Geometría de los números

por

Rosario Clement Fernández, Universidad del País Vasco-Euskal Herriko Unibertsitatea

Leí hace poco un artículo del geómetra inglés Michael Atiyah sobre las Matemáticas del siglo XX . Afirmaba en él que entender el mundo que nos rodea es sobre todo entender lo que vemos, y que la intuición espacial es nuestra arma más poderosa. En su opinión esto explica el lugar central que ocupa la geometría dentro de las matemáticas: muchos problemas que no tienen nada que ver con la geometría se resuelven cuando uno es capaz de transformarlos en problemas geométricos. Seguía diciendo Atiyah que de hecho, en matemáticas, cuando uno deja de pensar geométricamente, deja uno de entender lo que está haciendo y únicamente hace cálculos.

Desde luego no estoy de acuerdo con esta última parte de la opinión de Atiyah: en el área de las matemáticas que conozco un poco, abundan los problemas que no tienen nada de geométricos ni en su planteamiento ni en su resolución. Sin embargo no pretendo polemizar aquí sobre este tema. Más bien al contrario, lo que voy a exponer a continuación ilustra perfectamente la primera parte de la tesis de Atiyah: veremos como ciertos problemas de teoría de números se pueden resolver de una forma muy sencilla geométricamente.

Las personas que iniciaron la parte de la teoría de números que hoy se conoce por

"Geometría de los Números" fueron Minkowski y Dirichlet. Minkowski, de hecho, fue el que acuñó este término: publicó un libro con ese título en 1896. Minkowski nació en Rusia en 1864, pero vivió casi toda su vida entre Suiza y Alemania, donde murió en 1909.

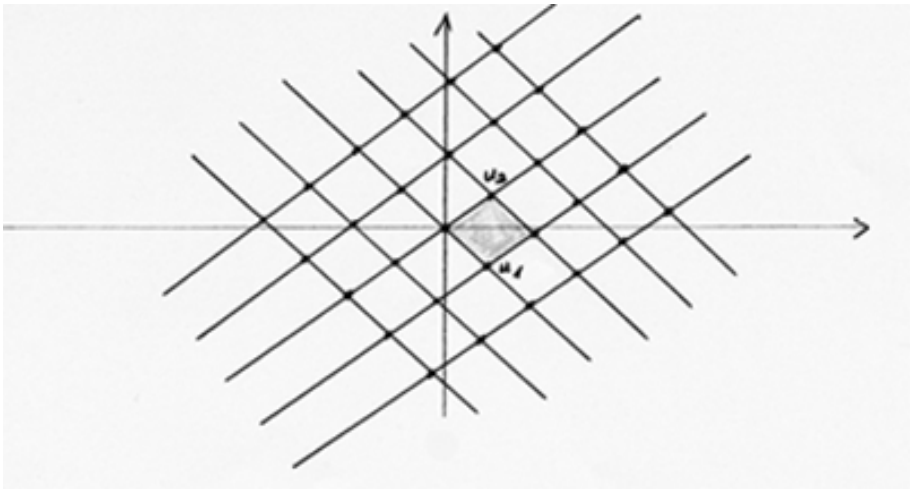
Interesado por un problema de formas cuadráticas, Minkowski probó un teorema que vamos a ver a continuación y que es esencialmente trivial; pero él mismo se dió cuenta de que este teorema tiene consecuencias nada triviales.

Recordemos brevemente algunas cosas:

Una **RED** en $\mathbb{R}^n$ es un $\mathbb{Z}$-módulo libre de rango n con una base formada por n vectores de $\mathbb{R}^n$ linealmente independientes. Es decir una red Γ es:

$$\Gamma = \{\lambda_1 u_1 + \cdots + \lambda_n u_n | \lambda_i \in \mathbb{Z}\},$$

siendo $u_1, \ldots, u_n$ vectores de $\mathbb{R}^n$ linealmente independientes. Por tanto, se tiene $\Gamma = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n$.



Un **Dominio Fundamental** de la red Γ es el paralelepípedo determinado por los vectores $u_1, \ldots, u_n$, es decir

$$D_\Gamma = \{\lambda_1 u_1 + \cdots + \lambda_n u_n \,|\, \lambda_i \in \mathbb{R}, \quad 0 \leq \lambda_i < 1\}.$$

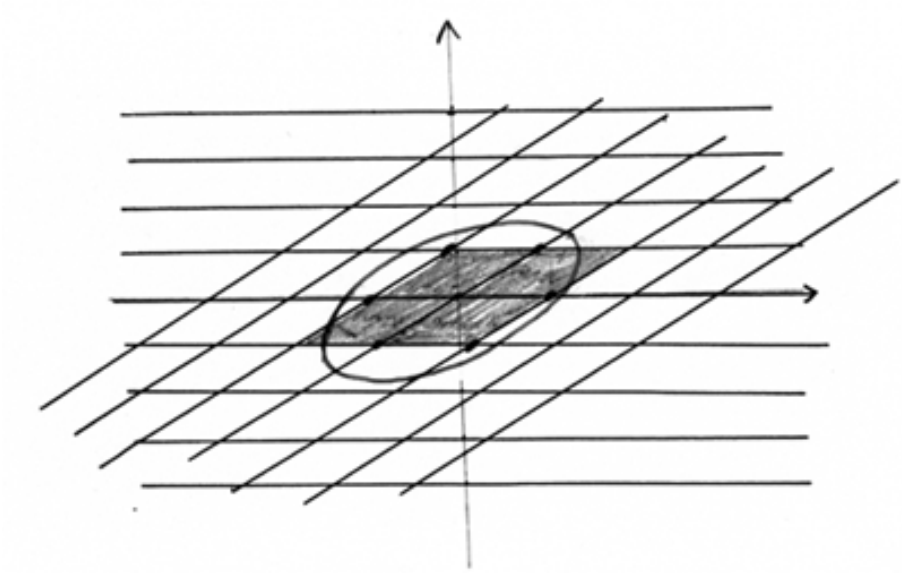
Se llama **Volumen de la red** Γ, $Vol(\Gamma)$, al volumen de un dominio fundamental D_Γ. Este volumen es por supuesto independiente de la base elegida para Γ como $\mathbb{Z}$-módulo: la matriz de paso de una base a otra de Γ como $\mathbb{Z}$-módulo tiene determinante igual a ± 1.

Teorema de Minkowski de los Cuerpos Convexos: *Sea Γ una red de $\mathbb{R}^n$ y $S \subset \mathbb{R}^n$ un conjunto medible con medida $\mu(S)$, simétrico respecto del origen y convexo.*

a) *Si $\mu(S) > 2^n Vol(\Gamma)$, entonces $S \cap \Gamma$ contiene algún punto distinto del origen.*

b) *Si S es además compacto, basta con que $\mu(S) \geq 2^n Vol(\Gamma)$ para poder asegurar lo mismo.*

Este teorema es totalmente intuitivo y muy sencillo de demostrar. Por ejemplo, en el caso $n = 2$, nos dice que si la medida de S es mayor que cuatro veces el volumen de Γ, entonces S contiene algún punto de la red distinto del origen.

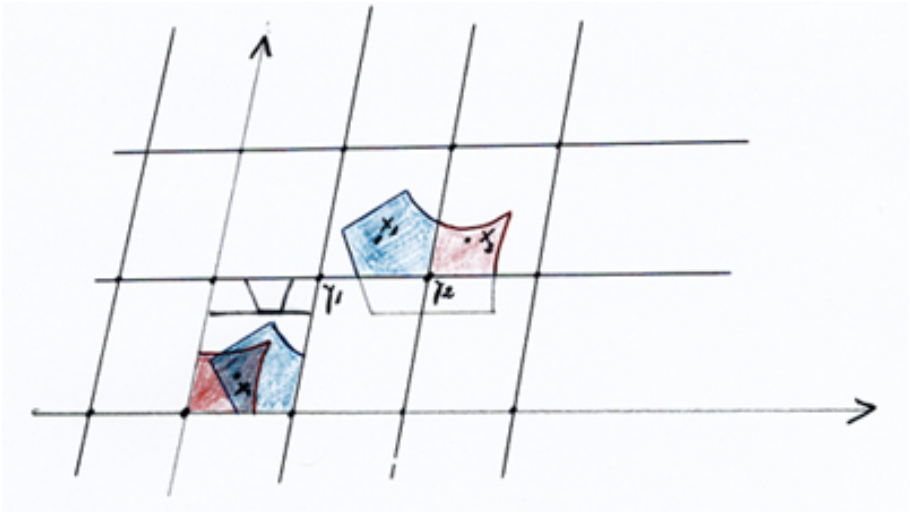


La demostración se basa en una idea muy sencilla: Para todo conjunto $S' \subseteq \mathbb{R}^n$ tal que

$$\mu(S') > Vol(\Gamma)$$

existen dos puntos distintos $x_1, x_2 \in S'$ tales que $x_1 - x_2 \in \Gamma$.

¿Como se prueba esto? Veámoslo primero en un ejemplo:



Tenemos aquí una red en $\mathbb{R}^2$ y un conjunto S' que interseca a cuatro cuadrículas; mediante una traslación por un elemento de la red cada una de estas cuadrículas va a parar al dominio fundamental de la red; las imágenes, dentro del dominio fundamental, de las cuatro partes que componen el conjunto S' no pueden ser disjuntas, pues, si lo fueran, la medida de S' sería menor o igual que la del dominio fundamental, es decir $\mu(S') \leq Vol(\Gamma)$, y esto es contrario a la hipótesis que tenemos. Por lo tanto existe $x = x_1 - \gamma_1 = x_2 - \gamma_2$. Deducimos que $x_1 - x_2 = \gamma_1 - \gamma_2 \in \Gamma$, como queríamos probar.

En general:

$$S' = \bigcup_{\gamma \in \Gamma} (S' \cap (\gamma + D_\Gamma)).$$

De donde:

$$\mu(S') = \sum_{\gamma \in \Gamma} \mu(S' \cap (\gamma + D_\Gamma)) = \sum_{\gamma \in \Gamma} \mu((-\gamma + S') \cap D_\Gamma).$$

Por ser $\mu(S) > Vol(\Gamma)$, necesariamente existen $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$, tales que $(-\gamma_1 + S') \cap (-\gamma_2 + S') \neq \phi$. Por tanto existen $x_1, x_2 \in S'$ tales que $-\gamma_1 + x_1 = -\gamma_2 + x_2$. De donde $x_1 - x_2 = \gamma_1 - \gamma_2$ está en Γ.

Podemos ahora demostrar rápidamente el teorema de Minkowski:

Ponemos $S' = \frac{1}{2}S$. S' es un conjunto de medida $\mu(S') = \frac{1}{2^n}\mu(S) > Vol(\Gamma)$. Por tanto existen $x_1, x_2 \in S'$ tales que $x_1 - x_2 \in \Gamma$. Pero $x_1 - x_2 = \frac{1}{2}(2x_1 - 2x_2)$.

Por supuesto $2x_1$ y $2x_2$ están en el conjunto S; por ser S simétrico $-2x_2 \in S$, y por ser convexo $\frac{1}{2}(2x_1 - 2x_2) \in S$. Luego $x_1 - x_2 \in \Gamma \cap S$.

Antes de hablar de alguna de las consecuencias que Minkowski dedujo del teorema que acabamos de probar, vamos a ver como este permite demostrar de forma sencilla algunos teoremas clásicos de la teoría de números.

Teorema de los dos cuadrados (Fermat): *Sea p un número primo. Entonces*

$$p = x^2 + y^2 \quad con \quad x, y \in \mathbb{Z} \Longleftrightarrow p = 2 \quad o \quad p \equiv 1 \bmod 4.$$

Es decir, los números primos que son suma de dos cuadrados son el 2 y los congruentes con 1 módulo 4. La implicación $\Rightarrow$ es trivial: basta con reducir módulo 4 y observar que en $\mathbb{Z}/4\mathbb{Z}$, las clases que son cuadrados son las clases $\overline{0}$ y $\overline{1}$.

Para probar la otra implicación consideramos un primo p congruente con 1 módulo 4 (el caso del 2 es evidente: $2 = 1^2 + 1^2$). Vamos a buscar una red $\Gamma \subseteq \mathbb{Z}^2 \subseteq \mathbb{R}^2$ tal que para todos los puntos $(x_1, x_2) \in \Gamma$ se verifique que $x_1^2 + x_2^2$ sea un múltiplo de p, y tal que se pueda aplicar el teorema de Minkowski a esa red y a la bola abierta $B(0, \sqrt{2p})$ centrada en el origen y con radio $\sqrt{2p}$. Si conseguimos una tal red, tenemos el teorema demostrado: por el teorema de Minkowski existe un punto $(x_1, x_2) \in \Gamma \cap B(0, \sqrt{2p})$; por tanto $x_1^2 + x_2^2$ es un múltiplo de p y por otra parte es estrictamente menor que $2p$; luego necesariamente $x_1^2 + x_2^2 = p$.

La condición que impone el teorema de Minkowski respecto al volumen de la red es: $\mu(B(0, \sqrt{2p})) > 4Vol(\Gamma)$, es decir $2\pi p > 4Vol(\Gamma)$; esta condición se cumple si, por ejemplo, el volumen de Γ es p. Una forma natural de buscar subredes de $\mathbb{Z}^2$ de volumen p es considerar aplicaciones lineales

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}/(p) \\ (x_1, x_2) & \longrightarrow & x_1 + ax_2 + (p). \end{array}$$

Cualquiera de estas aplicaciones es suprayectiva y su núcleo es, por tanto, una subred de $\mathbb{Z}^2$ de volumen p. Veamos si podemos elegir a de tal forma que los elementos del núcleo verifiquen la otra condición que necesitamos, es decir que $x_1^2 + x_2^2$ sea un múltiplo de p. Si (x_1, x_2) está en el núcleo, entonces $x_1 \equiv -ax_2 \bmod p$ y por tanto $x_1^2 + x_2^2 \equiv (a^2 + 1)x_2^2 \bmod p$. Si pudiesemos elegir a de tal forma que $a^2 + 1$ fuese múltiplo de p, todo estaría resuelto. Y aquí es donde necesitamos la hipótesis que tenemos sobre p: $p \equiv 1 \bmod 4$.

Es bien sabido que el grupo multiplicativo $\mathbb{Z}/(p) - \{0\}$ es un grupo cíclico con $p-1$ elementos, generado digamos por la clase $\alpha + (p)$; $-1 + (p)$ es el elemento de orden dos, por tanto $-1 + (p) = (\alpha + (p))^{\frac{p-1}{2}}$. Por ser $p \equiv 1 \bmod 4$ se tiene que $\frac{p-1}{2} = 2m$ para algún m de $\mathbb{Z}$, y por tanto resulta que $-1 + (p)$ es un cuadrado en $\mathbb{Z}/(p)$, es decir existe $a \in \mathbb{Z}$ tal $-1 \equiv a^2 \bmod p$. Con este a construyo la aplicación de la que hablamos arriba y tenemos el teorema de los dos cuadrados demostrado.

De forma totalmente análoga se pueden demostrar otros teoremas del mismo estilo como por ejemplo los siguientes, enunciados por Fermat y probados, con gran esfuerzo según él mismo reconoció, por Euler:

Para todo primo p se verifica

$$p = x^2 + 2y^2 \quad x, y \in \mathbb{Z} \Longleftrightarrow p = 2 \quad o \quad p \equiv 1, 3 \bmod 8$$

$$p = x^2 + 3y^2 \quad x, y \in \mathbb{Z} \Longleftrightarrow p = 3 \quad o \quad p \equiv 1 \bmod 3$$

$$p = x^2 + 5y^2 \quad x, y \in \mathbb{Z} \Longleftrightarrow p = 5 \quad o \quad p \equiv 1, 9 \bmod 20.$$

A título de ejemplo resumimos como se demuestra que si $p \equiv 1 \bmod 3$ entonces existen x e y en $\mathbb{Z}$ tales que $p = x^2 + 3y^2$.

Si $p \equiv 1 \bmod 3$ entonces -3 es un cuadrado módulo p (este es un caso particular de la **Ley de Reciprocidad Cuadrática**, descubierta por Euler precisamente cuando intentaba probar los teoremas citados mas arriba). Si -3 es un cuadrado $\bmod p$, su inverso, es decir $-1/3$ también lo es, y por tanto existe $a \in \mathbb{Z}$ tal que $1 + 3a^2$ es un múltiplo de p.

Considero la aplicación lineal suprayectiva

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}/(p) \\ (x_1, x_2) & \longrightarrow & x_2 - ax_1 + (p). \end{array}$$

Su núcleo, Γ, es una red de volumen p y tal que para todo $(x_1, x_2) \in \Gamma$ se tiene

$$x_1^2 + 3x_2^2 + (p) = x_1^2 + 3a^2x_1^2 + (p) = (1 + 3a^2)x_1^2 = 0 + (p)$$

es decir, para todo $(x_1, x_2) \in \Gamma$ se verifica que $x_1^2 + 3x_2^2$ es un múltiplo de p.

Se considera la elipse abierta:

$$B = \{(x, y) \in \mathbb{R}^2 | x^2 + 3y^2 < 3p\}.$$

La medida de B, $\pi\sqrt{3}p$, es estrictamente mayor que $4p$; entonces el Teorema de Minkowski asegura que existe (x_1, x_2) en $B \cap \Gamma$ distinto de $(0, 0)$ y por tanto para este punto, $x_1^2 + 3x_2^2$ es estrictamente menor que $3p$ y múltiplo de p, luego tiene que ser igual a p o a $2p$. Si fuese $x_1^2 + 3x_2^2 = 2p$, reduciendo módulo 3 tendríamos $\overline{x_1}^2 = \overline{2p} = \overline{2}$ (por ser $p \equiv 1 \mod 3$), lo que es absurdo pues 2 no es un cuadrado módulo 3. Luego necesariamente $x_1^2 + 3x_2^2 = p$ como queríamos probar.

Hay otro teorema clásico, enunciado también por Fermat en una de sus cartas, que Euler trató infructuosamente de probar, cosa que consiguió hacer Lagrange, y que puede demostrarse muy fácilmente a partir del Teorema de Minkowski de una forma similar a como hemos hecho en los casos anteriores. Se trata del

Teorema de los cuatro cuadrados: *Todo número positivo n es suma de cuatro cuadrados. Es decir para todo $n \in \mathbb{N}$ existen $x, y, z, t \in \mathbb{Z}$ tales que*

$$n = x^2 + y^2 + z^2 + t^2.$$

Observemos en primer lugar que basta probar el teorema para los números primos. En efecto, si dos números son suma de dos cuadrados su producto también lo es, como se deduce de la siguiente identidad:

$$(a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2) = x^2 + y^2 + z^2 + t^2,$$

donde

$$\begin{aligned} x &= ap + bq + cr + ds \\ y &= aq - bp + cs - dr \\ z &= ar - bs - cp + dq \\ t &= as + br - cq - dp. \end{aligned}$$

Esta fórmula la encontró Euler; una forma de llegar a ella razonadamente es utilizando el cuerpo de los cuaternios de Hamilton.

Supongamos entonces que p es un número primo. Si $p = 2$ el teorema se verifica trivialmente: basta tomar $x = 1, y = 1, z = 0, t = 0$. Podemos suponer por tanto p impar.

En primer lugar veamos que existen $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 + 1 \equiv 0 \mod p$. Ya hemos comentado anteriormente que el grupo multiplicativo $\mathbb{Z}/(p) - \{0\}$ es un grupo cíclico con $p - 1$ elementos; los cuadrados en $\mathbb{Z}/(p)$ son el 0 y las potencias

pares de un generador, y por lo tanto hay $\frac{p-1}{2}+1=\frac{p+1}{2}$ cuadrados. Así, los subconjuntos de $\mathbb{Z}/(p)$, $\{a^2+(p)|a\in\mathbb{Z}\}$ y $\{-b^2-1+(p)|b\in\mathbb{Z}\}$ tienen ambos $\frac{p+1}{2}$ elementos, luego necesariamente tienen intersección no vacía, lo que prueba la afirmación hecha al principio de este párrafo.

Con los elementos a y b cuya existencia acabamos de probar, construimos la aplicación, obviamente suprayectiva

$$\begin{array}{rcl}\mathbb{Z}^4 & \longrightarrow & \mathbb{Z}/(p)\times\mathbb{Z}/(p)\\ (x_1,x_2,x_3,x_4) & \longrightarrow & (x_3-ax_1-bx_2+(p),x_4-bx_1+ax_2+(p)).\end{array}$$

El núcleo Γ de esta aplicación lineal es una subred de $\mathbb{Z}^4$ de volumen p^2 y tal que, como se comprueba inmediatamente por la elección de a y b que hemos hecho, para todo $(x_1,x_2,x_3,x_4)\in\Gamma$ se tiene que $x_1^2+x_2^2+x_3^2+x_4^2$ es un múltiplo de p.

Ahora considero la bola abierta en $\mathbb{R}^4$, $B(0,\sqrt{2p})$, de centro el origen y radio $\sqrt{2p}$. Su medida verifica

$$\mu(B(0,\sqrt{2p}))=2\pi^2p^2>2^4Vol(\Gamma)$$

y por tanto el Teorema de Minkowski asegura que existe un punto $(x_1,x_2,x_3,x_4)\in\Gamma\cap B(0,\sqrt{2p})$ distinto del origen. Para dicho punto, $x_1^2+x_2^2+x_3^2+x_4^2$ es por un lado un mútiplo de p y por otro estrictamente menor que $2p$, luego necesariamente $x_1^2+x_2^2+x_3^2+x_4^2=p$, como queríamos demostrar.

Hasta ahora hemos visto como puede utilizarse el Teorema de Minkowski para dar demostraciones muy sencillas de ciertos teoremas clásicos de teoría de números. Pero Minkowski para lo que aplicó su teorema fue, entre otras cosas, para estudiar ciertas propiedades nada triviales de los anillos de enteros de los cuerpos de números.

Se llama **Cuerpo de números** a cualquier cuerpo $\mathbb{K}$ que sea una extensión finita de $\mathbb{Q}$ (es decir que sea de dimensión finita como $\mathbb{Q}$-espacio vectorial). Es sabido que todo elemento de $\mathbb{K}$ es raíz de algún polinomio no nulo, con coeficientes en $\mathbb{Q}$ y mónico (es decir con el coeficiente del término de mayor grado igual a uno). Se puede probar que el conjunto de los elementos de $\mathbb{K}$ que son raíz de algún polinomio, no nulo y mónico, con coeficientes en $\mathbb{Z}$, forman un anillo, subanillo de $\mathbb{K}$: a este anillo, que designaremos por B, se le llama **Anillo de enteros** del cuerpo de números $\mathbb{K}$. Por ejemplo se puede demostrar que

Si $\mathbb{K}=\mathbb{Q}$ entonces $B=\mathbb{Z}$.

Si $\mathbb{K}=\mathbb{Q}(i)$ entonces $B=\mathbb{Z}[i]=\mathbb{Z}\oplus\mathbb{Z}i$.

Si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ entonces $B = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$.

Si $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ entonces $B = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \subsetneq \mathbb{Z}[\sqrt{5}]$.

Estos anillos juegan un papel respecto de $\mathbb{K}$ parecido al que juega $\mathbb{Z}$ respecto de $\mathbb{Q}$. Conocer sus propiedades es imprescindible para resolver casi cualquier problema en teoría algebraica de números. Gauss ya fue consciente de ello: el probó el Teorema de los dos cuadrados que hemos demostrado antes, basándose en las propiedades del anillo $\mathbb{Z}[i]$. Pero la persona que verdaderamente inició el estudio sistemático de estos anillos fue Kummer: se vió abocado a ello intentando demostrar el último Teorema de Fermat.

Si $\mathbb{K}$ es un cuerpo de números de grado n sobre $\mathbb{Q}$ y B es su anillo de enteros, se puede probar que B es un $\mathbb{Z}$-módulo libre de rango n, como veíamos en los ejemplos citados mas arriba; es decir

$$B = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n.$$

Si pensamos en la identificación habitual de $\mathbb{C}$ con $\mathbb{R}^2$, está claro que podemos ver el anillo $\mathbb{Z}[i]$ como una red de $\mathbb{R}^2$: es simplemente la red $\mathbb{Z}^2$. Minkowski ideó como representar cualquier anillo de enteros como una red en algún $\mathbb{R}^n$; veamos como lo hizo.

Se sabe que si el grado de $\mathbb{K}$ sobre $\mathbb{Q}$ es n hay n homomorfismos de anillos de $\mathbb{K}$ en $\mathbb{C}$; si σ es uno de ellos, $\overline{\sigma} = \tau \circ \sigma$ (donde τ es la conjugación compleja) es otro de ellos; esto quiere decir que los homomorfismos cuya imagen no está dentro de $\mathbb{R}$ van por pares. O sea en general podemos decir que hay r_1 homomorfismos reales y $2r_2$ homomorfismos complejos:

$$\begin{aligned} \sigma_1, \ldots, \sigma_{r_1} &: \mathbb{K} \longrightarrow \mathbb{R} \\ \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}} &: \mathbb{K} \longrightarrow \mathbb{C}. \end{aligned}$$

Por supuesto se tiene $n = r_1 + 2r_2$. Al par (r_1, r_2) se le llama la **signatura** del cuerpo $\mathbb{K}$; por ejemplo la signatura de $\mathbb{Q}(i)$ es (0,1), la de $\mathbb{Q}(\sqrt{2})$ es (2,0).

Mediante estos homomorfismos se construye la aplicación

$$\begin{aligned} \mathbb{K} &\longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\longrightarrow (\sigma_1(x), \ldots, \sigma_{r_1(x)}, \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)). \end{aligned}$$

Identificando $\mathbb{C}$ con $\mathbb{R}^2$ se obtiene la aplicación

$$\begin{aligned} \sigma\colon \mathbb{K} &\longrightarrow \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} = \mathbb{R}^n \\ x &\longrightarrow (\sigma_1(x), \ldots, \sigma_{r_1(x)}, Re(\sigma_{r_1+1}(x)), Im(\sigma_{r_1+1}(x)), \ldots\ldots) \end{aligned}$$

σ es una aplicación $\mathbb{Z}$-lineal e inyectiva que transforma el anillo de enteros B de $\mathbb{K}$ en una red de $\mathbb{R}^n$

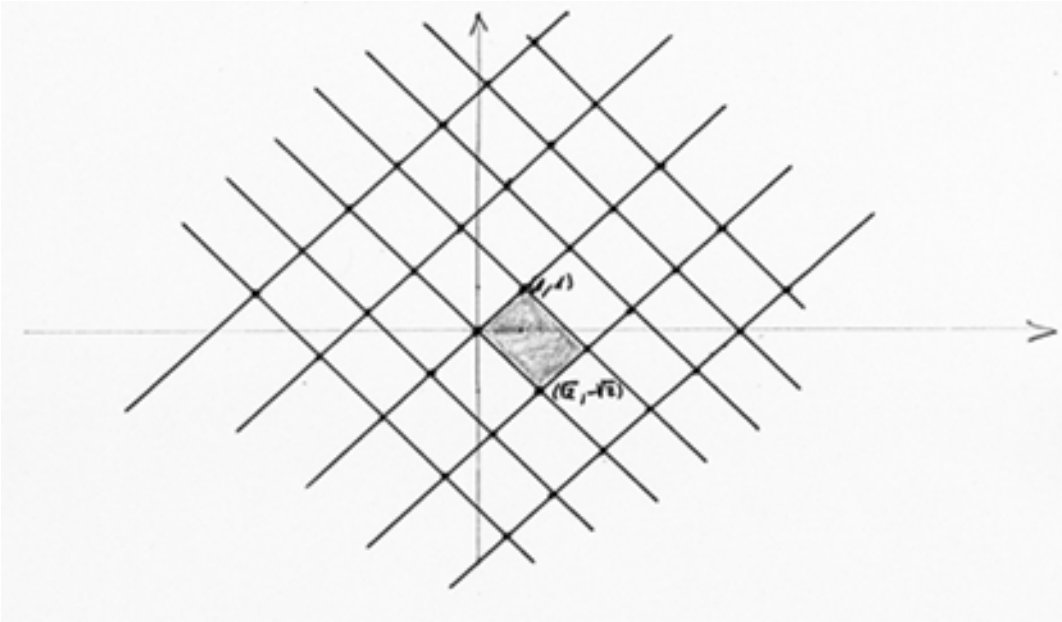
$$\sigma(B) = \mathbb{Z}\sigma(u_1) \oplus \cdots \oplus \mathbb{Z}\sigma(u_n).$$

Por ejemplo si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$

$$\begin{array}{rcl} \sigma\colon \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{R}^2 \\ a + b\sqrt{2} & \longrightarrow & (a + b\sqrt{2}, a - b\sqrt{2}). \end{array}$$

La imagen mediante σ del anillo de enteros $\mathbb{Z}[\sqrt{2}]$ es

$$\sigma(\mathbb{Z}[\sqrt{2}]) = \mathbb{Z}\sigma(1) \oplus \mathbb{Z}\sigma(\sqrt{2}). = \mathbb{Z}(1,1) \oplus \mathbb{Z}(\sqrt{2}, -\sqrt{2})$$



Hay un dato muy importante para conocer la aritmética de un cuerpo $\mathbb{K}$: su **discriminante** $d_{\mathbb{K}}$, que definimos a continuación:

Si $B = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n$ entonces

$$d_{\mathbb{K}} = (\det(\sigma_i(u_j)))^2.$$

Se puede probar fácilmente que el discriminante de $\mathbb{K}$ es un número entero distinto de 0, y que no depende más que de $\mathbb{K}$, es decir no depende de la base elegida para B como $\mathbb{Z}$-módulo.

Por ejemplo si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ y por tanto $B = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$, se tiene

$$d_{\mathbb{Q}(\sqrt{2})} = (\det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix})^2 = 8.$$

Es trivial comprobar que el volumen de la red $\sigma(B)$ es

$$Vol(\sigma(B)) = \frac{1}{2^{r_2}} \sqrt{|d_{\mathbb{K}}|}.$$

Hemos conseguido así "visualizar" los objetos que queremos estudiar: tenemos representados los anillos de enteros de los cuerpos de números como redes en $\mathbb{R}^n$. Utilizando su teorema sobre los cuerpos convexos, Minkowski probó el siguiente

Teorema: *Si $\mathbb{K}$ es un cuerpo de números distinto de $\mathbb{Q}$, su discriminante $d_{\mathbb{K}}$ tiene valor absoluto estrictamente mayor que 1, es decir $d_{\mathbb{K}} \neq \pm 1$.*

Este resultado, que es absolutamente clave y tiene muchas consecuencias en la teoría algebraica de números, no se ha demostrado nunca de una manera esencialmente distinta a como lo hizo Minkowski. Vamos a dar una idea de la demostración.

Para cada $t \in \mathbb{R}, t \geq 0$, considero el conjunto

$$B_t = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \quad |x_i| \leq t, \quad |y_j| \leq t\}.$$

Cada conjunto B_t es simétrico, convexo y compacto; como es un producto de segmentos por discos, su medida se calcula fácilmente:

$$\mu(B_t) = (2t)^{r_1} (\pi t^2)^{r_2} = 2^{r_1} \pi r_2 t^n.$$

Al ser B_t compacto, el menor t para el cual se puede aplicar el Teorema de Minkowski a B_t y a la red $\sigma(B)$ es el que verifica la igualdad

$$2^{r_1} \pi r_2 t^n = 2^n \frac{1}{2^{r_2}} \sqrt{|d_{\mathbb{K}}|}.$$

O sea

$$t^n = (\frac{2}{\pi})^{r_2} \sqrt{|d_{\mathbb{K}}|}.$$

El Teorema de los cuerpos convexos nos asegura que, para ese valor de t, existe $x \in B, x \neq 0$ tal que $\sigma(x) \in B_t$; pero, recordando la definición de la aplicación σ, esto quiere decir que $|\sigma_i(x)| \leq t$ para todo $i : 1, \ldots, n$.

Por otro lado, por ser x un elemento de B, la **norma** de x que se define como

$$N_{\mathbb{K}/\mathbb{Q}}(x) := \prod_{i=1}^{n} \sigma_i(x),$$

es un número entero no nulo (x es raíz de un polinomio irreducible mónico con coeficientes enteros; pues bien, la norma de x es, salvo el signo, una potencia del término constante de dicho polinomio). Por tanto

$$1 \leq |N_{\mathbb{K}/\mathbb{Q}}(x)| \leq t^n,$$

luego

$$1 \leq |N_{\mathbb{K}/\mathbb{Q}}(x)| \leq (\frac{2}{\pi})^{r_2}\sqrt{|d_{\mathbb{K}}|}.$$

Se deduce que

$$1 \leq (\frac{2}{\pi})^{r_2}\sqrt{|d_{\mathbb{K}}|},$$

y por tanto

$$(\frac{\pi}{2})^{r_2} \leq \sqrt{|d_{\mathbb{K}}|}.$$

Si $r_2 \neq 0$ (es decir si existen homomorfismos de $\mathbb{K}$ en $\mathbb{C}$ cuya imagen no cae dentro de $\mathbb{R}$ se deduce que $|d_{\mathbb{K}}| > 1$ como queríamos probar; pero en el caso en que $r_2 = 0$ no se obtiene nada. Minkowski modificó ingeniosamente esta demostración tomando otros conjuntos B_t para cada t. No voy a dar los detalles de la demostración, solamente diré que de esta forma consigue probar que

$$|d_{\mathbb{K}}| \geq \frac{n^{2n}}{(n!)^2}(\frac{\pi}{4})^n$$

donde n es el grado del cuerpo $\mathbb{K}$ sobre $\mathbb{Q}$. Si ponemos

$$c_n := \frac{n^{2n}}{(n!)^2}(\frac{\pi}{4})^n$$

se comprueba fácilmente que la sucesión $\{c_n\}$ es monótona estrictamente creciente y que $1 < c_2 < c_3 < \ldots$.

Se obtiene así no solamente el teorema que queriamos demostrar sino, además, una cota inferior para el valor absoluto del discriminante de un cuerpo de números $\mathbb{K}$ que depende únicamente del grado de $\mathbb{K}$ sobre $\mathbb{Q}$. En particular el valor absoluto del discriminante de $\mathbb{K}$ crece con el grado de $\mathbb{K}$ sobre $\mathbb{Q}$.

A partir de aquí se puede probar (aunque, de nuevo hay que recurrir al Teorema de los cuerpos convexos de Minkowski) que, para cada $d \in \mathbb{Z}$, hay a lo sumo un número finito de cuerpos de números de discriminante d.

Además del estudio de los anillos de enteros de los cuerpos de números, Minkowski encontró aplicaciones a su Teorema de los cuerpos convexos en otros muchos

ámbitos, por ejemplo en problemas de aproximaciones diofánticas (es decir aproximaciones de números reales por números racionales) o también en el problema de recubrimientos por esferas.

Para terminar me gustaría mencionar a Dirichlet. Fue un matemático alemán que vivió durante la primera mitad del siglo diecinueve; murió diez años antes de que naciera Minkowski. Entre las muchas aportaciones que hizo a las matemáticas en general y a la teoría de números en particular hay una especialmente importante para el estudio de los anillos de enteros de los cuerpos de números. En estos anillos un problema que siempre se plantea es como descompone un elemento en producto de elementos irreducibles; pero evidentemente, para ocuparse de esto, uno tiene que saber algo sobre las unidades de estos anillos, es decir sobre los elementos cuyo inverso está en el propio anillo. Veamos algunos ejemplos en los que denotaremos por B^* el conjunto de las unidades de B. Se puede probar que

Si $\mathbb{K} = \mathbb{Q}$, $B = \mathbb{Z}$ y $B^* = \{\pm 1\}$.

Si $\mathbb{K} = \mathbb{Q}(i)$, $B = \mathbb{Z}[i]$ y $B^* = \{\pm 1, \pm i\}$.

Si $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$, $B = \mathbb{Z}[\sqrt{-2}]$ y $B^* = \{\pm 1\}$.

Si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, $B = \mathbb{Z}[\sqrt{2}]$ y $B^* = \{\pm(1+\sqrt{2})^n | n \in \mathbb{Z}\}$.

Después de ver lo que ocurre en muchos ejemplos, Dirichlet fue capaz de determinar la estructura del grupo de las unidades del anillo de enteros de cualquier cuerpo de números. Probó el siguiente

Teorema: *El grupo de las unidades del anillo de enteros de un cuerpo de números $\mathbb{K}$ es un grupo abeliano finitamente generado de rango $r = r_1 + r_2 - 1$ donde (r_1, r_2) es la signatura del cuerpo $\mathbb{K}$. Por tanto*

$$B^* \simeq \mu_{\mathbb{K}} \times \mathbb{Z}^r$$

donde $\mu_{\mathbb{K}}$ es el conjunto de las raíces de la unidad contenidas en $\mathbb{K}$.

O en la forma en que lo enunció Dirichlet:

Existen $r = r_1 + r_2 - 1$ unidades en B, $\epsilon_1, \ldots, \epsilon_r$ tales que toda unidad se escribe de manera única como

$$\epsilon = \eta \prod_{i=1}^{r} \epsilon_i^{n_i}$$

donde η es una raíz de la unidad y $n_i \in \mathbb{Z}$ para todo i.

Por ejemplo, si $B = \mathbb{Z}[\sqrt{2}]$, $r = 2 + 0 - 1 = 1$; como las raíces de la unidad contenidas en $\mathbb{Q}(\sqrt{2})$ son ± 1, el teorema afirma que existe una unidad η tal que $B^* = \{\pm\eta^n | n \in \mathbb{Z}\}$; y efectivamente, tomando $\eta = 1 + \sqrt{2}$, se puede comprobar, como he comentado antes, que el teorema es cierto en este caso. Si $B = \mathbb{Z}[i]$, $r = 0 + 1 - 1 = 0$: en este anillo las únicas unidades que hay son las raíces de la unidad contenidas en él, a saber ± 1 y $\pm i$.

Por supuesto no voy a demostrar aquí este teorema que es el más complicado de los que uno encuentra al empezar a estudiar los anillos de enteros de los cuerpos de números. Solo diré que, de nuevo, es un resultado que se prueba "geométricamente": Dirichlet se las arregla para representar las unidades que quiere estudiar como puntos de una red. (Utiliza la función logaritmo para transformar el grupo multiplicatico de las unidades en una red, que es un grupo aditivo). Según afirma Minkowski la idea de esta demostración se le ocurrió a Dirichlet mientras asistía a la misa de Pascua en la capilla Sixtina de Roma en 1844.

Por último querría decir que la geometría de los números que, como he explicado en esta charla, tiene su origen en las ideas de Dirichlet y Minkowski, se desarrolló bastante a principios del siglo XX, pero hoy parece que ya ha dado todos los frutos que cabía esperar (aunque esto nunca se puede afirmar tajantemente). Lo que hoy se entiende por métodos geométricos en la teoría de números no tiene nada que ver con lo que hemos visto hoy aquí. Se trata de aplicar a la teoría de números la potente maquinaria de la geometría algebraica desarrollada fundamentalmente en la segunda mitad del siglo XX. Y esto si que parece tener mucho futuro por delante; no hay más que pensar en la demostración de Wiles del último Teorema de Fermat. O sea que, en conclusión, parece que las opiniones de Atiyah que he citado al principio pueden ser bastante acertadas.

Bibliografía

[1] M. Atiyah, *Mathematics in the* 20^{th} *century*, Bull. London Math. Soc. 34 (2002).

[2] J. W. S. Cassels, *Introduction to the Geometry of Numbers*, Springer (1997).

[3] H. Koch, *Zahlentheory*, Vieweg (1997).

[4] C.D. Olds, A. Lax, G. Davidoff, *The Geometry of Numbers*, The Mathematical Association of America (2000).

[5] P. Samuel, *Théorie Algebrique des Nombres*, Hermann (1967).

[6] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat Last Theorem*, (3^{rd} edition). A.K.Peters (2002).