Universidad Autónoma de Madrid
Facultad de Ciencias
Departamento de Matemáticas

Espacios pequeños entre primos

dirigido por Fernando Chamizo

Carlos Vinuesa del Río

2006

Introducción

En 2005 Daniel Alan Goldston, János Pintz y Cem Yalçın Yıldırım hicieron un sensacional descubrimiento en el estudio de los números primos. Probaron que hay infinitos números primos para los que el espacio hasta el siguiente primo es tan pequeño como queramos comparado con el espacio medio entre primos consecutivos.

Veamos con más detalle qué quiere decir esto. En primer lugar, acordemos que p denotará a partir de ahora un número primo y p_n el primo n-ésimo (es decir $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...). Además, $\pi(x) = |\{p : p \leq x\}|$, o sea, el número de primos menores o iguales que x.

La historia comienza en 1793. Gauss, que contaba con 16 años de edad, observó, estudiando tablas de los números primos hasta 3 millones, que "el número de primos hasta x es aproximadamente $x/\log x$". Con más rigor

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

y eso no es otra cosa que el teorema del número primo, demostrado cien años después, en 1896, por Hadamard y de la Vallée Poussin haciendo uso de la función zeta de Riemann. En 1949, Selberg y Erdös encontraron una prueba elemental (evitaba el uso del análisis complejo) de este mismo hecho, aunque quizá sea preciso decir que esta prueba era muy complicada y estaba menos motivada que la analítica.

De una forma u otra, la moraleja que podemos sacar del teorema es que si miramos a los primos que están cerca de x el espacio medio entre primos consecutivos es más o menos $\log x$. Uno puede preguntarse si habrá espacios entre primos consecutivos significativamente más grandes o significativamente más pequeños que el espacio medio. Esto es, uno puede preguntarse si se cumplen

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty \tag{1}$$

y

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0. \tag{2}$$

Para los impacientes, podemos decir que ambas cosas son ciertas, pero cada una tiene su historia.

Probar (1) es más fácil. En la década de 1930 Westzynthius, Erdös y Rankin escribieron ingeniosos artículos en los que mostraban cadenas largas de números compuestos, demostrando todos ellos estimaciones más fuertes que (1). Haciendo honor a su nombre, Rankin (en 1938) se convirtió en el primero del "ranking", al obtener la mejor estimación. Probó que existe una constante positiva c tal que

$$\frac{p_{n+1}-p_n}{\log p_n} > c\frac{(\log\log p_n)(\log\log\log\log p_n)}{(\log\log\log p_n)^2}$$

se cumple para infinitos valores de n. Como la fracción de la derecha tiende a ∞ con n (aunque muy muy despacio), esto implica obviamente (1). En los últimos 68 años, sólo se ha mejorado el valor de c, pero salvo por el valor de la constante la estimación de Rankin sigue siendo la mejor. Paul Erdös ofreció 10.000 $ a quien demostrara que se puede hacer tender $c \to \infty$ en este resultado (aunque los "cazarrecompensas" deberían saber que el mayor premio de Erdös que se ha recogido fueron los 1.000 $ que cobró Szemerédi por su maravilloso resultado sobre la existencia de progresiones aritméticas arbitrariamente largas en conjuntos de densidad positiva). Lo que se conjetura es que

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^2} = c$$

donde c es una constante mayor que 1 (que no tiene nada que ver con la c anterior, vayamos acostumbrándonos a estas cosas...).

Pero el título de este capítulo no es "Espacios grandes entre primos", por lo que nos centraremos en (2). El teorema del número primo nos decía que el espacio medio entre p_n y p_{n+1} es como $\log p_n$, por lo que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \leq 1$$

por el mismo motivo que si todo el mundo cobrara más que el salario medio entonces el salario medio sería mayor.

En 1940, Erdös probó que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} < 1.$$

En 1965, Bombieri y Davenport probaron que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \leq 0,4665\ldots$$

En 1977, Huxley probó que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \leq 0,4349\ldots$$

En 1988, Maier probó que

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \leq 0,2484\ldots$$

y esto era lo mejor que se sabía desde entonces... hasta el año pasado.

Es decir, después de tantos años, sólo se sabía que había infinitos espacios entre primos que medían aproximadamente 1/4 del espacio medio, lo que resulta un poco patético si creemos que existen infinitos espacios de longitud 2, como nos dice la conjetura de los primos gemelos.

Y aquí es donde entran Goldston, Pintz y Yildirim, que en 2005 nos sorprendieron demostrando la conjetura que se había resistido durante tantos años:

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0.$$

Probar este resultado será nuestro objetivo.

En otras palabras, como anunciábamos al principio de la introducción, probaremos que existen infinitas parejas de primos que distan infinitamente menos que la distancia media entre primos consecutivos.

Pero aún así uno puede pensar en ir más allá. De todas formas, pese a lo espectacular del resultado anterior, nos puede seguir pareciendo un poco pobre el hecho de que todavía seguimos sin saber si existe una constante d tal que la diferencia $p_{n+1}-p_n \leq d$ para infinitos valores de n. De manera que esperamos que haya infinitas parejas de primos que disten 2 y ¡ni siquiera sabemos que existan infinitas parejas que disten menos que mil millones!

Pues bien, veremos también la forma en que Goldston, Pintz y Yıldırım han probado que asumiendo cierta conjetura (es verdad que la conjetura es difícil, y ahí está el truco) sobre la distribución de los primos en progresiones aritméticas tendríamos $p_{n+1}-p_n \leq 20$ para infinitos valores de n. Esto implicaría inmediatamente que $p_{n+1}-p_n = d$ en infinitas ocasiones para algún d que podría ser 2, 4, 6, 8, 10, 12, 14, 16, 18 o 20. El problema, aparte de que no sabemos probar la conjetura sobre la distribución de los primos en progresiones aritméticas, es que no sabemos cuál de esas 10 diferencias sería la que se repetiría en infinitas ocasiones. ¿Y si fuera la diferencia 2? ¡Entonces tendríamos la conjetura de los primos gemelos! Pero dejemos de soñar y comencemos ya...

Capítulo 1

El lema básico

En este primer capítulo vamos a probar una fórmula asintótica, que modificaremos en el segundo capítulo para incluir de alguna manera a los primos. Combinando las dos fórmulas asintóticas en un argumento de criba con pesos demostraremos nuestro resultado en el tercer capítulo. Finalmente, en el cuarto capítulo veremos cómo una mejora del teorema de Bombieri-Vinogradov nos daría la existencia de infinitas diferencias acotadas entre primos.

Comenzamos definiendo algunas cosas. Sea N un parámetro que crece monótonamente hacia infinito. Sean R y H tales que[1]

$$H \ll \log N \ll \log R \leq \log N. \tag{1.1}$$

Sean también

$$k, l > 0 \text{ dos enteros positivos arbitrarios pero acotados.} \tag{1.2}$$

En lo que sigue, todas las constantes implícitas dependen a lo sumo de k y de l. Además, escribiremos c para representar una constante positiva con la misma dependencia y el valor de c puede ser distinto en cada aparición.

Sea

$$\mathcal{H} = \{h_1, h_2, \ldots, h_k\} \subseteq [1, H] \cap \mathbb{Z},$$

[1] Probablemente todas las personas interesadas en leer este trabajo conozcan sobradamente las notaciones que explicaremos a continuación. Pero quizá haya alguien que sólo quiera leer esta nota...

Cuando desconocemos la forma exacta de un término o sólo nos interesa tener una idea de su tamaño, empleamos las notaciones de Landau siguientes:

- "$f(x) = o(g(x))$ cuando $x \to a$" significa $\lim_{x\to a} \frac{|f(x)|}{|g(x)|} = 0$
- "$f(x) = O(g(x))$ cuando $x \to a$" significa $\limsup_{x\to a} \frac{|f(x)|}{|g(x)|} = C < \infty$ (sí, una o también es una O)

La notación de Vinogradov "$f(x) \ll g(x)$ cuando $x \to a$" significa lo mismo que "$f(x) = O(g(x))$ cuando $x \to a$". Emplearemos una u otra según nos interese.

Obsérvese que $f \ll g$ no implica $f \leq g$. Un ejemplo es nuestro caso, $\log N \ll \log R \leq \log N$, donde podemos pensar en $R = N^\alpha$ para cierto $0 < \alpha < 1$.

donde $h_i \neq h_j$ si $i \neq j$. Para cada primo, p, definimos

$$\Omega(p) = \{\text{diferentes clases residuales que ocupan los } -h \pmod p, h \in \mathcal{H}\}$$

y escribiremos $n \in \Omega(p)$ en lugar de $n \pmod p \in \Omega(p)$. Decimos que $\mathcal{H}$ es admisible si

$$|\Omega(p)| < p \quad \text{para todo } p, \tag{1.3}$$

y supondremos también que $\mathcal{H}$ es admisible, salvo que se diga lo contrario[2]. Además, vamos a extender Ω a los números libres de cuadrados de la siguiente forma:

$$n \in \Omega(d) \text{ con } d \text{ libre de cuadrados} \Leftrightarrow n \in \Omega(p) \text{ para todo } p|d.$$

Observemos varias cosas. La primera es que si d es primo la definición coincide con la que ya teníamos. La segunda, si $d = p_1 p_2 \dots p_r$,

$$n \in \Omega(d) \Leftrightarrow \begin{cases} n \equiv -h_{i_1} \pmod{p_1} & \text{para algún } 1 \leq i_1 \leq k \\ n \equiv -h_{i_2} \pmod{p_2} & \text{para algún } 1 \leq i_2 \leq k \\ \dots & \\ n \equiv -h_{i_r} \pmod{p_r} & \text{para algún } 1 \leq i_r \leq k \end{cases} \tag{1.4}$$

$$\Leftrightarrow d|(n+h_1)(n+h_2)\cdots(n+h_k). \tag{1.5}$$

Por último, el teorema chino del resto[3] nos dice que la extensión es multiplicativa en el sentido de que

$$|\Omega(d)| = |\Omega(p_1)||\Omega(p_2)|\cdots|\Omega(p_r)|. \tag{1.6}$$

Definimos, con μ la función de Möbius[4] (a es un entero positivo),

$$\lambda_R(d;a) = \begin{cases} 0 & \text{si } d > R \\ \frac{1}{a!}\mu(d)\left(\log\left(\frac{R}{d}\right)\right)^a & \text{si } d \leq R \end{cases}$$

[2]Imponer esta condición es natural. En principio (aunque luego nos conformaremos con algo menos) al definir $\mathcal{H} = \{h_1, \dots, h_k\}$ buscamos que todos los números $n + h_1$, $\dots$, $n + h_k$ sean primos para infinitos valores de n. Si $-h_1$, $\dots$, $-h_k$ ocuparan todas las clases módulo algún primo, p, entonces para todo n tendríamos que alguno de los números $n + h_1$, $\dots$, $n + h_k$ es múltiplo de p.

[3]El teorema chino del resto dice que si $(n, m) = 1$ (la notación (n, m) representa el máximo común divisor de n y m) y se cumplen las dos ecuaciones $x \equiv a \pmod n$ y $x \equiv b \pmod m$ entonces existe una única solución al sistema, $x \pmod{nm}$. Así, si nos fijamos en la expresión de $n \in \Omega(d)$ como sistema de congruencias (1.4) y tenemos en cuenta que además en nuestro caso los módulos son primos distintos cuyo producto es d, llegamos a la igualdad (1.6). Al igual que en el caso de un primo, $n \in \Omega(d)$ puede ser visto como una clase módulo d.

[4]La función μ de Möbius es

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n = p_1 p_2 \cdots p_r \text{ (primos distintos)} \\ 0 & \text{en otro caso} \end{cases}$$

luego si $d > 1$ no es libre de cuadrados entonces $\lambda_R(d;a) = 0$.

y

$$\Lambda_R(n;\mathcal{H},a)=\sum_{\substack{d\\ n\in\Omega(d)}}\lambda_R(d;a)=\frac{1}{a!}\sum_{\substack{d|(n+h_1)\cdots(n+h_k)\\ d\le R}}\mu(d)\left(\log\left(\frac{R}{d}\right)\right)^a \quad (1.7)$$

donde en la última igualdad hemos usado (1.5).

Con todo esto, evaluaremos la suma

$$\sum_{N<n\le 2N}\Lambda_R(n;\mathcal{H},k+l)^2 \quad (1.8)$$

que es igual a

$$\sum_{N<n\le 2N}\sum_{\substack{d_1\\ n\in\Omega(d_1)}}\lambda_R(d_1;k+l)\sum_{\substack{d_2\\ n\in\Omega(d_2)}}\lambda_R(d_2;k+l)$$

$$=\sum_{d_1,d_2}\lambda_R(d_1;k+l)\lambda_R(d_2;k+l)\sum_{\substack{N<n\le 2N\\ n\in\Omega(d_1),n\in\Omega(d_2)}}1$$

y teniendo en cuenta que $d_1|(n+h_1)\cdots(n+h_k)$ y $d_2|(n+h_1)\cdots(n+h_k)\Leftrightarrow [d_1,d_2]|(n+h_1)\cdots(n+h_k)$, donde la notación $[n,m]$ representa el mínimo común múltiplo de n y m,

$$=\sum_{d_1,d_2}\lambda_R(d_1;k+l)\lambda_R(d_2;k+l)\sum_{\substack{N<n\le 2N\\ n\in\Omega([d_1,d_2])}}1.$$

Si dividimos el intervalo $(N,2N]$ en trocitos que midan $[d_1,d_2]$ entonces en cada intervalito sumamos

$$\sum_{d_1,d_2}|\Omega([d_1,d_2])|\lambda_R(d_1;k+l)\lambda_R(d_2;k+l)$$

y como hay $N/[d_1,d_2]$ intervalitos, si ponemos

$$\mathcal{T}=\sum_{d_1,d_2}\frac{|\Omega([d_1,d_2])|}{[d_1,d_2]}\lambda_R(d_1;k+l)\lambda_R(d_2;k+l)$$

la suma (1.8) es

$$N\mathcal{T}+O\left(\left(\sum_d|\Omega(d)||\lambda_R(d;k+l)|\right)^2\right).$$

El término de error viene del último intervalito, que podría no estar completo y aporta entre 0 y $\sum_{d_1,d_2}|\Omega([d_1,d_2])||\lambda_R(d_1;k+l)||\lambda_R(d_2;k+l)|$. Ahora bien,

por (1.6) esto es $\leq \sum_{d_1,d_2} |\Omega(d_1)||\Omega(d_2)||\lambda_R(d_1;k+l)||\lambda_R(d_2;k+l)|$ que es lo que hay dentro de la O.

A continuación afirmamos que $|\Omega(d)| \leq \tau_k(d)$ para d libre de cuadrados (si no, $\Omega(d)$ no está definido). Aquí, $\tau_k(m)$ es la función "número de formas de poner m como producto de k factores"[5] y está definida para todo $m \geq 1$, no sólo para los libres de cuadrados. El "truco" para darse cuenta de que esta función acota a $|\Omega(d)|$ es mirar a la expresión de $n \in \Omega(d)$ como sistema de congruencias (1.4). A cada sistema de congruencias le asignamos la descomposición de d que tiene los k factores siguientes (en este orden):

⊛ factor 1: producto de los p_i tales que $n \equiv -h_1 \pmod{p_i}$

⊛ factor 2: producto de los p_i tales que $n \equiv -h_2 \pmod{p_i}$

...

⊛ factor k: producto de los p_i tales que $n \equiv -h_k \pmod{p_i}$.

Puede que algunos sistemas nos den el mismo $n \in \Omega(d)$ (basta con que existan $i \neq j$ tales que $h_i \equiv h_j \pmod{p}$ para alguno de los primos que dividen a d) pero lo que seguro que es cierto es que dado un $n \in \Omega(d)$ tenemos al menos un sistema y, por tanto, una descomposición. Eso demuestra nuestra afirmación.

Luego para acotar el término de error nos va a interesar acotar $\sum_{d\leq R} \tau_k(d)$. Consideraremos para ello la función zeta de Riemann, que en el semiplano $\Re s > 1$ está definida por $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Cuando $s \to 1$ tenemos $\zeta(s) \ll \frac{1}{s-1}$. Si nos fijamos,

$$\zeta^k(s) = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)^k = \sum_{n=1}^{\infty} \frac{\tau_k(n)}{n^s}$$

pues al elevar la suma central a la potencia k sumamos $1/m^s$ tantas veces como podemos poner m como producto de k factores (es más fácil pensarlo que escribirlo). Si tomamos $s = 1 + 1/\log x$, que tiende a 1 cuando $x \to \infty$ y tenemos en cuenta que $\zeta^k(s) \ll \frac{1}{(s-1)^k}$ podemos escribir (siempre cuando $x \to \infty$):

$$(\log x)^k \gg \zeta^k(1 + 1/\log x) = \sum_{n=1}^{\infty} \frac{\tau_k(n)}{n^{1+1/\log x}} \gg \sum_{x/2<n\leq x} \frac{\tau_k(n)}{x}$$

donde en el último paso hemos aplicado $x^{1/\log x} = e$. De aquí

$$\sum_{x/2<n\leq x} \tau_k(n) \ll x(\log x)^k$$

[5]Ojo, aquí sí que importa el orden de los factores, si cambia el orden es otra forma distinta. Así, por ejemplo, un primo p se puede poner de k formas como producto de k factores: $p11\cdots11$, $1p1\cdots11$, ..., $111\cdots1p$. Esto no es ningún problema, de hecho es mucho más fácil calcular esta función que la que considera iguales las factorizaciones en las que sólo cambia en orden.

y dando a x el valor $x/2$

$$\sum_{x/4<n\leq x/2} \tau_k(n) \ll \frac{x}{2}\left(\log\left(\frac{x}{2}\right)\right)^k \ll \frac{x}{2}(\log x)^k$$

y dando a x el valor $x/4$

$$\sum_{x/8<n\leq x/4} \tau_k(n) \ll \frac{x}{4}(\log x)^k$$

y así sucesivamente. Por lo tanto

$$\sum_{n\leq x} \tau_k(n) = \sum_{m=1}^{\infty}\left(\sum_{x/2^m<n\leq x/2^{m-1}} \tau_k(n)\right) \ll \sum_{m=1}^{\infty} \frac{x}{2^{m-1}}(\log x)^k \ll x(\log x)^k$$

que es la acotación que buscábamos para τ_k en media.

Podemos dar ahora una cota para el término de error, pues

$$\sum_d |\Omega(d)||\lambda_R(d;k+l)| \leq (\log R)^a \sum_{d\leq R} |\Omega(d)| \ll R(\log R)^c$$

implica que

$$O\left(\left(\sum_d |\Omega(d)||\lambda_R(d;k+l)|\right)^2\right) \ll R^2(\log R)^c$$

y así la suma (1.8) es

$$\sum_{N<n\leq 2N} \Lambda_R(n;\mathcal{H},k+l)^2 = N\mathcal{T} + O(R^2(\log R)^c). \tag{1.9}$$

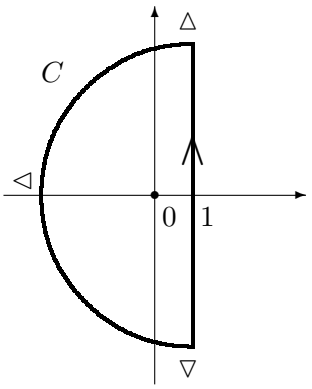
Vayamos ahora al libro de variable compleja, que nos dice que si tenemos una función analítica, basta con conocerla en una curva cerrada simple para conocerla, a ella o a cualquiera de sus derivadas, en cualquier punto interior a la curva. Es decir, en contra de lo que suele pasar, con las funciones analíticas sí que podemos ser "superficiales", no encontraremos nada en el interior que no supiéramos ya al mirarlas por fuera[6].

Cogiendo $f(s) = \left(\frac{R}{d}\right)^s$ (su derivada a-ésima es $f^{(a)}(s) = \left(\frac{R}{d}\right)^s \left(\log\left(\frac{R}{d}\right)\right)^a$) y el contorno C de la figura (observemos que el 0 está en el interior del contorno)

[6]Como se podía esperar, este discurso filosófico merece una nota con símbolos "feos" que lo justifique. El teorema que formaliza lo expuesto es el siguiente:

TEOREMA: *Sea f analítica en la frontera y en el interior de un contorno cerrado simple C orientado positivamente y sea z_0 un punto interior a C. Entonces (acordando $f^{(0)}(z) = f(z)$ y $0! = 1$)*

$$f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_C \frac{f(z)}{(z-z_0)^{n+1}}dz \quad n = 0, 1, 2\ldots$$



tenemos que para todo $a \geq 1$ y $d \leq R$

$$\frac{1}{a!}\left(\log\left(\frac{R}{d}\right)\right)^a = \frac{1}{2\pi i}\int_C \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}}$$

o sea

$$\lambda_R(d;a) = \frac{\mu(d)}{2\pi i}\int_C \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}}.$$

Y esto sigue valiendo si estiramos nuestro contorno C según indican las flechas de la figura. Si nos fijamos, a medida que aumentamos el radio del arco de circunferencia la integral sobre él es menor. Concretamente, si el radio es A, podemos acotar el módulo de la función que integramos así:

$$\left|\left(\frac{R}{d}\right)^s \frac{1}{s^{a+1}}\right| = \left|\left(\frac{R}{d}\right)^{\Re s}\right| \frac{1}{|s|^{a+1}} \leq \frac{R}{d}\frac{1}{(A-1)^{a+1}}$$

donde en el último paso hemos usado que $\Re s \leq 1$ y $\frac{R}{d} \geq 1$ sobre nuestra mitad de la circunferencia y la desigualdad triangular para afirmar que $A - 1 = |s-1| - 1 \leq |s|$ para los puntos s del arco de circunferencia. Eso quiere decir que el módulo de la integral sobre el arco de circunferencia (recordemos que mide πA) se puede acotar por

$$\left|\int_C \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}}\right| \leq \frac{R}{d}\frac{\pi A}{(A-1)^{a+1}}$$

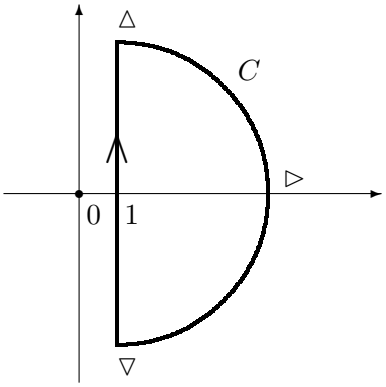
que, como $a \geq 1$, ciertamente tiende a 0 cuando $A \to \infty$.

Así, cuando el contorno crece, la recta se lleva todo el peso de la integral y tenemos para $a \geq 1$ y $d \leq R$ la fórmula

$$\lambda_R(d;a) = \frac{\mu(d)}{2\pi i}\int_{(1)} \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}}.$$

donde la notación (α) representa la recta vertical del plano complejo que pasa por α.

¿Y qué pasa para $d > R$? ¿También es válida la fórmula? Para que lo fuera, la integral $\int_{(1)} \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}}$ debería ser 0 para $d > R$ (en realidad, sólo para los libres de cuadrados). Pensemos en el contorno



y observemos que $f(s) = \left(\frac{R}{d}\right)^s \frac{1}{s^{a+1}}$ es analítica en la frontera y el interior de nuestro nuevo contorno C (el 0, que es el único que podría dar problemas, está ahora fuera del contorno). Volvemos al libro de variable compleja que nos dice que entonces la integral sobre C es nula[7].

Luego si conseguimos ver, como antes, que la integral sobre el arco de circunferencia tiende a 0 cuando aumentamos el radio, tendremos que la integral sobre (1) es 0, que es lo que queríamos. Bien, pues haciendo como antes (ahora $\Re s \geq 1$, $\frac{R}{d} < 1$ y $|s| \geq A$) podemos acotar el módulo de la función en el arco de circunferencia por $\frac{R}{d}\frac{1}{A^{a+1}}$ y la integral por $\frac{R}{d}\frac{\pi}{A^a}$, que tiende a 0 cuando $A \to \infty$.

Resumiendo, para todo $a \geq 1$ y para todo $d \geq 1$ tenemos la fórmula

$$\lambda_R(d;a) = \frac{\mu(d)}{2\pi i} \int_{(1)} \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}},$$

de donde

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} \underbrace{\sum_{d_1,d_2} \mu(d_1)\mu(d_2) \frac{|\Omega([d_1,d_2])|}{[d_1,d_2] d_1^{s_1} d_2^{s_2}}}_{F(s_1,s_2;\Omega)} \frac{R^{s_1+s_2}}{(s_1 s_2)^{k+l+1}} ds_1 ds_2.$$

En este punto, conviene recordar la expresión como producto de Euler

[7] **Teorema de Cauchy-Goursat:** *Si f es analítica en el interior y en la frontera de un contorno cerrado simple, C, entonces*

$$\int_C f(z)dz = 0.$$

de la función zeta de Riemann. En el semiplano $\Re s > 1$ tenemos

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}. \tag{1.10}$$

Para convencerse de ello, es mucho mejor escribir el productorio así

$$\left(1 + \frac{1}{2^s} + \frac{1}{(2^2)^s} + \frac{1}{(2^3)^s} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{(3^2)^s} + \frac{1}{(3^3)^s} + \cdots\right)\cdots$$

donde tenemos la suma de una progresión geométrica para cada primo. Ahora, fijado un n, basta pensar qué sumando tenemos que coger en cada factor para obtener $1/n^s$. La respuesta es sencilla, basta descomponer n en factores primos elevados a potencias y coger el sumando de la potencia correspondiente para los primos que están en n y el sumando 1 para los primos que no están en n. La fórmula de la suma de los elementos de una progresión geométrica nos da (1.10).

Del mismo modo, podemos expresar la función que hemos llamado $F(s_1, s_2; \Omega)$ como un producto de Euler. Mirando a la expresión de F como suma tenemos

$$\sum_{d_1,d_2} |\mu(d_1)||\mu(d_2)| \frac{|\Omega([d_1,d_2])|}{|[d_1,d_2]|} \frac{1}{|d_1|^{s_1}|d_2|^{s_2}} \leq \sum_{d_1} \frac{1}{|d_1|^{s_1}} \sum_{d_2} \frac{1}{|d_2|^{s_2}}$$

lo que nos dice que tenemos convergencia absoluta en $\Re s_1, \Re s_2 > 1$, región en la que vale lo siguiente. Teniendo en cuenta (1.6),

$$\begin{aligned} F(s_1, s_2; \Omega) &= \sum_{d_1,d_2} \mu(d_1)\mu(d_2) \frac{|\Omega([d_1,d_2])|}{[d_1,d_2] d_1^{s_1} d_2^{s_2}} \\ &= \prod_p \left(1 - \frac{|\Omega(p)|}{p}\left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right). \end{aligned}$$

De nuevo, la forma de entenderlo es fijar d_1 y d_2 y pensar cuál de los 4 sumandos tenemos que coger en el factor correspondiente a cada primo p. En primer lugar, si d_1 o d_2 no es libre de cuadrados se toma el sumando 1 en todos los factores (el 1 no afecta al producto y en la suma obtenemos un 0 que tampoco afecta). Ahora, si los 2 son libres de cuadrados habrá que coger el sumando 1 si p no está en d_1 ni en d_2, el sumando $\frac{|\Omega(p)|}{p^{s_1+1}}$ si p está sólo en d_1, el sumando $\frac{|\Omega(p)|}{p^{s_2+1}}$ si p está sólo en d_2 y el sumando $\frac{|\Omega(p)|}{p^{s_1+s_2+1}}$ si p está en d_1 y en d_2. Con eso y recordando (1.6) vemos que todo cuadra, incluidos los signos pues cuando añadimos un primo que está en d_1 y d_2 el signo es positivo y cuando añadimos primos "sueltos" (que sólo están en uno de ellos) el signo es negativo.

Definimos ahora, con ζ la función zeta Riemann,

$$G(s_1, s_2; \Omega) = F(s_1, s_2; \Omega) \left(\frac{\zeta(s_1+1)\zeta(s_2+1)}{\zeta(s_1+s_2+1)} \right)^k \tag{1.11}$$

y afirmamos que es analítica y acotada para $\Re s_1, \Re s_2 > -c$ (donde recordemos que c es una constante positiva, pronto aclararemos su valor). ¡Un momento! ¿Estamos locos? F era analítica en $\Re s_1, \Re s_2 > 1$. Las funciones $\zeta(s_1+1)$, $\zeta(s_2+1)$, $\zeta(s_1+s_2+1)$ lo son para $\Re s_1, \Re s_2 > 0$. Y ahora decimos que al multiplicar y dividir funciones de éstas nos sale algo analítico en una región mayor ¿Qué pasa? ¿Que multiplicándolas se arreglan?

La idea es que si dos funciones analíticas coinciden en un semiplano entonces han de ser la misma función en todo el dominio en el que estén definidas ambas simultáneamente[8], en otras palabras, "la extensión analítica es única". Así, si la fórmula del producto (1.11) resulta ser analítica en un semiplano mayor que aquel en el que lo son F o el producto de funciones ζ, podemos darle validez en todo ese semiplano porque estamos seguros de que esa es "la" extensión analítica.

Tenemos la acotación

$$G(s_1, s_2; \Omega) \ll \exp(c(\log N)^{-2\sigma} \log\log\log N) \tag{1.12}$$

donde $\sigma = \min\{\Re s_1, \Re s_2, 0\} \geq -c$.

Para comprobarlo separamos la expresión de G como producto de Euler en los primos $p > H$ y en los primos $p \leq H$. Para los primos $p > H$, sabemos que $|\Omega(p)| = k$ y la parte del producto correspondiente es

$$\prod_{p>H} \left(\left(1 - \left(\frac{k}{p^{s_1+1}} + \frac{k}{p^{s_2+1}} - \frac{k}{p^{s_1+s_2+1}} \right)\right) \left(1 - \frac{1}{p^{s_1+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_2+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_1+s_2+1}}\right)^{k} \right).$$

La fórmula de Taylor nos dice que cuando $s \to 0$

$$\frac{1}{(1-s)^k} = (1+s)^k + O(s^2) = 1 + ks + O(s^2)$$

y usando esto en cada uno de los factores del producto, éste se convierte en

$$\prod_{p>H} \left(1 + O\left(\frac{1}{p^{2\Re s_1 + 2\Re s_2 + 2}} \right)\right)$$

[8] De hecho, no necesitamos tanto, pues basta con que f y g sean analíticas en un dominio D y exista un conjunto $A \subseteq D$ con un punto de acumulación en el que $f = g$ para concluir que $f = g$ en todo D

donde al hacer las acotaciones estábamos pensando que $\Re s_1, \Re s_2 < 0$. Si las dos son positivas, $O\left(\frac{1}{p^{2\Re s_1+2\Re s_2+2}}\right) \ll O\left(\frac{1}{p^2}\right)$ y si una, digamos $\Re s_2$ es positiva, $O\left(\frac{1}{p^{2\Re s_1+2\Re s_2+2}}\right) \ll O\left(\frac{1}{p^{2\Re s_1+2}}\right)$. Analizando todas las posibilidades, llegamos a que podemos escribir

$$\prod_{p>H}\left(1+O\left(\frac{1}{p^{4\,\mín\{\Re s_1,\Re s_2,0\}+2}}\right)\right).$$

En cualquier caso, mientras tengamos

$$4\,\mín\{\Re s_1,\Re s_2,0\}+2>1 \Leftrightarrow \sigma=\mín\{\Re s_1,\Re s_2,0\}>\frac{-1}{4}$$

todo va a ir bien (obsérvese que de la última desigualdad se obtiene el valor de la constante $-c$). Digamos que $4\,\mín\{\Re s_1,\Re s_2,0\}+2$ es igual a $1+\alpha$ con $\alpha>0$. Entonces el producto es

$$\prod_{p>H}\left(1+O\left(\frac{1}{p^{1+\alpha}}\right)\right)$$

y su logaritmo (teniendo en cuenta que ahora Taylor nos dice $\log(1+x)=x+O(x^2)$ cuando $x\to 0$) es

$$\sum_{p>H}\log\left(1+O\left(\frac{1}{p^{1+\alpha}}\right)\right)=\sum_{p>H}O\left(\frac{1}{p^{1+\alpha}}\right)+\sum_{p>H}O\left(\frac{1}{p^{2+2\alpha}}\right)<\infty$$

lo que demuestra que para los $p>H$ el producto está uniformemente acotado en la región $\sigma=\mín\{\Re s_1,\Re s_2,0\}\geq -c$.

Vamos con la otra parte del producto:

$$\prod_{p\leq H}\quad\left(\left(1-\frac{|\Omega(p)|}{p}\left(\frac{1}{p^{s_1}}+\frac{1}{p^{s_2}}-\frac{1}{p^{s_1+s_2}}\right)\right)\right.$$
$$\left.\left(1-\frac{1}{p^{s_1+1}}\right)^{-k}\left(1-\frac{1}{p^{s_2+1}}\right)^{-k}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^{k}\right).$$

Teniendo en cuenta la acotación trivial $|\Omega(p)|\leq p$ y las fórmulas de Taylor que hemos usado antes, su logaritmo es

$$\ll\sum_{p\leq H}\frac{1}{p^{\Re s_1+\Re s_2+1}}\leq\sum_{p\leq H}\frac{1}{p^{2\,\mín\{\Re s_1,\Re s_2,0\}+1}}\leq H^{-2\sigma}\sum_{p\leq H}\frac{1}{p}.$$

Recordando[9] que $\sum_{p\leq x}\frac{1}{p}=\log\log x+O(1)$ y mirando a (1.1) llegamos a que el logaritmo del producto en los primos menores o iguales que H es

$$\ll H^{-2\sigma}\log\log H\ll(\log N)^{-2\sigma}\log\log\log N$$

[9]La fórmula se puede obtener, por ejemplo, sumando por partes a partir de la fórmula de Mertens $\sum_{p\leq x}\frac{\log p}{p}=\log x+O(1)$. Ver, por ejemplo, [4].

y por lo tanto

$$G(s_1, s_2; \Omega) \ll \exp(c(\log N)^{-2\sigma} \log\log\log N)$$

que es (1.12).

En particular tenemos lo que se conoce como "serie singular":

$$\mathfrak{S}(\mathcal{H}) = G(0,0;\Omega) = \prod_p \left(1 - \frac{|\Omega(p)|}{p}\right)\left(1 - \frac{1}{p}\right)^{-k},$$

que es un número que no se anula por la condición (1.3) y por el hecho ya observado de que, para $p > H$, $|\Omega(p)| = k$ (tomando logaritmos, si la suma de los logaritmos converge entonces ese producto no puede ser 0).

Así que ahora tenemos

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} G(s_1, s_2; \Omega) \left(\frac{\zeta(s_1 + s_2 + 1)}{\zeta(s_1 + 1)\zeta(s_2 + 1)}\right)^k \frac{R^{s_1+s_2}}{(s_1 s_2)^{k+l+1}} ds_1 ds_2.$$

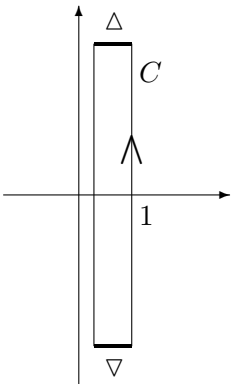
Escribimos $U = \exp(\sqrt{\log N})$, y cambiamos los contornos de s_1 y s_2 a las líneas verticales $c_0(\log U)^{-1} + it$ y $c_0(2\log U)^{-1} + it$, $t \in \mathbb{R}$, respectivamente, donde $c_0 > 0$ es una constante suficientemente pequeña, como quedará claro más adelante.

Tanto para la elección de c_0 como para las acotaciones que realizaremos, necesitamos conocer un par de cosas sobre la función zeta de Riemann (ver [6]). Escribiendo un número complejo como $s = \sigma + it$ (esta mezcla de letras griegas y latinas es clásica):

- Existe una constante pequeña y positiva $\bar{c}$ tal que $\zeta(\sigma + it) \neq 0$ en la región $\sigma \geq 1 - \frac{4\bar{c}}{\log(|t|+3)}$ para todo t.
- Además, en la misma región, se cumplen

$$\zeta(\sigma + it) - \frac{1}{\sigma - 1 + it} \ll \log(|t| + 3) \quad \text{y} \quad \frac{1}{\zeta(\sigma + it)} \ll \log(|t| + 3). \tag{1.13}$$

Esto podemos hacerlo porque la integral de nuestra función (ojo que ahora tenemos una función con dos variables complejas) sobre los segmentos marcados más gruesos en el dibujo siguiente tiende a 0 a medida que estiramos el contorno según indican las flechas.

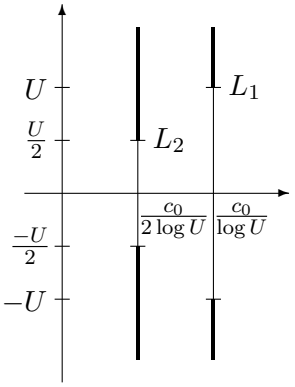


La acotación se consigue teniendo en cuenta las acotaciones (1.12) y (1.13) y observando que lo que más puede a medida que la parte imaginaria tiende a infinito son las eses del denominador (elevadas a $k+l+1$, que es un número mayor o igual que 3, porque $k, l \in \mathbb{Z}_{>0}$). Así, estirando el contorno hasta el infinito, el teorema de Cauchy-Goursat nos dice que la integral sobre (1) es igual a la integral sobre la nueva recta vertical.

Es más, si truncamos las nuevas verticales de s_1 y s_2 a $|t| \leq U$ y $|t| \leq U/2$ y las llamamos L_1 y L_2 respectivamente entonces

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int_{L_2} \int_{L_1} G(s_1, s_2; \Omega) \left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)} \right)^k \frac{R^{s_1+s_2}}{(s_1 s_2)^{k+l+1}} ds_1 ds_2$$
$$+O\left(\exp\left(-c\sqrt{\log N}\right)\right).$$

El motivo es que (con (1.1), (1.12) y (1.13)) podemos acotar la integral en las semirrectas marcadas más gruesas en el siguiente dibujo por una $O\left(\exp\left(-c\sqrt{\log N}\right)\right)$.



Ahora definimos $L_3 : -c_0(\log U)^{-1} + it, |t| \leq U$ (el segmento simétrico de L_1 respecto al eje vertical) y consideramos la integral sobre el contorno rectangular cuyos lados verticales son L_1 y L_3. Encontramos singularidades (recordemos, a riesgo de ser pesados, que nuestra función tiene dos variables complejas, así que lo que hay que hacer es considerar s_2 como algún punto fijo en L_2) en:

- $s_1 = 0$:
$$G(0, s_2; \Omega) \frac{1}{\zeta^k(s_1+1)} \frac{R^{s_2}}{s_1^{k+l+1} s_2^{k+l+1}}$$
y como $\zeta^k(s_1+1)$ tiene un polo de orden k en $s_1 = 0$, el polo de nuestra función es de orden $l+1$.

- $s_1 = -s_2$: en este caso lo único que "da problemas" es $\zeta^k(s_1+s_2+1)$ y por lo tanto el polo es de orden k.

Observemos que, para que no haya otros polos, L_3 tiene que estar a la derecha de $-c$ (la que era $\leq \sigma = \min\{\Re s_1, \Re s_2, 0\}$) y también en la región libre de ceros, es decir, a la derecha de $-\frac{4\overline{c}}{\log(|t|+3)}$. Esto impone las dos condiciones sobre c_0 siguientes: $\frac{c_0}{\sqrt{\log N}} \leq c$ y $\frac{c_0}{\sqrt{\log N}} \leq \frac{4\overline{c}}{\log\left(\exp\left(\sqrt{\log N}\right)+3\right)}$. Y siempre podemos encontrar un valor suficientemente pequeño de c_0 que las cumpla.

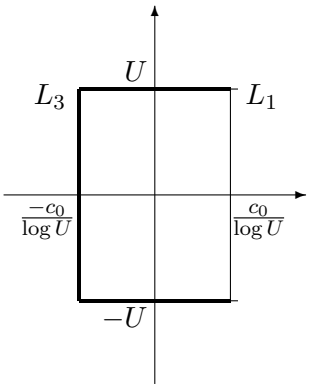
Si ahora integramos nuestra función respecto de s_1 en el contorno rectangular cuyos lados verticales son L_1 y L_3, el teorema de los residuos[10] nos dice que la integral en el contorno es:

$$2\pi i \left(\mathrm{Res}_{s_1=0} + \mathrm{Res}_{s_1=-s_2}\right).$$

Si conseguimos ver que el peso de la integral en el contorno rectangular está todo en L_1 (salvo quizá por una $O\left(\exp\left(-c\sqrt{\log N}\right)\right)$), podremos escribir

$$\mathcal{T} = \frac{1}{2\pi i}\int_{L_2} \left(\mathrm{Res}_{s_1=0} + \mathrm{Res}_{s_1=-s_2}\right) ds_2 + O\left(\exp\left(-c\sqrt{\log N}\right)\right). \quad (1.14)$$

En efecto, si integramos en el contorno de la figura



vemos que usando nuestras acotaciones, ya habituales, la integral en todas las líneas gruesas es una $O\left(\exp\left(-c\sqrt{\log N}\right)\right)$, lo que da validez a la fórmula (1.14).

[10] ¿Acabaremos escribiendo el libro de variable compleja a base de notas al pie?

TEOREMA DE LOS RESIDUOS: *Si C es un contorno cerrado simple orientado positivamente, dentro del cual y sobre el cual una función f es analítica a excepción de en un número finito de puntos interiores a C, z_k $(k = 1, 2, \ldots, n)$, entonces*

$$\int_C f(z)dz = 2\pi i \sum_{k=1}^{n} Res_{z=z_k} f(z)$$

El libro de variable compleja nos dice[11] que podemos escribir el residuo como $\frac{1}{2\pi i}\int_C$ si C es un círculo centrado en el polo en el que la función no tiene más singularidades. Así,

$$\mathrm{Res}_{s_1=-s_2} = \frac{1}{2\pi i}\int_{C(s_2)} G(s_1,s_2;\Omega)\left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)}\right)^k \frac{R^{s_1+s_2}}{(s_1s_2)^{k+l+1}}ds_1,$$

donde $C(s_2)$ es la circunferencia $|s_1+s_2| = \frac{1}{\log N}$. De nuevo podemos usar nuestras acotaciones para tener: $G(s_1,s_2;\Omega) \ll (\log\log N)^c$ (porque $(\log N)^{(1/\sqrt{\log N})} = O(1)$), $\zeta(s_1+s_2+1) \ll \log N$, $R^{s_1+s_2} \ll 1$. Además, como $|s_2| \ll |s_1| \ll |s_2|$, tenemos que $\frac{1}{s_1\zeta(s_1+1)} \ll \frac{\log(|s_2|+2)}{|s_2|+1}$. Luego

$$\mathrm{Res}_{s_1=-s_2} \ll (\log N)^{k-1}(\log\log N)^c\left(\frac{\log(|s_2|+2)}{|s_2|+1}\right)^{2k}|s_2|^{-2l-2}.$$

Si ponemos esto en (1.14) tenemos

$$\mathcal{T} = \frac{1}{2\pi i}\int_{L_2}(\mathrm{Res}_{s_1=0})\,ds_2 + O\left((\log N)^{k+l-1/2}(\log\log N)^c\right), \qquad (1.15)$$

porque la parte importante es $|s_2|^{-2l-2}$ y la estamos integrando con s_2 en L_2, donde el módulo mínimo es $\frac{c_0}{2\sqrt{\log N}}$, lo que nos da la $O((\log N)^{l+1/2})$.

Para evaluar la última integral, escribimos

$$Z(s_1,s_2) = G(s_1,s_2;\Omega)\left(\frac{(s_1+s_2)\zeta(s_1+s_2+1)}{s_1\zeta(s_1+1)s_2\zeta(s_2+1)}\right)^k,$$

que es analítica en un entorno del punto $(0,0)$, lo cual se comprueba teniendo en cuenta lo que ya hemos observado anteriormente sobre que la función $\zeta(s+1)$ es como $1/s$ cuando $s\to 0$. Además, como "la fracción de las zetas" tiende a 1 cuando $s_1, s_2 \to 0$, tenemos que $Z(0,0) = \mathfrak{S}(\mathcal{H})$.

Como el polo de la función que estamos integrando era de orden $l+1$ en $s_1 = 0$, el residuo vendrá dado por

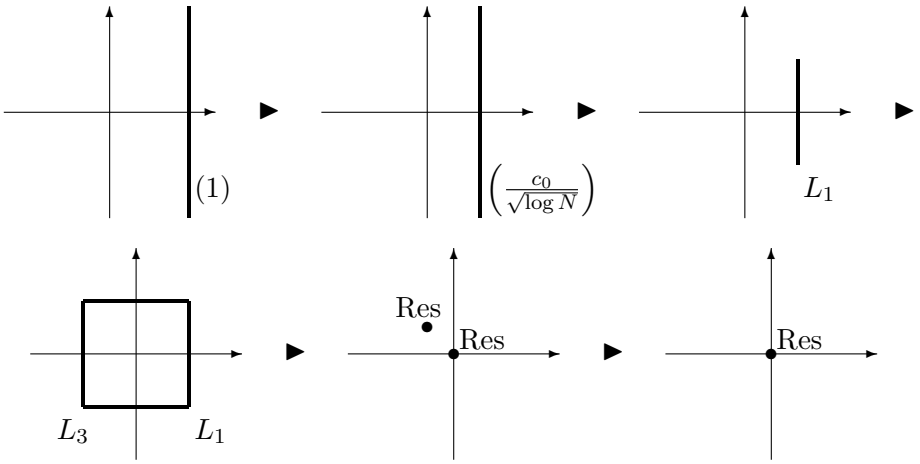
$$\mathrm{Res}_{s_1=0} = \frac{R^{s_2}}{l!s_2^{l+1}}\left(\frac{\partial}{\partial s_1}\right)^l_{s_1=0}\left(\frac{Z(s_1,s_2)}{(s_1+s_2)^k}R^{s_1}\right).$$

Poniendo esto en (1.15), definiendo $L_4 : -c_0(\log U)^{-1} + it, |t| \le U/2$ (el segmento simétrico de L_2 respecto al eje vertical), y considerando la integral sobre el contorno rectangular cuyos lados verticales son L_2 y L_4, vemos, igual que antes, que

$$\mathcal{T} = \mathrm{Res}_{s_2=0}\left(\mathrm{Res}_{s_1=0}\right) + O\left((\log N)^{k+l}\right). \qquad (1.16)$$

[11] Y ya no lo vamos a escribir aquí abajo ¡hombre!

Así que, resumiendo el proceso hasta aquí, teníamos una integral sobre (1) tanto para s_1 como para s_2. Fijándonos ahora en s_1, hemos visto que salvo pequeños errores podíamos pasar a la integral sobre $\left(\frac{c_0}{\log U}\right)$, a la integral sobre L_1, a la integral sobre el contorno rectangular cuyos lados verticales son L_1 y L_3, a la suma de los residuos en $s_1 = 0$ y en $s_1 = -s_2$ y, finalmente, al residuo en $s_1 = 0$. El siguiente dibujo (que muy posiblemente alegrará a la mitad derecha de nuestro cerebro) resume todo el proceso para s_1:



Con s_2 hemos hecho lo mismo sobre L_2 y L_4 y (ahora sólo teníamos un residuo) hemos llegado a que la integral era igual al residuo en $s_2 = 0$ del otro residuo.

Tras este resumen, continuamos. Teniendo en cuenta de nuevo que los residuos se pueden poner como $\frac{1}{2\pi i}\int_C$ siempre que C sólo contenga una singularidad, (1.16) se convierte en

$$\mathcal{T} = \frac{1}{(2\pi i)^2}\int_{C_2}\int_{C_1}\frac{Z(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{l+1}}ds_1ds_2 + O\left((\log N)^{k+l}\right)$$

donde C_1 y C_2 son los círculos $|s_1| = \rho$ y $|s_2| = 2\rho$ respectivamente para un $\rho > 0$ pequeño. Ahora hacemos el cambio de variable $s_1 = s$, $s_2 = s\xi$. Entonces (nótese que el Jacobiano es s) la integral doble es igual a

$$\frac{1}{(2\pi i)^2}\int_{C_3}\int_{C_1}\frac{Z(s,s\xi)R^{s(\xi+1)}}{(\xi+1)^k\xi^{l+1}s^{k+2l+1}}dsd\xi,$$

donde C_3 es el círculo $|\xi| = 2$.

La integral respecto de s la calculamos por residuos (tenemos un polo de orden $k+2l+1$ y para calcular el residuo hay que hacer una derivada $(k+2l)$-ésima) y tenemos que lo anterior es igual a

$$\frac{Z(0,0)}{2\pi i(k+2l)!}(\log R)^{k+2l}\int_{C_3}\frac{(\xi+1)^{2l}}{\xi^{l+1}}d\xi + O\left((\log N)^{k+2l-1}(\log\log N)^c\right)$$

donde hemos usado (1.12).

Teniendo en cuenta la observación de que $Z(0,0) = \mathfrak{S}(\mathcal{H})$, recordando la, ya antigua, fórmula (1.9) y calculando la integral que nos queda también por residuos (ahora tenemos un polo de orden $l+1$ y hay que hacer una derivada l-ésima) llegamos a nuestro ansiado lema.

Lema 1. *Si se cumplen (1.1), (1.2) y $R \leq \frac{N^{1/2}}{(\log N)^C}$ para una $C > 0$ suficientemente grande que depende sólo de k y l, tenemos*

$$\sum_{N<n\leq 2N} \Lambda_R(n;\mathcal{H},k+l)^2 = \frac{\mathfrak{S}(\mathcal{H})}{(k+2l)!}\binom{2l}{l} N(\log R)^{k+2l}$$

$$+O\left(N(\log N)^{k+2l-1}(\log\log N)^c\right).$$

Capítulo 2

Y ahora con primos

Definimos la función

$$\varpi(n) = \begin{cases} \log n & \text{si } n \text{ es primo} \\ 0 & \text{si no} \end{cases}$$

y consideramos la suma

$$\sum_{N<n\leq 2N} \varpi(n+h)\Lambda_R(n;\mathcal{H},k+l)^2, \tag{2.1}$$

con un entero positivo arbitrario $h \leq H$. Observamos que esto es igual a

$$\sum_{N<n\leq 2N} \varpi(n+h)\Lambda_R(n;\mathcal{H}\backslash\{h\},k+l)^2, \tag{2.2}$$

con tal de que $R < N$. Para convencernos de ello escribimos, como en (1.7),

$$\Lambda_R(n;\mathcal{H},k+l) = \frac{1}{(k+l)!} \sum_{\substack{d|(n+h_1)\cdots(n+h_k) \\ d\leq R}} \mu(d)\left(\log\left(\frac{R}{d}\right)\right)^{k+l}$$

y vemos que los d en los que estamos sumando cumplen $d \leq R < N < n$. Luego, mirando ahora a la suma (2.1), si $\varpi(n+h) \neq 0$ (equivalentemente, si $n+h$ es primo) y $h \in \mathcal{H}$ entonces $n+h$ es un primo mayor que d. Por lo tanto d no puede dividir a $n+h$ y por lo tanto h no influye en la condición $d|(n+h_1)\cdots(n+h_k)$, que es la única en la que aparece algo que tenga que ver con h en la suma. En particular, podemos asumir que $h \notin \mathcal{H}$ en (2.1).

Asumiremos también que se cumple la afirmación siguiente:

Existe una constante absoluta $0 < \theta < 1$ tal que para todo $A > 0$ fijado se tiene

$$\sum_{q\leq x^\theta} \max_{y\leq x} \max_{\substack{a \\ (a,q)=1}} \left|\vartheta^*(y;a,q) - \frac{y}{\varphi(q)}\right| \ll \frac{x}{(\log x)^A} \tag{2.3}$$

con

$$\vartheta^*(y;a,q) = \sum_{\substack{y<n\leq 2y\\ n\equiv a(\text{mód } q)}} \varpi(n),$$

donde φ es la función de Euler y la constante implícita depende sólo de A.

Aquí deberíamos hacer algunos comentarios. Comencemos admitiendo que al principio de la introducción no dijimos toda la verdad sobre el teorema del número primo (lo que dijimos era todo cierto, pero el teorema nos dice más cosas). Concretamente, podemos escribir $\pi(x) = Li(x) + E(x)$, donde $Li(x)$ es el logaritmo integral, $\int_2^x \frac{dt}{\log t}$, que es el término principal esperado, y $E(x)$ es el término de error. Obsérvese que por integración por partes se puede ver que $Li(x)$ es como $x/\log x$, lo que cuadra con lo que dijimos. El teorema del número primo nos dice además para el término de error que dado cualquier $A > 0$ existe una constante $C(A)$ tal que $|E(x)| \leq C(A)\frac{x}{(\log x)^A}$ (sin embargo con la aproximación de $\pi(x)$ por $\frac{x}{\log x}$ el error sería mayor que $C\frac{x}{(\log x)^2}$). Es más, si se cumpliera la hipótesis de Riemann, tendríamos la maravillosa fórmula: $\pi(x) = Li(x) + O(x^{1/2}\log x)$.

Esto se puede generalizar a primos en progresiones. Dada una progresión aritmética $a \pmod q$ con $(a,q) = 1$, escribimos $\pi(x;a,q) = \frac{Li(x)}{\varphi(q)} + E(x;a,q)$, donde $\pi(x;a,q)$ es el número de primos menores o iguales que x congruentes con $a \pmod q$, $\frac{Li(x)}{\varphi(q)}$ es el término principal esperado y $E(x;a,q)$ es el término de error. De nuevo hay un teorema que nos dice que para todo $A > 0$ existe una constante $C(q,A)$ tal que $|E(x;a,q)| \leq C(q,A)\frac{x}{(\log x)^A}$. Es importante hacer hincapié en el hecho de que la constante depende ahora de q, por lo que el resultado sólo nos sirve si tenemos q fijo y $x \to \infty$. Pero en la mayoría de las aplicaciones, como es nuestro caso, eso no nos vale, necesitamos que q crezca con x (estudiaremos primos en progresiones (mód $[d_1,d_2]$), lo cual crece con R).

Un teorema de Siegel y Walfisz nos dice que, dado $A > 0$, tenemos, uniformemente en q, $\pi(x;a,q) = \frac{Li(x)}{\varphi(q)} + O\left(\frac{x}{(\log x)^A}\right)$. Esto es mejor que el resultado para q fijo, pero el rango de q para el que podemos aplicarlo es todavía bastante restrictivo, hasta $(\log x)^{\text{algo}}$. Si se cumpliera la hipótesis de Riemann generalizada tendríamos $\pi(x;a,q) = \frac{Li(x)}{\varphi(q)} + O(x^{1/2}\log x)$, lo cual sería mucho mejor, pues podría aplicarse para valores de q hasta un poco menos que $x^{1/2}$. Si queremos escribirlo para ϑ^*, tendríamos $\vartheta^*(x;a,q) = \frac{x}{\varphi(q)} + O(x^{1/2}(\log x)^2)$ y vemos que esto nos serviría, por ejemplo, para $q \leq x^{1/2}/(\log x)^3$.

Desafortunadamente no sabemos probar la hipótesis de Riemann generalizada (¡la otra tampoco!), que es la que nos da las cotas buenas en rangos de q razonablemente grandes, pero afortunadamente en la mayoría de las aplicaciones, ¡incluyendo la nuestra!, basta con una cota en media para q variando (en nuestro caso queremos primos en progresiones (mód $[d_1,d_2]$), pero también tenemos una suma sobre d_1 y d_2 que crecen hasta R). Un resultado extremadamente potente de Bombieri y Vinogradov nos da exactamente eso, una estimación en media. Es más, el resultado es casi tan bueno como lo que nos diría la hipótesis de Riemann generalizada. Pero dejemos de venderlo antes de mostralo.

Teorema de Bombieri-Vinogradov: Para toda constante $A > 0$ existe una constante $B > 0$ tal que

$$\sum_{q\leq \frac{x^{1/2}}{(\log x)^B}} \max_{y\leq x} \max_{\substack{a\\(a,q)=1}} \left|\vartheta^*(y;a,q) - \frac{y}{\varphi(q)}\right| \ll \frac{x}{(\log x)^A}.$$

Luego el teorema nos dice que en media (incluso cogiendo dentro de cada módulo la progresión aritmética que da lugar al mayor error), para $q \leq \frac{x^{1/2}}{(\log x)^B}$, $\vartheta^*(x;a,q) = \frac{x}{\varphi(q)} + O(x^{1/2}(\log x)^{B-A})$, lo que, olvidándonos de los logaritmos, es tan bueno como lo que nos decía la hipótesis de Riemann generalizada.

Si nos fijamos un poco, el teorema de Bombieri-Vinogradov garantiza que nuestra afirmación (2.3) se cumple para todo $0 < \theta < 1/2$. Y de hecho eso es todo lo que se sabe probar. Entonces ¿por qué asumimos como cierta la afirmación para un $0 < \theta < 1$? Bueno, es lo mismo que cuando decimos que asumiendo como cierta la hipótesis de Riemann podemos demostrar "tal cosa". Así, el día que alguien la demuestre, probará a la vez los cientos de teoremas que la suponen cierta. Y, como hemos anunciado, si el teorema de Bombieri-Vinogradov se cumpliera para algún $1/2 < \theta < 1$ tendríamos infinitas diferencias acotadas entre primos. En el cuarto capítulo veremos cómo se puede probar esto.

Resumiendo, la afirmación es cierta para $0 < \theta < 1/2$ y todo lo que probemos con esos valores de θ estará bien probado. Luego, en el último capítulo veremos hasta dónde podemos llegar si suponemos cierta la afirmación para valores de θ mayores. Aunque los recelosos deberían observar que la siguiente conjetura tenía nombres propios antes de que la necesitáramos para este particular:

CONJETURA DE ELLIOTT-HALBERSTAM: Dados $\varepsilon > 0$ y $A > 0$

$$\sum_{q\le x^{1-\varepsilon}} \max_{y\le x} \max_{\substack{a\\(a,q)=1}} \left|\vartheta^*(y;a,q) - \frac{y}{\varphi(q)}\right| \ll \frac{x}{(\log x)^A}.$$

Y tras estos comentarios continuamos. Asumimos que $R \le N^{\theta/2}$.

Haciendo las mismas cuentas que con la suma de (1.8), tenemos que (2.1) es igual a

$$\sum_{d_1,d_2} \lambda_R(d_1;k+l)\lambda_R(d_2;k+l) \sum_{\substack{N<n\le 2N\\ n\in\Omega([d_1,d_2])}} \varpi(n+h). \tag{2.4}$$

Afirmamos que esta suma es igual a

$$\sum_{d_1,d_2} \lambda_R(d_1;k+l)\lambda_R(d_2;k+l) \sum_{b\in\Omega([d_1,d_2])} \delta((b+h,[d_1,d_2]))\vartheta^*(N;b+h,[d_1,d_2])$$

$$+O(R^2(\log N)^c) \tag{2.5}$$

donde $\delta(x)$ es la función que vale 1 en 1 y 0 en cualquier otro sitio. La δ no afecta porque como

$$\vartheta^*(N;b+h,[d_1,d_2]) = \sum_{\substack{N<n\le 2N\\ n\equiv b+h(\text{mód }[d_1,d_2])}} \varpi(n),$$

si $(b+h,[d_1,d_2]) \neq 1$ entonces todos los n del sumatorio son compuestos y ϑ^* es 0. O sea, estamos diciendo que, salvo un error, la suma (2.4) es

$$\sum_{d_1,d_2} \lambda_R(d_1;k+l)\lambda_R(d_2;k+l) \sum_{b\in\Omega([d_1,d_2])} \overbrace{\sum_{\substack{N<n+h\le 2N\\ n+h\equiv b+h(\text{mód }[d_1,d_2])}} \varpi(n+h)}^{\vartheta^*(N;b+h,[d_1,d_2])}.$$

Si nos fijamos, la condición del segundo sumatorio junto con la de abajo del tercer sumatorio, nos da $n \in \Omega([d_1,d_2])$, luego tenemos exactamente la

fórmula (2.4), salvo que ahora n se mueve en $(N-h, 2N-h]$ en lugar de en $(N, 2N]$. Y esto no debe preocuparnos porque $h \le H \ll \log N$, $\varpi \le 1$ y $|\Omega([d_1,d_2])| \le \tau_k([d_1,d_2])$, luego aplicando la acotación que obtuvimos en el capítulo anterior para τ_k en media, concluimos que el error es $O(R^2(\log N)^c)$, lo que da validez a (2.5).

Entonces, por (2.3), esto es igual a

$$N\mathcal{T}^* + O\left(\frac{N}{(\log N)^{A/3}}\right)$$

con

$$\mathcal{T}^* = \sum_{d_1,d_2} \frac{\lambda_R(d_1;k+l)\lambda_R(d_2;k+l)}{\varphi([d_1,d_2])} \sum_{b \in \Omega([d_1,d_2])} \delta((b+h,[d_1,d_2])). \quad (2.6)$$

El término de error se explica de la siguiente manera. Consideramos primero la parte de (2.5) en la que $|\Omega([d_1,d_2])| \le \tau_k([d_1,d_2]) < (\log N)^{A/2}$ y aplicamos (2.3) (observemos que $|\{d_1,d_2 : [d_1,d_2]=d\}| = \tau_3(d)$). La parte restante es

$$\ll N(\log R)^{2(k+l)} \log N \sum_{d_1,d_2 \le R} \frac{\tau_k([d_1,d_2])}{(\log N)^{A/2}} \frac{|\Omega([d_1,d_2])|}{[d_1,d_2]} \ll \frac{N}{(\log N)^{A/3}}$$

si A es suficientemente grande[1].

Nos resta evaluar $\mathcal{T}^*$. Recordando la definición de Ω para un número libre de cuadrados, la suma interior de (2.6) es igual a

$$\prod_{p|[d_1,d_2]} \left(\sum_{b \in \Omega(p)} \delta((b+h,p)) \right) = \prod_{p|[d_1,d_2]} (|\Omega^+(p)| - 1)$$

donde Ω^+ corresponde al conjunto $\mathcal{H}^+ = \mathcal{H} \cup \{h\}$. El motivo de la última igualdad es que $\delta((b+h,p))$ se anula si y sólo si $-h \in \Omega(p)$, es decir, si $\Omega(p) = \Omega^+(p)$. Observemos que ahora el análogo de (1.3) puede no cumplirse.

En cualquier caso, tenemos, igual que antes,

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} \prod_p \left(1 - \frac{|\Omega^+(p)|-1}{p-1}\left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right)$$

[1]El último $\ll$ requiere una explicación. Empleando $|\{d_1,d_2 : [d_1,d_2]=d\}| = \tau_3(d)$, observamos que basta comprobar que la suma $S = \sum_{n \le R^2} \frac{\tau_3(n)(\tau_k(n))^2}{n}$ es una $O((\log N)^c)$. Definimos la función $Z(s) = \sum_{n=1}^{\infty} \frac{\tau_3(n)(\tau_k(n))^2}{n^s} = \prod_p \left(1 + \frac{3k^2}{p^s}\right)$, porque τ_k es multiplicativa y $\tau_k(p) = k$ para todo $k \in \mathbb{Z}_{>0}$. Tenemos que $S \ll Z\left(1 + \frac{1}{\log R^2}\right)$ cuando $R \to \infty$ porque $n^{\frac{1}{\log R^2}} \ll 1$. Usando la fórmula de Taylor y el hecho de que, cuando $s \to 1$, $-\log(s-1) \sim \sum_p \frac{1}{p^s}$ (porque la función ζ de Riemann es como $\frac{1}{s-1}$) llegamos a que $\log Z(s) = -3k^2 \log(s-1) + O(1)$. De aquí $Z(s) \ll (s-1)^{-3k^2}$ y, por lo tanto, $S \ll (\log R^2)^{3k^2}$.

$$\frac{R^{s_1+s_2}}{(s_1s_2)^{k+l+1}}ds_1ds_2. \tag{2.7}$$

Para $p > H$ tenemos $|\Omega^+(p)| = k+1$, porque $h \notin \mathcal{H}$. Consideramos la función

$$\prod_p (\cdots)\left(\frac{\zeta(s_1+1)\zeta(s_2+1)}{\zeta(s_1+s_2+1)}\right)^k$$

como en (1.11). Si $\mathcal{H}^+$ es admisible, la serie singular es $\mathfrak{S}(\mathcal{H}^+)$ y el argumento y el cálculo de los residuos es igual que en el capítulo anterior. Si $h \notin \mathcal{H}$, tenemos

$$\mathcal{T}^* = \frac{\mathfrak{S}(\mathcal{H}^+)}{(k+2l)!}\binom{2l}{l}(\log R)^{k+2l} + O\left((\log N)^{k+2l-1}(\log\log N)^c\right). \tag{2.8}$$

Por otra parte, si $\mathcal{H}^+$ no es admisible, es decir, $\mathfrak{S}(\mathcal{H}^+) = 0$, entonces el producto de Euler de (2.7) se anula tanto en $s_1 = 0$ como en $s_2 = 0$ con orden igual al número de primos tales que $|\Omega^+(p)| = p$. De cualquier modo, como en ese caso $p \leq k+1$, los cambios que hay que hacer sólo resultan en la pérdida del término principal de la ecuación anterior (2.8) y el término de error permanece igual o incluso menor.

Finalmente, si $h \in \mathcal{H}$, se aplica lo mismo pero con la traslación $k \mapsto k-1$, $l \mapsto l+1$ por la observación (2.2) (para que $k+l$ siga sumando lo mismo, si restamos uno a k tenemos que sumárselo a l).

De todo esto deducimos el siguiente

Lema 2. *Si se cumplen (1.1), (1.2) y (2.3) tenemos, para $R \leq N^{\theta/2}$,*

$$\sum_{N<n\leq 2N} \varpi(n+h)\Lambda_R(n;\mathcal{H},k+l)^2 =$$

$$\begin{cases} \dfrac{\mathfrak{S}(\mathcal{H}\cup\{h\})}{(k+2l)!}\binom{2l}{l}N(\log R)^{k+2l} + O\left(N(\log N)^{k+2l-1}(\log\log N)^c\right) \\ \\ \textit{si } h \notin \mathcal{H}, \\ \\ \dfrac{\mathfrak{S}(\mathcal{H})}{(k+2l+1)!}\binom{2(l+1)}{l+1}N(\log R)^{k+2l+1} + O\left(N(\log N)^{k+2l}(\log\log N)^c\right) \\ \\ \textit{si } h \in \mathcal{H}. \end{cases}$$

Capítulo 3

La prueba

Ya estamos preparados para probar nuestro resultado. Para ello, evaluaremos la expresión

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{N<n\leq 2N}\left(\sum_{h\leq H}\varpi(n+h)-\log(3N)\right)\Lambda_R(n;\mathcal{H},k+l)^2 \tag{3.1}$$

donde ponemos $R=N^{\theta/2}$ para poder aplicar el lema 1[1] y el lema 2.

Si (3.1) resulta ser positivo, entonces existe un entero $n\in(N,2N]$ tal que

$$\sum_{h\leq H}\varpi(n+h)-\log(3N)>0.$$

Es decir, en ese caso, existe un subintervalo de longitud H en $(N,2N+H]$ que contiene dos primos (para N grande, el logaritmo de un número menor o igual que $2N+H$ no puede ser mayor que $\log(3N)$, por lo que es necesario que haya al menos dos primos, pues ϖ de un número compuesto da 0).

Por lo tanto, si (3.1) resulta ser positivo entonces

$$\min_{N<p_r\leq 2N+H}(p_{r+1}-p_r)\leq H. \tag{3.2}$$

Ahora, Gallagher nos dice en [5] que

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\mathfrak{S}(\mathcal{H})=(1+o(1))H^k \tag{3.3}$$

cuando H tiende a infinito.

[1]La condición $R\leq\frac{N^{1/2}}{(\log N)^C}$ se cumple con $R=N^{\theta/2}$ porque $\theta<1$.

Podemos escribir (3.1) como

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{N<n\leq 2N}\left(\sum_{\substack{h\leq H\\h\notin\mathcal{H}}}\varpi(n+h)+\sum_{\substack{h\leq H\\h\in\mathcal{H}}}\varpi(n+h)\right)\Lambda_R(n;\mathcal{H},k+l)^2 \quad (3.4)$$

$$-\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{N<n\leq 2N}\log(3N)\Lambda_R(n;\mathcal{H},k+l)^2. \quad (3.5)$$

La suma (3.5) se puede escribir, gracias al lema 1 como

$$-\log(3N)\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\frac{\mathfrak{S}(\mathcal{H})}{(k+2l)!}\binom{2l}{l}N(\log R)^{k+2l}$$
$$+O(NH^k(\log N)^{k+2l}(\log\log N)^c)$$

lo cual, aplicando la fórmula de Gallagher (3.3), es igual a

$$-\log(3N)\frac{H^k}{(k+2l)!}\binom{2l}{l}N(\log R)^{k+2l}$$
$$+o(NH^k(\log N)(\log R)^{k+2l})$$
$$+O(NH^k(\log N)^{k+2l}(\log\log N)^c)$$

y teniendo en cuenta que $R\leq N$ podemos escribir esto como

$$-\frac{1}{(k+2l)!}\binom{2l}{l}NH^k(\log N)(\log R)^{k+2l}$$
$$+o(NH^k(\log N)^{k+2l+1})$$

cuando $H\to\infty$.

Por otro lado, la suma (3.4) es

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{N<n\leq 2N}\left(\sum_{\substack{h\leq H\\h\notin\mathcal{H}}}\varpi(n+h)\right)\Lambda_R(n;\mathcal{H},k+l)^2$$

$$+\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{N<n\leq 2N}\left(\sum_{\substack{h\leq H\\h\in\mathcal{H}}}\varpi(n+h)\right)\Lambda_R(n;\mathcal{H},k+l)^2$$

y podemos aplicar el lema 2 a cada una de las sumas para tener

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{\substack{h\leq H\\h\notin\mathcal{H}}}\left(\frac{\mathfrak{S}(\mathcal{H}\cup\{h\})}{(k+2l)!}\binom{2l}{l}N(\log R)^{k+2l}+O(N(\log N)^{k+2l-1}(\log\log N)^c)\right)$$

$$+\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}\sum_{\substack{h\leq H\\h\in\mathcal{H}}}\left(\frac{\mathfrak{S}(\mathcal{H})}{(k+2l+1)!}\binom{2(l+1)}{l+1}N(\log R)^{k+2l+1}+O(N(\log N)^{k+2l}(\log\log N)^c)\right)$$

$$=\sum_{\substack{\mathcal{H}\cup\{h\}\subseteq[1,H]\\|\mathcal{H}\cup\{h\}|=k+1}}\left(\frac{\mathfrak{S}(\mathcal{H}\cup\{h\})}{(k+2l)!}\binom{2l}{l}N(\log R)^{k+2l}+O(N(\log N)^{k+2l-1}(\log\log N)^c)\right)$$

$$+\sum_{\substack{\mathcal{H}\subseteq[1,H]\\|\mathcal{H}|=k}}k\left(\frac{\mathfrak{S}(\mathcal{H})}{(k+2l+1)!}\binom{2(l+1)}{l+1}N(\log R)^{k+2l+1}+O(N(\log N)^{k+2l}(\log\log N)^c)\right)$$

donde en la última igualdad hemos hecho desaparecer los dos sumatorios en h, el primero observando que siempre añadía un elemento nuevo a $\mathcal{H}$ e incluyendo esta condición en el otro sumatorio y el segundo cambiándolo por una k, pues este es el número de elementos de cada $\mathcal{H}$ y para cada uno de ellos sumamos la misma cantidad una vez fijado un $\mathcal{H}$. Aplicando de nuevo la fórmula de Gallagher (3.3), esto es igual a

$$\begin{aligned}&\frac{1}{(k+2l)!}\binom{2l}{l}NH^{k+1}(\log R)^{k+2l}\\&+\frac{k}{(k+2l+1)!}\binom{2(l+1)}{l+1}NH^k(\log R)^{k+2l+1}\\&+o(NH^k(\log N)^{k+2l+1}).\end{aligned}$$

Luego (3.1) es igual a

$$\begin{aligned}&\frac{1}{(k+2l)!}\binom{2l}{l}NH^{k+1}(\log R)^{k+2l}\\&+\frac{k}{(k+2l+1)!}\binom{2(l+1)}{l+1}NH^k(\log R)^{k+2l+1}\\&-\frac{1}{(k+2l)!}\binom{2l}{l}NH^k(\log N)(\log R)^{k+2l}\\&+o(NH^k(\log N)^{k+2l+1}).\end{aligned}$$

Sacando factor común (y "olvidándonos" ya de la o, infinitamente más pequeña), tenemos que (3.1) es asintóticamente igual a

$$\left(H+\frac{2k(2l+1)}{(k+2l+1)(l+1)}\log R-\log N\right)\frac{1}{(k+2l)!}\binom{2l}{l}NH^k(\log R)^{k+2l}$$

donde hemos tenido en cuenta que $\frac{\binom{2(l+1)}{l+1}}{\binom{2l}{l}}=\frac{2(2l+1)}{l+1}$. Y recordando que hemos puesto $R=N^{\theta/2}$, tenemos que (3.1) es positivo si para algún $\varepsilon>0$

fijado

$$\frac{H}{\log N} \geq 1 + \varepsilon - \frac{k(2l+1)}{(k+2l+1)(l+1)}\theta.$$

Nos fijamos ahora en la fracción $\frac{k(2l+1)}{(k+2l+1)(l+1)}$ y observamos que siempre es menor que 2. Nosotros queremos que sea lo más cercana a 2 posible, con el propósito de minimizar el tamaño de H. Para ello elegimos, por ejemplo, $l = \lfloor \sqrt{k} \rfloor$ y observamos que entonces ($l \leq \sqrt{k}$ y $l \geq \sqrt{k} - 1$)

$$\frac{k(2l+1)}{(k+2l+1)(l+1)} \geq \frac{2k\sqrt{k}}{k\sqrt{k} + 3k + 3\sqrt{k} + 1} \tag{3.6}$$

que tiende a 2 cuando k tiende a infinito. Es decir, si al principio del todo elegimos un $\varepsilon > 0$ entonces podemos encontrar un k tal que nuestra fracción sea $> 2 - \varepsilon$. A partir de este momento, para no escribir números negativos ni tonterías, suponemos que $0 < \theta < 1/2$, en el próximo capítulo analizaremos qué ocurre para valores mayores. Así, podemos elegir $H = (1 - 2\theta + 2\varepsilon)\log N$ (obsérvese que esta elección respeta (1.1)) y lo que queremos que se cumpla es

$$1 - 2\theta + 2\varepsilon \geq 1 + \varepsilon - \frac{k(2l+1)}{(k+2l+1)(l+1)}\theta$$

o sea

$$\frac{k(2l+1)}{(k+2l+1)(l+1)} + \frac{\varepsilon}{\theta} \geq 2$$

y la parte de la izquierda es $> 2 - \varepsilon + 2\varepsilon > 2$, así que se cumple lo que queríamos para nuestras elecciones de ε, k, l y H.

Luego (3.2) nos dice que

$$\min_{N < p_r \leq 2N+H} (p_{r+1} - p_r) \leq (1 - 2\theta + 2\varepsilon)\log N$$

y por lo tanto

$$\min_{N < p_r \leq 2N+H} \frac{p_{r+1} - p_r}{\log p_r} \leq \min_{N < p_r \leq 2N+H} \frac{p_{r+1} - p_r}{\log N} \leq 1 - 2\theta + 2\varepsilon.$$

Es decir, para cualquier $\varepsilon > 0$ que nos inventemos, ese mínimo es $\leq 1 - 2\theta + \varepsilon$. Eso significa que es $\leq 1 - 2\theta$ (¡podemos inventarnos números tan pequeños como queramos!). Así,

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 1 - 2\theta$$

y como el teorema de Bombieri-Vinogradov nos da permiso para elegir cualquier $0 < \theta < 1/2$ tenemos que ese $\liminf$ es menor o igual que 0, lo que implica que sólo puede ser 0. *Quod erat demonstrandum.*

Capítulo 4

¿Y si... ?

Imaginemos que viviéramos en un mundo en el que el teorema de Bombieri-Vinogradov estuviera demostrado para algún $\theta > 1/2$.

> *¡Oh! ¡Mírame! ¡Estoy haciendo feliz a la gente! ¡Qué bien! ¡Soy un hombre mágico, del país de la gominola, de la calle de la piruleta!... Ah, por cierto, intentaba ser sarcástico.* Homer Simpson.

Entonces tomando, por ejemplo, como antes $l = \lfloor \sqrt{k} \rfloor$, podríamos elegir k tal que (ver (3.6))

$$\frac{k(2l+1)}{(k+2l+1)(l+1)}\theta > 1. \tag{4.1}$$

Para ese k, elegimos un $\mathcal{H}$ tal que $|\mathcal{H}| = k$, y que sea admisible[1]. Entonces ahora nuestro H es una constante, digamos que el mayor elemento de $\mathcal{H}$. Como hemos elegido k en función de θ y H depende de k, la constante será $c = c(\theta)$. Teniendo pues en mente que $H = c(\theta)$, consideramos la suma

$$\begin{aligned}
&\sum_{N<n\leq 2N}\left(\sum_{h\in\mathcal{H}}\varpi(n+h)-\log(3N)\right)\Lambda_R(n;\mathcal{H},k+l)^2\\
&=\sum_{N<n\leq 2N}\sum_{h\in\mathcal{H}}\varpi(n+h)\Lambda_R(n;\mathcal{H},k+l)^2\\
&-\sum_{N<n\leq 2N}\log(3N)\Lambda_R(n;\mathcal{H},k+l)^2
\end{aligned}$$

e igual que antes si resulta ser positiva entonces

$$\min_{N<p_r\leq 2N+H}(p_{r+1}-p_r)\leq H.$$

[1]Uno debería preguntarse si existe al menos un $\mathcal{H}$ admisible con $|\mathcal{H}| = k$ para cada $k > 0$. La respuesta es que sí. Por ejemplo, dado k, sea p_b el primer primo mayor que k. Entonces $\mathcal{H} = \{p_b, p_{b+1}, \ldots, p_{b+k}\}$ es admisible, pues, al ser primos, ninguno de sus elementos puede ser igual a 0 módulo cualquier primo menor o igual que k, así que esa clase siempre queda libre. Si queremos ser más elegantes, y dado que una traslación no afecta a la admisibilidad, podemos dar mejor este otro $\mathcal{H} = \{0, p_{b+1} - p_b, \ldots, p_{b+k} - p_b\}$.

Usando el lema 2 en la primera suma y el lema 1 en la segunda, nuestra expresión se convierte en

$$\begin{aligned}
&\sum_{h\in\mathcal{H}} \frac{\mathfrak{S}(\mathcal{H})}{(k+2l+1)!}\binom{2(l+1)}{l+1} N(\log R)^{k+2l+1} \\
&+\sum_{h\in\mathcal{H}} O(N(\log N)^{k+2l}(\log\log N)^c) \\
&-\log(3N)\frac{\mathfrak{S}(\mathcal{H})}{(k+2l)!}\binom{2l}{l} N(\log R)^{k+2l} \\
&-\log(3N)O(N(\log N)^{k+2l-1}(\log\log N)^c)
\end{aligned}$$

$$\begin{aligned}
&= k\frac{\mathfrak{S}(\mathcal{H})}{(k+2l+1)!}\binom{2(l+1)}{l+1} N(\log R)^{k+2l+1} \\
&-\frac{\mathfrak{S}(\mathcal{H})}{(k+2l)!}\binom{2l}{l} N(\log N)(\log R)^{k+2l} \\
&+o(N(\log N)^{k+2l}(\log\log N)^c),
\end{aligned}$$

y no es que en la última igualdad hayamos confundido la O con una o, sino que hemos aumentado el valor de la constante c un poquito.

Así, olvidando la o y recordando que $R = N^{\theta/2}$, nuestra suma inicial es asintóticamente

$$\left(\frac{k(2l+1)}{(k+2l+1)(l+1)}\theta - 1\right)\frac{\mathfrak{S}(\mathcal{H})}{(k+2l)!}\binom{2l}{l} N(\log N)(\log R)^{k+2l}$$

y sabemos por (4.1) que esto es positivo para nuestro θ y nuestras elecciones de k, l y $N = c(\theta)$.

Por lo tanto

$$\min_{N<p_r\leq 2N+H}(p_{r+1} - p_r) \leq c(\theta)$$

y tenemos que $p_{n+1} - p_n \leq c(\theta)$ para infinitos valores de n.

Más aún, supongamos que el teorema de Bombieri-Vinogradov estuviera probado para $\theta > \frac{20}{21}$, digamos $\theta = \frac{20}{21} + \alpha$ (obviamente, la conjetura de Elliott-Halberstam implicaría este hecho). Entonces vamos a ver que al menos dos de los siete enteros $\{n, n+2, n+6, n+8, n+12, n+18, n+20\}$ son primos para infinitos valores de n.

En primer lugar, si tomamos $\mathcal{H} = \{0, 2, 6, 8, 12, 18, 20\}$ vemos que es admisible. Sólo hay que ver que esos números no llenan todas las clases módulo 2, 3, 5 y 7. Ninguno es congruente con 1 módulo 2, ninguno es congruente con 1 módulo 3, ninguno es congruente con 4 módulo 5 y ninguno es congrente con 3 módulo 7.

Ahora ponemos $k = 7$ y $l = 1$ y consideramos, para ese $\mathcal{H}$, la suma

$$\begin{aligned}
&\sum_{N<n\leq 2N}\left(\sum_{h\in\mathcal{H}}\varpi(n+h)-\log(3N)\right)\Lambda_R(n;\mathcal{H},8)^2\\
&=\sum_{N<n\leq 2N}\sum_{h\in\mathcal{H}}\varpi(n+h)\Lambda_R(n;\mathcal{H},8)^2\\
&-\sum_{N<n\leq 2N}\log(3N)\Lambda_R(n;\mathcal{H},8)^2.
\end{aligned}$$

El lema 2 y el lema 1 vienen de nuevo en nuestra ayuda para dar

$$\left(\frac{21}{10}\log R-\log N\right)\frac{2}{9!}\mathfrak{S}(\mathcal{H})N(\log R)^9+o(N(\log N)^9(\log\log N)^c)$$

Queremos poner $R = N^{10/21+\xi}$ para algún $\xi > 0$. ¿Qué condiciones tiene que cumplir ξ? En primer lugar, observamos que nuestra elección respeta (1.1) siempre que $\xi < \frac{11}{21}$. En segundo lugar, la condición del lema 1, impone $N^{10/21+\xi}(\log N)^c \leq N^{1/2}$, lo cual se cumple si $\xi < \frac{1}{42}$. Por último, la condición del lema 2 dice que $N^{10/21+\xi} \leq N^{10/21+\alpha/2}$ y eso es cierto si $\xi \leq \alpha/2$. Cogiendo $\xi < \text{mín}\{1/42, \alpha/2\}$, cosa que podemos hacer, estamos salvados.

Entonces, con ese valor de R y olvidando la o, la suma es asintóticamente

$$\left(\frac{21}{10}\left(\frac{10}{21}+\xi\right)-1\right)\frac{2}{9!}\mathfrak{S}(\mathcal{H})N(\log N)(\log R)^9$$

que es positivo porque $\xi > 0$.

Esto prueba que, para N suficientemente grande, en cada intervalo $(N, 2N]$ existe un n tal que al menos 2 de los 7 números $\{n, n+2, n+6, n+8, n+12, n+18, n+20\}$ son primos. Así que hay infinitas parejas de primos que distan 20 o menos. No sólo eso, al menos una de las posibles diferencias que se pueden formar con esos 7 números (2, 4, 6, 8, 10, 12, 14, 16, 18 o 20) se tiene que repetir en infinitas ocasiones, pues si todas se dieran un número finito de veces nuestra afirmación anterior sería falsa.

Una diferencia entre primos que se repite infinitas veces...

[Ruido de despertador]

Bibliografía

[1] D. A. Goldston - Y. Motohashi - J. Pintz - C. Y. Yildirim, *Small gaps between primes exist*, Proceedings of the Japan Academy, Series A. Mathematical Sciences, Volume 82, Number 6 (June 2006).

[2] K. Soundararajan, *Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım* Mathematics ArXiv, NT/0605696v1 (27 May 2006).

[3] Andrew Granville, *A good new millenium for the primes*, Madrid Intelligencer, International Congress of Mathematicians, Madrid (August 2006).

[4] Fernando Chamizo, *Temas de teoría de números. Seminario avanzado*, Departamento de Matemáticas, UAM (2006).

[5] P. X. Gallagher, *On the distribution of primes in short intervals*, Mathematika, 23 (1976), 4-9. Corrigendum, ibid, 28 (1981), 86.

[6] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, The Clarendon Press, Oxford University Press.