Los Números Complejos

Los **números complejos** son los números de la forma $a+ib$ donde a y b son números reales, y $\mathbf{i}$ es un **numero imaginario** tal que $\mathbf{i}^2 = -1$.

Los números complejos a veces se representan con una sola letra $\mathbf{z}=a+bi$, decimos que a es la **parte real** de $\mathbf{z}$ y que b es su **parte imaginaria**. Los números complejos distintos de 0 con parte real 0 se llaman **imaginarios**.

Los números complejos pueden sumarse coordenada a coordenada. Si $\mathbf{z}=a+bi$ y $\mathbf{w}=c+di$

$$\mathbf{z}+\mathbf{w} = (a+b\mathbf{i}) + (c+d\mathbf{i}) = (a+c)+(b+d)\mathbf{i}$$

Es inmediato que la suma es conmutativa y asociativa, que hay un neutro aditivo y que cada numero $\mathbf{z}=a+b\mathbf{i}$ tiene un inverso aditivo, $-\mathbf{z}=-a-b\mathbf{i}$.

Ejemplo. Si $\mathbf{z}=1+\sqrt{2}\mathbf{i}$ y $\mathbf{w}=1-\sqrt{2}\mathbf{i}$ entonces $\mathbf{z}+\mathbf{w}=2$ y $\mathbf{z}-\mathbf{w}=2\sqrt{2}\mathbf{i}$

Los números complejos también pueden multiplicarse, distribuyendo el producto con la suma y haciendo que el numero i conmute con los números reales: $\mathbf{z}=a+b\mathbf{i}$ y $\mathbf{w}=c+d\mathbf{i}$ entonces

$$\mathbf{z}\cdot\mathbf{w} = (a+b\mathbf{i}) \cdot (c+d\mathbf{i}) = ac+ad\mathbf{i}+b\mathbf{i}c+bd\mathbf{i}^2 = (ac-bd) + (ad+bc)\mathbf{i}$$

Ejemplos. Si $\mathbf{z}=-2+3\mathbf{i}$ y $\mathbf{w}=5+7\mathbf{i}$ entonces $\mathbf{z}\cdot\mathbf{w} = (-2\cdot5 -3\cdot7)+(-2\cdot7+3\cdot5)\mathbf{i} = -31+\mathbf{i}$

Si $\mathbf{z}=1+\sqrt{2}\mathbf{i}$ y $\mathbf{w}=1-\sqrt{2}\mathbf{i}$ entonces $\mathbf{z}\cdot\mathbf{w} = (1+2)+(-\sqrt{2}+\sqrt{2})\mathbf{i} =3$

Es fácil ver que el producto es conmutativo pero no es inmediato que sea asociativo (tarea).

El 1 es un neutro multiplicativo, y la multiplicación por $\mathbf{i}$ es sencilla: si $\mathbf{z}=a+bi$ entonces $\mathbf{iz}=-b+ai$

Lema. Para cada numero complejo $\mathbf{z}\neq0$ existe un único numero complejo que multiplicado por $\mathbf{z}$ da 1. Este es el inverso multiplicativo de $\mathbf{z}$, y es denotado por $\mathbf{z}^{-1}$.

Demostración. Si $\mathbf{z}=a+b\mathbf{i}$ y $\mathbf{w}=c+d\mathbf{i}$ entonces $\mathbf{zw}=(ax-by)=(ay+bx)\mathbf{i}$ y este numero es 1 si y solo si

$$ax -by = 1$$

$$bx +ay = 0$$

Si multiplicamos la primera ecuación por a y la segunda por b y las sumamos obtenemos

$(a^2+b^2)x = a$ así que $x = \dfrac{a}{a^2+b^2}$ siempre que $a^2+b^2\neq0$.

Si multiplicamos la primera ecuación por b y la segunda por a y las restamos obtenemos

$-(a^2+b^2)y = b$ así que $y = \dfrac{-b}{a^2+b^2}$ siempre que $a^2+b^2\neq0$.

Observar que $a^2+b^2=0$ solamente cuando $a=b=0$, es decir, cuando $\mathbf{z}=0$.

Se puede verificar fácilmente que $(a+b\mathbf{i})\left(\dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}\mathbf{i}\right) = 1$, asi que este es un inverso.

La demostración de que los inversos multiplicativos son únicos es la misma que en cualquier anillo conmutativo: Si $zw=1=zw'$ entonces $w'=w'1=w'(zw)=(w'z)w=(zw')w=1w=w$. •

Ejemplos.

- El inverso multiplicativo de $\mathbf{i}$ es $-\mathbf{i}$, ya que $\mathbf{i}(-\mathbf{i}) = -\mathbf{i}\cdot\mathbf{i} = 1$
- El inverso multiplicativo de $z = 2+3\mathbf{i}$ es $z^{-1} = \dfrac{2}{2^2+3^2} - \dfrac{3}{2^2+3^2}\mathbf{i} = \dfrac{2}{13} - \dfrac{3}{13}\mathbf{i}$

Como cada número complejo distinto de 0 tiene un inverso multiplicativo, podemos definir la división de complejos $\mathbf{z}$ y $\mathbf{w}\neq 0$, como $\mathbf{z}/\mathbf{w} = \mathbf{z}\mathbf{w}^{-1}$.

Ejemplos.

- $\dfrac{3+4\mathbf{i}}{\mathbf{i}} = (3+4\mathrm{i})\, \mathbf{i}^{-1} = (3+4\mathbf{i})\,(-\mathbf{i}) = 4-3\mathbf{i}$
- $\dfrac{4+5\mathbf{i}}{2+3\mathbf{i}} = (4+5\mathbf{i})\cdot(2+3\mathbf{i})^{-1} = (4+5\mathbf{i})\,\left(\dfrac{2}{13} - \dfrac{3}{13}\mathbf{i}\right) = \dfrac{23}{13} - \dfrac{2}{13}\mathbf{i}$

Las observaciones anteriores demuestran el siguiente

Teorema. Los complejos forman un campo, denotado por **C**, que es una extensión del campo de los números reales **R**.

Los números complejos conservan muchas de las propiedades de los números reales, pero con los complejos se pueden hacer otras cosas que son imposibles con los reales.

La raíz *cuadrada* de un numero $\mathbf{z}$ es un numero $\mathbf{w}$ tal que $\mathbf{w}^2=\mathbf{z}$. Ya sabemos que cada numero real positivo r tiene 2 raíces cuadradas reales, una positiva y otra negativa, denotadas $\sqrt{r}$ y $-\sqrt{r}$.

El 0 solo tiene una raíz cuadrada real, y los números negativos no tienen ninguna raíz real.

Como $\mathbf{i}^2=-1$, cada numero real negativo r tiene al menos dos raíces complejas: $\sqrt{-r}\,\mathbf{i}$ y $-\sqrt{-r}\,\mathbf{i}$.

Así que todos los números reales tienen raíces cuadradas complejas (que incluyen a las reales) y es natural preguntarse cuales otros números complejos tendrán raíces cuadradas complejas.

Ejemplo. ¿El número $\mathbf{i}$ tendrá raíz cuadrada? Hay que ver si existe un numero complejo $\mathbf{w}$ tal que $\mathbf{w}^2=\mathbf{i}$.

Si escribimos $\mathbf{w}=x+y\mathbf{i}$, entonces $\mathbf{w}^2 = (x+y\mathbf{i})(x+y\mathbf{i}) = (x^2-y^2) + (2xy)\mathbf{i}$

Así que $\mathbf{w}^2 = \mathbf{i}$ si y solo si $x^2-y^2= 0$ y $2xy = 1$.

La primera ecuación dice que $x=y$ o $x= -y$, la segunda ecuación dice que $2x^2=1$ o $-2x^2=1$, la primera de estas tiene soluciones $x=1/\sqrt{2}$, $x=- 1/\sqrt{2}$ y la segunda no tiene soluciones (porque x debe ser real), así que $x=y$ y los dos posibles valores de $\mathbf{w}$ son

$\mathbf{w}_1 = 1/\sqrt{2} + 1/\sqrt{2}\,\mathbf{i}$

$\mathbf{w}_2 = -1/\sqrt{2} - 1/\sqrt{2}\,\mathbf{i}$

y es fácil comprobar que $\mathbf{w}_1$ y $\mathbf{w}_2$ son raíces de $\mathbf{i}$.

Lema. Cada número complejo $\mathbf{z}\neq 0$ tiene exactamente dos raíces cuadradas complejas.

Demostración. Si $\mathbf{z}=a+b\mathbf{i}$ entonces $\mathbf{w}=x+y\mathbf{i}$ es una raíz cuadrada de $\mathbf{z}$ si y solo si $\mathbf{w}^2 = \mathbf{z}$, es decir si

$(x+y\mathbf{i})(x+y\mathbf{i}) = (x^2-y^2)+(2xy)\mathbf{i} = a+b\mathbf{i}$ o sea si

$x^2-y^2 = a$ (1)

$2xy = b$ (2)

De (2) podemos despejar $y= b/2x$ y si sustituimos en (1) obtenemos $x^2 -b^2/4x^2 = a$

y multiplicando por x^2 obtenemos $x^4 -b^2/4 = ax^2$ que equivale a $x^4 -ax^2 -b^2/4 = 0$

Esta es una ecuación cuadrática en la incógnita x^2 y sus soluciones (en caso de existir) son

$$x^2 = \frac{a \pm\sqrt{a^2+b^2}}{2}$$

como $a^2+b^2>0$ la raíz es real y como a $a^2+b^2\geq a$ entonces $\frac{a +\sqrt{a^2+b^2}}{2}$ es positivo y $\frac{a -\sqrt{a^2+b^2}}{2}$ es negativo, así que solo la primera tiene raíces reales, que son

$$x= \pm\sqrt{\frac{a +\sqrt{a^2+b^2}}{2}}$$

así que hay dos valores posibles para x. De manera similar podemos hallar los dos valores posibles para y

$$y= \pm\sqrt{\frac{-a +\sqrt{a^2+b^2}}{2}}$$

Se puede checar que solo 2 de las 4 combinaciones posibles de valores de x y y (tomando los 2 signos positivos o los 2 negativos) dan números complejos $\mathbf{w}=x+y\mathbf{i}$ que son raíces cuadradas de $a+b\mathbf{i}$. •

Ejemplos.

Las raíces cuadradas de $-\mathbf{i}$ son $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\mathbf{i}$ y $-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\mathbf{i}$

Las raíces cuadradas de $2+3\mathbf{i}$ son $\sqrt{\frac{2 +\sqrt{13}}{2}} + \sqrt{\frac{-2+\sqrt{13}}{2}}\,\mathbf{i}$ y $-\sqrt{\frac{2 +\sqrt{13}}{2}} - \sqrt{\frac{-2+\sqrt{13}}{2}}\,\mathbf{i}$.

Teorema. Todo polinomio de segundo grado con coeficientes complejos tiene raíces (soluciones) complejas.

Demostración. Sea $a\mathbf{z}^2 + b\mathbf{z} + c = 0$ un polinomio con a, b, c números complejos.

$\mathbf{z}^2 +{}^b/_a\,\mathbf{z} +{}^c/_a = 0 \quad\Leftrightarrow$

$\mathbf{z}^2 +{}^b/_a\,\mathbf{z} +({}^b/_{2a})^2 +{}^c/_a = ({}^b/_{2a})^2 \quad\Leftrightarrow$

$(\mathbf{z}+{}^b/_{2a})^2 + {}^c/_a = ({}^b/_{2a})^2 \quad\Leftrightarrow$

$$(\mathbf{z}+{}^b/_{2a})^2 = \frac{b^2-4ac}{4a^2}$$

Como todos los números complejos tienen raíces cuadradas, la ultima igualdad equivale a:

$$\mathbf{z}+{}^b/_{2a} = \pm\frac{\sqrt{b^2-4ac}}{2a}$$

o sea

$$\mathbf{z} = \frac{-b \pm\sqrt{b^2-4ac}}{2a}$$

que es la misma formula para resolver ecuaciones cuadráticas reales. •

Ejemplos. ¿Cuales son las raíces de los siguientes polinomios?

$z^2+3z+5 = 0$ Las soluciones son $z = \dfrac{-3 \pm \sqrt{3^2-4(1)5}}{2(1)} = \dfrac{-3 \pm \sqrt{-11}}{2} = -\dfrac{3}{2} \pm \dfrac{11}{\sqrt{2}}\,\mathbf{i}$

$iz^2+z+i = 0$ Las soluciones son $z = \dfrac{-1 \pm \sqrt{1^2-4(\mathbf{i})\mathbf{i}}}{2(\mathbf{i})} = \dfrac{-1 \pm \sqrt{5}}{2(\mathbf{i})} = \dfrac{1 \mp \sqrt{5}}{2}\,\mathbf{i}$

$iz^2+z+1-i = 0$ Las soluciones son $z = \dfrac{-1 \pm \sqrt{12-4(\mathbf{i})(1+\mathbf{i})}}{2(\mathbf{i})} = \dfrac{-1 \pm \sqrt{-3-4\mathbf{i}}}{2(\mathbf{i})} = \dfrac{-1\pm(1-2\mathbf{i})}{2\mathbf{i}} = -1,\ 1+\mathbf{i}$

Problemas.

1. Calcula a. $(2+3i)(4-3i)$ b. $(1-i)^3$ c. $(1-i)(2-i)(3-i)$

2. Escribe a los siguientes números en la forma a+bi

a. $\dfrac{1}{3+2i}$ b. $\dfrac{4+5i}{1-2i}$ c. $(1+i)^{-2}$ d. $\sqrt{3+4i}$

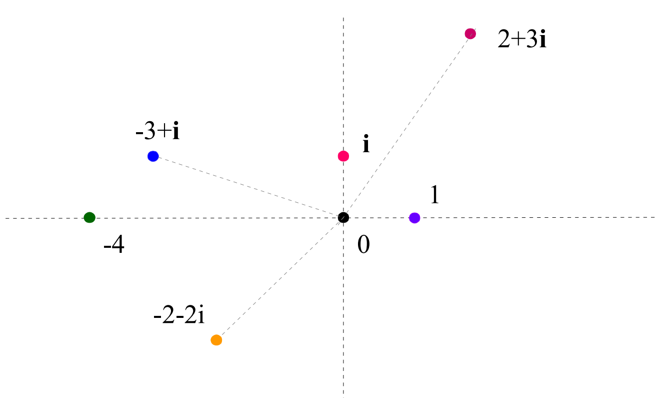
3. a. Da dos números complejos cuya suma sea real y su diferencia sea imaginaria.
   b. Da dos números complejos cuyo producto sea real y su cociente sea imaginario.

4. Demuestra que la multiplicación de números complejos es asociativa.

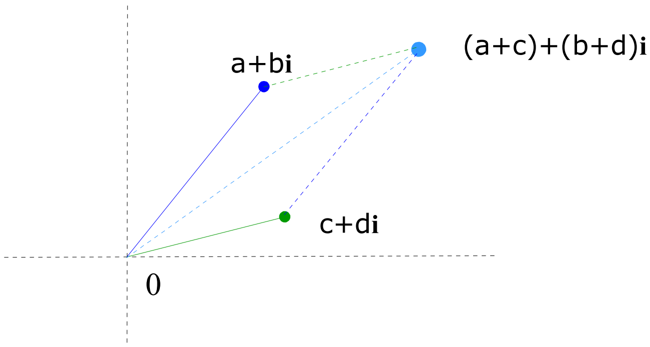
5. Encuentra las soluciones de los siguientes polinomios
   a. $z^2+2z+3=0$ b. $z^2+2z+i=0$

Representación geométrica de los números complejos.

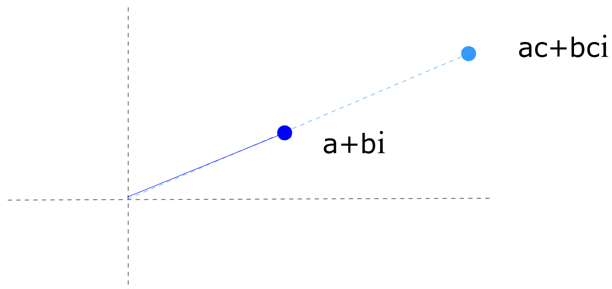
Así como los números reales pueden identificarse con los puntos o segmentos en una recta, los números complejos pueden identificarse con los puntos o vectores en el plano.



La suma de números complejos corresponde a la suma de vectores:

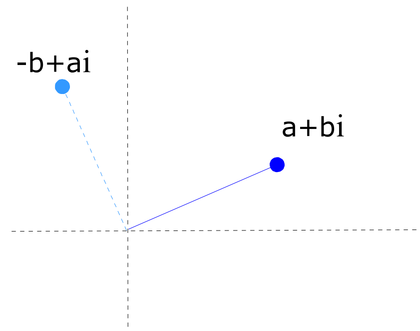


La multiplicación de complejos es mas interesante.



Al multiplicar un complejo a+bi por un real c obtenemos ac+bci, asi que multiplicar por un real positivo c equivale a escalar por el factor c.

La multiplicación por -1 invierte la dirección.



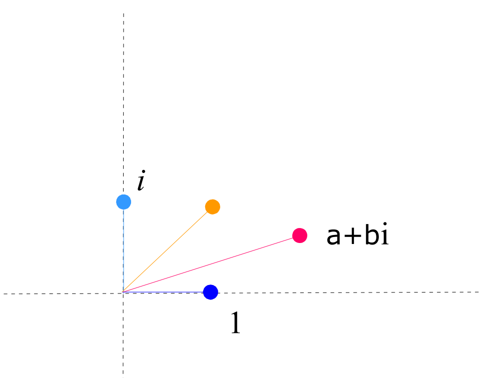
Al multiplicar a un complejo a+bi por i obtenemos -b+ai,o sea que el vector (a,b) va al vector perpendicular (-b,a).

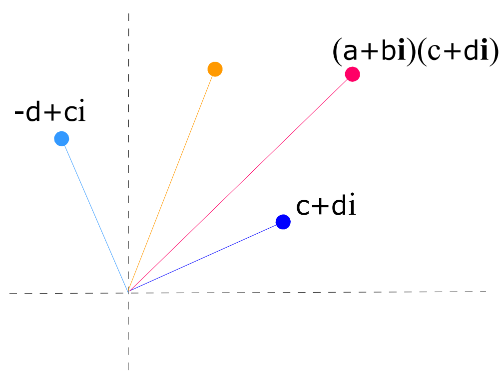
Así que multiplicar por i equivale a rotar 90°.

Para ver que hace la multiplicación por un complejo c+di, consideremos la función que a cada complejo x+yi lo multiplica por c+di, es decir f(x+yi) = (cx-dy)+(dx+cy)i

Si vemos a los complejos como vectores, f(x,y)=(cx-dy,dx+cy) es una transformación lineal por lo que esta determinada por f(1,0) y f(0,1).

Como f(1,0)=(c,d) y f(0,1)=(-d,c) los dos vectores rotan el mismo ángulo y crecen en la misma proporción, entonces todos los vectores del plano deben rotar y girar en la misma proporción.





Así que la multiplicación por un complejo rota y escala a todos los complejos por igual.

Problemas.

6. Si $\mathbf{z}=1+2\mathrm{i}$ $\mathbf{w}=3-\mathrm{i}$ dibuja cuidadosamente los puntos del plano que corresponden a
   $\mathbf{z}$ $\mathbf{w}$ $\mathbf{z}+\mathbf{w}$ $\mathbf{z}-\mathbf{w}$ $\mathbf{zw}$

7. Dibuja cuidadosamente los puntos del plano que corresponden a $\mathbf{z}$ y a $\mathbf{1/z}$

   a. $\mathbf{z}=1+2\mathrm{i}$ b. $\mathbf{z}=3-\mathrm{i}$

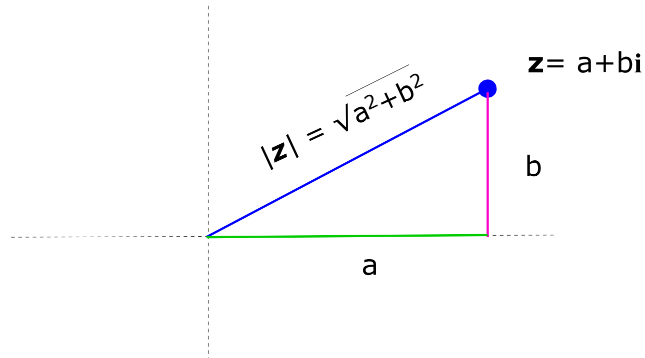
8. Si $\mathbf{z}=1+\mathrm{i}$ dibuja cuidadosamente juntos a $\mathbf{z}^0$, $\mathbf{z}^1$, $\mathbf{z}^2$, $\mathbf{z}^3$, $\mathbf{z}^4$.

9. a. Encuentra dos números complejos que sumados den $1+2\mathrm{i}$ y restados den $3+4\mathrm{i}$.

   b. Encuentra dos números complejos que multiplicados den $2+\mathrm{i}$ y divididos den $1+2\mathrm{i}$.

   c. Encuentra dos números complejos que sumados den 1 y multiplicados den 2.

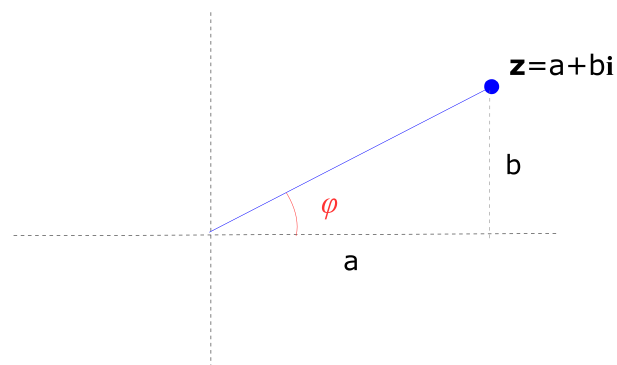
Módulo y argumento.



El **módulo**, **magnitud** o **norma** de un número complejo $\mathbf{z}=a+b\mathrm{i}$ es el número real $|\mathbf{z}|$ que mide el tamaño de $\mathbf{z}$ como vector

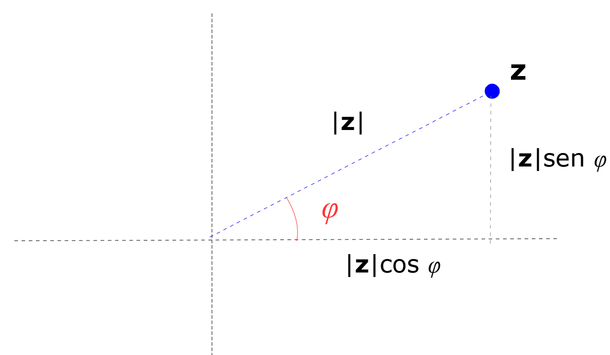
$$|\mathbf{z}| = \sqrt{a^2+b^2}$$

Ejemplo. $|2+3\mathrm{i}| = \sqrt{2^2+3^2} = \sqrt{13}$



El **argumento** de $\mathbf{z}$ es el ángulo φ entre $\mathbf{z}$ y 1 vistos como los vectores (a,b) y $(1,0)$ es decir $\arg(\mathbf{z})= \tan^{-1}({}^{b}/_{a})$.

Observar que $\arg(\mathbf{z})$ solo esta bien definido salvo múltiplos de 2π, así por ejemplo, podemos escribir $\arg(-\mathrm{i}) = -{}^{1}/_{2}\,\pi$ y también $\arg(-\mathrm{i}) = {}^{3}/_{2}\,\pi$.



Ejemplo. Si $\mathbf{z} = 2+3\mathrm{i}$ entonces $|\mathbf{z}| = \sqrt{2^2+3^2} = \sqrt{13}$

$\arg(\mathbf{z})=\tan^{-1}(3/2) \approx 0.9827$ radianes.

Observar que si un número complejo $\mathbf{z}$ tiene argumento φ entonces $\mathbf{z} = |\mathbf{z}|\,(\cos\varphi + \operatorname{sen}\varphi\ \mathrm{i})$

Esta es la **expresión polar** de los números complejos.

Ejemplo. La expresión polar de $\mathbf{z}=1+\mathbf{i}$ es $\mathbf{z}=\sqrt{2}(\cos{}^{\pi}/_{4}+\operatorname{sen}{}^{\pi}/_{4}\,\mathbf{i})$.

Los complejos de norma 1 se llaman **unitarios**, son los que pueden escribirse $\mathbf{z} = \cos\varphi + \operatorname{sen}\varphi\ \mathbf{i}$

Lema. Las magnitudes de los complejos cumplen las *desigualdades del triángulo*

1. $|\mathbf{z}+\mathbf{w}| \leq |\mathbf{z}| + |\mathbf{w}|$
2. $|\mathbf{z}-\mathbf{w}| \geq ||\mathbf{z}|-|\mathbf{w}||$

Demostración.

1. Hay que ver que si $\mathbf{z}=a+bi$ y $\mathbf{w}=c+di$ entonces $|(a+ib)+(c+id)| \leq |a+ib|+|c+id|$

   Esto se sigue inmediatamente de la desigualdad del triángulo para vectores en el plano demostrada en geometría analítica. También se puede demostrar algebráicamente viendo que las siguientes desigualdades son equivalentes:

   $|(a+c)+(b+di)| \leq |a+ib|+|c+id|$ ⇔ (elevando al cuadrado)

   $|(a+c)+(b+di)|^2 \leq (|a+ib|+|c+id|)^2$ ⇔ (desarrollando)

   $(a+c)^2+(b+d)^2 \leq (\sqrt{a^2+b^2} + \sqrt{c^2+d^2})^2$ ⇔

   $(a+c)^2+(b+d)^2 \leq a^2+b^2+2\sqrt{a^2+b^2}\sqrt{c^2+d^2} + c^2+d^2$ ⇔ (desarrollando y simplificando)

   $2ac + 2bd \leq 2\sqrt{a^2+b^2}\sqrt{c^2+d^2}$ ⇔ (entre 2 y elevando al ciuadrado)

   $(ac + bd)^2 \leq (a^2+b^2)(c^2+d^2)$ ⇔ (desarrollando)

   $a^2c^2+2abcd+b^2d^2 \leq a^2c^2+a^2b^2+b^2c^2+b^2d^2$ ⇔ (simplificando)

   $2abcd \leq a^2b^2+b^2c^2$ ⇔ (agrupando)

   $0 \leq a^2b^2-2abcd+b^2c^2$ ⇔

   $0 \leq (ab-cd)^2$ lo que es cierto porque los cuadrados de números reales son ≥0

   así que podemos invertir todos los pasos y llegar a la desigualdad que queríamos.

2. Se sigue de 1, ya que $|\mathbf{z}| = |\mathbf{w}-\mathbf{z}+\mathbf{w}| \leq |\mathbf{w}-\mathbf{z}| + |\mathbf{w}|$ por lo tanto $|\mathbf{z}|-|\mathbf{w}| \leq |\mathbf{w}-\mathbf{z}|$. •

Lema. $|\mathbf{z}\cdot\mathbf{w}|=|\mathbf{z}|\cdot|\mathbf{w}|$ y $arg(\mathbf{z}\cdot\mathbf{w}) = arg(\mathbf{z}) + arg(\mathbf{w})$

Demostración. Si $\mathbf{z} = |\mathbf{z}|(\cos(\varphi) + \operatorname{sen}(\varphi)\,i)$ y $\mathbf{w} = |\mathbf{w}|(\cos(\psi) + \operatorname{sen}(\psi)\,i)$ entonces

$\mathbf{z}\cdot\mathbf{w} = |\mathbf{z}|(\cos(\varphi) + \operatorname{sen}(\varphi)\,i)\cdot|\mathbf{w}|(\cos(\psi) + \operatorname{sen}(\psi)\,i)$

$= |\mathbf{z}|\cdot|\mathbf{w}|\,(\cos^2(\varphi) - \operatorname{sen}^2(\varphi)) + (\cos(\varphi)\operatorname{sen}(\psi) + \operatorname{sen}(\varphi)\cos(\psi))\,i)$

$= |\mathbf{z}|\cdot|\mathbf{w}|\,(\cos(\varphi+\psi) + \operatorname{sen}(\varphi+\psi)\,i)$ *(por las formulas trigonométricas de una suma de ángulos)*

que es la expresión polar para un numero con modulo $|\mathbf{z}|\cdot|\mathbf{w}|$ y argumento $\varphi+\psi$. •

Corolario. $|1/\mathbf{z}|=1/|\mathbf{z}|$ y $arg(1/\mathbf{z}) = -arg(\mathbf{z})$

Demostración. Se sigue del lema anterior ya que $1 = |1| = |\mathbf{z}\cdot1/\mathbf{z}| = |\mathbf{z}|\cdot|1/\mathbf{z}|$

$0 = arg(1) = arg(\mathbf{z}\cdot1/\mathbf{z}) = arg(\mathbf{z}) + arg(1/\mathbf{z})$ •

Problemas.

10. Demuestra *directamente* (sin usar la forma polar) que para cada par de números complejos se cumple $|\mathbf{z}\cdot\mathbf{w}| = |\mathbf{z}|\cdot|\mathbf{w}|$

11. Calcular sin trabajar de mas

a. $|(3+4\mathbf{i})(2+3\mathbf{i})|$ b. $\left|\frac{5-5\mathbf{i}}{7+\mathbf{i}}\right|$ c. $|(1+\mathbf{i})^{10}|$ d. $|\sqrt[2]{2-3\mathbf{i}}\,|$

12. Encuentra un número complejo que tenga la magnitud de $2+3\mathbf{i}$ y el argumento de $4+5\mathbf{i}$.

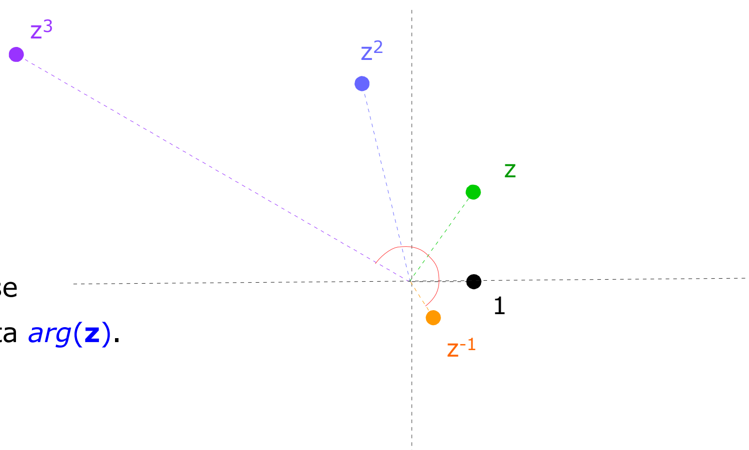
13. ¿En que casos es cierto que $arg(\mathbf{z}+\mathbf{w})$ es el promedio de $arg(\mathbf{z})$ y $arg(\mathbf{w})$?

14. Demuestra que si $\mathbf{z}$ y $1/\mathbf{z}$ están alineados con 0, entonces $\mathbf{z}$ es real o imaginario.

Potencias y raíces

Fórmula de De Moivre. Si $\mathbf{z} = |\mathbf{z}|\,(\cos(\theta) + \operatorname{sen}(\theta)\,\mathbf{i})$ entonces $\mathbf{z}^n = |\mathbf{z}|^n\,(\cos(n\theta) + \operatorname{sen}(n\theta)\,\mathbf{i})$ para cada entero n.

Esta fórmula es una consecuencia inmediata de las fórmulas para el módulo y argumento de un producto cuando n>0, y de la fórmula para el modulo y argumento de los inversos cuando n<0.



Cada vez que multiplicamos por $\mathbf{z}$, el módulo se multiplica por $|\mathbf{z}|$ y el argumento se incrementa $arg(\mathbf{z})$.

Lema. Cada número complejo $\mathbf{z}\neq 0$ tiene n raíces n-esimas.

Demostración. Si $\mathbf{w}$ es una raíz n-esima de $\mathbf{z}$, entonces el módulo de w elevado a la potencia n debe ser el módulo de $\mathbf{z}$ y al argumento de $\mathbf{w}$ multiplicado por n debe ser el argumento de $\mathbf{z}$ mas un múltiplo de 2π. Por lo tanto $|\mathbf{w}|=|\mathbf{z}|^{1/n}$ y $arg(\mathbf{w}) = {}^1/_n\, arg(\mathbf{z})$ para algún valor de $\arg(\mathbf{z})$ *pero* $\mathbf{z}$ *tiene muchos argumentos* que difieren por múltiplos de 2π. Al dividir entre n dan argumentos que corresponden a n números distintos.

Así que si $\mathbf{z} = |\mathbf{z}|\,(\cos(\theta)+ \operatorname{sen}(\theta)\,\mathbf{i})$ las raíces n-esimas de z son los números complejos

$\mathbf{w}_k=|\mathbf{z}|^{1/n}\,(\cos(\frac{\theta+2k\pi}{n}) + \operatorname{sen}(\frac{\theta+2k\pi}{n})\,\mathbf{i})$ para $0\leq k<n$. •

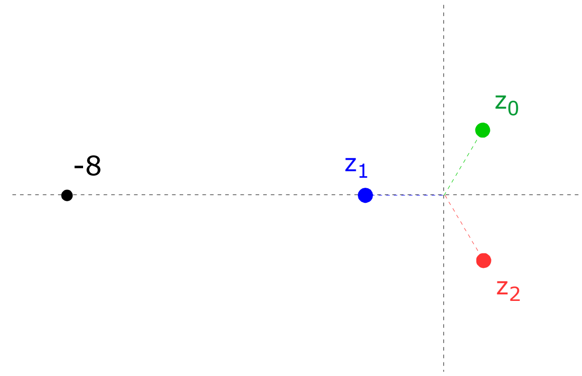
Ejemplo. Como -8 = 8 (cos(π) + sen(π) **i**)

entonces las raíces 3 cubicas de -8 son en forma polar

$w_0 = 8^{1/3}\left(\cos\left(\frac{\pi+0\pi}{3}\right) + \text{sen}\left(\frac{\pi+0\pi}{3}\right)\mathbf{i}\right) = 2\cos\left(\frac{\pi}{3}\right) + 2\text{sen}\left(\frac{\pi}{3}\right)\mathbf{i}$

$w_1 = 8^{1/3}\left(\cos\left(\frac{\pi+2\pi}{3}\right) + \text{sen}\left(\frac{\pi+2\pi}{3}\right)\mathbf{i}\right) = 2\cos\left(\frac{3\pi}{3}\right) + 2\text{sen}\left(\frac{3\pi}{3}\right)\mathbf{i}$

$w_2 = 8^{1/3}\left(\cos\left(\frac{\pi+4\pi}{3}\right) + \text{sen}\left(\frac{\pi+4\pi}{3}\right)\mathbf{i}\right) = 2\cos\left(\frac{5\pi}{3}\right) + 2\text{sen}\left(\frac{5\pi}{3}\right)\mathbf{i}$



Ejemplo. Como 16**i** = 16 cos($\frac{\pi}{2}$) +16 sen($\frac{\pi}{2}$) **i**

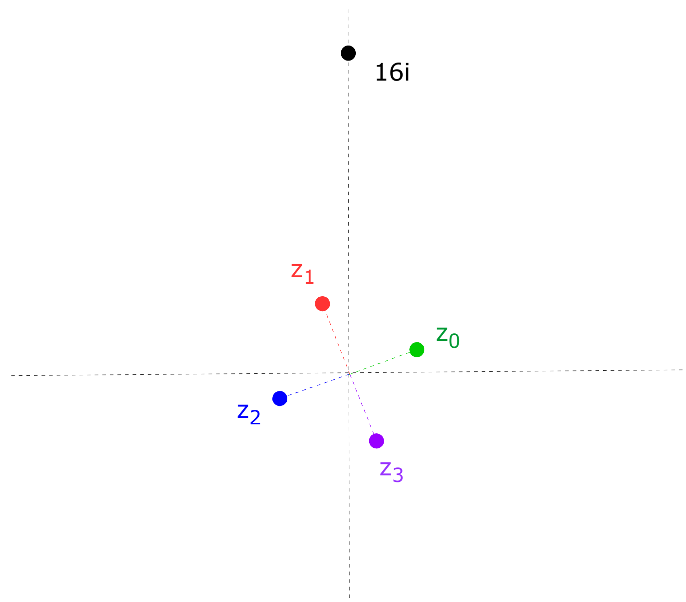
entonces las raíces cuartas de 16i son:

$z_0 = 2\cos\left(\frac{\pi}{8}\right) + 2\text{sen}\left(\frac{\pi}{8}\right)\mathbf{i}$

$z_1 = 2\cos\left(\frac{5\pi}{8}\right) + 2\text{sen}\left(\frac{5\pi}{8}\right)\mathbf{i}$

$z_2 = 2\cos\left(\frac{9\pi}{8}\right) + 2\text{sen}\left(\frac{9\pi}{8}\right)\mathbf{i}$

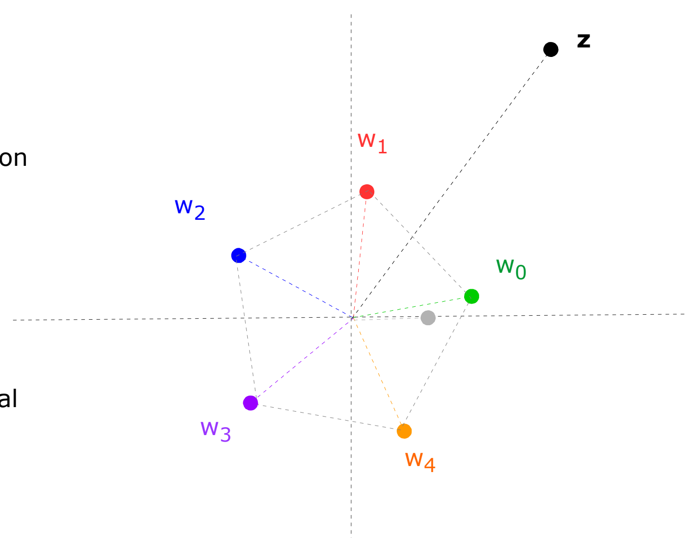
$z_3 = 2\cos\left(\frac{13\pi}{8}\right) + 2\text{sen}\left(\frac{13\pi}{8}\right)\mathbf{i}$



Ejemplo. Las raíces quintas de un complejo **z** son los complejos $\mathbf{w}_i$ situados en los vértices de un pentágono con centro en 0.

Sus módulos son $|\mathbf{z}|^{1/5}$.

El argumento de $\mathbf{w}_0$ es un quinto del argumento de **z**.
Los argumentos de los otros $\mathbf{w}_k$ se obtienen sumándole al argumento anterior un quinto de vuelta, o sea $^{2\pi}/_5$.

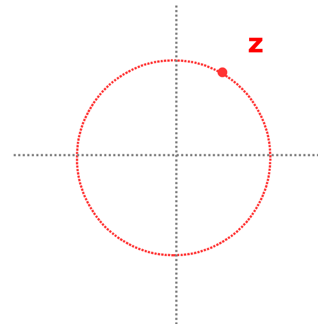


Problemas.

15. Calcula y dibuja cuidadosamente (usando la fórmula de De Moivre).
a. Las raíces cuartas de -1. b. Las raíces cúbicas de $-\mathbf{i}$. c. Las raíces quintas de 1.

16. ¿Por que número complejo hay que multiplicar a las raíces sextas de 1 para obtener las raíces sextas de -1? ¿Y para obtener las raíces sextas de $-\mathbf{i}$?

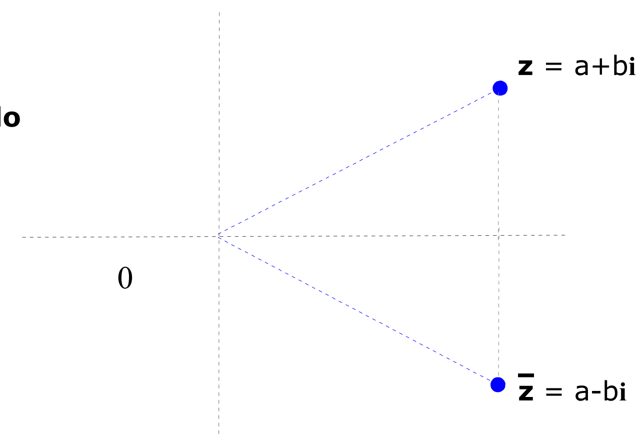
17.* Muestra que si **z** es un complejo unitario, entonces existe una n>0 tal que $\mathbf{z}^n=1$ (y entonces **z** una raíz n-esima de 1) o se pueden hallar potencias de **z** tan cercanas como se quiera a cada punto del círculo (y las potencias de **z** se acumulan en todo el círculo).



Conjugación

En los complejos existe una operación que no existe en los reales, y que se parece a la multiplicación por -1 en que al hacerla dos veces da la identidad.

Si $\mathbf{z} = a+b\mathbf{i}$ es un numero complejo, el **conjugado** de **z** es el numero complejo $\overline{\mathbf{z}} = a-b\mathbf{i}$.



Ejemplos. $\overline{3} = 3$, $\overline{\mathbf{i}} = -\mathbf{i}$, $\overline{2-3\mathbf{i}} = 2+3\mathbf{i}$

Geométricamente, la conjugación corresponde a reflejar en el eje real.

Lema. La conjugación en **C** tiene las siguientes propiedades:

- $\overline{\mathbf{z}+\mathbf{w}} = \overline{\mathbf{z}} + \overline{\mathbf{w}}$
- $\overline{\mathbf{z}\cdot\mathbf{w}} = \overline{\mathbf{z}} \cdot \overline{\mathbf{w}}$
- $\overline{\mathbf{w}/\mathbf{z}} = \overline{\mathbf{w}} / \overline{\mathbf{z}}$ en particular, $\overline{1/\mathbf{z}} = 1 / \overline{\mathbf{z}}$
- $\mathbf{z} \cdot \overline{\mathbf{z}} = |\mathbf{z}|^2$ por lo tanto $1/\mathbf{z} = \overline{\mathbf{z}} /|\mathbf{z}|^2$
- $\overline{\overline{\mathbf{z}}} = \mathbf{z}$
- $\mathrm{Re}(\mathbf{z}) = \dfrac{\mathbf{z}+\overline{\mathbf{z}}}{2}$ $\mathrm{Im}(\mathbf{z}) = \dfrac{\mathbf{z}-\overline{\mathbf{z}}}{2}$

Las operaciones aritméticas reales corresponden a operaciones geométricas en la recta:

- Las sumas dan traslaciones

Ejemplo: $\mathbf{x} \to \mathbf{x}+3$

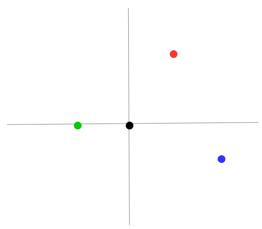
- Los productos dan homotecias.

Ejemplo: $\mathbf{x} \to {}^{3}/_{2}\mathbf{x}$

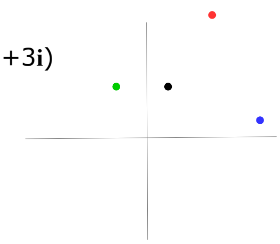
Las operaciones aritméticas complejas corresponden a operaciones geométricas del plano:

- Las sumas dan traslaciones

Ejemplo:

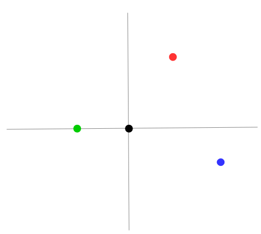


$\mathbf{z} \to \mathbf{z}+(1+3\mathbf{i})$

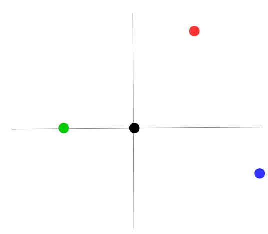


- Los productos por reales dan homotecias (centradas en 0)

Ejemplo:

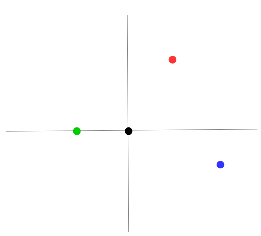


$\mathbf{z} \to {}^{3}/_{2}\,\mathbf{z}$

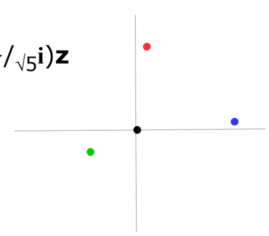


- Los productos por complejos unitarios dan rotaciones (centradas en 0)

Ejemplo:

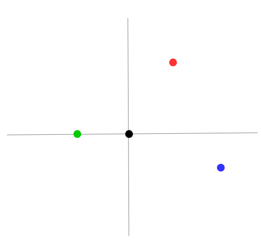


$\mathbf{z} \to ({}^{2}/_{\sqrt{5}}+{}^{1}/_{\sqrt{5}}\mathbf{i})\mathbf{z}$

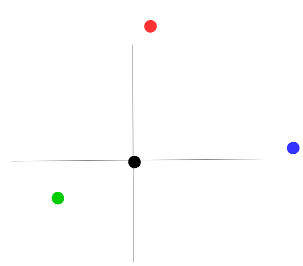


- Los productos por complejos arbitrarios dan homotecias con rotación (centradas en 0)

Ejemplo:

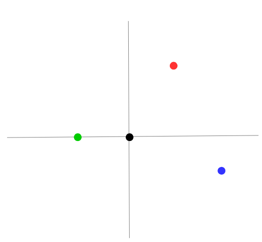


$\mathbf{z} \to (2+\mathbf{i})\mathbf{z}$

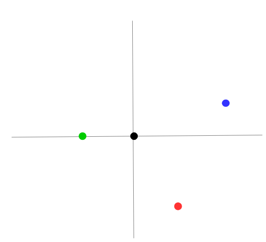


- La conjugación da una reflexión en el eje real

Ejemplo:



$\mathbf{z} \to \overline{\mathbf{z}}$



Combinando las operaciones aritméticas complejas podemos obtener rotaciones con cualquier centro, reflexiones en cualquier recta y homotecias centradas en cualquier punto del plano.

Ejemplos.

Para rotar el plano 90° alrededor de 1 podemos llevar 1 a 0, rotar 90° alrededor de 0 y regresar el 0 a 1, lo que se logra restando 1, multiplicando por $\mathbf{i}$ y sumando 1, es decir con la composición

$$\mathbf{z} \;\to\; \mathbf{z}-1 \;\to\; \mathbf{i}(\mathbf{z}-1) \;\to \mathbf{i}(\mathbf{z}-1)+1 = \;\mathbf{iz}+1-\mathbf{i}$$

Para reflejar en la recta Im$\mathbf{z}$=1 podemos llevarla a la recta Im$\mathbf{z}$=0 (el eje real), reflejar en el eje real y regresar la recta Im$\mathbf{z}$=0 a la recta Im$\mathbf{z}$=1, lo que se logra restando $\mathbf{i}$, conjugando y luego sumando $\mathbf{i}$, es decir por medio de la composición

$$\mathbf{z} \;\to\; \mathbf{z}-\mathbf{i} \;\to\; \overline{\mathbf{z}-\mathbf{i}} \;\to \overline{\mathbf{z}-\mathbf{i}}+\mathbf{i} = \;\overline{\mathbf{z}}+\mathbf{i}+\mathbf{i} = \overline{\mathbf{z}}+2\mathbf{i}$$

Problemas.

18. Si *arg*($\mathbf{z}$)=φ, cuanto valen...

   a. $arg(-\mathbf{z})$ b. $arg(\overline{\mathbf{z}})$ c. $arg(-{}^1/_{\mathbf{z}})$ d. $arg({}^1/_{\overline{\mathbf{z}}})$

19. Demostrar que si un complejo $\mathbf{z}$ es raíz del polinomio $a_n\mathbf{z}^n+a_{n-1}\mathbf{z}^{n-1}+...+a_2\mathbf{z}^2+a_1\mathbf{z}+a_0 = 0$, entonces $\overline{\mathbf{z}}$ es raíz del polinomio con coeficientes conjugados $\overline{a}_n\mathbf{z}^n+\overline{a}_{n-1}\mathbf{z}^{n-1}+...+\overline{a}_2\mathbf{z}^2+\overline{a}_1\mathbf{z}+\overline{a}_0 = 0$.

20. Demostrar que si un complejo $\mathbf{z}$ es raíz de un polinomio real, entonces $\overline{\mathbf{z}}$ también es raíz de ese polinomio. Mostrar que esto falla si el polinomio no es real.

21. ¿Como se expresan las siguientes transformaciones del plano como operaciones algebraicas complejas?

   a. La reflexión del plano en el eje imaginario.

   b. La rotación de 45° con centro en 0

   c. La reflexión del plano en la recta Re($\mathbf{z}$)=Im($\mathbf{z}$)

   d. La rotación de 90° con centro en $\mathbf{i}$

22. ¿Que hacen geométricamente estas operaciones algebraicas?

   a. $\mathbf{z} \to 2\mathbf{z}+3\mathbf{i}$ b. $\mathbf{z} \to 2\mathbf{iz}+3$ c. $\mathbf{z} \to ({}^3/_5-{}^4/_5\mathbf{i})\mathbf{z}$ d. $\mathbf{z} \to (3-4\mathbf{i})\mathbf{z}$

23.* Muestra que todas las operaciones algebráicas complejas preservan la forma de las figuras del plano (aunque pueden cambiar su tamaño y su orientación).

Los enteros gaussianos.

Los **enteros gaussianos** son los complejos de la forma $\mathbf{z} = m+n\mathbf{i}$ con m y n enteros.

Las sumas y productos de enteros gaussianos son enteros gaussianos, y los inversos aditivos de enteros gaussianos también lo son (pero los inversos multiplicativos generalmente no lo son).

Así que los enteros gaussianos forman un anillo **E** con propiedades similares a **Z**.

Lema. Si $\mathbf{u}$ y $\mathbf{v}$ son enteros gaussianos entonces

1. $|\mathbf{u}|^2$ es un entero que es suma de dos cuadrados.
2. $|\mathbf{uv}|^2=|\mathbf{u}|^2|\mathbf{v}|^2$

Demostración.

1. Si $\mathbf{z}=m+n\mathbf{i}$ entonces $|\mathbf{z}|^2=m^2+n^2$ que es la suma de los cuadrados de dos enteros.

2. La norma del producto de dos complejos es el producto de sus normas. •

Si $\mathbf{u}$ y $\mathbf{v}$ son enteros gaussianos, decimos que $\mathbf{u}$ *divide* a $\mathbf{v}$ si existe un entero gaussiano $\mathbf{z}$ tal que $\mathbf{uz}=\mathbf{v}$. Por el lema anterior, si $\mathbf{u}$ divide a $\mathbf{v}$ entonces el entero $|\mathbf{u}|^2$ debe dividir al entero $|\mathbf{v}|^2$.

Ejemplos:

- $2+3\mathbf{i}$ divide a $3-2\mathbf{i}$ ya que $(2+3\mathbf{i})(-\mathbf{i}) = 3-2\mathbf{i}$.
- $1+\mathbf{i}$ divide a 2 ya que $(1+\mathbf{i})(1-\mathbf{i})=2$
- $1+2\mathbf{i}$ no divide a 3 ya que $|1+2\mathbf{i}|^2=5$ y $|3|^2=9$ y 5 no divide a 9.

Diremos que un entero gaussiano $\mathbf{u}$ es una **unidad** si existe un entero gaussiano $\mathbf{v}$ tal que $\mathbf{uv}=1$.

Lema. Las unidades de **E** son los enteros gaussianos de norma 1, que son $1,-1,\mathbf{i},-\mathbf{i}$.

Demostración. Por el lema anterior si el producto de dos enteros gaussianos da 1, el producto de sus normas debe ser 1, así que sus normas deben ser 1. Pero los únicos enteros gaussianos con norma 1 son los números $m+n\mathbf{i}$ con $m^2+n^2=1$ así que m o n debe ser 0 y el otro debe ser 1 o -1, por lo que los únicos enteros gaussianos de norma 1 son $1, -1, \mathbf{i}, -\mathbf{i}$ y es fácil ver que todos estos son unidades. •

Cada entero gaussiano $\mathbf{u}$ es divisible entre las unidades y entre el producto de unidades por $\mathbf{u}$.

Un entero gaussiano $\mathbf{u}$ que no es una unidad es un **primo gaussiano** si la única manera de escribir a $\mathbf{u}$ como producto de dos enteros gaussianos es con alguno de ellos una unidad.

Como la norma del producto es el producto de las normas y las unidades son los enteros de norma 1, un entero gaussiano $\mathbf{u}$ es un primo gaussiano si y solo si $\mathbf{u}$ no es producto de dos enteros gaussianos de norma menor que $\mathbf{u}$.

Ejemplos.

- 2 no es un primo gaussiano, ya que $2=(1+\mathbf{i})(1-\mathbf{i})$.
- $3+2\mathbf{i}$ es primo gaussiano: si $3+2\mathbf{i}$ fuera el producto de dos enteros gaussianos **u** y **v** entonces $|\mathbf{u}|^2|\mathbf{v}|^2 = 13$ por lo que $|\mathbf{u}|^2=1$ y $|\mathbf{v}|^2=13$ o $|\mathbf{u}|^2=13$ y $|\mathbf{v}|^2=1$, asi que **u** o **v** son unidades.
- 3 sí es un primo gaussiano: Si 3 fuera producto de dos enteros gaussianos **u** y **v** entonces se tendría $|\mathbf{u}|^2|\mathbf{v}|^2=|3|^2 = 9$ así que si **u** y **v** no son unidades entonces $|\mathbf{u}|^2=|\mathbf{v}|^2=3$.

  Pero 3 no es suma de dos cuadrados, así que no hay enteros gaussianos con esa norma.
- ¿5 es primo gaussiano? Para verlo busquemos sus posibles factores.

  Si $5=\mathbf{uv}$ entonces $|\mathbf{u}|^2|\mathbf{v}|^2 = |\mathbf{5}|^2 = 25$ y la única posiblilidad si no son unidades es que $|\mathbf{u}|^2=|\mathbf{v}|^2=5$

  Como $5=2^2+1^2$ si hay enteros gaussianos con esa norma: $\pm2\pm i$ o $\pm1\pm2i$

  Si tomamos $\mathbf{u}=2+\mathbf{i}$ y $\mathbf{v}=2-i$ entonces $\mathbf{uv}=(2+\mathbf{i})(2-\mathbf{i})=5$ asi que 5 no es primo gaussiano.

Problemas.

24. ¿Cuales de estos primos son primos gaussianos y cuales no?

    a. 7 b. 11 c. 13 d. 17

25. Demuestra que si **z** es primo gaussiano entonces $-\mathbf{z}$ y $\bar{\mathbf{z}}$ también son primos gaussianos.

26. Escribe a **z** como producto de dos enteros gaussianos que no sean unidades

    a. $\mathbf{z} = -2+9\mathbf{i}$ b. $\mathbf{z} = 11+10\mathbf{i}$

27. Muestra que si **n** es un número natural cuyo cuadrado es la suma de dos cuadrados mas chicos, entonces **n** no es un primo gaussiano.

Lema. Cada entero gaussiano es una unidad o es producto de primos gaussianos.

Demostración. Si un entero gaussiano no es primo, podemos escribirlo como producto de dos enteros gaussianos con normas menores. Si estos son primos ya acabamos y si no entonces podemos escribirlos como producto de enteros gaussianos con normas aun menores, y podemos repetir el procedimiento, que debe acabar en algún momento porque las normas al cuadrado de los enteros gaussianos son enteros positivos, así que sólo podemos hallar otros con normas menores una cantidad finita de veces. •

Ejemplo. Hallar una factorización de $\mathbf{z} = -1+13\mathbf{i}$ como producto de primos gaussianos.

Primero veamos cuales pueden ser las normas de los factores.

Si $\mathbf{z}=\mathbf{uv}$ entonces $|\mathbf{u}|^2|\mathbf{v}|^2 = |\mathbf{z}|^2 = (-1)^2+13^2 = 170$ donde $|\mathbf{u}|^2$ y $|\mathbf{v}|^2$ son enteros mayores que 1 que son sumas de dos cuadrados.

Una posibilidad es $|\mathbf{u}|^2=10$ y $|\mathbf{v}|^2=17$, veamos si funciona:

$|\mathbf{u}|^2=3^2+1^2$ de donde $\mathbf{u}=\pm3\pm\mathbf{i}$ o $\mathbf{u}=\pm1\pm3\mathbf{i}$

$|\mathbf{v}|^2=4^2+1^2$ de donde $\mathbf{v}=\pm4\pm\mathbf{i}$ o $\mathbf{v}=\pm1\pm4\mathbf{i}$

y se puede ver que $(3+\mathbf{i})(1+4\mathbf{i})=-1+13\mathbf{i}$.

Podemos ver que $\mathbf{v}=1+4\mathbf{i}$ es primo ya que $|\mathbf{v}|^2=1^2+4^2=17$ no es producto de enteros mas chicos.

Veamos ahora si $\mathbf{u}=3+\mathbf{i}$ es primo: $|\mathbf{u}|^2=10$, así que podría ser $\mathbf{u}=\mathbf{u}'\mathbf{u}''$ con $|\mathbf{u}'|^2=2$, $|\mathbf{u}''|^2=5$

$|\mathbf{u}'|^2=1^2+1^2$ de donde $\mathbf{u}'=\pm1\pm i$

$|\mathbf{u}''|^2=5=2^2+1^2$ de donde $\mathbf{u}''=\pm2\pm i$ o $\mathbf{u}''=\pm1\pm2i$

y se puede ver que $(1+\mathbf{i})(2-\mathbf{i})=3+\mathbf{i}$.

Ahora $\mathbf{u}'=1+\mathbf{i}$ y $\mathbf{u}''=2-\mathbf{i}$ si son primos ya que $|\mathbf{u}'|^2=2$ y $|\mathbf{u}'|^2=5$ no son productos de enteros positivos mas chicos. Así que una factorización prima que buscamos es $-1+13\mathbf{i}=(1+4\mathbf{i})(1+\mathbf{i})(1+2\mathbf{i})$.

Si la factorización que elegimos de la norma al cuadrado no da una factorización del numero, hay que intentar las otras factorizaciones (en este caso 170=5x34 o 170=2x65).

Vamos a demostrar que la factorización en primos gaussianos es única, salvo por multiplicación por unidades. Para esto necesitamos definir una división entera con residuo.

Algoritmo de la división. Si $\mathbf{u}$ y $\mathbf{v}$ son enteros gaussianos con $\mathbf{u}\neq0$, entonces existen enteros gaussianos $\mathbf{q}$ y $\mathbf{r}$ tales que $\mathbf{v}=\mathbf{qu}+\mathbf{r}$ con $|\mathbf{r}|<|\mathbf{u}|$.

$\mathbf{q}$ es el cociente y $\mathbf{r}$ es el residuo de la división.

Demostración. El cociente $\mathbf{v/u}$ es un numero complejo $\mathbf{z}=a+bi$, donde $\mathbf{a}$ y $\mathbf{b}$ en general no son enteros, pero podemos 'redondearlos' a los enteros mas cercanos m y n, de modo que $-1/2<a-m\le1/2$ y $-1/2<b-n\le1/2$.

Entonces $\mathbf{q}=m+ni$ es un entero gaussiano y $\mathbf{r}=\mathbf{v}-\mathbf{qu}$.

Como $|\mathbf{z}-\mathbf{q}|\le\sqrt{(1/2)^2+(1/2)^2}=\sqrt{1/2}$ entonces $|\mathbf{r}|=|\mathbf{v}-\mathbf{qu}|=|\mathbf{zu}-\mathbf{qu}|=|\mathbf{z}-\mathbf{q}||\mathbf{u}|\le\sqrt{1/2}|\mathbf{u}|<|\mathbf{u}|$.

Ejemplo. Si $\mathbf{u}=1+2\mathbf{i}$ y $\mathbf{v}=5+3\mathbf{i}$ entonces como complejos $\mathbf{z}=\mathbf{v/u}=(5+3\mathbf{i})(1+2\mathbf{i})^{-1}=(5+3\mathbf{i})(1/5-2/5\,\mathbf{i})=11/5-7/5\,\mathbf{i}$

y el cociente es el entero gaussiano 'redondeado' $\mathbf{q}=10/5-5/5\,\mathbf{i}=2-\mathbf{i}$

Ahora $\mathbf{qu}=(2-\mathbf{i})(1+2\mathbf{i})=4+3\mathbf{i}$ y el residuo es $\mathbf{r}=\mathbf{v}-\mathbf{qu}=1$.

Geométricamente la división anterior puede verse como sigue:

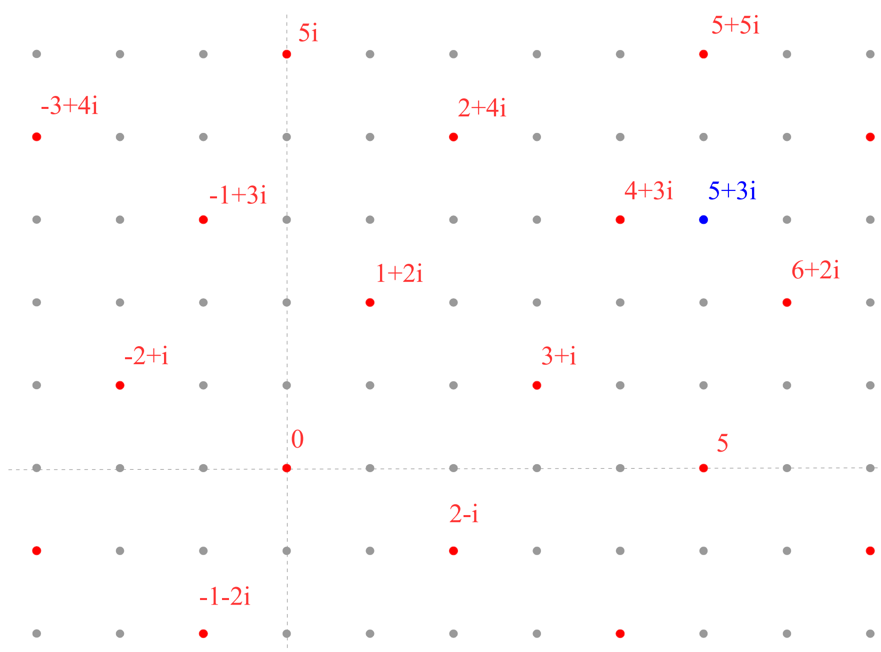
Los enteros gaussianos están en gris.

Los múltiplos de $1+2\mathbf{i}$ están en rojo, y forman una cuadrícula.

El múltiplo de $1+2\mathbf{i}$ mas cercano a $5+3\mathbf{i}$ es $4+\mathbf{i}\mathbf{i}=(2-\mathbf{i})(1+2\mathbf{i})$

Así que el cociente es $2-\mathbf{i}$.

El residuo es la diferencia entre $5+3\mathbf{i}$ y $4+3\mathbf{i}$, que es 1.



Ejemplo. Dividir a $\mathbf{v}=4+5\mathbf{i}$ entre $\mathbf{u}=2+\mathbf{i}$ como enteros gaussianos.

Como números complejos $\mathbf{v/u} = (4+5\mathbf{i})(2+\mathbf{i})^{-1} = (4+5\mathbf{i})(^2/_5-{}^1/_5\mathbf{i}) = {}^{13}/_5+{}^6/_5\,\mathbf{i}$

El cociente de la división entera es el entero gaussiano mas cercano, que es $\mathbf{d} = 3+\mathbf{i}$

$\mathbf{du} = (3+\mathbf{i})(2+\mathbf{i}) = 5+5\mathbf{i}$ de donde $\mathbf{v}-\mathbf{du} = -1$ así que el residuo es $\mathbf{r} = -1$.

Problemas.

27. Calcula el cociente y el residuo de dividir **v** entre **u** como enteros gaussianos

    a. $\mathbf{v}=7-6\mathbf{i}$ entre $\mathbf{u}=3+2\mathbf{i}$ b. $\mathbf{v}=7+8\mathbf{i}$ entre $\mathbf{u}=4-\mathbf{i}$

28. Factoriza a los siguientes enteros gaussianos como productos de primos gaussianos

    a. $3+4\mathbf{i}$ b. $-4+7\mathbf{i}$ c. 10

Observar que si **u**,**v**,**w** son enteros gaussianos tales que $\mathbf{u}|\mathbf{v}$ y $\mathbf{u}|\mathbf{w}$ entonces $\mathbf{u}|\mathbf{av}+\mathbf{bw}$ para cada par de enteros gaussianos **a** y **b**.

Lema. Si **u** y **v** son enteros gaussianos, entonces existe una combinación lineal entera $\mathbf{au}+\mathbf{bv}$ (con **a** y **b** enteros gaussianos) que divide a ambos.

Demostración. Sea **w** una combinación lineal entera de **u** y **v** con norma (distinta de 0) mínima

Si **w** no dividiera a **u**, entonces $\mathbf{u}=\mathbf{dw}+\mathbf{r}$ con $0<|\mathbf{r}|<|\mathbf{w}|$

Pero **r** es una combinación lineal entera de **u** y **v** ya que $\mathbf{r} = \mathbf{u}-\mathbf{dw} = \mathbf{u}-\mathbf{d}(\mathbf{au}+\mathbf{bv}) = (1-\mathbf{da})\mathbf{u}+(-1)\mathbf{v}$

y esto contradice la suposición de que **w** era la combinación lineal entera de norma mínima. •

Corolario. Si **u** y **v** son enteros gaussianos distintos de 0, entonces existe un entero gaussiano **w** que divide a ambos, y que es divisible entre todos los divisores comunes de **u** y **v**.
Este numero es el **máximo común divisor** de **u** y **v**.

Demostración. Si **w** es la combinación lineal entera de norma mínima de **u** y **v** entonces por el lema anterior **w** divide a **u** y **v**. Y cualquier divisor común de **u** y **v** divide a las combinaciones lineales enteras de **u** y **v**, en particular a **w**. •

Observar que el máximo común divisor de **u** y **v** esta bien definido salvo unidades.

Lema. Si un primo gaussiano divide a un producto entonces divide a uno de los factores.

Demostración. Supongamos que el primo gaussiano **z** divide a **uv** y que **z** no divide a **u**.

Entonces el máximo común divisor de **z** y **u** debe ser una unidad, ya que los únicos divisores de **z** son unidades y productos de **z** por unidades, y si uno de estos dividiera a **u** entonces **z** dividiría a **u**.

Como el mdd de **z** y **u** es 1, por el lema anterior existe una combinación lineal entera $\mathbf{az}+\mathbf{bu}=1$.

Multiplicando por **v** obtenemos $\mathbf{azu}+\mathbf{buv}=\mathbf{v}$.

Como **z** divide a **z** y también a **uv** entonces divide a $\mathbf{azu}+\mathbf{buv}=\mathbf{v}$. •

Teorema. La factorización de cada entero gaussiano como producto primos gaussianos es única salvo multiplicación por unidades.

Demostración. Tomemos dos factorizaciones primas de $\mathbf{z}$, $\mathbf{z}=p_1p_2p_3...p_m=q_1q_2q_3...q_n$.

Como p_1 divide a $\mathbf{z}=q_1q_2...q_n$ entonces por el lema anterior p_1 debe dividir a algún q_i, digamos a q_1.

Como p_1 divide a q_1 que es primo entonces $q_1=u_1p_1$ para alguna unidad u_1.

Podemos dividir a $\mathbf{z}$ entre p_1 y obtener el entero $\mathbf{z}/p_1 = p_2...p_m=u_1q_2...q_n$

Ahora p_2 divide a $\mathbf{z}/p_1 =q_2...q_n$ así que debe dividir a algún q_i, digamos a q_2.

Como p_2 divide a q_2 que es primo entonces $q_2=u_2p_2$ para alguna unidad u_2.

Podemos dividir a $\mathbf{z}/p_1$ entre p_1 y obtener el entero $\mathbf{z}/p_1p_2 = p_3.....q_n$

Y podemos seguir dividiendo hasta que del lado izquierdo no quede ningún p_i, de modo que queda 1 y del lado derecho no puede quedar ningún q_j (porque el producto es 1) y solo pueden quedar unidades. •

Ejemplo. Ya vimos que -1+13i tiene factorización prima -1+13i = (1+2i)(1-i)(1+4i).

Podemos hallar otras factorizaciones primas multiplicando los factores primos por unidades cuyo producto sea 1. Por ejemplo, multiplicandolos por i, -1 y i obtenemos -1+13i = (-2+i)(-1+i)(-4+i).

Problemas.

29. Calcula el máximo común divisor de **u** y **v**

a. **u**=1+3i **v**=4+2i b. **u**=11+10i **v**=3+11i

30. Muestra que el mcd de cualquier entero gaussiano y su conjugado es real (salvo unidades).

31. (2+i)(1-3i) = 5-5i = 5(1-i) ¿Por que no contradice esto al teorema de factorización única?

32. Las ternas pitagóricas son ternas de números naturales **a**, **b**, **c** tales que $\mathbf{a}^2+\mathbf{b}^2=\mathbf{c}^2$, por ejemplo 3,4,5 y 5,12,13.

a. Cada cuadrado gaussiano produce una terna pitagórica ¿pueden adivinar como?

b. ¿Que terna pitagórica produce $(1+4i)^2$? ¿Y $(2+5i)^2$?

c. ¿De que cuadrado gaussiano viene 3,4,5? ¿y 5,12,13?