DIVULGACIÓN MATEMÁTICA

Problemas con Subgrupos Discretos y Subgrupos Densos

José O. Araujo & Laura B. Fernández

Resumen

En este trabajo presentamos algunas aplicaciones de la geometría reticular y subgrupos densos en la recta y el plano real, especialmente del teorema de Minkowski en el plano.
Los problemas tratados son sobre polígonos regulares, aproximación y teoría elemental de números.
Palabras y frases claves: Minkowski, retículos, aproximación. [1]

Discrete and Dense Subgroup Problems

Abstract

In this work we present some aplications of the reticular geometry and dense subgroups of the real line and the real plane, especially of the Minkowski's theorem in the plane.
The problems we deal are over regular polygons, approximation and elemental theory of numbers.
Key words and phrases: Minkowski, lattices, approximation.

1 Introducción

En estas notas presentamos los conceptos de conjuntos densos y conjuntos discretos sobre la recta y el plano real. Se analiza particularmente, los subgrupos de la recta real con su estructura aditiva y, un poco más general, los subconjuntos aditivos de los números reales. Por otra parte, se presenta el teorema de Minkowski en el plano relativo a puntos reticulares en una figura convexa. Con el propósito de ilustrar sobre la utilidad de estos conceptos, las conclusiones obtenidas se aplican a una serie de problemas de aproximación de números por elementos de un subgrupo o de un conjunto aditivo. También se tratan aplicaciones del teorema de Minkowski relacionadas con el teorema de los cuatro

[1] 1991 Mathematics Subject classfication: Primary 52C05

cuadrados y con la ecuación de Pell. Finalmente se plantean problemas sobre los números complejos unitarios, teniendo en cuenta que la estructura multiplicativa de estos responde a la estructura aditiva de sus argumentos.

Los símbolos utilizados corresponden a la siguiente asignación:
$\mathbb{N}$: números naturales
$\mathbb{Z}$: números enteros
$\mathbb{R}$: números reales
$\mathbb{C}$: números complejos.

2 En la Recta Real

Un subconjunto $\mathcal{A}$ de los números reales $\mathbb{R}$ se dirá un *subconjunto denso* si para $r \in \mathbb{R}$ y $\varepsilon > 0$, existe $a \in A$ tal que $|r - a| < \varepsilon$.
Un subconjunto $\mathcal{A}$ de los números reales $\mathbb{R}$ se dirá un *subconjunto discreto* si para cada $a \in A$ existe $\varepsilon > 0$ tal que $(a - \varepsilon, a + \varepsilon) \cap \mathcal{A} = \{a\}$.
Por ejemplo, los siguientes subconjuntos son densos:
i) Los números racionales.
ii) Los números irracionales.
iii) $\{x \in \mathbb{R} / sen\,(x) \neq 0\}$.
iv) El complemento de un subconjunto discreto.
Los siguientes subconjuntos son discretos:
i) Cualquier conjunto finito.
ii) Los números naturales
iii) Los enteros múltiplos de 7.
iv) $\{x \in \mathbb{R} / \cos(x) = 0\}$.
Se propone como ejercicio comprobar las afirmaciones precedentes.

El concepto de densidad está estrechamente ligado al concepto de aproximación, por ejemplo al decir que los números racionales son densos, decimos que todo número real puede aproximarse arbitrariamente con números racionales. En general, que el conjunto $\mathcal{A}$ sea denso en $\mathbb{R}$, significa que cualquier número real puede ser aproximado arbitra-riamente con elementos de $\mathcal{A}$.
Es particularmente interesante el caso en que los subconjuntos considerados son subgrupos de $\mathbb{R}$ considerado con su estructura aditiva. Damos a continuación los conceptos de grupo abeliano y subgrupos.

Un conjunto $\mathcal{G}$ provisto de una operación binaria "+" se dice *grupo* si se verifican:
i) $(a + b) + c = a + (b + c) \quad \forall\, a, b, c \in \mathcal{G}$ *(Asociativa).*
ii) Existe $o \in \mathcal{G}$ tal que $a + o = o + a = a \quad \forall\, a \in \mathcal{G}$ *(con elemento neutro).*

iii) $\forall\, a \in \mathcal{G}$ existe $b \in \mathcal{G}$ tal que $a + b = b + a = o$ *(con inverso).*
Un grupo $\mathcal{G}$ se dice *abeliano* si además se verifica:
iv) $a + b = b + a \quad \forall a, b \in \mathcal{G}$.

El elemento b de la condición *iii)* resulta único, se llama el *inverso de* a y se notará con $-a$, y como es usual, se usará $a - b$ para indicar la suma $a + (-b)$.

Un subconjunto $\mathcal{H}$ de un grupo $\mathcal{G}$ se dice un *subgrupo de* $\mathcal{G}$ si se cumplen:
i) $o \in \mathcal{H}$.
ii) Si a y $b \in \mathcal{H}$ entonces $a - b \in \mathcal{H}$.

Como consecuencias de las condiciones *i)* y *ii)* precedentes, se tiene:
Si $\mathcal{H}$ es un subgrupo de un grupo $\mathcal{G}$, se verifican:
i) Si $a \in \mathcal{H}$ entonces $-a \in \mathcal{H}$.
ii) Si $a, b \in \mathcal{H}$ entonces $a + b \in \mathcal{H}$.

Como ejemplos de grupos abelianos tenemos:
i) Los números enteros $\mathbb{Z}$ con la suma usual.
ii) Los números reales con la suma usual.
iii) Los vectores en el plano con la suma usual de vectores.
iv) El conjunto $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ con la suma módulo n.
v) $\mathbb{R} - \{0\}$ con el producto usual.
Como ejemplos de subgrupos:
i) Los números pares forman un subgrupo de los enteros con la suma.
ii) Los números enteros forman un subgrupo de los reales con la suma.
iii) $\mathbb{Z}\left[\sqrt{2}\right] = \left\{m + n\sqrt{2} : m, n \in \mathbb{Z}\right\}$ es un subgrupo de $\mathbb{R}$ con la suma.
iv) Los números reales positivos forman un subgrupo de $\mathbb{R} - \{0\}$ con el producto usual.
Se propone como ejercicio comprobar las afirmaciones precedentes.

Naturalmente que hay subconjuntos de $\mathbb{R}$ que no son discretos ni densos por ejemplo los reales positivos entre otros tantos, pero si consideramos como $\mathbb{R}$ el grupo abeliano con la operación suma, el teorema a conti-nuación, no deja otra alternativa para un subgrupo de $\mathbb{R}$ que la de ser un subconjunto discreto o un subconjunto denso.

Teorema 2.1. *Si* $\mathcal{H}$ *es un subgrupo de* $\mathbb{R}$*, entonces* $\mathcal{H}$ *es un subgrupo discreto o* $\mathcal{H}$ *es un subconjunto denso.*

Demostración: Comencemos observando que, si $n \in \mathbb{Z}$ y $h \in \mathcal{H}$, entonces $nh \in \mathcal{H}$. En efecto: $1h = h \in \mathcal{H}$, $2h = h + h \in \mathcal{H}$, $3h = 2h + h \in \mathcal{H}$, y en general se tiene

$$(n+1)\,h = nh + h$$

identidad que permite probar por inducción que $nh \in \mathcal{H}\,, \forall\, n \in \mathbb{N}$ y h arbitrario en $\mathcal{H}$. Ahora si n es un entero negativo, expresando $nh = (-n)\,(-h) \in \mathcal{H}$ y teniendo en cuenta que $-h \in \mathcal{H}$, del caso anterior se tiene $nh \in \mathcal{H}$.
Finalmente, $0h = 0$, lo que concluye con la prueba de nuestra afirmación.
Si $\mathcal{H} = \{0\}, \mathcal{H}$ es discreto. En caso contrario, $\mathcal{H}$ tiene un elemento $h \neq 0$. Dado que $-h \in \mathcal{H}$, resulta que $\mathcal{H}$ tiene un elemento positivo h_0 y podemos considerar

$$r = \inf\ \{h \in \mathcal{H} : h > 0\}$$

Si $r = 0$, sea x arbitrario en $\mathbb{R}$ y definimos los conjuntos

$$\mathcal{I} = \{h \in \mathcal{H} : h < x\} \quad \text{y} \quad \mathcal{J} = \{h \in \mathcal{H} : h > x\}$$

Acorde con lo observado al comienzo de la demostración, se tiene que

$$\mathbb{Z}h_0 = \{nh_0 : n \in \mathbb{Z}\} \subseteq \mathcal{H}$$

En consecuencia, $\mathcal{I}$ y $\mathcal{J}$ resultan conjuntos no vacíos. Es claro que

$$\sup \mathcal{I} \leq x \leq \inf \mathcal{J}$$

Como $r = 0$, para $\varepsilon > 0$ existe $h \in \mathcal{H}$ tal que $0 < h < \varepsilon$. En tal caso podemos elegir $k \in \mathbb{Z}$ de modo que

$$kh \leq x < (k+1)\,h$$

es decir $kh \in \mathcal{I}$ y $(k+1)\,h \in \mathcal{J}$, luego

$$\inf \mathcal{J} - \sup \mathcal{I} \leq (k+1)\,h - kh = h < \varepsilon \qquad \forall \varepsilon > 0$$

Debe ser $\sup \mathcal{H} = x = \inf \mathcal{J}$. Esto indica que un número real cualquiera puede ser aproximado arbitrariamente, tanto por la izquierda como por la derecha por elementos de $\mathcal{H}$, siendo $\mathcal{H}$ de este modo un subconjunto denso de $\mathbb{R}$.
En otro caso, $r > 0$ y $\mathcal{H}$ no puede tener más que un elemento en el intervalo

$$[r, 2r) = \{x \in \mathbb{R} : r \leq x < 2r\}$$

pues de haber dos elementos $h < h'$ de $\mathcal{H}$ en este intervalo, tendríamos que

$$0 < h - h' < r$$

pero esto contradice la condición de ínfimo del número r. En conclusión, $r \in \mathcal{H}$.
En este caso tenemos

$$\mathbb{Z}r = \{nr :\ n \in \mathbb{Z}\} \subseteq \mathcal{H}$$

Razonando como antes, encontraremos que

$$[nr, (n+1)\ r) \cap \mathcal{H} = \{nr\}$$

es decir

$$\mathcal{H} = \mathbb{Z}r$$

y resulta claro que $\mathbb{Z}\,r$ es un subconjunto discreto de $\mathbb{R}$. ■

Observemos que los subgrupos discretos de $\mathbb{R}$ quedan caracterizados por los subconjuntos de la forma $\mathbb{Z}\,r$, para algún $r \in \mathbb{R}$. Usaremos los términos *subgrupos discretos* o *subgrupos densos* para referirnos a subgrupos que son respectivamente conjuntos discretos o conjuntos densos.
Como aplicación del teorema 2.1, consideraremos los siguientes pro-blemas.

Problema 1. *Demostrar que todo número real puede aproximarse arbitrariamente por elementos del conjunto*

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{n + m\sqrt{2} : n, m \in \mathbb{Z}\right\}$$

El conjunto $\mathbb{Z}\left[\sqrt{2}\right]$ es un subgrupo de $\mathbb{R}$ con la suma, luego es denso o de la forma $\mathbb{Z}r$ para algún $r \in \mathbb{R}$. Si no fuese denso tendríamos enteros n y m tales que

$$1 = nr \quad \text{y} \quad \sqrt{2} = mr$$

Luego $\sqrt{2} = m/n$ resultaría un número racional.

Problema 2. *Sea α un número irracional, mostrar que todo número real y tal que $0 < y < 1$ puede aproximarse arbitrariamente por elementos del conjunto*

$$\{\{n\alpha\} : n \in \mathbb{Z}\}$$

donde $\{x\}$denota la mantisa del número real x, más precisamente $\{x\}$ es $x - [x]$ donde $[x]$ es la parte entera de x.

Como en el caso anterior, dado que α es irracional, puede mostrarse sin mayor dificultad que el conjunto

$$\{n + m\alpha : n, m \in \mathbb{Z}\}$$

es un subgrupo denso de $\mathbb{R}$. Escribimos

$$n + m\alpha = n + [m\alpha] + \{m\alpha\} = [n + m\alpha] + \{m\alpha\}$$

Si y es un número real tal que $0 < y < 1, y$ se aproxima arbitrariamente por la elementos de la forma $n + my$, dándose las mejores aproximaciones cuando $[n + my] = 0$, es decir por los elementos de la forma $\{my\}$.

Consideremos $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$, $\mathcal{C}$ es un grupo abeliano con el producto de números complejos. Los elementos en $\mathcal{C}$ pueden presentarse en su forma exponencial o polar como

$$z = \exp(2\pi i\theta) = cos(2\pi i\theta) + i\, sen(2\pi i\theta) \quad \text{con} \quad 0 \leq \theta < 1$$

es decir, $z \in \mathcal{C}$ depende sólo del parámetro real θ.

Problema 3. *Si $\mathcal{H}$ es un subgrupo de $\mathcal{C}$, mostrar que $\mathcal{H}$ es finito o bien todo elemento de $\mathcal{C}$ puede ser aproximado arbitrariamente por elementos de $\mathcal{H}$, esto último se expresa diciendo que $\mathcal{H}$ es denso en $\mathcal{C}$.*

Consideremos

$$\mathcal{H}' = \{x \in \mathbb{R} : \exp(2\pi ix) \in \mathcal{H}\}$$

Se tiene

i) $0 \in \mathcal{H}'$, pues $\exp(2\pi i0) = 1$.

ii) Si $x, y \in \mathcal{H}'$, entonces $x - y \in \mathcal{H}'$ pues

$$\exp(2\pi i(x-y)) = \exp(2\pi ix)\exp(2\pi iy)^{-1}$$

De aquí resulta que $\mathcal{H}'$ un subgrupo de $\mathbb{R}$ con la estructura aditiva, luego $\mathcal{H}'$ es denso o discreto. Si $\mathcal{H}'$es denso, todo número real θ en $[0,1)$ se aproxima arbitrariamente por elementos de $\mathcal{H}'$, luego todo elemento de $\mathcal{C}$ se aproxima arbitrariamente por elementos de la forma $\exp(2\pi ix)$ con $x \in \mathcal{H}'$, es decir, con elementos de $\mathcal{H}$.

Para precisar esta última afirmación, usaremos la desigualdad

$$|sen(t)| \leq |t| \qquad \forall t \in \mathbb{R}$$

En primer lugar notemos que

$$\begin{aligned} |\exp(2\pi ix) - \exp(2\pi i\theta)| &= |\exp(2\pi i\theta)|\,|\exp(2\pi i(x-\theta)) - 1| \\ &= |\exp(2\pi i(x-\theta)) - 1| \end{aligned}$$

Por otra parte, para $\alpha \in \mathbb{R}$

$$\begin{aligned} |\exp(i\alpha) - 1| &= \sqrt{(cos(\alpha) - 1)^2 + sen(\alpha)^2} \\ &= 2sen\left(\frac{\alpha}{2}\right) \end{aligned}$$

Se sigue que

$$\begin{aligned} |\exp(2\pi ix) - \exp(2\pi i\theta)| &= 2\,|sen(\pi(x-\theta))| \\ &\leq 2\pi\,|x-\theta| \end{aligned}$$

lo que muestra la densidad de $\mathcal{H}$ en $\mathcal{C}$.
Si $\mathcal{H}'$ es discreto, hay sólo un número finito de elementos de $\mathcal{H}'$ en el intervalo $[0,1)$, en consecuencia hay sólo un número finito de elementos en $\mathcal{H}$.

La afirmación en el teorema expuesto sigue siendo válida con bajo una hipótesis ligeramente más débil.
Diremos que $\mathcal{H}$ es un *subconjunto aditivo* de $\mathbb{R}$ si dados a y b en $\mathcal{H}$ entonces $a+b$ también pertenece a $\mathcal{H}$.
Observemos que si $\mathcal{H}$ es aditivo, usando inducción, puede mostrarse que si $a \in \mathcal{H}$ y $n \in \mathbb{N}$, entonces $na \in \mathcal{H}$.
Ejemplos de subconjuntos aditivos que no sean subgrupos podemos citar:
i) El conjunto $\mathbb{N}$ de los números naturales.
ii) Los número racionales menores que -1.
iii) $\left\{\ln\left(\frac{2^n}{3^m}\right) : n, m \in \mathbb{N}\right\}$
Tenemos entonces el siguiente teorema:

Teorema 2.2. *Si $\mathcal{H}$ es un subconjunto aditivo de $\mathbb{R}$ conteniendo elementos positivos y elementos negativos, entonces $\mathcal{H}$ es un subconjunto denso en $\mathbb{R}$ ó $\mathcal{H}$ es un subgrupo discreto de $\mathbb{R}$.*

Demostración: Notemos con I y S respectivamente

$$I = \inf\{h \in \mathcal{H} : h > 0\}$$

$$S = \sup\{h \in \mathcal{H} : h < 0\}$$

Se tiene $S \leq 0 \leq I$, de este modo es

$$S \leq S + I \leq I$$

En el intervalo $[S, I]$ pueden aproximarse arbitrariamente con elementos de $\mathcal{H}$ únicamente S, I y eventualmente el cero. Dado que $S+I$ puede ser aproximado arbitrariamente por elementos de $\mathcal{H}$, las posibilidades son

$$S + I = I \quad S + I = 0 \quad \text{o} \quad S + I = S$$

Si $S + I \neq 0$, entonces $S = 0$ ó $I = 0$. Supongamos que $S = 0$, debe ser $I > 0$. De aquí que podemos elegir $h \in \mathcal{H}$ tal que

$$-I < h < 0$$

pues $S = 0$ es el supremo de los elementos negativos de $\mathcal{H}$. Si $h' \in \mathcal{H}$ es positivo, $h' + nh \in \mathcal{H}$ para todo $n \in \mathbb{N}$, siendo $h' \geq I$, existe $k \in \mathbb{N}$ tal que

$$h' + kh \geq I > h' + (k+1)\,h$$

luego

$$I > h' + (k+1)\, h = h' + k\, h + h \geq I + h > 0$$

Encontramos una contradicción pues I es el ínfimo de los elementos positivos de $\mathcal{H}$.
En forma análoga, se trata el caso $I = 0$, y como conclusión se obtiene que $I + S = 0$.
Si $I = S = 0$, $\mathcal{H}$ posee elementos positivos y elementos negativos de módulos arbitrariamente pequeños, o sea cero puede ser aproximado, en forma arbitraria, por la izquierda y por la derecha con elementos de $\mathcal{H}$.
Sea $\varepsilon > 0$ y $r \in \mathbb{R}$ cualquier número positivo. Consideremos $h \in \mathcal{H}$ tal que

$$0 < h < \min\{r, \varepsilon\}$$

La sucesión nh con $n \in \mathbb{N}$, está formada por elementos de $\mathcal{H}$. Existe un número natural k tal que

$$kh \leq r < (k+1)\, h$$

Se tiene

$$r - \varepsilon < r - h < kh \leq r < (k+1)\, h = kh + h \leq r + h < r + \varepsilon$$

es decir el intervalo $(r - \varepsilon, r + \varepsilon)$ contiene dos elementos de $\mathcal{H}$, uno a la izquierda y otro a la derecha de r.
En forma similar se trata el caso en que r sea negativo, concluyendo que $\mathcal{H}$ es denso.
Sea ahora $I > 0$, $S = -I$. Supongamos que $\mathcal{H}$ posea un elemento h en el intervalo $(I, 2I)$. Consideremos h' en $\mathcal{H}$ tal que

$$-I - (h - I) < h' \leq -I$$

es decir

$$0 \leq h' + h$$

pero como

$$h < 2I \quad \text{y} \quad h' \leq -I$$

tendremos que $h' + h < I$ y esto no es posible pues I es el ínfimo de los elementos positivos de $\mathcal{H}$.
Resulta entonces que $I \in \mathcal{H}$. Al sumarle $2I$ a los elementos de $\mathcal{H}$ en el intervalo $(-2I, -I)$ obtenemos elementos de $\mathcal{H}$ en el intervalo $(0, I)$, por lo que no hay elementos de $\mathcal{H}$ en $(-2I, -I)$ y en consecuencia $-I \in \mathcal{H}$.
Finalmente, tenemos $\mathbb{Z}I \subseteq \mathcal{H}$ y en forma análoga a la demostración del teorema 2.1, obtenemos que $\mathcal{H} = \mathbb{Z}I$. ■

Es preciso mostrar que hay subconjuntos aditivos en las condiciones del teorema 2.2 que no son subgrupos, y en tal casos son subconjuntos densos.

Por ejemplo

$$\mathcal{H} = \left\{ n - m\sqrt{2} : n, m \in \mathbb{N} \right\}$$

es un subconjunto aditivo con elementos positivos y elementos negativos. Es simple mostrar que $0 \notin \mathcal{H}$, más aún, resulta claro que si $h \in \mathcal{H}$ entonces $-h \notin \mathcal{H}$. Como aplicación del teorema 2.2 tenemos:

Problema 4. *Sean p y q números naturales con $q > 1$, sea*

$$\mathcal{K} = \left\{ \frac{p^i}{q^j} : i, j \in \mathbb{N} \right\}$$

Entonces $\mathcal{K}$ es denso en los reales positivos ó p y q son ambos potencias de un mismo número natural h.

En efecto, sea

$$\mathcal{H} = \{\ln(k) : k \in \mathcal{K}\}$$

Como $\mathcal{K}$ es multiplicativo y contiene elementos mayores que 1 y elementos menores que 1, resulta $\mathcal{H}$ un subconjunto aditivo de $\mathbb{R}$ en las condiciones del teorema 2.2. Si $\mathcal{H}$ es discreto, entonces $\mathcal{H} = \mathbb{Z}\alpha$ para algún real α positivo. Definiendo

$$\beta = e^{\alpha} = \frac{p^r}{q^s}$$

los elementos de $\mathcal{K}$ son exactamente los números

$$\mathcal{K} = \{\beta^m : m \in \mathbb{Z}\}$$

Por otra parte como $0 \in \mathcal{H}$, $1 \in \mathcal{K}$, de modo que existen números naturales i y j tales

$$1 = \frac{p^i}{q^j}$$

luego, de las identidades

$$p = \frac{p^{i+1}}{q^j} \quad \text{y} \quad \frac{1}{q} = \frac{p^i}{q^{j+1}}$$

obtenemos que p y $1/q$ están en $\mathcal{K}$. Dado que $\beta > 1$, existen números naturales n y m tales que

$$p = \beta^n \quad \text{y} \quad q = \beta^m$$

de donde β, que en principio es racional, debe ser un número natural.
Por otra parte, si $\mathcal{H}$ es denso en $\mathbb{R}$, $\mathcal{K}$ es denso en los reales positivos por la continuidad de la función exponencial.

Problema 5. *Mostrar que dado un número natural k existen infinitas potencias de 2 cuyo desarrollo decimal comienza con k.*

Por ejemplo:

$$\begin{array}{cc} k=1 & 2^0=1 \\ k=3 & 2^5=32 \\ k=6 & 2^6=64 \\ k=10 & 2^{10}=1024 \\ k=13 & 2^{17}=131072 \end{array}$$

El problema se reduce a encontrar números naturales n y m tal que

$$10^m k \leq 2^n < 10^m\,(k+1)$$

En tal caso $2^n = 10^m k + h$ con $0 \leq h < 10^m$ lo que garantiza que los dígitos iniciales de 2^n son los dígitos de k.
Del problema anterior sabemos que

$$\{2^n/10^m : n, m \in \mathbb{N}\}$$

es un conjunto denso en los reales positivos, luego el intervalo $[k, k+1)$ contiene infinitos números de este conjunto.

Nota: Por el problema 4, en el problema precedente, puede reemplazarse 2 por cualquier número natural que no sea una potencia de 10. También podría cambiarse la base de numeración y enunciarse un problema análogo.

3 En el Plano

Si consideramos el plano real $\mathbb{R}^2$ como grupo abeliano con la suma de vectores, no es cierto que un subgrupo de $\mathbb{R}^2$ sea denso o discreto, entendiendo en este caso por *subconjuntos densos*, aquellos conjuntos cuyos elementos pueden aproximar arbitrariamente cualquier vector del plano, y por *subconjuntos discretos*, aquellos conjuntos en los que cada uno de sus puntos puede ubicarse en el centro de un círculo que deje en su exterior a los puntos restantes del conjunto. Una definición más formal de estos conceptos se dará más adelante.
Como ejemplos tenemos:

i) Una recta por el origen, en el plano, es un subgrupo de $\mathbb{R}^2$ que no es discreto ni es denso en $\mathbb{R}^2$.

ii) Los puntos de coordenadas enteras forman un subgrupo discreto del plano.

iii) Los puntos de coordenadas racionales forman un subgrupo denso del plano.

iv) Los puntos con primer coordenada entera y segunda coordenada racional, forman un subgrupo del que no es discreto ni denso.

En el plano, considerando la distancia y norma euclídeas dadas por

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad \|x\| = \sqrt{x_1^2 + x_2^2}$$

para cada $x, y \in \mathbb{R}^2$, $x = (x_1, x_2)$ e $y = (y_1, y_2)$, puede afirmarse lo siguiente:

Teorema 3.1. *Sea $\mathcal{H}$ un subgrupo de $\mathbb{R}^2$ y*

$$\delta = \inf\{\|h\| : h \in \mathcal{H} \text{ y } h \neq 0\}$$

Entonces, $\mathcal{H}$ es un subgrupo discreto si y sólo si $\delta > 0$.

Demostración: Supongamos que $\mathcal{H}$ es un subgrupo discreto. Dado que $\mathcal{H}$ es un subgrupo, $0 \in \mathcal{H}$, y por ser $\mathcal{H}$ un subconjunto discreto de $\mathbb{R}^2$, existe $\varepsilon > 0$ tal que

$$\|h - 0\| = \|h\| > \varepsilon \qquad \forall h \in \mathcal{H}, h \neq 0$$

Luego $\delta > 0$.
Recíprocamente, si $\delta > 0$, para $h \in \mathcal{H}$ consideremos el círculo dado por

$$\|x - h\| < \delta$$

es decir la totalidad de puntos del plano que distan de h en menos que δ.
Si h' es un elemento de $\mathcal{H}$ en dicho círculo, se tiene:

$$\|h' - h\| < \delta$$

por la definición de δ, debe ser $h' - h = 0$, o sea $h' = h$. Se sigue que $\mathcal{H}$ es un subconjunto discreto de $\mathbb{R}^2$. ■

Observación: Un subconjunto discreto en el plano, y a la vez de la recta, es el formado por los elementos de la sucesión $\left(\frac{1}{n}, 0\right)$. A medida que n aumenta, es necesario un círculo más pequeño para aislar a $\left(\frac{1}{n}, 0\right)$ del resto de los elementos de la sucesión. En cambio, en un subgrupo discreto, sea en la recta o el plano, es posible aislar todos sus elementos con círculos del mismo radio. En efecto, el caso de la recta es claro, a partir de la caracterización dada en el teorema 2.1. En el plano, sea $\varepsilon > 0$ de modo que un círculo con radio ε aisla un elemento $h \in \mathcal{H}$ del resto de los elementos de $\mathcal{H}$, es decir

$$\left\{x \in \mathbb{R}^2 : \|x - h\| < \varepsilon\right\} \cap \mathcal{H} = \{h\}$$

Si dos elementos $f, g \in \mathcal{H}$ se encontraran a menor distancia que ε, entonces la distancia entre $h + f - g \in \mathcal{H}$ y h es

$$\|h + f - g - h\| = \|f - g\| < \varepsilon$$

por lo que debe ser

$$h + f - g = h$$

o sea $f = g$.
Concluímos que todos los puntos de $\mathcal{H}$ pueden ser aislados usando círculos con mismo radio.
Como consecuencia de la observación precedente, tenemos:

Proposición 3.2. *Si $\mathcal{H}$ es un subgrupo discreto del plano, una región acotada $\mathcal{F}$ del plano sólo puede contener un número finito de elementos de $\mathcal{H}$.*

Demostración: Dado que $\mathcal{F}$ es acotada, podemos elegir un círculo $\mathcal{D}$ que contenga a $\mathcal{F}$. Supongamos que con círculos de radio δ se puede aislar los elementos de $\mathcal{H}$ entre sí. Si c es el centro de $\mathcal{D}$ y ρ su radio, el círculo $\mathcal{D}'$ con centro c y radio $\delta + \rho$, contiene todos los discos, disjuntos dos a dos, dados por

$$\left\{x \in \mathbb{R}^2 : \|x - h\| < \delta\right\} \qquad \forall h \in \mathcal{H} \cap \mathcal{D}$$

lo que resulta de

$$\|x - c\| = \|x - h + h - c\| \leq \|x - h\| + \|h - c\| < \delta + \rho$$

El área de la figura formada por estos discos es

$$|\mathcal{H} \cap \mathcal{D}| \times \pi\delta^2$$

y no puede exceder al área de $\mathcal{D}'$, de modo que $|\mathcal{H} \cap \mathcal{D}|$, el número de elementos de $\mathcal{H}$ en $\mathcal{D}$, debe ser finito, y en consecuencia, también resulta finito el número de elementos de $\mathcal{H}$ en $\mathcal{F}$. ■

Consideremos ahora $\mathcal{C}^2 = \mathcal{C} \times \mathcal{C}$, el producto cartesiano del conjunto de complejos unitarios $\mathcal{C}$ consigo mismo. $\mathcal{C}^2$ tiene estructura de grupo abeliano definiendo

$$(z, w) \cdot (z', w') = (zz', ww')$$

En $\mathcal{C}^2$ definimos la distancia entre dos de sus elementos como

$$d\left((z, w), (z', w')\right) = \sqrt{|z - z'|^2 + |w - w'|^2}$$

Conservando las notaciones precedentes, una aplicación del teorema 3.1 es la siguiente:

Problema 6. *Si $\mathcal{H}$ es un subgrupo de $\mathcal{C}^2$, entonces $(1,1)$ se aproxima arbitrariamente con elementos de $\mathcal{H}$, o $\mathcal{H}$ es finito.*

Poniendo

$$z = \exp(2\pi i\alpha), \quad w = \exp(2\pi i\beta) \quad \text{con} \quad 0 \leq \alpha, \beta < 1$$

$\mathcal{C}^2$ queda parametrizado por

$$[0,1) \times [0,1) \subset \mathbb{R}^2.$$

Si $\mathcal{H}'$ es el subconjunto de $\mathbb{R}^2$ dado por

$$\mathcal{H}' = \left\{(\alpha,\beta) \in \mathbb{R}^2 : (\exp(2\pi i\alpha), \exp(2\pi i\beta)) \in \mathcal{H}\right\}$$

comprobamos sin mayor dificultad que $\mathcal{H}'$ es un subgrupo de $\mathbb{R}^2$ con su estructura aditiva. Si $(1,1)$ no pudiera ser aproximado arbitrariamente con elementos de $\mathcal{H}$, entonces $(0,0)$ no podrá ser aproximado arbitrariamente por elementos de $\mathcal{H}'$, en este caso, del teorema 3.1 se sigue que $\mathcal{H}'$ es discreto y, según la proposición 3.2, sólo puede tener un número finito de puntos en la región acotada $\mathcal{F} = [0,1) \times [0,1)$, luego $\mathcal{H}$ sería finito.

Llamaremos *rango de un subgrupo de* $\mathbb{R}^2$, a la dimensión del subespacio generado por sus elementos. Los subgrupos de rango 1, pueden ser tratados en forma análoga a los de la recta real, es decir, son discretos o densos en la recta que los contiene. Es claro que un subgrupo discreto de rango 1 tendrá la forma

$$\mathbb{Z}v = \{nv : n \in \mathbb{Z}\}$$

para algún vector v no nulo y de longitud mínima entre los vectores del subgrupo.
Un *retículo* en el plano, es un conjunto de la forma

$$\mathbb{Z}v \oplus \mathbb{Z}w = \{nv + mw : n, m \in \mathbb{Z}\}$$

donde v, w son vectores linealmente independientes de $\mathbb{R}^2$.
A continuación daremos una caracterización de los subgrupos discretos de rango 2 en el plano desde un contexto algebraico.

Teorema 3.3. *$\mathcal{H}$ es un subgrupo discreto de $\mathbb{R}^2$ si, y sólo si $\mathcal{H}$ es un retículo.*

Demostración: Sea $\mathcal{H}$ un retículo de $\mathbb{R}^2$ que indicaremos con $\mathbb{Z}v \oplus \mathbb{Z}w$. Es claro que $\mathcal{H}$ es un subgrupo de $\mathbb{R}^2$. Por otra parte, si en el vector $u = nv + mw$ es $m \neq 0$, consideremos l la recta que une el origen con v. Denotando por d a la distancia, tenemos las siguientes desigualdades

$$\|u\| \geq d(u,l) = d(mw,l) = |m|\, d(w,l) \geq d(w,l)$$

Si θ es el ángulo que encierran v y w, resulta

$$d(w,l) = \|w\| \times sen(\theta)$$

Simétricamente, se trata el caso $n \neq 0$ y en conclusión se obtiene que para todo $u \in \mathcal{H}$, $u \neq 0$ tenemos que

$$\|u\| \geq sen(\theta) \times \min\{\|v\|, \|w\|\}$$

Recíprocamente, dado $u \in \mathcal{H}$, $u \neq 0$, se sigue de la proposición 3.2 que el círculo dado por

$$\|x\| \leq \|u\|$$

contiene un número finito de elementos de $\mathcal{H}$. Podemos encontrar entonces, entre los elementos no nulos de $\mathcal{H}$, un vector v cuya longitud sea mínima. Sea entonces $\delta > 0$ definido por

$$\delta = \inf\{\|h\| : h \in \mathcal{H} \text{ y } h \neq 0\} = \|v\|$$

De esto se desprende que la distancia entre dos elementos distintos en $\mathcal{H}$ es mayor o igual que $\delta = \|v\|$.
Sea l la recta que une el origen con v. Es claro que $\mathcal{H} \cap l$ es un subgrupo discreto de l, y por la elección de v, debe ser $\mathcal{H} \cap l = \mathbb{Z}v$.
Dado que $\mathcal{H}$ es de rango 2, existen elementos de $\mathcal{H}$ que no están en l. Fijado $u \in \mathcal{H} - l$, la recta $l + u$ es paralela l y se tiene que

$$\mathcal{H} \cap (l + u) = \mathbb{Z}v + u$$

puesto que no hay puntos distintos en $\mathcal{H}$ que disten en menos que $\delta = \|v\|$. Por la misma razón, resulta que cualquier segmento en $l+u$ cuya longitud sea mayor que δ, debe contener un elemento de $\mathcal{H}$ en su interior, y consecuentemente la recta $l + u$ cortaría al círculo

$$\|x\| \leq \delta$$

en un segmento de longitud menor o igual que δ.
Es decir, que las rectas l y $l+u$ tienen una distancia que, como mínimo, es igual a $\frac{\sqrt{3}}{2}\delta$.
Pongamos

$$\gamma = \inf\{d(l + u, l) : u \in \mathcal{H} - l\}$$

Para dos rectas distintas $l + p$ y $l + q$ tenemos

$$d(l + q, l + p) = d(l + p - q, l) \geq \frac{\sqrt{3}}{2}\delta$$

lo que indica que γ es en realidad un mínimo. Sea $w \in \mathcal{H}$ tal que

$$\gamma = d(l + w, l)$$

Naturalmente que

$$\mathbb{Z}v \oplus \mathbb{Z}w \subseteq \mathcal{H}$$

Dado $u \in \mathcal{H}$ podemos expresar

$$u = \alpha v + \beta w$$

descomponiendo β en su parte entera más su mantisa

$$\beta = [\beta] + \{\beta\}$$

tenemos que

$$\alpha v + \{\beta\} w \in \mathcal{H}$$

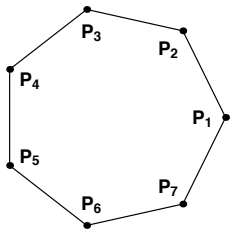
siendo

$$\begin{aligned} d(\alpha v + \{\beta\} w, l) &= d(\{\beta\} w, l) \\ &= \{\beta\} d(w, l) \\ &= \{\beta\} \gamma < \gamma \end{aligned}$$

por la minimalidad de γ, debe ser $\{\beta\} = 0$. Resulta entonces $\alpha v \in \mathcal{H} \cap l$, y con esto, $\alpha \in \mathbb{Z}$, es decir $\mathbb{Z}v \oplus \mathbb{Z}w = \mathcal{H}$. ■

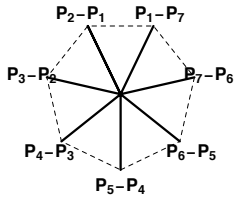
Problema 7. *Supongamos que un polígono regular de n lados tiene todos sus vértices en un retículo de* $\mathbb{R}^2$*. Entonces* $n = 3,\ 4$ *ó* 6*.*

Consideremos primero $n \geq 7$. Si $P_1, P_2, \ldots, P_n$ son los sucesivos vértices del polígono regular sobre un retículo los puntos $P_2 - P_1, P_3 - P_2, \ldots, P_n - P_{n-1}, P_1 -$

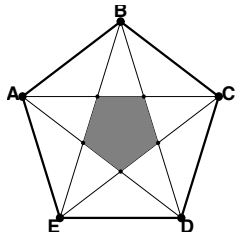


P_n serán también los vértices de un polígono regular sobre el mismo retículo, sólo que más pequeño, ya que el radio de la circunferencia que circunscribe a este último coincide con la longitud del lado del polígono original. Si R y r denotan los radios de las respectivas circunferencias circuns-criptas al primer y segundo polígono, tenemos

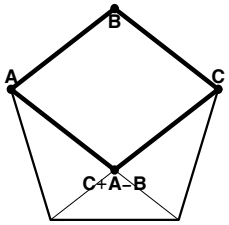
$$r = 2R\, sen\left(\frac{\pi}{n}\right)$$



Iterando este proceso, encontraríamos una sucesión de polígonos re-gulares sobre el retículo que converge a un punto, pero esto contradice el hecho que dos puntos en un retículo deben distar en más que un número $\delta > 0$.
Si $n = 5$ y A, B, C, D, E son los vértices de un pentágono regular sobre un retículo, los puntos $C + A - B$, $D + B - C$, $E + C - D$, $A + D - E$ y $B + E - A$ son los vértices de un pentágono regular sobre el mismo retículo, pero estos



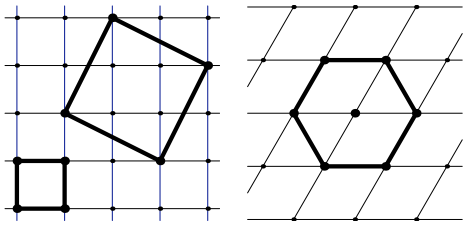
puntos son todos los que se obtienen al intersecar, dos a dos, las diagonales del pentágono A, B, C, D, E, y ahora utilizamos el mismo argumento que en el caso anterior.



Sobre el retículo $\mathbb{Z}^2$ se puede inscribir cuadrados y sobre el retículo

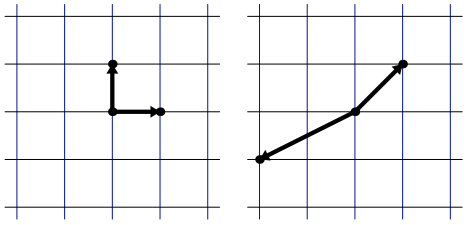
$$\mathbb{Z}\,(1,0) \oplus \mathbb{Z}\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$

se puede inscribir hexágonos regulares, y en consecuencia también triángulos equiláteros.



A continuación presentamos una versión en el plano, a la manera de lo expuesto en [3], de dos hechos que pueden ser enunciados con mayor generalidad (ver por ejemplo [4], [5] ó [9]). Estos son el lema de Blichfëldt y el teorema de Minkowski. Particularmente, el teorema de Minkowski es central en el estudio de la geometría de números.

Fijemos un retículo $\mathbb{Z}v \oplus \mathbb{Z}w$ en el plano. En particular, si $v = (1, 0)$ y $w = (0, 1)$ el correspondiente retículo es $\mathbb{Z}^2$. En lo que sigue, nos referiremos a los puntos del retículo como *puntos reticulares*. La si-guiente figura ilustra como un mismo retículo puede ser generado por distintos pares de vectores



El área del paralelogramo con vértices $0, v, w, v + w$ se llama *discriminante del retículo*. Es posible ver que los paralelogramos determinados por un par de vectores que generen el retículo, tienen todos la misma área (ver ejercicio *iii)* al final de estas notas).

Lema 3.4. *(Blichfëldt) Sea $n \geq 0$ un número entero. Una figura $\mathcal{F}$ acotada de área $\delta > n$ puede ser ubicada en el plano de modo que cubra al menos $n + 1$ puntos reticulares en $\mathbb{Z}^2$.*

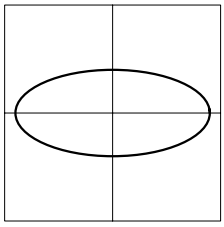
Demostración: Dado $(i,j) \in \mathbb{Z}^2$, consideremos los cuadrados dados por

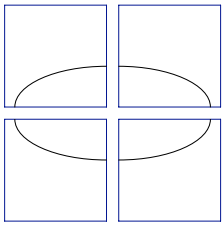
$$\mathcal{C}_{ij} = \{(x,y) : i < x < i+1, j < y < j+1\}$$

El área de $\mathcal{F}$ resulta igual a la suma de las áreas de las figuras dadas por

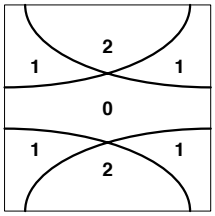
$$\mathcal{F}_{ij} = \begin{cases} (\mathcal{F} \cap \mathcal{C}_{ij}) - (i,j) & \text{si} \quad \mathcal{F} \cap \mathcal{C}_{ij} \neq \emptyset \\ \emptyset & \text{si} \quad \mathcal{F} \cap \mathcal{C}_{ij} = \emptyset \end{cases}$$

Todas las figuras $\mathcal{F}_{ij}$ tienen área menor o igual a 1. Podemos descomponer el





cuadrado $\mathcal{C}_{00}$ en regiones $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_m$ donde $\mathcal{R}_k$ es el conjunto de puntos cubiertos por exactamente k de las $\mathcal{F}_{ij}$. Ahora las regiones $\mathcal{R}_k$ son disjuntas



dos a dos y si $\delta_0, \delta_1, \ldots, \delta_m$ denotan sus respectivas áreas, tenemos

$$\begin{aligned} \delta &= 0 \times \delta_0 + 1 \times \delta_1 + \cdots + m \times \delta_m \\ &\leq m\,(\delta_0 + \delta_1 + \cdots + \delta_m) \leq m \end{aligned}$$

Como $\delta > n$, se sigue que existe un punto (a, b) que es cubierto por al menos $n + 1$ de las figuras $\mathcal{F}_{ij}$, para estos pares (i, j), se tiene que los puntos

$$(a, b) + (i, j)$$

son puntos en $\mathcal{F}$. Si trasladamos la figura para que uno de estos puntos quede sobre un punto reticular, entonces, todos los puntos $(a, b) + (i, j)$ indicados anteriormente serán puntos reticulares. ■

Nota: En el enunciado del lema, la hipótesis que la figura considerada sea acotada no es necesaria, se agrega para simplificar la demostración. Es posible mostrar que hay una parte acotada de la figura cuya área es mayor que n.

Una figura $\mathcal{F}$ es *convexa* si para cada par de puntos en $\mathcal{F}$ el segmento que los une está contenido en $\mathcal{F}$.
El segmento que une dos puntos p y q puede parametrizarse como:

$$[p, q] = \{\lambda p + (1 - \lambda)\, q : 0 \leq \lambda \leq 1\}$$

Una figura $\mathcal{F}$ es *simétrica* cuando verifica que; si $p \in \mathcal{F}$, entonces $-p \in \mathcal{F}$.

Teorema 3.5. *(Minkowski) Dado un retículo $\mathcal{R}$ con discriminante Δ, cualquier figura convexa y simétrica cuya área sea mayor que 4Δ, contiene al menos un punto reticular no nulo.*

Demostración: Sea

$$\mathcal{R} = \mathbb{Z}v \oplus \mathbb{Z}w$$

La transformación lineal $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ dada por

$$\varphi\,(\alpha, \beta) = \alpha v + \beta w$$

es un isomorfismo que aplica $\mathbb{Z}^2$ en $\mathcal{R}$ y su jacobiano es precisamente el discriminante de $\mathcal{R}$, es decir Δ. Sea $\mathcal{G} \subseteq \mathbb{R}^2$ la preimagen de $\mathcal{F}$ a través de φ, entonces

$$\Delta \times |\mathcal{G}| = |\mathcal{F}| > 4\Delta$$

donde con las barras indicamos el área de la figura. Luego

$$|\mathcal{G}| > 4$$

Si definimos

$$\frac{1}{2}\mathcal{G} = \left\{\frac{1}{2}u : u \in \mathcal{G}\right\}$$

resulta

$$\left|\frac{1}{2}\mathcal{G}\right| = \frac{1}{4}\left|\mathcal{G}\right| > 1$$

Por el lema de Blichfëldt, $\frac{1}{2}\mathcal{G}$ puede desplazarse en el plano de modo que cubra al menos dos puntos reticulares en $\mathbb{Z}^2$. En consecuencia, $\frac{1}{2}\mathcal{F}$, la imagen por φ de $\frac{1}{2}\mathcal{G}$, puede desplazarse en el plano de modo que cubra al menos dos puntos reticulares en $\mathcal{R}$. Notemos estos dos puntos como

$$p = \tfrac{1}{2}p_0 + r \quad \text{y} \quad q = \tfrac{1}{2}q_0 + r$$

donde $p, q \in \mathcal{R}$ y $p_0, q_0 \in \mathcal{F}$. Se sigue que

$$0 \neq p - q = \frac{1}{2}p_0 + \frac{1}{2}\left(-q_0\right) \in \mathcal{R}$$

Por ser $\mathcal{F}$ simétrica, $-q_0 \in \mathcal{F}$, y $p - q$ es el punto medio del segmento que une p_0 con $-q_0$, resulta $p - q \in \mathcal{R} \cap \mathcal{F}$ pues $\mathcal{F}$ es convexa. ■

Los problemas que siguen a continuación ilustran aplicaciones del teorema de Minkowski.

Problema 8. *Todo número primo de la forma $4k+1$ es suma de dos cuadrados.*

Si p es un primo de la forma $4k + 1$, es conocido que -1 es residuo cuadrático módulo p. Es decir, existe un entero a tal que $a^2 + 1$ es divisible por p. Una demostración de este hecho puede obtenerse usando el teorema de Wilson que establece que

$$(p-1)! \equiv -1 \quad (\mod p)$$

Por otra parte, si elegimos el sistema de restos $0, \pm 1, \pm 2, \cdots, \pm\frac{p-1}{2}$, tenemos

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \quad (\mod p)$$

siendo p de la forma $4k + 1$, resulta $(p-1)!$ un residuo cuadrático.
Consideremos el retículo $\mathcal{R}$ dado por

$$\mathbb{Z}\left(p, 0\right) \oplus \mathbb{Z}\left(a, 1\right)$$

donde $a \in \mathbb{Z}$ es tal que $a^2 + 1$ es divisible por p. El discriminante de este retículo es p. Si $\mathcal{C}$ es el círculo dado por

$$\mathcal{C} = \left\{(x, y) : x^2 + y^2 < 2p\right\}$$

el área de $\mathcal{C}$ es

$$2p\pi > 4p$$

Por el teorema de Minkowski, $\mathcal{C}$ contiene un punto reticular no nulo, es decir, existe $(n, m) \neq (0, 0)$ tal que

$$0 < (np + ma)^2 + m^2 < 2p$$

Pero

$$(np + ma)^2 + m^2 \equiv m^2 \left(a^2 + 1\right) \equiv 0 \quad (\mod p)$$

De aquí que

$$p = (np + ma)^2 + m^2$$

Observación: En forma similar al problema anterior, a partir de la versión general del teorema de Minkowski (ver [4], [5], [6] ó [9]), se puede probar el *teorema de Langrange de los cuatro cuadrados* que afirma que todo número natural es suma de cuatro cuadrados, por ejemplo

$$\begin{aligned} 1 &= 1^2 + 0^2 + 0^2 + 0^2 \\ 7 &= 2^2 + 1^2 + 1^2 + 1^2 \\ 30 &= 5^2 + 2^2 + 1^2 + 0^2 \end{aligned}$$

Este teorema, también conocido como la conjetura de Bachet, fue probado por Lagrange en 1770. Usando propiedades básicas de los números cuaterniónicos, el problema puede reducirse a ver que todo número primo positivo p es suma de cuatro cuadrados. A tal fin será necesario además establecer que -1 es suma de dos cuadrados, módulo p (ver el ejercicio *xv)* al final de estas notas).
Asociados con las descomposiciones de un número natural en suma de cuadrados podemos mencionar los siguientes teoremas debidos a Jacobi, (ver [1] ó [7]).

Sea n un número natural.
El número de pares enteros (p, q) tales que $p^2 + q^2 = n$ es igual a 4 veces la diferencia entre el número de divisores de n congruentes con 1 módulo 4 y el número de divisores de n congruentes con 3 módulo 4.
El número de cuaternas enteras (p, q, r, s) tales que $p^2 + q^2 + r^2 + s^2 = n$ es igual a 8 veces la suma de todos los divisores de n que no son congruentes con 0 módulo 4.

Volviendo al teorema de Minkowski, si la figura considerada en él es además compacta, o sea cerrada y acotada, la condición sobre el área puede ser debilitada como se muestra a continuación.

Proposición 3.6. *Dado un retículo $\mathcal{R}$ con discriminante Δ, cualquier figura compacta convexa y simétrica cuya área sea mayor o igual que 4Δ, contiene al menos un punto reticular no nulo.*

Demostración: Sea $\mathcal{F}$ la figura considerada. Para $\lambda > 1$ considere-mos la figura

$$\mathcal{F}_\lambda = \{\lambda v : v \in \mathcal{F}\}$$

Es claro que $\mathcal{F}_\lambda$ es convexa y simétrica, además

$$|\mathcal{F}_\lambda| = \lambda^2 \, |\mathcal{F}| > |\mathcal{F}| \geq 4\Delta$$

Por el teorema de Minkowski, $\mathcal{F}_\lambda$ contiene un punto reticular no nulo.
Consideremos la sucesión de figuras dadas por

$$\mathcal{F}_{1+\frac{1}{n}} \qquad n \geq 1$$

Supongamos que $0 = (0,0)$ sea el único punto reticular en $\mathcal{F}$. En la región dada por

$$\mathcal{F}_2 - \mathcal{F}$$

existe un conjunto finito $v_1, v_2, \ldots, v_k$ de puntos reticulares.
Dado que el área de $\mathcal{F}$ es mayor que cero, $\mathcal{F}$ no puede estar contenida en una recta, en consecuencia $\mathcal{F}$ contiene dos vectores u y v que son linealmente independientes, luego, por ser $\mathcal{F}$ convexa y simétrica, el paralelogramo con vértices $\pm u, \pm v$ está incluído en $\mathcal{F}$. De este hecho se sigue que si l es una recta que pasa por el origen, $l \cap \mathcal{F} \neq \{0\}$ y por ser esta intersección un subconjunto simétrico, convexo, cerrado y acotado de l, se tiene que existe un vector $w \neq 0$ en l tal que

$$l \cap \mathcal{F} = [-w, w]$$

En particular, para las rectas $l_i = \mathbb{R}v_i$, $(1 \leq i \leq k)$, encontraremos escalares λ_i con $0 < \lambda_i < 1$ y tales que

$$l_i \cap \mathcal{F} = [-\lambda_i v_i, \lambda_i v_i] \quad \text{y} \quad \lambda v_i \notin \mathcal{F} \quad \text{si} \quad \lambda > \lambda_i$$

Si elegimos $n \in \mathbb{N}$ tal que

$$1 + \frac{1}{n} < \frac{1}{\lambda_i}, \ \forall i$$

encontramos que

$$v_i \notin \mathcal{F}_{1+\frac{1}{n}}, \ \forall i$$

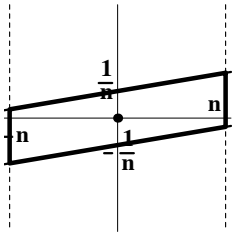
pues

$$\left\| \left(1 + \frac{1}{n}\right) \lambda_i v_i \right\| = \left(1 + \frac{1}{n}\right) \lambda_i \, \|v_i\| < \|v_i\|$$

Resulta entonces que 0 es el único punto reticular en $\mathcal{F}_{1+\frac{1}{n}}$, pero el área de $\mathcal{F}_{1+\frac{1}{n}}$ es mayor que 4Δ, y esto contradice el teorema de Minkowski. En consecuencia $\mathcal{F}$ contiene un punto reticular distinto de 0. ■

Problema 9. *Dados un número real α y un número entero n existen números enteros p y q tales que $0 < q \leq n$ y*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qn}$$



Consideremos la figura $\mathcal{P}$ dada por el interior del paralelogramo cerrado limitado por las rectas

$$y - \alpha x = \tfrac{1}{n}, \quad y - \alpha x = -\tfrac{1}{n}, \quad x = n \quad \text{y} \quad x = -n$$

$\mathcal{P}$ es una figura convexa y simétrica y su área es 4. Por la proposición 3.6 existe un par $(q, p) \neq (0, 0)$ en el retículo $\mathbb{Z}^2$ tal que

$$p - \alpha q \geq \tfrac{1}{n}, \quad p - \alpha q \geq -\tfrac{1}{n}, \quad q \leq n \quad \text{y} \quad q \geq -n$$

o sea

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{n\,|q|}$$

Para concluir, observemos que, teniendo en cuenta la simetría de $\mathcal{F}$, q puede elegirse positivo.

Problema 10. *Mostrar que si $d \in \mathbb{N}$ y d no es un cuadrado perfecto, entonces la ecuación*

$$x^2 - dy^2 = 1$$

tiene infinitas soluciones enteras.

Supongamos que el par (m, n) sea una solución entera de la ecuación distinta de $(\pm 1, 0)$ y sin pérdida de generalidad asumamos que $m > 0$. Entonces descomponemos

$$m^2 - n^2 d = \left(m + n\sqrt{d}\right)\left(m - n\sqrt{d}\right) = 1$$

y si $k \in \mathbb{N}$, tenemos que

$$\left(m + n\sqrt{d}\right)^k \left(m - n\sqrt{d}\right)^k = 1$$

Pero entonces existen enteros m_k y n_k tales que

$$\left(m + n\sqrt{d}\right)^k = m_k + n_k\sqrt{d} \quad \text{y} \quad \left(m - n\sqrt{d}\right)^k = m_k - n_k\sqrt{d}$$

de donde

$$m_k^2 - n_k^2 d = 1$$

La sucesión (m_k, n_k) está dada por la ley recursiva

$$\begin{bmatrix} m_{k+1} & n_{k+1} \end{bmatrix} = \begin{bmatrix} m_k & n_k \end{bmatrix} \begin{bmatrix} m & n \\ dn & m \end{bmatrix}$$

Si notamos con A a la matriz

$$A = \begin{bmatrix} m & n \\ dn & m \end{bmatrix}$$

se tiene que A es inversible con determinante igual a 1 y la sucesión puede reescribirse como

$$\begin{bmatrix} m & n \end{bmatrix} A^k \quad \text{con} \quad k \geq 0$$

Ahora, si para valores dos distintos de k los correspondientes elementos de esta suceción coincidieran, podríamos simplificar la identidad a una expresión del tipo

$$\begin{bmatrix} m & n \end{bmatrix} A^j = \begin{bmatrix} m & n \end{bmatrix}$$

para algún entero $j > 0$. Esto significa que 1 debe ser valor propio de A^j, pero siendo los valores propios de A iguales a

$$m + \sqrt{m^2 - 1} \quad \text{y} \quad m - \sqrt{m^2 - 1}$$

es decir el primero mayor que 1 y el segundo menor que 1, los valores propios de A^j son precisamente

$$\left(m + \sqrt{m^2 - 1}\right)^j \quad \text{y} \quad \left(m - \sqrt{m^2 - 1}\right)^j$$

siendo el primero mayor que 1 y el segundo menor que 1, lo que contradice la condición que 1 sea valor propio de A^j, luego la sucesión no tiene términos repetidos.
Resta ver que hay al menos una solución distinta de $(\pm 1, 0)$.
Usando el resultado del problema 9, para $n = 1$, existe un par $(q_0, p_0) \in \mathbb{Z}^2$ tal que

$$\left| q_0\sqrt{d} - p_0 \right| < 1 \quad \text{y} \quad 0 < q_0 \leq 1$$

es claro que q_0 es igual a 1 y p_0 es la parte entera de $\sqrt{d}$. Elijamos ahora $n_1 \in \mathbb{N}$ tal que

$$\frac{1}{n_1} < \left| q_0\sqrt{d} - p_0 \right|$$

y nuevamente usando el problema 9, tomemos un par $(q_1, p_1) \in \mathbb{Z}^2$ tal que

$$\left| q_1\sqrt{d} - p_1 \right| < \tfrac{1}{n_1} \quad \text{y} \quad 0 < q_1 \leq n_1$$

Ahora fijamos $n_2 \in \mathbb{N}$ tal que

$$\frac{1}{n_2} < \left| q_1\sqrt{d} - p_1 \right|$$

y elegimos $(q_2, p_2) \in \mathbb{Z}^2$ tal que

$$\left| q_2\sqrt{d} - p_2 \right| < \tfrac{1}{n_2} \quad \text{y} \quad 0 < q_2 \leq n_2$$

continuando de esta manera obtenemos una sucesión $(q_i, p_i) \in \mathbb{Z}^2$ y una sucesión $n_i \in \mathbb{N}$ tales que

$$\tfrac{1}{n_{i+1}} < \left| q_i\sqrt{d} - p_i \right| \qquad \left| q_i\sqrt{d} - p_i \right| < \tfrac{1}{n_i} \qquad 0 < q_i \leq n_i$$

De estas desigualdades, encontramos que

$$|p_i| < q_i\sqrt{d} + \frac{1}{n_i} < n_i\sqrt{d} + 1$$

y luego

$$\left| q_i^2 d - p_i^2 \right| = \left| q_i\sqrt{d} - p_i \right| \left| q_i\sqrt{d} + p_i \right| < \frac{1}{n_i}\left(2n_i\sqrt{d} + 1\right) < 2\sqrt{d} + 1$$

Por otra parte, en la sucesión (q_i, p_i) todos los pares son distintos entre sí dado que los valores

$$\left| q_i\sqrt{d} - p_i \right|$$

forman una sucesión estrictamente decreciente. Como la sucesión de enteros $p_i^2 - q_i^2 d$ está acotada, debe haber una cantidad infinita de pares (q_i, p_i) tal que

$$p_i^2 - q_i^2 d = k$$

para algún número entero $k \neq 0$. Entonces podemos elegir dos soluciones distintas (α, β) y (γ, δ) de la ecuación anterior tales que

$$\alpha \equiv \gamma \pmod{k} \quad \text{y} \quad \beta \equiv \delta \pmod{k}$$

Si denotamos

$$\begin{aligned} \zeta &= \left(\alpha + \beta\sqrt{d}\right)\left(\gamma - \delta\sqrt{d}\right) \\ &= (\alpha\gamma - \beta\delta d) + (\beta\gamma - \alpha\delta)\sqrt{d} \\ &= p + q\sqrt{d} \end{aligned}$$

tenemos que

$$\begin{aligned} p &= \alpha\gamma - \beta\delta d \equiv \alpha^2 - \beta^2 d = 0 \pmod{k} \\ q &= \beta\gamma - \alpha\delta \equiv \beta\alpha - \alpha\beta = 0 \pmod{k} \end{aligned}$$

luego existen enteros m y n tales que

$$p = km \quad \text{y} \quad q = kn$$

y resulta

$$\begin{aligned} m^2 - n^2\sqrt{d} &= \left(m + n\sqrt{d}\right)\left(m - n\sqrt{d}\right) \\ &= \frac{1}{k^2}\left(p + q\sqrt{d}\right)\left(p - q\sqrt{d}\right) \\ &= \frac{1}{k^2}\left(\alpha + \beta\sqrt{d}\right)\left(\gamma - \delta\sqrt{d}\right)\left(\alpha - \beta\sqrt{d}\right)\left(\gamma + \delta\sqrt{d}\right) \\ &= \frac{1}{k^2}\left(\alpha^2 - \beta^2\sqrt{d}\right)\left(\gamma^2 - \delta^2\sqrt{d}\right) \\ &= 1 \end{aligned}$$

La ecuación $x^2 - dy^2 = k$ es conocida como *la ecuación de Pell* y fue tratada por Lagrange usando fracciones continuas (ver [8]).

Finalizamos estas notas incluyendo en ellas las definiciones formales, en el espacio $\mathbb{R}^n$, de algunos de los conceptos utilizados hasta aqui.

Consideremos $\mathbb{R}^n$ provisto con la métrica usual. Para $x, y \in \mathbb{R}^n$, con $d(x, y)$ denotaremos la distancia euclídea entre x e y dada por

$$d(x, y) = \sqrt{\sum_i (x_i - y_i)^2}$$

Dados $\mathcal{A}$ y $\mathcal{B}$, con $\mathcal{A} \subseteq \mathcal{B}$, dos subconjuntos de $\mathbb{R}^n$, decimos que $\mathcal{A}$ *es denso en* $\mathcal{B}$ si dados $b \in \mathcal{B}$ y $\varepsilon > 0$ y , existe $a \in \mathcal{A}$ tal que $d(a,b) < \varepsilon$.
Un subconjunto $\mathcal{A}$ de $\mathbb{R}^n$ se dice *discreto* si dado $a \in \mathcal{A}$, existe $\varepsilon > 0$ tal que

$$\mathcal{A} \cap \{x \in \mathbb{R}^n : d(x,a) < \varepsilon\} = \{a\}$$

$\mathbb{R}^n$ con la suma usual es un grupo abeliano. Un subgrupo G de $\mathbb{R}^n$ se dirá *subgrupo denso* o *subgrupo discreto* si G es un conjunto denso o si es un conjunto discreto. El *rango de un subgrupo* es la dimensión del subespacio generado por sus elementos.
Finalmente, *un retículo* es un subgrupo de rango n de la forma

$$\mathcal{R} = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n \qquad (v_i \in \mathbb{R}^n)$$

siendo su *discriminante* el valor absoluto del determinante de la matriz que tiene por filas a los vectores $v_1, v_2, \ldots, v_n$. Los resultados vistos en el plano se extienden en el ejercicio *iv)* y la consistencia de la definición del discriminante se plantea en el ejercicio *iii)*.

4 Ejercicios propuestos

i) Sea $\mathcal{H}$ el subgrupo de $\mathbb{R}$ dado por

$$\mathcal{H} = \left\{ \frac{2n}{3} + \frac{4m}{5} + \frac{6k}{7} : n, m, k \in \mathbb{Z} \right\}$$

Decidir si $\mathcal{H}$ es denso o discreto, de ser discreto expresarlo en la forma $\mathbb{Z}r$.
ii) Dados los números racionales $q_1, q_2, \ldots, q_m$ y el subgrupo de $\mathbb{R}$ definido por

$$\mathcal{H} = \{n_1 q_1 + n_2 q_2 + \cdots + n_m q_m : n_i \in \mathbb{Z}\}$$

Decidir si $\mathcal{H}$ es denso o discreto.
iii) Mostrar que el discriminante de un retículo no depende de la base que lo defina.
iv) Considerando $\mathbb{R}^n$ con la suma de vectores y la norma euclídea, generalizar la proposición 3.2 y el teorema 3.3.
v) Mostrar que la intersección de dos subgrupos es un grupo discreto si uno de ellos lo es.
vi) ¿Qué polígonos regulares pueden inscribirse en el retículo $\mathbb{Z}^2$?
vii) Si $\mathcal{H}$ es un subgrupo discreto del plano, mostrar que en un círculo dado contiene a lo sumo un número finito de puntos de $\mathcal{H}$. ¿Es cierta esta afirmación si $\mathcal{H}$ no es subgrupo?

viii) Si $\mathcal{H}$ es un subgrupo discreto del plano, mostrar que existen vectores u y v en $\mathbb{R}^2$, tales que $\mathcal{H} = \{nu + mv : n, m \in \mathbb{Z}\}$.
ix) Si $\mathcal{L}$ es una recta por el origen $\mathbb{R}^2$, un subgrupo de $\mathcal{L}$ es discreto o denso. Si se proyectan los puntos de coordenadas enteras sobre $\mathcal{L}$ se obtiene un subgrupo de $\mathcal{L}$, ¿en qué casos es este subgrupo discreto y en qué casos es denso?
x) Si las asíntotas de una hipérbola contienen cada una al menos dos puntos de coordenadas enteras, mostrar que en la hipérbola hay a lo sumo un número finito de puntos con coordenadas enteras.
xi) ¿Es cierto que si una de las asíntotas de una hipérbola pasa por dos puntos de coordenadas enteras, entonces ocurre lo mismo con la otra asíntota?.
xii) Mostrar que la ecuación

$$ax^2 + 2bxy + cy^2 = 1$$

tiene un número finito de soluciones enteras si a, b son enteros y existe un número natural n tal que $n^2 = b^2 - ac$.
xiii) Hallar las soluciones enteras de la ecuación

$$xy + 3x - 5y = 75$$

xiv) Sea

$$Q(x, y) = ax^2 + 2bxy + cy^2$$

una forma cuadrática positiva definida. Demostrar que

$$\min_{n,m \in \mathbb{Z}} \{Q(m, n) \neq 0\} \leq \frac{2}{\sqrt{3}} \sqrt{ac - b^2}$$

xv) Usando la versión general del teorema de Minkowski (ver [4], [5] ó [9]) es posible probar el teorema de los cuatro cuadrados:
a) Si dos números naturales son suma de cuatro cuadrados, probar que el producto de estos es suma de cuatro cuadrados.
b) Dado un número primo p, probar que la ecuación de congruencias

$$m^2 + n^2 \equiv -1 \quad (\mod p)$$

admite solución (ver por ejemplo [2] ó [5]).
c) Sea p un número primo y sean m y n soluciones de la ecuación en *b)*. Considerando el retículo de $\mathbb{R}^4$

$$\mathcal{R} = \mathbb{Z}(p, 0, 0, 0) \oplus \mathbb{Z}(0, p, 0, 0) \oplus \mathbb{Z}(m, n, 1, 0) \oplus \mathbb{Z}(m, -n, 0, 1)$$

1) Mostrar que el discriminante de $\mathcal{R}$ es p^2.
2) Probar que si $(x, y, z, t) \in \mathcal{R}$ entonces $x^2 + y^2 + z^2 + t^2 \equiv 0 \quad (\mod p)$.
3) Aplicar el teorema de Minkowski teniendo en cuenta la esfera centrada en el origen cuyo radio es $2\sqrt{p}$.

xvi) Sea z un complejo unitario, $\mathcal{H} = \{z^n : n \in \mathbb{N}\}$. Probar que $\mathcal{H}$ es denso en los complejos unitarios ó z es una raíz de la unidad .
xvii) ¿Es denso $\left\{\frac{n\,\pi}{m} : n, m \in \mathbb{N}\right\}$ en los reales positivos?
xviii) Sean $z_1, ..., z_n$ complejos unitarios. Mostrar que dado $\varepsilon > 0$, existe un número natural n tal que $|z_i^n - 1| < \varepsilon\ \forall i = 1, 2, ..., n$.
xix) El conjunto de todas las raíces de la unidad ¿es denso en los complejos unitarios?
xx) Sea $f(x)$ un polinomio mónico con coeficientes enteros tal que sus raíces son complejos unitarios. Probar que las raíces de $f(x)$ son raíces de la unidad. (Sugerencia: usar *xviii)*) y el siguiente hecho: si $z_1, ..., z_n$ son las raíces de $f(x)$ entonces para $m \in \mathbb{N}$ el polinomio

$$g\,(x) = \prod (x - z_i^m)$$

es mónico y con coeficientes enteros.

Referencias

[1] Andrews, G., Ekhad, S., Zeilberger, D., *A short proof of Jacobi's formula for the number of representations of an integer as the sum of four squares.* American Mathematical Monthly **100**, 1993, 274-276.
[2] Araujo, J.O., Fernández, L. B., *Contando con Sumas de Gauss.* Divulgaciones Matemáticas, vol. 12, N^{o}2, 2004, 171-180.
[3] De Guzmán, M., *Mirar y Ver.* Red Olímpica, 1993.
[4] Hardy, G., Wright, E., *An introduction to the theory of numbers.* 5^{o}edición, Oxford, 1979.
[5] Ivorra Castillo, C.,*Teoría de Números*, 2004. Url: www.uv.es/˜ivorra/ Libros/ Numeros.pdf
[6] Jacobi, C. G. J., *Note sur la décomposition d 'un nombre donné en quatre carrés.* J. Reine Angew. Math. **3** (1828)., 191. Werke, vol.I, 247.
[7] Lagrange, J. L., Nouveau Mém. Acad. Roy. Sci. Berlin (1772), 123-133; *Oevres*, vol. 3, 189-201.
[8] Le Veque, W.J., *Teoria Elemental de los Números.* Herreros Hnos. México. 1968.
[9] Narkiewicz, W., *Number Theory.* World Scientific Publishing Co. 1983.

Fac. de Ciencias Exactas, UNICEN,
Tandil, 7000 Buenos Aires, Argentina
araujo@exa.unicen.edu.ar, lfernan@exa.unicen.edu.ar