ESTALMAT ANDALUCÍA ORIENTAL

Geometría en una retícula-2

Segundo curso (20/10/2018)

2018–2019

Ponentes:
Pascual Jara
Magdalena Rodríguez

Índice general

Vamos a estudiar problemas relativos a polígonos simples (aquellos en los que los lados no se cruzan) cuyos vértices son puntos de una retícula rectangular (que podemos suponer es la retícula entera). Como aplicación vamos a estudiar algunos otros problemas aritméticos y geométricos que surgen en una retícula de forma natural, utilizando como modelo algebraico a los números enteros de Gauss. Haremos un breve estudio de los enteros de Gauss, centrándonos en los números primos. Como aplicaciones estudiaremos circunferencias y círculos sobre una retícula y otras actividades.

Introducción

En Matemáticas amén de trabajar en el desarrollo del cálculo, automático o no, conviene orientarse en la construcción de modelos de situaciones reales; para ello tenemos que construir un modelo de forma clara y precisa, dar las reglas a las que nos vamos a someter y determinar los resultados posibles de la teoría así construida. En este contexto, y siguiendo la intuición geométrica, el trabajar en una retícula puede ser de interés, pues vemos de forma natural las restricciones de nuestro modelo en contraposición a la geometría del plano que todo hemos estudiado y usado. En esta nueva geometría tenemos restricciones que no se tiene en la geometría usual del plano, y por tanto los resultados que podemos establecer, aunque similares a los clásicos, deben ser adaptados a la realidad que nos hemos dado.

Existen dos modelos de retículas que podemos usar; vamos a seguir con el ya usado de una retícula cuadrada discreta formada por ejes ortogonal. En ella vamos a establecer algunos resultados, propios de la geometría discreta y los relacionaremos con los resultados clásicos. Veremos también las interrelaciones que existen entre distintas partes de la Matemática, como son el álgebra y la geometría, y veremos aplicaciones a la industria, la economía y otras ramas del saber, pero no es nuestra intención explorar estas aplicaciones, sino, de una forma lúdica aproximarnos a resultados profundos de la teoría y la aplicaciones.

El soporte teórico nos lo van a proporcionar las números enteros de Gauss; éstos son números complejos $a + bi$, con a y b enteros; de esta forma los enteros de Gauss son los puntos de una retícula como la que queremos estudiar, y podemos dar una base algebraica y computacional a la teoría.

Hoy no vamos a probar, de forma explícita, los resultados que vamos a ir obteniendo, pero si vamos a procurar que vosotros deduzcáis los fórmulas más relevantes que van a aparecer. Bueno, en realidad vamos a demostrar algún resultado, más bien un Teorema, para incitaros en el uso de técnicas de razonamiento matemático avanzado. Esperamos que no sea demasiado difícil para vosotros.

Agradeceríamos al lector que nos facilite sugerencias o comentarios sobre este texto, posibles errores y erratas y posibles extensiones de la teoría. Para ello puede utilizar la página

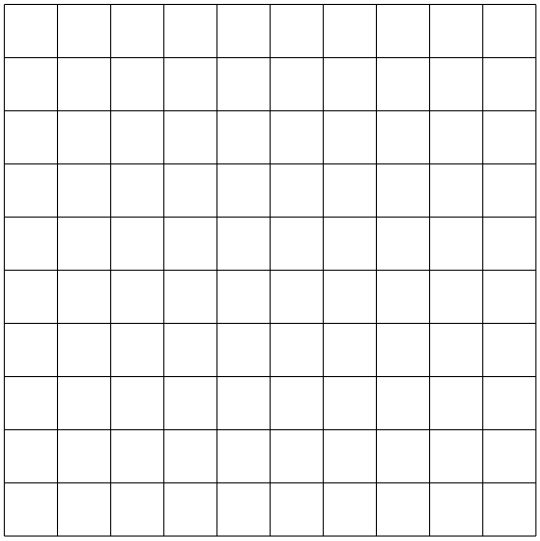
`http://www.ugr.es/local/anillos/textos/pick2.htm`

Índice de temas

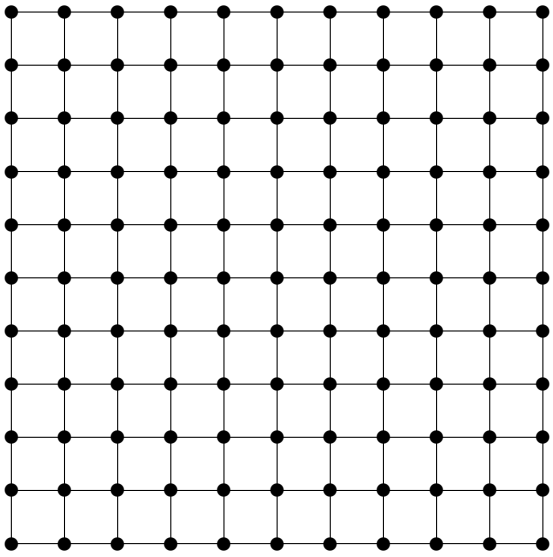
1. ¿Qué es una retícula?

Una retícula es la configuración de rectas, horizontales y verticales, que se obtienen en el plano al considerar las rectas horizontales que pasan por los puntos $(0, a)$, con $a \in \mathbb{Z}$ y las rectas verticales que pasan por los puntos $(a, 0)$, con $a \in \mathbb{Z}$.

Por lo tanto una retícula es algo parecido a lo siguiente:

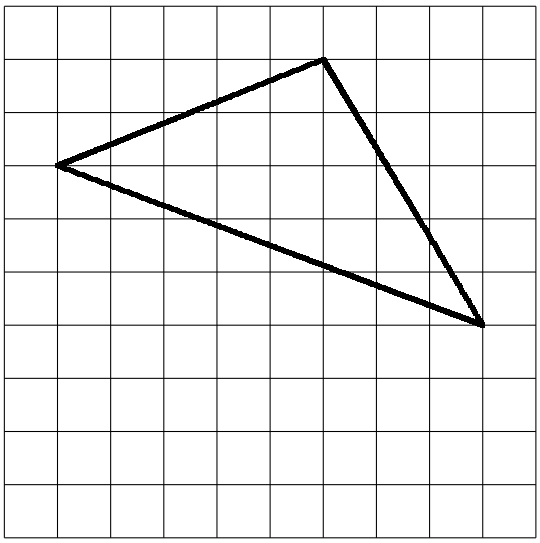


A nosotros nos interesan sólo los puntos de la retícula, los que determinan las intersecciones de estas rectas, esto es, los que aparecen señalados con un circulito negro.



Por razones de estética no vamos a dibujar con estos circulitos negros los puntos de la retícula, salvo cuando sea necesario destacar algo con ellos.

Una figura en una retícula está delimitada por segmentos que van de un punto de la retícula a otro. Un polígono reticulado es un polígono que es una figura en la retícula. Un triángulo reticulado es, por ejemplo:



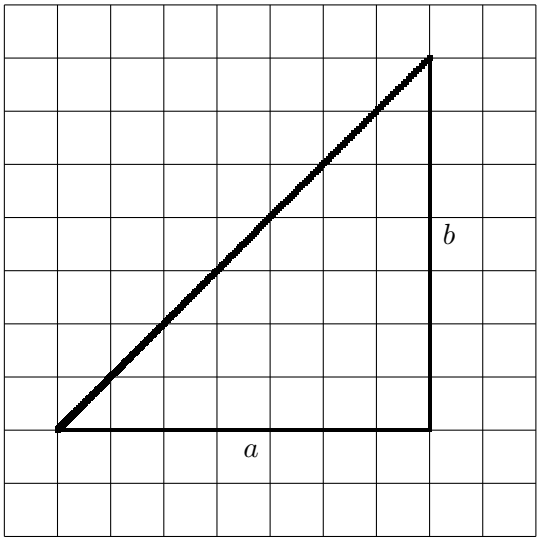
2. Medidas en una retícula

¿Qué medidas podemos hacer en una retícula?, esto es, ¿qué números nos aparecen como distancias entre dos puntos de una retícula?

Una simple aplicación del Teorema de Pitágoras nos dice que los números que nos aparecen son aquellos de la forma

$$\sqrt{a^2 + b^2}$$

donde $a, b \in \mathbb{Z}$.



Actividad: Haz una lista de los primeros números que aparecen como distancias entre puntos de la retícula. ¿Echas en falta alguno?

3. Introducción a los enteros de Gauss

Los enteros de Gauss, llamados así en referencia a C. Gauss[1], forman un subconjunto de los números complejos que es cerrado para la suma y el producto y contiene a $\mathbb{Z}$. Por lo tanto forman un subanillo.

Hacemos una representación de los enteros de Gauss como los vértices de una retícula entera en el plano. El objetivo es hacer un uso intensivo de esta representación y obtener los primeros resultados sobre la aritmética de los enteros de Gauss.

Estudiamos la división con resto de enteros de Gauss, lo que nos permite desarrollar un algoritmo para el cálculo del máximo común divisor; probar que cada entero de Gauss irreducible es primo; caracterizar los enteros de Gauss irreducibles y establecer un teorema de factorización única.

Recogemos las aplicaciones que hemos encontrado de los enteros de Gauss, y es sobre esta sección sobre la que queremos tratar de forma más exhaustiva. Por esto vamos a utilizar los contenidos de las secciones primera y segunda únicamente como referencias para el desarrollo que queremos hacer en ésta.

[1] Carl Gauss (30-04-1777/23-02-1855) Braunschweig. Alemania. Conocido como el "*Príncipe de las Matemáticas*".

4. Definición de los enteros de Gauss

Llamamos $\mathbb{Z}[i]$ al conjunto de los números complejos de la forma $a + bi$, siendo $a, b \in \mathbb{Z}$. Esto es,

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid \ a, b \in \mathbb{Z}\}.$$

Cada uno de los elementos de $\mathbb{Z}[i]$ se llama un **entero de Gauss**.

Recuerda que $i^2 = -1$, podemos entonces comprobar que la suma de dos enteros de Gauss es también un entero de Gauss y lo mismo para el producto.

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i, \tag{1}$$

$$(a_1 + b_1 i)\,(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i, \tag{2}$$

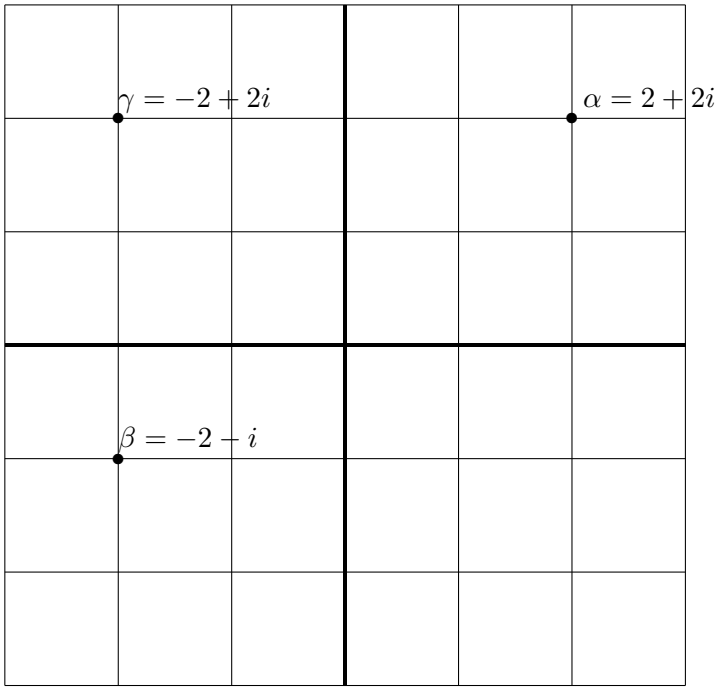
para cualesquiera $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{Z}[i]$.

Tenemos entonces un conjunto de números que tiene unas propiedades similares a las de $\mathbb{Z}$, de hecho podemos considerar $\mathbb{Z} \subseteq \mathbb{Z}[i]$, identificando $\mathbb{Z}$ con $\{a + 0i \in \mathbb{C} \mid \ a \in \mathbb{Z}\}$. Las operaciones suma y producto tienen el mismo comportamiento en $\mathbb{Z}$ que en $\mathbb{Z}[i]$. Tenemos que $\mathbb{Z}[i]$ es un dominio de integridad, esto es, si $\alpha, \beta \in \mathbb{Z}[i]$ verifica $\alpha\beta = 0$, entonces $\alpha = 0$ ó $\beta = 0$.

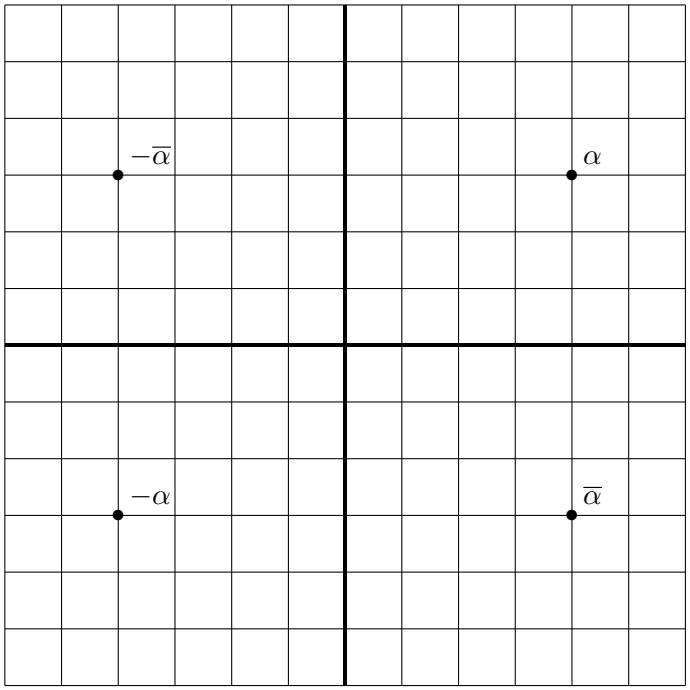
4.1. Representación

Podemos asociar a cada entero de Gauss $\alpha = a + bi$ otro entero de Gauss, que vamos a representar por $\overline{\alpha}$, y que definimos $\overline{\alpha} = a - bi$. Llamamos a $\overline{\alpha}$ el **conjugado** de α.

Los enteros de Gauss se suelen representar como los puntos de una retícula en un plano, ya que habitualmente los números complejos se suelen representar como los puntos de un plano.



Observa que si α es un entero de Gauss distinto de 0, tenemos otros enteros de Gauss relacionados con α, y que representamos en la siguiente figura:

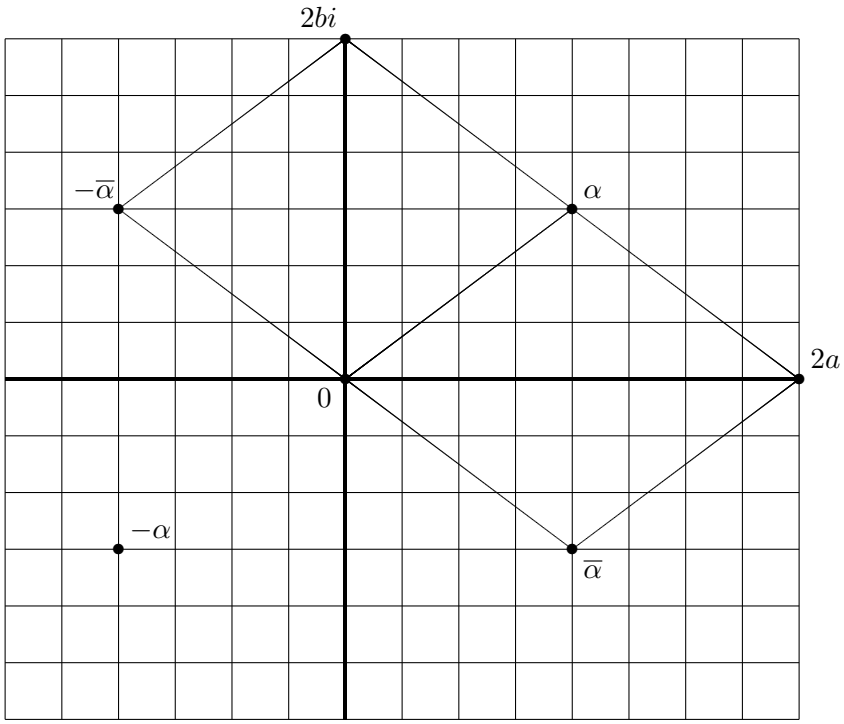


Dado un entero de Gauss $\alpha = a + bi$, llamamos a a la **parte real** de α, y la representamos por $\mathrm{Re}(\alpha)$;

llamamos a b la **parte imaginaria** de α, y la representamos por $\mathrm{Im}(\alpha)$. Con los cuatro números antes mencionados podemos obtener las partes real y imaginaria de α de forma sencilla:

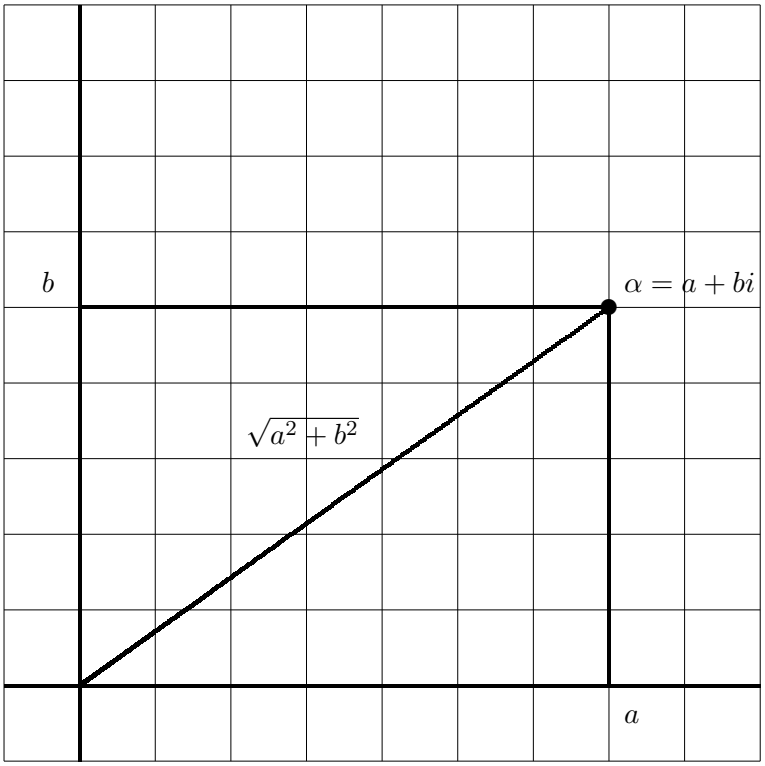
$$\alpha + \overline{\alpha} = 2\mathrm{Re}(\alpha);$$

$$\alpha - \overline{\alpha} = 2\mathrm{Im}(\alpha)i.$$



Esta figura se asemeja a la utilizada para representar la suma de dos vectores en el plano. De hecho la suma de dos enteros de Gauss sigue la misma regla.

Observa que cada entero de Gauss α define un segmento, el que va del punto 0 al punto α; la longitud de este segmento se puede calcular fácilmente mediante el **Teorema de Pitágoras**.



Llamamos a este número el **módulo** de α, y lo representamos por $|\alpha|$.

Observa que $|\alpha| = \sqrt{a^2 + b^2} = \sqrt{\alpha\,\overline{\alpha}}$.

En lo que sigue vamos a utilizar el cuadrado del módulo. Observa que si $\alpha = 1+i$, entonces $|\alpha| = \sqrt{1+1} = \sqrt{2}$ no es un número entero. Con objeto de trabajar exclusivamente con números enteros consideramos el cuadrado del módulo, y así evitamos el uso de radicales.

Definimos la **norma** del entero de Gauss α, y la representamos por $N(\alpha)$, como $N(\alpha) = \alpha\,\overline{\alpha} = a^2 + b^2$; la última igualdad si $\alpha = a + bi$, esto es, la norma de un entero de Gauss es el cuadrado del módulo.

Es importante observar que la aplicación $\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$, definida $\varphi(\alpha) = \overline{\alpha}$, verifica las siguientes propiedades:

(1) $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$, que resulta $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, para todos $\alpha, \beta \in \mathbb{Z}[i]$.
(2) $\varphi(\alpha\,\beta) = \varphi(\alpha)\,\varphi(\beta)$, que resulta $\overline{\alpha\,\beta} = \overline{\alpha}\;\overline{\beta}$, para todos $\alpha, \beta \in \mathbb{Z}[i]$.

Además se tiene $\varphi(\alpha) = \alpha$ si, y solo si, $\alpha \in \mathbb{Z}$.

Como consecuencia se tiene

$$N(\alpha\,\beta) = N(\alpha)N(\beta), \qquad \text{para cualesquiera } \alpha, \beta \in \mathbb{Z}[i]. \tag{3}$$

Otra consecuencia, esta vez de la suma de vectores en el plano, es que dados $\alpha, \beta \in \mathbb{Z}[i]$ se tiene

$$N(\alpha+\beta) \leq N(\alpha) + N(\beta), \tag{4}$$

que no es más que la desigualdad triangular.

La propiedad en (3) es de gran utilidad en lo que sigue, ya que, entre otras cosas, nos permite determinar todos los elementos de $\mathbb{Z}[i]$ que son **invertibles** (los elementos $\alpha \in \mathbb{Z}[i]$ para los que existe $\beta \in \mathbb{Z}[i]$ tal que $\alpha\,\beta = 1$). En efecto, si $\alpha\,\beta = 1$, entonces $1 = N(\alpha\beta) = N(\alpha)N(\beta)$, y tiene que ser $N(\alpha) = \pm 1$, pero como $N(\alpha)$ es siempre positivo resulta $N(\alpha) = 1$. Si $\alpha = a + bi$ y $N(\alpha) = 1$, las únicas posibilidades para α son: 1, -1, i, $-i$.

Lema. 4.1.
Un entero de Gauss α es invertible si, y sólo si, $\alpha = 1, -1, i, -i$.

Teorema. 4.2. (Pequeño Teorema de Fermat)
Sea p un entero primo positivo, para cada $n \in \mathbb{Z}$ se tiene $n^p \equiv n \pmod{p}$.

Demostración. Si $p \mid n$, el resultado es cierto, Supongamos que $p \nmid n$, entonces los restos, módulo p de $n, 2n, \ldots, (p-1)n$ son todos distintos, y por lo tanto son $1, 2, \ldots, (p-1)$. Se tiene: $\prod_{k=1}^{p-1}(kn) = (\prod_{k=1}^{p-1} k)n^{p-1} \equiv \prod_{k=1}^{p-1} k \pmod{p}$, y entonces $n^{p-1} \equiv 1 \pmod{p}$, ya que $p \nmid (\prod_{k=1}^{p-1} k)$. □

Problema. 4.3.
Sea $p \in \mathbb{Z}$ un entero primo positivo y $N = \prod_{k=1}^{p-1}(k^2+1)$. Determina el resto de la división de N por p.

Solución. Definimos $F(X) = (1+X)(2+X)\cdots(p-1+X)$. Observa que sus raíces son: $-1, -2, \ldots, -(p-1)$, por lo tanto módulo p este polinomio es igual al polinomio $X^{p-1} - 1$, ya que para cada $0 < n < p$ se tiene $n^{p-1} - 1 \equiv 0 \pmod{p}$ por el Pequeño Teorema de Fermat. Por lo tanto existe un polinomio $G(X) \in \mathbb{Z}[X]$ tal que $F(X) = X^{p-1} - 1 + pG(X)$.

Como $k^2 + 1 = (k+i)(k-i)$, tenemos

$$N = \prod_{k=1}^{p-1}(k^2+1) = F(i)F(-i) = (i^{p-1} - 1 + pG(i))((-i)^{p-1} - 1 + pG(-i)).$$

Si $p = 2$ se tiene $N = 1 + 1 = 2 \equiv 0 \pmod{p}$.

Si $p \equiv 1 \pmod 4$, entonces $p = 4h+1$, y se tiene

$$N = (i^{4h+2} - 1 + pG(i))((-i)^{4h+2} - 1 + pG(-i)) \equiv 4 \pmod p.$$

Si $p \equiv 3 \pmod 4$, entonces $p = 4h+3$, y se tiene

$$N = (i^{4h} - 1 + pG(i))((-i)^{4h} - 1 + pG(-i)) \equiv 0 \pmod p.$$

Como consecuencia tenemos $N \equiv 4 \pmod p$ si $p \equiv 3 \pmod 4$, y $N \equiv 0 \pmod p$ en otro caso. □

4.2. Enteros de Gauss irreducibles

Dados dos enteros de Gauss α y β, decimos que α **divide** a β, y escribimos $\alpha \mid \beta$, si existe un entero de Gauss γ tal que $\beta = \alpha\gamma$. Cada entero de Gauss α tiene siempre los siguientes **divisores triviales**: α, $-\alpha$, $i\alpha$ y $-i\alpha$. Además cada entero de Gauss invertible es también divisor de α. Los divisores de α que no son triviales y no son invertibles se llaman los **divisores propios** de α.

Un entero de Gauss α se llama **irreducible** si no es cero ni invertible y no tiene divisores propios.

Ejemplo. 4.4.
Vamos a ver que 3 es un entero de Gauss irreducible.

Solución. Si $3 = \alpha\beta$, entonces $9 = N(3) = N(\alpha\beta) = N(\alpha)N(\beta)$, y como $N(\alpha)$ es un entero positivo tenemos las siguientes tres posibilidades:

(1) Si $N(\alpha) = 1$, entonces α es invertible.
(2) Si $N(\alpha) = 9$, entonces $N(\beta) = 1$ y por lo tanto invertible, entonces α es un divisor trivial.
(3) Si $N(\alpha) = 3$, entonces $3 = a^2 + b^2$, si $\alpha = a + bi$. Pero no existen valores enteros de a y b que cumplan esta igualdad.

En consecuencia no existen divisores propios de 3. □

Ejemplo. 4.5.
Por el contrario 2 no es un entero de Gauss irreducible, ya que se tiene $2 = 1 + 1 = (1+i)(1-i)$, y es claro que $1+i$ y $1-i$ son divisores propios de 2.

Puedes hacer una lista de enteros de Gauss que no sean irreducibles. Tenemos, por ejemplo:

$$\begin{aligned} 5 &= (2+i)(2-1); \\ 13 &= (3+2i)(3-2i); \\ 17 &= (4+i)(4-i). \end{aligned}$$

Observa que al determinar enteros de Gauss que no son irreducibles, determinamos enteros de Gauss irreducibles.

Pregunta. 4.6.
Estas descomposiciones producen enteros de Gauss irreducibles. ¿Cuáles son estos? ¿Por qué?

Ejemplo. 4.7.
Por otro lado tenemos que 7 y 11 son enteros de Gauss irreducibles.

Veamos el caso de 7. Si $7 = \alpha\,\beta$, entonces $49 = N(7) = N(\alpha\beta) = N(\alpha)N(\beta)$. Si $N(\alpha) = 7$ existen enteros a, b tales que $a^2 + b^2 = 7$, lo que es imposible.

Para 11 se trabaja de la misma forma.

Un resultado general sobre elementos irreducibles es el siguiente:

Lema. 4.8.
Si p es un entero primo positivo tal que $p \equiv 3 \pmod 4$, entonces p es un entero de Gauss irreducible.

Para probar este hecho vamos a seguir las mismas ideas que empleamos en el Ejemplo (4.4.).

Demostración. Supongamos que $p = \alpha\,\beta$ es una factorización en divisores propios de p, entonces $p^2 = N(p) = N(\alpha\,\beta) = N(\alpha)N(\beta)$. Como $N(\alpha)$ es un entero positivo tenemos las siguientes tres posibilidades:

(1) Si $N(\alpha) = 1$, entonces α es invertible.
(2) Si $N(\alpha) = p^2$, entonces $N(\beta) = 1$ y por lo tanto invertible, entonces α es un divisor trivial.
(3) Si $N(\alpha) = p$, entonces $p = a^2 + b^2$, si $\alpha = a + bi$. Módulo 4 los únicos cuadrados son 0 y 1, por lo tanto los únicos valores de la suma $a^2 + b^2$ módulo 4 son 0,1 ó 2, y nunca 3.

En consecuencia no existen divisores propios de p y p es un entero de Gauss irreducible. □

Como ya conocemos 2 no es un entero de Gauss irreducible. Nos queda por analizar el caso de los enteros primos positivos p tales que $p \equiv 1$ (mód 4). Para estudiar este caso necesitamos introducir nuevas herramientas para trabajar con los enteros de Gauss.

Ejercicio. 4.9.
Prueba que si un entero de Gauss α es irreducible, también lo es $\overline{\alpha}$.

SOLUCIÓN. Si $\overline{\alpha}$ no es irreducible, existen β, γ no invertibles tales que $\overline{\alpha} = \beta\gamma$, y se tiene $\alpha = \overline{\overline{\alpha}} = \overline{\beta}\,\overline{\gamma}$ y se tiene que $\overline{\beta}$ o $\overline{\gamma}$ es invertible, lo que implica que β o γ es invertible. □

5. División de enteros de Gauss

Dados dos enteros de Gauss α y β no tenemos herramientas para compararlos, pero sí una medida de su *tamaño*: la norma. Observa que la norma es siempre un entero positivo o nulo, por lo tanto podemos imaginar que un entero de Gauss α será más pequeño que otro β si $N(\alpha) < N(\beta)$. Existirán enteros de Gauss que no sean comparables y que tengan la misma norma, com por ejemplo $1+i$ y $1-i$ que tienen norma 2.

Dados $\alpha, \beta \in \mathbb{Z}[i]$, con $\beta \neq 0$, vamos a definir la **división** de α por β. Ésta consistirá en determinar dos enteros de Gauss Q y R verificando las siguientes propiedades:

(1) $\alpha = \beta Q + R$;
(2) $N(R) < N(\beta)$).

Procedemos como sigue:

(1) Si $\alpha = 0$, entonces $Q = 0$ y $R = 0$;
(2) Si $\alpha \neq 0$
  (2.1) Si $N(\alpha) < N(\beta)$, entonces $Q = 0$ y $R = \alpha$;
  (2.2) Si $N(\alpha) \geq N(\beta)$, trabajando en $\mathbb{C}$ tenemos que $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}}$ se puede escribir en la forma $r + si$, con $r, s \in \mathbb{Q}$. Tomamos c y d, los enteros más próximos a r y s, respectivamente. Se verifica:

$$\frac{\alpha}{\beta} = r + si = (c + di) + ((r - c) + (s - d)i)\,.$$

Por lo tanto $\alpha = \beta(c + di) + \beta\,((r - c) + (s - d)i)$. Es claro que $\beta\,((r - c) + (s - d)i)$ es un entero de Gauss, ya que es la diferencia de dos enteros de Gauss. Tomamos $Q = c + di$ y $R = \beta\,((r - c) + (s - d)i)$. Falta comprobar que $N(R) < N(\beta)$; esto es consecuencia de que $N((r - c) + (s - d)i) < 1$, ya que $(r - c)^2 + (s - d)^2 \leq 2\left(\frac{1}{2}\right)^2 \leq \frac{1}{2}$.


Observa que no tenemos un resultado de unicidad en la división. Para conseguirlo deberíamos imponer condiciones extra que no nos aportan nada al desarrollo que estamos haciendo.

5.1. Divisibilidad de enteros de Gauss

La existencia de la división nos permite establecer una teoría de la divisibilidad en $\mathbb{Z}[i]$.

Dados enteros de Gauss α y β, decimos que $\gamma \in \mathbb{Z}[i]$ es un **divisor común** si $\gamma \,|\, \alpha$ y $\gamma \,|\, \beta$, y decimos que es un **máximo común divisor** si para cualquier otro divisor común δ de α y β se verifica $\delta \,|\, \gamma$.

Lema. 5.1.
Cada par de enteros de Gauss tienen un máximo común divisor al que representaremos por $\mathrm{mcd}\{\alpha, \beta\}$*, o simplemente por* D*.*

Demostración. Dados $\alpha, \beta \in \mathbb{Z}[i]$, procedemos como sigue:

(1) Si $\beta \,|\, \alpha$ definimos $D = \beta$.
(2) Si $\beta \nmid \alpha$ hacemos la división $\alpha = \beta Q + R$.
  (2.1) Asignamos $\alpha := \beta$ y $\beta := R$ y volvemos al paso (1).

El proceso finaliza ya que tenemos una cadena descendente de enteros positivos: $N(\beta) > N(R) > \cdots$, que necesariamente es finita.

Sólo resta por comprobar que el resultado es un máximo común divisor; la razón es que, con la notación de (2.1) se tiene

$$\mathrm{mcd}\{\alpha, \beta\} = \mathrm{mcd}\{\beta, R\},$$

y así en cada uno de los pasos. □

Lema. 5.2. (Identidad de Bezout)
Dados dos enteros de Gauss, α *y* β*, con máximo común divisor* D *existen enteros de Gauss,* U *y* V*, tales que* $D = U\alpha + V\beta$*.*

Demostración. HACER □

El problema ahora es calcular el máximo común divisor como una combinación de los dos enteros de Gauss. El resultado es la **identidad de Bezout** para enteros de Gauss. Hacemos un esquema del algoritmo.

	α	β	Q	R	U	V	D
-1	α				1	0	α
0	α	β	Q_1	R_1	0	1	β
1	β	R_1	Q_2	R_2	1	$-Q_1$	R_1
2	R_1	R_2	Q_3	R_3	$-Q_2$	$1+Q_1Q_2$	R_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	R_{i-1}	R_i	Q_{i+1}	R_{i+1}	U_i	V_i	R_i
$i+1$	R_i	R_{i+1}	Q_{i+2}	R_{i+2}	$U_{i-1}-U_iQ_{i+1}$	$V_{i-1}-V_iq_{i+1}$	R_{i+1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$t+1$	R_t	R_{t+1}	Q_{t+2}	$R_{t+2}=0$	U_t	V_t	R_{t+1}

$$R_{i-1} = R_iQ_{i+1} + R_{i+1}.$$

$$D = R_{t+1} = U_t\alpha + V_t\beta.$$

El máximo común divisor es el último resto no nulo, que aquí hemos llamado R_{t+1}.

5.2. Enteros de Gauss primos y factorización única

Veamos la equivalencia entre enteros de Gauss irreducibles y primos.

Un entero de Gauss α no nulo y no invertible se llama **primo** si cuando divide a un producto divide a uno de los factores. Es un ejercicio fácil probar que todo entero de Gauss primo es irreducible. Para el recíproco tenemos:

Lema. 5.3.
Si π es un entero de Gauss irreducible y $\pi \mid \alpha\beta$, entonces $\pi \mid \alpha$ ó $\pi \mid \beta$. Esto es, todo entero de Gauss irreducible es primo.

Demostración. Llamamos $D = \text{mcd}\{\pi, \alpha\}$. Existe $\gamma \in \mathbb{Z}[i]$ tal que $\pi = D\gamma$. Si γ es invertible, entonces $\pi \mid \alpha$. Si D es invertible, consideramos la identidad de Bezout: $D = U\pi + V\alpha$, y podemos escribir $1 = \frac{U}{D}\pi + \frac{V}{D}\alpha$; multiplicando por β resulta $\beta = \frac{U}{D}\pi\beta + \frac{V}{D}\alpha\beta$, luego π divide a β. □

Como consecuencia de este resultado podemos establecer que los enteros de Gauss tienen factorización única como producto de elementos irreducibles.

Lema. 5.4.
Cada entero de Gauss no nulo y no invertible se escribe, de forma única, salvo en el orden y elementos invertibles, como producto de elementos irreducibles.

DEMOSTRACIÓN. Dado un entero de Gauss no nulo y no invertible, α, si α es irreducible ya tenemos la expresión a que hace referencia el enunciado. Si α no es irreducible existe una factorización propia, sea $\alpha = \alpha_1\beta_1$. Si α_1 no es irreducible tendrá una factorización propia, sea $\alpha_1 = \alpha_2\beta_2$; y así seguimos si no encontramos un elemento irreducible, obteniendo en el paso t una factorización propia $\alpha_t = \alpha_{t+1}\beta_{t+1}$. Observa que se tiene la siguiente relación con las normas:

$$N(\alpha) > N(\alpha_1) > \cdots > N(\alpha_t) > N(\alpha_{t+1}) > \cdots$$

Esto es imposible, ya que los $N(\alpha_i)$ son enteros positivos. Por tanto existe un divisor propio de α que es irreducible. Supongamos que sea π, y que se tiene $\alpha = \pi\,\beta$. Aplicamos ahora el mismo argumento a β, si éste no es irreducible, llegamos a una factorización $\alpha = \pi_1 \cdots \pi_s$ formada por elementos irreducibles.

Dadas dos factorizaciones de enteros de Gauss en irreducibles

$$\alpha = \pi_1 \cdots \pi_s = \eta_1 \cdots \eta_t$$

como cada irreducible es primo, resulta que π_1 divide a algún η_j, por ejemplo a η_1. Se tiene entonces $\eta_1 = \pi_1\gamma$, y por ser η_1 irreducible tenemos que γ es invertible. El resultado sigue por inducción sobre el número de elementos irreducibles en la factorización. □

5.3. Caracterización de enteros de Gauss irreducibles

Podemos ahora abordar el problema de determinar todos los enteros de Gauss irreducibles. Lo haremos en dos partes; para la primera necesitamos un resultado de teoría de números enteros.

Proposición. 5.5. (Teorema de Wilson)
Si p es un entero positivo son equivalentes:

(a) p es un entero primo.
(b) $(p-1)! \equiv -1 \pmod{p}$

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Como p es primo, por la identidad de Bezout para enteros, se tiene que para cada entero $2 \leq x \leq p-2$ existe $y \neq x$, dentro del mismo rango, tal que $xy \equiv 1 \pmod{p}$, esto es, las clases de resto módulo p forman un cuerpo y podemos emparejar los elementos dos a dos cada uno con

su inverso. Quedan fuera de este emparejamiento los elementos 1 y $p-1$. Por lo tanto si multiplicamos de 1 a $p-1$ el resultado es congruente con $p-1$ módulo p.

(b) $\Rightarrow$ (a). Si p no es primo existen, $x, y < p$, $x \neq y$, tales que $xy = p$, entonces $(p-1)! \equiv 0 \pmod{p}$, lo que es una contradicción. □

Utilizando el Teorema de Wilson tenemos:

Lema. 5.6.
Si p es un entero primo positivo tal que $p \equiv 1 \pmod 4$, entonces p no es un entero de Gauss primo.

Demostración. Como p es un entero primo, por el Teorema de Wilson tenemos $(p-1)! \equiv -1 \pmod p$. Por otro lado por la hipótesis se tiene $p \equiv 1 \pmod 4$, luego existe un entero h tal que $p - 1 = 4h$, y por tanto $(4h)! \equiv -1 \pmod p$. Emparejamos las clases de resto módulo p de la siguiente forma; en la tercera fila hemos señalado en resultado de multiplicar los elementos de cada columna. (Observa que siempre es $(x(-x) = -x^2$.)

1 $4h = p-1$	2 $p-2$	$\ldots$ $\ldots$	$2h-1$ $2h+2$	$2h$ $2h+1$
-1^2	-2^2	$\ldots$	$-(2h-1)^2$	$-(2h)^2$

Como tenemos un número par de columnas, podemos prescindir del signo, ya que el producto será siempre positivo. De esta forma tenemos:

$$(4h)! \equiv ((2h)!)^2 \equiv -1 \pmod p$$

Si llamamos $x \equiv (2h)! \pmod p$, tenemos $x^2 \equiv -1 \pmod p$, o equivalentemente $p \mid (x^2+1) = (x+i)(x-i)$.

Si suponemos que p es un entero de Gauss irreducible, entonces p divide a uno de los factores, por ejemplo a $x+i$, y existe un entero de Gauss, llamémoslo $a+bi$, tal que $p(a+bi) = x+i$. De aquí se deduce, al igualar las partes imaginarias, que $pb = 1$. Tenemos entonces que p es un entero invertible, lo que es una contradicción. □

Como consecuencia ya sabemos cuales son los enteros positivos que son enteros de Gauss irreducibles: "*aquellos que son enteros primos y son congruentes con 3 módulo 4*".

Podemos ahora establecer el teorema de caracterización de enteros de Gauss irreducibles.

Teorema. 5.7.
Un entero de Gauss π es irreducible si, y sólo si, $N(\pi)$ es de uno de los siguientes tipos:

(1) $N(\pi) = 2$; *(en este caso* $\pi = 1+i, 1-i, -1+i, -1-i$, *hay 4 posibles valores).*
(2) $N(\pi) = p$, *donde* p *es un entero primo positivo tal que* $p \equiv 1 \pmod 4$; *(en este caso* $\pi = a+bi$ *con* $a^2+b^2 = p$*).*
(3) $N(\pi) = p^2$, *donde* p *es un entero primo positivo tal que* $p \equiv 3 \pmod 4$; *(en este caso* $\pi = p, -p, pi, -pi$*).*

Demostración. Veamos que la condición es suficiente. Es claro que si $N(\pi) = p$, con p entero primo, entonces π es primo; tenemos que observar que p no puede ser congruente con 3 módulo 4, ya que estos enteros no pueden escribirse como suma de dos cuadrados.

Por otro lado si $N(\pi) = p^2$ y p es primo verificando $p \equiv 3 \pmod 4$, entonces π es primo, pues cualquier factorización propia llevaría a que p es una suma de dos cuadrados, lo que sabemos que es imposible.

Para comprobar que la condición es necesaria, sea $\pi = a+bi \in \mathbb{Z}[i]$ un entero de Gauss primo. Tenemos que $N(\pi) = \pi\,\overline{\pi}$ es una factorización en primos en $\mathbb{Z}[i]$. Si consideramos la factorización en primos de $N(\pi)$ en $\mathbb{Z}$, sea ésta $N(\pi) = p_1 \cdots p_s$, al considerarla en $\mathbb{Z}[i]$ tiene al menos s factores; esto implica que $s \leq 2$.

Si $s = 1$, entonces $N(\pi) = p_1 = (a+bi)(a-bi) = a^2+b^2$, entonces p es igual a 2 o un primo congruente con 1 módulo 4.

Si $s = 2$, entonces $N(\pi) = p_1\,p_2 = \pi\,\overline{\pi}$; se verifica, por ejemplo, que p_1 y π son iguales salvo multiplicar por un elemento invertible en $\mathbb{Z}[i]$, por lo que $\pi \in \{p_1, -p_1, ip_1, -ip_1\}$ y por tanto se tiene $\overline{\pi} \in \{p_1, -p_1, ip_1, -ip_1\}$, lo que implica $p_1 = p_2$. Si no se verifica $p_1 \equiv 3 \pmod 4$, entonces $p_1 = u^2+v^2 = (u+vi)(u-vi)$ y tenemos $N(\pi) = p_1^2 = (u+vi)^2(u-vi)^2$, un producto de cuatro elementos no invertibles, lo que es una contradicción. □

Problema. 5.8.
Resolver la ecuación $Y^5 - 1 = X^2$ *en* $\mathbb{Z}$.

Solución. Dada una solución (y, x), se tiene $y^5 - 1 = x^2$, esto es, $y^5 = x^2+1 = (x+i)(x-i)$.

Vamos a descartar el caso de 2. Si y es par, entonces $2^5 \,|\, x^2+1$, y por tanto $x^2 \equiv 3 \pmod 4$, lo que es imposible.

Tenemos entonces que y es impar. En este caso $2 \nmid (x+i)(x-i)$. Supongamos que $x+i = p_1 \cdots p_s$, entonces $x-i = \overline{p_1} \cdots \overline{p_s}$. Si $p_j = \overline{p_j}$, entonces $p_j^2 \,|\, (x+i)-(x-i) = 2i$, luego $p_j \,|\, 2$, lo que es una contradicción. Como consecuencia $x+i$ y $x-i$ son primos relativos, y por lo tanto son potencias quintas.

Sea $x+i=(a+bi)^5=a(a^4-10a^2b^2+5b^4)+b(5a^4-10a^2b^2+b^4)i$. De aquí se obtiene $b(5a^4-10a^2b^2+b^4)=1$, por tanto

$$\begin{array}{llll} b=1 & 5a^4-10a^2b^2+b^4=1 & 1=5a^4-10a^2+1 \Rightarrow a=0 \\ b=-1 & 5a^4-10a^2b^2+b^4=-1 & 1=5a^4-10a^{+}1 & \Rightarrow a=0. \end{array}$$

En consecuencia

$$\begin{array}{l} x+i=i \quad \Rightarrow x=0, y=1 \\ x+i=-i \Rightarrow x=-2i, y^5=-2+1=-1, y=-1. \end{array}$$

Las soluciones enteras son $y=1$, $x=0$. $x+i=\pm i$ □

Problema. 5.9.
Sean x,y,z enteros verificando $xy=z^2+1$. Demuestra que existen enteros a,b,c,d y un racional r tales que $\left\{\begin{array}{l} x=(a^2+b^2)r, \\ y=(c^2+d^2)r, \\ z=(ac+bd)r. \end{array}\right\}$

Solución. En el caso en el que $x=0$ ó $y=0$ no existe solución. Supongamos pues que x,y son no nulos.

Tenemos un resultado general en todo DFU de forma que si $ab=cd\neq 0$, existen que elementos u_1,u_2,v_1,v_2 tales que $\left\{\begin{array}{l} a=u_1v_1, \\ b=u_2v_2, \\ c=u_1v_2, \\ d=u_2v_1. \end{array}\right\}$. la demostración es la misma que en $\mathbb{Z}$ utilizando factorización en elementos primos.

Tenemos $xy=z^2+1=(z+i)(z-i)$, luego existen $u_1,u_2,v_1,v_2\in\mathbb{Z}[i]$ tales que $\left\{\begin{array}{l} x=u_1v_1, \\ y=u_2v_2, \\ z+i=u_1v_2, \\ z-i=u_2v_1. \end{array}\right\}$

Como $x=\overline{x}$, se tiene $x=u_1v_1=\overline{u_1}\,\overline{v_1}$, luego $v_1=\frac{\overline{v_1}}{u_1}\overline{u_1}=r_1\overline{u_1}$. De la misma forma se tiene $v_2=\frac{\overline{v_2}}{u_2}\overline{u_2}=r_2\overline{u_2}$.

Se tiene $z-i=u_2v_1=u_2r_1\overline{u_1}=\overline{u_1r_2\overline{u_2}}=u_2r_2\overline{u_1}$, y por tanto $r_1=r_2$. Llamamos $r=r_1=r_2$.

Sea $u_1=a+bi$ y $u_2=c+di$, entonces:

$$\begin{array}{l} x=u_1\overline{u_1}r=(a^2+b^2)r, \\ y=u_2\overline{u_2}r=(c^2+d^2)r, \\ 2z=(z+i)+(z-i)=u_1\overline{u_2}r+u_2\overline{u_1}r=(a+bi)(c-di)r+(c+di)(a-bi)r= \\ \quad =(ac+bd+ca+db)r+(bc-ad-cb+da)ri=2(ac+bd)r. \end{array}$$

Además se tiene la relación $Im(u_1\overline{u_2})r = 1$, esto es, $(bc - ad)r = 1$. □

Problema. 5.10.
Sea $p \equiv 1 \pmod 4$ un entero primo positivo. Prueba que $X^2 + Y^2 = p$ tiene exactamente una solución (x, y), verificando $x > y > 0$.

Solución. Como $p \equiv 1 \pmod 4$, entonces p descompone en $\mathbb{Z}[i]$. Supongamos que $p = (x + yi)(x - yi)$ con $x > y > 0$. Si tenemos otra solución $p = a^2 + b^2$ con $a > y > 0$, entonces $p = (a + bi)(a - bi)$. Por la unicidad de la factorización en $\mathbb{Z}[i]$ tenemos:

$$x + yi = \pm(a \pm bi), \text{ ó } x + yi = \pm i(a \pm bi).$$

Si $x + yi = \pm(a \pm bi)$, por la relación $a > b > 0$, tenemos $x + yi = a + bi$, luego $x = a$ e $y = b$.

Si $x+yi = \pm i(a\pm bi) = \pm(ai\mp b) = \pm(b\mp ai)$, y por la relación $a > b > 0$, esta relación es imposible. □

Problema. 5.11.
Encontrar las soluciones x, y de la ecuación $X^2 + Y^2 = 221$ que verifican $x > y > 0$.

Solución. Consideramos la factorización $221 = 13 \times 17$, y descomponemos 13 y 17 en $\mathbb{Z}[i]$:

$$13 = (3 + 2i)(3 - 2i),$$
$$17 = (4 + 1)(4 - 1).$$

Entonces tenemos:

$$(3 + 2i)((4 + i) = 14 + 11i \text{ y se verifica: } (14 + 11i)(14 - 11i) = 221.$$
$$(3 + 2i)(4 - i) = 14 + 5i \quad \text{y se verifica: } (14 + 5i)(14 - 5i) = 221.$$

Además éstas son las única soluciones verificando la propiedad. □

Problema. 5.12.
Sea $a \in \mathbb{Z}$ y p un entero positivo tal que $p \equiv 1 \pmod 4$.

(1) Definimos $b \equiv a^{\frac{p-1}{4}} \pmod p$. Prueba que $b^2 \equiv -1 \pmod p$ ó $b^2 \equiv 1 \pmod p$. Prueba que si a es una raíz primitiva módulo 4p4, entonces se verifica la primera opción.
(2) Prueba que existe exactamente un entero m tal que $2 \leq m^{\frac{p-1}{2}}$ tal que $m^2 \equiv -1 \pmod p$.
(3) Describe una forma (razonable) de determinar el elemento m del apartado anterior.
(4) Supongamos que $\text{mcd}\{p, m + i\} = x + yi \in \mathbb{Z}[i]$. Prueba que $p = x^+y^2$.
(5) Encuentra el entero m en el caso $p = 137$.
(6) Resuelve la ecuación diofántica $X^2 + Y^2 = 137$.

SOLUCIÓN. (1). Tenemos $(b^2)^2 \equiv a^{4\frac{p-1}{4}} \equiv a^{p-1} \equiv 1 \pmod{p}$, por lo tanto b^2 es raíz del polinomio X^2-1 módulo p. y se tiene $b^2 \equiv \pm 1 \pmod{p}$. Si a es una raíz primitiva módulo p y $a^e \equiv 1$, se tiene $e = p-1$, por lo tanto $b^2 \equiv -1 \pmod{p}$ ya que $b^2 \not\equiv 1 \pmod{p}$.

(2). De $m^2 \equiv -1 \pmod{p}$ se tiene $m^4 \equiv 1 \pmod{p}$ y no se tiene $m^e \equiv 1 \pmod{p}$ para $e < 4$. Como m es raíz de X^2+1 módulo p, tenemos como máximo dos posibilidades para m. Si a es una raíz primitiva módulo p entonces $a^{\frac{p-1}{4}}$ es raíz de X^2+1. Tenemos entonces dos raíces $u = a^{\frac{p-1}{4}}$ y $-u$. Sólo una de ellas está en el rango pedido.

(3). Es claro que podemos probar con todos los elementos m en el rango $2 \leq m \leq \frac{p-1}{2}$, pero esto es muy lento si p es grande. Veamos otro método. Tomamos $c_1 = 2$ y llamamos $c_2 = c^{\frac{p-1}{4}}$. Como c_2 es una raíz cuarta de 1 es el cuadrado de -1, y por lo tanto c_2 es una raíz cuadrada de -1, en este caso la solución será c_2 ó $-c_2$. Si c_2 no es una raíz cuadrada de -1, cambiamos c_1 por c_1+1 y repetimos el proceso. En realidad se trata de determinar una raíz primitiva módulo p, y sabemos que hay $\varphi(p-1)$.

(4). Tenemos que $x+yi$ divide a p, luego $N(x+yi) \,|\, N(p) = p^2$, por lo tanto $N(x+yi) = 1, p, p^2$.

Si $N(x+yi) = p^2$ y $p = (x+yi)(a,bi)$, entonces $N(a+bi) = 1$ y $a+bi$ es invertible. Entonces $x+yi \sim p$ divide a $m+i$, lo que es una contradicción ya que entonces $p \,|\, m$.

Si $N(x+yi) = 1$ vamos a llegar también a una contradicción. Se tiene $(m+i)(m-i) = m^2+1 \equiv 0 \pmod{p}$, por lo tanto $p \,|\, (m+i)(m-i)$, entonces $p \,|\, (m-i)$ y por tanto $p = \overline{p} \,|\, \overline{m-i} = m+i$, lo que es una contradicción.

En consecuencia $p = N(x+yi) = x^2+y^2$.

(5). Mediante el algoritmo descrito en (3) tenemos $m = 37$.

(6). Basta determinar el mcd de 137 y $37+i$ en $\mathbb{F}[i]$; la solución es $x+yi = 11+4i$, por lo tanto $11^2+4^2 = 137$. □

6. Aplicaciones

Veamos algunas aplicaciones de los enteros de Gauss.

6.1. Ternas pitagóricas

Vamos a calcular las ternas pitagóricas de números enteros; esto es, ternas de enteros positivos x, y, z verificando $x^2+y^2 = z^2$.

Podemos suponer que los enteros x, y, z son primos relativos dos a dos, y que y es un entero par. Vamos


a escribir $z^2 = (x + yi)(x - yi)$, utilizando enteros de Gauss.

Como x e y son primos relativos, también lo son $x + yi$ y $x - yi$. En efecto, si π divide a $x + yi$ y a $x - yi$, entonces π divide a $2x$, π divide a $2y$, y por tanto $N(\pi)$ divide a $4x^2$ y a $4y^2$. Como x e y son primos relativos, resulta que $N(\pi)$ divide a 4, por lo tanto es par o invertible. Además $N(\pi)$ divide a $N(x+yi) = x^2+y^2 = N(x-yi)$, que es impar, luego $N(\pi)$ es impar o invertible. Por lo tanto $N(\pi) = 1$ y π es un entero de Gauss invertible.

De la igualdad $z^2 = (x + yi)(x - yi)$ se deduce que $x + yi$ y $x - yi$ son cuadrados, salvo unidades. Supongamos que $x + yi = (a + bi)^2 = (a^2 - b^2) + 2abi$, tenemos $x = a^2 - b^2$, $y = 2ab$. Entonces $z^2 = x^2 + y^2 = (a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$, y se tiene $z = a^2 + b^2$.

La solución es:

$$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2.$$

Observa que hemos hecho uso de la factorización única de enteros de Gauss.

6.2. Teorema de Fermat–Euler

Diofanto[2] planteó el problema de determinar los enteros positivos que se pueden escribir como la suma de dos cuadrados. Este problema fue resuelto por P. de Fermat[3] y enviado, sin demostración, por carta fechada el 25 de diciembre de 1640, a Marin Mersenne[4]; por esto al Teorema (6.3.) se le conoce también como **Teorema de Navidad de Fermat**. Posteriormente L. Euler[5] en 1749 da la primera demostración que se conoce de este resultado. La primera demostración basada en el uso de los enteros de Gauss fue dada por R. Dedekind[6].

Antes de comenzar vamos a ver el comportamiento de los conjugados de enteros de Gauss respecto a los enteros de Gauss invertibles. Dados dos enteros de Gauss, α y β, decimos que son **asociados** si existe un entero de Gauss invertible, υ, tal que $\alpha = \upsilon\,\beta$.

Lema. 6.1.
Si π es un entero de Gauss irreducible, se tiene que π y $\overline{\pi}$ son asociados si, y sólo si, $N(\pi) \neq p$, con $p \equiv 1$ (mód 4).

[2]Diofanto de Alejandría (214/284). Antiguo matemático griego.
[3]Pierre de Fermat (17-08-1601/12-01-1665) Beaumont-de-Lomagne. Francia.
[4]Marin Mersenne (8-09-1588/1-09-1648) Oizé. Francia.
[5]Leonard Euler (15-04-1707/18-09-1783) Basilea. Suiza.
[6]Richard Dedekind (6-10-1831/12-02-1916) Brunswick. Alemania. Trabajó en la Universidad de Göttingen (Alemania).

Corolario. 6.2.
Un entero de Gauss α es asociado a $\overline{\alpha}$ si, y sólo si, no tiene factores irreducibles π con $N(\pi) = p$ y $p \equiv 1$ (mód 4).

Teorema. 6.3. (Teorema de Fermat–Euler)
Un entero positivo x es una suma de dos cuadrados si, y sólo si, en la descomposición de x en factores primos los primos congruentes con 3 módulo 4 tienen exponente par.

DEMOSTRACIÓN. Observamos que si $x_1 = a_1^2 + b_1^2$ y $x_2 = a_2^2 + b_2^2$, entonces x_1x_2 también es una suma de cuadrados:

$$\begin{aligned} x_1x_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) &= N(a_1 + b_1i)N(a_2 + b_2i) \\ &= N((a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2. \quad (5) \end{aligned}$$

Es claro que la condición es suficiente, ya que: 2 se puede escribir como la suma de dos cuadrados, y por tanto también cualquier potencia de 2; si p es un factor primo de x que verifica $p \equiv 1$ (mód 4), entonces p es una suma de dos cuadrados, ver Lema (5.6.); y por último, es claro que cualquier factor al cuadrado es una suma de dos cuadrados, uno de ellos igual a cero.

Para ver que la condición es necesaria, si x es una suma de dos cuadrados, podemos escribir $x = a^2 + b^2 = (a + bi)(a - bi)$. El entero de Gauss $a + bi$ tendrá una factorización en irreducibles:

$$a + bi = \pi_0^{e_0}\pi_1^{e_1} \cdots \pi_s^{e_s}\pi_{s+1}^{e_{s+1}} \cdots \pi_{s+t}^{e_{s+t}},$$

donde: π_0 verifica $N(\pi_0) = 2$; los $\pi_1, \ldots, \pi_s$ verifican $N(\pi_i) = p_i$, con $p_i \equiv 1$ (mód 4) y los $\pi_{s+1}, \ldots, \pi_{s+t}$ verifican $N(\pi_j) = p_j^2$, con $p \equiv 3$ (mód 4).

Al conjugar $a + bi$ tenemos una expresión con las mismas características.

Observamos que el producto $\pi_0\,\overline{\pi_0}$ es igual a 2; el producto $\pi_i\,\overline{\pi_1}$, $1 \leq i \leq s$, es una suma de dos cuadrados no nulos, mientras que el producto $\pi_j\,\overline{\pi_j}$, $s + 1 \leq j \leq s + t$, es el cuadrado de p_j.

Tenemos entonces que x es un producto de primos iguales a 2, o congruentes con 1 módulo 4, y primos congruentes con 3 módulo 4, en este caso todos ellos con exponente par. □

6.3. Enteros de Gauss con la misma norma

Sean α, β enteros de Gauss, vamos a buscar una condición necesaria y suficiente para que $N(\alpha) = N(\beta)$.

Supongamos que $\alpha = \pi_0^{e_0}(\pi_1^{e_{1,1}}\overline{\pi}_1{}^{e_{1,2}})\cdots(\pi_s^{e_{s,1}}\overline{\pi}_s{}^{e_{s,2}})\pi_{s+1}^{e_{s+1}}\cdots\pi_{s+t}^{e_{s+t}}$, donde: π_0 verifica $N(\pi_0) = 2$; los $\pi_1, \ldots, \pi_s$ verifican $N(\pi_i) = p_i$, con $p_i \equiv 1 \pmod 4$; los $\pi_{s+1}, \ldots, \pi_{s+t}$ verifican $N(\pi_j) = p_j^2$, con $p \equiv 3 \pmod 4$. Entonces se tiene

$$N(\alpha) = 2^{e_0} p_1^{e_{1,1}+e_{1,2}} \cdots p_s^{e_{s,1}+e_{s,2}} p_{s+1}^{2e_{s+1}} \cdots p_{s+t}^{2e_{s+t}}.$$

Si la factorización de β en irreducibles es: $\beta = \omega_0^{f_0}(\omega_1^{f_{1,1}}\overline{\omega_1}^{f_{1,2}})\cdots(\omega_u^{f_{u,1}}\overline{\omega_u}^{f_{u,2}})\omega_{u+1}^{f_{u+1}}\cdots\omega_{u+v}^{f_{s+v}}$, donde: ω_0 verifica $N(\omega_0) = 2$; los $\omega_1, \ldots, \omega_u$ verifican $N(\omega_i) = q_i$, con $q_i \equiv 1 \pmod 4$; los $\omega_{u+1}, \ldots, \omega_{u+v}$ verifican $N(\omega_j) = q_j^2$, con $q \equiv 3 \pmod 4$.

Como $N(\alpha) = N(\beta)$, entonces tenemos las siguientes igualdades (para una reordenación de los índice de la factorización de β):

$$e_0 = f_0.$$

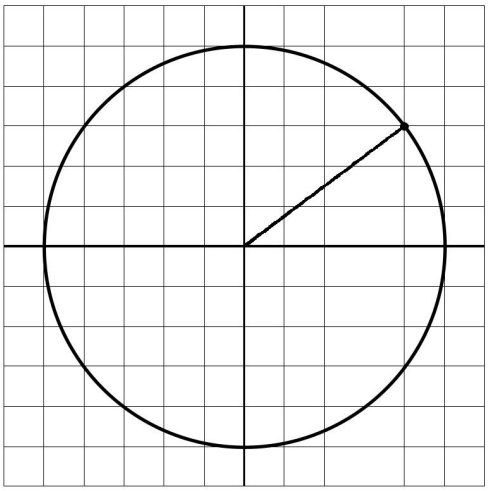
$$s = u, \quad e_{1,1} + e_{1,2} = f_{1,1} + f_{1,2}, \quad \ldots, e_{s,1} + e_{s,2} = f_{s,1} + f_{s,2}.$$

$$t = v, \quad e_{s+1} = f_{s+1}, \quad \ldots, e_{s+t} = f_{s+t}.$$

Además π_0 es asociado a ω_0. Entre los índices $s+1$ y $s+t$ se tiene π_j es asociado a ω_j. Entre los índices 1 y s se tiene $\{\pi_i, \overline{\pi_i}\} = \{\omega_i, \overline{\omega_i}\}$.

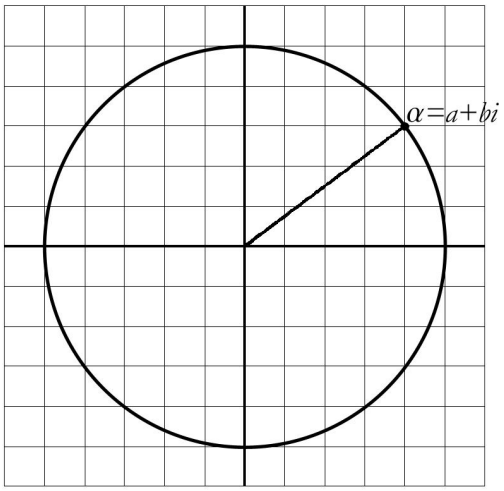
6.4. Circunferencias en una retícula

Si consideramos una retícula en el plano, estamos interesados en las circunferencias que podemos dibujar con la condición de que el centro de la circunferencia sea un punto de la retícula y que ésta pase por un punto del plano. Es evidente que podemos suponer que la circunferencia está centrada en el punto $(0, 0)$.



Si el punto tiene de coordenadas (a, b), el radio de la circunferencia es $r = \sqrt{a^2 + b^2}$. Para ver si un punto de coordenadas (c, d) está o no en la circunferencia, basta comprobar si $\sqrt{c^2 + d^2} = r$.

Observa que los posibles radios son números enteros positivos o nulos o raíces cuadradas (positivas) de números enteros que son sumas de dos cuadrados, por lo tanto r puede no ser un número entero. Los primeros valores para r son: 0, 1, $\sqrt{2}$, 2, ...



Problema. 6.4.
Determinar todos los puntos del plano que están sobre la circunferencia centrada en el punto $(0,0)$ *que pasa por el punto* (a,b).

SOLUCIÓN. Es claro que tenemos que determinar todos los puntos (c,d) que verifiquen $c^2+d^2=a^2+b^2$. Vamos a utilizar la representación que de los puntos de la retícula nos proporcionan los enteros de Gauss. Así el punto de coordenadas (a,b) se representa por el entero de Gauss $\alpha=a+bi$. Un punto arbitrario de la retícula de coordenadas (c,d) que esté sobre la circunferencia se representará por el entero de Gauss $\beta=c+di$.

Tenemos pues que determinar todos los enteros de Gauss β tales que $N(\beta)=N(\alpha)$.

Llamamos $N=N(\alpha)$, y sea $N=2^{e_0}p_1^{e_1}\cdots p_s^{e_s}p_{s+1}^{2e_{s+1}}\cdots p_{s+t}^{2e_{s+t}}$ la descomposición en factores primos de N con las siguientes condiciones: los $p_i\equiv 1 \pmod 4$ si $1\leq i\leq s$ y $p_j\equiv 3 \pmod 4$ si $s+1\leq j\leq s+t$. Como N es una suma de dos cuadrados, resulta que los exponentes de los p_j son pares.

Si π es un entero de Gauss irreducible que divide a β, entonces $N(\pi)$ divide a $N=N(\alpha)$, esto es, $N(\pi)=2, p_i o p_j^2$. Tenemos que contar cuantos enteros de Gauss irreducibles dividen a β; vamos a tener uno por cada uno de los siguientes factores de N: $2,p_1,\ldots,p_s,p_{s+1}^2,\ldots,p_{s+t}^2$.

El siguiente problema es ver en los conjuntos en los que varían estos elementos.

En el caso del factor primo 2, tenemos que elegir un elemento del conjunto $\{1+i, 1-i, -1+i, -1-i\}$, luego hay 4 posibilidades. Si llamamos $\pi = 1+i$, los demás son asociados a π. Si el exponente de 2 es e_0, como hay que elegir e_0 de ellos, resulta que tendremos π^{e_0} multiplicado por un elemento invertible. Las posibilidades que hay, independientemente del exponente, son 4.

En el caso del factor primo $p_i = x+yi$, tenemos que elegir un elemento del conjunto $\{x+yi, x-yi, -x+yi, -x-yi\} \cup \{y+xi, y-xi, -y+xi, -y-xi\}$, luego hay 8 posibilidades. Si llamamos $\pi = x+yi$, el primer conjunto está formado por los asociados de π, y el segundo por los asociados de $\overline{\pi}$. Si el exponente es e_i, tenemos que elegir e_i de ellos; esto lo podemos hacer de e_1+1 formas, y ahora tenemos que hacer intervenir a los elementos invertibles. En total tenemos: $4(e_1+1)$.

En el caso del factor primo p_j, tenemos que elegir un elemento del conjunto $\{p, -p, pi, -pi\}$, luego hay 4 posibilidades. Si llamamos $\pi = p$, el resto de los elementos son asociados a π. Si el exponente es e_j, com tenemos que elegir e_j de ellos, podemos tomar todos iguales a p y hacer intervenir a los elementos invertibles. En total tenemos 4.

Tenemos que el número de diferentes enteros de Gauss que están sobre la circunferencia centrada en $(0,0)$ y que pasa por el punto (a,b) es:

$$4 \times (1 \times (e_1+1) \times \cdots \times (e_s+1) \times 1 \times \cdots \times 1) = 4 \times (1 \times (e_1+1) \times \cdots \times (e_s+1)),$$

ya que basta hacer el producto de los primos y adornarlos de cada uno de los elementos invertibles. □

Ejemplo. 6.5.
Determinar los puntos por los que pasa la circunferencia centrada en $(0,0)$ y que pasa por el punto $(3,4)$.

Solución. Tomamos $\alpha = 3+4i$, entonces $N = 3^2+4^2 = 5^5$. Como $5 \equiv 1 \pmod 4$, y tenemos $5 = (2+i)(2-i)$, resulta que los enteros de Gauss que determina son:

$$\begin{array}{l}(2+i)(2+i), -(2+i)(2+i), i(2+i)(2+i), -i(2+i)(2+i);\\ (2+i)(2-i), -(2+i)(2-i), i(2+i)(2-i), -i(2+i)(2-i);\\ (2-i)(2-i), -(2-i)(2-i), i(2-i)(2-i), -i(2-i)(2-i).\end{array}$$

En total 12 que corresponde a $4 \times (2+1)$.

$$\begin{array}{cccc} 3+4i, & -3-4i, & -4+3i, & 4-3i;\\ 5, & -5, & 5i, & -5i;\\ 3-4i, & -3+4i, & 4+3i, & -4-3i.\end{array}$$

Los puntos son:

$$\begin{array}{cccc} (3,4) & (-3,-4) & (-4,3) & (4,-3)\\ (5,0) & (-5,0) & (0,5) & (0,-5)\\ (3,-4) & (-3,4) & (4,3) & (-4,-3)\end{array}$$

□

Ejemplo. 6.6.
Determinar los puntos por los que pasa la circunferencia centrada en $(0,0)$ y que pasa por el punto $(27,39)$.

SOLUCIÓN. Llamamos $\alpha = 27+39i$; la norma de α es: $N = N(\alpha) = 27^2+39^2 = 2250$.

La factorización en primos de $N = 2250$ es: $N = 2\times 5^3\times 3^2$. El número de puntos de la circunferencia en la retícula es: $4\times(3+1) = 16$. Los puntos son:

$$\begin{array}{rr}
(1+i)(2+i)(2+i)(2+i)3, & (1+i)(2+i)(2+i)(2-i)3,\\
(1+i)(2+i)(2-i)(2-i)3, & (1+i)(2-i)(2-i)(2-i)3\\
-(1+i)(2+i)(2+i)(2+i)3, & -(1+i)(2+i)(2+i)(2-i)3,\\
-(1+i)(2+i)(2-i)(2-i)3, & -(1+i)(2-i)(2-i)(2-i)3\\
i(1+i)(2+i)(2+i)(2+i)3, & i(1+i)(2+i)(2+i)(2-i)3,\\
i(1+i)(2+i)(2-i)(2-i)3, & i(1+i)(2-i)(2-i)(2-i)3\\
-i(1+i)(2+i)(2+i)(2+i)3, & -i(1+i)(2+i)(2+i)(2-i)3,\\
-i(1+i)(2+i)(2-i)(2-i)3, & -i(1+i)(2-i)(2-i)(2-i)3
\end{array}$$

que son:

$$\begin{array}{rrrr}
-27+39i, & 15+45i, & 45+15i, & 39-27i\\
27-39i, & -15-45i, & -45-15i, & -39+27i\\
-39-27i, & -45+15i, & -15+45i, & 27+39i\\
39+27i, & 45-15i, & 15-45i, & -27-39i
\end{array}$$

Que corresponden a los puntos:

$$\begin{array}{rrrr}
(-27,39) & (15,45) & (45,15) & (39,-27)\\
(27,-39) & (-15,-45) & (-45,-15) & (-39,27)\\
(-39,-27) & (-45,15) & (-15,45) & (27,39)\\
(39,27) & (45,-15) & (15,-45) & (-27,-39)
\end{array}$$

□

Ya hemos visto que para todos los enteros positivos r existe una circunferencia centrada en $(0,0)$ de radio r, y que esto es también cierto para algunos números de la forma $\sqrt{r}$; por ejemplo para $\sqrt{2}$. Planteamos ahora el siguiente problema:

Problema. 6.7.
Para qué valores de s podemos construir circunferencias centradas en $(0,0)$, que tengan algún punto de la retícula y sean de radio $\sqrt{s}$.

SOLUCIÓN. Si podemos construir una circunferencia de este tipo, existe un punto (a, b) tal que $\sqrt{s} = \sqrt{a^2 + b^2}$, y por lo tanto $s = a^2 + b^2$. Ahora por el Teorema de Fermat–Euler (6.3.), resulta que los factores primos de s que son congruentes con 3 módulo 4 tienen que tener exponente par. □

Podemos extender la lisa de posibles radios de circunferencias en la retícula en la siguiente forma:

$$0, 1, \sqrt{2}, 2, \sqrt{5}, 2\sqrt{2}, 3, \sqrt{10}, \sqrt{13}, 4, \sqrt{17}, 3\sqrt{2}, \ldots$$

que corresponde a la siguiente lista de valores de s:

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, \ldots$$

Problema. 6.8.
¿Cuántos divisores, salvo asociados, tiene en el anillo de los enteros de Gauss el número 2^k?, siendo k un entero positivo.

SOLUCIÓN. Tenemos $2 = (1+i)(1-i) = (1+i)(-i)(1+i) = -i(1+i)^2$. Por lo tanto, para $k \geq 1$ se tiene:

$$2^k = (-i(1+i)^2)^k = (-i)^k(1+i)^{2k}.$$

Como los divisores se piden salvo asociados, podemos prescindir de $(-i)^k$. Los divisores de $(1+i)^{2k}$ son:

$$(1+i)^{2k}, \quad (1+i)^{2k-1}(1-i), \quad (1+i)^{2k-2}(1-i)^2, \quad \ldots, (1+i)(1-i)^{2k-1}, \quad (1-i)^{2k}$$

a los que hay que añadir el 1. Resulta que 2^k tiene, salvo asociados, exactamente $2k+1$ divisores. □

Ejercicio. 6.9.
Prueba que para cualesquiera enteros de Gauss α, β, con $\beta \neq 0$, se tiene $\overline{(\alpha/\beta)} = \overline{\alpha}/\overline{\beta}$.

SOLUCIÓN. Tenemos:

$$\overline{\left(\frac{\alpha}{\beta}\right)} = \overline{\left(\frac{\alpha\,\overline{\beta}}{\beta\,\overline{\beta}}\right)} = \frac{\overline{\alpha}\,\beta}{\overline{\beta}\,\beta} = \frac{\overline{\alpha}}{\overline{\beta}}.$$

□

Problema. 6.10.
Prueba que no existe ninguna terna de enteros positivos no nulos x, y, z tales que $x^4 + y^4 = z^4$.

SOLUCIÓN. Primero probamos que no existen enteros positivos x, y, z tales que $x^4+y^4 = z^2$. Supongamos lo contrario; podemos suponer que x, y, z son primos relativos dos a dos, y se tiene $(x^2)^2 + (y^2)^2 = z^2$, y existen enteros positivos a, b, que podemos suponer primos relativos, tales que:

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2.$$

Como a, b son primos relativos y $y^2 = 2ab$, entonces a, b son cuadrados; sean $a = a_1^2$ y $b = b_1^2$. se tiene:

$$x^2 = a_1^4 - b_1^4, \text{ luego } x^2 + b_1^4 = a_1^4.$$

Existen a_2, b_2, primos relativos, tales que

$$x = a_2^2 - b_2^2, \quad b_1^2 = 2a_2b_2, \quad a_1^2 = a_2^2 + b_2^2.$$

Observamos que a_2, b_2 son cuadrados, luego existen a_3, b_3 tales que $a_2 = a_3^2$, $b_2 = b_3^2$, Por lo tanto resulta $a_1^2 = a_3^4 + b_3^4$, que es una ecuación del mismo tipo que la ecuación inicial. Se tiene

$$z = a^2 + b^2 = a_1^4 + b_1^4.$$

Por lo tanto $z > a_1$. Esto significa que podemos repetir el proceso e ir disminuyendo el valor del cuadrado original, lo cual s imposible. Por lo tanto no existe una terna $xmymz$ tal que $x^4 + y^4 = z^2$.

Como consecuencia no existe una terna x, y, z tal que $x^4 + y^4 = z^4$.

Este método se llama de **descenso infinito**, y es debido a Fermat. □

Problema. 6.11.
Prueba que no existen enteros positivos x, y tales que $x^3 = y^2 + 1$.

SOLUCIÓN. Supongamos que existen $x, y \in \mathbb{Z}$, $x, y > 0$, tales que $x^3 = y^2 + 1$. Escribimos $x^3 = (y + i)(y - i)$.

Vamos a ver que $y + i$, $y - i$ son primos relativos. Sea $\pi \in \mathbb{Z}[i]$ un entero de Gauss irreducible que divide a ambos, entonces se tiene:

$$\begin{cases} \pi \mid 2y; \\ \pi \mid 2i; \\ \pi^2 \mid x^3; \end{cases} \Rightarrow \quad 2 \mid x^3 \Rightarrow \quad 2 \mid x \Rightarrow \quad \pi^2 \mid x.$$

Sea π^t la mayor potencia de π que divide a $y + i$, entonces existe $\gamma \in \mathbb{Z}[i]$ tal que $\pi^t\gamma = y + i$, y se tiene:

$$y - i = \overline{y + i} = \overline{\pi^t\gamma} = \overline{\pi}^t\,\overline{\gamma} = \pi^t(-i)^t\overline{\gamma}$$

Por lo tanto π^t es la mayor potencia de π que divide a $y - i$. Entonces $\pi^t \mid 2i$, luego $\pi^t \mid 2$. Resulta $t = 1$ ó 2. En estos casos la potencia de π que divide a x^3 es 2 ó 4, lo que es imposible, ya que ésta debería ser un múltiplo de 3. En consecuencia $y + i$, $y - i$ son primos relativos.

Como $y+i, y-i$ son primos relativos y $x^3 = (y+i)(y-i)$, ambos son cubos. Supongamos que $y+i = (a+bi)^3$, entonces:

$$y+i = (a+bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i.$$

Igualando componentes resulta:

$$\begin{aligned} &y = a^3 - 3ab^2, \\ &1 = 3a^2b - b^3, \ \Rightarrow \ 1 = (3a^2 - b)b^2 \ \Rightarrow \ b = \pm 1 \end{aligned}$$

En este caso se tiene:

$$\begin{aligned} &b = 1 \ \Rightarrow \ 3a^2 - 1 = 1 \ \Rightarrow \ a^2 = 2/3 && \text{(imposible).} \\ &b = -1 \ \Rightarrow \ 3a^2 + 1 = 1 \ \Rightarrow \ a = 0 \ \Rightarrow \ y + i = -i \ \Rightarrow \ y = 0 && \text{(imposible).} \end{aligned}$$

□

Problema. 6.12.
Encontrar la factorización en $\mathbb{Z}[i]$ de un entero de Gauss.

Solución. Dado el entero de Gauss $\alpha = a + bi \in \mathbb{Z}[i]$, consideramos $N(\alpha) = a^2 + b^2$ y la factorización en $\mathbb{Z}$, sea ésta:

$$N(\alpha) = 2^e p_1^{e_1} \cdots p_2{}^{e_s} p_{s+1}^{e_{s+1}} \cdots p_{s+t}{}^{e_{s+t}},$$

en donde $p_i \equiv 1 \pmod 4$, si $i = 1, \ldots, s$ y $p_j \equiv 3 \pmod 4$ si $j = s+1, \ldots, s+t$. Por el Teorema de Fermat-Euler (6.3.) los exponentes e_j son pares, supongamos que $e_j = 2f_j$. Para 2 se tiene la factorización $2 = (1+i)(1-1)$, y para cada uno de los p_i existen enteros de Gauss primos, π_i tales que $p_i = \pi_i \overline{\pi}_i$; éstos se pueden calcular según el Lema (5.6.). Por otro lado cada p_j es un entero de Gauss primo.

Escribimos ahora la siguiente igualdad:

$$\begin{aligned} \alpha\,\overline{\alpha} = N(\alpha) &= 2^e p_1^{e_1} \cdots p_2{}^{e_s} p_{s+1}^{2f_{s+1}} \cdots p_{s+t}{}^{2f_{s+t}} \\ &= [(1+i)(1-i)]^e [\pi_1\,\overline{\pi}_1]^{e_1} \cdots [\pi_s\,\overline{\pi}_s]^{e_s} p_{s+1}^{2f_{s+1}} \cdots p_{s+t}{}^{2f_{s+t}} \\ &= [(1+i)^e \pi_1^{e_1} \cdots \pi_s^{e_s} p_{s+1}^{f_{s+1}}][(1-i)^e\,\overline{\pi}_1^{e_1} \cdots \overline{\pi}_s^{e_s} p_{s+1}^{f_{s+1}}]. \end{aligned}$$

En esta ordenación cada $\pi_i^{e_i}$ puede aparecen en el primero o en el segundo factor, aquí los hemos puesto todos en el primer factor. Como $\pi_i\,\overline{\pi}_i = N(\pi_i) = p_i$ divide a $N(\alpha) = \alpha\,\overline{\alpha}$, entonces π_i divide a α o $\overline{\pi}_i$ divide a α; agrupamos en el primer factor aquellos que dividan a α (sólo uno para cada índice), y lo mismo para $1+i$ y $1+i$. Concluimos entonces que α es un asociado a $(1+i)^e \pi_1^{e_1} \cdots \pi_s^{e_s} p_{s+1}^{f_{s+1}}$ (en donde hemos puesto el π_i o $\overline{\pi} i$ que divida a α). Como hay cuatro posibles asociados, es fácil ver cuál de ellos es. □

Ejemplo. 6.13.
Factorizar en $\mathbb{Z}[i]$ el número $\alpha = 5 + 7i$.

Solución. Calculamos $N(\alpha) = \alpha\,\overline{\alpha} = (5+7i)(5-7i) = 25 + 49 = 74 = 2 \times 37$.

Si π en un entero de Gauss irreducible tal que $\pi \mid \alpha$, entonces $N(\pi)|N(\alpha)$. Por lo tanto $N(\pi)|2$ ó $N(\pi)|37$.

Tenemos entonces:

$$N(\pi)|2 \;\Rightarrow\; \pi = 1 + i$$

$$N(\pi)|37; \Rightarrow\; \pi = 6 + i \text{ ó } 6 - i.$$

Comprobamos que $6 - i$ no divide a $5 - 7i$:

$$\frac{5+7i}{6-i} = \frac{(5+7i)(6+i)}{(6-i)(6+i)} = \frac{23}{37} + \frac{47}{37}\,i \notin \mathbb{Z}[i].$$

Por el contrario $6 + i$ divide a $5 + 7i$:

$$\frac{5+7i}{6+i} = \frac{(5+7i)(6-i)}{(6+i)(6-i)} = \frac{37}{37} - \frac{37}{37}\,i = 1 + i \in \mathbb{Z}[i].$$

Tenemos entonces la factorización $5 + 7i = (1 + i)(6 + i)$. □

Problema. 6.14.
¿Cómo obtener una terna pitagórica?

Solución. Se parte de un entero de Gauss, por ejemplo $\alpha = a + bi$; se calcula $\alpha^2 = (a^2 - b^2) + 2abi$. Entonces $N(\alpha^2) = N(\alpha)N(\alpha)$ es un entero y es un cuadrado.

Por otro lado $N(\alpha^2) = (a^2 - b^2)^2 + (2ab)^2$ es una terna pitagórica. □

Problema. 6.15.
¿Puede ser z par si $x^2 + y^2 = z^2$ y x, y, z son primos relativos dos a dos?

Solución. La respuesta es no, ya que si z es par, entonces x e y son impares, y se tiene:

$$(2h+1)^2 + (2k+1)^2 = 4h^2 + 4h + 1 + 4k^2 + 4k + 2 = 4(h^2 + h + k^2 + k) + 2.$$

Como éste tiene que ser un múltiplo de 4, llegamos a una contradicción. □

Teorema. 6.16.
Dado $0 \neq \alpha \in \mathbb{Z}[i]$, no invertible, se considera el anillo cociente $\mathbb{Z}[i]/(\alpha)$. El cardinal de este conjunto es exactamente la norma de α, esto es, $|\mathbb{Z}[i]/(\alpha)| = N(\alpha)$.

Lema. 6.17.
Si $\alpha = 1 + i$, para cada entero positivo t se tiene $|\mathbb{Z}[i]/(\alpha^t)| = 2^t$.

Demostración. Tenemos $\alpha^t \sim 2^s$ si $t = 2s$ y $\alpha^t \sim 2^s(1+i)$ si $t = 2s+1$.

Si $t = 2s$, y $\beta \in \mathbb{Z}[i]$, entonces $\beta \equiv c + di \pmod{\alpha^t}$, con $0 \leq c, d < 2^s$, y resulta $|\mathbb{Z}[i]/(\alpha^t)| \leq 2^s \times 2^s = 2^t$. Además, si $0 \leq c, d, c', d' < 2^s$ y $c + di \equiv c' + d'i \pmod{\alpha^t}$, entonces $(c - c') + (d - d')i \equiv 0 \pmod{\alpha^t} = \pmod{2^s}$, luego $s^2 \mid c - c'$ y $2^s \mid d - d'$, y resulta $|\mathbb{Z}[i]/(\alpha^t)| = 2^t$.

Si $t = 2s+1$, consideramos $\varphi : \mathbb{Z}[i]/(\alpha^t) \longrightarrow \mathbb{Z}[i]/(\alpha^t(1-i))$ definida $\beta + (\alpha^t) \mapsto \beta(1-i) + (\alpha^t(1-i))$. es un homomorfismo inyectivo y su imagen es $((1+i)\mathbb{Z}[i] + (\alpha^t(1-i)))/(\alpha^t(1-i)) = ((1-i)\mathbb{Z}[i])/(\alpha^t(1-i))$. Tenemos entonces

$$\frac{\mathbb{Z}[i]/(\alpha^t(1-i))}{\mathrm{Im}(\varphi)} \cong \frac{\mathbb{Z}[i]/(\alpha^t(1-i))}{((1+i)\mathbb{Z}[i] + (\alpha^t(1-i)))/(\alpha^t(1-i))} \cong \frac{\mathbb{Z}[i]}{(1+i)}$$

que tiene orden 2. Luego $|\mathbb{Z}[i]/(\alpha^t)| = 2^t$. □

Lema. 6.18.
Si α es un entero de Gauss primo tal que $N(\alpha) = p$ es primo y $p \equiv 1 \pmod 4$, entonces $|\mathbb{Z}[i]/(\alpha^t)| = p^t$.

Demostración. Dado $\beta \in \mathbb{Z}[i]$ existen $c, d \in \mathbb{Z}$ tales que $\beta \equiv c + di \pmod{\alpha^t}$. Como $p^t = \alpha^t\,\overline{\alpha}^t \in (\alpha^t)$, podemos suponer que $0 \leq c, d < p^t$. Llamamos $\alpha^t = a + bi$, tenemos $a^2 + b^2 = p^t$, luego $0 \leq b < p^t$. Si $p \mid b$, entonces $p \mid a$ y $p \mid \alpha^t$; como $p = \alpha\,\overline{\alpha}$, resulta que $\overline{\alpha} \mid \alpha$, lo que es una contradicción. Por tanto $p \nmid b$, y b es invertible módulo p. Sea $u \in \mathbb{Z}$ tal que $ub \equiv 1 \pmod p$, entonces

$$\begin{aligned} a + bi &\equiv 0 \pmod{\alpha^t} \\ bi &\equiv -a \pmod{\alpha^t} \\ i &\equiv -ua \pmod{\alpha^t} \end{aligned}$$

Se verifica ahora $\beta = c + di \equiv c - dua \pmod{\alpha^t}$, y cada entero de Gauss es congruente con un entero. Luego $\beta \equiv c \pmod{\alpha^t}$ para algún $0 \leq c < p^t$. Esto implica que $|\mathbb{Z}[i]/(\alpha^t)| \leq p^t$. Dados $0 \leq c, c' < p^t$ tales que $c - c' \equiv 0 \pmod{\alpha^t}$, se tiene $c - c' = \alpha^t \omega$ para cierto $\omega \in \mathbb{Z}[i]$, por lo tanto $(c-c')^2 = N(\alpha^t\omega) = p^t N(\omega)$. Si $t = 1$, entonces $p \mid (c - c')$ y tenemos $c = c'$. Luego $|\mathbb{Z}[i]/(\alpha)| = p$. Consideramos

$$\frac{\mathbb{Z}[i]}{(\alpha)} \xrightarrow{\varphi_1} \frac{\mathbb{Z}[i]}{(\alpha^2)} \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{t-2}} \frac{\mathbb{Z}[i]}{(\alpha^{t-1})} \xrightarrow{\varphi_1} \frac{\mathbb{Z}[i]}{(\alpha^t)}.$$

Definidas $\varphi_j(x + (\alpha^j) = \alpha x + (\alpha^{j+1})$, para $j = 1, \ldots, t-1$. Tenemos

$$\frac{\mathbb{Z}[i]/(\alpha^{j+1})}{\mathrm{Im}(\varphi_j)} = \frac{\mathbb{Z}[i]/(\alpha^{j+1})}{\alpha\mathbb{Z}[i]/(\alpha^{j+1})} \cong \frac{\mathbb{Z}[i]}{(\alpha)},$$

luego tiene p elementos, y por inducción podemos concluir que $|\mathbb{Z}[i]/(\alpha^t)| = p^t$. □

Lema. 6.19.
Si α es un entero de Gauss primo tal que $N(\alpha) = p^2$ es primo y $p \equiv 3 \pmod{4}$, entonces $|\mathbb{Z}[i]/(\alpha^t)| = p^{2t}$.

Demostración. Tenemos $\alpha \sim p$, entonces para cada $\beta \in \mathbb{Z}[i]$ existen $c, d \in \mathbb{Z}$ tales que $\beta \equiv c + di \pmod{p^t}$, con $0 \leq c, d < p^t$, y por tanto $|\mathbb{Z}[i]/(\alpha^t| \leq p^{2t}$. Dados $0 \leq c, d < p$, tales que $c + di \equiv 0 \pmod{\alpha^t}$, existe $\omega \in \mathbb{Z}[i]$ tal que $c + di = P^t\omega$. se tiene entonces $c^2 + d^2 = p^{2t}N(\omega)$. Luego $p^t \mid c^2$ y $p^t \mid d^2$. Si $t = 1$ se tiene $c = 0$ y $d = 0$, luego $|\mathbb{Z}[i]/(\alpha)| = p^2$. Consideramos la cadena

$$\frac{\mathbb{Z}[i]}{(\alpha)} \xrightarrow{\varphi_1} \frac{\mathbb{Z}[i]}{(\alpha^2)} \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{t-2}} \frac{\mathbb{Z}[i]}{(\alpha^{t-1})} \xrightarrow{\varphi_1} \frac{\mathbb{Z}[i]}{(\alpha^t)}.$$

Definidas $\varphi_j(x + (\alpha^j) = \alpha x + (\alpha^{j+1})$, para $j = 1, \ldots, t-1$. Tenemos

$$\frac{\mathbb{Z}[i]/(\alpha^{j+1})}{\mathrm{Im}(\varphi_j)} = \frac{\mathbb{Z}[i]/(\alpha^{j+1})}{\alpha\mathbb{Z}[i]/(\alpha^{j+1})} \cong \frac{\mathbb{Z}[i]}{(\alpha)},$$

luego tiene p^2 elementos, y por inducción podemos concluir que $|\mathbb{Z}[i]/(\alpha^t)| = p^{2t}$. □

Demostración. [del Teorema] Basta ahora para un entero de Gauss α no nulo y no invertible considerar la descomposición en irreducibles. Si ésta es: $\alpha = \pi_0^{e_0}\pi_1^{e_1}\cdots\pi_s{}^{e_s}\pi_{s+1}^{e_{s+1}}\cdots\pi_{s+t}^{e_{s+t}}$, con $\pi_0 = 1 + i$, $N(\pi_i) = p_i \equiv 1 \pmod{4}$, si $i = 1, \ldots, s$, y $N(\pi_{s+j}) = p_{s+j}^2$, con $p_{s+j} \equiv 3 \pmod{4}$, si $j = 1, \ldots, t$, entonces tenemos el isomorfismo

$$\frac{\mathbb{Z}[i]}{(\alpha)} \cong \frac{\mathbb{Z}[i]}{((1+i)^{e_0})} \times \frac{\mathbb{Z}[i]}{(\pi_1^{e_1})} \times \cdots \times \frac{\mathbb{Z}[i]}{(\pi_s^{e_s})} \times \frac{\mathbb{Z}[i]}{(\pi_{s+1}^{e_{s+1}})} \times \cdots \times \frac{\mathbb{Z}[i]}{(\pi_{s+t}^{e_{s+t}})}.$$

Su orden es:

$$2^{e_0}\, p_1^{e_1} \cdots p_s^{e_s}\, p_{s+1}^{2e_{s+1}} \cdots p_{s+t}^{2e_{s+t}} = N(\alpha).$$

□

6.5. El área del círculo

Problema. 6.20. (Problema abierto)
Un problema aún no resuelto es el de determinar, en función de α, el número de elementos de $\mathbb{Z}[i]$, o equivalentemente el número de puntos de la retícula, que son interiores, o están en el borde, de una circunferencia centrada en el origen que pase por el punto α.

En general el problema es: determinar los puntos de la retícula que son interiores a una circunferencia centrada en el origen y que pase por un punto de la retícula.

En este sentido vamos a ver una aproximación a este problema, que según parece es debida a C. F. Gauss y que la desarrolló cuando contaba 22 años.

Para cada entero positivo r vamos a definir

$$c(s) =\mid \{(a,b) \mid \ a^2+b^2=s\} \mid,$$

esto es, el número de puntos de la retícula en la circunferencia de radio $\sqrt{r}$. Como ya sabemos este número, aunque fácil de calcular, tiene un comportamiento algo errático. Veamos algunos de sus valores:

$$\begin{array}{ll} c(0)=1; & (0,0) \\ c(1)=4; & (0,\pm 1),(\pm 1,0) \\ c(2)=4; & (\pm 1,\pm 1) \\ c(3)=0; & \\ c(4)=4; & (0,\pm 2),(\pm 2,0) \\ c(5)=8; & (\pm 1,\pm 2),(\pm 2,\pm 1) \\ c(6)=0; & \\ c(25)=12 & (\pm 3,\pm 4),(\pm 4,\pm 3),(0,\pm 5),(\pm 5,0). \end{array}$$

Vamos a estudiar en vez de la sucesión $\{c(s)\}_{s\geq 0}$, la sucesión de sus sumas. Definimos una nueva sucesión $\{C(s)\}_{s\geq 0}$ mediante:

$$C(s)=c(0)+c(1)+\cdots+c(s).$$

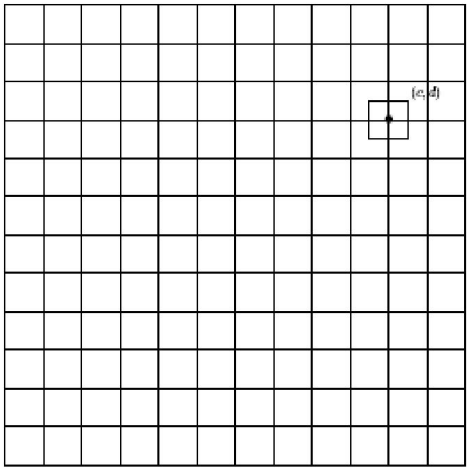
Observa que la sucesión de los valores medios de los $c(s)$, esto es, la sucesión $\{\frac{C(s)}{s+1}\}_{s\geq 0}$ toma valores más predecibles ¿? Veamos cuales son los primeros valores:

$$\begin{array}{l} C(0)/1=1/1=1 \\ C(1)/2=(1+4)/2=2,5 \\ C(2)/3=(1+4+4)/3=3 \\ C(3)/4=(1+4+4+0)/4=2,25 \\ C(4)/5=(1+4+4+0+4)/5=2,6 \\ C(5)/6=(1+4+4+0+4+8)/6=3,5 \\ C(6)/7=(1+4+4+0+4+8+0)/7=3 \end{array}$$

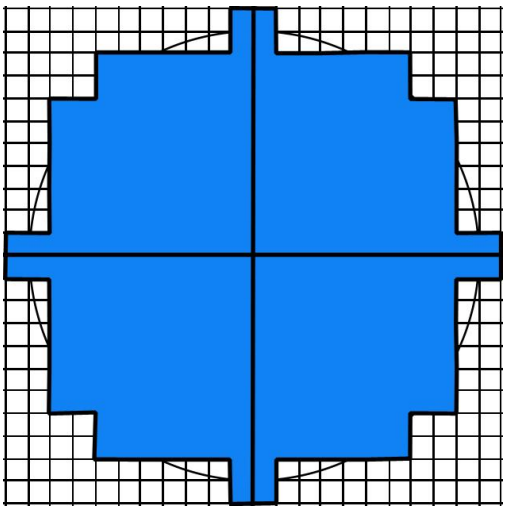
Como se puede observar, los valores de $C(s)/(s+1)$ están próximos a 3. En esta sucesión lo que nos interesa es cual es el valor al que tiende cuando s crece hasta ∞. Gauss observó que este límite es precisamente el número π.

Vamos a adaptar una demostración de este hecho para que se pueda entender en un nivel elemental.

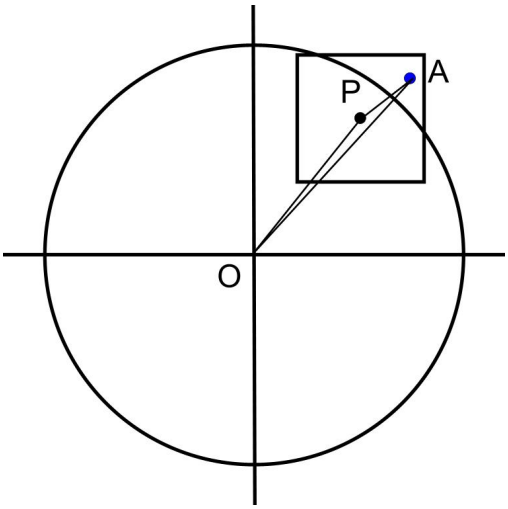
Consideramos la la circunferencia centrada en el punto $(0,0)$ de radio $\sqrt{s}$. Vamos a asociar a cada punto (c,d) de la retícula un cuadrado 1×1 centrado en el punto.



A continuación coloreamos cada uno de estos cuadrados de un color: azul si el punto (c,d) es interior a la circunferencia y blanco si el punto es exterior. Observa que de esta forma tenemos el plano coloreado de azul y blanco. El valor de $C(s)$ se puede calcular contando el área marcada en azul, ya que hay tantos cuadrados de área 1 como puntos hay en el interior y en la frontera.

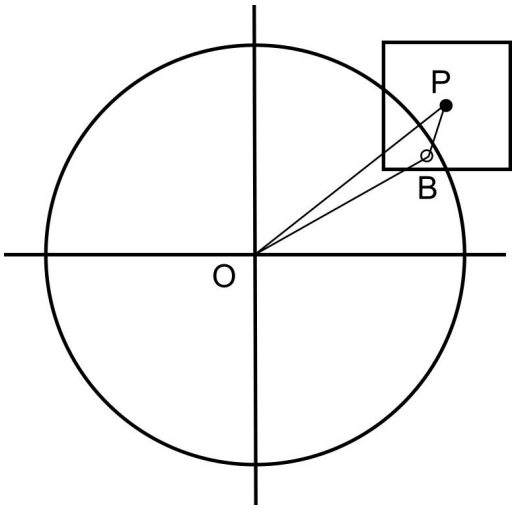


Existen puntos P que están en el interior de la circunferencia (o en el borde) y por lo tanto definen un cuadrado azul, pero éste no está completamente incluido en la circunferencia; es el siguiente caso:



Dado un punto A del cuadrado con centro P, como el cuadrado es azul, la longitud $\overline{OP}$ es menor o igual que $\sqrt{s}$, y la longitud $\overline{PA}$ es menor o igual que $1/\sqrt{2}$, al estar los dos puntos en un cuadro de lado 1. Entonces, por la desigualdad triangular resulta $\overline{OA} \leq \overline{OP}+\overline{PQ} \leq \sqrt{s}+\frac{1}{\sqrt{2}}$. Como consecuencia cualquier punto azul del plano está a una distancia menor ó igual a $\sqrt{s}+\frac{1}{\sqrt{2}}$ del centro O. Esto es, la región azul está contenida en la circunferencia de radio $\sqrt{s}+\frac{1}{\sqrt{2}}$

Por el contrario, hay puntos P que están en el exterior, y definen un cuadrado blanco, pero éste no está totalmente en el exterior; es el siguiente caso:



Dado un punto B del cuadrado con centro P, como el cuadrado es blanco, la longitud $\overline{OP}$ se mayor que $\sqrt{s}$, y la longitud $\overline{PB}$ es menor o igual que $1/\sqrt{2}$. Entonces, por la desigualdad triangular resulta

$\overline{OP} \leq \overline{OB} + \overline{BP}$, y de aquí tenemos $\overline{OB} \geq \overline{OP} - \overline{OB} > \sqrt{s} - \frac{1}{\sqrt{2}}$. Como consecuencia cualquier punto blanco del plano está a una distancia mayor que $\sqrt{s} - \frac{1}{\sqrt{2}}$ del centro O. Esto es, la región azul contiene a la circunferencia de radio $\sqrt{s} - \frac{1}{\sqrt{2}}$.

En resumen, el polígono, que es contorno de la región azul, está en la corona circular delimitada por las dos circunferencias de radios $\sqrt{s} - \frac{1}{\sqrt{2}}$ y $\sqrt{s} + \frac{1}{\sqrt{2}}$ respectivamente. Si queremos medir las áreas tendremos:

$$\pi\left(\sqrt{s} - \frac{1}{\sqrt{2}}\right)^2 \leq C(s) \leq \pi\left(\sqrt{s} + \frac{1}{\sqrt{2}}\right)^2$$

Que podemos desarrollar como sigue:

$$\begin{gathered}
\pi\left(s - \frac{2\sqrt{s}}{\sqrt{2}} + \frac{1}{2}\right) \leq C(s) \leq \pi\left(s + \frac{2\sqrt{s}}{\sqrt{2}} + \frac{1}{2}\right) \\
\pi\left(\frac{1}{2} - \frac{2\sqrt{s}}{\sqrt{2}}\right) \leq C(s) - s\pi \leq \pi\left(\frac{1}{2}\frac{2\sqrt{s}}{\sqrt{2}}\right) \\
\pi\left(\frac{1}{2s} - \frac{2}{\sqrt{2s}}\right) \leq \frac{C(s)}{s} - \pi \leq \pi\left(\frac{1}{2s}\frac{2}{\sqrt{2s}}\right)
\end{gathered}$$

Cuando s crece los términos de los extremos tienden a cero, y por tanto resulta que el límite de $\frac{C(s)}{s}$, cuando s tiende a ∞, es igual a π.

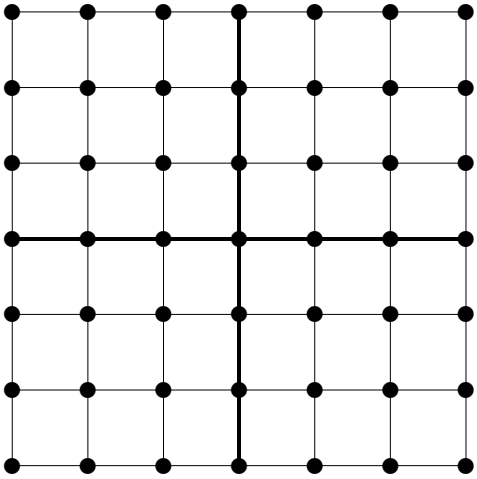
Observa que esta relación lo que nos dice es que π es la razón del área de un círculo al cuadrado del radio.

7. Actividades. Miscelánea

7.1. Distancias en una retícula

Se considera una retícula entera, esto es, los puntos de la misma tienen coordenadas enteras y cada par de punto de coordenadas enteras define un punto de la retícula. Por simplicidad vamos a considerara retículas acotadas.

Consideramos la siguiente retícula: Dada la retícula



¿Qué distancias se pueden medir entre los puntos de la misma? En este caso suponemos que los posibles segmentos van siempre de un punto de la retícula a otro punto de la retícula.

Posibles preguntas:

(1) ¿De qué tipo son las posibles distancias en esta retícula?
(2) ¿Cuántas distancias son posibles en esta retícula?
(3) ¿De qué tipo son las posibles distancias en una retícula, esta vez, $n \times n$?
(4) ¿Cuántas distancias son posibles en una retícula $n \times n$?
(5) Encuentra un triángulo en la retícula con lados enteros.
(6) Encuentra un triángulo en la retícula, que no sea rectángulo, con lados enteros o prueba que no es posible construir tal triángulo.

7.2. Actividades varias

(1) ¿Qué números enteros n se pueden escribir en la forma

$$n = x^2 + y^2,$$

siendo $x, y \in \mathbb{Z}$? Puedes ayudarte de la siguiente tabla, marcando cuales de los números que en ella aparecen cumplen con esta propiedad.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

(2) ¿Hay alguno de ellos que se pueda expresar de varias formas distintas?

(3) Escribe cada entero primo positivo de los siguientes como $p = x^2 + y^2$ o prueba que es imposible.

$$p = 101, 127, 419, 421, 10\,009$$

(4) En la actividad (7.1) habrás encontrado longitudes enteras de segmentos, que no son horizontales ni verticales. Trata de dar un método para encontrar estas longitudes en una retícula cualquiera.
(5) Describe un método para encontrar ternas pitagóricas.
(6) ¿Qué números n pueden escribirse en la forma $n = x^2 - y^2$?
(7) ¿Qué números n pueden escribirse en la forma $n = x^2 + y^2 + z^2$?

Pascual Jara. Departamento de Álgebra. Universidad de Granada
Magdalena Rodríguez. Departamento de Geometría y Topología. Universidad de Granada

Pick en el ajedrez

P. Jara

18 de octubre de 2018

1. El teorema de Pick en el juego del ajedrez

Se considera un tablero de ajedrez, y la pieza correspondiente al caballo. Todos conocen cual es el movimiento del caballo: avanza dos casillas en una dirección, vertical u horizontal, y luego una a la derecha o izquierda.

Es posible hacer caminos realizando sucesivos movimientos de esta pieza; estamos interesados en caminos cerrados que no se cortan a sí mismos. Un ejemplo es el que aparece en la siguiente figura:

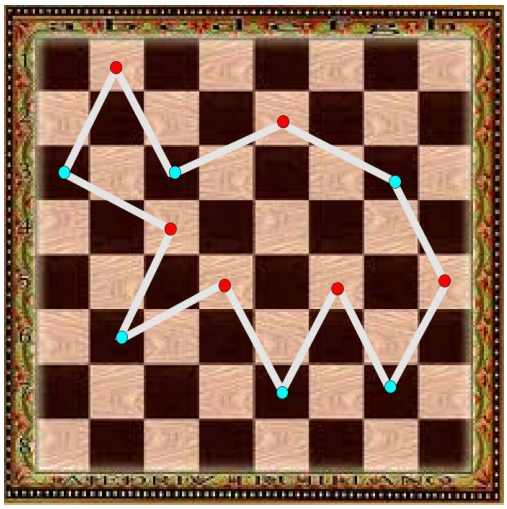
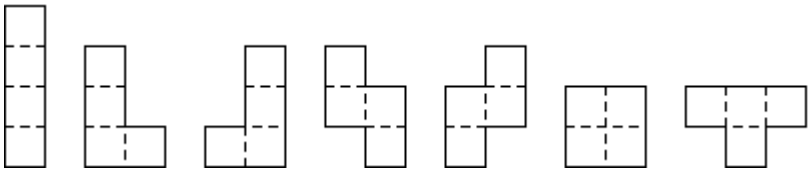


Figura 1: Camino cerrado del caballo.

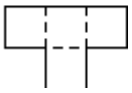
Problema. 1.1.
Prueba que el área encerrada por un camino cerrado de un caballo en un tablero de ajedrez $n \times n$, con $n \geq 4$, es siempre un entero positivo, suponiendo que cada cuadrícula tiene área igual a uno.

ACTIVIDAD 2: Tetraminos.

Un tetramino es una figura plana que está formada por cuatro cuadrados unidos por lados comunes. Salvo rotación y traslación en el plano existen exactamente siete tetraminos distintos; los que aparecen en la siguiente figura.



Planteamos el problema de estudiar cuando una pieza rectangular del plano reticulado puede ser cortada en tetraminos del tipo “T”, esto es:

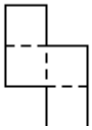


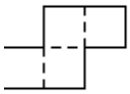
La forma de cortar es seguir las líneas del plano reticulado; las piezas “T” pueden aparecer en cualquier posición

RESPONDER A LAS SIGUIENTES PREGUNTAS:

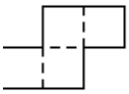
1. ¿Es posible cortar de esta forma, en tetraminos “T”, un cuadrado 10x10?
2. ¿Para qué valores de n es posible cortar cuadrados nxn?
3. ¿Para qué valores de n y m es posible cortar rectángulos nxm?
4. ¿Para cuáles no?

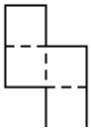
Planteamos el problema de estudiar si una pieza rectangular del plano reticulado puede ser cortada en tetraminos del tipo “S”, esto es:





La forma de cortar es seguir las líneas del plano reticulado, y las piezas “S” pueden aparecer en cualquier posición





RESPONDER A LAS SIGUIENTES PREGUNTAS:

1. ¿Es posible cortar de esta forma, en tetraminos “S”, un cuadrado?
2. ¿Es posible cortar de esta forma, en tetraminos “S”, un rectángulo?

ACTIVIDAD 3a: JUEGO EN UNA RETÍCULA (dividiendo rectángulos)

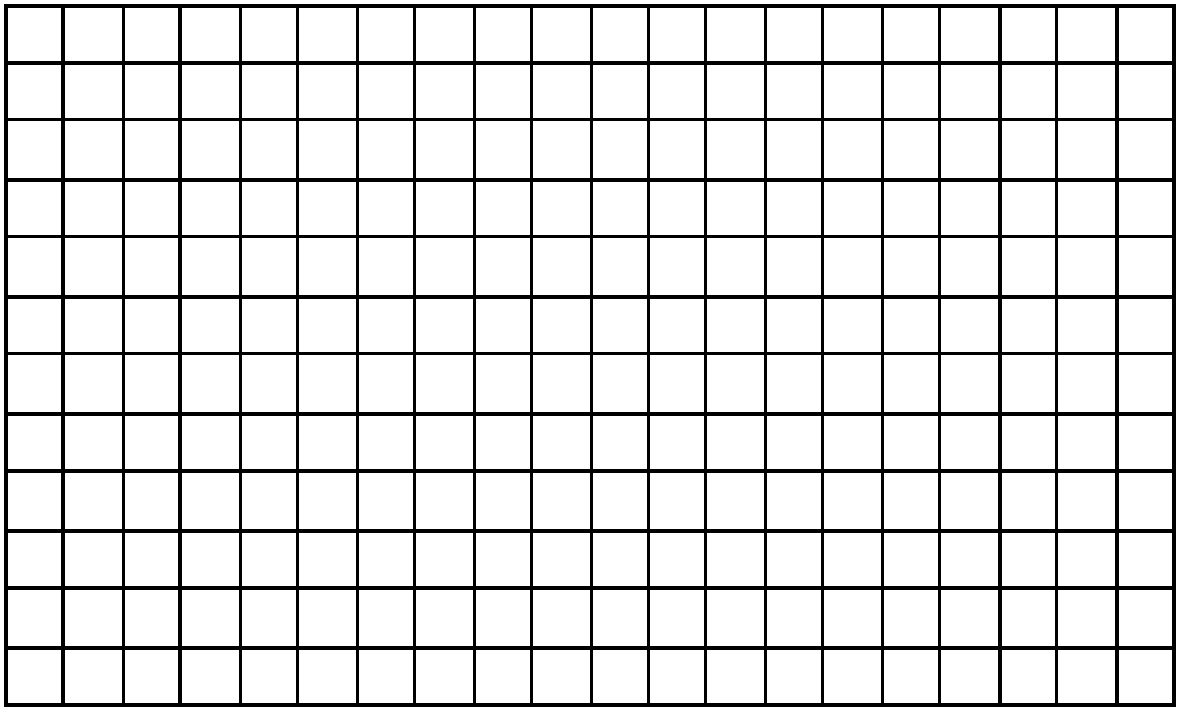
En una retícula se dibuja se rectángulo de las dimensiones que se estimen (por ejemplo 17x15) y se marca uno de los cuadrados básicos de la retícula que queden dentro del rectángulo.

En el juego participan dos jugadores, en su turno cada jugador traza un segmento que corte el interior del rectángulo (siguiendo las líneas de la retícula) y elimina la parte del mismo que no contiene al cuadradito marcado. Pierde el jugador que no puede realizar su jugada, esto es, que no puede dividir el rectángulo resultante.

ACTIVIDAD:

Puedes considerar en un principio rectángulos de dimensiones más bajas, y te aconsejo que marques siempre el cuadro situado en una de las esquinas.

1. Diseña estrategias para ganar, si las hay.
2. Cuando hayas encontrado estas estrategias, en función de las dimensiones del rectángulo, puedes modificar el juego y colocar el cuadrado marcado en lugares distintos a los de las esquinas.



ACTIVIDAD 3b: JUEGO EN UNA RETÍCULA (haciendo rayitas) I

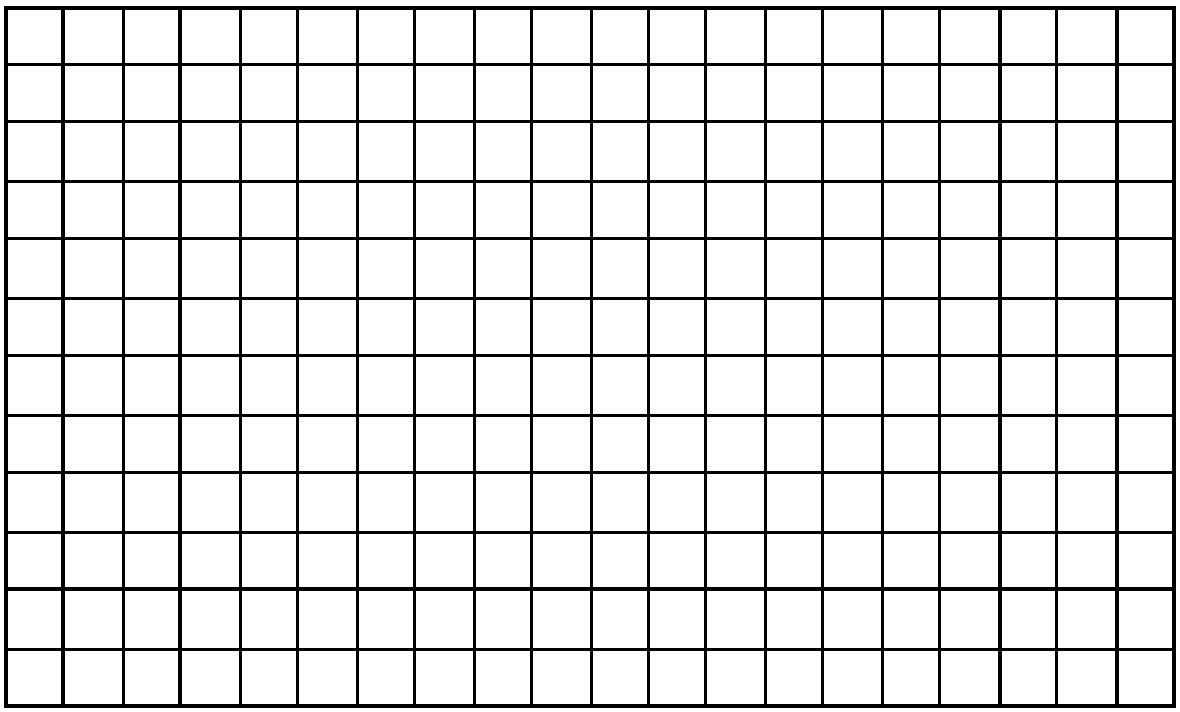
Se delimita una región cerrada de la retícula, por ejemplo un rectángulo. Las reglas del juego son los siguientes:

1. El primer jugador une por un segmento dos puntos de la retícula que estén contiguos en la misma fila o columna.
2. El segundo jugador elige uno de los puntos extremos y lo une con otro nuevo que esté contiguo en la misma fila o columna.
3. Por turnos cada jugador en su turno une un el nuevo punto con otro nuevo que esté contiguo en la misma fila o columna.
4. Pierde el jugador que no puede realizar movimientos.

ACTIVIDAD:

Puedes considerar en un principio rectángulos de dimensiones más pequeñas y desarrollar estrategias ganadoras si las hay.

1. Diseña estrategias para ganar, si las hay.
2. Cuando hayas encontrado estas estrategias, en función de las dimensiones del rectángulo, puedes modificar el juego.



ACTIVIDAD 3c: JUEGO EN UNA RETÍCULA (haciendo rayitas) II

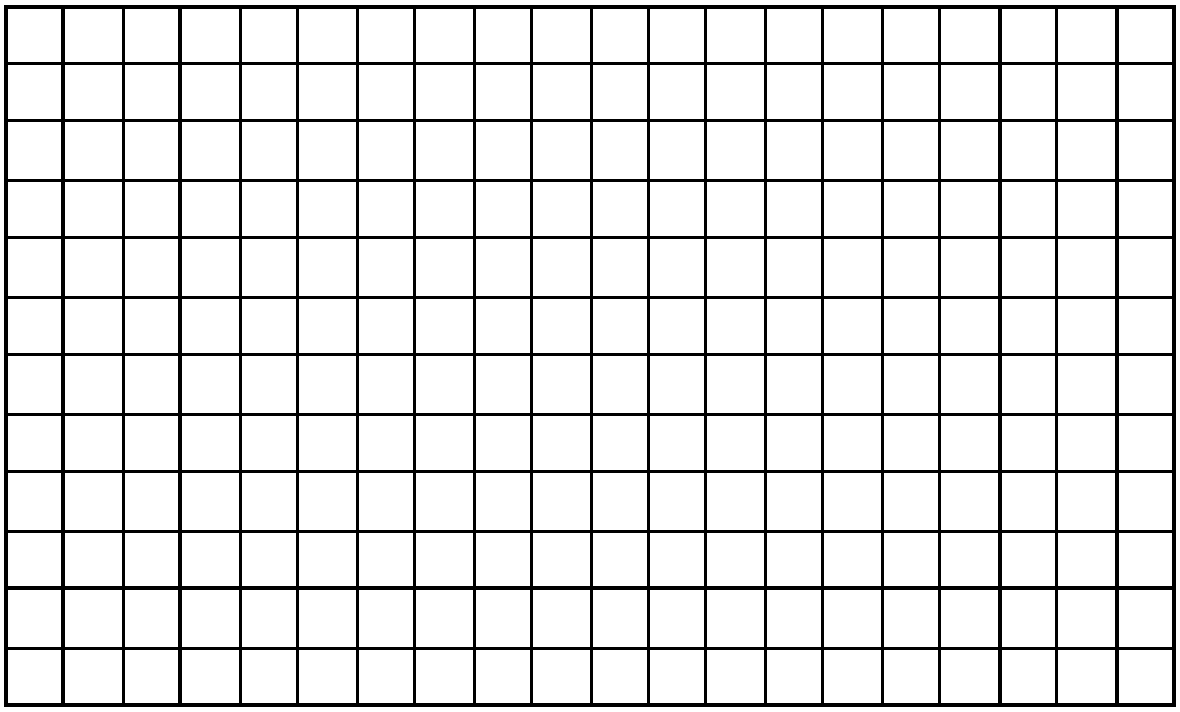
Se delimita una región cerrada de la retícula, por ejemplo un rectángulo. Las reglas del juego son los siguientes:

1. El primer jugador une por un segmento dos puntos de la retícula que estén contiguos en la misma fila o columna.
2. El segundo jugador elige uno de los puntos extremos y lo une con otro nuevo que esté contiguo en la misma fila o columna.
3. Por turnos cada jugador en su turno une un punto extremo con otro nuevo que esté contiguo en la misma fila o columna.
4. Pierde el jugador que no puede realizar movimientos.

ACTIVIDAD:

Puedes considerar en un principio rectángulos de dimensiones más pequeñas y desarrollar estrategias ganadoras si las hay.

3. Diseña estrategias para ganar, si las hay.
4. Cuando hayas encontrado estas estrategias, en función de las dimensiones del rectángulo, puedes modificar el juego.



ACTIVIDAD 4: Zapatero a tus zapatos

Tienes un zapato, como el que aparece en la figura.

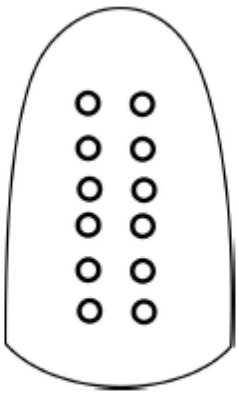


Figura 11. Zapato

Queremos acordonarlo de forma que la longitud del cordón usado sea mínima. Aquí tienes dos ejemplos.

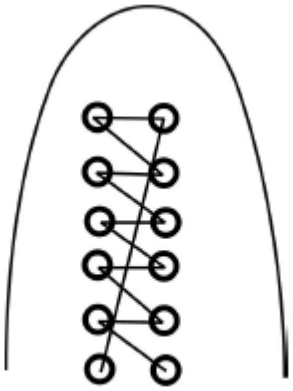


Figura 12. Modo clásico

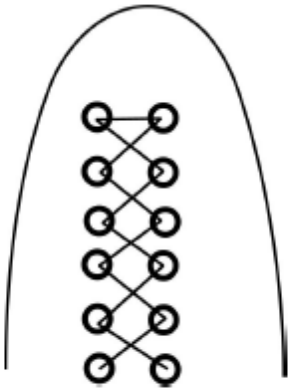


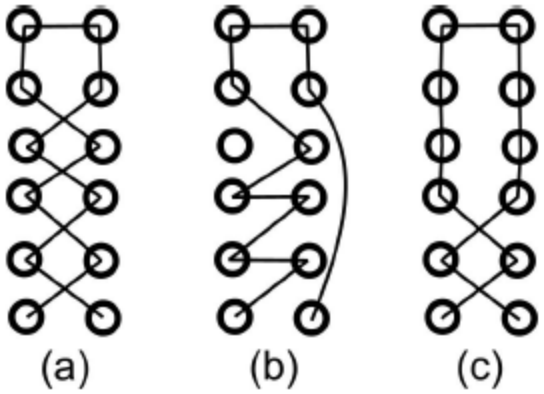
Figura 13. Modo deportivo

¿Cuál de ellos utiliza menos cordón?

PARTE 1: Definición de acordonado

La primera actividad consiste en definir cuando un acordonado es correcto o no.

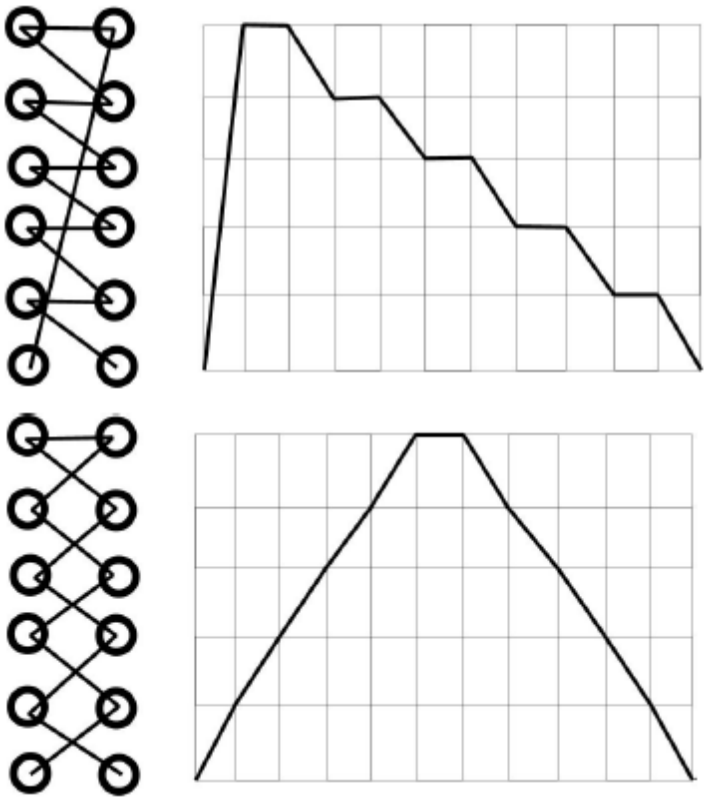
En los siguientes ejemplos, solo el primero representa un acordonado correcto.



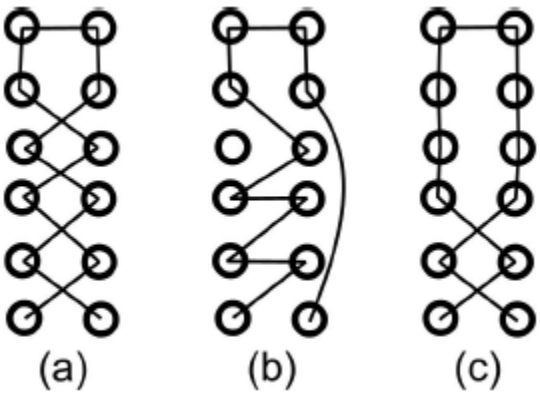
PROBLEMA: Haz una definición de acordonado.

PARTE 2: Representación de un acordonado

Cada acordonado se puede representar en una retícula, aquí tienes dos ejemplos.



PROBLEMA: Representa los siguientes acordonados mediante una retícula.



PARTE 3: Acordonado mínimo

Buscar LA forma de acordonar un zapato que utilice menor longitud de cordón.