En esta hoja vamos a ver algunas aplicaciones aritméticas que derivan de los contenidos de las dos hojas anteriores.

La primera aplicación es relativa a la función $r(n)$ que da el número de representaciones de $n \in \mathbb{Z}^+$ como suma de dos cuadrados de enteros. Esto es,

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

Por ejemplo, $r(10) = 8$ ya que $10 = (\pm 3)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 3)^2$ con todas las combinaciones de signos. También se tiene $r(2023) = r(2024) = 0$ y $r(2050) = 24$. La pregunta que nos hacemos es si hay una fórmula para calcular esta función tan caótica.

1) Considera el desarrollo en serie de potencias (en q) de cada uno de los miembros de (3) de la hoja anterior. Demuestra que el coeficiente de q^n en el primer miembro es $r(n)$ y en el segundo miembro es $4\sum_{2d+1|n}(-1)^d$ donde $2d+1 \mid n$ indica que $2d+1$ recorre los divisores impares (positivos) de n. Por tanto,

$$r(n) = 4 \sum_{2d+1|n} (-1)^d. \tag{1}$$

Indicación: Toma $x = q^k$ en $x/(1+x^2) = x\sum_{d=0}^{\infty}(-1)^d x^{2d} = \sum_{d=0}^{\infty}(-1)^d x^{2d+1}$.

El resultado se puede también reformular como un producto de series. El siguiente enunciado incluye $\Re(s) > 1$ porque es lo que garantiza que las series converjan. Si no entiendes por qué, olvídate de esa condición y supón la convergencia.

2) Prueba que para $\Re(s) > 1$ se tiene la relación

$$\sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\zeta(s) \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}$$

y calcula $\lim_{s\to 1^+}(s-1)\sum_{n=1}^{\infty} r(n)/n^s$.

Por último, derivemos una fórmula que es computacionalmente más eficiente. Para ello, dado $n \in \mathbb{Z}^+$ empleamos la siguiente notación para su descomposición en factores primos:

$$n = 2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s} \qquad \text{con } \gamma, \alpha_j, \beta_j \in \mathbb{Z}_{\geq 0}, \quad p_j \equiv 1\ (4) \quad \text{y} \quad q_j \equiv -1\ (4).$$

Es decir, separamos los primos dependiendo de si son de la forma $4k+1$ o $4k-1$ o si es el primo 2. El primer paso del siguiente ejercicio quizá te cueste un poco. Si no te sale, consulta [6, §6.15] o [7].

3) Demuestra que $\sum_{2d+1|n_1n_2}(-1)^d = \sum_{2d_1+1|n_1}(-1)^{d_1}\cdot\sum_{2d_2+1|n_2}(-1)^{d_2}$ si n_1 y n_2 son coprimos. De la fórmula (1) deduce $r\big(2^\gamma\big)=4$, $r\big(p_j^{\alpha_j}\big)=4(\alpha_j+1)$ y $r\big(q_j^{\alpha_j}\big)=2\big(1+(-1)^{\beta_j}\big)$. Concluye de todo ello que $r(n)=0$ excepto si todos los β_j son pares, en cuyo caso

$$r(n)=4(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1).$$

Por ejemplo, $r(2050)=4(2+1)(1+1)=24$ debido a la factorización $2\cdot 5^2\cdot 41$ que no contiene ningún q_j (consideramos que $\beta_j=0$ es par) y $\gamma=1$, $\alpha_1=2$, $\alpha_2=1$. La fórmula anterior también se puede obtener estudiando la factorización única en $\mathbb{Z}[i]$, el anillo de *enteros gaussianos*, [3, §5.5].

Para la segunda aplicación, recuerda de la primera hoja que habíamos definido $\zeta(s)$ como una serie que convergía para $\Re(s)>1$ y después dedujimos que admitía una extensión meromorfa a $\Re(s)>0$ con un único polo (simple de residuo 1) en $s=1$. Ahora completaremos esta extensión a todo $\mathbb{C}$ y, sobre todo, veremos que admite una simetría insospechada que también involucra la función Γ. Esto tiene consecuencias importantes acerca de la distribución de los números primos. Analizarlas con detalle llevaría a un TFG distinto del tuyo. Aquí solo presentaremos la relación con la conjetura más famosa del área.

Hay muchas pruebas de la extensión meromorfa y de la simetría de ζ. En los siguientes ejercicios seguiremos la original de Riemann en su famosa memoria [4, §8], [5]. Con este fin, introducimos la función $\omega:\mathbb{R}^+\longrightarrow\mathbb{R}$ definida por

$$\omega(x)=\sum_{n=1}^{\infty}e^{-\pi n^2x}.$$

Esta función es *de decaimiento rápido*[1] en $\mathbb{R}^+$, aunque no hace falta que lo pruebes.

4) Con lo que sabes de la hoja anterior, muestra que ω satisface

$$\omega(x^{-1})=\frac{\sqrt{x}-1}{2}+\sqrt{x}\,\omega(x)\qquad\text{para cualquier } x>0.$$

El siguiente paso es comprobar que las funciones ζ y Γ de la primera hoja están relacionadas con ω, asociada a la segunda hoja.

5) Sea $\xi(s)=s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s)$. Utilizando la serie que define ζ y la representación integral de Γ, demuestra para $\Re(s)>1$

$$\xi(s)=s(1-s)\int_0^\infty x^{s/2-1}\omega(x)\,dx.$$

[1] Se dice que una función es de decaimiento rápido si es C^∞ y ella y sus derivadas de cualquier orden tienden a cero cuando $x\to\infty$ al multiplicar por x^N, sea cual sea N.

Efectuando el cambio $x \mapsto 1/x$ en el intervalo $(0,1]$ del rango de integración, deduce también

$$\xi(s) = -1 + s(1-s)\int_1^\infty \big(x^{s/2-1} + x^{(1-s)/2-1}\big)\omega(x)\,dx.$$

6) A partir de la expresión anterior, demuestra los siguientes puntos:

1. $\xi(s)$ se extiende a una función entera.
2. $\zeta(s) - 1/(s-1)$ se extiende a una función entera y $\zeta(0) = -1/2$.
3. Se cumple $\xi(s) = \xi(1-s)$ para todo $s \in \mathbb{C}$.

El último punto es la simetría que buscábamos, lo que se llama *la ecuación funcional* por antonomasia. Permite relacionar $\zeta(s)$ y $\zeta(1-s)$.

La función ζ tiene una estrecha conexión con la distribución de los primos que se manifiesta a través de sus ceros. Lo realmente difícil no es tanto establecerla (se conoce desde Riemann), sino entender la localización de los ceros, que es todavía un problema abierto. Dicha conexión, que no probaremos aquí (mira [2, §5] o [1, §1.4] si quieres ver un esbozo de la demostración), se resume en lo siguiente:

Sean $\sigma_0 = \sup\big\{\Re(\rho) \,:\, \zeta(\rho) = 0\big\}$ *y* $\mathrm{Li}(N) = \int_2^N \frac{dt}{\log t}$, *entonces*

$$\lim_{N\to\infty} \frac{\#\{p \text{ primo} \,:\, p \le N\} - \mathrm{Li}(N)}{N^\sigma} = 0 \qquad \text{para cualquier } \sigma > \sigma_0.$$

Además el límite no existe para ningún $\sigma < \sigma_0$.

En otras palabras, σ_0 coincide con el orden con el que $\mathrm{Li}(N)$ aproxima a la cantidad de números primos hasta N. Aunque $\mathrm{Li}(N)$ tenga una forma integral no expresable en términos de funciones elementales, es una función suave y monótona, llamada *logaritmo integral*, fácil de tabular con métodos numéricos, bien lejos del comportamiento caótico individual de los primos.

7) Sabiendo que $\zeta(s)$ tiene ceros en $0 \le \Re(s) \le 1$ (de hecho infinitos, esto viene de una aplicación del principio del argumento [4, §15]), demuestra que $\sigma_0 \ge 1/2$ y que en el caso $\sigma_0 = 1/2$, correspondiente a la mejor aproximación de la cantidad de primos, todos los ceros en $0 \le \Re(s) \le 1$ deben estar en la línea vertical $\Re(s) = 1/2$. Esto es lo que se llama *hipótesis de Riemann*, porque Riemann mencionó tal posibilidad en su memoria. Según algunos, es el problema abierto más importante de las matemáticas.

La última aplicación es una prueba de lo que se llama la *ley de reciprocidad cuadrática*, un sorprendente resultado sobre congruencias que conjeturó Euler y probó Gauss. Entre sus consecuencias está el diseño de un algoritmo efectivo para saber si una ecuación cuadrática

tiene solución módulo un entero. Para su enunciado se suele introducir el *símbolo de Legendre* que para $n \in \mathbb{Z}$ y p primo $p \nmid n$ se define como

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv n \ (p) \ \text{ tiene solución,} \\ -1 & \text{si } x^2 \equiv n \ (p) \ \text{ no tiene solución.} \end{cases}$$

La ley de reciprocidad cuadrática afirma que si p y q son primos distintos entre sí y distintos de 2, se cumple

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

En breve, que hay una relación entre la solubilidad de $x^2 \equiv p \ (q)$ y la de $x^2 \equiv q \ (p)$, lo cual es muy sorprendente porque, en principio, las congruencias con diferentes módulos no tienen absolutamente nada que ver.

En lo sucesivo, sin recordarlo cada vez, supondremos que p y q son como en el enunciado anterior ($p, q > 2$ primos distintos). En la prueba que seguiremos aquí, serán importantes las llamadas *sumas de Gauss* que definimos para cada fracción irreducible M/N, $M \in \mathbb{Z}$, $N \in \mathbb{Z}^+$, como

$$G(M/N) = \sum_{k=0}^{N-1} e^{2\pi i k^2 M/N}.$$

Los siguientes ejercicios son más difíciles que los anteriores. Si las indicaciones no son suficientes, pídeme ayuda. Los tres primeros muestran que de la evaluación de las sumas de Gauss $G(1/N)$ con N impar se obtiene la ley de reciprocidad cuadrática. El resto muestran que tal evaluación se deduce de una de las propiedades de la función θ.

8) Si $\left(\frac{q}{p}\right) = 1$ explica por qué $G(q/p) = G(1/p)$. Si $\left(\frac{q}{p}\right) = -1$ prueba que

$$q(\pm 1)^2,\ q(\pm 2)^2,\ \ldots,\ q\Big(\pm\frac{p-1}{2}\Big)^2,\ 0,\ (\pm 1)^2,\ (\pm 2)^2,\ \ldots,\ \Big(\pm\frac{p-1}{2}\Big)^2$$

dan todas las clases módulo p sin repeticiones cuando se fija uno de los dos signos. Deduce de ello $2\sum_{k=0}^{p-1} e^{2\pi i k/p} = G(q/p) + G(1/p)$. Concluye $G(q/p) = \left(\frac{q}{p}\right) G(1/p)$. Indicación: Una vez probado que las clases son distintas, necesariamente son todas porque $\frac{p-1}{2} + 1 + \frac{p-1}{2} = p$.

9) Demuestra $G(p/q)G(q/p) = G\big(1/(pq)\big)$. Indicación: Después de algunas manipulaciones multiplicando las sumas, esto se reduce a entender que si k_1 recorre todos los residuos módulo p y k_2 recorre todos los residuos módulo q, entonces la expresión $qk_1 + pk_2$ recorre todos los residuos módulo pq [6, Th. 5.1].

10) Prueba la ley de reciprocidad cuadrática suponiendo que para $N \in \mathbb{Z}^+$ impar $G(1/N) = \sqrt{N} e^{\pi i (N-1)^2/8}$. Indicación: Nota que esto es $i\sqrt{N}$ si $N \equiv 3 \ (4)$ y $\sqrt{N}$ si $N \equiv 1 \ (4)$.

Los ejercicios restantes están dedicados a esta evaluación de $G(1/N)$. Utilizaremos la función θ. Para aligerar un poco la notación y de paso para distinguir $q = e^{\pi i \tau}$ del primo q, tomaremos como segundo argumento τ en lugar de q. Es decir, consideramos

$$\vartheta(z,\tau) = \theta\big(z, e^{i\pi\tau}\big).$$

11) Demuestra que, para M/N como antes (fracción irreducible, $N>0$) y $\varepsilon > 0$

$$\vartheta\big(0, \frac{2M}{N} + i\varepsilon^2\big) = \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i k^2 M/N} \sum_{\ell=0}^{N-1} e^{-2\pi i k\ell M/N}\vartheta\big(\frac{\ell M}{N}, i\varepsilon^2\big).$$

Aplicando (2) de la hoja anterior al segundo miembro, deduce que

$$\frac{G(M/N)}{N} = \lim_{\varepsilon\to 0^+} \varepsilon\,\vartheta\big(0, \frac{2M}{N} + i\varepsilon^2\big) \qquad \text{y} \qquad G(1/N) = 2\lim_{\varepsilon\to 0^+} \varepsilon\,\vartheta\big(0, \frac{2}{N} + \frac{4i\varepsilon^2}{N^2}\big)$$

Indicación: Aunque la primera identidad sea muy aparatosa, después de sustituir la definición de $\vartheta\big(\frac{\ell M}{N}, i\varepsilon^2\big)$ como una suma en n, se reduce a intercambiar el orden de las sumas en ℓ y n y a usar que $\sum_{\ell=0}^{N-1} e^{2\pi i a\ell/N}$ es cero si $N \nmid a$. Para la segunda parte, al aplicar (2) todos los límites salen nulos excepto el correspondiente a $\ell = 0$. El segundo límite es consecuencia del primero.

12) Prueba finalmente la cadena de igualdades para $N \in \mathbb{Z}^+$ impar:

$$\frac{G(1/N)}{\sqrt{N}} = (1+i)\lim_{\varepsilon\to 0^+} \varepsilon\,\vartheta\big(0, -\frac{N}{2} + i\varepsilon^2\big) = \frac{1+i}{4} G(-N/4) = e^{\pi i (N-1)^2/8}.$$

Indicación: Para la primera igualdad hay que transformar $\vartheta\big(0, \frac{2}{N} + \frac{4i\varepsilon^2}{N^2}\big)$ con (2) de la hoja anterior, pero no sale exactamente $\vartheta\big(0, -\frac{N}{2} + i\varepsilon^2\big)$ sino algo parecido. Para justificar que no afecta al límite puedes usar que si $|f(\varepsilon)| \le K\varepsilon^4$ entonces existe un K' tal que $\big|1 - e^{n^2 f(\varepsilon)}\big| \le K'\varepsilon\, e^{\pi n^2\varepsilon^2/2}$ para cualquier $0 < \varepsilon < \sqrt{\pi/(2K)}$.

Por si tienes interés, la desigualdad de la indicación anterior para $n \le \varepsilon^{-2}$ se sigue por Taylor aplicado a $1 - e^x$ porque $n^2\varepsilon^2 \le e^{\pi n^2\varepsilon^2/2}$ y para $n \ge \varepsilon^{-2}$ se sigue de que $\varepsilon^{-1}\exp\big(|K| - \frac{1}{2}\pi\varepsilon^{-2}\big)$ está acotada para $\varepsilon > 0$.

Tarea a entregar. Debes escribir un documento que combine las soluciones de los ejercicios anteriores. Trata de no pasarte de 7 páginas con el formato de esta hoja. El resultado conformará el tercer capítulo de tu TFG bajo el nombre *Algunas aplicaciones* o la variante que prefieras. Sé que la parte de la ley de reciprocidad cuadrática es dura. Si no consigues ajustarla a un espacio razonable, podemos llegar a un acuerdo sobre algunas reducciones. Por ejemplo cambiándola a una evaluación de $G(1/N)$ sin referencia a la ley de reciprocidad cuadrática.

Referencias

[1] F. Chamizo. Ocho lecciones de teoría de números. https://matematicas.uam.es/~fernando.chamizo/libreria/fich/lecc8.pdf, 2011.

[2] F. Chamizo. Convergencia de funciones holomorfas. https://matematicas.uam.es/~fernando.chamizo/asignaturas/1819vcII/resumenes/cnv.pdf, 2019.

[3] J. Cilleruelo and A. Córdoba. *La teoría de los números*. Biblioteca Mondadori. Mondadori España, Madrid, 1992.

[4] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by H. L. Montgomery.

[5] H. M. Edwards. *Riemann's zeta function*. Pure and Applied Mathematics, Vol. 58. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1974.

[6] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin-New York, 1982. Translated from the Chinese by P. Shiu.

[7] Wikipedia contributors. Lambert series — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Lambert_series&oldid=1183921576, 2023. [Online; accessed 15-November-2023].