ABC, 3 de Noviembre de 2017
CIENCIA - El ABCdario de las matemáticas
Alfonso Jesús Población Sáez

La explicación al descubrimiento de dos teóricos de los números que incluye dulces glaseados, curvas elípticas y la teoría de las locuras mostruosas

En un donut real, se percibe dónde están los confites. Sin embargo, si estuviéramos a oscuras no lo sabríamos sin tocarlo. Eso es lo que pasa con las curvas elípticas, que no sabemos dónde están dispuestos esos dulces (los puntos racionales), pero probablemente gracias al grupo de O'Nan sea más fácil descubrirlos

El pasado mes de septiembre algunos medios de divulgación norteamericanos se hicieron eco de una “sorprendente” noticia comunicada por los especialistas en teoría de números **Ken Ono y John Duncan**, de la Universidad Emory, institución privada de Atlanta, en el estado de Georgia.

En su afán por hacer entendible a la sociedad el contenido de resultados técnicos, los redactores suelen intentar relacionar las noticias científicas con aplicaciones a nuestra vida cotidiana o a objetos familiares, y tratar de comprimirlo en el reducido espacio de texto que consideran apropiado antes de que el lector se canse y deje de leerlo para pasar a otra cosa más interesante o que al menos entienda. En definitiva, sin mayores explicaciones, y como suele decirse, acaba siendo peor el remedio que la enfermedad, ya que se monta un batiburrillo tal, que ni siquiera un especialista es capaz de reconocer algo medianamente ininteligible. En el caso que nos ocupa, se mezclaban **dónuts glaseados con chispitas de colores**, con el **grupo de O’Nan**, los parias, **las curvas elípticas**, la **teoría de las locuras monstruosas**, etc., y encima lo útil que resulta todo ello. Imaginen.

Ken Ono y John Duncan, de la Universidad Emory, posan frente a sus ordenadores con unos donuts de colores e

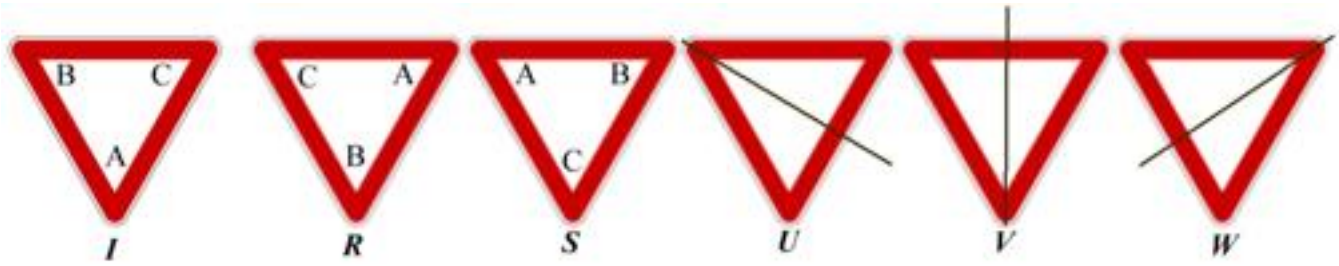
Stephen Nowland

Empecemos por el principio. Como saben, las matemáticas han ido evolucionando a lo largo de la historia, yendo de lo particular (casos concretos) a lo más general. Los famosos teoremas, proposiciones, corolarios, lemas, etc., que conforman las diferentes disciplinas matemáticas (que sólo tienen validez y adquieren esas denominaciones después de una correcta y rigurosa demostración formal) son resultados lo más general y abstractos posibles, aplicables a multitud de situaciones que verifiquen las hipótesis correspondientes.

En nuestra vida real también se hace algo parecido continuamente: un médico examina a un paciente para detectar unos determinados síntomas (es decir, comprueba las hipótesis que tiene) antes de aplicarle tal o cual tratamiento (el teorema correspondiente); un fontanero observa la avería (las hipótesis) antes de aplicar el remedio con las herramientas más apropiadas (los teoremas). El álgebra abstracta surge a principios del siglo XX estudiando lo que llamamos estructuras algebraicas, que no son más que conjuntos de objetos a los que se les aplica una o varias operaciones, y que verifican determinadas propiedades (axiomas). Una de esas estructuras son los **grupos**. Se llama así a todo conjunto que con dicha operación (suma, producto, derivar y dividir, la que sea, pudiendo ser también una manipulación geométrica, en definitiva, cualquier transformación a los elementos del conjunto) verifica tres propiedades básicas: asociativa, existencia de elemento neutro o identidad, y existencia de elemento opuesto. Además, debe cumplir que, al operar dos objetos cualesquiera del conjunto, no nos salimos de él, es decir, que el resultado vuelve a ser un elemento del conjunto (ley de composición interna, en nuestra jerga específica). Si además da igual el orden en el que operemos dos elementos cualesquiera (primero uno y luego el otro, o al revés), el grupo es además conmutativo o abeliano (en honor al matemático noruego
Niels Henrik Abel
).

Vale, eso es un grupo, ¿y para qué lo definimos? Pues porque resulta que existen muchísimos conjuntos, en los más dispares contextos, que junto a la operación que les dota de esa estructura, se comportan todos del mismo modo. Por ejemplo, la estructura de grupo subyace en la comprensión de las simetrías (y éstas aparecen en los más variopintos lugares, desde composiciones artísticas, a la estructura interna de los átomos de los elementos químicos, por poner dos situaciones evidentes; o de nuevo en la seguridad de nuestras tarjetas de crédito, o en los métodos de resolución de juegos como el cubo de Rubik). Y los especialistas en teoría de grupos han descubierto y desarrollado muchos teoremas que pueden aplicar a cualquiera de estas estructuras para entender su comportamiento, o para resolver las situaciones en las que aparezcan.

Vamos a ver un ejemplo concreto de grupo, muy sencillo, enmarcado precisamente en la simetría. Tomemos la conocida señal de tráfico de ceda el paso (un triángulo corriente con el vértice hacia abajo). Si giramos la señal 120º, 240º o 360º, a nuestros ojos la señal queda tal y como la vemos, como si no hubiéramos hecho nada sobre ella (tiene simetría rotacional), aunque la hemos aplicado tres operaciones diferentes, tres giros. Para verificar esos giros etiquetemos los vértices con letras, llamando a esas rotaciones I (giro de 360º; lo deja como está, es la identidad), R (giro de 120º), S (giro de 240º). ¿Qué sucede al combinar dos de esas operaciones? Por ejemplo, si hacemos un giro de 240º y luego uno de 120º (matemáticamente se denota por S ∘ R), evidentemente el resultado es el mismo que girar 360º, por lo que escribiríamos S ∘ R = I. De un modo similar podemos calcular todos los posibles pares de operaciones, y ordenarlos en una tabla, conocida como tabla de multiplicación, o tabla de Cayley (en honor al matemático **Arthur Cayley**).



∘	I	R	S
I	I	R	S
R	R	S	I
S	S	I	R

La tabla quedaría tal y como se ve en la imagen. Podemos comprobar que la señal de ceda el paso con estas tres operaciones es un grupo conmutativo sin más que observar dicha tabla: todas las posibles combinaciones de operaciones dan como resultado los tres elementos (I, R, S), hay un elemento identidad (I; al combinarlo con cualquiera de los demás, deja invariante el resultado), todos los elementos tienen un inverso (el que nos da la identidad; el inverso de S es R, y viceversa), no importa el orden en que se asocien tres elementos (propiedad asociativa, (a ∘ b) ∘ c = a ∘ (b ∘ c)), y tampoco dos a dos (conmutativa, a ∘ b = b ∘ a). El orden del grupo es 3, ya que tiene tres elementos.

$\circ$	I	R	S	U	V	W
I	I	R	S	U	V	W
R	R	S	I	V	W	U
S	S	I	R	W	U	V
U	U	W	V	I	S	R
V	V	U	W	R	I	S
W	W	V	U	S	R	I

[redacted]

$$J(r) = \frac{1}{} + 196884\,q + 21493760\,q^2 + 864299970\,q^3 + \ldots\ldots\ldots\ldots, \text{ con } q = e^{2\pi i r}$$

[redacted]

[redacted] Matemática Española (RSME) [redacted] Real Sociedad [redacted]