Temas de teoría de números

Seminario Avanzado

Departamento de Matemáticas

UAM 2006

Lorente Fernando Colozimah 2005/2006

Revisado: Agosto 2010

Un experimento

Entre los matemáticos que tienen algún contacto casual con los libros de Física es muy fácil criticar la falta de rigor, que en algunos casos llega a ser exasperante. Posiblemente a los físicos les parecerá por su lado que los libros de Matemáticas están llenos de hipótesis ridículas y enrevesadas que ocultan las ideas principales (y eso que ninguno de ellos habrá llegado hasta el libro de teoría de conjuntos de Bourbaki, que en una de las primeras páginas establece ufano: "A es una letra").

Varios ejemplos muestran que, desde el punto de vista didáctico y psicológico, los físicos en muchos casos llevan la delantera. No es necesario ir a la divulgación, donde la diferencia es abrumadora. Por ejemplo, la demostración sin rigor del teorema de la divergencia que aparece en los libros de Física al tiempo que se transforman las ecuaciones de Maxwell, le hace sentir al lector que entiende por qué aquello funciona y que además el nombre de "divergencia" está bien puesto. Sin embargo comprender la idea matemática rigurosa lleva a unos requisitos sólidos y unos cálculos abstractos donde todo acaba cuadrando por razones desconocidas.

A lo largo de estos apuntes, y todavía más en las lecciones del curso, se experimentará tratando de inclinar la balanza ligeramente hacia la propedéutica de los físicos: las ideas predominarán sobre las demostraciones. Naturalmente no se pueden hacer Matemáticas con medias verdades o engaños, por ello se indicarán los argumentos que no son completos o las faltas de rigor. Se empleará una notación tomada del ajedrez: (!?) señala un movimiento dudoso, (?!) expresa un nivel mayor de duda y (??) es un paso desastroso.

Madrid, febrero de 2006

Notación básica

Incluso en el conjunto indudablemente protagonista de cualquier curso de teoría de números, los naturales, no hay acuerdo en la notación. Aquí consideraremos que el cero no es un número muy natural (nació después que el resto) y por tanto escribiremos:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}.$$

Alentados por las necesidades tipográficas tendremos el valor de cambiar levemente la notación clásica de las congruencias $a \equiv b \pmod{n}$ debida al gran Gauss, con el significado "$a - b$ es múltiplo de n", por $a \equiv b\ (n)$. Para el máximo común divisor de m y n usaremos la notación abreviada (m, n) que raramente inducirá a confusión con un elemento de $\mathbb{Z}^2$. Así $(m, n) = 1$ significa que m y n son coprimos.

Emplearemos continuamente la *notación de Landau* O y o para ocultar nuestro desconocimiento sobre la forma exacta de términos de error o manifestar nuestro desinterés por ella en favor de una idea sobre su tamaño. Usando esta notación $O(g)$ y $o(g)$, con g positiva en el rango de interés, representan respectivamente funciones f tales que

$$\limsup \frac{|f|}{g} < \infty \qquad \text{y} \qquad \lim \frac{f}{g} = 0.$$

El valor hacia el que tiende la variable se sobreentiende en cada caso y en este curso será típicamente ∞.

La *notación de Vinogradov* $f \ll g$ tiene el mismo significado que $f = O(|g|)$ y se muestra conveniente e intuitiva para manipular desigualdades olvidándose de las constantes. A veces se escribe $f \ll_t g$ para hacer notar que *la constante* O, esto es, el valor de $\limsup |f|/|g|$, depende de un parámetro t y puede no estar uniformemente acotada cuando t varía.

Una variante obvia de la notación de Vinogradov es $f \gg g$ (significando $g \ll f$). También se emplea con cierta frecuncia $f \asymp g$ para indicar $f \ll g \ll f$. Otro autores emplean $f \sim g$ pero entonces se enfrentan al uso más extendido de este símbolo para indicar la igualdad asintótica. Es decir, $f \sim g$ como notación para $\lim f/g = 1$.

Ejemplos: $1/x \ll 1$, $\operatorname{sen} x = O(1)$, $e^x = 1 + x + O(x^2)$ si $x \to 0$, $\int_2^x dt/\log t = (1+o(1))x/\log x \sim x/\log x$, $(x^2+O(x))/(x+o(1)) = x+o(x)$, $x \gg \log x$, $(x+3)^2 \asymp 7x^2$.

Una notación menos universal aunque bastante extendida en la teoría analítica de números es el uso de $e(t)$ para representar $e^{2\pi it}$. Está ligada a la normalización más sencilla de la *transformada de Fourier* y de su *transformada inversa*:

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e(-\xi x)\, dx \qquad \text{y} \qquad f^\vee(x) = \int_{-\infty}^{\infty} f(\xi)e(x\xi)\, d\xi.$$

La fórmula de inversión asegura $(\widehat{f})^\vee = f$.

Bibliografía general

Un libro de reciente aparición y tremendamente original es:

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

A pesar de su tamaño (615 páginas) mantiene una notoria y agradable economía en las demostraciones que en muchos puntos complementa con explicaciones muy acertadas. El lector puede encontrar allí temas que pocas veces han bajado de los artículos de investigación a los libros de texto. Incluso en los temas clásicos hay giros inesperados.

Con un contenido más clásico y con explicaciones en general muy buenas, cabe destacar:

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

Además contiene muchos ejercicios propuestos.

Un libro bastante enciclopédico con incursiones tanto en la teoría algebraica como analítica y que trata con éxito de minimizar los detalles técnicos, es:

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

La amplitud de la red mundial nos brinda un mundo de buenos textos por un gasto virtual nulo (calidad/precio=∞, aunque quien vende el *toner* tenga otro cálculo). Un curso gemelo de éste con otras direcciones, interesantes ejercicios y un último capítulo muy destacable es:

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

Otras notas electrónicas dignas de mención por la variedad de temas tratados son:

[**Elk**] N.D. Elkies. `http://www.math.harvard.edu/~elkies/M259.02/index.html`

Para los viajeros interesados en la teoría analítica de números y que tengan poco espacio en su maleta, es muy aconsejable:

[**Da**] H. Davenport. Multiplicative number theory. Third edition. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

En sólo 177 páginas explica muy bien el material clásico. El precio que debe pagar el lector es leer cada línea con cuidado.

Un libro muy cercano y de los pocos de teoría "avanzada" de números escrito en la lengua de Cervantes es:

[**Ci-Co**] J. Cilleruelo y A. Córdoba, La teoría de los números, Mondadori, Madrid, 1992.

Desafortunadamente desde hace años está descatalogado. Aparte de cubrir buena parte del material habitual, hay algunos capítulos destacables, como el dedicado a la teoría aditiva.

En el siguiente título se unen bastantes ventajas (ejercicios, buenas explicaciones, temas variados) y se puede usar, con algunas selecciones, como material para un curso de licenciatura:

[**Ro**] H.E. Rose. A course in number theory. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

Para contrarrestrar lo tendencioso de la selección anterior, nada mejor que terminar con un buen libro "algebraico" y en cualquier caso delicioso de leer:

[**Ir-Ro**] K. Ireland, M. Rosen. A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

Propaganda

Si los teoremas se vendieran en las tiendas, los autores se preocuparían de organizar bellos escaparates. Como afortunadamente no es así e incluso los libros académicos más famosos de Matemáticas tienen poca tirada, los matemáticos podemos permitirnos el lujo de escribir para un club selecto de fanáticos.

Esto no deja de tener sus ventajas, por ejemplo causa un gran respeto y tiene la virtud de alejar a molestos visitantes intempestivos, así un "Nadie entre aquí que no sepa geometría" a tiempo aleja a más intrusos que un *cave canem*.

Un peligro indudable es que lleguemos a asustarnos nosotros mismos, a nuestros estudiantes o a los visitantes bienintencionados escribiendo historias sin argumento o capítulos intermedios de una novela sin comienzo. Por poner un ejemplo, el libro "Introducción al álgebra conmutativa" de Atiyah y Macdonald verdaderamente hace honor a su título, además tiene buenas explicaciones y una gran selección de ejercicios, pero ¿qué cosas podríamos poner en el escaparate? ¿qué le podríamos contar a Gauss? En la página 25 se da la definición de sucesión exacta, en la 26 el lema de la serpiente, en la 27 ya hemos pasado a la definición de producto tensorial por su propiedad universal de factorización. Se pide al lector que pruebe que el homomorfismo borde está bien definido, y evidentemente puede hacerlo combinando definiciones, y puede resolver todos los ejercicios del libro pero lo que sobre todo se le exige al lector es que tenga una fe blindada y mantenida hasta un curso de topología en el que el borde sea el borde. ¿Para qué escribir $\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}\big(M, \mathrm{Hom}(N, P)\big)$ (página 32) para indicar que al fijar una variable en una función que tiene dos, se queda sólo con una? El estudiante que supere esta ardua disciplina lingüística esta capacitado para entender los poéticos teoremas futuros, pero ¿no puede haberse quedado alguien valioso desalentado por el camino? Hay demasiadas pirámides invertidas y la sombra de su construcción oculta el punto de apoyo. No hay lugar para tantos teoremas egoístas que responden a preguntas naturales en contextos antinaturales.

Otro peligro es la especialización como excusa para la ignorancia impenitente o la petulancia, y si nos fiamos de Ortega y Gasset cuando coge bríos en su capítulo "La barbarie del especialismo" (de su obra "La rebelión de las masas"): "El resultado más inmediato de este especialismo *no compensado* ha sido que hoy, cuando hay mayor número de 'hombres de ciencia', hay muchos menos 'hombre cultos' que, por ejemplo, hacia 1750". Más allá de esta exageración, ¿no es triste que pueda haber catedráticos de análisis que apenas conozcan una palabra de álgebra, o viceversa? ¿No es aún más triste que se pueda cercenar la educación de un estudiante de Matemáticas permitiéndole que no vea nunca un grupo de Galois o una serie de Fourier?

En las siguientes líneas se muestra un pequeño escaparate con algunos resultados de propaganda que se probarán en el curso[1] y que añaden algo a nuestro conocimiento previo sin necesidad de concatenar definiciones de crucigrama. El lector puede juzgar el género

[1]Nota de 2010: El curso se quedó un poco más corto de lo previsto. Aprovecho para agradecer la atención de todos los asistentes con una mención especial a Carlos Vinuesa que me hizo notar muchas erratas en estas notas.

y tomar su decisión. Los supervivientes del curso, hayan sido las explicaciones buenas o malas, por el hecho de haberlo soportado, no tendrán dudas al final y engrosarán el número de los creyentes indubitados. Su fe se tornará en devoción.

¿Se puede decir algo sobre los primos gemelos?

En primer lugar qué son. Nada más que primos impares consecutivos como 3 y 5 o 101 y 103. Se cree que hay infinitos pero habida cuenta que ya tenemos bastantes problemas al pelear con los primos de uno en uno, no estamos como para enfrentarnos a parejas de ellos. No obstante, V. Brun en 1919 demostró que el espaciamiento medio entre parejas de primos gemelos es al menos del orden del cuadrado del espaciamiento medio entre primos y formuló su resultado de una manera más débil pero espectacular: la suma de los inversos de los primos gemelos converge. Con un ordenador y un análisis teórico del error se puede aproximar el límite obteniéndose:

$$\sum_{p \text{ gemelos}} \frac{1}{p} = 1'9021602\ldots$$

¿No es fantástico que uno pueda probar algo de este tipo? Y lo es más sabiendo que en la prueba no se utiliza ninguna finura acerca de la distribución de los primos. Es puramente combinatoria, elemental pero no sencilla. En última instancia se basa en quitar los números n tales que él y $n+2$ tengan factores primos pequeños. Con métodos más avanzados se demuestra que hay infinitos primos p (de hecho un infinito relativamente grande) tales que $p+2$ tiene a lo más dos factores primos.

La venganza contra Goldbach

Es bien conocida la conjetura de Goldbach[2] de que todo número para mayor que 2 se puede escribir como suma de dos primos ($14 = 7+7$, $16 = 3+13$, $18 = 7+11$), y también es conocido, para cualquiera con inquietud aritmética suficiente para estar leyendo este párrafo, que constituye un problema abierto hasta nuestros días. Como en otros problemas de nuestra rigurosa área, todo parece confabularse contra nosotros para que nos quedemos cerca pero no lleguemos. No obstante, con pócimas a base de sesos de matemático, sangre de tinta y pasta de árbol, se han conseguido algunos resultados asombrosos que conceden una pequeña revancha frente a Goldbach. Por ejemplo, si damos por perdida la batalla y pensamos que la conjetura de Goldbach puede fallar para algunos números, ¿en qué proporción podría ser? ¿para menos de un 10 %? ¿para menos de un 2 %? ¿o para un 0'123 %? Resulta que podemos probar que falla en un 0 % de los casos. Esto evidentemente involucra un límite:

$$\lim_{N\to\infty} \frac{\#\{n \leq N \text{ con } 2n \neq p_1 + p_2\}}{N} = 0.$$

Incluso se puede demostrar que este límite tiende con cierta velocidad a cero.

[2]En realidad en los tiempos de Euler y Goldbach se consideraba el uno como número primo, de manera que la formulación actual de las conjeturas que hizo Goldbach, conlleva una leve adaptación.

Goldbach también conjeturó que todo número impar mayor que 5 es suma de tres primos. Pues bien, en eso casi se ha vencido porque I.M. Vinogradov probó en 1937 que a partir de cierto número grande (actualmente se sabe que grande $\approx 10^{43000}$, demasiado para un ordenador) esta conjetura es cierta. Todavía más, probó que el número de representaciones de un N impar como suma de tres primos se aproxima bien por

$$\frac{N^2}{2(\log N)^3}\prod_{p\not| N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)$$

en el sentido de que el cociente de ambas cantidades tiende a uno. Por alguna misteriosa razón el número de representaciones depende de la factorización. Por otro lado, es asombroso que la demostración original y natural de estos resultados requiera integrales, y en última instancia entender bien qué tipo de resonancias e interferencias puede haber entre osciladores armónicos de frecuencias primas.

El tercer grado

Si queremos estudiar las soluciones racionales de ecuaciones diofánticas de dos variables (esto es lo mismo que resolver ecuaciones diofánticas homogéneas de tres variables), aspirando a ser ordenaditos, podemos dosificar nuestro esfuerzo haciendo una clasificación por el grado de la ecuación.

El caso de primer grado $ax + by = c$ es trivial: se puede despejar "racionalmente" una variable en términos de las otras y dar valores. El caso de segundo grado es un poco más complicado, pero una vez que sabemos si existe una solución (lo cual se puede decidir en tiempo finito resolviendo ciertas congruencias) se parametrizan todas, como en el caso de grado uno. Así por ejemplo todas las soluciones racionales de $x^2 + y^2 = 1$ vienen dadas por $x = (t^2 - 1)/(t^2 + 1)$, $y = 2t/(t^2 + 1)$ para $t = \mathbb{Q}$ ó $t = \infty$.

El caso de grado tres es mucho más complejo y hasta la fecha nadie sabe de ningún algoritmo que permita decidir sin género de dudas en cualquier ejemplo si hay un número finito o infinito de soluciones (para el caso de grado mayor que tres –no reducible a grado menor– hay un profundísimo teorema de calibre medalla Fields, por el que se sabe que el número es siempre finito). Lo más llamativo es que las posibles soluciones tienen una estructura riquísima y el problema aritmético tiene fructíferas interpretaciones algebraicas y geométricas. Una primera reducción es que toda ecuación diofántica "verdaderamente" cúbica se puede escribir tras un cambio de variable como $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$ así que uno puede limitarse a estudiar ese caso.

A modo de ejemplo, digamos que buscamos dos números racionales, un cuadrado perfecto y un cubo perfecto de forma que el primero difiera del segundo en una unidad. En símbolos:

$$y^2 = x^3 + 1.$$

A simple vista se tienen soluciones como $(0, 1)$ o $(2, 3)$. Y podemos "verlas" mejor si las dibujamos como puntos en la curva cúbica definida por la ecuación. Un procedimiento antiguo e ingenioso para hallar un nueva solución a partir de dos consiste en construir la recta que las une y calcular el tercer punto de intersección con la cúbica. En nuestro

caso, a partir de $(0,1)$ y $(2,3)$ se obtiene $(-1,0)$. Nada espectacular. Podemos también aplicar la simetría $y \leftrightarrow -y$ o construir la tangente en una solución (ésta es la recta que pasa por ella y por ella misma). Pero en este ejemplo obtenemos sólo cinco soluciones (y un infinito) porque los puntos acaban "rebotando" unos en otros y se repiten. ¿Es casualidad que estos puntos sean enteros? ¿no buscábamos soluciones racionales? Pues bien, no hace falta esperar al redoble de tambor: el teorema de Lutz-Nagell implica que si un conjunto finito de puntos solución no da soluciones nuevas al proceder como antes, entonces todas las coordenadas son ¡enteras! Además establece un método para encontrar en cualquier ejemplo un conjunto finito maximal de estos puntos.

¿Y si hay infinitas soluciones? Entonces unos pocos puntos que rebotan no pueden ser toda la historia y los denominadores aparecen indefectiblemente. En este caso el teorema de Mordell-Weil nos da un consuelo para matemáticos: el procedimiento anterior de secantes, tangentes y simetrías permite llegar a cualquier solución a partir de un número finito de ellas convenientemente seleccionado. Pero aquí este "convenientemente" permanece sumido en un gran misterio algorítmico. Si uno escarba encuentra nombres raros, y grupos raros, y viene la alianza con las formas modulares y la teoría de Galois, y el último teorema de Fermat... pero hablar de ello aquí es demasiado pretencioso.

Índice general

Capítulo 1

Funciones aritméticas

1.1. Introducción

Ejemplos básicos. Series de Dirichlet. Inversión de Möbius.

Hablar de *funciones aritméticas* en general, no es decir demasiado ya que se conoce bajo esta denominación cualquier función cuyo dominio son los naturales de toda la vida, $f : \mathbb{N} \longrightarrow \mathbb{C}$. La mayor parte de las veces la imagen también estará dentro de $\mathbb{N}$, o al menos de $\mathbb{R}$.

Entre las funciones aritméticas tienen especial interés las que dependen de la factorización en primos.

Definición: Se dice que una función aritmética f es *multiplicativa* si $f(nm) = f(n)f(m)$ siempre que n y m sean coprimos, y se dice que es *completamente multiplicativa* si $f(nm) = f(n)f(m)$ es cierto en general.

Si n se descompone en primos como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ entonces cualquier f multiplicativa verifica

$$f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i}). \tag{1.1}$$

Por convenio se toma $f(1) = 1$.

Uno de los ejemplos más relevantes de funciones multiplicativas es la *función de Möbius* que tiene la extraña definición $\mu(1) = 1$, $\mu(p) = -1$ y $\mu(p^\alpha) = 0$ para $\alpha > 1$. Esto es

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

Por tanto μ^2 es la función característica de los *libres de cuadrados* (los no divisibles por ningún cuadrado mayor que 1).

Hay otras funciones sencillas multiplicativas (aunque comprobar que lo son por ahora no sea obvio) que tienen un puesto de palco en los textos de teoría de números:

- $d(n) = \#\{d \,:\, d|n\}$ (función divisor)
- $\sigma(n) = \sum_{d|n} d$
- $\phi(n) = \{1 \le m \le n \,:\, (m,n) = 1\}$ (función ϕ de Euler)
- $\lambda(n) = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r}$ si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ (función de Liouville).

De todas estas funciones, sólo la de Liouville es completamente multiplicativa.

Entre las funciones aritméticas no multiplicativas tiene especial interés la llamada *función de von Mangoldt*

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^\alpha \\ 0 & \text{en otro caso} \end{cases}$$

También cabe mencionar dos funciones relacionadas con la distribución de los primos:

$$\pi(n) = \#\{p \le n\} = \sum_{p \le n} 1, \qquad \psi(n) = \sum_{m \le n} \Lambda(m).$$

En realidad estas funciones se suelen extender a funciones no aritméticas $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ escribiendo $\pi(x) = \pi([x])$ y $\psi(x) = \psi([x])$, con $[\,\cdot\,]$ denotando la parte entera. Seguiremos la misma política en otras funciones que expresan sumas o promedios.

A cada función aritmética f se le puede asociar una *serie de Dirichlet* formal[1]

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

La serie de Dirichlet asociada a la función idénticamente uno es la famosa función ζ *de Riemann*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(en rigor esto sólo define el trozo de la función ζ correspondiente a $\Re(s) > 1$).

De acuerdo con lo anterior, una función es multiplicativa si y sólo si se tiene la igualdad formal (ejercicio)

$$D_f(s) = \prod_p D_{f,p}(s) \qquad \text{con} \qquad D_{f,p}(s) = 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \ldots \tag{1.2}$$

Se dice que esta expresión es un *producto de Euler*. En el caso de la función ζ, para $\Re(s) > 1$ se puede sumar la progresión geométrica $D_{f,p}(s)$ y llegar a la igualdad de series convergentes

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \tag{1.3}$$

[1] Aquí "formal" significa que nos despreocupamos de la convergencia. Para algunas funciones puede que no converja para ningún valor.

que es el producto de Euler por antonomasia. Usando un poco de análisis[2] se tiene $\zeta(2) = \pi^2/6$, en particular

$$\frac{6}{\pi^2} = \prod_p (1 - p^{-2}).$$

Impresionante, a un lado la razón entre longitud de la circunferencia y diámetro, y al otro los primos. Además empleando que $6/\pi^2$ es irracional ([Sp] cap. 16) se concluye que ¡hay infinitos primos! Euclides y los pitagóricos temblarían de terror.

Dadas dos funciones aritméticas f y g se define su *convolución* como

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

Nótese que es conmutativa (ejercicio).

Es sencillo comprobar que si $f(1) = g(1) = 1$

$$D_f(s)D_g(s) = D_{f*g}(s) \quad \text{y que} \quad D_{f,p}(s)D_{g,p}(s) = D_{f*g,p}(s).$$

Por tanto, empleando (1.2), hemos probado:

Proposición 1.1.1 *Si f y g son multiplicativas entonces $f * g$ también lo es y su serie de Dirichlet es $D_f(s)D_g(s)$.*

Antes de poner ejemplos, concedámonos una pausa para digerir las definiciones y dar un vistazo a la brújula de la intuición. Las funciones generatrices son un instrumento natural para tratar problemas aditivos. Así, cuando uno considera $f(x) = \sum_{a\in A} x^a$ (la función generatriz de A) su cuadrado tiene como coeficientes el número de representaciones como $a + a'$, y si multiplicamos f por $\sum_{b\in B} x^b$ se obtiene el número de representaciones de la forma $a + b$. En problemas multiplicativos estas funciones generatrices no sirven, porque al multiplicar se suman los exponentes, no se multiplican. La idea es intercambiar el papel que desempeñan a y x, si el exponente es el mismo, las bases se multiplicarán y eso es justamente una serie de Dirichlet. Lo de escribir $-s$ en lugar de x, es inofensivo.

Ejemplo. La función divisor es multiplicativa por ser convolución de dos funciones idénticamente uno, $d(n) = \sum_{d|n} 1$, y σ es multiplicativa por ser convolución con la identidad. En general $\sigma_k(n) = \sum_{d|n} d^k$ es multiplicativa (convolución de $f(n) = n^k$ y $g = 1$). Por ejemplo, la suma de los cuadrados de los divisores de un millón es

$$\sigma_2(10^6) = \sigma_2(2^6)\sigma_2(5^6) = (1^2 + 2^2 + \cdots + 2^{12})(1^2 + 5^2 + \cdots + 5^{12}) = (2^{14} - 1)(5^{14} - 1)/72.$$

Cuando (1.2) se aplica a la función μ se tiene $D_\mu(s) = \prod(1 - p^{-s})$ que combinado con (1.3) se puede leer como $\zeta(s)D_\mu(s) = 1$. Esta humilde relación permite invertir la convolución con 1:

$$\zeta(s)D_f(s) = D_{1*f}(s) \quad \Rightarrow \quad D_f(s) = D_\mu(s)D_{1*f}(s).$$

Escrito sin tantos símbolos:

[2] Por ejemplo la fórmula producto del análisis complejo $\operatorname{sen}(\pi x) = \pi x \prod_{n=1}^{\infty}(1 - x^2/n^2)$, o la identidad de Parseval aplicada al desarrollo de Fourier de la parte fraccionaria (véase [Co] para una prueba elemental).

Proposición 1.1.2 (Inversión de Möbius) *Dada una función aritmética f, sea la función $F(n) = \sum_{d|n} f(d)$, entonces $f(n) = \sum_{d|n} \mu(d)F(n/d)$.*

Observación: Desde el punto de vista histórico la inversión de Möbius original era la fórmula $F(x) = \sum_{n\leq x} f(x/n) \Rightarrow f(x) = \sum_{n\leq x} \mu(n)F(x/n)$ (véase [El] Th. 1.9).

Ejemplo. Se cumple $n = \sum_{d|n} \#\{1 \leq k \leq n \ : \ (n,k) = d\}$ (porque todo número tiene algún máximo común divisor con n). Entonces

$$n = \sum_{d|n} \#\{1 \leq l \leq n/d \ : \ (n/d, l) = 1\} = (1 * \phi)(n)$$

de donde $\phi(n) = (\mu * \mathrm{Id})(n) = \sum_{d|n} \mu(d)n/d$ y se concluye que ϕ es multiplicativa. De ello y (1.1) se sigue la fórmula bien conocida:

$$\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \prod_j \big(p_j^{\alpha_j - 1}(p_j - 1)\big).$$

La importancia de la función Λ de von Mangoldt proviene de que da los coeficientes de la serie de Dirichlet de $-\zeta'/\zeta$, que es crucial en la demostración del teorema de los números primos. Tomando logaritmos en (1.3), derivando y usando la suma de una progresión geométrica (todo esto tiene sentido en $\Re(s) > 1$)

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

Multiplicando por $\zeta(s)$ en ambos miembros, se deduce

$$\log n = \sum_{d|n} \Lambda(d)$$

y por inversión de Möbius,

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

Simbólicamente $\log = 1 * \Lambda$ y $\Lambda = \mu * \log$. La primera igualdad conecta una función de las de cálculo de toda la vida (el logaritmo) con algo que depende de los primos (la función Λ). Sólo jugando adecuadamente con esta relación ya es posible avanzar un poco en el estudio de la distribución de los primos.

1.2. Promedios de funciones aritméticas

Sumación por partes. Fórmula de sumación de Abel. Teorema de Wirsing.

Los valores que toman algunas de las funciones aritméticas más habituales son bastante caóticas pero podemos "domesticarlas" tomando promedios, lo que nos puede

ayudar a formarnos una idea global más acertada. Si la función viene dada por una suma sobre los divisores es pertinente emplear la identidad elemental:

$$\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\big[\frac{x}{n}\big] \tag{1.4}$$

cuya prueba se reduce a invertir el orden de sumación.

Raramente sabremos evaluar los promedios, y consideraremos suficiente una aproximación con un buen término de error, es ahí donde entra la notación de Landau.

Aplicando (1.4) a $f(n) = \Lambda(n)$ y teniendo en cuenta que $\log = 1 * \Lambda$, se obtiene un ejemplo espectacular:

$$\sum_{n\le x} \log n = \sum_{n\le x} \Lambda(n)\big[\frac{x}{n}\big].$$

La primera suma se puede aproximar por la integral [Sp] cap. 22 (más adelante veremos algo más preciso) que es $x\log x + O(x)$. Empleando que $[t/n] - 2[t/2n] = 1$ para $t/2 < n \le t$ se deduce $\sum_{t/2<n\le t}\Lambda(n) = O(t)$ y de aquí $\sum_{n\le x}\Lambda(n) = O(x)$. Esto permite quitar sin gran peligro la parte entera en el segundo miembro y obtener la llamativa *fórmula de Mertens*

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1) \tag{1.5}$$

donde se ha acumulado la contribución de p^k con $k > 1$ en la constante.

Ejemplo. La función ϕ, como función multiplicativa que es, toma valores ligados a la factorización, lo que causa variaciones tan drásticas como $\phi(210) = 48$, $\phi(211) = 210$. Introduciendo la fórmula $\phi(n) = \sum_{d|n}\mu(d)n/d$ en (1.4) se obtiene

$$\sum_{n\le x}\frac{\phi(n)}{n} = \sum_{d\le x}\frac{\mu(d)}{d}\big[\frac{x}{d}\big] = \sum_{d\le x}\frac{\mu(d)}{d}\big(\frac{x}{d} + O(1)\big) = x\sum_{d\le x}\frac{\mu(d)}{d^2} + O(\log x).$$

Recordando que $D_\mu(s) = 1/\zeta(s)$, $\zeta(2) = \pi^2/6$, y empleando $\sum_{d>x} d^{-2} = O(x^{-1})$ se llega a

$$\sum_{n\le x}\frac{\phi(n)}{n} = \frac{6}{\pi^2}x + O(\log x).$$

Esta fórmula no está en el limbo de las aproximaciones asintóticas que sólo aproximan para infinitos muy infinitos. Con un pequeño programa se tiene que $\sum_{n\le 100}\phi(n)/n = 60'83268\ldots$ que no está lejos, en términos relativos de $600/\pi^2 = 60'7927\ldots$

Se podría juzgar, con razón, que un promedio de ϕ más natural es $x^{-1}\sum_{n\le x}\phi(n)$, en vez de la expresión del ejemplo anterior. Como $\phi(n)$ es "en media" $6n/\pi^2$ entonces $x^{-1}\sum_{n\le x}\phi(n)$ debe ser (?!) como $x^{-1}\sum_{n\le x} 6n/\pi^2 \sim 3x/\pi^2$. Esto es cierto y también demostrable. El artificio para poner o quitar coeficientes no oscilatorios se conoce bajo el nombre genérico de *sumación por partes*. Merece la pena detenerse en dos versiones: una discreta y otra continua (hasta cierto punto).

Lema 1.2.1 (Sumación por partes) *Se cumple la identidad*

$$\sum_{n=1}^{N} a_n b_n = a_N S_N + \sum_{n=1}^{N-1} (a_n - a_{n+1}) S_n$$

donde $S_n = \sum_{k=1}^{n} b_k$.

Demostración: Basta escribir $b_n = S_n - S_{n-1}$ y agrupar convenientemente los términos. □

Un uso habitual de la sumación por partes es deshacerse de coeficientes monótonos.

Corolario 1.2.2 *Si* $(a_n)_{n=1}^{N}$ *es una sucesión real monótona no creciente y positiva, entonces*

$$\big|\sum_{n=1}^{N} a_n b_n\big| \leq a_1 \sup_{1\leq n\leq N} |S_n|.$$

En la variante "continua" aparece una integral.

Lema 1.2.3 (Lema de Abel) *Sea* $(c_n)_{n=1}^{\infty}$ *una sucesión arbitraria de números complejos y sea* $C(t) = \sum_{n\leq t} c_n$. *Dado* $x \geq 1$, *para cualquier* $g : [1,\infty) \longrightarrow \mathbb{C}$, $g \in C^1$, *se verifica*

$$\sum_{n\leq x} c_n g(n) = C(x)g(x) - \int_1^x C(t)g'(t)\, dt.$$

Demostración: Por continuidad podemos suponer que x no es entero, entonces el primer miembro es $\int_{1/2}^{x} h(t)g(t)\, dt$ con $h(t) = \sum c_n \delta(t-n)$ y δ la delta de Dirac. Como (?!) $C'(t) = h(t)$, el lema de Abel se reduce a integrar por partes. □

Para aplicar la primera versión al promedio de ϕ, tomemos $a_n = n$ y $b_n = \phi(n)/n$, entonces se sigue

$$\begin{aligned}\sum_{n=1}^{N} \phi(n) &= N\big(\frac{6N}{\pi^2} + O(\log N)\big) - \sum_{n=1}^{N-1} \big(\frac{6n}{\pi^2} + O(\log n)\big) \\ &= \frac{6}{\pi^2}\big(N^2 - \frac{N(N-1)}{2}\big) + O(N\log N) = \frac{3N^2}{\pi^2} + O(N\log N)\end{aligned}$$

que coincide con nuestras expectativas.

Por otra parte, el Lema de Abel con $c_n = \phi(n)/n$ y $g(x) = x$ lleva a un cálculo similar:

$$\begin{aligned}\sum_{n\leq x} \phi(n) &= x\big(\frac{6x}{\pi^2} + O(\log x)\big) - \int_1^x \big(\frac{6t}{\pi^2} + O(\log t)\big)\, dt \\ &= \frac{6}{\pi^2}\big(x^2 - \frac{x^2}{2}\big) + O(x\log x) = \frac{3x^2}{\pi^2} + O(x\log x).\end{aligned}$$

La sumación por partes es útil pero no la panacea. Por ejemplo, no podemos deducir el comportamiento de $\sum_{n\le x} t_n$ a partir de $\sum_{n\le x} t_n/n = 1+o(1)$, o lo que es lo mismo de $\sum_{n=1}^{\infty} t_n/n = 1$, porque hay muchas formas de hacer que la suma de la serie infinita sea uno. Por ejemplo $t_1 = 1$, $t_n = 0$ si $n > 1$ que cumple $\sum_{n\le x} t_n = 1$ o $t_n = (-1)^{n+1}/\log 2$ para los que $\sum_{n\le x} t_n$ tiene un comportamiento oscilante. Estos ejemplos prueban que ni siquiera $\sum_{n\le x} t_n/n = 1+O(x^{-1})$ puede llevarnos a deducir el comportamiento asintótico de $\sum_{n\le x} t_n$. Veamos qué parte de la maquinaria salta cuando aplicamos el lema de Abel con $c_n = t_n/n$ y $g(x) = x$:

$$\sum_{n\le x} t_n = x\big(1+O(x^{-1})\big) - \int_1^x \big(1+O(t^{-1})\big)\,dt = O(\log x).$$

Los términos principales se volatilizan y lo que resta es absorbido por el término de error. Nos chocamos contra un muro similar cuando intentamos deducir la asintótica de $\pi(x)$ a partir de la fórmula de Mertens (1.5), es analíticamente imposible, necesitaríamos más información.

Las técnicas de sumación por partes no son coto privado de la funciones aritméticas, uno puede emplearlas como un instrumento natural del análisis.

Ejemplo. Aplicando el lema de Abel con $c_n = 1$ y $g(t) = 1/t$ se deduce

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

Escribiendo la integral como $\int_1^x = \int_1^\infty - \int_x^\infty = \text{cte} + O(1/x)$, se concluye el resultado clásico $\sum_{n\le x} n^{-1} = \log x + \gamma + O(1/x)$, donde $\gamma = 0'577\ldots$ es una constante llamada *constante de Euler*, [Sp] p. 566.

Ejemplo. Eligiendo $c_n = 1$ y $g(n) = \log n$, se tiene (tómese $x = N \in \mathbb{N}$)

$$\log N! = N\log N - \int_1^N [t]t^{-1}\,dt = N\log N - N + O(\log N).$$

Incluso se puede ir un poco más lejos. Manipulando la integral mediante integración por partes se deduce

$$\log N! = N\log N - N + \frac{1}{2}\log N + K - \int_N^\infty h(t)t^{-2}\,dt$$

donde $h(t)$ es la función periódica $1/6+\int_0^t (x-[x]-1/2)\,dx$. No es fácil identificar la constante K que se prueba que es $\frac{1}{2}\log(2\pi)$. Esto es suficiente para concluir la *aproximación de Stirling*:

$$N! \sim \sqrt{2\pi N}N^N e^{-N}.$$

Integrando por partes más veces se obtienen aproximaciones en las que el error relativo tiende a cero tan rápido como una potencia negativa arbitraria fijada (aunque el error absoluto no está acotado). El desarrollo "completo" de la aproximación depende de los números de Bernoulli [Sp] p. 713.

A medio camino entre el análisis y la artimética hay algunas aplicaciones de la sumación por partes relacionadas con la función ζ que son particularmente útiles. En primer lugar, tomando $c_n = 1$ y $g(x) = x^{-s}$ en el Lema de Abel (véase [Da] p. 32 si se quiere usar el Lema 1.2.1) se obtiene $\sum_{n=1}^{\infty} n^{-s} = s\int_1^{\infty}[x]x^{-s-1}\,dx$, que maquillado un poco se puede escribir como

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{\mathrm{Frac}(x)}{x^{s+1}}\,dx. \tag{1.6}$$

Nótese que aunque originalmente $\zeta(s)$ sólo estaba definida para $\Re(s) > 1$, el segundo miembro permite extender la definición a $\Re(s) > 0$ y así se tiene que ζ se puede considerar como una función meromorfa[3] en $\Re(s) > 0$ con un único polo en $s = 1$. Con un poco de ingenio se puede integrar por partes (sacando la basura que pueda ensuciar la convergencia) y conseguir una extensión meromorfa a todo $\mathbb{C}$ de manera que $\zeta(s) - 1/(s-1)$ sea entera. Normalmente se llama función ζ de Riemann al fruto de esta extensión.

El mismo argumento aplicado a $-\zeta'(s)/\zeta(s)$ conduce a la fórmula:

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{s}{s-1} + s\int_1^{\infty} (\psi(x) - x)x^{-s-1}dx. \tag{1.7}$$

A pesar de que (1.1) nos dice que una función multiplicativa f está determinada por sus valores en los primos y sus potencias, no parece nada claro que haya una relación entre promediar f sobre los primos y sus potencias y promediar la función sobre todos los números. Hay sin embargo algunas desigualdades obvias que se pueden establecer. Por ejemplo, si suponemos que f es completamente multiplicativa y $|f(p)| < \mathrm{cte} < 1$

$$\sum_{n\le x} f(n) \le \prod_{p\le x} \big(1 + f(p) + f(p^2) + \dots\big) = \prod_{p\le x} \big(1 - f(p)\big)^{-1}.$$

Tomando logaritmos se sigue $\log\sum_{n\le x} f(n) \le \sum_{p\le x} f(p) + \dots$ donde los puntos suspensivos son controlables si $f(p)$ tiende a cero. Todavía más, bajo buenas condiciones no debería haber gran diferencia entre $\log\sum_{n\le x} f(n)$ y $\sum_{p\le x} f(p)$. ¿Qué significa lo de "buenas condiciones"? En primer lugar que las potencias de los primos no molesten mucho, y en segundo lugar que se tenga un comportamiento adecuado de $\sum_{p\le x} f(p)$ (que $f(p)$ tienda correctamente a cero). E. Wirsing [Wi] logró materializar estas ideas en un teorema que, bajo ciertas hipótesis, traslada la asintótica de $\sum_{p\le x} f(p)$ a la de $\sum_{n\le x} f(n)$.

La versión que veremos aquí es una adaptación de la incluida en [Iw-Ko], ésta admite hipótesis más débiles que la formulación original. Además resuelve de forma elegante el tratamiento conjunto de los primos y sus potencias considerando la función de von Mangoldt generalizada $\Lambda_f(n)$ que se define formalmente como:

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

[3] Si uno quiere ser pedante, la integral es holomorfa por el teorema de Morera

Como contrapartida algunas manipulaciones previas en algunos ejemplos concretos (para el teorema en su forma más conocida y su demostración véase [Po] o el original [Wi]).

Teorema 1.2.4 (Wirsing) *Sea f una función aritmética multiplicativa tal que*

$$\sum_{n\le x}\Lambda_f(n)=\kappa\log x+C+o(1)\qquad y\qquad \sum_{n\le x}|f(n)|\ll(\log x)^{|\kappa|}$$

para algún $\kappa\in\mathbb{R}$. Entonces

$$\sum_{n\le x}f(n)=K(\log x-C)^{\kappa}+o((\log x)^{|\kappa|-1})$$

donde K es la constante

$$K=\frac{1}{\Gamma(\kappa+1)}\prod_p\big((1-p^{-1})^{\kappa}(1+f(p)+f(p^2)+f(p^3)+\dots)\big).$$

Además el resultado también se cumple si se sustituye en la hipótesis y la conclusión "o" por "O" (en ese caso la C es superflua).

Observación: Nótese que el resultado sólo da una fórmula asintótica para $\kappa\ge -1/2$.

Aquí $\Gamma(z)$ es la *función Gamma*, $\int_0^\infty t^{z-1}e^{-t}\,dt$ para $\Re z>0$, que generaliza el factorial, $\Gamma(N+1)=N!$, y puede extenderse a una función homomorfa y sin ceros en $\mathbb{C}-\{0,-1,-2,\dots\}$ por medio de $\Gamma(z+1)=z\Gamma(z)$.

Demostración: Todo el truco está en emplear $f\log=f*\Lambda_f$ para relacionar $\sum\Lambda_f(n)$ con $\sum f(n)$:

$$\begin{aligned}\sum_{n\le x}f(n)\log n &= \sum_{n\le x}f(n)\sum_{m\le x/n}\Lambda_f(m)\\ &= (\kappa\log x+C)\sum_{n\le x}f(n)-\kappa\sum_{n\le x}f(n)\log n+o\big((\log x)^{|\kappa|}\big).\end{aligned}$$

Escribamos para abreviar $g(x)=\sum_{n\le x}f(n)$. Gracias al Lema de Abel se puede relacionar $\sum_{n\le x}f(n)\log n$ con $g(x)$, simplemente es igual a $g(x)\log x-\int_1^x g(t)t^{-1}\,dt$. Sustituyendo en la igualdad anterior se tiene que

$$\Delta(x)=(\log x-C)g(x)-(\kappa+1)\int_{x_0}^x g(t)t^{-1}\,dt$$

es muy pequeño, $o((\log x)^{|\kappa|})$. Ahora vamos a despejar g. Para ello lo mejor es soñar que todo es derivable (?!) y reducir el problema a una ecuación diferencial ordinaria en la que la incógnita es $g=g(x)$

$$\Delta'(x)=(\log x-C)g'(x)-\kappa g(x)x^{-1}.$$

Multiplicando por el factor integrante $(\log x-C)^{-\kappa-1}$ se tiene

$$\Delta'(x)(\log x-C)^{-\kappa-1}=\big((\log x-C)^{-\kappa}g(x)\big)'$$

que integrando conduce a

$$g(x) = \Delta(x)(\log x - C)^{-1} + (\kappa+1)(\log x - C)^{\kappa} \int_{x_0}^{x} \Delta(t)(\log t - C)^{-\kappa-2} t^{-1}\, dt.$$

Supongamos $\kappa \geq -1/2$, que es el único caso de interés. Si se completa la integral añadiendo la porción $\int_x^\infty$ se obtiene una constante y se pierde un factor $o((\log x - C)^{|\kappa|-\kappa-1})$. Lo cual prueba

$$g(x) = K(\log x - C)^{\kappa} + o((\log x)^{|\kappa|-1}).$$

El cálculo de la constante se lleva a cabo indirectamente. Sumando por partes se tiene

$$D_f(s) = s\int_1^\infty g(t)t^{-s-1}\, dt = Ks\int_1^\infty (\log t)^{\kappa}\big(1 + O((\log t)^{-1/4})\big)t^{-s-1}\, dt$$

que usando la fórmula $\Gamma(\kappa+1) = s^{\kappa+1}\int_1^\infty (\log t)^{\kappa} t^{-s-1}\, dt$ produce

$$K\Gamma(\kappa+1) \sim s^{\kappa} D_f(s) \sim (\zeta(s+1))^{-\kappa} D_f(s) = \prod_p \big((1-p^{-1})^{\kappa}(1+f(p)+f(p^2)+f(p^3)+\dots)\big)$$

cuando $s \to 0^+$. tomando límites se termina la evaluación de la constante. □

Veamos primero un par de ejemplos sencillos sólo para tantear por dónde respira el teorema.

Ejemplo. Si $f(n) = |\mu(n)|/n$ entonces tomando derivadas logarítmicas en $D_f(s) = \prod(1 + p^{-s-1})$ se sigue $\Lambda_f(p^k) = -(-p)^{-k}\log p$ y es cero en otro caso. Sabemos que

$$\sum_{n\leq x} \Lambda_f(n) = \log x + O(1)$$

y trivialmente $\sum_{n\leq x} f(n) \ll \log x$. La conclusión del Teorema de Wirsing es

$$\sum_{n\leq x} \frac{|\mu(n)|}{n} \sim \prod \big((1-p^{-1})(1+p^{-1})\big)\log x = \frac{6}{\pi^2}\log x.$$

En realidad la aplicación del Teorema de Wirsing es ridícula porque un argumento elemental (ejercicio) ya conduce a $\sum_{n\leq x} |\mu(n)| \sim 6x/\pi^2$ y basta sumar por partes.

Ejemplo. La fórmula de Mertens (1.5) implica, usando el teorema de Wirsing con $f(n) = 1/n$ que $\sum_{n\leq x} n^{-1} = \log x + O(1)$ (aquí $K = \kappa = 1$). Esto no es nada espectacular y ya lo habíamos obtenido en una versión más refinada $\sum_{n\leq x} n^{-1} = \log x + \gamma + O(x^{-1})$. Podemos ahora dar la vuelta al teorema con $C = -\gamma$ y concluir que

$$\lim_{x\to\infty}\left(\log x - \sum_{n\leq x}\frac{\Lambda(n)}{n}\right) = \gamma$$

si el límite existe. De hecho es fácil asegurar la existencia del límite a partir del teorema de los números primos (que aunque no se ha enunciado, seguro que el lector conoce). Aparentemente esta igualdad tan limpia no aparece reflejada en la literatura (por ejemplo [In] parece evitarla calculando otra constante menos natural).

Veamos ahora una aplicación más complicada[4], a cambio debemos creernos algún resultado.

Ejemplo. Intentemos decidir la asintótica de de los libres de cuadrados representables como suma de dos cuadrados, esto es, de

$$N(x) = \{n \leq x \ : \ n = a^2 + b^2 \text{ es libre de cuadrados}\}.$$

Como recordaremos en la siguiente sección, un número n libre de cuadrados es representable como suma de dos cuadrados si y sólo si $p|n \ \Rightarrow \ p = 2$ o $p \equiv 1 \ (4)$. Escojamos por tanto $f(n)$ como la función multiplicativa con $f(p^k) = c(p^k)p^{-k}$ donde $c(n)$ es la función característica de $\{p \equiv 1 \ (4)\} \cup \{2\}$. Procediendo como antes, $\Lambda_f(p^k) = -(-p)^{-k} \log p$ para este conjunto de primos (y cero en el resto). Como son la mitad de todos los primos (??) se debería tener

$$\sum_{n \leq x} \Lambda_f(n) = \frac{1}{2} \log x + O(1).$$

Dentro de dos capítulos tendremos las fuerzas necesarias para zarandear un poco al $O(1)$ hasta hacerle soltar una constante indeterminada:

$$\sum_{n \leq x} \Lambda_f(n) = \frac{1}{2} \log x + C + o(1).$$

Lo que moviendo el manubrio del teorema produce

$$\sum_{n \leq x} f(n) = K(\log x - C)^{1/2} + o\big((\log x)^{-1/2}\big)$$

y sumando por partes

$$N(x) = \sum_{n \leq x} nf(n) = Kx(\log x - C)^{1/2} - K \int_{x_0}^{x} (\log t - C)^{1/2} \, dt + o\big(x(\log x)^{-1/2}\big).$$

Integrando por partes dos veces, se tiene que la integral es $x(\log x - C)^{1/2} - \frac{1}{2}x(\log x - C)^{-1/2}$ más términos de orden inferior, por consiguiente

$$N(x) \sim \frac{Kx}{2\sqrt{\log x}}.$$

Con trabajo se puede limpiar un poco el aspecto de la constante.

1.3. Algunas técnicas algebraicas y analíticas

Teoría de anillos. Teoría de Galois. La delta de Dirac. Sumas trigonométricas.

Esta larga sección pretende ser algo así como un "repaso de todo" o al menos un repaso de todo lo que un estudiante de teoría de números debería haber conservado

[4]Ésta es el ejercicio 4 de [Iw-Ko] p. 28 salvo una pequeña variante. Aparentemente no es suficiente con utilizar la versión del Teorema de Wirsing allí establecida.

de la licenciatura si se lo hubieran explicado. Por si no se sospechara por el forzado retruécano, la visión trata de ser original, en comparación con los cursos originarios, y está posiblemente muy sesgada.

Respetando el orden alfabético vayamos primero con el álgebra.

Comencemos con algunas mentiras piadosas que, al ser de repaso, el lector sabrá tolerar (para las definiciones reales véase [Cl], [Do-He], [Ja]).

Un *anillo* es un conjunto en el que podemos sumar, restar y multiplicar con las propiedades habituales. En álgebra se consideran anillos con multiplicación no conmutativa o sin elemento neutro pero aquí huiremos de ellos. En un anillo quizá se pueda dividir entre algunos elementos, con una notación un poco confusa se dice que son las *unidades*, en pocas palabras una unidad es un elemento con inverso multiplicativo. Si se puede dividir entre todos los elementos distintos de cero, se dice que tenemos un cuerpo.

Por ejemplo $\mathbb{Z}$ es un anillo con unidades 1 y -1 pero no es un cuerpo, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ es un cuerpo (las unidades son $\mathbb{Q}(\sqrt{2}) - \{0\}$ porque siempre se puede racionalizar) y $\mathbb{Z}[i]$ no es un cuerpo pero sí un anillo y las unidades son 1, -1, i y $-i$.

En teoría de números los cuerpos más importantes son los *cuerpos de números* consistentes en tomar unos cuantos números algebraicos sobre $\mathbb{Q}$, $r_1, r_2, \ldots, r_k$ y hacer todas las posibles sumas, restas, multiplicaciones y divisiones, se escribe $\mathbb{Q}(r_1, r_2, \ldots, r_k)$. Y los anillos más importantes son los *anillos de enteros* que consisten en los elementos de un cuerpo (de números) que son raíces de polinomios mónicos de $\mathbb{Z}[x]$. Sus elementos se llaman *enteros algebraicos*. Esta definición tan rara viene motivada porque gozan de propiedades parecidas a las de los enteros, por ejemplo forman un anillo (aunque no sea trivial probarlo [St-Ta]) y (como veremos) se puede hacer aritmética con ellos. Por ahora notemos que el anillo de enteros de $\mathbb{Q}$ es $\mathbb{Z}$, el anillo de enteros de $\mathbb{Q}(i)$ es $\mathbb{Z}[i]$ y el de $\mathbb{Q}(\sqrt{-5})$ es $\mathbb{Z}[\sqrt{-5}]$, sin embargo el de $\mathbb{Q}(\sqrt{-7})$ es $\{a + b(1 + \sqrt{-7})/2 \ : \ a, b \in \mathbb{Z}\}$ (ejercicio: investigar esto calculando el anillo de enteros de $\mathbb{Q}(\sqrt{N})$ en general).

En un anillo (de enteros) A los *ideales* son las combinaciones lineales de ciertos elementos dados, llamados *generadores*. La notación para los ideales en función de sus generadores es:

$$\langle a_1, a_2, \ldots, a_n \rangle = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \ : \ \lambda_j \in A\}.$$

En $\mathbb{Z}$ los ideales son muy aburridos porque gracias al algoritmo de Euclides (o la identidad de Bezout) se cumple

$$\langle a, b \rangle = \langle (a, b) \rangle. \tag{1.8}$$

Un ideal consistente en los múltiplos de un solo número se dice que es *principal*. Todos lo son en $\mathbb{Z}$, según lo anterior. Los anillos en los que ocurre esto (y $a, b \neq 0 \Rightarrow ab \neq 0$) se dice que son *dominios de ideales principales*. Cuando éste es el caso números e ideales están en correspondencia biyectiva salvo multiplicar por unidades porque $\langle a \rangle = \langle b \rangle \Leftrightarrow a = ub$. Esto no ocurre siempre, por ejemplo $\langle 2, 1 + \sqrt{-5} \rangle$ no es principal en $\mathbb{Z}[\sqrt{-5}]$.

Los ideales se emplean como sustituto de los enteros algebraicos cuando éstos se portan mal. Por ello conviene saber cómo operarlos, sobre todo cómo multiplicarlos porque

la suma de ideales es una tontería, simplemente se unen los conjuntos de generadores. Para hacer el producto de dos ideales se multiplican los generadores de todas las formas posibles. En el caso de ideales principales el producto coincide con el de números $\langle a\rangle \cdot \langle b\rangle = \langle ab\rangle$ y en cualquier caso podemos definir los *ideales primos* del anillo A (se excluyen $\langle 0\rangle$ y $A = \langle 1\rangle$) como los que no se pueden factorizar.

Lo visto hasta ahora no deja de ser una sarta de definiciones, además imprecisas. La pregunta que subyace es ¿para qué quiero los ideales o los enteros algebraicos? ¿harán mi vida más sencilla? Remontándose a la historia, los ideales fueron introducidos por E. Kummer tratando de probar el último teorema de Fermat. Se puede encontrar una descripción fiel de la historia en [Ri] (o leyendo directamente [Sm]), lo que aquí veremos será un cuentecillo para aprender rápidamente la utilidad de las ideas.

Resulta que al resolver algunas ecuaciones diofánticas a uno le gustaría poder factorizar expresiones que no se pueden factorizar. Por ejemplo, compárense las siguientes ecuaciones:

$$a)\quad xy = 15^n, \qquad b)\quad x^2 + y^2 = 15^n.$$

La ecuación $a)$ es trivial, usando la factorización $15 = 3 \cdot 5$ se tiene que dado n todas las soluciones son $x = \pm 3^\alpha 5^\beta$, $y = \pm 3^{n-\alpha} 5^{n-\beta}$ con $0 \le \alpha, \beta \le n$, en total hay $2(n+1)^2$. Para la ecuación $b)$ no es inmediato cómo calcular ni siquiera el número de soluciones, en cambio si se sustituyera el "+" por "−" todo volvería a ser fácil porque $x^2 - y^2$ factoriza como $(x-y)(x+y)$ y todo se reduciría a despejar en $x-y = \pm 3^\alpha 5^\beta$, $x+y = \pm 3^{n-\alpha} 5^{n-\beta}$, de nuevo $2(n+1)^2$ soluciones ¿Podemos hacer trampas y factorizar $x^2+y^2 = (x+iy)(x-iy)$ y seguir adelante? Esto significa trabajar en el anillo de enteros algebraicos $\mathbb{Z}[i]$ y nos arriesgamos a que en él la factorización de 15 no sea $3\cdot 5$, de hecho es $15 = 3\cdot(2+i)(2-i)$ en el sentido de que 3, $2+i$ y $2-i$ no se pueden escribir como producto de más cosas si excluimos los "cuatro signos" (las unidades) de $\mathbb{Z}[i]$ que son $1, -1, i, -i$. Así pues tenemos

$$(x + iy)(x - iy) = 3^n (2 + i)^n (2 - i)^n.$$

La propiedad de que $x + iy$ y $x - iy$ sean conjugados restringe mucho las posibilidades, de hecho para n impar no hay ninguna solución, y para n par nos vemos obligados a escoger $3^{n/2}(2+i)^\alpha(2-i)^{n-\alpha}$ para un factor y el resto para el otro, salvo multiplicar por unidades. En resumen si n es par las soluciones son:

$$x = 3^{n/2}\Re\big(\epsilon(2+i)^\alpha(2-i)^{n-\alpha}\big), \qquad y = 3^{n/2}\Im\big(\epsilon(2+i)^\alpha(2-i)^{n-\alpha}\big),$$

con $\epsilon \in \{1, -1, i, -i\}$ y $0 \le \alpha \le n$, en total $4(n+1)$ soluciones.

Este invento de utilizar la aritmética de $\mathbb{Z}[i]$ para trabajar en $\mathbb{Z}$ se debe a Gauss, de ahí que los elementos de $\mathbb{Z}[i]$ reciban el nombre de *enteros gaussianos*. La justificación de que todo esto es lícito pasa por hurgar en la demostración del teorema fundamental de la aritmética y adaptarlo a $\mathbb{Z}[i]$. En pocas palabras todo lo que se necesita es un algoritmo de Euclides y para ello una división inexacta con resto menor que el divisor. En $\mathbb{Z}[i]$ se escoge como cociente de $a + bi$ entre $c + di$ al elemento de $\mathbb{Z}[i]$ más cercano a $(a + bi)/(c + di)$, y como resto lo que sobra.

Probemos ahora con otro ejemplo similar:

$$x^2 + 5y^2 = 21^n.$$

En $\mathbb{Z}[\sqrt{-5}]$ se tendría

$$(x+y\sqrt{-5})(x-y\sqrt{-5}) = (1+2\sqrt{-5})^n(1-2\sqrt{-5})^n$$

y se puede probar que $1+2\sqrt{-5}$, $1-2\sqrt{-5}$ son "primos": no se pueden factorizar salvo multiplicar por unidades, que en este caso son 1 y -1. Deberíamos por tanto tener que las soluciones son:

$$x = \pm\Re\big((1+2\sqrt{-5})^\alpha(1-2\sqrt{-5})^{n-\alpha}\big), \qquad x = \pm\frac{1}{\sqrt{5}}\Im\big((1+2\sqrt{-5})^\alpha(1-2\sqrt{-5})^{n-\alpha}\big),$$

con $0 \le \alpha \le n$, en total $2(n+1)$ soluciones. Los datos numéricos nos dan ahora un buen bofetón: resulta que por ejemplo para $n = 2$ tenemos las soluciones

x	6	11	14	19	-6	-11	-14	-19	6	11	14	19	21	-6	-11	-14	-19	-21
y	9	8	7	4	9	8	7	4	-9	-8	-7	-4	0	-9	-8	-7	-4	0

esto hacen ¡18 soluciones! lejos de $2(2+1)$.

¿Por qué Gauss puede invertarse nuevos enteros y nosotros no? Si intentamos definir la división inexacta en $\mathbb{Z}[\sqrt{-5}]$ como antes, no se consigue que el resto sea menor que el divisor. Peor todavía, no existe ni factorización única ni el concepto de máximo común divisor, así se cumple

$$3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

y sin embargo 3 y $1 \pm 2\sqrt{-5}$ no tienen divisores comunes no triviales en $\mathbb{Z}[\sqrt{-5}]$, ni 7 y $1 \pm 2\sqrt{-5}$. De hecho todos estos números son "primos" en el sentido de que no se pueden descomponer más. Si nos pidieran un deseo, partiendo de $3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, nos gustaría que existiesen los divisores comunes antes indicados, digamos $\mathfrak{a}_\pm = \mathrm{mcd}(3, 1 \pm 2\sqrt{-5})$, $\mathfrak{b}_\pm = \mathrm{mcd}(7, 1 \pm 2\sqrt{-5})$, de forma que

$$(1.9)\quad 3 = \mathfrak{a}_+ \cdot \mathfrak{a}_-, \qquad 7 = \mathfrak{b}_+ \cdot \mathfrak{b}_-, \qquad 1+2\sqrt{-5} = \mathfrak{a}_+ \cdot \mathfrak{b}_+, \qquad 1-2\sqrt{-5} = \mathfrak{a}_- \cdot \mathfrak{b}_-.$$

Como hemos mencionado, tales $\mathfrak{a}_\pm, \mathfrak{b}_\pm$ no existen. Pero según (1.8), al menos en $\mathbb{Z}$, un ideal con dos generadores es un sustituto para el máximo común divisor. Y así resulta que (1.9) pasa a ser cierto reemplazando 3, 7 y $1 \pm 2\sqrt{-5}$ por los ideales que generan, $\mathfrak{a}_\pm$ por $\langle 3, 1 \pm 2\sqrt{-5}\rangle$ y $\mathfrak{b}_\pm$ por $\langle 7, 1 \pm 2\sqrt{-5}\rangle$.

Las cantidades $\mathfrak{a}_\pm$, $\mathfrak{b}_\pm$ son literalmente "ideales" en (1.9), no existen, y en general sólo corresponderían a cantidades "reales" cuando los ideales fueran principales (esta cantidad real sería el generador). Vemos también que el concepto de primalidad de números (como aquellos que no se pueden descomponer) sólo nos lleva a problemas y es mejor desterrarlo, a cambio se puede reestablecer el orden considerando ideales primos. Con ellos la factorización vuelve a ser única.

Nuestro ejemplo para $n = 2$ se transforma con el lenguaje de los ideales en

$$\langle x+y\sqrt{-5}\rangle\langle x-y\sqrt{-5}\rangle = \mathfrak{a}_+^2\mathfrak{a}_-^2\mathfrak{b}_+^2\mathfrak{b}_-^2$$

y las soluciones son $\langle x+y\sqrt{-5}\rangle = \mathfrak{a}_+^\alpha\mathfrak{a}_-^{2-\alpha}\mathfrak{b}_+^\beta\mathfrak{b}_-^{2-\beta}$, $0 \le \alpha, \beta \le 2$ siempre que el segundo miembro sea principal, en este caso es así y $x+y\sqrt{-5}$ queda determinando salvo unidades, de ahí las $2 \cdot 3 \cdot 3 = 18$ soluciones.

Todo esto nos lleva a la conclusión de que la pregunta de cuántos ideales no principales hay y cómo detectarlos está íntimamente relacionada con el estudio del fallo en la factorización única y es muy importante en el estudio de ecuaciones diofánticas. Por ejemplo, Kummer sólo tuvo un éxito parcial al atacar el último teorema de Fermat porque es difícil saber en general si los ideales que aparecen en ciertas factorizaciones son principales[5], y por tanto si posibles soluciones "ideales" de la ecuación de Fermat son "irreales".

Para descontar los ideales principales uno puede considerar la relación de equivalencia entre ideales no nulos

$$\mathfrak{a} \sim \mathfrak{b} \iff (r)\mathfrak{a} \sim (s)\mathfrak{b} \qquad \text{con} \quad r, s \neq 0.$$

Al cociente

$$\mathcal{H} = \text{Ideales no nulos}/\sim$$

se le llama *grupo de clases* y tiene estructura de grupo (multiplicativo) porque para todo ideal $\mathfrak{a}$ siempre existe $\mathfrak{b}$ tal que $\mathfrak{ab}$ es principal. Los elementos de $\mathcal{H}$ se pueden identificar con "cosas" del tipo $\mathfrak{a}/(s)$ (se dice que son ideales fraccionarios) de la misma forma que $\mathbb{Q}$ es como $\mathbb{Z} \times \mathbb{Z}$ estableciendo la relación $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

Por ejemplo, el grupo de clases de $\mathbb{Z}[\sqrt{-5}]$ se puede probar que es isomorfo a $\mathbb{Z}_2$, como $\mathfrak{a}_+$, $\mathfrak{a}_-$, $\mathfrak{b}_+$, $\mathfrak{b}_-$ no son principales deben corresponder a $\overline{1}$ en $\mathbb{Z}_2$ y el producto $\mathfrak{a}_+^{\alpha}\mathfrak{a}_-^{2-\alpha}\mathfrak{b}_+^{\beta}\mathfrak{b}_-^{2-\beta}$ corresponde a la clase de $\alpha+(n-\alpha)+\beta+(n-\beta)$, que es siempre cero en $\mathbb{Z}_2$ y por tanto el ideal producto es principal, lo que prueba que el número de soluciones de $x^2 + 5y^2 = 21^n$ es $2(n + 1)^2$.

Cuando en primero nos dieron los números primos enseguida hicimos cocientes de $\mathbb{Z}$ por ellos para obtener $\mathbb{Z}_p$, que cuando fuimos mayores y supimos que era un cuerpo finito, llamamos $\mathbb{F}_p$. Además el resto de los $\mathbb{Z}_n$ eran peores, no se podía invertir siempre y al multiplicar dos elementos podía dar cero. ¿Serán igualmente buenos los cocientes de anillos de enteros por ideales primos? La respuesta es un sí sin matices: Si A es un anillo de enteros entonces $A/\mathfrak{a}$ es un cuerpo $\Leftrightarrow$ $\mathfrak{a}$ es un ideal primo. En realidad no hace falta que sea un anillo de enteros, se puede ampliar el resultado siempre que los ideales primos sean *maximales*, esto es, que no haya otros ideales propios que los contengan, esto ocurre por ejemplo en todos los anillos de polinomios de una variable con coeficientes en

[5]La ecuación de Fermat $x^n + y^n = z^n$, digamos con $n = p > 3$ por razones técnicas, se puede factorizar como

$$(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^n y) = z \cdot z^{\overset{n \text{ veces}}{\cdots}} z$$

con $\zeta = e^{2\pi i/n}$. Esto conduce a estudiar cuándo dos productos coinciden en el anillo $\mathbb{Z}[\zeta]$. En $\mathbb{Z}$ es evidente que si tenemos unos cuantos números que son coprimos dos a dos unos con otros y su producto es una n-potencia, cada uno de ellos lo es. Se puede probar que si $(x, y) = 1$ entonces los ideales generados por $x+\zeta^j y$ son "coprimos" así que una solución no trivial conduce a que cada uno de estos ideales es una n-potencia. Si los ideales son principales se puede escribir esto como una igualdad entre elementos de $\mathbb{Z}[\zeta]$ y se sabe llegar a una contradicción esencialmente usando congruencias [Bo-Sh], [St-Ta]. Con esto, Kummer sabía probar el último teorema de Fermat cuando se puede asegurar que la potencia n-ésima de cualquier ideal es principal, en el lenguaje que se introducirá a continuación, cuando el grupo de clases tiene orden no divisible por n.

un cuerpo. Este edificio no son alharacas lingüísticas. Por ejemplo, para $p \in \mathbb{N}$ primo de los de siempre:

$$\begin{aligned} \langle p\rangle \text{ primo en } \mathbb{Z}[i] \quad &\Leftrightarrow \quad \mathbb{Z}[i]/\langle p\rangle \text{ es un cuerpo} \quad \Leftrightarrow \ \mathbb{Z}_p[i] \text{ es un cuerpo} \\ &\Leftrightarrow \quad \mathbb{Z}_p[x]/\langle x^2+1\rangle \text{ es un cuerpo} \quad \Leftrightarrow \ x^2+1 \text{ es irreducible en } \mathbb{Z}_p \end{aligned}$$

Pero que $\langle p\rangle$ sea primo en $\mathbb{Z}[i]$ es lo mismo que decir que $p = (a+bi)(a-bi)$ (tomando normas se ve que no se puede descomponer más) y por uno de los casos especiales de la ley de reciprocidad cuadrática[6] (o más fácil) sabemos que -1 es un cuadrado en $\mathbb{Z}_p$ si y sólo si $p \equiv 3\ (4)$. En definitiva

$$p \text{ es suma de dos cuadrados} \quad \Leftrightarrow \ p \equiv 3\ (4)$$

y como subproducto se pueden caracterizar todos los ideales primos en $\mathbb{Z}[i]$.

Lo mismo que la factorización única en $\mathbb{Z}$ lleva asociada la función ζ con su producto de Euler, también es posible asociar funciones ζ (llamadas de Dedekind) a los ideales. La relación de los ideales con los números naturales de toda la vida se hace a través de la *norma*. La norma de un ideal $\mathfrak{a}$ en un anillo A se define como $N\mathfrak{a} = \#A/\mathfrak{a}$. Nos podemos sentir complacidos con la notación observando que si $z \in \mathbb{Z}[i]$, $N\langle z\rangle = |z|^2$.

Ejemplo. Sea

$$r(n) = \#\{(a,b) \in \mathbb{Z}^2 \ : \ a^2+b^2 = n\}.$$

Esta definición se puede reescribir como $\#\{z \in \mathbb{Z}[i] \ : \ |z|^2 = n\}$. El anillo $\mathbb{Z}[i]$ es un dominio de factorización única, concretamente de ideales principales, esto es, los números están en correspondencia biyectiva con los ideales salvo multiplicar por alguna de las cuatro unidades $\{1,-1,i,-i\}$. Entonces

$$r(n) = 4\#\{\mathfrak{a} \text{ ideal } \subset \mathbb{Z}[i] \ : \ N\mathfrak{a} = n\} \ \Rightarrow \ \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\sum_{n=1}^{\infty} \frac{1}{(N\mathfrak{a})^s}$$

como en el caso de números naturales (1.2), aquí también se puede descomponer en "factores locales"

$$\sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\prod_{\wp} \left(1 + \frac{1}{(N\wp)^s} + \frac{1}{(N\wp)^{2s}} + \dots\right)$$

donde $\wp$ recorre los ideales primos de $\mathbb{Z}[i]$. Por el análisis anterior, los *primos racionales* p (los normales y corrientes) factorizan en $\mathbb{Z}[i]$ de la siguiente forma:

$$\langle p\rangle = \begin{cases} \langle a+bi\rangle\langle a-bi\rangle & \text{si } p \equiv 1\ (4) \\ \langle p\rangle & \text{si } p \equiv 3\ (4) \\ \langle 1+i\rangle^2 & \text{si } p = 2 \end{cases}$$

[6] Ésta afirma que para $p, q > 2$ primos distintos se cumple

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \qquad \text{además} \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

donde (a/r), con r primo $r \nmid a$, es el símbolo de Legendre que vale uno si $x^2 \equiv a\ (r)$ tiene solución y -1 si no la tiene. Se escribe $(a/r) = 0$ si $r|a$.

Estos factores son por tanto todos los ideales primos en $\mathbb{Z}[i]$ y se sigue

$$\sum_{n=1}^{\infty}\frac{r(n)}{n^s}=4(1+2^{-s}+2^{-2s}+\dots)\prod_{p\equiv 1\ (4)}(1+p^{-s}+p^{-2s}+\dots)^2\prod_{p\equiv 3\ (4)}(1+p^{-2s}+p^{-4s}+\dots)$$

que se puede escribir como (ejercicio)

$$\sum_{n=1}^{\infty}\frac{r(n)}{n^s}=4\zeta(s)\prod_{p\equiv 1\ (4)}(1-p^{-s})^{-1}\prod_{p\equiv 3\ (4)}(1+p^{-s})^{-1}=\zeta(s)D_\chi(s)$$

donde $\chi=\chi(n)$ es la función multiplicativa que vale 1 si $n\equiv 1\ (4)$, -1 si $n\equiv 3\ (4)$ y 0 en el resto de los casos. Se deduce que $r(n)/4$ es multiplicativa y la fórmula

$$\frac{r(n)}{4}=\sum_{d|n}\chi(d)=\#\{d|n\ :\ d\equiv 1\ (4)\}-\#\{d|n\ :\ d\equiv 3\ (4)\}.$$

Por ejemplo, $r(10^6)=4(r(2^6)/4)(r(5^6)/4)=4\cdot 1\cdot 7=28$. En particular un número n es representable como suma de dos cuadrados si y sólo si los únicos posibles factores primos de n de la forma $p\equiv 3\ (4)$ aparecen con exponente par.

No abandonaremos los placeres del álgebra sin visitar brevemente a la teoría de Galois, una de las asignaturas más bellas de la licenciatura y una de las pocas que se muestra autocontenida con su planteamiento, nudo y desenlace.

Su propósito y gran logro es establecer una relación exacta entre la estructura de ciertos cuerpos y sus simetrías. Pensemos por ejemplo en cualquier identidad en $\mathbb{Q}(i)$, digamos $(3+2i)/(1+i)=5/2-i/2$, entonces al cambiar i por $-i$ la igualdad se conserva. Simetrías como éstas son lo que se llaman $\mathbb{Q}$-*automorfismos*: funciones biyectivas que respetan las sumas, restas, multiplicaciones y divisiones y que dejan a cada racional invariante. En general, dados dos cuerpos $L\supset K$ (se suele escribir L/K y se dice que es una *extensión* de cuerpos), se llama *grupo de Galois* de L/K al grupo $\mathcal{G}(L/K)$ formado por los automorfismos que respetan las operaciones y dejan fijo a cada elemento de K. Es muy fácil ver que si $\alpha\in L$ es raíz de un polinomio $P\in K[x]$, entonces $\sigma(\alpha)$ también lo es para todo $\sigma\in\mathcal{G}(L/K)$. Esto es, los elementos del grupo de Galois lo único que hacen es permutar raíces de polinomios. Una permutación de raíces (incluidas en L) puede no corresponder a ningún elemento de $\mathcal{G}(L/K)$ porque haya relaciones entre ellas. Por ejemplo, un $\mathbb{Q}$-automorfismo σ no puede mandar $\sqrt{2}$ a $\sqrt{3}$ aunque ambas sean raíces de x^4-5x^2+6 porque $\sigma(\sqrt{2})=\sqrt{3}\Rightarrow\sigma(\sqrt{2}\cdot\sqrt{2})=\sqrt{3}\cdot\sqrt{3}\Rightarrow 2=3$, que es muy feo. Sin embargo sí es cierto que si tenemos un polinomio irreducible $P\in K[x]$ con raíces en L siempre hay un elemento de $\mathcal{G}(L/K)$ que aplica una de las raíces en cualquier otra, ambas escogidas arbitrariamente.

Ejemplo. En $\mathbb{Q}(\sqrt{n})$ con $|n|\in\mathbb{N}$ libre de cuadrados, todo lo que se puede hacer es enviar $\sqrt{n}$ a $-\sqrt{n}$ o dejarlo fijo pues éstas son las dos raíces de x^2-n; lo que implica que $\mathcal{G}(\mathbb{Q}(\sqrt{n})/\mathbb{Q})=\{\mathrm{Id},\mathrm{conj.}\}$

Ejemplo. Si p es primo, el polinomio ciclotómico $x^{p-1}+\cdots+x+1=(x^p-1)/(x-1)$ es irreducible [St] y tiene como raíces a $\zeta,\zeta^2,\ldots,\zeta^{p-1}$ con $\zeta=e(1/p)$. Un elemento de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ queda determinado por la imagen de ζ, ya que el resto de las raíces dependen de ésta. Así pues los únicos $\mathbb{Q}$-automorfismos son los dados por $\sigma_j(\zeta)=\zeta^j$, $j=1,2,\ldots,p-1$. En símbolos

$$\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})=\{\mathrm{Id}=\sigma_1,\sigma_2,\ldots,\sigma_{p-1}\}\cong\mathbb{Z}_{p-1}.$$

El último isomorfismo no es evidente pero el lector debería saber al menos sutituir $\mathbb{Z}_{p-1}$ por $\mathbb{Z}_p^*$ (los elementos $\{\overline{1},\overline{2},\ldots,\overline{p-1}\}$ con el producto) y leer en algún sitio qué son las raíces primitivas [Ro].

El llamado *teorema fundamental de la teoría de Galois* afirma que suponiendo $L=K(r_1,r_2,\ldots,r_n)\subset\mathbb{C}$ donde r_j son todas las raíces de cierto polinomio de $K[x]$ (se dice que L/K es normal), entonces los subgrupos de $\mathcal{G}(L/K)$ están en correspondencia biyectiva con los subcuerpos de L conteniendo a K por medio de

$$\text{subcuerpo } M \quad\longrightarrow\quad \text{subgrupo } \mathcal{G}(L/M)\subset\mathcal{G}(L/K)$$

Además la dimensión de M como espacio vectorial sobre K, llamada *grado*, coincide con el índice de $\mathcal{G}(L/M)$ en $\mathcal{G}(L/K)$ (el cociente de sus órdenes). El teorema fundamental de la teoría de Galois tiene realmente una formulación más general y otro "además" importante [St]. Cualquier matemático debería conocer su enunciado completo.

Una utilidad de esta relación entre subcuerpos y simetrías es la facultad de poder "descomponer" una extensión de cuerpos L/K con sus elementos feísimos llenos de radicales, decimales y otras guarrerías indescriptibles (véase el teorema de Abel en [St]); gracias al estudio de los subgrupos de un grupo finito, algo que a primera vista tiene un aspecto tan limpio y discreto como los números naturales.

Ejemplo. Sea la raíz de la unidad $\zeta=e(1/17)$. Sabemos que $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})\cong\mathbb{Z}_{16}$, que es cíclico de orden 16 y por tanto la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ tendrá sólo tres subcuerpos propios (conteniendo a $\mathbb{Q}$): los correspondientes a los subgrupos $\langle\overline{2}\rangle$, $\langle\overline{4}\rangle$ y $\langle\overline{8}\rangle$

$$\mathbb{Q}(\zeta)=M_0\supset M_1\supset M_2\supset M_3\supset M_4=\mathbb{Q}.$$

Cada extensión M_{i-1}/M_i tiene grado 2, entonces cada elemento de M_{i-1} es de la forma $a\cdot 1+b\cdot u$ con $a,b\in M_i$, $u\in M_{i-1}$. En particular u^2 es de esta forma y por tanto es raíz de un polinomio cuadrático. Por consiguiente M_{i-1} es lo mismo que M_i añadiendo cierta raíz cuadrada de algún elemento. Se deduce que el polígono de 17 lados es construible con regla y compás, porque $\zeta=\cos(2\pi/17)+i\sin(2\pi/17)$ y siempre podemos extraer raíces cuadradas con útiles de dibujo [Cl]. Este resultado se debe a Gauss y es una delicia leer de primera mano [Ga] cómo hacía teoría de Galois cuando todavía Galois no tenía ni bozo.

Pasemos ahora al análisis.

Al igual que la dinámica tiene como personaje canónico a la partícula (cero dimensional) de masa unidad, se puede conocer una buena porción del reparto de la película del análisis a través de su "función de densidad": la delta de Dirac[7].

Si llamamos δ a esta presunta función de densidad de una partícula unidad en el origen de la recta real, rápidamente topamos con un ramillete de contradicciones frente al concepto más básico de función, pues debería cumplir

$$\delta(x) = 0 \quad \forall x \neq 0, \qquad \delta(0) = \infty, \qquad \int_{-\infty}^{\infty} \delta(x)\, dx = 1,$$

y los rudimentos de la teoría de la integral (de Lebesgue) nos aseguran que esto no tiene sentido porque un cambio de una función en un conjunto de medida cero no puede influir en el valor de la integral, así que en sana puridad matemática debería cumplirse la igualdad $\int_{-\infty}^{\infty} \delta = \int_{-\infty}^{\infty} 0 = 0$ y no se podría ver la definición $\delta(0) = \infty$ más que como una exótica aberración. No obstante nuestra intuición no se ve fabulosamente perturbada al emplear $masa = \int densidad$ para todas las masas, incluso partículas unidad, todavía más, si en $\mathbb{R}$ no se emplea la medida usual dx sino $f(x)dx$ (con f una función decente), debería cumplirse

$$\int_{-\infty}^{\infty} f(x)\delta(x)\, dx = f(0)$$

que generaliza la relación anterior.

Puestos a hacer barbaridades, consideremos la δ de Dirac 1-periódica, esto es, $\delta_p(x) = \sum_{n\in\mathbb{Z}} \delta(x-n)$ que integrando contra f da lugar a

$$\sum_{n=-\infty}^{\infty} f(n) = \int_{-\infty}^{\infty} f\delta_p.$$

Esto es interesante porque permite escribir sumas como integrales (como en la "demostración" del Lema de Abel). Si calculamos formalmente los coeficientes de Fourier de δ_p son todos unos y se infiere la igualdad

$$\delta_p(x) = \sum_{n=-\infty}^{\infty} e(nx) \tag{1.10}$$

que no tiene sentido aparente pero sustituida en la igualdad anterior conduce a

[7]El artífice de este regalo, P.A.M. Dirac, es bien conocido por sus importantísimas contribuciones a la Física. En `http://www-groups.dcs.st-andrews.ac.uk/` podemos leer que su vocación eran las Matemáticas: "*Although mathematics was his favourite subject he chose to study an engineering course at university since he thought that the only possible career for a mathematician was school teaching and he certainly wanted to avoid that profession. He obtained his degree in engineering in 1921 but following this, after an undistinguished summer job in an engineering works, he did not find a permanent position. By this time he was developing a real passion for mathematics but his attempts to study at Cambridge failed for rather strange reasons*".

Teorema 1.3.1 (fórmula de sumación de Poisson) *Para* $f \in C_0^\infty$

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}(n).$$

Una fórmula utilísima[8] sin deltas fantasmagóricas que permite pasar una suma sobre enteros en otra, confiando en que la segunda sea más sencilla.

Ejemplo. Sea $\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}$ con $t > 0$. Aplicando la fórmula de sumación de Poisson a $f(x) = e^{-\pi t x^2}$, se obtiene $\theta(t) = t^{-1/2}\theta(1/t)$. Para apreciar los beneficios, nótese que por ejemplo $\theta(0'01) = \sum e^{-\pi n^2 0'01}$ es muy costoso de aproximar con precisión empleando una calculadora de bolsillo debido a la lenta convergencia inicial, mientras que la relación anterior permite asegurar $\theta(0'01) \approx 10$ con una precisión de más de 100 decimales.

Al igual que los sólidos se pueden estudiar en mecánica integrando partículas de masa pequeña, toda función 1-periódica se puede ver como una "combinación lineal continua" de deltas de Dirac:

$$f(x) = \int_{-1/2}^{1/2} f(t)\delta_p(x-t)\, dt,$$

lo que combinado con (1.10) implica

$$\boxed{f(x) = \sum_{n=-\infty}^{\infty} a_n e(nx)} \qquad \text{con} \qquad a_n = \int_0^1 f(t)e(-nt)\, dt.$$

Es decir, a partir de (1.10) se puede "deducir" el desarrollo de Fourier genérico de una función.

De la misma forma, a partir de $\widehat{\delta}(\xi) = 1$ si uno confía ciegamente en la fórmula de inversión de la transformada de Fourier, $\delta = \widehat{\delta}^{\,\vee}$, se debería cumplir

$$\delta(x) = \int_{-\infty}^{\infty} e(x\xi)\, d\xi.$$

De este caso de la fórmula de inversión, cambiando x por $x-t$ e integrando (en t) contra $f(t)$, se deduce

$$\boxed{f = \widehat{f}^{\,\vee}}$$

que es la fórmula de inversión en general.

Lo bueno de todo esto no es sólo que podemos ver y deducir intuitivamente fórmulas cruciales teniendo una fe vana en una función inexistente, sino que en muchos casos nos anticipa la demostración de verdad, lo que nos lleva a la definición matemática de δ:

[8] De acuerdo con la introducción de [Iw-Ko]: "Poisson summation for number theory is what a car is for people in modern communities –it transports things to other places and it takes you back home when applied next time– one cannot live without it". Lo de "takes you back home when applied next time" se deduce de que la transformada de Fourier es casi involutiva: $f\,\widehat{\ }\,\widehat{\ }(x) = f(-x)$.

Si $\eta \in C_0^\infty(\mathbb{R})$, digamos $\eta \geq 0$ con $\eta(0) = 1$, y suponemos $\int \eta = 1$, entonces la sucesión $\eta_n(x) = n\eta(nx)$, de algún modo tiende a δ porque $\lim_{n\to\infty} \int f(x)\eta_n(x)\, dx = f(0)$ para funciones "buenas" f. Para no pillarnos los dedos, podemos definir δ como la propia sucesión de funciones η_n (se dice que es una *aproximación de la identidad*) y entonces resulta que las "demostraciones" anteriores se vuelven demostraciones sin comillas a base de asegurar las condiciones de convergencia [Dy-Mc], [Fo]. Incluso en (1.10) se puede introducir la regularización $d_r(x) = \sum |r|^n e(nx)$ (núcleo de Poisson) y probar que realmente $\lim_{r\to 1^-} \int f d_r = f(0)$. Todas las pruebas requieren la dualidad, δ no aparece nunca como singularidad desnuda, sino bien arropada integrada contra una función buena para que no nos asustemos con el infinito. Se puede llevar esta idea al extremo definiendo herméticamente δ como el sencillo funcional que aplica una función en su valor en cero.

La gran maravilla del análisis de Fourier es que, de acuerdo con las fórmulas recuadradas, permite expresar una función como una combinación de tonos puros, a fin de cuentas sencillos senos y cosenos. Hay varias ideas básicas que permiten avanzar con soltura al razonar con este análisis. Una de ellas está basada en el comportamiento de la transformada de Fourier bajo cambios de escala:

$$g(x) = f(Tx) \quad \Rightarrow \quad \widehat{g}(\xi) = T^{-1}\widehat{f}(\xi/T).$$

Si pensamos que f y $\widehat{f}$ son funciones decentes que más o menos tienen casi toda su masa en $[-1, 1]$, lo que dice esta relación es que al achuchar f para confinarla al intervalo $[-1/T, 1/T]$, la transformada se extenderá a $[-T, T]$. Esto es una forma débil del *principio de incertidumbre*, que de una manera gráfica se puede enunciar de la manera siguiente:

Principio de incertidumbre. Una oscilación de frecuencia ω se salta los objetos de tamaño ω^{-1}.

Explicado en tiempo, en lugar de en espacio, si jugando al escondite inglés miro un instante dos veces por minuto y alguien se mueve sólo una vez y durante mucho menos de medio minuto, es difícil que lo vea moverse (ahí está la gracia del juego).

En términos matemáticos, las transformadas de Fourier (que dan el contenido en frecuencia) de dos funciones que sólo difieren a escala δ (pequeña) sólo empezarán a distinguirse sustancialmente para $|\xi| \gg \delta^{-1}$. Esto se aplica sobre todo al tratar regularizaciones. Por ejemplo, si

$$f(x) = \begin{cases} 1 & \text{si } x \in [-1, 1] \\ 0 & \text{si } x \notin [-1, 1] \end{cases} \qquad \text{y} \qquad g(x) = \begin{cases} 1 & \text{si } x \in [-1 + \delta/2, 1 - \delta/2] \\ 0 & \text{si } x \notin [-1 - \delta/2, 1 + \delta/2] \\ \text{redondeado } C^\infty \text{ en el resto} \end{cases}$$

entonces $\widehat{f}(\xi) = \text{sen}(2\pi\xi)/\pi\xi$, en particular decae como $|\xi|^{-1}$ cuando $\xi \to \infty$, mientras que $\widehat{g}(\xi)$, por ser $g \in C^\infty$, decae más rápido que $|\xi|^{-N}$ para cualquier N (simplemente integrando por partes). Lo que nos dice el principio de incertidumbre es que el precio a pagar por esta regularización de f a g es no ver este decaimiento cuando $|\xi| \ll \delta^{-1}$.

Lo habitual en los ejemplos concretos es que haya que optimizar el valor de δ para contentar a dos tendencias en oposición: 1) la función regularizada debe parecerse a la original; 2) la transformada de Fourier de la función regularizadora debe empezar a decaer rápidamente. La primera requiere disminuir δ y la segunda aumentarlo.

Todo esto funciona de la misma forma en más dimensiones cambiando valores absolutos por normas. En general el análisis armónico (fórmulas recuadradas, sumación de Poisson,...) se extiende al caso multidimensional simplemente añadiendo más variables. La transformada de Fourier pasa a ser $\int f(\vec{x})e(-\vec{x}\cdot\vec{\xi})\,d\vec{x}$ y la serie de Fourier $\sum a_{\vec{n}}e(\vec{n}\cdot\vec{x})$.

Ejemplo. ¿Cuántos puntos de coordenadas enteras hay en la esfera de radio R (con R grande)? Aproximadamente el volumen, esto es $4\pi R^3/3$. Pero ¿de qué orden es el error $E(R) = \text{nº de puntos} - 4\pi R^3/3$? Esto no tiene respuesta fácil. La acotación trivial, contando puntos cerca de la cáscara de la esfera, es $E(R) = O(R^2)$ (ejercicio). Veamos cómo mejorar este resultado.

Formalmente, tomando como f la función característica de la esfera de radio R en la fórmula de sumación de Poisson en tres dimensiones

$$E(R) = \sum_{\vec{n}\in\mathbb{Z}^3} f(\vec{n}) - \frac{4\pi}{3}R^3 = \sum_{\vec{n}\in\mathbb{Z}^3-\{\vec{0}\}} \widehat{f}(\vec{n}).$$

¡Una fórmula exacta! Nuestro entusiasmo se desvanece cuando hacemos los cálculos y vemos que $\widehat{f}(\vec{n})$ es como $R\|\vec{n}\|^{-2}$ salvo un factor acotado oscilante (se puede hallar la fórmula explícita [Dy-Mc] §2.11), por tanto la serie no converge absolutamente[9]. Para remediar este desaguisado tomamos una función $g_+ \in C^\infty(\mathbb{R}^3)$ con $g_+(\vec{x}) = 1$ si $\|\vec{x}\| \le R$, $g_+(\vec{x}) = 0$ si $\|\vec{x}\| \ge R+\delta$ y redondeada positiva entre medias. Igualmente se define $g_- \in C^\infty(\mathbb{R}^3)$ con $g_-(\vec{x}) = 1$ si $\|\vec{x}\| \le R-\delta$, $g_-(\vec{x}) = 0$ si $\|\vec{x}\| \ge R$. Entonces

$$\sum_{\vec{n}\in\mathbb{Z}^3-\{\vec{0}\}} \widehat{g}_-(\vec{n}) + O(R^2\delta) \le E(R) \le \sum_{\vec{n}\in\mathbb{Z}^3-\{\vec{0}\}} \widehat{g}_+(\vec{n}) + O(R^2\delta)$$

(el $R^2\delta$ viene de $R^3 - (R\pm\delta)^3$). Por el principio de incertidumbre, $\widehat{g}_+(\vec{n})$ y $\widehat{g}_-(\vec{n})$ serán como $R\|\vec{n}\|^{-2}$ hasta $\|\vec{n}\| \ll \delta^{-1}$ pero después ya se ve la suavidad y todo decae estupendamente, por tanto

$$E(R) \ll R \sum_{\|\vec{n}\|\ll\delta^{-1}} \|\vec{n}\|^{-2} + R^2\delta \ll R\delta^{-1} + R^2\delta.$$

Con la elección óptima $\delta = R^{-1/2}$ ambos sumandos se igualan y se tiene $E(R) \ll R^{3/2}$, un resultado de Landau [La].

[9] La serie $\sum \|\vec{n}\|^{-2}$ es divergente, no como su análoga unidimensional. Concretamente se verifica $\sum_{\|\vec{n}\|\le x} \|\vec{n}\|^{-2} \gg x$ (ejercicio).

Si el análisis de Fourier permite reducir las funciones a montones de senos y cosenos, el problema de estimar promedios con precisión se traslada a estimar sumas trigonométricas. Terminando este larguísimo repaso con algo que no lo es, adentrémonos en este árido terreno (véase [Gr-Ko] para más información y [Hu] si a alguno le quedan ganas de más).

Digamos que tenemos

$$S = \sum \phi(n)\, e(f(n))$$

donde $\phi \in C_0^\infty$ es una función adaptada a un intervalo entero $[a, b]$ (una regularización de su función característica). Por la fórmula de sumación de Poisson

$$S = \sum_n \int \phi(x)\, e(f(x) - nx)\, dx.$$

Supongamos que f' es monótona en el soporte de ϕ, por ejemplo creciente con $N_1 < f' < N_2$, $N_1, N_2 \in \mathbb{Z}$. Si n está lejos del intervalo $[N_1, N_2]$ la derivada de $f(n) - nx$ es grande y por tanto la integral pequeña (mucha oscilación $\Rightarrow$ mucha cancelación). El caso límite es cuando f' apenas varía, digamos $|f'| < \epsilon$, entonces el término que más contribuye a S es $\int \phi\, e(f) = \int f' e(f)\, \phi/f'$ y sumando por partes para sacar ϕ/f', todo queda mayorado por una cota inferior para f'. Poniendo todo esto en limpio (??)

Proposición 1.3.2 *Sea $f \in C^1([a, b])$ con f' monótona y $\lambda_1 < |f'| < 1/2$, entonces*

$$\sum_{a<n\leq b} e(f(n)) \ll \lambda_1^{-1}.$$

Típicamente f' varía más y con la notación anterior la parte del león en S es

$$\sum_{N_1<n<N_2} \int \phi(x)\, e(f(x) - nx)\, dx. \tag{1.11}$$

Ahora la derivada de $f(x) - nx$ puede ser nula. Si llamamos x_n al punto crítico (no puede haber más que uno si f' es monótona), entonces en las cercanías de x_n se tiene por Taylor $f(x) - nx = f(x_n) - nx_n + f''(x_n)(x - x_n)^2/2 + \ldots$. Pero es bien conocido[10] que $\int_{-\infty}^{\infty} e(\lambda x^2)\, dx = C/\sqrt{\lambda}$, por tanto con un cambio de variable es creíble que $\int \phi(x)\, e(f(x) - nx)\, dx$ se parezca a (??) $C\phi(x_n) e(f(x_n) - nx_n)/\sqrt{f''(x_n)}$. Entonces cada término de (1.11) es del orden de $(f'')^{-1/2}$ y se tienen $N_2 - N_1 = \Delta f' + 1 \asymp (b-a)f'' + 1$ términos. Multiplicando, se sigue (??)

Proposición 1.3.3 *Sea $f \in C^2([a, b])$, $a, b \in \mathbb{Z}$ con $\lambda_2 \ll |f''| \ll \lambda_2$, entonces*

$$\sum_{a<n\leq b} e(f(n)) \ll (b-a)\lambda_2^{1/2} + \lambda_2^{-1/2}.$$

Este resultado se debe a van der Corput (véase en [Gr-Ko] una prueba elemental).

[10] En realidad basta probar que $\int_{-\infty}^{\infty} e(x^2)\, dx$ converge y hacer un cambio de variable.

1.4. La distribución de los primos

El teorema de los números primos. Ideas básicas de la demostración. La función ζ.

Ya sea con argumentos heurísticos, por ejemplo a partir de la fórmula de Mertens (1.5) o con pruebas experimentales[11] no es difícil sospechar que la "densidad" de los primos en los naturales se comporta como $1/\log x$. En términos más precisos:

Teorema 1.4.1 (teorema de los números primos) *Se cumple*

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

Antes de seguir es justo confesar que $Li(x) \sim x/\log x$ (basta aplicar la regla de L'Hôpital) y por tanto el teorema se podría haber escrito más claramente como $\pi(x) \sim x/\log x$ o $\lim_{x\to\infty} \pi(x)\log x/x = 1$. Para acallar de golpe cualquier murmullo linchador basta exhibir la siguiente tabla:

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

Si nuestra conjetura favorita (la hipótesis de Riemann) se cumpliera, entonces $Li(x)$ sería una aproximación para $\pi(x)$ con más o menos la mitad de sus cifras significativas correctas, como sugieren los resultados numéricos, sin embargo se sabe positivamente (sin interrogaciones) que $x/\log x$ es una aproximación tan mala que no muchas más de las primeras $\log\log x$ cifras significativas pueden ser correctas, esto es prácticamente nada desde el punto de vista numérico.

Por razones que aparecerán más adelante, para probar el teorema de los números primos es más fácil trabajar con $\psi(x)$ (véase §1.1) que directamente con $\pi(x)$. Intuitivamente $\psi(x)$ es como $\pi(x)$ salvo un logaritmo. Como prontuario ínfimo de diferentes equivalencias naturales del teorema de los números primos se enuncia el siguiente resultado:

Lema 1.4.2 *Las siguientes afirmaciones son equivalentes*

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

Demostración: Ya hemos mencionado que $a) \Leftrightarrow b)$. Claramente $\pi(p_n) = n$, así pues $b)$ implica $p_n/\log p_n \sim n$ y tomando logaritmos $\log p_n \sim \log n$. Multiplicando estas

[11] Éstas pueden ser triviales en el actual mundo del *bit*, en el que cualquier tonto puede pulsar una tecla y tener una lista inmensa de primos y pulsar otra y analizarla estadísticamente, pero en tiempos de Gauss y Legendre fue algo notable.

relaciones se obtiene c). El recíproco se prueba en las mismas líneas: $p_n \leq x < p_{n+1}$, $c) \Rightarrow p_n \sim x$.

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

$$\pi(x) = Li(x) + \frac{\psi(x)-x}{\log x} + \int_2^x \frac{\psi(t)-t}{t(\log t)^2}\, dt + O(x^{1/2}) \tag{1.12}$$

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

Más importante que el propio enunciado es la relación (1.12) y para subrayarlo machaconamente se enuncia de nuevo débilmente.

Lema 1.4.3 *Si $\psi(x) = x + O(E(x))$ para cierta E creciente, entonces se cumple $\pi(x) = Li(x) + O(x^{1/2} + E(x)/\log x)$.*

Observación: Insistiendo en las repeticiones, de $Li(x) - x/\log x \sim x/(\log x)^2$ se deduce que en cuanto se pruebe una acotación ligeramente buena para $E(x)$, el error $\pi(x) - x/\log x$ está prácticamente dominado por $x/(\log x)^2$.

Una equivalencia más profunda y curiosa tiene que ver con el promedio de la función de Möbius, como destaca la siguiente (meta-)proposición; cuya demostración elemental (originariamente debida a Landau) está tomada de [Iw-Ko].

Proposición 1.4.4 *El teorema de los números primos es equivalente a que el promedio de μ tienda a cero, esto es,*

$$\pi(x) \sim Li(x) \quad \Longleftrightarrow \quad \lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \mu(n) = 0.$$

Demostración: Nos olvidaremos en ambas implicaciones de $\pi(x) \sim Li(x)$ y emplearemos $\psi(x) \sim x$ que ya hemos visto que es equivalente.

$\Rightarrow$) La relación $\log = 1 * \Lambda$ multiplicando por $\mu(n)$ y sumando, da lugar a

$$\sum_{n\leq x} \mu(n)\log n = -\sum_{n\leq x} \mu(n)\psi(x/n).$$

Por otra parte la igualdad $f = \mu * 1$ con $f(1) = 1$ y $f(n) = 0$ si $n \neq 1$, implica después de sumar $1 = \sum_{n\leq x} \mu(n)[x/n]$ (ejercicio). Restando estas igualdades y usando que por hipótesis $\psi(x/n) - [x/n] = o(x/n)$ se sigue $\sum_{n\leq x} \mu(n)\log n = o(x\log x)$ y sumando por partes se tiene el resultado deseado.

$\Leftarrow$) Se relaciona ψ con μ "despejando" Λ en $\log = 1 * \Lambda$, lo que implica $\Lambda = \mu * \log$ y por tanto

$$\psi(x) = \sum_{n\leq x} \sum_{d|n} \mu(d)\log\frac{n}{d} = \sum_{m\leq x} \log m \sum_{d\leq x/m} \mu(d).$$

Por otro lado, empleando de la misma forma $1 = \mu * d$ y $f = \mu * 1$ (como en la implicación directa), se deduce combinando las fórmulas resultantes

$$\psi(x) - x + C = \sum_{m \le x} (\log m - d(m) + C) \sum_{d \le x/m} \mu(d)$$

para cualquier constante C. Dado $M \in \mathbb{N}$, usando la hipótesis y sumación por partes en el rango $m \le M$ e intercambiando el orden de sumación en $M < m \le x$, se obtiene

$$\psi(x) - x = -C + o(x(\log M)^2) + \sum_{d \le x/m} \mu(d) \sum_{M < m \le x/d} (\log m - d(m) + C).$$

De un ejemplo anterior, sabíamos que $\sum_{n \le x} d(n) = \sum_{n \le x} [x/n]$ pero notando que a cada divisor $d|n$ con $d \le \sqrt{n}$ le corresponde un divisor $n/d \ge \sqrt{n}$ y viceversa, se tiene

$$\sum_{n \le x} d(n) = 2 \sum_{n \le x} \left[\frac{x}{n}\right] - [\sqrt{x}]^2$$

donde $[\sqrt{x}]^2$ descuenta los divisores $d = n/d$, contados dos veces. Aproximando $[x/n] = x/n + O(1)$ y usando la fórmula para las sumas parciales de la serie armónica, se deduce sumando por partes (ejercicio)

$$\sum_{M < m \le x/d} (\log m - d(m) + C) = (C - 2\gamma)(x/d - M) + O(x^{1/2} d^{-1/2} + M^{1/2}).$$

Escogiendo $C = 2\gamma$ y sustituyendo en la fórmula para $\psi(x) - x$, se sigue

$$\limsup |\psi(x)/x - 1| \ll M^{-1/2}.$$

Como M es arbitrario, el límite de $\psi(x)/x - 1$ existe y es nulo. □

Antes de pasar a esbozar demostraciones del teorema de los números primos, veamos una prueba falsa utilizando el comportamiento de $\zeta(s)$ cuando $s \to 1$. Todo el razonamiento es una línea:

$$\zeta(s) \sim (s-1)^{-1} \quad \overset{?}{\Rightarrow} \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \sim s - 1 \quad \overset{?}{\Rightarrow} \quad \sum_{n \le x} \mu(n) = o(x) \quad \overset{?}{\Rightarrow} \quad \text{TNP}.$$

En favor de la primera implicación está la relación $\zeta(s) D_\mu(s) = 1$, en favor de la segunda, la relación $\sum_{n \le x} \mu(n) = \sum_{n \le x} \sum_{m \ge n} \mu(m)/m$ y en favor de la última que la acabamos de probar. Se deja al lector el pasatiempo de localizar el error.

Las demostraciones clásicas del teorema de los números primos tienen como motivación tratar de despejar de alguna forma los primos de la identidad de Euler (1.3). Como allí están metidos de una manera complicada que involucra un producto, se muestra más sencillo despejar $\psi(x)$ de la relación

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

Veamos un esquema de dos demostraciones[12], como son sólo esquemas el lector debe imaginar interrogaciones donde sean necesarias.

a) Con análisis de Fourier:
Restemos $\zeta(s)$ en ambos miembros para quitar la singularidad de $s=1$. Escribiendo $n^{-\sigma-it} = n^{-\sigma}e(-t(\log n)/2\pi)$, al integrar contra una función f en los dos miembros (supóngase que es buena y hágase la vista gorda cuando se elija, o viceversa, más adelante habrá una justificación), se tiene para $\sigma > 1$

$$\int_{-\infty}^{\infty} g_\sigma(t)f(t)\,dt = \sum_{n=1}^{\infty}(\Lambda(n)-1)\frac{\widehat{f}((\log n)/2\pi)}{n^\sigma} \qquad \text{con} \quad g_\sigma(t) = -\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} - \zeta(\sigma+it).$$

Eligiendo una función f tal que

$$\widehat{f}(u) = \begin{cases} e^{2\pi\sigma u} & \text{si } u \in [0,(2\pi)^{-1}\log x] \\ 0 & \text{si } u \notin [0,(2\pi)^{-1}\log x] \end{cases}$$

se tiene una expresión exacta en términos de la función ζ para $\psi(x)-x$. Si nos molestamos en calcular la transformada inversa veremos que $f(t) = (x^{\sigma+it}-1)/(2\pi(\sigma+it))$. En un pequeño entorno del origen la función g_σ no difiere mucho de una constante, mientras que para x grande f se comporta como $x^{\sigma+it}$, entonces la contribución correspondiente es del orden de $x^\sigma/\log x$ y esto es malo si $\sigma > 1$, lo cual sugiere (¿obliga?) tomar $\sigma = 1$ entendiéndolo como una especie de límite. Hay dos problemas al respecto. El primero es el más serio y consiste en que no está claro que g_1 esté bien definida (un cero de ζ en $\Re s = 1$ causaría un desastre). Esto se resuelve con un estudio cuidadoso de la función ζ que prueba que g_1 crece como una potencia de logaritmo. El otro problema, más técnico, es que la convergencia de la integral no está asegurada, necesitábamos una función buena y hemos escogido una mala que sólo decae como t^{-1} y tiene transformada de Fourier discontinua. La solución pasa por regularizar un poco la f para ganar todas las potencias de logaritmo que deseemos aunque el principio de incertidumbre esté contra nosotros.

b) Con variable compleja:
Se puede despejar la suma de los coeficientes de una serie de Dirichlet gracias a la fórmula mágica

$$\lim_{T\to\infty} \frac{1}{2\pi i}\int_{L_T} \frac{y^s}{s}\,ds = \begin{cases} 0 & \text{si } 0 < y < 1 \\ 1 & \text{si } y > 1 \end{cases} \tag{1.13}$$

donde L_T es el segmento $\{s \;:\; \Re s = \sigma_0 > 0,\ |\Im s| < T\}$ orientado hacia arriba. La demostración se reduce al teorema de los residuos aplicado a la derecha o a la izquierda de L_T.

[12]Por si el lector está interesado, hay algunas pruebas muy simplificadas que siguen las líneas clásicas, por ejemplo las incluidas en [Ne] y en [Iw-Ko] p.40. También hay diferentes pruebas elementales (pero no sencillas) comenzando por las que dieron Erdős y Selberg (véase una en [El]). A pesar de su interés, tienen la desventaja de no revelar la verdadera naturaleza del término de error.

Si se tiene la convergencia adecuada (y si no se trunca la integral y se acota el error [Da]) entonces

$$\sum_{n\le x} f(n) = \frac{1}{2\pi i}\int_{L_\infty} D_f(s)\frac{x^s}{s}\,ds \qquad \text{para } x\in\mathbb{R}^+-\mathbb{N}.$$

En nuestro caso elegimos $\sigma_0>1$, $f(n)=\Lambda(n)$ y $D_f(s)=-\zeta(s)/\zeta(s)$. Sabemos que esta última función tiene una extensión meromorfa con al menos un polo simple de residuo 1 en $s=1$ (porque $\zeta(s)\sim(s-1)^{-1}$). Si $\mathcal{R}$ es una región que contiene al semiplano $\Re s\ge 1$ (y por tanto a L_∞) en la cual no hay ceros de ζ, entonces por el teorema de los residuos

$$\psi(x) = x - \frac{1}{2\pi i}\int_{\partial\mathcal{R}} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds \tag{1.14}$$

donde $\partial\mathcal{R}$ es el borde de $\mathcal{R}$ (orientado como L_∞). Si se tiene cierto control sobre ζ'/ζ y se asegura la existencia de tal región con $\partial\mathcal{R}$ contenido en $\Re s<1$, de (1.14) se deduce el teorema de los números primos. También queda el cabo suelto de la convergencia de las integrales, pero como ya hemos insinuado se resuelve sustituyendo (1.13) por una fórmula con T finito y término de error.

La prueba que acabamos de ver es muy ilustrativa. ¿Qué pasaría si se amplía la región $\mathcal{R}$ llevándola más y más a la izquierda sin importarnos que aparezcan ceros de ζ en su interior? Entonces x^s tendería a cero cuando $\Re s\to-\infty$ y habida cuenta que los polos del integrando en (1.14) son $s=0$ y $s=\rho$ donde ρ recorre los ceros de ζ, se tendría la llamada *fórmula explícita*

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

(como antes, para $x>0$ no natural). ¡Una fórmula explícita! A decir verdad, debido a la convergencia pobre es mucho más útil una fórmula no explícita sino truncada, como

$$\psi(x) = x - \sum_{|\rho|<T}\frac{x^\rho}{\rho} + O\big(\frac{x}{T}\log^2(xT)+\log x\big) \tag{1.15}$$

que es válida para cualquier $x>0$ porque la diferencia entre la contribución a $\psi(x)$ de un número entero y uno casi entero es absorbida por $O(\log x)$. Con esta fórmula tenemos que cuanto menor sea la parte real de los ceros, más pequeño será el error en el teorema de los números primos, recuérdese (1.12), y si un solo cero malvado tiene parte real casi uno, nos tendremos que aguantar con un error malo. ¿No es increíble que la distribución de los primos dependa tan estrechamente de una función de variable compleja?

Se sabe que hay infinitos ceros con $\Re\rho=1/2$ (esto se debe a Hardy, véase [El]) por tanto lo mejor que podemos esperar es lo que ya esperaba Riemann en 1860 (véase el apéndice de [Ed] con la traducción inglesa de la memoria original).

Hipótesis de Riemann: *Todos los ceros de ζ en el semiplano derecho tienen parte real* $1/2$.

Lo de restringirse al semiplano derecho se debe a que se conoce que los únicos ceros en el semiplano izquierdo son $-2, -4, -6, \ldots$, se dice que éstos son *ceros triviales*. Por otra parte, si hubiera ceros en $0 < \Re s < 1/2$, como veremos, también estarían sus simétricos por $\Re s = 1/2$ en $1/2 < \Re s < 1$.

Se sabe que hay $O(\log T)$ ceros de ζ con $T < |\rho| < T + 1$, $T > 2$, con lo cual de (1.15) y del Lema 1.4.3 se deduce

Corolario 1.4.5 *Si la hipótesis de Riemann es cierta, entonces*

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

La hipótesis de Riemann es un problema abierto desde hace casi 150 años (a pesar de los premios del paso a la posteridad y un millón de dólares) lo cual es suficiente para ahuyentar a casi todos los investigadores y atraer a no pocos diletantes. El avance actual es tan leve que siquiera se conoce ningún semiplano abierto conteniendo a $\Re s \geq 1$ en el que no haya ceros.

Para no sucumbir al desánimo ante un muro infranqueable, terminaremos con una breve lista de utensilios que sí podemos adquirir y que constituyen los puntos fundamentales que se han dejado en suspenso en los esquemas anteriores y los comentarios que los siguen.

1. Simetría de los ceros y ceros triviales.

2. Crecimiento del módulo de los ceros.

3. Región libre de ceros.

4. Acotaciones de ζ y ζ'/ζ.

El primer punto es la ecuación funcional por antonomasia y se debe al propio Riemann.

Proposición 1.4.6 *La función ζ tiene una extensión holomorfa a $\mathbb{C} - \{1\}$ y verifica la ecuación funcional*

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

Observación: Recuérdese que $\Gamma(z)$ está definida por $\int_0^\infty t^{z-1}e^{-t}\,dt$ si $\Re z > 0$ y se extiende analíticamente a $\mathbb{C} - \mathbb{Z}^- - \{0\}$ mediante $\Gamma(z+1) = z\Gamma(z)$. Casi todas las propiedades de la función Γ se pueden deducir de la fórmula (véase [Ah]) $1/\Gamma(z) = se^{\gamma s}\prod(1 + z/n)e^{-z/n}$ donde n recorre $\mathbb{Z}^+$ y γ es la constante de Euler. La aproximación de Stirling es válida para $\Gamma(z+1)$ cambiando N por z, se cumple $|\Gamma(z)/\Gamma'(z)| = O(\log|z|)$ y $\Gamma(z) \neq 0$.

Demostración: Hay varias pruebas de la ecuación funcional [Ti], aquí seguiremos la de la memoria de Riemann, que parte de la siguiente fórmula fruto de la definición de la función Γ en $s/2$, tras el cambio variable $t \mapsto \pi n^2 t$

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

o equivalentemente

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

Lo que se gana es que se puede aplicar la fórmula de Poisson a $\theta(t)$ dentro de la integral. Con ello esencialmente t pasará a $1/t$ y por tanto la parte de la integral $\int_0^1$ se transformará en $\int_1^{\infty}$. Esto es interesante para llevar a cabo la extensión ya que la divergencia de $\int_0^1 t^{s/2-1}t^{-1/2}dt$ para $\Re s < 1$ es la responsable de que se pueda extender el segundo miembro. Con esta idea en mente separando el rango de integración y utilizando $\theta(t) = t^{-1/2}\theta(1/t)$, el segundo miembro es

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

Con el cambio $t \mapsto 1/t$ en la primera integral se llega a que para $\Re s > 1$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s(s-1)} + \frac{1}{2}\int_1^{\infty} (t^{s/2-1} + t^{-1/2-s/2})(\theta(t)-1)\, dt \tag{1.16}$$

Ahora la integral tiene sentido para todo $s \in \mathbb{C}$ y como $\Gamma(s/2)$ no se anula, la función ζ así definida (que coincide con $\sum n^{-s}$ en $\Re s > 1$) es meromorfa en $\mathbb{C}$ y holomorfa en $\mathbb{C} - \{0, 1\}$. Usando que $\lim_{s\to 0} s\Gamma(s/2) = 2$ y $\Gamma(1/2) = \pi^{1/2}$ (véase [Ah]), se deduce que ζ es de hecho meromorfa en $\mathbb{C}$ con un único polo en $s = 1$ de residuo 1. Además la invariancia del segundo miembro de (1.16) al cambiar s por $1 - s$ termina la prueba. □

Corolario 1.4.7 *La función ζ tiene ceros simples en $s = -2, -4, -6$ (los llamados ceros triviales) y todos los ceros restantes están en la banda crítica $0 \le \Re s \le 1$. Además si ρ es un cero no trivial, también lo son $\overline{\rho}$, $1 - \rho$ y $1 - \overline{\rho}$.*

Demostración: De (1.3) se deduce que $\zeta(s) \neq 0$ en $\Re s > 1$ y por la ecuación funcional, $\Gamma(s/2)\zeta(s)$ no se anula en $\Re s < 0$. Como $\Gamma(s/2)$ tiene polos simples en $s = -2, -4, -6, \ldots$, es fácil deducir que éstos son ceros simples de ζ.

Finalmente, las simetrías de los ceros se deducen de la ecuación funcional y la relación $\zeta(s) = \overline{\zeta(\overline{s})}$ que es obvia en $\Re s > 1$ por $\zeta(s) = \sum n^{-s}$ y se extiende analíticamente. □

Para el resto de las propiedades se aplica la teoría de funciones de orden finito de de Hadamard [Ah] (quien la creó en relación con la función ζ) para obtener una bella fórmula.

Proposición 1.4.8 *Si s no es un polo de $\zeta'(s)/\zeta(s)$, se cumple*

$$\frac{\zeta'(s)}{\zeta(s)} = K - \frac{1}{s-1} - \frac{1}{2}\frac{\Gamma'(s/2+1)}{\Gamma(s/2+1)} + \sum_\rho \big(\frac{1}{s-\rho} + \frac{1}{\rho}\big)$$

donde ρ recorre los ceros no triviales de ζ y K es cierta constante.

Demostración: De acuerdo con (1.16) y la ecuación funcional, la función

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

es entera, cumple $\xi(s) = \xi(1-s)$ y $|\xi(s)| = O\big(e^{C|s|\log|s|}\big)$ para cierta constante $C > 0$ cuando $|s| \to \infty$. La teoría de funciones de orden finito asegura en este caso [Ah] que

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

donde el producto es sobre todos los ceros ρ no triviales de ζ, esto es $0 \le \Re\rho \le 1$. Tomando logaritmos y derivando se tiene la relación buscada. □

Corolario 1.4.9 *Para $T > 2$ el número de ceros con $T \le |\Im\rho| \le T+1$ es $O(\log T)$.*

Demostración: Si en la proposición anterior escribimos $s = 2+iT$ y tomamos partes reales, se tiene

$$1 \gg -\log T + \sum_\rho \mathrm{Re}\,\big(\frac{1}{2+iT-\rho} + \frac{1}{\rho}\big).$$

Después de calcular la parte real (recuérdese que $0 \le \Re\rho \le 1$) se sigue $\log T \gg \sum(1 + (T - \Im\rho)^2)^{-1}$ y de aquí el resultado. □

Proposición 1.4.10 *Existe una constante C (efectiva) tal que la región*

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

está libre de ceros de la función ζ.

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

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

y con ello comienza la prueba.

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

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

De la Proposición 1.4.8 cuando $\sigma > 1$ está suficientemente cercano a 1 se cumple $-\zeta'(\sigma)/\zeta(\sigma) < (\sigma-1)^{-1} + \text{cte}$, y además

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

Para probar estas desigualdades utilícese, aparte de la Proposición 1.4.8, $\Gamma'(s)/\Gamma(s) = O(\log|s|)$ y que $\Re((s-\rho)^{-1}+\rho^{-1}) > 0$ para $\Re s > 1$. Sustituyendo se obtiene

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

Tomando $\sigma = 1 + \epsilon/\log(|t_n|+2)$ con ϵ pequeño se sigue que $\sigma_n \leq 1 - \text{cte}/\log(|t_n|+2)$ para cierta constante positiva, que equivale al resultado. □

Por último veamos acotaciones para ζ y ζ'/ζ en $\Re s = 1$ que permitirían completar la prueba con análisis de Fourier del teorema de los números primos. (En realidad con mucha menos precisión es suficiente [Dy-Mc] §3.10)

Proposición 1.4.11 *Para $|t| > 2$ se cumple*

$$\zeta(1+it) = O(\log t) \qquad y \qquad -\frac{\zeta'(1+it)}{\zeta(1+it)} = O\big((\log t)^2\big).$$

Demostración: La primera es más elemental, sólo requiere sumar por partes en $\sum_{n>t} n^{-s}$ (con $\Re s > 1$) para concluir como en (1.6) que la fórmula

$$\zeta(s) - \sum_{n\leq t} n^{-s} = O(1) - s\int_t^\infty \frac{u-[u]}{u^{s+1}}\,du$$

es válida para $\Re s \geq 1$. Eligiendo $s = 1+it$ y haciendo las acotaciones triviales, se obtiene el resultado.

Para la segunda, tomando $s = 1+iT$ en la Proposición 1.4.8 y restando lo obtenido al sustituir $s = 2+iT$, se sigue

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

Los $O(\log T)$ sumandos correspondientes a $|T - \Im\rho| \leq 1$ contribuyen $O(\log^2 T)$ en total por la condición de la distancia. La contribución de los correspondientes a $|T - \Im\,\rho| > 1$ es menor sin más que emplear la acotación para $\sum(1+(T-\Im\rho)^2)^{-1}$ (véase el final de la prueba del Corolario 1.4.9). □

Bibliografía

[Ah] L.V. Ahlfors. Análisis de variable compleja: Introducción a la teoría de funciones analíticas de una variable compleja. Aguilar, Madrid 1971.

[Bo-Sh] A.I. Borevich, I.R. Shafarevich. Number theory. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[Cl] A. Clark. Elementos de álgebra abstracta. Alhambra, 1987.

[Co] A. Córdoba. Disquisitio numerorum. Gac. R. Soc. Mat. Esp. 4 (2001), no. 1, 249–260.

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

[Do-He] J.R. Dorronsoro, E. Hernández. Números, grupos y anillos. Addison-Wesley Iberoamericana–UAM, 1996.

[Dy-Mc] H. Dym, H.P. McKean. Fourier series and integrals. Probability and Mathematical Statistics 14. Academic Press, New York-London, 1972.

[Ed] H.M. Edwards. Riemann's zeta function. Pure and Applied Mathematics, Vol. 58. Academic Press, New York-London, 1974.

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

[Fo] G.B. Folland. Fourier analysis and its applications. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1992.

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

[Gr-Ko] S.W. Graham, G. Kolesnik. Van der Corput's method of exponential sums. London Mathematical Society lecture note series 126. Cambridge University Press, 1991.

[In] A.E. Ingham. The distribution of prime numbers. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990.

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

[Hu] M.N. Huxley. Area, lattice points, and exponential sums. London Mathematical Society Monographs 13. The Clarendon Press, Oxford University Press, New York, 1996.

[Ja] N. Jacobson. Lectures in Abstract Algebra. Vol.1,2,3. Van Nostrand, 1964.

[La] E. Landau. Über die Anzahl der Gitterpunkte in Gewissen Bereichen. Göttinger Nachr. (1912) 687–771.

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

[Po] A.G. Postnikov. Introduction to analytic number theory. Translations of Mathematical Monographs, 68. American Mathematical Society, Providence, RI, 1988.

[Ri] P. Ribenboim. 13 Lectures on Fermat's Last Theorem. Springer-Verlag, 1979.

[Ro] H.E. Rose. A course in number theory. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

[Sm] D.E. Smith. A Source Book in Mathematics. Dover Publications Inc., 1959.

[Sp] M. Spivak. Calculus. Vol. 1 y 2. Reverté, Barcelona, 1984.

[St] I. Stewart. Galois Theory. Chapman & Hall/CRC Mathematics, Boca Raton, FL, 2004.

[St-Ta] I. Stewart, D. Tall. Algebraic number theory. Chapman and Hall Mathematics Series. Chapman & Hall, London, 1987.

[Ti] E.C. Titchmarsh. The theory of the Riemann zeta-function. Second edition. The Clarendon Press, Oxford University Press, New York, 1986.

[Wi] E. Wirsing. Das asymptotische Verhalten von Summen über multiplikative Funktionen. Math. Ann. 143 (1961) 75–102.

Capítulo 2

Métodos de criba

2.1. Inclusión-exclusión e ideas básicas

Inclusión-exclusión. Acotación elemental de $\pi(x)$.

Viajemos por la historia a la leyenda hasta los tiempos de Eratóstenes. Según se dice, para confeccionar su tabla de números primos tomaba el 2 y tachaba todos sus múltiplos (propios); tras el 2, el primero que se había salvado de la criba es el 3; repitiendo la operación con él sobrevivirán todos los números primos con 6 distintos de 2 y 3. Si este proceso se continuase indefinidamente (y nos olvidamos del 1), se obtendría la lista de los números primos.

1ª pasada		**2**	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2ª pasada		2	**3**		5		7		9		11		13		15
		17		19		21		23		25		27		29	
3ª pasada		2	3		**5**		7				11		13		
		17		19				23		25				29	

Como máquina de generar primos, el procedimiento de Eratóstenes no se muestra muy práctico, y más hoy en día cuando en la más oscura oficina se oyen tartamudeos de disco duro y murmullos de ventilador. Sin embargo pertenece a los prolegómenos teóricos de algunas técnicas combinatorias agrupadas bajo el nombre de *métodos de criba* que se han mostrado muy efectivas en el estudio de problemas variopintos que involucran los primos. En realidad es poco más que una cortesía histórica apelar al nombre de Eratóstenes, pues en nada es comparable la simpleza de poner cruces (a pesar de las quinielas) con el refinamiento técnico alcanzado por los métodos de criba. La contribución temprana de Legendre está más cercana del contenido de esta sección pero aun así no es vituperable afirmar que los métodos de criba comenzaron con V. Brun [Br] en 1915.

Tanto Eratóstenes como nosotros encontramos cansino tachar infinitos números y por tanto nos restringiremos a los primos en $[1, N]$. Todavía menos, en vez de una lista

de primos, para ilustrar los aspectos del método supongamos que sólo queremos aproximar $\pi(N)$, contar primos[1] en lugar de exhibirlos. Para ello representamos el proceso de Eratóstenes como restar el cardinal de la unión de algunos conjuntos y se vuelve especialmente útil el siguiente principio.

Principio de inclusión-exclusión: Sean $C_1, C_2, \ldots, C_M$ conjuntos finitos, entonces

$$\#(C_1 \cup C_2 \cup \cdots \cup C_M) = \sum_{l=1}^{M} (-1)^{l+1} \sum_{1 \le j_1 < j_2 < \ldots < j_l \le M} \#(C_{j_1} \cap C_{j_2} \cap \cdots \cap C_{j_l}).$$

Con la sencilla fórmula $\#(A \cup B) = \#A + \#B - \#(A \cap B)$ la prueba se reduce a inducción o sentido común.

Si se tomase $C_j = \{n \le N \ : \ p_j | n\}$ con p_j el primo j-ésimo entonces $\#C_j = [N/p_j]$ y como todo número natural excepto el 1 es divisible por algún primo,

$$N - 1 = \left[\frac{N}{2}\right] + \left[\frac{N}{3}\right] + \cdots - \left[\frac{N}{2\cdot 3}\right] - \left[\frac{N}{2\cdot 5}\right] - \cdots + \left[\frac{N}{2\cdot 3\cdot 5}\right] + \left[\frac{N}{2\cdot 3\cdot 7}\right] + \ldots$$

que aislando el 1 se puede escribir como

$$1 = \sum_{n \le N} \mu(n) \left[\frac{N}{n}\right]$$

ya conocido por inversión de Möbius[2]. La razón de este valor tan escuálido es que en el proceso de Eratóstenes se ha cribado demasiado, hasta los propios primos se han tachado de la lista. Si se hubiera tratado de utilizar $C_j = \{n \le N \ : \ p_j | n, \ p_j > n\}$ las fórmulas habrían sido más complicadas y en cualquier caso dependerían de los primos, ¿tiene sentido dar una fórmula para $\pi(N)$ que depende a su vez de los primos?

El espíritu que anima y constriñe los métodos de criba llamados combinatorios es que hay que tratar de tachar lo menos posible para evitar una gran suma de errores y la dependencia de propiedades de los primos más fuertes que las buscadas. Por ejemplo, si sólo se criba con los primos 2 y 3

$$\pi(N) \le N - ([N/2] + [N/3] - [N/6]) + O(1) = N/3 + O(1).$$

Esto es, a lo más el 33'33 % de los números son primos, si se criba también con el 5, esta proporción pasa a ser del 26'66 %. Cuando se añaden más o menos primos para cribar el coeficiente de N disminuye pero el error $O(1)$ aumenta. Con suerte, estudiando esta dependencia en el número de primos "cribadores" y relacionándolo con N, quizá aparezca un $N/\log N$, y como todo número no primo en $[1, N]$ tiene algún factor menor que $\sqrt{N}$, quizá la cota superior devenga en una igualdad con término de error, un flamante teorema

[1] Naturalmente, tras lo visto en el capítulo anterior y la relación con los ceros de la función ζ, los razonamientos posteriores se muestran burdos pero es interesante y sorprendente notar cuán lejos se puede llegar con técnicas puramente combinatorias.

[2] El segundo miembro es $\sum_{n\le N} \mu(n) \sum_{m \le N/n} 1 = \sum_{k \le N} \sum_{n|k} \mu(n) = \sum_{k \le N} (1 * \mu)(k) = 1$ porque $\zeta(s) D_\mu(s) = 1$.

de los números primos sin emplear artillería pesada. Antes de seguir soñando es justo señalar que por el llamado *fenómeno de paridad* [He] hay impedimentos teóricos para demostrar el teorema de los números primos de esta forma o con cualquier técnica de criba clásica (las de este capítulo) sin emplear información adicional. Esto no es óbice para estudiar el procedimiento y comprobar dónde lleva.

Sea $\mathcal{A}_d = \{n \leq N \ : \ d|n\}$, está claro que $\mathcal{A}_{d_1} \cap \mathcal{A}_{d_2} = \mathcal{A}_{[d_1,d_2]}$ donde $[d_1, d_2]$ es el mínimo común múltiplo de d_1 y d_2. Para cada z se cuentan los números que no han sido cribados por primos menores o iguales que z

$$\pi(N) - \pi(z) + 1 \leq N - \#\bigcup_{p<z} \mathcal{A}_p.$$

Por el principio de inclusión-exclusión, escribiendo $A_d = \#\mathcal{A}_d$

$$\pi(N) \leq \sum_{d|P(z)} \mu(d) A_d + \pi(z) - 1 \qquad \text{con} \qquad P(z) = \prod_{p<z} p. \tag{2.1}$$

Se tiene $A_d = [N/d] = N/d + O(1)$ y trivialmente $\pi(z) \leq z$ (una estimación menos burda no cambiaría el orden del resultado final) por tanto

$$\pi(N) \leq \sum_{d|P(z)} \mu(d)\frac{N}{d} + O\big(z + \sum_{d|P(z)} 1\big).$$

Como $f(d) = 1/d$ es una función multiplicativa es fácil escribir la primera suma como un producto, mientras que la segunda suma es $2^{\pi(z)}$ que, esta vez con una pérdida mayor pero no decisiva, estimamos por $O(2^z)$. Entonces

$$\pi(N) \leq N \sum_{p<z} (1 - p^{-1}) + O(2^z).$$

Utilizando la fórmula de Mertens (1.5) y sumando por partes

$$\log \prod_{p<z} (1 - p^{-1}) = -\sum_{p<z} \frac{1}{p} + O(1) = -\log\log x + O(1).$$

Por tanto

$$\pi(N) \ll \frac{N}{\log z} + 2^z.$$

Usando esta desigualdad está claro que ni siquiera se puede deducir $\pi(N) \ll N/\log N$, porque $z = N^\alpha$ causa que el último sumando sea exponencialmente grande. Eligiendo $z = (\log N - \log\log N)/\log 2$ se deduce

$$\pi(N) \ll \frac{N}{\log\log N}$$

que es lo mejor que se puede obtener con cualquier elección de z. Es un resultado bastante débil pero aun así contrasta con la simplicidad de las ideas empleadas.

Se puede dar al argumento visos de generalidad, al menos como pretexto para introducir alguna terminología. Para cualquier neófito que quiera introducirse en los métodos de criba, uno de los obstáculos primeros es una notación endiablada (el lector no experimentado puede contrastar esta opinión abriendo al azar el libro clásico de Halberstam y Richert [Ha-Ri]). Aquí, aun a riesgo de perder generalidad, utilizaremos una versión muy reducida de ella que extiende ligeramente la empleada en el ejemplo anterior.

Notación:

- $\mathcal{A}$ es un subconjunto finito de $\mathbb{N}$.
- $P(z) = \prod_{p<z} p$.
- $S(\mathcal{A}, z) = \#\{a \in \mathcal{A} \ : \ (a, P(z)) = 1\}$.
- $\mathcal{A}_d = \{a \in \mathcal{A} \ : \ d|a\}$ y $A_d = \#\mathcal{A}_d$.
- X, $g(d)$ y r_d son tales que para d libre de cuadrados $A_d = Xg(d)/d + r_d$ con g multiplicativa, $0 \leq g(n) < n$ y X dependiendo sólo de $\mathcal{A}$.

Respecto a la última definición, la idea es que r_d es un término de error pequeño, así que X es el cardinal de $\mathcal{A}$ o un número cercano a él y $g(d)/d$ es como la probabilidad de que un elemento de $\mathcal{A}$ escogido al azar sea divisible por d. Es conveniente notar que $g(d)$ y r_d sólo están definidas para d libre de cuadrados, si aparecieran en una suma sobre d se sobreentiende que sólo se suma sobre dichos valores (típicamente basta con definirlas como cero en el resto de los casos).

Proposición 2.1.1 (criba de Eratóstenes-Legendre) *Con la notación anterior*

$$\left| S(\mathcal{A}, z) - X \prod_{p<z} (1 - g(p)/p) \right| \leq \sum_{d|P(z)} |r_d|.$$

Demostración: Basta repetir el razonamiento que llevó a (2.1). □

Observación: Interpretando X como $\#\mathcal{A}$ y $g(d)/d$ como la probabilidad de que un elemento de $\mathcal{A}$ sea divisible por d, la fórmula $S(\mathcal{A}, z)/X \approx \prod_{p<z}(1 - g(p)/p)$ que sugiere la proposición se muestra natural y cuantifica que la divisibilidad por diferentes primos son sucesos independientes[3] en cierta manera.

El siguiente lema auxiliar que probaremos a medias da el comportamiento de lo que pretende ser el término principal cuando g es constante.

[3]Estos sucesos no pueden ser independientes "del todo", si fuera así entonces $x \prod_{p \leq x^{1/2}}(1 - 1/p)$ debería comportarse como $\pi(x) - \pi(x^{1/2})$ pero estas expresiones no son asintóticamente iguales, su cociente tiende a una constante distinta de uno.

Lema 2.1.2 *Dado* $k \in \mathbb{Z} - \{0\}$

$$\prod_{k<p<x} \big(1 - \frac{k}{p}\big) = C_k (\log x)^{-k} + O((\log x)^{-k-1})$$

donde C_k *es una constante positiva. De hecho* $C_1 = e^{-\gamma}$ *con* γ *es la constante de Euler.*

Demostración: Tomando logaritmos y empleando $\log(1-h) = -h + O(h^2)$, basta probar

$$\sum_{p<x} \frac{1}{p} = \log\log x + \alpha_k + O((\log x)^{-1}).$$

Y esto es consecuencia de sumar por partes en la fórmula de Mertens $\sum_{p<x} p^{-1} \log p = \log x + O(1)$.

El cálculo de C_1 no es sencillo y se lleva a cabo comparando $\sum p^{-s}$ y $\log \zeta(s)$. Para una prueba completa véase [Ha-Wr] §22.8. □

Ejemplo. Vamos a estimar la cantidad de enteros en $[1, N]$ tales que todos sus divisores (diferentes de 1) sean mayores que $\sqrt{\log N}$. Con la notación recién introducida esto es $S(\mathcal{A}, \sqrt{\log N})$ donde $\mathcal{A} = [1, N] \cap \mathbb{N}$. Como antes, $A_d = N/d + O(1)$ y se tiene

$$S(\mathcal{A}, \sqrt{\log N}) = N \prod_{p<\sqrt{\log N}} (1 - p^{-1}) + O\big(2^{\sqrt{\log N}}\big).$$

Por el lema anterior,

$$S(\mathcal{A}, \sqrt{\log N}) \sim \frac{2e^{-\gamma} N}{\log\log N}.$$

Como se ve en este ejemplo, la criba no sólo sirve para dar acotaciones, también se puede utilizar para obtener resultados asintóticamente correctos, aunque tiene sus limitaciones (véase [Bo]).

2.2. La criba de Brun

Mejora de la acotación elemental de $\pi(x)$. La suma de los inversos de los primos gemelos converge.

Si $\mathcal{A} = [1, N] \cap \mathbb{N}$, al cribar por ejemplo con los primos menores que 8 (que son nada más que 4), se obtiene una fórmula kilométrica:

$$\begin{aligned} S(\mathcal{A}, 8) \;=\; & N - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] - \left[\frac{N}{5}\right] - \left[\frac{N}{7}\right] + \left[\frac{N}{2\cdot 3}\right] + \left[\frac{N}{2\cdot 5}\right] + \left[\frac{N}{2\cdot 7}\right] \\ & + \left[\frac{N}{3\cdot 5}\right] + \left[\frac{N}{3\cdot 7}\right] + \left[\frac{N}{5\cdot 7}\right] - \left[\frac{N}{2\cdot 3\cdot 5}\right] - \left[\frac{N}{2\cdot 3\cdot 7}\right] - \left[\frac{N}{2\cdot 5\cdot 7}\right] \\ & - \left[\frac{N}{3\cdot 5\cdot 7}\right] + \left[\frac{N}{2\cdot 3\cdot 5\cdot 7}\right] \end{aligned}$$

Esto explica por qué la criba de Eratóstenes no es muy buena, hay demasiados sumandos lo cual obliga a tomar z excesivamente pequeño. Si sólo se aspira a cotas superiores o inferiores uno podría considerar la parte de la suma anterior correspondiente a los denominadores con menos de dos o tres primos:

$$\begin{aligned} S^- &= N - \left[\frac{N}{2}\right] - \left[\frac{N}{3}\right] - \left[\frac{N}{5}\right] - \left[\frac{N}{7}\right] \\ S^+ &= S^- + \left[\frac{N}{2\cdot 3}\right] + \left[\frac{N}{2\cdot 5}\right] + \left[\frac{N}{2\cdot 7}\right] + \left[\frac{N}{3\cdot 5}\right] + \left[\frac{N}{3\cdot 7}\right] + \left[\frac{N}{5\cdot 7}\right] \end{aligned}$$

que son sumas un poco menos extensas.

Esta claro que $S^- \leq S(\mathcal{A}, 8) \leq S^+$ porque los positivos ganan a los negativos o viceversa. Pues bien, éste es un hecho general: los que tienen menos de $2k+1$ factores primos contribuyen siempre más y los que tienen menos de $2k$ factores primos, menos. Ésta es la idea básica de Brun (aunque su aportación es mucho más compleja y poderosa que esto). Jugando con k se puede disminuir a voluntad el número de sumandos y aun así conservar desigualdades. En general los métodos de criba basados en seleccionar sólo algunos de los sumandos que aparecerían en la criba de Eratóstenes-Legendre se dice que son metodos de *criba combinatoria*. A primera vista no parece que haya muchas más posibilidades que la apuntada inicialmente por Brun, pero muchos años de investigación sobre el tema han probado lo equivocado de esta impresión.

Un resultado simple que formaliza la idea anterior es

$$\sum_{\substack{d|n \\ \nu(d)<2k}} \mu(d) \leq \sum_{d|n} \mu(d) \leq \sum_{\substack{d|n \\ \nu(d)<2k+1}} \mu(d)$$

donde $\nu(d)$ representa el número de factores primos distintos de d y $k, n \in \mathbb{N}$.

En vez de dar la demostración[4] y seguir la línea anterior encontrando S^+ y S^-, daremos una expresión exacta para $S(\mathcal{A}, z)$ que muestra claramente la dependencia en la paridad de los factores. Con este fin es conveniente enunciar una identidad elemental llamada *identidad de Buchstab* que desempeña un papel destacado en los métodos de criba. Se acompaña de otra identidad hermana similar.

Lema 2.2.1 (identidad de Buchstab) *Con la notación anterior*

$$S(\mathcal{A}, z) = \#\mathcal{A} - \sum_{p<z} S(\mathcal{A}_p, p).$$

Además (para q recorriendo los primos)

$$\prod_{p<z}(1 - g(p)/p) = 1 - \sum_{p<z} \frac{g(p)}{p} \prod_{q<p}(1 - g(q)/q).$$

[4]Es bastante simple [Ci-Co] y se basa en la sencilla fórmula trivial $\sum \mu(d) = (-1)^r \binom{\nu(n)}{r}$ donde la suma recorre los divisores d de n con $\nu(d) = r$.

Demostración: La primera identidad dice que (!?) los elementos sin factores menores que z son todos excepto los que tienen como menor factor a un primo menor que z. La segunda identidad es la misma (??) salvo que se indican probabilidades en vez de cardinales. □

La expresión antes anunciada es:

Proposición 2.2.2 *Sea $r \in \mathbb{N}$, entonces*

$$S(\mathcal{A}, z) = \sum_{\substack{d|P(z) \\ \nu(d)<r}} \mu(d) A_d + (-1)^r \sum_{\substack{d|P(z) \\ \nu(d)=r}} S(\mathcal{A}_d, p_d)$$

donde p_d indica el menor factor primo de d. Además

$$\prod_{p<z}(1 - g(p)/p) = \sum_{\substack{d|P(z) \\ \nu(d)<r}} \mu(d)\frac{g(d)}{d} + (-1)^r \sum_{\substack{d|P(z) \\ \nu(d)=r}} \frac{g(d)}{d} \prod_{q<p_d}(1 - g(q)/q)$$

con p_d como antes y q recorriendo los primos.

Observación: Nótese que inmediatamente se deducen de aquí las desigualdades:

$$\sum_{\substack{d|n \\ \nu(d)<2k}} \mu(d) A_d \leq S(\mathcal{A}, z) \leq \sum_{\substack{d|n \\ \nu(d)<2k+1}} \mu(d) A_d.$$

Demostración: En el primer caso basta aplicar inductivamente la identidad de Buchstab. Si se la emplea dos veces

$$S(\mathcal{A}, z) = |\mathcal{A}| - \sum_{p_1<z} A_{p_1} + \sum_{p_2<p_1<z} S(\mathcal{A}_{p_1p_2}, p_2),$$

y otra vez más

$$S(\mathcal{A}, z) = |\mathcal{A}| - \sum_{p_1<z} A_{p_1} + \sum_{p_2<p_1<z} A_{p_1p_2} - \sum_{p_3<p_2<p_1<z} S(\mathcal{A}_{p_1p_2p_3}, p_3)$$

y así sucesivamente. La prueba de la otra identidad es similar. □

Recapitulemos la ventaja de las desigualdades de la observación: la fórmula exacta para $S(\mathcal{A}, z)$ (empleando la criba de Eratóstenes-Legendre) da lugar a una suma muy larga, exponencial en el número de factores primos en $P(z)$, donde se acumulan muchos términos de error. A través del parámetro k se puede controlar la longitud de sumas mayorantes y minorantes de $S(\mathcal{A}, z)$ y muy similares a ella (lo único que se hace es seleccionar algunos sumandos de la suma inicial). Por un lado nos gustaría tomar k pequeño para que hubiera pocos sumandos y por otra parte necesitaríamos que k sea moderadamente grande para que las cotas no sean burdas.

A partir de aquí los ajustes dependen de cada problema y se pueden relacionar con ciertas variables y estructuras asignadas genéricamente al escenario de la criba que requieren pagar el precio de una notación críptica que aquí se intenta evitar. Antes de mostrar un resultado general, jugaremos con el método empleando el ejemplo de la sección anterior.

Sea $\mathcal{A} = [1, N] \cap \mathbb{N}$, ya sabemos que $A_d = N/d + O(1)$ y aplicando la proposición con $r = 2k$ y $r = 2k + 1$

$$N \sum_{\substack{d|P(z)\\ \nu(d)<2k}} \frac{\mu(d)}{d} - z^{2k} \leq S(\mathcal{A}, z) \leq N \sum_{\substack{d|P(z)\\ \nu(d)<2k+1}} \frac{\mu(d)}{d} + z^{2k}$$

donde se ha usado la cota $\#\{d|P(z) \ : \ 0 < \nu(d) \leq r\} \leq \sum_{t=1}^{r} \binom{z}{t} \leq z^r$ (si esto es dudoso, $\pm z^{2k}$ se puede reemplazar por $O(z^{2k})$ sin problemas).

Para que esta cota sea operativa necesitamos ver cuánto es el sumatorio. Sin la condición sobre $\nu(d)$ es trivialmente $\prod_{p<z}(1 - 1/p)$ pero como esta condición es esencial al método no es posible obviarla y se hace necesaria la ingrata tarea de compensar los términos que faltan. Ésta es la razón de ser de la segunda identidad de la Proposición 2.2.2 que para $g(d) = 1$ produce

$$\sum_{\substack{d|P(z)\\ \nu(d)<r}} \frac{\mu(d)}{d} = \prod_{p<z} \left(1 - \frac{1}{p}\right) - (-1)^r \sum_{\substack{d|P(z)\\ \nu(d)=r}} \frac{1}{d} \prod_{q<p_d} \left(1 - \frac{1}{q}\right). \tag{2.2}$$

Teniendo en cuenta que el último producto es menor que 1, la suma está mayorada por $\big(\sum_{p<z} 1/p\big)^r/r!$ que usando la fórmula de Mertens es $(\log\log z + O(1))^r/r!$. Escogiendo $r = [A \log\log N]$ se tiene (ejercicio) que la contribución de la suma final en (2.2) es $O((\log N)^{-B})$ donde $B > 0$ es arbitrariamente grande si A lo es. En definitiva ese término no molesta.

Por otro lado, el primer producto es del mismo orden que $1/\log z$ y (2.2) implica

$$\sum_{\substack{d|P(z)\\ \nu(d)<r}} \frac{\mu(d)}{d} \asymp \frac{1}{\log z}.$$

Sustituyendo

$$S(\mathcal{A}, z) \asymp \frac{N}{\log z} \qquad \text{si} \qquad z^{2k} = o(N/\log z).$$

Escogiendo $z = \epsilon(N/\log N)^{1/2k}$ y recordando que $k \asymp \log\log N$, se obtiene $S(\mathcal{A}, z) \asymp N(\log\log N)/\log N$ y de aquí

$$\pi(N) \ll \frac{N}{\log N} \log\log N$$

que da el orden correcto de la función $\pi(N)$ salvo un factor $\log\log N$.

La mejora con respecto a la criba de Eratóstenes-Legendre se puede hacer general apurando bien las desigualdades.

Teorema 2.2.3 (criba de Brun) *Para cualquier $r \in \mathbb{N}$ se cumple*

$$\left|S(\mathcal{A},z) - X\prod_{p<z}(1-g(p)/p)\right| \leq X\sum_{\substack{d|P(z)\\ \nu(d)=r}}\frac{g(d)}{d} + \sum_{\substack{d|P(z)\\ \nu(d)\leq r}}|r_d|$$

Demostración: Por la Proposición 2.2.2, $S(\mathcal{A},z) - X\prod_{p<z}(1-g(p)/p)$ es

$$\sum_{\substack{d|P(z)\\ \nu(d)<r}}\mu(d)A_d - X\prod_{p<z}(1-g(p)/p) + (-1)^r\sum_{\substack{d|P(z)\\ \nu(d)=r}}S(\mathcal{A}_d,q_d)$$

$$= \sum_{\substack{d|P(z)\\ \nu(d)<r}}\mu(d)r_d + (-1)^r\sum_{\substack{d|P(z)\\ \nu(d)=r}}\left(S(\mathcal{A}_d,p_d) - X\frac{g(d)}{d}\prod_{q<p_d}(1-g(q)/q)\right)$$

Se cumple que $0 \leq S(\mathcal{A}_d,p_d) \leq A_d = Xg(d)/d + r_d$ y evidentemente el último producto está entre cero y uno. □

¿No parece todo esto combinatoria barata en la que uno quita y pone cosas irrelevantes? Las siguientes consecuencias hablan por sí solas.

Corolario 2.2.4 *Sea $\pi_2(x) = \#\{p \leq x \ : \ p \text{ y } p+2 \text{ son primos}\}$. Se cumple*

$$\pi_2(x) \ll x\left(\frac{\log\log x}{\log x}\right)^2.$$

Demostración: Sea $\mathcal{A} = \{n(n+2) \ : \ n \leq x\}$. Si q es un primo impar $A_q = 2X/q + O(1)$ y en general para d libre de cuadrados impar $A_d = 2^{\nu(d)}X/d + O\big(2^{\nu(d)}\big)$ (ejercicio), que se completa fácilmente con $A_2 = X/2+O(1)$ y $A_{2d} = 2^{\nu(d)}X/2d+O\big(2^{\nu(d)}\big)$. Así pues se toma $X = x$ y $g(d) = 2^{\nu(d)+1}/(3+(-1)^d)$ para d libre de cuadrados con $r_d = O(2^{\nu(d)})$. Para aplicar el teorema se necesitan las estimaciones:

$$\sum_{\substack{d|P(z)\\ \nu(d)=r}}\frac{2^{\nu(d)}}{d} = \sum_{\substack{d|P(z)\\ \nu(d)=r}}\frac{2^r}{d} \leq \frac{1}{r!}\left(\sum_{p<z}\frac{2}{p}\right)^r = \frac{(2\log\log z + O(1))^r}{r!}$$

y

$$\sum_{\substack{d|P(z)\\ \nu(d)\leq r}}2^{\nu(d)} \leq z^r\sum_{d|P(z)}\frac{2^{\nu(d)}}{d} = z^r\prod_{p<z}\big(1+\frac{2}{p}\big).$$

Como ya sabemos, eligiendo $r = [A\log\log x]$ la contribución de la suma con $\nu(d) = r$ está bajo control. Teniendo en cuenta estas acotaciones y $\prod_{p<z}(1+2/p) \asymp (\log z)^2$, el teorema asegura

$$\left|S(\mathcal{A},z) - x\prod_{p<z}(1-2/p)\right| \ll z^r(\log z)^2.$$

Así pues

$$\pi_2(x) \leq S(\mathcal{A}, z) + O(z) \ll \frac{x}{(\log z)^2} + z^r (\log z)^2$$

y tomando $z = x^{1/r}(\log x)^{-4/r}$ se termina la prueba. □

Más famosa y atractiva es la consecuencia de la consecuencia.

Corolario 2.2.5 *La suma de los inversos de los primos gemelos converge.*

Observación: Como todas las constantes en estos resultados son efectivas, es posible acotar el error en las sumas parciales y con ello dejar trabajando al ordenador día y noche para obtener el valor del límite de la serie con unas cuantas cifras decimales (véase [Sh-Wr], actualmente hay resultados mucho más precisos). El número obtenido, usando primos hasta $2'55 \cdot 10^{15}$, es $1'90216058\ldots$. Se dice que ésta es la *constante de Brun*.

Demostración: Basta sumar por partes. Sea $a_n = 1$ si n y $n+2$ son primos y $a_n = 0$ en otro caso,

$$\sum_{\substack{p,p+2 \text{ primos} \\ p \leq x}} \left(\frac{1}{p} + \frac{1}{p+2} \right) < 2 \sum_{n \leq x} \frac{a_n}{n} = 2\frac{\pi_2(x)}{x} + 2\int_1^x \frac{\pi_2(t)}{t^2}\, dt$$

y empleando el resultado anterior, la integral converge cuando $x \to \infty$. □

2.3. La criba de Selberg

La criba cuadrática. Mejora del resultado de Brun. Otras aplicaciones.

Ya habíamos visto que la base de la criba de Brun era seleccionar algunos términos en $S(\mathcal{A}, z) = \sum_{d|n} \mu(d) A_d$ pasando la igualdad a desigualdades. En esta sección veremos una criba no combinatoria, es decir, no se omiten términos, lo que se hará es reemplazar el coeficiente $\mu(d)$ por otra función. En principio esto no parece tener sentido porque las propiedades de μ son esenciales en el proceso de criba. Ver para creer, por ejemplo se cumple

$$S(\mathcal{A}, 4) \leq A_1 + \frac{1 - 2\sqrt{2}}{2} A_2 + \frac{1 - 2\sqrt{3}}{3} A_3 + \frac{2}{\sqrt{6}} A_6,$$

y en general, para cualquier $\alpha, \beta \in \mathbb{R}$

$$S(\mathcal{A}, 4) \leq A_1 + (\alpha^2 + 2\alpha) A_2 + (\beta^2 + 2\beta) A_3 + 2\alpha\beta A_6.$$

La prueba es elemental, simplemente desarrollar y agrupar en

$$S(\mathcal{A}, 4) = \sum_{\substack{a \in \mathcal{A} \\ (a,6)=1}} 1 \leq \sum_{\substack{a \in \mathcal{A} \\ (a,6)=1}} 1 + \sum_{\substack{a \in \mathcal{A} \\ (a,6)=2}} (1+\alpha)^2 + \sum_{\substack{a \in \mathcal{A} \\ (a,6)=3}} (1+\beta)^2 + \sum_{\substack{a \in \mathcal{A} \\ (a,6)=6}} (1+\alpha+\beta)^2$$

En 1947 A. Selberg desarrolló esta idea creando un método de criba consistente en buscar la "desigualdad óptima"que responde a demostraciones como la anterior con formas cuadráticas en los parámetros (véase [Se]). La optimización se adapta al problema, lo que permite en general superar los resultados de Brun. En el ejemplo anterior si se cumpliera $A_d \approx N/d$, $d = 1, 2, 3, 6$, entonces al minimizar en α y β se obtiene más o menos $A_1 - 0'98A_2 - 0'95A_3 + 1'36A_6$. Sin embargo si todos los números de A son pares con $A_1 \approx A_2 \approx N$, $A_3 \approx A_6 \approx N/3$, la desigualdad óptima sería $A_1 - 0'99A_2 - 0'79A_3 + 0'49A_6$.

El poder grandioso de la criba de Selberg contrasta enormemente con la simplicidad de su punto de partida (honor que comparten otras ideas geniales). Más que en el propio enunciado del siguiente resultado, el lector debería detenerse en la prueba.

Lema 2.3.1 *Sea $\{\lambda_n\}_{n=1}^{\infty}$ una sucesión de números reales con $\lambda_1 = 1$ y $\lambda_n = 0$ si n no es libre de cuadrados o $n \geq z$, entonces*

$$S(\mathcal{A}, z) \leq \sum_{d_1, d_2} \lambda_{d_1} \lambda_{d_2} A_{[d_1, d_2]}$$

donde $[d_1, d_2]$ representa el mínimo común múltiplo.

Demostración: Si $a \in \mathcal{A}$ no tiene divisores primos menores que z se tiene que $\left(\sum_{d|a} \lambda_d\right)^2$ es uno, en cualquier caso esta cantidad es positiva y por consiguiente

$$S(\mathcal{A}, z) \leq \sum_{a \in \mathcal{A}} \left(\sum_{d|a} \lambda_d\right)^2 = \sum_{a \in \mathcal{A}} \sum_{d_1|a} \sum_{d_2|a} \lambda_{d_1} \lambda_{d_2}$$

y basta intercambiar el orden de sumación. □

Observación: La criba de Selberg en toda generalidad permite jugar con un parámetro llamado *nivel* que, al igual que r en la criba de Brun, sirve para controlar el tamaño de las sumas. Para simplificar, aquí no se considerará tal diversión.

Con la confianza, o la hipótesis de que A_d está bien aproximado por $Xg(d)/d$ (para d libre de cuadrados) lo que se necesita es minimizar la siguiente forma cuadrática en los λ_n

$$Q = \sum_{d_1, d_2} \frac{g([d_1, d_2])}{[d_1, d_2]} \lambda_{d_1} \lambda_{d_2}$$

y esto parece muy difícil porque sus coeficientes son aritméticos. Una luz de esperanza es que si d_1 y d_2 fueran coprimos siempre, $g([d_1, d_2])/[d_1, d_2] = g(d_1)/d_1 \cdot g(d_2)/d_2$ y Q sería simplemente $(\sum g(d)\lambda_d/d)^2$. Para salvar este obstáculo se puede tratar de separar el máximo común divisor porque $[d_1, d_2]$ coincide con $d_1 d_2$ salvo dividir por (d_1, d_2). Antes de acabar de violentar las normas de los libros de estilo, anunciemos dónde queremos llegar.

Proposición 2.3.2 *Se tiene*

$$\min Q = \left(\sum_{d<z} h(d)\right)^{-1} \qquad con \quad h(n) = \mu^2(n)\prod_{p|n}\frac{g(p)}{p-g(p)}$$

donde el mínimo se toma sobre todas las sucesiones λ_n como en el lema anterior. Además los valores para los que se alcanza el mínimo verifican $|\lambda_n| \le 1$.

Demostración: Según lo dicho anteriormente,

$$Q = \sum_{d_1,d_2}\frac{g(d_1d_2)}{d_1d_2}\gamma((d_1,d_2))\lambda_{d_1}\lambda_{d_2} \qquad \text{donde} \quad \gamma(d) = \begin{cases} d/g(d) & \text{si } g(d)\neq 0 \\ 0 & \text{en otro caso} \end{cases}$$

Por inversión de Möbius, $\gamma(n) = \sum_{d|n} f(d)$ con $f = \mu * \gamma$ y se puede escribir

$$Q = \sum_{d_1,d_2}\frac{g(d_1d_2)}{d_1d_2}\lambda_{d_1}\lambda_{d_2}\sum_{m|(d_1,d_2)} f(m) = \sum_m f(m)\Big(\sum_{d\equiv 0\ (m)}\frac{g(d)}{d}\lambda_d\Big)^2.$$

Aquí y en el resto de la prueba se supondrá que m es libre cuadrados y $m < z$.

Si se denota con x_m la suma bajo el cuadrado, la forma cuadrática ya está diagonalizada. La restricción $\lambda_1 = 1$ equivale a $\sum \mu(m)x_m = 1$ porque

$$\sum_m \mu(m)\sum_{d\equiv 0\ (m)}\frac{g(d)}{d}\lambda_d = \sum_d \big(\sum_{m|d}\mu(m)\big)\frac{g(d)}{d}\lambda_d = \lambda_1.$$

En definitiva, el mínimo buscado es el de $\sum f(m)x_m^2$ sujeto a $\sum \mu(m)x_m = 1$. Éste es un problema de Cálculo II con letras raras pero sencillo. El mínimo se alcanza para

$$x_m = \frac{\mu(m)}{f(m)H} \qquad \text{con} \quad H = \sum\frac{1}{f(d)}$$

donde d recorre los libres de cuadrados menores que z. Para asegurar que esto tiene sentido, nótese que $f(p) = (\mu*\gamma)(p) = p/g(p) - 1 \neq 0$ y por tanto $H = \sum_{d\le z} h(d)$. Evaluando $\sum f(m)x_m^2$ se tiene que el mínimo buscado es H^{-1}.

La comprobación de $|\lambda_n| \le 1$ es indirecta y más compleja de lo que cabría esperar. Fijado n libre de cuadrados

$$H = \sum_{k|n} h(k)\sum_{\substack{d<z/k\\(d,n)=1}} h(d) \ge \big(\sum_{k|n} h(k)\big)\sum_{\substack{d<z/n\\(d,n)=1}} h(d). \tag{2.3}$$

No es difícil "despejar" los λ_n a partir de x_m (ejercicio), esto prueba de paso que el cambio de variable era lícito:

$$\lambda_n = \mu(n)\frac{n}{g(n)}\sum_{m\equiv 0\ (n)}\mu(m)x_m.$$

Utilizando la fórmula para los x_m minimizantes se tiene

$$\sum_{\substack{d<z/n\\(d,n)=1}} h(d) = \frac{1}{h(n)} \sum_{m\equiv 0 \ (n)} h(m) = \frac{g(n)}{nh(n)} H\lambda_n = H\lambda_n \prod_{p|n} \frac{g(p)}{ph(p)},$$

mientras que por las propiedades multiplicativas

$$\sum_{k|n} h(k) = \prod_{p|n} (1+h(p)) = \prod_{p|n} \frac{ph(p)}{g(p)}.$$

Sustituyendo en (2.3) se llega a $|\lambda_n| \leq 1$. □

Con esto ya se tiene el cerebro de la criba de Selberg, sólo resta moldear unas formas bellas.

Teorema 2.3.3 (criba de Selberg) *Para cada $z > 1$*

$$S(\mathcal{A}, z) \leq X\big(\sum_{d<z} h(d)\big)^{-1} + \sum_{d<z^2} \mu^2(d) 3^{\nu(d)} |r_d|$$

donde $h(n) = \mu^2(n) \prod_{p|n} g(p)/(p-g(p))$.

Demostración: Por el Lema 2.3.1

$$S(\mathcal{A}, z) \leq \sum_{d_1,d_2} \frac{g([d_1,d_2])}{[d_1,d_2]} \lambda_{d_1}\lambda_{d_2} + \sum_{d_1,d_2} |r_{[d_1,d_2]}| \lambda_{d_1}\lambda_{d_2}.$$

con la elección óptima de la Proposición 2.3.2

$$S(\mathcal{A}, z) \leq X\big(\sum_{d<z} h(d)\big)^{-1} + \sum_{d<z^2} |r_d| \mu^2(d) \sum_{[d_1,d_2]=d} 1$$

y el último sumatorio es exactamente $3^{\nu(d)}$ para d libre de cuadrados. □

Ejemplo. con $\mathcal{A} = [1, N] \cap \mathbb{N}$ se tiene $g(d) = 1$ y $|r_d| \leq 1$ por lo cual $h(p) = p^{-1} + p^{-2} + p^{-3} + \ldots$ y se cumple

$$S(\mathcal{A}, z) \leq N\big(\sum_{d<z} \frac{1}{d}\big)^{-1} + \sum_{d<z^2} \mu^2(d) 3^{\nu(d)}.$$

Con un "truquito" se puede estimar la última suma

$$\sum_{d<z^2} \mu^2(d) 3^{\nu(d)} < z^2 \sum_{d<z^2} \frac{\mu^2(d)}{d} 3^{\nu(d)} = z^2 \sum_{d_1d_2d_3<z^2} \frac{\mu^2(d_1d_2d_3)}{d_1d_2d_3} \leq z^2\big(\sum_{d<z^2} \frac{1}{d}\big)^3.$$

Por consiguiente, con las cotas para la serie armónica, $\log N < \sum_{n<N} 1/n < 1 + \log N$ se concluye

$$S(\mathcal{A}, z) < N/\log z + z^2(1 + 2\log z)^3. \tag{2.4}$$

Eligiendo $z = N^{1/2}/(\log N)^2$ se tiene para $N > 100$

$$S(\mathcal{A}, z) < 44\frac{N}{\log N}.$$

Con esto ¡por fin conseguimos una cota superiorpara $\pi(x)$ del orden correcto de magnitud! Hay otra cosa notoria y es que z es "casi" como $N^{1/2}$ y por tanto $S(\mathcal{A}, z)$ es "casi" como $\pi(N) - \pi(z)$.

Con hipótesis adicionales es posible transformar el teorema anterior en un artículo de consumo en el que se sustituyen unos parámetros por un lado y se recoge el producto por otro.

Teorema 2.3.4 *Con la notación del teorema anterior, si*

$$\sum_{p<z} h(p)\log p = \kappa \log z + O(1) \qquad y \qquad r_d = O(M^{\nu(d)})$$

para alguna constante $M \in \mathbb{N}$, entonces

$$S(\mathcal{A}, z) \leq C\frac{X}{(\log z)^\kappa} + O\big(\frac{X}{(\log z)^{\kappa+1}} + z^2(\log z)^{3M}\big)$$

donde $C = \Gamma(\kappa+1)\prod(1 - g(p)/p)/(1-1/p)^\kappa$.

Demostración: Por el teorema de Wirsing se tiene

$$\sum_{n<z} h(n) = \frac{(\log z)^\kappa}{\Gamma(\kappa+1)}\prod(1+h(p))(1-1/p)^\kappa + O((\log z)^{\kappa-1})$$

y por otra parte con el truco ya empleado para (2.4),

$$\sum_{d<z^2}\mu^2(d)(3M)^{\nu(d)} < z^2\sum_{d<z^2}\mu^2(d)\frac{(3M)^{\nu(d)}}{d} \leq z^2\bigg(\sum_{d<z^2}\frac{\mu^2(d)}{d}\bigg)^{3M} = O(z^2(\log z)^{3M}).$$

Basta sustituir estas dos estimaciones en el teorema anterior. □

Vayamos ahora con las aplicaciones.

Corolario 2.3.5 *Sea $\pi_2(x) = \#\{p \leq x \ : \ p \ y \ p+2 \ son \ primos\}$, entonces*

$$\pi_2(x) \leq \frac{16x}{(\log x)^2}\prod_{p>2}\frac{p(p-2)}{(p-1)^2}\bigg(1 + O\big(\frac{\log\log x}{\log x}\big)\bigg)$$

Observación: Si se cumplen conjeturas profundas, debidas a Hardy y Littlewood, la desigualdad debería poder reemplazarse por una igualdad cambiando 16 por 4. En relación con estas conjeturas, la criba de Selberg también produce cotas superiores del orden de magnitud esperado para primos "trillizos" y otras familias numerosas.

Demostración: Tómese $\mathcal{A} = \{n(n+2) \,:\, n \le x\}$, entonces $A_d = xg(d)/d + r_d$ (para d libre de cuadrados) con $g(d) = 2^{\nu(d)}$ si d es impar y $g(d) = 2^{\nu(d)-1}$ si es par. En cualquier caso $g(d) \ge |r_d|$. De $h(p) = 2/(p-2)$ para $p > 2$ se deduce $\sum_{p<z} h(p)\log p = 2\log z + O(1)$ (fórmula de Mertens) y el teorema se aplica produciendo

$$S(\mathcal{A}, z) \le 4\prod_{p>2}(1-2/p)(1-1/p)^{-2}\frac{X}{(\log z)^2} + O\Big(\frac{X}{(\log z)^3} + z^2(\log z)^6\Big).$$

Escogiendo $z = x^{1/2}(\log x)^{-6}$ y notando que $S(\mathcal{A}, z) \ge \pi_2(x) + O(z)$ se termina la prueba. □

Corolario 2.3.6 *Para $x, y > 1$*

$$\pi(x+y) - \pi(x) \le \frac{2y}{\log y} + O\left(\frac{y\log\log y}{(\log y)^2}\right).$$

Demostración: Evidentemente se puede aplicar el teorema con $\mathcal{A} = [x, x+y] \cap \mathbb{N}$ pero ya hemos hecho el trabajo porque todo funciona exactamente igual que en la deducción de (2.4) (allí $x = 1$, $y = N - 1$), por tanto

$$S(\mathcal{A}, z) < \frac{y}{\log z} + O(z^2(\log z)^3)$$

y basta tomar $z = y^{1/2}(\log y)^{-3}$ □

Nada impide considerar progresiones aritméticas en vez de intervalos trasladados o ¿por qué no? ambas cosas a la vez.

Corolario 2.3.7 (desigualdad de Brun-Titchmarsh) *Sea $\pi(x; q, a) = \#\{p \le z \,:\, p \equiv a\ (q)\}$ con $a, q \in \mathbb{N}$, $(a, q) = 1$. Para $x, y > 1$ se cumple*

$$\pi(x+y; q, a) - \pi(x; q, a) < \frac{2y}{\phi(q)\log(y/q)} + O\left(\frac{y}{\phi(q)(\log(y/q))^2}\right)$$

Demostración: Tómese $\mathcal{A} = \{n \in [x, x+y] \,:\, n \equiv a\ (q)\}$, $X = y/q$, $g(d) = 1$ si $(d, q) = 1$ y $g(d) = 0$ en otro caso. Entonces (para d libre de cuadrados) $A_d = Xg(d)/d + r_d$ con $r_d = O(1)$ y todo lo que hay que hacer es meter estos ingredientes en la máquina del teorema. □

Después de todos estos ejemplos que alaban las glorias de la criba de Selberg es justo señalar el inconveniente de que no proporciona directamente cotas inferiores para $S(\mathcal{A}, z)$. Dando algún rodeo es posible paliar en parte esta deficiencia, por ejemplo la identidad de Buchstab permite pasar cotas superiores a inferiores. En otro contexto, esta idea será explotada en la próxima sección.

2.4. Nociones y aplicaciones de la criba lineal

Una criba combinatoria. El teorema de Jurkat-Richert. Algunos ejemplos

La criba de Selberg es la mejor criba entre aquellas cuyos coeficientes vienen determinados por ciertas formas cuadráticas. En esta sección volvemos a una criba de tipo combinatorio como la de Brun, es decir, se eligen sumandos $\sum_{d|P(z)} \mu(d)A_d$. En el caso que aquí se analiza resulta ser óptima (aunque no entraremos en ello) dejando un sabor agridulce porque por una parte permite mejorar algunas estimaciones y al tiempo muestra que sin hipótesis más restrictivas o particularidades específicas de algunos problemas no es posible ir más allá.

El teorema central de esta sección, el *teorema de Jurkat-Richert*, tiene una prueba que no es en absoluto sencilla y es difícil entrever las ideas principales siguiéndola paso a paso. Aferrándonos a las directrices del curso y favorecidos por la falta de diligencia, se omitirá dicha prueba aquí, reemplazándola por algunas ideas a veces etéreas, a veces tangibles.

Antes de nada volvamos a primeros principios para introducir algo más de notación. Por el principio de inclusión-exclusión (criba de Eratóstenes-Legendre) sabíamos que

$$S(\mathcal{A}, z) = \sum_{d|P(z)} \mu(d)A_d.$$

Una criba combinatoria consiste en hallar dos conjuntos $\mathcal{D}^-, \mathcal{D}^+ \subset \mathbb{N}$ tales que

$$\sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)|A_d| \leq S(A, z) \leq \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)|A_d|.$$

El siguiente paso es sustituir $A_d = Xg(d)/d + r_d$ y crear un término principal a partir de la suma de $Xg(d)/d$ y un término de error a partir de la de r_d. Si $\mathcal{D}^-$ y $\mathcal{D}^+$ son "sustanciosos" este término principal debe ser comparable a $X\prod_{p<z}(1 - g(p)/p)$.

Digamos que $\mathcal{D}^-, \mathcal{D}^+ \subset [1, D]$. No tiene sentido $D < z$ porque esto significaría que se puede reducir z teniendo el mismo resultado. Si $D = z^s$ con $s > 1$ estaremos vedando los valores que tengan más de s factores primos próximos a z. De esta forma el parámetro s se asemeja a r en la criba de Brun, dando cierto control sobre el número de factores y si s es suficientemente grande, se llegará a la criba de Eratóstenes-Legendre y el inconveniente es ya conocido: hay problemas para controlar el término de error. El tamaño admisible depende del término principal de que dispongamos, con las hipótesis que aparecerán más adelante este término será al menos comparable a $X/\log z$ y con un error $o(X/\log X)$ estamos a salvo porque en los ejemplos ya vistos no tiene sentido $z > X$.

Resumiendo, dados z y $s > 1$ se define $D = z^s$ y se supone

$$\sum_{\substack{d|P(z)\\ d<D}} |r_d| \ll \frac{X}{(\log X)^C} \qquad \text{para algún} \quad C > 1. \tag{2.5}$$

Dependiendo del valor de s el valor del término principal se puede ver amplificado o disminuido. Se esperan por tanto desigualdades del tipo:

$$f(s)\,\Pr(\mathcal{A},z)+O(E)\le S(\mathcal{A},z)\le F(s)\,\Pr(\mathcal{A},z)+O(E) \tag{2.6}$$

donde

$$\Pr(\mathcal{A},z)=X\prod_{p<z}(1-g(p)/p)\quad\text{y}\qquad E=\frac{X}{(\log X)^C}.$$

Dar a $f(s)$ y $F(s)$ nombre de función en vez de nombre de constante tiene su lógica por los razonamientos posteriores. De acuerdo con lo dicho anteriormente, si $\mathcal{D}^-$ y $\mathcal{D}^+$ se eligen "de la mejor manera", cuando $s\to\infty$ se tiene que cumplir $f(s),F(s)\to 1$ porque la criba de Eratóstenes da una igualdad con $\Pr(\mathcal{A},z)$ salvo el término de error. Por otro lado, si s se empequeñece, las cotas se volverán burdas y parece creíble que para $s\in[1,\beta]$ sólo se pueda obtener la cota inferior trivial[5] $f(s)=0$.

Supongamos que tenemos alguna de las desigualdades de (2.6), digamos por ejemplo la inferior. En principio esta cota podría ser trivial o casi trivial (porque s esté cerca de β). Lo que se mostrará es un proceso que transforma cotas inferiores en superiores mejorándolas cada vez. El objetivo es buscar el límite. Este proceso no es más que la identidad de Buchstab que se debería reflejar en los términos principales como

$$S(\mathcal{A},z)\lesssim X-\sum_{p<z}f(s_p)X_p\prod_{q<p}(1-g(q)/q)$$

donde ahora X_p es la aproximación del cardinal de $\mathcal{A}_p$, así pues $X_p\approx Xg(p)/p$, y s_p debería cumplir $D/p=p^{s_p}$ ya que éste es el análogo natural de $D=z^s$ al cambiar $S(\mathcal{A},z)$ por $S(\mathcal{A}_p,p)$. Teniendo todo esto en cuenta y restando a la fórmula anterior la siguiente forma de la segunda identidad del Lema 2.2.1

$$\Pr(\mathcal{A},z)=X-\sum_{p<z}\Pr(\mathcal{A}_p,p) \tag{2.7}$$

se obtiene

$$S(\mathcal{A},z)\lesssim\Pr(\mathcal{A},z)+\sum_{p<z}\left(1-f\big(\frac{\log(D/p)}{\log p}\big)\right)\Pr(\mathcal{A}_p,p).$$

Ahora ya estamos preparados para hacer la trampa mayor. Supondremos que se puede sustituir $\Pr(\mathcal{A},z)$ por $\mathrm{cte}X/\log z$ (lo cual es como decir de algún modo que $g(p)$ es igual a 1 en promedio). Si $\Pr(\mathcal{A},z)$ fuera realmente muy igual a $\mathrm{cte}X/\log z$, derivando en (2.7) se tendría (??) $X(\mathrm{cte}(\log z)^{-1})'=-\sum\Pr(\mathcal{A}_p,p)\delta(z-p)$ donde δ es la delta de Dirac. Por supuesto esto no tiene ningún sentido riguroso comenzando porque $\Pr(\mathcal{A},z)$ toma valores discretos y $\mathrm{cte}X/\log z$ es una función continua. Cerrando los ojos se sigue

$$\begin{aligned}S(\mathcal{A},z)&\lesssim\Pr(\mathcal{A},z)-X\int_1^z\left(1-f\big(\frac{\log(D/t)}{\log t}\big)\right)d(\mathrm{cte}(\log t)^{-1})\\&\approx\Pr(\mathcal{A},z)\left[1-\int_1^z\left(1-f\big(\frac{\log(D/t)}{\log t}\big)\right)\log z\;d((\log t)^{-1})\right].\end{aligned}$$

[5] Una analogía a través de un ejemplo es lo que ocurriría si en el proceso de Brun sólo se consideraran números con un factor primo ($r=1$), entonces $X-X/2-X/3-\cdots-X/p$ con $p\approx X$ es negativo y la cota es trivial.

Con el cambio de variable de $u = \log D/\log t$ y recordando que $D = z^s$, se llega a

$$S(\mathcal{A}, z) \lesssim \Pr(\mathcal{A}, z)\left(1 + \frac{1}{s}\int_s^\infty (1 - f(u-1))\, du\right).$$

Esto significa que dada una f para la que se verifique la primera desigualdad de (2.6) se halla una F válida para la segunda mediante

$$F(s) = 1 + \frac{1}{s}\int_s^\infty (1 - f(u-1))\, du$$

que se puede escribir en forma diferencial como $(sF(s))' = f(s-1)$. De la misma forma, dada una F válida se obtiene una f tal que $(sf(s))' = F(s-1)$. Si hasta $s = \beta$ sólo se tiene la cota inferior trivial, esto es, $f(s) = 0$ para $s \leq \beta$, entonces $F(s) = \text{cte}/s$ para $s \leq \beta+1$, ahora se podría sustituir en $(sf(s))' = F(s-1)$ y llegar a $f(s) = \text{cte}s^{-1}\log(s-1)$ para $\beta \leq s < \beta + 1$. No olvidemos que β y la constante son desconocidas pero tenemos a nuestro favor que sabemos que f y F son 1 en el infinito, e iterando infinitas veces (??) se tendría un sistema 2×2 para estas incógnitas (??). En fórmulas, lo que se pretende es resolver

$$\begin{cases} (sF(s))' = f(s-1) & \text{si } s > \beta + 1 \\ (sf(s))' = F(s-1) & \text{si } s > \beta \\ 0 \leq f \leq f(\infty) = 1, & 1 = F(\infty) \leq F \\ f(s) = 0 \ \text{ si } s \leq \beta, & F(s) = \text{cte}/s \ \text{ si } \ s \leq \beta + 1 \end{cases}$$

Pues bien, se puede probar que las únicas posibilidades son $\beta = 2$ y que la constante tome el valor $2e^\gamma$ con γ la constante de Euler. Entonces f y F son soluciones de la ecuación rara[6]

$$\begin{cases} (sF(s))' = f(s-1) & \text{si } s > 3 \\ (sf(s))' = F(s-1) & \text{si } s > 2 \\ f(s) = 0 \ \text{ si } s \leq 2, & F(s) = 2e^\gamma/s \ \text{ si } \ s \leq 3 \end{cases} \tag{2.8}$$

Dado un s se puede hallar fácilmente $f(s)$ y $F(s)$ iterando a partir de las condiciones iniciales.

Después de toda esta historieta quedan dos cabos sueltos. En primer lugar el enunciado exacto en el que se materializan las ideas anteriores, y en segundo lugar explicar qué tiene que ver todo esto con la criba combinatoria mencionada al principio.

En la argumentación anterior se había empleado que $\Pr(\mathcal{A}, z)$ era, salvo constantes, como $X/\log z$ lo cual indica que de algún modo $g(p)$ es uno en promedio (por la fórmula de Mertens), incluso en intervalos pequeños porque por ejemplo la dudosa derivación en (2.7) parece requerir algún control en los incrementos.

[6]Esto es lo que se llama una *ecuación diferencial en diferencias*. Estas ecuaciones son naturales en modelos de población. Por ejemplo, que la tasa de variación de la población sea proporcional a la propia población no es muy creíble si los individuos tardan un tiempo t_0 grande en poder reproducirse tras su nacimiento. Esto se refleja en sustituir la ecuación $P'(t) = \alpha P(t)$ por $P'(t) = \alpha P(t - t_0)$.

La hipótesis se puede escribir como

$$\sum_{w\le p<z}\frac{g(p)\log p}{p}=\log z-\log w+O(1)\qquad\text{para}\quad 2\le w\le z. \tag{2.9}$$

Cuando se verifica esto se dice que la criba es *lineal* o que tiene *dimensión* uno. Se puede probar que es posible relajar la hipótesis cambiando la igualdad por menor o igual. En ese caso se dice que uno es la *dimensión débil*.

Con todo esto ya se puede enunciar el resultado principal.

Teorema 2.4.1 (Jurkat-Richert) *Sea un problema de criba con dimensión (débil) uno tal que para D se cumple* (2.5)*. Entonces para $s=\log D/\log z>2$*

$$\big(f(s)+O(\Delta)\big)X\Pr(\mathcal{A},z)+O(E)\le S(A,z)\le\big(F(s)+O(\Delta)\big)X\Pr(\mathcal{A},z)+O(E)$$

donde $E=X/(\log X)^C$, $\Delta=(\log\log\log D)^3/\log\log D$ y $f(s)$ y $F(s)$ son las soluciones de (2.8)*.*

La segunda tarea pendiente es una explicación de la relación de este resultado con una criba combinatoria.

Supongamos que sabemos *a priori* que para $s\le 2$ sólo podemos obtener cotas inferiores triviales, entonces es una pérdida de términos de error aplicar la identidad de Buchstab con todos sus sumandos. Ya se mencionó que el s correspondiente a $S(\mathcal{A}_p,p)$ es $s_p=\log(D/p)\big/\log p$, así que de nada sirven los términos con $2\ge\log(D/p)\big/\log p$. Despreciarlos pasa la igualdad a una desigualdad

$$S(\mathcal{A},z)\le\#\mathcal{A}-\sum_{\substack{p<z\\ p^3<D}}S(\mathcal{A}_p,p).$$

En una segunda iteración de Buchstab no se pueden descartar términos sin perder la desigualdad, por tanto

$$S(\mathcal{A},z)\le\#\mathcal{A}-\sum_{\substack{p_1<z\\ p_1^3<D}}A_{p_1}+\sum_{\substack{p_2<p_1<z\\ p_1^3<D}}S(\mathcal{A}_{p_1p_2},p_2).$$

Pero en la tercera iteración sí se pueden eliminar los términos con $2\ge s_{p_1p_2p_3}$, donde $s_{p_1p_2p_3}=\log(D/p_1p_2p_3)\big/\log p_3$, y se tiene

$$S(\mathcal{A},z)\le\#\mathcal{A}-\sum_{\substack{p_1<z\\ p_1^3<D}}A_{p_1}+\sum_{\substack{p_2<p_1<z\\ p_1^3<D}}A_{p_1p_2}-\sum_{\substack{p_3<p_2<p_1<z\\ p_1^3<D,\ p_3^3p_2p_1<D}}S(\mathcal{A}_{p_1p_2p_3},p_3).$$

Razonamientos análogos dan lugar a cotas inferiores. Con ello se tiene una criba combinatoria determinada por

$$\begin{aligned}\mathcal{D}^+ &= \{p_1p_2\cdots p_m\ :\ p_m<p_{m-1}<\ldots<p_1\text{ y }p_{2r+1}^3p_{2r}\cdots p_2p_1<D\text{ para }2r+1\le m\}\\ \mathcal{D}^- &= \{p_1p_2\cdots p_m\ :\ p_m<p_{m-1}<\ldots<p_1\text{ y }p_{2r}^3p_{2r-1}\cdots p_2p_1<D\text{ para }2r\le m\}\end{aligned}$$

Ésta es la *criba de Rosser*.

Al ser una criba combinatoria, se pueden controlar los términos de error bajo la condición (2.5) y se obtienen cotas del tipo

$$X \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)\frac{g(d)}{d} + \texttt{error} \le S(A,z) \le X \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)\frac{g(d)}{d} + \texttt{error}.$$

Ahora se espera extraer de estos sumandos un factor $\Pr(\mathcal{A}, z)$ y acumular las cantidades sobrantes en las funciones f y F pero eso es un trabajo duro y el torrente de palabras que precede al teorema la excusa para evitarlo.

Para festejar el fin del capítulo, veamos algunos ejemplos (esencialmente tomados de [He]). Cuando queramos subrayarlos los denominaremos corolarios.

Ejemplo. Volviendo al ejemplo de prueba de las secciones anteriores, para $\mathcal{A} = [1, N]$ se puede tomar $X = N$, $g(d) = 1$ y $r_d = O(1)$. La condición (2.5) está asegurada eligiendo $D \ll X/(\log X)^C$ y (2.9) es la fórmula de Mertens. Por otro lado, $s > 2$ requiere que z no llegue a $N^{1/2}$ ¡justo el caso que se necesita para que $S(\mathcal{A}, z)$ sea como $\pi(z)$ con un error despreciable! Resignándonos a $z = N^{1/2-\epsilon}$ con ϵ pequeño, digamos $0 < \epsilon \le 1/6$, entonces $2 < s \le 3$ y según el teorema

$$\frac{2N}{\log N}\big(1 + o_\epsilon(1)\big)\log((1+2\epsilon)/(1-2\epsilon)) \le S(\mathcal{A}, N^{1/2-\epsilon}) \le \frac{2N}{\log N}\big(1 + o_\epsilon(1)\big)$$

donde se ha empleado que $\prod_{p<x}(1-1/p) \sim e^{-\gamma}/\log x$.

Ejemplo. Si se repite el ejemplo anterior pero ahora con $\mathcal{A} = [(N-1)^k, N^k]$ la diferencia es que $X = N^k - (N-1)^k = kN^{k-1} + O(N^{k-2})$ y $s > 2$ sugiere $z = N^{(k-1)/2-\epsilon}$ para lograr una cota inferior. Con ello se consigue $S(\mathcal{A}, N^{(k-1)/2-\epsilon}) > 0$ si N es suficientemente grande. Por otro lado, si $n \in \mathcal{A}$ tienen todos sus factores primos mayores que $N^{(k-1)/2-\epsilon}$, necesariamente tiene a lo más $k/((k-1)/2-\epsilon)$ de ellos (pues $n \le N^k$) y este número es menor que 3 si $k \ge 4$ y ϵ es pequeño. Los casos $k = 2$ y $k = 3$ son peores.

Corolario 2.4.2 *Entre dos cuadrados consecutivos (suficientemente grandes) siempre hay un número con a lo más cuatro factores primos y entre dos cubos consecutivos (suficientemente grandes) siempre hay un número con a lo más tres factores primos.*

Observación: Con los conocimientos actuales sobre diferencias de primos [Ba-Ha-Pi] la segunda parte de este corolario está muy anticuada pues se sabe que hay primos entre dos cubos (la primera también, pero sigue siendo un problema abierto saber si entre dos cuadrados hay siempre un primo).

Ejemplo. Sea $\mathcal{A} = \{n^2 + 1 \ : \ n \le N\}$. De la fórmula $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, se tiene

$$A_p = |\{n \le N \ : \ p|n^2+1\}| = \begin{cases} 2N/p + O(1) & \text{si } p \equiv 1 \ (4) \\ 0 & \text{si } p \equiv 3 \ (4) \\ N/2 + O(1) & \text{si } p = 2 \end{cases}$$

Por tanto la elección natural es $X = N$, $g(2) = 1$, $g(p) = 2$ si $p \equiv 1$ (4) y $g(p) = 0$ si $p \equiv 3$ (4). En general se tiene por el teorema chino de resto $A_d = g(d)N/d + O(2^{\nu(d)})$ para d libre de cuadrados. Así que con $D \ll X/\log^{C+1} X$ se tiene asegurado (2.5). Un punto más delicado es comprobar que (2.9) se cumple porque ahora a la suma sólo contribuyen la "mitad" de los primos (los de la forma $4k+1$) pero como para cada uno de ellos el valor de g es 2 una cosa compensa a la otra (??); la explicación rigurosa de que los primos de esta forma son la mitad requiere un caso particular del teorema de los números primos en progresiones aritméticas.

La condición $s > 2$ que se necesita para tener una cota inferior no trivial lleva a tomar como z aceptable $N^{1/2-\epsilon}$ con ϵ arbitrariamente pequeño. Es decir, por el teorema se cumple $S(\mathcal{A}, N^{1/2-\epsilon}) > 0$ para N grande. Teniendo en cuenta que el mayor elemento de $\mathcal{A}$ es $N^2 + 1$, esto implica

Corolario 2.4.3 *Hay infinitos números de la forma n^2+1 con a lo más cuatro factores primos.*

Por último un ejemplo doble de Selberg sin trabajar, a modo de comentario, que tiene gran interés teórico. Sean

$$\mathcal{A}^{\text{par}} = \{n \leq 2N \ : \ \lambda(n) = 1\} \qquad \text{y} \qquad \mathcal{A}^{\text{impar}} = \{n \leq 2N \ : \ \lambda(n) = -1\}$$

donde λ es la función de Liouville que vale 1 si el número de factores primos (contando multiplicidades) es par y -1 si es impar. Se cumple $A_d^{\text{par}} = \frac{1}{2}\sum_{n \leq 2X/d}(1 + \lambda(d)\lambda(n))$ y se conoce por métodos como los empleados en la demostración del teorema de los números primos que $\sum_{n \leq N} \lambda(n) = O(N/\log^C N)$ para cualquier $C > 0$, por tanto para $X = D = N$, y $g(d) = 1$ se cumplen las hipótesis (2.5) y (2.9). Lo mismo se aplica a $\mathcal{A}^{\text{impar}}$.

Por la peculiar estructura de $\mathcal{A}^{\text{par}}$ y $\mathcal{A}^{\text{impar}}$ es posible aplicar el proceso de iteraciones de identidades de Buchstab indicado anteriormente y concluir [He] que para cada $s > 1$

$$S(\mathcal{A}^{\text{par}}, z) = f(s)N\Pr(\mathcal{A}, z) + O(E) \quad \text{y} \quad S(\mathcal{A}^{\text{impar}}, z) = F(s)N\Pr(\mathcal{A}, z) + O(E)$$

con $E = N/(\log N)^2$. Esto es lo mejor que se podría obtener con el teorema (salvo términos de error). Es decir, el teorema de criba es óptimo en el sentido de que los términos principales no se pueden mejorar, ya que para $\mathcal{A}^{\text{par}}$ y $\mathcal{A}^{\text{impar}}$ se alcanzan.

Como aspecto negativo, nótese que los conjuntos $\mathcal{A}^{\text{par}}$ y $\mathcal{A}^{\text{impar}}$ son indistinguibles desde el punto de vista de la criba (ya que A_d^{par} y A_d^{impar} son similares), y sin embargo los comportamientos asintóticos de $S(\mathcal{A}^{\text{par}}, z)$ y $S(\mathcal{A}^{\text{impar}}, z)$ son diferentes. Esto limita la posibilidad de obtener ciertas fórmulas asintóticas con métodos de criba si no se introduce información adicional que no está en las hipótesis del teorema de Jurkat-Richert.

Bibliografía

[Ba-Ha-Pi] R.C. Baker, G. Harman, J. Pintz. The difference between consecutive primes. II. Proc. London Math. Soc. (3) 83 (2001), no. 3, 532–562.

[Bo] E. Bombieri. The asymptotic sieve. Rend. Accad. Naz. XL (5) 1/2 (1975/76), 243–269 (1977).

[Br] V. Brun. Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare. Archiv for Math. og Naturvid B34 (2001), no. 8.

[Ci-Co] J. Cilleruelo y A. Córdoba. La teoría de los números. Mondadori, Madrid, 1992.

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

[Ha-Wr] G.H. Hardy, E. Wright. An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

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

[Sh-Wr] D. Shanks; J.W. Wrench. Brun's constant. Math. Comp. 28 (1974), 293–299; corrigenda, ibid. 28 (1974), 1183.

[Se] A. Selberg. Collected papers. Vol. II. Springer-Verlag, Berlin, 1991.

Capítulo 3

Primos en progresiones aritméticas

3.1. Caracteres y funciones L

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

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

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

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

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

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

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

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

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

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

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

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

y la multiplicatividad nos asegura un producto de Euler

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

Por ejemplo, con los caracteres de la tabla anterior

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

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

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

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

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

Si χ recorre todos los caracteres módulo q

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

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

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

Corolario 3.1.2 *Si q y a son coprimos*

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

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

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

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

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

Sumando por partes se tiene la representación integral

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

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

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

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

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

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

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

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

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

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

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

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

Teniendo en cuenta (3.2),

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

y basta tomar $s\to 1^+$. □

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

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

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

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

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

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

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

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

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

Sustituyendo

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

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

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

para cualquier carácter real no principal. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2. Primos en progresión aritmética

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

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

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

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

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

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

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

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

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

Por otro lado, la fórmula

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

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

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

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

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

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

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

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

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

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

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

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

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

donde

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

que satisface

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

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

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

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

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

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

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

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

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

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

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

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

uniformemente en $q \le x$.

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

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

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

Lo que soñaríamos es:

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

De los dos últimos resultados resultados se deduce:

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

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

uniformemente en q.

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

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

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

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

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

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

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

Antes de entrar en la demostración de

Corolario 3.2.9 *Para cualquier carácter χ de módulo q*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3. El Teorema de Siegel

Enunciado y demostración. El teorema de Siegel-Walfisz

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

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

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

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

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

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

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

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

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

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

donde C es una constante positiva, absoluta y efectiva.

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

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

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

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

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

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

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

con

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.4. El Teorema de Bombieri-Vinogradov

Enunciado y significado. Algunas aplicaciones.

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 3.4.2 *Se cumple*

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

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

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

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

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

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

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

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

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

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

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

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

Demostración del Teorema 3.4.2: Es muy fácil comprobar

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

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

$$\begin{aligned} \frac{X}{\sum_{d<z} h(d)} &= C\frac{X}{(\log z)^\kappa} + O\Big(\frac{X}{(\log z)^{\kappa+1}}\Big) \\ &= \frac{\mathrm{Li}(2N)}{\log z} \prod_{p\nmid 2N} \big(1 - \frac{1}{p-1}\big)\big(1 - \frac{1}{p}\big)^{-1} \prod_{p|2N} \big(1 - \frac{1}{p}\big)^{-1} = \mathfrak{G}(N)\frac{\mathrm{Li}(2N)}{2\log z}. \end{aligned}$$

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

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

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

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

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

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

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

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

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

$$d|r_d| \ll N$$

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

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

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

Demostración del Teorema 3.4.3: Sean

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

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

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

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

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

Por el Lema 2.1.2

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

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

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

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

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

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

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

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

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

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

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

Bibliografía

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

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

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

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

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

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

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

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

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

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

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

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

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

Capítulo 4

El método del círculo

4.1. Arcos mayores y menores

En 1918 Hardy y Ramanujan [Ha-Ra] introdujeron una técnica analítica muy poderosa, denominada actualmente *método del círculo*, para tratar problemas aditivos. Su propósito inicial fue el estudio de las particiones pero Hardy y Littlewood desarrollaron la técnica en una serie artículos aplicándola a diversos problemas, por ello el método del círculo también es conocido como *método de Hardy y Littlewood*.

Para fijar ideas nos centraremos en el problema consistente en dar una aproximación asintótica del número de representaciones, $r_k(N)$, de un número grande N como suma de k elementos de un conjunto $\mathcal{B}$ de enteros no negativos. Es decir, se busca una fórmula asintótica para

$$r_k(N) = \#\{(b_1, b_2, \ldots, b_k) \in \mathcal{B}^k \ : \ N = b_1 + b_2 + \cdots + b_k\}.$$

Se comienza construyendo la función generatriz de $r_k(n)$

$$F(z) = \sum_{b \in \mathcal{B}} z^b \qquad \Rightarrow \qquad F^k(z) = \sum_{n=0}^{\infty} r_k(n) z^n.$$

El radio de convergencia de F es 1, por tanto la aplicación de la fórmula integral de Cauchy

$$r_k(N) = \frac{1}{2\pi i} \int_{C_r} F^k(z) \frac{dz}{z^{N+1}} \tag{4.1}$$

es correcta si C_r es la circunferencia $\{|z| = r\}$ con $0 < r < 1$.

A partir de (4.1), como es habitual en teoría analítica de números, se intenta obtener información a partir de las singularidades el problema es que la única singularidad encerrada por C_r es el polo $z = 0$ que no podemos aprovechar porque hallar su residuo es tanto como calcular $r_k(N)$ y volvemos al problema inicial. Por otra parte, típicamente no tiene sentido extender C_r más allá en busca de nuevas singularidades porque fuera del círculo $|z| < 1$ no hay función, en el lenguaje de la variable compleja se dice que la circunferencia unidad es la frontera natural [Ru].

A efectos de tener no sólo un círculo sino también un método, se elige r muy cercano a 1 buscando sentir la influencia de las "principales singularidades" de F en la circunferencia unidad. Por otra parte r debe estar suficientemente separado de 1 como para que no haya "interferencias" entre las influencias de diferentes singularidades. El tamaño de r está en realidad relacionado con el de N, siendo la elección natural (si $r_k(N)$ no crece desmesuradamente rápido) tomar $1-r$ comparable a $1/N$. En este caso r^n es muy pequeño justamente cuando n es mucho mayor que N, de modo que en la definición de $F(z)$ los términos con b mucho mayor que N son despreciables, lo que concuerda con el hecho de que $N = b_1 + b_2 + \cdots + b_k \Rightarrow b_i \leq N$. Es decir, como los $b \in \mathcal{B}$ grandes en comparación con N no afectan a la definición de $r_k(N)$, tampoco deben ser relevantes en el comportamiento asintótico de F.

Para cuantificar la influencia de las singularidades se divide la circunferencia C_r en los llamados *arcos mayores* y *arcos menores*. Los primeros serán aquellos arcos en los que se pueden dar buenas aproximaciones de F, gracias a la cercanía de grandes singularidades, mientras que en los segundos nos tendremos que contentar con una cota superior. Para que el método funcione, la contribución de los arcos mayores debe ser de orden superior que la de los arcos menores, con ello se conseguirá una fórmula asintótica para $r_k(N)$. Esto no implica que la medida de los arcos mayores sea más grande que la de sus hermanos menores, antes bien, en la mayoría de las aplicaciones la medida de los arcos mayores tiende a cero cuando $N \to \infty$ pero en ese conjunto esquelético está la mayor contribución.

Las potencias $\{z^n\}_{n=1}^{\infty}$ "resuenan" cuando $z = r\ e(a/b)$ siendo la resonancia más notoria cuanto menor sea b, por ello los arcos mayores están naturalmente centrados en puntos cuyo argumento es un múltiplo racional de 2π con denominador pequeño. El análisis de F cerca de puntos de este tipo lleva al estudio de la distribución de los elementos de $\mathcal{B}$ en progresiones aritméticas. Por ejemplo, si $\#\mathcal{B} \cap [0, N] \sim CN$ y todos los elementos de $\mathcal{B}$ son impares, sumando por partes se puede obtener $F(r) \sim -F(-r) \sim C(1-r)^{-1}$ cuando $r \to 1^-$, y si todos son de la forma $3n+1$, $F(re(1/3)) \sim Ce(1/3)(1-r)^{-1}$. Sin embargo si hubiera tantos pares como impares, por ejemplo si $2n \in \mathcal{B} \Rightarrow 2n+1 \in \mathcal{B}$, entonces $F(-r) = O(1)$ y en las cercanías de -1 no tendríamos un arco mayor. De esta forma, el método del círculo llega a funcionar en ocasiones como una forma analítica cuantitativa de un principio local-global que transforma resultados módulo q (locales) en resultados en $\mathbb{Z}$ (globales). La misma filosofía apareció al estudiar los métodos de criba, si se conocía la distribución de los elementos de un conjunto en progresiones aritméticas se podía decir algo de su distribución en $\mathbb{Z}$. El método del círculo aspira a resultados más poderosos: fórmulas asintóticas más que acotaciones, y por ello hay que disponer de una información de mayor entidad.

En algunas de las primeras aplicaciones del método del círculo, F tenía propiedades muy específicas que no heredaban sus sumas parciales (propiedades de autoemejanza dadas por relaciones modulares). Sin embargo, en general, trabajar con series infinitas puede conllevar algunas incomodidades técnicas que se evitan con una formulación ligeramente distinta del método del círculo, cronológicamente posterior. Está basada en la sencilla observación, antes comentada, de que $N = b_1 + b_2 + \cdots + b_k \Rightarrow b_i \leq N$. Por

tanto en (4.1), se puede reemplazar F por F_N, la suma parcial de la serie que define F correspondiente a los $b \leq N$. Como F_N es un polinomio, no hay problemas para escoger $r = 1$, lo que con el cambio $z = e(x)$ transforma (4.1) en la sencilla igualdad:

$$r_k(N) = \int_I S^k(x)\, e(-Nx)\, dx \qquad \text{con} \quad S(x) = \sum_{b \in \mathcal{B}_N} e(bx) \tag{4.2}$$

donde I es cualquier intervalo de longitud uno, digamos por ejemplo $I = [-1/2, 1/2]$, y $\mathcal{B}_N = \mathcal{B} \cap [0, N]$. Los arcos mayores serán ahora subintervalos de $[-1/2, 1/2]$ en los que tengamos una buena aproximación para $S(x)$ que se traduzca en otra para la integral correspondiente sobre ellos; mientras que en el resto, los arcos menores, confiamos en que acotaciones de la suma trigonométrica $S(x)$ sean suficientes para acumular su contribución en un témino de error. Por el análisis anterior, los arcos mayores serán intervalos alrededor de ciertos racionales con denominador pequeño.

Sólo para ilustrar un poco la estructura del método, supongamos que nos empeñamos en aproximar con el método del círculo

$$r_k(N) = \#\{(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k \ : \ N = n_1 + n_2 + \cdots + n_k\}$$

para $k \geq 2$. Esto es un objetivo ridículo porque es fácil probar directamente la fórmula

$$r_k(N) = \left(\begin{array}{c} N-1 \\ k-1 \end{array} \right)$$

Si no nos arredramos, en las formulaciones (4.1) y (4.2) se ha de escoger respectivamente

$$F(z) = z + z^2 + z^3 + \cdots = \frac{z}{1-z} \qquad \text{y} \qquad S(x) = \sum_{n=1}^{N} e(nx) = \frac{e(Nx) - 1}{1 - e(-x)}.$$

En el arco del círculo de radio $r = 1 - 1/N$ y argumento $|\arg(z)| \ll 1/N$, la función F es como N y se hace pequeña cuando nos alejamos de este arco. De la misma forma, la suma $S(x)$ es como N si $|x| \ll 1/N$ y es pequeña cuando estamos lejos de este intervalo (siempre dentro de $[-1/2, 1/2]$). En ambos casos hay un "arco mayor" asociado a $0/1$ (a través del argumento en el primer caso y a través del propio valor de la variable en el segundo) de donde proviene la parte del león de $r_k(N)$, y tanto (4.1) como (4.2) hacen sospechar $r_k(N) \sim CN^{k-1}$. Concretando matemáticamente las imprecisiones semánticas disfrazadas en "es como" y "lejos" se puede llegar a la fórmula asintótica (cf. [Cr] §2)

$$r_k(N) \sim \frac{N^{k-1}}{(k-1)!}$$

que está de acuerdo con la expresión exacta.

4.2. Las conjeturas de Goldbach

Nuestro objetivo, por supuesto no son las tonterías recién comentadas, sino enfrentarnos a los grandes problemas aditivos. Uno de los más conocidos es la llamada *Conjetura*

de Goldbach que debe su nombre a que esencialmente fue planteada por C. Goldbach en una carta a Euler:

Conjetura de Goldbach: *Todo número par mayor que* 2 *se puede escribir como suma de dos primos.*

Aunque ésta sea la conjetura de Goldbach por antonomasia, al mismo autor se debe otra conjetura más débil pero de enunciado igualmente simple[1].

Conjetura de Goldbach ternaria: *Todo número impar mayor que* 5 *se puede escribir como suma de tres primos.*

Los apelativos de "conjetura" ya nos hace sospechar que por mucho que el lector escudriñe en la literatura no encontrará el gran teorema que las pruebe. Lo cierto es que el método del círculo tiene algo que decir y produce algunos resultados parciales de interés, en particular la forma ternaria de la conjetura de Goldbach está resuelta salvo un número finitio de casos (inalcanzables por cualquier ordenador imaginable).

Para empezar veamos rápidamente cómo el método del círculo nos puede dar con poco esfuerzo una gran intuición incluso cuando no funciona.

Al aplicarlo a la conjetura de Goldbach, con la formulación de (4.2), se tiene

$$r_2(N) = \int_0^1 (S(x))^2 e(-Nx)\, dx \qquad \text{con} \qquad S(x) = \sum_{p\le N} e(px).$$

La "densidad" de los primos hasta N es $\pi(N)/N \sim 1/\log N$, con lo cual muy cerca de $x = 0$ se debería cumplir algo así como (??)

$$S(x) \sim \frac{D(x)}{\log N} \qquad \text{con} \qquad D(x) = \sum_{n\le N} e(nx).$$

Por otro lado, muy cerca por ejemplo de $x = 1/2$, la aproximación debe ser

$$S(x) \sim -\frac{D(x-1/2)}{\log N}$$

simplemente porque todos los primos, excepto $p = 2$, son impares y por tanto $e(px) = -e(p(x-1/2))$. Si $x = 1/3$, debemos considerar el hecho de que $e(p/3)$ es $e(1/3)$ ó $e(2/3)$ dependiendo de si $p \equiv 1\ (3)$ o $p \equiv 2\ (3)$. Como la "mitad" de los primos es de cada uno de estos dos tipos,

$$S(x) \sim \left(\frac{e(1/3)}{2\log N} + \frac{e(2/3)}{2\log N}\right) D(x-1/3) = -\frac{D(x-1/3)}{2\log N}.$$

[1]En realidad en ambos casos las conjeturas están ligeramente reformuladas con respecto al original porque en tiempos de Goldbach y Euler se consideraba que 1 era primo.

En general, el teorema de los números primos en progresiones aritméticas asegura que los primos están equidistribuidos en cada una de las $\phi(q)$ progresiones aritméticas módulo q que contienen infinitos primos y según el Lema 4.2.5 que probaremos más adelante, $\sum_{(n,q)=1} e(n/q) = \mu(q)$; por todo esto se espera (y de hecho se prueba) que muy cerca de la fracción irreducible $x = a/q$ se cumple

$$S(x) = \frac{\mu(q)}{q \log N} D(x - a/q) + \text{ términos de error.}$$

Como veremos, la prueba de verdad consiste nada más en sumar por partes empleando el teorema de los números primos en progresiones aritméticas (véase la Proposición 4.2.4). Los pocos conocimientos que se tienen en la dirección de la hipótesis de Riemann generalizada se reflejan en que realmente el término de error no se *come* al principal sólo cuando q es muy pequeño (como un logaritmo de N) y x está realmente muy cerca de a/q.

La función $D(x)$ es pequeña si x no está próxima a un entero, lo que sugiere que no se pierde mucho aproximando $\int_{|x|<\epsilon} (D(x))^2 e(-Nx)\ dx$ por $\int_0^1 (D(x))^2 e(-Nx)\ dx$. Teniendo esto en cuenta, la parte principal de la contribución de los arcos mayores es

$$\sum_{(a,q)=1} \frac{\mu(q)}{q^2 (\log N)^2} e(-Na/q) \int_0^1 (D(x))^2 e(-Nx)\ dx \sim \sum_q \frac{\mu(q)}{q^2 (\log N)^2} c_q(-N) N$$

donde $c_q(-N)$ es como se indica en el Lema 4.2.5 y usando la evaluación allí indicada, no es difícil escribir esta suma de funciones multiplicativas como el producto

$$\frac{N}{(\log N)^2} \prod_{p \not| N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|N} \left(1 + \frac{1}{p-1}\right).$$

Si podemos justificar todos los argumentos anteriores y que la contribución de los arcos mayores es dominante haciendo honor a su nombre, entonces habremos probado la conjetura de Goldbach, porque para N par el producto anterior no se anula. Demasiado bueno para ser cierto...

El fallo no está en los pasos anteriores, que son incondicionalmente ciertos, sino en la imposibilidad de probar que la contribución de los arcos menores es pequeña. Además esta imposibilidad es teórica, es más una limitación del método que un reflejo de nuestra ignorancia sobre el conjunto de primos. Una explicación poco precisa de esta afirmación pasa por notar que si $x \notin \mathbb{Q}$, las oscilaciones $e(px)$ no tienen ninguna razón por la deban resonar, es lógico pensar que no difieren mucho de variables aleatorias independientes aunque realmente no lo son). Por el teorema central del límite entonces la parte real e imaginaria de $S(x)/\pi(x)$ cuando N crece se deberían comportan como una distribución normal lo que hace sospechar que no se puede mejorar la acotación $S(x) \ll N^{1/2+\epsilon}$ y como los arcos menores tienen casi toda la medida (hay "pocos" números cerca de los racionales) la integral de $|S(x)|^2$ sobre los arcos menores ya supera al término principal. ¿No significa eso que es imposible que la contribución heurística de los arcos mayores que hemos hallado antes sea correcta? De ningún modo, porque al estimar la contribución de

los arcos menores mediante una cota superior estamos perdiendo el signo, es plausible que al integrar $S^2(x)e(-Nx)$ y sumar en los arcos menores haya mucha cancelación.

Este razonamiento también se aplica en general al aproximar $r_2(N)$ cuando, hablando sin rigor, $\mathcal{B}$ tiene densidad positiva en $\mathbb{N}$ o si la densidad decae menos que $N^{-\epsilon}$ para cualquier $\epsilon > 0$. Esta idea se puede resumir en la frase: *El método del círculo no se aplica a problemas binarios.* Lo cual deja fuera del alcance del método del círculo la Conjetura de Goldbach y otros problemas como el número de representaciones $N = x_1^{2k} + \cdots + x_{4k}^{2k}$ con $x_j \in \mathbb{Z}$, $k < 2$, ya que $\mathcal{B} = \{x_1^{2k} + \cdots + x_{2k}^{2k}\}$ tiene en cierto sentido densidad positiva en $\mathbb{N}$ porque, si nos olvidamos de las multiplicidades, cualquier elección de $|x_j| \leq N^{1/2k}/2k$, $1 \leq j \leq 2k$, da lugar a un elemento de de $\#\mathcal{B}_N$ y hay $c_k N$ posibles elecciones .

Reparar esta limitación del método del círculo requiere no estimar arcos menores individualmente, sino estudiar la cancelación que puede haber entre varios de ello. En un importante trabajo [Kl] H.D. Kloosterman consiguió este objetivo para formas cuadráticas diagonales cuaternarias (de cuatro variables).

Después de esta disgresión y este desengaño vamos a demostrar que para más de dos sumandos no hay problema bajo una condición de paridad obvia: si por ejemplo escribimos N como suma de tres primos, típicamente N es impar porque si N es par uno de los sumandos es necesariamente el 2 y en realidad estamos representando $N-2$ como suma de dos primos. En general, si $N-k$ es impar, $r_k(N)$ se relaciona con $r_{k-1}(N-2)$ y por tanto las representaciones "genuinas" de N como suma de k primos requieren que N y k tengan la misma paridad.

Teorema 4.2.1 *Dado un entero $k > 2$, para $N \equiv k \pmod 2$ se verifica la fórmula asintótica*

$$r_k(N) \sim \frac{\mathfrak{G}_k(N) N^{k-1}}{(k-1)!(\log N)^k} \qquad con \quad \mathfrak{G}_k(N) = \prod_{p \not| N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right) \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right).$$

Corolario 4.2.2 (Teorema de Vinogradov) *Cualquier número impar suficientemente grande se puede expresar como suma de tres primos.*

Según las consideraciones anteriores la conjetura de Goldbach es inalcanzable con el método del círculo porque nos falta al menos un sumando. Podemos crearlo artificialmente promediando, y si un promedio da lo que tiene que dar y la dispersión es poca, entonces es que casi todos los términos son los que tienen que ser. Sin divagar, de un resultado en media deduciremos:

Teorema 4.2.3 *Casi todo número par es suma de dos primos, esto es,*

$$\#\{2n \leq N \ : \ r_2(2n) = 0\} = o(N).$$

Observación: Se conocen resultados más precisos que aseguran que incluso en intervalos "cortos" casi todo número par es suma de dos primos [Mo-Va] (véase también [Pe]).

Para la prueba de estos resultados utilizaremos consideraremos en lugar de $r_k(N)$ y $S(x)$ las cantidades

$$r_k^*(N) = \sum_{p_1+p_2+\cdots+p_k=N} (\log p_1)(\log p_2)\cdots(\log p_k) \qquad \text{y} \qquad S^*(x) = \sum_{p\le N} e(px)\log p.$$

La razón es la misma por la que nos decidimos por $\psi(x)$ en lugar de $\pi(x)$: las fórmulas son más sencillas y se puede pasar de una cantidad a la otra sumando por partes. Con estas definiciones (4.2) tiene su análogo en

$$r_k^*(N) = \int_{-1/2}^{1/2} \big(S^*(x)\big)^k e(-Nx)\,dx. \tag{4.3}$$

Pretendemos aproximar en los arcos mayores $S^*(x)$ por $S^*(a/q+\delta)$ con δ pequeño y dividir la sumación en sucesiones módulo q para aproximar mediante el Teorema de Siegel-Walfisz después de extraer el factor $e(n\delta)$ sumando por partes. Recuérdese que los primos en progresiones aritméticas sólo quedan controlados asintóticamente con el Teorema de Siegel-Walfisz cuando q es a lo más una potencia de logaritmo ya que el término de error sólo gana a la estimación trivial una cantidad de este orden. Esto nos sugiere exigir $q < (\log N)^B$ y $N|\delta| < (\log N)^B$. En definitiva, los arcos mayores serán

$$\mathfrak{M}_{a/q} = \{x \,:\, \|x - a/q\| < (\log N)^B/N\} \cap [-1/2, 1/2]$$

con $\|\cdot\|$ la distancia al entero más cercano y $q < (\log N)^B$, $(a,q) = 1$, $1 \le a \le q$.

Denotaremos por $\mathfrak{M}$ la unión de todos ellos. Nótese que la medida de $\mathfrak{M}$ tiende a cero, aun así esperamos que la mayor contribución a la integral de (4.3) esté allí.

Nuestro proyectos en los arcos mayores se materializa en el siguiente resultado:

Proposición 4.2.4 *Si $x \in \mathfrak{M}_{a/q}$, entonces*

$$S^*(x) = \frac{\mu(q)}{\phi(q)} \sum_{n\le N} e((x-a/q)n) + O\bigg(\frac{N}{(\log N)^{2B}}\bigg).$$

Antes de dar la prueba nos detendremos en el resultadillo al que nos habíamos referido en la exposición informal.

Lema 4.2.5 *Sea la* suma de Ramanujan

$$c_q(N) = \sum_{\substack{n=1\\(n,q)=1}}^{q} e\big(N\frac{n}{q}\big).$$

Si $N/q = N'/q'$ con N' y q' coprimos entonces $c_q(N) = \mu(q')\phi(q)/\phi(q')$.

Demostración: Es fácil ver, usando el teorema chino del resto, que $c_{q_1q_2}(N) = c_{q_1}(N) \cdot c_{q_2}(N)$, esto es, que $c_q(N)$ es multiplicativa en q, por ello basta considerar el caso $q = p^r$ con p primo.

Si $r = 1$ y $p \not| N$ entonces $c_q(N)$ es la suma de las raíces q-ésimas de la unidad excepto la raíz 1, por tanto $c_q(N) = 0 - 1 = \mu(q)$. Si $r > 1$ y $p \not| N$

$$c_q(N) = \sum_{n=1}^{q} e(Nn/q) - \sum_{m=1}^{q/p} e(pNm/q)$$

y ambas sumas son nulas por ser sumas de todas las raíces de la unidad.

Si $p|N$ y $N/q = N'/q'$ con $p \not| N'$,

$$c_q(N) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(Nn/q) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(N'n/q') = \frac{\phi(q)}{\phi(q')} \sum_{\substack{n=1 \\ (n,q')=1}}^{q'} e(N'n/q').$$

La última igualdad se sigue porque $f(n) = e(N'n/q')$ tiene periodo q' y por tanto podemos agrupar los $\phi(q)$ sumandos del sumatorio anterior de $\phi(q')$ en $\phi(q')$ términos. □

Demostración de la Proposición 4.2.4: No es difícil probar (ejercicio) que la contribución a $S^*(x)$ de los sumandos con $(n, q) \neq 1$ es pequeña y que tampoco perdemos mucho más que una raíz cuadrada al añadir a mano las potencias de los primos:

$$S^*(x) = \sum_{\substack{n \leq N \\ (n,q)=1}} \Lambda(n)e(nx) + O(N^{1/2}).$$

Escribamos, para abreviar, $\delta = x - a/q$. Factorizando $e(nx) = e(an/q)e(n\delta)$ y empleando la ortogonalidad de los caracteres, se sigue

$$S^*(x) = \frac{1}{\phi(q)} \sum_{r=1}^{q} \sum_{\chi} \overline{\chi}(r) \sum_{n \leq N} \chi(n)\Lambda(n)e(ar/q)e(n\delta) + O(N^{1/2}),$$

y agrupando términos

$$S^*(x) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\overline{\chi}, a)\psi_\delta(N, \chi) + O(N^{1/2}) \tag{4.4}$$

donde

$$\tau(\overline{\chi}, a) = \sum_{r=1}^{q} \overline{\chi}(r)e(ar/q) \qquad \text{y} \qquad \psi_\delta(N, \chi) = \sum_{n \leq N} \chi(n)\Lambda(n)e(n\delta).$$

Sumando por partes y por el Teorema de Siegel-Walfisz (empléese mejor para $\psi(x, \chi)$, en vez de para $\pi(x; q, a)$, con $A = 4B$), si $\chi \neq \chi_0$

$$\psi_\delta(N, \chi) = e(N\delta)\psi(N, \chi) - 2\pi i\delta \int_1^N e(\delta t)\psi(t, \chi)\, dt \ll (1 + |\delta|N)\frac{N}{(\log N)^{4B}}.$$

Además aplicando las propiedades de ortogonalidad, se tiene que

$$\sum_{\chi} |\tau(\overline{\chi}, a)|^2 = \sum_{r,s=1}^{q} \sum_{\chi} \overline{\chi}(r)\chi(s)e(a(r-s)/q) \leq q\phi(q).$$

Así pues, por la desigualdad de Cauchy-Schwarz, la contribución a (4.4) de $\chi \neq \chi_0$ es $O\big((1+|\delta|N)q^{1/2}N(\log N)^{-4B}\big)$. Mientras que si $\chi = \chi_0$,

$$\psi_\delta(N, \chi_0) = \sum_{n\leq N} e(n\delta) + \sum_{n\leq N} (\Lambda(n) - 1)e(n\delta),$$

y procediendo como antes, el segundo sumatorio es $O(N(\log N)^{-4B})$. Como $\tau(\overline{\chi_0}, a)$ coincide con la suma de Ramanujan $c_q(a) = \mu(q)$ (según el Lema 4.2.5), se deduce finalmente de (4.4)

$$S^*(x) = \frac{\mu(q)}{\phi(q)} \sum_{n\leq N} e(n\delta) + O\bigg((1+|\delta|N)q^{1/2}\frac{N}{(\log N)^{4B}}\bigg).$$

Sustituyendo $\delta = x - a/q$ y recordando los rangos de δ y q (de la definición de los arcos mayores), se llega al resultado deseado. □

Los arcos menores son los que conforman el complementario de la unión de los mayores, es decir, la unión de los arcos menores es:

$$\mathfrak{m} = [-1/2, 1/2] - \mathfrak{M}.$$

La contribución cuando integramos sobre $\mathfrak{m}$ en (4.3) queremos que sea despreciable pero eso no significa en absoluto que sea sencillo acotar $S^*(x)$ en $\mathfrak{m}$ y sobre su dificultad reposa toda la enjundia del teorema. I.M. Vinogradov utilizó originalmente unos argumentos basados en la idea de que una suma sobre primos se puede escribir como una suma de sumas sobre enteros (mediante un proceso de criba), y de que hay razones analíticas para que todas sean grandes (cf. [El]). Cuarenta años después, R.C. Vaughan encontró una curiosa identidad que simplificaba mucho los argumentos y su atajo es el que emplearemos aquí.

Proposición 4.2.6 *Se cumple la acotación*

$$\max_{x\in\mathfrak{m}} |S^*(x)| \ll \frac{N}{(\log N)^{B/2-4}}.$$

Demostración: La *identidad de Vaughan* afirma que dados $N_1, N_2 \in \mathbb{N}$ con $N_1N_2 \leq N$, para cualquier función g

$$\sum_{n\leq N} \Lambda(n)g(n) = S_1 + S_2 + S_3 + S_4$$

donde

$$S_1 = \sum_{n\le N_1} \Lambda(n)g(n), \qquad S_2 = -\sum_{n\le N_1N_2} \Big(\sum_{\substack{l\le N_1,\ m\le N_2\\ lm=n}} \mu(m)\Lambda(l)\Big) \sum_{k\le N/n} g(nk),$$

$$S_3 = \sum_{n\le N_2} \mu(n) \sum_{k\le N/n} g(nk)\log k, \quad S_4 = \sum_{N_1<n<N/N_2} \Lambda(n) \sum_{N_2<j\le N/n} \Big(\sum_{l|j,\ l\le N_2} \mu(l)\Big) g(nj).$$

La prueba consiste simplemente en partir de la siguiente trivialidad

$$-\frac{\zeta'(s)}{\zeta(s)} = F(s) - \zeta(s)F(s)G(s) - \zeta'(s)G(s) + \big(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\big)(1-\zeta(s)G(s))$$

con $F(s) = \sum_{n\le N_1} \Lambda(n)n^{-s}$ y $G(s) = \sum_{n\le N_2} \mu(n)n^{-s}$. Comparando los coeficientes de n^{-s} en cada miembro y multiplicándolos por $g(n)$ y sumando, se obtiene la identidad deseada.

En el caso $g(n) = e(f(n))$ si $1 \le n \le N$ y cero en otro caso, vamos a deducir

$$\begin{aligned}(4.5)\qquad \sum_{n\le N} \Lambda(n)e(f(n)) \ll N_1 + \log N \sum_{n\le N_1N_2} \Big| \sum_{k\le N/n} g(nk)\Big| \\ + N^{1/2}(\log N)^3 \max_{N_1<I\le N/N_2} \max_{N_2\le j\le N/I} \sum_{N_2<k\le N/I} \Big| \sum_{I<n\le 2I} g(nj)\,\overline{g}(nk)\Big|.\end{aligned}$$

Para ello, estimando trivialmente S_1 se obtiene el primer término del segundo miembro, N_1. Usando que $|\mu(m)| \le 1$ y que $\sum_{l|n} \Lambda(l) = \log n$, de S_2 se obtiene el segundo término, y S_3 se acota de la misma forma. Antes de tratar S_4, se divide en intervalos diádicos el rango de n, esto es, se considera $I < n \le 2I$ con I una potencia de dos, $N_1 < I < N/N_2$. Entonces

$$|S_4| \le \max_{N_1<I\le N/N_2} \Big| \sum_{I<n\le 2I} \sum_{N_2<j\le N/n} \Lambda(n)a_j g(nj)\Big|$$

con $|a_j| \le d(j)$ el número de divisores de j. Tras las acotaciones elementales (!?) $\sum_{i\le x} \Lambda^2(i) \ll x\log x$ y $\sum_{j\le x} d^2(j) \ll x(\log x)^3$, se concluye la prueba de (4.5).

Eligiendo $N_1 = N_2 = N^{2/5}$ y $f(n) = nx$, se tiene

$$(4.6)\qquad S^*(x) \ll N^{1/2} + M_1\log N + M_2^{1/2}N^{1/2}(\log N)^3$$

donde M_1 y M_2 son, respectivamente, los máximos valores posibles de las sumas

$$\sum_{n\le N^{4/5}} \Big| \sum_{k\le N/n} e(nkx)\Big| \qquad \text{y} \qquad \sum_{N^{2/5}<k\le N/I} \Big| \sum_{I<n\le 2I} e(n(j-k)x)\Big|$$

con $N^{2/5} < I \le N^{3/5}$ y $N^{2/5} \le j \le N/I$. Operando las sumas geométricas interiores, se deduce

$$M_1 \ll \sum_{n\le N^{4/5}} \min(N/n, |\operatorname{sen}(2\pi nx)|^{-1}),\ M_2 \ll N^{3/5} + \sum_{k'\le N^{3/5}} \min(N/k', |\operatorname{sen}(2\pi k'x)|^{-1})$$

donde se ha escrito $k' = |j-k|$, separando el caso $k' = 0$, y se ha empleado $I \le N/k'$.

Dado $x \in \mathfrak{m}$ sea a/q la fracción irreducible con $1 \le q \le N/(\log N)^B$ más cercana a x, entonces $q \ge (\log N)^B$ porque en otro caso $x \in \mathfrak{M}$, así pues $x = a/q + \delta$ con $qN|\delta| \le (\log N)^B$ y $(\log N)^B \le q \le N/(\log N)^B$. Por tanto para $n \le N^{4/5}$ se tiene $|nx - na/q| = n|\delta| = o(1/q)$, de manera que $\operatorname{sen}(2\pi nx)$ y $\operatorname{sen}(2\pi na/q)$ son comparables (su cociente está acotado) siempre que $2n/q \notin \mathbb{Z}$. Bajo esta hipótesis, según varía n, $|\operatorname{sen}(2\pi na/q)|^{-1}$ tomará $O(1 + N^{4/5}/q)$ veces periódicamente valores acotados por $q/1$, $q/2$, $q/3$,... q/q (ya que $|\operatorname{sen} t|^{-1} \ll |t|^{-1}$ en $[-\pi/2, \pi/2]$). La contribución a M_1 de los términos con $2n/q \in \mathbb{Z}$ es claramente $Nq^{-1}\log N$, con lo cual

$$M_1 \ll Nq^{-1}\log N + (1 + N^{4/5}q^{-1})(q/1 + q/2 + \cdots + q/q) \ll N/(\log N)^{B-1}.$$

Este razonamiento evidentemente también se aplica a M_2 obteniéndose la misma cota. Sustituyendo en (4.6), el teorema queda probado. □

Combinando los resultados anteriores se tiene el análogo del Teorema 4.2.1 pero con asteriscos.

Teorema 4.2.7 *Dado $A > 0$ y un entero $k > 2$, se cumple*

$$r_k^*(N) = \mathfrak{G}_k(N)\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^A}\right).$$

Además $\mathfrak{G}_k(N)$ permanece entre dos constantes absolutas positivas si N y k tienen la misma paridad (y $\mathfrak{G}_k(N) = 0$ si no la tienen).

Demostración: Veamos la contribución de cada uno de los $\mathfrak{M}_{a/q}$ pertenecientes a los arcos mayores. Según la Proposición 4.2.4

$$\int_{\mathfrak{M}_{a/q}} (S^*(x))^k e(-Nx)\,dx = \int_{\mathfrak{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)}\sum_{n\le N} e((x-a/q)n)\right)^k e(-Nx)\,dx + O\left(\frac{N^{k-1}}{(\log N)^{2B}}\right).$$

Como $\sum e(nt) \ll |t|^{-1}$ en $[-1/2, 1/2]$, se puede completar la segunda integral a este intervalo perdiendo $O\big(((\log N)^B/N)^{-k+1}\big)$ que es absorbido por el término de error.

Como se mencionó en la primera sección, un sencillo argumento combinatorio para contar el número de representaciones de un número natural como suma de otros, prueba

$$\begin{aligned}\int_{-1/2}^{1/2}\left(\sum_{n\le N} e((x-a/q)n)\right)^k e(-Nx)\,dx &= e(-Na/q)\int_{-1/2}^{1/2}\left(\sum_{n\le N} e(nt)\right)^k e(-Nt)\,dt \\ &= e(-Na/q)\binom{N-1}{k-1} = e(-Na/q)\frac{N^{k-1}}{(k-1)!} + O(N^{k-2}).\end{aligned}$$

Así pues, sumando la contribución de todos los $\mathfrak{M}_{a/q}$, se tiene (es fácil ver que son disjuntos, ejercicio)

$$\int_{\mathfrak{M}} (S^*(x))^k e(-Nx)\,dx = \sum_{q<(\log N)^B}\left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N)\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^B}\right).$$

Notando que $\phi(q) \gg q/\log q$ (de hecho se tiene algo mejor, Th. 328 [Ha-Wr]), se puede completar la sumación hasta infinito con un término de error despreciable, y empleando que $g(q) = c_q(-N)\big(\mu(q)/\phi(q)\big)^k$ es una función multiplicativa,

$$\int_{\mathfrak{M}} (S^*(x))^k e(-Nx)\, dx = \mathfrak{G}_k(N)\frac{N^{k-1}}{(k-1)!} + O\bigg(\frac{N^k}{(\log N)^B}\bigg).$$

ya que $\prod_p(1+g(p)) = \mathfrak{G}_k(N)$.

Por otra parte, por la Proposición 4.2.6 se tiene

$$\int_{\mathfrak{m}} (S(x))^k e(-Nx)\, dx \ll \bigg(\frac{N}{(\log N)^{B/2-4}}\bigg)^{k-2} \int_{-1/2}^{1/2} |S^*(x)|^2 dx.$$

Por la identidad de Parseval, la última integral es

$$\sum_{p\le N} (\log p)^2 \le \log N \sum_{n\le N} \Lambda(n) \ll N \log N.$$

Combinando la contribución de los arcos mayores y menores, y eligiendo adecuadamente B, se deduce la fórmula del enunciado.

Si N y k tienen la misma paridad, entonces todos los factores de $\mathfrak{G}_k(N)$ son estrictamente positivos y demostrar que $\mathfrak{G}_k(N)$ está entre dos constantes absolutas positivas equivale a ver que su logaritmo está uniformemente acotado, lo cual es muy sencillo. Evidentemente el factor correspondiente a $p = 2$ se anula si la paridad es distinta. □

Demostración del Teorema 4.2.1: Evidentemente $r_k(N)(\log N)^k$ mayora a $r_k^*(N)$. Por otro lado, la contribución de los sumandos en la definición de $r_k^*(N)$ con algún $p_i \le N^{1-\epsilon}$, $0 < \epsilon < 1$, es $O(N^{(k-2)+1-\epsilon}(\log N)^k)$, de forma que

$$r_k^*(N) \ge (1-\epsilon)^k (\log N)^k \sum_{\substack{p_1+p_2+\cdots+p_k=N \\ p_1,p_2,\ldots,p_k \ge N^{1-\epsilon}}} 1 + O(N^{k-1-\epsilon}(\log N)^k).$$

De la misma forma, podemos añadir los términos con $p_i \le N^{1-\epsilon}$ al último sumatorio con una pérdida comparable al término de error.

Combinando estas acotaciones,

$$(1-\epsilon)^k r_k(N)(\log N)^k + O(N^{k-1-\epsilon}(\log N)^k) \le r_k^*(N) \le r_k(N)(\log N)^k.$$

Diviendo entre $\mathfrak{G}_k(N)N^{k-1}/(k-1)!$ y aplicando el teorema anterior, se deduce que los límites superior e inferior de $(k-1)!r_k(N)(\log N)^k/(\mathfrak{G}_k(N)N^{k-1})$ están acotados entre 1 y $(1-\epsilon)^{-k}$, y basta tomar $\epsilon \to 0$. □

Demostración del Teorema 4.2.3: Nuestro objetivo es acotar

$$T(N) = \sum_{n\le N/2} \big|r_2^*(2n) - 2n\mathfrak{G}_2(2n)\big|^2$$

Empleando la Proposición 4.2.4 se tiene como en la prueba del Teorema 4.2.7

$$\int_{\mathfrak{M}} (S^*(x))^2 e(-2nx)\, dx = 2n \sum_{q<(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) + O\Big(\frac{N}{(\log N)^B}\Big).$$

A partir de (4.3) y de la descomposición en arcos mayores y menores $[-1/2, 1/2] = \mathfrak{M} \cup \mathfrak{m}$, se deduce

$$T(N) \le T_1 + T_2 + O\Big(\frac{N}{(\log N)^B}\Big)$$

con

$$\begin{aligned} T_1 &= 4 \sum_{n\le N/2} n^2 \Big| \mathfrak{G}_2(2n) - \sum_{q<(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) \Big|^2, \\ T_2 &= \sum_{n\le N/2} \Big| \int_{\mathfrak{m}} (S^*(x))^2 e(-2nx)\, dx \Big|^2. \end{aligned}$$

No es difícil probar ([Ha-Wr] Th. 324,329) que $\sum_{n\succeq N} (\phi(n))^{-2} \ll N^{-1}$ (también se podría aplicar el Teorema de Wirsing) y usando el Lema 4.2.5

$$\begin{aligned} \sum_{q\ge(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) &= \sum_{d|2n} \frac{\mu(d)}{\phi(d)} \sum_{\substack{q\ge(\log N)^B/d \\ (q,2n)=1}} \left(\frac{\mu(q)}{\phi(q)}\right)^2 \\ &\ll \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \operatorname{mín}\big(\frac{d}{(\log N)^B}, 1\big). \end{aligned}$$

Empleado $\phi(d) \gg d/\log d$ se tiene también la desigualdad más débil:

$$\sum_{q\ge(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) \ll \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \ll (\log n)^2.$$

Multiplicando ambas desigualdades se tiene

$$T_1 \ll N^2 (\log N)^2 \sum_{n\le N/2} \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \operatorname{mín}\big(\frac{d}{(\log N)^B}, 1\big).$$

Intercambiando el orden de sumación (y usando $\sum_{n\succeq N} (\phi(n))^{-1} \ll 1$) se deduce

$$T_1 = O(N^3 (\log N)^{3-B}).$$

Por otra parte la identidad de Parseval aplicada a $(S^*(x))^2$ multiplicada por la función característica de $\mathfrak{m}$ implica

$$T_2 \le \int_{\mathfrak{m}} |S^*(x)|^4\, dx$$

y procediendo como en la prueba del Teorema 4.2.7,

$$T_2 \ll \min_{x\in\mathfrak{m}} |S^*(x)|^2 \int_{-1/2}^{1/2} |S^*(x)|^2\, dx \ll \frac{N^2}{(\log N)^{B-8}} \cdot N \log N.$$

Con ello hemos demostrado que para cualquier $A > 0$

$$T(N) = O\big(N^3 (\log N)^{-A}\big).$$

Si en un intervalo $[N/2, N]$ hubiera una proporción positiva de números pares con $r_2(2n) = 0$, como $\mathfrak{G}_2(2n) \gg 1$, se tendría

$$T(N) \gg \sum_{n\asymp N} n^2 \gg N^3$$

que contradice lo que acabamos de probar. □

Bibliografía

[Cr] E. Cristóbal. El método del círculo. Trabajo de iniciación a la investigación para obtener el DEA en la UAM. Madrid 2003.

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

[Ha-Ra] G.H. Hardy, S. Ramanujan. Asymptotic formulae in combinatorial analysis. Proc. London Math. Soc., ser. 2, 17 (1918) 75–115.

[Ha-Wr] G.H. Hardy, E. Wright. An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[Kl] H.D. Kloosterman. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. Acta Mathematica 49 (1926), 407–464.

[Mo-Va] H.L. Montgomery, R.C. Vaughan. The exceptional set in Goldbach's problem. Acta Arith. 27 (1975), 353–370.

[Pe] A. Perelli. Goldbach numbers represented by polynomials. Rev. Mat. Iberoamericana 12 (1996), no. 2, 477–490.

[Ru] W. Rudin. Análisis real y complejo McGraw-Hill, 1987.

[Va] R.C. Vaughan. The Hardy-Littlewood method. Cambridge tracts in Mathematics 80. Cambridge University Press, 1981.

Capítulo 5

Introducción a las formas modulares

5.1. Funciones elípticas y curvas elípticas

Hoy en día las curvas elípticas deben gran parte de su fama, más allá del recoleto círculo de profesionales, a su participación crucial en la prueba del último teorema de Fermat y también es destacable su relevancia en criptografía. Sin embargo estos temas tan aritméticos son muy novedosos; hace mucho tiempo lo realmente importante eran las funciones elípticas (sobre las que trabajaron Gauss, Jacobi, Abel, Riemann y otros muchos ilustres), y más atrás todavía, hubo alguna elipse que motivó al menos el nombre.

En la actualidad uno podría leer un tratado sobre curvas elípticas con apenas referencias marginales a las funciones elípticas y ni una sola elipse. En principio es bastante lógico, porque las curvas elípticas se han convertido en grandes estrellas de la teoría de números que las considera definidas en $\mathbb{Q}$, en cuerpos finitos o en cuerpos de números, mientras que las funciones elípticas tienen su hogar natural en $\mathbb{C}$, demasiado grande para los que cuentan con los dedos.

A pesar de ello, el lector novato puede encontrar interesante saber a grandes líneas la conexión entre estos temas, que es el propósito de esta sección.

Históricamente el ancestro de la saga elíptica fue la integral que se obtiene al hallar la longitud de arco de una elipse genérica $x^2/a^2 + y^2/b^2 = 1$, en la que aparece la raíz de un polinomio bicuadrático

$$\int \frac{a^3 - (a^2 - b^2)x^2/a}{\sqrt{(a^2 - x^2)(a^4 - (a^2 - b^2)x^2)}}\, dx.$$

En vano buscaremos en las tablas de integrales: no hay una fórmula "cerrada" general. Al mirar esa hipotética tabla o el libro para ingenieros del pasado (¿ahora usan ordenadores?) veremos que cuando se tienen funciones algebraicas con la raíz cuadrada de un polinomio de primer o segundo grado, hay métodos pero no más allá. Eso sí, con cambios de variable ingeniosos se pueden transformar integrales desconocidas en integrales desconocidas, no es un gran negocio pero permite clasificar nuestro desconocimiento al estudiar integrales con la raíz de un polinomio bicuadrático, y se habla de integrales elípticas de primera, segunda y tercera especie. Las que salen al calcular arcos de elipse

pertenecen a la segunda división, mientras que la división de honor la ocupan integrales de la forma[1]

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \tag{5.1}$$

con k un número real a pesar del nombre (no hay aritmética todavía). Con un cambio de variable $x = \sqrt{\lambda u + \mu}$ otra forma de escribir estas integrales es

$$\int \frac{dx}{\sqrt{x^3 + ax + b}}. \tag{5.2}$$

El caso de grado dos formalmente corresponde en (5.1) a $k = 0$ y $\int_0^t dx/\sqrt{1-x^2} = \operatorname{arc\,sen} t$ que es una función bastante fea (multivaluada), sin embargo su inversa es entera y tan bella como las suaves ondulaciones de un estanque. Jacobi demostró que algo similar ocurría con la función inversa de $\int_0^t dx/\sqrt{(1-x^2)(1-k^2x^2)}$, llamado a veces *seno de amplitud* $\operatorname{sn}(x;k)$, presenta oscilaciones periódicas y en grado mayor que las funciones trigonométricas de toda la vida, pues incluso son periódicas en el plano complejo. Es decir, existen dos números ω_1 y ω_2, uno real y otro complejo tales que $\operatorname{sn}(z;k) = \operatorname{sn}(z+\omega_1;k) = \operatorname{sn}(z+\omega_2;k)$. Por otra parte, $\operatorname{sn}(z;k)$ cumple unas "fórmulas de adición" que recuerdan vagamente a las que aprendimos de memoria en nuestros años mozos para $\operatorname{sen}(\alpha+\beta)$ y $\cos(\alpha+\beta)$ [Ma].

La doble periodicidad impide que $\operatorname{sn}(z;k)$ sea entera porque entonces sería también acotada y por tanto constante (teorema de Liouville), sin embargo tenemos todavía una flamante función meromorfa.

Las funciones meromorfas elementales que conocemos tienen a lo sumo un periodo, por ello se quedan cortas para que sus inversas produzcan fórmulas explícitas para (5.1) y (5.2) más allá de unos casos triviales. Por otro lado, técnicas de cálculo numérico, algunas notablemente desarrolladas por Gauss, permiten aproximarlas con gran precisión.

Con la fiebre calculadora ya calmada, pasamos a centrarnos en las delicias de estas "funciones maravillosas" (denominación tomada del título de [Ma]).

Definición: Se dice que una función meromorfa f es una *función elíptica* si es doblemente periódica, esto es, si existen $\omega_1, \omega_2 \in \mathbb{C}$ linealmente independientes sobre $\mathbb{R}$ tales que $f(z) = f(z+\omega_1) = f(z+\omega_2)$ para todo $z \in \mathbb{C}$.

Ovbiamente también se cumplirá $f(z) = f(z+m\omega_1+n\omega_2)$, recíprocamente para f no constante el conjunto $\{\lambda \ : \ f(z) = f(z+\lambda)\}$ es un retículo llamado *retículo de periodos*

$$\Lambda = \{m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}\}.$$

Siempre que escribamos ω_1 y ω_2 daremos por supuesto que son generadores de Λ. Escribiremos también

$$\Lambda^* = \Lambda - \{0\}.$$

[1]Estas integrales se obtienen por ejemplo al tratar de resolver la ecuación del péndulo $x''(t) = \operatorname{sen}(2x(t))$. Multiplicando por x' e integrando, $(x')^2 = \text{cte} - \cos^2 x \Rightarrow t = \int dx/\sqrt{\text{cte} - \cos^2 x}$ que lleva a (5.1) con el cambio $u = \cos x$. Se podrían dar también ejemplos tomados de la teoría de la gravitación de Newton o de la relatividad general.

Una función elíptica puede considerarse por tanto como un elemento del cuerpo de funciones de la superficie de Riemann[2] $\mathbb{C}/\Lambda$, es decir, de un toro complejo. Aquí el cociente se hace de la manera obvia: $z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \Lambda$. Denotaremos la clase de z con $[z]$.

¿Cómo construir alguna función elíptica? Lo más sencillo es forzar la doble periodicidad sumando trasladados. A partir de un retículo de periodos Λ la función

$$f(z) = \sum_{\omega\in\Lambda} g(z+\omega)$$

es elíptica para cualquier g para la que la suma infinita tenga sentidoen el mundo de las funciones meromorfas. Digamos por ejemplo que g es una potencia. No es difícil probar que $\sum_{\omega\in\Lambda}(z+\omega)^{-k}$ converge si $k > 2$ y diverge si $k \leq 2$. En busca del ejemplo más sencillo modificaremos un poco ("renormalizaremos") el caso límite $k = 2$ para obligarlo a converger.

Definición: Dado un retículo de periodos Λ se llama *función $\wp$ de Weierstrass* asociada a Λ a la función elíptica

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^*}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right).$$

Nótese que las derivadas sucesivas de esta función producen los casos $k > 2$ ya libres de constantes de convergencia, por ejemplo. Por ejemplo

$$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z+\omega)^3}.$$

¿Parece poco haber construido dos funciones elípticas? Pues en realidad potencialmente en ella están incluidas todas.

Proposición 5.1.1 *Cualquier función elíptica f puede escribirse como*

$$f(z) = G\big(\wp(z)\big) + \wp'(z)H\big(\wp(z)\big)$$

donde G y H son funciones racionales (cocientes de polinomios).

Demostración: Por la identidad

$$f(z) = \frac{f(z)+f(-z)}{2} + \wp'(z)\frac{f(z)-f(-z)}{2\wp'(z)}$$

basta probar que toda función elíptica par g es una función racional de $\wp(z)$.

Sea el paralelogramo

$$R = \{\lambda\omega_1 + \mu\omega_2 \ : \ |\lambda|, |\mu| \leq 1/2\}.$$

[2]Una variedad de dimensión compleja uno con cambios de carta holomorfos.

Supondremos inicialmente que g no tiene ceros ni polos en el origen ni en la frontera γ de R. Por la doble periodicidad $\int_\gamma g'/g = 0$ (cada lado se anula con el opuesto). Lo que implica, por el principio del argumento [Ah], que hay tantos ceros como polos contando multiplicidades. Sean c y p un cero y un polo de g, entonces $g(z)\big(\wp(z)-\wp(p)\big)/\big(\wp(z)-\wp(c)\big)$ tiene menos ceros y menos polos que g en R, porque hemos cancelado los de c, $-c$, p y $-p$, y no hemos añadido ninguno nuevo ya que la función elíptica $\wp(z)-\text{cte}$ tiene exactamente un polo de orden 2 en R y por tanto sólo dos ceros.

Repitiendo el proceso se llega a una función elíptica entera y por tanto constante, esto es,

$$g(z) = C\prod_j \frac{\wp(z)-\wp(c_j)}{\wp(z)-\wp(p_j)}.$$

Si hubiera un polo o un cero en el origen, se puede eliminar multiplicando o dividiendo por potencias de $\wp$.

Los posibles ceros y polos que cayeran justamente en la frontera γ no causan problemas deformando ligeramente R (!?). □

La función $(\wp')^2$ es elíptica y par, por consiguiente, como se ha visto en la anterior demostración se puede escribir en términos de $\wp$. En vez de analizar el "algoritmo" allí aplicado, usaremos algo tan básico como el álgebra lineal:

Las partes principales de las cuatro funciones elípticas $\wp$, $\wp^2$, $\wp^3$ y $(\wp')^2$ son de la forma $P(z^{-1})$ con P un polinomio de grado a lo más 3 y $P(0)=0$. Tal espacio de polinomios tiene dimensión 3, entonces hay una combinación lineal no trivial que anula las partes principales y por consiguiente

$$\lambda_1\wp + \lambda_2\wp^2 + \lambda_3\wp^3 + \lambda_4(\wp')^2 = \text{cte}.$$

Los coeficientes se pueden hacer explícitos a partir del desarrollo de Laurent de $\wp$, digamos $z^{-2}+a_2z^2+a_4z^4+\dots$ obteniéndose

$$(\wp')^2 = 4\wp^3 - 20a_2\wp - 28a_4.$$

Podemos precisar fácilmente a_2 y a_4 a partir del retículo Λ usando la definición de $\wp$, siguiéndose $a_2 = 3\sum_{\omega\in\Lambda^*}\omega^{-4}$ y $a_4 = 5\sum_{\omega\in\Lambda^*}\omega^{-6}$. En resumidas cuentas, hemos probado:

Proposición 5.1.2 *La función $\wp$ verifica*

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

con $g_2 = 60\sum_{\omega\in\Lambda^*}\omega^{-4}$ *y* $g_3 = 140\sum_{\omega\in\Lambda^*}\omega^{-6}$.

Es fácil ver que ω_1, ω_2 y $(\omega_1+\omega_2)/2$ son ceros de $\wp'$ por tanto se puede escribir

$$4x^3 - g_2x - g_3 = 4\big(x-\wp(\omega_1/2)\big)\big(x-\wp(\omega_2/2)\big)\big(x-\wp((\omega_1+\omega_2)/2)\big),$$

en particular este polinomio tiene raíces simples (como habíamos visto en la demostración de la proposición anterior, $\wp(z)-\text{cte}$ tiene sólo dos ceros $\pm c$).

Desde el punto de vista de las superficies de Riemann lo que hemos hecho es hallar el cuerpo de funciones de $\mathbb{C}/\Lambda$ y probar que la ecuación algebraica de la superficie es $y^2 = 4x^3 - g_2x - g_3$, que no es singular por la ausencia de raíces dobles, y el cálculo de álgebra lineal es un caso muy sencillo del teorema de Riemann-Roch [Fa-Kr]. Con un poco más de lenguaje:

Proposición 5.1.3 *La aplicación*

$$\begin{aligned} \Phi: \ \mathbb{C}/\Lambda &\longrightarrow E \\ z &\mapsto \big(\wp(z), \wp'(z)\big) \end{aligned}$$

establece un isomorfismo holomorfo entre la superficie de Riemann $\mathbb{C}/\Lambda$ y la curva proyectiva $E:\ y^2 = 4x^3 - g_2x - g_3$, entendiendo que $\Phi([0])$ es el punto del infinito de E, de coordenadas proyectivas $(0:1:0)$.

Nota: La inyectividad se sigue porque, como hemos visto, definiendo R como en la demostración de la Proposición 5.1.1, $\wp(z) - \wp(z_1)$ sólo tiene como ceros z_1 y $-z_1$. La sobreyectividad se sigue porque ambas son superficies de Riemann compactas y Φ no es constante [Fa-Kr].

En el toro se puede sumar fácilmente, simplemente lo hacemos en $\mathbb{C}$ y tomamos módulo Λ, por ejemplo, si $\omega_1 = 1$, $\omega_2 = i$, entonces $[2 + \sqrt{2} + \pi i] + [17 - \sqrt{2} + ei] = [(\pi + e - 5)i]$. Se dice que $\mathbb{C}/\Lambda$ es una *variedad abeliana* porque sus puntos conforman un grupo abeliano. Entonces en E debe haber también una forma de sumar puntos.

Lema 5.1.4 *Si $u+v+w \in \Lambda$, esto es, si $[u]$, $[v]$ y $[w]$ suman cero en $\mathbb{C}/\Lambda$ entonces los puntos $\Phi(u)$, $\Phi(v)$ y $\Phi(w)$ están alineados.*

Demostración: Supondremos que $[u]$, $[v]$ y $[w]$ no son $[0]$, es decir, que $u, v, w \notin \Lambda$. Las tres imágenes están alineadas si y sólo si

$$\begin{vmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{vmatrix} = 0.$$

Si $u + v + w \in \Lambda$ se puede reemplazar en este determinante w por $-u - v$ sin que varíe su valor. Sea $F(u)$ la función así obtenida (para v fijado). Es evidente que F es elíptica y no es difícil ver que F no tiene un polo en $u = 0$: multiplicando la segunda columna por $u/2$ y sumándosela a la primera se tiene

$$F(u) = \begin{vmatrix} \wp(u) - u\wp'(u)/2 & \wp'(u) & 1 \\ \wp(v) - u\wp'(v)/2 & \wp'(v) & 1 \\ \wp(-u-v) - u\wp'(-u-v)/2 & \wp'(-u-v) & 1 \end{vmatrix} = 0.$$

La segunda y la tercera filas coinciden hasta orden dos, por tanto no hay polo en $u = 0$.

De forma similar, por simetría, se deduce que no hay un polo en $u = -v$, entonces F es entera y elíptica, por tanto constante, además como $F(v) = 0$, debe ser idénticamente nula.

Si alguno de los elementos es [0] aparece el punto del infinito, pero el argumento no es diferente. Digamos por ejemplo $[v] = 0$ (el resto de los casos se reducen a éste), entonces la segunda fila del determinante inicial pasa a ser $(0, 1, 0)$. □

Se puede probar que el proceso se puede invertir asociando a cada curva no singular de la forma $E:\ y^2 = 4x^3 - \alpha x - \beta$ un toro $\mathbb{C}/\Lambda$ cuya imagen por Φ es E. El retículo Λ estará formado por los valores de $\int_\gamma \omega$ con ω la diferencial holomorfa dx/y y γ un lazo definido en (la superficie de Riemann que determina) E. Incluso tal retículo se puede calcular numéricamente con gran precisión [Kn] VI§9. Nótese que $\int \omega$ es como (5.2). Las "fórmulas de adición" antes mencionadas para este tipo de integrales corresponden a la suma en $\mathbb{C}/\Lambda$.

Simplemente para que las cosas sean más simples y se parezcan a las de los libros actuales, consideraremos $E:\ y^2 = x^3 + ax + b$ en lugar de $E:\ y^2 = 4x^3 - \alpha x - \beta$, tales curvas sólo difieren en un cambio lineal que por tanto no destruye la alineación de los puntos. La no singularidad de E equivale a que $x^3 + ax + b$ no tenga raíces dobles, o lo que es lo mismo, a que el determinante $4a^3 + 27b^2$ no sea nulo.

Proposición 5.1.5 *Sea $E:\ y^2 = x^3 + ax + b$ curva proyectiva sobre $\mathbb{C}$ no singular. Entonces se puede dotar a sus puntos de una ley de grupo $(E, +)$ de forma que el elemento neutro O es el punto del infinito, el elemento inverso de $P = (x, y)$ es $P = (x, -y)$ y si $P + Q = R$ entonces P, Q y $-R$ están alineados.*

Observación: Ciertamente uno podría definir directamente la ley de grupo en $E:\ y^2 = x^3 + ax + b$ con el simétrico del tercer punto de intersección de la recta secante, y demostrar que realmente es ley de grupo sin referencia a la función $\wp$ (como en los libros actuales) pero entonces la asociativa daría algún dolor de cabeza (cf. [Ca]).

Demostración: La ley de grupo viene heredada de la suma en $\mathbb{C}/\Lambda$, es decir,

$$P + Q = \Phi\big(\Phi^{-1}(P) + \Phi^{-1}(Q)\big)$$

y trivialmente comparte las propiedades de grupo abeliano con la suma usual.

Considerando $\Phi([0])$ y la paridad de $\wp$ es fácil deducir los elementos neutro y opuesto. Si $P + Q - R = 0$, por definición $\Phi^{-1}(P) + \Phi^{-1}(Q) + \Phi^{-1}(-R) = [0]$ y el lema anterior prueba que P, Q y $-R$ están alineados. □

Si dos raíces de un polinomio cúbico en $K[x]$ pertenecen a K, entonces la tercera raíz pertenece también a K. Esta sencilla observación prueba que la ley de grupo anterior tiene aplicaciones aritméticas. Desde el punto de vista de las ecuaciones diofánticas, las curvas de primer y segundo grado se pueden parametrizar si tienen un punto racional

(y esto se puede decidir algorítmicamente con el Teorema de Hasse-Minkowski [Bo-Sh], [Ca]), lo cual permite calcular fácilmente todos los puntos racionales[3]. La ley de grupo permite enfrentarse al caso de tercer grado.

Definición: Una *curva elíptica* E sobre un cuerpo K es una curva proyectiva cúbica no singular sobre K con al menos un punto en este cuerpo.

En cuerpos normales y corrientes (por ejemplo en característica cero), es fácil ver que toda curva elíptica tras un cambio de variable se escribe como $y^2 = x^3 + ax + b$ con $4a^3 + 27b^2 \neq 0$, y en los casos patológicos donde no siempre puede hacerse (por ejemplo en $\mathbb{F}_2$) hay una expresión similar [Ca], [Si]. Por ello la ley de grupo se extiende a todas las curvas cúbicas no singulares.

Para los amigos de los formulones, unos cálculos consistentes en intersecar una recta y una cúbica, prueban que para una curva elíptica $E:\ y^2 = x^3 + ax + b$, se tienen las fórmulas:

$$P = (x_1, y_1), \qquad Q = (x_2, y_2), \qquad P + Q = (x, y)$$

con

$$x = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2, \qquad y = -\frac{y_1 - y_2}{x_1 - x_2}x - \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$$

siempre que $x_1 \neq x_2$. Si $x_1 = x_2$ pero $P \neq Q$ debemos entender que el resultado es el punto del infinito y si $P = Q$, es el "límite" en E de la expresión anterior:

$$x = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1, \qquad y = -\frac{3x_1^2 + A}{2y_1}x - \frac{-x_1^3 + ax_1 + 2b}{2y_1}.$$

¿Y qué se sabe de la aritmética de las curva elípticas? Muchas cosas pero todavía hay grandes lagunas.

Se conoce que el grupo de puntos sobre $\mathbb{Q}$ de una curva elíptica está finitamente generado (teorema de Mordell), es decir, que a partir de algunas soluciones podemos generar todas a base de sumas. También se saben calcular los puntos de torsión: los puntos racionales que al ser operados consigo mismos vuelven a repetirse a la larga; pero se desconoce un algoritmo infalible desde el punto de vista teórico para calcular los puntos que no se repiten, los que dan lugar a infinitas soluciones, o saber si no existen.

Otro punto importante tiene que ver con las relaciones locales-globales. Por ejemplo, se cree que si en una curva elíptica hay "muchos" puntos módulo p para todo p, entonces debe contener infinitos puntos racionales (conjetura de Birch–Swinnerton-Dyer).

5.2. Formas modulares

Según hemos visto, las curvas elípticas se corresponden con los retículos. Una pregunta natural es si retículos diferentes pueden dar lugar a la misma curva salvo isomorfismos

[3]Por ejemplo $x^2 + y^2 = 1$ se parametriza como $x = (t^2 - 1)/(t^2 + 1)$, $y = 2t/(t^2 + 1)$ y eligiendo $t \in \mathbb{Q}$ se obtienen todas las soluciones racionales salvo $(1, 0)$.

(cambios de variable). Atacaremos primero el problema más básico, y realmente muy sencillo, consistente en decidir si dos retículos son iguales a partir de sus generadores.

Si Λ es el retículo (en $\mathbb{C}$) generado por $\{\omega_1, \omega_2\}$ y Λ' es el generado por $\{\eta_1, \eta_2\}$, entonces $\Lambda = \Lambda'$ si y sólo si hay un cambio de variable lineal con matriz entera e inversa entera que pase los generadores de uno a los del otro. Es decir

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \qquad \text{con} \quad ad - bc = \pm 1. \tag{5.3}$$

Si reordenamos los generadores de forma que tengan la misma orientación, por ejemplo $\angle\omega_2\omega_1,\ \angle\eta_2\eta_1 < \pi$, entonces $+1$ es la única posibilidad. La orientación elegida corresponde a exigir que $z_\Lambda = \omega_1/\omega_2$ y $z_{\Lambda'} = \eta_1/\eta_2$ estén en el semiplano superior

$$\mathbb{H} = \{x + iy \ :\ x \in \mathbb{R},\ y > 0\}.$$

Si dividimos las ecuaciones de la primera y la segunda coordenadas en (5.3) podemos escribir esta relación en términos de z_Λ y $z_{\Lambda'}$, y sólo perdemos la información de multiplicar ambas ecuaciones por una constante. Con un poco de lenguaje pero sin nada nuevo:

Lema 5.2.1 *Si $\Lambda = \Lambda'$ entonces*

$$z_{\Lambda'} = \gamma z_\Lambda \qquad \textit{con } \gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$$

donde se define $\gamma z = (az + b)/(cz + d)$. Además, si $z_\Lambda = z_{\Lambda'}$ entonces $\Lambda' = \mu\Lambda$ para algún $\mu \in \mathbb{C}$.

Nota: Recuérdese que $\mathrm{SL}_2(\mathbb{Z})$ es el grupo de matrices enteras con determinante uno. Sería más propio escribir $\gamma(z)$ en vez de γz, pero el uso ha privilegiado a esta última notación.

Es fácil ver que $\mathrm{SL}_2(\mathbb{Z})$ actúa "bien" en $\mathbb{H}$. Cada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ define una biyección $\mathbb{H} \longrightarrow \mathbb{H}$ y la acción es propia y discontinua[4]. Un pequeño borrón en el historial de $\mathrm{SL}_2(\mathbb{Z})$ es que γ y $-\gamma$ actúan igual, por ello a veces se toma en consideración el grupo menos intuitivo $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Los elementos de $\mathrm{SL}_2(\mathbb{Z})$ no envían un punto fijado a cualquier punto de $\mathbb{H}$ porque no todos los retículos son iguales. La relación es un poco más sutil.

Proposición 5.2.2 *Dado $z \in \mathbb{H}$ existe $\gamma \in SL_2(\mathbb{Z})$ tal que γz pertenece al* dominio fundamental

$$D = \{z \ :\ |\Re z| \le 1/2,\ |z| \ge 1\}.$$

De hecho z corresponde exactamente a un punto en D si se suprime la parte de la frontera en $\Re z < 0$.

[4]Que la acción sea discontinua significa que la órbita de un punto no tiene puntos límite (las imágenes de un punto caen en puntos aislados). Por poner más apellidos, $\mathrm{SL}_2(\mathbb{Z})$ es un grupo Fuchsiano de primera especie [Iw].

Demostración: El grupo $\mathrm{SL}_2(\mathbb{Z})$ está generado por las matrices $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ y $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ [Kn] Prop. 5.3, la primera corresponde a la traslación $z \mapsto z+1$ y la segunda a la inversión $z \mapsto -1/z$. A base de trasladar podemos enviar cualquier $z \in \mathbb{H}$ a $|\Re z| \leq 1/2$ y con una inversión podemos sacar fuera lo que está dentro del círculo unidad $|z| \leq 1$.

La traslación y la inversión pasan la frontera izquierda a la derecha de ahí la ambigüedad de estos puntos y hay que suprimir una de ellas para preservar la unicidad. □

Hay varias maneras de leer este resultado. Si consideramos el conjunto[5]

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} = \{\text{órbitas de } z \text{ en } \mathbb{H}\},$$

entonces hemos probado que $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ es como D con las fronteras derecha e izquierda identificadas. Topológicamente es una esfera en la que un punto se ha llevado a infinito, si se emplea la métrica heredada de la natural[6] en $\mathbb{H}$.

Un isomorfismo de curvas elípticas $f : E \longrightarrow E'$ (pedimos que se conserve el punto del infinito, $f(O) = O$, lo cual es como decir que el isomorfismo también lo es de grupos) da lugar, a través de Φ^{-1}, a un isomorfismo holomorfo $F : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$. En particular F se puede extender a $\mathbb{C} \longrightarrow \mathbb{C}$ con $F(0) = 0$ y envía Λ en Λ'. Como las funciones holomorfas no singulares son conformes (conservan ángulos) es fácil deducir (!?) que F sólo puede ser un giro quizá combinado con una homotecia, es decir, $F(z) = \mu z$ y por tanto $\Lambda' = \mu\Lambda$. Con ello hemos resuelto el problema original.

Proposición 5.2.3 *Dos retículos $\Lambda, \Lambda' \subset \mathbb{C}$ corresponden a curvas elípticas isomorfas si y sólo si z_Λ y $z_{\Lambda'}$ están en la misma clase de $\mathbb{H}\backslash SL_2(\mathbb{Z})$, esto es, si $z_{\Lambda'} = \gamma z_\Lambda$ para algún $\gamma \in SL_2(\mathbb{Z})$.*

Si tuviéramos una función inyectiva $J : \mathbb{H}\backslash\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{C}$ al "desenrollarla" a $\mathbb{H}$, definiendo $J(z) = J(\text{órbita de } z)$, se obtendría una función que satisface la relación modular[7]

$$J(z) = J(\gamma z) \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}) \tag{5.4}$$

y la condición del resultado anterior equivaldría a $J(z_\Lambda) = J(z_{\Lambda'})$.

Por otro lado, dadas dos curvas elípticas $E : y^2 = x^3 + ax + b$, $E' : y^2 = x^3 + a'x + b'$, parece claro que no podemos hacer cambios de grado mayor o igual que uno para pasar de una a otra porque no serían invertibles, y entre los cambios lineales sólo aquellos

[5] Recuérdese de los cursos de teoría de grupos que la órbita de un elemento es la colección de imágenes por la acción de un grupo.

[6] La métrica de Poincaré en $\mathbb{H}$, $ds^2 = y^{-2}(dx^2+dy^2)$, es la métrica coherente con las transformaciones $\gamma \in \mathrm{SL}_2(\mathbb{R})$ porque éstas la dejan invariante (son isometrías). Con ella los puntos $-1/2+iy$ y $1/2+iy$ se acercan más cuanto mayor es y, de ahí que D sea como una esfera con un punto en el infinito y no una esfera con un círculo en el infinito como podría dictarnos nuestra visión euclídea.

[7] Este desafortunado nombre es una vetusta herencia de la teoría de funciones e integrales elípticas que deriva del nombre *módulo* que recibía la constante k de (5.1).

de la forma $y \mapsto \lambda^3 y$, $x \mapsto \lambda^2 x$ preservan la forma de la ecuación cúbica (con otros aparecería por ejemplo un término en x^2). Así pues la única posibilidad para que sean isomorfas es que $a' = \lambda^{-4}a$ y $b' = \lambda^{-6}b$. Entonces cualquier función $g = g(a,b)$ con $g(a,b) = g(\lambda^{-4}a, \lambda^{-6}b)$ será invariante en las curvas elípticas isomorfas y corresponderá a través de Φ^{-1} a una función que satisface (5.4). Hay muchas posibilidades, por ejemplo $g(a,b) = a^3/b^2$. Tomaremos sin embargo $g(a,b) = \text{cte}\ a^3/(4a^3 + 27b^2)$ que tiene la ventaja de que no produce nunca infinitos. Recuérdese que $y^2 = x^3 + ax + b$ se puede transformar en $y^2 = 4x^3 - g_2 x - g_3$ con g_2 y g_3 dependiendo del retículo como se indica en la Proposición 5.1.2.

Escribiendo como antes $z = \omega_1/\omega_2$ y revisando las cuentas, todo este galimatías se traduce en que una posibilidad para la función J que buscábamos es

$$J(z) = \frac{E_4^3(z)}{20E_4^3(z) - 49E_6^2(z)} \qquad \text{con} \qquad E_k(z) = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{(nz+m)^k}.$$

Nótese que es muy fácil comprobar que $J(z) = J(z+1)$ y $J(z) = J(-1/z)$, consecuentemente (5.4) admite una prueba directa una vez que sabemos que $z \mapsto z+1$ y $z \mapsto -1/z$ generan la acción de $\mathrm{SL}_2(\mathbb{Z})$. La invariancia de J se deriva de que las funciones $E_k(z)$ satisfacen $E_k(z) = E_k(z+1)$ y $E_k(z) = z^{-2k}E_k(-1/z)$. Estas dos fórmulas se combinan en la expresión general

$$E_k(z) = j_\gamma^{-k}(z)E_k(\gamma z) \qquad \text{donde } j_\gamma(z) = cz + d \quad \text{para } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Es hora de dar alguna definición que justifique el título del capítulo.

Definición: Se dice que una función holomorfa $f : \mathbb{H} \longrightarrow \mathbb{C}$ es una *función modular de peso* k si satisface

$$f(z) = j_\gamma^{-k}(z) f(\gamma z) \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Se dice que una función modular es una *forma modular* si además es holomorfa en el infinito, $\lim_{y\to+\infty} f(x+iy) < \infty$. Si este límite es cero se dice que es una *forma parabólica* (o *cuspidal*).

Notación: Denotaremos con $\mathcal{M}_k$ el conjunto de formas modulares de peso k y con $\mathcal{S}_k$ las formas parabólicas de peso k.

Evidentemente $\mathcal{M}_k$ es un espacio vectorial sobre $\mathbb{C}$ y $\mathcal{S}_k$ es un subespacio suyo. Como γ y $-\gamma$ dan lugar a la misma acción sobre $\mathbb{H}$, estos espacios sólo pueden ser no triviales cuando k es par. No obstante hay generalizaciones de la definición anterior que cubren los casos $k \in \mathbb{R}$ (véase [Iw]). Así como una función modular de peso 0 corresponde a una función definida en $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, una de peso 2 corresponde a una forma diferencial[8] y las de peso superior a diferenciales de orden superior. De alguna manera las formas parabólicas suplen a las diferenciales de soporte compacto que no existen en el mundo holomorfo. Todas ellas pueden verse como funciones homogéneas de cierto grado definidas en el

[8] La expresión $f(z)dz$ es invariante bajo $\mathrm{SL}_2(\mathbb{Z})$ si f es de peso 2 porque $d\gamma z = j_\gamma^{-2}(z)$.

espacio de retículos. Por ejemplo, si F es homogénea (de grado 0), la condición (5.3) para que no dependa de los generadores elegidos es $F(\omega_1, \omega_1) = F(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ y equivale a que $J(z) = F(z, 1)$ verifique (5.4) con $z = \omega_1/\omega_2$ como antes.

Una forma modular f en particular es periódica de periodo uno y por tanto debe admitir un desarrollo de Fourier

$$f(z) = \sum_{m=0}^{\infty} a_m e(mz)$$

y $f \in \mathcal{S}_k$ cuando $a_0 = 0$.

Para las funciones E_k, llamadas *series de Eisenstein*, se puede obtener este desarrollo derivando el bien conocido desarrollo de la cotangente:

$$\pi i - 2\pi i \sum_{m=0}^{\infty} e(mz) = \pi \cot(\pi z) = \sum_{-\infty}^{\infty} \frac{1}{z+m}.$$

El resultado obtenido es

$$E_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi i)^k}{(2k-1)!} \sum_{m=1}^{\infty} \sigma_{2k-1}(m) e(mz)$$

donde $\sigma_{2k-1}(m) = \sum_{d|m} d^{2k-1}$.

Una de las propiedades básicas de los espacios vectoriales $\mathcal{M}_k$ y $\mathcal{S}_k$ es que tienen dimensión finita y además computable. La prueba de este hecho sólo requiere los rudimentos de variable compleja pero no la reproduciremos aquí (véase [Se]).

Proposición 5.2.4 *Para $k \geq 0$ par*

$$\dim \mathcal{M}_k = \begin{cases} [k/12] & si\ 12|k-2 \\ [k/12]+1 & si\ 12|k-2 \end{cases} \qquad \dim \mathcal{S}_k = \begin{cases} 0 & si\ k < 12 \\ \dim \mathcal{M}_{k-12} & si\ k \geq 12 \end{cases}$$

donde $[\cdot]$ indica la parte entera.

Esto permite demostrar algunas identidades asombrosas.

Por ejemplo, $\dim \mathcal{M}_8 = 1$ y como $E_4^2, E_8 \in \mathcal{M}_8$ deben ser proporcionales, comparando el primer coeficiente $2\zeta^2(4)E_8(z) = \zeta(8)E_4^2(z)$. Mirando una tabla o haciendo los cálculos, se cumple $\zeta(4) = \pi^4/90$ y $\zeta(8) = \pi^8/9450$ y el desarrollo de Fourier conduce a

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Otro ejemplo tiene que ver con la primera forma parabólica, que aparece para el peso $k = 12$. Buscando la anulación del primer coeficiente de Fourier se tiene que la forma

modular $(2\zeta(6))^2 E_4^3(z) - (2\zeta(4))^3 E_6^2(z)$ está en $\mathcal{S}_{12}$. Por otra parte es posible probar, haciendo algunos pases mágicos con derivadas logarítmicas (véase [Se]), que

$$\Delta(z) = e(z) \prod_{m=1}^{\infty} (1 - e(mz))^{24} \in \mathcal{S}_{12}$$

de donde se deduce la extraña igualdad (¿se podría probar de forma elemental y sencilla? quizá no)

$$\Delta(z) = \frac{675}{256\pi^{12}} \big(20E_4^3(z) - 49E_6^2(z)\big).$$

Todavía hay más misterios relativos a esta función. Si $\tau(n)$ es el n-ésimo coeficiente de Fourier de $\Delta(z)$ entonces z es una función multiplicativa. Esto fue conjeturado por S. Ramanujan, quien notó otras asombrosas propiedades como la fórmula $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ o la congruencia $\tau(n) \equiv \sigma_{11}(n)$ (691). Además la "función L" asociada a Δ

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

satisface una ecuación funcional sorprendentemente similar a la de la función ζ. Todas estas propiedades se encuadran y demuestran dentro de la teoría de formas modulares desarrollada por Hecke. Un asunto mucho más espinoso es el tamaño de los coeficientes de Fourier de una forma modular, en particular de $\Delta(z)$. Por ejemplo, la inocente conjetura de Ramanujan $|\tau(p)| < 2p^{11/2}$ debió esperar hasta el trabajo de P. Deligne que mereció la medalla Fields en los años 70. La sencilla distribución conjeturada para $p^{-11/2}\tau(p)$ cuando p varía (conjetura de Sato-Tate) es todavía un problema abierto[9].

De las anteriores propiedades, la ecuación funcional es la más sencilla y nos ocuparemos de ella ahora. En la siguiente sección daremos los ingredientes para poder probar la multiplicatividad de los coeficientes.

Proposición 5.2.5 *Dada $f \in S_{2k}$ con $f(z) = \sum_{m=0}^{\infty} a_m e(mz)$, sea*

$$L(s, f) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}.$$

Entonces $L(s, f)$ admite una extensión entera que verifica la ecuación funcional

$$(2\pi)^{-s}\Gamma(s)L(s, f) = (-1)^k (2\pi)^{s-2k}\Gamma(2k - s)L(2k - s, f).$$

Demostración: Por la definición de la función Γ y el desarrollo de Fourier de f, se tiene

$$(2\pi)^{-s}\Gamma(s)L(s, f) = \int_0^{\infty} f(it)t^{s-1}\, dt.$$

Esto prueba que $L(s, f)$ se extiende a una función entera. Por la relación modular $f(z) = z^{-2k} f(-1/z)$ se cumple $f(it) = (-1)^k t^{-2k} f(i/t)$ y sustituyendo en la integral

[9]Nota añadida en 2010: En 2009 se presentó la prueba de este hecho.

y cambiando la variable $t \mapsto 1/u$ se deduce que el segundo miembro es invariante al reemplazar s por $2k - s$, salvo la multiplicación por $(-1)^k$. □

Una rica fuente de funciones y formas modulares son las funciones θ asociadas a formas cuadráticas. No se ajustan en general a la estricta definición dada aquí pero nos valdremos de un ejemplo para ilustrar la situación.

La función

$$\theta(z) = \sum_{m=-\infty}^{\infty} e(m^2 z/2),$$

por la periodicidad y la fórmula de sumación de Poisson, cumple

$$\theta(z) = \theta(z+2) \qquad \text{y} \qquad \theta(z) = (iz)^{-1/2}\theta(-1/z).$$

Es una forma modular de peso $1/2$ con dos salvedades frente a la definición de esta sección: En primer lugar el grupo que actúa no es todo $\mathrm{SL}_2(\mathbb{Z})$ pues no aparece $z \mapsto z+1$, y en segundo lugar, la relación modular está afectada por un "multiplicador" $i^{-1/2}$. Elevando a una potencia adecuada el multiplicador no será molesto. Por ejemplo, si estamos interesados en $r_8(m)$, el número de representaciones de m como suma de ocho cuadrtados,

$$\theta^8(z) = \sum_{m=0}^{\infty} r_8(m) e(mz/2)$$

y se tiene

$$\theta^8(z) = j_\gamma^{-4}(z)\theta(\gamma z) \qquad \text{para} \quad \gamma \in G$$

donde G es el grupo generado por $z \mapsto z+2$ y $z \mapsto -1/z$.

La teoría es paralela al caso de $\mathrm{SL}_2(\mathbb{Z})$ y por cuestiones de dimensión se puede deducir que $\theta^8(z)$ debe ser proporcional a una variante de la serie de Eisenstein y de ahí la fórmula cerrada

$$r_8(m) = 16(-1)^m m^3 \sum_{d|m} (-1)^{m/d} d^{-3}.$$

No hay fórmulas bonitas cuando la dimensión del espacio de formas modulares crece, pues entonces $\theta^{4k}(z)$ no se puede expresar sólo como suma de series de Eisenstein. Por ejemplo, el caso de 24 cuadrados lleva a considerar formas de peso $12 = 24 \cdot 1/2$ y el resultado final es una parte principal con sumas de divisores, que proviene de las series de Eisenstein, y otra menos influyente que contiene los coeficientes $\tau(n)$ de $\Delta(z)$, la "única" forma parabólica de peso 12. El método del círculo permite deducir el término principal sin necesidad de entrar en la teoría de formas modulares.

5.3. Operadores de Hecke

Se puede definir una función invariante en un retículo tomando otra y promediándola en retículos más finos que coinciden con el original tras aplicar una transformación lineal

de determinante n. Elaborando esta idea en el contexto de las formas modulares [Kn], [Se], que a fin de cuentas son funciones homogéneas de retículos [Iw], se llega al concepto de operadores de Hecke.

Para definirlos se considera un conjunto Δ_n de representantes de los cogrupos a la derecha $\mathrm{SL}_2(\mathbb{Z})\backslash M_n$ con M_n las matrices de determinante n, o dicho de otra forma, se escoge Δ_n de manera que

$$M_n = \bigcup_{\alpha\in\Delta_n} \mathrm{SL}_2(\mathbb{Z})\alpha$$

sea una partición.

Proposición 5.3.1 *Para $n \in \mathbb{N}$ el* operador de Hecke *definido como*

$$T_n f = n^{k/2-1} \sum_{\alpha\in\Delta_n} j_\alpha^{-k}(z) f(\alpha z)$$

aplica $\mathcal{M}_k$ en $\mathcal{M}_k$ y $\mathcal{S}_k$ en $\mathcal{S}_k$.

La definición anterior se puede escribir de forma mucho más pedestre comprobando que un conjunto válido de representantes es (véase [Se], [Iw])

$$\Delta_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ : \ ad = n,\ 0 \le b < d \right\}.$$

Es decir,

$$T_n f(z) = n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} d^{-k} f\big(\frac{az+b}{d}\big).$$

Con esta fórmula simplificada en nuestras manos no es difícil dar una prueba directa de la proposición anterior y estudiar cómo actúa T_n sobre el desarrollo de Fourier de una forma modular.

Proposición 5.3.2 *Sea $f(z) = \sum_{m=0}^{\infty} a_m e(mz) \in \mathcal{M}_k$, entonces*

$$T_n f(z) = \sum_{m=0}^{\infty} b_m e(mz) \qquad \textit{con} \qquad b_m = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}.$$

En particular, si $n = p$ es primo el coeficiente de Fourier m-ésimo de $T_n f(z)$ con $p \not| m$ es a_{pm}.

Empleando la proposición anterior o, mejor todavía, con la definición en términos de retículos [Kn] VIII.7, se deduce

Proposición 5.3.3 *Los operadores de Hecke verifican*

$$T_m T_n = \sum_{d|(n,m)} d^{k-1} T_{mn/d^2}.$$

En particular los operadores de Hecke conmutan y si $(n, m) = 1$ se tiene $T_m T_n = T_{mn}$.

Los operadores de Hecke son autoadjuntos con respecto al producto escalar de fromas modulares dado por

$$\langle f, g\rangle = \int_D f(z)\overline{g(z)}y^{k-2}\,dxdy$$

y por tanto se puede diagonalizar. Por simple álgebra lineal si tenemos endomorfismos diagonalizables y que conmutan, debe existir una base en la que todos ellos diagonalicen simultáneamente.

Definición: Se dice que $\mathcal{B} = \{f_1, f_2, \ldots, f_r\}$ es una *base de Hecke* de $\mathcal{M}_k$ o de $\mathcal{S}_k$ si cada $f \in \mathcal{B}$ cumple $T_n f(z) = \lambda_n f(z)$ para todo $n \in \mathbb{N}$ y ciertos λ_n (dependiendo de f).

El misterioso comportamiento de los coeficientes de la función $\Delta(z)$ está a punto de ser desvelado.

Proposición 5.3.4 *Sea $f(z) = \sum_{m=0}^{\infty} a_m e(mz)$ un elemento de una base de Hecke con $a_1 = 1$, entonces*

a) $a_n = \lambda_n$, el autovalor de f en T_n.

b) $a_n a_m = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}$.

Demostración: Por la Proposición 5.3.2 el coeficiente de $e(z)$ en el desarrollo de Fourier de $T_n f(z)$ es a_n y la relación $T_n f(z) = \Lambda_n f(z)$ termina la prueba de *a*).

Para *b*) basta aplicar *a*) junto con la Proposición 5.3.3. □

Corolario 5.3.5 *Sea $\tau(n)$ el n-ésimo coeficiente de $\Delta(z) = e(z)\prod_{m=1}^{\infty}(1-e(mz))^{24}$ entonces τ es una función multiplicativa que satisface $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ para p primo.*

Demostración: Como $\dim \mathcal{S}_{12} = 1$, $\mathcal{B} = \{\Delta(z)\}$ es una base de Hecke. Obviamente $\tau(1)1$ y se aplica la proposición. La conclusión buscada es consecuencia directa de *b*). □

Corolario 5.3.6 *La función $L(s, \Delta)$ admite el producto de Euler*

$$L(s,\Delta) = \prod_p \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}.$$

Demostración: Por ser τ multiplicativa

$$L(s,\Delta) = \prod_p \left(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \frac{\tau(p^3)}{p^{3s}} + \ldots\right).$$

Multiplicando cada factor por $1 - \tau(p)p^{-s} + p^{11-2s}$ el coeficiente de p^{-rs}, $r \geq 2$ es $\tau(p^r) - \tau(p)\tau(p^{r-1}) + p^{11}\tau(p^{r-2}) = 0$ y de aquí (!?) cada uno de ellos es igual a $\left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}$. □

En esta sección más que en otras es necesario mencionar que esto es sólo una mínima parte de una inmensa teoría que se esconde detrás. La conexión de las formas modulares con la aritmética se realiza fundamentalmente a través de los operadores de Hecke. Esta relación involucra ideas muy profundas. Por ejemplo, para peso $k = 2$ los operadores de Hecke se pueden "dualizar" para que actúen en la homología con coeficientes enteros en superficies de Riemann uniformizadas por ciertos subgrupos sencillos de $\mathrm{SL}_2(\mathbb{Z})$. Esto permite probar que los coeficientes de Fourier de las formas modulares de peso 2 de la base de Hecke correspondiente a estos subgrupos, son números algebraicos. Si además son enteros, la teoría de M. Eichler y G. Shimura les asocia una curva elíptica sobre $\mathbb{Q}$ cuyo número de soluciones módulo p está relacionado con estos coeficientes. Las importantes contribuciones actuales, partiendo del trabajo de A. Wiles, han permitido ir en el sentido contrario asociando a las curvas elípticas sobre $\mathbb{Q}$ una forma modular, con algunas consecuencias bien conocidas.

Bibliografía

[Ah] L.V. Ahlfors. Análisis de variable compleja: Introducción a la teoría de funciones analíticas de una variable compleja. Aguilar, Madrid 1971.

[Bo-Sh] A.I. Borevich, I.R. Shafarevich. Number theory. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[Ca] J.W.S. Cassels. Lectures on elliptic curves, London Mathematical Society Student Texts 24, Cambridge University Press, 1991.

[Fa-Kr] H.M. Farkas, I. Kra. Riemann surfaces. Graduate Texts in Mathematics, 71. Springer-Verlag, New York-Berlin, 1980.

[Iw] H. Iwaniec. Topics in classical automorphic forms. Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.

[Kn] A.W. Knapp. Elliptic curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[Ma] A.I. Markushevich. Curvas maravillosas. Números complejos y representaciones conformes. Funciones maravillosas. Lecciones populares de Matemáticas. Editorial Mir, 1977.

[Se] J.-P. Serre. A course in arithmetic. Graduate Texts in Mathematics, 7. Springer-Verlag, New York-Heidelberg, 1973.

[Si] J. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, 1986.