Una identidad curiosa e importante

En julio de 2014 tuvo lugar en el IHÉS el encuentro *École d'été 2014 Théorie analytique des nombres*. Los vídeos están disponibles en el canal de YouTube del IHÉS. En este curso de verano algunos de los protagonistas de la teoría analítica de números moderna dieron charlas sobre temas no demasiado específicos a un nivel asequible para estudiantes graduados (a juzgar por los vídeos que he tenido la oportunidad de ver hasta ahora). En uno de ellos, *Sifting for primes*, el orador, H. Iwaniec, escribe en la pizarra la siguiente fórmula:

$$-\sum_d g(d)\mu(d)\log d = \prod_p \big(1-g(p)\big)\big(1-\frac{1}{p}\big)^{-1} \tag{1}$$

donde g es una función multiplicativa y, como es habitual, μ representa la función de Möbius, en la primera suma d recorre $\mathbb{Z}^+$ y en el producto p recorre los primos. Inmediatamente (minuto 19 en el vídeo), A. Granville duda de esta fórmula. Sus palabras me resultan inaudibles en su mayoría y además participan otras personas en la audiencia sin micrófono, por tanto lo siguiente no es una transcripción y las intervenciones marcadas con [*] son incompletas, aproximadas y no de la misma persona. Con estas precauciones, la conversación que siguió a la duda y a una breve réplica fue la siguiente:

> [*] –*No es cierta.*
> [I] –*¿No es cierta?*
> [*] –*El producto de Euler no es correcto. Tienes* $\log d$.
> [I] –*Es cierta porque está en mis notas* [risas].
> [*] –*Tienes una función multiplicativa por* $\log d$. [...] *Es correcto si es convergente* [otra persona].
> [I] –*Yo no digo que sea directo a partir del producto de Euler. Mirad, esto no es multiplicativo* [la parte interior de la suma]. *Sin* $\log d$ *debería ser* $\big(1-g(p)\big)$ *sin esto* [señalando al último factor de la fórmula]. *Andrew, es hora de despertarse. Seguro que me vais a pillar en algo incorrecto enseguida, así que tengo que ser cuidadoso porque podéis vengaros rápidamente. Esto solamente es cierto cuando* $g(p)$ *es como* $1/p$ *en media.*

La queja de Granville es muy razonable porque si pensamos en qué saldría al operar el producto en (1), parece bien diferente del primer miembro. Es decir, no es que la identidad parezca difícil, es que parece falsa. ¿Sabrías probarla sin seguir leyendo? Venga, al menos garabatea un poco en un papel.

Unas líneas sobre productos de Euler

Si f es una función aritmética multiplicativa entonces formalmente (sin atender a cuestiones de convergencia)

$$\sum_d f(d) = \prod_p \big(1+f(p)+f(p^2)+f(p^3)+\dots\big).$$

La prueba se reduce a multiplicar el segundo miembro para obtener un montón (infinitos) sumandos del tipo $f\big(p_1^{\alpha_1}\big)f\big(p_2^{\alpha_2}\big)\cdots f\big(p_k^{\alpha_k}\big)$ que coinciden con $f\big(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\big)$, por ser f multiplicativa, y basta apelar al teorema fundamental de la aritmética.

En relación con la identidad que nos ocupa, si tomamos $f(d)=\mu(d)g(d)$, se sigue (1) sin $-\log d$ en el primer miembro y sin $\big(1-p^{-1}\big)^{-1}$ en el segundo, como sugiere el orador. Parece bastante raro que introducir el producto de $\big(1-p^{-1}\big)^{-1}$, que por cierto no converge, haga aparecer un logaritmo.

Eligiendo la función $f(d)=d^{-s}g(d)$ donde g es multiplicativa y s es un parámetro libre, se deduce la forma habitual del *producto de Euler*

$$\sum_{n=1}^{\infty}\frac{g(n)}{n^s}=\prod_p\big(1+\frac{g(p)}{p^s}+\frac{g(p^2)}{p^{2s}}+\frac{g(p^3)}{p^{3s}}+\dots\big).$$

Por ejemplo, con $g(n)=1$ y con $g(n)=\mu(n)$, tenemos respectivamente

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\big(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots\big)=\prod_p\big(1-p^{-s}\big)^{-1}\qquad\text{y}\qquad\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\prod_p\big(1-p^{-s}\big).$$

Una vez extendida analíticamente, la primera suma es la famosa función ζ de Riemann y la identidad es crucial para estudiar la distribución de los primos. La segunda coincide, por tanto, con $1/\zeta(s)$. Estas fórmulas dan lugar a algunas identidades curiosas, por ejemplo, para $s=2$ se sigue $\sum\mu(n)n^{-2}=6/\pi^2$. Como notó L. Euler, $s=1$ junto con $\zeta(1)=\infty$ implica que hay infinitos primos. Sin embargo, hay que tener precaución al tratar con series no convergentes (Euler tendría problemas en los exámenes de Variable Real). Por ejemplo, formalmente con $s=1$ también se sigue $\sum\mu(n)n^{-1}=0$ pero si hubiera una forma fácil de probar esto sin suponer de antemano la convergencia, también tendríamos una prueba sencilla del teorema de los números primos [MV07].

La prueba sin prestar atención a la convergencia

Consideremos la función

$$F(s)=\prod_p\big(1-g(p)p^{-s}\big)=\sum_{d=1}^{\infty}\frac{\mu(d)g(d)}{d^s}.$$

Si tienes problemas en entender la segunda igualdad, es que no has leído el apartado anterior. La motivación es que si nos creemos que se puede derivar la serie término a término, el primer miembro de (1) coincide con

$$F'(0)=-\sum_d g(d)\mu(d)\log d \tag{2}$$

y la estrategia es calcular $F'(0)$ de otra forma usando el producto de Euler de F debidamente maquillado para la ocasión. Comenzamos escribiendo una identidad tonta:

$$F(s)=P(s)Q(s) \tag{3}$$

donde

$$P(s)=\prod\left(1-p^{-s-1}\right)\qquad\text{y}\qquad Q(s)=\prod_p\frac{1-g(p)p^{-s}}{1-p^{-s-1}}.$$

La gracia es que el segundo miembro de (1) es $Q(0)$.

También se tiene la definición alternativa

$$Q(s)=\prod_p\Big(1+\frac{1/p-g(p)}{p^s}+\frac{1/p^2-g(p)/p}{p^{2s}}+\frac{1/p^3-g(p)/p^2}{p^{3s}}+\dots\Big). \tag{4}$$

La prueba está al alcance de cualquiera que no sea perezoso y sepa sumar progresiones geométricas.

Ahora derivamos la factorización (3) en $s=0$, con la falta de cuidado habitual,

$$F'(0)=P'(0)Q(0)+P(0)Q'(0). \tag{5}$$

Sabemos del apartado anterior que $P(s)=1/\zeta(s+1)$ y utilizando el desarrollo de Laurent $\zeta(s+1)=s^{-1}+\gamma s+\dots$ [Ivi03], se deduce $P(0)=0$ y $P'(0)=1$. Si $g(p)$ se parece a $1/p$, el producto en (4) convergerá muy bien y en un entorno de 0 definirá una función derivable, asegurando la existencia de $Q'(0)$. Recordando (2), se obtiene la identidad (1) en la forma $F'(0)=Q(0)$.

Unas palabras sobre los detalles técnicos

Hemos utilizado fundamentalmente la identidad (5) pero todos los términos que participan en ella están bajo sospecha por la falta de convergencia. Una forma de proceder para esconder los no infinitos bajo la alfombra, es considerar una forma regularizada

$$F'(s)=P'(s)Q(s)+P(s)Q'(s).\qquad\text{con } s>0$$

y después hacer tender s a cero por la derecha. El producto $P(s)=1/\zeta(s+1)$ converge bien y podemos justificar $P(s)\to 0$ y $P'(s)\to 1$ cuando $s\to 0^+$.

Por otro lado deberíamos justificar que en (2) se puede reemplazar el primer miembro por el límite de $F'(s)$. Para ello se necesita algún tipo de teorema de los números primos para g, alguna cuantificación de la cancelación en las sumas parciales de $g(d)\mu(d)\log d$. Es ahí donde entra que $g(p)$ se parece a $1/p$, pues $\sum d^{-1}\mu(d)\log d=-1$. En el Corolario A.12 de [FI10] hay una estimación en este sentido bajo cierta condición [FI10, (A.54)] que refleja el comportamiento similar de $1/p$ y de $g(p)$ en media y que en el lenguaje de los métodos de criba se relaciona con que la *dimensión* de la criba sea 1.

Con $Q(s)$ el problema se resuelve de manera similar. Tomando logaritmos, el control sobre las sumas de $1/p-g(p)$ se traduce en un control sobre la velocidad de convergencia de la serie. Sólo para ilustrar este punto, nótese que si $\left|g(p)-p^{-1}\right|<Cp^{-\alpha}$ para algún $\alpha>1$ entonces $Q(s)$ definiría una función holomorfa en un entorno de cero.

Cómo estimar la cantidad de primos en una sucesión razonable

Ahora veremos por qué (1) es importante. Permite hacer algo fundamental que los matemáticos deberíamos practicar más a menudo: enunciar cosas que no sabemos probar.

Consideremos un conjunto de enteros positivos $\mathcal{A} = \{a_1, a_2, a_3, \dots\}$. Nuestro propósito es estimar la cantidad de primos en $\mathcal{A}$ menores que cierto número (grande) dado. Por razones técnicas es mejor contar también potencias de primos. La hipótesis fundamental es que para cada d fijo libre de cuadrados

$$\lim_{N\to\infty} \frac{\#\{a_n \le N \ : \ d \mid a_n\}}{\#\{a_n \le N\}} = g(d) < 1 \qquad \text{con } g \text{ multiplicativa,}$$

complementada con la hipótesis de que $g(p)$ se parezca en media a $1/p$. Una condición concreta en este sentido es la ya citada [FI10, (A.54)]. El lector interesado debe hacer el ejercicio (físico) de ir a la biblioteca y abrir el libro.

¿Por qué estas hipótesis son naturales en sucesiones "razonables"? La primera dice que hay independencia en las probabilidades $g(d_1)$ y $g(d_2)$ de que un a_n escogido al azar sea divisible por d_1 y por d_2 cuando d_1 y d_2 no tienen nada que ver, cuando son coprimos. Si permitiéramos, por ejemplo, que a_n fuera divisible por 3 siempre que lo fuera por 2, de forma que $g(2)g(3) \neq g(6)$, entonces la información sobre $g(p)$, la única que aparece en el segundo miembro de (1), sería insuficiente para resolver el problema planteado. Respecto al comportamiento en media de $g(p)$, refleja que al elegir números al azar, típicamente uno de cada d será divisible por d.

La fórmula

$$\Lambda(n) = -\sum_{d\mid n} \mu(d)\log d \qquad \text{con} \qquad \Lambda(n) = \begin{cases} \log p & \text{si } n = p^k,\ k \in \mathbb{Z}^+ \\ 0 & \text{en otro caso} \end{cases} \tag{6}$$

es elemental y bien conocida [IK04, §1.4]. De ella se deduce

$$\sum_{a_n\le N} \Lambda(a_n) = -\sum_{a_n\le N}\sum_{d\mid a_n} \mu(d)\log d = -\sum_{d\le N} \mu(d)(\log d)\#\{a_n \le N \ : \ d \mid a_n\}.$$

Si dividimos entre $\#\{a_n \le N\}$ y soñamos que es posible intercambiar el límite con la suma, empleando (1) se obtiene la fórmula conjetural

$$\lim_{N\to\infty} \frac{\sum_{a_n\le N} \Lambda(a_n)}{\#\{a_n \le N\}} = \prod_p \big(1 - g(p)\big)\big(1 - p^{-1}\big)^{-1}. \tag{7}$$

¿Cómo que conjetural? ¿Es tan difícil justificar en el siglo XXI el intercambio de la suma y el límite? Sólo cabe un sí rotundo cuando contemplamos las consecuencias de (7) que incluyen a la conjetura de los primos gemelos y otros problemas abiertos bien conocidos. A pesar de que parece que sólo tenemos que solventar una cuestión analítica técnica, está estrechamente relacionada con la "ley del azar de Möbius" [IK04, §13.1] [Sar12] que ni es ley ni tiene un enunciado muy concreto pero decididamente es fundamentalmente aritmética.

Las ideas que conducen a (7) son reminiscentes de la *criba asintótica* de E. Bombieri [Bom76] [FI10, Ch.3]. La diferencia con la criba clásica es que, en vez de (6), en ésta se usa $\sum_{d|(n,Q)} \mu(d)$ y uno intenta ajustar Q como producto de muchos primos para que esta función aritmética detecte primos mayores.

Un primer ejemplo de juguete consiste en tomar $\mathcal{A} = \mathbb{Z}^+$. Entonces $g(d) = 1/d$ y se sigue

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} \Lambda(n) = \prod_p \big(1-p^{-1}\big)\big(1-p^{-1}\big)^{-1} = 1$$

que es una de las formas del teorema de los números primos.

Tomamos ahora como ejemplo "de verdad" $\mathcal{A} = \big\{p+2 \ : \ p \text{ es primo}\big\}$. En este caso para d impar

$$\lim_{N\to\infty} \frac{\#\big\{p+2\le N \ : \ d \mid p+2\big\}}{\#\big\{p+2\le N\big\}} = \lim_{N\to\infty} \frac{\pi(N-2;d,-2)}{\pi(N-2)} = \frac{1}{\phi(d)}$$

donde se ha usado el teorema de los números primos en progresiones aritméticas (véase el enunciado y la notación en [Dav80]). Si d es par el límite es claramente nulo porque $p+2$ es siempre impar si $p \neq 2$. Sustituyendo en (7), cambiando N por $N+2$ y aplicando de nuevo el teorema de los números primos,

$$\lim_{N\to\infty} \frac{\log N}{N} \sum_{p\le N} \Lambda(p+2) = \big(1-\frac{1}{2}\big)^{-1} \prod_{p>2} \big(1-\frac{1}{p-1}\big)\big(1-p^{-1}\big)^{-1}.$$

La contribución de los $p+2$ que son potencias de primo pero no primos es despreciable con la estimación trivial. De esta forma $\Lambda(p+2)$ se puede reemplazar por la función que vale $\log(p+2)$ si $p+2$ es primo y se anula en otro caso. Con técnicas de sumación por partes [CC92, II] [Mur08, 2], el logaritmo, que es casi constante, se puede sacar de la suma como $\log N$ para obtener

$$\lim_{N\to\infty} \frac{(\log N)^2}{N} \#\big\{p\le N \ : \ p+2 \text{ es primo}\big\} = 2\prod_{p>2} \big(1-(p-1)^{-2}\big).$$

Lo cual es una versión fuerte de la conjetura de los primos gemelos. Fórmulas de este tipo fueron conjeturadas por G.H. Hardy y J.E. Littlewood por medio del método del círculo [HL23, §5]. Comparativamente, la deducción de (7) a partir de (1) es más simple.

Un ejercicio

Se deja al aburrido lector que aplique las ideas anteriores para justificar la conjetura

$$\lim_{N\to\infty} \frac{\log N}{N} \#\big\{n\le N \ : \ n^2+1 \text{ es primo}\big\} = \prod_{p>2} \Big(1-\frac{(-1)^{(p-1)/2}}{(p-1)^2}\Big).$$

De ello se deduciría que existen infinitos primos de la forma n^2+1, lo cual es uno de los cuatro famosos problemas relativos a los primos que planteó E. Landau en el Congreso

Internacional de Matemáticas de 1912. Ninguno de ellos se ha resuelto todavía y todos menos uno se deducen de (7) o sus variantes.

Si todavía te ronda en la cabeza lo de la suma y el límite, al menos para el caso de los primos gemelos, preferiblemente piénsalo sólo hasta los 40, porque después ya no dan la medalla Fields.

Referencias

[Bom76] E. Bombieri. The asymptotic sieve. *Rend. Accad. Naz. XL (5)*, 1/2:243–269 (1977), 1975/76.

[CC92] J. Cilleruelo and A. Córdoba. *La teoría de los números*. Biblioteca Mondadori. Mondadori España, Madrid, 1992.

[Dav80] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. Revised by Hugh L. Montgomery.

[FI10] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[HL23] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.

[IK04] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Ivi03] A. Ivić. *The Riemann zeta-function*. Dover Publications Inc., Mineola, NY, 2003. Theory and applications, Reprint of the 1985 original [Wiley, New York; MR0792089 (87d:11062)].

[Mur08] M. R. Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[Sar12] P. Sarnak. Mobius randomness and dynamics. *Not. S. Afr. Math. Soc.*, 43(2):89–97, 2012.