicados a $|f|$.

- No está de más recalcar que la notación $f(x) = O(g(x))$ es abusiva en cuanto que no es una auténtica igualdad. Por ejemplo, es cierto que $O(x^2) = O(x^3)$ (en $+\infty$) en el sentido de que toda función que permanece acotada al dividirla entre x^2 es también una función que permanece acotada al dividirla entre x^3, pero, entendido así, es falso que $O(x^3) = O(x^2)$, pues una función que permanezca acotada al dividirla entre x^3 (por ejemplo x^3) no tiene por qué permanecer acotada al dividirla entre x^2.

■

Nuestra intención es describir el crecimiento de funciones "complicadas" comparándolas con otras más sencillas, pero para ello conviene que tengamos una idea clara de cómo es el crecimiento de las funciones más habituales que usaremos como referencia.

- Podríamos considerar que $O(x)$ representa la velocidad "básica" de crecimiento hacia $+\infty$, es el ritmo de crecimiento en el que la función crece a la misma velocidad que avanza la variable. Alrededor de $O(x)$ tenemos las potencias $O(x^\alpha)$, con $\alpha > 0$. Notemos que si $0 < \alpha < \beta$, entonces $x^\alpha = o(x^\beta)$, de modo que al aumentar el exponente aumenta el orden de crecimiento de la potencia.

- Por encima de todos los órdenes de crecimiento $O(x^\alpha)$ están los crecimientos exponenciales $O(e^{\beta x})$, con $\beta > 0$. En efecto,

$$\lim_{x\to+\infty} \frac{e^{\beta x}}{x^\alpha} = \lim_{x\to+\infty} e^{(\beta \frac{x}{\log x} - \alpha)\log x} = +\infty,$$

de modo que $x^\alpha = o(e^{\beta x})$, cualesquiera que sean α y β. En otras palabras: cualquier exponencial crece más rápidamente que cualquier potencia. Notemos también que $a^x = e^{x \log a}$, por lo que las funciones a^x con $a > 1$ son las mismas que las $e^{\beta x}$ con $\beta > 0$.

- Por debajo de todos los crecimientos potenciales $O(x^\alpha)$ están los crecimientos logarítmicos $O(\log^\beta x)$. En efecto, aplicando la regla de L'Hôpital,

$$\lim_{x\to+\infty} \frac{\log^\beta x}{x^\alpha} = \lim_{x\to+\infty} \left(\frac{\log x}{x^{\alpha/\beta}}\right)^\beta = \lim_{x\to+\infty} \left(\frac{1}{(\alpha/\beta)x^{1+\alpha/\beta}}\right)^\beta = 0,$$

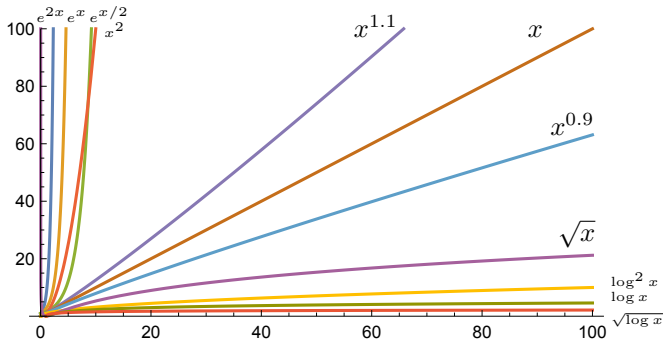
  teniendo en cuenta que estamos considerando $\alpha, \beta > 0$.

  En particular, observamos que $\log x = o(x^\epsilon)$, para todo $\epsilon > 0$.

- Alrededor de cada crecimiento potencial $O(x^\alpha)$ tenemos una "aureola" de crecimientos logarítmicos, en el sentido de que, por ejemplo, sucede que $x^2 \log x = O(x^{2+\epsilon})$ para todo $\epsilon > 0$, es decir, que $x^2 \log x$ deja de tender a $+\infty$ cuando se divide entre cualquier $x^{2+\epsilon}$, pero sigue tendiendo a $+\infty$ si se divide entre x^2.

- Similarmente se comprueba que la función e^{e^x} crece más deprisa que cualquier $e^{\beta x}$, mientras que $\log\log x$ crece más despacio que cualquier $\log^\beta x$.

La figura muestra algunas de las funciones que acabamos de considerar:



2.3 Cálculo de órdenes

Todos los ejemplos de órdenes de funciones que hemos mostrado en la sección anterior eran triviales. Probamos ahora un resultado general que usaremos en incontables ocasiones y que de momento nos permitirá calcular el orden de crecimiento de algunas funciones un poco más sofisticadas. Puede considerarse como una versión discreta de la integración por partes que incluye como caso particular a la fórmula de Abel [ITAn 2.32]:

Teorema 2.20 *Sea $\{c_n\}_{n=1}^{\infty}$ una sucesión en $\mathbb{C}$, sea $C(x) = \sum_{n\le x} c_n$ y consideremos cualquier función $f : [0, +\infty[\longrightarrow \mathbb{R}$. Entonces*

$$\sum_{n\le x} c_n f(n) = \sum_{n\le x-1} C(n)(f(n) - f(n+1)) + C(x)f(E[x]),$$

donde E representa la parte entera. Si además $c_n = 0$ para $n < n_1$ y f es de clase C^1 en un entorno de $[n_1, +\infty[$, entonces

$$\sum_{n\le x} c_n f(n) = C(x)f(x) - \int_{n_1}^{x} C(t)f'(t)\,dt.$$

DEMOSTRACIÓN: Llamemos $N = E[x]$. Entonces

$$\begin{aligned}
\sum_{n\le x} c_n f(n) &= C(1)f(1) + \sum_{n=2}^{N} (C(n) - C(n-1))f(n) \\
&= \sum_{n=1}^{N} C(n)f(n) - \sum_{n=1}^{N-1} C(n)f(n+1) \\
&= \sum_{n=1}^{N-1} C(n)(f(n) - f(n+1)) + C(N)f(N) \\
&= \sum_{n\le x-1} C(n)(f(n) - f(n+1)) + C(x)f(E[x]).
\end{aligned}$$

Para la segunda parte observamos que si $n \le t < n+1$ entonces $C(t) = C(n)$, luego

$$C(n)(f(n) - f(n+1)) = -\int_{n}^{n+1} C(t)f'(t)\,dt,$$

y $C(t) = 0$ si $t < n_1$. Así, la integral desde n_1 hasta $N = E[x]$ es el sumatorio de la expresión que hemos obtenido, mientras que

$$-\int_{N}^{x} C(t)f'(t)\,dt = -C(x)(f(x) - f(E[x])) = C(x)f(E[x]) - C(x)f(x),$$

luego falta sumar $C(x)f(x)$. ∎

Como primera aplicación estimamos el crecimiento de las sumas parciales de algunas series, tanto convergentes como divergentes.

Teorema 2.21 *Se cumple*

1. $\displaystyle\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O(1/x),$
2. $\displaystyle\sum_{n\le x} \frac{1}{n^2} = \frac{\pi^2}{6} + O(1/x),$
3. $\displaystyle\sum_{n\le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O(1/x),$

4. $\displaystyle\sum_{n\le x}\phi(n)=\frac{3}{\pi^2}\,x^2+O(x\log x)$.

DEMOSTRACIÓN: 1) Aquí γ es la constante de Euler, definida en [ITAn 4.12] como

$$\gamma=\lim_N\sum_{n=1}^{N}\frac{1}{n}-\log N, \tag{2.4}$$

pero la prueba que vamos a dar no presupone que exista el límite, sino que aquí veremos una prueba alternativa. Notemos que la existencia del límite equivale a la fórmula del enunciado con una estimación $o(1)$, pero aquí la vamos a refinar a $O(1/x)$, que no sólo expresa que la función

$$\lim_n\sum_{n\le x}\frac{1}{n}-\log n-\gamma$$

converge a 0, sino que permanece acotada cuando se multiplica por x.

Aplicamos el teorema anterior a $c_n=1$ y $f(t)=1/t$. Entonces $C(x)=E[x]$ y obtenemos que

$$\sum_{n\le x}\frac{1}{n}=\frac{E[x]}{x}+\int_1^x\frac{E[t]}{t^2}\,dt=\log x+\gamma+R(x),$$

donde, en principio, estamos llamando γ a

$$\gamma=1-\int_1^{+\infty}\frac{t-E[t]}{t^2}\,dt$$

y

$$R(x)=\int_x^{+\infty}\frac{t-E[t]}{t^2}\,dt-\frac{x-E[x]}{x}=O(1/x),$$

pues

$$|R(x)|\le\int_x^{+\infty}\frac{dt}{t^2}+\frac{1}{x}=\frac{2}{x}.$$

Así pues:

$$\sum_{n\le x}\frac{1}{n}=\frac{E[x]}{x}+\int_1^x\frac{E[t]}{t^2}\,dt=\log x+\gamma+O(1/x),$$

lo que en particular implica que γ cumple (2.4), por lo que se trata de la constante de Euler que ya conocemos.

2) Ahora tomamos $f(t)=1/t^2$, con lo que

$$\sum_{n\le x}\frac{1}{n^2}=\frac{E[x]}{x^2}+2\int_1^x\frac{E[t]}{t^3}\,dt=\frac{E[x]}{x^2}-2\int_1^x\frac{t-E[t]}{t^3}\,dt+2\int_1^x\frac{1}{t^2}\,dt$$

$$=2+\frac{E[x]}{x^2}-\frac{2}{x}-2\int_1^x\frac{t-E[t]}{t^3}\,dt.$$

Si hacemos tender x a $+\infty$ queda

$$\frac{\pi^2}{6} = 2 - 2\int_1^\infty \frac{t - E[t]}{t^3}\,dt,$$

luego

$$\frac{\pi^2}{6} - \sum_{n\le x}\frac{1}{n^2} = \frac{2}{x} - \frac{E[x]}{x^2} - 2\int_x^{+\infty}\frac{t-E[t]}{t^3}\,dt$$

$$\le \frac{2}{x} - \frac{x-1}{x^2} \le \frac{x+1}{x^2} = O(1/x).$$

3) En 2.8 hemos probado que la serie converge a $6/\pi^2$. Ahora se trata de estimar las aproximaciones por sumas parciales:

$$\left|\frac{6}{\pi^2} - \sum_{n\le x}\frac{\mu(n)}{n^2}\right| = \left|\sum_{n>x}\frac{\mu(n)}{n^2}\right| \le \sum_{n>x}\frac{1}{n^2} = \frac{\pi^2}{6} - \sum_{n\le x}\frac{1}{n^2} = O(1/x).$$

4) La relación $\phi = m * N$ nos da que

$$\sum_{n\le x}\phi(n) = \sum_{n\le x}\sum_{d|n}\mu(d)\,\tfrac{n}{d} = \sum_{d\le x}\sum_{m\le x/d}\mu(d)m = \sum_{d\le x}\mu(d)\sum_{m\le x/d} m.$$

Si llamamos $f(x) = \sum_{n\le x} n - \frac{x^2}{2}$, la relación (2.1) equivale a que $|f(x)| \le Cx$. Usando los apartados anteriores concluimos que

$$\sum_{n\le x}\phi(n) = \sum_{d\le x}\mu(d)\left(\frac{x^2}{2d^2} + f(x/d)\right) \le \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + C\sum_{d\le x}\frac{x}{d}$$

$$= \frac{x^2}{2}\left(\frac{6}{\pi^2} + O(1/x)\right) + Cx(\log x + O(1)) = \frac{3}{\pi^2}\,x^2 + O(x) + O(x\log x) + O(x)$$

$$= \frac{3}{\pi^2}\,x^2 + O(x\log x).$$

Hemos usado que si dividimos entre $x\log x$ la suma de dos funciones que permanecen acotadas cuando se dividen entre x y una que permanece acotada cuando se divide entre $x\log x$, obtenemos la suma de dos funciones que tienden a 0 y otra acotada, luego la suma total está acotada. ∎

Veamos un par de aplicaciones:

Números libres de cuadrados No es posible hablar en sentido estricto (es decir, en el sentido de la teoría de probabilidades) de la probabilidad de que un número natural sea par. Sin embargo, podemos decir que esta probabilidad es igual a 1/2 en el sentido de que, si elegimos al azar un número natural no nulo entre los números $\le x$, la probabilidad de que sea par (definida como el cociente entre los $E[x/2]$ casos favorables sobre los $E[x]$ casos posibles) cumple que

$$\lim_{x\to+\infty}\frac{E[x/2]}{E[x]} = \frac{1}{2}.$$

En otras palabras: la probabilidad de que un número natural elegido al azar en el intervalo $[1, x]$ sea par es aproximadamente $1/2$, y el error de la aproximación tiende a 0 cuando x tiende a infinito.

En este mismo sentido, es fácil ver que, por ejemplo, la probabilidad de que un número sea un cuadrado perfecto es 0, pues en este caso se trata de

$$\lim_{x\to+\infty} \frac{E[\sqrt{x}]}{E[x]} = 0.$$

Ahora vamos a calcular una probabilidad no trivial:

La probabilidad de que un número natural no nulo sea libre de cuadrados es $6/\pi^2 \approx 0.6$.

En efecto, si llamamos $L(x)$ al número de números libres de cuadrados $\leq x$, se trata de probar que

$$\lim_{x\to+\infty} \frac{L(x)}{x} = \frac{6}{\pi^2}.$$

(en principio falta una parte entera en el denominador, pero es claro que es irrelevante ponerla o no).

Para ello observamos que si $y > 0$, cada número natural menor o igual que y^2 es de la forma $m^2 n \leq y^2$, donde n es libre de cuadrados, y el número total de tales números con un m fijo es $L(y^2/m^2)$, luego

$$E[y^2] = \sum_{m\leq y} L((y/m)^2).$$

La fórmula de inversión 2.13 nos da que

$$L(y^2) = \sum_{m\leq y} \mu(m) E[(y/m)^2].$$

Si quitamos la parte entera, estamos quitando una función acotada por

$$\sum_{m\leq y} |\mu(m)| \leq y,$$

luego

$$L(y^2) = y^2 \sum_{m\leq y} \frac{\mu(m)}{m^2} + O(y) = \frac{6y^2}{\pi^2} + y^2 O(1/y) + O(y) = \frac{6y^2}{\pi^2} + O(y).$$

Equivalentemente:

$$L(x) = \frac{6x}{\pi^2} + O(\sqrt{x}).$$

Esto implica en particular que la probabilidad es la indicada. ∎

Números primos entre sí Similarmente podemos probar:

> *La probabilidad de que dos números naturales elegidos al azar sean primos entre sí es de* $6/\pi^2 \approx 0.6$.

Si N es un número natural grande, las posibilidades de elegir dos números al azar $\leq N$ son N^2. El número de casos en que éstos son primos entre sí puede calcularse como sigue:

Llamemos $A_n = \big\{(m,n) \;\big|\; 1 \leq m \leq n,\ (m,n) = 1\big\}$. Entonces A_n tiene $\phi(n)$ elementos y

$$\bigcup_{n\leq N} A_n = \big\{(m,n) \;\big|\; 1 \leq m \leq n \leq N,\ (m,n) = 1\big\}$$

tiene $\sum_{n\leq N} \phi(n)$ elementos. El conjunto que queremos contar es

$$\big\{(m,n) \;\big|\; 1 \leq m,n \leq N,\ (m,n) = 1\big\},$$

y es claro que consta de $2\sum_{n\leq N} \phi(n) - 1$ pares, pues al multiplicar por 2 estamos contando dos veces el par $(1,1)$, que es el único con componentes iguales.

Así pues, queremos calcular el límite de la sucesión

$$\frac{1}{N^2}\Big(2\sum_{n\leq N} \phi(n) - 1\Big),$$

o, equivalentemente, el de la función

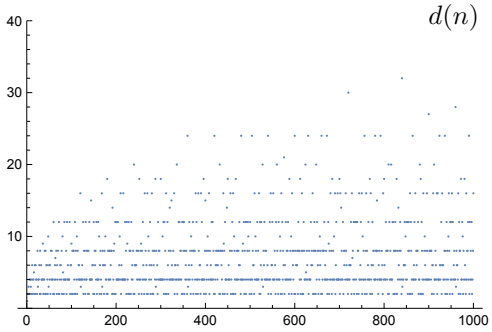
$$\frac{1}{x^2}\Big(2\sum_{n\leq x} \phi(n) - 1\Big) = \frac{6}{\pi^2} + \frac{2}{x^2}\,O(x\log x) - \frac{1}{x^2} = \frac{6}{\pi^2} + O\left(\frac{\log x}{x}\right) - \frac{1}{x^2}.$$

Obviamente el límite vale $6/\pi^2$. ∎

El número de divisores Estudiamos ahora el orden de crecimiento de la función $d(n)$ que asigna a cada número n su número de divisores. Recordemos que si

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

entonces $d(n) = (e_1 + 1)\cdots(e_r + 1)$. Se trata de una función muy irregular, como muestra la figura siguiente:



Observemos que, salvo en el caso $d(1) = 1$, tenemos que $d(n) \geq 2$, y, de hecho, $d(p) = 2$ si y sólo si p es un número primo, por lo que d toma infinitas veces el valor 2. Más precisamente, tenemos el límite inferior

$$\underline{\lim}_n d(n) = 2.$$

Por otra parte, es obvio que $d(n)$ puede tomar valores arbitrariamente grandes.

La mayor dificultad a la hora de estimar el crecimiento de $d(n)$ es que depende de la descomposición en factores primos de n, y la factorización de un número no tiene nada que ver con la del número anterior o posterior, sino que después de un número con muchos divisores puede venir un primo o viceversa. Por ello el estudio del orden de crecimiento de $d(n)$ es un problema más complicado que el de todas las funciones que hemos abordado hasta ahora. Pese a ello, estamos en condiciones de aproximarlo con precisión. De hecho, lo difícil es "no pasarse", porque vamos a ver, por ejemplo, que

$$d(n) = o(n^\epsilon), \qquad \text{para todo } \epsilon > 0, \tag{2.5}$$

de modo que si dividimos $d(n)$ entre n^ϵ, no sólo hacemos que la sucesión pase a estar acotada, sino que de hecho la hemos hecho tender a 0. Una estimación más fina es la siguiente:

Teorema 2.22 *Para todo $\epsilon > 0$ existe un n_0 tal que, si $n \geq n_0$, entonces*

$$\log d(n) \leq (1+\epsilon)\log 2 \frac{\log n}{\log\log n}.$$

Equivalentemente,

$$\overline{\lim_n} \frac{\log d(n) \log\log n}{\log n} \leq \log 2,$$

o también

$$d(n) \leq e^{(1+\epsilon)\log 2 \frac{\log n}{\log\log n}} = 2^{\frac{(1+\epsilon)\log n}{\log\log n}} = n^{\frac{(1+\epsilon)\log 2}{\log\log n}}.$$

De aquí se sigue (2.5), pues

$$\frac{d(n)}{n^\epsilon} \leq e^{(\frac{(1+\epsilon)\log 2}{\log\log n} - \epsilon)\log n} \to 0.$$

Demostración: Dado $n = p_1^{e_1} \cdots p_r^{e_r}$, consideremos un $\delta > 0$ que luego especificaremos. Entonces

$$\frac{d(n)}{n^\delta} = \prod_{i=1}^r \frac{e_i + 1}{p_i^{e_i\delta}}.$$

La serie de Taylor de e^x muestra que, si $x > 0$, entonces $1 + x \leq e^x$, por lo que

$$e_i\delta\log 2 \leq e^{e_i\delta\log 2} = 2^{e_i\delta} \leq p_i^{e_i\delta}.$$

$$\frac{e_i+1}{p_i^{e_i\delta}} \le \frac{e_i+p_i^{e_i\delta}}{p_i^{e_i\delta}} = 1+\frac{e_i}{p_i^{e_i\delta}} \le 1+\frac{1}{\delta\log 2} \le e^{1/(\delta\log 2)}.$$

Por otra parte, si $p_i \ge 2^{1/\delta}$, entonces $p^\delta \ge 2$ y

$$\frac{e_i+1}{p_i^{e_i\delta}} \le \frac{e_i+1}{2^{e_i}}.$$

Por lo tanto,

$$\frac{d(n)}{n^\delta} = \prod_{p_i<2^{1/\delta}} \frac{e_i+1}{p_i^{e_i\delta}} \prod_{p_i\ge 2^{1/\delta}} \frac{e_i+1}{p_i^{e_i\delta}} \le \prod_{p\le 2^{1/\delta}} e^{1/(\delta\log 2)} \le e^{2^{1/\delta}/(\delta\log 2)}.$$

Equivalentemente,

$$\log d(n) - \delta\log n \le \frac{2^{1/\delta}}{\delta\log 2}.$$

Ahora tomamos, concretamente,

$$\delta = \frac{(1+\epsilon/2)\log 2}{\log\log n},$$

con lo que

$$2^{1/\delta} = 2^{\frac{\log\log n}{(1+\epsilon/2)\log 2}} = e^{\frac{\log\log n}{1+\epsilon/2}} = (\log n)^{1/(1+\epsilon/2)}.$$

Por lo tanto,

$$\log d(n) \le \frac{(1+\epsilon/2)\log 2\log n}{\log\log n} + \frac{(\log n)^{1/(1+\epsilon/2)}\log\log n}{(1+\epsilon/2)\log^2 2}.$$

Observemos ahora que, para todo n suficientemente grande,

$$\frac{(\log n)^{1/(1+\epsilon/2)}\log\log n}{(1+\epsilon/2)\log^2 2} \le \frac{\epsilon\log 2\log n}{2\log\log n},$$

pues esto equivale a

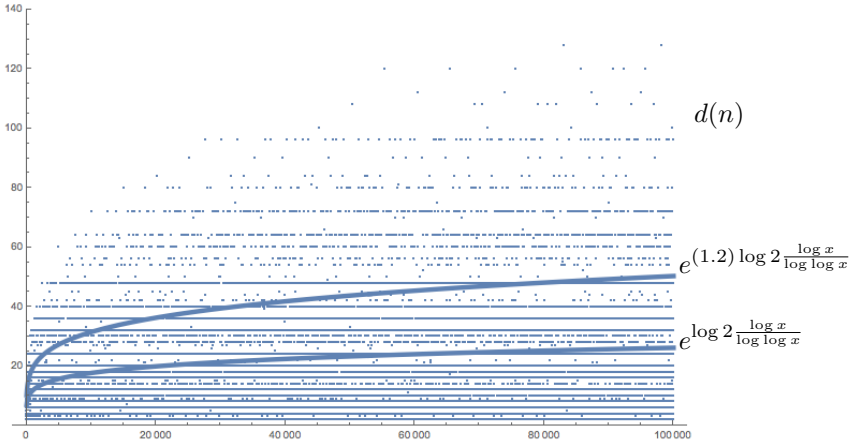
$$\frac{\log^2\log n}{(\log n)^{\frac{\epsilon/2}{1+\epsilon/2}}} \le \frac{\epsilon}{2}\left(1+\frac{\epsilon}{2}\right)\log^3 2 \tag{2.6}$$

y el miembro izquierdo tiende a 0 con n (pues, si llamamos $x = \log n$, es de la forma $\frac{\log^2 x}{x^\alpha}$). Así pues,

$$\log d(n) \le \frac{(1+\epsilon/2)\log 2\log n}{\log\log n} + \frac{(\epsilon/2)\log 2\log n}{\log\log n} = \frac{(1+\epsilon)\log 2\log n}{\log\log n}.$$

■

Nota A la vista de la figura siguiente:

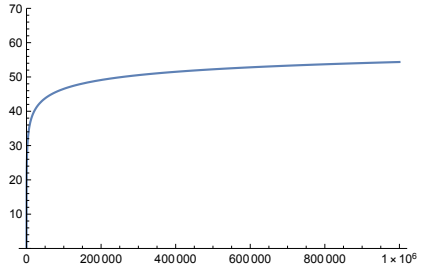


lo primero que cabe pensar es que el teorema es falso, pues deberíamos ver que, a partir de cierto valor, la función $d(n)$ queda por debajo de la mayor de las dos curvas. Si extendemos la gráfica hasta, digamos, $n = 10^6$, la imagen es similar.

La razón es que hemos probado que la función $d(n)$ debe quedar por debajo de la curva mayor para todo n suficientemente grande, pero ¿cómo de grande? El único punto de la prueba que requiere que n sea grande es (2.6) que, para $\epsilon = 0.2$, es, concretamente

$$\frac{\log^2 \log n}{(\log n)^{0.09}} \leq 0.037.$$

Ahora bien, llamando $x = \log n$, ésta es la gráfica de $\dfrac{\log^2 x}{x^{0.09}}$:



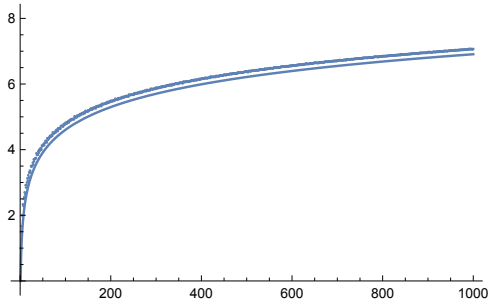
La prueba se basa en que esta función tiende a 0 en $+\infty$, pero nada en la gráfica apunta a que esto es así. Sucede que la función crece hasta tomar su valor máximo en $x_0 = e^{2/0.09} \approx 3.58 \cdot 10^9$, y sólo a partir de ahí empieza a descender hacia 0, y no llega a 0.037 hasta $x \approx 2.6 \cdot 10^{63}$, luego hemos probado que la función $d(n)$ queda por debajo de $e^{(1.2)\log 2\frac{\log n}{\log\log n}}$ para $n \geq e^{2.6\cdot 10^{63}}$. En realidad nada impide que el teorema se cumpla para valores menores de n, pero sólo hemos probado que se cumple a partir de este valor.

Así pues, el teorema anterior prueba una propiedad de la función $d(n)$ que sólo es aplicable a números prácticamente inalcanzables para la capacidad de cálculo de cualquier ordenador. ∎

La irregularidad de la sucesión $d(n)$ contrasta con la regularidad que exhibe la función

$$\frac{1}{n}\sum_{k\le n} d(k)$$

que determina el número medio de divisores que tienen los números hasta n. He aquí su gráfica junto con la de $\log x$ (que es la menor de las dos):



Vemos que la distancia entre ambas se mantiene aproximadamente constante. Esto se debe al teorema siguiente, debido a Dirichlet:

Teorema 2.23 *Se cumple que*

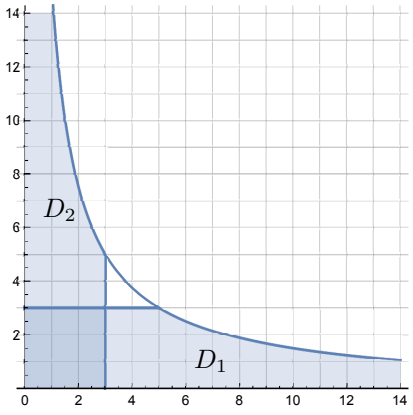
$$\sum_{k\le x} d(k) = x\log x + (2\gamma - 1)x + O(\sqrt{x}).$$

En particular,

$$\lim_{x\to+\infty} \frac{\sum_{k\le x} d(k)}{x} - \log x = 2\gamma - 1 = 0.1544313298\ldots$$

Demostración: Observemos que $d(k)$ es el número de pares de números naturales (u, v) tales que $uv = k$, luego $\sum_{k\le x} d(k)$ es el número de pares de números naturales no nulos tales que $uv \le x$.

Equivalentemente, es el número de pares de números naturales no nulos situados en la región D situada bajo la hipérbola $uv = x$. Llamemos $w = E[\sqrt{x}]$ y sean D_1 y D_2 los conjuntos de los puntos $(u, v) \in D$ que cumplen $1 \le u \le w$ y $1 \le v \le w$, respectivamente. Sucede que D_1 y D_2 cubren todo D salvo una pequeña región "triangular".



Pero en dicha región no puede haber puntos con coordenadas enteras, pues tendría que ser $u, v > w$ y $uv \le x$, pero entonces $(w + 1)^2 \le uv \le x$, luego $w + 1 \le \sqrt{x}$, contradicción.

Por consiguiente, el número de puntos con coordenadas enteras (no nulas) en D es la suma de los puntos en D_1 más los puntos en D_2 menos w^2, pues $D_1 \cap D_2$ contiene w^2 puntos. Por simetría, hay el mismo número de pares en D_1 que en D_2, así que basta contar los situados en D_1.

Puntos con $v = 1$ hay $E[x/1]$, puntos con $v = 2$ hay $E[x/2]$, etc. En total:

$$\sum_{k\le x} d(k) = 2\sum_{d\le\sqrt{x}} E[x/d] - w^2 = 2\sum_{d\le\sqrt{x}} (E[x/d] - d) + w,$$

donde hemos usado que $2\sum_{d\le\sqrt{x}} d = w^2 + w$. Si quitamos las partes enteras estamos añadiendo una función acotada por $\sqrt{x}$, luego, usando 2.21:

$$\sum_{k\le x} d(k) = 2\sum_{d\le\sqrt{x}} (x/d - d) + O(\sqrt{x}) = 2x\sum_{d\le\sqrt{x}} \tfrac{1}{d} - 2\sum_{d\le\sqrt{x}} d + O(\sqrt{x})$$

$$= 2x(\log\sqrt{x} + \gamma + O(1/\sqrt{x})) - 2(\sqrt{x}^2/s + O(\sqrt{x})) + O(\sqrt{x}))$$

$$= x\log x + (2\gamma - 1)x + O(\sqrt{x}).$$

■

Terminamos esta sección calculando el orden de crecimiento de un par de funciones que necesitaremos más adelante:

Teorema 2.24 *Se cumple:*

$$\sum_{n\le x} d^2(n) = O(x\log^3 x), \qquad \sum_{m<n\le x} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)} = O(x\log^3 x).$$

Demostración: Por el teorema anterior existe una constante $c > 0$ tal que

$$\sum_{k\le x} d(k) \le cx\log x.$$

$$\sum_{n\le x} d^2(n) = \sum_{n\le x} d(n)\sum_{k|n} 1 = \sum_{k\le x}\sum_{km\le x} d(km) \le \sum_{k\le x}\sum_{m\le k/x} d(k)d(m)$$

$$= \sum_{k\le x} d(k)\sum_{m\le x/k} d(m) \le c\sum_{k\le x} d(k)\frac{x}{k}\log(x/k) \le cx\log x\sum_{k\le x}\frac{d(k)}{k}$$

Por el teorema 2.20:

$$\sum_{k\le x}\frac{d(k)}{k} = \sum_{k\le x} d(k)\frac{1}{x} + \int_1^x \sum_{k\le t} d(k)\frac{1}{t^2}dt$$

$$\le cx\log x\frac{1}{x} + c\int_1^x t\log t\frac{1}{t^2}\,dt = c\log x + c\int_1^x \frac{\log t}{t}\,dt$$

$$= c\log x + \frac{c}{2}\log^2 x = O(\log^2 x).$$

En total obtenemos que

$$\sum_{n\le x} d^2(n) = O(x\log^3 x).$$

Para probar la segunda estimación demostramos primero lo siguiente: si k es un número natural no nulo y $k \le x$, entonces

$$\sum_{1\le r\le x-k} d(r)d(r+k) < 4x(\log x+1)^2 \sum_{d\mid k}\frac{1}{d}. \tag{2.7}$$

El sumatorio de la izquierda es igual al número de descomposiciones $r = mm'$ y $r + k = nn' \le x$, es decir, el número de cuádruplas (m, m', n, n') de números naturales no nulos tales que $mm' - nn' = k$, $mm' \le x$. Si llamamos S al número de cuádruplas que además cumplen $mn \le x$ y S' al de las que cumplen $m'n' \le x$, por simetría tenemos que $S = S'$, y toda cuádrupla está contada al menos en S o en S', pues $mnm'n' = mm'nn' < (mm')^2 \le x^2$. Así pues,

$$\sum_{1\le r\le x-k} d(r)d(r+k) \le S + S' = 2S = 2\sum_{mn\le x} N(m,n),$$

donde $N(m, n)$ es el número de pares (m', n') que cumplen

$$mm' - nn' = k, \qquad 0 < m' \le x/m, \qquad n' > 0.$$

Fijados m y n, sea $d = (m, n)$, $m = dm_0$, $n = dn_0$. Así, si $d \nmid k$, entonces $N(m, n) = 0$, mientras que si $d \mid k$, es conocido [ITAl 2.1] que las soluciones de la ecuación diofántica $mm' - nn' = k$ son de la forma

$$m' = m'_0 + rn/d, \qquad n' = n'_0 + rm/d,$$

donde (m'_0, n'_0) es una solución particular y r es un entero arbitrario. Por lo tanto $N(m, n)$ es menor o igual que el número de enteros r que cumplen

$$0 < m'_0 + rn/d \le x/m.$$

Tales enteros están en el intervalo $\Big[-\frac{m'_0 d}{n}, \frac{xd}{mn} - \frac{m'_0 d}{n}\Big]$, luego

$$N(m,n) \le E[\frac{xd}{mn} - \frac{m'_0 d}{n}] - E[-\frac{m'_0 d}{n}] = E[\frac{xd}{mn}] < \frac{xd}{mn} + 1 \le \frac{2xd}{mn} = \frac{2x}{dm_0 n_0}.$$

Por consiguiente,

$$\sum_{1\le r\le x-k} d(r)d(r+k) < 4x\sum_{d\mid k}\frac{1}{d}\sum_{m_0,n_0\le x}\frac{1}{m_0 n_0}$$

$$\le 4x\sum_{d\mid k}\frac{1}{d}\Big(\sum_{1\le m\le x}\frac{1}{m}\Big)^2 \le 4x\sum_{d\mid k}\frac{1}{d}(\log x+1)^2,$$

donde hemos acotado $1/m \le \int_{m-1}^{m}(1/t)\,dt$, con lo que $\sum_{1\le m\le x}(1/m) \le \log x$. Esto termina la prueba de (2.7).

Si $1 \le m < n$, tenemos que

$$\log^{-1}(n/m) = (-\log(1 - \frac{n-m}{n}))^{-1} < \frac{n}{n-m} = 1 + \frac{m}{n-m} < 1 + \frac{(mn)^{1/2}}{n-m}.$$

Por lo tanto,

$$\sum_{m<n\le x} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)} < \sum_{m<n\le x} \frac{d(m)d(n)}{(mn)^{1/2}} + \sum_{m<n\le x} \frac{d(m)d(n)}{n-m}.$$

Por una parte,

$$\sum_{m<n\le x} \frac{d(m)d(n)}{(mn)^{1/2}} < \left(\sum_{n=1}^{E[x]} \frac{d(n)}{\sqrt{n}}\right)^2 = O(\sqrt{x}\log x)^2 = O(x\log^2 x),$$

aplicando el teorema 2.20 igual que antes. Por otra parte, llamando $k = n - m$ y aplicando (2.7),

$$\sum_{m<n\le x} \frac{d(m)d(n)}{n-m} = \sum_{k=1}^{E[x-1]} \frac{1}{k} \sum_{m=1}^{E[x-k]} d(m)d(m+k)$$

$$< 4x(\log x + 1)^2 \sum_{k=1}^{E[x-1]} \frac{1}{k} \sum_{d|k} \frac{1}{d} \le 4x(\log x + 1)^2 \sum_{dd'\le x} \frac{1}{d^2 d'}$$

$$\le 4x(\log x + 1)^2 \sum_{d\le x} \frac{1}{d^2} \sum_{d'\le x} \frac{1}{d'}$$

$$\le 4x(\log x + 1)^2 \sum_{d=1}^{\infty} \frac{1}{d^2} \sum_{d'\le x} \frac{1}{d'} = O(x\log^3 x),$$

donde nuevamente hemos acotado $\sum_{d'\le x} \frac{1}{d'} \le 1 + \log x = O(\log x)$. ∎

Capítulo III

La distribución de los números primos

Empezamos a abordar aquí uno de los temas principales de la teoría analítica de números: el estudio de la distribución de los números primos, en el sentido que hemos explicado en la introducción. En particular, demostraremos el teorema de los números primos haciendo uso de la teoría de funciones de variable compleja, pero dedicaremos las primeras secciones a probar algunos resultados que sólo requieren técnicas analíticas más elementales.

3.1 Preliminares

Empezamos probando algunos hechos variados que vamos a necesitar en las secciones siguientes. Por ejemplo, en la introducción hemos presentado dos versiones del teorema de los números primos:

$$\pi(x) \sim \frac{x}{\log x} \sim \mathrm{Il}(x) = \int_2^x \frac{dt}{\log t}.$$

Empezamos probando que son equivalentes:

Teorema 3.1 *Se cumple*

$$\frac{x}{\log x} \sim \mathrm{Il}(x).$$

Demostración: Integrando por partes obtenemos

$$\mathrm{Il}(x) = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t},$$

luego

$$\frac{\mathrm{Il}(x)}{x/\log x} = 1 - \frac{2}{\log 2}\frac{\log x}{x} + \frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}.$$

Ahora basta probar que

$$\lim_{x\to+\infty} \frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} = 0.$$

En efecto:

$$\frac{\log x}{x} \int_2^x \frac{1}{\log^2 t}\, dt = \frac{\log x}{x} \left(\int_2^{\sqrt{x}} \frac{1}{\log^2 t}\, dt + \int_{\sqrt{x}}^x \frac{1}{\log^2 t}\, dt \right)$$

$$\leq \frac{\log x}{x} \left(\int_2^{\sqrt{x}} \frac{1}{\log^2 2}\, dt + \int_{\sqrt{x}}^x \frac{1}{\log^2 \sqrt{x}}\, dt \right) \leq \frac{\log x}{x} \left(\frac{\sqrt{x}}{\log^2 2} + \frac{x}{\log^2 \sqrt{x}} \right)$$

$$= \frac{\log x}{(\log^2 2)\sqrt{x}} + \frac{4}{\log x} \to 0. \qquad \blacksquare$$

En la sección siguiente demostraremos varias equivalencias adicionales. Probamos ahora un resultado que necesitaremos en la última sección.

Teorema 3.2 *Sea $\{b_n\}_{n=2}^{\infty}$ una sucesión de números complejos y $\alpha \in \mathbb{C}$. Si*

$$\sum_{2\leq n\leq x} b_n = \alpha x + o(x),$$

entonces

$$\sum_{2\leq n\leq x} \frac{b_n}{\log n} = \alpha \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Demostración: Llamando $C(x) = \sum_{2\leq n\leq x} b_n$, por 2.20 tenemos que

$$\sum_{2\leq n\leq x} \frac{b_n}{\log n} = \frac{1}{\log x} C(x) + \int_2^x \frac{C(t)}{t} \frac{1}{\log^2 t}\, dt.$$

Por lo tanto,

$$\frac{\log x}{x} \Big| \sum_{2\leq n\leq x} \frac{b_n}{\log n} - \alpha \frac{x}{\log x} \Big| \leq \frac{C(x) - \alpha x}{x} + \frac{\log x}{x} \Big| \int_2^x \frac{C(t)}{t} \frac{1}{\log^2 t}\, dt \Big|.$$

Como el cociente $C(t)/t$ converge a α, está acotado, digamos por M, con lo que

$$\frac{\log x}{x} \Big| \int_2^x \frac{C(t)}{t} \frac{1}{\log^2 t}\, dt \Big| \leq M \frac{\log x}{x} \Big| \int_2^x \frac{1}{\log^2 t}\, dt \Big|$$

y en la prueba del teorema anterior hemos visto que el miembro derecho tiende a 0. $\blacksquare$

Un resultado elemental que vamos a necesitar y que tiene interés en sí mismo es la descomposición en factores primos de los factoriales:

$$n! = \prod_p p^{j(n,p)}, \tag{3.1}$$

donde $j(n,p) = \sum_{m\geq 1} E[n/p^m]$.

Basta tener en cuenta que en $n!$ hay $E[n/p]$ múltiplos de p, de los cuales $E[n/p^2]$ son múltiplos de p^2, etc.

Otro hecho interesante es la cota siguiente del producto de los primeros primos:

Teorema 3.3 $\prod_{p\leq n} p < 4^n$.

DEMOSTRACIÓN: Lo probamos por inducción sobre n. Es claro que se cumple para los primeros valores de n, así que podemos suponer $n \geq 3$. Si n es par, entonces no es primo, luego

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p < 4^{n-1} < 4^n.$$

Si $n = 2m+1$, entonces, como

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!},$$

los primos $p > m+1$ no dividen al denominador, luego

$$\prod_{m+1<p\leq 2m+1} p \quad | \binom{2m+1}{m} = \tfrac{1}{2}\left(\binom{2m+1}{m} + \binom{2m+1}{m+1}\right) \leq \tfrac{1}{2}(1+1)^{2m+1} = 4^m.$$

Por lo tanto,

$$\prod_{p\leq n} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq n} p \leq 4^{m+1}4^m = 4^n. \qquad \blacksquare$$

Nota En realidad puede demostrarse que $\prod_{p\leq n} p < 3^n$, pero la prueba es más complicada. $\blacksquare$

Con la misma técnica podemos obtener una cota superior sencilla de la función $\pi(x)$:

Teorema 3.4 *Para todo $x > 1$ se cumple que*

$$\pi(x) \leq 6 \log 2 \frac{x}{\log x}.$$

DEMOSTRACIÓN: Como en la prueba del teorema anterior,

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}.$$

Tomando logaritmos, $(\pi(2n)-\pi(n))\log n \le 2n\log 2$, luego

$$\pi(2n) \le \pi(n) + 2\log 2\frac{n}{\log n}.$$

Ahora una simple inducción prueba que $\pi(2^k) \le 3\dfrac{2^k}{k}$. En efecto, se verifica directamente para $k \le 5$ y, en general,

$$\pi(2^{k+1}) \le \pi(2^k) + 2\log s\frac{2^k}{k\log 2} = \pi(2^k) + \frac{2^{k+1}}{k}$$

$$\le \frac{3\cdot 2^k}{k} + \frac{2\cdot 2^k}{k} = \frac{5\cdot 2^k}{k} \le \frac{3\cdot 2^{k+1}}{k}.$$

Por último, para $x > 4$, tomamos $4 \le 2^k < x \le 2^{k+1}$, con lo que

$$\pi(x) \le \pi(2^{k+1}) \le 6\frac{2^k}{k+1} \le 6\log 2\,\frac{x}{\log x}.$$

Se comprueba directamente que el resultado es válido para $1 < x \le 4$. ∎

Veamos un ejemplo mucho más elemental de cota superior:

Teorema 3.5 *Para todo $x \ge 1$ se cumple que*

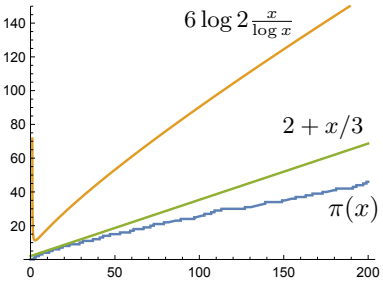
$$\pi(x) \le \frac{x}{3} + 2.$$

Demostración: Si $E[x] = 6k + r$, con $0 \le r < 6$, observamos que entre los seis primeros números naturales, $0, 1, 2, 3, 4, 5$ hay 3 primos, en cada uno de los $k-1$ bloques siguientes de 6 naturales puede haber a lo sumo 2 primos (pues todo primo $p > 3$ cumple $p \equiv 1, 5$ (mód 6)), y en el último bloque de $r < 6$ números naturales puede haber a lo sumo 1 primo si $r < 5$ o 2 primos si $r = 5$. Así pues,

$$\pi(x) \le 3 + 2(k-1) + \delta = 2k + \delta + 1 \le 2 + \frac{6k+r}{3} \le 2 + \frac{x}{3},$$

donde $\delta = 1$ salvo si $r = 5$, en cuyo caso $r = 2$. La penúltima desigualdad equivale a $3(\delta - 1) \le r$, que se cumple por definición de δ. ∎

La figura muestra las dos aproximaciones que hemos encontrado de $\pi(x)$. No son muy buenas, y empeoran cuando aumenta x. Podría pensarse que el teorema anterior implica el precedente, pero no es así, porque $2 + x/3$ sólo es mejor aproximación provisionalmente, pues es claro que



$$\lim_{x\to+\infty} 6\log 2\frac{x}{2+x/3}\frac{1}{\log x} = 0,$$

luego a partir de un momento dado las posiciones se invierten. Concretamente, ambas funciones se igualan cuando $x = 262069.13$, pero para entonces ambas están tan alejadas de $\pi(x)$ que importa poco cuál esté más cerca.

3.2 Las funciones de Chebyshev

Definición 3.6 Las *funciones de Chebyshev* son las dadas por

$$\vartheta(x) = \sum_{p\le x} \log p, \qquad \psi(x) = \sum_{n\le x} \Lambda(n),$$

donde Λ es la función de Mangoldt definida en 2.10. Más precisamente, ϑ y ψ se conocen, respectivamente, como la *primera* y la *segunda función de Chebyshev.*

Como hemos indicado en la introducción, las funciones de Chebyshev recogen información relevante sobre la distribución de los números primos, que se plasma en las relaciones $\psi(x) \sim x \sim \vartheta(x)$. No estamos en condiciones de probarlas ahora, pero sí que podemos probar que equivalen al teorema de los números primos.

En efecto, por una parte podemos expresar

$$\vartheta(x) = \sum_{n\le x} \chi(n)\log n,$$

donde χ es la función característica de los números primos, y aplicar 2.20, que nos da que

$$\vartheta(x) = \sum_{p\le x} \log p = \pi(x)\log x - \int_2^x \pi(t)\frac{1}{t}\,dt.$$

El teorema 3.4 nos da que

$$\int_2^x \pi(t)\frac{1}{t}\,dt \le 6\log 2 \int_2^x \frac{dt}{\log t} = 6\log 2\,\mathrm{li}(x),$$

y el teorema 3.1 implica que

$$\vartheta(x) = \pi(x)\log x + O(x/\log x),$$

luego

$$\frac{\pi(x)}{x/\log x} = \frac{\vartheta(x)}{x} + O(\frac{1}{\log x}). \tag{3.2}$$

Esto ya muestra que el teorema de los números primos es equivalente a $\vartheta(x) \sim x$.

Nos ocupamos ahora de la segunda función de Chebyshev. Observemos en primer lugar que, según la definición de la función de Mangoldt, se cumple que

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{p^m\le x} \log p,$$

donde en la segunda expresión hay que entender que hay un sumando $\log p$ por cada potencia $p^m \le x$. Equivalentemente,

$$\psi(x) = \sum_{p\le x} E[\tfrac{\log x}{\log p}]\log p.$$

Teniendo en cuenta que $p^m \le x$ equivale a $p \le x^{1/m}$, tenemos que:

$$\psi(x) = \sum_m \vartheta(x^{1/m}) = \vartheta(x) + \sum_{m\ge 2} \vartheta(x^{1/m}).$$

Notemos que la serie es finita, pues los sumandos son nulos a partir del momento en que $x^{1/m} < 2$, es decir, cuando $m > \log x/\log 2$.

El número de primos $p \le x^{1/m}$ es a lo sumo $x^{1/m}$, y $\log p \le \frac{1}{m}\log x \le \log x$, luego, para $m \ge 2$, tenemos que

$$\vartheta(x^{1/m}) \le x^{1/m}\log x \le x^{1/2}\log x,$$

luego

$$\sum_{m\ge 2} \vartheta(x^{1/m}) \le \frac{1}{\log 2} x^{1/2}\log^2 x,$$

(puesto que el número de sumandos es a lo sumo $\log x/\log 2$). Más brevemente:

$$\sum_{m\ge 2} \vartheta(x^{1/m}) = O(x^{1/2}\log^2 x),$$

o también

$$\psi(x) = \vartheta(x) + O(x^{1/2}\log^2 x). \tag{3.3}$$

Esto implica a su vez que

$$\frac{\psi(x)}{x} = \frac{\vartheta(x)}{x} + O(\frac{\log^2 x}{x^{1/2}}). \tag{3.4}$$

Con el teorema 3.1 y las equivalencias (3.2) y (3.4) hemos probado el teorema siguiente:

Teorema 3.7 *Las afirmaciones siguientes son equivalentes:*

1. $\pi(x) \sim \dfrac{x}{\log x}$.
2. $\pi(x) \sim \mathrm{Il}(x)$.
3. $\vartheta(x) \sim x$.
4. $\psi(x) \sim x$.

En 3.41 probaremos que todas las afirmaciones del teorema anterior son ciertas, pero podemos probar otras propiedades más débiles de las funciones de Chebyshev que, no obstante, tienen repercusiones notables sobre la distribución de los números primos. Por ejemplo, tomando logaritmos en la desigualdad del teorema 3.3 (aplicado a $n = E[x]$) obtenemos el teorema siguiente:

Teorema 3.8 *Para todo $x \ge 1$, se cumple que $\vartheta(x) < 2x\log 2$. En particular, $\vartheta(x) = O(x)$.*

Esto no basta para probar el teorema de los números primos, pero sí para obtener un hecho notable que fue conjeturado por Joseph Bertrand en 1845 y demostrado por Chebyshev en 1852. La prueba clásica de Euclides sobre la existencia de infinitos primos consiste esencialmente en observar que, dado un número cualquiera n, tiene que existir un primo $n < p \leq n! + 1$, pero esta cota del menor primo mayor que n es exageradamente elevada y puede mejorarse mucho:

Teorema 3.9 (Postulado de Bertrand) *Para cada número natural $n \geq 1$, existe al menos un primo $n < p \leq 2n$. Equivalentemente, la sucesión de los primos cumple $p_{n+1} \leq 2p_n$.*

DEMOSTRACIÓN: Si

$$N = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{k_p}, \tag{3.5}$$

entonces, por (3.1),

$$k_p = \sum_{m=1}^{\infty} (E[2n/p^m] - 2E[n/p^m]).$$

Cada sumando de esta serie es 0 o 1, según si $E[2n/p^m]$ es par o impar. En efecto, si $2n/p^m = 2k + r$, con $0 \leq r < 1$, entonces $n/p^m = k + r/2$, luego el sumando es $2k - 2k = 0$. Si es $2n/p^m = 2k+1+r$, entonces $n/p^m = k+(r+1)/2$ y el sumando es $2k + 1 - 2k = 1$. En particular, los sumandos son nulos para $p^m > 2n$, luego

$$k_p \leq E\left(\frac{\log 2n}{\log p}\right). \tag{3.6}$$

Supongamos que existe un $n > 2^9 = 512$ para el que no existe ningún primo p en las condiciones del enunciado. Sea N el dado por (3.5) y sea $p \mid N$, de modo que $p \leq 2n$, luego por hipótesis $p \leq n$.

Supongamos que $2n/3 < p \leq n$, con lo que $2p \leq 2n < 3p$, luego también $p^2 > 4n^2/9 > 2n$. Entonces

$$k_p = E[2n/p] - 2E[n/p] = 2 - 2 = 0,$$

lo que contradice que $p \mid N$. Por lo tanto, tiene que ser $p \leq 2n/3$, luego, por el teorema 3.8, tenemos que

$$\sum_{p|N} \log p \leq \sum_{p \leq 2n/3} \log p = \vartheta(2n/3) \leq \frac{4}{3} n \log 2.$$

Si se cumple $k_p \geq 2$, entonces, por (3.6), tenemos que

$$2 \log p \leq k_p \log p \leq \log 2n,$$

luego $p \leq \sqrt{2n}$, luego hay a lo sumo $\sqrt{2n}$ primos que cumplen $k_p \geq 2$. Por lo tanto:

$$\sum_{k_p \geq 2} k_p \log p \leq \sqrt{2n} \log 2n,$$

luego

$$\log N \le \sum_{k_p=1} \log p + \sum_{k_p\ge 2} k_p \log p \le \sum_{p|N} \log p + \sqrt{2n}\log 2n$$

$$\le \frac{4}{3} n \log n + \sqrt{2n}\log 2n.$$

Por otra parte, N es el mayor de los $2n$ términos del desarrollo de $(1+1)^{2n}$, luego $2^{2n} \le 2nN$, luego

$$2n\log 2 \le \log 2n + \log N \le \frac{4}{3} n \log 2 + (1+\sqrt{2n})\log 2n,$$

de donde

$$2n\log 2 \le 3(1+\sqrt{2n})\log 2n. \tag{3.7}$$

Estamos suponiendo que $n > 512$, luego

$$\alpha = \frac{\log(n/512)}{10\log 2} > 0$$

y además

$$2^{10(1+\alpha)} = 2^{10}2^{10\alpha} = 2^{10}\frac{n}{2^9} = 2n.$$

Así (3.7) se convierte en $2^{10(1+\alpha)} \le 30(2^{5+5\alpha}+1)(1+\alpha)$, con lo que

$$2^{5\alpha} \le 30\cdot 2^{-5}(1+2^{-5-5\alpha})(1+\alpha) < (1-2^{-5})(1+2^{-5})(1+\alpha) < 1+\alpha,$$

pero

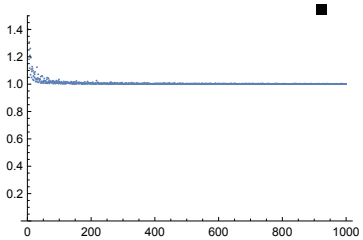
$$2^{5\alpha} = e^{5\alpha\log 2} > 1 + 5\alpha\log 2 > 1+\alpha.$$

Tenemos así una contradicción, que prueba el postulado de Bertrand para todo $n > 512$. Para primos menores también se cumple, pues basta considerar los primos:

$$2,\quad 3,\quad 5,\quad 7,\quad 13,\quad 23,\quad 43,\quad 83,\quad 63,\quad 317,\quad 631.$$

Cada uno es menor que el doble del anterior, por lo que entre n y $2n$ hay siempre uno de ellos, para todo $n < 631$. ∎

La gráfica representa la función p_{n+1}/p_n, y muestra que la cota 2 que proporciona el postulado de Bertrand no es muy fina.



Seguidamente obtenemos más estimaciones de las funciones de Chebyshev:

Teorema 3.10 *Si $x \ge 2$, existen constantes A, $B > 0$ tales que*

$$Ax \le \vartheta(x) \le 2x\log 2, \qquad \frac{1}{4}x\log 2 \le \psi(x) \le Bx.$$

DEMOSTRACIÓN: Dado $n \geq 1$, considerando de nuevo (3.5), y teniendo en cuenta (3.6), vemos que

$$\log N = \sum_{p \leq 2n} k_p \log p \leq \sum_{p \leq 2n} E\left(\frac{\log 2n}{\log p}\right) \log p = \psi(2n).$$

Por otra parte,

$$N = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdot \ldots \cdot \frac{2n}{n} \geq 2^n,$$

luego $\psi(2n) \geq n \log 2$. Si tomamos $n = E[x/2] \geq 1$, obtenemos que

$$\psi(x) \geq \psi(2n) \geq n \log 2 \geq \frac{1}{4} x \log 2.$$

En particular, $\psi(x)/x$ está acotado inferiormente, y por (3.4), lo mismo vale para $\vartheta(x)/x$ (pues se diferencia de la función anterior en una función que tiende a 0), lo que nos da la constante A del enunciado. Análogamente, el teorema 3.8 nos da la cota superior de $\vartheta(x)/x$ y entonces (3.4) nos da la constante B del enunciado. ∎

Como aplicación mejoramos el teorema 2.22:

Teorema 3.11

$$\overline{\lim_n} \frac{\log d(n) \log\log n}{\log n} = \log 2.$$

DEMOSTRACIÓN: El teorema 2.22 equivale a que el límite superior es menor o igual que $\log 2$. Para probar la desigualdad opuesta tomamos $\epsilon > 0$ y tenemos que demostrar que hay valores de n arbitrariamente grandes que cumplen

$$\frac{\log d(n) \log\log n}{\log 2 \log n} > 1 - \epsilon.$$

Basta ver que esto sucede para los números de la forma $n = p_1 \cdots p_r$, para los cuales $d(n) = 2^r$. Sea A la constante dada por el teorema anterior. Entonces

$$A p_r \leq \vartheta(p_r) = \sum_{i=1}^{r} \log p_i = \log n,$$

luego $\log A + \log p_r \leq \log\log n$. Por otra parte,

$$\pi(p_r) \log p_r = \log p_r \sum_{p \leq p_r} 1 \geq \sum_{p \leq r} \log p = \vartheta(p_r) = \log n.$$

Por consiguiente,

$$\log d(n) = \log 2^r = r \log 2 = \pi(p_r) \log 2$$

$$\geq \frac{\log n \log 2}{\log p_r} \geq \frac{\log n \log 2}{\log\log n - \log A} \geq \frac{(1-\epsilon) \log n \log 2}{\log\log n}$$

para todo n suficientemente grande, ya que la última desigualdad equivale a

$$\log\log n \geq -\frac{(1+\epsilon) \log A}{\epsilon},$$

(notemos que $\log A < 0$, pues $\vartheta(x) < x$). ∎

3.3 Los teoremas de Mertens

Vamos a estudiar ahora la serie de los inversos de los primos. En primer lugar observamos que es divergente. El argumento siguiente se debe a Clarkson y es de 1966:

Teorema 3.12 *La serie* $\sum_p \frac{1}{p}$ *es divergente.*

DEMOSTRACIÓN: Supongamos que $\sum_p \frac{1}{p} < +\infty$. Entonces existe un N tal que $\sum_{p>N} \frac{1}{p} < 1/2$. Por lo tanto

$$\sum_{t=0}^{\infty}\Big(\sum_{p>N}\frac{1}{p}\Big)^t \le \sum_{t=0}^{\infty}\frac{1}{2^t} < +\infty.$$

Ahora bien, la serie de la izquierda no es más que $\sum_{n\in A}\frac{1}{n}$, donde A es el conjunto de los números naturales no divisibles entre primos menores que N. Si llamamos P al producto de los primos menores o iguales que N tenemos que $nP+1 \in A$ para todo n, luego

$$\sum_{n=1}^{\infty}\frac{1}{nP+1} < +\infty,$$

pero por otra parte es claro que esta serie diverge, por comparación con la serie $\sum_{n=1}^{\infty}\frac{1}{n}$. Por lo tanto la serie de partida no puede converger. ∎

Ahora necesitamos un resultado técnico:

Teorema 3.13 *Si* $h > 0$*, entonces*

$$\sum_{n\le x}\log^h(x/n) = O(x).$$

DEMOSTRACIÓN: Para $n \ge 2$ tenemos que

$$\log^h(x/n) \le \int_{n-1}^{n}\log^h(x/t)\,dt.$$

Por lo tanto

$$\sum_{n=2}^{E[x]}\log^h(x/n) \le \int_1^x \log^h(x/n)\,dt = x\int_1^x \frac{\log^h u}{u^2}\,du < x\int_1^\infty \frac{\log^h u}{u^2}\,du.$$

Notemos que la integral es convergente, pues con el cambio de variable $\log u = x$ se convierte [IC 3.30] en la función factorial $\Pi(h)$. Así pues,

$$\sum_{n\le x}\log^h(x/n) < \log^h x + Ax = O(x).$$

∎

En particular,

$$\sum_{n\le x}\log n = E[x]\log x - \sum_{n\le x}\log(x/n) = E[x]\log x + O(x) = x\log x + O(x).$$

Por (3.1) tenemos que

$$\sum_{n\le x}\log n = \sum_{n\le x} j(E[x],p)\log p = \sum_{p^m\le x} E[x/p^m]\log p = \sum_{n\le x} E[x/n]\Lambda(n).$$

Si quitamos la parte entera de la última suma estamos añadiendo un término acotado por

$$\sum_{n\le x}\Lambda(n) = \psi(x) = O(x),$$

luego

$$\sum_{n\le x}\frac{x}{n}\Lambda(n) = \sum_{n\le x}\log n + O(x) = x\log x + O(x).$$

Dividiendo entre x obtenemos el teorema siguiente:

Teorema 3.14

$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \log x + O(1).$$

Y de aquí deducimos a su vez:

Teorema 3.15 (Primer teorema de Mertens)

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1).$$

Demostración: Observemos que

$$\sum_{n\le x}\frac{\Lambda(n)}{n} - \sum_{p\le x}\frac{\log p}{p} = \sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m} < \sum_p \log p \sum_{m\ge 2}\frac{1}{p^m}$$

$$= \sum_p \frac{\log p}{p(p-1)} < \sum_{n\ge 2}\frac{\log n}{n(n-1)} = \sum_{n\ge 2}\frac{n}{n-1}\frac{\log n}{n^2} \le 2\sum_{n\ge 2}\frac{\log n}{n^2}.$$

La serie converge por [ITAn 4.9], pues puede mayorarse por la suma de $1/n^{3/2}$. ∎

Ahora aplicamos 2.20 con $c_p = \frac{\log p}{p}$ y $f(x) = 1/\log x$. Así

$$C(x) = \sum_{p\le x}\frac{\log p}{p} = \log x + \tau(x),$$

donde $\tau(x)$ está acotada por el teorema anterior. Así obtenemos que

$$\sum_{p\le x}\frac{1}{p} = \frac{C(x)}{\log x} + \int_2^x \frac{C(t)}{t\log^2 t}\,dt = 1 + \frac{\tau(x)}{\log x} + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{\tau(t)}{t\log^2 t}\,dt.$$

La primera integral es $\log\log x - \log\log 2$, y la segunda es convergente, porque podemos acotar $\tau(t)$ y el resto es $1/\log 2 - 1/\log x$. Por lo tanto,

$$\sum_{p\le x}\frac{1}{p} = \log\log x + M + R(x), \tag{3.8}$$

donde

$$M = 1 - \log\log 2 + \int_2^{+\infty}\frac{\tau(t)}{t\log^2 t}\,dt$$

y

$$R(x) = \frac{\tau(x)}{\log x} - \int_x^{+\infty}\frac{\tau(t)}{t\log^2 t}\,dt = O(1/\log x).$$

En definitiva:

$$\sum_{p\le x}\frac{1}{p} = \log\log x + M + O(1/\log x).$$

Esto nos da una prueba alternativa de la divergencia de la serie de los primos. Más aún, ahora está justificada la definición siguiente:

Definición 3.16 Se define la *constante de Mertens* como

$$M = \lim_{x\to+\infty}\sum_{p\le x}\frac{1}{p} - \log\log x = 0.26149721284764278375542683\ldots$$

La constante M resulta ser el análogo para la serie de los inversos de los primos de la constante de Euler γ para la serie de los inversos de los números naturales, pero, más precisamente, hemos probado el teorema siguiente (compárese con el primer apartado del teorema 2.21):

Teorema 3.17 (Segundo teorema de Mertens)

$$\sum_{p\le x}\frac{1}{p} = \log\log x + M + O(1/\log x).$$

Existe un tercer teorema de Mertens, pero su prueba ya no es elemental, sino que requiere resultados de la teoría de funciones de variable compleja, así que lo posponemos hasta una sección posterior (teorema 3.29).

3.4 Consecuencias del teorema de los números primos

Antes de introducir las técnicas de la teoría de funciones de variable compleja que nos permitirán probar el teorema de los números primos, dedicamos esta sección a mostrar algunas consecuencias del mismo que pueden obtenerse por medios elementales. En la introducción hemos señalado que la gráfica de p_n/n se parece a la de $\log n$. Eso no era casual:

Teorema 3.18 *Sea p_n el primo n-simo. Entonces $p_n \sim n \log n$.*

DEMOSTRACIÓN: Tomando logaritmos en la fórmula del teorema de los números primos queda

$$\log \pi(x) + \log\log x - \log x \longrightarrow 0,$$

luego también

$$\frac{\log \pi(x)}{\log x} + \frac{\log\log x}{\log x} \longrightarrow 1.$$

El segundo sumando tiende a 0, con lo que

$$\lim_{x\to+\infty} \frac{\log \pi(x)}{\log x} = 1.$$

Multiplicando y dividiendo por x el denominador y aplicando de nuevo el teorema de los números primos obtenemos

$$\lim_{x\to+\infty} \frac{\pi(x)\log \pi(x)}{x} = 1,$$

Y si hacemos $x = p_n$ es claro que $\pi(p_n) = n$, luego

$$\lim_{n} \frac{n \log n}{p_n} = 1,$$

es decir, $p_n \sim n \log n$. ∎

La diferencia ostensible entre las gráficas de p_n/n y $\log n$ se debe a que, como hemos señalado en la introducción, la convergencia a 1 de $\frac{\pi(x)\log x}{x}$ es muy lenta.

El teorema siguiente es un refinamiento asintótico del postulado de Bertrand:

Teorema 3.19 *Para todo $\epsilon > 0$, existe un $x_0 > 0$ tal que, para todo $x \geq x_0$ existe un número primo $x < p \leq (1+\epsilon)x$.*

DEMOSTRACIÓN: Tenemos que

$$\frac{\pi((1+\epsilon)x)}{\pi(x)} \sim \frac{(1+\epsilon)x/\log((1+\epsilon)x)}{x/\log x} = (1+\epsilon)\frac{\log x}{\log(1+\epsilon)+\log x} \to 1+\epsilon,$$

luego

$$\lim_{x\to+\infty} \frac{\pi((1+\epsilon)x)}{\pi(x)} = 1+\epsilon.$$

Por lo tanto, para todo x suficientemente grande, $\pi(x) < \pi((1+\epsilon)x)$, luego existe un primo $x < p \leq (1+\epsilon)x$. ∎

He aquí una consecuencia curiosa:

La tabla siguiente muestra el menor primo que empieza por 1, el menor primo que empieza por 2, el menor primo que empieza por 3, y así sucesivamente hasta el menor primo que empieza por 100.

11	**2**	**3**	**41**	**5**	**61**	**7**	**83**	**97**	**101**
11	**127**	**13**	**149**	**151**	**163**	**17**	**181**	**19**	**2003**
211	**223**	**23**	**241**	**251**	**263**	**271**	**281**	**29**	**307**
31	**3203**	**331**	**347**	**353**	**367**	**37**	**383**	**397**	**401**
41	**421**	**43**	**443**	**457**	**461**	**47**	**487**	**491**	**503**
5101	**521**	**53**	**541**	**557**	**563**	**571**	**587**	**59**	**601**
61	**6203**	**631**	**641**	**653**	**661**	**67**	**683**	**691**	**701**
71	**727**	**73**	**743**	**751**	**761**	**773**	**787**	**79**	**809**
811	**821**	**83**	**8419**	**853**	**863**	**877**	**881**	**89**	**907**
911	**929**	**937**	**941**	**953**	**967**	**97**	**983**	**991**	**1009**

El teorema siguiente prueba que esta lista puede prolongarse indefinidamente:

Teorema 3.20 *Para cada número natural $N > 0$, existe un primo cuyas primeras cifras decimales son las de N.*

Demostración: Se trata de encontrar un primo p tal que $10^m N \leq p < 10^m(N+1)$, para algún m. Basta aplicar el teorema anterior con $\epsilon = 1/(N+1)$. Tomamos m suficientemente grande para que sea aplicable a $x = 10^m N$ y tenemos que un primo p tal que

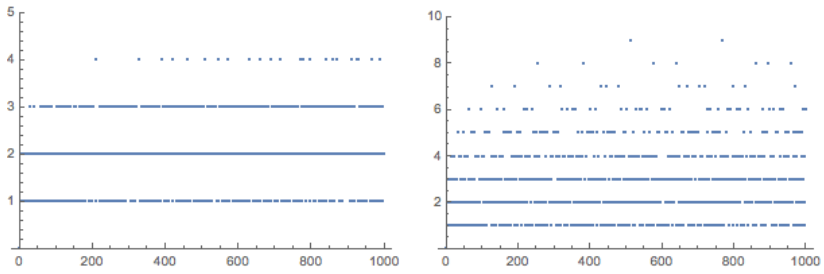
$$10^m N < p \leq \left(1 + \frac{1}{N+1}\right) 10^m N < \left(1 + \frac{1}{N}\right) 10^m N = 10^m(N+1),$$

como requeríamos. ∎

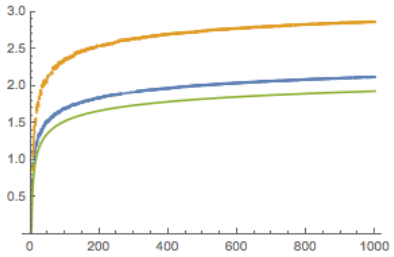
El número de divisores primos Para cada número natural n no nulo, llamamos $\omega(n)$ al número de primos distintos que lo dividen, mientras que $\Omega(n)$ será el número total de primos que lo dividen (contando multiplicidades). Equivalentemente, si $n = p_1^{e_1} \cdots p_r^{e_r}$, entonces

$$\omega(n) = r, \qquad \Omega(n) = e_1 + \cdots + e_r.$$

La figura de la izquierda es la gráfica de $\omega(n)$, y la de la derecha la de $\Omega(n)$.



En la figura siguiente, la curva superior es el valor medio de Ω, la intermedia el de ω y la inferior es $\log\log x$.



El teorema siguiente prueba lo que se observa en las gráficas (y aporta información más precisa):

Teorema 3.21

$$\sum_{n\le x}\omega(n) = x\log\log x + Mx + o(x),$$
$$\sum_{n\le x}\Omega(n) = x\log\log x + M'x + o(x),$$

donde M es la constante de Mertens y $M' = M + \displaystyle\sum_p \frac{1}{p(p-1)}$.

Demostración: Llamemos

$$S_1 = \sum_{n\le x}\omega(n) = \sum_{n\le x}\sum_{p|n} 1 = \sum_{p\le x} E[x/p],$$

pues hay $E[x/p]$ múltiplos de p menores o iguales que x. Si eliminamos la parte entera, estamos sumando un número menor que 1 a cada uno de los $\pi(x)$ sumandos, luego, por el segundo teorema de Mertens y el teorema de los números primos:

$$S_1 = \sum_{p\le x}\frac{x}{p} + O(\pi(x)) = x\log\log x + Mx + O(x/\log x).$$

Del mismo modo,

$$S_2 = \sum_{n\le x}\Omega(n) = \sum_{n\le x}\sum_{p^m|x} 1 = \sum_{p^m\le x} E[x/p^m],$$

donde hay que entender que $p^m \mid x$ significa que hay un sumando para cada potencia p^m que divide a x, con $m \ge 1$. Por consiguiente

$$S_2 - S_1 = \sum_{p^{m+1}\le x} E[x/p^{m+1}].$$

Si eliminamos las partes enteras estamos añadiendo un término acotado por

$$\sum_{p^{m+1}\le x} 1 \le \sum_{p^{m+1}\le x}\frac{\log p}{\log 2} = \sum_{p^m\le x}\frac{\log p}{\log 2} - \sum_{p\le x}\frac{\log p}{\log 2} = \frac{\psi(x)-\vartheta(x)}{\log 2} = o(x),$$

por (3.3). Por lo tanto,

$$S_2 - S_1 = x \sum_{p^{m+1}\le x} \frac{1}{p^{m+1}} + o(x).$$

Por otra parte,

$$\lim_{x\to+\infty} \sum_{p^{m+1}\le x} \frac{1}{p^{m+1}} = \sum_p \sum_{m=2}^{\infty} \frac{1}{p^m} = \sum_p \frac{1}{p(p-1)} = M' - M.$$

Así pues,

$$\sum_{p^{m+1}\le x} \frac{1}{p^{m+1}} = M' - M + o(1)$$

y a su vez $S_2 - S_1 = x(M' - M) + o(x)$. Ahora basta aplicar la estimación ya probada para S_1. ∎

De aquí podemos extraer a su vez algunas consecuencias, para lo cual necesitamos algunos conceptos:

Definición 3.22 Diremos que un conjunto $A \subset \mathbb{N}$ es *nulo* si

$$\lim_n \frac{|\{m \in A \mid m \le n\}|}{n} = 0.$$

Diremos que una propiedad $P(n)$ la cumplen *casi todos* los números naturales si el conjunto de los que no la poseen es nulo.

Dadas dos funciones aritméticas $f, g : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{R}$, diremos que f *orden normal* g si, para cada $\epsilon > 0$, casi todos los números naturales cumplen

$$\left|\frac{f(n)}{g(n)} - 1\right| < \epsilon$$

(o, equivalentemente, $(1-\epsilon)g(n) < f(n) < (1+\epsilon)g(n)$).

Es claro que la unión finita de conjuntos nulos es nula y todo subconjunto de un conjunto nulo es nulo.

Teorema 3.23 *Las funciones $\omega(n)$ y $\Omega(n)$ tienen orden normal $\log\log n$. Más precisamente, para todo $\delta > 0$, casi todos los números naturales cumplen*

$$|\omega(n) - \log\log n| \le (\log\log n)^{\frac{1}{2}+\delta},$$

e igualmente con Ω en lugar de ω.

Demostración: Notemos que la propiedad del enunciado implica ciertamente que las funciones tienen orden normal $\log\log n$. Lo que estamos afirmando, por ejemplo para $\delta = 1/2$ es que casi todos los números naturales cumplen

$$\left|\frac{\omega(n)}{\log\log n} - 1\right| \le \frac{1}{(\log\log n)^{1/2}},$$

luego, dado $\epsilon > 0$, existe un n_0 a partir del cual el miembro derecho es $< \epsilon$, y así, el conjunto de números que no cumple

$$\left|\frac{\omega(n)}{\log\log n} - 1\right| < \epsilon$$

es la unión del conjunto nulo que no cumple la desigualdad precedente más el conjunto finito formado por los números $n < n_0$.

Veamos en primer lugar que basta probar que la cantidad de números $n \leq x$ que no cumplen

$$|\omega(n) - \log\log x| \leq (\log\log x)^{\frac{1}{2}+\delta} \tag{3.9}$$

es $o(x)$. Esto se debe a que si $x^{1/e} \leq n \leq x$, entonces

$$\log\log x - 1 \leq \log\log n \leq \log\log x, \tag{3.10}$$

y la cantidad de $n \leq x$ que no cumplen $x^{1/e} \leq n$ es $O(x^{1/e}) = o(x)$.

Así pues, si hemos probado, para todo $\delta > 0$, que la cantidad de números $n \leq x$ que no cumplen (3.9) es $o(x)$, dado $\delta > 0$, tenemos que la cantidad de números naturales que no cumplen

$$|\omega(n) - \log\log x| \leq (\log\log x)^{\frac{1}{2}+\frac{\delta}{2}}$$

y (3.10) es $o(x)$, y los que sí que cumplen estas dos condiciones cumplen también

$$|\omega(n) - \log\log n| \leq |\omega(n) - \log\log x + \log\log x - \log\log n|$$

$$\leq (\log\log x)^{\frac{1}{2}+\frac{\delta}{2}} + 1 \leq (\log\log n + 1)^{\frac{1}{2}+\frac{\delta}{2}} + 1 \leq (\log\log n)^{\frac{1}{2}+\delta},$$

donde para que se cumpla la última desigualdad tenemos que exigir también que n sea suficientemente grande.

Así pues, el conjunto de los números $n \leq x$ que no cumplen la desigualdad del enunciado es $o(x)$, que es lo que hay que probar. Notemos también que esta reducción vale igualmente para Ω.

Consideremos todos los pares ordenados (p, q) de divisores primos de n tales que $p \neq q$. En total hay

$$\omega(n)^2 - \omega(n) = \sum_{\substack{pq|n \\ p\neq q}} 1 = \sum_{pq|n} 1 - \sum_{p^2|n} 1,$$

donde en el penúltimo sumatorio hay que entender que es sobre los pares ordenados (p, q) tales que $pq \mid n$. Por lo tanto,

$$\sum_{n\leq x} \omega(n)^2 - \sum_{n\leq x} \omega(n) = \sum_{pq\leq x} E[\frac{x}{pq}] - \sum_{p^2\leq x} E[\frac{x}{p^2}],$$

donde el penúltimo sumatorio es sobre los pares (p, q) tales que $pq \leq x$. Ahora

$$\sum_{p^2\leq x} E[\frac{x}{p^2}] \leq \sum_{p^2\leq x} \frac{x}{p^2} \leq x \sum_{p} \frac{1}{p^2} = O(x).$$

Por otra parte,

$$\sum_{pq\le x} E[\frac{x}{pq}] = x\sum_{pq\le x}\frac{1}{pq} + O(x),$$

pues al quitar las partes enteras estamos sumando a lo sumo $2E[x]$ números (porque cada $pq = qp$ con $p \neq q$ cuenta dos veces) menores que 1, luego el término añadido es $O(x)$. Usando el teorema anterior llegamos a que

$$\sum_{n\le x}\omega(n)^2 = x\sum_{pq\le x}\frac{1}{pq} + O(x\log\log x)$$

Ahora observamos que

$$\Big(\sum_{p\le\sqrt{x}}\frac{1}{p}\Big)^2 \le \sum_{pq\le x}\frac{1}{pq} \le \Big(\sum_{p\le x}\frac{1}{p}\Big)^2,$$

pues al elevar al cuadrado el primer sumatorio, obtenemos una suma sobre todos los pares (p,q) tales que $p,q \le \sqrt{x}$, que están entre los que cumplen $pq \le x$, y al elevar al cuadrado el último sumatorio obtenemos la suma sobre todos los pares (p,q) tales que $p,q \le x$, los cuales incluyen a los que cumplen $pq \le x$. Los dos extremos de la última fórmula son

$$(\log\log x + O(1))^2 = \log^2\log x + O(\log\log x),$$

luego

$$\sum_{n\le x}\omega(n)^2 = x\log^2\log x + O(x\log\log x).$$

A su vez,

$$\sum_{n\le x}(\omega(n)-\log\log x)^2 = \sum_{n\le x}\omega(x)^2 - 2\log\log x\sum_{n\le x}\omega(x) + E[x]\log^2\log x$$

$$= x\log^2\log x + O(x\log\log x) - 2\log\log x(x\log\log x + O(x)) +$$
$$(x+O(1))\log^2\log x$$
$$= x\log^2\log x - 2x\log^2\log x + x\log^2\log x + O(x\log\log x) = O(x\log\log x).$$

Supongamos finalmente que la cantidad de números $n \le x$ que no cumplen la condición (3.9) no fuera $o(x)$. Esto significa que para todo $\epsilon > 0$ existen valores de x arbitrariamente grandes tales que hay más de ϵx números $n \le x$ que cumplen

$$|\omega(n) - \log\log x| > (\log\log x)^{\frac{1}{2}+\delta},$$

luego

$$\sum_{n\le x}(\omega(n)-\log\log x)^2 \ge \epsilon x(\log\log x)^{1+2\delta},$$

para valores de x arbitrariamente grandes, lo cual contradice la estimación $O(x\log\log x)$ que hemos obtenido para el miembro izquierdo.

Esto prueba el teorema para $\omega(x)$, y el caso de $\Omega(x)$ se deduce fácilmente de éste, pues el teorema anterior implica que

$$\sum_{n\le x}(\Omega(n)-\omega(n)) = O(x),$$

luego la cantidad de números $n \le x$ que cumplen

$$\Omega(n)-\omega(n) > (\log\log x)^{1/2} \tag{3.11}$$

es $o(x)$. En caso contrario, dado $\epsilon > 0$, habría valores de x arbitrariamente grandes para los que habría más de ϵx números n que cumplirían esta desigualdad, y así

$$\sum_{n\le x}(\Omega(n)-\omega(n)) \ge \epsilon x(\log\log x)^{1/2},$$

en contra de la estimación $O(x)$ para el miembro izquierdo. Por lo tanto, por la parte ya probada, la cantidad de números $n \le x$ que cumplen (3.11) y

$$|\omega(n)-\log\log x| > (\log\log x)^{\frac{1}{2}+\frac{\delta}{2}}$$

es $o(x)$, luego también lo es la cantidad de los que cumplen alguna de las dos. Por el contrario, los $n \le x$ que no cumplen ninguna, cumplen también

$$|\Omega(n)-\log\log x| = |\Omega(n)-\omega(n)+\omega(n)-\log\log x|$$

$$\le (\log\log x)^{1/2} + (\log\log x)^{1/2+\delta/2} < (\log\log x)^{1/2+\delta}$$

si x es suficientemente grande. Así pues, la cantidad de números $n \le x$ que no cumplen esto es $o(x)$, que es lo que había que probar. ∎

Así pues, tanto el orden medio como el orden normal de $\omega(n)$ y $\Omega(n)$ es $\log\log n$. Para otras funciones aritméticas no tiene por qué darse la igualdad.

Teorema 3.24 *La función* $\log d(n)$ *tiene orden normal* $\log 2\log\log n$.

DEMOSTRACIÓN: Si $n = p_1^{e_1}\cdots p_r^{e_r}$, tenemos que

$$d(n) = (1+e_1)\cdots(1+e_r),$$

y $2 \le 1+e_i \le 2^{e_i}$, luego

$$2^{\omega(n)} = 2^r \le d(n) \le 2^{e_1+\cdots+e_r} = 2^{\Omega(n)},$$

y a su vez

$$\omega(n)\log 2 \le \log d(n) \le \Omega(n)\log 2,$$

luego

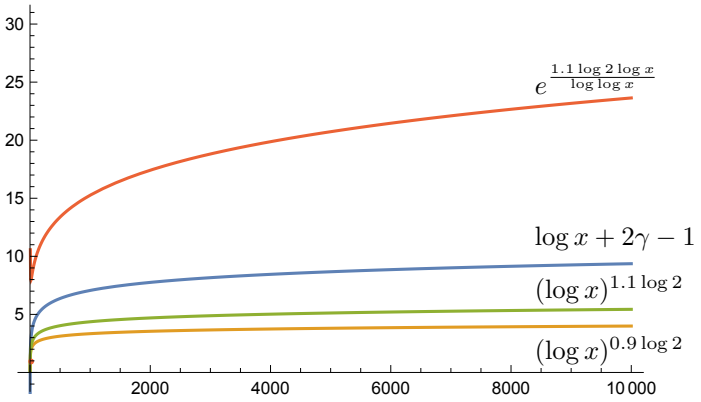
$$\frac{\omega(n)}{\log\log n} \le \frac{\log d(n)}{\log 2\log\log n} \le \frac{\Omega(n)}{\log\log n}.$$

Dado $\epsilon > 0$, los dos extremos de las desigualdades anteriores distan de 1 menos que ϵ para casi todo n, luego lo mismo le sucede al término central. ∎

Explícitamente, esto significa que, para todo $\epsilon > 0$, casi todos los números naturales cumplen

$$(\log n)^{(1-\epsilon)\log 2} = 2^{(1-\epsilon)\log\log n} \leq d(n) \leq 2^{(1+\epsilon)\log\log n} = (\log n)^{(1+\epsilon)\log 2}.$$

Cabe señalar que estas cotas son bastante inferiores al valor medio de la función $d(n)$ que, de acuerdo con el teorema 2.23, es $\log x + 2\gamma - 1$.



La figura muestra también la cota superior que proporciona el teorema 2.22. Esto se interpreta como que la función $d(n)$ toma pocas veces valores muy grandes, de modo que su valor medio es sustancialmente mayor que su "valor típico", que oscila alrededor de $(\log n)^{\log 2}$. No obstante, estos resultados sólo se aplican a intervalos desorbitadamente grandes. Si superponemos la gráfica de $d(n)$ (véase la página 45) a las gráficas anteriores en un intervalo asequible al cálculo computacional no veremos nada que corrobore los teoremas que hemos demostrado.

3.5 Series de Dirichlet

La conexión entre el estudio de la distribución de los primos que hemos iniciado y la teoría de funciones de variable compleja se realiza fundamentalmente a través de las series de Dirichlet. En esta sección recordamos sus propiedades principales, todas ellas demostradas en las secciones [ITAn 8.4], [An 10.6]. Recordemos la definición:

Definición 3.25 Una *serie de Dirichlet* es una serie de la forma

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

donde los coeficientes a_n son números complejos.

Adoptamos aquí el convenio usual en teoría de números de representar por $s = \sigma + i\tau$ a una variable compleja arbitraria. Al principio de la sección [An 10.6] vimos que toda serie de Dirichlet tiene una abscisa de convergencia σ_c y una abscisa de convergencia absoluta σ_a, de modo que la serie converge casi uniformemente (a una función holomorfa) en el semiplano $\sigma > \sigma_c$ y converge absoluta y casi uniformemente en el semiplano $\sigma > \sigma_a$ (sin perjuicio de que sea $\sigma_c = +\infty$, en cuyo caso la serie no converge en ningún punto, o $\sigma_c = -\infty$, en cuyo caso converge en todo el plano complejo).

En particular tenemos que cada función aritmética f tiene asociada una serie de Dirichlet

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Si dos series de Dirichlet convergen (al menos) en un semiplano $\sigma > \sigma_0$, entonces en dicho semiplano se cumple que

$$\sum_{n=1}^{\infty} \frac{(f+g)(n)}{n^s} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} + \sum_{n=1}^{\infty} \frac{g(n)}{n^s}, \quad \sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{n=1}^{\infty} \frac{g(n)}{n^s}.$$

La primera igualdad es trivial y la segunda —aunque también es elemental— es [ITAn 8.23]. Esto proporciona una interpretación analítica del producto de convolución.

En particular, si f tiene inversa f^{-1} y las series de Dirichlet de ambas funciones convergen (al menos) en un semiplano común, entonces las funciones a las que convergen son mutuamente inversas. Del teorema 2.5 se sigue (véanse las observaciones tras [ITAn 8.23]) que si f es completamente multiplicativa entonces la serie de f^{-1} converge absolutamente al menos en todo el semiplano de convergencia absoluta de f.

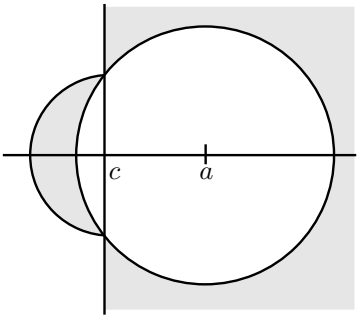
Puesto que la derivación es cerrada para la convergencia casi uniforme, las series de Dirichlet se pueden derivar término a término, y eso se traduce [An 10.30], que la serie de Dirichlet asociada a la función aritmética $-f'$ convere a la derivada de la serie de Dirichlet asociada a f en su semiplano de convergencia.

La *función dseta de Riemann* es la función definida por la serie de Dirichlet asociada a la función c_1, es decir,

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

Tras el teorema [An 10.30] probamos que converge en el semiplano $\sigma > 1$ y en [An 10.36] probamos que se extiende a una función meromorfa en $\mathbb{C}$ con un único polo simple en $s = 1$, pero éste es un resultado no trivial que no vamos a necesitar de momento. No obstante, vamos a probar que la presencia de dicho polo no es casual:

Teorema 3.26 *Sea* $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *una serie de Dirichlet convergente en un semiplano* $\sigma > c$ *y con coeficientes* $a_n \geq 0$. *Si la función* f *admite una prolongación analítica a un entorno de* c, *entonces existe un* $\epsilon > 0$ *tal que la serie converge en el semiplano* $\sigma > c - \epsilon$.



Demostración: Sea $a = 1 + c$ y consideremos la serie de Taylor de f en un entorno de a:

$$f(s) = \sum_{n=0}^{\infty} \frac{f^{n)}(a)}{n!}\,(s-a)^n$$

Su radio de convergencia es el máximo posible, luego ha de ser mayor que 1 y, en particular, la serie converge en un número de la forma $s = c - \epsilon$, con $\epsilon > 0$.

Sustituimos las derivadas de f por su valor según el teorema [An 10.30]:

$$f^{n)}(a) = (-1)^n \sum_{k=1}^{\infty} \frac{a_k (\log k)^n}{k^a}.$$

El resultado es:

$$f(c-\epsilon) = \sum_{n=0}^{\infty} (-1)^n \sum_{k=1}^{\infty} \frac{a_k (\log k)^n}{n!\,k^a}\,(-1-\epsilon)^n = \sum_{n=0}^{\infty}\sum_{k=1}^{\infty} \frac{a_k (\log k)^n}{n!\,k^a}\,(1+\epsilon)^n.$$

Como todos los términos son positivos todas las convergencias son absolutas, y podemos reordenar los sumandos como sigue:

$$\begin{aligned} f(c-\epsilon) &= \sum_{k=1}^{\infty} \frac{a_k}{k^a} \sum_{n=0}^{\infty} \frac{((1+\epsilon)\log k)^n}{n!} = \sum_{k=1}^{\infty} \frac{a_k}{k^a}\, e^{(1+\epsilon)\log k} \\ &= \sum_{k=1}^{\infty} \frac{a_k}{k^a}\, k^{1+\epsilon} = \sum_{k=1}^{\infty} \frac{a_k}{k^{c-\epsilon}}, \end{aligned}$$

luego la serie converge en $c - \epsilon$ y, por lo tanto, en todo el semiplano $\sigma > c - \epsilon$. ∎

Esto significa que si una función definida mediante una serie de Dirichlet con coeficientes positivos admite una extensión meromorfa a un semiplano mayor (como le ocurre a la función dseta, entonces la extensión ha de tener un polo en σ_c, pues en caso contrario la serie convergería en puntos anteriores a σ_c, lo cual es absurdo.

Las relaciones que conocemos entre las distintas funciones aritméticas que hemos considerado en el capítulo anterior se traducen inmediatamente en resultados sobre series de Dirichlet:

- La relación $\mu = c^{-1}$, junto con el hecho de que c_1 es completamente multiplicativa, se traduce en que

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \qquad \text{para } \sigma > 1.$$

- La relación $c_1' = \log$ se traduce en que

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}, \qquad \text{para } \sigma > 1.$$

- La relación $\Lambda * c_1 = \log$ se traduce en que

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \qquad \text{para } \sigma > 1.$$

- Tras [ITAn 8.27] se prueba que

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n\, n^s}, \qquad \text{para } \sigma > 1.$$

- La relación $c_1 * c_1 = d$ se traduce en que

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}.$$

- La relación $N = \phi * c_1$, junto con que, obviamente, la serie de N converge a $\zeta(s-1)$, se traduce en que

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}, \qquad \text{para } \sigma > 2.$$

- La relación $\sigma = N * c_1$ se traduce en que

$$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}, \qquad \text{para } \sigma > 2.$$

A éstas podemos añadir:

- La función potencia k-ésima, dada por

$$p^k(n) = \begin{cases} 1 & \text{si } n \text{ es una potencia } k\text{-ésima,} \\ 0 & \text{en caso contrario,} \end{cases}$$

claramente cumple que

$$\zeta(ks) = \sum_{n=1}^{\infty} \frac{p^k(n)}{n^s}, \qquad \text{para } \sigma > 1/k.$$

- La *función de Liouville* es la función completamente multiplicativa definida por $\lambda(p) = -1$ para todo primo p. Veamos que $\lambda * c_1 = p^2$. Como todas las funciones son multiplicativas basta probar que actúan igual sobre potencias de primos, pero

$$(\lambda * c_1)(p^n) = \sum_{k=0}^{n} \lambda(p^k) = \sum_{k=0}^{n} (-1)^k = p^2(p^n).$$

  Por lo tanto,

$$\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}, \qquad \text{para } \sigma > 1.$$

- Ess claro que $\lambda^{-1} = \mu\lambda = |\mu|$, luego

$$\frac{\zeta(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{|\mu|(n)}{n^s}, \qquad \text{para } \sigma > 1.$$

Una última propiedad básica de la función dseta es su desarrollo en producto de Euler [ITAn 8.25]:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}, \qquad \text{para } \sigma > 1, \tag{3.12}$$

donde el producto es también absolutamente convergente.

Euler observó que si hacemos tender s a 1, la serie tiende a $+\infty$, luego el producto también diverge, y ello implica que es infinito, es decir, que existen infinitos primos. Obviamente, hay demostraciones mucho más simples de este hecho, pero de esta fórmula podemos sacar un poco más. Aplicando el teorema [ITAn 8.3] al producto infinito resulta que

$$\log \zeta(s) = \sum_{p} \log \frac{1}{1 - \frac{1}{p^s}} \tag{3.13}$$

es un logaritmo de $\zeta(s)$. Más aún, la serie es absolutamente convergente por la definición de convergencia absoluta de un producto. Ahora consideramos el desarrollo en serie de Taylor

$$\log \frac{1}{1-z} = \sum_{n=1}^{\infty} \frac{z^n}{n}, \qquad \text{para } |z| < 1,$$

que nos lleva a

$$\log \zeta(s) = \sum_{p} \sum_{n=1}^{\infty} \frac{1}{n\, p^{ns}},$$

donde la serie converge absolutamente. Separando los términos correspondientes a $n = 1$ queda:

$$\log \zeta(s) = \sum_{p} \frac{1}{p^s} + \sum_{p} \sum_{n \geq 2} \frac{1}{n\, p^{ns}},$$

pero el segundo sumando se puede acotar,[1] para $s > 1$:

$$\sum_p \sum_{n\geq 2} \frac{1}{n\,p^{ns}} \leq \sum_p \sum_{n\geq 2} \frac{1}{p^n} = \sum_p \frac{1}{p^2-p} \leq \sum_{n\geq 2} \frac{1}{n^2-n} = 1.$$

De nuevo tenemos que $\log\zeta(s)$ tiende a $+\infty$ cuando s tiende a 1, pero, teniendo en cuenta que $1/p^s \leq 1/p$, ahora podemos concluir:

Teorema 3.27 *La serie* $\displaystyle\sum_p \frac{1}{p}$ *es divergente.*

(Pues si la serie fuera convergente, la serie $\sum_p (1/p^s)$ también estaría acotada cuando s tiende a 1, y acabamos de ver que no lo está.)

En 3.12 hemos dado una prueba elemental de este mismo hecho, pero la razón por la que, pese a todo, este argumento tiene interés es que es *generalizable.* es la base del argumento con el que Dirichlet demostró el teorema sobre primos en progresiones aritméticas [TAl 4.28], del que nos ocupamos en la sección siguiente.

Como segunda aplicación de (3.12) demostraremos el tercer teorema de Mertens. Recordemos que la constante de Mertens 3.16 es la análoga a la constante de Euler para la serie de los inversos de los primos en lugar de la serie de los inversos de los números naturales. Ahora vamos a relacionar ambas constantes. Para ello necesitamos una observación sobre la función dseta:

Como $\zeta(s)$ tiene un polo simple en $s = 1$ con residuo 1, la función $(s-1)\zeta(s)$ es holomorfa en 1 y toma el valor 1, luego en un entorno tiene definido un logaritmo holomorfo $\log((s-1)\zeta(s))$, que vale 0 en $s = 1$. Por lo tanto, la función

$$\frac{\log((s-1)\zeta(s))}{s-1}$$

está acotada en un entorno de 1. A su vez, esto equivale a que, en el semiplano $\sigma > 1$ y cuando s tiende a 1, se cumpla que

$$\log\zeta(s) = \log\frac{1}{s-1} + O(s-1). \tag{3.14}$$

Teorema 3.28 *Se cumple que*

$$M = \gamma + \sum_p \left(\log(1-1/p) + 1/p\right).$$

Demostración: Para probar la convergencia de la serie consideramos el desarrollo de Taylor

$$0 < \log\left(\frac{1}{1-p^{-1}}\right) - \frac{1}{p} = \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots < \frac{1}{2p^2} + \frac{1}{2p^3} + \cdots = \frac{1}{2p(p-1)}$$

[1] Para sumar la última serie basta ver que es telescópica, es decir, que, teniendo en cuenta que,

$$\frac{1}{n^2-n} = \frac{1}{n-1} - \frac{1}{n}$$

vemos que en las sumas parciales se cancelan todos los términos menos el primero y el último.

y la serie

$$\sum_p \frac{1}{2p(p-1)} < \sum_n \frac{1}{2n(n-1)}$$

es convergente. Similarmente, si $\delta \geq 0$, tenemos que

$$0 < -\log\left(1 - \frac{1}{p^{1+\delta}}\right) - \frac{1}{p^{1+\delta}} < \frac{1}{2p^{1+\delta}(p^{1+\delta}-1)} \leq \frac{1}{2p(p-1)},$$

por lo que la serie funcional

$$F(\delta) = \sum_p \left(\log\left(1 - \frac{1}{p^{1+\delta}}\right) + \frac{1}{p^{1+\delta}}\right)$$

converge uniformemente en $[0, +\infty[$ a una función continua. A partir de aquí suponemos $\delta > 0$, pero debemos recordar que podemos calcular $F(0)$. Al tomar logaritmos en la fórmula del producto de Euler (3.12) obtenemos:

$$\log \zeta(s) = \sum_p \log \frac{1}{1 - \frac{1}{p^s}}, \qquad \text{para } \sigma > 1.$$

De aquí se sigue que $F(\delta) = g(\delta) - \log \zeta(1+\delta)$, donde

$$g(\delta) = \sum_p \frac{1}{p^{1+\delta}}.$$

Ahora aplicamos el teorema 2.20 a $c_p = 1/p$ y $f(x) = 1/x^\delta$, con lo que, teniendo en cuenta (3.8),

$$C(x) = \sum_{p \leq x} \frac{1}{p} = \log\log x + M + R(x)$$

y el teorema nos da que

$$\sum_p \frac{1}{p^{1+\delta}} = \frac{C(x)}{x^\delta} + \delta \int_2^x \frac{C(t)}{t^{1+\delta}}\, dt.$$

Si hacemos tender x a $+\infty$ queda

$$g(\delta) = \delta \int_2^{+\infty} \frac{C(t)}{t^{1+\delta}}\, dt = \delta \int_2^{+\infty} \frac{\log\log t + M}{t^{1+\delta}}\, dt + \delta \int_2^{+\infty} \frac{R(t)}{t^{1+\delta}}\, dt.$$

Hacemos el cambio $t = e^{u/\delta}$:

$$\delta \int_1^{+\infty} \frac{\log\log t}{t^\delta} \frac{dt}{t} = \int_0^{+\infty} e^{-u} \log(u/\delta)\, du$$

$$= \int_0^{+\infty} e^{-u} \log u\, du - \int_0^{+\infty} e^{-u} \log \delta\, du = -\gamma - \log \delta,$$

donde hemos usado la fórmula

$$\gamma = -\int_0^{+\infty} e^{-x} \log x \, dx$$

probada tras [VC 4.25]. Por otra parte:

$$\delta \int_1^{+\infty} \frac{M}{t^{1+\delta}} \, dt = M.$$

Por lo tanto:

$$g(\delta) + \gamma - M + \log \delta = \delta \int_2^{+\infty} \frac{R(t)}{t^{1+\delta}} \, dt - \delta \int_1^2 \frac{\log\log t + M}{t^{1+\delta}} \, dt.$$

Ahora, llamando $T = e^{1/\sqrt{\delta}}$ y teniendo en cuenta que $|R(t)| \leq A/\log t$, tenemos que

$$\left| \delta \int_2^{+\infty} \frac{R(t)}{t^{1+\delta}} \, dt \right| \leq \delta A \int_2^T \frac{dt}{t^{1+\delta} \log t} + \delta A \int_T^{+\infty} \frac{dt}{t^{1+\delta} \log t}$$

$$\leq \frac{\delta A}{2^\delta \log 2} \int_2^T \frac{dt}{t} + \frac{\delta A}{\log T} \int_T^{+\infty} \frac{dt}{t^{1+\delta}} = \frac{\delta A \log T}{2^\delta \log 2} + \frac{A}{T^\delta \log T}$$

$$< \frac{\delta A}{\sqrt{\delta}} + A\sqrt{\delta} = 2A\sqrt{\delta}.$$

Por otra parte,

$$\left| \delta \int_1^2 \frac{\log\log t + M}{t^{1+\delta}} \, dt \right| \leq \delta \int_1^2 \frac{|\log\log t| + M}{t} \, dt$$

(notemos que la integral converge, pues se puede calcular haciendo el cambio $u = \log t$). Concluimos que

$$\lim_{\delta \to 0} g(\delta) + \log \delta = M - \gamma.$$

Pero por (3.14) también tenemos que $\log \zeta(1+\delta) + \log \delta \to 0$. Por consiguiente,

$$F(\delta) = g(\delta) + \log \delta - (\log \zeta(1+\delta) + \log \delta) \to M - \gamma,$$

luego $F(0) = 0$, es decir,

$$\sum_p \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right) = M - \gamma$$

■

Por consiguiente:

$$\lim_{x \to \infty} \log\log x + \gamma + \sum_{p \leq x} \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right) - \sum_{p \leq x} \frac{1}{p} = 0,$$

o también:

$$\lim_{x\to\infty} \log\log x + \gamma + \sum_{p\le x} \log\left(1-\frac{1}{p}\right) = 0,$$

y aplicando la exponencial,

$$\lim_{x\to+\infty} \log x\, e^{\gamma} \prod_{p\le x}\left(1-\frac{1}{p}\right) = 1.$$

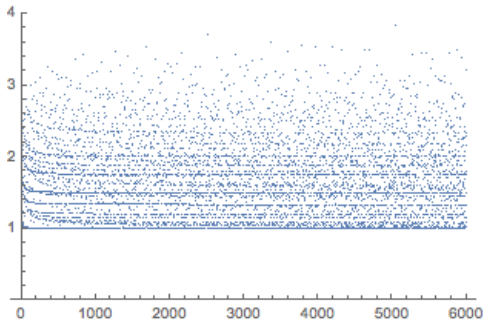
Con esto hemos probado:

Teorema 3.29 (Tercer teorema de Mertens)

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}.$$

Veamos a su vez una aplicación:

La media de los divisores Ya hemos estudiado el crecimiento del número medio de divisores de un número natural. Ahora vamos a estudiar el crecimiento del valor medio de los divisores de un número dado, es decir, la función $\sigma(n)/n$.



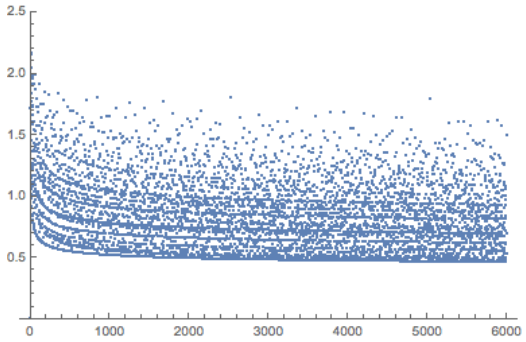
Su comportamiento es irregular. Por ejemplo, es claro que

$$\sigma(p)/p = 1 - 1/p \approx 1,$$

luego la función tiene una subsucesión convergente a 1, mientras que es claro que otras subsucesiones tienden a infinito. Sucede que su orden de crecimiento es $O(\log\log x)$. En efecto, la figura siguiente muestra la gráfica de la función

$$\frac{\sigma(n)}{n\log\log n},$$

y en ella podemos ver que está acotada.



Más precisamente, podemos probar lo siguiente:

Teorema 3.30

$$\overline{\lim_n} \frac{\sigma(n)}{n \log\log n} = e^{\gamma}, \qquad \underline{\lim_n} \frac{\phi(n) \log\log n}{n} = e^{-\gamma},$$

donde σ es la función suma de divisores, ϕ es la función de Euler y γ es la constante de Euler.

Demostración: Observemos que $\sigma(n)\phi(n) < n^2$. En efecto, como las tres funciones son multiplicativas, basta probarlo para $n = p^a$, pero

$$\sigma(p^a)\phi(p^a) = \frac{p^{a+1}-1}{p-1}(p-1)p^{a-1} = p^{2a} - p^{a-1} < (p^a)^2.$$

Llamemos

$$f_1(n) = \frac{\sigma(n)}{ne^{\gamma} \log\log n}, \qquad f_2(n) = \frac{\phi(n)e^{\gamma} \log\log n}{n}.$$

Hay que probar que $\overline{\lim_n} f_1 = 1$ y $\underline{\lim_n} f_2 = 1$, para lo cual basta encontrar funciones $F_1(t)$, $F_2(t)$ que tiendan a 1 en $+\infty$ de modo que

$$f_1(n) \le \frac{1}{F_1(\log n)}, \qquad f_2(n) \ge F_1(\log n)$$

para todo $n \ge 3$, y

$$f_1(n_j) \ge F_2(j), \qquad f_2(n_j) \le \frac{1}{F_2(j)},$$

para cierta sucesión $\{n_j\}_j$ estrictamente creciente.

Por la observación previa, tenemos que $f_1(n)f_2(n) < 1$, luego basta probar las desigualdades

$$f_2(n) \ge F_1(\log n), \qquad f_1(n_j) \ge F_2(j).$$

Dado n, sean $p_1, \dots p_{r-r_0}$ los divisores primos de n que cumplen $p_i \le \log n$ y sean $p_{r-r_0+1}, \dots, p_r$ los que cumplen $p_i > \log n$. Entonces

$$(\log n)^{r_0} < p_{r-r_0+1} \dots p_r \le n,$$

luego $r_0 < \log n / \log\log n$, luego[2]

$$\frac{\phi(n)}{n} = \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) \ge \left(1-\frac{1}{\log n}\right)^{r_0}\prod_{i=1}^{r-r_0}\left(1-\frac{1}{p_i}\right)$$

$$> \left(1-\frac{1}{\log n}\right)^{\log n/\log\log n}\prod_{p\le\log n}\left(1-\frac{1}{p}\right).$$

Por consiguiente, basta tomar

$$F_1(t) = e^\gamma \log t\left(1-\frac{1}{t}\right)^{t/\log t}\prod_{p\le t}\left(1-\frac{1}{p}\right).$$

El teorema de Mertens nos da que

$$\lim_{t\to+\infty} e^\gamma \log t\prod_{p\le t}\left(1-\frac{1}{p}\right) = 1,$$

y es fácil ver que también

$$\lim_{t\to+\infty}\left(1-\frac{1}{t}\right)^{t/\log t} = 1,$$

luego $\lim_{t\to+\infty} F_1(t) = 1$. Tomemos ahora

$$n_j = \prod_{p\le e^j} p^j,$$

de modo que $\log n_j = j\vartheta(e^j) \le Aje^j$, para cierta constante $A > 0$, por 3.10. Por lo tanto

$$\log\log n_j \le A_0 + j + \log j.$$

Ahora:

$$\prod_{p\le e^j}\left(1-\frac{1}{p^{j+1}}\right) > \prod_p\left(1-\frac{1}{p^{j+1}}\right) = \frac{1}{\zeta(j+1)}.$$

Por lo tanto,

$$f_1(n_j) = \frac{\sigma(n_j)}{n_h e^\gamma \log\log n_j} = \frac{e^{-\gamma}}{\log\log n_j}\prod_{p\le e^j}\left(\frac{1-1/p^{j+1}}{1-p^{-1}}\right)$$

$$\ge \frac{e^{-\gamma}}{\zeta(j+1)(A_0+j+\log j)}\prod_{p\le e^j}\frac{1}{1-p^{-1}} = F_2(j),$$

donde la última igualdad es la definición que adoptamos de $F_2(j)$, y a partir de aquí consideramos a j como variable real.

[2]Notemos que $\phi(p^a) = (p-1)p^{a-1} = p^a(p-1)/p$, luego $\phi(p^a)/p^a = 1 - 1/p$.

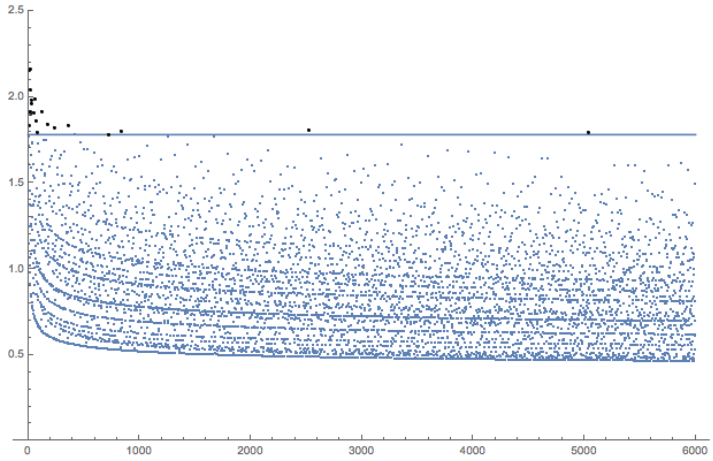
Si j tiende a $+\infty$ sabemos que $\zeta(j+1) \to 1$ y, por el teorema de Mertens,

$$\lim_{j\to+\infty} \frac{e^{-\gamma}}{\log e^j} \prod_{p\le e^j} \frac{1}{1-p^{-1}} = 1,$$

luego

$$\lim_{j\to+\infty} F_2(j) = \lim_{j\to+\infty} \frac{j}{A_0 + j + \log j} = 1. \qquad \blacksquare$$

Situemos en la gráfica el límite superior que hemos calculado, $e^\gamma = 1.781\ldots$



Vemos que algunos valores superan el límite superior. No hay nada de extraño en ello, pero podemos afirmar que la sucesión de todos los valores por encima del límite superior (si es infinita) converge a dicho límite superior. Los puntos en el rango mostrado en la figura que sobrepasan el límite superior son

$$3,\quad 4,\quad 5,\quad 6,\quad 8,\quad 9,\quad 10,\quad 12,\quad 16,\quad 18,\quad 20,\quad 24,\quad 30,\quad 36,\quad 48,$$

$$60,\quad 72,\quad 84,\quad 120,\quad 180,\quad 240,\quad 360,\quad 720,\quad 840,\quad 2\,520,\quad 5\,040.$$

El caso es que no se conoce ninguno mayor que $7! = 5\,040$.

3.6 El teorema de Dirichlet

Recordemos el enunciado del teorema de Dirichlet sobre primos en progresiones aritméticas:

Teorema 3.31 (Dirichlet) *En toda progresión aritmética $mx+n$, donde m y n son enteros primos entre sí, hay infinitos números primos.*

Según hemos explicado en la introducción, aquí vamos a dar una prueba de este teorema intermedia entre la prueba "elemental" que dada en [ITAn 7.24] y la prueba de [TAl 4.28] basada en la aritmética ideal de los cuerpos ciclotómicos. El apéndice al final de este capítulo contiene los pocos resultados sobre caracteres que vamos a necesitar, todos ellos elementales.

Si llamamos U_m al grupo de las unidades del anillo $\mathbb{Z}/m\mathbb{Z}$, es decir

$$U_m = \{[n] \in \mathbb{Z}/m\mathbb{Z} \mid (m,n) = 1\},$$

el teorema de Dirichlet equivale a que cada clase de U_m contiene infinitos primos.

Es claro que todo carácter modular $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ (definición 3.51) es una función aritmética completamente multiplicativa. Las series de Dirichlet que definen son las llamadas *funciones L*:

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

La convergencia (absoluta) es inmediata, pues $|\chi(n)| \leq 1$, luego $L(s,\chi)$ está mayorada en módulo por $\zeta(\sigma)$. En el caso del carácter principal módulo m tenemos que

$$L(s,1) = \prod_{(p,m)=1} \frac{1}{1-\frac{1}{p^s}} = \prod_{p|m} \left(1-\frac{1}{p^s}\right)\zeta(s). \tag{3.15}$$

Como el producto finito es una función entera, es claro que $L(s,1)$ se prolonga analíticamente[3] al semiplano $\sigma > 0$ con un polo simple en $s = 1$.

Por otra parte, si $\chi \neq 1$ entonces la sucesión $\chi(n)$ tiene periodo m, ya que, por las relaciones de ortogonalidad 3.50, la suma de m términos consecutivos vale 0, luego podemos aplicar el teorema [ITAn 8.31] y concluir que $L(s,\chi)$ converge en el semiplano $\sigma > 0$ a una función holomorfa. Resumimos estos hechos en un teorema:

Teorema 3.32 *Sea χ un carácter modular. Entonces la función $L(s,\chi)$ está definida y es holomorfa en el semiplano $\sigma > 0$, salvo si $\chi = 1$, en cuyo caso tiene un polo simple en $s = 1$.*

Ahora tratemos de demostrar el teorema de Dirichlet imitando el argumento de Euler que hemos empleado al final de la sección anterior. Para ello, fijado un número natural $m > 1$, sustituimos la función dseta por

$$\zeta_m(s) = \prod_{\chi} L(s,\chi),$$

donde (aquí y en lo sucesivo) χ recorre los caracteres módulo m.

Por el teorema anterior, tenemos que $\zeta_m(s)$ es una función holomorfa en el semiplano $s > 0$ salvo quizá un polo en $s = 1$. El punto más delicado de la prueba es demostrar que si χ es un carácter no principal, entonces $L(1,\chi) \neq 0$, con lo que $\zeta_m(s)$ sí que tiene un polo en $s = 1$, en perfecta analogía con lo que le sucede a la función dseta de Riemann.

[3] De hecho, al igual que la función dseta, se prolonga a una función meromorfa en $\mathbb{C}$ con un único polo en $s = 1$, tal y como se prueba en [An 10.38], pero esto es un hecho profundo que no necesitamos aquí. Nos basta con saber que la función dseta se puede prolongar hasta el semiplano $\sigma > 0$, que es un hecho elemental.

En primer lugar vamos a ver que $\log \zeta_m(s) \geq 0$ cuando $s > 1$, de donde se sigue que $\zeta_m(s) \geq 1$ cuando $s > 1$, y tendremos al menos que ζ_m no tiene un cero en $s = 1$. Podemos definir

$$\log \zeta_m(s) = \sum_{\chi} \log L(s, \chi),$$

donde, a su vez, cada $\log L(s, \chi)$ es la función dada por el teorema [ITAn 8.27], es decir:

$$\log L(s, \chi) = \sum_{n=2}^{\infty} \frac{\chi(n)\Lambda(n)}{\log n\, n^s}.$$

Por lo tanto:

$$\log \zeta_m(s) = \sum_{n=2}^{\infty} \frac{\sum_{\chi} \chi(n)\Lambda(n)}{\log n\, n^s} \geq 0, \qquad \text{para } s > 1,$$

pues, por las relaciones de ortogonalidad 3.50 se cumple $\sum_{\chi} \chi(n) \geq 0$.

Como ya hemos dicho, esto implica que $\zeta_m(s) \geq 1$ para $s > 1$, luego ζ_m no puede tener un cero en $s = 1$.

De la continuidad de la conjugación se sigue que $L(s, \overline{\chi}) = \overline{L(s, \chi)}$, luego si un carácter cumple $L(1, \chi) = 0$, también tenemos $L(1, \overline{\chi}) = 0$. Por lo tanto, si $\chi \neq \overline{\chi}$, ha de cumplirse que $L(1, \chi) \neq 0$, o de lo contrario en el producto que define a ζ_m habría al menos dos factores con ceros y un único polo simple, luego ζ_m tendría un cero en 1, en contradicción con lo que hemos visto.

Así pues, sólo queda probar que $L(1, \chi) \neq 0$ cuando $\chi = \overline{\chi}$, es decir, cuando χ sólo toma valores reales, que serán necesariamente $-1, 0, 1$ (porque los caracteres en sentido propio sólo toman valores de módulo 1).

Sea χ un carácter real y supongamos que $L(1, \chi) = 0$. Entonces consideramos la función

$$G(s) = \frac{\zeta(s)}{\zeta(2s)} L(s, \chi) = \sum_{n=1}^{\infty} \frac{(|\mu| * \chi)(n)}{n^s}, \qquad \text{para } \sigma > 1.$$

La función $|\mu| * \chi$ es multiplicativa y es fácil ver que

$$(|\mu| * \chi)(p^k) = \chi(p)^k + \chi(p)^{k-1} = \begin{cases} 0 & \text{si } \chi(p) = -1,\ 0, \\ 2 & \text{si } \chi(p) = 1. \end{cases}$$

Por lo tanto $|\mu| * \chi \geq 0$ y podemos aplicar el teorema 3.26, que nos da que la serie converge en realidad para $\sigma > 1/2$. Además, puesto que el primer término es igual a 1 y los restantes son positivos, queda que $G(s) \geq 1$ para $s > 1/2$. Por lo tanto

$$1 \leq \lim_{s \to (1/2)^+} G(s) = \lim_{s \to (1/2)^+} \frac{\zeta(s)}{\zeta(2s)} L(s, \chi) = \frac{\zeta(1/2)L(1/2, \chi)}{\infty} = 0.$$

Con esta contradicción concluimos que $L(1,\chi) \neq 0$ siempre que χ no es el carácter principal, luego en efecto ζ_m tiene un polo simple en 1. El resultado sobre las funciones L tiene interés por sí mismo. Lo recogemos en el teorema siguiente:

Teorema 3.33 *Si χ es un carácter modular no principal, entonces $L(1,\chi) \neq 0$.*

Ahora seguimos el argumento del teorema 3.27 (y el de [TAl 4.28]). Vamos a probar que si A es una clase del grupo U_m, entonces la serie $\sum_{p\in A}(1/p)$ es divergente, con lo que en particular A deberá contener infinitos primos. Para ello hemos de considerar de nuevo el logaritmo de ζ_m, es decir,

$$\log \zeta_m(s) = \sum_{\chi} \log L(s,\chi).$$

Cada sumando puede desarrollarse en serie a partir de la factorización de las funciones L:

$$\log L(s,\chi) = \sum_p \log \frac{1}{1-\frac{\chi(p)}{p^s}}$$

A su vez desarrollamos cada logaritmo en serie de Taylor como hicimos en el teorema 3.27:

$$\log L(s,\chi) = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{n\,p^{ns}}, \qquad \text{para } \sigma > 1. \tag{3.16}$$

Descomponemos

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + R(s,\chi),$$

donde

$$R(s,\chi) = \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)^n}{n\,p^{ns}} \quad \text{cumple} \quad |R(s,\chi)| \leq \sum_p \sum_{n=2}^{\infty} \frac{1}{p^n} \leq 1.$$

Si hacemos variar C en las clases de U_m tenemos

$$\sum_p \frac{\chi(p)}{p^s} = \sum_C \chi(C) \sum_{p\in C} \frac{1}{p^s},$$

con lo que

$$\log L(s,\chi) = \sum_C \chi(C) \sum_{p\in C} \frac{1}{p^s} + R(s,\chi), \qquad \text{para todo } \chi.$$

Podemos pensar en estas ecuaciones como un sistema lineal con incógnitas las series $\sum_{p\in C} 1/p^s$. Queremos despejar estas series para comprobar que tienden

a ∞ cuando s tiende a 1, lo que probará que cada clase C tiene infinitos primos. Fijemos, pues, una clase A de U_m, multiplicamos las ecuaciones por $\chi(A^{-1})$ y sumamos sobre χ:

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) = \sum_C \sum_\chi \chi(CA^{-1}) \sum_{p\in C} \frac{1}{p^s} + R_A(s),$$

donde $|R_A(s)| = \left|\sum_\chi \chi(A^{-1})R(s,\chi)\right| \le \sum_\chi |R(s,\chi)| \le \phi(m)$ para todo $s > 1$.

Por el teorema 3.50, la suma $\sum_\chi \chi(CA^{-1})$ vale $\phi(m)$ si $C = A$ y es cero en otro caso. Así pues

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) = \phi(m) \sum_{p\in A} \frac{1}{p^s} + R_A(s), \tag{3.17}$$

con lo que tenemos despejada la serie de A.

Ahora tomaremos límites cuando $s \to 1^+$. Debemos detenernos en el comportamiento de $\log L(s,\chi)$. Puesto que $L(1,\chi)$ (para χ no principal) es un número complejo no nulo, sabemos que en un entorno de $L(1,\chi)$ existe una determinación continua del logaritmo. Componiéndola con $L(s,\chi)$ obtenemos una función continua $\log' L(s,\chi)$ definida en un entorno de 1, digamos $]1-\epsilon, 1+\epsilon[$. La función $\log L(s,\chi) - \log' L(s,\chi)$ es continua en el intervalo $]1, 1+\epsilon[$ y sólo puede tomar los valores $2k\pi i$, para k entero, luego por conexión k ha de ser constante en $]1, 1+\epsilon[$ y consecuentemente existe

$$\lim_{s\to 1^+} \log L(s,\chi) = \log' L(1,\chi) + 2k\pi i.$$

Agrupamos todos los sumandos acotados del miembro derecho de (3.17) junto con $R_A(s)$ y queda que

$$\log L(s,1) = \phi(m) \sum_{p\in A} \frac{1}{p^s} + T_A(s),$$

donde $T_A(s)$ es una función acotada en un entorno de 1.

Por otro lado $\lim_{s\to 1^+} L(s,1) = +\infty$, luego también $\lim_{s\to 1^+} \log L(s,1) = +\infty$. Esto implica que la función $\sum_{p\in A} \frac{1}{p^s}$ no está acotada en un entorno de 1, luego la serie $\sum_{p\in A} \frac{1}{p}$ es divergente, como queríamos probar. ∎

Terminamos esta sección con una generalización ligera, pero crucial, del teorema 3.33:

Teorema 3.34 *Sea χ un carácter modular. Entonces $L(1+it,\chi) \neq 0$ para todo $t \in \mathbb{R}$ ($t \neq 0$ si $\chi = 1$). En particular $\zeta(1+it) \neq 0$ para todo $t \in \mathbb{R}$ no nulo.*

DEMOSTRACIÓN: El caso particular se obtiene aplicando el teorema al carácter principal módulo 1. El caso $t = 0$ es el teorema 3.33, luego ahora podemos suponer $t \neq 0$. Consideramos la función

$$F(s) = \zeta^3(s)L^4(s+it,\chi)L(s+2it,\chi^2).$$

Las funciones $L(s+it,\chi)$ y $L(s+2it,\chi^2)$ son holomorfas en 1. Si suponemos que $L(1+it,\chi) = 0$ entonces el polo triple de $\zeta^3(s)$ se cancela con el cero cuádruple del segundo factor, con lo que F es holomorfa en 1 y además $F(1) = 0$.

Así pues, basta probar que $F(1) \neq 0$. Lo haremos estudiando su logaritmo. En primer lugar notamos que

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

donde $f(n) = \chi(n)/n^{it}$ es una función aritmética completamente multiplicativa, y lo mismo es válido para $L(s+2it,\chi^2)$ cambiando f por f^2. Según el teorema [ITAn 8.25] tenemos los desarrollos en productos de Euler

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}, \quad L(s+it,\chi) = \prod_p \frac{1}{1-\frac{f(p)}{p^s}}, \quad L(s+2it,\chi^2) = \prod_p \frac{1}{1-\frac{f^2(p)}{p^s}},$$

válidos en el semiplano $\sigma > 1$.

Ahora aplicamos el teorema [ITAn 8.3] junto con el desarrollo de Taylor

$$\log \frac{1}{1-z} = \sum_{n=1}^{\infty} \frac{z^n}{n},$$

con lo que obtenemos

$$\log \zeta(s) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}, \quad \log L(s+it,\chi) = \sum_p \sum_{n=1}^{\infty} \frac{f(p^n)}{np^{ns}},$$

$$\log L(s+2it,\chi^2) = \sum_p \sum_{n=1}^{\infty} \frac{f^2(p^n)}{np^{ns}}.$$

Es claro que las series son absolutamente convergentes (las series de los módulos son todas iguales a $\log \zeta(\sigma)$). Consecuentemente podemos agruparlas y formar la serie

$$\log F(s) = \sum_p \sum_{n=1}^{\infty} \frac{3 + 4f(p^n) + f^2(p^n)}{np^{ns}},$$

que es, efectivamente, un logaritmo de $F(s)$ en el semiplano $\sigma > 1$. Teniendo en cuenta que $|f(n)| = 1$, si θ_{p^n} es un argumento cualquiera de $f(p^n)$, tenemos que $\operatorname{Re} f(p^n) = \cos\theta_{p^n}$ y $\operatorname{Re} f^2(p^n) = \cos 2\theta_{p^n}$. Se cumple

$$3 + 4\cos\theta + \cos 2\theta = 3 + 4\cos\theta + 2\cos^2\theta - 1 = 2(1+\cos\theta)^2 \geq 0,$$

con lo que concluimos $\operatorname{Re}\log F(s) \geq 0$ y, en consecuencia, $|F(s)| \geq 1$ para todo $s > 1$. Por continuidad no puede ser $F(1) = 0$. ∎

Nota En la sección [An 10.6] vimos que los ceros de la función $\zeta(s)$ (extendida a todo el plano complejo) se dividen en los ceros triviales (los números pares negativos) y los ceros no triviales, que están necesariamente en la banda crítica $0 \le \sigma \le 1$. Acabamos de probar que ninguno puede estar en la recta $\sigma = 1$ y, por la ecuación funcional, tampoco puede haber ceros en la recta $\sigma = 0$, luego ahora podemos afirmar que los ceros no triviales de la función dseta se encuentran en la banda abierta $0 < \sigma < 1$. ∎

3.7 Prueba del teorema de los números primos

Nos ocupamos ahora de demostrar el teorema de los números primos, que hemos discutido en la introducción del libro:

Teorema 3.35 (Teorema de los números primos)

$$\pi(x) \sim \frac{x}{\log x} \sim \mathrm{Il}(x).$$

Según 3.1 es suficiente con demostrar la primera equivalencia.

Una consecuencia inmediata del desarrollo en producto de Euler de la función dseta es que ésta no se anula en el semiplano $\sigma > 1$. Sucede que un ingrediente clave en la prueba del teorema de los números primos es que tampoco se anula en la recta $\sigma = 1$. Esto lo hemos probado en 3.34 como caso particular del resultado análogo para funciones L, pero, para mostrar que la prueba que vamos a dar no requiere para nada tratar con caracteres modulares y funciones L, particularizamos aquí el argumento:

Teorema 3.36 *Para todo número real τ, se cumple que $\zeta(1+\tau i) \neq 0$.*

Demostración: Como en el caso de 3.34, la prueba se basa en la desigualdad

$$3 + 4\cos\theta + \cos 2\theta = 3 + 4\cos\theta + 2\cos^2\theta - 1 = 2(1+\cos\theta)^2 \ge 0.$$

Por el desarrollo en serie de Dirichlet de $\log\zeta(s)$ tenemos que, para $\sigma > 1$,

$$\log|\zeta(s)| = \mathrm{Re}\sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}e^{-s\log n} = \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n\, n^\sigma}\cos(\tau\log n).$$

Por lo tanto,

$$\log|\zeta(\sigma)^3\zeta(\sigma+\tau i)^4\zeta(\sigma+2\tau i)| = 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+\tau i)| + \log|\zeta(\sigma+2\tau i)|$$

$$= \sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n\, n^\sigma}(3 + 4\log(\tau\log n) + \cos(2\tau\log n)) \ge 0.$$

Por lo tanto,

$$((\sigma-1)\zeta(\sigma))^3\left|\frac{\zeta(\sigma+\tau i)}{\sigma-1}\right|^4|\zeta(\sigma+2\tau i)|\geq\frac{1}{\sigma-1},$$

para $\sigma>1$ y cualquier τ. Si fuera $\zeta(1+\tau i)=0$, entonces

$$\lim_{\sigma\to1}\frac{\zeta(\sigma+\tau i)}{\sigma-1}=\lim_{\sigma\to1}\frac{\zeta(1+\tau i+\sigma)-\zeta(1+\tau i)}{\sigma-1}=\zeta'(1+\tau i)$$

y el miembro izquierdo de la desigualdad precedente tendería a

$$|\zeta'(1+\tau i)|^4|\zeta(1+2\tau i)|,$$

cuando, en vista de la desigualdad, tiende a $+\infty$. ∎

Usamos este hecho en el teorema siguiente, donde nos apoyamos además en que la función dseta se prolonga analíticamente a una función meromorfa en el semiplano $\sigma>0$ con un único polo simple en $s=1$. Esto está probado en [An 10.31] con un argumento mucho más elemental que el necesario para probar la prolongación analítica a todo el plano complejo.

Teorema 3.37 *La función*

$$\Phi(s)=\sum_p\frac{\log p}{p^s}$$

es holomorfa en el semiplano $\sigma>1$ y se prolonga a una función meromorfa en el semiplano $\sigma>1/2$ con un polo simple en $s=1$ con residuo 1, que es el único sobre la recta $\sigma=1$.

Demostración: Tenemos que

$$-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=\sum_{p,m}\frac{\log p}{p^{ms}}=\sum_p\frac{\log p}{p^s}+\sum_{p,m\geq2}\frac{\log p}{p^{ms}},$$

donde p recorre los números primos y m los naturales no nulos.

Como la convergencia es absoluta, los dos sumandos de la derecha definen funciones holomorfas en el semiplano $\sigma>1$. Al sumar la serie geométrica de la segunda obtenemos

$$\sum_{p,m\geq2}\frac{\log p}{p^{ms}}=\sum_p\frac{\log p}{p^{2s}-p^s},$$

y al comparar esta serie con $\Phi(2s)$ concluimos que de hecho converge (a una función holomorfa) en el semiplano $\sigma>1/2$. Por lo tanto, $\Phi(s)$ se prolonga analíticamente hasta la función meromorfa

$$\Phi(s)=-\frac{\zeta'(s)}{\zeta(s)}-\sum_p\frac{\log p}{p^{2s}-p^s}$$

en el semiplano $\sigma > 1/2$. Sus polos son los de la derivada logarítmica $\zeta'(s)/\zeta(s)$, que por [VC 3.20] son todos simples, y se corresponden con los ceros y polos de $\zeta(s)$. Como $\zeta(s)$ tiene un polo simple en $s = 1$, resulta que $\Phi(s)$ tiene también un polo simple en $s = 1$ con residuo 1. Los polos restantes de $\Phi(s)$ se corresponden con los ceros de $\zeta(s)$, luego por el teorema anterior no hay ninguno más en la recta $\sigma = 1$. ∎

Ahora necesitamos un resultado técnico que traduce propiedades analíticas de una serie de Dirichlet en una propiedad de la sucesión de sus coeficientes:

Teorema 3.38 *Sea*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

una serie de Dirichlet con coeficientes $a_n \geq 0$ y convergente en un semiplano $\sigma > \sigma_0 \geq 0$. Llamemos

$$\phi(x) = \sum_{\log n \leq x} a_n.$$

Entonces

$$f(s) = s \int_0^{+\infty} \phi(x) e^{-sx}\, dx, \quad \textit{para } \sigma > \sigma_0.$$

DEMOSTRACIÓN: Podemos suponer que $\sigma_0 > 0$, pues si el teorema se cumple para todo $\sigma_0 > 0$, entonces se cumple obviamente para $\sigma_0 = 0$. La función $\phi(x)e^{-sx}$ tiene módulo $\phi(x)e^{-\sigma x}$, que es una función positiva y acotada en intervalos acotados. Además es medible porque $\phi(x)$ es escalonada y $e^{-\sigma x}$ es continua. Por lo tanto es integrable en intervalos acotados. Sea k un número natural.

$$\begin{aligned}
s \int_0^{\log(k+1)} \phi(x) e^{-sx}\, dx &= s \sum_{r=1}^{k} \int_{\log r}^{\log(r+1)} e^{-sx} \sum_{n=1}^{r} a_n\, dx \\
= s \sum_{r=1}^{k} \sum_{n=1}^{r} a_n \int_r^{r+1} e^{-s\log t}\, \frac{1}{t}\, dt &= s \sum_{n=1}^{k} \sum_{r=n}^{k} a_n \int_r^{r+1} t^{-(s+1)} dt \\
= -\sum_{n=1}^{k} a_n \sum_{r=n}^{k} \big((r+1)^{-s} - r^{-s}\big) &= \sum_{n=1}^{k} a_n \big(n^{-s} - (k+1)^{-s}\big).
\end{aligned}$$

De aquí se sigue que

$$\sum_{n=1}^{k} \frac{a_n}{n^s} = s \int_0^{\log(k+1)} \phi(x) e^{-sx}\, dx + \frac{h(k)}{(k+1)^s},$$

donde $h(k) = \sum_{n=1}^{k} a_n$. Sea $\sigma > \sigma_1 > \sigma_0 > 0$. Entonces

$$\sum_{n=1}^{k} \frac{a_n}{n^s} = s \int_0^{\log(k+1)} \phi(x) e^{-sx}\, dx + \frac{h(k)}{(k+1)^{\sigma_1}} \frac{1}{(k+1)^{s-\sigma_1}}. \tag{3.18}$$

Claramente

$$0 \le \frac{h(k)}{(k+1)^{\sigma_1}} \le \sum_{n=1}^{k} \frac{a_n}{n^{\sigma_1}} \le f(\sigma_1), \quad \left|\frac{1}{(k+1)^{s-\sigma_1}}\right| = \frac{1}{(k+1)^{\sigma-\sigma_1}} \xrightarrow{k} 0,$$

luego tomando límites en (3.18) obtenemos la igualdad buscada. ∎

El teorema que acabamos de probar enlaza con el siguiente:

Teorema 3.39 *Sea $\phi : [0, +\infty[\longrightarrow \mathbb{R}$ una función acotada, integrable en cada intervalo $[0, x]$, y supongamos que la función*

$$g(s) = \int_0^{+\infty} \phi(x) e^{-sx}\, dx,$$

definida en el semiplano $\sigma > 0$, se prolonga analíticamente a un abierto que contiene al semiplano $\sigma \ge 0$. Entonces existe

$$\int_0^{+\infty} \phi(x)\, dx = g(0).$$

Demostración: Llamemos

$$g_t(s) = \int_0^{t} \phi(x) e^{-sx}\, dx.$$

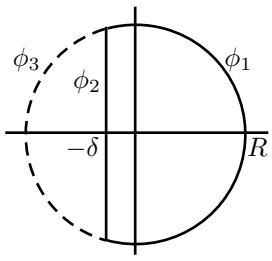
Por el teorema [IC 7.10] tenemos[4] que g_t es una función entera. Claramente

$$\int_0^{+\infty} \phi(x)\, dx = \lim_{t \to +\infty} g_t(0),$$

y hemos de probar que este límite existe y vale $g(0)$.

Dado $R > 0$, podemos tomar un $\delta > 0$ tal que g es holomorfa en un entorno del cerrado

$$A = \{s \in \mathbb{C} \mid |s| \le R,\ \operatorname{Re} s \ge -\delta\}.$$



Llamemos γ a la parametrización de la frontera de A formada por el arco $\gamma_1(u) = Re^{iu}$, $u \in [-\pi/2, \pi/2]$, y el arco γ_2 formado por dos pequeños arcos de circunferencia y un segmento.

Aplicamos la fórmula integral de Cauchy a la función

$$h(s) = (g(s) - g_t(s))e^{st}\left(1 + \frac{s^2}{R^2}\right).$$

[4]En realidad [IC 7.10] tiene como hipótesis que el integrando sea una función continua en las dos variables, cosa que aquí no tenemos garantizada, porque ϕ no tiene por qué ser continua, pero si en la prueba, en lugar de aplicar [IC 3.11], aplicamos [An 5.27], vemos que este teorema admite que el integrando tenga un factor integrable acotado no necesariamente continuo, que dependa únicamente de x, por lo que la prueba de [IC 7.10] se aplica igualmente a este caso.

Así:

$$g(0) - g_t(0) = h(0) = \frac{1}{2\pi i}\int_\gamma (g(s) - g_t(s))e^{st}\left(1 + \frac{s^2}{R^2}\right)\frac{ds}{s}.$$

Si C es una cota de ϕ, en el semiplano $\sigma > 0$ se cumple que

$$|g(s) - g_t(s)| = \left|\int_t^{+\infty} \phi(x)e^{-sx}\,dx\right| \leq C\int_t^{+\infty} |e^{-sx}|\,dx = \frac{Ce^{-\sigma t}}{\sigma},$$

mientras que, sobre la circunferencia de radio R,

$$\left|e^{st}\left(1 + \frac{s^2}{R^2}\right)\frac{1}{s}\right| = e^{\sigma t}\frac{2\sigma}{R^2},$$

donde hemos usado que $|1 + s^2/|s|^2| = 2\sigma/|s|$, como se comprueba sin más que sustituir $s = a + bi$. Por lo tanto,

$$\left|\frac{1}{2\pi i}\int_{\gamma_1} \frac{h(s)}{s}\,ds\right| \leq \frac{1}{2\pi}\frac{2C}{R^2}\pi R = \frac{C}{R}.$$

Sobre γ_2 descomponemos la integral en dos. Como g_t es entera, se cumple que

$$\frac{1}{2\pi i}\int_{\gamma_2} g_t(s)e^{st}\left(1 + \frac{s^2}{R^2}\right)\frac{ds}{s}$$

coincide con la integral de la misma función sobre el arco $\gamma_3(u) = Re^{ui}$, para $u \in [\pi/2, 3\pi/2]$, pues la integral sobre $\gamma_1 \cup \gamma_2$, al igual que la integral sobre $\gamma_1 \cup \gamma_3$, es el valor del integrando en 0. Sobre γ_3^* tenemos igual que antes que

$$|g_t(s)| = \left|\int_0^t \phi(x)e^{-sx}\,dx\right| \leq C\int_0^t |e^{-sx}|\,dx \leq C\int_{-\infty}^t e^{-\sigma x}\,dx = \frac{Ce^{-\sigma t}}{\sigma},$$

luego el integrando está acotado por $2C/R^2$ y la integral por C/R.

Así pues, si fijamos un $\epsilon > 0$, podemos tomar un $R > 0$ (y su $\delta > 0$ correspondiente), de modo que las dos integrales que hemos analizado tengan módulo menor que $\epsilon/4$. Fijados estos R y δ, consideramos la integral

$$\frac{1}{2\pi i}\int_{\gamma_2} e^{st}g(s)\left(1 + \frac{s^2}{R^2}\right)\frac{ds}{s}.$$

Tomamos una cota C' de $g(s)(1+s^2/R^2)/s$ sobre γ_2^* y, por compacidad, podemos tomar $t_0 > 0$ tal que si $t > x_0$ entonces,

$$|e^{st}| < \frac{2\pi\epsilon}{2L(\gamma_2)C'}$$

para todo $s \in \gamma_2^*$. Esto hace que la integral sea menor que $\epsilon/2$ y, en definitiva, que $|g(0) - g_t(0)| < \epsilon$, para todo $t \geq t_0$. ∎

Ahora ya podemos probar un teorema cuya conclusión no tiene nada que ver con series de Dirichlet: bajo ciertas hipótesis sobre una serie de Dirichlet, nos asegura que una función que por hipótesis está acotada, de hecho converge a 1:

Teorema 3.40 *Consideremos una serie de Dirichlet*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

con coeficientes $a_n \geq 0$ tales que exista una constante $A > 0$ de modo la función de las sumas finitas

$$\theta(x) = \sum_{n \leq x} a_n$$

cumpla $\theta(x) \leq Ax$. Supongamos que f converge[5] *en el semiplano $\sigma > 1$ a una función holomorfa que admite una prolongación analítica a un abierto que contiene al semiplano $\sigma \geq 1$, salvo el punto $s = 1$, donde la prolongación tiene un polo simple con residuo 1. En tal caso*

$$\lim_{x \to +\infty} \frac{\theta(x)}{x} = 1.$$

Demostración: Observemos que la función $\phi(x)$ definida en el enunciado del teorema 3.38 no es sino $\phi(x) = \theta(e^x)$. Por consiguiente,

$$f(s) = s \int_0^{+\infty} \theta(e^x) e^{-sx}\, dx, \qquad \text{para } \sigma > 1.$$

Al igual que $f(s)$, la función $f(s)/s$ se prolonga a una función holomorfa en un abierto que contiene al semiplano $\sigma \geq 1$ salvo un polo simple en $s = 1$ con residuo 1. Notemos que el residuo sigue siendo 1 porque

$$\lim_{s \to 1} (s-1) \frac{f(s)}{s} = 1.$$

Por consiguiente, la función

$$\frac{f(s)}{s} - \frac{1}{s-1} = \int_0^{+\infty} \theta(e^x) e^{-sx} - e^{-(s-1)x}\, dx$$

se prolonga analíticamente a un abierto que contiene al semiplano $\sigma \geq 1$. Para ajustarnos a las hipótesis del teorema anterior consideramos la función

$$g(s) = \frac{f(s+1)}{s+1} - \frac{1}{s} = \int_0^{+\infty} (\theta(e^x) e^{-x} - 1) e^{-sx}\, dx,$$

que es holomorfa en un abierto que contiene al semiplano $\sigma \geq 0$. La hipótesis sobre θ hace que $\phi(x) = \theta(e^x)e^{-x} - 1$ esté acotada, y obviamente es integrable en intervalos acotados. Así pues, existe la integral

$$\int_0^{+\infty} (\theta(e^x) e^{-x} - 1)\, dx = \int_1^{+\infty} \frac{\theta(x) - x}{x^2}\, dx.$$

[5]Según el teorema [VC 4.25], la hipótesis $\theta(x) \leq Ax$ ya implica que la serie converge para $\sigma > 1$. No obstante, puede probarse que la hipótesis sobre θ no es realmente necesaria.

Supongamos ahora que existe un $\lambda > 1$ para el que hay valores de x arbitrariamente grandes con $\theta(x) \geq \lambda x$. Como θ es monótona, para estos x se cumple que

$$\int_x^{\lambda x} \frac{\theta(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^{\lambda} \frac{\lambda - t}{t^2}\, dt > 0,$$

y el hecho de que esto suceda con valores de x arbitrariamente grandes contradice la convergencia de la integral.

Si existe $0 < \lambda < 1$ tal que, para valores de x arbitrariamente grandes, tenemos $\theta(x) \leq \lambda x$, entonces

$$\int_{\lambda x}^{x} \frac{\theta(t) - t}{t^2}\, dt \leq \int_{\lambda x}^{x} \frac{\lambda x - t}{t^2}\, dt = \int_{\lambda}^{1} \frac{\lambda - t}{t^2}\, dt < 0,$$

y de nuevo tenemos una contradicción.

Esto implica que, para todo $\epsilon > 0$, tomando $\lambda = 1 \pm \epsilon$, se cumple, para todo x suficientemente grande, que $1 - \epsilon < \theta(x)/x < 1 + \epsilon$, luego en efecto, $\lim_{x\to+\infty} \theta(x)/x = 1$. ∎

Ahora basta aplicar este teorema a la función considerada en 3.37:

Teorema 3.41 *Se cumple $\vartheta(x) \sim x$.*

Demostración: La función $\Phi(x)$ del teorema 3.37 cumple las hipótesis del teorema anterior. Notemos que la sucesión de sumas finitas de sus coeficientes es precisamente $\vartheta(x)$, y la hipótesis $\vartheta(x) \leq Ax$ es el teorema 3.8. La conclusión es precisamente que $\vartheta(x) \sim x$. ∎

Por consiguiente, todas las afirmaciones del teorema 3.7 son ciertas, y queda demostrado el teorema de los números primos.

Probamos ahora una variante de 3.40 para sucesiones de números complejos cualesquiera que usaremos en la sección siguiente.

Teorema 3.42 *Sea $f(s)$ una serie de Dirichlet en las condiciones del teorema anterior y sea $g(s)$ una serie de Dirichlet con coeficientes $b_n \in \mathbb{C}$ convergente en el semiplano $\sigma > 1$ y prolongable analíticamente a la recta $\sigma = 1$ salvo quizá a $s = 1$, donde tiene un polo simple con residuo α (entendiendo que $\alpha = 0$ si no hay tal polo). Supongamos que existe una constante C tal que $|b_n| \leq Ca_n$ y sea $\psi(x) = \sum_{n\leq x} b_n$. Entonces*

$$\lim_{x\to+\infty} \frac{\psi(x)}{x} = \alpha.$$

Demostración: Supongamos primero que los coeficientes de g son reales (y por lo tanto α también). Podemos tomar $C > \alpha$. Entonces la función $f^* = (Cf + g)/(C + \alpha)$ cumple las mismas hipótesis que f, luego el teorema anterior nos da que

$$\lim_{x\to+\infty} \frac{\psi_{f^*}(x)}{x} = \lim_{x\to+\infty} \frac{C\psi_f(x) + \psi_g(x)}{(C + \alpha)x} = 1$$

o equivalentemente,

$$C \lim_{x\to+\infty} \frac{\psi_f(x)}{x} + \lim_{x\to+\infty} \frac{\psi_g(x)}{x} = C + \alpha,$$

donde el segundo límite existe porque existe el primero y el de la suma. Como el primer límite es 1, la conclusión es inmediata.

En el caso general consideramos la serie

$$\bar{g}(s) = \sum_{n=1}^{\infty} \frac{\bar{b}_n}{n^s}.$$

Claramente $\bar{g}(s) = \overline{g(s)}$ y además

$$g = \frac{g+\bar{g}}{2} + \frac{g-\bar{g}}{2i}.$$

Las funciones $g \pm \bar{g}$ cumplen las hipótesis del teorema y sus coeficientes son reales. Por el caso anterior cumplen la tesis, y de aquí se sigue fácilmente que lo mismo sucede con g. ∎

3.8 Más sobre primos en progresiones aritméticas

Finalmente demostramos el refinamiento del teorema de Dirichlet que hemos discutido en la introducción. Si $m \geq 2$ y k es un entero primo con m, llamamos $\pi_k(x)$ al número de primos $p \leq x$ tales que $p \equiv k \pmod{m}$. El teorema de Dirichlet sobre primos en progresiones aritméticas equivale a que

$$\lim_{x\to+\infty} \pi_k(x) = +\infty,$$

mientras que ahora vamos a probar lo siguiente:

Teorema 3.43 *Sea $m \geq 2$ y k un número entero primo con m. Entonces*

$$\lim_{x\to+\infty} \frac{\pi_k(x)}{\pi(x)} = \frac{1}{\phi(m)}.$$

Empezamos introduciendo un concepto general de equidistribución de funciones en términos de caracteres de grupos abelianos:

Definición 3.44 Sea G un grupo abeliano finito. Sea $\mathbb{C}^G$ el espacio vectorial de todas las aplicaciones de G en $\mathbb{C}$. Para cada $f \in \mathbb{C}^G$ definimos

$$\int_G f(g)\,dg = \frac{1}{|G|} \sum_{g\in G} f(g).$$

Este operador integral define una aplicación lineal $\mathbb{C}^G \longrightarrow \mathbb{C}$. Las relaciones de ortogonalidad 3.50 afirman en estos términos que

$$\int_G \chi(g)\,dg = \begin{cases} 1 & \text{si } \chi = 1 \\ 0 & \text{si } \chi \neq 1 \end{cases}$$

para todo carácter χ de G.

De aquí se sigue que los caracteres de G son linealmente independientes como elementos de $\mathbb{C}^G$. En efecto, dada una combinación lineal nula

$$\sum_\chi \alpha_\chi \chi = 0,$$

si ψ es un carácter fijo también se cumple

$$\sum_\chi \alpha_\chi \chi\psi^{-1} = 0,$$

y al integrar queda $\alpha_\psi = 0$.

Como la dimensión de $\mathbb{C}^G$ es $|G|$, concluimos que los caracteres forman una base, con lo que toda función $f \in \mathbb{C}^G$ se expresa como combinación lineal de los caracteres de G.

Sea A un conjunto de primos no vacío y sea $A_x = \{p \in A \mid p \leq x\}$. Diremos que una aplicación $\lambda : A \longrightarrow G$ está *equidistribuida* si para todo carácter χ de G se cumple

$$\lim_{x\to+\infty} \frac{\sum\limits_{p\in A_x} \chi(\lambda(p))}{|A_x|} = \int_G \chi(g)\,dg. \tag{3.19}$$

Observemos que si χ es el carácter principal el miembro derecho de (3.19) vale 1 y se cumple trivialmente la igualdad. Si χ no es principal las relaciones de ortogonalidad implican que el miembro derecho vale 0. Notemos también que los dos miembros de (3.19) son lineales en χ. Como toda aplicación $f : G \longrightarrow \mathbb{C}$ puede expresarse como combinación lineal de los caracteres de G, resulta que si λ está equidistribuida entonces

$$\lim_{x\to+\infty} \frac{\sum\limits_{p\in A_x} f(\lambda(p))}{|A_x|} = \int_G f(g)\,dg.$$

En particular, si f es la función que vale 1 sobre un elemento fijo $g \in G$ y es 0 en los restantes, resulta

$$\lim_{x\to+\infty} \frac{\big|\{p \in A \mid p \leq x, \lambda(p) = g\}\big|}{\big|\{p \in A \mid p \leq x\}\big|} = \frac{1}{|G|}.$$

Esto significa que para valores grandes de x hay aproximadamente el mismo número de primos $p \leq x$ en A con la misma imagen por λ. Es fácil ver que esta última igualdad equivale a la equidistribución.

Así pues, para probar 3.43 basta ver que si A es el conjunto de los primos que no dividen a m, la aplicación $\lambda : A \longrightarrow U_m$ dada por $\lambda(p) = [p]$ está equidistribuida. Esto implica que

$$\lim_{x\to+\infty} \frac{\pi_k(x)}{\pi(x) - c} = \frac{1}{\phi(m)},$$

donde c es el número de primos que dividen a m, pero es claro que dicha c puede eliminarse.

Así pues, basta probar que todo carácter no principal χ módulo m cumple que el límite de (3.19) es igual a 0.

Para ello partimos de la fórmula (3.16):

$$\log L(s,\chi) = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}}$$

que obtuvimos en la prueba del teorema de Dirichlet. Al derivar queda

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{p,n} \frac{\log p\, \chi(p^m)}{p^{ns}}.$$

Por el teorema 3.34 esta función es holomorfa sobre toda la recta $\sigma = 1$. Si separamos los términos con $n \geq 2$ obtenemos una serie mayorada en módulo por

$$\sum_{p,n\geq 2} \frac{\log p}{p^{ns}},$$

y en la demostración del teorema 3.37 hemos probado que esta serie converge en el semiplano $\sigma > 1/2$. Por consiguiente, la serie restante,

$$\sum_p \frac{\log p\, \chi(p)}{p^s}$$

define una función holomorfa en el semiplano $\sigma > 1$ que se prolonga analíticamente a la recta $\sigma = 1$. Aplicamos el teorema 3.42 tomando como g a esta serie y como f a

$$\sum_p \frac{\log p}{p^s}.$$

La conclusión es que

$$\sum_{p\leq x} \log p\, \chi(p) = o(x),$$

y el teorema 3.2 nos permite eliminar los logaritmos:

$$\sum_{p\leq x} \chi(p) = o\left(\frac{x}{\log x}\right).$$

El teorema de los números primos nos da finalmente que

$$\lim_{x\to+\infty} \frac{\sum\limits_{p\le x} \chi(p)}{\pi(x)} = 0.$$

Esta fórmula sigue siendo cierta si en el denominador ponemos $\pi(x) - c$, donde c es el número de primos que dividen a m, y entonces tenemos (3.19). ∎

3.9 Apéndice: Caracteres modulares

Los caracteres modulares que pretendemos estudiar aquí son esencialmente los caracteres de los grupos de unidades U_m de $\mathbb{Z}/m\mathbb{Z}$, pero conviene probar los resultados básicos en el contexto más general de los grupos abelianos finitos.

Definición 3.45 Si G es un grupo abeliano finito, un *carácter* de G es un homomorfismo de grupos $\chi : G \longrightarrow \mathbb{C} \setminus \{0\}$. Llamaremos G^* al conjunto de todos los caracteres de G. Es claro que G^* es un grupo con el producto definido puntualmente. Se llama *grupo dual* de G. El elemento neutro es el llamado *carácter principal,* dado por $1(g) = 1$ para todo $g \in G$.

Observemos que si χ es un carácter de G y g es un elemento de orden n, entonces se cumple $\chi(g)^n = \chi(g^n) = \chi(1) = 1$, luego $|\chi(g)| = 1$. De aquí se sigue que el carácter inverso de χ es precisamente su carácter conjugado, dado por $\overline{\chi}(g) = \overline{\chi(g)}$.

Necesitamos un único hecho adicional sobre caracteres, pero para demostrarlo nos harán falta otros resultados intermedios. En primer lugar veremos que $|G| = |G^*|$. Lo probamos primero para grupos cíclicos:

Teorema 3.46 *Sea G un grupo abeliano finito. Supongamos que existe $g \in G$ tal que $G = \langle g\rangle$. Entonces $|G| = |G^*|$.*

Demostración: Sea n el orden de g. Sea $\zeta = e^{2\pi i/n}$. Es claro que el orden de ζ en $\mathbb{C} \setminus \{0\}$ también es n y de aquí es fácil deducir que la aplicación $\chi : \langle g\rangle \longrightarrow \langle\zeta\rangle$ es un isomorfismo de grupos, y en particular un carácter de G.

Como $\chi^k(g) = \zeta^k$ y las potencias $1, \zeta, \ldots, \zeta^{n-1}$ son todas distintas, es claro que los caracteres $1, \chi, \ldots, \chi^{n-1}$ son todos distintos, y así $|G| = n \le |G^*|$. Veamos que G no tiene más caracteres que éstos.

Si ψ es cualquier carácter de G entonces $\psi(g)^n = \psi(g^n) = \psi(1) = 1$, luego ha de ser $\psi(g) = \zeta^k$ para $0 \le k < n$. Así, $\psi(g) = \chi^k(g)$ y es claro entonces que $\psi = \chi^k$. ∎

Teorema 3.47 *Sea G un grupo abeliano finito y H un subgrupo de G. Entonces todo carácter de H se extiende a un carácter de G.*

DEMOSTRACIÓN: Si $H = G$ es obvio. Sea $g \in G \setminus H$ y consideremos $H_1 = \{g^k h \mid k \in \mathbb{Z},\ h \in H\}$. Claramente H_1 es un subgrupo de G que contiene estrictamente a H. Basta probar que todo carácter de H se extiende a H_1, pues tras repetir el proceso de extensión un número finito de veces llegaremos hasta una extensión a todo G.

Sea, pues, $\chi \in H^*$. Sea n el orden de la clase $[g]$ en el grupo cociente G/H, esto es, el mínimo $n > 0$ tal que $g^n \in H$. Sea $\zeta \in \mathbb{C}$ tal que $\zeta^n = \chi(g^n)$. Definimos $\psi(g^k h) = \zeta^k \chi(h)$. Si probamos que esta definición no depende de la representación de un elemento de H_1 en la forma $g^k h$ tendremos claramente que ψ es un carácter de H_1 que extiende a χ.

Supongamos que $g^k h_1 = g^j h_2$. Entonces $g^{k-j} = h_2 h_1^{-1} \in H$, luego $n \mid k-j$, es decir, $k - j = nr$. Entonces

$$\zeta^{k-j} = (\zeta^n)^r = \chi(g^n)^r = \chi(g^{nr}) = \chi(g^{k-j}) = \chi(h_2 h_1^{-1}),$$

luego $\zeta^k \chi(h_1) = \zeta^j \chi(h_2)$. ∎

Una consecuencia inmediata es la siguiente:

Teorema 3.48 *Sea G un grupo abeliano finito y $g \in G$. Si $\chi(g) = 1$ para todo carácter de G, entonces $g = 1$.*

DEMOSTRACIÓN: Supongamos que $g \neq 1$. Entonces el grupo $\langle g \rangle$ tiene más de un elemento, luego por el teorema 3.46 tiene más de un carácter. Si χ es un carácter de $\langle g \rangle$ no principal entonces es claro que $\chi(g) \neq 1$, y por el teorema anterior χ se extiende a un carácter de G con la misma propiedad. ∎

Teorema 3.49 *Sea G un grupo abeliano finito. Entonces $|G| = |G^*|$.*

DEMOSTRACIÓN: Supongamos que el teorema es falso y tomemos un grupo G que lo incumpla con el mínimo número de elementos posible. Obviamente ha de ser $G \neq 1$. Sea $h \in G$ tal que $h \neq 1$. Consideremos el subgrupo $H = \langle h \rangle$. Claramente $|G/H| < |G|$, luego por la elección de G se cumple que $|(G/H)^*| = |G/H|$ y por el teorema 3.46 también $|H^*| = |H|$.

Consideremos la aplicación $G^* \longrightarrow H^*$ dada por $\chi \longrightarrow \chi|_H$. Claramente es un homomorfismo de grupos y por el teorema 3.47 es suprayectiva. Su núcleo es $N = \{\chi \in G^* \mid \chi|_H = 1\}$.

Claramente $G^*/N \cong H^*$, luego $|G^*| = |G^*/N|\,|N| = |H^*|\,|N| = |H|\,|N|$. Basta probar que $|N| = |(G/H)^*|$, pues entonces $|G^*| = |H|\,|(G/H)^*| = |H|\,|G/H| = |G|$, contradicción.

Es claro que todo $\chi \in N$ induce un carácter de G/H dado por $\chi\big([g]\big) = \chi(g)$ y, recíprocamente, todo $\chi \in (G/H)^*$ es inducido por el carácter de N dado por $\chi(g) = \chi\big([g]\big)$. De hecho ambos grupos son isomorfos. ∎

El único resultado no trivial que necesitamos sobre los caracteres de un grupo abeliano, aparte de su número, es el siguiente:

Teorema 3.50 (Relaciones de ortogonalidad) *Sea G un grupo abeliano finito.*

1. *Si $\chi \in G^*$ entonces*

$$\sum_{g\in G}\chi(g) = \begin{cases} |G| & si\ \chi = 1,\\ 0 & si\ \chi \neq 1.\end{cases}$$

2. *Si $g \in G$ entonces*

$$\sum_{\chi\in G^*}\chi(g) = \begin{cases} |G| & si\ g = 1,\\ 0 & si\ g \neq 1.\end{cases}$$

Demostración: 1) El caso $\chi = 1$ es obvio. Si $\chi \neq 1$ existe un $h \in G$ tal que $\chi(h) \neq 1$. Notar que cuando g recorre G entonces gh también recorre G, luego

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

con lo que $(\chi(h)-1)\sum_{g\in G}\chi(g) = 0$ y por lo tanto $\sum_{g\in G}\chi(g) = 0$.

2) Es claro que la aplicación $\delta_g : G^* \longrightarrow \mathbb{C}\setminus\{0\}$ dada por $\delta_g(\chi) = \chi(g)$ es un carácter de G^*. Basta aplicarle el apartado 1). ∎

Los caracteres de Dirichlet son simplemente las funciones aritméticas inducidas por los caracteres de los grupos de unidades:

Definición 3.51 Sea $m > 1$ un número natural. Si χ es un carácter del grupo U_m, llamaremos *carácter de Dirichlet módulo m* inducido por χ a la función aritmética dada por

$$\chi(n) = \begin{cases} \chi\big([n]\big) & \text{si } (n.m) = 1,\\ 0 & \text{si } (n,m) \neq 1.\end{cases}$$

Capítulo IV

La función dseta de Riemann I

En la prueba del teorema de los números primos que hemos presentado en el capítulo anterior ha sido esencial el hecho de que la función dseta de Riemann no se anula en la recta $\sigma = 1$. Concretamente, hemos usado esto para asegurar que $s = 1$ es el único polo de la función Φ del teorema 3.37. En este capítulo estudiaremos más a fondo la función dseta, y veremos que las propiedades que obtendremos tienen repercusiones notables en la distribución de los números primos. Empecemos recapitulando lo que hemos probado sobre la función dseta en [ITAn], [IC] y [An]:

Por completitud recordamos primero que, sobre el semiplano $\sigma > 1$, la función dseta está definida por las expresiones [ITAn 8.26]

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

Sabemos evaluarla explícitamente en los números naturales pares [ITAn 6.17]:

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(-1)^{k+1} 2^{2k-1} \pi^{2k} B_{2k}}{(2k)!},$$

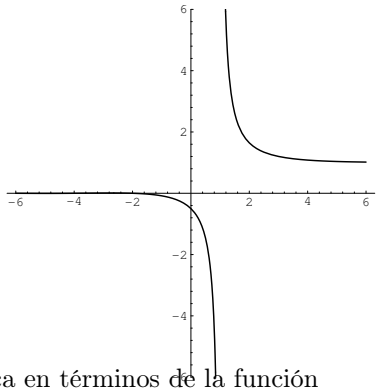
donde los números B_{2k} son los números de Bernoulli definidos en [ITAn 6.17] y determinados recurrentemente en la sección [ITAn 6.5]. En [An 10.38] hemos visto que esta función holomorfa admite una prolongación analítica a una función meromorfa en $\mathbb{C}$ con un único polo en el punto $s = 1$, que es un polo simple con residuo 1.

El teorema [An 10.39] nos da el valor de esta prolongación en 0 y sobre los números negativos:

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

En particular la función dseta se anula en los enteros negativos pares, mientras que $\zeta(0) = -1/2$.

La figura muestra la gráfica de $\zeta(s)$ sobre el eje real. La función dseta satisface la ecuación funcional [An 10.43]



$$\zeta(s) = \chi(s)\zeta(1-s),$$

donde

$$\chi(s) = 2\Pi(-s)(2\pi)^{s-1}\operatorname{sen}(\pi s/2)$$
$$= \pi(2\pi)^{s-1}\frac{1}{\cos(\pi s/2)\Pi(s-1)}.$$

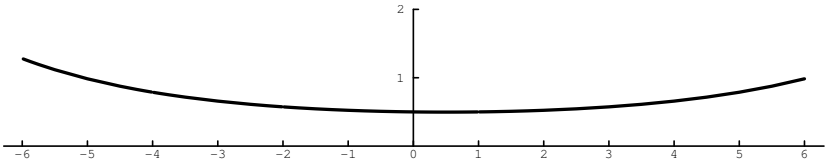
Esta ecuación se expresa de forma simétrica en términos de la función

$$\xi(s) = \pi^{-s/2}\Pi(s/2)(s-1)\zeta(s),$$

que satisface la ecuación funcional

$$\xi(s) = \xi(1-s).$$

Ésta es la gráfica de $\xi(s)$ sobre el eje real:



En la sección [An 10.6] se justifica que, tal y como se observa en la gráfica:

$$\xi(0) = \xi(1) = \pi^{-1/2}\Pi(1/2) = 1/2.$$

He aquí otros hechos básicos sobre la función ξ:

1. *La función $\xi(s)$ es entera.*

   En efecto, la función factorial tiene únicamente polos simples en los enteros negativos, luego $\Pi(s/2)$ tiene polos simples en los enteros pares negativos, que se cancelan con los ceros simples de $\zeta(s)$, y el único polo de $\zeta(s)$ se cancela con el cero de $s-1$.

2. *Las funciones $\zeta(s)$ y $\xi(s)$ tienen los mismos ceros con las mismas multiplicidades, salvo los enteros pares negativos, que son ceros de $\zeta(s)$, pero no de $\xi(s)$.*

   En efecto, la función factorial no se anula, y el cero de $s-1$ se cancela con el polo de $\zeta(s)$, luego todo cero de $\xi(s)$ es un cero de $\zeta(s)$ con la misma multiplicidad. Recíprocamente, todo cero de $\zeta(s)$ es un cero de $\xi(s)$ salvo los enteros negativos, que se cancelan con los polos de la función factorial.

3. *Todos los ceros de $\xi(s)$ se encuentran en la banda $0 \le \sigma \le 1$.*

   En efecto, la expresión en producto de Euler prueba que la función $\zeta(s)$ no se anula en el semiplano $\sigma > 1$, luego tampoco lo hace ξ y, por la ecuación funcional, ξ tampoco se anula en el semiplano $\sigma < 0$.

4. *Se cumple que $\overline{\xi(s)} = \xi(\bar{s})$.*

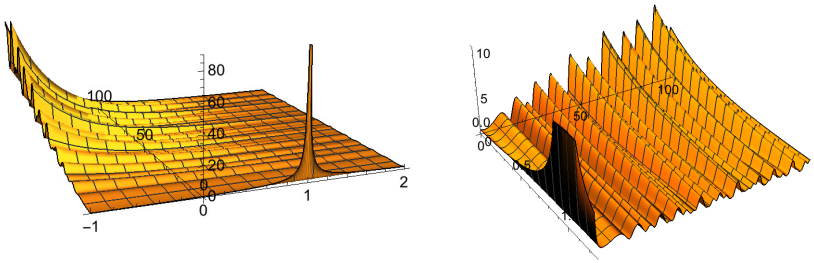
   Basta tener en cuenta que ξ es real sobre el semieje real $\sigma > 1$, $\tau = 0$, por lo que su serie de Taylor en $s_0 = 2$, por ejemplo, (que converge en todo el plano complejo) tiene coeficientes reales, y la conjugación conmuta con el sumatorio por continuidad. Esto implica a su vez que $\zeta(s)$ tiene la misma propiedad.

5. *Si ρ es un cero de ξ, también lo son $1-\rho$, $\bar{\rho}$ y $1-\bar{\rho}$, y los cuatro tienen la misma multiplicidad.*

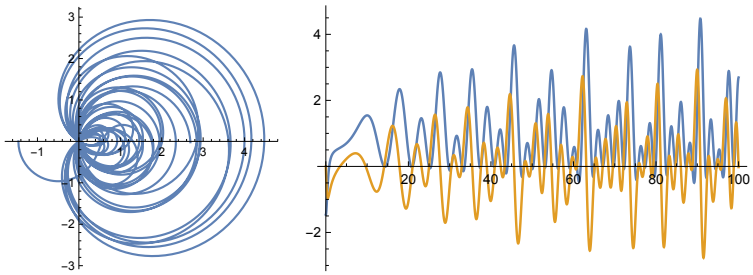
   Esto es consecuencia inmediata de la ecuación funcional y del apartado anterior.

Los enteros negativos se llaman *ceros triviales* de $\zeta(s)$, mientras que sus otros posibles ceros (necesariamente situados en la banda $0 \le \sigma \le 1$) se llaman *ceros no triviales* de $\zeta(s)$ y coinciden (en posición y multiplicidad) con los ceros de la función $\xi(s)$. Todavía no hemos demostrado la existencia de ceros no triviales.

El teorema 3.36 implica, junto con la ecuación funcional, que los ceros no triviales de $\zeta(s)$ tienen que estar necesariamente en la banda abierta $0 < \sigma < 1$. Esta banda se conoce habitualmente como la *banda crítica* de la función dseta.



Las figuras muestran dos gráficas de la función $|\zeta(s)|$. La primera en la región $[-1, 2] \times [0, 100]$ y la segunda en $[0, 1.25] \times [0, 100]$. Las oscilaciones que vemos en cada recta vertical $\sigma = \sigma_0$ se corresponden con giros de $\zeta(\sigma_0 + \tau i)$. Por ejemplo, la figura de la izquierda muestra la curva $\zeta(1/2+\tau i)$, mientras que la de la derecha muestra las gráficas de $\operatorname{Re}\zeta(1/2+\tau i)$, $\operatorname{Im}\zeta(1/2+\tau i)$.



Las gráficas muestran que la curva pasa muchas veces por el punto 0, es decir, que la función dseta tiene ceros no triviales. Más adelante probaremos que esto es realmente así.

4.1 Aproximación de la función dseta

En el semiplano $\sigma > 1$ la función dseta de Riemann se puede aproximar por las sumas parciales de su serie de Dirichlet. En realidad esto sirve de poco si no podemos estimar la precisión de las aproximaciones obtenidas, pero peor es el hecho de que esto ya no es válido en el resto del plano complejo, en particular en la banda crítica $0 < \sigma < 1$, que es donde —como veremos— tiene más interés conocer el comportamiento de la función dseta.

En esta sección demostraremos una fórmula que no sólo resuelve estos inconvenientes y nos permite calcular en la práctica la función dseta sobre el semiplano $\sigma > 0$ con cualquier precisión deseada, sino que también nos será útil en diversas ocasiones en el estudio teórico de la función.

Para empezar fijamos un número real $s > 0$ y aplicamos el teorema 2.20 con $c_n = 1$ y $f(x) = 1/x^s$. La conclusión es que

$$\sum_{n\le x}\frac{1}{n^s} = \frac{E[x]}{x^s} + s\int_1^x \frac{E[t]}{t^{s+1}}\,dt = \frac{E[x]}{x^s} - s\int_1^x \frac{t-E[t]}{t^{s+1}}\,dt + s\int_1^x \frac{1}{t^s}\,dt$$

$$= \frac{E[x]}{x^s} + \frac{s}{s-1} - \frac{s}{(s-1)x^{s-1}} - s\int_1^x \frac{t-E[t]}{t^{s+1}}\,dt$$

$$= \frac{s}{s-1} - \frac{x-E[x]}{x^s} - \frac{1}{(s-1)x^{s-1}} - s\int_1^x \frac{t-E[t]}{t^{s+1}}\,dt.$$

Ahora bien, la última integral, para un x fijo, define una función entera, luego por el principio de prolongación analítica, la igualdad

$$\sum_{n\le x}\frac{1}{n^s} = \frac{s}{s-1} - \frac{x-E[x]}{x^s} - \frac{1}{(s-1)x^{s-1}} - s\int_1^x \frac{t-E[t]}{t^{s+1}}\,dt \tag{4.1}$$

es válida para todo $s \in \mathbb{C}$ y todo $x > 0$. De aquí deducimos:

Teorema 4.1 *En el semiplano $\sigma > 0$ se cumple que*

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

$$\zeta(s) - \sum_{n\le x}\frac{1}{n^s} = \frac{1}{(s-1)x^{s-1}} + \frac{x-E[x]}{x^s} - s\int_x^{+\infty} \frac{t-E[t]}{t^{s+1}}\,dt.$$

Demostración: Partimos de la igualdad (4.1). Cuando s está en el semiplano $\sigma > 1$ podemos hacer que x tienda a $+\infty$ y así obtenemos la primera igualdad del enunciado.

Ahora bien, si fijamos $\delta > 0$, para todo s en el semiplano $\sigma > 0$ se cumple que

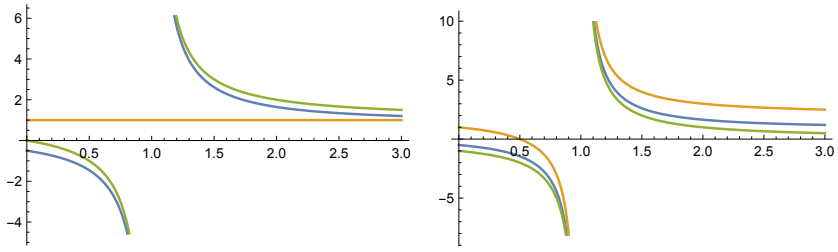
$$\left|\frac{t - E[t]}{t^{s+1}}\right| < \frac{1}{t^{\sigma+1}} < \frac{1}{t^{\delta+1}}.$$

Como esta función es integrable en $[1, +\infty[$, el teorema [VC 1.24] nos da que la integral de la primera igualdad del enunciado es una función holomorfa en el semiplano $\sigma > 0$, luego por el principio de prolongación analítica no sólo es válida cuando $\sigma > 1$, sino también cuando $\sigma > 0$. La segunda fórmula se obtiene restando (4.1) de la primera. ∎

En la segunda fórmula del teorema anterior el segundo término del segundo miembro se anula si tomamos $x = k$ natural. En el semiplano $\sigma > 1$ todos los términos del segundo miembro tienden a 0, lo cual nos permite acotar el error de la aproximación de $\zeta(s)$ por las sumas parciales de su serie de Dirichlet. Si $0 < \sigma < 1$ sólo tiende a 0 el primer término, pero en cualquier caso al sumárselo a la suma parcial obtenemos una aproximación mejor fácil de calcular, para la cual el error está acotado por:

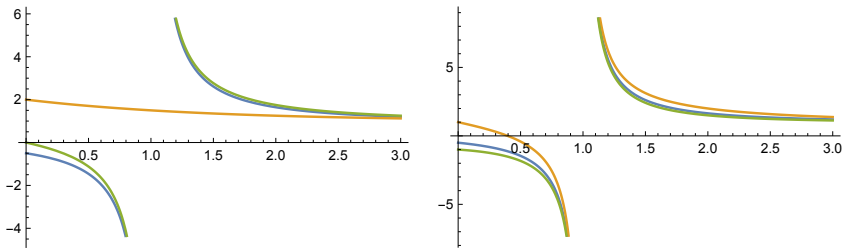
$$\left|\zeta(s) - \sum_{n=1}^{k} \frac{1}{n^s} - \frac{1}{(s-1)k^{s-1}}\right| \leq |s| \int_k^{+\infty} \frac{1}{t^{\sigma+1}}\, dt = \frac{|s|}{\sigma k^\sigma}. \tag{4.2}$$

Veamos algunas ilustraciones de esta fórmula. La gráfica de la izquierda muestra $\zeta(s)$ "exacta" sobre el eje real (es decir, aproximada con técnicas numéricas más sofisticadas más allá del margen de precisión de la gráfica), la suma parcial de la serie de Dirichlet hasta $k = 1$ y la suma aumentada con el término $(s-1)^{-1}k^{1-s}$. La gráfica de la derecha contiene de nuevo la función $\zeta(s)$ y y las de la suma parcial modificada a la que hemos sumado y restado la cota del error $|s|\sigma^{-1}k^{-\sigma}$.



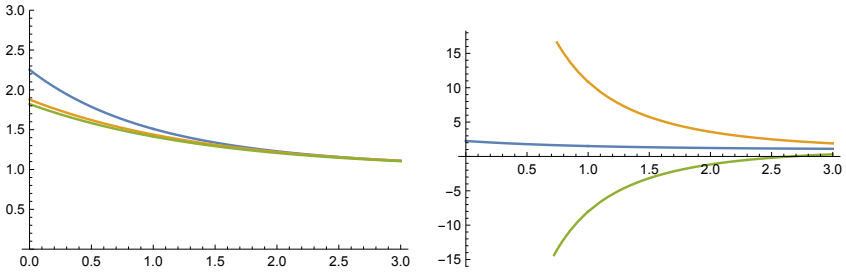
$\zeta(\sigma + 0i)$, $k = 1$

Vemos que simplemente con $k = 1$ ya obtenemos una aproximación razonable sobre el eje real. Las figuras siguientes contienen las mismas gráficas, pero con $k = 2$. Vemos que la mejora es sustancial. Con $k = 10$ las sumas parciales modificadas ya casi no se distinguen del valor exacto para $s \geq 1/2$.

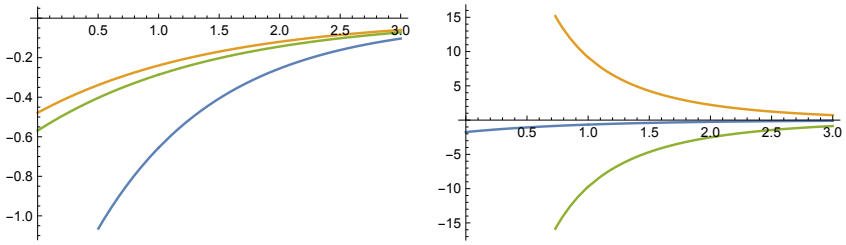


$\zeta(\sigma + 0i)$, $k = 2$

Las gráficas siguientes muestran las aproximaciones sobre la recta $\tau = 6\pi$ con $k = 2$ (hemos escogido precisamente el valor 6π porque nos interesará en un ejemplo posterior). Vemos que la aproximación de la parte real es buena, pero la estimación del error no lo es. Resulta que es necesario aumentar mucho k para reducir la cota de error a niveles aceptables.



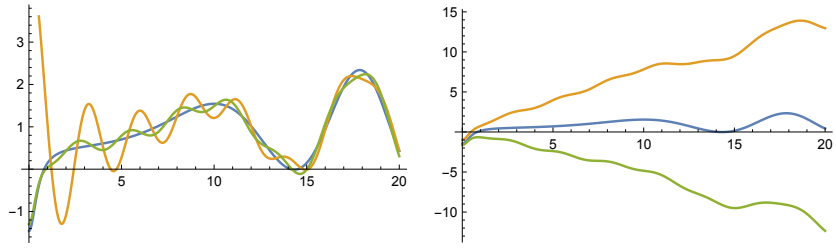
$\operatorname{Re}\zeta(\sigma + 6\pi i)$, $k = 2$



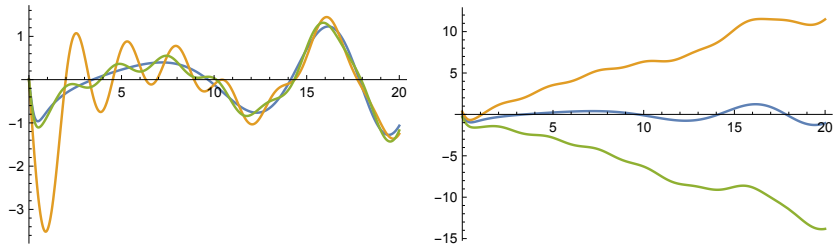
$\operatorname{Im}\zeta(\sigma + 6\pi i)$, $k = 2$

En la página siguiente mostramos aproximaciones sobre la recta $\sigma = 1/2$. Nuevamente vemos que la aproximación con la suma parcial modificada es mucho más precisa que lo que indica la cota de error que hemos obtenido. Esto se debe a la estimación cruda que hemos hecho de la integral acotando $t - E[t] \leq 1$. Descomponiendo la integral en sumas sobre intervalos $[c, c+1]$ es posible refinar la cota del error, pero de una forma bastante laboriosa.

Enseguida daremos una forma alternativa de acotar el error con más precisión, pero antes vamos a extraer las primeras consecuencias teóricas del teorema 4.1:



$\operatorname{Re}\zeta(1/2+\tau I)$, $k=10$



$\operatorname{Im}\zeta(1/2+\tau I)$, $k=10$

Teorema 4.2 *Si $0<s<1$, entonces $\zeta(s)<0$. Por consiguiente, los únicos ceros reales de la función dseta son sus ceros triviales.*

DEMOSTRACIÓN: Basta observar que si $0<s<1$ la integral que aparece en la primera expresión del teorema 4.1 es claramente positiva. ∎

Así pues, es equivalente hablar de ceros no triviales o de ceros imaginarios de la función dseta.

Como segunda aplicación determinamos el segundo término de la serie de Laurent de $\zeta(s)$:

Teorema 4.3 *En un entorno de $s=1$ se cumple que*

$$\zeta(s)=\frac{1}{s-1}+\gamma+O(s-1).$$

DEMOSTRACIÓN: Sabemos que $\zeta(s)$ tiene un polo simple en $s=1$ con residuo 1, luego el primer término de su serie de Laurent es el que indica el enunciado. Al restárselo, tenemos una función entera y queremos calcular su valor en 1. Para ello partimos de que

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

y sabemos que la integral define una función holomorfa en el semiplano $\sigma>0$, luego podemos tomar el límite cuando $s\to 1$, y el resultado es

$$\lim_{s\to 1}\left(\zeta(s)-\frac{1}{s-1}\right)=1-\int_1^{+\infty}\frac{t-E[t]}{t^2}\,dt$$

$$= \lim_n \sum_{m=1}^{n-1} \left(\int_m^{m+1} \frac{E[t]}{t^2}\,dt - \int_m^{m+1} \frac{1}{t}\,dt \right) + 1$$

$$= \lim_n \sum_{m=1}^{n-1} \left(m \int_m^{m+1} \frac{1}{t^2}\,dt - (\log(m+1) - \log m) \right) + 1$$

$$= \lim_n \sum_{m=1}^{n-1} m \left(\frac{1}{m} - \frac{1}{m+1} \right) + 1 - \log n$$

$$= \lim_n \sum_{m=1}^{n-1} \left(1 - \frac{m}{m+1} \right) + 1 - \log n = \lim_n \sum_{m=1}^{n-1} \frac{1}{m+1} + 1 - \log n = \gamma. \qquad \blacksquare$$

Aunque no nos va a ser necesario más adelante, vamos mejorar la cota del error dada por la fórmula (4.2). Para ello calcularemos las colas de la serie de Dirichlet por un método similar al empleado en el teorema [An 10.29] para sumar series mediante el teorema de los residuos.

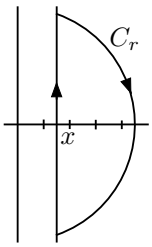
Teorema 4.4 *Dado un número complejo s en el semiplano $\sigma > 0$ y $x = k+1/2$, donde k es un número natural, cumple $x > |\tau|/2\pi$, entonces*

$$\left| \zeta(s) - \sum_{n<x} \frac{1}{n^s} - \frac{1}{(s-1)x^{s-1}} \right| \le \frac{2x^{-\sigma}}{2\pi - |\tau|/x}.$$

Demostración: La idea básica es que la función $\pi \cot \pi z$ tiene polos simples en los números enteros con residuo 1, por lo que la función

$$\frac{\pi \cot \pi z}{z^s},$$

definida en el semiplano $\sigma > 0$ con la rama holomorfa del logaritmo que toma partes imaginarias en $]-\pi/2, \pi/2[$, tiene residuo $1/n^s$ en todos los números naturales no nulos. Fijamos un número real de la forma $x = k + 1/2$, donde $k \ge 1$ es un número natural, y consideramos el arco cerrado que indica la figura:



El arco C_r es por definición el arco de circunferencia de centro 0 y radio $r + 1/2$ que empieza y termina sobre la recta $\operatorname{Re} z = x$ y se encuentra a la derecha de ésta, recorrido en sentido horario. Por el teorema de los residuos

$$\frac{1}{2i} \int_{x-T_r i}^{x+T_r i} \frac{\cot \pi z}{z^s}\,dz + \frac{1}{2i} \int_{C_r} \frac{\cot \pi z}{z^s}\,dz = -\sum_{n=k+1}^{r} \frac{1}{n^s},$$

donde $x + T_r i$ es el extremo superior de C_r y el signo negativo final se debe a que arco está orientado en sentido negativo. De momento vamos a suponer que el exponente s cumple $\sigma > 1$, lo que garantiza la convergencia de la serie de la derecha cuando r tiende a ∞.

Ahora probamos que la integral sobre C_r tiende a 0 cuando r tiende a ∞. Para ello recordamos que en la prueba de [An 10.29] hemos visto que la función

$\cot \pi z$ está acotada (digamos por M) en el conjunto que resulta de eliminar en el plano complejo un disco de centro en cada número entero y radio menor que $1/2$. Como C_r no pasa por ninguno de tales discos, la cota vale para el integrando. Además,

$$|z^{-s}| = |e^{-s\log z}| = |e^{-(\sigma+\tau i)(\log|z|+i\arg z)}| = e^{-\sigma\log|z|+\tau\arg z} = |z|^{-\sigma}e^{\tau\arg z}.$$

Por lo tanto,

$$\left|\frac{1}{2i}\int_{C_r}\frac{\cot\pi z}{z^s}\,dz\right| \le \frac{\pi}{2}(r+1/2)M(r+1/2)^{-\sigma}e^{|\tau|\pi/2}$$

$$= \frac{\pi}{2}Me^{|\tau|\pi/2}(r+1/2)^{1-\sigma},$$

que ciertamente converge a 0 si $\sigma > 1$. Concluimos que

$$\zeta(s) - \sum_{n<x}\frac{1}{n^s} = -\frac{1}{2i}\int_{x-\infty i}^{x+\infty i}\frac{\cot\pi z}{z^s}\,dz.$$

Hemos probado que la integral existe como límite simultáneo de sus dos extremos de integración, pero el límite es también finito si sólo hacemos tender a infinito uno de los extremos, porque $|z^{-s}\cot\pi z| \le Me^{|\tau|\pi/2}|z|^{-\sigma}$, luego

$$\int_x^{x+Ti}\frac{\cot\pi z}{z^s}\,dz = \int_0^T\frac{i\cot\pi z}{z^s}\,dy$$

y el módulo del integrando está acotado por $cy^{-\sigma}$ (con c constante) que (siempre para $\sigma > 1$) es integrable en $[1,+\infty[$, luego la función es integrable en $[1,+\infty[$ y, por continuidad, también en $[0,+\infty[$. Por consiguiente podemos separar:

$$\zeta(s) - \sum_{n<x}\frac{1}{n^s} = -\frac{1}{2i}\int_{x-\infty i}^{x}\frac{\cot\pi z}{z^s}\,dz - \frac{1}{2i}\int_x^{x+\infty i}\frac{\cot\pi z}{z^s}\,dz.$$

Ahora observamos que

$$\int_{x-\infty i}^{x}\frac{1}{z^s}\,dz = \lim_{T\to+\infty}\int_{x-Ti}^{x}\frac{1}{z^s}\,dz = \lim_{T\to+\infty}\left[\frac{-1}{(s-1)z^{s-1}}\right]_{x-Ti}^{x} = -\frac{1}{(s-1)x^{s-1}},$$

e igualmente

$$\int_x^{x+\infty i}\frac{1}{z^s}\,dz = \frac{1}{(s-1)x^{s-1}}.$$

Por lo tanto,

$$\zeta(s) - \sum_{n<x}\frac{1}{n^s} - \frac{1}{(s-1)x^{s-1}} = -\frac{1}{2i}\int_{x-\infty i}^{x}\frac{\cot\pi z - i}{z^s}\,dz$$

$$-\frac{1}{2i}\int_x^{x+\infty i}\frac{\cot\pi z + i}{z^s}\,dz, \tag{4.3}$$

pues los términos $-i$ y $+i$ añadidos dentro de la integral equivalen a sumar las integrales precedentes multiplicadas por $1/2$ y $-1/2$, respectivamente. Vamos a ver que, con esta modificación, no sólo ha aparecido la modificación de la suma parcial que ya habíamos considerado en el teorema 4.1, sino que así las integrales convergen en el semiplano $\sigma > 0$.

En efecto, si suponemos que $\sigma > 0$ y $z = x + yi$ con $y < 0$, entonces

$$\cot \pi z - i = i\frac{e^{i\pi z} + e^{-i\pi z}}{e^{i\pi z} - e^{-i\pi z}} - i = \frac{2ie^{-i\pi z}}{e^{i\pi z} - e^{-i\pi z}} = \frac{2ie^{-2\pi zi}}{1 - e^{-2\pi zi}},$$

luego

$$|\cot \pi z - i| = \frac{2e^{2\pi y}}{|1 - e^{-2\pi zi}|} \le \frac{2e^{2\pi y}}{1 - e^{2\pi y}} = \frac{2}{e^{-2\pi y} - 1} \le 2e^{2\pi y}.$$

Similarmente, si $y > 0$ tenemos que $|\cot \pi z + i| \le 2e^{-2\pi y}$. Por otra parte,[1]

$$|z^{-s}| = |z|^{-\sigma} e^{\tau \arg z} \le x^{-\sigma} e^{|\tau||\arg z|} \le x^{-\sigma} e^{|\tau| \arctan(|y|/x)} \le x^{-\sigma} e^{|\tau||y|/x}.$$

En total, para $y < 0$,

$$\left|\frac{\cot \pi z - i}{z^s}\right| \le x^{-\sigma} e^{(2\pi - |\tau|/x)y}$$

y, teniendo en cuenta que, por hipótesis, $x > \frac{|\tau|}{2\pi}$, la función de la derecha es integrable en $]-\infty, 0]$. Más precisamente, si K es un compacto en el semiplano $\sigma > 0$, $|\tau| < 2\pi x$, existen δ_1, $\delta_2 > 0$ tales que todo $s \in K$ cumple $\sigma > \delta_1$, $|\tau| < 2\pi x - \delta_2$, luego

$$\left|\frac{\cot \pi z - i}{z^s}\right| \le x^{-\delta_1} e^{(\delta_2/x)y},$$

luego [IC 7.10] nos da que la integral

$$\int_{x-\infty i}^{x} \frac{\cot \pi z - i}{z^s}\, dz$$

define una función holomorfa en $\sigma > 0$, $|\tau| < 2\pi x$. Igualmente se razona con la segunda integral que aparece en (4.3), con lo que concluimos que los dos miembros de dicha ecuación son funciones holomorfas en el dominio indicado, luego la igualdad, que sabemos que se cumple para $\sigma > 1$, se cumple de hecho para $\sigma > 0$ (y $|\tau| < 2\pi x$). Más aún, si $T > 0$, tenemos que

$$\left|\frac{1}{2i}\int_{x-Ti}^{x} \frac{\cot \pi z - i}{z^s}\, dz\right| = \left|\frac{1}{2}\int_{-T}^{0} \frac{\cot \pi z - i}{z^s}\, dy\right|$$

$$\le x^{-\sigma} \int_{-T}^{0} e^{(2\pi - |\tau|/x)y}\, dy = \frac{x^{-\sigma}}{2\pi - |\tau|/x}(1 - e^{-(2\pi - |\tau|/x)T}),$$

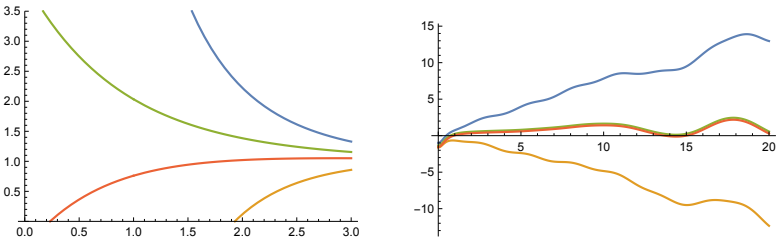
[1] Es fácil ver que, si $x \ge 0$, se cumple que $\arctan x \le x$. Basta tener en cuenta que la derivada de $x - \arctan x$ es no negativa.

luego

$$\left|\frac{1}{2i}\int_{x-\infty i}^{x}\frac{\cot\pi z - i}{z^s}\,dz\right| \le \frac{x^{-\sigma}}{2\pi - |\tau|/x}.$$

La segunda integral de (4.3) se acota análogamente y así llegamos a la fórmula del enunciado. ∎

Las gráficas siguientes muestran las acotaciones de la parte real de $\zeta(\sigma+6\pi i)$ con $k=3$ y $\zeta(1/2+\tau i)$ con $k=10$, respectivamente, que proporcionan (4.2) y el teorema anterior. En ambos casos, las más ajustadas son las correspondientes al teorema anterior.



Más adelante usaremos el hecho siguiente:

Ejemplo Vamos a comprobar que $\operatorname{Re}\zeta(\sigma+6\pi i)>0$ para $\sigma\ge 1/2$.

Esto se ve en la gráfica de la izquierda, pues la cota inferior que se muestra para $\zeta(\sigma+6\pi i)$ con $k=3$ esta por encima de 0 cuando $\sigma\ge 1/2$. Para comprobarlo sin apoyarnos en la gráfica conviene tomar $k=4$. Del teorema anterior se sigue inmediatamente que

$$\left|\zeta(\sigma+6\pi i)-\sum_{n=1}^{4}\frac{1}{n^{\sigma+6\pi i}}\right| \le \frac{1}{|\sigma-1+6\pi i|4.5^{\sigma-1}}+\frac{2\cdot 4.5^{-\sigma}}{2\pi-6\pi/4.5}$$

$$\le \frac{1}{6\pi 4.5^{-1/2}}+\frac{2\cdot 4.5^{-1/2}}{2\pi-6\pi/4.5}\approx 0.5627.$$

Por otra parte,

$$\operatorname{Re}\sum_{n=1}^{4}\frac{1}{n^{\sigma+6\pi i}} = 1+2^{-\sigma}\cos(6\pi\log 2)+3^{-\sigma}\cos(6\pi\log 3)+4^{-\sigma}\cos(6\pi\log 4)$$

$$= 1+0.877992\cdot 2^{-\sigma}-0.284037\cdot 3^{-\sigma}+0.541739\cdot 4^{-\sigma}$$

$$\ge 1-0.284037\cdot 3^{-1/2}\approx 0.836.$$

Por lo tanto,

$$\operatorname{Re}\zeta(\sigma+6\pi i)\ge 0.836-0.5627>0.$$

∎

4.2 El crecimiento de la función dseta

Muchas cuestiones en las que interviene la función dseta de Riemann dependen de estimaciones sobre su crecimiento en distintas regiones del plano complejo, especialmente en rectas verticales de la forma $\sigma = \sigma_0$. En esta sección obtendremos los resultados básicos a este respecto.

Crecimiento en el semiplano $\sigma > 1$ El comportamiento de la función dseta es más sencillo en el semiplano $\sigma > 1$, donde converge su desarrollo en serie de Dirichlet (y en producto de Euler). Para empezar, una mínima variante de la prueba de [ITAn 8.21] nos da que[2]

$$\lim_{\sigma\to+\infty} \zeta(s) = 1$$

uniformemente en τ.

En otras palabras, tomando σ_0 suficientemente grande podemos asegurar que en todo el semiplano $\sigma > \sigma_0$ la función $\zeta(s)$ se aproxime a 1 tanto como queramos. Podríamos decir que en los semiplanos $\sigma > \sigma_0$ con σ_0 grande es donde "menos interesante" es la función dseta.

En particular, $\zeta(s)$ está acotada en cualquier semiplano $\sigma > \sigma_0$, con $\sigma_0 > 1$. Más precisamente, un hecho elemental es que, para todo s en el semiplano $\sigma > 1$, se cumple que

$$|\zeta(s)| = \left|\sum_{n=1}^{\infty} \frac{1}{n^s}\right| \le \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma),$$

de modo que el supremo de $|\zeta(s)|$ sobre una recta $\sigma = \sigma_0$ es precisamente $\zeta(\sigma_0)$. Más aún, como $\zeta(\sigma)$ es claramente decreciente en $]1, +\infty[$, tenemos que $\zeta(\sigma_0)$ es de hecho el supremo de $|\zeta(s)|$ en todo el semiplano $\sigma > \sigma_0$.

A su vez, el comportamiento de $\zeta(\sigma)$ en la semirrecta $\sigma > 1$ está bien determinado por las desigualdades

$$\frac{1}{\sigma - 1} \le \zeta(\sigma) \le 1 + \frac{1}{\sigma - 1}. \tag{4.4}$$

(Véanse el razonamiento previo a [An 10.31]).

Es obvio que $\zeta(s)$ no está acotada en el semiplano $\sigma > 1$, pues tiende a ∞ en $s = 1$. Sin embargo, se cumple algo menos trivial, y es que sigue sin estar acotada aunque eliminemos del semiplano un entorno de 1. Más precisamente, sucede que $|\zeta(\sigma + \tau i)|$ no sólo tiende a $\zeta(\sigma)$ cuando τ tiende a 0, sino que también hay puntos en los que $|\zeta(\sigma + \tau i)|$ está arbitrariamente cerca de $\zeta(\sigma)$ con τ arbitrariamente grande. Para probarlo necesitamos un resultado elemental de aproximación diofántica:

[2] La acotación que se muestra en la prueba vale en realidad para todo s tal que $\sigma > c$.

Teorema 4.5 (Dirichlet) *Si $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$, $q > 0$ es un número natural y $t_0 > 0$, existen $m_1, \ldots, m_n \in \mathbb{Z}$ y $t_0 \le t \le t_0 q^n$ tales que $|t\alpha_k - m_k| < 1/q$, para todo $k = 1, \ldots, n$.*

DEMOSTRACIÓN: Consideramos los $q^n + 1$ puntos de $\mathbb{R}^n$ de la forma

$$(u\alpha_1, \ldots, u\alpha_n),$$

donde $u = 0, t_0, 2t_0, \ldots, q^n t_0$. Si los reducimos tomando las partes fraccionarias de sus componentes obtenemos $q^n + 1$ puntos del cubo $[0,1]^n$. Si dividimos este cubo en q^n cubos de arista $1/q$, al menos dos de las reducciones deben estar en el mismo cubo de la división. Pongamos que son los correspondientes a $u_1 < u_2$ y tomemos $t = u_2 - u_1 = mt_0$, con $1 \le m \le q^n$, luego $t_0 \le t \le t_0 q^n$. Entonces

$$|(u_2\alpha_k - E[u_2\alpha_k]) - (u_1\alpha_k - E[u_1\alpha_k])| < 1/q,$$

luego, llamando $m_k = E[u_2\alpha_k] - E[u_1\alpha_k]$, tenemos que $|t\alpha_k - m_k| < 1/q$. ∎

Teorema 4.6 *Si $\sigma > 1$ y $\epsilon > 0$, existen valores de τ arbitrariamente grandes tales que $|\zeta(\sigma + \tau i)| \ge \zeta(\sigma) - \epsilon$.*

DEMOSTRACIÓN: Tenemos que

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} e^{-i\tau \log n},$$

luego, dado un número natural $N > 0$,

$$|\zeta(s)| \ge \operatorname{Re}\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma}\cos(\tau \log n) \ge \sum_{n=1}^{N} \frac{1}{n^\sigma}\cos(\tau \log n) - \sum_{n=N+1}^{\infty} \frac{1}{n^\sigma}.$$

Fijados $t_0 > 0$ y $q \ge 4$, por el teorema anterior existen enteros $m_1, \ldots, m_N$ y $t_0 \le t \le t_0 q^N$ tales que

$$\left|\frac{t \log n}{2\pi} - m_n\right| \le 1/q, \qquad n = 1, \ldots, N.$$

Esto equivale a que

$$-\frac{\pi}{2} \le -\frac{2\pi}{q} \le t \log n - 2\pi m_n \le \frac{2\pi}{q} \le \frac{\pi}{2}$$

y las propiedades de la función coseno implican claramente que

$$\cos(t \log n) \ge \cos(2\pi/q).$$

Por lo tanto,

$$\sum_{n=1}^{N} \frac{1}{n^\sigma}\cos(t \log n) \ge \cos(2\pi/q) \sum_{n=1}^{N} \frac{1}{n^\sigma} > \cos(2\pi/q)\zeta(\sigma) - \sum_{n=N+1}^{\infty} \frac{1}{n^\sigma}.$$

Por consiguiente

$$|\zeta(\sigma+it)| \geq \cos(2\pi/q)\zeta(\sigma) - 2\sum_{n=N+1}^{\infty}\frac{1}{n^\sigma}.$$

Por otra parte,

$$\sum_{n=1}^{\infty}\frac{1}{n^\sigma} < \int_N^{+\infty}\frac{1}{u^\sigma}\,du = \frac{N^{1-\sigma}}{\sigma-1} < N^{1-\sigma}\zeta(\sigma).$$

Concluimos que

$$|\zeta(\sigma+it)| \geq (\cos(2\pi/q) - 2N^{1-\sigma})\zeta(\sigma),$$

Y siempre podemos tomar N y q suficientemente grandes como para que

$$\cos(2\pi/q) - 2N^{1-\sigma} \geq 1-\epsilon.$$

■

Así pues, ahora podemos asegurar que $\zeta(s)$ no está acotada, por ejemplo, sobre el cuadrante $\sigma > 1$, $\tau > 1$, pues el supremo de $|\zeta(s)|$ sobre cada semirrecta $\sigma = \sigma_0$ en dicho cuadrante sigue siendo $\zeta(\sigma_0)$, que tiende a $+\infty$ cuando σ_0 tiende a 1.

Esto nos plantea el problema opuesto, es decir, estimar el orden de crecimiento de $\zeta(s)$ en un cuadrante como $\sigma > 1$, $\tau \geq 2$ (la cota sobre τ es irrelevante, con tal de que excluya un entorno del polo de la función dseta). El teorema 4.1 nos da la solución:

Teorema 4.7 *En el cuadrante $\sigma \geq 1$, $\tau \geq 2$ se cumple que $\zeta(s) = O(\log\tau)$. Si $0 < \delta < 1$, en el cuadrante $\sigma \geq \delta$, $\tau \geq 1$ tenemos que $\zeta(s) = O(\tau^{1-\delta})$, donde la constante depende de δ.*

Demostración: La fórmula del teorema 4.1, para $\tau > 0$, usando que

$$|s-1| \geq \operatorname{Im}(s-1) = \tau,$$

se reduce a

$$\begin{aligned}|\zeta(s)| &\leq \sum_{n\leq x}\frac{1}{n^\sigma} + \frac{1}{\tau x^{\sigma-1}} + \frac{1}{x^\sigma} + |s|\int_x^{+\infty}\frac{dt}{t^{\sigma+1}}\\ &< \sum_{n\leq x}\frac{1}{n^\sigma} + \frac{1}{\tau x^{\sigma-1}} + \frac{1}{x^\sigma} + \frac{\sigma+\tau}{\sigma}\frac{1}{x^\sigma}.\end{aligned}$$

En particular, si $\sigma \geq 1$, $\tau \geq 1$, $x \geq 1$

$$|\zeta(s)| < \sum_{n\leq x}\frac{1}{n} + \frac{1}{\tau} + \frac{1}{x} + \frac{1+\tau}{x} \leq 4 + \int_1^x\frac{1}{t}\,dt + \frac{\tau}{x} = 4 + \log x + \frac{\tau}{x},$$

y haciendo $x = \tau \geq 2$ queda que $|\zeta(s)| < 5 + \log\tau = O(\log\tau)$.

Suponemos ahora que $\sigma \geq \delta$, $\tau \geq 1$, con lo que

$$|\zeta(s)| \leq \sum_{n\leq x} \frac{1}{n^\sigma} + \frac{1}{\tau x^{\delta-1}} + \left(2+\frac{\tau}{\delta}\right)\frac{1}{x^\delta} < \int_0^x \frac{1}{t^\delta}\,dt + \frac{x^{1-\delta}}{\tau} + \frac{3\tau}{\delta x^\delta}$$

$$\leq \frac{x^{1-\delta}}{1-\delta} + x^{1-\delta} + \frac{3\tau}{\delta x^\delta}.$$

En particular, para $x = \tau$, queda

$$|\zeta(s)| \leq \frac{\tau^{1-\delta}}{1-\delta} + \tau^{1-\delta} + \frac{3}{\delta}\tau^{1-\delta} = O(\tau^{1-\delta}),$$

donde la constante de O depende de δ. ∎

Crecimiento en el semiplano $\sigma < 0$ Los teoremas precedentes describen con detalle suficiente el crecimiento de la función dseta en el semiplano $\sigma > 1$. La situación es bastante distinta en el resto del plano complejo. Por ejemplo, hemos visto que $\zeta(s)$ está acotada sobre cada recta $\sigma = \sigma_0$ con $\sigma_0 > 1$, pero veremos que ya no lo está sobre las rectas con $\sigma_0 \leq 1$. De momento dejamos pendiente la prueba de este hecho y vamos a estudiar el crecimiento en las rectas con $\sigma_0 < 0$ aprovechando la ecuación funcional y lo que ya sabemos en el caso $\sigma_0 > 1$. El intervalo $0 \leq \sigma_0 \leq 1$ es mucho más difícil de tratar.

Recordemos que la ecuación funcional es $\zeta(s) = \chi(s)\zeta(1-s)$, donde

$$\chi(s) = \pi(2\pi)^{s-1}\frac{1}{\cos(\pi s/2)\Pi(s-1)}.$$

Vamos a estimar la función $\chi(s)$:

Teorema 4.8 *En cualquier conjunto de la forma $\sigma_1 \leq \sigma \leq \sigma_2$, $\tau \geq \delta$ se cumple*

$$\chi(s) = \left(\frac{2\pi}{\tau}\right)^{\sigma+i\tau-1/2} e^{i(\tau+\pi/4)}(1+O(1/\tau)).$$

En particular,

$$|\chi(s)| = \left(\frac{2\pi}{\tau}\right)^{\sigma-1/2}(1+O(1/\tau)).$$

Demostración: Ampliando el conjunto, no perdemos generalidad si suponemos que s varía en un conjunto de la forma $S = [1-c, 1+c]\times[\delta, +\infty[$ con $c \geq 1$. Entonces $s-1$ varía en $S = [-c, c]\times[\delta, +\infty[$. Vamos a aplicar la fórmula de Stirling [VC 4.30]:

$$\log\Pi(s) = \log\sqrt{2\pi} + (s+\frac{1}{2})\log s - s + \mu(s),$$

válida para todo s con argumento distinto de π. Podemos tomar un $\delta_0 > 0$ suficientemente pequeño para que todo $s \in S_0$ cumpla que $|\arg s| < \pi - \delta_0$, y así el teorema [VC 4.29] nos asegura que

$$|\mu(s)| \le \frac{1}{8\,\mathrm{sen}^2(\delta_0/2)|s|} \le \frac{1}{8\,\mathrm{sen}^2(\delta_0/2)\tau}.$$

Por consiguiente, para todo $s \in S$ tenemos que

$$\log \Pi(s-1) = \log\sqrt{2\pi} + (s-\frac{1}{2})\log(s-1) - s + 1 + O(1/\tau)$$

$$= \log\sqrt{2\pi} + (\sigma + i\tau - \frac{1}{2})\log(i\tau) - i\tau +$$

$$(\sigma + i\tau - \frac{1}{2})\log\frac{\sigma - 1 + i\tau}{i\tau} - (\sigma - 1) + O(1/\tau),$$

donde la constante implícita en O depende de c, pero no de σ. Ahora observamos que

$$(\sigma + i\tau - \frac{1}{2})\log\frac{\sigma - 1 + i\tau}{i\tau} - \sigma + 1 = (\sigma + i\tau - \frac{1}{2})\log\left(1 - i\frac{\sigma-1}{\tau}\right) - (\sigma - 1)$$

$$= (\sigma + i\tau - \frac{1}{2})\sum_{r=1}^{\infty}\frac{-1}{r}\left(\frac{i(\sigma-1)}{\tau}\right)^r - (\sigma-1) =$$

$$(\sigma - \frac{1}{2})\sum_{r=1}^{\infty}\frac{-(i\sigma-1)^r}{r}\tau^{-r} + i\tau\sum_{r=2}^{\infty}\frac{-1}{r}\left(\frac{i(\sigma-1)}{\tau}\right)^r =$$

$$(\sigma - \frac{1}{2})\sum_{r=1}^{\infty}\frac{-(i(\sigma-1))^r}{r}\tau^{-r} + \sum_{r=1}^{\infty}\frac{-i(i(\sigma-1))^{r+1}}{r+1}\tau^{-r} = O(1/\tau).$$

En efecto, observemos que las series provienen del desarrollo en serie de $\log(1+z)$, que, para $|\sigma - 1| \le c$, converge absolutamente para todo $\tau > c$, luego las series que hemos obtenido a partir de dicho desarrollo convergen también absolutamente. El módulo de la expresión anterior está acotado por

$$(c - \frac{1}{2})\sum_{r=1}^{\infty}\frac{c^r}{r}\tau^{-r} + \sum_{r=1}^{\infty}\frac{c^{r+1}}{r+1}\tau^{-r} =$$

$$\left((c - \frac{1}{2})\sum_{r=0}^{\infty}\frac{c^{r+1}}{r+1}\tau^{-r} + \sum_{r=0}^{\infty}\frac{c^{r+2}}{r+2}\tau^{-r}\right)\frac{1}{\tau}$$

pero τ^{-1} varía en $]0, 1/c[$ y podemos ver las dos series como series de potencias actuando sobre τ^{-1}, luego están acotadas en cualquier intervalo ligeramente menor, de modo que la expresión anterior está acotada por A/τ, para todo $\tau > c+1$, por ejemplo, y usando que la expresión inicial tiene que estar acotada en el compacto $[1-c, 1+c] \times [\delta, c+1]$, podemos aumentar la constante para que valga en todo el conjunto S.

Teniendo en cuenta que $\log(i\tau) = \log\tau + i\pi/2$, resulta que[3]

$$\Pi(s-1) = \sqrt{2\pi}\,\tau^{\sigma+i\tau-1/2}e^{i\frac{\pi}{2}(\sigma-\frac{1}{2})-\frac{\pi}{2}\tau-i\tau}(1+O(1/\tau)),$$

pues si $f(s) = O(1/\tau)$, entonces, como antes,

$$|e^{f(s)}-1| = \left|\sum_{n=1}^{\infty}\frac{f(s)^n}{n!}\right| \le \sum_{n=1}^{\infty}\frac{|f(s)|^n}{n!} \le \sum_{n=1}^{\infty}\frac{A^n}{n!}\tau^{-n} = O(1/\tau).$$

Por otra parte,

$$\frac{1}{\cos(\pi s/2)} = \frac{2}{e^{i\pi(\sigma+i\tau)/2}+e^{-i\pi(\sigma+i\tau)/2}} = \frac{2}{e^{i\sigma\pi/2-\pi\tau/2}+e^{-i\pi\sigma/2+\pi\tau/2}}$$

$$= \frac{2e^{i\pi\sigma/2-\pi\tau/2}}{e^{i\pi\sigma-\pi\tau}+1} = 2e^{i\pi\sigma/2-\pi\tau/2}(1+O(1/\tau)),$$

pues

$$\tau\left|\frac{1}{e^{i\pi\sigma-\pi\tau}+1}-1\right| = \frac{\tau e^{-\pi\tau}}{|e^{i\pi\sigma-\pi\tau}+1|} \to \frac{0}{1} = 0.$$

Notemos que el denominador admite una cota inferior independiente de σ, por lo que la constante en $O(1/\tau)$ es independiente de σ. En total,

$$\chi(s) = \pi(2\pi)^{s-1}\sqrt{2\pi}\tau^{\sigma+i\tau-1/2}e^{i\frac{\pi}{2}(\sigma-\frac{1}{2})-\frac{\pi}{2}\tau-i\tau}2e^{i\pi\sigma/2-\pi\tau/2}(1+O(1/\tau))$$

$$= \left(\frac{2\pi}{\tau}\right)^{\sigma+i\tau-1/2}e^{i(\tau+\pi/4)}(1+O(1/\tau)).$$

■

En particular, si $\sigma \le -\delta < 0$, tenemos que

$$|\zeta(s)| \le |\chi(s)|\zeta(1-\sigma) = (2\pi)^{\sigma-1/2}\tau^{1/2-\sigma}\zeta(1-\sigma)(1+O(1/\tau))$$

$$\le (2\pi)^{-\delta-1/2}\zeta(1+\delta)\tau^{1/2-\sigma}O(1) = O(\tau^{\frac{1}{2}-\sigma}).$$

Notemos además que el exponente no se puede mejorar, pues si $0 < \epsilon < 1$,

$$\left|\frac{\zeta(s)}{\tau^{\frac{1}{2}-\sigma-\epsilon}}\right| = (2\pi)^{\sigma-1/2}\tau^{\epsilon}(1+O(1/\tau)) = (2\pi)^{\sigma-1/2}(\tau^{\epsilon}+O(\tau^{-(1-\epsilon)})),$$

y esta expresión tiende a $+\infty$ con τ.

[3]En los cálculos precedentes hemos usado que $\log(z_1/z_2) = \log z_1 - \log z_2$. En principio, esto no tiene por qué ser correcto con la misma determinación holomorfa del logaritmo en ambos miembros, sino que podría hacer falta añadir un término $2k(z_1,z_2)\pi i$, pero como ahora aplicamos la exponencial, dicho término desaparecería.

Crecimiento en $[0,1]$ Para analizar el crecimiento de la función dseta en la banda crítica y su frontera conviene dar una definición:

Definición 4.9 Para cada $\sigma \in \mathbb{R}$ definimos la *función de Lindelöf* como

$$\mu(\sigma) = \text{ínf}\{c \in \mathbb{R} \mid \zeta(\sigma + i\tau) = O(|\tau|^c)\}.$$

Hay que entender que O hace referencia al orden de crecimiento cuando $|\tau| \to +\infty$, luego no perdemos generalidad si suponemos $|\tau| > 1$ (para evitar el polo cuando $\sigma = 1$). Además, como $|\zeta(\sigma - i\tau)| = |\overline{\zeta(\sigma + i\tau)}| = |\zeta(\sigma + i\tau)|$, podemos limitarnos a considerar $\tau > 1$.

Si $\sigma > 1$, sabemos que $\zeta(\sigma+\tau i)$ está acotada, es decir, que $\zeta(\sigma+\tau i) = O(1)$, luego $\mu(\sigma) \le 0$. Por otra parte (y aquí μ es la función de Möbius),

$$\frac{1}{|\zeta(\sigma + i\tau)|} = \left|\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\sigma+i\tau}}\right| \le \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma) > 0,$$

luego $|\zeta(\sigma + i\tau)| \ge 1/\zeta(\sigma) > 0$, lo que prueba que $\mu(\sigma) = 0$ (y el ínfimo de la definición de μ es realmente un mínimo, en el sentido de que se cumple $\zeta(\sigma + \tau i) = O(\tau^{\mu(\sigma)})$).

Los últimos resultados del apartado precedente implican que, para $\sigma < 0$, se cumple que $\mu(\sigma) = 1/2 - \sigma$, y de nuevo el ínfimo de la definición es un mínimo en este caso.

El teorema 4.7 nos asegura que μ está definida en el intervalo $]0,1]$ y nos da la estimación $\mu(\sigma) \le 1 - \sigma$. Veremos que se puede mejorar, pero antes tenemos un problema más básico, y es que no tenemos ninguna estimación de $\zeta(i\tau)$ que justifique la existencia (o la finitud) de $\mu(0)$. Esto se sigue de la ecuación funcional junto con la estimación del teorema 4.8 y la finitud de $\mu(1)$, pero podemos probar algo más general:

Por 4.7 sabemos que $\zeta(s) = O(\tau^{1/2})$ en el semiplano $\sigma \ge 1/2$. Por lo tanto, si $\sigma_0 \le \sigma \le 1/2$, tenemos que $1 - \sigma \ge 1/2$ y, si además $\tau > 2\pi$,

$$|\zeta(s)| = |\chi(s)||\zeta(1 - s)| = \left(\frac{2\pi}{\tau}\right)^{\sigma-1/2} (1 + O(1/\tau))O(\tau^{1/2})$$

$$\le (2\pi)^{\sigma_0-1/2}\tau^{1/2-\sigma_0}O(\tau^{1/2}) = O(\tau^{1-\sigma_0}).$$

En particular vemos que la estimación $\mu(\sigma) \le 1 - \sigma$ es válida también para $\sigma = 0$ (de hecho, hemos probado que vale para todo $\sigma \le 1/2$ y ya sabíamos que valía para $0 < \sigma \le 1$), pero, como hemos señalado, vamos a mejorarla. La clave es el teorema siguiente:

Teorema 4.10 (Lindelöf) *Sea $f(s)$ una función holomorfa en un entorno de una semibanda $S = [\sigma_1, \sigma_2] \times [\tau_0, +\infty[$. Si en S se cumple que $f(s) = O(\tau^c)$, $f(\sigma_1 + i\tau) = O(\tau^{c_1})$ y $f(\sigma_2 + i\tau) = O(\tau^{c_2})$, entonces,*

$$f((1 - \lambda)\sigma_1 + \lambda\sigma_2 + i\tau) = O(\tau^{(1-\lambda)c_1+\lambda c_2}).$$

DEMOSTRACIÓN: Por [VC 3.30] sabemos que $\log|f(s)|$ es una función harmónica donde f no se anula (y tiende a $-\infty$ en los ceros de f). También lo es $k(\sigma)\tau$, donde

$$k(\sigma) = \frac{\sigma_2 - \sigma}{\sigma_2 - \sigma_1}c_1 + \frac{\sigma - \sigma_1}{\sigma_2 - \sigma_1}c_2,$$

(pues $k(\sigma)\tau = a\sigma\tau + b\tau$), luego, dado $\epsilon > 0$, también lo es

$$g(s) = \log|f(s)| - k(\sigma)\log\tau - \epsilon\tau.$$

Por hipótesis $|f(\sigma_1 + i\tau)| \leq A_1\tau^{c_1}$, luego

$$g(\sigma_1 + i\tau) \leq \log A_1 - 2c_1\log\tau - \epsilon\tau = \log A_1 - \tau(\frac{2c_1\log\tau}{\tau} + \epsilon),$$

y el miembro derecho tiende a $-\infty$ cuando τ tiende a $+\infty$.

Así pues, $g(s)$ está acotada sobre la semirrecta $\{\sigma_1\} \times [\tau_0, +\infty[$, y lo mismo sucede con la semirrecta $\{\sigma_2\} \times [\tau_0, +\infty[$. Sea M una cota común que sea también una cota superior de $\log|f(s)|$ en el intervalo $[\sigma_1, \sigma_2] \times \{\tau_0\}$, con lo que también lo es de g.

Por otra parte,

$$g(\sigma + i\tau) \leq \log A - \epsilon\tau + c\log\tau - k(\sigma)\log\tau \leq \log A - \epsilon\tau + (c - k_0)\log\tau$$

$$= \log A - \tau(\frac{(c - k_0)\log\tau}{\tau} + \epsilon),$$

donde k_0 es el mínimo de $k(\sigma)$ en el intervalo $[\sigma_1, \sigma_2]$, y nuevamente el miembro derecho tiende a $-\infty$, uniformemente en σ, luego podemos encontrar un $T > \tau_0$ tal que si $\operatorname{Im} s = T$ se cumple que $g(s) \leq M$ en el segmento $[\sigma_1, \sigma_2] \times \{T\}$.

Así, la función g está acotada por M en toda la frontera del rectángulo $[\sigma_1, \sigma_2] \times [\tau_0, T]$, luego por el principio del máximo [An 8.17] (aplicado al rectángulo menos un disco alrededor de cada cero de f en el que g tome valores menores que M) concluimos que $g(s) \leq M$ en todo el rectángulo y, como T es arbitrariamente grande, de hecho esto vale para toda la semi banda S. En particular,

$$g(\sigma + i\tau) = \log|f(\sigma + i\tau)| - k(\sigma)\log\tau - \epsilon\tau \leq M,$$

luego

$$|f(\sigma + i\tau)| \leq M\tau^{k(\sigma)}e^{\epsilon\tau},$$

y, como M no depende de ϵ, concluimos que $|f(\sigma+i\tau)| \leq M\tau^{k(\sigma)}$. Esto es lo que había que probar, pues si $\sigma = (1-\lambda)\sigma_1 + \lambda\sigma_2$, entonces $k(\sigma) = (1-\lambda)c_1 + \lambda c_2$. ∎

Como consecuencia:

Teorema 4.11 *La función $\mu : \mathbb{R} \longrightarrow \mathbb{R}$ es convexa.*

DEMOSTRACIÓN: Dados $\sigma_1 < \sigma_2$, la función $\zeta(s)$ cumple las hipótesis del teorema anterior con $\tau_0 = 1$, luego, dado $\epsilon > 0$, como $f(\sigma_j + \tau i) = O(\tau^{\mu(\sigma_j)+\epsilon})$, concluimos que

$$\mu((1-\lambda)\sigma_1+\lambda\sigma_2) \le (1-\lambda)(\mu(\sigma_1)+\epsilon)+\lambda(\mu(\sigma_2)+\epsilon) = (1-\lambda)\mu(\sigma_1)+\lambda\mu(\sigma_2)+\epsilon.$$

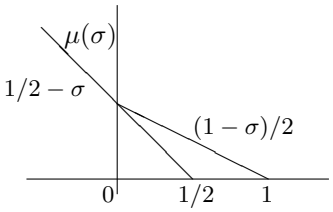
Como esto es cierto para todo $\epsilon > 0$, de hecho

$$\mu((1-\lambda)\sigma_1 + \lambda\sigma_2) \le (1-\lambda)\mu(\sigma_1) + \lambda\mu(\sigma_2).$$

■

Por [IC 1.20] sabemos que toda función convexa es continua, luego tenemos que la función de Lindelöf es continua. Más aún, por [IC 1.19] sabemos que μ está por encima de su recta tangente en cualquier punto donde sea derivable.

En resumen, ahora podemos afirmar que la gráfica de $\mu(\sigma)$ es como indica la figura. Cuando $\sigma \le 0$ se cumple que $\mu(\sigma) = 1/2 - \sigma$ (lo hemos probado para $\sigma < 0$, pero por continuidad también tiene que valer para $\sigma = 0$).



Para $\sigma \ge 1$ es $\mu(\sigma) = 0$ (y de nuevo el caso de $\sigma = 1$ lo deducimos por continuidad).

En la banda crítica $0 < \sigma < 1$ no sabemos cuánto vale exactamente $\mu(\sigma)$, pero por la definición de convexidad el valor tiene que estar por debajo del segmento que une los puntos $(0, \mu(0))$ y $(1, \mu(1))$, luego $\mu(\sigma) \le (1-\sigma)/2$, y por otra parte $\mu(\sigma)$ debe estar por encima de las prolongaciones de las rectas (tangentes) $y = 1/2 - \sigma$ e $y = 0$. En otras palabras, la gráfica de $\mu(\sigma)$ debe estar en el triángulo que muestra la figura.

En particular, tenemos, por ejemplo, que $0 \le \mu(1/2) \le 1/4$. En 6.9 probaremos que la cota $1/4$ puede ser mejorada.

Hemos visto que, para $\sigma > 1$, se cumple que $\mu(\sigma) = 0$ porque $\zeta(\sigma + \tau i)$ está acotada. En cambio, del hecho de que $\mu(1) = 0$ no podemos deducir que la función $\zeta(1 + \tau i)$ esté acotada. De hecho, no lo está:

Teorema 4.12 *Para cada $\sigma \le 1$ fijo, la función $\zeta(\sigma + \tau i)$ no está acotada.*

DEMOSTRACIÓN: Esto es inmediato si $\sigma \le 0$, pues entonces $\mu(\sigma) \ge 1/2$, luego $\zeta(\sigma+\tau i) \ne O(\tau^{1/4})$, lo que implica que la función no puede estar acotada. Supongamos, pues, que $0 < \sigma_0 \le 1$. Si $\zeta(s)$ estuviera acotada sobre $\sigma = \sigma_0$, como también lo está sobre la recta $\sigma = 2$, podemos aplicar el teorema 4.10 a la banda $\sigma_0 \le \sigma \le 2$, $\tau \ge 1$, en la cual tenemos la estimación $\zeta(s) = O(\tau^{1-\sigma_0})$ (justo antes de 4.10 hemos probado que es válida para $\sigma_0 \le \sigma \le 1/2$ —si es que $\sigma_0 < 1/2$—, pero para $1/2 \le \sigma \le 2$ el teorema 4.7 nos da que $\zeta(s) = O(\tau^{1/2})$, luego también $\zeta(s) = O(\tau^{1-\sigma_0})$). Como $\zeta(s) = O(1)$ en las dos rectas que limitan la banda, el teorema de Lindelöf nos asegura que $\zeta(s)$ está acotada en toda la banda, y en particular lo está para $1 < \sigma < 2$, $\tau \ge 1$, en contradicción con el teorema 4.6 (véase la observación posterior). ■

4.3 La función xi

Recordemos (sección [An 10.6]) que la función xi es la dada por

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

Se trata de una modificación de la función dseta que resulta ser entera y además satisface una ecuación funcional mucho más simple $\xi(s) = \xi(1-s)$. Esto la convierte en una herramienta muy útil para estudiar la función dseta. Empezamos calculando su orden de crecimiento:

Teorema 4.13 *Si $|s|$ es suficientemente grande, $|\xi(s)| \le e^{c|s|\log|s|}$.*

DEMOSTRACIÓN: Por la ecuación funcional podemos suponer que $\sigma \ge 1/2$.

$$|\log(\pi^{-s/2}(s-1))| \le \frac{|s|}{2}\log\pi + |\log(s-1)| = O(|s|\log|s|),$$

pues

$$\frac{|\log(s-1)|}{\log|s|} = \frac{\sqrt{\log^2|s| + \arg^2 s}}{\log|s|} = \sqrt{1 + \frac{\arg^2 s}{\log^2|s|}},$$

y el argumento está acotado. Por la fórmula de Stirling [VC 4.30],

$$\log\Pi(s/2) = \log\sqrt{2\pi} + \left(\frac{s+1}{2}\right)\log\frac{s}{2} - \frac{s}{2} + \mu(s/2) = O(|s|\log|s|),$$

pues

$$\frac{|s+1|}{2|s|}\frac{|\log(s/2)|}{\log|s|} \le \left(\frac{1}{2} + \frac{1}{|s|}\right)\frac{|\log|s| - \log 2 + i\arg(s/2)|}{\log|s|}$$

está claramente acotado y, por otra parte, por [VC 4.29], $\mu(s/2) = O(|s|^{-1})$. Por último, por el teorema 4.7 tenemos que

$$|\zeta(s)| \le c\tau^{1/2} = e^{c+\frac{1}{2}\log|s|} = O(|s|\log|s|).$$

■

Nota Observemos que el término $\log|s|$ no puede eliminarse en la estimación del teorema anterior, es decir, que no es cierto que existan constantes tales que $|\xi(s)| \le c_1 e^{c_2|s|}$. Esto implicaría que $\log|\xi(s)| = O(|s|)$, pero basta considerar los valores que toma ξ sobre la recta real:

$$\log|\xi(s)| = -\frac{s}{2}\log\pi + \log\Pi(s/2) + \log(s-1) + \log\zeta(s) =$$

$$-\frac{s}{2}\log\pi + \log\sqrt{2\pi} + \frac{s+1}{2}\log\frac{s}{2} - \frac{s}{2} + \mu(s/2) + \log(s-1) + \log\zeta(s) =$$

$$\log\sqrt{2\pi} + \frac{s}{2}\log\frac{s}{2\pi} + \frac{1}{2}\log\frac{s}{2} + \mu(s/2) + \log(s-1) + \log\zeta(s) =$$

$$\frac{s}{2}\log\frac{s}{2\pi} + o(s),$$

donde hemos usado que $\mu(s/2) = O(1/s)$ y que

$$\lim_{s\to+\infty} \zeta(s) = 1.$$

Por lo tanto, $\log|\xi(s)|/s$ no está acotado. ∎

Por consiguiente:

Teorema 4.14 *La función $\xi(s)$ tiene orden 1, en el sentido de* [VC 4.11].

DEMOSTRACIÓN: Si $M_\xi(r) = \sup_{|s|=r} |\xi(s)|$, para todo $\epsilon > 0$ se cumple que

$$M_\xi(r) \le e^{cr\log r} < e^{cr^{1+\epsilon}},$$

donde en el último paso hay que aumentar la constante c. Por lo tanto, el orden de ξ es ≤ 1. Si fuera menor que 1, existiría una constante tal que $M_\xi(r) \le e^{cr}$, en contra de la nota precedente. ∎

El teorema de Hadamard [VC 4.19] nos da entonces que existen constantes A y B tales que

$$\xi(s) = e^{A+Bs} \prod_{n=0}^{\infty} \left(1 - \frac{s}{\rho_n}\right) e^{s/\rho_n}, \tag{4.5}$$

donde $\{\rho_n\}_{n=0}^{\infty}$ es una enumeración de los ceros de $\xi(s)$ repetidos según su multiplicidad y ordenados de modo que su módulo sea creciente, donde en principio no excluimos que la función xi tenga un número finito de ceros o incluso que no tenga ninguno, en cuyo caso el producto será finito o vacío (en cuyo caso hay que entender que vale 1). Sin embargo, ahora podemos probar que de hecho $\xi(s)$ tiene infinitos ceros. Más aún:

Teorema 4.15 *La función $\xi(s)$ tiene infinitos ceros y, si $\{\rho_n\}_{n=0}^{\infty}$ es una enumeración en la que cada uno se repite tantas veces como indica su multiplicidad y de modo que la sucesión de los módulos sea creciente, entonces la serie*

$$\sum_{n=0}^{\infty} \frac{1}{|\rho_n|^\lambda}$$

converge si y sólo si $\lambda > 1$.

DEMOSTRACIÓN: Supongamos que el número de ceros fuera finito o que convergiera la serie

$$\sum_{n=0}^{\infty} \frac{1}{|\rho_n|} = \alpha.$$

(En el primer caso llamamos α a la suma de la serie finita.) Claramente existe una constante c tal que

$$|(1-z)e^z| \le (1+|z|)e^{|z|} = e^{|z|+\log(1+|z|)} \le e^{c|z|},$$

luego

$$\left|\left(1-\frac{s}{\rho_n}\right)e^{s/\rho_n}\right| \le e^{c|s|/|\rho_n|}.$$

Por consiguiente,

$$\left|\prod_{n=0}^{\infty}\left(1-\frac{s}{\rho_n}\right)e^{s/\rho_n}\right| \le e^{c\alpha|s|},$$

y también es claro que $e^{A+Bs} \le e^{c|s|}$, luego en total tendríamos que $|\xi(s)| \le e^{c|s|}$, en contradicción con la nota posterior al teorema 4.13.

Así pues, el número de ceros es infinito y la serie de los inversos de sus módulos diverge. La convergencia de las series con exponentes $\lambda > 1$ es consecuencia directa del teorema [VC 4.17], según el cual el exponente de convergencia de la sucesión de los ceros tiene que ser ≤ 1 (y el argumento precedente prueba que de hecho es exactamente 1). ∎

Así pues, hemos probado que la función dseta de Riemann tiene infinitos ceros no triviales.

Nota En lo sucesivo entenderemos que la variable ρ como índice de una suma o producto recorre los ceros de la función ξ repetidos tantas veces como indica su multiplicidad y ordenados de modo que la sucesión de sus módulos sea creciente.

∎

Pasamos ahora a calcular las constantes A y B de (4.5):

Teorema 4.16 *Se cumple que*

$$\xi(s) = \frac{1}{2}(4\pi)^{s/2}e^{-(\gamma/2+1)s}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{s/\rho}.$$

Demostración: Como $\xi(0) = 1/2$, evaluando (4.5) en $s = 0$ obtenemos que $e^A = 1/2$, luego

$$\xi(s) = \frac{1}{2}e^{Bs}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{s/\rho}.$$

Para calcular B consideramos la derivada logarítmica:

$$\frac{\xi'(s)}{\xi(s)} = B + \sum_{\rho}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right). \tag{4.6}$$

Por otra parte, de la definición de la función xi obtenemos que

$$\frac{\xi'(s)}{\xi(s)} = -\frac{1}{2}\log\pi + \frac{1}{2}\frac{\Pi'(s/2)}{\Pi(s/2)} + \frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)}$$

La ecuación funcional implica que $\xi'(s) = -\xi'(1-s)$, luego

$$B = \frac{\xi'(0)}{\xi(0)} = -\frac{\xi'(1)}{\xi(1)} = \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Pi'(1/2)}{\Pi(1/2)} - \lim_{s\to 1}\left(\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}\right).$$

La factorización de Π dada en [ITAn 8.16] implica que

$$-\frac{\Pi'(z)}{\Pi(z)} = \gamma + \sum_{k=1}^{\infty}\left(\frac{1}{k+z} - \frac{1}{k}\right),$$

luego

$$-\frac{1}{2}\frac{\Pi'(1/2)}{\Pi(1/2)} = \frac{\gamma}{2} + \sum_{k=1}^{\infty}\left(\frac{1}{2k+1} - \frac{1}{2k}\right) = \frac{\gamma}{2} + \log 2 - 1,$$

por la expresión para $\log 2$ que se sigue de la serie de Taylor del logaritmo.[4]

Por otra parte, según 4.3 tenemos que $\zeta(s) = \frac{1}{s-1} + \gamma + g(s)$, con $g(1) = 0$, luego $\zeta'(s) = -\frac{1}{(s-1)^2} + g'(s)$, luego

$$\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s+1} = \frac{(s-1)\zeta'(s) + \zeta(s)}{(s-1)\zeta(s)} = \frac{(s-1)g'(s) + \gamma + g(s)}{(s-1)\zeta(s)},$$

luego

$$\lim_{s\to 1}\left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s+1}\right) = \gamma.$$

En total

$$B = \log\sqrt{\pi} + \frac{\gamma}{2} + \log 2 - 1 - \gamma = \log\sqrt{4\pi} - \frac{\gamma}{2} - 1,$$

lo que nos da la fórmula del enunciado. ∎

La derivada en 0 de la función dseta La prueba del teorema precedente nos permite calcular $\zeta'(0)$. En efecto, tenemos que

$$\frac{\zeta'(0)}{\zeta(0)} = 1 + \log\sqrt{\pi} - \frac{1}{2}\frac{\Pi'(0)}{\Pi(0)} + B$$

$$= 1 + \log\sqrt{\pi} + \frac{\gamma}{2} + \log 2\sqrt{\pi} - \frac{\gamma}{2} - 1 = \log 2\pi,$$

luego $\zeta'(0) = -\frac{1}{2}\log 2\pi$. ∎

Otra consecuencia:

Teorema 4.17 *Si ρ es un cero de la función $\xi(s)$, entonces $|\operatorname{Im}\rho| \geq 6.5$.*

Demostración: Hacemos $s = 1$ en (4.6), con lo que

$$-B = B + \sum_{\rho}\left(\frac{1}{1-\rho} + \frac{1}{\rho}\right).$$

La serie no es absolutamente convergente, por lo que no podemos reordenarla de cualquier forma, pero sabemos que la igualdad es cierta con cualquier ordenación

[4] Véase, por ejemplo [ITAn 4.15].

de los ceros de la función ξ que haga monótona creciente a la sucesión de los módulos. En particular, podemos exigir que cada cero que cumpla $\operatorname{Im}\rho > 0$ vaya seguido de $\bar{\rho}$. Entonces tenemos también que

$$\sum_{\operatorname{Im}\rho>0}\left(\frac{1}{1-\rho}+\frac{1}{\rho}+\frac{1}{1-\bar{\rho}}+\frac{1}{\bar{\rho}}\right)=-2B,$$

pues las sumas parciales de esta serie son la subsucesión formada por los términos pares de la serie anterior. Ahora bien,

$$\frac{1}{\rho}+\frac{1}{\bar{\rho}}=\frac{\rho+\bar{\rho}}{|\rho|^2}=\frac{2\operatorname{Re}\rho}{|\rho|^2}\le\frac{2}{|\rho|^2},$$

y la última serie es convergente. Lo mismo vale para los sumandos con $1-\rho$ y $1-\bar{\rho}$, luego podemos descomponer la serie en suma de dos series de términos positivos:

$$\sum_{\operatorname{Im}\rho>0}\frac{2\operatorname{Re}(1-\rho)}{|1-\rho|^2}+\sum_{\operatorname{Im}\rho>0}\frac{2\operatorname{Re}\rho}{|\rho|^2}=-2B.$$

La convergencia absoluta nos permite reordenar sus términos, y la conclusión es que ambas series son la misma, ya que, por la ecuación funcional, cuando ρ recorre los ceros de $\xi(s)$, también lo hace $1-\rho$. Así pues,

$$\sum_{\operatorname{Im}\rho>0}\frac{2\operatorname{Re}\rho}{|\rho|^2}=-B=1+\frac{\gamma}{2}-\log\sqrt{4\pi}\approx 0.023.$$

Si $\operatorname{Re}\rho\ge 1/2$ tenemos que

$$0.023\ge\frac{2\operatorname{Re}\rho}{|\rho|^2}\ge\frac{1}{1+\operatorname{Im}^2\rho},$$

de donde $\operatorname{Im}\rho\ge 6.5$. ∎

La función Xi Definimos la función Xi como $\Xi(t)=\xi(1/2+it)$. Claramente se trata de una función entera, y su interés reside en que, como vamos a ver enseguida, es real sobre los números reales.

En efecto, la función $f(s)=\xi(1/2+s)$ es real sobre los números reales (porque ξ cumple esto mismo), luego los coeficientes de su serie de Taylor alrededor de 0 son reales. La ecuación funcional implica que $f(s)=f(-s)$, luego sus coeficientes de orden impar son nulos. En definitiva:

$$\xi(1/2+s)=\sum_{n=0}^{\infty}a_{2n}s^{2n},$$

donde los coeficientes a_{2n} son números reales. Por lo tanto

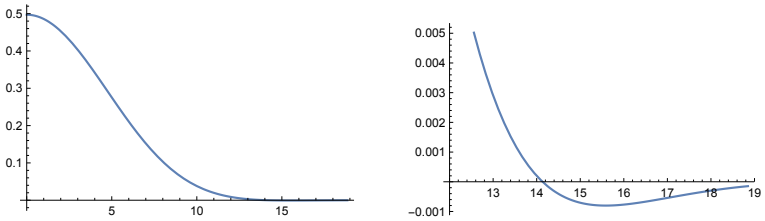
$$\xi(s)=\sum_{n=0}^{\infty}a_{2n}(s-1/2)^{2n},$$

y a su vez

$$\Xi(t) = \xi(1/2+it) = \sum_{n=0}^{\infty} a_{2n}(it)^{2n} = \sum_{n=0}^{\infty}(-1)^n a_{2n} t^{2n},$$

lo que prueba que, tal y como habíamos afirmado, $\Xi(t)$ es real cuando $t \in \mathbb{R}$. Además $\Xi(t) = \Xi(-t)$.

Observemos que los ceros reales de $\Xi(t)$ son las partes imaginarias de los ceros de $\xi(s)$ sobre la recta crítica $\sigma = 1/2$. He aquí la gráfica de $\Xi(t)$ y una ampliación en la que se ve claramente que ξ tiene un cero con parte real $\sigma = 1/2$ y parte imaginaria $14 < \tau < 15$.



Observemos que estas gráficas muestran "más claramente" la existencia de un cero no trivial que las de la página 103. En ellas "se veía" que la curva $\zeta(1/2+it)$ pasaba "más o menos" por el 0 o que las funciones $\operatorname{Re}\zeta(1/2+it)$ e $\operatorname{Im}\zeta(1/2+it)$ se anulaban "más o menos" en el mismo punto, pero nada en las figuras nos permitía garantizar que la curva pasaba exactamente por 0 y no por un punto muy próximo a 0, ni que los puntos donde se anulaban las partes real e imaginaria no eran dos puntos muy parecidos, pero no el mismo. En cambio, ahora "vemos" una función real de variable real que es continua y pasa de tomar valores positivos a tomar valores negativos, lo que nos asegura que pasa por 0.

Más aún, aunque existen medios mucho más eficientes, hemos visto cómo aproximar la función $\zeta(s)$ con cualquier precisión deseada y lo mismo puede hacerse con la función factorial y, por supuesto, con las funciones elementales (como hace cualquier calculadora de bolsillo), luego se puede calcular $\Xi(14)$ y $\Xi(15)$ acotando el error para asegurar que $\Xi(14) > 0$ y $\Xi(15) < 0$, y eso prueba —sin el apoyo de ninguna gráfica— que la función Xi tiene un cero entre ambos valores.

De hecho, usando técnicas potentes de cálculo numérico (las mismas que permiten calcular las gráficas de Xi que hemos mostrado[5]) podemos acotar la posición de este cero tanto como queramos. El resultado es

$$\rho_1 = 0.5 + 14.1347251417\ldots i$$

En la sección siguiente probaremos que es el primer cero no trivial de la función dseta, en el sentido de que no hay ningún otro con menor parte imaginaria positiva.

[5]En realidad para estos cálculos no se suele emplear la función Xi, sino la llamada función Z de Riemann-Siegel, pero no vamos a entrar en cuestiones computacionales. Tan sólo queremos mostrar cómo es posible probar con rigor que existen ceros no triviales de la función dseta sobre la recta $\sigma = 1/2$, sin entrar en la cuestión de cuál es la forma más práctica de hacer las comprobaciones.

4.4 La fórmula de Riemann-von Mangoldt

En esta sección daremos una prueba alternativa de la existencia de ceros no triviales de la función dseta obteniendo una estimación de su densidad:

Definición 4.18 Para cada $T > 0$, llamaremos $N(T)$ al número de ceros no triviales de la función dseta de Riemann contenidos en $[0,1] \times [0,T]$ contados tantas veces como indica su multiplicidad, que, según ya hemos observado en la introducción a este capítulo, coincide con el número de ceros en $[0,1] \times [-T,0]$.

Como norma general, siempre que contemos ceros no triviales de $\zeta(s)$ en cualquier contexto se sobrentenderá que los contamos con sus multiplicidades, es decir, que un cero doble se cuenta como dos ceros. Nos proponemos demostrar el teorema siguiente:

Teorema 4.19 (Fórmula de Riemann-von Mangoldt) *Si $N(T)$ es el número de ceros no triviales de la función dseta (contados según su multiplicidad) con $0 < \tau \le T$, entonces*

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T).$$

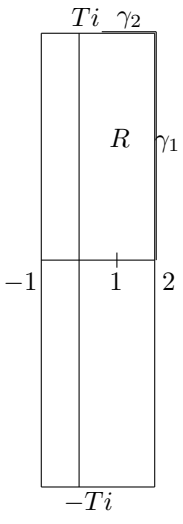
De aquí se desprende que los ceros no triviales son infinitos. Más aún, la densidad del número de ceros en cada rectángulo de la banda crítica cumple

$$\lim_{T\to+\infty} \frac{N(T)}{T} = +\infty,$$

pues

$$\frac{N(T)}{T} = \frac{1}{2\pi}\log\frac{T}{2\pi} + \frac{1}{2\pi} + O(\frac{\log T}{T}).$$

Demostración: Tomemos $T > 3$ que no sea la parte imaginaria de ningún cero no trivial de la función dseta y consideremos el rectángulo R que muestra la figura. Los ceros no triviales de ζ son los ceros de la función ξ, luego ésta tiene $2N(T)$ ceros dentro de R (y ninguno en su frontera). Por [VC 3.10] y el teorema de los residuos concluimos que



$$N(T) = \frac{1}{4\pi}\,\mathrm{Im}\int_R \frac{\xi'(s)}{\xi(s)}\,ds.$$

Ahora

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

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

Por lo tanto,

$$\frac{\xi'(s)}{\xi(s)} = \frac{1}{s} + \frac{1}{s-1} + \frac{\Phi'(s)}{\Phi(s)}.$$

Por el teorema de los residuos,

$$\frac{1}{4\pi}\operatorname{Im}\int_R\left(\frac{1}{s}+\frac{1}{s-1}\right)ds=1.$$

Como $\Phi(s)=\Phi(1-s)$ y $\Phi(\bar{s})=\overline{\Phi(s)}$ (esto es cierto para ξ, luego también para Φ), la integral toma el mismo valor en los cuatro cuadrantes del la frontera de R, de modo que

$$\frac{1}{4\pi}\operatorname{Im}\int_R\frac{\Phi'(s)}{\Phi(s)}\,ds=\frac{1}{\pi}\operatorname{Im}\int_\gamma\frac{\Phi'(s)}{\Phi(s)}\,ds,$$

donde γ es el segmento γ_1 que va de 2 a $2+iT$ seguido del segmento γ_2 que va de $2+iT$ hasta $1/2+iT$. A su vez

$$\frac{1}{4\pi}\operatorname{Im}\int_\gamma\frac{\Phi'(s)}{\Phi(s)}\,ds=\frac{1}{\pi}\operatorname{Im}\int_\gamma\left(-\frac{1}{2}\log\pi+\frac{1}{2}\frac{\Pi'((s-2)/2)}{\Pi((s-2)/2)}+\frac{\zeta'(s)}{\zeta(s)}\right)ds=$$

$$-\frac{T}{2\pi}\log\pi+\frac{1}{\pi}\operatorname{Im}\int_\gamma\left(\frac{1}{2}\frac{\Pi'((s-2)/2)}{\Pi((s-2)/2)}+\frac{\zeta'(s)}{\zeta(s)}\right)ds.$$

Por otra parte, por la regla de Barrow,

$$\frac{1}{\pi}\operatorname{Im}\int_\gamma\frac{1}{2}\frac{\Pi'((s-2)/2)}{\Pi((s-2)/2)}\,ds=\frac{1}{\pi}\operatorname{Im}\log\Pi(-\frac{3}{4}+i\frac{T}{2}).$$

Por la fórmula de Stirling [VC 4.30]:

$$\log\Pi(-\frac{3}{4}+i\frac{T}{2})=\log\sqrt{2\pi}+(-\frac{1}{4}+i\frac{T}{2})\log(-\frac{3}{4}+i\frac{T}{2})+\frac{3}{4}-i\frac{T}{2}+\mu(-\frac{3}{4}+i\frac{T}{2})$$

y, como el argumento de $-3/4+iT/2$ se aleja de $-\pi$ cuando T tiende a ∞, por [VC 4.29] el último término es $O(|-3/2+iT/2|^{-1})=O(1/T)$. Por lo tanto

$$\operatorname{Im}\log\Pi(-\frac{3}{4}+i\frac{T}{2})=\operatorname{Im}((-\frac{1}{4}+i\frac{T}{2})\log(-\frac{3}{4}+i\frac{T}{2}))-\frac{T}{2}+O(1/T)$$

$$=\frac{T}{2}\log|-\frac{3}{4}+i\frac{T}{2}|-\frac{1}{4}\arg(-\frac{3}{4}+i\frac{T}{2})-\frac{T}{2}+O(1/T).$$

Veamos ahora que

$$\frac{T}{2}\log|-\frac{3}{4}+i\frac{T}{2}|=\frac{T}{2}\log\frac{T}{2}+O(1/T).$$

En efecto, en general,

$$\frac{T}{2}\log|x+i\frac{T}{2}|-\frac{T}{2}\log\frac{T}{2}=\frac{T}{4}\log\left(1+\frac{4x^2}{T^2}\right)$$

y es fácil ver que

$$\lim_{T\to+\infty}\frac{T^2}{4}\log\left(1+\frac{4x^2}{T^2}\right)=x^2.$$

Por otra parte,

$$\arg(-\frac{3}{4}+i\frac{T}{2}) = \frac{\pi}{2} + \arctan\frac{3/4}{T/2} = \frac{\pi}{2} + O(1/T),$$

pues

$$\lim_{T\to+\infty} \frac{\arctan(3/2T)}{1/T} = \frac{3}{2}.$$

Por consiguiente,

$$\frac{1}{\pi}\operatorname{Im}\log\Pi(-\frac{3}{4}+i\frac{T}{2}) = \frac{T}{2\pi}\log\frac{T}{2} - \frac{1}{8} - \frac{T}{2\pi} + O(1/T).$$

Reuniendo todo lo que hemos obtenido queda que

$$N(T) = 1 - \frac{T}{2\pi}\log\pi + \frac{T}{2\pi}\log\frac{T}{2} - \frac{1}{8} - \frac{T}{2\pi} + \frac{1}{\pi}\operatorname{Im}\int_\gamma \frac{\zeta'(s)}{\zeta(s)}\,ds + O(1/T)$$

$$= \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + \frac{1}{\pi}\operatorname{Im}\int_\gamma \frac{\zeta'(s)}{\zeta(s)}\,ds + O(1/T).$$

Nos falta estimar la última integral. Para ello observamos que $\operatorname{Re}\zeta(s)$ no se anula sobre γ_1, pues

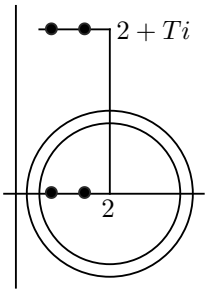
$$\operatorname{Re}\zeta(2+it) = 1 + \operatorname{Re}\sum_{n=2}^{\infty}\frac{e^{-it\log n}}{n^2} = 1 + \sum_{n=2}^{\infty}\frac{\cos(t\log n)}{n^2} \geq 1 - \sum_{n=2}^{\infty}\frac{1}{n^2}$$

$$= 2 - \zeta(2) = 2 - \frac{\pi^2}{6} > 1/4.$$

Por lo tanto, si $\operatorname{Re}\zeta(s)$ se anula en algún punto de γ, lo hace concretamente en puntos de γ_2, es decir, en puntos de la forma $\sigma+iT$, con $1/2 \leq \sigma \leq 2$. Además, σ es entonces un cero de la función

$$g(s) = \frac{1}{2}(\zeta(s+iT) + \zeta(s-iT)),$$

que es holomorfa en $\mathbb{C}$ salvo en $1 \pm iT$.



Así, los ceros de $\operatorname{Re}\zeta(s)$ sobre γ_2 se corresponden con los ceros de una función holomorfa en un intervalo cerrado, luego son un número finito. Digamos que g tiene m ceros en $[1/2, 2]$. Vamos a aplicar el teorema [VC 2.29] a la función g y a los discos $\overline{D(2,3/2)} \subset \overline{D(2,7/4)}$. El menor de ellos contiene al menos los m ceros de g que estamos considerando. Como $T > 3$, tenemos que g es holomorfa en el disco mayor. Por 4.7 con $\delta = 1/4$ tenemos que, si $|s-2| = 7/4$, entonces[6]

$$|g(s)| < \frac{1}{2}c(|\tau+T|^{3/4} + |\tau-T|^{3/4}) < c(2+T)^{3/4}.$$

[6]Por comodidad vamos a adoptar el convenio de que la letra c representará una constante arbitraria que puede ir modificándose en cada paso. Así, en las dos desigualdades siguientes la misma letra c representa a dos constantes distintas.

Por lo tanto, [VC 2.29] nos da que

$$|g(2)| \le c(2+T)^{3/4}\left(\frac{6}{7}\right)^m.$$

Por otra parte, hemos visto que $g(2) = \operatorname{Re}\zeta(2+iT) > 1/4$, luego

$$\left(\frac{7}{6}\right)^m \le 4c(2+T)^{3/4} < T,$$

para T suficientemente grande. Por lo tanto $m \le c\log T$, para T suficientemente grande.

Por otra parte, γ queda dividida en $m+1$ arcos consecutivos en los que $\operatorname{Re}\zeta(s)$ tiene signo constante. Si $\gamma_j : [a,b] \longrightarrow \mathbb{C}$ es uno de estos arcos, entonces

$$\operatorname{Im}\int_{\gamma_j}\frac{\zeta'(s)}{\zeta(s)}\,ds = \operatorname{Im}\int_{\gamma_j\circ\zeta}\frac{1}{z}\,dz.$$

Ahora, el arco $(\gamma_j\circ\zeta)^*$ está contenido en uno de los semiplanos $\operatorname{Im} z \ge 0$ o $\operatorname{Im} z \le 0$. En dicho semiplano existe un logaritmo holomorfo $\log z$, de modo que

$$\left|\operatorname{Im}\int_{\gamma_j}\frac{\zeta'(s)}{\zeta(s)}\,ds\right| = |\operatorname{Im}(\log\zeta(\gamma(b)) - \log\zeta(\gamma(a)))| \le \pi$$

(pues las partes imaginarias de los logaritmos son argumentos en un mismo intervalo de longitud π). Por consiguiente,

$$\left|\operatorname{Im}\int_{\gamma}\frac{\zeta'(s)}{\zeta(s)}\,ds\right| \le (m+1)\pi \le c\pi\log T,$$

para todo T suficientemente grande. Con esto concluimos que

$$\begin{aligned} N(T) &= \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + c_3\pi\log T + O(1/T)\\ &= \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T). \end{aligned}$$

En la prueba hemos supuesto que T no es la parte imaginaria de ningún cero de la función dseta. Esto no supone ninguna restricción, pues, si T no cumple esta condición, el hecho de que $N(T) = N(T+\epsilon)$ para todo $\epsilon > 0$ suficientemente pequeño y que $T+\epsilon$ cumple la estimación que hemos probado, implica que T también la cumple. ∎

Más adelante necesitaremos esta consecuencia sencilla del teorema anterior:

Teorema 4.20 *Para cada $h > 0$ fijo, se cumple que*

$$N(T+h) - N(T-h) = O(\log T),$$

(donde la constante implícita depende de h).

DEMOSTRACIÓN: Llamemos

$$f(t) = \frac{t}{2\pi}\log\frac{t}{2\pi} - \frac{t}{2\pi},$$

de modo que

$$f'(t) = \frac{1}{2\pi}\log\frac{t}{2\pi}.$$

Por el teorema del valor medio, existe un $T < \alpha < T + h$ tal que

$$f(T+h) - f(T) = f'(\alpha),$$

luego

$$N(T+h)-N(T) = \frac{1}{2\pi}\log\frac{\alpha}{2\pi}+O(\log T) \le \frac{1}{2\pi}\log\frac{T+h}{2\pi}+O(\log T) = O(\log T).$$

Igualmente se prueba que $N(T) - N(T-h) = O(\log T)$, y la conclusión es inmediata. ∎

Más adelante necesitaremos esta estimación:

Teorema 4.21

$$\sum_{0<\operatorname{Im}\rho\le T}\frac{1}{\operatorname{Im}\rho} = O(\log^2 T).$$

DEMOSTRACIÓN: Hemos probado que la parte imaginaria de los ceros no triviales es mayor o igual que 6.5 (en particular mayor o igual que 2), luego

$$\sum_{0<\operatorname{Im}\rho\le T}\frac{1}{\operatorname{Im}\rho} \le \sum_{m=2}^{E[T]}\sum_{m\le\operatorname{Im}\rho<m+1}\frac{1}{\operatorname{Im}\rho} \le \sum_{m=2}^{E[T]}\sum_{m\le\operatorname{Im}\rho<m+1}\frac{1}{m}.$$

Por el teorema anterior, $N(m+1) - N(m) \le c\log m \le c\log T$, luego

$$\sum_{0<\operatorname{Im}\rho\le T}\frac{1}{\operatorname{Im}\rho} \le c\log T\sum_{m=2}^{E[T]}\frac{1}{m} \le c\log^2 T.$$

∎

Ejemplo: El primer cero no trivial Vamos a usar el proceso seguido en la demostración de la fórmula de Riemann-von Mangoldt para calcular $N(6\pi)$. Como tenemos un valor concreto de T, podemos hacer de forma exacta parte de los cálculos, evitando las aproximaciones. Concretamente, partimos de la expresión

$$N(T) = 1 - \frac{T}{2\pi}\log\pi + \frac{1}{\pi}\operatorname{Im}\log\Pi(-\frac{3}{4}+i\frac{T}{2}) + \frac{1}{\pi}\operatorname{Im}\log\zeta(\frac{1}{2}+iT),$$

donde hemos usado la regla de Barrow para calcular la integral sobre γ de la derivada logarítmica de la función dseta. Al aplicar la fórmula de Stirling, el término que contiene la función factorial se convierte en

$$\frac{T}{2\pi}\log|-\frac{3}{4}+i\frac{T}{2}| - \frac{1}{4\pi}\arg(-\frac{3}{4}+i\frac{T}{2}) - \frac{T}{2\pi} + \frac{1}{\pi}\operatorname{Im}\mu(-\frac{3}{4}+i\frac{T}{2}).$$

Casi todos los términos pueden calcularse exactamente sin dificultad, y el resultado es

$$N(6\pi) \approx 1.174 + \frac{1}{\pi}\operatorname{Im}\mu(-\frac{3}{4}+3\pi i) + \frac{1}{\pi}\operatorname{Im}\log\zeta(\frac{1}{2}+6\pi i).$$

Según [VC 4.29] con $\delta = 1/2$ tenemos que

$$\frac{1}{\pi}\operatorname{Im}\mu(-\frac{3}{4}+3\pi i) \le \frac{1}{\pi}|\mu(-\frac{3}{4}+3\pi i)| \le \frac{1}{8\pi\operatorname{sen}^2(\pi/4)|-\frac{3}{4}+3\pi i|} \approx 0.0084.$$

Respecto al último término, observemos que $\operatorname{Im}\log\zeta(\frac{1}{2}+6\pi i)$ es un argumento de $\zeta(\frac{1}{2}+6\pi i)$, pero no uno cualquiera, sino el que le asigna la función $\log\zeta(\frac{1}{2}+6\pi i)$, que es continua y toma valores reales en $]1,+\infty[$. En la prueba del teorema anterior hemos visto que $\operatorname{Re}\zeta(2+it)$ es siempre positiva, y en el ejemplo de la página 111 hemos visto que lo mismo sucede sobre la semirrecta $\sigma \ge 1/2$, $\tau = 6\pi$, luego concluimos que, sobre el arco γ considerado en la prueba del teorema anterior, la función ζ toma valores en el semiplano $\sigma \ge 0$, luego, siempre sobre dicho arco, $-\pi/2 \le \operatorname{Im}\log\zeta(s) \le \pi/2$. Por lo tanto, el argumento que buscamos es el argumento de $\zeta(1/2+6\pi i)$ comprendido en este intervalo.

Basta aplicar el teorema 4.4 con $k = 4$ para asegurar que $\operatorname{Im}\zeta(1/2+6\pi i) < 0$, y ya sabemos que la parte real es positiva, lo que nos permite concluir que $-\pi/2 < \operatorname{Im}\log\zeta(\frac{1}{2}+6\pi i) < 0$. En definitiva:

$$N(6\pi) < 1.174 + 0.0084 < 2,$$

y, como tiene que ser un número natural, $N(6\pi) = 1$. En realidad, nuestros cálculos muestran también que es $N(6\pi) > 0$, con lo que obtenemos otra prueba de la existencia de ceros no triviales, pero lo cierto es que esto ya lo garantizamos al final de la sección anterior. Ahora podemos afirmar que el cero ρ_1 que encontramos allí es el único cero con parte imaginaria $0 < \tau < 6\pi$ y es, pues, "el primer cero no trivial" de la función dseta. Más aún, que $N(6\pi) = 1$ afirma que en la región considerada hay un único cero contando multiplicidades, luego ahora podemos afirmar que ρ_1 es un cero simple de la función dseta. ∎

La hipótesis de Riemann En general, al margen de que las técnicas computacionales que se emplean en la práctica son más sofisticadas y eficientes, la forma de encontrar ceros de la función dseta consiste esencialmente en evaluar $N(T)$ para un valor grande de T y contar los ceros de la forma $1/2+\tau i$ con $0 < \tau \le T$. Si el número de ceros encontrado coincide con el valor calculado de $N(T)$, esto significa que todos ellos son simples y son los únicos ceros de la función dseta que cumplen $0 < \operatorname{Im}\rho < T$ (así que, en particular, no hay otros en ese rango con una parte real distinta de $1/2$).

Si el número de ceros encontrado fuera inferior al valor calculado de $N(T)$ ello podría significar, o bien que alguno de los ceros hallados es múltiple, o bien que hay ceros con parte real distinta de $1/2$. Sin embargo, no se ha dado el caso hasta ahora. Los resultados computacionales afirman que los 10^{13} primeros ceros no triviales de la función dseta son todos simples y están todos sobre la recta crítica $\sigma = 1/2$.

Ya en 1859 Riemann afirmó que era "muy probable" que todos los ceros no triviales de la función dseta estuvieran sobre la recta crítica, y por ello tal afirmación se conoce como la *hipótesis de Riemann.* Hasta el momento nadie la ha demostrado ni refutado. Al margen del interés que tiene en sí misma, veremos que tiene consecuencias destacables sobre la distribución de los números primos. ∎

El orden de crecimiento de ζ'/ζ Vamos a estimar el crecimiento de la derivada logarítmica $\zeta'(s)/\zeta(s)$ en función de τ. Para que esto tenga sentido tenemos que "esquivar" sus polos, pues haciendo que s se acerque a un polo siempre podemos conseguir que $|\zeta'(s)/\zeta(s)|$ se haga arbitrariamente grande manteniendo τ acotado. En el caso de los polos asociados a los ceros triviales de $\zeta(s)$ y a su polo es fácil evitarlos:

Teorema 4.22 *En el semiplano $\sigma \le -1$ menos un disco de radio $\le 1/2$ centrado en cada número entero par así como en -1, se cumple que*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| = O(\log|s|).$$

Demostración: La ecuación funcional de la función dseta es

$$\zeta(s) = 2(2\pi)^{s-1}\operatorname{sen}\frac{\pi s}{2}\Pi(-s)\zeta(1-s).$$

Tomando derivadas logarítmicas, vemos que

$$\frac{\zeta'(s)}{\zeta(s)} = \log(2\pi) + \frac{\pi}{2}\cot\frac{\pi s}{2} - \frac{\Pi'(-s)}{\Pi(-s)} - \frac{\zeta'(1-s)}{\zeta(1-s)}.$$

Aplicamos la derivación logarítmica a la fórmula de Stirling:

$$\Pi(z) = \sqrt{2\pi}z^{z+1/2}e^{-s}e^{\mu(z)},$$

válida para $z \in \mathbb{C}\setminus\,]-\infty,0]$, lo que nos da

$$\frac{\Pi'(z)}{\Pi(z)} = \log z + 1 + \frac{1}{2z} - 1 + \mu'(z) = \log z + \frac{1}{2z} + \mu'(z),$$

donde

$$\mu(z) = -\int_0^{+\infty} \frac{u - E[u] - 1/2}{z+u}\,du,$$

luego

$$\mu'(z) = \int_0^{+\infty} \frac{u - E[u] - 1/2}{(z+u)^2}\,du,$$

y así, para $x = \operatorname{Re} z > 0$,

$$|\mu'(z)| \le \int_0^{+\infty} \frac{1/2}{(x+u)^2+y^2}\,du \le \frac{1}{2}\int_0^{+\infty}\frac{1}{(x+u)^2}\,du = \frac{1}{2x}.$$

En particular, si $\sigma \le -1$,

$$\left|\frac{\Pi'(-s)}{\Pi(-s)}\right| \le |\log(-s)| + \frac{1}{2} + \frac{1}{2} = \log|s| + \frac{\pi}{2} + 1 < c\log|s|,$$

donde en la última desigualdad tenemos usamos que s está fuera de un disco $D(-1,r)$, con lo que $|s| \ge \sqrt{1+r^2}$ y así $\log|s| \ge \log\sqrt{1+r^2} > 0$. Por otra parte,

$$\cot\frac{\pi s}{2} = i\frac{e^{i\pi s/2} + e^{-i\pi s/2}}{e^{i\pi s/2} - e^{-i\pi s/2}} = i\frac{e^{i\pi s}+1}{e^{i\pi s}-1},$$

luego, para $\tau \ge 1$,

$$|\cot(\pi s/2)| \le \frac{e^{-\pi\tau}+1}{|e^{i\pi s}-1|} \le \frac{e^{-\pi}+1}{|e^{i\pi s}-1|} \le c,$$

y si $\tau \le -1$ llegamos a la misma conclusión multiplicando el numerador y el denominador de la expresión inicial por $e^{-i\pi s/2}$. Para $|\tau| \le 1$ usamos que $\cot(\pi s/2)$ es una función meromorfa con polos en los enteros pares, luego está acotada en el compacto que resulta de eliminar del rectángulo $[-2,0]\times[-1,1]$ un disco abierto de centro -2 y otro de centro 0, y como tiene periodo 2, también lo está en toda la banda $|\tau| \le 1$ menos un disco alrededor de cada entero par. Por último

$$\left|\frac{\zeta'(1-s)}{\zeta(1-s)}\right| = \left|\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{1-s}}\right| \le \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{1-\sigma}} \le \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^2} = c.$$

En total,

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| < \log(2\pi) + \frac{\pi}{2}c + c\log|s| + c < c\log|s|. \qquad \blacksquare$$

Ahora probaremos un resultado similar para $-1 \le \sigma \le 2$, donde tenemos que esquivar los ceros no triviales de la función dseta. La situación es más delicada, y aquí es donde interviene la fórmula de Riemann von-Mangoldt. Para empezar probamos lo siguiente:

Teorema 4.23 *Sea $s \in \mathbb{C}$ tal que $-1 \le \sigma \le 2$, $\tau \ge 2$. Entonces*

$$\frac{\zeta'(s)}{\zeta(s)} - \sum_{|\operatorname{Im}\rho-\tau|<1}\frac{1}{s-\rho} = O(\log\tau),$$

donde ρ recorre los ceros no triviales de la función dseta que cumplen la condición indicada.

Demostración: Observemos que la función del enunciado no se hace nunca infinita. Podría pensarse que lo es cuando $s = \rho$ es un cero no trivial de la función dseta, pero hay que entender que en el sumatorio ρ aparece repetido tantas veces como indica su multiplicidad, es decir, que la suma contiene a $o(\zeta,\rho)/(s-\rho)$, pero esto es justamente la parte singular de la serie de Laurent de $\zeta'(s)/\zeta(s)$ alrededor de ρ, luego ésta se cancela con parte del sumatorio y la expresión toma un valor finito.

Tenemos que

$$\zeta(s) = \pi^{s/2}\Pi^{-1}(s/2)(s-1)^{-1}\xi(s) =$$
$$\frac{1}{2}(2\pi)^s\Pi^{-1}(s/2)(s-1)^{-1}\prod_\rho\left(1-\frac{s}{\rho}\right)e^{s/\rho},$$

luego, si s no es un cero de la función dseta,

$$\frac{\zeta'(s)}{\zeta(s)} = \log 2\pi - \frac{1}{s-1} - \frac{1}{2}\frac{\Pi'(s/2)}{\Pi(s/2)} + \sum_\rho\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right). \tag{4.7}$$

En primer lugar consideramos (4.7) para $s+3$, que sin duda no es un cero de la función dseta. Como en la prueba del teorema anterior, usamos la derivada logarítmica de la fórmula de Stirling sobre $z = (s+3)/2$, para el que se cumple $x = (\sigma+3)/2 \geq 1$, $y = \tau/2 \geq 1$. La conclusión es que

$$\left|\frac{\Pi'((s+3)/2)}{\Pi((s+3)/2)}\right| \leq |\log z| + \frac{1}{2} + \frac{1}{2} \leq \log|z| + \frac{\pi}{2} + 1 < c\log\tau.$$

En la última desigualdad usamos que $\tau \geq 2$. Por otra parte,

$$\left|\frac{\zeta'(s+3)}{\zeta(s+3)}\right| = \left|\sum_{n=1}^\infty \frac{\Lambda(n)}{n^{s+3}}\right| \leq \sum_{n=1}^\infty \frac{\Lambda(n)}{n^{\sigma+3}} \leq \sum_{n=1}^\infty \frac{\Lambda(n)}{n^2} = c.$$

así pues, por (4.7) aplicado a $s+3$ concluimos que

$$\left|\sum_\rho\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right)\right| \leq c + \log 2\pi + 1 + c\log\tau < c\log\tau.$$

Dentro de esta suma, separamos los términos

$$\sum_{|\operatorname{Im}\rho-\tau|<1}\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right).$$

Por el teorema 4.20, el número de sumandos es $N(\tau+1)-N(\tau-1) = O(\log\tau)$, y cada uno de ellos tiene módulo

$$\left|\frac{1}{s+3-\rho}+\frac{1}{\rho}\right| \leq \frac{1}{\sigma+3-1}+\frac{1}{\tau-1} \leq 2,$$

luego

$$\left|\sum_{|\operatorname{Im}\rho-\tau|<1}\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right)\right| < c\log\tau.$$

Por lo tanto, también

$$\left|\sum_{|\operatorname{Im}\rho-\tau|\geq 1}\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right)\right| < c\log\tau.$$

Ahora que hemos separado los ceros que podrían coincidir con s, pasamos a estimar la suma con s en lugar de $s+3$. Para ello usamos 4.20:

$$\left|\sum_{\operatorname{Im}\rho\ge\tau+1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)-\sum_{\operatorname{Im}\rho\ge\tau+1}\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right)\right|=$$

$$=\left|\sum_{\operatorname{Im}\rho\ge\tau+1}\left(\frac{1}{s-\rho}-\frac{1}{s+3-\rho}\right)\right|=\left|\sum_{\operatorname{Im}\rho\ge\tau+1}\frac{3}{(s-\rho)(s+3-\rho)}\right|$$

$$\le\sum_{\operatorname{Im}\rho\ge\tau+1}\frac{3}{|\tau-\operatorname{Im}\rho||\tau-\operatorname{Im}\rho|}=3\sum_{\operatorname{Im}\rho\ge\tau+1}\frac{1}{(\tau-\operatorname{Im}\rho)^2}$$

$$=3\sum_{n=1}^{\infty}\sum_{\tau+n\le\operatorname{Im}\rho<\tau+n+1}\frac{1}{(\tau-\operatorname{Im}\rho)^2}\le 3\sum_{n=1}^{\infty}\sum_{\tau+n\le\operatorname{Im}\rho<\tau+n+1}\frac{1}{n^2}$$

$$<c\sum_{n=1}^{\infty}\frac{\log(\tau+n)}{n^2}\le c\sum_{n\le\tau}\frac{\log 2\tau}{n^2}+c\sum_{n>\tau}\frac{\log 2n}{n^2}$$

$$\le c\sum_{n=1}^{\infty}\frac{\log 2}{n^2}+c\sum_{n=1}^{\infty}\frac{\log 2n}{n^2}+c\log\tau\sum_{n=1}^{\infty}\frac{1}{n^2}<c\log\tau.$$

Similarmente,

$$\left|\sum_{\operatorname{Im}\rho\le\tau-1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)-\sum_{\operatorname{Im}\rho\le\tau-1}\left(\frac{1}{s+3-\rho}+\frac{1}{\rho}\right)\right|<c\log\tau,$$

luego

$$\left|\sum_{|\operatorname{Im}\rho-\tau|\ge 1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)\right|<c\log\tau.$$

Ahora volvemos a (4.7), que podemos escribir así:

$$\frac{\zeta'(s)}{\zeta(s)}-\sum_{|\operatorname{Im}\rho-\tau|<1}\frac{1}{s-\rho}=\log 2\pi-\frac{1}{s-1}-\frac{1}{2}\frac{\Pi'(s/2)}{\Pi(s/2)}$$

$$+\sum_{|\operatorname{Im}\rho-\tau|\ge 1}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)+\sum_{|\operatorname{Im}\rho-\tau|<1}\frac{1}{\rho}.$$

En principio, esto vale cuando s no es un cero de la función dseta, pero cuando $s=\rho_0$ la igualdad vale para los puntos $\rho_0\pm\delta$, para todo $\delta>0$ suficientemente pequeño (notemos que, como no cambiamos la parte imaginaria, los sumatorios son los mismos). Pero, según hemos explicado al principio, el primer miembro puede verse como una función continua de δ, la función definida por la serie de Laurent de $\zeta'(s)/\zeta(s)$ a la que hemos restado su parte singular y tal

vez una función holomorfa en un entorno de ρ_0 (la parte del sumatorio correspondiente a otros posibles ceros). Así, ambos miembros son funciones continuas de δ en un entorno de 0, luego la igualdad vale también para $\delta = 0$, es decir, para $s = \rho_0$.

En cuanto al miembro derecho, los sumandos del último término cumplen

$$\left|\frac{1}{\rho}\right| \le \frac{1}{\tau - 1} \le 1$$

y el número de sumandos es $N(\tau+1) - N(\tau-1) = O(\log\tau)$, luego el sumatorio es $O(\log\tau)$. Hemos probado que lo mismo vale para el penúltimo sumando, y es trivialmente cierto para los dos primeros. Sólo falta probar que $\Pi'(s/2)/\Pi(s/2) = O(\log\tau)$. En efecto, según la estimación general que hemos hecho antes sobre la función factorial:

$$\frac{\Pi'(s/s)}{\Pi(s/2)} = \log(s/2) + \frac{1}{s} + \mu'(s/2),$$

y $|\log(s/2)| \le \log|s/2| + \pi \le \log\sqrt{2\tau^2} + \pi = O(\log\tau)$, mientras que

$$|\mu'(s/2)| \le \int_0^{+\infty} \frac{1/2}{(\sigma/2+x)^2 + \tau^2/4}\,dx \le \frac{1}{2}\int_0^{+\infty} \frac{1}{(\sigma/2+x)^2+1}\,dx =$$

$$\frac{\pi}{4} - \frac{1}{2}\arctan\frac{\sigma}{2} \le c. \qquad \blacksquare$$

Ahora ya podemos continuar nuestro estudio de $\zeta'(s)/\zeta(s)$:

Teorema 4.24 *Para cada $T \ge 2$ existe $T < \tau < T+1$ con la propiedad de que todo cero no trivial de la función dseta cumple*

$$|\operatorname{Im}\rho - \tau|^{-1} \le c\log\tau$$

(donde c es una constante independiente de T). Sobre los números s cuya parte imaginaria cumple esta condición y cuya parte real es $-1 \le \sigma \le 2$, se cumple que

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log^2\tau).$$

Demostración: Por 4.20 tenemos que el número m de ceros no triviales ρ tales que $T \le \operatorname{Im}\rho < T+1$ (contados con su multiplicidad) es $m \le c\log T - 1$. Las partes imaginarias de dichos ceros dividen al intervalo $[T, T+1]$ en $m+1$ subintervalos, luego no puede ser que todos ellos tengan longitud menor que $(c\log T)^{-1}$. Si tomamos $T < \tau < T+1$ que sea el centro de un subintervalo de longitud $\ge (c\log T)^{-1}$, entonces $|\operatorname{Im}\rho - \tau| \ge (2c\log T)^{-1}$, para todo cero no trivial ρ, luego

$$|\operatorname{Im}\rho - \tau|^{-1} \le 2c\log T \le c\log\tau.$$

Ahora recordamos el teorema 4.23, según el cual, si $-1 \le \sigma \le 2$, se cumple que

$$\frac{\zeta'(s)}{\zeta(s)} - \sum_{|\operatorname{Im}\rho-\tau|<1} \frac{1}{s-\rho} = O(\log\tau).$$

Por 4.20, el número de sumandos es $O(\log\tau)$, y cada uno de ellos tiene módulo

$$|s-\rho|^{-1} \le |\tau - \operatorname{Im}\rho|^{-1} = O(\log\tau),$$

luego

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log^2\tau).$$

■

Obviamente, tomando conjugados se concluye que $\zeta'(s)/\zeta(s) = O(\log^2|\tau|)$ en la banda $-1 \le \sigma \le 2$ y $|\tau| \ge 2$ siempre que la parte imaginaria sea opuesta a una de las que cumplen el teorema anterior. Respecto al semiplano $\sigma \ge 2$ no hay nada que probar, pues en él la derivada logarítmica está acotada.

Terminamos con otra aplicación del teorema 4.23:

La hipótesis de Lindelöf Tras el teorema 4.11 hemos visto que la función de Lindelöf μ está determinada salvo en el intervalo $]0,1[$, donde sólo hemos sabido dar cotas superiores e inferiores. En particular, $0 \le \mu(0) \le 1/4$.

Lindelöf conjeturó lo que hoy se conoce como *hipótesis de Lindelöf,* que no es sino la afirmación:

$$\mu(0) = 0.$$

Notemos que los resultados que conocemos sobre la función μ (en especial su convexidad) hacen que la hipótesis de Lindelöf la determine completamente. A saber, si $\mu(0) = 0$, necesariamente

$$\mu(\sigma) = \begin{cases} 0 & \text{si } \sigma \ge 1/2, \\ \frac{1}{2} - \sigma & \text{si } \sigma \le 1/2. \end{cases}$$

Definimos $N(\sigma, T)$ como el número de ceros no triviales de la función dseta (contados con su multiplicidad) que cumplen $\operatorname{Re}\rho \ge \sigma$, $0 \le \operatorname{Im}\rho \le T$.

La hipótesis de Riemann implica que $N(\sigma, T) = 0$ para todo $\sigma > 1/2$, luego el teorema siguiente muestra en particular que la hipótesis de Riemann implica la hipótesis de Lindelöf:

Teorema 4.25 *La hipótesis de Lindelöf equivale a que, para todo $\sigma > 1/2$, se cumple que*

$$N(\sigma, T+1) - N(\sigma, T) = o(\log T).$$

Demostración: Sea $\delta = \sigma - 1/2$. Si se cumple la hipótesis de Lindelöf, aplicamos a la función $\zeta(s+2+iT)$ la fórmula de Jensen [VC 4.24] con $r = \frac{3}{2} - \frac{\delta}{4}$:

$$\sum_{|\rho-2-iT|<r} \log \frac{r}{|\rho-2-iT|} = \frac{1}{2\pi}\int_0^{2\pi} \log|\zeta(2+iT+re^{i\theta})|\,d\theta - \log|\zeta(2+iT)|.$$

donde ρ recorre los ceros de $\zeta(s)$ que cumplen la condición indicada. Por hipótesis, dado $\epsilon > 0$, tenemos que $\zeta(\sigma + i\tau) = O(\tau^{\epsilon/2})$ para $\sigma = \frac{1}{2} + \frac{\delta}{4}$ y para $\sigma = \frac{7}{2} - \frac{\delta}{4}$, y en la prueba del teorema de Lindelöf se ve que, para cualquier σ intermedio, se cumple que

$$|\zeta(\sigma + i\tau)| \leq M_\epsilon \tau^{\epsilon/2},$$

donde la constante M_ϵ no depende de σ. Por lo tanto,

$$\log|\zeta(2 + iT + re^{i\theta})| \leq \log M_\epsilon + \frac{\epsilon}{2}\log(T + r\,\mathrm{sen}\,\theta) \leq \log M_\epsilon + \frac{\epsilon}{2}\log(T + 3/2).$$

Por consiguiente, existe un $T_\epsilon > 0$ tal que si $T > T_\epsilon$ entonces

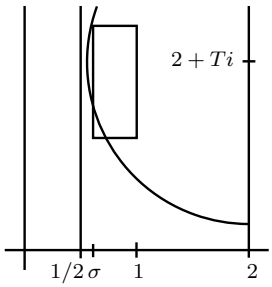
$$\log|\zeta(2 + iT + re^{i\theta})| \leq \epsilon \log T.$$

Lo mismo vale entonces para la integral, y trivialmente para el último término, que está acotado, luego todo el miembro derecho de la igualdad precedente es $o(\log T)$.

Si N es el número de ceros en el disco $|\rho - 2 - iT| < r_1 = \frac{3}{2} - \frac{\delta}{2} \leq r$, entonces

$$N \log \frac{\frac{3}{2} - \frac{\delta}{4}}{\frac{3}{2} - \frac{\delta}{2}} \leq \sum_{|\rho-2-iT|<r_1} \log \frac{r}{|\rho - 2 - iT|} \leq$$

$$\sum_{|\rho-2-iT|<r} \log \frac{r}{|\rho - 2 - iT|} = o(\log T).$$



Ahora bien, recordando que $\delta = \sigma - 1/2$, tenemos que $N(\sigma, t+1) - N(\sigma, t)$ es el número de ceros en el rectángulo $[\frac{1}{2} + \delta, 1] \times]t, t+1]$, el cual, por la compacidad de su clausura, puede cubrirse con un número finito de discos de la forma $D_j = D(2 + iT_j, \frac{3}{2} - \frac{\delta}{2})$, cuyo número K_δ depende de δ, pero no de t (si cubrimos un rectángulo para un t, cualquier otro rectángulo se cubre por trasladados de los mismos discos). Por consiguiente,

$$N(\sigma, t+1) - N(\sigma, t) \leq \frac{K_\delta}{\log \frac{\frac{3}{2} - \frac{\delta}{4}}{\frac{3}{2} - \frac{\delta}{2}}} o(\log T) = o(\log T).$$

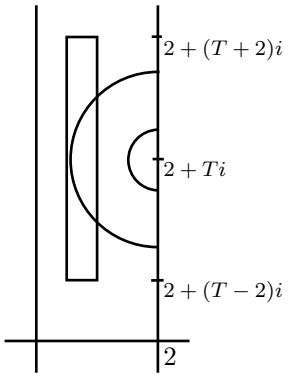
Supongamos ahora que se cumple la condición del enunciado. Esto implica, más en general, que

$$N(\sigma, T+2) - N(\sigma, T-2) = \sum_{k=-2}^{1} (N(\sigma, T+k+1) - N(\sigma, T+k))$$

$$= \sum_{k=-2}^{1} o(\log(T+k)) = o(\log T).$$

Fijemos un número $0 < \delta < 1/2$ y consideremos $D = D(2 + iT, \frac{3}{2} - \delta)$. Es fácil ver entonces que la intersección de D con la banda crítica está contenida en $\left[\frac{1}{2} + \delta, 1\right] \times]T - 2, T + 2[$, luego, por hipótesis, el número de ceros que contiene es a lo sumo

$$N(1/2 + \delta, T + 2) - N(1/2 + \delta, T - 2) = o(\log T).$$



Vamos a estimar la función meromorfa

$$F(s) = \frac{\zeta'(s)}{\zeta(s)} - \sum_{\rho \in D} \frac{1}{s - \rho}.$$

Como sucedía en el teorema 4.23, la función $\zeta'(s)/\zeta(s)$ tiene polos simples en los ceros de $\zeta(s)$, y el sumatorio elimina las partes singulares correspondientes a los ceros en D, luego F es holomorfa en D. En particular lo es en los puntos de la circunferencia $|s - 2 - iT| = \frac{3}{2} - 2\delta$. Fijado uno de estos puntos, podemos descomponer F como

$$\frac{\zeta'(s)}{\zeta(s)} - \sum_{\rho \in D} \frac{1}{s - \rho} = \frac{\zeta'(s)}{\zeta(s)} - \sum_{|\operatorname{Im}\rho - \tau| < 1} \frac{1}{s - \rho} + \sum_{\substack{|\operatorname{Im}\rho - \tau| < 1 \\ \rho \notin D}} \frac{1}{s - \rho} - \sum_{\substack{|\operatorname{Im}\rho - \tau| \geq 1 \\ \rho \in D}} \frac{1}{s - \rho}.$$

Ahora observamos que si ρ está en uno de los dos últimos sumatorios y $|s - \rho| < \delta$, entonces $|\tau - \operatorname{Im}\rho| < \delta < 1$, luego ρ tiene que estar concretamente en el penúltimo sumatorio, con $\rho \notin D$, pero entonces

$$|s - \rho| \geq |\rho - 2 - iT| - |s - 2 - iT| \geq \frac{3}{2} - \delta - \left(\frac{3}{2} - 2\delta\right) = \delta,$$

contradicción. Por lo tanto, todos los sumandos de los dos últimos sumatorios cumplen $|s - \rho| \geq \delta$.

Los ceros con $|\operatorname{Im}\rho - \tau| < 1$ cumplen también $|\operatorname{Im}\rho - T| < 1 + 3/2$, luego su número es $O(\log T)$, por el teorema 4.20. Por lo tanto, el penúltimo sumatorio es $O(\delta^{-1} \log T)$. Lo mismo vale para el último sumatorio, pues los ceros de D cumplen $|\operatorname{Im}\rho - T| < 3/2$, luego también son $O(\log T)$ (de hecho, hemos visto que por hipótesis son $o(\log T)$, pero en este punto de la prueba no podemos aprovechar realmente la hipótesis del teorema, ya que en cualquier caso sólo podemos afirmar que los dos últimos sumatorios son, conjuntamente, $O(\delta^{-1} \log T)$).

Por último, teniendo en cuenta el teorema 4.23, para $\sigma \leq 2$ tenemos que

$$F(s) = O(\log \tau) + O(\delta^{-1} \log T) = O(\delta^{-1} \log T),$$

mientras que si $\sigma > 2$, entonces $\zeta'(s)/\zeta(s) = O(1)$, pues en este semiplano admite un desarrollo en serie de Dirichlet, y el sumatorio para $\rho \in D$ tiene $O(\log T)$ sumandos (de nuevo, no necesitamos la hipótesis de que son $o(\log T)$), todos los cuales cumplen $|s - \rho| > 1 > \delta$, luego la conclusión es la misma.

En resumen, tenemos que, sobre la circunferencia $|s-2-iT| = \frac{3}{2} - 2\delta$, la función holomorfa F está acotada por $M(\delta, T) = (c/\delta)\log T$.

Consideremos ahora un punto de la circunferencia $|s-2-iT| = 1/2$. Aquí la situación es más simple, pues la circunferencia está contenida en el semiplano $\sigma > 1.25$, luego $\zeta'(s)/\zeta(s) = O(1)$ y $|s-\rho| \geq 1/2$, luego todos los sumandos que aparecen en el sumatorio que define a F están acotados por 2. Ahora sí que podemos aprovechar que el número de sumandos es $o(\log T)$, para concluir que el sumatorio es $o(\log T)$.

Así pues, sobre la circunferencia $|s-2-iT| = 1/2$ tenemos que F está acotada por $M_0(T) = o(\log T)$.

Con esto podemos aplicar el teorema de las tres circunferencias [VC 2.32] al anillo $D(0; \frac{1}{2}, \frac{3}{2} - 2\delta)$. La conclusión es que si $|s-2-iT| = r$, donde $1/2 \leq r \leq 3/2 - 3\delta$, entonces

$$|F(s)| \leq M_0(T)^\alpha M(\delta, T)^{1-\alpha} \leq M_0(T)M(\delta, T) = o(\log T),$$

donde $\alpha = \log(\frac{3-4\delta}{2r})/\log(3-6\delta)$.

Sea ahora γ el segmento de extremos $\frac{1}{2} + 3\delta + iT$ y $2 + iT$. Tenemos que

$$\left| \int_\gamma F(s)\, d\sigma \right| \leq \frac{3}{2} o(\log T) = o(\log T).$$

Por otra parte

$$\int_\gamma F(s)\, d\sigma = \log\zeta(2+iT) - \log\zeta(\frac{1}{2} + 3\delta + iT)$$

$$- \sum_{\rho \in D} (\log(2 + iT - \rho) - \log(\frac{1}{2} + 3\delta + iT - \rho)).$$

Aquí observamos que $\log\zeta(2+iT) = O(1)$, pues $\log\zeta$ admite un desarrollo en serie de Dirichlet absolutamente convergente en $\sigma > 1$. Tomando partes reales queda que

$$\log|\zeta(\frac{1}{2} + 3\delta + iT)| = o(\log T) + \sum_{\rho \in D} (\log|2 + iT - \rho| - \log|\frac{1}{2} + 3\delta + iT - \rho|).$$

Tenemos que $\log|2 + iT - \rho| \leq \log(3/2)$ y

$$\log|1/2 + 3\delta + iT - \rho| = \log|1/2 + 3\delta - 2 + (2 + iT - \rho)| \leq \log 6,$$

y el número de sumandos es $o(\log T)$, luego la suma es también $o(\log T)$. En definitiva,

$$\log|\zeta(\frac{1}{2} + 3\delta + iT)| = o(\log T).$$

Dado $\epsilon > 0$, vemos entonces que

$$\log \frac{|\zeta(\frac{1}{2} + 3\delta + iT)|}{T^\epsilon} = \left(\frac{\log |\zeta(\frac{1}{2} + 3\delta + iT)|}{\log T} - \epsilon \right) \log T \to -\infty,$$

luego

$$\lim_{T \to +\infty} \frac{|\zeta(\frac{1}{2} + 3\delta + iT)|}{T^\epsilon} = 0.$$

Esto significa que $\mu(\frac{1}{2} + 3\delta) = 0$ y, por continuidad, $\mu(1/2) = 0$. ∎

Capítulo V

La función dseta y los números primos

La demostración que hemos dado del teorema de los números primos se ha apoyado en el hecho de que la función dseta de Riemann no tiene ceros sobre la recta $\sigma = 1$. Es posible demostrar el teorema sin hacer referencia a la función dseta ni a funciones holomorfas en general, pero con ello se oculta la estrecha relación que existe entre la distribución de los números primos y los ceros no triviales de la función dseta. En este capítulo la pondremos de manifiesto.

5.1 Fórmulas explícitas

El teorema de los números primos proporciona una aproximación asintótica a la función contadora de primos $\pi(n)$. Sin embargo, Riemann se propuso encontrar una expresión analítica exacta, y llegó a una expresión que muestra explícitamente la conexión entre la función $\pi(n)$ y los ceros no triviales de la función dseta. Dicha fórmula se conoce como la "fórmula explícita" para $\pi(x)$. En principio, Riemann obtuvo una fórmula para la función $\pi^*(x)$ que definimos en 2.15:

$$\pi^*(x) = \mathrm{il}(x) - \sum_\rho \mathrm{il}(x^\rho) - \log 2 + \int_x^{+\infty} \frac{dt}{t(t^2-1)\log t}.$$

Aquí la función il es la integral logarítmica completa:

$$\mathrm{il}(x) = \int_0^x \frac{dt}{\log t} = \mathrm{Il}(x) + \mathrm{il}(2),$$

donde il(2) se define como el valor principal

$$\mathrm{il}(2) = \lim_{\epsilon\to 0^+} \left(\int_0^{1-\epsilon} \frac{dt}{\log t} + \int_{1-\epsilon}^2 \frac{dt}{\log t} \right) \approx 1.04516378\ldots$$

(El límite de cada sumando por separado es infinito.)

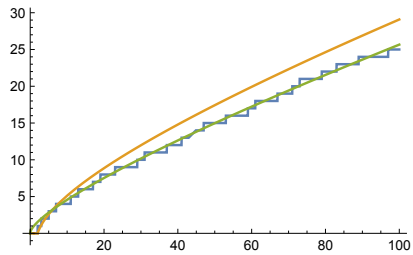
Además, para plantear la fórmula explícita es necesario extender la definición a una función holomorfa en el plano complejo, de modo que pueda actuar sobre los números x^ρ. Además, la convergencia de la serie no es absoluta, por lo que es necesario especificar el orden de los sumandos. Aplicando la fórmula probada en 2.16 se obtiene la fórmula explícita para π:

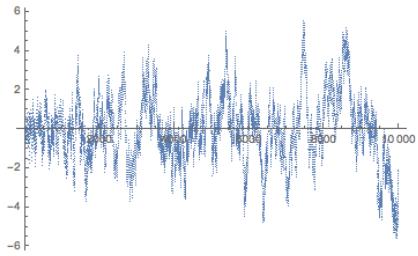
$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \left(\mathrm{il}(x^{1/n}) - \sum_\rho \mathrm{il}(x^{\rho/n}) - \log 2 + \int_{x^{1/n}}^{+\infty} \frac{dt}{t(t^2-1)\log t} \right).$$

Riemann conjeturó que la función

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{il}(x^{1/n})$$

sería una aproximación de $\pi(x)$ mucho mejor que $\mathrm{Il}(x)$. La figura de la izquierda muestra las gráficas de $\pi(x)$, $\mathrm{Il}(x)$ y $R(x)$. La que queda claramente por arriba es $\mathrm{Il}(x)$. La figura de la izquierda muestra los valores de $R(x) - \pi(x)$. Vemos que para $x \leq 10\,000$ el error no excede las 6 unidades.





En realidad Riemann no demostró la fórmula explícita, sino que la primera prueba rigurosa se debe a von Mangoldt, quien además obtuvo otra "fórmula explícita" para la función ψ, que resulta ser mucho más sencilla y manejable que la de π. En realidad, por razones técnicas, la fórmula en cuestión no calcula la función ψ propiamente dicha, sino una variante mínima:

$$\psi_0(x) = \frac{1}{2}(\lim_{t\to x^-} \psi(x) + \lim_{t\to x^+} \psi(x)).$$

Esta función coincide con $\psi(x)$ en los puntos en los que ésta es continua, es decir, salvo si x es potencia de primo, en cuyo caso $\psi_0(x) = \psi(x) - \frac{1}{2}\Lambda(x)$ es el punto medio del salto finito que presenta ψ en x.

Con esta salvedad, la fórmula explícita de von Mangoldt es la siguiente:

Teorema 5.1 *Si*[1] $x \geq 2$*, se cumple que*

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right),$$

donde ρ recorre los ceros no triviales de la función dseta repetidos según su multiplicidad.

[1] En realidad la fórmula vale si $x > 1$, pero por simplicidad supondremos $x \geq 2$.

Como vemos, en esta fórmula desaparecen las integrales logarítmicas, la integral final y también el sumatorio con la función de Möbius. Aun así, la fórmula retiene una dificultad, y es que la serie que aparece en ella no es absolutamente convergente, ya que $|x^\rho/\rho| \geq 1/|\rho|$ y en 4.15 hemos visto que esta serie diverge. Por ello hay que fijar una ordenación de los ceros y, concretamente, entenderemos que

$$\sum_\rho \frac{x^\rho}{\rho} = \lim_{T\to+\infty} \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho}.$$

Por otra parte, es interesante observar que el desarrollo en serie de Taylor

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

nos da que el último término de la fórmula explícita es

$$\frac{1}{2}\log\left(1-\frac{1}{x^2}\right) = -\frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{nx^{2n}} = \sum_{n=1}^{\infty}\frac{x^{-2n}}{-2n},$$

que es la serie análoga al primer término, pero para los ceros triviales de la función dseta, en lugar de los no triviales.

El hecho de que la serie que aparece en la fórmula de von Mangoldt no sea absolutamente convergente introduce dificultades en la demostración, las cuales desaparecen en la prueba de otra fórmula explícita para una función más sencilla, a saber, la integral

$$\psi_1(x) = \int_1^x \psi(t)\,dt = \sum_{n\leq x} \Lambda(n)(x-n).$$

La segunda igualdad se obtiene aplicando 2.20:

$$\sum_{n\leq x}\Lambda(n)n = \sum_{n\leq x}\Lambda(n)x - \int_1^x \psi(t)\,dt.$$

La fórmula explícita para ψ_1 es la siguiente:

Teorema 5.2 *Si $x \geq 1$, se cumple*

$$\psi_1(x) = \frac{x^2}{2} - \sum_\rho \frac{x^{\rho+1}}{\rho(\rho+1)} - x\log 2\pi + \frac{\zeta'(-1)}{\zeta(-1)} - \sum_{n=1}^{\infty}\frac{x^{1-2n}}{2n(2n-1)}.$$

Las dos series que aparecen en esta fórmula son absolutamente convergentes. La primera porque

$$\left|\frac{x^{\rho+1}}{\rho(\rho+1)}\right| = \frac{x^{\operatorname{Re}\rho+1}}{|\rho||\rho+1|} \leq \frac{x^2}{|\rho|^2},$$

y este último término define una serie convergente.

Se observa además que la fórmula para ψ_0 se obtiene derivando la correspondiente a ψ_1, admitiendo que las series pueden derivarse término a término, pero nada justifica que esto sea lícito (de hecho, suponiendo que fuera lícito hacerlo, ¿por qué la derivada tendría que ser $\psi_0(x)$ y no $\psi(x)$?). Así pues, tendremos que demostrar los dos teoremas independientemente. No entraremos, en cambio, en la prueba de la fórmula explícita para $\pi(x)$.

La fórmula explícita para ψ_1 Demostraremos primero el teorema 5.2, que es más sencillo que 5.1. Partimos de una variante del teorema 4.22 (del cual sólo necesitaremos el caso $k = 1$):

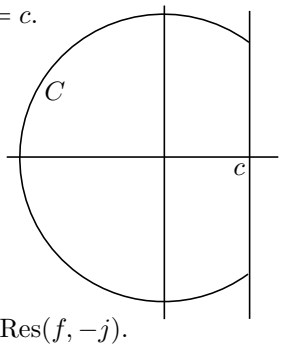
Teorema 5.3 *Sea $k \geq 1$ un número natural y $c > 0$, $y > 0$ números reales. Entonces*

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{y^s\, ds}{s(s+1)\cdots(s+k)} = \begin{cases} 0 & si\ y \leq 1 \\ \frac{1}{k!}\left(1-\frac{1}{y}\right)^k & si\ y \geq 1. \end{cases}$$

Demostración: Sea $f(s)$ el integrando. Observemos en primer lugar que, sobre los puntos de la forma $s = c + it$, puesto que $|s + j| \geq t$, tenemos que

$$|f(s)| = \left|\frac{y^s}{s(s+1)\cdots(s+k)}\right| \leq \frac{y^c}{|t|^{k+1}},$$

de donde se sigue que f es integrable sobre la recta $\sigma = c$.



Supongamos en primer lugar que $y \geq 1$. Para cada $T > 0$, consideramos el arco de circunferencia C de centro 0 y radio R que une los puntos $c \pm Ti$ y que está a la izquierda de la recta $\sigma = c$, tal y como indica la figura. Podemos suponer que T es lo suficientemente grande como para que $R > 2k$. Por el teorema de los residuos

$$\frac{1}{2\pi i}\int_{c-Ti}^{c+Ti} f(s)\, ds + \frac{1}{2\pi i}\int_C f(s)\, ds = \sum_{j=0}^{k} \operatorname{Res}(f, -j).$$

Por otra parte, sobre C^* tenemos que $|s+j| \geq |s|-j \geq R-k \geq R-R/2 = R/2$, así como que $|y^s| = y^\sigma \leq y^c$, y aquí es crucial que $y \geq 1$. Por lo tanto

$$\left|\int_C f(s)\, ds\right| \leq 2\pi R\frac{2^{k+1}y^c}{R^{k+1}} < 2\pi\frac{2^{k+1}y^c}{T^k}.$$

Como esta expresión tiende a 0 cuando T tiende a $+\infty$, concluimos que

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} f(s)\, ds = \sum_{j=0}^{k} \operatorname{Res}(f, -j).$$

Los residuos los podemos calcular con el teorema [An 10.27]: consideramos la función $P(s) = \prod_{r=0}^{k}(s+r)$, con lo que

$$\operatorname{Res}(f,-j) = \frac{y^{-j}}{P'(-j)},$$

ahora bien, $P(s) = (s+j)\prod_{r\neq j}(s+r)$, luego

$$P'(-j) = \prod_{r\neq j}(r-j) = \prod_{r=0}^{j-1}(r-j)\prod_{r=j+1}^{k}(r-j) =$$

$$(-1)^j\prod_{r=0}^{j-1}(j-r)\prod_{r=j+1}^{k}(k-j) = (-1)^j j!(r-j)!$$

Por lo tanto,

$$\sum_{j=0}^{k}\operatorname{Res}(f,-j) = \sum_{j=0}^{k}\frac{y^{-j}}{(-1)^j j!(k-j)!} = \frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1/y)^j = \frac{1}{k!}(1-1/y)^k.$$

Si $y \leq 1$ la diferencia es que tenemos que considerar como Ci el arco de circunferencia que queda a la derecha de la recta $\sigma = c$, para que podamos decir igualmente que, sobre C^*, se cumple $|y^s| = y^\sigma \leq y^c$, porque $\sigma \geq c$ e $y \leq 1$. En este caso el arco cerrado no encierra polos de f y la integral es nula. ∎

Con esto obtenemos una primera expresión para $\psi_1(x)$:

Teorema 5.4 *Si $x > 0$ y $c > 1$, se cumple:*

$$\psi_1(x) = -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds.$$

Demostración: Tenemos que

$$\frac{\psi_1(x)}{x} = \sum_{n\leq x}\left(1-\frac{n}{x}\right)\Lambda(n) = \frac{1}{2\pi i}\sum_{n=1}^{\infty}\Lambda(n)\int_{c-i\infty}^{c+i\infty}\frac{(x/n)^s\,ds}{s(s+1)}.$$

Ahora queremos intercambiar la suma y la integral. Para ello observamos que

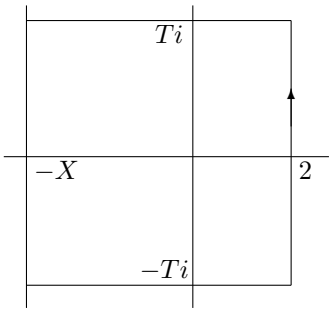
$$\left|\sum_{n=1}^{N}\frac{\Lambda(n)(x/n)^{c+it}}{(c+it)(c+1+it)}\right| \leq x^c\sum_{n=1}^{N}\frac{\Lambda(n)}{n^c}\frac{1}{c^2+t^2} \leq -x^c\frac{\zeta'(c)}{\zeta(c)}\frac{1}{c^2+t^2},$$

y esta última función es integrable en $\mathbb{R}$, por lo que podemos aplicar el teorema de la convergencia dominada de Lebesgue [An 4.55] (a la parte real y a la parte imaginaria de las sumas parciales). Así pues,

$$\frac{\psi_1(x)}{x} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{x^s}{s(s+1)}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}ds,$$

de donde se sigue la fórmula del enunciado. ∎

Ahora ya estamos en condiciones de obtener la fórmula explícita:



Demostración (de 5.2): Consideremos la integral

$$-\frac{1}{2\pi i}\int_R \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds,$$

donde R es el rectángulo que muestra la figura. Escogemos $X \geq 3$ de modo que sea un natural impar y $X < T < X+1$ de modo que cumpla la condición del teorema 4.24. Así, el teorema 4.22 nos asegura que $\zeta'(s)/\zeta(s) = O(\log|s|)$ sobre el lado izquierdo del rectángulo, y también sobre los lados horizontales desde X hasta -1. Por su parte, el teorema 4.24 nos asegura que $\zeta'(s)/\zeta(s) = O(\log^2|\tau|)$ sobre el resto de dichos lados. Así pues, sobre el lado izquierdo tenemos que

$$\left|\frac{1}{2\pi i}\int_{-X-Ti}^{-X+Ti} \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds\right| \leq \frac{2Tc\log|X+iT|x^{-X+1}}{2\pi X^2} \leq \frac{cX\log(3X)}{X^2},$$

mientras que, sobre cada lado horizontal:

$$\left|\frac{1}{2\pi i}\int_{-X\pm Ti}^{-1\pm Ti} \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds\right| \leq \frac{cX\log|X+iT|}{2\pi T^2} \leq \frac{cX\log(3X)}{X^2},$$

$$\left|\frac{1}{2\pi i}\int_{-1\pm Ti}^{2\pm Ti} \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds\right| \leq \frac{3c\log^2 T\, x^3}{2\pi T^2} \leq \frac{c\log^2(2X)x^3}{X^2}.$$

Todas las cotas tienden a 0 cuando X tiende a $+\infty$, luego la integral sobre R tiende a la integral sobre la recta $\sigma = 2$, que por el teorema anterior es $\psi_1(x)$. El teorema de los residuos nos da entonces que

$$\psi_1(x) = -\operatorname{Res}(f,-1) - \operatorname{Res}(f,0) - \operatorname{Res}(f,1) - \sum_\rho \operatorname{Res}(f,\rho) - \sum_{n=1}^{\infty}\operatorname{Res}(f,-2n),$$

donde $f(s)$ es el integrando. Sólo falta calcular los residuos:

- Como x^{s+1}/s toma el valor -1 en $s=-1$, es claro que

$$\operatorname{Res}(f,-1) = -\frac{\zeta'(-1)}{\zeta(-1)}.$$

- Como $x^{s+1}/(s+1)$ toma el valor x en $s=0$, concluimos que

$$\operatorname{Res}(f,0) = x\frac{\zeta'(0)}{\zeta(0)} = x\log 2\pi$$

(está calculado tras el teorema 4.16).

- Como $x^{s+1}/s(s+1)$ toma el valor $x^2/2$ en $s=1$ y la derivada logarítmica $\zeta'(s)/\zeta(s)$ tiene residuo -1 (por el teorema [VC 3.20]), llegamos a que

$$\operatorname{Res}(f,1) = -x^2/2.$$

- En un cero no trivial ρ, el residuo de la derivada logarítmica es su multiplicidad, luego

$$\operatorname{Res}(f,\rho) = \frac{x^{\rho+1}}{\rho(\rho+1)} o(\zeta,\rho).$$

- Análogamente,

$$\operatorname{Res}(f,-2n) = \frac{x^{-2n+1}}{2n(2n-1)}.$$

Al poner estos valores en la expresión que hemos obtenido para ψ_1 resulta la fórmula explícita. Notemos que $o(\zeta,\rho)$ desaparece por el convenio de que ρ recorre los ceros no triviales repetidos según su multiplicidad. ∎

La fórmula explícita para ψ_0 La prueba del teorema 5.1 es más delicada. Conviene probar una versión aproximada con sumas finitas:

Teorema 5.5 *Si $x \geq 2$ y $T \geq 2$, se cumple que*

$$\psi_0(x) = x - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right)$$

$$+O\Big(\frac{x\log^2(xT)}{T} + \min\{1, \frac{x}{T\langle x\rangle}\}\log x\Big),$$

donde $\langle x\rangle > 0$ representa la distancia de x a la potencia de primo más próxima.

De aquí se obtiene 5.1 sin más que hacer que T tienda a $+\infty$. Necesitamos una variante de 5.3:

Teorema 5.6 *Sea*

$$I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds, \qquad \delta(y) = \begin{cases} 0 & \text{si } 0<y<1,\\ \frac{1}{2} & \text{si } y=1,\\ 1 & \text{si } y>1.\end{cases}$$

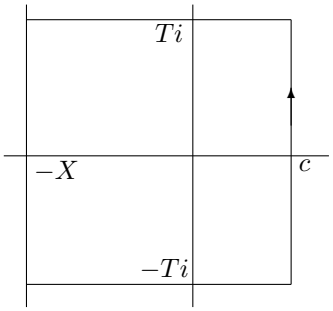
Entonces, para todo $y>0$, $c>0$, $T>0$, se cumple que

$$|I(y,T)-\delta(y)| < \begin{cases} y^c \min\{1, \frac{1}{\pi T|\log y|}\} & \text{si } y\neq 1,\\ \frac{c}{\pi T} & \text{si } y=1.\end{cases}$$

En particular tenemos que

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} \frac{y^s}{s}\,ds = \begin{cases} 0 & \text{si } 0<y<1,\\ \frac{1}{2} & \text{so } y=1,\\ 1 & \text{si } y>1,\end{cases}$$

pero con la precaución de que si $y = 1$ la función no es integrable, de modo que lo que hemos calculado es sólo su valor principal (la integral de c a $c + \infty i$ sería infinita, y la integral completa sale finita porque las partes imaginarias para $u > 0$ se cancelan con las partes imaginarias correspondientes para $u < 0$). Precisamente por esto es mejor no trabajar con la integral infinita, sino hacerlo en todo momento con integrales en segmentos finitos.



DEMOSTRACIÓN: Supongamos en primer lugar que $y > 1$ y consideremos el rectángulo R que muestra la figura, para $X > 0$. El teorema de los residuos implica que

$$\frac{1}{2\pi i}\int_R \frac{y^s}{s}\,ds = 1.$$

Observemos que

$$\left|\frac{1}{2\pi i}\int_{-X+iT}^{-X-iT} \frac{y^s}{s}\,ds\right| \le \frac{Ty^{-X}}{\pi X} < \frac{T}{\pi X},$$

$$\left|\frac{1}{2\pi i}\int_{-X-iT}^{c-iT} \frac{y^s}{s}\,ds\right| = \left|\frac{1}{2\pi i}\int_{-X}^{c} \frac{y^{u-iT}}{u-iT}\,du\right|$$

$$\le \frac{1}{2\pi}\int_{-X}^{c} \frac{y^u}{T}\,du = \frac{1}{2\pi T\log y}(y^c - y^{-X}),$$

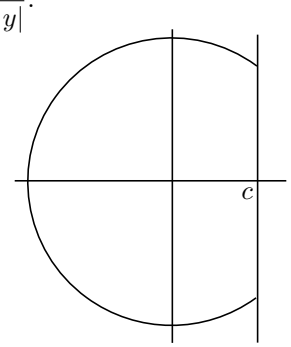
e igualmente

$$\left|\frac{1}{2\pi i}\int_{c+iT}^{-X+iT} \frac{y^s}{s}\,ds\right| \le \frac{1}{2\pi T\log y}(y^c - y^{-X}).$$

Por lo tanto, haciendo tender X a $+\infty$ resulta que

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds - 1\right| \le \frac{y^c}{\pi T|\log y|}.$$

Falta probar que y^c también es una cota. Para ello es mejor considerar el arco de circunferencia C de centro 0 que une $c+iT$ con $c-iT$ y que está a la izquierda de la recta $\sigma = c$. Así



$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds = 1 - \frac{1}{2\pi i}\int_C \frac{y^s}{s}\,ds,$$

luego

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds - 1\right| \le \frac{1}{2\pi}2\pi\sqrt{c^2+T^2}\,\frac{y^c}{\sqrt{c^2+T^2}} = y^c.$$

El caso $y < 1$ es totalmente análogo, aunque ahora tomamos el rectángulo y el arco de circunferencia a la derecha de la recta $\sigma = c$, con lo que los arcos cerrados sobre los que integramos no encierran el polo del integrando y la integral es nula. Por último, si $y = 1$ la integral se reduce a

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{1}{s}\,ds = \frac{1}{2\pi i}\int_{-T}^{T}\frac{i}{c+iu}\,du = \frac{1}{2\pi}\int_{-T}^{T}\frac{c-iu}{c^2+u^2}\,du$$

$$= \frac{1}{\pi}\int_0^T \frac{c}{c^2+u^2}\,du = \frac{1}{\pi}\int_0^{T/c}\frac{1}{1+v^2}\,dv = \frac{1}{2} - \frac{1}{\pi}\int_{T/c}^{+\infty}\frac{1}{1+v^2}\,dv,$$

luego

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{1}{s}\,ds - \frac{1}{2}\right| \le \frac{1}{\pi}\int_{T/c}^{+\infty}\frac{1}{1+v^2}\,dv < \frac{1}{\pi}\int_{T/c}^{+\infty}\frac{1}{v^2}\,dv = \frac{c}{\pi T}.$$

■

Ahora definimos

$$J(x,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds.$$

Teorema 5.7 *Si $x > 0$, $c > 1$ y $T > 0$, se cumple que*

$$|J(x,T) - \psi_0(x)| < \sum_{n=1(\neq x)}^{\infty}\Lambda(n)(x/n)^c \min\{1, \frac{1}{T|\log(x/n)|}\} + \frac{c}{T}\Lambda(x),$$

donde definimos $\Lambda(x) = 0$ cuando x no es una potencia de primo.

Demostración: Tenemos que

$$J(x,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\frac{x^s}{s}\,ds = \sum_{n=1}^{\infty}\Lambda(n)\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{(x/n)^s}{s}\,ds,$$

donde el cambio entre la integral y el sumatorio es correcto porque la serie converge uniformemente en la imagen del segmento sobre el que se extiende la integral. Ahora observamos que, con la notación del teorema anterior,

$$\psi_0(x) = \sum_{n=1}^{\infty}\Lambda(n)\delta(x/n),$$

luego, aplicando dicho teorema,

$$|J(x,T) - \psi_0(x)| \le \sum_{n=1}^{\infty}\Lambda(n)\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{(x/n)^s}{s}\,ds - \delta(x/n)\right|$$

$$\le \sum_{n=1(\neq x)}^{\infty}\Lambda(n)(x/n)^c \min\{1, \frac{1}{T|\log(x/n)|}\} + \frac{c}{T}\Lambda(x),$$

(donde hemos eliminado π de los denominadores). ■

De aquí obtenemos la estimación siguiente:

Teorema 5.8 *Si $x \geq 2$, $1 < c < 3$ y $T > 0$, se cumple que*

$$|J(x,T) - \psi_0(x)| = O(\frac{x^c}{T(c-1)} + \frac{x\log^2 x}{T} + \min\{1, \frac{x}{T\,\langle x\rangle}\}\log x).$$

Demostración: Observemos en primer lugar que[2]

$$\frac{c}{T}\Lambda(x) \leq \frac{3\log x}{T} \leq \frac{Ax\log^2 x}{T},$$

pues si $\Lambda(x) \neq 0$, es que $x = p^k$ y $\Lambda(x) = \log p \leq \log x$.

Ahora vamos a descomponer en varios sumandos la serie que aparece en el enunciado del teorema anterior. Para todo T suficientemente grande, tenemos que

$$\sum_{n\leq(3/4)x} \Lambda(n)(x/n)^c \min\{1, \frac{1}{T|\log(x/n)|}\} \leq x^c \sum_{n\leq(3/4)x} \frac{\Lambda(n)}{n^c} \min\{1, \frac{1}{T\log(4/3)}\}$$

$$\leq \frac{x^c}{T\log(4/3)} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^c} = -\frac{x^c}{T\log(4/3)} \frac{\zeta'(c)}{\zeta(c)} \leq \frac{Ax^c}{T(c-1)},$$

donde en la última desigualdad usamos que

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} + f(s) = \frac{1+(s-1)f(s)}{s-1} \leq \frac{A}{s-1},$$

donde $f(s)$ es una función holomorfa en un entorno del intervalo $[1,3]$, por lo que $1+(s-1)f(s)$ está acotada superiormente en dicho intervalo.

Similarmente, si $n \geq (5/4)x$ tenemos que $|\log(x/n)| \geq |\log(4/5)|$, y llegamos a la misma conclusión.

A continuación consideramos los sumandos para los que $(3/4)x < n < x$. Si x_1 es la mayor potencia de primo menor que x, podemos suponer que se cumple $(3/4)x < x_1 < x$, pues en caso contrario todos los sumandos indicados son nulos. Para $n = x_1$ tenemos que

$$\log(x/n) = -\log\left(1 - \frac{x-x_1}{x}\right) \geq \frac{x-x_1}{x},$$

luego el sumando correspondiente en la serie es

$$\Lambda(n)(x/n)^c \min\{1, \frac{1}{T|\log(x/n)|}\} \leq \Lambda(x_1)(4/3)^3 \min\{1, \frac{x}{T(x-x_1)}\}$$

$$= A\min\{1, \frac{x}{T\,\langle x\rangle}\}\log x$$

(pues $x_1 = p^k$ y $\Lambda(x_1) = \log p \leq \log x_1 < \log x$).

[2]Como en este contexto la c tiene un significado concreto, en lo sucesivo usaremos la letra A para representar constantes arbitrarias, no necesariamente la misma en cada aparición.

Los demás sumandos no nulos corresponden a índices de la forma $n = x_1 - m$, con $0 < m < x/4$ (pues $x_1 - m > (3/4)x$, luego $m < x_1 - (3/4)x < x/4$). Por lo tanto

$$\log(x/n) > \log(x_1/n) = -\log(1 - m/x_1) \geq m/x_1,$$

luego

$$\sum_{(3/4)x<n<x_1} \Lambda(n)(x/n)^c \operatorname{mín}\{1, \frac{1}{T|\log(x/n)|}\} \leq$$

$$\sum_{0<m<x/4} \Lambda(x_1 - m)(4/3)^3 \frac{x_1}{Tm} \leq \frac{(4/3)^3 x_1 \log x}{T} \sum_{0<m<x/4} \frac{1}{m} \leq \frac{Ax \log^2 x}{T},$$

donde hemos usado que

$$\lim_{x\to+\infty} \frac{\sum\limits_{m\leq x} \frac{1}{m}}{\log x} = 1.$$

Finalmente consideramos los términos para $x < n < (5/4)x$, para lo cual llamamos x_2 a la menor potencia de primo mayor que x, y podemos suponer que $x < x_2 < (5/4)x$, o de lo contrario todos los términos son nulos. Para $n = x_2$ tenemos que

$$|\log(x/n)| = -\log\left(1 - \frac{x_2 - x}{x_2}\right) \geq \frac{x_2 - x}{x_2},$$

luego el sumando correspondiente en la serie es

$$\Lambda(n)(x/n)^c \operatorname{mín}\{1, \frac{1}{T|\log(x/n)|}\} \leq \Lambda(x_2) \operatorname{mín}\{1, \frac{x}{T(x_2 - x)}\}$$

$$= A \operatorname{mín}\{1, \frac{x}{T\langle x\rangle}\} \log x.$$

Los demás términos corresponden a índices $n = x_2 + m$, con $0 < m < x/4$, luego

$$|\log(x/n)| = -\log(x/n) > -\log(x_2/n) = -\log\left(-\frac{m}{x_2 + m}\right) \geq \frac{m}{x_2 + m}.$$

Por lo tanto,

$$|\log(x/n)|^{-1} \leq \frac{x_2 + m}{m} \leq \frac{2x + x/4}{m} \leq \frac{Ax}{m},$$

donde hemos usado el postulado de Bertrand 3.9, que nos asegura que existe un primo (luego una potencia de primo) $\leq 2x$. A su vez,

$$\sum_{x_2<n<(5/4)x} \Lambda(n)(x/n)^c \operatorname{mín}\{1, \frac{1}{T|\log(x/n)|}\} \leq$$

$$\sum_{0<m<x/4} \Lambda(x_1 + m) \frac{Ax}{Tm} \leq \frac{Ax \log x}{T} \sum_{0<m<x/4} \frac{1}{m} \leq \frac{Ax \log^2 x}{T}.$$

Reuniendo todas las cotas que hemos obtenido, tenemos la conclusión buscada. ∎

La conclusión se simplifica si elegimos c adecuadamente:

Teorema 5.9 *Si $x \geq 2$ y $T > 0$, tomando $c = 1 + \log^{-1} x$ se cumple que*

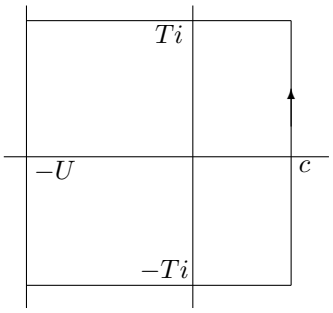
$$|J(x,T) - \psi_0(x)| = O(\frac{x \log^2 x}{T} + \text{mín}\{1, \frac{x}{T\,\langle x\rangle}\} \log x).$$

DEMOSTRACIÓN: Basta observar que

$$\frac{x^c}{T(c-1)} = \frac{e^{\log x+1} \log x}{T} = \frac{ex \log x}{T} \leq \frac{Ax \log^2 x}{T}.$$

■

En lo sucesivo supondremos que $J(x,T)$ se calcula con $c = 1 + \log^{-1} x$. Sea U un número natural impar y consideremos el rectángulo indicado en la figura. Suponemos además que T no es la parte imaginaria de ningún cero de la función dseta. Entonces, los polos del integrando de $J(x,T)$ contenidos en el rectángulo son los ceros no triviales que cumplen $|\operatorname{Im}\rho| < T$, los enteros pares $-U < 2m \leq 0$ y el 1. Vamos a calcular los residuos correspondientes:



- En $s = 1$ tenemos que $-\frac{\zeta'(s)}{\zeta(s)}$ tiene residuo 1 y y $x^1/1 = x$, luego el residuo del producto es x.
- En $s = 0$ tenemos que x^s/s tiene residuo 1, luego el residuo del producto es $-\frac{\zeta'(0)}{\zeta(0)} = -\log 2\pi$.
- En un cero no trivial ρ de la función dseta, el residuo de $\zeta'(s)/\zeta(s)$ es $o(\zeta,\rho)$, luego el del producto es $-o(\zeta,\rho)x^\rho/\rho$.
- En $s = -2m$ el residuo de $\zeta'(s)/\zeta(s)$ es 1.

Por consiguiente, la suma de los residuos es

$$x - \log 2\pi - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} - \frac{1}{2} \sum_{0<2m<U} \frac{x^{-2m}}{m},$$

donde estamos adoptando el convenio habitual de que en las sumas respecto de ρ cada cero se repite $o(\zeta,\rho)$ veces. El teorema de los residuos nos da entonces que

$$J(x,T) = \frac{1}{2\pi i} \int_\gamma -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s}\, ds + x - \log 2\pi - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} - \frac{1}{2} \sum_{0<2m<U} \frac{x^{-2m}}{m},$$

donde γ es la poligonal de vértices $c - iT$, $-U - iT$, $-U + iT$, $c + iT$. Notemos que, si U tiende a infinito, la última suma converge a

$$\sum_{m=1}^{\infty} \frac{(x^{-2})^m}{m} = \log(1 - x^{-2}).$$

Falta estudiar el límite de la integral cuando U a infinito. Empezamos con la integral sobre los segmentos horizontales. Hasta aquí hemos supuesto únicamente que T no era la parte imaginaria de un cero de dseta. Ahora vamos a suponer, más concretamente, que T cumple la condición del teorema 4.24. Esto nos asegura que en los dos segmentos horizontales, para $-1 \le \sigma \le 2$, se cumple que

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log^2 T).$$

Usando esto y 4.22, así como que la función $(\log u)/u$ es decreciente para $u > e$, obtenemos que

$$\left|\int_{-U}^{-1} -\frac{\zeta'(\sigma+iT)}{\zeta(\sigma+iT)}\frac{x^{\sigma+iT}}{\sigma+iT}\,d\sigma + \int_{-1}^{c} -\frac{\zeta'(\sigma+iT)}{\zeta(\sigma+iT)}\frac{x^{\sigma+iT}}{\sigma+iT}\,d\sigma\right| \le$$

$$A\int_{-U}^{-1}\frac{\log|\sigma+iT|x^\sigma}{|\sigma+iT|}\,d\sigma + A\int_{-1}^{c}\frac{\log^2 T\, x^\sigma}{T}\,d\sigma \le$$

$$A\int_{-U}^{-1}\frac{\log T\, x^\sigma}{T}\,d\sigma + A\int_{-1}^{c}\frac{\log^2 T\, x^\sigma}{T}\,d\sigma \le \frac{A\log T}{T}\frac{x^{-1}}{\log x} + \frac{A\log^2 T}{T}\frac{x^{1+\log^{-1}x}}{\log x}$$

$$\le \frac{A\log T}{Tx\log x} + \frac{Aex\log^2 T}{T\log x} = O(\frac{x\log^2 T}{T\log x}).$$

La misma estimación vale para la integral sobre el segmento inferior de γ. Para el segmento vertical, usando de nuevo 4.22 (y ahora es esencial que U es un número impar), tenemos que

$$\left|\int_{-T}^{T} -\frac{\zeta'(-U+i\tau)}{\zeta(-U+i\tau)}\frac{x^{-U+i\tau}}{-U+i\tau} i\,d\tau\right| \le \frac{2AT\log U}{Ux^U}.$$

Esto tiende a 0 cuando U tiende a infinito, luego concluimos que

$$J(x,T) = x - \sum_{|\operatorname{Im}\rho|<T}\frac{x^\rho}{\rho} - \frac{1}{2}\log(1-x^{-2}) + O(\frac{x\log^2 T}{\log x}).$$

Uniendo esto a 5.9 obtenemos la fórmula del teorema 5.5, pues

$$\frac{x\log^2 x}{T} + \frac{x\log^2 T}{T\log x} = O(\frac{x\log^2(xT)}{T}).$$

En realidad la prueba no está concluida, pues sólo hemos probado 5.5 bajo el supuesto de que T cumple la condición del teorema 4.24. Ahora bien, dicho teorema prueba que, dado un $T \ge 3$, existe un $T < T' < T+1$ que cumple la condición y, por consiguiente, cumple 5.5. Esto añade al sumatorio una cantidad de sumandos (de la forma x^ρ/ρ, con repeticiones según el orden de ρ) acotada por $A\log T$ y, por otra parte, cada sumando nuevo cumple

$$\left|\frac{x^\rho}{\rho}\right| = \frac{x^{\operatorname{Re}\rho}}{|\operatorname{Im}\rho|} \le \frac{x}{T},$$

luego el módulo de los sumandos añadidos al pasar de T a T' es $O(x\log T/T)$, luego también $O(\frac{x\log^2(xT)}{T})$, y puede incluirse en el término final de la fórmula de 5.5. ∎

En la sección siguiente mostraremos algunas aplicaciones de los resultados que hemos obtenido aquí.

5.2 Estimación del error en el teorema de los números primos

El teorema de los números primos afirma que la integral logarítmica $\mathrm{Il}(x)$ aproxima a la función $\pi(x)$, de modo que el error relativo de la aproximación tiende a 0. No obstante, el error absoluto $\mathrm{Il}(x)-\pi(x)$ tiende a ∞, y ahora nos vamos a ocupar de estimarlo. El problema está estrechamente relacionado con la estimación del error absoluto de las equivalencias asintóticas $\vartheta(x)\sim x$ y $\psi(x)\sim x$ de las funciones de Chebishev. Naturalmente, de la propia definición de equivalencia asintótica entre dos funciones se sigue que el error absoluto de la aproximación es del orden de cualquiera de ellas. Por ejemplo:

$$\pi(x)-\frac{x}{\log x}=O(\frac{x}{\log x}),\qquad \pi(x)-\mathrm{Il}(x)=O(\mathrm{Il}(x))=O(\frac{x}{\log x}).$$

Nuestro propósito es encontrar estimaciones con funciones de orden menor. Empezamos mostrando algunas relaciones elementales entre estos tres errores absolutos. Para relacionar ψ con π consideraremos también la función π^* definida en 2.15.

Teorema 5.10 *Se cumplen las relaciones siguientes:*

1. $\psi(x)-x=\vartheta(x)-x+O(x^{1/2}\log^2 x)$.
2. $\pi^*(x)-\pi(x)=O(x^{1/2})$.
3. $\pi^*(x)-\mathrm{Il}(x)=\dfrac{\psi(x)-x}{\log x}+\dfrac{2}{\log 2}+\displaystyle\int_2^x\frac{\psi(t)-t}{t\log^2 t}\,dt$.
4. $\vartheta(x)-x=(\pi(x)-\mathrm{Il}(x))\log x-\displaystyle\int_2^x\frac{\pi(t)-\mathrm{Il}(t)}{t}\,dt-2$.

Demostración: 1) es consecuencia inmediata de (3.3).

2) Claramente

$$\pi^*(x)-\pi(x)=\sum_{m=2}^{M}\frac{\pi(x^{1/m})}{m},$$

donde $M=E[\log x/\log 2]$ y, por el teorema de los números primos,

$$\pi(x^{1/m})\le c\frac{mx^{1/m}}{\log x}.$$

Por lo tanto,

$$\pi^*(x) - \pi(x) \le cx^{1/2} + cMx^{1/3} \le cx^{1/2} + cx^{1/3}\log x = O(x^{1/2}).$$

3) Sumando por partes (teorema 2.20):

$$\pi^*(x) = \sum_{n\le x} \frac{\Lambda(n)}{\log n} = \frac{\psi(x)}{\log x} + \int_2^x \frac{\psi(t)}{t\log^2 t}\,dt.$$

Integramos también por partes la integral que define a $\mathrm{Il}(x)$:

$$\mathrm{Il}(x) = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{t\,dt}{t\log^2 t}.$$

Restando ambas expresiones tenemos la igualdad buscada.

4) Sumamos por partes:

$$\vartheta(x) = \sum_{p\le x} \log p = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt$$

$$= \pi(x)\log x - \int_2^x \frac{\pi(t) - \mathrm{Il}(t)}{t}\,dt - \int_2^x \frac{\mathrm{Il}(t)}{t}\,dt.$$

Integrando por partes:

$$\int_2^x \frac{\mathrm{Il}(t)}{t}\,dt = \mathrm{Il}(x)\log x - x + 2,$$

y al sustituir esta expresión en la igualdad anterior obtenemos la fórmula requerida. ∎

Ahora podemos probar:

Teorema 5.11 *Si $0 < \alpha \le 1$, las afirmaciones siguientes son equivalentes:*

1. $\psi(x) - x = O(x^\alpha \log^2 x)$.
2. $\pi(x) - \mathrm{Il}(x) = O(x^\alpha \log x)$.
3. *Para todo $\epsilon > 0$, se cumple que* $\pi(x) - \mathrm{Il}(x) = O(x^{\alpha+\epsilon})$.
4. *Para todo $\epsilon > 0$, se cumple que* $\vartheta(x) - x = O(x^{\alpha+\epsilon})$.
5. *Para todo $\epsilon > 0$, se cumple que* $\psi(x) - x = O(x^{\alpha+\epsilon})$.
6. *Todo cero de la función dseta cumple* $\mathrm{Re}\,\rho \le \alpha$.

DEMOSTRACIÓN: Podemos suponer que $\alpha < 1$, porque todas las afirmaciones son ciertas cuando $\alpha = 1$. Por ejemplo, 2) se cumple, porque, de hecho, $\pi(x) - \mathrm{Il}(x) = o(x)$. En efecto,

$$\frac{\pi(x) - \mathrm{Il}(x)}{x} = \left(\frac{\pi(x)\log x}{x} + \frac{\mathrm{Il}(x)\log x}{x}\right)\frac{1}{\log x} \to 0,$$

por el teorema de los números primos y 3.1.

1) $\Rightarrow$ 2) Probaremos esta implicación bajo la hipótesis adicional de que $\alpha \geq 1/2$. Discutiremos el caso pendiente tras haber probado las demás implicaciones. Usamos los apartados 2) y 3) del teorema anterior:

$$\begin{aligned} |\pi(x) - \mathrm{Il}(x)| &\leq \left|\frac{\psi(x) - x}{\log x}\right| + \frac{2}{\log 2} + \int_2^x \frac{|\psi(t) - t|}{t\log^2 t}\,dt + cx^{1/2} \\ &\leq cx^\alpha \log x + c + c\int_2^x t^{\alpha-1}\,dt + cx^{1/2} \\ &\leq cx^\alpha \log x + c + \frac{x^\alpha}{\alpha} + cx^{1/2} = O(x^\alpha \log x). \end{aligned}$$

2) $\Rightarrow$ 3) es trivial.

3) $\Rightarrow$ 4) Usamos el apartado 4) del teorema anterior:

$$\begin{aligned} |\vartheta(x) - x| &\leq cx^{\alpha+\epsilon}\log x + c\int_2^x \frac{t^{\alpha+\epsilon}}{t}\,dt + 2 \\ &= cx^{\alpha+\epsilon}\log x + \frac{c}{\alpha+\epsilon}(x^{\alpha+\epsilon} - 2^{\alpha+\epsilon}) + 2, \end{aligned}$$

de donde $\vartheta(x) - x = O(x^{\alpha+2\epsilon})$.

4) $\Rightarrow$ 5) Usamos el apartado 1) del teorema anterior:

$$\frac{|\psi(x) - x|}{x^{\alpha+\epsilon}} \leq \frac{|\vartheta(x) - x|}{x^{\alpha+\epsilon}} + O(\frac{\log^2 x}{x^\epsilon}),$$

luego $\psi(x) - x = O(x^{\alpha+\epsilon})$.

5) $\Rightarrow$ 6) Supongamos que $\psi(x) - x = O(x^\alpha)$. Por el teorema 2.20, tenemos que

$$\sum_{n\leq x}\frac{\Lambda(n)}{n^s} = \sum_{n\leq x-1}\psi(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{\psi(x)}{E[x]^s},$$

$$\sum_{n\leq x}\frac{1}{n^s} = \sum_{n\leq x-1} n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{E[x]}{E[x]^s},$$

y los restos

$$\left|\frac{\psi(x)}{E[x]^s}\right| = \frac{\psi(x)/x}{x^{\sigma-1}}\left(\frac{x}{E[x]}\right)^\sigma, \qquad \left|\frac{E[x]}{E[x]^s}\right| = \frac{1}{E[x]^{\sigma-1}}$$

convergen a 0 en el semiplano $\sigma > 1$. Por lo tanto

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{n=1}^{\infty} \psi(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)$$

$$= \sum_{n=1}^{\infty} (\psi(n) - n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \sum_{n=1}^{\infty} n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)$$

$$= \sum_{n=1}^{\infty} (\psi(n) - n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \zeta(s). \tag{5.1}$$

Por el teorema del valor medio, existe $n < t < n+1$ tal que

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| = \left|\frac{1}{t^{s+1}}\right| \leq \frac{1}{n^{\sigma+1}}.$$

Por consiguiente

$$\left|(\psi(n) - n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \leq \frac{cn^\alpha}{n^{\sigma+1}} = \frac{c}{n^{\sigma-\alpha+1}},$$

luego la serie de (5.1) converge casi uniformemente en el semiplano $\sigma > \alpha$ a una función holomorfa. Concluimos que $\zeta'(s)/\zeta(s)$ es holomorfa en dicho semiplano salvo por un polo en $s = 1$. Esto implica que $\zeta(s)$ no tiene ceros en dicho semiplano o, equivalentemente, que todo cero cumple $\operatorname{Re}\rho \leq \alpha$.

Si la hipótesis no es sobre α, sino sobre $\alpha + \epsilon$, para todo $\epsilon > 0$, la conclusión es que $\operatorname{Re}\rho \leq \alpha + \epsilon$ para todo $\epsilon > 0$, pero esto implica igualmente que $\operatorname{Re}\rho \leq \alpha$.

6) $\Rightarrow$ 1) No perdemos generalidad si suponemos que x toma sólo valores naturales, pues, si se cumple en este caso y x es arbitrario,

$$|\psi(x) - x| = |\psi(E[x])) - E[x]| + |E[x] - x| \leq cE[x]^\alpha \log^2 E[x] + 1 \leq cx^\alpha \log^2 x.$$

También podemos suponer que $x \geq 2$. Para $T \geq 2$, el teorema 5.5 nos da que

$$\psi_0(x) = x - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)$$

$$+O\left(\frac{x\log^2(xT)}{T} + \min\{1, \frac{x}{T\langle x\rangle}\}\log x\right),$$

Al suponer que x es entero resulta que $\langle x\rangle \geq 1$, luego

$$O\left(\frac{x\log^2(xT)}{T} + \min\{1, \frac{x}{T\langle x\rangle}\}\log x\right) = O\left(\frac{x\log^2(xT)}{T} + \frac{x\log x}{T}\right) = O\left(\frac{x\log^2(xT)}{T}\right).$$

Por otro lado, $|x^\rho| = x^{\operatorname{Re}\rho} \leq x^\alpha$, luego, usando el teorema 4.21,

$$\sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} \leq x^\alpha \sum_{|\operatorname{Im}\rho|<T} \frac{1}{|\operatorname{Im}\rho|} \leq 2x^\alpha \sum_{0<\operatorname{Im}\rho<T} \frac{1}{\operatorname{Im}\rho} = O(x^\alpha \log^2 T).$$

Así pues,

$$\psi_0(x) = x + O(x^\alpha \log^2 T + \frac{x \log^2(xT)}{T}).$$

Tomamos concretamente $T = x^{1-\alpha}$, y así

$$\psi_0(x) = x + O(x^\alpha \log^2 x + x^\alpha \log^2 x) = x + O(x^\alpha \log^2 x).$$

Por último observamos que $\psi(x) = \psi_0(x) + \frac{1}{2}\Lambda(x) \leq \psi_0(x) + \frac{1}{2}\log x$, luego también $\psi(x) = x + O(x^\alpha \log^2 x)$.

Sólo falta probar 1) $\Rightarrow$ 2) cuando $\alpha < 1/2$, pero, si suponemos 1), tenemos trivialmente 5), luego también 6), que es claramente imposible para $\alpha < 1/2$, luego ese caso es imposible. ∎

Definición 5.12 Llamamos Θ al ínfimo de los números reales α que cumplen cualquiera de las afirmaciones de teorema anterior.

La afirmación 6) implica que el ínfimo es, de hecho, un mínimo, de modo que Θ cumple todas las afirmaciones del teorema anterior. Obviamente tenemos que $1/2 \leq \Theta \leq 1$ y la hipótesis de Riemann equivale a $\Theta = 1/2$.

En particular, ahora vemos que la hipótesis de Riemann es equivalente a la estimación

$$\pi(x) - \mathrm{li}(x) = O(\sqrt{x}\,\log x). \tag{5.2}$$

Como ya hemos señalado, la hipótesis de Riemann no está demostrada ni refutada, por lo que tal vez el lector se pregunte qué cotas superiores se conocen para Θ. La respuesta es decepcionante: nadie ha logrado probar hasta el momento que se cumpla $\Theta < 1$, por lo que el teorema anterior no proporciona ninguna estimación razonable (demostrable) del error absoluto en la equivalencia asintótica del teorema de los números primos.

Sucede que, aunque no se sepa probar que no hay ceros no triviales con parte real tan próxima a 1 como se quiera, sí se puede probar que, cuanto más próxima a 1 sea la parte real de un hipotético cero, mayor tiene que ser su parte imaginaria, y esto basta para obtener versiones del teorema de los números primos que incluyan una estimación del error.

Veamos un ejemplo sencillo de región libre de ceros:

Teorema 5.13 *Existe una constante $c > 0$ tal que no existen ceros de la función dseta en la región*

$$1 - \frac{c}{\log(|\tau| + 2)} \leq \sigma.$$

Demostración: Como en la prueba de 3.36, nos apoyaremos en la desigualdad elemental

$$3 + 4\cos\theta + \cos 2\theta \geq 0,$$

pero ahora, en lugar de $\log|\zeta(s)|$, consideraremos la derivada logarítmica de la función dseta, que para $\sigma > 1$ admite el desarrollo

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

Por lo tanto,

$$-\operatorname{Re}\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}\cos(\tau\log n).$$

Y en consecuencia

$$-3\frac{\zeta'(\sigma)}{\zeta(\sigma)} - 4\operatorname{Re}\frac{\zeta'(\sigma+\tau i)}{\zeta(\sigma+\tau i)} - \operatorname{Re}\frac{\zeta'(\sigma+2\tau i)}{\zeta(\sigma+2\tau i)} \geq 0. \tag{5.3}$$

Como $-\zeta'(s)/\zeta(s)$ tiene un polo simple en 1 con residuo 1, se cumple que

$$-\frac{\zeta'(\sigma)}{\zeta(\sigma)} \leq \frac{1}{\sigma-1} + O(1).$$

Combinando dos igualdades obtenidas en la prueba del teorema 4.16 tenemos que

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{2}\frac{\Pi'(s/2)}{\Pi(s/2)} + \frac{1}{s-1} - \sum_\rho\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right) + c$$

En la prueba del teorema 4.22 hemos visto que

$$\frac{\Pi'(s/2)}{\Pi(s/2)} = \log\frac{s}{2} + \frac{1}{s} + O(1/\sigma),$$

luego, si $1 \leq \sigma \leq 2$, $\tau \geq 2$,

$$\left|\frac{\Pi'(s/2)}{\Pi(s/2)}\right| \leq \log|s/2| + \pi/2 + 1 + O(1) = O(\log\tau).$$

Así pues,

$$-\operatorname{Re}\frac{\zeta'(s)}{\zeta(s)} = -\sum_\rho \operatorname{Re}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right) + O(\log\tau).$$

Los términos de la serie son no negativos, pues si $\rho = \beta + \gamma i$,

$$\operatorname{Re}\frac{1}{s-\rho} = \frac{\sigma-\beta}{|s-\rho|^2} \geq 0, \qquad \operatorname{Re}\frac{1}{\rho} = \frac{\beta}{|\rho|^2} \geq 0.$$

Por lo tanto,

$$-\operatorname{Re}\frac{\zeta'(\sigma+2\tau i)}{\zeta(\sigma+2\tau i)} \leq O(\log\tau).$$

Fijemos ahora un cero ρ y tomemos s con $1 < \sigma \leq 2$ tal que $\tau = \operatorname{Im}\rho \geq 2$. Si eliminamos todos los términos de la suma menos el correspondiente a ρ resulta que

$$-\operatorname{Re}\frac{\zeta'(\sigma+\tau i)}{\zeta(\sigma+\tau i)} \leq -\frac{1}{\sigma-\beta} + O(\log\tau).$$

Ahora sustituimos en (5.3) las cotas que hemos obtenido, y así obtenemos que

$$0 \le \frac{3}{\sigma-1} - \frac{4}{\sigma-\beta} + O(\log\tau).$$

Así pues, existe una constante c (independiente de s o de ρ) tal que

$$\frac{4}{\sigma-\beta} \le \frac{3}{\sigma-1} + c\log\tau,$$

donde β es la parte real de un cero no trivial, τ es su parte imaginaria y σ es cualquier número real $1 < \sigma \le 2$. En realidad, si $\sigma \ge 2$ también tenemos que

$$\frac{4}{\sigma-\beta} \le \frac{4}{\sigma-1} = \frac{3}{\sigma-1} + \frac{1}{\sigma-1} \le \frac{3}{\sigma-1} + 1 \le \frac{3}{\sigma-1} + c\log\tau,$$

si tomamos $c \ge 1/\log 2$. Así pues,

$$\sigma - \beta \ge \frac{4}{3/(\sigma-1) + c\log\tau},$$

luego

$$1-\beta \ge \frac{4}{3/(\sigma-1)+c\log\tau} - (\sigma-1) = \frac{1-c(\sigma-1)\log\tau}{3/(\sigma-1)+c\log\tau}.$$

Ahora elegimos concretamente $\sigma = 1 + 1/(2c\log\tau)$, para asegurar que el numerador sea positivo. Así obtenemos que

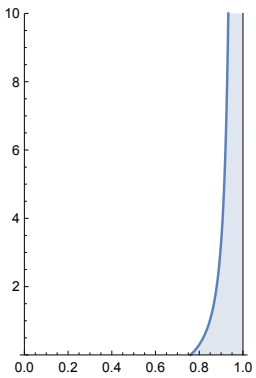
$$1-\beta \ge \frac{1/2}{5c\log\tau},$$

y esto tiene que cumplirlo la parte real de cualquier cero no trivial con parte imaginaria positiva. Cambiando la constante podemos pedir que

$$1 - \frac{c}{\log(\tau+2)} \le \beta$$

y, como los conjugados de los ceros también son ceros, lo mismo vale si $\tau < 0$, con $|\tau|$ en lugar de τ. ∎

Determinar explícitamente las constantes que aparecen en este tipo de estimaciones es una labor delicada, que a menudo requiere argumentos mucho más sofisticados que los que podemos emplear cuando no nos importa la magnitud de la constante obtenida, así como resultados computacionales (se comprueba que una propiedad se cumple para todo número mayor que una constante explícita y luego se investigan uno por uno todos los números menores para ver dónde está el primero que falla, si es que lo hay, y así se rebaja la constante hasta el último fallo). En este caso, puede probarse que sirve $c = 1/6$, lo que nos da la región que muestra la gráfica.



De aquí a su vez obtenemos una estimación del error en la aproximación del teorema de los números primos. La formulamos primero en términos de la función ψ.

Teorema 5.14 *Existe una constante $c > 0$ tal que $\psi(x) = x + O(xe^{-c\sqrt{\log x}})$.*

DEMOSTRACIÓN: No perdemos generalidad si nos restringimos al caso en que $x \geq 2$ es un número natural. Vamos a emplear la versión truncada de la fórmula explícita para $\psi_0(x)$ (teorema 5.5). Para todo $T \geq 2$ tenemos que

$$\psi_0(x) = x - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right) + R(x,T),$$

donde

$$R(x,T) = O(\frac{x\log^2(xT)}{T} + \text{mín}\{1, \frac{x}{T\langle x\rangle}\}\log x) = O(\frac{x\log^2(xT)}{T}),$$

donde la última igualdad se debe a que si x es un número natural, entonces $\langle x\rangle \geq 1$. Por el teorema anterior existe una constante tal que todo cero ρ tal que $|\operatorname{Im}\rho| \leq T$ cumple

$$\operatorname{Re}\rho < 1 - \frac{c}{\log|\operatorname{Im}\rho|} \leq 1 - \frac{c}{\log T}.$$

Por lo tanto,

$$|x^\rho| = x^{\operatorname{Re}\rho} = e^{\operatorname{Re}\rho\log x} < xe^{-\frac{c\log x}{\log T}},$$

luego, por 4.21,

$$\left|\sum_{|\operatorname{Im}\rho|<T}\frac{x^\rho}{\rho}\right| < xe^{-\frac{c\log x}{\log T}}\sum_{|\operatorname{Im}\rho|<T}\frac{1}{|\rho|} = 2xe^{-\frac{c\log x}{\log T}}\sum_{0<\operatorname{Im}\rho<T}\frac{1}{\operatorname{Im}\rho}$$

$$= O(x\log^2 Te^{-\frac{c\log x}{\log T}}).$$

Llevando todo a la fórmula explícita,

$$\psi(x) = \psi_0(x) + O(\log x) = x + O(\log x + x\log^2 Te^{-\frac{c\log x}{\log T}} + \frac{x\log^2(xT)}{T}).$$

Esto vale para todo número natural $x \geq 2$ y todo $T \geq 2$. Ahora tomamos $x \geq 3$ y $T = e^{\sqrt{\log x}} > 2$. Así obtenemos que

$$\psi(x) = x + O(\log x + x\log x\, e^{-c\sqrt{\log x}} + \frac{x(\log x + \sqrt{\log x})^2}{e^{\sqrt{\log x}}}) = x + O(xe^{-c'\sqrt{\log x}}),$$

donde c' es cualquier constante que cumpla $c' < 1$, $c' < c$. En efecto,

$$\frac{x\log x\, e^{-c\sqrt{\log x}}}{xe^{-c'\sqrt{\log x}})} = \frac{\log x}{e^{(c-c')\sqrt{\log x}}} = \frac{t}{e^{(c-c')t}} \to 0,$$

$$\frac{x(\log x + \sqrt{\log x})^2}{xe^{(1-c')\sqrt{\log x}}} = \frac{(t^2+t)^2}{e^{(1-c')t}} \to 0. \qquad \blacksquare$$

Notemos que hasta ahora sabíamos que $\psi(x)/x$ convergía a 1, pero el teorema anterior nos dice, más concretamente, que

$$\frac{\psi(x)}{x} = 1 + O(e^{-c\sqrt{\log x}}),$$

luego nos da información sobre la velocidad a que $\psi(x)/x$ se acerca a 1. Observemos también que

$$\lim_{x\to+\infty} \frac{xe^{-c\sqrt{\log x}}}{x/\log x} = 0,$$

por lo que la estimación $O(xe^{-c\sqrt{\log x}})$ que proporciona el teorema siguiente es mejor que la estimación $O(x/\log x)$ que es la que, en principio, tenemos para $\pi(x) - \mathrm{Il}(x)$.

Teorema 5.15 *Existe una constante $c > 0$ tal que*

$$\pi(x) = \mathrm{Il}(x) + O(xe^{-c\sqrt{\log x}}).$$

Demostración: Por el teorema 5.10 tenemos que

$$\vartheta(x) - x = O(xe^{-c\sqrt{\log x}} + x^{1/2}\log^2 x) = O(xe^{-c\sqrt{\log x}}),$$

de donde, a su vez, de nuevo por 5.10,

$$\pi^*(x) - \mathrm{Il}(x) = \frac{c'xe^{-c\sqrt{\log x}}}{\log x} + c' + c'\int_2^x \frac{te^{-c\sqrt{\log t}}}{t\log^2 t}dt = O(xe^{-c\sqrt{\log x}}),$$

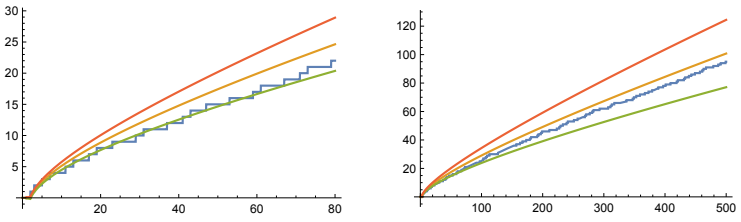
pues el integrando está acotado, luego la integral es $O(x)$. Por último

$$\pi(x) - \mathrm{Il}(x) = \pi(x) - \pi^*(x) + \pi^*(x) - \mathrm{Il}(x) = O(x^{1/2}) + O(xe^{-c\sqrt{\log x}})$$
$$= O(xe^{-c\sqrt{\log x}}). \qquad \blacksquare$$

Más adelante probaremos (véanse las observaciones tras el teorema 6.16) que, en realidad, el teorema anterior es cierto para toda constante c. La única salvedad es que, cuanto mayor sea la c que elijamos, mayor tendrá que ser también la constante implícita en O o, alternativamente, obtendremos una acotación válida únicamente para x suficientemente grande. Por ejemplo, puede probarse que

$$|\pi(x) - \mathrm{Il}(x)| < 0.1e^{-0.3\sqrt{\log x}} \qquad \text{para } x \geq 59.$$

Si aumentamos el 0.1 hasta 0.7 la desigualdad vale para todo x, pero, a cambio de incluir unos pocos números, la hacemos menos precisa para números mayores.



La figura muestra las funciones $\pi(x)$ e $\mathrm{Il}(x)$ (en el centro) y las cotas superior e inferior para $\pi(x)$ que proporciona la desigualdad anterior.

Veamos algunas aplicaciones del teorema de los números primos con la estimación del error.

Teorema 5.16 *Para todo $n \geq 0$ y todo $x > 2$, se cumple que*

$$\pi(x) = \frac{x}{\log x}\sum_{k=0}^{n}\frac{k!}{\log^k x} + O(\frac{x}{\log^{n+1} x}).$$

DEMOSTRACIÓN: La clave está en que esto es cierto si ponemos $\mathrm{Il}(x)$ en lugar de $\pi(x)$. En efecto, una simple inducción, integrando por partes, muestra que

$$\mathrm{Il}(x) = \frac{x}{\log x}\sum_{k=0}^{n}\frac{k!}{\log^k x} - \frac{2}{\log 2}\sum_{k=0}^{n}\frac{k!}{\log^k 2} + (n+1)!\int_2^x \frac{dt}{\log^{n+2} t},$$

y exactamente el mismo argumento empleado en la demostración de 3.1 prueba que

$$\lim_{x\to+\infty}\frac{\log^{n+1} x}{x}\int_2^x \frac{dt}{\log^{n+2} t} = 0.$$

Por lo tanto,

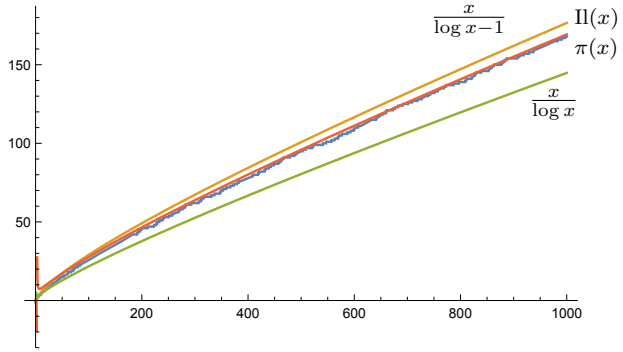
$$\pi(x) \leq \mathrm{Il}(x) + |\pi(x) - \mathrm{Il}(x)| = \frac{x}{\log x}\sum_{k=0}^{n}\frac{k!}{\log^k x} + O(\frac{x}{\log^{n+1} x}) + O(xe^{-c\sqrt{\log x}}),$$

pero

$$\lim_{x\to+\infty}\frac{xe^{-c\sqrt{\log x}}}{x/\log^{n+1} x} = \lim_{x\to+\infty}\frac{\log^{n+1} x}{e^{c\sqrt{\log x}}} = \lim_{t\to+\infty}\frac{t^{2(n+1)}}{e^{ct}} = 0,$$

luego podemos eliminar el último término de error. ∎

Una variante del teorema de los números primos Las gráficas muestran que $\mathrm{Il}(x)$ aproxima mucho mejor a $\pi(x)$ que $x/\log x$, pero la situación se puede mejorar un poco.



La figura muestra las gráficas de $\pi(x)$, $\mathrm{Il}(x)$, $x/\log x$ y también $x/(\log x - 1)$. Vemos que $\mathrm{Il}(x)$ sigue estando más cerca de $\pi(x)$ (sus gráficas se superponen), pero la función modificada $x/(\log x - 1)$ se acerca más a $\pi(x)$ que la original $x/\log x$.

Esto ya lo había observado Gauss, que conjeturó que, de entre las funciones

$$\frac{x}{\log x - a},$$

la que más se ajusta a $\pi(x)$ es la correspondiente a $a = 1$. Ahora podemos probar que tenía razón. Para ello definimos $A(x)$ como la función dada por

$$\pi(x) = \frac{x}{\log x - A(x)}$$

o, equivalentemente

$$A(x) = \log x - \frac{x}{\pi(x)}.$$

Vamos a probar que

$$A(x) = 1 + O(\frac{1}{\log x}),$$

lo que quiere decir que, cuanto mayor es x, el número que habría que restarle a $\log x$ para obtener el valor exacto de $\pi(x)$ se parece más a 1. Tenemos que

$$(A(x)-1)\log x = \log^2 x - \log x - \frac{x\log x}{\pi(x)} = \log^2 x - \log x - \frac{\log^2 x}{\pi(x)\log x/x},$$

y el teorema anterior nos proporciona la estimación

$$\frac{\pi(x)\log x}{x} = 1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + R(x), \qquad R(x) = O(\frac{1}{\log^2 x}).$$

Así,

$$\begin{aligned}(A(x)-1)\log x &= \log^2 x - \log x - \frac{\log^2 x}{1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + R(x)}\\ &= \frac{1 + \log^2 x\, R(x) - \frac{2}{\log x} - \log x\, R(x)}{1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + R(x)} \to 1.\end{aligned}$$

■

En la introducción dejamos planteado que la suma de los primos $\leq x$ es asintóticamente equivalente a $\mathrm{Il}(x^2)$. Ahora podemos demostrar este hecho, e incluso algo más general:

Teorema 5.17 *Si $k \geq 1$, se cumple que*

$$\sum_{p\leq x} p^k \sim \frac{x^{k+1}}{(k+1)\log x} \sim \mathrm{Il}(x^{k+1}).$$

Demostración: Observemos que la segunda equivalencia se sigue inmediatamente de $\mathrm{Il}(x) \sim x/\log x$ sin más que sustituir x por x^{k+1}.

Llamamos χ a la función característica del conjunto de los primos, de modo que

$$\sum_{p\leq x} p^k = \sum_{n\leq x} \chi(n) n^k = \pi(x)x^k - \int_2^x \pi(t) k t^{k-1}\, dt,$$

donde hemos aplicado el teorema 2.20 de suma por partes.

Ahora observamos que la fórmula de integración por partes nos da

$$\int_2^x \frac{t^k}{\log t}\,dt = x^k\,\mathrm{Il}(x) - \int_2^x \mathrm{Il}(t)kt^{k-1}\,dt.$$

Por lo tanto,

$$\sum_{p\le x} p^k = (\pi(x)-\mathrm{Il}(x))x^k - k\int_2^x (\pi(t)-\mathrm{Il}(t))t^{k-1}\,dt + \int_2^x \frac{t^k}{\log t}\,dt.$$

Aplicamos el cambio de variable $t = u^{1/(k+1)}$:

$$\int_2^x \frac{t^k}{\log t}\,dt = \int_{2^{k+1}}^{x^{k+1}} \frac{du}{\log u} = \int_2^{x^{k+1}} \frac{du}{\log u} - \int_2^{2^{k+1}} \frac{du}{\log u} = \mathrm{Il}(x^{k+1}) + a.$$

Así pues,

$$\sum_{p\le x} p^k - \mathrm{Il}(x^{k+1}) = (\pi(x)-\mathrm{Il}(x))x^k - k\int_2^x (\pi(t)-\mathrm{Il}(t))t^{k-1}\,dt + a.$$

Ahora aplicamos 5.15:

$$\left|\sum_{p\le x} p^k - \mathrm{Il}(x^{k+1})\right| \le c'x^{k+1}e^{-c\sqrt{\log x}} + kc'\int_2^x t^k e^{-c\sqrt{\log t}}\,dt$$

$$\le c'x^{k+1}e^{-c\sqrt{\log x}} + kc'\int_2^x t^k\,dt = c'x^{k+1}e^{-c\sqrt{\log x}} + kc'\frac{x^{k+1}}{k+1}$$

$$= O(x^{k+1}e^{-c\sqrt{\log x}}).$$

Por consiguiente,

$$\left|\frac{\sum\limits_{p\le x} p^k - \mathrm{Il}(x^{k+1})}{\mathrm{Il}(x^{k+1})}\right| \le \frac{\frac{x^{k+1}}{(k+1)\log x}}{\mathrm{Il}(x^{k+1})}\,c'\frac{x^{k+1}e^{-c\sqrt{\log x}}}{\frac{x^{k+1}}{(k+1)\log x}} \le c'\frac{\log x}{e^{c\sqrt{\log x}}},$$

pues el primer cociente de la expresión intermedia tiende a 1, luego está acotado para $x \ge 2$. Un cambio de variable $t = \sqrt{\log x}$ prueba que la última expresión también tiende a 0. ∎

5.3 Regiones sin ceros y el error en el teorema de los números primos

En la sección anterior hemos obtenido una estimación del error en la equivalencia asintótica que proporciona el teorema de los números primos a partir de un resultado que garantizaba la ausencia de ceros de la función dseta en una

pequeña región de la banda crítica. Ahora vamos a sistematizar la relación entre los resultados de ambos tipos, probando que cada resultado que garantiza que no hay ceros en una región de la banda crítica con determinadas condiciones se traduce inmediatamente en una estimación del error en el teorema de los números primos. El primer paso será aprovechar la ausencia de ceros para estimar "cómodamente" la derivada logarítmica de la función dseta:

Teorema 5.18 *Sea $\eta : [0, +\infty[\longrightarrow]0, 1/2]$ una función decreciente de clase C^1 y supongamos que $\lim_{t\to+\infty} \eta'(t) = 0$ y que $1/\eta(t) = O(\log t)$. Si $\zeta(s)$ no tiene ceros que cumplan $1 - \eta(|\tau|) < \sigma$ y $0 < \alpha < 1$, entonces*

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log^2 |\tau|)$$

sobre la región $\sigma \geq 1 - \alpha\eta(|\tau|)$.

DEMOSTRACIÓN: Si $\sigma \geq 1 + \alpha\eta(|\tau|)$, entonces

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{1+\alpha\eta(|\tau|)}} = -\frac{\zeta'(1+\alpha\eta(|\tau|))}{\zeta(1+\alpha\eta(|\tau|))} < \frac{1}{\alpha\eta(|\tau|)} + c = O(\log|\tau|),$$

porque ζ'/ζ tiene un polo simple en $s = 1$ con residuo -1, luego

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} + f(s),$$

donde $f(s)$ está acotada en un entorno de 1. Por lo tanto, podemos suponer que

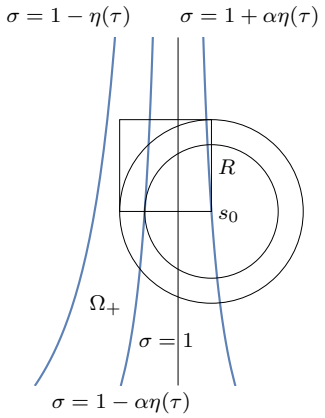
$$1 - \alpha\eta(|\tau|) \leq \sigma \leq 1 + \alpha\eta(|\tau|).$$

Sea

$$\Omega_\pm = \{s \in \mathbb{C} \mid \pm\tau > 0,\ 1 - \eta(|\tau|) < \sigma\},$$

que es un abierto simplemente conexo en el que $\log\zeta(s)$ es holomorfa. Para $\sigma > 1$ se cumple que

$$\log\zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n\, n^s} = \sum_{p,m} \frac{1}{mp^{ms}}.$$



Fijemos un número real $|T| > 1$, sea $\eta(|T|) = H$ y consideremos las circunferencias de centro

$$s_0 = 1 + \alpha H + iT$$

y radios $r = 2\alpha H$, $R = \frac{1}{2}(1 + 3\alpha)H$, de modo que $r < R < 1$. La circunferencia menor corta a la recta $\tau = T$ en los puntos $1 - \alpha H + iT$ y $1 + 3\alpha H + iT$, mientras que la mayor la corta en los puntos $1 - \frac{1}{2}(1+\alpha)H + iT$ y $1 + \frac{1}{2}(1+5\alpha)H + iT$.

Veamos que si $|T|$ es suficientemente grande, ambas circunferencias están contenidas en $\Omega_\pm$ (donde el signo es el de T). En efecto, si probamos que

$$1 - \frac{1}{2}(1+\alpha)H + i(T \pm R) \in \Omega_\pm,$$

es decir, que cumple

$$1 - \eta(|T| + R) < 1 - \frac{1}{2}(1+\alpha)H,$$

como η es decreciente, esto valdrá para para todos los puntos con parte real mayor y parte imaginaria menor (en valor absoluto), luego para todos los puntos del círculo de radio R, y también es claro que si $|T|$ es suficientemente grande la circunferencia de radio $R < 1$ no cortará al eje real. Ahora bien, por el teorema del valor medio, existe un $|T| < t < |T| + R$ tal que

$$\eta(R + |T|) - \eta(|T|) = R\eta'(t),$$

luego

$$1 - \frac{1}{2}(1+\alpha)H - 1 + \eta(R + |T|) = -\frac{1}{2}(1+\alpha)H + \eta(|T|) + R\eta'(t)$$

$$= -\frac{1}{2}(1+\alpha)H + H + \frac{1}{2}(1+3\alpha)H\eta'(t) = (\frac{1-\alpha}{2} + \frac{1}{2}(1+3\alpha)\eta'(t))H > 0$$

si $|T|$ es suficientemente grande, ya que η' es negativa, pero tiende a 0.

Así pues, $\log\zeta(s)$ es holomorfa en el disco $|s - s_0| < R$. En dicho disco $\sigma > 1/2$ y $|T| - 1 < |\tau| < |T| + 1$. Por 4.7, para $\delta = 1/2$, tenemos que

$$\operatorname{Re}\log\zeta(s) = \log|\zeta(s)| \le \log(c|\tau|^{1/2}) < \log|T|,$$

para $|T|$ suficientemente grande, pues

$$c|\tau|^{1/2} < c(|T|+1)^{1/2} < c(2|T|)^{1/2} = c\sqrt{2}|T|^{1/2} < |T|.$$

Por otra parte,

$$|\operatorname{Re}\log\zeta(s_0)| \le |\log\zeta(s_0)| \le \sum_{p,m} \frac{1}{mp^{m(1+\alpha H)}} < \sum_{n=2}^{\infty} \frac{1}{n^{1+\alpha H}} < \frac{1}{\alpha H},$$

por (4.4), teniendo en cuenta que a la serie le falta el primer término. Así estamos en condiciones de aplicar el teorema [VC 2.17] para $k = 1$, según el cual, si $|s - s_0| \le r$,

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \le \frac{2R}{(R-r)^2}(\log|T| - \operatorname{Re}\log\zeta(s_0)) < \frac{4(1+3\alpha)}{(1-\alpha)^2 H}(\log|T| + \frac{1}{\alpha H}).$$

Ahora observamos que si $1-\alpha\eta(|T|) \le \sigma \le 1+\alpha\eta(|T|)$, el punto $s=\sigma+iT$ está en el segmento que une $s_0 = 1+\alpha H + iT$ con $s_0 - r = 1-\alpha H + iT$, luego cumple $|s-s_0| \le r$ y le podemos aplicar la desigualdad anterior:

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \le \frac{4(1+3\alpha)}{(1-\alpha)^2}\frac{1}{\eta(\tau)}(\log|\tau| - \frac{1}{\alpha\eta(|\tau|)}),$$

donde hemos pasado a llamar τ a la parte imaginaria de s, que hasta ahora llamábamos T. Esto vale siempre que $|\tau|$ es suficientemente grande. Como $1/\eta(|\tau|) = O(\log|\tau|)$, es claro que la última expresión es $O(\log^2|\tau|)$. ∎

Como $\psi(x) \sim x$, la regla de L'Hôpital implica que $\psi_1(x) \sim x^2/2$. Ahora vamos a estimar el error de la aproximación.

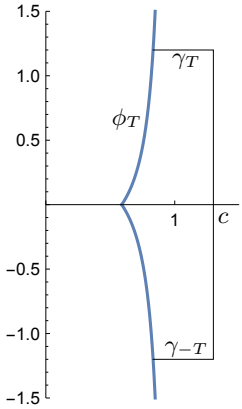
Teorema 5.19 *En las mismas condiciones del teorema anterior,*

$$\psi_1(x) = \frac{1}{2}x^2 + O(x^2 e^{-\alpha\omega(x)}),$$

donde $\omega(x)$ es el mínimo de la función $\eta(t)\log x + \log t$ en $[1,+\infty[$.

Demostración: Fijado $x > 1$ y $c > 1$, partimos de la relación que nos proporciona el teorema 5.4:

$$\psi_1(x) = -\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds.$$



Llamamos $\phi(t) = 1-\alpha\eta(|t|)+it$, para $t \in \mathbb{R}$ y $0 < \alpha < 1$. Aplicamos el teorema de los residuos al integrando en el recinto limitado por el segmento $[c-iT, c+iT]$, la restricción ϕ_T de ϕ a $[-T,T]$ y los segmentos horizontales $\gamma_{\pm T}$ que unen ambos arcos. Por hipótesis $\zeta(s)$ no se anula en ningún punto del recinto considerado, luego el integrando $f(s)$ tiene un único polo en $s=1$. Por [VC 3.10] sabemos que el residuo de $-\zeta'(s)/\zeta(s)$ es 1, de donde se sigue fácilmente que $\mathrm{Res}(f,1) = x^2/2$. Así pues:

$$\frac{1}{2\pi i}\int_{c-Ti}^{c+Ti} f(s)\,ds - \frac{1}{2\pi i}\int_{\phi_T} f(s)\,ds - \int_{\gamma_T} f(s)\,ds + \int_{\gamma_{-T}} f(s)\,ds = \frac{x^2}{2}.$$

Ahora bien, por el teorema anterior,[3]

$$\left|\int_{\gamma_{\pm T}} f(s)\,ds\right| \le c\frac{x^{c+1}}{T^2}A\log^2 T,$$

luego las dos últimas integrales tienden a 0 cuando T tiende a ∞. Esto implica que

$$\psi_1(x) = \frac{x^2}{2} - \frac{1}{2\pi i}\int_{\phi} \frac{x^{s+1}}{s(s+1)}\frac{\zeta'(s)}{\zeta(s)}\,ds.$$

[3]Usamos A para representar constantes distintas.

Ahora, también por el teorema anterior, sobre ϕ^* se cumple que

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq A\log^2(|\tau|+2)$$

(ponemos $|\tau|+2$ para que el logaritmo sea siempre positivo y, eligiendo adecuadamente la constante A, podamos garantizar la desigualdad para todo s). Por otra parte, $|\phi'(t)| = |-\alpha\eta'(|t|)+i| < A$, porque por hipótesis $\eta'(t)$ tiende a 0 en $+\infty$, luego está acotada. Por lo tanto,

$$\left|\frac{\psi_1(x)}{x^2}-\frac{1}{2}\right| \leq A\int_{-\infty}^{+\infty}\frac{x^{-\alpha\eta(|t|)}\log^2(|t|+2)}{|\phi(t)(\phi(t)+1)|}\,dt$$

$$= A\int_{-\infty}^{+\infty} e^{-\alpha\eta(|t|)\log x-\alpha\log|t|}\frac{|t|^\alpha\log^2(|t|+2)}{|\phi(t)(\phi(t)+1)|}\,dt$$

$$\leq Ae^{-\omega(x)}\int_{-\infty}^{+\infty}\frac{|t|^\alpha\log^2(|t|+2)}{|\phi(t)(\phi(t)+1)|}\,dt$$

$$\leq Ae^{-\omega(x)}\left(\int_{-1}^{1}\frac{|t|^\alpha\log^2(|t|+2)}{(1/2)(3/2)}\,dt+2\int_1^{+\infty}\frac{\log^2(t+2)}{t^{2-\alpha}}\,dt\right)=O(e^{-\omega(x)}),$$

donde la última integral converge porque $\delta = 2-\alpha > 1$, por lo que, para cualquier $1<\delta'<\delta$, el integrando es claramente $O(1/t^{\delta'})$, y la convergencia de

$$\int_1^{+\infty}\frac{dt}{t^{\delta'}}$$

implica la de la integral a la que hemos llegado. ∎

Nota Conviene observar que la función $\omega(x)$ es estrictamente creciente, al igual que $\log x-\omega(x)$. En efecto, si $0<x_1<x_2$ y t_1, t_2 son los puntos donde se alcanzan los mínimos respectivos, tenemos que

$$\omega(x_1)\leq\eta(t_2)\log x_1+\log t_2<\eta(t_2)\log x_2+\log t_2=\omega(x_2),$$

y

$$\omega(x_2)\leq\eta(t_1)\log x_2+\log t_1=\omega(x_1)+\eta(t_1)(\log x_2-\log x_1)$$
$$<\omega(x_1)+\log x_2-\log x_1.$$

Como $\omega(1)=0$ y $\log 1-\omega(1)=0$, concluimos además que

$$0<\omega(x)<\log x,\qquad \text{para } x>1.$$

∎

Veamos ahora cómo obtener una estimación del error de $\psi(x)\sim x$ a partir de la que acabamos de obtener para $\psi_1(x)$ y a su vez de aquí pasaremos a otra para $\pi(x)$:

Teorema 5.20 *Sea $\eta : [0, +\infty[\longrightarrow]0, 1/2]$ una función decreciente de clase C^1 y supongamos que $\lim_{t\to+\infty} \eta'(t) = 0$ y que $1/\eta(t) = O(\log t)$. Si $\zeta(s)$ no tiene ceros que cumplan $1 - \eta(|\tau|) < \sigma$ y $0 < \alpha < 1$, entonces*

$$\psi(x) = x + O(xe^{-\frac{1}{2}\alpha\omega(x)}), \qquad \pi(x) = \mathrm{Il}(x) + O(xe^{-\frac{1}{2}\alpha\omega(x)}),$$

donde $\omega(x)$ es el mínimo de la función $\eta(t)\log x + \log t$ en $[1, +\infty[$.

Demostración: Veamos un argumento muy general, aplicable a cualquier función $h :]2, +\infty[\longrightarrow]0, +\infty[$ tal que $0 < h(x) < x/2$. Como ψ es creciente,

$$\frac{1}{h}\int_{x-h}^{x} \psi(t)\,dt \le \psi(x) \le \frac{1}{h}\int_{x}^{x+h} \psi(t)\,dt.$$

los términos de los extremos son

$$\frac{\psi_1(x \pm h) - \psi_1(x)}{\pm h} = \frac{(x \pm h)^2/2 - x^2/2}{\pm h}$$

$$+\frac{1}{h}O((x-h)^2 e^{-\alpha\omega(x-h)}) + \frac{1}{h}O((x+h)^2 e^{-\alpha\omega(x+h)})$$

$$= x \pm \frac{h}{2} + O(x^2 \frac{e^{-\alpha\omega(x/2)}}{h}),$$

donde hemos aplicado el teorema anterior y, para la última igualdad, hemos usado que

$$\frac{(x \pm h)^2}{x^2} \le 1 + \frac{2h}{x} + \left(\frac{h}{x}\right)^2 \le 3,$$

así como que $x/2 < x - h < x < x + h$ y, como ω es creciente

$$e^{-\alpha\omega(x\pm h)} \le e^{-\alpha\omega(x/2)}.$$

Más aún, como $\log x - \omega(x)$ es creciente,

$$e^{-\alpha\omega(x/2)} = (x/2)^{-\alpha} e^{\alpha(\log(x/2) - \omega(x/2))} \le (x/2)^{-\alpha} e^{\alpha(\log x - \omega(x))} = 2^{\alpha} e^{-\alpha\omega(x)}.$$

Por lo tanto,

$$|\psi(x) - x| \le \frac{h}{2} + O(x^2 \frac{e^{-\alpha\omega(x)}}{h}).$$

Tomando $h(x) = \frac{1}{2}xe^{-\frac{1}{2}\alpha\omega(x)}$ obtenemos la primera afirmación del enunciado.

Para probar la segunda parte, el teorema 5.10 nos da que

$$\pi^*(x) - \mathrm{Il}(x) = \frac{\psi(x) - x}{\log x} + \frac{2}{\log 2} + \int_2^x \frac{\psi(t) - t}{t\log^2 t}\,dt$$

Por la parte ya probada del teorema,

$$\left|\frac{\psi(x) - x}{\log x}\right| \le cxe^{-\frac{1}{2}\alpha\omega(x)}$$

y, como $xe^{-\frac{1}{2}\alpha\omega(x)} > xe^{-\frac{1}{2}\alpha\log x} = x^{1-\alpha/2} > x^{1/2} > 1$, eligiendo la constante c suficientemente grande, también

$$\frac{2}{\log 2} < cxe^{-\frac{1}{2}\alpha\omega(x)}.$$

Además,

$$\left|\int_2^x \frac{\psi(t)-t}{t\log^2 t}\,dt\right| \le c_1\int_2^x \frac{e^{\frac{\alpha}{2}(\log t-\omega(t))}}{t^{\alpha/2}}\,dt \le e^{\frac{\alpha}{2}(\log x-\omega(x))}\int_2^x \frac{dt}{t^{\alpha/2}}$$

$$xe^{-\frac{1}{2}\alpha\omega(x)}x^{\alpha/2-1}\left(\frac{1}{(1-\alpha/2)x^{1-\alpha/2}} - \frac{1}{(1-\alpha/2)2^{1-\alpha/2}}\right)$$

$$= xe^{-\frac{1}{2}\alpha\omega(x)}\left(\frac{1}{(1-\alpha/2)x^{2-\alpha}} - \frac{1}{(1-\alpha/2)2^{1-\alpha/2}x^{1-\alpha/2}}\right)$$

$$= O(xe^{-\frac{1}{2}\alpha\omega(x)}).$$

Concluimos que

$$\pi^*(x) - \mathrm{Il}(x) = O(xe^{-\frac{1}{2}\alpha\omega(x)}).$$

Por otra parte, el teorema 5.10 nos da también que $\pi^*(x) - \pi(x) = O(x^{1/2})$, de donde

$$\pi(x) - \mathrm{Il}(x) = O(xe^{-\frac{1}{2}\alpha\omega(x)}) + O(x^{1/2}) = O(xe^{-\frac{1}{2}\alpha\omega(x)}),$$

pues hemos visto que $x^{1/2}/xe^{-\frac{1}{2}\alpha\omega(x)} < 1$. ∎

Observaciones Si la constante c cumple el teorema 5.13, entonces la función $\eta(t) = \frac{c}{\log(t+2)}$ cumple las hipótesis del teorema anterior (reduciendo c si es necesario[4] para que $\eta(0) < 1/2$). Veamos que, si $x \ge 2$, el valor mínimo de

$$\frac{c\log x}{\log(t+2)} + \log t$$

para $t \ge 1$ cumple $\omega(x) \ge k\sqrt{\log x}$, para cierto $k > 0$. En efecto, esto equivale a que

$$\frac{c\sqrt{\log x}}{\log(t+2)} + \frac{\log t}{\sqrt{\log x}} \ge k > 0.$$

Si $1 \le t \le 2$ tenemos que

$$\frac{c\sqrt{\log x}}{\log(t+2)} + \frac{\log t}{\sqrt{\log x}} \ge \frac{c\sqrt{\log 2}}{\log 4}.$$

[4] Alternativamente, si nos fijamos en los pocos pasos de las pruebas precedentes en los que interviene η', vemos que en realidad el teorema anterior sigue siendo válido si admitimos que η no sea derivable en un número finito de puntos, con tal de que η' esté acotada donde está definida. Así, en lugar de reducir la constante c, podemos usar $\eta^*(t) = \min\{1/2, \eta(t)\}$.

Para $t \geq 2$, existe una constante $a > 0$ tal que $\log(t+2) \leq a \log t$, con lo que

$$\frac{c\sqrt{\log x}}{\log(t+2)} + \frac{\log t}{\sqrt{\log x}} \geq \frac{c\sqrt{\log x}}{a \log t} + \frac{\log t}{\sqrt{\log x}} \geq 2\sqrt{\frac{c}{a}},$$

pues es fácil ver que la función $f(u) = cu + 1/u$ alcanza su mínimo en $u = 1/\sqrt{c}$, y éste es $2\sqrt{c}$.

Por consiguiente, el teorema anterior, con $\alpha = 1/2$, por ejemplo, nos da que

$$\pi(x) = \mathrm{Il}(x) + O(xe^{-(1/4)\omega(x)}) = O(xe^{-(k/4)\log x}),$$

que es la misma estimación que nos proporciona el teorema 5.15 (aunque obtenida ahora de forma más laboriosa).

Si suponemos la hipótesis de Riemann, entonces la función $\eta(t) = 1/2$ también cumple las condiciones del teorema anterior, y $\omega(x) = \frac{1}{2}\log x$, con lo que obtenemos

$$\pi(x) = \mathrm{Il}(x) + O(xe^{-(\alpha/4)\log x}) = \mathrm{Il}(x) + O(x^{1-\alpha/4}),$$

para todo $0 < \alpha < 1$, que es una estimación peor que (5.2).

Así pues, el teorema anterior no nos proporciona ninguna información que no supiéramos ya. Naturalmente, su interés estriba en que puede aplicarse a teoremas que proporcionen regiones sin ceros más amplias que la del teorema 5.13, o más complicadas que la que proporciona la hipótesis de Riemann, para las que no hay argumentos directos que nos proporcionen una estimación del error del teorema de los números primos más fácilmente que aplicando el teorema anterior.

En la sección siguiente veremos un ejemplo del interés que tiene obtener estimaciones mejores del error. ∎

5.4 Diferencias entre primos

El teorema 3.19 implica que la función que a cada primo p le asigna la distancia $s(p) = q - p$ al primo siguiente q es $o(p)$ (pues, dado $\epsilon > 0$, para todo p suficientemente grande se cumple que $s(p) < \epsilon p$, luego $s(p)/p$ tiende a 0). El teorema siguiente da condiciones suficientes para que podamos afirmar que $s(p) = O(p^\theta)$ lo cual, para $0 < \theta < 1$, es más fuerte que la estimación $o(p)$.

Teorema 5.21 (Hoheisel) *Supongamos que la función dseta no se anula en la región*

$$1 - \frac{A \log\log \tau}{\log \tau} < \sigma, \quad \tau > \tau_0 > 3,$$

y que si $\frac{1}{2} \leq S \leq 1$

$$N(S,T) = O(T^{b(1-S)} \log^B T),$$

para ciertas constantes $b > 0$ *y* $B \geq 0$.

Entonces, para todo $k > 0$ y todo θ que cumpla

$$1 - \frac{1}{b + B/A} < \theta < 1$$

se cumple que

$$\pi(x + kx^\theta) - \pi(x) \sim \frac{kx^\theta}{\log x},$$

luego $p_{n+1} - p_n = O(p_n^\theta)$.

Recordemos que $N(S,T)$ es la función que cuenta el número de ceros no triviales de la función dseta que cumplen $\operatorname{Re}\rho \geq S$, $\operatorname{Im}\rho \leq T$.

La última afirmación es consecuencia inmediata de la precedente, pues ésta (para $k = 1$) implica que $\pi(p_n + p_n^\theta) - \pi(p_n)$ tiende a infinito, luego, para todo n suficientemente grande, $p_{n+1} \leq p_n + p_n^\theta$, luego $p_{n+1} - p_n = O(p_n^\theta)$.

Vemos así que a partir de una hipótesis sobre la localización de los ceros no triviales de la función dseta y otra sobre su densidad obtenemos una consecuencia notable sobre la distancia entre primos consecutivos.

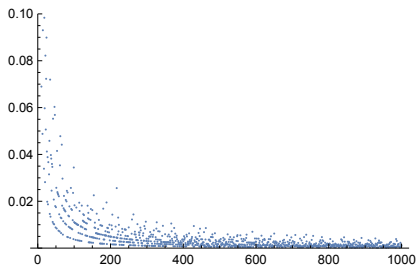
Por ejemplo, si suponemos la hipótesis de Riemann, la función $N(S,T)$ es nula para $S > 1/2$, y cumple trivialmente la hipótesis del teorema. Por otra parte, $N(1/2,T) = 0.5N(T)$ y, según la fórmula de Riemann-von Mangoldt, es $N(1/2,T) = O(T\log T)$, luego la hipótesis se cumple en este caso con $b = 2$ y $B = 1$. En cuanto a la hipótesis sobre la región sin ceros, se cumple trivialmente para todo $A > 0$. Por consiguiente, haciendo tender a A a $+\infty$ en la expresión que determina los valores válidos de θ, vemos que el teorema de Hoheisel se aplica a todo $\theta > 1/2$. En resumen, bajo la hipótesis de Riemann podemos asegurar que

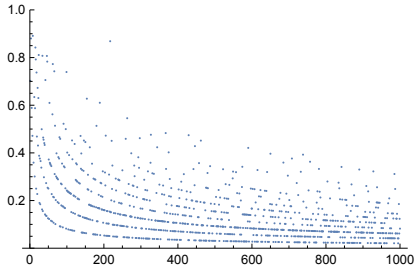
$$p_{n+1} - p_n = O(p_n^{1/2+\epsilon}), \qquad \text{para todo } \epsilon > 0.$$

En realidad, esto equivale a que $p_{n+1} - p_n = o(p_n^{1/2+\epsilon})$, pues

$$\frac{p_{n+1} - p_n}{p_n^{1/2+\epsilon}} = \frac{p_{n+1} - p_n}{p_n^{1/2+\epsilon/2}} \frac{1}{p_n^{1/2+\epsilon/2}},$$

y si el primer cociente está acotado, el producto tiende a 0.





La gráfica de la izquierda muestra la sucesión $(p_{n+1}-p_n)/p_n$, y en ella se puede apreciar que tiende a 0 rápidamente. La gráfica de la derecha muestra la sucesión $(p_{n+1}-p_n)/p_n^{1/2+0.01}$, y también se aprecia que tiende a 0, aunque mucho más lentamente (nótese la diferencia en la escala del eje vertical).

Si tratamos de obtener algún valor de θ que cumpla el teorema sin suponer la hipótesis de Riemann, nos encontramos con que ninguno de los resultados que tenemos probados nos aseguran que se cumplan las hipótesis. En particular, la región sin ceros que conocemos es más restrictiva que lo que exige el teorema, y tampoco tenemos una información adecuada sobre la densidad de los ceros. En el capítulo siguiente abordaremos este problema. En esta sección nos limitaremos a demostrar el teorema de Hoheisel.

Demostración: Observemos que

$$N(T) = 2N(1/2,T) = O(T^{b/2}\log^B T),$$

luego

$$\left|\frac{N(T)}{T}\right| \le cT^{b/2-1}\log^B T.$$

Si fuera $b<2$, el miembro derecho tendería a 0, pero sabemos que el miembro izquierdo tiende a infinito. Así pues, $b\ge 2$ y, por consiguiente, $\theta > 1/2$. Ahora, si $0 \le S < 1/2$ tenemos que

$$\frac{N(S,T)}{T^{b(1-S)}\log^B T} \le \frac{2N(T)}{T^{b(1-S)}\log^B T} \le \frac{cT\log T}{T^{b(1-S)}\log^B T} = \frac{c\log^{1-B} T}{T^{b-1-bS}},$$

donde $b-1-bS > b-1-b/2 = b/2-1 \ge 0$, luego el miembro derecho tiende a 0 tanto si $1-B$ es positivo o negativo. Esto significa que la hipótesis sobre $N(S,T)$ vale en realidad para $0 \le S \le 1$.

Por el teorema 5.5 tenemos que, si $3 \le T \le x$, cuando $x \to +\infty$ se cumple

$$\psi(x) = x - \sum_{|\operatorname{Im}\rho|<T} \frac{x^\rho}{\rho} + O(\frac{x\log^2 x}{T}).$$

En efecto, por una parte, $\psi(x) = \psi_0(s)+O(\log x)$, lo que nos permite cambiar ψ_0 por ψ. Por otra parte,

$$\frac{T}{x\log^2 x}\log 2\pi \le \frac{\log 2\pi}{\log^2 x} = O(1),$$

$$\frac{T}{x\log^2 x}\frac{1}{2}\left|\log\left(1-\frac{1}{x^2}\right)\right| \le \frac{1}{2\log^2 x}(\log(x^2-1)+\log x^2) \le \frac{2\log x}{\log^2 x} = O(1),$$

$$\frac{T}{x\log^2 x}\frac{x\log^2(xT)}{T} \le \left(\frac{\log x^2}{\log x}\right)^2 = 4,$$

$$\frac{T}{x\log^2 x}\operatorname{mín}\{1,\frac{x}{T\langle x\rangle}\}\log x \le \frac{1}{\log x} = O(1).$$

Por lo tanto, si $0 < h \le kx$,

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

donde la constante implícita depende de k. En efecto:

$$\frac{T}{x\log^2 x}\frac{(x+h)\log^2(x+h)}{T} \le (1+k)\left(\frac{\log(1+k)+\log x}{\log x}\right)^2 = O(1).$$

Ahora observamos que

$$\left|\frac{(x+h)^\rho - x^\rho}{\rho}\right| = \left|\int_x^{x+h} u^{\rho-1}\,du\right| \le \int_x^{x+h} u^{\operatorname{Re}\rho-1}\,du \le hx^{\operatorname{Re}\rho-1},$$

luego

$$\frac{\psi(x+h)-\psi(x)}{h} = 1 + O\Big(\sum_{|\operatorname{Im}\rho|<T} x^{\operatorname{Re}\rho-1}\Big) + O(\frac{x\log^2 x}{Th}).$$

Por otra parte, si $\{\rho_n\}_{n=1}^N$ es una enumeración de los ceros de la función dseta que cumplen $|\operatorname{Im}\rho_n| < T$, repetidos según su orden, tenemos que

$$\sum_{|\operatorname{Im}\rho|<T} (x^{\operatorname{Re}\rho-1} - x^{-1}) = \sum_{|\operatorname{Im}\rho|<T} \int_0^{\operatorname{Re}\rho} x^{u-1}\log x\,du$$

$$= \sum_{n=1}^N \int_0^{\operatorname{Re}\rho_n} x^{u-1}\log x\,du = \sum_{n=1}^N \int_0^1 \chi_{[0,\operatorname{Re}\rho_n]}(u)x^{u-1}\log x\,du$$

$$= \int_0^1 \sum_{n=1}^N \chi_{[0,\operatorname{Re}\rho_n]}(u)x^{u-1}\log x\,du = \int_0^1 \sum_{\substack{|\operatorname{Im}\rho|<T\\ \operatorname{Re}\rho\ge u}} x^{u-1}\log x\,du$$

$$= 2\int_0^1 N(u,T)x^{u-1}\log x\,du.$$

Así pues,

$$\sum_{|\operatorname{Im}\rho|<T} x^{\operatorname{Re}\rho-1} = 2x^{-1}N(T) + 2\int_0^1 N(u,T)x^{u-1}\log x\,du.$$

Si llamamos $\eta(T) = \frac{A\log\log T}{\log T}$, tenemos por hipótesis que $N(u,T) = 0$ para $u \ge 1-\eta(T)$, $T > \tau_0$, luego

$$\sum_{|\operatorname{Im}\rho|<T} x^{\operatorname{Re}\rho-1} = 2x^{-1}N(T) + 2\int_0^{1-\eta(T)} N(u,T)x^{u-1}\log x\,du.$$

Por lo tanto, teniendo en cuenta la fórmula de Riemann-von Mangoldt 4.19 y la hipótesis sobre $N(S,T)$,

$$\left|\sum_{|\operatorname{Im}\rho|<T} x^{\operatorname{Re}\rho-1}\right| \le \frac{cT\log T}{x} + c\int_0^{1-\eta(T)} \left(\frac{T^b}{x}\right)^{1-u} \log^B T \log x\, du.$$

Fijemos, concretamente, $T = x^\alpha$, para cierto α tal que $0 < \alpha < \frac{1}{b} \le \frac{1}{2}$. Entonces

$$\begin{aligned}
\left|\sum_{|\operatorname{Im}\rho|<x^\alpha} x^{\operatorname{Re}\rho-1}\right| &\le c\alpha x^{\alpha-1}\log x + c\alpha^B \int_0^{1-\eta(T)} (x^{b\alpha-1})^{1-u}\log^{B+1} x\, du \\
&= c\alpha x^{\alpha-1}\log x - c\alpha^B \frac{[(x^{b\alpha-1})^{1-u}]_0^{1-\eta(x^\alpha)}}{(b\alpha-1)\log x}\log^{B+1} x \\
&= c\alpha x^{\alpha-1}\log x + c\alpha^B \frac{(x^{b\alpha-1})^{\eta(x^\alpha)} - x^{b\alpha-1}}{(1-b\alpha)}\log^B x \\
&\le c\alpha x^{\alpha-1}\log x + \frac{c\alpha^B}{1-b\alpha} e^{(b-1/\alpha)A\log(\alpha\log x)}\log^B x \\
&\le cx^{\alpha-1}\log x + ce^{-(1/\alpha-b)A\log(\log x)}\log^B x \\
&= cx^{\alpha-1}\log x + c\log^{-\delta} x = O(\log^{-\delta} x),
\end{aligned}$$

donde $\delta = \left(\frac{1}{\alpha} - b\right)A - B$. Ahora elegimos α de modo que

$$1-\theta < \alpha < \frac{1}{b + B/A},$$

de modo que

$$\frac{1}{\alpha} > b + \frac{B}{A} \ge b$$

y así $\delta > 0$ y

$$\frac{\psi(x+h)-\psi(x)}{h} = 1 + O(\log^{-\delta} x) + O(\frac{x\log^2 x}{x^\alpha h}).$$

Ahora tomamos $h = kx^\theta$, con lo que

$$\frac{\psi(x+kx^\theta)-\psi(x)}{kx^\theta} = 1 + O(\log^{-\delta} x) + O\left(\frac{\log^2 x}{x^{\alpha+\theta-1}}\right)$$

y así $\psi(x+kx^\theta)-\psi(x) \sim kx^\theta$ (omitimos la k del término de error porque sólo modifica la constante implícita, que ya dependía de k). Por otra parte,

$$\psi(x+kx^\theta)-\psi(x) = \sum_{x<p\le x+kx^\theta} \log p + \sum_{\substack{x<p^m\le x+kx^\theta \\ m\ge 2}} \log p.$$

Para cada primo p tal que $p^2 \le x+kx^\theta$, el número de veces que $\log p$ aparece en el segundo sumatorio es menor que el máximo m que cumple $p^m \le x+kx^\theta$, luego

$$\left|\psi(x+kx^\theta)-\psi(x)-\sum_{x<p\le x+x^\theta}\log p\right| \le \sum_{p^2\le x+kx^\theta}\log p\,\frac{\log(x+kx^\theta)}{\log p}$$

$$\le \sum_{p^2\le (k+1)x}\log((k+1)x) \le \sqrt{(k+1)x}\log((k+1)x) = O(x^{1/2}\log x),$$

luego

$$\psi(x+kx^\theta)-\psi(x) = \sum_{x<p\le x+kx^\theta}\log p + O(x^{1/2}\log x)$$

$$= \sum_{x<p\le x+kx^\theta}\log x + \sum_{x<p\le x+kx^\theta}\log(p/x) + O(x^{1/2}\log x)$$

$$= (\pi(x+kx^\theta)-\pi(x))\log x + kx^\theta\log(\frac{x+kx^\theta}{x}) + O(x^{1/2}\log x)$$

luego

$$|\psi(x+kx^\theta)-\psi(x)-(\pi(x+kx^\theta)-\pi(x))\log x| \le kx^\theta\log(1+\frac{k}{x^{1-\theta}})+O(x^{1/2}\log x).$$

A su vez,

$$\left|\frac{\psi(x+kx^\theta)-\psi(x)}{kx^\theta}-\frac{(\pi(x+kx^\theta)-\pi(x))\log x}{kx^\theta}\right| \le \log(1+\frac{k}{x^{1-\theta}})+O\left(\frac{\log x}{x^{\theta-1/2}}\right).$$

Teniendo en cuenta que $1/2<\theta<1$, podemos concluir que

$$\lim_{x\to+\infty}\frac{(\pi(x+kx^\theta)-\pi(x))\log x}{kx^\theta}=1.$$

En particular, como ya habíamos señalado, $\pi(p_n+p_n^\theta)-\pi(p_n)$ tiende a infinito, luego, para todo n suficientemente grande, $p_{n+1}\le p_n+p_n^\theta$, luego $p_{n+1}-p_n = O(p_n^\theta)$. ∎

5.5 Orden de crecimiento y localización de ceros

Según hemos visto, para aplicar el teorema de Hoheisel necesitamos encontrar una región de la banda crítica sin ceros de la función dseta mejor que la que nos proporciona el teorema 5.13. En esta sección vamos a reducir el problema al estudio del orden de crecimiento de la función dseta:

Teorema 5.22 *Sean $\phi(t)$ y $1/\theta(t)$ funciones positivas, crecientes para $t \geq t_0$, tales que $\theta(t) \leq 1$ y $\lim_{t\to+\infty} \phi(t) = +\infty$. Si*

$$\frac{\phi(t)}{\theta(t)} = o(e^{\phi(t)}) \qquad y \qquad \zeta(s) = O(e^{\phi(\tau)})$$

para todo s que cumpla $1 - \theta(\tau) \leq \sigma \leq 2$, $\tau \geq t_0$, entonces existen un $c > 0$ y un $t_1 \geq t_0$ tal que $\zeta(s)$ no tiene ceros en la región

$$1 - c\frac{\theta(2\tau+1)}{\phi(2\tau+1)} \leq \sigma, \qquad \tau \geq t_1.$$

Por ejemplo, si tomamos $\theta(t) = 1/2$ y $\phi(t) = \log(t)$, la hipótesis sobre la función dseta es que $\zeta(s) = o(\tau)$, para $1/2 \leq \sigma \leq 2$, lo cual se cumple por el teorema 4.7. La conclusión es que $\zeta(s)$ no tiene ceros en la región

$$1 - \frac{c}{\log(2\tau+1)} \leq \sigma, \quad \tau \geq t_1$$

y, como

$$\frac{\log(2\tau+1)}{\log(\tau+2)} = O(1),$$

esto equivale a que $\zeta(s)$ no tenga ceros en una región de la forma

$$1 - \frac{c}{\log(|\tau|+2)} \leq \sigma,$$

con lo que recuperamos el teorema 5.13. Naturalmente, la finalidad de este teorema es mejorar 5.13 a partir de estimaciones mejores del crecimiento de la función dseta.

Necesitamos un resultado previo sobre funciones holomorfas:

Teorema 5.23 *Sea f una función holomorfa en un disco $D(s_0, r)$ y tal que $f(s_0) \neq 0$ y $|f(s)| < |f(s_0)|e^M$ en el disco, para cierto $M > 0$. Supongamos además que f no se anula en el semicírculo formado por los puntos de $D(s_0, r)$ con $\operatorname{Re} s > \operatorname{Re} s_0$. Entonces*

$$-\operatorname{Re}(f'(s_0)/f(s_0)) < 4M/r.$$

Si además f tiene un cero ρ_0 en el segmento abierto de extremos $s_0 - r/2$ y s_0, entonces

$$-\operatorname{Re}(f'(s_0)/f(s_0)) < \frac{4M}{r} - \frac{1}{s_0 - \rho_0}.$$

Demostración: Cambiando f por $f(s)/f(s_0)$ podemos suponer sin pérdida de generalidad que $f(s_0) = 1$. Igualmente, cambiando f por $f(s - s_0)$ podemos suponer que $s_0 = 0$. Consideremos la función

$$g(s) = \frac{f(s)}{\prod_\rho \left(1 - \frac{s}{\rho}\right)},$$

donde ρ recorre los ceros de f en el disco $|s| \leq r/2$ (que son un número finito y por hipótesis son todos no nulos), repetidos tantas veces como indica su orden.

Para $|s| = r$ tenemos que

$$\left|1 - \frac{s}{\rho}\right| \geq \left|\frac{s}{\rho}\right| - 1 = \frac{r}{|\rho|} - 1 \geq 1,$$

luego

$$|g(s)| \leq |f(s)| < e^M.$$

Como $g(0) = 1$ y $g(s)$ no tiene ceros en $|s| \leq r/2$, tenemos que $g(s) = e^{G(s)}$, para una cierta función holomorfa en un abierto que contiene al disco cerrado. Entonces $G(0) = 0$ y $\operatorname{Re} G(s) < M$. El teorema [VC 2.27] nos permite concluir que $G'(0) < 4M/r$ (notemos que, con la notación del teorema, $G'(0) = c_1$). Por lo tanto

$$\left|f'(0) + \sum_\rho \frac{1}{\rho}\right| = \left|\frac{g'(0)}{g(0)}\right| = |G'(0)| < \frac{4M}{r},$$

de donde

$$-\operatorname{Re} f'(0) - \sum_\rho \operatorname{Re}\frac{1}{\rho} < \frac{4M}{r},$$

o equivalentemente,

$$-\operatorname{Re} f'(0) < \frac{4M}{r} + \sum_\rho \operatorname{Re}\frac{1}{\rho}.$$

Por hipótesis $\operatorname{Re}\rho \leq 0$, luego también $\operatorname{Re}(1/\rho) \leq 0$, luego $-\operatorname{Re} f'(0) < 4M/r$, como había que probar, y si suponemos además que uno de los ceros cumple $-r/2 < \rho_0 < 0$, entonces $-\operatorname{Re} f'(0) < 4M/r + 1/\rho_0$. ∎

Demostración (de 5.22): La función $-\zeta'(s)/\zeta(s)$ tiene un polo simple en $s = 1$ con residuo 1, luego

$$\lim_{\sigma\to 1^+} -\frac{\zeta'(\sigma)}{\zeta(\sigma)}(\sigma - 1) = 1.$$

Por consiguiente, existe un $0 < \delta < 1$ tal que, si $1 < \sigma < 1 + \delta$, se cumple que

$$-\frac{\zeta'(\sigma)}{\zeta(\sigma)} < \frac{5/4}{\sigma - 1}. \tag{5.4}$$

Tomemos $t_1 \geq t_0 + 1$ tal que $e^{-\phi(\tau_1)} < \delta$ y supongamos que $a + bi$ es un cero de $\zeta(s)$ con $b > t_1$. Fijamos σ_0 tal que

$$1 + e^{-\phi(2b+1)} \leq \sigma_0 < 1 + \delta < 2. \tag{5.5}$$

En particular

$$-\frac{\zeta'(\sigma_0)}{\zeta(\sigma_0)} < \frac{5/4}{\sigma_0 - 1}.$$

Sea $s_0 = \sigma_0 + bi$, $s_0' = \sigma_0 + 2bi$, $r = \theta(2b + 1) \leq 1$. Entonces los discos $|s - s_0| \leq r$ y $|s - s_0'| \leq r$ están contenidos en la región

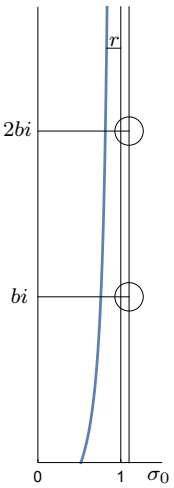
$$1 - \theta(\tau) \leq \sigma \leq 2, \qquad \tau \geq \tau_0.$$

De hecho, ambos están contenidos en el rectángulo

$$[\sigma_0 - r, 2] \times [\tau_0, 2b + 1],$$

y cualquier punto de este rectángulo cumple

$$\sigma \geq \sigma_0 - r \geq 1 - \theta(2b + 1) \geq 1 - \theta(\tau).$$



Como $1/\zeta(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ y $|\mu(n)| \leq 1$, para $1 < \sigma \leq 2$ tenemos que

$$\left|\frac{1}{\zeta(s)}\right| \leq \zeta(\sigma) \leq \frac{2}{\sigma - 1}.$$

En particular

$$\left|\frac{1}{\zeta(s_0)}\right| \leq \frac{2}{\sigma_0 - 1} \leq 2e^{\phi(2b+1)}.$$

Igualmente

$$\left|\frac{1}{\zeta(s_0')}\right| \leq 2e^{\phi(2b+1)}.$$

Veamos ahora que existe una constante $A_1 > 0$ tal que, si $|s - s_0| \leq r$,

$$\left|\frac{\zeta(s)}{\zeta(s_0)}\right| < e^{A_1\phi(2b+1)}.$$

En efecto, si $\sigma \leq 2$ tenemos que $\zeta(s) = O(e^{\phi(\tau)})$ en la región $1 - \theta(t) \leq \sigma \leq 2$, $\tau \geq \tau_0$, luego $|\zeta(s)| < ce^{\phi(\tau)} \leq ce^{\phi(2b+1)}$. A su vez,

$$\left|\frac{\zeta(s)}{\zeta(s_0)}\right| < e^{2\phi(2b+1)+c} < e^{A_1\phi(2b+1)},$$

donde usamos que ϕ tiende a $+\infty$, luego el cociente $(2\phi(2b + 1) + c)/\phi(2b + c)$ tiene una cota superior A_1. Por otra parte, si $\sigma \geq 2$ entonces

$$|\zeta(s)| \leq \zeta(\sigma) \leq \zeta(2),$$

y claramente llegamos a la misma conclusión. Igualmente podemos exigir que si $|s - s_0'| < r$ se cumpla

$$\left|\frac{\zeta(s)}{\zeta(s_0')}\right| < e^{A_1\phi(2b+1)}.$$

Aplicamos el teorema 5.23 a $\zeta(s)$ con $M = A_1\phi(2b + 1)$, de modo que

$$-\operatorname{Re}\frac{\zeta'(\sigma_0 + 2bi)}{\zeta(\sigma_0 + 2bi)} < \frac{A_2\phi(2b + 1)}{\theta(2b + 1)} \tag{5.6}$$

y si $a > \sigma_0 - r/2$ entonces

$$-\operatorname{Re}\frac{\zeta'(\sigma_0 + bi)}{\zeta(\sigma_0 + bi)} < \frac{A_2\phi(2b + 1)}{\theta(2b + 1)} - \frac{1}{\sigma_0 - a}. \tag{5.7}$$

Ahora usamos el argumento que ya hemos empleado en la prueba de 3.36 y de 5.13, en virtud del cual, la desigualdad $3+4\cos\alpha+\cos 2\alpha\geq 0$ se traduce en que, en el semiplano $\sigma>1$, tenemos que

$$-\operatorname{Re}\left(3\frac{\zeta'(\sigma)}{\zeta(\sigma)}+4\frac{\zeta'(\sigma+i\tau)}{\zeta(\sigma+i\tau)}+\frac{\zeta'(\sigma+i2\tau)}{\zeta(\sigma+i2\tau)}\right)\geq 0.$$

Usando (5.4), (5.6) y (5.7) llegamos a que

$$0\leq\frac{15}{4(\sigma_0-1)}+\frac{5A_2\phi(2b+1)}{\theta(2b+1)}-\frac{4}{\sigma_0-a},$$

de donde

$$\sigma_0-a\leq\left(\frac{15}{16(\sigma_0-1)}+\frac{5A_2}{4}\frac{\phi(2b+1)}{\theta(2b+1)}\right)^{-1},$$

y a su vez

$$1-a\geq\left(\frac{15}{16(\sigma_0-1)}+\frac{5A_2}{4}\frac{\phi(2b+1)}{\theta(2b+1)}\right)^{-1}-(\sigma_0-1)$$

$$=\frac{\frac{1}{16}-\frac{5A_2}{4}\frac{\phi(2b+1)}{\theta(2b+1)}(\sigma_0-1)}{\frac{15}{16(\sigma_0-1)}+\frac{5A_2\phi(2b+1)}{4\theta(2b+1)}}.$$

Todo esto es válido para cualquier σ_0 que cumpla (5.5). Observemos ahora que, si elegimos t_1 suficientemente grande, podemos tomar, concretamente,

$$\sigma_0=1+\frac{1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)}.$$

En efecto, se trata de comprobar que con esta elección se cumple

$$e^{-\phi(2b+1)}\leq\frac{1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)}<\delta$$

si $b>t_1$. Ahora bien, por hipótesis el término central tiende a 0, luego podemos asegurar que sea $<\delta$, y la otra desigualdad equivale a

$$\frac{\frac{\phi(2b+1)}{\theta(2b+1)}}{e^{\phi(2b+1)}}<\frac{1}{40A_2},$$

y por hipótesis el miembro izquierdo tiende a 0. Con esta elección queda que

$$1-a\geq\frac{\theta(2b+1)}{1240A_2\phi(2b+1)},$$

luego $a+bi$ está en la región del enunciado. Esto es así bajo la hipótesis de que $a>\sigma_0-r/2$, que hemos usado en (5.7). Pero si $a\leq\sigma_0-r/2$, la misma elección de σ_0 nos da que

$$a\leq\sigma_0-\frac{r}{2}=1+\frac{1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)}-\frac{\theta(2b+1)}{2},$$

luego

$$1-a \geq \frac{\theta(2b+1)}{2} - \frac{1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)} \geq \frac{\theta(2b+1)}{2\phi(2b+1)} - \frac{1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)}$$

$$= \frac{20A_2-1}{40A_2}\frac{\theta(2b+1)}{\phi(2b+1)},$$

y de nuevo tenemos la conclusión. ∎

Capítulo VI

La función dseta de Riemann II

En este capítulo probaremos algunos resultados más profundos y sofisticados sobre la función dseta de Riemann (sobre su orden de crecimiento, sobre la situación de sus ceros no triviales, etc.) que nos permitirán mejorar los resultados sobre la distribución de los números primos que obtuvimos en el capítulo precedente.

6.1 La ecuación funcional aproximada

Recordemos una vez más que la función dseta de Riemann satisface la ecuación funcional

$$\zeta(s) = \chi(s)\zeta(1-s),$$

donde

$$\chi(s) = 2\Pi(-s)(2\pi)^{s-1}\,\text{sen}\,\frac{\pi s}{2}.$$

En la sección 4.1 presentamos dos fórmulas que relacionaban la función dseta con las sumas parciales de su serie de Dirichlet válidas incluso en la banda crítica, donde ésta no converge. El objeto de esta sección es probar un resultado mucho más fino en esa misma línea, que por su forma recibe el nombre de "ecuación funcional aproximada":

Teorema 6.1 *Sean* $0 \le \sigma \le 1$, $x, y, |\tau| > \delta > 0$ *y* $2\pi xy = |\tau|$. *Entonces*

$$\zeta(s) = \sum_{n\le x} \frac{1}{n^s} + \chi(s)\sum_{n\le y} \frac{1}{n^{1-s}} + O(x^{-\sigma}) + O(|\tau|^{1/2-\sigma} y^{\sigma-1}).$$

Observemos en primer lugar que no perdemos generalidad si demostramos esta fórmula bajo la hipótesis adicional de que $x \le y$. En efecto, si admitimos

que vale en este caso y tomamos $x \geq y$, aplicando la fórmula a $1-s$ resulta que

$$\zeta(1-s) = \sum_{n\leq y} \frac{1}{n^{1-s}} + \chi(1-s) \sum_{n\leq x} \frac{1}{n^s} + O(y^{1-\sigma}) + O(|\tau|^{\sigma-1/2}x^{-\sigma}).$$

Ahora aplicamos la ecuación funcional:

$$\zeta(s) = \chi(s)\zeta(1-s) = \chi(s)\chi(1-s) \sum_{n\leq x} \frac{1}{n^s} + \chi(s) \sum_{n\leq y} \frac{1}{n^{1-s}}$$

$$+\chi(s)O(y^{\sigma-1}) + \chi(s)O(|\tau|^{\sigma-1/2}x^{-\sigma}).$$

Pero aplicando dos veces la ecuación funcional vemos que

$$\zeta(s) = \chi(s)\chi(1-s)\zeta(s),$$

por lo que $\chi(s)\chi(1-s) = 1$. Por otra parte, el teorema 4.8 nos da que

$$\chi(s) = O(|\tau|^{1/2-\sigma}),$$

y así la ecuación precedente se convierte en la del enunciado.

En segundo lugar observamos que tampoco perdemos generalidad si suponemos que $\tau > 0$ (es decir, que $\tau > \delta$). En efecto, si la ecuación funcional aproximada se cumple cuando $\tau > 0$ y tomamos s con $\tau < 0$, aplicamos la ecuación a $\bar{s}$, con lo que obtenemos que

$$\zeta(\bar{s}) = \sum_{n\leq x} \frac{1}{n^{\bar{s}}} + \chi(\bar{s}) \sum_{n\leq y} \frac{1}{n^{1-\bar{s}}} + O(x^{-\sigma}) + O(|\tau|^{1/2-\sigma}y^{\sigma-1}),$$

y basta tener en cuenta que

$$\zeta(\bar{s}) - \sum_{n\leq x} \frac{1}{n^{\bar{s}}} - \chi(\bar{s}) \sum_{n\leq y} \frac{1}{n^{1-\bar{s}}} = \overline{\zeta(s) - \sum_{n\leq x} \frac{1}{n^s} - \chi(s) \sum_{n\leq y} \frac{1}{n^{1-s}}},$$

por lo que

$$\left|\zeta(s) - \sum_{n\leq x} \frac{1}{n^s} - \chi(s) \sum_{n\leq y} \frac{1}{n^{1-s}}\right| = \left|\zeta(\bar{s}) - \sum_{n\leq x} \frac{1}{n^{\bar{s}}} - \chi(\bar{s}) \sum_{n\leq y} \frac{1}{n^{1-\bar{s}}}\right|$$

$$= O(x^{-\sigma}) + O(|\tau|^{1/2-\sigma}y^{\sigma-1}).$$

La prueba que presentamos de la ecuación funcional aproximada es una variante de la prueba de la ecuación funcional que vimos en [An]. Así, el teorema siguiente es una variante de [An 10.36]:

Teorema 6.2 *Para todo número natural m, en el semiplano $\sigma > 1$ se cumple que*

$$\zeta(s) = \sum_{n\leq m} \frac{1}{n^s} + \frac{1}{\Pi(s-1)} \int_0^{+\infty} \frac{x^{s-1}e^{-mx}}{e^x - 1}\, dx.$$

DEMOSTRACIÓN: Supongamos en primer lugar que $s > 1$ es real. Partimos de la expresión integral para la función factorial [VC 4.21]:

$$\Pi(s-1) = \int_0^{+\infty} e^{-y} y^{s-1}\,dy = n^s \int_0^{+\infty} e^{-nx} x^{s-1}\,dx,$$

donde hemos hecho el cambio de variable $y = nx$. De aquí obtenemos:

$$\begin{aligned}
\zeta(s) &= \sum_{n\le m} \frac{1}{n^s} + \sum_{n>m} \frac{1}{n^s} = \sum_{n\le m} \frac{1}{n^s} + \sum_{n>m} \frac{1}{\Pi(s-1)} \int_0^{+\infty} e^{-nx} x^{s-1}\,dx \\
&= \sum_{n\le m} \frac{1}{n^s} + \frac{1}{\Pi(s-1)} \int_0^{+\infty} \sum_{n>m} e^{-nx} x^{s-1}\,dx \\
&= \sum_{n\le m} \frac{1}{n^s} + \frac{1}{\Pi(s-1)} \int_0^{+\infty} \frac{x^{s-1} e^{-(m+1)x}}{1-e^{-x}}\,dx \\
&= \sum_{n\le m} \frac{1}{n^s} + \frac{1}{\Pi(s-1)} \int_0^{+\infty} \frac{x^{s-1} e^{-mx}}{e^x-1}\,dx.
\end{aligned}$$

En el segundo paso hemos intercambiado la serie con la integral. Esto es correcto porque las sumas parciales $\sum_{n=m+1}^{N} e^{-nx} x^{s-1}$ forman una sucesión creciente de funciones positivas, por lo que podemos aplicar el teorema de la convergencia monótona.

Para el caso general basta probar que la integral

$$\int_0^{+\infty} \frac{x^{s-1} e^{-mx}}{e^x-1}\,dx$$

define una función holomorfa en el semiplano $\sigma > 1$, pues entonces podemos concluir que la igualdad del enunciado vale en general en virtud del principio de prolongación analítica. Para ello, según [VC 1.24], basta probar que, en cada banda vertical $1 < 1+\delta \le \sigma \le c$, el integrando está acotado por una función integrable $f(x)$ (independiente de s). Ahora bien,

$$\left|\frac{x^{s-1} e^{-mx}}{e^x-1}\right| = \frac{x^{\sigma-1} e^{-mx}}{e^x-1}.$$

Si $0 < x \le 1$ entonces $x^{\sigma-1} \le x^{\delta}$ y $e^x - 1 \ge x$, luego

$$\frac{x^{\sigma-1} e^{-mx}}{e^x-1} \le \frac{x^{\delta} e^{-mx}}{e^x-1} \le x^{\delta-1},$$

y la función $x^{\delta-1}$ es integrable en $]0,1]$. Si $x \ge 1$ entonces

$$\frac{x^{\sigma-1} e^{-mx}}{e^x-1} \le \frac{x^{c-1} e^{-mx}}{e^x-1}$$

y la última función es integrable en $]0,+\infty[$ por el caso real ya probado. ∎

Ahora probamos una variante de [An 10.37]:

Teorema 6.3 *Sea m un número natural, sea $0 < \epsilon < 2\pi$ y sea C la unión de las curvas C_1, C_2, C_3 dadas por*

$$\begin{aligned} -C_1 &\equiv z = re^{0i}, \quad r \in [\epsilon, +\infty[\,,\\ C_2 &\equiv z = \epsilon e^{i\theta}, \quad \theta \in [0, 2\pi],\\ C_3 &\equiv z = re^{2\pi i}, \quad r \in [\epsilon, +\infty[\,, \end{aligned}$$

Entonces, la función

$$I(s,m) = \int_C \frac{z^{s-1}e^{-mz}}{e^z - 1}\, dz$$

es entera, no depende de la elección de ϵ y

$$\zeta(s) = \sum_{n\le m} \frac{1}{n^s} + \frac{e^{-\pi i s}\Pi(-s)}{2\pi i} I(s,m).$$

Como en [An 10.37], hay que entender que z^{s-1} se calcula con el logaritmo con parte imaginaria nula sobre C_1, con parte imaginaria en $[0, 2\pi]$ sobre C_2 y con parte imaginaria 2π sobre C_3.

Demostración: Como en [An 10.37], la integral sobre C_2 define una función entera. Sobre C_1 y C_2 basta probar que, cuando $|s-1| \le M$, el integrando está acotado por una función integrable independiente de s. Ahora bien, sobre C_1 tenemos que $z = x > \epsilon$ y $|z^{s-1}| = x^{\sigma-1} \le x^M$, mientras que sobre C_3 es

$$|z^{s-1}| = x^{\sigma-1}e^{-2\pi\tau} \le x^M e^{2\pi M}.$$

En ambos casos

$$\left|\frac{z^{s-1}e^{-mz}}{e^z-1}\right| \le \frac{cx^M e^{-mx}}{e^x - 1}$$

y esta función es integrable en $]0, +\infty[$ por el teorema anterior.

Esto prueba que $I(s,m)$ es una función entera, y el mismo argumento de [An 10.37] muestra que no depende de la elección de ϵ. Observemos ahora que, sobre C_3, la potencia z^{s-1} está definida como

$$z^{s-1} = e^{(s-1)(\log|z| + 2\pi i)} = x^{s-1}e^{2\pi i s}e^{-2\pi i} = x^{s-1}e^{2\pi i s},$$

luego

$$\begin{aligned} I(s,m) &= -\int_\epsilon^{+\infty} \frac{x^{s-1}e^{-mx}}{e^x-1}\, dx + \int_{|z|=\epsilon} \frac{z^{s-1}e^{-mz}}{e^z-1}\, dz + e^{2\pi i s}\int_\epsilon^{+\infty} \frac{x^{s-1}e^{-mx}}{e^x-1}\, dx\\ &= (e^{2\pi i s} - 1)\int_\epsilon^{+\infty} \frac{x^{s-1}e^{-mx}}{e^x-1}\, dx + \int_{|z|=\epsilon} \frac{z^{s-1}e^{-mz}}{e^z-1}\, dz. \end{aligned}$$

Veamos seguidamente que, si $\sigma > 1$, la última integral tiende a 0 cuando $\epsilon \to 0$. En efecto, la función $g(z) = e^{-mz}/(e^z - 1)$ es holomorfa en $D(0, 2\pi)$

salvo en $z = 0$, donde tiene un polo simple, por lo que $zg(z)$ está acotada. Por lo tanto,

$$\left|\int_{|z|=\epsilon} \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz\right| = \left|\int_0^{2\pi} e^{(s-1)(\log\epsilon+i\theta)}g(\epsilon e^{i\theta})i\epsilon e^{i\theta}\,d\theta\right|$$

$$\leq c\epsilon^{\sigma-1}\int_0^{2\pi} e^{-\tau\theta}\,d\theta \leq c\epsilon^{\sigma-1}2\pi e^{2\pi|\tau|},$$

que ciertamente tiende a 0 con ϵ. Así pues, por el teorema anterior,

$$I(s,m) = (e^{2\pi is}-1)\int_0^{+\infty}\frac{x^{s-1}e^{-mx}}{e^x-1}\,dx = (e^{2\pi is}-1)\Pi(s-1)\Big(\zeta(s)-\sum_{n\leq m}\frac{1}{n^s}\Big).$$

Equivalentemente,

$$\zeta(s) = \sum_{n\leq m}\frac{1}{n^s} = \frac{I(s,m)}{(e^{2\pi is}-1)\Pi(s-1)} = \frac{e^{-\pi is}I(s,m)}{(e^{\pi is}-e^{-\pi is})\Pi(s-1)}$$

$$= \frac{e^{-\pi is}I(s,m)}{2i(\operatorname{sen}\pi s)\Pi(s-1)},$$

y así [VC 4.26] nos da la fórmula del enunciado, en principio para $\sigma > 1$, pero por el principio de prolongación analítica la igualdad vale para todo s. ∎

El paso siguiente es una variante de [An 10.42]:

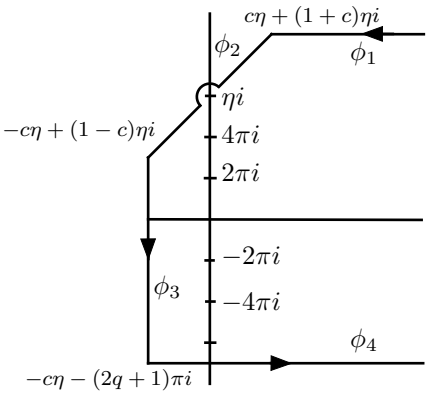
Teorema 6.4 *Fijados $0 \leq c \leq 1/2$, $\delta > 0$, $0 < r < 2\pi c\delta$, $r \leq \pi/2$, tomamos $s \in \mathbb{C}$ tal que $\tau > \delta$ y dos números reales $x, y > \delta$. Llamamos $m = E[x]$, $q = E[y]$, $\eta = 2\pi y$. Consideramos la curva $\phi = \phi_1 \cup \phi_2 \cup \phi_3 \cup \phi_4$ descrita en la figura, donde ϕ_2 es el segmento que une $c\eta + (1+c)\eta i$ con $-c\eta + (1-c)\eta i$ salvo si éste corta a un disco $D(2k\pi i, r)$, necesariamente con $k = q$ o $k = q+1$, en cuyo caso rodeamos el disco con un arco de circunferencia de radio r, el adecuado para que $2q\pi i$ quede por debajo del arco, pero $2(q+1)\pi i$ quede por encima. Entonces*

$$\zeta(s) = \sum_{n\leq x}\frac{1}{n^s} + \chi(s)\sum_{n\leq y}\frac{1}{n^{1-s}} + \frac{e^{-\pi is}\Pi(-s)}{2\pi i}\int_\phi \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz,$$

donde $z^{s-1} = e^{(s-1)\log z}$ se calcula con el logaritmo de z con parte imaginaria en $]0, 2\pi[$.

Demostración: Observemos que la condición $r < 2\pi c\delta$ garantiza dos cosas. Por una parte, que $r < c\eta$, por lo que, si es necesario rodear un punto $2k\pi i$, el arco de circunferencia queda "en medio" del segmento que constituye la mayor parte de ϕ_2, sin rebasar sus extremos. Por otra parte, hace imposible que dicho segmento entre en el disco $D(0,r)$, por lo que nunca puede ser $k = 0$. Más concretamente, para esto basta con que $r < 2\pi y/\sqrt{2}$ y, en particular, con que $r < \sqrt{2}\pi\delta$.

Veamos en primer lugar que la integral define una función entera, para lo cual basta probarlo para las integrales sobre ϕ_1 y ϕ_4. Las dos curvas son de la forma $\phi_j(x) = x + \alpha i$, y basta probar la integrabilidad en un intervalo $]a, +\infty[$, con a arbitrariamente grande. Ahora bien:[1]



$$\left|\frac{z^{s-1}e^{-mz}}{e^z-1}\right| \le \frac{|z|^{\sigma-1}e^{2\pi|\tau|}e^{-mx}}{e^x-1}$$

$$\le 2|z|^{\sigma-1}e^{2\pi|\tau|}e^{-x}$$

si $x > \log 2$ (pues entonces $e^x - 1 > e^x/2$). Para $x \ge |\alpha|$ se cumple que $|\phi_j(x)| \le \sqrt{2}x$. Por consiguiente, si llamamos $f(z)$ al integrando, tenemos que

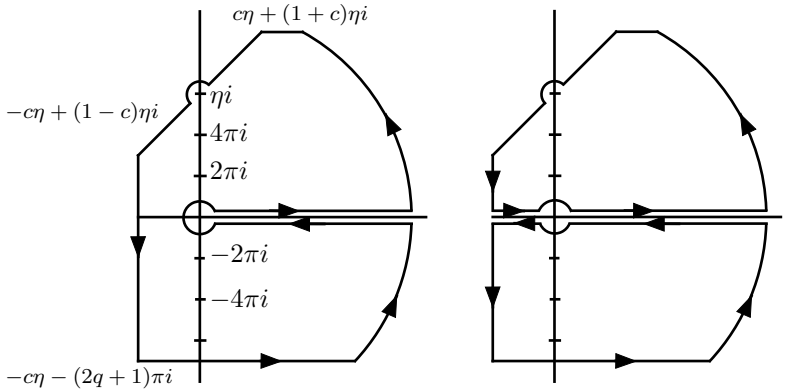
$$|f(\phi_i(x))\phi_j'(x)| \le 2A^{\sigma-1}e^{2\pi|\tau|}x^{\sigma-1}e^{-x}.$$

Si restringimos s a un compacto, podemos acotar $\sigma - 1 \le \sigma_0$ y $|\tau| \le \tau_0$, y así

$$|f(\phi_j(x))\phi_j'(x)| \le Ax^{\sigma_0}e^{-x},$$

y el miembro derecho es una función integrable en $]0, +\infty[$, pues la integral es la función factorial $\Pi(\sigma_0)$. El teorema [IC 7.10] prueba entonces que la integral del enunciado define una función entera.

Ahora consideramos el arco cerrado γ que muestra la figura de la izquierda:



Se trata de la curva ϕ truncada con dos arcos de circunferencia de centro 0 y radio R suficientemente grande, entre los cuales se intercala el segmento real $[\epsilon, R]$ en sentido negativo, con $0 < \epsilon < 2\pi i$, luego la circunferencia de radio ϵ, seguida del segmento $[\epsilon, R]$ en sentido positivo. Consideramos la integral de $f(z)$

[1] En todo lo que sigue x e y representan la parte real y la parte imaginaria de z, que no hay que confundir con los números x, y del enunciado, que no intervienen en ningún momento en los cálculos siguientes.

sobre γ, entendiendo que z^{s-1} se calcula con el logaritmo de parte imaginaria 2π en el segmento $[\epsilon, R]$ recorrido en sentido negativo, con parte imaginaria en $[0, 2\pi]$ sobre la circunferencia de radio ϵ y con parte imaginaria 0 sobre el segmento $[\epsilon, R]$ en sentido positivo.

No es posible aplicar el teorema de los residuos a $f(z)$ sobre este arco, porque $f(z)$ no se extiende a una función holomorfa en un entorno de γ^*. No obstante, podemos descomponer γ en los dos arcos cerrados que muestra la figura de la derecha, y en cada uno de ellos sí que es posible aplicar el teorema de los residuos, considerando una extensión distinta de f en cada caso a todo el plano complejo menos una semirrecta, de modo que z^{s-1} se calcula siempre con logaritmos con parte imaginaria en $[0, 2\pi]$. Al sumar las igualdades que proporciona el teorema de los residuos sobre ambos arcos, se cancelan las integrales sobre los dos segmentos que hemos introducido en el semieje real negativo y el resultado es formalmente idéntico a aplicar el teorema de los residuos a γ, es decir:

$$\frac{1}{2\pi i}\int_\gamma \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = \sum_{n=1}^{q}(\mathrm{Res}(f, 2n\pi i) + \mathrm{Res}(f, -2n\pi i)).$$

Ahora observamos que la longitud de los arcos de circunferencia de radio R tiende a $(1+c)\eta + (2a+1)\pi$, luego permanece acotada cuando R tiende a $+\infty$. En efecto, por ejemplo, la amplitud del arco superior es $\mathrm{arcsen}((1+c)\eta/R)$, luego la longitud es $R\,\mathrm{arcsen}((1+c)\eta/R)$ y, aplicando la regla de L'Hôpital, vemos que el límite es $(1+c)\eta$.

Si x_0 es el menor valor de x sobre el arco, vemos que guarda con R una relación de la forma $x_0^2 + k^2 = R^2$, luego, x_0/R tiende a 1 y, si R es suficientemente grande, $x_0 \geq R/2$. Además,

$$|f(z)| \leq 2R^{\sigma-1}e^{2\pi|\tau|}e^{-x} \leq 2R^{\sigma-1}e^{2\pi|\tau|}e^{-x_0},$$

luego la integral sobre el arco de circunferencia está acotada por $AR^{\sigma-1}e^{-R/2}$, que tiende a 0 cuando R tiende a $+\infty$. Así pues,

$$\int_\phi \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz - I(s,m) = 2\pi i\sum_{n=1}^{q}(\mathrm{Res}(f, 2n\pi i) + \mathrm{Res}(f, -2n\pi i)).$$

El teorema anterior implica entonces que

$$\zeta(s) = \sum_{n\leq m}\frac{1}{n^s} - e^{-\pi i s}\Pi(-s)\sum_{n=1}^{q}(\mathrm{Res}(f, 2n\pi i) + \mathrm{Res}(f, -2n\pi i)) + \int_\phi \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz.$$

El teorema [VC 3.16] nos permite calcular los residuos:

$$\mathrm{Res}(f, 2n\pi i) + \mathrm{Res}(f, -2n\pi i) = (2n\pi i)^{s-1} + (-2n\pi i)^{s-1}$$
$$= (2n\pi)^{s-1}(e^{\pi i(s-1)/2} + e^{3\pi i(s-1)/2}) = e^{\pi i s}(2n\pi)^{s-1}(-ie^{-\pi i s/2} + ie^{\pi i s/2})$$
$$= -2e^{\pi i s}(2n\pi)^{s-1}\,\mathrm{sen}\,\frac{\pi s}{2}.$$

Por consiguiente,

$$e^{-\pi is}\Pi(-s)\sum_{n=1}^{q}(\operatorname{Res}(f,2n\pi i)+\operatorname{Res}(f,-2n\pi i))$$

$$=-2(2\pi)^{s-1}\Pi(-s)\operatorname{sen}\frac{\pi s}{2}\sum_{n\le q}\frac{1}{n^{1-s}}=-\chi(s)\sum_{n\le q}\frac{1}{n^{1-s}}.$$

Esto nos da la fórmula del enunciado. ∎

Para probar el teorema 6.1 sólo tenemos que probar que el último término que aparece en la fórmula del teorema anterior es $O(x^{-\sigma})+O(\tau^{1/2-\sigma}y^{\sigma-1})$.

A partir de aquí suponemos que $0\le\sigma\le 1$ y que $2\pi xy=\tau$.

En primer lugar estimamos el término $e^{-\pi is}\Pi(-s)$ mediante la fórmula de Stirling [VC 4.30]:

$$\Pi(-s)=\sqrt{2\pi}(-s)^{1/2-s}e^{s}e^{\mu(-s)},$$

de donde

$$\begin{aligned}|e^{-\pi is}\Pi(-s)|&=\sqrt{2\pi}e^{\pi\tau}|s|^{1/2-\sigma}e^{\tau\arg(-s)}e^{\sigma}|e^{\mu(-s)}|\\&\le\sqrt{2\pi}e^{\pi\tau}|s|^{1/2-\sigma}e^{-\pi\tau/2}e|e^{\mu(-s)}|,\end{aligned}$$

donde hemos usado que $-s$ tiene parte real e imaginaria negativas, luego su argumento en $]-\pi,\pi[$ tiene que estar de hecho en $]-\pi,-\pi/2[$.

Teniendo en cuenta que $|-s|\ge\tau>\delta$, el teorema [VC 4.29] implica que $|\mu(-s)|$ está acotado. Por otra parte,

$$\frac{|s|^2}{\tau^2}=\frac{\sigma^2}{\tau^2}+1\le\frac{\sigma_0^2}{\delta^2}+1=A^2,$$

luego

$$\left(\frac{|s|}{\tau}\right)^{1/2-\sigma}\le\frac{|s|}{\tau}\le A.$$

Por consiguiente,

$$e^{-\pi is}\Pi(-s)=O(\tau^{1/2-\sigma}e^{\pi\tau/2}).$$

Ahora nos ocupamos de la integral, pero antes conviene hacer una observación general, y es que, si $A>0$, $e^{-A\tau}=O(y^{-1})$.

En efecto,

$$ye^{-A\tau}=ye^{-A2\pi xy}\le ye^{-A2\pi\delta y}$$

y la última expresión tiende a 0 con y, luego está acotada.

Para cada número complejo z que no esté en el semieje real positivo, sobrentenderemos que sus coordenadas polares son $z=\rho e^{i\theta}$, con $0<\theta<2\pi$.

Supongamos en primer lugar que $z=\phi_1(u)=u+(1+c)\eta i$. Entonces $\rho\ge(1+c)\eta\ge\eta$ y, si $u\ge\log 2$,

$$|e^z-1|\ge e^u-1\ge e^u/2.$$

Como $u \geq 2\pi\delta c$, existe una constante K tal que

$$|e^z - 1|^{-1} \leq (e^u - 1)^{-1} \leq Ke^{-u},$$

y así

$$\left|\frac{z^{s-1}e^{-mz}}{e^z - 1}\right| \leq K\rho^{\sigma-1}e^{-\tau\theta}e^{-(m+1)u} \leq K\eta^{\sigma-1}e^{-\tau\theta-(m+1)u}.$$

Además,

$$\theta = \arctan\frac{(1+c)\eta}{u}.$$

Como

$$\frac{d}{du}\left(\arctan\frac{(1+c)\eta}{u} + \frac{u}{\eta}\right) = -\frac{(1+c)\eta}{u^2 + (1+c)^2\eta^2} + \frac{1}{\eta} > -\frac{(1+c)\eta}{(1+c)^2\eta^2} + \frac{1}{\eta} = 0,$$

y $u \geq c\eta$, tenemos que

$$\theta = \arctan\frac{(1+c)\eta}{u} + \frac{u}{\eta} \geq \arctan\frac{1+c}{c} + c = \frac{\pi}{2} + c - \arctan\frac{c}{1+c} = \frac{\pi}{2} + A,$$

pues

$$\arctan\frac{c}{1+c} = \int_0^{c/(1+c)} \frac{dp}{1+p^2} < \int_0^{c/(1+c)} \frac{dp}{(1-p)^2} = c.$$

Notemos que $A < c \leq 1/2$. Teniendo en cuenta además que $m + 1 \geq x = \tau/\eta$, vemos que

$$\left|\frac{z^{s-1}e^{-mz}}{e^z - 1}\right| \leq K\eta^{\sigma-1}e^{-\tau(\pi/2+A-u/\eta)-\tau u/\eta} = K\eta^{\sigma-1}e^{-\tau(\pi/2+A)}.$$

Una cota alternativa es

$$\left|\frac{z^{s-1}e^{-mz}}{e^z - 1}\right| \leq K\rho^{\sigma-1}e^{-\tau\theta}e^{-(m+1)u} \leq K\eta^{\sigma-1}e^{-xu}.$$

Partimos la integral en dos y usamos cada cota en una de las partes:

$$\left|\int_{\phi_1} \frac{z^{s-1}e^{-mz}}{e^z - 1}\,dz\right| \leq \int_{c\eta}^{\pi\eta} K\eta^{\sigma-1}e^{-\tau(\pi/2+A)}\,du + \int_{\pi\eta}^{+\infty} K\eta^{\sigma-1}e^{-xu}\,du$$

$$\leq K\pi\eta^{\sigma}e^{-\tau(\pi/2+A)} + K\eta^{\sigma-1}\frac{1}{x}e^{-x\pi\eta} \leq$$

$$K\pi\eta^{\sigma}e^{-\tau(\pi/2+A)} + K\eta^{\sigma-1}\frac{1}{\delta}e^{-\tau\pi} \leq \frac{K}{2\pi\delta^2}\eta^{\sigma}e^{-\tau(\pi/2+A)} \leq$$

$$\frac{K}{\delta^2}y^{\sigma}e^{-\tau(\pi/2+A)},$$

pues, teniendo en cuenta que $A \leq 1/2 < \pi/2$,

$$\frac{\eta^{\sigma-1}e^{-\pi\tau}}{\eta^{\sigma}e^{-\tau(\pi/2+A)}} = \frac{1}{\eta}e^{-\tau(\pi/2-A)} \leq \frac{1}{2\pi\delta}.$$

Por lo tanto,

$$\frac{e^{-\pi is}\Pi(-s)}{2\pi i}\int_{\phi_1}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\tau^{1/2-\sigma}y^\sigma e^{-\tau A}) = O(\tau^{1/2-\sigma}y^{\sigma-1}).$$

Ahora consideramos un punto $z=\phi_3(u)=-c\eta+ui$. El menor valor de θ se alcanza cuando $u=\eta(1+c)$, con lo que

$$\theta \ge \frac{\pi}{2}+\arctan\frac{c}{1-c} = \frac{\pi}{2}+\int_0^{c/(1-c)}\frac{dp}{1+p^2} =$$

$$\frac{\pi}{2}+A+\int_0^{c/(1-c)}\frac{dp}{(1+p)^2} = \frac{\pi}{2}+A+c,$$

donde

$$A=\int_0^{c/(1-c)}\left(\frac{1}{1+p^2}-\frac{1}{(1+p)^2}\right)dp>0.$$

Obviamente $\rho\ge\eta$, luego

$$|z^{s-1}e^{-mz}| = \rho^{\sigma-1}e^{-\tau\theta}e^{mc\eta} \le \eta^{\sigma-1}e^{-\tau(\pi/2+A+c)}e^{\tau c} = \eta^{\sigma-1}e^{-\tau(\pi/2+A)}.$$

Por otra parte,

$$|e^z-1| \ge 1-e^{-c\eta} \ge 1-e^{-2\pi c\delta} = A > 0,$$

luego

$$\left|\int_{\phi_3}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz\right| \le \eta^{\sigma-1} \le A\eta^{\sigma-1}e^{-\tau(\pi/2+A)}\int_{-(2q+1)\pi}^{(1-c)\eta}du$$

$$\le A\eta^\sigma e^{-\tau(\pi/2+A)} \le A2\pi y^\sigma e^{-\tau(\pi/2+A)},$$

donde usamos que

$$(1-c)\eta+(2q+1)\pi \le \eta+2\pi y+\pi = 2\eta+\pi \le A\eta,$$

pues $2+\pi/\eta \le 2+\dfrac{\pi}{2\pi\delta} = A$. Como antes,

$$\frac{e^{-\pi is}\Pi(-s)}{2\pi i}\int_{\phi_3}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\tau^{1/2-\sigma}y^\sigma e^{-A\tau}) = O(\tau^{1/2-\sigma}y^{\sigma-1}).$$

Supongamos ahora que $z=\phi_4(u)=u-(2q+1)\pi i$. El menor valor de θ se obtiene cuando $u=-c\eta$ y cumple que

$$\frac{\operatorname{Re} z}{\operatorname{Im} z} = \frac{c\eta}{(2q+1)\pi} \le \frac{\pi y}{(2q+1)\pi} \le \frac{q+1}{2q+1} < 1,$$

luego $\theta > 5\pi/4$. Por otra parte, el mínimo de ρ se alcanza cuando $u=0$, con lo que $\rho \ge (2q+1)\pi \ge (q+1)\pi > y\pi = \eta/2$. Por otra parte,

$$|e^z-1| = |e^ue^{-(2q+1)\pi i}-1| = |-e^u-1| = e^u+1 \ge 1,$$

luego

$$\left|\frac{z^{s-1}e^{-mz}}{e^z-1}\right| \le \rho^{\sigma-1}e^{-\tau\theta}e^{-mu} \le (\eta/2)^{\sigma-1}e^{-5\tau\pi/4}e^{-mu} \le 2\eta^{\sigma-1}e^{-5\tau\pi/4}e^{-mu}.$$

Si $m \ge 1$,

$$\left|\int_{\phi_4}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz\right| \le A\eta^{\sigma-1}e^{-5\tau\pi/4}\int_{-c\eta}^{+\infty}e^{-mu}\,du$$

$$\le A\eta^{\sigma-1}e^{mc\eta-5\tau\pi/4} \le A\eta^{\sigma-1}e^{\tau c-5\pi\tau/4} \le 2\pi A y^{\sigma-1}e^{\tau c-5\pi\tau/4},$$

donde hemos usado que $m\eta = E[x]2\pi y \le 2\pi xy = \tau$. De aquí, a su vez,

$$\frac{e^{-\pi is}\Pi(-s)}{2\pi i}\int_{\phi_4}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\tau^{1/2-\sigma}y^{\sigma-1}e^{-\tau(3\pi/4-c)}) = O(\tau^{1/2-\sigma}y^{\sigma-1}).$$

Si $m = 0$, es decir, si $\delta \le x < 1$, dividimos en dos la integral y en la segunda parte usamos la cota $|e^z - 1| \ge e^u$:

$$\left|\int_{\phi_4}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz\right| \le \int_{-c\eta}^{\pi\eta}A\eta^{\sigma-1}e^{-5\tau\pi/4}\,du + \int_{\pi\eta}^{+\infty}A\eta^{\sigma-1}e^{-5\tau\pi/4}e^{-u}\,du$$

$$\le A\eta^{\sigma}e^{-5\tau\pi/4} + A\eta^{\sigma-1}e^{-5\tau\pi/4}e^{-\pi\eta} \le A\eta^{\sigma}e^{-5\tau\pi/4} + A\eta^{\sigma-1}e^{-5\tau\pi/4}e^{-\pi 2\pi xy}$$

$$= A\eta^{\sigma}e^{-5\tau\pi/4} + A\eta^{\sigma-1}e^{-5\tau\pi/4}e^{-\pi\tau} = A\eta^{\sigma}e^{-5\tau\pi/4} + A\eta^{\sigma-1}e^{-9\tau\pi/4}$$

$$= A\eta^{\sigma}e^{-5\tau\pi/4} \le A2\pi y^{\sigma}e^{-5\pi\tau/4},$$

y nuevamente,

$$\frac{e^{-\pi is}\Pi(-s)}{2\pi i}\int_{\phi_4}\frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\tau^{1/2-\sigma}y^{\sigma}e^{-3\pi\tau/4}) = O(\tau^{1/2-\sigma}y^{\sigma-1}).$$

Sólo falta considerar el caso en que z está sobre ϕ_2^*. Llamamos ϕ_{21} al segmento

$$\phi_{21}(\lambda) = \eta i + \lambda e^{\pi i/4}, \qquad \text{con } -\sqrt{2}c\eta \le \lambda \le \sqrt{2}c\eta,$$

de modo que ϕ_2 puede coincidir con ϕ_{21}, o bien es ϕ_{21} menos un segmento central que es sustituido por un arco de circunferencia ϕ_{22}.

Nos ocupamos en primer lugar de ϕ_{21}. Si $z = \phi_{21}(\lambda)$, entonces

$$z = i(\eta + \lambda e^{\pi i/4}) = i\eta(1 + (\lambda/\eta)e^{-i\pi/4}).$$

De aquí se sigue que

$$\log z = \frac{\pi}{2}i + \log\eta + \log(1 + \frac{\lambda}{\eta}e^{-i\pi/4}),$$

donde el logaritmo de la izquierda es el de parte imaginaria en $]0, 2\pi[$, mientras que los de la derecha son los de parte imaginaria en $]-\pi, \pi[$. En efecto, basta probar que

$$\mathrm{Re}(1 + \frac{\lambda}{\eta}e^{-i\pi/4}) > 0,$$

pues entonces la parte imaginaria del logaritmo está en $]-\pi/2, \pi/2[$, y al sumarle π obtenemos una parte imaginaria en $]0, 2\pi[$. Ahora bien,

$$\operatorname{Re}(1+\frac{\lambda}{\eta}e^{-i\pi/4}) = 1+\frac{\lambda}{\eta}\frac{\sqrt{2}}{2} \geq 1-\frac{\sqrt{2}}{2}\frac{\sqrt{2}}{2} = \frac{1}{2} > 0.$$

El logaritmo con parte imaginaria en $]0, 2\pi[$ es el que necesitamos para calcular la exponencial compleja z^{s-1} del integrando. Concretamente:

$$z^{s-1} = e^{(s-1)(\frac{\pi}{2}i+\log\eta+\log(1+\frac{\lambda}{\eta}e^{-\pi i/4}))},$$

luego

$$|z^{s-1}| = \eta^{\sigma-1}e^{-\pi/2}e^{\operatorname{Re}((s-1)\log(1+\frac{\lambda}{\eta}e^{-\pi i/4}))}.$$

El desarrollo de Taylor del logaritmo nos da que

$$\log(1+\frac{\lambda}{\eta}e^{-\pi i/4}) = \frac{\lambda}{\eta}e^{-i\pi/4} - \frac{\lambda^2}{2\eta^2}e^{-i\pi/2} + \frac{\lambda^3}{\eta^3}h_0(\lambda/\eta),$$

para cierta función continua $h_0 : [-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}] \longrightarrow \mathbb{C}$ (en realidad está definida en $]-1, 1[$, pero la restringimos a un intervalo compacto menor para tenerla acotada). Por lo tanto,

$$\operatorname{Re}((s-1)\log(1+\frac{\lambda}{\eta}e^{-i\pi/4})) = (\sigma-1)\frac{\lambda}{\eta}\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\frac{\lambda}{\eta}\tau - \frac{\lambda^2}{2\eta^2}\tau$$

$$+(\sigma-1)\frac{\lambda^3}{\eta^3}\operatorname{Re}h_0(\lambda/\eta) - \tau\frac{\lambda^3}{\eta^3}\operatorname{Im}h_0(\lambda/\eta).$$

Tanto $\sigma-1$ como λ/η y h_0 están acotados, luego concluimos que

$$|z^{s-1}| \leq A\eta^{\sigma-1}e^{(-\frac{\pi}{2}+\frac{\sqrt{2}}{2}\frac{\lambda}{\eta}-\frac{\lambda^2}{2\eta^2})\tau+(\lambda/\eta)^3h(\lambda/\eta)\tau},$$

donde $h : [-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}] \longrightarrow \mathbb{R}$ es la parte real de h_0.

Por [An 10.40] sabemos que existe una constante $A > 0$ tal que $|e^z-1|^{-1} \leq A$ en la región Ω que resulta de quitarle al plano complejo el disco abierto de centro cada punto $2n\pi i$ y radio r. Tomemos un punto $z \in \Omega$ y distingamos varios casos:

- Si $\operatorname{Re}z > \pi/2$, tenemos que

$$\left|\frac{e^{-mz+xz}}{e^z-1}\right| = \frac{e^{(x-m)\operatorname{Re}z}}{|e^z-1|} \leq \frac{e^{(x-m)\operatorname{Re}z}}{e^{\operatorname{Re}z}-1} = \frac{e^{(x-m-1)\operatorname{Re}z}}{1-e^{-\operatorname{Re}z}} \leq \frac{1}{1-e^{-\pi/2}}.$$

- Si $0 \leq \operatorname{Re}z \leq \pi/2$, entonces

$$\left|\frac{e^{-mz+xz}}{e^z-1}\right| \leq Ae^{(x-m)\operatorname{Re}z} \leq Ae^{\pi/2}.$$

- Si $\operatorname{Re} z < 0$, entonces

$$\left|\frac{e^{-mz+xz}}{e^z-1}\right| = \frac{e^{(x-m)\operatorname{Re} z}}{|e^z-1|} \le A.$$

Si además z está en ϕ_{21}^*,

$$|e^{-xz}| = |e^{-x(\eta i+\lambda e^{i\pi/4})}| = e^{-x\lambda\sqrt{2}/2} = e^{-\frac{\lambda\tau\sqrt{2}}{2\eta}}.$$

Concluimos que, para todo $z \in \phi_2^* \cap \Omega$, se cumple que

$$\left|\frac{e^{-mz}}{e^z-1}\right| \le Ae^{-\frac{\lambda\tau\sqrt{2}}{2\eta}},$$

y a su vez,

$$\left|\frac{z^{s-1}e^{-mz}}{e^z-1}\right| \le A\eta^{\sigma-1}e^{-\pi\tau/2}e^{-\frac{\lambda^2}{2\eta^2}\tau+\tau h(\lambda/\eta)\frac{\lambda^3}{\eta^3}}.$$

Recordemos que la función h depende únicamente de la serie de Taylor de $\log(1+z)$. Tenemos que $|\lambda/\eta| \le c\sqrt{2}$, y en este punto determinamos la constante c exigiendo que $|h(t)t| \le 1/4$ cuando $|t| \le c$. De este modo,

$$h(\lambda/\eta)\frac{\lambda^3}{\eta^3} \le \frac{\lambda^2}{4\eta^2},$$

luego

$$-\frac{\lambda^2}{2\eta^2}\tau + \tau h(\lambda/\eta)\frac{\lambda^3}{\eta^3} \le -\frac{\lambda^2}{4\eta^2}\tau.$$

De este modo

$$\left|\int_{\phi_{21}} \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz\right| \le A\eta^{\sigma-1}e^{-\tau\pi/2}\int_{-c\eta\sqrt{2}}^{c\eta\sqrt{2}} e^{-\frac{\lambda^2}{4\eta^2}\tau}\,d\lambda \le$$

$$A\eta^{\sigma-1}e^{-\tau\pi/2}\int_{-\infty}^{+\infty} e^{-\frac{\tau}{4\eta^2}\lambda^2}\,d\lambda$$

$$= \frac{2A\eta^\sigma}{\sqrt{\tau}}e^{-\tau\pi/2}\int_{-\infty}^{+\infty} e^{-t^2}\,dt = O(\eta^\sigma\tau^{-1/2}e^{-\tau\pi/2}).$$

Ahora nos ocupamos del posible arco ϕ_{22} de centro $2k\pi i$ y radio r, cuya longitud está acotada por $2\pi r$, luego sólo tenemos que preocuparnos de acotar el integrando. Recordemos que $k = q$ o bien $k = q+1$, pero que, en cualquier caso, $k \ne 0$. Consideremos un punto

$$z = \phi_{22}(\theta) = 2k\pi i + re^{i\theta} = 2k\pi i(1 - \frac{ri}{2k\pi}e^{i\theta}).$$

Entonces

$$\log z = \frac{\pi}{2}i + \log 2k\pi + \log(1 - \frac{ri}{2k\pi}e^{i\theta}),$$

donde, nuevamente, el logaritmo de la derecha es el de parte imaginaria en $]0, 2\pi[$ (el necesario para calcular z^{s-1}) y los de la derecha son los de parte imaginaria en $]-\pi, \pi[$. Nuevamente consideramos el desarrollo de Taylor de $\log(1-z)$, según el cual

$$\log z = \frac{\pi}{2}i + \log 2k\pi - \frac{ri}{2k\pi}e^{i\theta} + \frac{r^2}{4k^2\pi^2}e^{2\theta i}h(\frac{ri}{2k\pi}e^{i\theta}),$$

donde h es una función acotada en $\overline{D(0,r)}$. Consecuentemente,

$$(s-1)\log z = (\sigma-1)\frac{\pi}{2}i - \tau\frac{\pi}{2} + (s-1)\log 2k\pi - \frac{(\sigma-1)ri}{2k\pi}e^{i\theta} + \frac{\tau r}{2k\pi}e^{i\theta}$$

$$+\frac{(\sigma-1)r^2}{4k^2\pi^2}e^{2\theta i}h(\frac{ri}{2k\pi}e^{i\theta}) + \frac{\tau}{k^2}\frac{r^2 i}{4\pi^2}e^{2\theta i}h(\frac{ri}{2k\pi}e^{i\theta}).$$

Es claro que el primer término y el sexto están acotados. Como hemos visto al principio de la sección, no perdemos generalidad si suponemos que $x \leq y$, y vamos a ver que, bajo esta hipótesis, también está acotado el séptimo término. Sólo hay que probar que lo está τ/k^2. Ahora bien:

- Si $y \geq 1$, tenemos que

$$\frac{\tau}{k^2} \leq \frac{2\pi xy}{q^2} \leq \frac{2\pi y^2}{q^2} = 2\pi\left(\frac{q+\epsilon}{q}\right)^2 \leq 8\pi.$$

- Si $\delta \leq y < 1$, entonces

$$\frac{\tau}{k^2} \leq \frac{2\pi y^2}{1} \leq 2\pi.$$

Así pues:

$$(s-1)\log z = -\tau\frac{\pi}{2} + (s-1)\log 2k\pi + \frac{\tau r}{2k\pi}e^{i\theta} + O(1).$$

Por otra parte,

$$e^{-mz} = e^{-m(2k\pi i + re^{i\theta})} = e^{-mre^{i\theta}}.$$

Por consiguiente,

$$z^{s-1}e^{-mz} = e^{re^{i\theta}(\frac{\tau}{2k\pi}-m)-\tau\frac{\pi}{2}+(s-1)\log 2k\pi+O(1)}.$$

Ahora observamos que

$$\frac{\tau}{2k\pi} - m = \frac{xy-km}{k} = \frac{(x-m)k + (y-k)m + (x-m)(y-q)}{k}.$$

Como $|x-m| \leq 1$ y, por definición de k, también $|y-k| \leq 1$, la expresión anterior está acotada. Así llegamos a que

$$z^{s-1}e^{-mz} = e^{-\tau\frac{\pi}{2}+(s-1)\log 2k\pi+O(1)}.$$

Puesto que $(e^z-1)^{-1}$ está acotada sobre ϕ_{22}^*, concluimos que, sobre este arco,

$$\frac{z^{s-1}e^{-mz}}{e^z-1} = O((2k\pi)^{\sigma-1}e^{-\tau\pi/2}).$$

Más aún, $k \le y+1 \le 2y$ si $y \ge 1$ y $k = 1 \le y/\delta$ en otro caso, luego en cualquier caso $k = O(y)$ y llegamos a que

$$\int_{\phi_{22}^*} \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\eta^{\sigma-1}e^{-\tau\pi/2}).$$

Recapitulando, tenemos que

$$\frac{e^{-\pi i s}\Pi(-s)}{2\pi i}\int_{\phi_2} \frac{z^{s-1}e^{-mz}}{e^z-1}\,dz = O(\tau^{-\sigma}\eta^{\sigma}) + O(\tau^{1/2-\sigma}\eta^{\sigma-1})$$

$$= O(x^{-\sigma}) + O(\tau^{1/2-\sigma}y^{\sigma-1}),$$

donde hemos usado una vez más que $\eta^{\sigma-1} = (2\pi)^{\sigma-1}y^{\sigma-1} \le y^{\sigma-1}$. ∎

Un caso particular especialmente simple de la ecuación funcional aproximada se da si la restringimos a la recta crítica $\sigma = 1/2$ y tomamos $x = y = \sqrt{|\tau|/2\pi}$. Entonces se reduce a:

$$\zeta(1/2+\tau i) = \sum_{n\le\sqrt{|\tau|/2\pi}} \frac{1}{n^{1/2+\tau i}} + \chi(1/2+\tau i)\sum_{n\le\sqrt{|\tau|/2\pi}} \frac{1}{n^{1/2-\tau i}} + O(|\tau|^{-1/4}).$$

El teorema 4.8 prueba que la función $|\chi(1/2+\tau i)|$ tiende a 1 en ∞ y, en particular, está acotada, luego

$$|\zeta(1/2+\tau i)| \le c\sum_{n\le\sqrt{|\tau|/2\pi}} \frac{1}{n^{1/2+\tau i}} + O(|\tau|^{-1/4}). \tag{6.1}$$

En particular

$$|\zeta(1/2+\tau i)| \le c\sum_{n\le\sqrt{|\tau|/2\pi}} \frac{1}{n^{1/2}} + O(|\tau|^{-1/4})$$

Ahora bien,

$$\sum_{n\le\sqrt{|\tau|/2\pi}} \frac{1}{n^{1/2}} \le 1 + \int_1^{\sqrt{|\tau|/2\pi}} \frac{1}{\sqrt{u}}\,du \le \sqrt[4]{|\tau|/2\pi} = O(|\tau|^{1/4}),$$

luego concluimos que

$$\zeta(1/2+\tau i) = O(|\tau|^{1/4}).$$

Este resultado es ligeramente mejor que el que obtuvimos como consecuencia del teorema 4.11 (la convexidad de la función de Lindelöf). Habíamos visto que $\mu(1/2) \le 1/4$, lo cual significa que $\zeta(1/2+i\tau) = O(|\tau|^{1/4+\epsilon})$, para cualquier $\epsilon > 0$. Ahora acabamos de ver que el ϵ no es necesario. En la sección siguiente mejoraremos un poco más la estimación.

6.2 El método de Hardy-Littlewood

Se conocen varias técnicas para estudiar el orden de crecimiento de la función exponencial sobre la banda crítica. Aquí vamos a presentar una debida a Hardy y Littlewood, que, entre otras cosas, nos permitirá mejorar ligeramente la región sin ceros que conocemos, lo que a su vez tiene consecuencias sobre la estimación del error en el teorema de los números primos.

Antes de entrar en materia conviene discutir un resultado que usaremos en varias ocasiones de aquí en adelante.

Si $X \neq \varnothing$ es un conjunto finito, podemos considerar en $\mathcal{P}X$ la medida μ que a cada conjunto $A \subset X$ le asigna su cardinal. Como todo subconjunto de X es medible, resulta que toda función $f : X \longrightarrow \mathbb{R}$ es medible, y de hecho es integrable, pues se comprueba fácilmente que

$$\int_X f\,d\mu = \sum_{x\in X} f(x).$$

Observemos además que el único subconjunto nulo de X es el conjunto vacío, lo cual hace que los espacios $L^p(\mu)$ definidos en [An 6.8] son simplemente el espacio de todas las aplicaciones $f : X \longrightarrow \mathbb{R}$, con la norma

$$\|f\|_p = \Big(\sum_{x\in X} |f(x)|^p\Big)^{1/p}.$$

Notemos que esta definición vale igualmente si $f : X \longrightarrow \mathbb{C}$, y en tal caso $\|f\|_p$ coincide con la norma de $|f| : X \longrightarrow \mathbb{R}$.

La mayoría de las propiedades de la integral de Lebesgue se particularizan a hechos triviales sobre sumas finitas en este contexto, pero hay un hecho que no es trivial incluso en este caso particular, y es el que nos va a interesar. Nos referimos a la desigualdad de Hölder [An 6.12], que en este contexto se enuncia así:

Desigualdad de Hölder *Sea $X \neq \varnothing$ un conjunto finito, sean $p_1, \ldots, p_n$ números positivos tales que $\sum_{i=1}^n \frac{1}{p_i} = 1$ y sean $f_i : X \longrightarrow \mathbb{C}$ funciones cualesquiera. Entonces*

$$\Big\|\prod_{i=1}^n f_i\Big\|_1 \leq \prod_{i=1}^n \|f_i\|_{p_i}.$$

En efecto, [An 6.12] prueba el resultado para funciones reales, y el caso complejo se obtiene aplicándolo a los módulos de las funciones dadas.

Pasamos ya a exponer el método de Hardy-Littlewood, que es un estudio de las sumas de la forma

$$\sum_{n=a+1}^{b} \frac{1}{n^s}.$$

Necesitamos una ligera generalización del teorema [ITAn 2.32]:

Teorema 6.5 *Sea $\{b_n\}$ una sucesión decreciente de números reales ≥ 0, sea $s_n = \sum_{m=M+1}^{n} a_m$, donde los a_m son números complejos, entendiendo que $s_M = 0$. Entonces*

$$\left|\sum_{n=M+1}^{N} a_n b_n\right| \leq b_M \max_{M<n\leq N} |s_n|.$$

DEMOSTRACIÓN: Aplicamos [ITAn 2.32] a las sucesiones que empiezan en a_{M+1} y b_{M+1}, respectivamente:

$$\sum_{n=M+1}^{N} a_n b_n = \sum_{n=M+1}^{N-1} s_n(b_n - b_{n+1}) + s_N b_N,$$

luego

$$\left|\sum_{n=M+1}^{N} a_n b_n\right| \leq \sum_{n=M+1}^{N-1} |s_n|(b_n - b_{n+1}) + |s_N| b_N$$

$$\leq \left(\sum_{n=M+1}^{N-1} (b_n - b_{n+1}) + b_N\right) \max_{M<n\leq N} |s_n| = b_{M+1} \max_{M<n\leq N} |s_n| \leq b_M \max_{M<n\leq N} |s_n|.$$

■

En particular, si $a_n = 1/n^{i\tau}$, $b_n = 1/n^{\sigma}$, obtenemos que

$$\left|\sum_{n=a+1}^{b} \frac{1}{n^s}\right| \leq \frac{1}{a^\sigma} \max_{a<n\leq b} \left|\sum_{n=a+1}^{n} \frac{1}{n^{i\tau}}\right|.$$

Esto nos reduce a estudiar series con exponentes imaginarios puros. A su vez, vamos a ver que en cada término $1/n^{i\tau} = e^{-i\tau \log n}$ podemos truncar la serie de Taylor del logaritmo:

Teorema 6.6 *Sean k, a, b números naturales no nulos, $b - a \geq 1$ y $t \geq 1$ un número real tal que*

$$\frac{b-a}{a} \leq \frac{1}{2} t^{-1/(k+1)}.$$

Sea M tal que

$$\left|\sum_{n=1}^{m} e^{-it(\frac{n}{a} - \frac{1}{2}\frac{n^2}{a^2} + \cdots + (-1)^{k-1}\frac{n^k}{ka^k})}\right| \leq M$$

para todo $m \leq b - a$. Entonces

$$\left|\sum_{n=a+1}^{b} e^{-it\log n}\right| < 4M.$$

DEMOSTRACIÓN: Consideramos la serie de Taylor

$$\log\frac{1}{1-z}=\sum_{r=1}^{\infty}\frac{1}{r}z^r,$$

que converge en el disco $D(0,1)$, y lo mismo vale para la serie

$$\sum_{r=k+1}^{\infty}\frac{1}{r}z^r.$$

La función

$$f_t(z)=e^{t\sum\limits_{r=k+1}^{\infty}\frac{1}{r}z^r}$$

es holomorfa en el disco $D(0,1)$, luego admite un desarrollo en serie de Taylor

$$e^{t\sum\limits_{r=k+1}^{\infty}\frac{1}{r}z^r}=\sum_{r=0}^{\infty}c_r(t)z^r.$$

Vamos a probar, más concretamente, que $c_l(t)$ es un polinomio en t con coeficientes positivos. En efecto, en primer lugar observamos que

$$\Big(t\sum_{r=k+1}^{\infty}\frac{1}{r}z^r\Big)^m=\sum_{r=m(k+1)}^{\infty}c_{rm}(t)z^r,$$

donde cada c_{rk} es una forma de grado m (es decir, un polinomio cuyos monomios tienen todos grado m) con coeficientes positivos. Ciertamente, para $m=1$ es $c_{r1}=t/r$. Si vale para m, entonces

$$\Big(t\sum_{r=k+1}^{\infty}\frac{1}{r}z^r\Big)^{m+1}=\sum_{r=m(k+1)}^{\infty}c_{rm}(t)z^r\sum_{r=k+1}^{\infty}\frac{t}{r}z^r=\sum_{r=(m+1)(k+1)}^{\infty}\Big(\sum_{u=k+1}^{r-m(k+1)}c_{r-u,m}(t)\frac{t}{u}\Big)z^r$$

y, como cada $c_{r-u,m}(t)$ es una forma de grado m con coeficientes positivos, es claro que lo mismo vale para el coeficiente de z^r, pero ahora con grado $m+1$. A su vez,

$$e^{t\sum\limits_{r=k+1}^{\infty}\frac{1}{r}z^r}=\sum_{m=0}^{\infty}\frac{1}{m!}\Big(t\sum_{r=k+1}^{\infty}\frac{1}{r}z^r\Big)^m=\sum_{m=0}^{\infty}\frac{1}{m!}\sum_{r=m(k+1)}^{\infty}c_{rm}(t)z^r$$

$$=\sum_{r=0}^{\infty}\sum_{m=0}^{E[r/(k+1)]}\frac{c_{rm}(t)}{m!}z^r,$$

luego $c_r(t)=\sum\limits_{m=0}^{E[r/(k+1)]}\frac{c_{rm}(t)}{m!}$ es un polinomio con coeficientes positivos.

En particular, cambiando t por it y z por $-z$, tenemos que

$$e^{-it\sum_{r=k+1}^{\infty}\frac{(-1)^{r-1}}{r}z^r} = \sum_{r=0}^{\infty}(-1)^r c_r(it)z^r,$$

siempre que $|z| < 1$.

Se cumple que

$$\left|\sum_{n=a+1}^{b} e^{-it\log n}\right| = \left|\sum_{n=1}^{b-a} e^{-it\log(a+n)}\right| = \left|e^{-it\log a}\sum_{n=1}^{b-a} e^{-it\log(1+\frac{n}{a})}\right| =$$

$$\left|\sum_{n=1}^{b-a} e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r} - it\sum_{r=k+1}^{\infty}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}}\right|,$$

donde usamos que $n/a \le (b-a)/a \le 1/2$, luego la serie de Taylor de $\log(1+z)$ converge en n/a.

En términos del desarrollo precedente tenemos que

$$\left|\sum_{n=a+1}^{b} e^{-it\log n}\right| = \left|\sum_{n=1}^{b-a} e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}}\sum_{l=0}^{\infty}(-1)^l c_l(it)\left(\frac{n}{a}\right)^l\right|$$

$$= \left|\sum_{l=0}^{\infty}\frac{(-1)^l c_l(it)}{a^l}\sum_{n=1}^{b-a} n^l e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}}\right|.$$

Ahora usamos la fórmula de suma por partes [ITAn 2.32], según la cual

$$\sum_{n=1}^{b-a} n^l e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}} =$$

$$\sum_{u=1}^{b-a-1}(u^l-(u+1)^l)\sum_{n=1}^{u} e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}} + (b-a)^l\sum_{n=1}^{b-a} e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}}.$$

Por lo tanto,

$$\left|\sum_{n=1}^{b-a} n^l e^{-it\sum_{r=1}^{k}\frac{(-1)^{r-1}}{r}\frac{n^r}{a^r}}\right| \le \sum_{u=1}^{b-a-1}((u+1)^l-u^l)M + (b-a)^l M$$

$$= 2(b-a)^l M - M < 2M(b-a)^l.$$

Con esto hemos probado que

$$\left|\sum_{n=a+1}^{b} e^{-it\log n}\right| \le 2M\sum_{l=0}^{\infty}|c_l(it)|\left(\frac{b-a}{a}\right)^l.$$

Como $c_l(t)$ tiene coeficientes positivos, se cumple que $|c_l(it)| \le c_l(|it|)$, luego

$$\left|\sum_{n=a+1}^{b} e^{-it\log n}\right| \le 2M\sum_{l=0}^{\infty} c_l(t)\left(\frac{b-a}{a}\right)^l$$

$$= 2Me^{t\sum_{r=k+1}^{\infty}\frac{1}{r}\frac{(b-a)^r}{a^r}} \le 2Me^{t\sum_{r=k+1}^{\infty}\frac{(b-a)^r}{a^r}} \le 2Me^{t\frac{((b-a)/a)^{k+1}}{(1-(b-a)/a)}}.$$

A su vez

$$\frac{t\left(\frac{b-a}{a}\right)^{k+1}}{1-\frac{b-a}{a}} \le \frac{t\left(\frac{1}{2}t^{-1/(k+1)}\right)^{k+1}}{1/2} = \frac{1}{2^k}$$

y $e^{1/2^k} < 2$. ∎

Esto nos lleva a su vez a estudiar la acotación de expresiones de la forma

$$S = \sum_{n=1}^{m} e^{2\pi i P(n)},$$

donde $P(n)$ es un polinomio de grado k con coeficientes reales. Teniendo en cuenta que $|e^{2\pi iP(n)}| = 1$, una cota obvia es $|S| \le m$, pero podemos encontrar cotas mejores.

Por ejemplo, supongamos que $P(n) = \alpha n$ y α no es entero (si α es entero se cumple que $|S| = m$). Entonces tenemos una progresión geométrica:

$$|S| = \left|\frac{e^{2\pi i\alpha} - e^{2\pi i\alpha(m+1)}}{1-e^{2\pi i\alpha}}\right| \le \frac{2}{|1-e^{2\pi i\alpha}|} = \frac{2}{|e^{-\pi i\alpha} - e^{\pi i\alpha}|} = \frac{1}{|\operatorname{sen}\pi\alpha|}.$$

Por lo tanto,

$$|S| \le \min\{m, |\operatorname{sen}\pi\alpha|^{-1}\}.$$

Consideremos ahora el caso en que $P(n) = \alpha n^2 + \beta n$. Entonces

$$|S|^2 = S\bar{S} = \sum_{n=1}^{m}\sum_{n'=1}^{m} e^{2\pi i(\alpha n^2+\beta n-\alpha n'^2-\beta n')}.$$

Hacemos el cambio $n' = n - r$:

$$|S|^2 = \sum_{n=1}^{m}\sum_{r=n-m}^{n-1} e^{2\pi i(2\alpha nr-\alpha r^2+\beta r)} = \sum_{r=-m+1}^{m-1}\sum_{n=\max\{r+1,1\}}^{\min\{r+m,m\}} e^{2\pi i(2\alpha nr-\alpha r^2+\beta r)}$$

$$\le \sum_{r=-m+1}^{m-1} |e^{2\pi i(-\alpha r^2+\beta r)}|\left|\sum_{n=\max\{r+1,1\}}^{\min\{r+m,m\}} e^{4\pi i\alpha nr}\right|$$

$$= \sum_{r=-m+1}^{m-1}\left|\sum_{n=\max\{r+1,1\}}^{\min\{r+m,m\}} e^{4\pi i\alpha nr}\right| \le \sum_{r=-m+1}^{m-1}\min\{m, |\operatorname{sen}(2\pi\alpha r)|^{-1}\}$$

$$= m + 2\sum_{r=1}^{m-1}\min\{m, |\operatorname{sen}(2\pi\alpha r)|^{-1}\},$$

donde hemos usado una ligera variante del caso ya probado en que P tiene grado 1.

Notemos que si tenemos —como es aquí el caso— una suma de la forma

$$\sum_{n=k}^{l} e^{2\pi i\alpha n} = \sum_{n=1}^{l-k+1} e^{2\pi i\alpha(n-k+1)} = e^{2\pi i\alpha(-k+1)} \sum_{n=1}^{l-k+1} e^{2\pi i\alpha n},$$

el primer factor tiene módulo 1 y el segundo se puede acotar como hemos visto. Ahora obtenemos una cota para el caso general:

Teorema 6.7 (Desigualdad de Weyl) *Sea $k \geq 2$ un número natural y*

$$P(n) = \alpha n^k + \alpha_{k-1} n^{k-1} + \cdots + \alpha_1 n + \alpha_0$$

un polinomio con coeficientes reales, $\alpha \neq 0$. Sea

$$S = \sum_{n=1}^{m} e^{2\pi i P(n)},$$

donde $m \geq 1$ es un número natural. Sea $K = 2^{k-1}$. Entonces

$$|S|^K \leq 2^{2K} m^{K-1} + 2^K m^{K-k} \sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\pi\alpha k!\, r_1 \cdots r_{k-1})|^{-1}\}.$$

Demostración: Notemos que para $k = 2$ hemos obtenido una cota mejor incluso que la que proporciona el teorema. La hemos dado para un polinomio sin término independiente, pero esto es irrelevante porque en la expresión de S podemos sacar factor común $e^{2\pi i\alpha_0}$, que tiene módulo 1, y el exponente pasa a ser un polinomio sin término independiente. Supongamos que el resultado es cierto para $k - 1 \geq 2$ y veamos que se cumple para k.

$$|S|^2 = \sum_{n=1}^{m} \sum_{n'=1}^{m} e^{2\pi i(P(n)-P(n'))} = \sum_{n=1}^{m} \sum_{r_1=n-m}^{n-1} e^{2\pi i(P(n)-P(n-r_1))}$$

$$= \sum_{r_1=-m+1}^{m-1} \sum_{n=\text{máx}\{r_1+1,1\}}^{\text{mín}\{r_1+m,m\}} e^{2\pi i(P(n)-P(n-r_1))}.$$

Llamemos

$$S_1 = S_1(r_1) = \sum_{n=\text{máx}\{r_1+1,1\}}^{\text{mín}\{r_1+m,m\}} e^{2\pi i(P(n)-P(n-r_1))} = \sum_{n=\text{máx}\{r_1+1,1\}}^{\text{mín}\{r_1+m,m\}} e^{2\pi i(\alpha k r_1 n^{k-1}+\cdots)}.$$

En estos términos,

$$|S|^2 \leq \sum_{r_1=-m+1}^{m-1} |S_1(r_1)| \leq \left(\sum_{r_1=-m+1}^{m-1} 1\right)^{1-2/K} \left(\sum_{r_1=-m+1}^{m-1} |S_1|^{K/2}\right)^{2/K},$$

donde hemos usado la desigualdad de Hölder tal y como la hemos enunciado al principio de este capítulo. Esto implica que

$$|S|^2 \le (2m)^{1-2/K}\left(m^{K/2} + \sum_{r_1=-m+1}^{m-1}{}^{*}\ |S_1|^{K/2}\right)^{2/K},$$

donde el asterisco indica que falta el sumando correspondiente a $r_1 = 0$. Por lo tanto:

$$|S|^K \le (2m)^{K/2-1}\left(m^{K/2} + \sum_{r_1=-m+1}^{m-1}{}^{*}\ |S_1|^{K/2}\right).$$

A S_1 podemos aplicarle la hipótesis de inducción, pues un cambio de índice reduce su expresión a una suma para $n = 1, \dots, n_0 \le m$ y el exponente se convierte en otro polinomio también de grado $k-1$ con el mismo coeficiente director. La conclusión es que

$$|S_1|^{K/2} \le 2^K m^{K/2-1} + 2^{K/2} m^{K/2-k+1} \sum_{r_2,\dots,r_{k-1}=1}^{m-1} \min\{m, |\operatorname{sen}(r_1\pi\alpha k!\, r_2 \cdots r_{k-1})|^{-1}\},$$

y de aquí obtenemos la desigualdad para k. ∎

Con esto podemos probar la acotación básica en la que nos vamos a apoyar:

Teorema 6.8 *Sea $t > 3$, sean a, b números naturales tales que*

$$1 \le a < b \le 2a, \tag{6.2}$$

sea $k \ge 2$ un número natural y $K = 2^{k-1}$. Entonces

$$\left|\sum_{n=a+1}^{b} n^{-it}\right| < c\left(a^{1-\frac{1}{K}} t^{\frac{1}{(k+1)K}} + a t^{-\frac{1}{(k+1)K}} \log^{\frac{k-1}{K}} a\right)\log^{1/K} t,$$

donde c es una constante independiente de todos los datos.

Demostración: Supongamos en primer lugar que $a \le 4t^{1/(k+1)}$. Entonces

$$\left|\sum_{n=a+1}^{b} n^{-it}\right| \le b - a \le a = a^{1-\frac{1}{K}} a^{\frac{1}{K}} \le a^{1-\frac{1}{K}} t^{\frac{1}{(k+1)K}} 4^{1/K}$$

$$< 4a^{1-\frac{1}{K}} t^{\frac{1}{(k+1)K}} \log^{1/K} t,$$

pues esto equivale a que $1/4^{K-1} < 1 < \log t$. Es claro entonces que se cumple la desigualdad del enunciado con $c = 4$.

Así pues, podemos suponer que

$$a > 4t^{1/(k+1)}, \tag{6.3}$$

con lo que en particular $a > 4$. Llamamos

$$m = E\left[\frac{1}{2}at^{-\frac{1}{k+1}}\right] \geq 2, \quad N = E[(b-a)/m].$$

Así

$$\frac{1}{4}at^{-\frac{1}{k+1}} < m \leq \frac{1}{2}at^{-\frac{1}{k+1}}, \tag{6.4}$$

pues, teniendo en cuenta (6.3),

$$\frac{1}{2}at^{-\frac{1}{k+1}} - \frac{1}{4}at^{-\frac{1}{k+1}} = \frac{1}{2}at^{-\frac{1}{k+1}} > 2.$$

Además, por (6.2) y (6.4),

$$0 \leq N \leq \frac{b-a}{m} \leq \frac{a}{m} < 4t^{1/(k+1)}, \tag{6.5}$$

$$mN \leq b-a < mN+m.$$

Supongamos ahora que $N \leq 1$, con lo que $b-a < 2m$, luego, por (6.4),

$$\left|\sum_{n=a+1}^{b} n^{-it}\right| \leq b-a < 2m \leq at^{-\frac{1}{k+1}} < at^{-\frac{1}{k+1}} \log^{(k-1)/K} a \log^{1/K} t,$$

donde usamos que $a > 4$, $t > 3$, y de aquí se sigue la desigualdad del enunciado.

Por lo tanto, podemos suponer que $N \geq 2$, con lo que

$$m \leq \frac{b-a}{2}. \tag{6.6}$$

En tal caso descomponemos

$$\sum_{n=a+1}^{b} n^{-it} = \sum_{n=a+1}^{a+m} n^{-it} + \sum_{n=a+m+1}^{a+2m} n^{-it} + \cdots + \sum_{n=a+mN+1}^{b} n^{-it}$$

$$= \Sigma_1 + \Sigma_2 + \cdots \Sigma_{N+1}, \tag{6.7}$$

donde en la última igualdad ha de entenderse que cada Σ_j es, por definición, el sumando correspondiente del término anterior. Llamamos $v_j = a + jm$, para $1 \leq j \leq N+1$, con lo que, por (6.5), (6.2) y (6.6),

$$a < a+m = v_1 \leq v_j \leq v_{N+1} = a + (N+1)m \leq a+m+b-a$$

$$= b+m \leq 2a+m \leq 2a + \frac{b-a}{2} \leq \frac{5a}{2} < 3a. \tag{6.8}$$

Por otra parte, por (6.4),

$$\frac{m}{v_j} < \frac{m}{a} \leq \frac{1}{2}t^{-\frac{1}{k+1}}.$$

Fijemos $1 \le j \le N+1$ y sea M el máximo para $1 \le m' \le m$ de las sumas

$$S_j = \sum_{n=1}^{m'} e^{-it\left(\frac{n}{a+jm} - \frac{1}{2}\frac{n^2}{(a+jm)^2} + \cdots + (-1)^{k-1}\frac{n^k}{k(a+jm)^k}\right)}.$$

Así el teorema 6.6 nos da que $|\Sigma_j| \le 4M$. Por otra parte, según 6.7,

$$|S_j|^K \le 2^{2K} m^{K-1} + 2^K m^{K-k} \sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\frac{t(k-1)!\, r_1 \cdots r_{k-1}}{2(a+jm)^k})|^{-1}\}.$$

De aquí se sigue que[2]

$$|S_j| \le 2^2 m^{1-1/K} + 2m^{1-k/K} \left(\sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\frac{t(k-1)!\, r_1 \cdots r_{k-1}}{2(a+jm)^k})|^{-1}\} \right)^{1/K}.$$

A su vez,

$$|\Sigma_j| \le 2^4 m^{1-1/K} + 2^3 m^{1-k/K} \left(\sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\frac{t(k-1)!\, r_1 \cdots r_{k-1}}{2(a+jm)^k})|^{-1}\} \right)^{1/K},$$

de donde, volviendo a (6.7),

$$\left| \sum_{n=a+1}^{b} n^{-it} \right| \le$$

$$2^4(N+1)m^{1-1/K} + 2^3 m^{1-k/K} \sum_{j=0}^{N} \left(\sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\frac{t(k-1)!\, r_1 \cdots r_{k-1}}{2(a+jm)^k})|^{-1}\} \right)^{1/K}$$

$$\le 2^4(N+1)m^{1-1/K} + \tag{6.9}$$

$$2^3 m^{1-k/K}(N+1)^{1-\frac{1}{K}} \left(\sum_{j=0}^{N} \sum_{r_1,\ldots,r_{k-1}=1}^{m-1} \text{mín}\{m, |\operatorname{sen}(\frac{t(k-1)!\, r_1 \cdots r_{k-1}}{2(a+jm)^k})|^{-1}\} \right)^{1/K},$$

donde hemos usado la desigualdad de Hölder (a la suma sobre j, con un factor 1 en cada sumando, $p = (1-1/K)^{-1}$, $q = K$).

Llamemos $R = r_1 \cdots r_{k-1}$ y

$$\theta_j = \theta_j(t,k,m,R) = \frac{t(k-1)!\, R}{2(a+jm)^k} = \frac{t(k-1)!R}{2v_j^k}.$$

Observemos que

$$\frac{1}{v_j^k} - \frac{1}{v_{j+1}^k} = \frac{v_{j+1}^k - v_j^k}{v_j^k v_{j+1}^k} = \frac{(v_{j+1}/v_j)^k - 1}{v_{j+1}^k}$$

[2]Usamos que $(A+B)^{1/K} \le A^{1/K} + B^{1/K}$ (para $A, B \ge 0$), pues, llamando $x = A^{1/K}$, $y = B^{1/K}$, es equivalente a que $x^K + y^K \le (x+y)^K$.

$$= \frac{(v_{j+1}/v_j - 1)((v_{j+1}/v_j)^{k-1} + \cdots + 1)}{v_{j+1}^k} > \frac{(v_{j+1}/v_j - 1)k}{v_{j+1}^k}$$

$$= \frac{k(v_{j+1} - v_j)}{v_j v_{j+1}^k} > \frac{k(v_{j+1} - v_j)}{v_{j+1}^{k+1}}.$$

Usando esto, junto con (6.8) y (6.4),

$$\theta_j - \theta_{j+1} = \frac{t(k-1)!R}{2}\left(\frac{1}{v_j^k} - \frac{1}{v_{j+1}^k}\right) > \frac{t(k-1)!R}{2}\frac{k(v_{j+1} - v_j)}{v_{j+1}^{k+1}} > \frac{tk!R}{2}\frac{m}{(3a)^{k+1}}$$

$$> \frac{tk!R}{2}\frac{at^{-\frac{1}{k+1}}}{4(3a)^{k+1}} = \frac{k!Rt^{\frac{k}{k+1}}a^{-k}}{2^3 \cdot 3^{k+1}} = D,$$

donde $D > 0$ es independiente de j. Por otra parte

$$0 < \theta_1 = \frac{tk!R}{2k(a+m)^k} < \frac{tk!R}{a^k}. \tag{6.10}$$

Fijado $g \in \mathbb{Z}$, si $\theta_j, \theta_{j'} \in [g\pi, (g+1/2)\pi]$, con $j < j'$, entonces, para todo $j \le j'' \le j'$ se cumple también que $\theta_{j''} \in [g\pi, (g+1/2)\pi]$, porque la sucesión θ_j es decreciente. Por lo tanto, los índices para los que esto sucede serán de la forma $j_0 \le j \le j_0 + l$. Si $\theta_j = g\pi + \alpha_j$, con $0 \le \alpha_j \le \pi/2$, entonces

$$|\operatorname{sen}\theta_j| = \operatorname{sen}\alpha \ge 2\alpha/\pi,$$

luego

$$|\operatorname{sen}\theta_j| \ge (j_0 + l - j)\frac{2}{\pi}D,$$

pues $g\pi < \theta_{j_0+l} < \ldots < \theta_j = g\pi + \alpha_j$, luego hay $j_0 + l - j$ intervalos de longitud mayor que D entre 0 y α_j. Esta cota inferior es positiva salvo a lo sumo para $j = j_0 + l$, que puede cumplir $|\operatorname{sen}\theta_j| = |\operatorname{sen} g\pi| = 0$. Por consiguiente, acotando $1/2 + 1/3 + \cdots + 1/N \le \int_1^N dt/t = \log N$ y usando luego (6.5),

$$\sum_{\theta_j \in [g\pi, (g+1/2)\pi]} \text{mín}\{m, |\operatorname{sen}\theta_j|^{-1}\} \le m + \frac{\pi}{2}\sum_{j=1}^{N}\frac{1}{jD} \le m + \frac{\pi}{2}\frac{1+\log N}{D}$$

$$\le m + 2\frac{1+\log N}{D} < m + \frac{2}{D}(1 + \log 4t^{1/2}) < m + \frac{2}{D}(3 + \frac{1}{2}\log t)$$

$$< m + \frac{7}{D}\log t,$$

donde en la última desigualdad usamos que $t > 3$. Igualmente se concluye que

$$\sum_{\theta_j \in [(g-1/2)\pi, g\pi]} \text{mín}\{m, |\operatorname{sen}\theta_j|^{-1}\} < m + \frac{7}{D}\log t.$$

Por otra parte,

$$mD = \frac{mk!Rt^{\frac{k}{k+1}}a^{-k}}{2^3\cdot 3^{k+1}} < m^k k! t^{\frac{k}{k+1}}a^{-k} < k!(mt^{\frac{1}{k+1}}a^{-1})^k < k!$$

por (6.4). Por consiguiente, si I es cualquier intervalo de la forma $[g\pi,(g+1/2)\pi]$ o $[(g-1/2)\pi,g\pi]$,

$$\sum_{\theta_j\in I}\text{mín}\{m,|\operatorname{sen}\theta_j|^{-1}\} < \left(\frac{k!}{D}+\frac{7}{D}\right)\log t \le \frac{8k!}{D}\log t$$

$$\le \frac{2^6\cdot 3^{k+1}}{R}t^{-\frac{k}{k+1}}a^k\log t < \frac{2^{2k+8}}{R}t^{-\frac{k}{k+1}}a^k\log t \le \frac{2^{10k}}{R}t^{-\frac{k}{k+1}}a^k\log t,$$

Por (6.10), el número de intervalos I que pueden contener algún θ_j es a lo sumo

$$1+\frac{2}{\pi}tk!Ra^{-k} < 1+tk!Ra^{-k}.$$

Por lo tanto,

$$\sum_{j=0}^{N}\text{mín}\{m,|\operatorname{sen}\theta_j|^{-1}\} < (1+tk!Ra^{-k})\frac{2^{10k}}{R}t^{-\frac{k}{k+1}}a^k\log t$$

$$= \frac{2^{10k}}{R}t^{-\frac{k}{k+1}}a^k\log t + 2^{10k}k!\,t^{\frac{1}{k+1}}\log t. \tag{6.11}$$

Ahora:

$$\sum_{r_1,\dots,r_{k-1}=1}^{m-1}\frac{1}{r_1\cdots r_{k-1}} = \left(\sum_{r=1}^{m-1}\frac{1}{r}\right)^{k-1} \le (1+\log(m-1))^{k-1}$$

$$\le (1+\log a)^{k-1} < (2\log a)^{k-1},$$

donde hemos usado que $2m\le a$, por (6.6) y (6.2) y $a\ge 4$, y además, por (6.4),

$$\sum_{r_1,\dots,r_{k-1}=1}^{m-1}1 = (m-1)^{k-1} < m^{k-1} \le a^{k-1}t^{-\frac{k-1}{k+1}}.$$

Por consiguiente, de (6.11) se sigue que

$$\sum_{j=0}^{N}\sum_{r_1,\dots,r_{k-1}=1}^{m-1}\text{mín}\{m,|\operatorname{sen}(\theta_j)|^{-1}\} = \sum_{r_1,\dots,r_{k-1}=1}^{m-1}\sum_{j=0}^{N}\text{mín}\{m,|\operatorname{sen}(\theta_j)|^{-1}\}$$

$$\le \sum_{r_1,\dots,r_{k-1}=1}^{m-1}\left(\frac{1}{r_1\cdots r_{k-1}}2^{10k}t^{-\frac{k}{k+1}}a^k\log t + 2^{10k}k!\,t^{\frac{1}{k+1}}\log t\right)$$

$$\le (2\log a)^{k-1}2^{10k}t^{-\frac{k}{k+1}}a^k\log t + a^{k-1}t^{-\frac{k-1}{k+1}}2^{10k}k!\,t^{\frac{1}{k+1}}\log t$$

$$< 2^{11K}\log^{k-1}a\,t^{-\frac{k}{k+1}}a^k\log t + 2^{11K}\,t^{\frac{2-k}{k+1}}\log t\,a^{k-1},$$

donde hemos usado que $k\le K$ y que $k!\le\prod_{u=2}^{k}2^{2^{u-2}} < 2^{2^{k-1}} = 2^K$.

A su vez:

$$\Big(\sum_{j=0}^{N}\sum_{r_1,\dots,r_{k-1}=1}^{m-1}\text{mín}\{m,|\operatorname{sen}(\theta_j)|^{-1}\}\Big)^{1/K}<$$

$$2^{11}(\log^{(k-1)/K}a\,t^{-\frac{k}{(k+1)K}}a^{k/K}+t^{\frac{2-k}{(k+1)K}}a^{(k-1)/K})\log^{1/K}t,$$

donde hemos usado de nuevo que (véase la nota al pie de la página 208) que $(A+B)^{1/K}\le A^{1/K}+B^{1/K}$. Llamamos V a la última expresión que hemos obtenido. Con ella podemos volver a (6.9):

$$\left|\sum_{n=a+1}^{b}n^{-it}\right|\le 2^4(N+1)m^{1-1/K}+2^3m^{1-k/K}(N+1)^{1-\frac{1}{K}}V.$$

Por (6.4) y (6.5):

$$\begin{aligned}2^4(N+1)m^{1-1/K}&<2^4(N+1)a^{1-1/K}t^{-1/(k+1)(1-1/K)}\\&\le 2^4 4t^{1/(k+1)}a^{1-1/K}t^{-1/(k+1)(1-1/K)}\\&<2^7a^{1-1/K}t^{\frac{1}{K(k+1)}}<2^7a^{1-1/K}t^{\frac{1}{K(k+1)}}\log^{1/K}t,\end{aligned}$$

e igualmente

$$\begin{aligned}2^3m^{1-k/K}(N+1)^{1-\frac{1}{K}}&<2^6t^{\frac{1}{k+1}(1-\frac{1}{K})}(at^{-\frac{1}{k+1}})^{1-\frac{k}{K}}\\&=2^6a^{1-\frac{k}{K}}t^{\frac{k-1}{(k+1)K}}.\end{aligned}$$

Uniendo todas estas estimaciones resulta:

$$\begin{aligned}\left|\sum_{n=a+1}^{b}n^{-it}\right|&<(2^7a^{1-1/K}t^{\frac{1}{(k+1)K}}+2^{17}at^{-\frac{1}{K(k+1)}}\log^{(k-1)/K}a\\&\quad+2^{17}a^{1-1/K}t^{\frac{1}{(k+1)K}})\log^{1/K}t\\&<2^{18}\left(a^{1-\frac{1}{K}}t^{\frac{1}{(k+1)K}}+at^{-\frac{1}{(k+1)K}}\log^{\frac{k-1}{K}}a\right)\log^{1/K}t.\end{aligned}$$

∎

Si aplicamos el teorema anterior con $k=2$ obtenemos que, si $1\le a<b\le 2a$,

$$\left|\sum_{n=a+1}^{b}n^{-it}\right|<c\left(a^{\frac{1}{2}}t^{\frac{1}{6}}+at^{-\frac{1}{6}}\log^{\frac{1}{2}}a\right)\log^{1/2}t.$$

El teorema 6.5 nos da entonces que

$$\sum_{n=a+1}^{b}\frac{1}{n^{\frac{1}{2}+\tau i}}=O\Big((\tau^{\frac{1}{6}}+a^{1/2}\tau^{-\frac{1}{6}}\log^{\frac{1}{2}}a)\log^{1/2}\tau\Big).$$

Dado $\tau>0$, sea N tal que $2^{N-1}<\sqrt{\tau/2\pi}\le 2^N$. Así, tenemos la descomposición

$$a_0=1<2<4<\cdots<2^{N-1}<\sqrt{\tau/2\pi}=a_N,$$

de modo que

$$\sum_{n\le\sqrt{\tau/2\pi}} \frac{1}{n^{1/2+\tau i}} = 1 + \sum_{j=0}^{N-1} \sum_{a_j<n\le a_{j+1}} \frac{1}{n^{1/2+\tau i}}.$$

Como $a_j = O(\tau^{1/2})$, su suma correspondiente es

$$O(\tau^{1/6}\log^{1/2}\tau + \tau^{1/12}\log\tau) = O(\tau^{1/6}\log^{1/2}\tau).$$

Por otra parte, el número de sumandos es

$$N < 1 + \frac{\log(\tau/2\pi)}{2\log 2} = O(\log\tau).$$

Por consiguiente,

$$\sum_{n\le\sqrt{\tau/2\pi}} \frac{1}{n^{1/2+\tau i}} = O(\tau^{1/6}\log^{3/2}\tau),$$

y combinando esto con la fórmula (6.1) que nos proporciona la ecuación funcional aproximada, concluimos que

$$\zeta(1/2+\tau i) = O(\tau^{1/6}\log^{3/2}\tau) + O(\tau^{-1/4}).$$

En definitiva:

Teorema 6.9 *Si $\tau \ge 2$, se cumple que*

$$\zeta(1/2+\tau i) = O(\tau^{1/6}\log^{3/2}\tau).$$

En particular, la función de Lindelöf cumple $\mu(1/2) \le 1/6$.

Este resultado, debido a Hardy y Littlewood, mejora la cota $\mu(1/2) \le 1/4$ obtenida por Lindelöf, y a su vez ha ido siendo mejorado paulatinamente en muchas ocasiones mediante técnicas cada vez más sofisticadas. La mejor estimación conocida hasta el momento, debida a M.N. Huxley, es $\mu(1/2) \le 32/205$. Notemos que $1/6 = 0.166\ldots$, mientras que $32/205 = 0.156\ldots$, con lo que las sucesivas mejoras sólo han conseguido rebajar en una centésima la cota de Hardy y Littlewood. Recordemos, por otra parte, que la hipótesis de Lindelöf afirma que $\mu(1/2) = 0$.

Hasta aquí sólo hemos aprovechado el caso $k = 2$ del teorema 6.8. Lo usaremos en toda su potencia para refinar el siguiente resultado elemental:

Teorema 6.10 *Dado $\delta > 0$, en la región del plano complejo determinada por las condiciones $\frac{1}{2} + \delta \le \sigma \le 1$, $\tau \ge 3$ se cumple que*

$$\zeta(s) = \sum_{n\le\tau^2} \frac{1}{n^s} + O(1).$$

DEMOSTRACIÓN: En el teorema 4.1 tomamos $x = E[\tau^2]$, con lo que

$$\left|\zeta(s) - \sum_{n\le\tau^2}\frac{1}{n^s}\right| \le \frac{E[\tau^2]^{1-\sigma}}{|s|} + |s|\int_{E[\tau^2]}^{+\infty}\frac{dt}{t^{\sigma+1}}$$

$$\le \frac{E[\tau^2]^{1/2-\delta}}{\tau} + \sqrt{2}\tau\int_{E[\tau^2]}^{+\infty}\frac{dt}{t^{3/2+\delta}} \le \frac{E[\tau^2]^{1/2-\delta}}{\tau} + \sqrt{2}\tau\frac{1}{(1/2+\delta)E[\tau^2]^{1/2+\delta}}$$

$$\le \frac{E[\tau^2]^{1/2}}{\tau}\frac{1}{9^\delta} + \frac{\sqrt{2}}{(1/2+\delta)\tau^{2\delta}} \le \frac{\sqrt{2}}{9^\delta} + \frac{\sqrt{2}}{(1/2+\delta)9^\delta} = O(1),$$

donde hemos usado que $|s|/\tau \le \sqrt{1^1+\tau^2}/\tau = \sqrt{1/\tau^2+1} \le \sqrt{2}$, y también que $E[\tau^2]^{1/2}/\tau \le \sqrt{\tau^2+1}/\tau = \sqrt{1+1/\tau^2} \le \sqrt{2}$. ∎

El caso $k = 2$ del teorema 6.8 basta para probar esta versión, válida en una estrecha banda en el borde de la banda crítica:

Teorema 6.11 *En la región del plano complejo determinada por* $\frac{23}{24} \le \sigma \le 1$, $\tau \ge 3$, *se cumple que*

$$\zeta(s) = \sum_{n\le\sqrt{\tau}}\frac{1}{n^s} + O(1)$$

DEMOSTRACIÓN: Teniendo en cuenta el teorema anterior, basta probar que, en la región indicada,

$$\sum_{\tau^{1/2}<n\le\tau^2}\frac{1}{n^s} = O(1). \tag{6.12}$$

En efecto:

$$\sum_{\tau^{1/2}<n\le\tau^2}\frac{1}{n^s} = \sum_{n=E[\tau^{1/2}]+1}^{2E[\tau^{1/2}]}\frac{1}{n^s} + \sum_{n=2E[\tau^{1/2}]+1}^{4E[\tau^{1/2}]}\frac{1}{n^s} + \cdots + \sum_{2^rE[\tau^{1/2}]<n\le\tau^2}\frac{1}{n^s}, \tag{6.13}$$

donde r es el único número natural que cumple $2^rE[\tau^{1/2}] < \tau^2 \le 2^{r+1}E[\tau^{1/2}]$. Si $2^hE[\tau^{1/2}] \le \tau^2$, por la observación tras el teorema 6.5,

$$\left|\sum_{n=2^hE[\tau^{1/2}]+1}^{2^{h+1}E[\tau^{1/2}]}\frac{1}{n^s}\right| \le \frac{1}{2^{h\sigma}E[\tau^{1/2}]^\sigma}M,$$

donde

$$M = \max\left\{\left|\sum_{n=2^hE[\tau^{1/2}]+1}^{m}\frac{1}{n^{i\tau}}\right| \;\middle|\; 2^hE[\tau^2]+1 \le m \le 2^{h+1}E[\tau^2]\right\}.$$

Ahora aplicamos el teorema 6.8, con $k = K = 2$, según el cual

$$M \le c\left(2^{h/2}E[\tau^{1/2}]^{1/2}\tau^{1/6} + 2^hE[\tau^{1/2}]\tau^{-1/6}\log^{1/2}(2^hE[\tau^{1/2}])\right)\log^{1/2}\tau,$$

con lo que

$$\begin{aligned}\left|\sum_{n=2^h E[\tau^{1/2}]+1}^{2^{h+1}E[\tau^{1/2}]}\frac{1}{n^s}\right| &\le c(2^{-h(\sigma-1/2)}E[\tau^{1/2}]^{-(\sigma-1/2)}\tau^{1/6}\\ &+ (2^h E[\tau^{1/2}])^{1-\sigma}\tau^{-1/6}\log^{1/2}(2^h E[\tau^{1/2}]))\log^{1/2}\tau\\ &\le c(E[\tau^{1/2}]^{-(\sigma-1/2)}\tau^{1/6}+\tau^{2-2\sigma}\tau^{-1/6}\log^{1/2}\tau^2)\log^{1/2}\tau\\ &\le c(\tau^{-\sigma/2+1/4}\tau^{1/6}+\tau^{2-2\sigma}\tau^{-1/6}\log^{1/2}\tau)\log^{1/2}\tau\\ &\le c(\tau^{-1/16}\log^{1/2}\tau+\tau^{-1/12}\log\tau)=O(1/\log\tau).\end{aligned}$$

Por otra parte,

$$h+1\le\log\frac{\tau^2}{E[\tau^{1/2}]}\le\log\frac{\tau^2}{\tau^{1/2}}=\frac{3}{2}\log\tau,$$

luego el número de sumandos en (6.13) es $O(\log\tau)$, y esto nos da (6.12). ∎

La versión completa de 6.8 nos permite probar lo siguiente:

Teorema 6.12 *Sea $r\ge 6$ un número natural y $R=2^{r-1}$. Entonces, en la región del plano complejo determinada por las condiciones $1-1/R\le\sigma\le 1$, $\log\log\tau\ge r$, se cumple que*

$$\zeta(s)=\sum_{1\le n\le\tau^{2/r}}\frac{1}{n^s}+O(1),$$

donde la constante implícita en $O(1)$ no depende de r.

Demostración: Teniendo en cuenta el teorema anterior, basta probar que

$$\sum_{\tau^{2/r}<n\le\tau^{1/2}}\frac{1}{n^s}=O(1). \tag{6.14}$$

Notemos que $23/24\le 31/32=1-1/2^{6-1}\le 1-1/R$, por lo que bajo las hipótesis actuales se cumplen las del teorema anterior.

A su vez, para probar esto demostraremos primero que si $k\ge 3$, $K=2^{k-1}$, $1-\frac{1}{4K}\le\sigma\le 1$, $\tau>3$, entonces

$$\sum_{\tau^{2/(k+2)}<n\le\tau^{2/(k+1)}}\frac{1}{n^s}=O(\tau^{-\frac{1}{84K}}\log^2\tau), \tag{6.15}$$

donde la constante de O no depende de k.

Descomponemos la suma como

$$\sum_{n=E[\tau^{2/(k+2)}]+1}^{2E[\tau^{2/(k+2)}]}\frac{1}{n^s}+\sum_{n=2E[\tau^{2/(k+2)}]+1}^{4E[\tau^{2/(k+2)}]}\frac{1}{n^s}+\cdots+\sum_{n=2^h E[\tau^{2/(k+2)}]+1}^{2^{h+1}E[\tau^{2/(k+2)}]}\frac{1}{n^s}+\cdots$$

Observemos que, como $k \geq 3$, $\tau \geq 3$,

$$E[\tau^{\frac{2}{k+2}}]2^{\log\tau} > 2^{\log\tau} = \tau^{\log 2} > \tau^{2/(k+1)},$$

por lo que el número de sumandos es menor o igual que $\log\tau$. Por lo tanto, basta probar que el módulo de cada sumando es $O(1/\log\tau)$. Por la observación tras 6.5 es

$$\left|\sum_{n=2^h E[\tau^{2/(k+2)}]+1}^{2^{h+1}E[\tau^{2/(k+2)}]} \frac{1}{n^s}\right| \leq \frac{1}{2^{h\sigma}E[\tau^{2/(k+2)}]^\sigma} M,$$

donde

$$M = \text{máx}\left\{\left|\sum_{n=2^h E[\tau^{2/(k+2)}]+1}^{m} n^{-i\tau}\right| \;\middle|\; 2^h E[\tau^{2/(k+2)}]+1 \leq m \leq 2^{h+1}E[\tau^{2/(k+2)}]\right\}.$$

El teorema 6.8 nos da que

$$M \leq c((2^h E[\tau^{2/(k+2)}])^{1-\frac{1}{K}}\tau^{\frac{1}{(k+1)K}}$$

$$+2^h E[\tau^{2/(k+2)}]\tau^{-\frac{1}{(k+1)K}}\log^{\frac{k-1}{K}}(2^h E[\tau^{2/(k+2)}]))\log^{1/K}\tau,$$

luego

$$\left|\sum_{n=2^h E[\tau^{2/(k+2)}]+1}^{2^{h+1}E[\tau^{2/(k+2)}]} \frac{1}{n^s}\right| \leq c((2^h E[\tau^{2/(k+2)}])^{1-\frac{1}{K}-\sigma}\tau^{\frac{1}{(k+1)K}}$$

$$+(2^h E[\tau^{2/(k+2)}])^{1-\sigma}\tau^{-\frac{1}{(k+1)K}}\log^{\frac{k-1}{K}}(2^h E[\tau^{2/(k+2)}]))\log^{1/K}\tau$$

$$\leq c((2^h E[\tau^{2/(k+2)}])^{-\frac{3}{4K}}\tau^{\frac{1}{(k+1)K}} + \tau^{\frac{2-2\sigma}{k+1}}\tau^{-\frac{1}{(k+1)K}}\log^{\frac{k-1}{K}}\tau^{1/2})\log^{1/K}\tau$$

$$\leq c(\tau^{-\frac{3}{2K(k+2)}}\tau^{\frac{1}{(k+1)K}}\log^{1/K}\tau + \tau^{\frac{1}{2K(k+1)}}\tau^{-\frac{1}{(k+1)K}}\log^k\tau).$$

Ahora usamos que

$$-\frac{3}{2K(k+2)} + \frac{1}{(k+1)K} = \frac{1-k}{2K(k+1)(k+2)} = -\frac{1}{2K(k+2)}\frac{k-1}{k+1}$$

$$< -\frac{1}{4kK}\frac{1}{2} = -\frac{1}{8kK},$$

$$\frac{1}{2K(k+1)} - \frac{1}{(k+1)K} = -\frac{1}{2K(k+1)} < -\frac{1}{8kK},$$

luego

$$\left|\sum_{n=2^h E[\tau^{2/(k+2)}]+1}^{2^{h+1}E[\tau^{2/(k+2)}]} \frac{1}{n^s}\right| \leq c(\tau^{-\frac{1}{8kK}}\log^{1/K}\tau + \tau^{-\frac{1}{8kK}}\log^{k/K}\tau)$$

$$= O(\tau^{-\frac{1}{8kK}}\log\tau).$$

Como el número de sumandos es a lo sumo $\log\tau$, obtenemos (6.15). Pasamos a probar (6.14).

Suponemos, pues, que $6 \le r \le \log\log\tau$, $R = 2^{r-1}$ y que $1 - 1/R \le \sigma \le 1$. Sea $3 \le k \le r-2$, de modo que $K = 2^k$ cumple $4K = 2^{k+1} \le 2^{r-1} = R$. Por consiguiente,

$$\sigma \ge 1 - \frac{1}{R} \ge 1 - \frac{1}{4K}$$

y $Rr \ge 4Kr \ge 4K(k+2) \ge Kk$. Podemos aplicar (6.15), de modo que

$$\left|\sum_{\tau^{2/(k+2)}<n\le\tau^{2/(k+1)}} \frac{1}{n^s}\right| = O(\tau^{-\frac{1}{84K}}\log^2\tau) = O(\tau^{-\frac{1}{84rR}}\log^2\tau)$$

$$= O(\tau^{-\frac{1}{8}\frac{1}{\log\log\tau}2^{1-\log\log\tau}}\log^2\tau),$$

pues $Rr \le 2^{r-1}r \le 2^{\log\log\tau-1}\log\log\tau$. Ahora,

$$2^{1-\log\log\tau} = 2/e^{\log\log\tau\log 2} = 2/(\log\tau)^{\log 2} = 2(\log\tau)^{-\log 2},$$

luego

$$\left|\sum_{\tau^{2/(k+2)}<n\le\tau^{2/(k+1)}} \frac{1}{n^s}\right| = O(\tau^{-\frac{1}{4}\frac{(\log\tau)^{-\log 2}}{\log\log\tau}}\log^2\tau)$$

$$= O(e^{-\frac{1}{4}\frac{(\log\tau)^{1-\log 2}}{\log\log\tau}}\log^2\tau) = O(1/\log\tau).$$

Para comprobar la última igualdad basta ver que

$$\lim_{\tau\to+\infty} e^{-\frac{1}{4}\frac{(\log\tau)^\alpha}{\log\log\tau}}\log^3\tau = 0,$$

donde $\alpha = 1 - \log 2$. Equivalentemente, basta ver que:

$$\lim_{x\to+\infty} \frac{x^3}{e^{\frac{1}{4}\frac{x^\alpha}{\log x}}} = 0.$$

Observamos que $9\alpha < 3 < 10\alpha$, de modo que

$$\frac{x^3}{e^{\frac{1}{4}\frac{x^\alpha}{\log x}}} \le \frac{x^3}{\sum_{k=0}^{10}\frac{1}{4^k k!}\frac{x^{k\alpha}}{\log^k x}} = \frac{1}{\sum_{k=0}^{9}\frac{1}{4^k k!}\frac{1}{x^{3-k\alpha}\log^k x} + \frac{1}{4^{10}10!}\frac{x^{10\alpha-3}}{\log^{10} x}}.$$

El primer sumando del último denominador tiende a 0, pero el segundo tiende a $+\infty$, luego la fracción tiende a 0.

A su vez,

$$\left|\sum_{\tau^{2/r}<n\le\tau^{1/2}} \frac{1}{n^s}\right| \le \sum_{k=3}^{r-2}\left|\sum_{\tau^{2/(k+2)}<n\le\tau^{2/(k+1)}} \frac{1}{n^s}\right| \le \frac{Cr}{\log\tau} \le \frac{C\log\log\tau}{\log\tau} = O(1).$$

■

La estimación final que vamos a necesitar es la siguiente:

Teorema 6.13 (Hardy-Littlewood-Weyl) *En la región del plano complejo determinada por las condiciones* $\frac{63}{64} \le \sigma < 1$, $\tau \ge 3$, *se cumple que*

$$\zeta(s) = O\left(\tau^{4(1-\sigma)/\log\frac{1}{1-\sigma}} \frac{\log\tau}{\log\log\tau}\right).$$

DEMOSTRACIÓN: Fijamos $\tau > e^{e^6}$ y definimos

$$r = E[\text{mín}\{\frac{\log\frac{1}{1-\sigma}}{\log 2}, \log\log\tau\}].$$

Como $\frac{63}{64} \le \sigma < 1$, tenemos que $\frac{1}{1-\sigma} \ge 64 = 2^6$, luego $6 \le r \le \log\log\tau$. Además

$$\sigma \ge 1 - \frac{1}{2^r} > 1 - \frac{1}{R},$$

donde $R = 2^{r-1}$. Se cumplen, pues, todas las hipótesis del teorema anterior. Por consiguiente:

$$|\zeta(s)| \le \sum_{n=1}^{E[\tau^{2/r}]} \frac{1}{n^\sigma} + O(1). \tag{6.16}$$

Ahora distinguimos dos casos:

CASO 1 Si se cumple $1 - \sigma \le \frac{\log\log\tau}{\log\tau}$, entonces

$$r \ge E[\text{mín}\{\frac{\log\log\tau - \log\log\log\tau}{\log 2}, \log\log\tau\}]$$

y si tomamos el τ inicial suficientemente grande (mayor que una constante independiente de σ) podemos exigir que en este caso se cumpla $r > \frac{\log\log\tau}{2}$. Ahora:

$$\sum_{n=1}^{E[\tau^{2/r}]} \frac{1}{n^\sigma} = \sum_{n=1}^{E[\tau^{2/r}]} \frac{n^{1-\sigma}}{n} \le \tau^{\frac{2(1-\sigma)}{r}} \sum_{n=1}^{E[\tau^{2/r}]} \frac{1}{n},$$

pues $n^{1-\sigma} = e^{(1-\sigma)\log n} \le e^{(1-\sigma)\log\tau^{2/r}} = \tau^{\frac{2(1-\sigma)}{r}}$. Continuando:

$$\sum_{n=1}^{E[\tau^{2/r}]} \frac{1}{n^\sigma} \le e^{\log\tau\frac{4}{\log\log\tau}\frac{\log\log\tau}{\log\tau}} 2\log\tau^{2/r} < 4e^4\frac{\log\tau}{\log\log\tau}$$

$$< 4e^4\tau^{4(1-\sigma)/\log\frac{1}{1-\sigma}}\frac{\log\tau}{\log\log\tau},$$

donde hemos acotado

$$\sum_{n=1}^{E[\tau^{2/r}]} \frac{1}{n} \le 1 + \sum_{n=2}^{E[\tau^{2/r}]} \int_{n-1}^{n} \frac{dx}{x} \le 1 + \int_1^{\tau^{2/r}} \frac{dx}{x} = 1 + \log\tau^{2/r} < 2\log\tau^{2/r},$$

para τ suficientemente grande.

Caso 2 Si se cumple $1-\sigma > \frac{\log\log\tau}{\log\tau}$, entonces

$$\log\frac{1}{1-\sigma} < \log\log\tau - \log\log\log\tau < \log\log\tau,$$

luego

$$r = E\left[\frac{\log\frac{1}{1-\sigma}}{\log 2}\right] \geq E[\log\frac{1}{1-\sigma}] > \frac{1}{2}\log\frac{1}{1-\sigma}$$

y

$$\sum_{n=1}^{E[\tau^{2/r}]}\frac{1}{n^\sigma} < \int_0^{\tau^{2/r}}\frac{dx}{x^\sigma} = \frac{\tau^{2/r(1-\sigma)}}{1-\sigma} < \frac{\tau^{\frac{4(1-\sigma)}{\log\frac{1}{1-\sigma}}}}{\log\log\tau}\log\tau.$$

Así pues, en ambos casos tenemos que

$$\sum_{n=1}^{E[\tau^{2/r}]}\frac{1}{n^\sigma} < C\tau^{4(1-\sigma)/\log\frac{1}{1-\sigma}}\frac{\log\tau}{\log\log\tau},$$

y el término de la derecha tiende a $+\infty$ cuando τ tiende a $+\infty$, luego (6.16) implica ahora que

$$|\zeta(s)| \leq C\tau^{4(1-\sigma)/\log\frac{1}{1-\sigma}}\frac{\log\tau}{\log\log\tau}, \tag{6.17}$$

y esto es lo que había que probar. ∎

Observemos que si en (6.17) hacemos tender $\sigma \to 1$ obtenemos que

$$|\zeta(1+i\tau)| \leq C\frac{\log\tau}{\log\log\tau},$$

luego

$$\zeta(1+i\tau) = O(\frac{\log\tau}{\log\log\tau}).$$

Pero la consecuencia principal es la siguiente:

Teorema 6.14 *Existe una constante $A > 1$ tal que, para todo $s \in \mathbb{C}$ tal que $\tau \geq 3$ y $\sigma \geq 1 - \frac{(\log\log\tau)^2}{\log\tau}$ se cumple que*

$$\zeta(s) = O(\log^A\tau).$$

Demostración: Notemos que $1 - \frac{(\log\log\tau)^2}{\log\tau} > 63/64$, luego si $\sigma \leq 1$ el teorema anterior nos da que

$$\zeta(s) = O\left(\tau^{4(1-\sigma)/\log\frac{1}{1-\sigma}}\frac{\log\tau}{\log\log\tau}\right) = O\left(e^{\frac{4(\log\log\tau)^2}{\log\tau}\log\frac{1}{(\log\log\tau)^2}}\frac{\log\tau}{\log\log\tau}\right)$$

$$= O\left(e^{4\log\log\tau}\frac{\log\tau}{\log\log\tau}\right) = O(\frac{\log^5\tau}{\log\log\tau}) = O(\log^5\tau).$$

Para $\sigma \geq 1$ se cumple que $\zeta(s) = O(\log\tau)$, por el teorema 4.7. ∎

Este teorema nos permite aplicar el teorema 5.22 con

$$\theta(t) = \frac{(\log\log t)^2}{\log t}, \qquad \phi(t) = A\log\log t.$$

El resultado es:

Teorema 6.15 (Littlewood) *Existe una constante $A > 0$ tal que $\zeta(s)$ no se anula en la región*

$$1 - \frac{A\log\log\tau}{\log\tau} < \sigma, \qquad \tau > t_0.$$

En principio tendríamos que poner $2\tau + 1$ en lugar de τ dentro de los logaritmos, pero es fácil ver que, para τ suficientemente grande, se cumple que

$$\frac{2A\log\log\tau}{\log\tau} > \frac{A\log\log(2\tau+1)}{\log(2\tau+1)},$$

ya que el cociente tiende a 2, luego es finalmente mayor que 1.

A su vez esto nos permite aplicar el teorema 5.20:

Teorema 6.16 *Existe una constante $A > 0$ tal que*

$$\psi(x) = x + O(xe^{-A\sqrt{\log x\log\log x}}), \qquad \pi(x) = \mathrm{li}(x) + O(xe^{-A\sqrt{\log x\log\log x}}).$$

Demostración: Consideramos la función

$$\eta(t) = \begin{cases} A\frac{\log\log t}{\log t} & \text{si } t > e^e, \\ A/e & \text{si } 0 \le t \le e^e. \end{cases}$$

Es fácil ver que cumple las hipótesis del teorema 5.20 (salvo que no es derivable en el punto e^e, pero, como ya señalamos en la nota al pie en las observaciones posteriores al teorema, éste sigue siendo válido aunque la derivabilidad falle en un número finito de puntos). Notemos que tomando la constante A suficientemente grande podemos asegurarnos de que no haya ningún cero no trivial en la zona finita de la región $1 - \eta(\tau) < \sigma$ que no cubre el teorema de Littlewood.

La única dificultad es estimar la función $\omega(x)$. Ahora bien, consideramos la función $\xi(x) = e^{\sqrt{\log x}}$. Para todo x tal que $\xi(x) \ge e^e$, usando que $(a+b)^2 \ge 4ab$, vemos que

$$\eta(t)\log x + \log t \ge \begin{cases} 2\sqrt{A\log x\log\log t} \ge \sqrt{2A\log x\log\log x}, & \text{si } t \ge \xi(x), \\ \eta(\xi(x))\log x = (A/2)\sqrt{\log x}\log\log x, & \text{si } 1 \le t \le \xi(x). \end{cases}$$

Por lo tanto

$$\omega(x) \ge \sqrt{2A\log x\log\log x},$$

para todo x suficientemente grande. ∎

Esto prueba que, como habíamos adelantado, el teorema 5.15 se cumple para toda constante c. Al margen de la mejora que esto supone respecto de 5.15, lo más relevante es que el teorema 6.15 nos asegura que se cumple la primera de las hipótesis del teorema de Hoheisel 5.21. En la sección siguiente nos ocuparemos de la segunda.

6.3 El teorema de Ingham

En esta sección demostraremos el teorema siguiente:

Teorema 6.17 *Si* $\zeta(1/2+i\tau) = O(\tau^c)$, *entonces*

$$N(\sigma, T) = O(T^{2(1+2c)(1-\sigma)} \log^5 T),$$

para $1/2 \le \sigma \le 1$.

Esto tiene interés a causa del teorema de Hoheisel, 5.21, pues, teniendo en cuenta también el teorema 6.15, así podemos concluir que las hipótesis de 5.21 se satisfacen con $b = 2 + 4c$ y $B = 5$ (y la A dada por el teorema 6.15), luego llegamos a que todo θ que cumpla

$$\frac{1+4c+5/A}{2+4c+5/A} < \theta < 1$$

satisface la conclusión del teorema. El mero hecho de que exista una constante $0 < \theta < 1$ que cumpla el teorema ya es algo notable en sí mismo, pero en el capítulo siguiente demostraremos (véanse las observaciones tras el teorema 7.14) que, en realidad, el teorema 6.15 se cumple para cualquier valor de A, luego haciendo tender A a $+\infty$ obtenemos una cota para θ que depende exclusivamente de c, a saber:

Teorema 6.18 (Ingham) *Si* $\zeta(1/2+i\tau) = O(\tau^c)$, *con* $c > 0$ *y*

$$\frac{1+4c}{2+4c} < \theta < 1,$$

para todo $k > 0$ *se cumple que*

$$\pi(x + kx^\theta) - \pi(x) \sim \frac{kx^\theta}{\log x}, \qquad p_{n+1} - p_n = O(p_n^\theta).$$

Ya sabíamos que si admitimos la hipótesis de Lindelöf (en particular, si admitimos la hipótesis de Riemann) tenemos que la conclusión del teorema se cumple siempre que $1/2 < \theta < 1$. El teorema anterior, en cambio, nos permite encontrar valores de θ de los que podemos afirmar que cumplen la conclusión sin apoyarnos en hipótesis no demostradas. Concretamente, el teorema 6.9 nos permite tomar $c = 1/6 + \epsilon$, con lo que podemos afirmar que la conclusión se cumple siempre que $5/8 < \theta < 1$.

Pasamos, pues a la prueba del teorema 6.17. Para ello necesitamos algunos resultados previos. Empezamos con un resultado general sobre funciones holomorfas:

Teorema 6.19 (Hardy, Ingham, Pólya) *Sea* f *una función holomorfa en un entorno de la banda* $\sigma_1 \le \sigma \le \sigma_2$. *Supongamos que existe*

$$J(\sigma) = \int_{-\infty}^{+\infty} |f(\sigma + i\tau)|^2 \, d\tau$$

y que la convergencia de la integral es uniforme en $[\sigma_1, \sigma_2]$*, así como que*

$$\lim_{|\tau|\to+\infty} |f(\sigma + i\tau)| = 0$$

también uniformemente. Entonces

$$J(\sigma) \leq J(\sigma_1)^{\frac{\sigma_2-\sigma}{\sigma_2-\sigma_1}} J(\sigma_2)^{\frac{\sigma-\sigma_1}{\sigma_2-\sigma_1}}.$$

DEMOSTRACIÓN: Probaremos primero la conclusión para $\sigma = \sigma_0 = \frac{\sigma_1+\sigma_2}{2}$. Consideremos la frontera R del rectángulo dado por $\sigma_1 \leq \sigma \leq \sigma_2$, $-T \leq \tau \leq T$. Tenemos que f es holomorfa en un entorno de dicho rectángulo, al igual que lo es la función $f^*(s) = \overline{f(2\sigma_0 - \bar{s})}$ (basta considerar los desarrollos en serie de Taylor de la función $f(2\sigma_0 - s)$. Las dos conjugaciones equivalen a conjugar sus coeficientes.) Sobre la recta $\sigma = \sigma_0$ tenemos que $f^*(s) = \overline{f(s)}$, luego, por el teorema de Cauchy,

$$\int_{\sigma_0-iT}^{\sigma_0+iT} |f(s)|^2\, ds = \int_{\sigma_0-iT}^{\sigma_0+iT} f(s)f^*(s)\, ds = \int_{\gamma_2} f(s)f^*(s)\, ds,$$

donde $\gamma_2 : [a, b] \longrightarrow \mathbb{C}$ representa la poligonal formada por los tres segmentos de R situados a la derecha de la recta $\sigma = \sigma_0$. Así pues, aplicando la desigualdad de Hölder,

$$\int_{\sigma_0-iT}^{\sigma_0+iT} |f(s)|^2\, ds \leq \int_a^b |f(\gamma_2(t))||f^*(\gamma_2(t))|\, dt$$

$$\leq \left(\int_a^b |f(\gamma_2(t))|^2\, dt\right)^{1/2} \left(\int_a^b |f^*(\gamma_2(t))|^2\, dt\right)^{1/2}$$

$$= \left(\int_a^b |f(\gamma_2(t))|^2\, dt\right)^{1/2} \left(\int_a^b |f(\gamma_1(t))|^2\, dt\right)^{1/2},$$

donde $\gamma_1 : [a, b] \longrightarrow \mathbb{C}$ es la parte de R a la izquierda de la recta $\sigma = \sigma_0$, pues la aplicación $s \mapsto 2\sigma_0 - \bar{\sigma}$ biyecta los puntos de γ_2^* con los de γ_1^*. Explícitamente,

$$\int_a^b |f(\gamma_2(t))|^2\, dt = \int_{\sigma_0}^{\sigma_2} |f(\sigma - iT)|^2\, d\sigma + \int_{-T}^{T} |f(\sigma_2 + it)|^2\, dt + \int_{\sigma_0}^{\sigma_2} |f(\sigma + iT)|^2\, d\sigma.$$

Por hipótesis,

$$\lim_{T\to+\infty} \int_{\sigma_0}^{\sigma_2} |f(t \pm iT)|^2\, dt = 0,$$

por lo que

$$\lim_{T\to+\infty} \int_a^b |f(\gamma_2(t))|^2\, dt = \int_{-\infty}^{+\infty} |f(\sigma_2 + it)|^2\, dt = J(\sigma_2),$$

e igualmente

$$\lim_{T\to+\infty} \int_a^b |f(\gamma_1(t))|^2\, dt = J(\sigma_1),$$

lo que nos da la conclusión para σ_0.

Ahora observamos que si la conclusión es cierta para $\sigma_1 \le \sigma_1' < \sigma_2' \le \sigma_2$, también lo es para $\sigma_0' = (\sigma_1' + \sigma_2')/2$. En efecto, por la parte ya probada,

$$J(\sigma_0') \le J(\sigma_1')^{1/2} J(\sigma_2')^{1/2} \le$$

$$\left(J(\sigma_1)^{\frac{\sigma_2-\sigma_1'}{\sigma_2-\sigma_1}} J(\sigma_2)^{\frac{\sigma_1'-\sigma_1}{\sigma_2-\sigma_1}}\right)^{1/2} \left(J(\sigma_1)^{\frac{\sigma_2-\sigma_2'}{\sigma_2-\sigma_1}} J(\sigma_2)^{\frac{\sigma_2'-\sigma_1}{\sigma_2-\sigma_1}}\right)^{1/2} =$$

$$J(\sigma_1)^{\frac{\sigma_2-\sigma_0'}{\sigma_2-\sigma_1}} J(\sigma_2)^{\frac{\sigma_0'-\sigma_1}{\sigma_2-\sigma_1}}.$$

Pero la conclusión es trivialmente cierta para σ_1 y σ_2, luego tenemos el teorema probado para todos los valores $\sigma = \sigma_1 + (\sigma_1 - \sigma_1)\frac{m}{2^n}$, con $0 \le m \le 2^n$. Como $J(\sigma)$ es una función continua, esto implica que se cumple para todo σ. ∎

La parte más técnica de la prueba del teorema de Ingham es el resultado siguiente:

Teorema 6.20 *Sea $M_X(s) = \sum_{n<X} \frac{\mu(n)}{n^s}$, donde μ es la función de Möbius, y sea*

$$f_X(s) = \zeta(s) M_X(s) - 1.$$

Si $\zeta(1/2 + i\tau) = O(\tau^c)$, para cierta constante $c > 0$, entonces

$$\int_1^T |f_X(\sigma + i\tau)|^2 d\tau < A \frac{T^{4c(1-\sigma)}}{X^{2\sigma-1}} (T + X) \log^4(T + X),$$

para $1/2 \le \sigma \le 1$, $T > 1$, $X > 1$ y cierta constante $A > 0$.

Demostración: Notemos que si la conclusión se cumple para un valor de c, se cumple para cualquier otro mayor, y sabemos que la hipótesis se cumple para $c > 1/6$, luego no perdemos generalidad si suponemos que $c < 1/2$.

Si $1 < X < 2$, se cumple que $f_X = f_2$, por lo que no tampoco perdemos generalidad si suponemos que $X \ge 2$.

Podemos ver a $M_X(s)$ como una serie de Dirichlet que tiene nulos sus coeficientes correspondientes a índices $n \ge X$, con lo que el producto también es una serie de Dirichlet y

$$f_X(s) = \sum_{n=1}^{\infty} \frac{a_X(n)}{n^s}, \qquad \text{donde } a_X(n) = \sum_{\substack{d|n \\ d<X}} \mu(d), \quad \text{salvo } a_X(1) = 0.$$

Notemos que si $n < X$ entonces $a_X(n) = 0$, pues $\mu * c_1 = 1$. Por otro lado, es claro que $|a_X(n)| \le d(n)$.

Si $0 < \delta < 1$ y $T > 0$, tenemos que

$$\int_0^T |f_X(1 + \delta + i\tau)|^2 \, d\tau = \sum_{m,n \ge X} \frac{a_X(m) a_X(n)}{(mn)^{1+\delta}} \int_0^T (n/m)^{i\tau} \, d\tau$$

$$= T\sum_{m\ge X}\frac{a_X^2(m)}{m^{2+2\delta}} + \sum_{X\le m<n}\frac{a_X(m)a_X(n)}{(mn)^{1+\delta}}\int_0^T (n/m)^{i\tau}\,d\tau$$

$$+ \sum_{X\le n<m}\frac{a_X(m)a_X(n)}{(mn)^{1+\delta}}\int_0^T (n/m)^{i\tau}\,d\tau$$

$$= T\sum_{m\ge X}\frac{a_X^2(m)}{m^{2+2\delta}} + \sum_{X\le m<n}\frac{a_X(m)a_X(n)}{(mn)^{1+\delta}}\int_0^T (n/m)^{i\tau}\,d\tau$$

$$+ \sum_{X\le m<n}\frac{a_X(m)a_X(n)}{(mn)^{1+\delta}}\int_0^T (n/m)^{-i\tau}\,d\tau$$

$$= T\sum_{m\ge X}\frac{a_X^2(m)}{m^{2+2\delta}} + 2\sum_{X\le m<n}\frac{a_X(m)a_X(n)}{(mn)^{1+\delta}}\int_0^T \cos(\tau\log(n/m))\,d\tau$$

$$\le T\sum_{m\ge X}\frac{d^2(m)}{m^{2+2\delta}} + 2\sum_{X\le m<n}\frac{d(m)d(n)}{(mn)^{1+\delta}\log(n/m)}\operatorname{sen}(T\log(n/m))$$

$$\le T\sum_{m\ge X}\frac{d^2(m)}{m^{2+2\delta}} + 2\sum_{X\le m<n}\frac{d(m)d(n)}{(mn)^{1+\delta}\log(n/m)}.$$

Observamos ahora que, si $1<a<3$, en virtud del teorema 2.24,

$$\sum_{m\ge X}\frac{d^2(m)}{m^{1+a}} = \sum_{m\ge X} d^2(m)\int_m^{+\infty}\frac{1+a}{x^{2+a}}\,dx$$

$$= \int_X^{+\infty}\frac{1+a}{x^{2+a}}\sum_{m\ge X}\chi_{[m,+\infty[}(x)d^2(m)\,dx = \int_X^{+\infty}\frac{1+a}{x^{2+a}}\sum_{X\le m\le x} d^2(m)\,dx$$

$$< A\int_X^{+\infty}\frac{\log^3 x}{x^{1+a}}\,dx = A\int_1^{+\infty}\frac{\log^3(Xy^{1/a})}{aX^a y^2}\,dy$$

$$= \frac{A}{aX^a}\int_1^{+\infty}\frac{(\frac{\log X}{y^{1/6}} + \frac{1}{a}\frac{\log y}{y^{1/6}})^3}{y^{3/2}}\,dy < \frac{A}{X^a}\int_1^{+\infty}\frac{(A\log X + A)^3}{y^{3/2}}\,dy$$

$$< \frac{A}{X^a}(\log X+1)^3\int_1^{+\infty} y^{-3/2}\,dy = \frac{A}{X^a}\log^3 X.$$

Tomando concretamente $a = 1+2\delta$ obtenemos

$$\sum_{m\ge X}\frac{d^2(m)}{m^{2+2\delta}} < \frac{A}{X^{1+2\delta}}\log^3 X < \frac{A}{X\delta^3},$$

pues $X^{2\delta} = e^{2\delta\log X} > \frac{1}{6}(2\delta\log X)^3$, por la serie de Taylor de la exponencial.

Por otra parte observamos que, si $\lambda > 1$, se cumple que

$$1 < \log\lambda + \frac{1}{\lambda} < \log\lambda + \frac{1}{\sqrt{\lambda}}. \tag{6.18}$$

(basta ver que $\log\lambda - 1/\lambda - 1$ es creciente, porque tiene derivada positiva).

Lo aplicamos a $\lambda = n/m$, con lo que obtenemos que

$$\frac{1}{\log(n/m)} < 1 + \frac{1}{n^{1/2}m^{-1/2}\log(n/m)}.$$

Por consiguiente,

$$\frac{1}{(mn)^{1+\delta}\log(n/m)} < \frac{1}{(mn)^{1+\delta}} + \frac{1}{m^\delta n^{1+\delta}(mn)^{1/2}\log(n/m)},$$

y a su vez

$$\sum_{X\le m<n} \frac{d(m)d(n)}{(mn)^{1+\delta}\log(n/m)} < \sum_{X\le m<n} \frac{d(m)d(n)}{(mn)^{1+\delta}} +$$

$$\sum_{X\le m<n} \frac{d(m)d(n)}{m^\delta n^{1+\delta}(mn)^{1/2}\log(n/m)} <$$

$$\left(\sum_{n=1}^{\infty} \frac{d(n)}{n^{1+\delta}}\right)^2 + \sum_{1\le m<n} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)}\frac{1}{n^{1+\delta}}$$

$$= \zeta^4(1+\delta) + \sum_{1\le m<n} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)} \int_n^{+\infty} \frac{1+\delta}{x^{2+\delta}}\,dx$$

$$= \zeta^4(1+\delta) + \int_1^{+\infty} \frac{1+\delta}{x^{2+\delta}} \sum_{1\le m<n} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)} \chi_{[n,+\infty[}(x)\,dx$$

$$= \zeta^4(1+\delta) + \int_1^{+\infty} \frac{1+\delta}{x^{2+\delta}} \sum_{m<n\le x} \frac{d(m)d(n)}{(mn)^{1/2}\log(n/m)}\,dx$$

$$< \zeta^4(1+\delta) + \int_1^{+\infty} \frac{1+\delta}{x^{1+\delta}} c\log^3 x\,dx,$$

de nuevo por el teorema 2.24. Ahora, por una parte,

$$\zeta(1+\delta) \le 1 + \frac{1}{\delta} = \frac{\delta+1}{\delta} \le \frac{2}{\delta},$$

y por otra parte, como $x^{-\delta/2}\log^3 x$ está acotada,

$$\int_1^{+\infty} \frac{1+\delta}{x^{1+\delta}} A\log^3 x\,dx \le c\int_1^{+\infty} \frac{1}{x^{1+\delta/2}}\,dx \le \frac{2A}{\delta} \le \frac{A}{\delta^4}.$$

En definitiva,

$$\sum_{X\le m<n} \frac{d(m)d(n)}{(mn)^{1+\delta}\log(n/m)} < \frac{A}{\delta^4}.$$

En total tenemos que

$$\int_0^T |f_X(1+\delta+i\tau)|^2\,d\tau < A\left(\frac{T}{X}+1\right)\delta^{-4}.$$

Ahora obtendremos una estimación similar para $1/2 + i\tau$. Para ello observamos que de $(x-y)^2 \geq 0$ se sigue que $(x+y)^2 \leq 2(x^2+y^2)$, luego

$$|f_X(s)|^2 \leq (|\zeta(s)||M_X(s)|+1)^2 \leq 2(|\zeta(s)|^2|M_X(s)|^2+1).$$

Así, para $T > 0$,

$$\int_0^T |f_X(1/2+i\tau)|^2\,d\tau \leq 2\int_0^T (|\zeta(1/2+i\tau)|^2|M_X(1/2+i\tau)|^2+1)\,d\tau$$

$$\leq AT^{2c}\int_0^T |M_X(1/2+i\tau)|^2\,d\tau + 2T.$$

Como antes,

$$\int_0^T |M_X(1/2+i\tau)|^2\,d\tau = \int_0^T \sum_{m,n<X} \frac{\mu(m)\mu(n)}{m^{1/2+i\tau}n^{1/2-i\tau}}\,d\tau$$

$$= \sum_{m,n<X} \frac{\mu(m)\mu(n)}{(mn)^{1/2}} \int_0^T \Big(\frac{m}{n}\Big)^{i\tau}\,d\tau \leq$$

$$T\sum_{n<X}\frac{1}{n} + 4\sum_{m<n<X}\frac{1}{(mn)^{1/2}}\int_0^T \cos\log(m/n)\tau\,d\tau \leq$$

$$T\sum_{n<X}\frac{1}{n} + 4\sum_{m<n<X}\frac{1}{(mn)^{1/2}\log(m/n)}.$$

Seguidamente usamos que (6.18) equivale a

$$\frac{1}{\log\lambda} < 1 + \frac{\lambda^{1/2}}{\lambda-1},$$

luego

$$\frac{1}{\log(m/n)} < 1 + \frac{(mn)^{1/2}}{m-n},$$

luego

$$\int_0^T |M_X(1/2+i\tau)|^2\,d\tau \leq T\sum_{n<X}\frac{1}{n} + 4\sum_{m<n<X}\left(\frac{1}{(mn)^{1/2}} + \frac{1}{n-m}\right)$$

$$\leq T\log X + 4\sum_{m<X}\sum_{n<X}\frac{2}{n} \leq T\log X + 8X\log X.$$

En total tenemos que

$$\int_0^T |f_X(1/2+i\tau)|^2\,d\tau \leq AT^{2c}(T+X)\log X.$$

Faltaría un sumando $2T$, pero, si $T \geq 1$

$$T \leq T^{1+2c} \leq \frac{1}{\log 2} T^{1+2c} \log X \leq AT^{2c}(T+X)\log X,$$

mientras que, para $0 \leq T \leq 1$, tenemos una acotación más simple, ya que $\zeta(1/2+i\tau)$ está acotada en $[0,1]$, luego, si $0 \leq \tau \leq 1$,

$$|f_X(1/2+i\tau)| \leq A(\sum_{n<X} \frac{1}{\sqrt{n}} + 1) \leq A(\int_1^X \frac{1}{\sqrt{x}}\, dx + 2) = A(2\sqrt{X}+2) \leq A\sqrt{X},$$

con lo que

$$\int_0^T |f_X(1/2+i\tau)|^2\, d\tau \leq ATX \leq AT^{2c}X \leq AT^{2c}(T+X)\log X,$$

porque $2c < 1$ y $T \leq 1$, luego $T \leq T^{2c}$.

En resumen, si llamamos

$$I_\sigma(T) = \int_0^T |f_X(\sigma+i\tau)|^2\, d\tau,$$

hemos probado que

$$I_{1/2}(T) = O(T^{2c}(T+X)\log X), \qquad I_{1+\delta}(T) = O((\frac{T}{X}+1)\delta^{-4}).$$

Consideramos ahora

$$\phi(s) = \frac{s-1}{s\cos(s/2t)} f_X(s), \qquad t > 3/\pi.$$

Notemos que el coseno no se anula en la banda $1/2 \leq \sigma \leq 1+\delta$, por lo que, teniendo en cuenta que el factor $s-1$ cancela el polo de $\zeta(s)$, resulta que ϕ es holomorfa en un entorno de dicha banda. Observemos que, en ese mismo dominio,

$$|\cos(s/2t)|^2 = \frac{e^{\frac{-\tau+i\sigma}{2t}} + e^{\frac{\tau-i\sigma}{2t}}}{2} \frac{e^{\frac{-\tau-i\sigma}{2t}} + e^{\frac{\tau+i\sigma}{2t}}}{2} = \frac{1}{2}\cos\frac{\sigma}{t} + \frac{1}{4}(e^{\tau/t} + e^{-\tau/t}),$$

luego

$$|\cos(s/2t)|^2 e^{-|\tau|/t} = \frac{1}{2}e^{-|\tau|/t}\cos\frac{\sigma}{t} + \frac{1}{4}(1+e^{-2|\tau|/t}) \to \frac{1}{4} \tag{6.19}$$

cuando τ tiende a $\pm\infty$. Así pues,

$$\frac{1}{|\cos(s/2t)|^2} = O(e^{-|\tau|/t}).$$

Por 4.7, para $\sigma \geq 1/2$ y $|\tau| \geq 3$ tenemos que $\zeta(s) = O(|\tau|^{1/2})$, luego

$$\left|\frac{s-1}{s} f_X(s)\right| = \left|\frac{s-1}{s}\zeta(s)M_X(s) - \frac{s-1}{s}\right| \leq A|\tau|^{1/2}X + 2 \leq AX|\tau|^{1/2}.$$

Si la constante se toma suficientemente grande, esto vale para todo τ (con $\sigma \geq 1/2$). Así,

$$|\phi(s)|^2 \leq AX^2|\tau|e^{-|\tau|/t},$$

lo que prueba la convergencia de la integral

$$J_\sigma = \int_{-\infty}^{+\infty} |\phi(\sigma + i\tau)|^2 \, d\tau$$

uniformemente en la banda $1/2 \leq \sigma \leq 1 + \delta$, así como que

$$\lim_{|\tau|\to+\infty} |\phi(\sigma + i\tau)| = 0$$

también uniformemente. Similarmente concluimos que $|I_\sigma(T)| \leq AX^2T^2$.

El hecho de que ϕ tome valores reales sobre los números reales implica que $\phi(\bar{s}) = \overline{\phi(s)}$, luego $|\phi(\bar{s})| = |\phi(s)|$. Esto nos permite expresar

$$J_\sigma = 2\int_0^{+\infty} |\phi(\sigma + i\tau)|^2 \, d\tau.$$

Integrando por partes:

$$J_\sigma \leq 2\int_0^{+\infty} Ae^{-\tau/t}|f_X(\sigma + i\tau)|^2 \, d\tau =$$

$$2A \lim_{T\to+\infty} \left(-\frac{1}{t}e^{-T/t}I_\sigma(T) + \frac{1}{t}\int_0^T e^{-\tau/t}I_\sigma(\tau)\, d\tau\right)$$

$$= 2A \lim_{T\to+\infty} \int_0^{T/t} e^{-w}I_\sigma(tw)\, dw = 2c\int_0^{+\infty} e^{-w}I_\sigma(tw)\, dw,$$

donde hemos eliminado el primer término por la acotación $|I_\sigma(T)| \leq AX^2T^2$ y luego hemos hecho el cambio de variable $\tau = tw$. Ahora podemos usar las cotas que hemos obtenido para I_σ:

$$J_{1+\delta} \leq 2A\int_0^{+\infty} e^{-w}\left(\frac{tw}{X} + 1\right)\delta^{-4}\, dw = A\left(1 + \frac{t}{X}\right)\delta^{-4},$$

donde hemos integrado por partes. Similarmente,

$$J_{1/2} \leq 2A\int_0^{+\infty} e^{-w}(tw)^{2c}(tw + X)\log X\, dw$$

$$= 2At^{2c}\log X\int_0^{+\infty} e^{-w}w^{2c}(tw + X)\, dw.$$

Descomponemos la integral en suma de las integrales en $[0,1]$ y en $[1,+\infty[$. En el primer intervalo acotamos $w^{2c} \le 1$, con lo que

$$\int_0^1 e^{-w} w^{2c}(tw+X)\,dw \le \int_0^1 e^{-w}(tw+X)\,dw.$$

En el segundo usamos que $w^{2c} \le w$ e integramos por partes:

$$\int_1^{+\infty} e^{-w} w^{2c}(tw+X)\,dw = (t+X)e^{-1} + \int_1^{+\infty} e^{-w}(2tw+X)\,dw$$

$$\le (t+X)e^{-1} + 2\int_1^{+\infty} e^{-w}(tw+X)\,dw.$$

Uniendo de nuevo las dos partes resulta que

$$\int_0^{+\infty} e^{-w} w^{2c}(tw+X)\,dw \le (t+X)e^{-1} + 2\int_0^{+\infty} e^{-w}(tw+X)\,dw.$$

Integrando otra vez por partes llegamos a que

$$\int_0^{+\infty} e^{-w} w^{2c}(tw+X)\,dw \le (t+X)e^{-1} + 2(t+X) = (2+e^{-1})(t+X).$$

En total,

$$J_{1/2} \le At^{2c}(t+X)\log X.$$

Así podemos aplicar el teorema 6.19, según el cual, para cada $1/2 \le \sigma \le 1+\delta$, tenemos que

$$J_\sigma \le \left(A\left(1+\frac{t}{X}\right)\delta^{-4}\right)^{\frac{\sigma-1/2}{1/2+\delta}} \left(At^{2c}(t+X)\log X\right)^{\frac{1+\delta-\sigma}{1/2+\delta}} \le$$

$$X^{\frac{1-2\sigma}{2\delta+1}} t^{\frac{4c(1+\delta-\sigma)}{2\delta+1}} (X+t)\,\text{máx}\{A\delta^{-4}, A\log X\}.$$

Por otra parte, en dicha banda, para $\tau \ge 1$, en virtud de (6.19) tenemos que

$$|\phi(s)|^2 \ge Ae^{-\tau/t}|f_X(s)|^2,$$

pues el cociente sin la constante tiende a 4, luego

$$J_\sigma \ge \int_1^T |\phi(\sigma+i\tau)|^2\,d\tau \ge \int_1^T Ae^{-\tau/t}|f_X(\sigma+i\tau)|^2\,d\tau$$

$$\ge Ae^{-T/t}\int_1^T |f_X(\sigma+i\tau)|^2\,d\tau.$$

En total,

$$\int_1^T |f_X(\sigma+i\tau)|^2\,d\tau \le Ae^{T/t} X^{\frac{1-2\sigma}{2\delta+1}} t^{\frac{4A(1+\delta-\sigma)}{2\delta+1}} (X+t)\,\text{máx}\{A\delta^{-4}, A\log X\}.$$

Tomamos $t = T$, $\delta = A/\log(T+X)$, donde $A = \frac{1}{4}\log 3$, para que se cumpla $0 < \delta \le 1/4$. Así,

$$X^{\frac{1-2\sigma}{2\delta+1}} \le X^{-(1-2\delta)(2\sigma-1)} \le X^{-(2\sigma-1)+2\delta} \le e^{2A} X^{-(2\sigma-1)}.$$

En efecto, la primera desigualdad se reduce a que $1-(2\delta)^2 \le 1$, mientras que la segunda se reduce a $\delta(\sigma-1) \le \sigma - 1/2$, que se cumple trivialmente si $\sigma \le 1$ y, para $\sigma > 1$ tenemos que

$$\delta(\sigma-1) \le \delta^2 \le 1/2 < \sigma - 1/2.$$

Por otra parte, teniendo en cuenta que $c < 1/2$,

$$T^{\frac{4c(1+\delta-\sigma)}{2\delta+1}} \le T^{4c(1+\delta-\sigma)} \le T^{4c(1-\sigma)+2\delta} \le e^{2A} T^{4c(1-\sigma)}.$$

Ahora la conclusión es inmediata. ∎

Para probar el teorema 6.17 nos falta una última observación general sobre las funciones holomorfas. Observemos en primer lugar que la función $\frac{|x|}{x^2+y^2}$ es integrable en $B_r(0)$. En efecto, si

$$A(0,\delta,r) = \{x \in \mathbb{R}^2 \mid \delta < \|x\| < r\},$$

pasando a coordenadas polares tenemos que

$$\int_{A(0,\delta,r)} \frac{|x|}{x^2+y^2} dxdy = \int_\delta^r \int_0^{2\pi} \frac{\rho|\cos\theta|}{\rho^2} \rho\, d\theta d\rho$$

$$= (r-\delta)\int_0^{2\pi} |\cos\theta|\, d\theta = 4(r-\delta),$$

luego, por el teorema de la convergencia monótona, la función es integrable en $B_r(0)$ y

$$\int_{B_r(0)} \frac{|x|}{x^2+y^2}\, dxdy = \lim_n \int_{A(0,1/n,r)} \frac{|x|}{x^2+y^2}\, dxdy = 4r.$$

Como consecuencia, también es integrable $x/(x^2+y^2)$, y es fácil ver que la integral es nula. A su vez, si definimos la integral de una función compleja como

$$\int_\Omega f(x,y)\, dxdy = \int_\Omega \operatorname{Re} f(x,y)\, dxdy + i\int_\Omega \operatorname{Im} f(x,y)\, dxdy,$$

tenemos que

$$\frac{1}{z} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2},$$

luego $1/z$ es integrable en $B_r(0)$ y su integral es nula. Esto implica a su vez que $1/(z-z_0)$ es integrable en $B_r(z_0)$, con integral nula, lo que a su vez implica que toda función holomorfa es integrable en un entorno de un punto en el que tenga un polo simple.

DEMOSTRACIÓN (de 6.17): Consideramos las funciones $f_X(s)$ y $M_X(s)$ definidas en el teorema anterior, para $X > 1$. Definimos además

$$h_X(s) = 1 - f_X^2(s) = (1 + f_X(s))(1 - f_X(s)) = \zeta(s)M_X(s)(2 - M_X(s)\zeta(s)).$$

Llamamos $g_X(s) = M_X(s)(2 - M_X(s)\zeta(s))$, de modo que $h_X(s) = \zeta(s)g_X(s)$. Las funciones h_X y g_X son holomorfas en $\mathbb{C}$ salvo a lo sumo en $s = 1$. En la prueba del teorema anterior hemos visto que

$$|f_X(s)| \le \sum_{n\ge X} \frac{d(n)}{n^\sigma} \le \sum_{n\ge X} \frac{d(n)}{n^2}$$

para $\sigma \ge 2$ y, por (2.5) sabemos que $d(n) = o(n^{1/4})$, luego existe un $X_0 > 1$ tal que si $X \ge X_0$, entonces, $d(n) \le n^{1/4}$ y, usando el teorema 4.1,

$$|f_X(s)| \le \sum_{n\ge X} \frac{n^{1/4}}{n^2} = \sum_{n\ge X} \frac{1}{n^{7/4}} = \zeta(7/4) - \sum_{n<X} \frac{1}{n^{7/4}} \le$$

$$\zeta(7/4) - \sum_{n\le X} \frac{1}{n^{7/4}} + \frac{1}{X^{7/4}} \le \frac{1}{X^{7/4}} + \frac{4}{3X^{3/4}} + \frac{1}{X^{7/4}} = O(X^{-3/4}),$$

luego $X|f_X(s)|^2 = O(X^{-1/2})$ y, si X_0 se elige suficientemente grande, tenemos que, para $X \ge X_0$,

$$|f_X(s)|^2 \le \frac{1}{2X} < \frac{1}{2}. \tag{6.20}$$

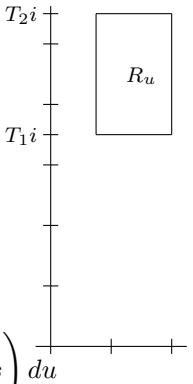
Por lo tanto, $h_X(s) \ne 0$ si $\sigma \ge 2$. De hecho, $\operatorname{Re} h_X(s) > 1/2$.

Llamemos $N_h(\sigma, T)$ al número de ceros (contando multiplicidades) de h_X con $\operatorname{Re}\rho \ge \sigma$, $0 < \operatorname{Im}\rho \le T$. Si $T_1 < T_2$, llamamos

$$N_h(\sigma, T_1, T_2) = N_h(\sigma, T_2) - N_h(\sigma, T_1).$$

Dados $X > X_0$ y $T > 4$, elegimos T_1 y T_2 tales que $3 < T_1 < 4$ y $T < T_2 < T+1$ y de modo que h no se anule en los segmentos $1/2 \le \sigma \le 2$, $\tau = T_1, T_2$.

Para $1/2 \le u \le 2$, llamamos R_u al rectángulo de vértices $u+iT_1$, $2+iT_1$, $2+iT_2$, $u+iT_2$. A lo sumo, h_X puede anularse en su lado izquierdo. Si no es así, tenemos que



$$\int_{R_u} \frac{h_X'(s)}{h_X(s)}\,ds = 2\pi i N_h(u, T_1, T_2).$$

Sea $1/2 \le \sigma_0 \le 1$ tal que h no se anula en R_{σ_0}. Entonces

$$2\pi i \int_{\sigma_0}^2 N_h(u, T_1, T_2)\,du = \int_{\sigma_0}^2 \int_{R_u} \frac{h_X'(s)}{h_X(s)}\,ds\,du =$$

$$\int_{\sigma_0}^2 \left(\int_{u+iT_1}^{2+iT_1} \frac{h_X'(s)}{h_X(s)}\,ds + \int_{2+iT_1}^{2+iT_2} \frac{h_X'(s)}{h_X(s)}\,ds + \int_{2+iT_2}^{u+iT_2} \frac{h_X'(s)}{h_X(s)}\,ds \right) du$$

$$+ \int_{\sigma_0}^2 \int_{u+iT_2}^{u+iT_1} \frac{h_X'(s)}{h_X(s)}\,ds\,du.$$

Notemos que la integral sobre R_u no está definida para un número finito de valores de u, pero esto es irrelevante. Lo mismo sucede con la integral interior del último término. Desarrollándola tenemos que

$$\int_{\sigma_0}^{2}\int_{u+iT_2}^{u+iT_1}\frac{h'_X(s)}{h_X(s)}\,dsdu = -i\int_{\sigma_0}^{2}\int_{T_1}^{T_2}\frac{h'_X(u+it)}{h_X(u+it)}dtdu.$$

Ahora bien, el integrando es una función holomorfa en el rectángulo salvo a lo sumo en un número finito de puntos donde tiene polos simples, luego por la observación previa al teorema sabemos que es integrable en el rectángulo, y podemos aplicar el teorema de Fubini:

$$\int_{\sigma_0}^{2}\int_{u+iT_2}^{u+iT_1}\frac{h'_X(s)}{h_X(s)}\,dsdu = -i\int_{[2,\sigma_0]\times[T_1,T_2]}\frac{h'_X(u+it)}{h_X(u+it)}dudt$$

$$= -i\int_{T_1}^{T_2}\int_{\sigma_0}^{2}\frac{h'_X(u+it)}{h_X(u+it)}dudt,$$

donde la integral interior no está definida para un número finito de valores de t. Tomando partes imaginarias llegamos a que

$$2\pi\int_{\sigma_0}^{2}N_h(u,T_1,T_2)\,du = -\int_{T_1}^{T_2}\operatorname{Re}\int_{\sigma_0}^{2}\frac{h'_X(u+it)}{h_X(u+it)}dudt +$$

$$\int_{\sigma_0}^{2}\left(\int_{u+iT_1}^{2+iT_1}\operatorname{Im}\frac{h'_X(s)}{h_X(s)}\,ds + \int_{2+iT_1}^{2+iT_2}\operatorname{Im}\frac{h'_X(s)}{h_X(s)}\,ds + \int_{2+iT_2}^{u+iT_2}\operatorname{Im}\frac{h'_X(s)}{h_X(s)}\,ds\right)du.$$

Por otra parte,

$$-\int_{T_1}^{T_2}\operatorname{Re}\int_{\sigma_0}^{2}\frac{h'_X(u+it)}{h_X(u+it)}dudt = \int_{T_1}^{T_2}(\log|h_X(\sigma_0+it)| - \log|h_X(2+it)|)\,dt.$$

Ahora observamos que

$$\log|h_X(s)| \le \log(1+|f_X(s)|^2) \le |f_X(s)|^2,$$

lo que nos permite aplicar el teorema anterior para acotar la integral del primer logaritmo. Para el segundo logaritmo no podemos usar el teorema, pero, teniendo en cuenta (6.20), vemos que

$$-\log|h_X(2+it)| \le -\log(1-|f_X(2+it)|^2) \le 2|f_X(2+it)|^2 < 1/X.$$

Por consiguiente, teniendo en cuenta que $T_2 < T+1$ y que $T_2-T_1 \le T+1-3 < T$,

$$-\int_{T_1}^{T_2}\operatorname{Re}\int_{\sigma_0}^{2}\frac{h'_X(u+it)}{h_X(u+it)}dudt <$$

$$A\frac{(T+1)^{4c(1-\sigma_0)}}{X^{2\sigma_0-1}}(T+X+1)\log^4(T+X+1) + \frac{T}{X}. \tag{6.21}$$

Ahora estimaremos las otras tres integrales. La más sencilla es

$$\int_{\sigma_0}^{2}\int_{2+iT_1}^{2+iT_2} \operatorname{Im}\frac{h_X'(s)}{h_X(s)}\,dsdu \le 2(\operatorname{Im}\log h_X(2+iT_2) - \operatorname{Im}\log h_X(2+iT_1)),$$

donde hemos usado que $h_X(s)$ no se anula cuando $\sigma = 2$, pues, de hecho, $\operatorname{Re} h_X(s) > 1/2$, y esto implica además que la variación del argumento tiene que ser menor que π. Así pues,

$$\int_{\sigma_0}^{2}\int_{2+iT_1}^{2+iT_2} \operatorname{Im}\frac{h_X'(s)}{h_X(s)}\,dsdu < 2\pi.$$

Sean ahora γ_1 y γ_2 los segmentos determinados por $\tau = T_1$ y $\tau = T_2$, respectivamente, y $\sigma_0 \le \sigma \le 2$. Los puntos de γ_j en los que se anula $\operatorname{Re} h_X$ son los ceros de la función holomorfa

$$H_j(s) = \frac{1}{2}(h_X(s+iT_j) + h_X(s-iT_j))$$

sobre el segmento $\sigma_0 \le \sigma \le 2$, $\tau = 0$, luego son un número finito, digamos m_j, y están contenidos en el conjunto de ceros de H_j en el disco $D(2, 3/2)$. Notemos que H_j es holomorfa salvo a lo sumo en los puntos $1 \pm iT_j$, luego en particular lo es en $D(2, 7/4)$ (ya que $3 < T_1 < T_2$). El teorema [VC 2.29] nos da que

$$\frac{1}{2} < \operatorname{Re} h_X(2) = |H_j(2)| \le \left(\frac{6}{7}\right)^{m_j} \text{máx}\{|H_j(s)| \mid |s-2| = 7/4\}.$$

Ahora bien,

$$|H_j(s)| = |\frac{1}{2}(h_X(s+iT_j) + \overline{h_X(\bar{s}+iT_j)})| \le \frac{1}{2}(|h_X(s+iT_j)| + |h_X(\bar{s}+iT_j)|)$$

y si $|s-2| = 7/4$, entonces $\operatorname{Re}(s \pm iT_j) = \operatorname{Re} s \ge 1/4$ y

$$-2 \le \operatorname{Im} s,\ \operatorname{Im}\bar{s} \le 2,$$

luego

$$1 \le \operatorname{Im}(s+iT_j),\ \operatorname{Im}(\bar{s}+iT_j) \le T+3,$$

y por lo tanto

$$\left(\frac{7}{6}\right)^{m_j} \le \text{máx}\{|h_X(s)| \mid \sigma \ge 1/4,\ 1 \le \tau \le T+3\}.$$

Ahora bien,

$$|h_X(s)| \le 1 + |f_X(s)|^2 \le 2 + |\zeta(s)M_X(s)|^2.$$

Por 4.7 tenemos que $|\zeta(s)| = O(\tau^{3/4}) = O(T^{3/4}) = O((T+X)^{3/4})$, y

$$|M_X(s)| \le \sum_{n<X} \frac{1}{n^{1/4}} \le 1 + \int_1^X \frac{dx}{x^{1/4}} = O(X^{3/4}) = O((T+X)^{3/4}),$$

luego $h_X(s) = O((T+X)^{3/2})$ y a su vez

$$m_j \log(7/6) \le 2\log(A(T+X)^{3/2}) \le A(1+\log(T+X)),$$

luego $m_j \le A\log(T+X)$.

Ahora el mismo argumento empleado en la prueba del teorema 4.19 prueba que

$$\left|\operatorname{Im}\int_{\gamma_j}\frac{h_X'(s)}{h_X(s)}\,ds\right| = |\arg|h_X(\sigma_0+iT_j)| - \arg|h_X(2+iT_j)||$$
$$\le (m_j+1)\pi \le A\log(T+X),$$

(pues entre cada par de puntos de γ_j^* donde $\operatorname{Re} h_X$ no se anula, el argumento no puede variar más de π unidades). Por lo tanto.

$$\left|\int_{\sigma_0}^{2}\int_{u+iT_j}^{2+iT_j}\operatorname{Im}\frac{h_X'(s)}{h_X(s)}\,dsdu\right| \le 2A\log(T+X).$$

Concluimos que

$$\int_{\sigma_0}^{2} N_h(u,T_1,T_2)\,du \le AT^{4c(1-\sigma_0)}(TX^{1-2\sigma_0}+X^{2(1-\sigma_0)})\log^4(T+X),$$

donde hemos retocado (6.21) cambiando $T+1$ por T y eliminando el término $T/X \le TX^{1-2\sigma_0}$ y hemos despreciado las cotas de las otras tres integrales, ya que son menores que (6.21), trivialmente en el caso de 2π y, en el caso de las otras dos porque

$$\log(T+X) \le X^{2(1-\sigma_0)}\log^4(T+X).$$

Por otra parte, todos los ceros de la función dseta son ceros de h, luego, llamando $N(\sigma,T_1,T_2) = N(\sigma,T_2) - N(\sigma,T_1)$, para $0<\delta<1$, tenemos que

$$\int_{\sigma_0}^{2} N_h(u,T_1,T_2)\,du \ge \int_{\sigma_0}^{\sigma_0+\delta} N(u,T_1,T_2)\,du \ge \delta N(\sigma_0+\delta,T_1,T_2).$$

Como la función dseta no tiene ceros con parte imaginaria $\le T_1 < 4$, resulta que $N(\sigma,T) \le N(\sigma,T_1,T_2)$, luego, si $1/2+\delta \le \sigma \le 1$, tomando $\sigma_0 = \sigma-\delta$, tenemos que

$$N(\sigma,T) \le \frac{A}{\delta}T^{4c(1-\sigma+\delta)}(TX^{1-2\sigma+2\delta}+X^{2(1-\sigma+\delta)})\log^4(T+X). \tag{6.22}$$

Por otra parte, si $1/2 \le \sigma \le 1/2+\delta$, la fórmula de Riemann-von Mangoldt nos da que

$$N(\sigma,T) \le N(T) \le AT\log T \le AT^{2(1-\sigma+\delta)}\log T. \tag{6.23}$$

Finalmente tomamos $X = T > \max\{X_0,4\}$ y $\delta = 1/\log T$, con lo que (6.22) se reduce a

$$N(\sigma,T) \le AT^{2(1+2c)(1-\sigma+\delta)}\log^5 T,$$

en el caso de la primera, y (6.23) implica la misma desigualdad. Finalmente basta observar que $T^{2(1+2c)\delta} = e^{2(1+2c)} \le e^4$. ∎

Capítulo VII

El método de Vinogradov

En este capítulo presentamos otra forma de estudiar con precisión el crecimiento de la función dseta a la izquierda de la recta $\sigma = 1$, lo que a su vez nos proporcionará una región sin ceros mejor que las que ya hemos obtenido y a su vez una mejor estimación del error en el teorema de los números primos. En realidad el resultado principal se enmarca en un contexto más general y tiene aplicaciones a otros problemas de la teoría analítica de números.

7.1 La conjetura de Vinogradov

Definición 7.1 Dados números naturales, $k, l, q \geq 1$, llamaremos $J_l^k(q)$ al número de soluciones enteras del sistema de ecuaciones

$$\begin{aligned} x_1 + \cdots + x_l &= y_1 + \cdots + y_l \\ x_1^2 + \cdots + x_l^2 &= y_1^2 + \cdots + y_l^2 \\ \cdots\cdots\cdots\cdots & \quad \cdots\cdots\cdots\cdots \\ x_1^k + \cdots + x_l^k &= y_1^k + \cdots + y_l^k \end{aligned}$$

tales que $1 \leq x_j, y_j \leq q$.

Un hecho fundamental es que se cumple algo más general que lo que exige la definición:

Teorema 7.2 *Dados números naturales $k, l, q \geq 1$ y enteros a, b, con $b \neq 0$, se cumple que $J_l^k(q)$ es el número de soluciones enteras del sistema de ecuaciones*

$$\sum_{j=1}^{l} (a + bx_j)^h = \sum_{j=1}^{l} (a + by_j)^h, \qquad h = 1, \ldots, k,$$

tales que $1 \leq x_j, y_j \leq q$.

DEMOSTRACIÓN: Sucede, más concretamente, que las soluciones del sistema del enunciado son las mismas que las del sistema de la definición 7.1. En efecto, la ecuación h-ésima del enunciado es

$$\sum_{j=1}^{l}\sum_{r=0}^{h}\binom{h}{r}a^r b^{h-r}x_j^{h-r} = \sum_{j=1}^{l}\sum_{r=0}^{h}\binom{h}{r}a^r b^{h-r}y_j^{h-r},$$

que equivale a

$$\sum_{r=0}^{h}\binom{h}{r}a^r b^{h-r}\sum_{j=1}^{l}x_j^{h-r} = \sum_{r=0}^{h}\binom{h}{r}a^r b^{h-r}\sum_{j=1}^{l}y_j^{h-r}.$$

Por lo tanto, cada solución del sistema de ecuaciones de la definición 7.1 es también solución del sistema del enunciado. Recíprocamente, si x_j, y_j es una solución del sistema del enunciado y suponemos inductivamente que cumple las ecuaciones de la definición 7.1 hasta el exponente $h-1$, entonces cada sumando de cada miembro de la ecuación anterior es igual al correspondiente del miembro opuesto para $r = 1, \ldots, h$, luego lo mismo vale para $r = 0$, lo que implica que x_j, y_j también cumplen la ecuación de exponente h. ∎

En particular, tanto en la definición 7.1 como en el teorema anterior es indistinto exigir que $1 \le x_i, y_i \le q$ que exigir $c < x_j, y_j \le c+q$, para cualquier entero prefijado c, pues si x_j, y_j forman una solución con esta condición y llamamos $x'_j = x_j - c, y'_j = y_j - c$, entonces $1 \le x'_j, y'_j \le q$ y

$$a + bx'_j = -ac + bx_j, \qquad a + by'_j = -ac + by_j,$$

por lo que x'_j, y'_j son una solución del sistema de 7.2 cambiando a por $-ac$, luego el número de soluciones es igualmente $J_l^k(q)$.

El segundo hecho fundamental se deriva de la observación elemental de que, si c es entero, entonces

$$\int_0^1 e^{2\pi i c x}\,dx = \begin{cases} 1 & \text{si } c = 0,\\ 0 & \text{si } c \neq 0.\end{cases}$$

La relación con lo anterior se obtiene considerando la función

$$f^k(x; a_0, \ldots, a_k) = a_k x^k + \cdots + a_1 x + a_0,$$

y a su vez

$$S^k(q, a; a_0, \ldots, a_k) = \sum_{a < n \le a+q} e^{2\pi i f(n)}. \tag{7.1}$$

El teorema siguiente puede interpretarse como que $J_l^k(q)$ es el valor medio de $|S^k(q,a)|^{2l}$ cuando las variables $a_1, \ldots, a_l$ varían sobre el cubo unitario. Por ello la expresión $J_l^k(q)$ se conoce como "valor medio de Vinogradov":

Teorema 7.3 *Dados números naturales $k, l, q \geq 1$ y un entero a, se cumple que*

$$J_l^k(q) = \int_{[0,1]^k} |S^k(q,a)|^{2l} da_1 \cdots da_k.$$

DEMOSTRACIÓN: Tenemos que

$$S^k(q,a)^l = \sum_{a<n_1,\ldots,n_l\leq a+q} e^{2\pi i \sum_{h=0}^{k} a_h(n_1^h+\cdots+n_l^h)}$$

y, multiplicando por el conjugado,

$$|S^k(q,a)|^{2l} = \sum_{\substack{a<m_1,\ldots,m_l\leq a+q\\ a<n_1,\ldots,n_l\leq a+q}} e^{2\pi i \sum_{h=0}^{k} a_h(m_1^h+\cdots+m_l^h-n_1^h+\cdots-n_l^h)}.$$

Por lo tanto,

$$\int_{[0,1]^k} |S^k(q,a)|^{2l} da_1 \cdots da_k = \sum_{\substack{a<m_1,\ldots,m_l\leq a+q\\ a<n_1,\ldots,n_l\leq a+q}} \prod_{h=0}^{k} \int_0^1 e^{2\pi i(m_1^h+\cdots+m_l^h-n_1^h+\cdots-n_l^h)a_h} da_h$$

y, por la observación previa al teorema, cada sumando vale 0 o 1, y los sumandos que valen 1 se corresponden con las soluciones del sistema de ecuaciones de la definición 7.1. (Notemos que los factores correspondientes a $h = 0$ valen[1] siempre 1). ∎

Una estimación elemental de $J_l^k(q)$ es

$$q^l \leq J_l^k(q) \leq q^{2l}. \tag{7.2}$$

En efecto, por una parte obtenemos q^l soluciones del sistema de 7.1 sin más que dar valores arbitrarios a las variables x_j y tomar $y_j = x_j$. Por otra parte, es claro que $|S^k(q,a)| \leq q$, lo que nos da la cota superior.

Soluciones triviales En realidad hay más de q^l soluciones triviales, pues cada asignación arbitraria de las variables x_j no da lugar a unos únicos valores para las variables y_j, sino a tantos como permutaciones admitan dichos valores, que serán a lo sumo $l!$, en el caso en que los valores asignados a las x_j sean distintos dos a dos. En cualquier caso, el número de soluciones triviales es a lo sumo $l!\, q^l$.

Si sólo hubiera soluciones triviales, sería fácil calcular exactamente $J_l^k(q)$. Por ejemplo, es fácil probar que en el caso $k = l = 2$ sólo hay soluciones triviales,[2] por lo que

$$J_2^2(q) = 2q(q-1) + q = 2q^2 - q.$$

A su vez, esto implica que, para $k \geq 2$, se cumple $J_2^k(q) = J_2^2(q)$.

[1] Alternativamente, la expresión $|S^k(q,a)|$ no depende de a_0, ya que en la definición de $S^k(q,a)$ podemos sacar factor común $e^{2\pi i a_0}$, que tiene módulo 1, luego podemos suponer que $a_0 = 0$ y que el menor valor para h es $h = 1$.

[2] La ecuación cuadrática equivale a $(x_1 + y_1)(x_1 - y_1) = (x_2 + y_2)(y_2 - x_2)$, de donde, usando la ecuación lineal, se sigue que si $x_1 \neq y_1$, entonces $x_1 = y_2$.

En cambio, para $k = 2$, $l = 3$ ya hay soluciones no triviales. La menor es

$$1 + 4 + 4 = 9 = 2 + 2 + 5, \qquad 1^2 + 4^2 + 4^2 = 33 = 2^2 + 2^2 + 5^2.$$

El número de soluciones triviales en este caso es

$$q(q-1)(q-2)6 + 3q(q-1)3 + q = 6q^3 - 9q^2 + 4q,$$

sin embargo, ahora no son todas. ∎

Nuestro objetivo a medio plazo es encontrar estimaciones más finas que (7.2).

Si $c = (c_1, \dots, c_k)$ son números enteros, definimos, más en general, $J_l^k(q; c)$ como el número de soluciones enteras del sistema de ecuaciones

$$\sum_{j=1}^{l} (x_j^h - y_j^h) = c_h, \qquad h = 1, \dots, k, \tag{7.3}$$

con $0 \le x_j, y_j < q$, de modo que $J_l^k(q) = J_l^k(q; 0)$.

Una ligera variante de la prueba del teorema anterior muestra que

$$J_l^k(q; c) = \int_{[0,1]^k} |S^k(q, a)|^{2l} e^{2\pi i (a \cdot c)}\, da_1 \cdots da_k.$$

En efecto, basta observar que

$$|S^k(q, a)|^{2l} e^{2\pi i (a \cdot c)} = \sum_{\substack{0 \le m_1, \dots, m_l < q \\ 0 \le n_1, \dots, n_l < q}} e^{2\pi i \sum_{h=1}^{k} a_h (m_1^h + \cdots + m_l^h - n_1^h + \cdots - n_l^h + c_h)},$$

y se concluye igualmente. Por consiguiente.

$$J_l^k(q; c) = |J_l^k(q; c)| \le \int_{[0,1]^k} |S^k(q, a)|^{2l}\, da_1 \cdots da_k \le J_l^k(q).$$

Ahora observamos que una solución de (7.3) cumple que

$$|c_h| \le \sum_{j=1}^{l} |x_j^h - y_j^h| \le \sum_{j=1}^{l} \max\{x_j^h, y_j^h\} < l q^h$$

y, recíprocamente, el sistema no tiene solución cuando $|c_h| \ge l q^h$, para algún h. Por consiguiente,

$$\sum_c J_l^k(q; c) \le (2l)^k \prod_{h=1}^{k} q^h J_l^k(q) = (2l)^k q^{k(k+1)/2} J_l^k(q).$$

Ahora bien, el miembro izquierdo de esta desigualdad es el número de soluciones del sistema (7.3) cuando las c_h son consideradas también variables, luego

es q^{2l}, ya que existe una única solución para cada valor que demos arbitrariamente a las variables x_j, y_j (dentro del rango permitido). Así pues,

$$J_l^k(q) \geq (2l)^{-k} q^{2l-k(k+1)/2}$$

lo que, combinado con (7.2), nos da que

$$J_l^k(q) \geq \max\{(2l)^{-k} q^{2l-k(k+1)/2}, q^l\}.$$

Podemos precisar cuál de las dos cotas inferiores es mejor. Basta observar que

$$\frac{(2l)^{-k} q^{2l-k(k+1)/2}}{q^l} = (2l)^{-k} q^{l-k(k+1)/2},$$

luego si $l \leq k(k+1)/2$ el denominador es mayor, mientras que si $l > k(k+1)/2$ es mayor el numerador siempre que $q \geq l^k$. Por lo tanto, para $q \geq l^k$, podemos desglosar la cota inferior así:[3]

$$J_l^k(q) \geq \begin{cases} q^l & \text{si } l \leq k(k+1)/2, \\ (2l)^{-k} q^{2l-k(k+1)/2} & \text{si } l > k(k+1)/2. \end{cases}$$

Vinogradov conjeturó en 1935 que esta estimación por defecto del crecimiento del valor medio $J_l^k(q)$ está muy cerca de ser una estimación por exceso. Concretamente, conjeturó que, para todo $\epsilon > 0$, cuando q tiende a ∞ se cumple que

$$J_l^k(q) = \begin{cases} O(q^{l+\epsilon}) & \text{si } l \leq k(k+1)/2, \\ O(q^{2l-k(k+1)/2+\epsilon}) & \text{si } l \geq k(k+1)/2. \end{cases}$$

Vinogradov demostró una versión débil de su conjetura, y es costumbre referirse a ella y a cualquiera de las mejoras subsiguientes como *"teorema del valor medio de Vinogradov"*.

La conjetura ha sido demostrada recientemente (en 2015) por Bourgain, Demeter y Guth mediante técnicas del análisis harmónico. Aquí no vamos a entrar en la demostración de este hecho, sino que nos limitaremos a probar una versión débil que será suficiente para nuestros fines. No obstante, terminaremos esta sección con algunas observaciones elementales sobre la conjetura.

El caso crítico Se llama *caso crítico* de la conjetura de Vinogradov al correspondiente a $l_k = k(k+1)/2$. Sucede que si la conjetura es cierta para un caso crítico (k, l_k), entonces es cierta para dicho k y cualquier valor de l.

En efecto, si $l > l_k$, entonces

$$\begin{aligned} J_l^k(q) &= \int_{[0,1]^k} |S^k(q,a)|^{2l-k(k-1)} |S^k(q,a)|^{k(k-1)} da_1 \cdots da_k \\ &\leq q^{2(l-l_k)} \int_{[0,1]^k} S^k(q,a)|^{k(k-1)} da_1 \cdots da_k = q^{2(l-l_k)} J_{l_k}^k, \end{aligned}$$

[3] Incidentalmente, esto prueba la existencia de soluciones no triviales cuando $l > k(k+1)/2$, pues el número de soluciones triviales es $O(q^l)$.

y por la hipótesis $J^k_{l_k} = O(q^{l_k+\epsilon})$ sobre el caso crítico, llegamos a que

$$J^k_l(q) = O(q^{2(l-l_k)+l_k+\epsilon}) = O(q^{2l-k(k+1)/2+\epsilon}).$$

En el caso $l < l_k$ aplicamos la desigualdad de Hölder a $\frac{1}{p} + \frac{1}{l_k/l} = 1$:

$$\begin{aligned} J^k_l(q) &= \int_{[0,1]^k} 1 \cdot |S^k(q,a)|^{2l} da_1 \cdots da_k \\ &\le \left(\int_{[0,1]^k} 1^p \, da_1 \cdots da_k\right)^{1/p} \left(\int_{[0,1]^k} |S^k(q,a)|^{2l_k} \, da_1 \cdots da_k\right)^{l/l_k} \\ &= (J^k_{l_k})^{1/l_k} = O(q^{l_k+\epsilon})^{l/l_k} = O(q^{l+\epsilon}) \end{aligned}$$

pues

$$\frac{O(q^{l_k+\epsilon})^{l/l_k}}{q^{l+\epsilon}} = \left(\frac{O(q^{l_k+\epsilon})}{q^{l_k+\epsilon l_k/l}}\right)^{l/l_k} = \left(\frac{O(q^{l_k+\epsilon})}{q^{l_k+\epsilon}} \frac{1}{q^{\epsilon(l_k/l-1)}}\right)^{l/l_k} = O(1).$$

■

Por ejemplo, $l_1 = 1$ y es obvio que $J^1_1(q) = q$, luego la conjetura de Vinogradov se cumple para $J^1_l(q)$ (incluso con $\epsilon = 0$).

El caso $k = 2$ También es fácil demostrar que la conjetura de Vinogradov se cumple para $k = 2$. Basta considerar el caso crítico $l = 3$. Podemos escribir las ecuaciones así:

$$x_1 + x_2 - y_3 = y_1 + y_2 - x_3,$$
$$x_1^2 + x_2^2 - y_3^2 = y_1^2 + y_2^2 - x_3^2.$$

Usando la identidad $(a+b-c)^2 - (a^2+b^2-c^2) = 2(a-c)(b-c)$, al restar la primera ecuación al cuadrado menos la segunda resulta

$$(x_1 - y_3)(x_2 - y_3) = (y_1 - x_3)(y_2 - x_3)$$

Vamos a contar las posibles elecciones de x_1, x_2, y_3 que hacen no nulos los dos miembros de la ecuación anterior.

Si elegimos $x_1 \neq x_2$, tenemos $q(q-1)$ posibilidades, que pueden completarse con $q-2$ posibilidades para y_3. En total, $q(q-1)(q-2)$. Si elegimos $x_1 = x_2$ tenemos q posibilidades, que pueden completarse con $q-1$ posibilidades para y_3. En total $q(q-1)$. Los dos casos suman $q(q-1)^2 = O(q^3)$.

Para cada elección en estas condiciones, $p = (x_1 - x_3)(x_2 - y_3)$ cumple $|p| < q^2$, y el número de descomposiciones en dos factores es (teniendo en cuenta los signos) $2d(p) \le cp^{\epsilon/2} \le cq^\epsilon$, donde hemos usado (2.5). La ecuación

$$x_1 + x_2 - y_3 = (y_1 - x_3) + (y_2 - x_3) + x_3$$

implica que, una vez fijados $y_1 - x_3$, $y_2 - x_3$, el valor de x_3 queda unívocamente determinado, y éste a su vez determina y_1, y_2. Por consiguiente, hay a lo sumo $O(q^3)O(q^\epsilon) = O(q^{3+\epsilon})$ soluciones en este caso.

En caso de que los dos miembros de la ecuación se anulen, tenemos cuatro subcasos, según qué factor se anule en cada factor. Si suponemos, por ejemplo, que $x_1 = y_3$, $y_2 = x_3$, entonces la primera ecuación nos da que $x_2 = y_1$, luego hay q^3 posibilidades. Lo mismo vale para los otros tres subcasos, luego concluimos que el número de soluciones en el segundo caso es $O(x^3)$, luego el número total de soluciones es $O(x^{3+\epsilon})$, como había que probar. ∎

El caso $k = 3$ ya no es trivial, y la primera prueba de la conjetura en este caso fue obtenida por Wooley poco antes que la prueba en el caso general.

7.2 El teorema del valor medio de Vinogradov

Vamos a probar uno de los llamados "teorema del valor medio de Vinogradov", es decir, una estimación del crecimiento del valor medio $J_k^l(q)$ bajo ciertas condiciones sobre k y l.

Empezamos con un hecho algebraico general:

Teorema 7.4 (Identidades de Newton) *Sea K un cuerpo, sean $e_0, \dots, e_n$ los polinomios simétricos elementales en $K[X_1, \dots, X_n]$ y $p_h = X_1^h + \cdots + X_n^h$. Entonces*

$$he_h = \sum_{i=1}^{h} (-1)^{i-1} e_{h-i} p_i.$$

Demostración: Para $2 \le i \le h$, llamemos $r_i^h(X_1, \dots, X_n)$ a la suma de todos los monomios de grado h (con coeficiente 1) en los que una variable tiene grado i y las demás tienen grado 1. Entonces, para $2 \le i < h$, es claro que

$$p_i e_{h-i} = r_i^h + r_{i+1}^h.$$

En efecto, e_{h-i} está formado por todos los monomios M de grado $h - i$ con variables de grado 1. Cuando uno de estos monomios se multiplica por una potencia X_j^i, obtenemos uno de los monomios de r_i^h si X_j no está en M, o bien uno de los monomios de r_{i+1}^h si X_j está en M. Además, así se obtienen todos los monomios de $r_i^h + r_{i+1}^h$ sin repeticiones.

Para $i = h$ tenemos trivialmente:

$$p_h e_0 = p_h = r_h^h,$$

mientras que para $i = 1$ se cumple que

$$p_1 e_{h-1} = he_h + r_2^h.$$

En efecto, al multiplicar un monomio M de grado $h-1$ con variables de grado 1 por una variable X_j, obtenemos un monomio de r_2^h si X_j está en M, o bien un monomio de e_h si no lo está. Sin embargo, los monomios de r_2^h aparecen una vez cada uno, pero los de e_h aparecen h veces cada uno, una por cada una de sus variables.

Ahora basta sumar:

$$\sum_{i=1}^{h}(-1)^{i-1}e_{h-i}p_i =$$

$$he_h + r_2^h - (r_2^h + r_3^h) + \cdots (-1)^{h-2}(r_{h-1}^h + r_h^h) + (-1)^{h-1}r_h^h = he_h. \quad \blacksquare$$

Como consecuencia:

Teorema 7.5 *Si un sistema de ecuaciones*

$$\begin{gathered} x_1 + \cdots + x_k = m_1 \\ \cdots\cdots\cdots\cdots \\ x_1^k + \cdots + x_k^k = m_k \end{gathered}$$

tiene solución en un cuerpo K y k es menor que la característica de K si ésta es no nula, entonces la solución es única salvo reordenación de las variables.

Demostración: Si $1 \le h < k$, como h no divide a la característica de K, podemos expresar

$$\begin{aligned} e_h(x_1,\ldots,x_k) &= \frac{1}{k}\sum_{i=1}^{h}(-1)^{i-1}e_{h-i}(x_1,\ldots,x_k)p_i(x_1,\ldots,x_k) \\ &= \frac{1}{k}\sum_{i=1}^{h}(-1)^{i-1}m_i e_{h-i}(x_1,\ldots,x_k), \end{aligned}$$

y esto es una relación recurrente que determina unívocamente todos los valores $e_h(x_1,\ldots,x_k) \in K$ a partir de $m_1,\ldots,m_k$. Por lo tanto, el polinomio

$$(X-x_1)\cdots(X-x_k) = \sum_{i=0}^{k}(-1)^{k-i}e_{k-i}(x_1,\ldots,x_k)X^i$$

está unívocamente determinado por $m_1,\ldots,m_k$, y $x_1,\ldots,x_k$ son las raíces de este polinomio, luego están unívocamente determinadas salvo el orden. $\blacksquare$

Si consideramos las soluciones del sistema anterior como k-tuplas ordenadas, entonces resulta que, o bien no hay ninguna, o bien hay a lo sumo $k!$ (habría exactamente $k!$ si sus coordenadas fueran distintas dos a dos, pero si hay repeticiones, las permutaciones posibles son menos).

En particular, si el sistema de la definición 7.1 para $l = k$ tiene una solución, entonces $x_j = y_j$ salvo reordenación. Por lo tanto, $x_1,\ldots,x_k$ pueden elegirse arbitrariamente (y hay q^k posibilidades) y, para cada una de ellas, hay a lo sumo $k!$ posibilidades para los y_j, luego en total hay a lo sumo $k!q^k$ soluciones. Así pues, $J_k^k(q) \le k!q^k$. Más en general, para $k \le l$,

$$\begin{aligned} J_l^k(q) &= \int_{[0,1]^k} |S^k(q,a)|^{2l}da_1\cdots da_k \\ &= \int_{[0,1]^k} |S^k(q,a)|^{2(l-k)}|S^k(q,a)|^{2k}da_1\cdots da_k \\ &\le q^{2(l-k)}\int_{[0,1]^k} |S^k(q,a)|^{2k}da_1\cdots da_k = q^{2(l-k)}J_k^k(q), \end{aligned}$$

luego

$$J_l^k(q) \le k! q^{2l-k}.$$

Esto ya es un refinamiento de (7.2) para el caso $k \ge l$, pero necesitamos mucho más. Para ello probamos primero un resultado sobre congruencias:

Teorema 7.6 *Si k, M son números naturales no nulos, $p > k$ es primo y $m_1, \dots, m_k$ son enteros, el número T de soluciones del sistema de congruencias*

$$\begin{gathered} x_1 + \cdots + x_k \equiv m_1 \pmod p \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^k + \cdots + x_k^k \equiv m_k \pmod{p^k} \end{gathered}$$

con $0 \le x_j \le Mp^k - 1$ y $x_j \not\equiv x_{j'} \pmod p$ para $j \ne j'$ cumple

$$T \le k! M^k p^{k(k-1)/2}.$$

Demostración: Dada una solución del sistema, es claro que podemos desarrollar

$$x_j = x_{j1} + p x_{j2} + \cdots + p^k x_{j,k+1},$$

donde $0 \le x_{js} \le p-1$, para $s = 1, \dots, k$ y $0 \le x_{j,k+1} \le M-1$. Por hipótesis $x_{j1} \ne x_{j'1}$, para $j \ne j'$, y además

$$\begin{gathered} x_{11} + \cdots + x_{k1} \equiv m_1 \pmod p \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_{11}^k + \cdots + x_{k1}^k \equiv m_k \pmod p \end{gathered}$$

Por el teorema anterior, el número de soluciones de este sistema de ecuaciones (sin descartar que sea nulo) es $T_1 \le k!$ Por otra parte, la solución dada debe cumplir también el sistema de congruencias

$$\begin{gathered} (x_{11} + p x_{12})^2 + \cdots + (x_{k1} + p x_{k2})^2 \equiv m_2 \pmod{p^2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ (x_{11} + p x_{12})^k + \cdots + (x_{k1} + p x_{k2})^k \equiv m_k \pmod{p^2} \end{gathered}$$

que es equivalente a otro sistema

$$\begin{gathered} x_{11}x_{12} + \cdots + x_{k1}x_{k2} \equiv m_2' \pmod p \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_{11}^{k-1}x_{12} + \cdots + x_{k1}^{k-1}x_{k2} \equiv m_k' \pmod p \end{gathered}$$

Como $x_{11}, \dots, x_{k1}$ son distintos dos a dos, a lo sumo uno de ellos es 0. Podemos suponer que $x_{11}, \dots, x_{k-1,1}$ son no nulos, y entonces

$$\begin{vmatrix} x_{11} & \cdots & x_{k-1,1} \\ \vdots & & \vdots \\ x_{11}^{k-1} & \cdots & x_{k-1,1}^{k-1} \end{vmatrix} = x_{11} \cdots x_{k-1,1} \prod_{i<j} (x_{j1} - x_{i1}) \ne 0,$$

luego cada valor para x_{k2} determina una única solución del sistema $x_{12},\dots,x_{k2}$, luego en total tiene $T_2 = p$ soluciones. A continuación consideramos el sistema

$$\begin{gathered}((x_{11}+px_{12})+p^2x_{13})^3+\cdots+((x_{k1}+px_{k2})+p^2x_{k3})^3 \equiv m_3 \pmod{p^3}\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ ((x_{11}+px_{12})+p^2x_{13})^k+\cdots+((x_{k1}+px_{k2})+p^2x_{k3})^k \equiv m_k \pmod{p^3}\end{gathered}$$

que equivale a un sistema

$$\begin{gathered}x_{11}x_{13}+\cdots+x_{k1}x_{k3} \equiv m'_3 \pmod{p}\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ x_{11}^{k-1}x_{13}+\cdots+x_{k1}^{k-1}x_{k3} \equiv m'_k \pmod{p}\end{gathered}$$

en el que ahora podemos fijar libremente $x_{k-1,3}$ y $x_{k,3}$, luego tiene $T_3 = p^2$ soluciones. Así podemos proseguir, con la única salvedad de que en el último paso es $T_{k+1} = M^k$ (los $x_{j,k+1}$ pueden fijarse libremente, sin que tengan que cumplir ningún sistema de congruencias).

Así pues, el número total de soluciones $x_1,\dots,x_k$ del sistema inicial es a lo sumo $T_1\cdots T_{k+1} = k!\,p\,p^2\cdots p^{k-1}M^k$, que es la cota del enunciado. ∎

El teorema del valor medio que vamos a probar se apoya en el siguiente resultado técnico:

Teorema 7.7 *Sean k,l,q números naturales tales que*

$$k \ge 2, \quad l \ge k^2+k, \quad q \ge 2^{-k}(2k)^{2k} = (2k^2)^k.$$

Entonces

$$J_l^k(q) < 3l^{2k}q_1^{2k}p_1^{2l-k(k+1)/2}J_{l-k}^k(q_1),$$

donde p_1 es cualquier primo que cumpla $\frac{1}{2}q^{1/k} \le p_1 \le q^{1/k}$ y $q_1 = E[qp_1^{-1}]+1$.

Demostración: Notemos que el postulado de Bertrand asegura la existencia de un primo p_1 en las condiciones indicadas.

Por definición de q_1 tenemos que $q < p_1q_1$, luego $J_l^k(q) < J_l^k(p_1q_1)$. Notemos que la desigualdad es estricta, pues $J_l^k(p_1q_1)$ es el número de soluciones enteras del sistema de la definición 7.1 con

$$0 \le x_j, y_j \le p_1q_1 - 1,$$

(por el teorema 7.2 con $a = -1$ y $b = 1$), y obviamente existen soluciones con $x_1 = q$ que no aparecen en el cálculo de $J_l^k(q)$, si en este consideramos soluciones con $0 \le x_j, y_j \le q-1$.

Alternativamente, $J_l^k(p_1q_1)$ es el número de soluciones enteras del sistema

$$(m_1+p_1x_1)^h+\cdots+(m_l+p_1x_l)^h = (n_1+p_1y_1)^h+\cdots+(n_l+p_1y_l)^h, \quad (7.4)$$

para $h = 1,\dots,k$, con $0 \le m_j, n_j \le p_1-1$ y $0 \le x_j, y_j \le q_1-1$.

Diremos que una solución del sistema (7.4) es *de primera clase* si los conjuntos $\{m_1,\dots,m_l\}$ y $\{n_1,\dots,n_l\}$ tienen al menos k elementos cada uno, y en caso contrario diremos que es *de segunda clase*. Así, podemos descomponer

$$J_l^k(p_1q_1) = J_1 + J_2,$$

donde los sumandos representan el número de soluciones de (7.4) de primera y segunda clase, respectivamente. Sea

$$U(m) = \sum_{x=0}^{q_1-1} e^{2\pi i g(m+p_1x)},$$

donde $g(x;a_1,\dots,a_k) = a_kx^k + \cdots + a_1x$. Notemos que $|U(m)| \le q_1$. Además

$$J_2 = \int_{[0,1]^k} \sum_{m_j,n_j} U(m_1)\cdots U(m_l)\overline{U(n_1)}\cdots\overline{U(n_l)}\,da_1\cdots da_k,$$

donde m_j, n_j varían entre los pares de l-tuplas de números naturales menores que p_1 tales que al menos una de las dos tenga menos de k elementos distintos.

Hay $\binom{p_1}{k-1}$ conjuntos de $k-1$ números naturales menores que p_1, y con los elementos de cada uno de ellos se pueden formar $(k-1)^l$ l-tuplas, luego el número total de tales l-tuplas es

$$\binom{p_1}{k-1}(k-1)^l < \frac{1}{2}k^lp_1^{k-1}.$$

Por otra parte, el número de l-tuplas de números menores que p_1 es p_1^l, luego pares de l-tuplas con el primer par restringido a l-tuplas con a lo sumo k elementos distintos es a lo sumo $k^lp_1^{l+k-1}/2$, y el número de sumandos del integrando anterior es a lo sumo $k^lp_1^{l+k-1}$. Aplicamos la desigualdad de Hölder:

$$\left|\sum_{m_j,n_j} U(m_1)\cdots U(m_l)\overline{U(n_1)}\cdots\overline{U(n_l)}\right| \le$$

$$\Big(\sum_{m_j,n_j}|U(m_1)|^{2l}\Big)^{1/2l}\cdots\Big(\sum_{m_j,n_j}|U(n_l)|^{2l}\Big)^{1/2l}.$$

Ahora acotamos $|U(m_j)|^{2l}, |U(n_j)|^{2l} \le \sum_{m=0}^{p_1-1}|U(m)|^{2l}$, con lo que

$$\left|\sum_{m_j,n_j} U(m_1)\cdots U(m_l)\overline{U(n_1)}\cdots\overline{U(n_l)}\right| \le$$

$$k^lp_1^{l+k-1}\sum_{m=0}^{p_1-1}|U(m)|^{2l} \le k^lq_1^{2k}p_1^{l+k-1}\sum_{m=0}^{p_1-1}|U(m)|^{2l-2k},$$

donde hemos usado que $|U(m)| \le q_1$.

Por consiguiente

$$J_2 \le k^l q_1^{2k} p_1^{l+k-1} \int_{[0,1]^k} \sum_{m=0}^{p_1-1} |U(m)|^{2l-2k}\, da_1 \cdots da_k$$

$$= k^l q_1^{2k} p_1^{l+k-1} \sum_{m=0}^{p_1-1} \int_{[0,1]^k} |U(m)|^{2l-2k}\, da_1 \cdots da_k,$$

pero la integral es el número de soluciones enteras del sistema de ecuaciones

$$(m+p_1x_1)^h + \cdots + (m+p_1x_{l-k})^h = (m+p_1y_1)^h + \cdots + (m+p_1y_{l-k})^h,$$

para $h = 1, \ldots, k$, con $0 \le x_j, y_j < q_1$, que por 7.2 es igual a $J_{l-k}^k(q_1)$, luego

$$J_l^2 \le k^l q_1^{2k} p_1^{l+k} J_{l-k}^k(q_1).$$

Ahora observamos que, por las hipótesis del teorema, tenemos $l \ge k^2+k \ge 2k$ (porque $k \ge 2$), luego

$$k^{l-2k} p_1^k = (k^2)^{l/2-k} p_1^k \le p_1^{l/2-k} p_1^k = p_1^{l/2} \le p_1^{l-k(k+1)/2},$$

pues, también por las hipótesis del teorema, $p_1 \ge \frac{1}{2} q^{1/k} \ge k^2$. A su vez, multiplicando por $k^{2k} p_1^l$,

$$k^l p_1^{l+k} \le p_1^{2l-k(k+1)/2} k^{2k},$$

con lo que

$$J_2 \le k^{2k} q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1) \le l^{2k} q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1).$$

Pasamos ahora a estimar J_1. Para ello observamos que toda solución de primera clase de (7.4) puede reordenarse para que $m_1, \ldots, m_k$ y $n_1, \ldots, n_k$ sean distintos dos a dos, luego el número total de soluciones será a lo sumo el número de soluciones de este tipo multiplicado por $\binom{l}{k}^2$, pues una k-tupla de números distintos y una $l-k$-tupla de números arbitrarios pueden intercalarse de $\binom{l}{k}$ formas distintas para obtener (con repeticiones) todas las l-tuplas con al menos k números distintos. Así pues,

$$J_1 \le \binom{l}{k}^2 \int_{[0,1]^k} \sum_{m_j, n_j} U(m_1) \cdots U(m_l) \overline{U(n_1)} \cdots \overline{U(n_l)}\, da_1 \cdots da_k$$

$$= \binom{l}{k}^2 \int_{[0,1]^k} \sum_{m_j} U(m_1) \cdots U(m_l) \overline{\sum_{n_j} U(n_1) \cdots U(n_l)}\, da_1 \cdots da_k$$

$$= \binom{l}{k}^2 \int_{[0,1]^k} \Big| \sum_{m_j} U(m_1) \cdots U(m_l) \Big|^2\, da_1 \cdots da_k,$$

donde m_j y n_j recorren l-tuplas con las k primeras componentes distintas dos a dos.

A su vez,

$$J_1 \le \binom{l}{k}^2 \int_{[0,1]^k} \Big|\sum_{m_j} U(m_1)\cdots U(m_k)\Big|^2 \Big|\sum_{m_j} U(m_{k+1})\cdots U(m_l)\Big|^2 da_1\cdots da_k,$$

donde en el primer sumatorio m_j recorre las k-tuplas con todas sus componentes distintas dos a dos y en el segundo las $l-k$-tuplas arbitrarias. Por la desigualdad de Hölder:

$$\Big|\sum_{m_j} U(m_{k+1})\cdots U(m_l)\Big|^2 = \Big|\sum_{m_j,n_j} U(m_{k+1})\cdots U(m_l)\overline{U(n_{k+1})}\cdots\overline{U(n_l)}\Big| \le$$

$$\Big(\sum_{m_j,n_j} |U(m_{k+1})|^{2l-2k}\Big)^{1/(2l-2k)} \cdots \Big(\sum_{m_j,n_j} |U(n_l)|^{2l-2k}\Big)^{1/(2l-2k)}$$

$$= \Big(p_1^{2l-2k-1}\sum_{m=0}^{p_1-1} |U(m)|^{2l-2k}\Big)^{1/(2l-2k)} \cdots \Big(p_1^{2l-2k-1}\sum_{m=0}^{p_1-1} |U(m)|^{2l-2k}\Big)^{1/(2l-2k)}$$

$$= p_1^{2l-2k-1}\sum_{m=0}^{p_1-1} |U(m)|^{2l-2k}.$$

Por lo tanto,

$$J_1 \le \binom{l}{k}^2 p_1^{2l-2k-1} \int_{[0,1]^k} \Big|\sum_{m_j} U(m_1)\cdots U(m_k)\Big|^2 \sum_{m=0}^{p_1-1} |U(m)|^{2l-2k} da_1\cdots da_k.$$

La integral es el número N_l de soluciones enteras del sistema de ecuaciones

$$(m_1+p_1x_1)^h+\cdots+(m_k+p_1x_k)^h-(n_1+p_1y_1)^h-\cdots-(n_k+p_1y_k)^h$$
$$=(m+p_1x_{k+1})^h+\cdots+(m+p_1x_l)^h-(m+p_1y_{k+1})^h-\cdots-(m+p_1y_l)^h$$

para $h=1,\dots,k$ y con $0\le m,m_j,n_j\le p_1-1$, $0\le x_j,y_j\le q_1-1$ y los m_j, al igual que los n_j, son distintos dos a dos.

Por el mismo argumento empleado en la prueba del teorema 7.2, dichas soluciones coinciden con las del sistema

$$(m_1-m+p_1x_1)^h+\cdots+(m_k-m+p_1x_k)^h-(n_1-m+p_1y_1)^h-\cdots-(n_k-m+p_1y_k)^h$$
$$=p_1^h(x_{k+1}^h+\cdots+x_l^h-y_{k+1}^h-\cdots-y_l^h).$$

Así pues, tenemos que

$$J_1 \le \binom{l}{k}^2 p_1^{2l-2k-1} N_l.$$

Llamemos $N_k(c_1p_1,\dots,c_kp_1^k)$ al número de soluciones enteras del sistema de ecuaciones

$$(m_1-m+p_1x_1)^h+\cdots+(m_k-m+p_1x_k)^h$$
$$-(n_1-m+p_1y_1)^h-\cdots-(n_k-m+p_1y_k)^h=c_hp_1^h,$$

para $h=1,\dots,k$, donde las variables cumplen las mismas condiciones precedentes.

Así tenemos que

$$N_l \le \sum_{|c_h|<lq_1^h} N_k(d_1p_1,\dots,d_kp_1^k)J_{l-k}^k(q_1;c),$$

donde, recordemos, $J_{l-k}^k(q_1;c)$ es el número de soluciones del sistema de ecuaciones (7.3), que es nulo si algún $|c_h| \ge lq_1^h$. Además hemos probado la desigualdad $J_{l-k}^k(q_1;c) \le J_{l-k}^k(q_1)$.

Finalmente, llamemos T al número de soluciones del sistema de congruencias

$$(m_1 - m + p_1x_1)^h + \cdots + (m_k - m + p_1x_k)^h$$

$$-(n_1 - m + p_1y_1)^h - \cdots - (n_k - m + p_1y_k)^h \equiv 0 \ (\text{mód } p_1^h),$$

también en las mismas condiciones precedentes. Así

$$N_l \le J_{l-k}^k(q_1) \sum_{|c_h|\le lq_1^h} N_k(c_1p_1,\dots,c_kp_1^k) \le J_{l-k}^k(q_1)T.$$

Ahora vamos a acotar T usando el teorema 7.6. Esto requiere que $p_1 > k$, que ya sabemos que se cumple. Por el mismo argumento empleado en la prueba del teorema 7.2, vemos que T es también el número de soluciones del sistema de congruencias

$$(m_1 - m + p_1 + p_1x_1)^h + \cdots + (m_k - m + p_1 + p_1x_k)^h \equiv$$

$$(n_1 - m + p_1 + p_1y_1)^h + \cdots + (n_k - m + p_1 + p_1y_k)^h \equiv 0 \ (\text{mód } p_1^h),$$

para $h = 1,\dots,k$, con $0 \le m, m_j, n_j \le p_1 - 1$, $0 \le x_j, y_j \le q_1 - 1$ y los m_j, al igual que los n_j, son distintos dos a dos.

Si llamamos $x'_j = m_j - m + p_1 + p_1x_j \ge 0$ y $M = E[q_1p_1^{-k+1}] + 1$, entonces $M > q_1p_1^{-k+1}$, luego $p_1q_1 < Mp_1^k$, luego $q_1 \le Mp_1^{k-1} - 1$, y

$$x'_j \le p_1 - 1 - m + p_1q_1 \le p_1(q_1 + 1) - 1 \le Mp_1^k - 1.$$

Además los x'_j no son congruentes módulo p_1. Así pues, fijados m, n_j, y_j, existen a lo sumo $k!M^kp_1^{k(k-1)/2}$ soluciones posibles del sistema

$$x_1'^h + \cdots + x_k'^h \equiv$$

$$(n_1 - m + p_1 + p_1y_1)^h + \cdots + (n_k - m + p_1 + p_1y_k)^h \equiv 0 \ (\text{mód } p_1^h),$$

en las condiciones requeridas, cada una de las cuales determina unos valores para m_j y x_j. Como n_j y m pueden tomar p_1 valores cada una e y_j puede tomar q_1 valores, concluimos que

$$T \le k!p_1(p_1q_1)^kM^kp_1^{k(k-1)/2}.$$

Ahora usamos que $p_1 \le q^{1/k}$ y que $q_1 > qp_1^{-1}$, con lo que $q_1p_1^{-k+1} > 1$ y

$$M = E[q_1p_1^{-k+1}] + 1 \le 2E[q_1p_1^{-k+1}] \le 2q_1p_1^{-k+1}.$$

Por lo tanto

$$T \le k!2^k q^{2k} p_1^{k+1-k(k-1)/2} = k!2^k q^{2k} p_1^{2k+1-k(k+1)/2}$$

luego

$$N_l \le k!2^k q_1^{2k} p_1^{2k+1-k(k-1)/2} J_{l-k}^k(q_1)$$

y a su vez

$$J_1 \le \binom{l}{k}^2 k!2^k q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1) = q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1) \frac{l^{2k}2^k}{k!}$$

$$\le 2l^{2k} q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1).$$

Recapitulando,

$$J_l^k(q) < J_l^k(p_1 q_1) = J_1 + J_2 \le 3l^{2k} q_1^{2k} p_1^{2l-k(k+1)/2} J_{l-k}^k(q_1). \qquad \blacksquare$$

De aquí deducimos a su vez:

Teorema 7.8 (Teorema del valor medio de Vinogradov) *Sean r, k, l, q números naturales tales que*

$$r \ge 1, \quad k \ge 2, \quad l \ge k^2 + kr, \quad q \ge (2^k k^{2k})^{(1+1/(k-1))^{r-1}}.$$

Entonces

$$J_l^k(q) \le (3l^{2k})^r 3^{4lr-k(k+1)r/2} q^{2l-k(k+1)/2+\delta_r},$$

donde

$$\delta_r = \frac{k(k+1)}{2}\left(1 - \frac{1}{k}\right)^r.$$

En particular, $J_l^k(q) = O(q^{2l-l(k+1)/2+\delta_r})$. Notemos que δ_r tiende a 0 cuando r tiende a ∞, por lo que el teorema implica que, fijados $k \ge 2$ y $\epsilon > 0$, la conjetura de Vinogradov se cumple para dichos k y ϵ y todo l suficientemente grande.

Demostración: Sea $q_0 = q$ y, para $u = 1, \ldots, r$, definimos el número q_u y el primo p_u mediante:

$$\frac{1}{2} q_{u-1}^{1/k} \le p_u \le q_{u-1}^{1/k}, \qquad q_u = E[q_{u-1} p_u^{-1}] + 1.$$

Veamos que se cumple

$$q_{u-1} < p_u q_u, \qquad q^{(1-1/k)^u} < q_u < 3^u q^{(1-1/k)^u}, \quad p_u > k^2.$$

La primera desigualdad es inmediata, por definición. Para probar la segunda observamos que, por la primera y la elección de p_u,

$$q_u > \frac{q_{u-1}}{p_u} \ge q_{u-1}^{1-1/k} \ge q^{(1-1/k)^u},$$

y que, por definición de q_u y la elección de p_u,

$$q_u \le \frac{q_{u-1}}{p_u} + 1 \le 2q_{u-1}^{1-1/k} + 1 < 3q_{u-1}^{1-1/k} < 3^u q^{(1-1/k)^u}.$$

La tercera desigualdad se debe a que, por la segunda y la hipótesis sobre q:

$$p_u \ge \frac{1}{2}q_{u-1}^{1/k} > \frac{1}{2}q^{(1-1/k)^{u-1}/k} \ge \frac{1}{2}(2k^2)^{(1+1/(k-1))^{r-1}(1-1/k)^{u-1}}$$

$$\ge \frac{1}{2}(2k^2)^{(1+1/(k-1))^{u-1}(1-1/k)^{u-1}} = \frac{1}{2}2k^2 = k^2.$$

Además, si $u < r$, por la segunda desigualdad y la hipótesis sobre q:

$$q_u > q^{(1-1/k)^u} \ge (2^k k^{2k})^{(1+1/(k-1))^{r-1}(1-1/k)^u}$$

$$\ge (2^k k^{2k})^{(1+1/(k-1))^u(1-1/k)^u} = 2^k k^{2k},$$

y por la hipótesis sobre l, también $l - uk \ge k^2 + (r-u)k \ge k^2 + k$. Por lo tanto, podemos aplicar reiteradamente el teorema anterior a k y $l - uk$:

$$J_l^k(q) < 3l^{2k}q_1^{2k}p_1^{2l-k(k+1)/2}J_{l-k}^k(q_1) <$$

$$(3l^{2k})^2(q_1q_2)^{2k}(p_1p_2)^{2l-k(k+1)/2}p_2^{-2k}J_{l-2k}^k(q_2) < \cdots$$

$$\cdots < (3l^{2k})^r(q_1\cdots q_r)^{2k}(p_1\cdots p_r)^{2l-k(k+1)/2}(p_2p_3^2\cdots p_r^{r-1})^{-2k}J_{l-kr}^k(q_r).$$

Ahora bien,

$$q_1\cdots q_r < p_2p_3^2\cdots p_r^{r-1}q_r^r,$$

luego

$$J_l^k(q) < (3l^{2k})^r q_r^{2kr}(p_1\cdots p_r)^{2l-k(k+1)/2}J_{l-kr}^k(q_r).$$

Ahora, como $q_{u-1}/p_u > q_{u-1}^{1-1/k} \ge 1$, tenemos que $q_{u-1}/p_u < 2q_{u-1}/p_u - 1$, luego $q_u = E[q_{u-1}p_u^{-1}] + 1 < 2q_{u-1}/p_u$, luego $p_u < 2q_{u-1}/q_u$, luego

$$p_1\cdots p_r < 2\frac{q}{q_1}2\frac{q_1}{q_2}\cdots 2\frac{q_{r-1}}{q_r} = 2^r\frac{q}{q_r} < 2^r q q^{-(1-1/k)^r} < 3^r q^{1-(1-1/k)^r}.$$

A esto añadimos la cota trivial $J_{l-kr}^k(q_r) \le q_r^{2(l-kr)}$, con lo que

$$J_l^k(q) < (3l^{2k})^r 3^{(2l-k(k+1)/2)r}q^{(1-(1-1/k)^r)(2l-k(k+1)/2)}q_r^{2l}. \tag{7.5}$$

Usando que

$$q_r^{2l} < 3^{2lr}q^{(1-1/k)^r 2l},$$

se llega a la desigualdad del enunciado. ∎

En realidad necesitaremos únicamente esta versión más débil del teorema anterior, según el cual la conjetura de Vinogradov se cumple para $\epsilon = 1/2$ y todo l suficientemente grande (respecto de un k prefijado):

Teorema 7.9 *Sean k, l, q números naturales tales que*

$$k \geq 2, \quad l \geq k^2 + 4k^2 \log k, \quad q \geq 2.$$

Entonces existe una constante c tal que

$$J_l^k(q) \leq e^{clk \log^2 k} q^{2l-k(k+1)/2+1/2}.$$

DEMOSTRACIÓN: Si $q < 2^{-k}(2k)^{2k}$, tenemos trivialmente que

$$J_l^k(q) \leq q^{2l} = e^{2l \log q} < e^{4kl \log 2k} < e^{clk \log^2 k}$$

y como, por hipótesis,

$$2l - k(k+1)/2 + 1/2 \geq 2k^2 + 8k^2 \log k - k(k+1)/2 + 1/2$$

$$= \frac{3k^2 - k + 1}{2} + 8k^2 \log k > 0,$$

la conclusión es inmediata.

Supongamos ahora que $q \geq 2^{-k}(2k)^{2k}$. Definimos la sucesión q_u como en la prueba del teorema anterior. Notemos que, mientras $q_{u-1} \geq 2^{-k}(2k)^{2k} \geq 4^3$ se cumple que $q_{u-1}^{1/k} \geq 2k^2$ y es posible definir $p_u \geq k^2$ y, a partir de él, q_u, que cumplirá $q_u \leq q_{u-1}$, pues

$$q_u - 1 \leq \frac{q_{u-1}}{p_1} \leq \frac{q_{u-1}}{2} \leq q_{u-1} - 1,$$

ya que la última desigualdad equivale a $q_{u-1} \geq 2$. Distinguimos dos casos:

1. Existe un número natural $1 \leq r \leq 4k \log k$ tal que
$$q_r < 2^{-k}(2k)^{2k} \leq q_{r-1}.$$
2. Para todo natural $1 \leq r \leq 4k \log k$ se cumple $q_r \geq 2^{-k}(2k)^{2k}$.

En el primer caso tenemos que $l \geq k^2 + 4k^2 \log k \geq k^2 + kr$, lo cual basta para aplicar r veces el teorema 7.7 para obtener (7.5), de donde a su vez

$$J_l^k(q) < (3l^{2k})^{4k \log k} 3^{(2l-k(k+1)/2)4k \log k} q^{(1-(1-1/k)^{4k \log k})(2l-k(k+1)/2)} (2^k k^{2k})^{2l}$$

$$\leq (3l^{2k})^{4k \log k} 3^{8lk \log k} (2^k k^{2k})^{2l} q^{(2l-k(k+1)/2)}$$

$$= e^{4k \log k \log 3 + 8k^2 \log k \log l + 8lk \log k \log 3 + 2lk \log 2 + 4lk \log k} q^{(2l-k(k+1)/2)}.$$

Ahora usamos que $k \log l \leq l \log k$ para $l \geq k^2 \geq k \geq 2$. Así

$$4k \log k \log 3 + 8k^2 \log k \log l + 8lk \log k \log 3 + 2lk \log 2 + 4lk \log k$$

$$\leq ck \log k + clk \log^2 k + clk \log k + clk + clk \log k \leq clk \log^2 k,$$

luego se cumple también la desigualdad del enunciado.

En el segundo caso tomamos $r = E[k\log(k^2+k)]+1$. Se cumple que $r \le 4k\log k$, pues

$$4k\log k - k\log(k^2+k) = k\log\frac{k^3}{k+1} \ge 1,$$

pues $k+1 < k^3$, ya que $k \ge 2$. Por otra parte,

$$r\log\frac{k}{k-1} \ge \frac{r}{k} \ge \log(k^2+k),$$

pues la primera desigualdad equivale a $\log\frac{k}{k-1} \ge \frac{1}{k}$, para $k \ge 2$ o, con el cambio $k = 1/x$, equivale a que $x \le -\log(1-x)$, para $x \le 1/2$, lo cual es fácil de comprobar, por ejemplo, teniendo en cuenta el desarrollo de Taylor de la función $-\log(1-x)$. Por lo tanto

$$\delta_r = \frac{1}{2}k(k+1)(1-1/k)^r \le \frac{1}{2},$$

pues esto equivale a que

$$\log(k^2+k) - r\log\frac{k}{k-1} \le 0.$$

Por la hipótesis de este segundo caso tenemos que $q_r \ge 2^{-k}(2k)^{2k}$ y, como en el primer caso, esto implica a su vez que $l \ge k^2+kr$, por lo que podemos llegar igualmente a (7.5) y de ahí pasar a la conclusión del teorema anterior, con lo que

$$J_l^k(q) \le (3l^{2k})^r 3^{4lr-k(k+1)r/2} q^{2l-k(k+1)/2+1/2}.$$

Los primeros factores se reducen a la forma $e^{clk\log^2 k}$ como en el caso precedente. ∎

7.3 Aplicación a la función dseta

Veamos ahora cómo aplicar el teorema del valor medio de Vinogradov al estudio del crecimiento de la función dseta. La clave será un resultado conocido como desigualdad de Vinogradov, en cuya prueba usaremos el teorema siguiente:

Teorema 7.10 *Sea M un número entero y $N > 1$ un número natural. Sea $\phi(n)$ una función con valores en $\mathbb{R}$ definida sobre los enteros $M \le n \le M+N-1$ tal que existen $a \ge 1$ y $\delta > 0$ tales que $\delta \le \phi(n+1)-\phi(n) \le a\delta$, para todo $M \le n \le M+N-2$. Entonces, para todo $W > 0$, el número de enteros n tales que $D(\phi(n)) \le W\delta$ (donde $D(n)$ es la distancia al entero más próximo) es menor que $(Na\delta+1)(2W+1)$.*

Demostración: Si $W\delta \ge 1/2$, los $N-2$ posibles valores de n cumplen la condición y

$$(Na\delta+1)(2W+1) \ge 2NW\delta a \ge N > N-2.$$

Suponemos, pues, que $W\delta < 1/2$.

Para cada $x \in \mathbb{R}$ y cada $h \in \mathbb{Z}$, existe a lo sumo un n en el intervalo considerado tal que

$$x + h \leq \phi(n) < x + h + \delta.$$

En efecto, si hubiera dos valores de n que cumplieran esto, como ϕ es estrictamente monótona creciente por hipótesis, habría dos consecutivos n y $n+1$, y entonces sería $\phi(n+1) - \phi(n) < \delta$, contradicción.

Llamemos G_x al número de enteros n para los que existe un entero h_n con el que se cumple esta condición. Si $G_x > 0$, entonces $G_x \leq H_2 - H_1 + 1$, donde H_1 y H_2 son el menor y el mayor valor de h_n (porque $n \mapsto h_n$ es inyectiva). Además,

$$\phi(M) < x + H_1 + \delta, \qquad x + H_2 \leq \phi(M + N - 1),$$

pues si $H_1 = h_{n_1}$, tenemos que $\phi(M) \leq \phi(n_1) < x + H_1 + \delta$, e igualmente $x + H_2 \leq \phi(n_2) \leq \phi(M + N - 1)$. Por lo tanto

$$H_2 - H_1 - \delta < \phi(M + N - 1) - \phi(M) \leq (N-1)a\delta,$$

luego

$$G_x < (N-1)a\delta + \delta + 1 \leq (N-1)a\delta + a\delta + 1 = Na\delta + 1.$$

Hemos probado esto bajo la hipótesis de que $G_x > 0$, pero es trivialmente cierto si $G_x = 0$.

Ahora dividimos el intervalo $[-W\delta, W\delta]$ en $E[2W+1]$ subintervalos $[x_i, x_{i+1}]$ de longitud menor que δ. Si $D(\phi(n)) \leq W\delta$, existe un entero h para el que $\phi(n) - h \in [-W\delta, W\delta]$, luego existe un i tal que $\phi(n) - h \in [x_i, x_{i+1}]$, luego

$$x_i \leq \phi(n) - h \leq x_{i+1} < x_i + \delta,$$

luego

$$x_i + h \leq \phi(n) < x_i + h + \delta.$$

Así pues, n está contado en G_{x_i}, luego el número total de tales n es a lo sumo el número de intervalos $E[2W+1]$ por la cota $Na\delta + 1$ al número posible de tales n para cada intervalo, lo que nos da la conclusión del teorema. ∎

Teorema 7.11 (Desigualdad de Vinogradov) *Sean P, Q números naturales no nulos, $Q \geq 2$ y sea $F : [P+1, P+Q] \longrightarrow \mathbb{R}$ una función de clase C^{k+1}, con $k \geq 7$. Sea $\lambda \in \mathbb{R}$ tal que, para todo $x \in [P+1, P+Q]$,*

$$0 < \lambda \leq \left| \frac{F^{k+1)}(x)}{(k+1)!} \right| \leq 2\lambda$$

y $\lambda^{-1/4} \leq Q \leq \lambda^{-1}$. Entonces existen constantes K y c tales que

$$\left| \sum_{n=P+1}^{P+Q} e^{2\pi i F(n)} \right| < K e^{ck \log^2 k} Q^{1-\rho},$$

donde $\rho = (70k^2 \log k)^{-1}$.

DEMOSTRACIÓN: Llamemos

$$C = \sum_{n=P+1}^{P+Q} e^{2\pi i F(n)}$$

y veamos en primer lugar que

$$|C| \le q^{-1} \sum_{n=P+1}^{P+Q-q} |T(n)| + q,$$

donde q es un número natural $1 \le q < Q$ y

$$T(n) = \sum_{m=1}^{q} e^{2\pi i (F(m+n)-F(n))}.$$

Concretamente, tomamos $q = E[\lambda^{(\eta-1)/(k+1)}]$, donde $\eta = (6k^2 \log k)^{-1}$. Notemos que las hipótesis $Q \le \lambda^{-1}$ y $Q \ge 2$ implican que $\lambda \le 1/2$, luego $q \ge E[\lambda^0] = 1$. Por otra parte, como $\lambda^{-1/4} \le Q$, tenemos que

$$q \le \lambda^{(\eta-1)/(k+1)} \le Q^{4(1-\eta)/(k+1)} \le Q^{4/(k+1)} < Q. \tag{7.6}$$

Ahora

$$|qC| = \left| \sum_{m=1}^{q} \sum_{n=P+1}^{P+Q} e^{2\pi i F(n)} \right| \le \left| \sum_{m=1}^{q} \sum_{n=P+1+m}^{P+Q-q+m} e^{2\pi i F(n)} \right| + \sum_{m=1}^{q} q$$

(hemos acotado por 1 parte de los sumandos)

$$= \left| \sum_{m=1}^{q} \sum_{n=P+1}^{P+Q-q} e^{2\pi i F(n+m)} \right| + q^2 = \left| \sum_{n=P+1}^{P+Q-q} \sum_{m=1}^{q} e^{2\pi i F(n+m)} \right| + q^2$$

$$= \left| \sum_{n=P+1}^{P+Q-q} e^{2\pi i F(n)} \sum_{m=1}^{q} e^{2\pi i (F(n+m)-F(n))} \right| + q^2 \le \sum_{n=P+1}^{P+Q-q} |T(n)| + q^2.$$

Ahora expresamos $|T(n)| = 1 \cdot |T(n)|$ y aplicamos la desigualdad de Hölder con exponentes $2l$ (para cualquier $l \ge 1$) y $(1 - \frac{1}{2l})^{-1}$, lo que nos da que

$$q|C| \le \left(\sum_{n=P+1}^{P+Q-q} 1 \right)^{1-1/2l} \left(\sum_{n=P+1}^{P+Q-q} |T(n)|^{2l} \right)^{1/2l} + q^2$$

$$\le Q^{1-1/2l} \left(\sum_{n=P+1}^{P+Q-q} |T(n)|^{2l} \right)^{1/2l} + q^2. \tag{7.7}$$

Fijado $P + 1 \le n \le P + Q - q$, el teorema de Taylor nos da que, para cada $1 \le m \le q$,

$$F(m+n) - F(n) = \sum_{r=1}^{k} \frac{F^{r)}(n)}{r!} m^r + \frac{F^{k+1)}(x)}{(k+1)!} m^{k+1},$$

con $0 < x < m$.

Equivalentemente,

$$F(m+n) - F(n) = \sum_{r=1}^{k} \frac{F^{r)}(n)}{r!} m^r + 2\lambda\theta q^{k+1},$$

con $|\theta| \leq 1$, pues

$$\left| \frac{F^{k+1)}(x)}{(k+1)!} \left(\frac{m}{q}\right)^{k+1} \right| \leq 2\lambda.$$

Llamamos $A_r = F^{r)}(n)/r!$ y definimos $\Omega_n \subset \mathbb{R}^k$ como el conjunto de los $a \in \mathbb{R}^k$ tales que

$$|a_r - A_r| \leq \frac{1}{2}\frac{1}{q^r}\lambda q^{k+1}, \qquad r = 1, \ldots, k.$$

Así, si $a \in \Omega_n$ tenemos que[4]

$$|e^{2\pi i(F(m+n)-F(n))} - e^{2\pi i(a_k m^k + \cdots + a_1 m)}| \leq 2\pi |F(m+n) - F(n) - a_k m^k - \cdots - a_1 m|$$

$$\leq 2\pi \sum_{r=1}^{k} |A_r - a_r| m^r + 4\pi\lambda q^{k+1} \leq \pi\lambda q^{k+1} \sum_{r=1}^{k} \left(\frac{m}{q}\right)^r + 4\pi\lambda q^{k+1}$$

$$\leq \pi\lambda q^{k+1}(k+4) \leq 2\pi k\lambda q^{k+1},$$

donde usamos que $k + 4 \leq 2k$, ya que $k \geq 7$. Por lo tanto,

$$|T(n)| \leq |S(q)| + 2\pi k\lambda q^{k+2},$$

donde $S(q) = S(q, 0; 0, a_1, \ldots, a_k)$ es el dado por (7.1).

A su vez, por la convexidad[5] de la función x^{2l},

$$|T(n)|^{2l} \leq 2^{2l}|S(q)|^{2l} + (4\pi k\lambda q^{k+2})^{2l}.$$

Por lo tanto,

$$m(\Omega_n)|T(n)|^{2l} = \int_{\Omega_n} |T(n)|^{2l} da_1 \cdots da_k \leq$$

$$2^{2l} \int_{\Omega_n} |S(q)|^{2l} da_1 \cdots da_k + m(\Omega_n)(4\pi k\lambda q^{k+2})^{2l}.$$

[4]En la primera desigualdad usamos que $|e^{ix_1} - e^{ix_2}| \leq |x_1 - x_2|$. Geométricamente, esto equivale a que la longitud de una cuerda en una circunferencia es menor o igual que su arco. Analíticamente equivale a que $|e^{ix} - 1| \leq |x|$, que a su vez equivale a que $\cos x - 1 + x^2/2 \geq 0$, lo cual se prueba fácilmente viendo que la función tiene un mínimo en 0.

[5]Concretamente, usamos que

$$(x+y)^n = (\frac{1}{2}2x + \frac{1}{2}2y)^n \leq \frac{1}{2}(2x)^n + \frac{1}{2}(2y)^n \leq (2x)^n + (2y)^n.$$

Como Ω_n es un producto de intervalos, tenemos que

$$m(\Omega_n) = \prod_{r=1}^{k} (q^{-r}\lambda q^{k+1}) = (\lambda q^{k+1})^k q^{-k(k+1)/2},$$

luego

$$|T(n)|^{2l} \le 2^{2l} q^{k(k+1)/2} (\lambda q^{k+1})^{-k} \int_{\Omega_n} |S(q)|^{2l} da_1 \cdots da_k + (4\pi k \lambda q^{k+2})^{2l}.$$

Como $S(q)$ tiene periodo 1 respecto de cada una de las variables a_r, la integral de $|S(q)|^{2l}$ sobre Ω_n coincide con la integral sobre $g + \Omega_n$, para todo $g \in \mathbb{Z}^k$. Observemos que

$$\lambda q^k \le \lambda^{\frac{(\eta-1)k}{k+1}+1} < 1,$$

pues, como $0 < \lambda \le 1/2$, esto equivale a que el exponente sea positivo, es decir, a que $\eta k + 1 > 0$, lo cual es cierto. Esto implica que Ω_n es producto de intervalos de diámetro menor que 1, luego los trasladados $g + \Omega_n$ son disjuntos dos a dos. Sea

$$\Omega'_n = [0,1]^k \cap \bigcup_{g \in \mathbb{Z}^k} (g + \Omega_n).$$

Entonces

$$\int_{\Omega_n} |S(q)|^{2l} da_1 \cdots da_k = \int_{\Omega'_n} |S(q)|^{2l} da_1 \cdots da_k,$$

pues Ω_n puede cubrirse por un número finito de trasladados del cubo unitario I^k, luego la integral sobre Ω_n es la suma de las integrales sobre los trasladados $(g + I^k) \cap \Omega_n$, que coinciden con las integrales sobre $I^k \cap (-g + \Omega_n)$, cuya suma es la integral sobre Ω'_n. Así pues,

$$|T(n)|^{2l} \le 2^{2l} q^{k(k+1)/2} (\lambda q^{k+1})^{-k} \int_{[0,1]^k} |S(q)|^{2l} \chi_{\Omega'_n} da_1 \cdots da_k + (4\pi k \lambda q^{k+2})^{2l},$$

y a su vez

$$\sum_{n=P+1}^{P+Q-q} |T(n)|^{2l} \le 2^{2l} q^{k(k+1)/2} (\lambda q^{k+1})^{-k} \int_{[0,1]^k} |S(q)|^{2l} \sum_{n=P+1}^{P+Q-q} \chi_{\Omega'_n} da_1 \cdots da_k$$
$$+ (Q-q)(4\pi k \lambda q^{k+2})^{2l}.$$

A continuación observamos que $\sum_{n=P+1}^{P+Q-q} \chi_{\Omega'_n}(a)$ es el número de números naturales $P+1 \le n \le P+Q-q$ tales que $a \in \Omega'_n$. Si $a \in \Omega'_n \cap \Omega'_{n'}$, entonces Ω_n y $\Omega_{n'}$ tienen trasladados no disjuntos, luego lo mismo vale para sus proyecciones respecto de la k-ésima componente, que son los intervalos de centros $A_k(n)$ y $A_k(n')$ y radio $\lambda q/2$. Equivalentemente, existe un $h \in \mathbb{Z}$ tal que los intervalos de centros $A_k(n)$ y $A_k(n') + h$ y dicho radio no son disjuntos, luego $|A_k(n) - A_k(n') - h| \le \lambda q$ o, equivalentemente,

$$D(A_k(n) - A_k(n')) \le \lambda q,$$

donde D indica la distancia al entero más próximo.

Por consiguiente, si $a \in \Omega'_{n'}$, entonces $\sum_{n=P+1}^{P+Q-q} \chi_{\Omega'_n}(a)$ es menor o igual que el número de números n en $[P+1, P+Q-q]$ tales que $D(A_k(n) - A_k(n')) \le \lambda q$.

Vamos a probar que este número es menor o igual que $4kq$, para lo cual aplicamos el teorema anterior con

$$\phi(n) = A_k(n) - A_k(n'), \quad M = P+1, \quad N = Q-q > 1, \quad a = 2, \quad \delta = \lambda(k+1),$$

$W = q/(k+1)$ (si $Q - q = 1$ el intervalo es $\{P+1\}$ y la conclusión es trivial).

Observemos que

$$\phi(n+1) - \phi(n) = \frac{1}{k!}(F^{k)}(n+1) - F^{k)}(n)) = \frac{F^{k+1)}(x)}{k!},$$

para cierto $n < x < n+1$. La hipótesis del teorema implica que $F^{k+1)}$ no se anula, luego no puede cambiar de signo en el intervalo que estamos considerando. Observemos además que ni las hipótesis ni la conclusión del teorema que estamos probando se alteran si cambiamos F por $-F$, por lo que no perdemos generalidad si suponemos que el signo es positivo. Esto garantiza que ϕ cumple las hipótesis del teorema anterior. La conclusión es que el número de números n que estamos estudiando es menor o igual que

$$(2\lambda(k+1)Q+1)(\frac{2q}{k+1}+1) \le (2k+3)(\frac{2q}{k+1}+1) \le 3k\left(\frac{q}{4}+q\right) < 4kq,$$

donde hemos usado que $Q \le 1/\lambda$ y luego que $k \ge 7$.

Así pues,

$$\sum_{n=P+1}^{P+Q-q} |T(n)|^{2l} \le 2^{2l} q^{k(k+1)/2} (\lambda q^{k+1})^{-k} 4kq J_l^k(q) + (Q-q)(4\pi k\lambda q^{k+2})^{2l},$$

de donde a su vez, volviendo a (7.7) (véase la nota al pie de la página 208):

$$\begin{aligned}
|C| &\le q^{-1}Q^{1-1/2l}\left(2^{2l}q^{-k(k+1)/2}\lambda^{-k}4kqJ_l^k(q) + (Q-q)(4\pi k\lambda q^{k+2})^{2l}\right)^{1/2l} + q \\
&\le q^{-1}Q^{1-1/2l}\left(2^{2l}q^{-k(k+1)/2}\lambda^{-k}4kqJ_l^k(q)\right)^{1/2l} + \\
&\quad q^{-1}Q^{1-1/2l}\left((Q-q)(4\pi k\lambda q^{k+2})^{2l}\right)^{1/2l} + q \\
&= 2q^{-1}Q^{1-1/2l}\left(q^{-k(k+1)/2}\lambda^{-k}4kqJ_l^k(q)\right)^{1/2l} + 4Q\pi k\lambda q^{k+1} + q.
\end{aligned}$$

De acuerdo con el teorema 7.9, elegimos $l = E[k^2 + 4k^2 \log k] + 1$, con lo que

$$\begin{aligned}
|C| &\le 2q^{-1}Q^{1-1/2l}\left(q^{-k(k+1)/2}\lambda^{-k}4kqe^{clk\log^2 k}q^{2l-k(k+1)/2+1/2}\right)^{1/2l} \\
&\quad +4Q\pi k\lambda q^{k+1} + q \\
&\le e^{(c/2)k\log^2 k}2Q^{1-1/2l}\left(q^{3/2-k(k+1)}4k\lambda^{-k}\right)^{1/2l} + 4Q\pi k\lambda q^{k+1} + q.
\end{aligned}$$

Por (7.6) $q \le Q^{4/(k+1)}$ y, por definición de q, además $\lambda q^{k+1} \le \lambda^\eta \le Q^{-\eta}$.

Por otra parte, como $\lambda^{(\eta-1)/(k+1)} \ge 1$, tenemos que[6] $q \ge \frac{1}{2}\lambda^{(\eta-1)/(k+1)}$, luego

$$\lambda q^{k+1} \ge 2^{-(k+1)}\lambda^\eta \ge 2^{-(k+1)}Q^{-4\eta}.$$

Usando estas cotas obtenemos que

$$|C| \le e^{(c/2)k\log^2 k} 2Q^{1-1/2l}\left(q^{3/2}(\lambda q^{k+1})^{-k}4k\right)^{1/2l} + 4Q\pi k\lambda q^{k+1} + q$$

$$\le e^{ck\log^2 k} 2Q^{1-1/2l}\left(Q^{6/(k+1)}2^{k(k+1)}Q^{4\eta k}4k\right)^{1/2l} + 4\pi kQ^{1-\eta} + Q^{4/(k+1)}$$

$$\le e^{ck\log^2 k} 2Q^{1-1/2l}Q^{3/(k+1)l}Q^{2\eta k/l}\left(2^{k(k+1)}4k\right)^{1/2l} + 4\pi kQ^{1-\eta} + Q^{4/(k+1)}$$

Como $l \ge k^2 + 4k^2\log k$, tenemos que

$$2^{k(k+1)/2l} \le 2, \quad (4k)^{1/2l} = e^{(\log 4+\log k)/2l} \le e,$$

luego

$$|C| \le Ke^{ck\log^2 k}Q^{1-1/2l}Q^{3/(k+1)l}Q^{2\eta k/l} + 4\pi kQ^{1-\eta} + Q^{4/(k+1)}$$
$$= Ke^{ck\log^2 k}Q^{1-\frac{1}{l}(\frac{1}{2}-\frac{3}{k+1}-2\eta k)} + 4\pi kQ^{1-\eta} + Q^{4/(k+1)}.$$

Ahora observamos que, como $k \ge 7$,

$$\frac{1}{2} - \frac{3}{k+1} - 2\eta k = \frac{1}{2} - \frac{3}{k+1} - \frac{1}{3k\log k} \ge \frac{1}{2} - \frac{3}{8} - \frac{1}{21} > \frac{1}{14},$$

y $l < 5k^2\log k$, luego

$$|C| \le Ke^{ck\log^2 k}Q^{1-\frac{1}{70k^2\log k}} + 4\pi kQ^{1-\frac{1}{6k^2\log k}} + Q^{\frac{4}{k+1}}$$
$$\le (Ke^{ck\log^2 k} + 4\pi k + 1)Q^{1-\rho} \le Ke^{ck\log^2 k}Q^{1-\rho}.$$

donde hemos usado que, para $k \ge 7$,

$$\frac{4}{k+1} + \frac{1}{70k^2\log k} \le 1.$$

■

En la práctica sólo necesitaremos la consecuencia siguiente:

Teorema 7.12 *Sean P, N números naturales, sea $F : [P+1, P+N] \longrightarrow \mathbb{R}$ una función de clase C^{k+1}, con $k \ge 7$, sean λ, Q números reales tales que $N \le Q$, $\lambda^{-1/3} \le Q \le \lambda^{-1}$ y, para todo $x \in [P+1, P+N]$,*

$$0 < \lambda \le \left|\frac{F^{k+1)}(x)}{(k+1)!}\right| \le 2\lambda.$$

Entonces existen constantes K y c tales que

$$\left|\sum_{n=P+1}^{P+N} e^{2\pi iF(n)}\right| < Ke^{ck\log^2 k}Q^{1-\rho},$$

donde $\rho = (70k^2\log k)^{-1}$.

[6] En general, si $x \ge 2$ es claro que $E[x] \ge x - 1 \ge x/2$, mientras que si $1 \le x < 2$, entonces $x/2 < 1 = E[x]$.

DEMOSTRACIÓN: Si $\lambda^{-1/4} \le N$, la conclusión se sigue del teorema anterior, aplicado con N en lugar de Q. Si $N < \lambda^{-1/4}$ tenemos que

$$\left| \sum_{n=P+1}^{P+N} e^{2\pi i F(n)} \right| \le N < \lambda^{-1/4} \le Q^{3/4} \le Q^{1-\rho}.$$

■

Vamos a elegir adecuadamente números reales $1 < a < b \le 2a$ y $\tau \ge 1$ de modo que el teorema anterior sea aplicable con $Q = a$ y

$$k = E[\log \tau / \log a] + 1.$$

Para empezar exigimos que

$$2 \log^{1/2} \tau < \log a \le \frac{1}{6} \log \tau. \tag{7.8}$$

Así, la segunda desigualdad garantiza que $k \ge 7$. Por definición de k vemos que

$$a^{k+1} > Q a^{\log \tau / \log a} = Q\tau, \qquad a^{k+1} \le a^2 a^{\log \tau / \log a} = Q^2 \tau,$$

con lo que

$$Q < \frac{a^{k+1}}{\tau} \le Q^2. \tag{7.9}$$

Consideramos la función $F : [a, 2a] \longrightarrow \mathbb{R}$ dada por

$$F(x) = -\frac{\tau \log x}{2\pi}.$$

Así

$$F^{k+1)}(x) = (-1)^{k+1} \frac{k!\tau}{2\pi x^{k+1}}.$$

En $[a, 2a]$ se cumple que

$$\frac{\tau}{2\pi(k+1)(2a)^{k+1}} \le \left| \frac{F^{k+1)}(x)}{(k+1)!} \right| \le \frac{\tau}{2\pi(k+1)a^{k+1}}. \tag{7.10}$$

Podemos dividir el intervalo $[a, b]$ en a lo sumo $k+1$ subintervalos, en cada uno de los cuales exista un λ tal que[7]

$$\frac{\tau}{2\pi(k+1)(2a)^{k+1}} \le \lambda \le \frac{\tau}{2\pi(k+1)a^{k+1}}, \qquad \lambda \le \left| \frac{F^{k+1)}(x)}{(k+1)!} \right| \le 2\lambda.$$

Teniendo en cuenta (7.9), las primeras desigualdades implican que

$$\frac{1}{\pi(k+1)2^{k+2}Q^2} \le \lambda < \frac{1}{Q},$$

[7]Para el primer intervalo, de extremo a, tomamos como 2λ el miembro derecho de (7.10), y el extremo derecho del intervalo es el punto en el que el miembro central se reduce a la mitad. Ése es el valor de λ para el intervalo siguiente, y, como el miembro izquierdo se obtiene del derecho dividiéndolo entre 2^{k+1}, el número de intervalos necesarios para superar b será a lo sumo $k+1$.

que se simplifica hasta

$$\frac{1}{Q^3} \le \lambda < \frac{1}{Q}$$

si se cumple $Q \ge 2^{k+2}\pi(k+1)$. Esta condición equivale a

$$(k+2)\log 2 + \log\pi + \log(k+1) \le \log a.$$

Para que se cumpla esto es suficiente con que se cumpla

$$\left(\frac{\log\tau}{\log a} + 3\right)\log 2 + \log\pi + \log\left(\frac{\log\tau}{\log a} + 2\right) \le \log a,$$

pues, por definición de k, el miembro izquierdo de esta desigualdad es mayor o igual que el de la precedente. A su vez, teniendo en cuenta (7.8), basta con que se cumpla

$$\left(\frac{\log\tau}{2\log^{1/2}\tau} + 3\right)\log 2 + \log\pi + \log\left(\frac{\log\tau}{2\log^{1/2}\tau} + 2\right) \le 2\log^{1/2}\tau$$

o, equivalentemente,

$$\left(\frac{1}{2} + \frac{3}{\log^{1/2}\tau}\right)\log 2 + \frac{\log\pi}{\log^{1/2}\tau} + \frac{\log\left(\frac{\log^{1/2}\tau}{2} + 2\right)}{\log^{1/2}\tau} \le 2,$$

y esto se cumple para todo τ suficientemente grande. En resumen: si partimos de un τ suficientemente grande y elegimos a de modo que se cumpla (7.8), entonces se cumple todo lo que hemos afirmado hasta ahora.

Así, si $[a_{j-1}, a_j]$ es uno de los subintervalos en los que hemos dividido $[a,b]$ y $a_{j-1} < P+1 \le P+N \le a_j$ son el menor y el mayor de los números naturales contenidos en él, tenemos que $N \le a_j - a_{j-1} \le 2a - a = a = Q$, y se cumplen todas las hipótesis del teorema anterior. La conclusión es que

$$\left|\sum_{a_{j-1}<n\le a_j} e^{2\pi i F(n)}\right| < Ke^{ck\log^2 k}Q^{1-\rho},$$

o, equivalentemente, sumando para todos los subintervalos:

$$\left|\sum_{a<n\le b}\frac{1}{n^{i\tau}}\right| < K(k+1)e^{ck\log^2 k}a^{1-\rho} \le 2Kke^{ck\log^2 k}a^{1-\rho}.$$

Por la observación tras el teorema 6.5, para $0<\sigma<1$ se cumple que

$$\left|\sum_{a<n\le b}\frac{1}{n^s}\right| \le \frac{1}{E[a]^\sigma}2Kke^{ck\log^2 k}a^{1-\rho} = O(ke^{ck\log^2 k}a^{1-\rho-\sigma}), \tag{7.11}$$

donde $\rho = (70k^2\log k)^{-1}$.

Debemos tener presente que esta desigualdad se cumple cuando a, τ y k se toman sujetos a unas condiciones muy concretas. Vamos a probar que, dado un $\epsilon > 0$, es posible exigir además que

$$k \log k < \epsilon \log^{1/3} a. \tag{7.12}$$

Para ello probaremos que esto se cumple si

$$A(\log \tau \log\log \tau)^{3/4} < \log a, \tag{7.13}$$

para cierta constante A dependiente de ϵ y de τ. Observemos antes que, fijado $A > 0$, para todo τ suficientemente grande, se cumple que

$$2\log^{1/2} \tau < A(\log \tau \log\log \tau)^{3/4} < \frac{1}{6}\log \tau,$$

por lo que si τ es suficientemente grande, cualquier a que cumpla

$$A(\log \tau \log\log \tau)^{3/4} < \log a < \frac{1}{6}\log \tau \tag{7.14}$$

hace que se cumplan todas las condiciones que estamos considerando.

En efecto, si se cumple (7.13), entonces

$$k < \frac{2\log \tau}{\log a} < \frac{2}{A}\frac{\log^{1/4} \tau}{(\log\log \tau)^{3/4}}$$

y por otra parte, por (7.8),

$$k < \frac{2\log \tau}{\log a} < \log^{1/2} \tau,$$

luego $\log k < \frac{1}{2}\log\log \tau$ y, usando de nuevo (7.13),

$$k \log k < \frac{1}{A}(\log \tau \log\log \tau)^{1/4} < \frac{1}{A}\left(\frac{1}{A}\log a\right)^{1/3}$$

$$= \frac{1}{A^{4/3}}\log^{1/3} a < \frac{1}{A^{4/3}6^{1/3}}\log^{1/3} \tau,$$

luego eligiendo A suficientemente grande se cumple (7.12).

En estas condiciones (7.11) nos da que

$$\sum_{a<n\le b} \frac{1}{n^s} = O\left(\frac{\log \tau}{\log a} a^{1-\sigma} e^{ck\log^2 k - \frac{\log a}{70k^2 \log k}}\right)$$

$$= O\left(\frac{\log \tau}{\log a} a^{1-\sigma} e^{\frac{(70c\epsilon^3 - 1)\log a}{70k^2 \log k}}\right).$$

Elegimos ϵ suficientemente pequeño para que $70c\epsilon^3 - 1 < 0$. Así podemos usar de nuevo las cotas superiores que tenemos para k y $\log k$, con lo que

$$\sum_{a<n\le b} \frac{1}{n^s} = O\left(\log\tau\, a^{1-\sigma} e^{\frac{(70c\epsilon^3-1)\log^3 a}{70\cdot 2\log^2\tau\log\log\tau}}\right).$$

Finalmente usamos (7.13), de modo que

$$\sum_{a<n\le b} \frac{1}{n^s} = O\left(\log\tau\, a^{1-\sigma} e^{\frac{-B\log a(\log\tau\log\log\tau)^{3/2}}{\log^2\tau\log\log\tau}}\right),$$

y así

$$\sum_{a<n\le b} \frac{1}{n^s} = O\left(\log\tau\, a^{1-\sigma} e^{\frac{-B\log a(\log\log\tau)^{1/2}}{\log^{1/2}\tau}}\right), \tag{7.15}$$

donde $B > 0$ es una constante que depende de A, que a su vez depende de τ. Recordemos que esto es válido para todo τ suficientemente grande, todo a que cumpla (7.14) y todo $a < b \le 2a$.

Ahora recordamos el teorema 6.12, según el cual, si $r \ge 6$ y $R = 2^{r-1}$, entonces

$$\zeta(s) = \sum_{1\le n\le\tau^{2/r}} \frac{1}{n^s} + O(1), \tag{7.16}$$

en la región dada por $1 - 1/R \le \sigma \le 1$ para $\log\log\tau \ge r$.

Fijamos una constante $A_1 > 0$ que determinaremos después y llamamos $\alpha = e^{A_1(\log\tau\log\log\tau)^{3/4}}$. Notemos que si τ es suficientemente grande se cumple que $\alpha < \tau^{2/r}$. Descomponemos

$$\sum_{1\le n\le\tau^{2/r}} \frac{1}{n^s} = \sum_{1\le n\le\alpha} \frac{1}{n^s} + \sum_{\alpha<n\le\tau^{2/r}} \frac{1}{n^s}.$$

Fijamos otra constante $A_2 > 0$ y definimos σ_0 mediante

$$1 - \sigma_0 = \frac{A_2(\log\log\tau)^{1/2}}{\log^{1/2}\tau},$$

de modo que, si τ es suficientemente grande, $0 < \sigma_0 < 1$. Así, si $\sigma > \sigma_0$, tenemos que

$$\left|\sum_{1\le n\le\alpha} \frac{1}{n^s}\right| \le \sum_{1\le n\le\alpha} \frac{1}{n^{\sigma_0}} \le \int_0^\alpha \frac{dx}{x^{\sigma_0}} = \frac{\alpha^{1-\sigma_0}}{1-\sigma_0} \le e^{(1-\sigma_0)\log\alpha} \frac{\log^{1/2}\tau}{A_2(\log\log\tau)^{1/2}}$$

$$\le e^{A_1A_2\log^{1/4}\tau(\log\log\tau)^{5/4}} \frac{\log^{1/2}\tau}{A_2(\log\log\tau)^{1/2}} \le e^{A_3\log^{1/4}\tau(\log\log\tau)^{5/4}}, \tag{7.17}$$

para todo τ suficientemente grande, pues

$$\frac{\log^{1/2}\tau}{A_2(\log\log\tau)^{1/2}} \le \frac{\log^{1/2}\tau}{A_2} \le e^{\log^{1/4}\tau} \le e^{\log^{1/4}\tau(\log\log\tau)^{5/4}},$$

donde la desigualdad intermedia se debe a que $\lim_{x\to+\infty} e^x/x^2 = +\infty$.

Tomando τ suficientemente grande podemos exigir que $1/R \ge 1-\sigma_0$, pues esto equivale a

$$\frac{A_2(\log\log\tau)^{1/2}}{\log^{1/2}\tau} \le \frac{1}{R},$$

y el miembro izquierdo tiende a 0 con τ. Así, si $\sigma_0 < \sigma \le 1$ se cumple también que $1 - 1/R \le \sigma \le 1$, luego se cumple (7.16).

Ahora descomponemos

$$\sum_{\alpha<n\le\tau^{2/r}} \frac{1}{n^s} = \sum_{\alpha<n\le 2\alpha} \frac{1}{n^s} + \sum_{2\alpha<n\le 4\alpha} \frac{1}{n^s} + \cdots$$

(donde el último sumatorio es para $2^{v-1}\alpha < n \le \tau^{2/r}$). Así, el número v de sumandos cumple que $(v-1)\log 2 + \log\alpha \le (2/r)\log\tau \le 2\log\tau$, luego $v - 1 \le 2\log\tau$ y $v \le 3\log\tau$.

A cada uno de estos sumatorios (digamos al que empieza en $2^u\alpha < \tau^{2/r}$) les podemos aplicar (7.15), pues para ello se requiere que

$$A(\log\tau\log\log\tau)^{3/4} < \log(2^u\alpha) < \frac{1}{6}\log\tau.$$

La segunda desigualdad se cumple si $r \ge 12$, pues entonces

$$\log(2^u\alpha) < \frac{2}{r}\log\tau \le \frac{1}{6}\log\tau,$$

mientras que la primera se cumple si $A < A_1$, pues entonces

$$A(\log\tau\log\log\tau)^{3/4} < A_1(\log\tau\log\log\tau)^{3/4}$$

$$\le u\log 2 + A_1(\log\tau\log\log\tau)^{3/4} = \log(2^u\alpha).$$

Por otra parte observamos que

$$(2^u\alpha)^{1-\sigma} \le (2^u\alpha)^{1-\sigma_0} = e^{(1-\sigma_0)\log(2^u\alpha)} = e^{\frac{A_2(\log\log\tau)^{1/2}}{\log^{1/2}\tau}(\log\alpha + u\log 2)},$$

luego (7.15) nos da que la suma que empieza en $2^u\alpha$ es de orden

$$O\left(\log\tau\, e^{\frac{-(B-A_2)(\log\log\tau)^{1/2}(\log\alpha+u\log 2)}{\log^{1/2}\tau}}\right).$$

Si tomamos $0 < A_2 < B$, el numerador del exponente es negativo, luego podemos eliminar el término $u \log 2$ y, como el número de sumandos está acotado por $3 \log \tau$, concluimos que

$$\sum_{\alpha < n \le \tau^{2/r}} \frac{1}{n^s} = O\left(\log^2 \tau \, e^{\frac{-(B-A_2)\log\alpha(\log\log\tau)^{1/2}}{\log^{1/2}\tau}}\right).$$

Ahora aplicamos la definición de α:

$$\sum_{\alpha < n \le \tau^{2/r}} \frac{1}{n^s} = O\left(\log^2 \tau \, e^{-c\log^{1/4}\tau(\log\log\tau)^{5/4}}\right) = O(1).$$

Teniendo en cuenta (7.16) y (7.17), hemos probado el teorema siguiente:

Teorema 7.13 *En una región de la forma*

$$1 - \frac{A_2(\log\log\tau)^{1/2}}{\log^{1/2}\tau} < \sigma, \qquad \tau > \tau_0$$

se cumple que

$$\zeta(s) = O(e^{A_3 \log^{1/4}\tau(\log\log\tau)^{5/4}}).$$

En principio hemos probado el teorema con la hipótesis adicional $\sigma \le 1$, pero para $\sigma \ge 1$ el teorema 4.7 nos da que $\zeta(s) = O(\log\tau) = O(e^{\log\log\tau})$, que es una estimación más fina.

Si comparamos este teorema con 6.14, vemos que la estimación es peor, pero la región en la que se cumple es mayor, y esto es lo que realmente importa, porque a través del teorema 5.22 nos da una región sin ceros mayor que la dada por el teorema de Littlewood 6.15.

En efecto, aplicamos 5.22 con

$$\phi(t) = A_3 \log^{1/4} t(\log\log t)^{5/4}, \quad \theta(t) = \frac{A_2(\log\log t)^{1/2}}{\log^{1/2} t}$$

Observamos que

$$\frac{\phi(t)}{\theta(t)e^{\phi(t)}} = \frac{A_3}{A_2} \frac{(\log t \log\log t)^{3/4}}{e^{A_3(\log t\log\log t)^{1/4}\log\log t}} \le \frac{A_3}{A_2} \frac{(\log t \log\log t)^{3/4}}{e^{A_3(\log t\log\log t)^{1/4}}}$$

y la última función tiende a 0 porque x^3/e^x tiende a 0. La conclusión es:

Teorema 7.14 (Chudakov) *Existen constantes A y τ_0 tales que $\zeta(s)$ no tiene ceros en la región*

$$1 - \frac{A}{\log^{3/4}\tau(\log\log\tau)^{3/4}} \le \sigma, \qquad \tau \ge \tau_0.$$

Observaciones Una versión más débil del teorema anterior afirma que, para todo $\epsilon > 0$, existe un τ_1 tal que $\zeta(s)$ no tiene ceros en la región

$$\sigma > 1 - \frac{1}{\log^{3/4+\epsilon} \tau}, \qquad \tau \geq \tau_1.$$

En efecto, basta observar que

$$1 - \frac{1}{\log^{3/4+\epsilon} \tau} > 1 - \frac{A}{\log^{3/4} \tau (\log\log \tau)^{3/4}}$$

para todo τ suficientemente grande, ya que esto equivale a que

$$A > \frac{(\log\log \tau)^{3/4}}{\log^{\epsilon} \tau},$$

y el miembro derecho tiende a 0.

A su vez, esto implica que el teorema 6.15 se cumple para todo $A > 0$, es decir, que para todo $A > 0$ existe un t_0 tal que la función dseta no se anula en la región

$$1 - \frac{A \log\log \tau}{\log \tau} < \sigma, \quad \tau > t_0.$$

En efecto, tenemos que

$$1 - \frac{1}{\log^{3/4+\epsilon} \tau} < 1 - \frac{A \log\log \tau}{\log \tau}$$

equivale a

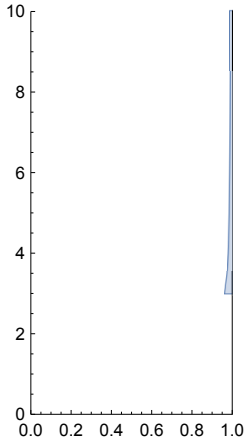
$$A < \frac{\log^{1/4-\epsilon} \tau}{\log\log \tau},$$

y si $\epsilon < 1/4$ el miembro derecho tiende a infinito.

El teorema 7.14 puede refinarse ligeramente. La mejor estimación que se conoce afirma que la función dseta no tiene ceros en la región

$$1 - \frac{1}{57.54 \log^{2/3} \tau (\log\log \tau)^{1/3}} \leq \sigma, \quad \tau \geq 3.$$

A la vista de la figura, puede parecer peor que la región dada por el teorema 5.13, pero es fácil ver que, para valores grandes de τ, la que acabamos de obtener es más amplia.



A su vez, el teorema 5.20 nos proporciona una estimación mejor del error en el teorema de los números primos. Concretamente, ahora podemos tomar

$$\eta(t) = \frac{A}{\log^{3/4} t \, (\log\log t)^{3/4}}$$

(extendida con un valor constante para $t < \tau_1$). La conclusión es:

Teorema 7.15 *Existe una constante $c > 0$ tal que*

$$\pi(x) = \mathrm{Il}(x) + O(xe^{-c\log^{4/7}x\,(\log\log x)^{-3/7}}).$$

DEMOSTRACIÓN: Sea $x_1 = e^{\frac{\log\tau_1}{\eta(\tau_1)}}$. Así $\eta(\tau_1)\log x_1 = \log\tau_1$ y si $x \geq x_1$ entonces $\eta(\tau_1)\log x - \log\tau_1 \geq 0$, luego existe un único $t_0 = t_0(x) \geq \tau_1$ tal que

$$\eta(t_0)\log x - \log t_0 = 0,$$

pues el miembro izquierdo, como función de t, decrece hacia $-\infty$, luego pasa por 0 una única vez. Entonces, para todo $t \geq 1$, se cumple que

$$\eta(t)\log x + \log t \geq \log t_0.$$

En efecto, si $t \geq t_0$ tenemos trivialmente que

$$\eta(t)\log x + \log t \geq \log t \geq \log t_0,$$

mientras que si $1 \leq t \leq t_0$ entonces

$$\eta(t)\log x + \log t \geq \eta(t_0)\log x = \log t_0.$$

Por consiguiente, en términos de la función ω considerada en 5.20, tenemos que

$$\omega(x) \geq \log t_0,$$

pero

$$\log t_0 = \frac{A\log x}{\log^{3/4} t_0\,(\log\log t_0)^{3/4}},$$

luego

$$\log t_0 = \frac{(A\log x)^{4/7}}{(\log\log t_0)^{3/7}},$$

luego

$$\log\log t_0 < \log\log t_0 + \frac{3}{7}\log\log\log t_0 = \frac{4}{7}\log\log x + \frac{4}{7}\log A < c\log\log x,$$

para x suficientemente grande, luego

$$\omega(x) \geq \frac{(A\log x)^{4/7}}{(\log\log t_0)^{3/7}} \geq c\log^{4/7}x\,(\log\log x)^{-3/7}.$$

Ahora basta aplicar 5.20. ∎

Capítulo VIII

Números compuestos

Tras haber dedicado grandes esfuerzos al estudio de la distribución de los números primos, en este capítulo nos ocupamos de varias familias de números que, en distintos sentidos, "tienen muchos divisores".

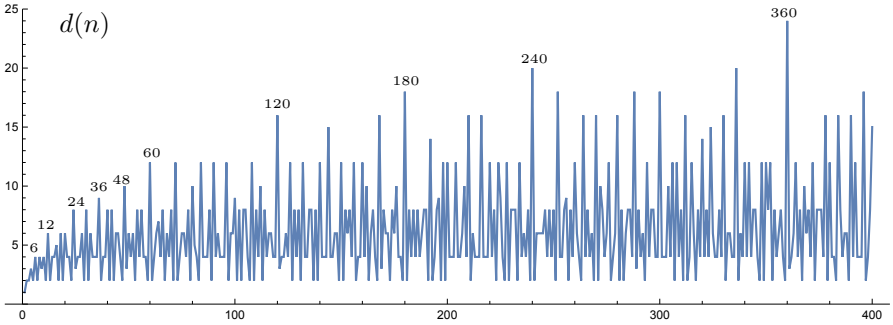
8.1 Números altamente compuestos

Recordemos que $d(n)$ es la función aritmética multiplicativa que asocia a cada número natural n su número de divisores. En términos de la función d, los números primos pueden caracterizarse como los números que cumplen $d(p) = 2$, es decir, los números en los que d toma el valor mínimo posible (sin contar el caso excepcional $d(1) = 1$). Naturalmente, no podemos hablar de los números en los que d toma el valor máximo posible, pues no existe tal máximo, pero sí que podemos considerar los que baten "récords" de divisores:

Definición 8.1 Un número natural $n \geq 1$ es *altamente compuesto* si $d(n)$ es mayor que $d(m)$, para todo $m < n$.

Los primeros números altamente compuestos son

$$1, \quad 2, \quad 4, \quad 6, \quad 12, \quad 24, \quad 36, \quad 48, \quad 60\ldots$$



No es casual que muchos de ellos nos resulten familiares: 12 horas, 24 horas, 60 minutos, 360 grados... Avanzando más en la sucesión nos encontramos con $7! = 5\,040$, que fue propuesto por Platón como el número ideal de habitantes de una *polis,* precisamente por su gran número de divisores.

Es evidente que hay infinitos números altamente compuestos, pero podemos decir algo más preciso:

Teorema 8.2 *Si N es un número altamente compuesto, existe otro número altamente compuesto N' tal que $N < N' \leq 2N$.*

DEMOSTRACIÓN: Basta observar que, si $N = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p}$, entonces

$$\frac{d(2N)}{d(N)} = \frac{e_2 + 2}{e_2 + 1} > 1,$$

luego el menor número natural N' que tiene más de $d(N)$ divisores es altamente compuesto y cumple $N < N' \leq 2N$. ∎

Las descomposiciones en primos de los números altamente compuestos deben cumplir ciertas propiedades:

Teorema 8.3 *Si $N \geq 2$ es un número altamente compuesto, entonces factoriza en la forma $N = 2^{e_2} \cdot 3^{e_3} \cdots p_r^{e_{p_r}}$, donde $p_1, \ldots, p_r$ son los primeros primos consecutivos y $e_2 \geq e_3 \geq \cdots \geq e_{p_r}$. Además, $e_{p_r} = 1$ salvo si $n = 4$ o $n = 36$.*

DEMOSTRACIÓN: La primera parte es inmediata, pues si $\pi_1, \ldots \pi_r$ son primos distintos arbitrarios, entonces

$$d(\pi_1^{m_1} \cdots \pi_r^{m_r}) = d(2^{m_1} \cdot 3^{m_2} \cdots p_r^{m_r}),$$

pero el número de la derecha es menor que el primero (salvo que $\pi_1, \ldots, \pi_r$ sean los r primeros primos). Por lo tanto, $N = 2^{e_2} \cdot 3^{e_3} \cdots p_r^{e_{p_r}}$, y si $e_{p_i} < e_{p_j}$ con $i < j$, el número que resulta de intercambiar ambos exponentes es menor y tiene los mismos divisores. Por lo tanto, la sucesión de los exponentes es decreciente.

La última parte del teorema es un poco más delicada. Se comprueba que 4 y 36 son las únicas excepciones para $n \leq 36$, luego sólo hay que probar que $e_{p_r} = 1$ cuando $N > 36$. Observemos en primer lugar que si $e_{p_r} \geq 2$, entonces $e_2 \geq 3$. En caso contrario, es decir, si $e_2 = 1, 2$, tiene que ser $r \geq 3$, pues de lo contrario $n \leq 2^2 3^2 = 36$, luego $5 \mid n$ y podemos considerar[1]

$$d(4n/5) = d(2^{e_2+1} 3^{e_3} 5^{e_5-1} \cdots p_r^{e_{p_r}}) = \frac{e_2 + 3}{e_2 + 1} \frac{e_5}{e_5 + 1} d(n) \geq \frac{5}{3} \frac{2}{3} d(n) > d(n),$$

contradicción.

Ahora consideramos

$$d(\frac{p_{r+1} n}{2p_r}) = d(2^{e_2-1} 3^{e_3} \cdots p_r^{e_{p_r}-1} p_{r+1}) = \frac{e_2}{e_2 + 1} \frac{e_{p_r}}{e_{p_r+1}} 2d(n) \geq \frac{3}{4} \frac{2}{3} 2d(n) = d(n),$$

[1] Aquí usamos que la sucesión $n/(n+1) = 1 - 1/(n+1)$ es creciente.

pero

$$\frac{p_{r+1}n}{2p_r} < n,$$

ya que esto equivale a que $p_{r+1} < 2p_r$, y esto es el postulado de Bertrand (teorema 3.9). ∎

El teorema anterior se expresa de forma más conveniente en términos de primoriales.

Definición 8.4 El *primorial* (factorial primo) de un primo p se define como el producto $p\#$ de todos los primos menores o iguales que p.

El teorema anterior afirma que todo número altamente compuesto se expresa de forma única como producto de primoriales

$$N = P_1\# \cdots P_k\#,$$

para una sucesión decreciente de primos $P_1 \geq P_2 \geq \cdots \geq P_k$, y además $P_1 > P_2$ salvo si $N = 4, 36$. Más explícitamente:

$$\begin{aligned} N = \quad & 2 \cdot 3 \cdot \cdots \cdots P_1 \\ & 2 \cdot 3 \cdot \cdots P_2 \\ & \cdots\cdots \\ & 2 \cdot 3 \cdots P_k \end{aligned} \tag{8.1}$$

Nota En lo sucesivo, si N es un número altamente compuesto, sobrentenderemos que su descomposición en primoriales (decrecientes) es

$$N = P_1\# \cdots P_k\#,$$

con lo que P_1 es el mayor primo que divide a N, y que su descomposición en primos es

$$N = 2^{e_2} \cdots P_1^{e_{P_1}}.$$

Notemos que $k = e_2$. Si en la sucesión de los P_i no hubiera repeticiones sería $e_{P_i} = i$, pero como puede haberlas, sólo podemos afirmar que $i \leq e_{P_i}$. Similarmente, si P_i^* es el primo siguiente a P_i, podemos afirmar que $e_{P_i^*} \leq i - 1$. ∎

Hay que tener presente que todas estas condiciones son necesarias, pero no suficientes, para que un número N sea altamente compuesto. Podemos dar algunas más:

Teorema 8.5 *Si $N = 2^{e_2} \cdots P_1^{e_{P_1}}$ es un número altamente compuesto, entonces $p_i^{e_{p_i}} < P_1^6$, para todo primo $p_i \leq P_1$.*

Demostración: Por abreviar escribiremos $p = p_i$. Como $e_{P_1} \leq 2$, podemos suponer que $p < P_1$. Si fuera $p^{e_p} > P_1^6$, llamemos a al menor natural tal que $P_1^2 < p^a$. Entonces $p^{a-1} < P_1^2$, luego $p^a < P_1^3$. Entonces $p^{2a} < P_1^6$, luego $2a < e_p$.

Sea $N' = NP_1^*/p^a$, donde P_1^* es el primo siguiente a P_1. Por el postulado de Bertrand tenemos que $P_1^* \le 2P_1 \le P_1^2 < p^a$, luego $N' < N$ y, como N es altamente compuesto, tiene que ser $d(N') < d(N)$, pero

$$\frac{d(N')}{d(N)} = \frac{2(e_p - a + 1)}{e_p + 1} > \frac{2e_p - e_p + 1}{e_p + 1} = 1,$$

contradicción. ∎

Esto implica que sólo hay un número finito de números altamente compuestos cuyo mayor divisor primo sea un primo P_1 dado. Equivalentemente, la sucesión formada por el mayor divisor primo de cada número altamente compuesto tiende a infinito. Podemos precisar esto:

Teorema 8.6 *Existen constantes c_1 y c_2 tales que, para todo número altamente compuesto N,*

$$c_1 \log N < P_1 < c_2 \log N.$$

DEMOSTRACIÓN: Por el teorema anterior, $N \le P_1^{6\pi(P_1)}$, donde $\pi(x) = \sum_{p \le x} 1$. Por consiguiente

$$\log N \le 6\pi(P_1) \log P_1 = 6\frac{\pi(P_1)\log P_1}{P_1} P_1,$$

pero, por el teorema de los números primos, la fracción está acotada, así que $\log N < \frac{1}{c_1} P_1$, para cierta constante[2] $c_1 > 0$. Por otro lado, $N > P_1\#$, luego, por el teorema 3.10,

$$\log N > \vartheta(P_1) \ge P_1 \frac{1}{4} \log 2,$$

luego basta tomar $c_2 = 4/\log 2 < 5.771$. ∎

Teorema 8.7 *Si N es un número altamente compuesto suficientemente grande y $P_1/2 < p \le P_1$, entonces $e_p = 1$.*

DEMOSTRACIÓN: Necesitamos que N sea lo suficientemente grande como para que existan primos $p_1 < p_2 < p_3 < p$. Sean $P_1^* < P_1^{**}$ los dos primos siguientes a P_1. Consideramos $N' = NP_1^*P_1^{**}/(p_1p_2p_3)$ y veamos que si N es suficientemente grande, entonces $N' < N$.

En efecto, por el postulado de Bertrand sabemos que $P_1^* < 2P_1$, $P_1^{**} < 4P_1$, $p_3 > p/2 > P_1/4$, $p_2 > P_2/8$, $p_3 > P_1/16$, luego

$$\frac{P_1^* P_1^{**}}{p_1p_2p_3} < \frac{8P_1^2}{P_1^3/512} = \frac{4\,096}{P_1}.$$

Por el teorema anterior, tomando N suficientemente grande podemos garantizar que $P_1 > 4\,096$, y así $N' < N$. Sin embargo, si $e_p \ge 2$,

$$\frac{d(N')}{d(N)} = \frac{4e_{p_1}e_{p_2}e_{p_3}}{(e_{p_1}+1)(e_{p_2}+1)(e_{p_3}+1)} \ge 4\left(\frac{2}{3}\right)^3 > 1,$$

pues la función $x/(x+1)$ es creciente y en $x = 2$ vale $2/3$. ∎

[2] Tomando 1.256 como cota para el cociente, obtenemos $c_1 < 0.132$.

Nota Hemos probado que la condición $N' < N$ se cumple cuando $P_1 > 4\,096$, pero es fácil comprobar con un ordenador que también se cumple[3] para los primos en el rango $37 \le P_1 < 4\,096$, por lo que el teorema vale, de hecho, para $P_1 \ge 37$. Más aún, una comprobación directa sobre los números altamente compuestos con $P_1 < 37$ muestra que el teorema se cumple de hecho para $P_1 \ge 11$, es decir, a partir de $N = 55\,440 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. ∎

Similarmente podemos probar que, los números altamente compuestos suficientemente grandes tienen divisores primos con exponente 2:

Teorema 8.8 *Si N es un número altamente compuesto suficientemente grande y $2\sqrt{P_1} < p < 4\sqrt{P_1}$, entonces $e_p = 2$.*

Demostración: Supongamos que $p > 2\sqrt{P_1}$ y que $e_p \ge 3$. Entonces, con la misma notación de la prueba del teorema anterior, esta vez tomamos $N' = NP_1^*P_1^{**}/(p_1p_2p_3p_4)$, que cumple $N' < N$ cuando N es suficientemente grande. Además

$$\frac{d(N')}{d(N)} = \frac{4e_{p_1}e_{p_2}e_{p_3}e_{p_4}}{(e_{p_1}+1)(e_{p_2}+1)(e_{p_3}+1)(e_{p_4}+1)} \ge 4\left(\frac{3}{4}\right)^4 > 1,$$

contradicción.

Sea ahora p el menor primo para el que $e_p = 1$ y supongamos que $p < 4\sqrt{P_1}$. Tomando N suficientemente grande, podemos asegurar que haya al menos 11 primos comprendidos estrictamente entre $4\sqrt{P_1}$ y P_1.

En efecto, por el teorema de los números primos, dado $\epsilon > 0$, tomando P_1 suficientemente grande podemos exigir que

$$1 - \epsilon < \frac{\pi(P_1)\log P_1}{P_1}, \qquad \frac{\pi(4\sqrt{P_1})\log 4\sqrt{P_1}}{4\sqrt{P_1}} < 1 + \epsilon,$$

luego

$$\pi(P_1) > (1-\epsilon)\frac{P_1}{\log P_1}, \qquad \pi(4\sqrt{P_1}) < (1+\epsilon)\frac{4\sqrt{P_1}}{\log 4\sqrt{P_1}}.$$

Por lo tanto,

$$\pi(P_1) - \pi(4\sqrt{P_1}) > (1-\epsilon)\frac{P_1}{\log P_1} - (1+\epsilon)\frac{4\sqrt{P_1}}{\log 4\sqrt{P_1}}$$

$$\ge (1-\epsilon)\frac{P_1}{\log P_1} - (1+\epsilon)\frac{4\sqrt{P_1}}{\log \sqrt{P_1}} = \frac{(1-\epsilon)P_1 - (1+\epsilon)8\sqrt{P_1}}{\log P_1},$$

y aplicando la regla de L'Hôpital vemos que el último término tiende a $+\infty$ cuando P_1 tiende a $+\infty$. Por lo tanto, si P_1 es suficientemente grande, podemos exigir que $\pi(P_1) - \pi(4\sqrt{P_1}) > 12$.

[3]Más concretamente, se trata de comprobar que si $5 \le P_1 < 4\,096$ (hay 560 primos en estas condiciones) y p es el menor primo $p > P_1/2$, entonces $P_1^*P_1^{**}/p_1p_2p_3 > 1$ siempre que $P_1 \ge 37$.

Pongamos que $p = p_i$ y que $P_1 = p_j$ y consideremos

$$N' = N\frac{p_{i+1}p_{i+2}p_{i+3}p_{i+4}p_{i+5}p_{i+6}p_{i+7}}{p_{j-1}p_{j-2}p_{j-3}p_{j-4}}.$$

La elección de P_1 garantiza que los 11 primos son distintos entre sí. Ahora $p_{i+t} \le 2^{t+2}\sqrt{P_1}$ y $p_{j+t} \ge P_1/2^t$, luego

$$\frac{N'}{N} \le K\frac{\sqrt{P_1}^7}{P_1^4} = \frac{K}{\sqrt{P_1}} < 1$$

cuando P_1 es suficientemente grande. Por otra parte,

$$\frac{d(N')}{d(N)} = \left(\frac{3}{2}\right)^7 \frac{1}{2^4} > 1,$$

pues todos los primos considerados tienen exponente 1 en N, luego los del numerador dan lugar a factores 3/2 y los del denominador a factores 2. Así tenemos nuevamente una contradicción. ∎

Nota Las pruebas de los teoremas anteriores pueden generalizarse para probar que un número altamente compuesto suficientemente grande es divisible entre primos con cualquier exponente en un conjunto finito prefijado. ∎

Hemos señalado que 7! es altamente compuesto, y es fácil ver que lo mismo sucede con todos los factoriales precedentes, pero no con los posteriores:

Teorema 8.9 *El número $n!$ es altamente compuesto si y sólo si $n \le 7$.*

Demostración: Vamos a probar que $n!$ no es altamente compuesto si $n \ge 20$. El resto del enunciado puede comprobarse analizando los factoriales anteriores uno por uno. Sea $n' = n!13/16$. Claramente $n' < n!$, y basta probar que $d(n') > d(n!)$ o, equivalentemente, que

$$\frac{d(n')}{d(n!)} = \frac{(e_2-3)(e_{13}+2)}{(e_2+1)(e_{13}+1)} > 1.$$

Esto equivale a su vez a que $(e_2-3)(e_{13}+2) > (e_2+1)(e_{13}+1)$, que se simplifica hasta $e_2 > 4e_{13} + 7$. Según (3.1) tenemos que

$$e_2 = \sum_{m=1}^{E[\log_2 n]} E[n/2^m] > \sum_{m=1}^{E[\log_2 n]} n/2^m - 1 = n - n/2^{E[\log_2 n]} - E[\log_2 n]$$

$$\ge n - 2 - \log_2 n,$$

donde hemos usado que $n/2^{E[\log_2 n]} \le n/2^{\log_2 n} = 1$ y que $E[\log_n 2] \le \log_2 n + 1$. Similarmente,

$$e_{13} = \sum_{m=1}^{E[\log_{13} n]} E[n/13^m] \le \sum_{m=1}^{\infty} n/13^m = n/12.$$

Por consiguiente, basta probar la desigualdad central de la cadena siguiente:

$$e_2 > n - 2 - \log_2 n \geq n/3 + 7 \geq 4e_{13} + 7,$$

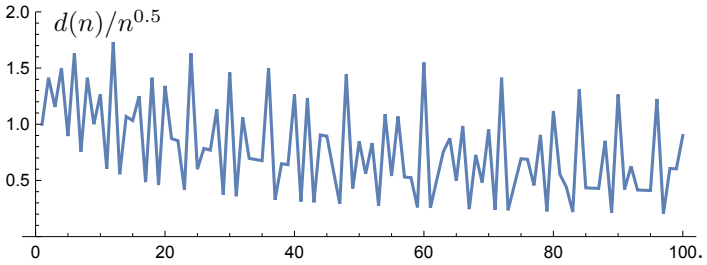
pero es fácil ver que la función $x - 2 - \log_2 x - x/3 - 7$ es positiva en $x = 20$ y tiene derivada positiva para $x \geq 20$, luego siempre es positiva. ∎

8.2 Números altamente compuestos superiores

Todas las características de los números altamente compuestos que hemos probado en la sección anterior son condiciones necesarias, pero no suficientes. De hecho, no tenemos ningún criterio para reconocer los números altamente compuestos más allá del obvio de comparar su número de divisores con los de todos sus precedentes. Sin embargo, Ramanujan introdujo una clase de números altamente compuestos fáciles de calcular.

La definición se apoya en que, por el teorema 2.22 (véanse las observaciones tras el enunciado), para todo $\epsilon > 0$ se cumple que $d(n) = o(n^\epsilon)$. Por consiguiente, para todo $\epsilon > 0$ la sucesión $d(n)/n^\epsilon$ alcanza un valor máximo, lo cual justifica la definición siguiente:

Definición 8.10 Un número natural $N \geq 1$ es *altamente compuesto superior* si existe un $\epsilon > 0$ tal que la función $d(n)/n^\epsilon$ toma en N su valor máximo.



La figura muestra la función $d(n)/n^{0.5}$, que toma su máximo en $N = 12$, por lo que 12 es un número altamente compuesto superior.

Nota Es importante advertir que acabamos de afirmar, pero no hemos demostrado, que 12 sea altamente compuesto superior, pues la gráfica no prueba que no haya valores de $n > 100$ donde la función exceda el valor que toma en $N = 12$. En principio, no tenemos ningún método para saber si un número dado es o no altamente compuesto superior. Podría parecer que los números altamente compuestos superiores son más difíciles de identificar que los altamente compuestos, pero enseguida veremos que la situación es justo la contraria. ∎

Todo número N altamente compuesto superior es altamente compuesto, pues si N cumple la definición con ϵ y $n < N$, entonces

$$\frac{d(n)}{n^\epsilon} \leq \frac{d(N)}{N^\epsilon},$$

luego

$$d(n) \le d(N)\left(\frac{n}{N}\right)^{\epsilon} < d(N).$$

Supongamos ahora $N = 2^{e_2}\cdots p_r^{e_{p_r}}$ es altamente compuesto superior (respecto de ϵ) y consideremos un primo $p \mid N$. Sea $N' = N/p$, de modo que

$$\frac{d(N')}{N'^{\epsilon}} \le \frac{d(N)}{N^{\epsilon}}. \tag{8.2}$$

Usando que d es multiplicativa, esto se simplifica a

$$\frac{e_p}{p^{(e_p-1)\epsilon}} \le \frac{e_p+1}{p^{e_p\epsilon}},$$

que equivale a

$$p^{\epsilon} \le 1 + \frac{1}{e_p}$$

o también a

$$\epsilon \le \frac{\log((e_p+1)/e_p)}{\log p} \tag{8.3}$$

Similarmente, si p es un primo cualquiera y consideramos $N' = Np$, la condición

$$\frac{d(N')}{N'^{\epsilon}} \le \frac{d(N)}{N^{\epsilon}}$$

se traduce ahora en que

$$\frac{e_p+2}{p^{(e_p+1)\epsilon}} \le \frac{e_p+1}{p^{e_p\epsilon}},$$

de donde

$$p^{\epsilon} \ge \frac{e_p+2}{e_p+1}$$

o, equivalentemente,

$$\epsilon \ge \frac{\log((e_p+2)/(e_p+1))}{\log p}. \tag{8.4}$$

Ahora necesitamos distinguir casos según que puedan darse o no las igualdades en las fórmulas precedentes. Para ello conviene introducir la notación siguiente:

Definición 8.11 Consideramos la función

$$F(p,e) = \frac{\log((e+1)/e)}{\log p}$$

Para cada primo p definimos el conjunto

$$E_p = \{F(p,e) \mid e = 1,2,3,\ldots\}.$$

Llamamos $E = \bigcup_p E_p$.

En estos términos (8.3) y (8.4) equivalen respectivamente a $\epsilon \le F(p, e_p)$ y $\epsilon \ge F(p, e_p + 1)$. La primera vale también para $e_p = 0$ si convenimos en que $F(p, 0) = +\infty$. Si $\epsilon > 0$ no está en E, ambas desigualdades son estrictas.

Teorema 8.12 *Para cada número real $\epsilon > 0$ tal que $\epsilon \notin E$, la función $d(n)/n^\epsilon$ alcanza su máximo en un único número N_ϵ, que es, por definición, altamente compuesto superior. Concretamente $N_\epsilon = \prod_p p^{e_p(\epsilon)}$, con*

$$e_p(\epsilon) = E\left[\frac{1}{p^\epsilon - 1}\right].$$

DEMOSTRACIÓN: Sea N un número donde $d(n)/n^\epsilon$ alcance su valor máximo (en principio puede haber más de uno). Si p divide a N con exponente e_p, hemos probado que

$$F(p, e_p + 1) < \epsilon < F(p, e_p), \tag{8.5}$$

es decir,

$$\frac{\log((e_p+2)/(e_p+1))}{\log p} < \epsilon < \frac{\log((e_p+1)/e_p)}{\log p}$$

o también

$$\frac{e_p+2}{e_p+1} < p^\epsilon < \frac{e_p+1}{e_p},$$

de donde se llega fácilmente hasta

$$\frac{1}{p^\epsilon - 1} - 1 < e_p < \frac{1}{p^\epsilon - 1}.$$

Esto implica en particular que $(p^\epsilon - 1)^{-1}$ no es entero, y que, necesariamente, $e = E[(p^\epsilon - 1)^{-1}]$, luego N está completamente determinado por ϵ. ∎

Notemos ahora que, como la función $F(p, e)$ decrece hacia 0 tanto si aumenta p como si aumenta e, para cada $\delta > 0$ hay un número finito de elementos en E mayores que δ, lo que se traduce en que E puede ordenarse en una sucesión decreciente[4]

$$\epsilon_1 > \epsilon_2 > \epsilon_3 > \cdots$$

convergente a 0. Definimos $\epsilon_0 = +\infty$.

Así, si $\epsilon > 0$ no está en E, existe un único i tal que $\epsilon_i < \epsilon < \epsilon_{i-1}$, y se cumple que cualquier par de números ϵ en $]\epsilon_i, \epsilon_{i-1}[$ tienen por debajo y por encima exactamente los mismos elementos de E. A su vez, esto implica que ambos cumplen las desigualdades (8.5) con los mismos valores de p y e_p, por lo que N_ϵ es el mismo para ambos.

Definición 8.13 Para cada $i \ge 0$, definimos N_i como el número altamente compuesto superior N_ϵ determinado por cualquier $\epsilon \in]\epsilon_{i+1}, \epsilon_i[$.

[4]Concretamente para calcular todos los términos de la sucesión mayores que un $\delta > 0$ vamos calculando $F(2,1), F(2,2), F(2,3), \ldots$ hasta obtener un valor menor que δ, luego calculamos $F(3,1), F(3,2), \ldots$ hasta obtener de nuevo un valor menor que δ, y seguimos así hasta que $F(p,1) < \delta$. Por último ordenamos todos los números obtenidos.

La tabla siguiente contiene los $\epsilon_i > 0.3$ junto con sus números altamente compuestos superiores asociados. No obstante, cabe señalar que se ha impuesto el convenio de no considerar al 1 como número altamente compuesto superior (aunque sí que se considera altamente compuesto).

i	ϵ_i	N_i	Factorización	Fact. en primoriales
0	$+\infty$	1		
1	1	2	2	$2\#$
2	0.63093	6	$2 \cdot 3$	$3\#$
3	0.58496	12	$2^2 \cdot 3$	$3\# \cdot 2\#$
4	0.43067	60	$2^2 \cdot 3 \cdot 5$	$5\# \cdot 2\#$
5	0.41503	120	$2^3 \cdot 3 \cdot 5$	$5\# \cdot 2\# \cdot 2\#$
6	0.36907	360	$2^3 \cdot 3^2 \cdot 5$	$5\# \cdot 3\# \cdot 2\#$
7	0.35620	2 520	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	$7\# \cdot 3\# \cdot 2\#$
8	0.32192	5 040	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$7\# \cdot 3\# \cdot 2\# \cdot 2\#$

Ejemplo Si $\epsilon = 0.5$, tenemos que

$$e_2 = E[(2^{0.5} - 1)^{-1}] = 2, \quad e_3 = E[(3^{0.5} - 1)^{-1}] = 1, \quad e_5 = E(5^{0.5} - 1)^{-1}) = 0,$$

por lo que $N_3 = 2^2 \cdot 3 = 12$. ∎

Falta por estudiar si los $\epsilon \in E$ dan lugar a números altamente compuestos superiores que no aparecen al prolongar la lista precedente.

Teorema 8.14 *Si ϵ_i está en un único conjunto E_q, entonces la función $d(n)/n^{\epsilon_i}$ alcanza su máximo exactamente en dos números altamente compuestos superiores, que no son sino N_{i-1} y N_i. Además $N_i = N_{i-1}q$.*

Demostración: Estamos suponiendo que hay un único primo q tal que $\epsilon_i = F(q, e)$, para un e que, claramente, también será único. Si N es uno de los números donde la función $d(n)/n^{\epsilon_i}$ toma su valor máximo, se sigue cumpliendo (8.5) para todos los primos $p \neq q$, por lo que necesariamente $e_p = E[(p^{\epsilon_i} - 1)^{-1}]$. Más aún, es claro que (8.5) se cumple con el mismo e_p aunque cambiemos ϵ_i por un número ligeramente mayor o menor, luego e_p coincide con el exponente de p en N_i y en N_{i-1}. En cambio, para q tenemos que

$$F(q, e_q + 1) \leq \epsilon_i \leq F(q, e_q),$$

lo que nos lleva a

$$\frac{1}{q^{\epsilon_i} - 1} - 1 \leq e_q \leq \frac{1}{q^{\epsilon_i} - 1}.$$

Hay exactamente dos valores de e_q que cumplen estas desigualdades, a saber $e_q = e$ y $e_q = e - 1$. Además, $e_q = e$ es el mismo exponente que se obtiene con un ϵ ligeramente menor que ϵ_i, luego $N = N_i$, mientras que $e_q = e - 1$ es el mismo exponente que se obtiene con un ϵ ligeramente mayor que ϵ_i, luego $N = N_{i-1}$.

En particular, vemos que N_{i-1} y N_i son divisibles entre los mismos primos con los mismos exponentes, salvo en el caso de q, que divide a N_{i-1} con exponente $e-1$ y a N_i con exponente e. Por consiguiente, $N_i = N_{i-1}q$.

Si partimos de (8.2) aplicado a $N = N_i$, $N' = N_i/q = p$, entonces (8.3) es la igualdad $\epsilon_i = F(p, e_q)$, luego (8.2) también es una igualdad, luego concluimos que N_{i-1} y N_i son ambos máximos de la función $d(n)/n^{\epsilon_i}$. ∎

Nos falta considerar la posibilidad de que un mismo ϵ_i esté en varios conjuntos E_p. Observemos que $\epsilon_i \in E_p$ equivale a que existe un e tal que $\epsilon_i = F(p, e)$, lo cual equivale a su vez a que $p^{\epsilon_i} = 1 + 1/e$.

Si $\epsilon_i \in E_p \cap E_q$, tenemos que p^{ϵ_i} y q^{ϵ_i} son números racionales. La conjetura de las cuatro exponenciales (véase la página 11) implica que esto sólo es posible si ϵ_i es entero, lo cual a su vez sería absurdo porque $1 + 1/e$ no puede ser una potencia de primo.

Así pues, la conjetura de las cuatro exponenciales implica que los conjuntos E_p son disjuntos dos a dos, y el teorema anterior recoge todas las posibilidades de generación de números altamente compuestos superiores.

Si no nos apoyamos en la conjetura, el teorema 1.5 nos asegura al menos que un mismo ϵ_i puede pertenecer a lo sumo a dos conjuntos E_p y E_q. En tal caso, los mismos razonamientos del teorema anterior implican que la función $d(n)/n^{\epsilon_i}$ alcanza su máximo en cuatro números, que son N_{i-1}, $N_i = N_{i-1}pq$, $N_{i-1}p$, $N_{i-1}q$, con lo que hay dos números altamente compuestos superiores que no aparecen en la sucesión de los N_i.

En particular vemos que una consecuencia de la conjetura de las cuatro exponenciales es que el cociente de dos números altamente compuestos superiores consecutivos es un número primo. Sin la conjetura, sólo podemos afirmar que los cocientes N_i/N_{i-1} son primos o productos de dos primos, y en el segundo caso (para los primos $p < q$), hay dos números altamente compuestos comprendidos entre N_{i-1} y N_i, a saber, $N_{i-1} < N_{i-1}p < N_{i-1}q < N_i$. Sin embargo, es muy poco probable que pueda darse este caso.

Una última observación es que si al calcular los ϵ_i recordamos con qué valores $F(p, e)$ se genera cada uno, el cálculo de los N_i se reduce a ir multiplicando los primos p. Por ejemplo, $\epsilon_1 = F(2, 1) \in E_2$, $\epsilon_2 = F(3, 1) \in E_3$, $\epsilon_3 = F(2, 2) \in E_2$, $\epsilon_4 = F(5, 1) \in E_5$, etc., lo que se traduce en que la sucesión de los N_i es

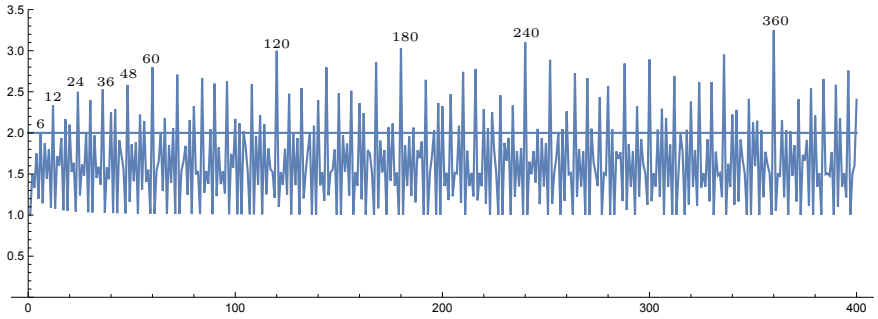
$$1, \quad 2, \quad 2 \cdot 3, \quad 2 \cdot 3 \cdot 2, \quad 2 \cdot 3 \cdot 2 \cdot 5, \quad \ldots$$

8.3 Números abundantes y superabundantes

Los antiguos griegos dividieron los números entre *deficientes, perfectos* y *abundantes*, según si la suma de sus divisores propios es inferior, igual o superior al propio número, respectivamente.[5]

[5] Véase la sección [ITAl 3.5] para una discusión de los números perfectos.

Recordemos que la función σ es la que a cada número natural le asigna la suma de sus divisores. En términos de σ, un número n es deficiente, perfecto o abundante según si $\sigma(n)$ es menor, igual o mayor que $2n$ (porque en $\sigma(n)$ se suma también el propio n). Equivalentemente, según si $\sigma(n)/n$ es menor, igual o mayor que 2.



La gráfica muestra la función $\sigma(n)/n$, de modo que podemos apreciar cómo se distribuyen los números deficientes, perfectos y abundantes. Los números en los que $\sigma(n)/n$ toma un valor mayor que cualquier otro anterior se llaman[6] *superabundantes.*

Observación Podríamos dar nombre a los números para los que $\sigma(n)/n$ es menor que en cualquier número anterior, pero dichos números son simplemente los primos. En efecto, si n cumple esto y no es primo, tiene un factor primo $p \le \sqrt{n}$, luego $n/p \ge \sqrt{n}$, luego

$$\frac{\sigma(n)}{n} \ge \frac{n+n/p}{n} \ge \frac{n+\sqrt{n}}{n} = 1 + \frac{1}{\sqrt{n}}.$$

Por otra parte, es fácil ver que si $n \ge 4$, entonces $2\sqrt{n} \le n$, por lo que el postulado de Bertrand nos da un primo $\sqrt{n} \le p < n$ (la desigualdad es estricta porque n no es primo), y entonces

$$\frac{\sigma(p)}{p} = 1 + \frac{1}{p} \le 1 + \frac{1}{\sqrt{n}} \le \frac{\sigma(n)}{n},$$

contradicción. ∎

Los primeros números abundantes son

$$12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96, 100\ldots$$

Los números perfectos son más escasos: $6, 28, 496, 8\,128, \ldots$

Los primeros números superabundantes son $1, 2, 4, 6, 12, \ldots$ Es obvio que, una vez superado el 6 (el primer número perfecto) es decir, a partir del 12, los números superabundantes son abundantes.

[6] Ramanujan los llamó números altamente compuestos generalizados, pero Erdős los llamó superabundantes y actualmente se conocen con este nombre.

Los 19 primeros números superabundantes (hasta $7! = 5\,040$) coinciden con los 19 primeros números altamente compuestos, pero el siguiente número altamente compuesto (7 560) no es superabundante, mientras que 1 163 962 800 es el menor número superabundante que no es altamente compuesto.

Todo múltiplo de un número abundante es abundante, pues si n es abundante, entonces

$$2kn < \sum_{d|n} kd \leq \sum_{d|kn} d.$$

Parece que los números abundantes tengan que ser pares, pero no es así. El primer número abundante impar es 945. Otra conjetura falsa sobre los números superabundantes es que son múltiplos de la suma de sus cifras. El primer contraejemplo es 149 602 080 797 769 600.

Pese a que, como hemos indicado, los números superabundantes no tienen por qué ser altamente compuestos ni viceversa, ambas clases de números comparten muchas propiedades. Por ejemplo:

Teorema 8.15 *Si $n \geq 2$ es un número superabundante, entonces factoriza en la forma $n = 2^{e_2} \cdot 3^{e_3} \cdots p_r^{e_{p_r}}$, donde $p_1, \ldots, p_r$ son los primeros primos consecutivos y $e_2 \geq e_3 \geq \cdots \geq e_{p_r}$. Además, $e_{p_r} = 1$ salvo si $n = 4, 36$.*

Demostración: Si la sucesión de exponentes no es decreciente, existen dos primos $q < p$ divisores de n cuyos exponentes cumplen $e_q < e_p$. Entonces $n' = nq/p < n$, luego $\sigma(n')/n' < \sigma(n)/n$. Al aplicar que σ es multiplicativa y simplificar los factores correspondientes a primos distintos de q, p, esta desigualdad se reduce a

$$\frac{q^{e_q+2}-1}{q^{e_q+2}-q} < \frac{p^{e_p+1}-1}{p^{e_p+1}-p}.$$

No es difícil comprobar que la función $(x^n-1)/(x^n-x)$ tiene derivadas parciales (respecto de n y x) negativas para $x, n \geq 2$, lo que nos da que

$$\frac{q^{e_q+2}-1}{q^{e_q+2}-q} \geq \frac{q^{e_p+2}-1}{q^{e_p+2}-q} \geq \frac{p^{e_p+1}-1}{p^{e_p+1}-p},$$

con lo que tenemos una contradicción.

Supongamos ahora que $e_r \geq 2$. Si $r = 1$, es decir, si $n = 2^e$, consideramos $n' = n3/4 < n$, y al simplificar $\sigma(n')/n' < \sigma(n)/n$ obtenemos

$$\frac{(2^{e-1}-1)4}{3} < \frac{2^{e+1}-1}{4},$$

de donde llegamos a que $2^{e+1} < 13$, luego $e \leq 2$, y tiene que ser $n = 4$.

Así pues, podemos suponer que $r \geq 2$. Llamamos $q = p_{r-1}$, $p = p_r$, $t = p_{r+1}$, de modo que $n' = nt/pq < n$, pues, por el postulado de Bertrand,

$$\frac{t}{pq} < \frac{2p}{pq} = \frac{2}{q} < 1$$

si $q \geq 3$, pero si $q = 2$ también es cierto: $t/pq = 5/6 < 1$. Por consiguiente, $\sigma(n')/n' < \sigma(n)/n$. Al simplificar esta desigualdad obtenemos que

$$1 + \frac{1}{t} < \left(1 + \frac{q-1}{q^{e_q+1} - q}\right)\left(1 + \frac{p-1}{p^{e_p+1} - p}\right).$$

Supongamos en primer lugar que $r = 2$, con lo que $q = 2$, $p = 3$, $t = 5$. Entonces

$$1 + \frac{1}{5} < \left(1 + \frac{1}{2^{e_2+1} - 2}\right)\left(1 + \frac{2}{3^{e_3+1} - 3}\right) \leq \left(1 + \frac{1}{2^{e_2+1} - 2}\right)\left(1 + \frac{2}{3^3 - 3}\right).$$

Operando llegamos a que $2^{e_2+1} < 79/7 \approx 11.3$, luego $e_3 \leq 2$, lo que a su vez implica que $e_2 = e_3 = 2$ y $n = 36$. Ahora supongamos que $r > 2$, luego $q \geq 3$, y acotamos

$$1 + \frac{1}{t} < \left(1 + \frac{q-1}{q^3 - q}\right)\left(1 + \frac{p-1}{p^3 - p}\right) = \left(1 + \frac{1}{q(q+1)}\right)\left(1 + \frac{1}{p(p+1)}\right)$$

$$< \left(1 + \frac{1}{q^2}\right)\left(1 + \frac{1}{p^2}\right).$$

Por otro lado, la desigualdad

$$\left(1 + \frac{1}{q^2}\right)\left(1 + \frac{1}{p^2}\right) \leq 1 + \frac{1}{t}$$

equivale a

$$\frac{1}{q^2} + \frac{1}{p^2} + \frac{1}{q^2p^2} < \frac{1}{t},$$

pero

$$\frac{1}{q^2} + \frac{1}{p^2} + \frac{1}{q^2p^2} \leq \frac{2q^2+1}{q^4}, \qquad \frac{1}{4q} < \frac{1}{t},$$

la última desigualdad por el postulado de Bertrand. Luego si

$$\frac{2q^2+1}{q^3} \leq \frac{1}{4}$$

tenemos una contradicción. Pero esto equivale a que $q^3 - 8q^2 - 4 \geq 0$, y un análisis de esta función muestra que es positiva para $q \geq 9$, o sea, salvo si $q = 3, 5, 7$, pero en estos tres casos podemos comprobar directamente que se cumple

$$\left(1 + \frac{1}{q^2}\right)\left(1 + \frac{1}{p^2}\right) < 1 + \frac{1}{t}$$

e igualmente tenemos una contradicción. ∎

En el caso de los números superabundantes es posible demostrar hechos adicionales. Por ejemplo:

Teorema 8.16 *Si $n = 2^{e_2} \cdot 3^{e_3} \cdots p_r^{e_{p_r}}$ es superabundante y $1 \le i < j \le r$, entonces e_{p_j} toma uno de los valores $k-1, k, k+1$, donde $k = E[e_{p_i} \log p_i / \log p_j]$.*

DEMOSTRACIÓN: Sea m el número natural que cumple $p_i^{m-1} < p_j < p_i^m$. Supongamos que $e_{p_j} \le k-2$, lo que a su vez implica que $m \le e_{p_i}$, pues en caso contrario tendríamos que $p_i^{e_{p_i}} \le p_i^{m-1} < p_j < p_j^{e_{p_j}+2} \le p_j^k \le p_i^{e_{p_i}}$. Por lo tanto, $n' = np_jp_i^{-m} < n$ y tiene que cumplirse que $\sigma(np_jp_i^{-m})/np_jp_i^{-m} < \sigma(n)/n$. Al simplificar esta desigualdad resulta

$$p_j^{e_{p_j}+2}(p_i^m - 1) + p_j > p_i^{e_{p_i}+1}(p_j - 1) + p_i^m,$$

pero por otra parte, teniendo en cuenta que $p_i^{m-1} \le p_j - 1$,

$$p_j^{e_{p_j}+2}(p_i^m - 1) + p_j \le p_j^k(p_i^m - 1) + p_i^m \le p_i^{e_{p_i}}(p_ip_j - p_j - 1) + p_i^m$$

$$< p_i^{e_{p_i}}(p_ip_j - p_i) + p_i^m < p_i^{e_{p_i}+1}(p_j - 1) + p_i^m.$$

Si $e_{p_j} \ge k+2$ consideramos $n' = p_i^{m-1}p_j^{-1}n < n$ y llegamos a

$$p_j^{e_{p_j}+1}(p_i^{m-1} - 1) + p_j < p_i^{e_{p_i}+m}(p_j - 1) + p_i^{m-1}.$$

Por otra parte

$$p_i^{e_{p_i}+m}(p_j - 1) + p_i^{m-1} \le p_j^{k+1}p_i^m(p_j - 1) + p_j \le p_j^{e_{p_j}-1}p_i^m(p_j - 1) + p_j,$$

luego tendremos una contradicción si probamos que

$$p_j^{e_{p_j}-1}p_i^m(p_j - 1) + p_j \le p_j^{e_{p_j}+1}(p_i^{m-1} - 1) + p_j,$$

lo que equivale a

$$p_i^m(p_j - 1) \le p_j^2(p_i^{m-1} - 1).$$

Si llamamos $P = p_i^{m-1}$ y $p = p_i$, tenemos que $P \ge p \ge 2$ y $P < p_j < pP$, y se trata de probar que la función

$$F(t) = (P-1)t^2 - pPt + pP$$

es ≥ 0 en el intervalo $[P, pP]$. Ahora bien, se trata de una parábola con vértice en $t = \frac{pP}{2(P-1)} \ge P$, pues $p \ge 2$ implica que $p \le 2(p-1) \le 2(P-1)$. Así pues, $F(t)$ es creciente en $[P, +\infty[$, y basta observar que

$$F(P) = (P-1)P^2 - pP^2 + pP = P(P-1)(P-p) \ge 0.$$

■

El teorema anterior limita sustancialmente las factorizaciones de los números superabundantes, pero todavía podemos decir más:

Teorema 8.17 *$n = 2^{e_2} \cdot 3^{e_3} \cdots p_r^{e_{p_r}}$ es superabundante, entonces $p_j^{e_{p_j}} < 2^{e_2+2}$.*

DEMOSTRACIÓN: Aplicamos el teorema anterior con $i = 2$. Si se cumple $e_{p_j} \le k = E[e_2 \log 2/\log p_j]$, trivialmente $p_j^{e_{p_j}} \le 2^{e_2}$, luego podemos suponer que $e_{p_j} = k + 1$. Si fuera $2^{e_2+2} < p_j^{e_{p_j}}$, consideramos el número m tal que $2^{m-1} < p_j < 2^m$ y $n' = n2^{m-1}/p_j < n$. Como en la prueba del teorema anterior, la condición $\sigma(n')/n' < \sigma(n)/n$ se simplifica hasta

$$p_j^{e_{p_j}+1}(2^{m-1}-1) + p_j < 2^{e_2+m}(p_j - 1) + 2^{m-1},$$

y por otra parte

$$2^{e_2+m}(p_j-1) + 2^{m-1} \le p_j^{e_{p_j}} 2^{m-2} p_j + p_j \le p_j^{e_{p_j}+1}(2^{m-1}-1),$$

luego tenemos una contradicción. ∎

Vemos así que sólo hay un número finito de números superabundantes con un exponente e_2 dado.

Nota Una última observación elemental es que, al igual que sucede con los números altamente compuestos, el cociente entre dos números superabundantes consecutivos es menor o igual que 2, pues

$$\frac{\sigma(2n)/2n}{\sigma(n)/n} = \frac{2^{e_2+2}-1}{2^{e_2+2}-2} > 1,$$

luego el menor número superabundante mayor que n es menor o igual que $2n$. ∎

8.4 Números colosalmente abundantes

Ramanujan llamó números altamente compuestos generalizados superiores a una familia de números análoga a la de los números altamente compuestos superiores, pero respecto de los números superabundantes. Actualmente estos números se conocen con el nombre que les dio Erdős, que es el que da título a esta sección. Para definirlos observamos que, para todo $\epsilon > 0$, se cumple que

$$\lim_n \frac{\log\log n}{n^\epsilon} = 0,$$

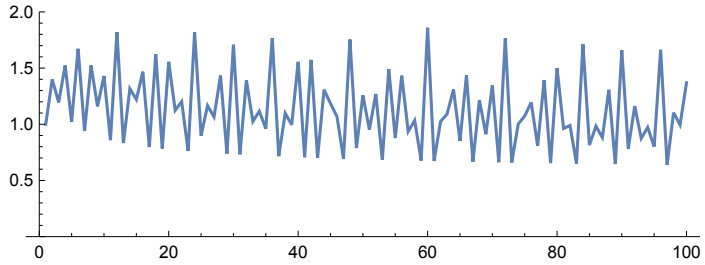
por lo que, teniendo en cuenta el teorema 3.30,

$$\lim_n \frac{\sigma(n)}{n^{1+\epsilon}} = \lim_n \frac{\sigma(n)}{n\log\log n}\frac{\log\log n}{n^\epsilon} = 0,$$

pues el primer factor está acotado. Por lo tanto, la sucesión $\sigma(n)/n^{1+\epsilon}$ alcanza un valor máximo.

Definición 8.18 Un número natural N es *colosalmente abundante* si existe un $\epsilon > 0$ tal que la sucesión $\sigma(n)/n^{1+\epsilon}$ alcanza un valor máximo en N.

Por ejemplo, ésta es la gráfica de la sucesión $\sigma(n)/n^{1.1}$, que alcanza su valor máximo en $n = 60$:



Como en el caso de los números altamente compuestos superiores, la gráfica no prueba que 60 sea colosalmente abundante, pero enseguida veremos que la situación es idéntica: es fácil generar la sucesión de los números colosalmente abundantes.

Observemos que todo número colosalmente abundante N es superabundante, pues si $n < N$ tenemos que

$$\frac{\sigma(n)}{n^{1+\epsilon}} \leq \frac{\sigma(N)}{N^{1+\epsilon}},$$

luego

$$\frac{\sigma(n)}{n} \leq \frac{\sigma(N)}{N}\left(\frac{n}{N}\right)^{\epsilon} < \frac{\sigma(N)}{N}.$$

Por otra parte, si N es colosalmente abundante y $p \mid N$, aplicamos la definición a $N' = N/p$, con lo que

$$\frac{\sigma(N')}{N'^{1+\epsilon}} \leq \frac{\sigma(N)}{N^{1+\epsilon}}.$$

Al desarrollar esta desigualdad se reduce a

$$\frac{p^{e_p}-1}{p^{(e_p-1)(1+\epsilon)}} \leq \frac{p^{e_p+1}-1}{p^{e_p(1+\epsilon)}},$$

y operando llegamos a

$$\epsilon \leq \frac{\log\left(\frac{p^{e_p+1}-1}{p^{e_p+1}-p}\right)}{\log p}.$$

Similarmente, si p es un primo cualquiera y $N' = Np$, la definición de número colosalmente abundante se reduce a

$$\frac{p^{e_p+2}-1}{p^{(e_p+1)(1+\epsilon)}} \leq \frac{p^{e_p+1}-1}{p^{e_p(1+\epsilon)}},$$

y al despejar queda

$$\epsilon \geq \frac{\log\left(\frac{p^{e_p+2}-1}{p^{e_p+2}-p}\right)}{\log p}.$$

Esto nos lleva a las definiciones siguientes:

Definición 8.19 Consideramos la función

$$F(p,e) = \frac{\log \frac{p^{e+1}-1}{p^{e+1}-p}}{\log p},$$

para $p \geq 2$ y $e > 0$, con el convenio de que $F(p,0) = +\infty$. Más aún, observemos que

$$F(p,e) = \frac{\log(1 + \frac{p-1}{p(p^e-1)})}{\log p} = \frac{\log(1 + \frac{1}{p+p^2+\cdots+p^e})}{\log p}.$$

La última expresión muestra que la función $p \mapsto F(p,e)$ es estrictamente decreciente, y una comprobación rutinaria nos da que biyecta el intervalo $]1,+\infty[$ con $]0,+\infty[$. También es claro que la sucesión $e \mapsto F(p,e)$ decrece hacia 0, para $e = 0, 1, 2, 3\ldots$

En estos términos, hemos probado que si N es colosalmente abundante (respecto de ϵ) y p es un primo cualquiera, entonces $F(p, e_p + 1) \leq \epsilon \leq F(p, e_p)$.

Para cada primo p definimos el conjunto

$$E_p = \{F(p,e) \mid e \geq 1\},$$

y llamamos $E = \bigcup_p E_p$. Como $F(p,e)$ decrece cuando crece cualquiera de sus argumentos, es claro que los elementos de E forman una sucesión decreciente $\epsilon_1 > \epsilon_2 > \epsilon_3 > \ldots$ convergente a 0. Definimos además $\epsilon_0 = +\infty$.

Observemos que si $\epsilon \in E_p$ entonces

$$p^\epsilon = 1 + \frac{1}{p + p^2 + \cdots + p^e} \in \mathbb{Q},$$

luego, por el mismo argumento empleado en el caso de los números altamente compuestos superiores, la conjetura de las cuatro exponenciales implica que los conjuntos E_p son disjuntos dos a dos y, en su defecto, el teorema de las seis exponenciales garantiza que un mismo $\epsilon > 0$ pertenece a lo sumo a dos conjuntos E_p, E_q.

Si $\epsilon > 0$ no está en E y N es colosalmente abundante respecto de ϵ, entonces $F(p, e_p + 1) < \epsilon < F(p, e_p)$, lo cual equivale a

$$\frac{\log \frac{p^{1+\epsilon}-1}{p^\epsilon-1}}{\log p} - 1 < e_p - 1 < \frac{\log \frac{p^{1+\epsilon}-1}{p^\epsilon-1}}{\log p}.$$

A partir de aquí la situación es formalmente idéntica a la que hemos encontrado al estudiar los números altamente compuestos superiores. El teorema siguiente se demuestra exactamente con los mismos razonamientos, sin más que cambiar las definiciones del conjunto E y la función F:

Teorema 8.20 *Sea $\epsilon > 0$.*

1. *Si $\epsilon \notin E$, la función $\sigma(n)/n^{1+\epsilon}$ alcanza su máximo en un único número N_ϵ, cuya descomposición en factores primos es $N_\epsilon = \prod_p p^{e_p(\epsilon)}$, con*

$$e_p(\epsilon) = E\left[\frac{\log((p^{1+\epsilon}-1)/(p^\epsilon-1))}{\log p}\right] - 1.$$

2. *Para cada $i \geq 1$, todos los $\epsilon \in]\epsilon_{i+1}, \epsilon_i[$ determinan un mismo número N_ϵ, al que llamaremos también N_i.*

3. *Si los conjuntos E_p son disjuntos dos a dos, entonces todo número colosalmente abundante es de la forma N_i. La función $\sigma(n)/n^{1+\epsilon_i}$ alcanza su máximo en dos puntos, N_i y N_{i+1}.*

4. *Si $\epsilon_i \in E_p \cap E_q$, entonces la función $\sigma(n)/n^{1+\epsilon_i}$ alcanza su máximo en cuatro puntos, N_i, pN_i, qN_i, $qrN_i = N_{i+1}$ (y los cuatro son colosalmente abundantes).*

La tabla siguiente contiene los números colosalmente abundantes correspondientes a $\epsilon_i > 0.04$ (aunque se ha impuesto el convenio de no considerar al 1 como colosalmente abundante):

i	ϵ_i	N_i	Factorización	Fact. en primoriales
0	$+\infty$	1		
1	0.58496	2	2	$2\#$
2	0.26186	6	$2 \cdot 3$	$3\#$
3	0.22239	12	$2^2 \cdot 3$	$3\# \cdot 2\#$
4	0.11328	60	$2^2 \cdot 3 \cdot 5$	$5\# \cdot 2\#$
5	0.09953	120	$2^3 \cdot 3 \cdot 5$	$5\# \cdot 2\# \cdot 2\#$
6	0.07285	360	$2^3 \cdot 3^2 \cdot 5$	$5\# \cdot 3\# \cdot 2\#$
7	0.06862	2 520	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	$7\# \cdot 3\# \cdot 2\#$
8	0.04730	5 040	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$7\# \cdot 3\# \cdot 2\# \cdot 2\#$

Vemos que coinciden con los primeros números altamente compuestos superiores, sin embargo, la coincidencia termina en N_{15}, pues el decimosexto número colosalmente abundante es

$$N_{16} = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23,$$

mientras que el decimosexto número altamente compuesto superior es

$$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$

Índice de Materias