ALGEBRA I - Práctica N°5 - Verano de 2007

Números complejos

Ejercicio 1. En cada uno de los siguientes casos hallar $\mathrm{Re}(z)$, $\mathrm{Im}(z)$, $|z|$, $\mathrm{Re}(z^{-1})$ e $\mathrm{Im}(z^{-1})$:

i) $z = (1+2i) + i.(2+i)$ ii) $z = (1-i)^2 + 1$
iii) $z = \left[(\sqrt{2}-i).(\sqrt{2}+i)\right]^4$ iv) $z = (1+3i)^{-1}.(1+i)$
v) $z = (1+i).\overline{(2+i)}$

Ejercicio 2. Expresar en forma binomial los complejos:

i) $i^{43} - i^{38}$
ii) $\dfrac{i^{86}}{i^{165}}$
iii) $(i+1)^{213}$
iv) $(-3+3i)^{228}$

Ejercicio 3. Dados $z = 1+2i$ y $w = 2+3i$, representar gráficamente en el plano los siguientes números complejos:

$$z, \qquad w, \qquad z+w, \qquad z-w, \qquad \overline{z}, \qquad -w, \qquad 4.z, \qquad |z|$$

Ejercicio 4. Graficar los siguientes conjuntos en el plano complejo:

i) $\{z \in \mathbb{C} \ / \ \mathrm{Re}(z) = |z|\}$
ii) $\{z \in \mathbb{C} \ / \ |z| = 2\}$
iii) $\{z \in \mathbb{C} \ / \ 2z - \overline{z} = i.z\}$
iv) $\{z \in \mathbb{C} \ / \ 1 \leq |z-3+i| < 4\}$
v) $\{z \in \mathbb{C} \ / \ z.\mathrm{Re}(z) = |z|^2\}$
vi) $\{z \in \mathbb{C} \ / \ |z| = 2 \ \text{ y } \ \mathrm{Re}(z) \geq 1\}$

Ejercicio 5. Demostrar las siguientes afirmaciones:

i) $\overline{\overline{z}} = z \qquad \forall\, z \in \mathbb{C}$
ii) $\overline{z+w} = \overline{z} + \overline{w} \qquad \forall\, z, w \in \mathbb{C}$
iii) $\overline{z.w} = \overline{z}.\overline{w} \qquad \forall\, z, w \in \mathbb{C}$
iv) $z \in \mathbb{R} \iff z = \overline{z}$

v) $\overline{z^{-1}} = (\overline{z})^{-1} \qquad \forall\ z\ \in\ \mathbb{C} - \{0\}$

vi) $z.\overline{z} = |z|^2 \qquad \forall\ z\ \in\ \mathbb{C}$

vii) $|z.w| = |z|.|w| \qquad \forall\ z, w\ \in \mathbb{C}$

viii) $|z| = 0 \iff z = 0$

ix) $|z^{-1}| = |z|^{-1} \qquad \forall\ z\ \in\ \mathbb{C} - \{0\}$

x) $|\mathrm{Re}(z)| \leq |z| \qquad \forall\ z\ \in\ \mathbb{C}$. ¿Cuándo vale la igualdad?

xi) $|\mathrm{Im}(z)| \leq |z| \qquad \forall\ z\ \in\ \mathbb{C}$. ¿Cuándo vale la igualdad?

Ejercicio 6. Resolver en $\mathbb{C}$ las siguientes ecuaciones:

i) $x^2 = 1 + i$

ii) $x^2 = 2 + 3i$

iii) $x^2 + 2x + 2 = 0$

iv) $x^2 + (1 + 2i)x + 1 - 5i = 0$

Ejercicio 7. Determinar todos los complejos z que satisfacen:

i) $z^{-1} = \overline{z}$

ii) $z^2\ \in\ \mathbb{R}$

iii) $z + z^{-1}\ \in\ \mathbb{R}$

iv) $\mathrm{Re}(z).z = \mathrm{Im}(z).z$

v) $z^2 + 2 = \mathrm{Re}(z).z$

vi) $|z - i| = |z + 2|$

vii) $z^2 + |z|^2 = i.\overline{z}$

Ejercicio 8. Calcular los módulos y los argumentos de los siguientes complejos:

i) $\sqrt{3} + i$

ii) $(1 - i)(1 + i\sqrt{3})$

iii) $(\sqrt{3} - i)^{-1}$

iv) $\cos x + i \operatorname{sen} x,\ -\pi \leq x \leq \pi$

v) $\cos\frac{17}{5}\pi - i\ \operatorname{sen}\frac{17}{5}\pi$

vi) $-3(i \operatorname{sen}\frac{19}{5}\pi - \cos\frac{11}{5}\pi)$

Ejercicio 9. Graficar en el plano complejo los siguientes conjuntos:

i) $\{z \in \mathbb{C} \,/\, 2 \leq |z| < 3 \text{ y } \frac{\pi}{2} < \arg(z) < \frac{2\pi}{3}\}$

ii) $\{z \in \mathbb{C} \,/\, \arg(z^4) < \pi\}$

iii) $\{z \in \mathbb{C} \,/\, \frac{\pi}{4} < \arg(i.z) < \frac{2\pi}{3}\}$

iv) $\{z \in \mathbb{C} \,/\, z^6 \in \mathbb{R} \text{ y } |z| \geq 1\}$

Ejercicio 10. Expresar en forma binomial los siguientes complejos:

i) $(-\sqrt{3} - i)^9$

ii) $(2 + 2i)^{18}$

iii) $\left(\dfrac{\sqrt{3} - i}{-2 + 2i}\right)^{15}$

Ejercicio 11.

i) Hallar todos los $n \in \mathbb{N}$ tales que $(1 + i\sqrt{3})^n \in \mathbb{R}$

ii) Hallar todos los $n \in \mathbb{N}$ tales que $(1 + i\sqrt{3})^n = (\sqrt{2} + i\sqrt{2})^n$

iii) Hallar todos los $n \in \mathbb{N}$ tales que $\arg((1 + i)^n) = \frac{3}{4}\pi$ y $\arg((1 - i\sqrt{3})^{2n}) = \frac{4}{3}\pi$

Ejercicio 12. Calcular las raíces n-ésimas de z en los siguientes casos:

i) $n = 3$, $z = i$

ii) $n = 5$, $z = 2$

iii) $n = 5$, $z = -\sqrt{2} + i\sqrt{6}$

iv) $n = 8$, $z = \dfrac{1 + i}{\sqrt{3} - i}$

Ejercicio 13. Determinar todos los complejos z que satisfacen:

i) $z^3 = \overline{z}^{\,3}$

ii) $(z + 1)^4 = z^4$

iii) $z^3 = (2 + i2\sqrt{3})^9$

iv) $z^n + i\overline{z} = 0, \;\; n \in \mathbb{N}$

v) $z^6 + z^3 + 1 = 0$

vi) $(z + i)^2 = (1 + z)^4$

Ejercicio 14.

i) Hallar los vértices del hexágono regular con centro en $(0, 0)$ y uno de cuyos vértices es el $(1, 1)$

ii) Hallar los vértices del hexágono regular con centro en $(1, 2)$ y uno de cuyos vértices es el $(3, 5)$

Ejercicio 15. Se define para cada $n \in \mathbb{N}$ el conjunto de raíces n-ésimas de la unidad:

$$G_n = \{w \in \mathbb{C} \ / \ w^n = 1\}$$

G_n tiene exactamente n elementos:

$$w_k = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\frac{2k\pi}{n}, \quad 0 \leq k \leq n-1$$

i) Probar que si $w, w' \in G_n$, entonces $w.w', w^{-1} \in G_n$

(Dado que $1 \in G_n$, esto indica que G_n con el producto ordinario de números complejos es un grupo abeliano)

ii) Probar que si $w \in G_n$ entonces $w^{-1} = \overline{w}$ (y, por lo tanto, $\overline{w} \in G_n$)

iii) ¿Es cierto que si $w \in G_n$, entonces $-w \in G_n$?

iv) Probar que si $m, n \in \mathbb{N}$, entonces $G_n \cap G_m = G_{(m\,:\,n)}$

Deducir que $G_n \subset G_m \iff n \mid m$

v) Se dice que $w \in G_n$ es una *raíz n-ésima primitiva de* 1 si todo elemento $u \in G_n$ se puede escribir en la forma $u = w^k$ para algún $k \in \mathbb{N} \cup \{0\}$

Determinar las raíces primitivas para $n = 2$, 3, 4, 5 y 6.

vii) Probar que dado $n \in \mathbb{N}$ existe siempre por lo menos una raíz n-ésima primitiva en G_n

viii) Probar que w_k es raíz n-ésima primitiva de 1 si y sólo si $(n : k) = 1$

ix) Sea $w \in G_n, w \neq 1$. Probar que $1 + w + w^2 + ... + w^{n-1} = 0$. Deducir que la suma de todas las raíces n-ésimas de 1 es igual a 0.

x) Probar que el producto de todas las raíces n-ésimas de 1 es $(-1)^{n+1}$.

Ejercicio 16.

i) Si $w^3 = 1$, calcular $w^{100} + w^{35} - 7w^3 - 3$

ii) Si $w^3 = 1$, calcular $w + \dfrac{1}{w}$

iii) Si $w^5 = 1$, calcular $w^{24} + \overline{w^2 + w^{24}} + w^7$

iv) Si $w^7 = 1$, probar que $i(w^{24} + 1)(w^{32} - 1)$ es un número real.

v) Sea $w \in G_{2n}$, $n \in \mathbb{N}$. Probar que $w + w^n + w^{-1}$ es un número real.

Ejercicio 17.

i) Sea $z \in G_5$ una raíz quinta primitiva de 1. Hallar todos los $n \in \mathbb{N}$ tales que

$$\sum_{i=2}^{n} z^i = 0$$

ii) Sea $w \in G_8$ una raíz octava primitiva de 1. Hallar todos los $n \in \mathbb{N}$ tales que

$$\sum_{i=1}^{n-1} z^{2i} = 0$$

Ejercicio 18. Sea $w \in G_3$ una raíz cúbica primitiva de 1 y sea $(z_n)_{n\in\mathbb{N}}$ la sucesión de números complejos definida por

$$\begin{cases} z_1 = w^2 \\ z_{n+1} = (1 + \overline{z_n})^2 \quad \forall\, n \in \mathbb{N} \end{cases}$$

Probar que, $\forall\, n \in \mathbb{N}$, z_n es una raíz cúbica primitiva de 1.

Aplicación de los números complejos a la aritmética entera

Introducción

Si nuestras aspiraciones fueran tan modestas como para estar interesados únicamente en los números naturales, de todos modos nos convendría estudiar los números enteros aunque más no fuera para restar con comodidad. Y si accediéramos a estudiar los enteros, difícilmente podríamos ignorar los racionales, aunque más no fuera para dividir con comodidad. Así, una cosa trae la otra y cuando uno tiene que estudiar los números complejos puede estar tentado a creer que eso no tiene nada de *real*. No es así, lo que hay de concreto o de abstracto en la matemática está presente desde el principio, desde la noción misma de número. Los complejos no son menos reales que los reales ni éstos que los racionales o los enteros. En este apunte quiero que veamos en qué puede ayudar el estudio de los números "complejos" para entender un poco más a los "naturales".

No todos los primos son iguales

Además del hecho de que 2 es el único primo par, no todos los primos son iguales. Tomemos un primo impar p. Si pensamos en su desarrollo binario, vemos que éste debe terminar en 1 ya que si terminara en 0, sería par. Por lo tanto, las últimas dos cifras de p pueden ser 01 o 11. Tenemos entonces dos clases de primos: los que (en binario) terminan en 01 y los que terminan 11. Por ejemplo, en 01 teminan $5, 13, 17, 29, \ldots$, y en 11 terminan $3, 7, 11, 19, \ldots$.

En general, las n últimas cifras binarias de un número entero corresponden al resto de la división entera de ese número por 2^n (¿por qué?). Gracias a esto, las divisiones enteras por potencias de 2 son inmediatas en una computadora binaria. En nuestro caso los primos que terminan en 01 son los que tienen resto 1 en su división por 4 y los que terminan en 11 son los que tienen resto 3. Exceptuando al 2, no puede haber primos que tengan resto 0 o resto 2 en su división por 4.

Ahora revisemos nuestra lista de primos del primer grupo. Cada uno de ellos se puede expresar como una suma de dos cuadrados:

$$5 = 2^2 + 1^2$$
$$13 = 3^2 + 2^2$$
$$17 = 4^2 + 1^2$$
$$29 = 5^2 + 2^2$$

Ahora recorramos la lista de los primos que terminan en 11. Vemos que ninguno de ellos, ni 3, ni 7, ni 11, ni 19 pueden ser escritos como suma de dos cuadrados. Por ejemplo, $19 - 1^2 = 18$, $19 - 2^2 = 15$, $19 - 3^2 = 10$ y $19 - 4^2 = 3$ y ni 18, ni 15, ni 10, ni 3 son cuadrados en $\mathbb{Z}$.

La pregunta es ¿habrá alguna relación entre estos dos hechos?, es decir, será pura casualidad que a los primos del grupo 01 que miramos los hayamos podido escribir como suma de dos cuadrados y a los otros no?

Demos vuelta al asunto a ver si podemos entender un poco más. Si un primo impar p es suma de cuadrados ¿será cierto que pertenece al grupo 01? Veamos. Supongamos que $p = a^2 + b^2$ y examinemos los restos de p módulo 4. En principio a puede tener cualquier resto: 0, 1, 2 o 3; pero al elevar al cuadrado solamente quedan dos posibilidades 0 y 1. Lo mismo ocurre para b. Por lo tanto en binario a^2 y b^2 terminan en 00 o en 01. Pero no pueden terminar los dos en 00 ni los dos en 01 porque en ese caso su suma p sería par (y era impar). Esto significa que, por ejemplo, a^2 termina en 01 y b^2 en 00. Así tenemos probado que p termina en 01. Bien!

Ahora sabemos que los primos que son sumas de dos cuadrados terminan en 01. Por eso 3, 7, 11 y 19 no podrían ser suma de dos cuadrados. El asunto parece aclarado. O no?

Mmm... bueno, en realidad lo que está claro es que los primos que terminan en 11 no pueden ser suma de dos cuadrados; pero por qué vamos a poder escribir como suma de dos cuadrados a los primos que terminan en 01. Los otros no se pueden escribir, pero sabemos que estos sí? Por ejemplo, cómo sería un algoritmo que encuentre la suma? Mejor paremos acá hasta que el asunto madure un poco.*

Wilson y los otros primos

Los primos que terminan en 01 son los que tienen resto 1 en su división por 4. Eso significa que son de la forma $4k + 1$. Si $p = 4k + 1$, entonces $(p - 1)/2$ es par.

Ahora, $(p - 1)/2$ es la mitad de los números que hay en la lista

$$1,\ 2,\ \ldots,\ \frac{p-1}{2},\ \frac{p-1}{2} + 1,\ \ldots,\ p - 1$$

Cada uno de los números entre 1 y $(p-1)/2$ tiene su inverso aditivo en $\mathbb{Z}_p$ simétricamente dispuesto entre los números que van de $(p-1)/2+1$ a $p-1$. Por ejemplo, el inverso aditivo

* Piense en todo esto y no pase a la próxima sección hasta haber comprendido bien el problema.

de 1 en $\mathbb{Z}_p$ es $p-1$, el de 2 es $p-2$, ..., el de $(p-1)/2$ es $(p-1)/2+1$. Con esto en mente podemos reescribir la lista así:

$$1,\ 2,\ \ldots,\ \frac{p-1}{2},\ -\frac{p-1}{2},\ \ldots,\ -2,\ -1$$

Multipliquemos entre sí los números de la primera mitad de la lista. Quedándonos con el resto módulo p de ese producto obtenemos un entero $\alpha < p$. Si hacemos lo mismo con los números de la segunda mitad, vamos a obtener el mismo resultado α porque ahora estaríamos multiplicando los inversos aditivos de los números de la primera mitad, lo que no importa porque la cantidad de signos menos va a ser par ($(p-1)/2$ era par).

Resumiendo, para los primos p que terminan en 01, encontramos un número $\alpha < p$ que verifica:

$$1 \times 2 \times \cdots \times (p-1) = \alpha^2 \pmod{p}$$

Por ejemplo, para $p = 13$, el producto $1 \times 2 \times 3 \times 4 \times 5 \times 6$ es congruente a 5 módulo p; así que en este caso $\alpha = 5$. Si revisamos nuestra lista de primos de tipo 01 una cuenta similar muestra que, módulo p, tenemos:

p	α	α^2
5	2	4
13	5	12
17	13	16
29	12	28

Mirando la tercera columna de esta tabla vemos un patrón de comportamiento: en todos los casos α^2 es congurente a -1 módulo p (glup!).

Claro, éste es precisamente el teorema de Wilson. Este teorema dice que $(p-1)!$ es congruente a -1 módulo p. El teorema de Wilson no es difícil de demostrar. Cada número entre 2 y $p-2$ tiene en $\mathbb{Z}_p$ un inverso multiplicativo que está en esa misma lista. Los únicos números que son inversos multiplicativos de sí mismos son 1 y $p-1$ (pruebe esto el lector). Por lo tanto al efectuar el producto, todos se van excepto 1 y $p-1$; eso termina la demostración.

Volviendo a lo nuestro, hemos encontrado un α que verifica $\alpha^2 = -1 \pmod{p}$; o lo que es lo mismo, $p \mid \alpha^2 + 1$. Y esto ya se parece más a lo que estamos buscando.

El asunto es que $p \mid \alpha^2 + 1$. ¿Y si fuera $p = \alpha^2 + 1$? Bueno, en ese caso nuestro problema estaría resuelto.

De acuerdo, pero no tenemos que engañarnos. En la tabla de arriba, la tercera columna está reducida módulo p. Repasémosla. Para $p = 5$, α es 2 y $2^2 + 1 = 5$. Pero para $p = 13$,

α es 5 y desafortunadamente $5^2 + 1 = 26$. O sea, $p \mid \alpha^2 + 1$ pero en general no va a ser igual. Hemos avanzado otro poco, pero todavía falta.*

Gauss, el hombre que factorizaba primos

Los irreducibles son aquellos que no se pueden factorizar como producto de dos números, a menos que uno de los factores sea inversible y el otro un asociado. Recordemos que a es *asociado* a b cuando $a = ub$ para u inversible.

Por ejemplo, 2 es irreducible porque no se puede escribir como $n.m$ a menos que uno de estos dos números n o m sea 1 o -1 y el otro 2 o -2. Sin embargo, si agrandamos el conjunto de enteros agregándole $\sqrt{2}$, entonces vamos a poder "factorizar" 2 como $\sqrt{2} \cdot \sqrt{2}$. El conjunto de todas las expresiones de la forma $n + m\sqrt{2}$, con n y m en $\mathbb{Z}$, es un subconjunto de $\mathbb{R}$ cerrado para sumas y productos.

Ejercicio 1. Demuestre que la suma y el producto de expresiones de la forma $n + m\sqrt{2}$ con $n, m \in \mathbb{Z}$ vuelven a dar expresiones del mismo tipo.

Este conjunto se llama $\mathbb{Z}[\sqrt{2}]$, es un anillo que contiene a $\mathbb{Z}$ como subanillo, solamente que en $\mathbb{Z}[\sqrt{2}]$, el número 2 no es irreducible. Podríamos pensar que en $\mathbb{Z}$ no hay "suficientes" elementos como para factorizar a 2, pero en $\mathbb{Z}[\sqrt{2}]$, sí los hay.

Al agregar estos nuevos elementos a $\mathbb{Z}$ ocurre que otros primos dejan de ser irreducibles; por ejemplo, también $7 = (3 - \sqrt{2})(3 + \sqrt{2})$ se puede factorizar en $\mathbb{Z}[\sqrt{2}]$.

Volviendo al problema que estábamos tratando, lo que queremos entender es qué tienen de especial los primos que pueden escribirse como suma de dos cuadrados. Supongamos que tenemos un primo p que admite una escritura de ese tipo:

$$p = a^2 + b^2$$

En ese caso ni a ni b pueden ser divisibles por p (demuestre). Al tomar restos módulo p, queda

$$a^2 + b^2 = 0 \pmod{p}$$

y multiplicando por el inverso multiplicativo de b^2 en $\mathbb{Z}_p$, obtenemos:

$$(ab^{-1})^2 + 1 = 0 \qquad \text{en } \mathbb{Z}_p$$

Este es otro punto de contacto entre los primos que en binario terminan con 01 y los primos que son suma de dos cuadrados (vea la sección anterior). En ambos casos, existe un elemento α en $\mathbb{Z}_p$ tal que su cuadrado es -1.

* Pare, medite el material de esta sección.

Tal vez fue este hecho el que indujo a Gauss a decir, si $p = a^2 + b^2$, entonces $p = (a - bi)(a + bi)$ y por lo tanto p se puede factorizar usando números complejos!

Se trata de una construcción análoga a la anterior, solamente que en lugar de agregar $\sqrt{2}$ a $\mathbb{Z}$ ahora hemos agregado el número complejo i. Al subconjunto de $\mathbb{C}$ formado por todas las expresiones de la forma $a + bi$ con $a, b \in \mathbb{Z}$, lo vamos a denotar $\mathbb{Z}[i]$.

Recíprocamente, si p se puede factorizar usando números complejos no inversibles, o sea $p = (a + bi)(c + di)$ para ciertos enteros a, b, c y d, entonces tomando la norma al cuadrado y utilizando que la norma es una función multiplicativa obtenemos:

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

Pero ahora volvimos a $\mathbb{Z}$ y ahí, p es irreducible. Eso significa que o bien cada una de los dos factores es igual a p, o bien uno de ellos es 1 y el otro es p^2.

La segunda posibilidad solamente ocurre cuando una suma de cuadrados es 1. Pero si por ejemplo, $a^2 + b^2 = 1$, entonces $a + bi$ es inversible (su inversa es su conjugado $a - bi$); de modo que la pretendida factorización de p contenía un elemento inversible, en contra de nuestra suposición.

Siendo imposible la segunda alternativa, debe ocurrir que cada uno de los dos factores sea igual a p, pero eso implica que p es una suma de cuadrados.

Para fijar las ideas, dejemos constancia de lo que hemos demostrado: *un entero primo es suma de dos cuadrados si, y solamente si, se puede factorizar en* $\mathbb{Z}[i]$.

Combinando este resultado con el de la sección anterior vemos que si p es un primo que termina en 01, entonces existe un entero α tal que $p \mid \alpha^2 + 1$, o sea $p \mid (\alpha - i)(\alpha + i)$.

Usando esto estamos a un paso de probar que p debe ser reducible en $\mathbb{Z}[i]$. Así habremos probado que p es suma de dos cuadrados.*

Primos e irreducibles

Recordemos que un elemento es *irreducible* si no es ni cero ni inversible y no se puede escribir como producto de dos factores a menos que uno de esos factores sea inversible y el otro asociado.

Un elemento es *primo* si no es ni cero ni inversible y solamente divide a un producto de dos factores cuando divide a alguno de esos factores.

En símbolos, p es irreducible si verifica: $p = ab \Rightarrow a$ es inversible y $p \sim b$ (es asociado a) o viceversa. En cambio, p es primo si: $p \mid ab \Rightarrow p \mid a$ o bien $p \mid b$.

* Relea esta sección antes de pasar a la siguiente.

Ejercicio 2. Pruebe que primo implica irreducible.

Todo elemento primo es un elemento irreducible (ejercicio anterior), sin embargo no siempre vale la recíproca. Por ejemplo en $\mathbb{Z}[\sqrt{-5}]$ el número 2 es irreducible (ejercicio) sin embargo no es primo. En efecto, en $\mathbb{Z}[\sqrt{-5}]$ vale que $2.3 = (1-\sqrt{-5})(1+\sqrt{-5})$ y sin embargo 2 no divide ni a $(1-\sqrt{-5})$ ni a $(1+\sqrt{-5})$ (ejercicio).

Estas nociones valen en $\mathbb{Z}$ y en $k[x]$ pero también en otros anillos. En la próxima sección vamos a aplicarlas a $\mathbb{Z}[i]$. Vamos a ver que, como en el caso de los enteros y los polinomios, en $\mathbb{Z}[i]$ irreducible implica primo.

Los enteros de Gauss

En una sección anterior introdujimos el siguiente conjunto:

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

llamado de *enteros de Gauss*. Este conjunto es un subanillo de $\mathbb{C}$ dado que la suma y el producto de complejos con partes real e imaginaria enteras da como resultado otro complejo con partes real e imaginaria enteras.

En $\mathbb{Z}[i]$ existe un algoritmo de división, con teorema de existencia y unicidad de cociente y resto. Ese algoritmo de división da como resultado un algoritmo de Euclides totalmente análogo al algoritmo de Euclides para enteros o polinomios.

El algoritmo de Euclides permite escribir al máximo divisor común de dos enteros de Gauss como combinación lineal de ellos. Esto es análogo a lo que ocurre en $\mathbb{Z}$ o en $k[x]$. Con ese teorema es fácil ver que los elementos irreducibles de $\mathbb{Z}[i]$ son en realidad primos. Empecemos por el principio.

Teorema. *Dados $a+bi$ y $c+di$ en $\mathbb{Z}[i]$ con $c+di \neq 0$, existe un único par de enteros de Gauss $u+vi$ y $r+si$ que verifican*:

a) $a + bi = (c + di)(u + vi) + (r + si)$
b) $|r + si| < |c + di|$

Demostración de la existencia. Definamos el número complejo $u' + v'i = (a + bi)(c - di)/(c^2 + d^2)$. Las partes real e imaginaria u' y v' son números racionales. Llamemos u al entero más cercano a u' y v al entero más cercano a v'. Eso significa que $|u - u'| \leq 1/2$ y $|v - v'| \leq 1/2$. Tomando la norma en $\mathbb{C}$ resulta:

$$|(u' + v'i) - (u + vi)| = \sqrt{(u' - u)^2 + (v' - v)^2} \leq \sqrt{1/2} < 1.$$

Reemplazando por la definición de $u' + v'i$ y multiplicando por $|c + di|$ obtenemos:

$$|(a + bi) - (c + di)(u + vi)| < |c + di|.$$

Ahora podemos llamar $r + si$ a la diferencia $(a + bi) - (c + di)(u + vi)$ y esto termina la demostración de la existencia.

Demostración de la unicidad. Queda como ejercicio para el lector.

El *máximo divisor común* de dos enteros de Gauss es el entero de Gauss con norma compleja máxima que divide a los enteros dados.

Ejercicio 3. Enuncie y demuestre el algoritmo de Euclides para el anillo de enteros de Gauss.

Ejercicio 4. Demuestre que el máximo divisor común de dos enteros de Gauss es combinación lineal de los enteros dados. (Sugerencia: imite la demostración que se da en el caso de $\mathbb{Z}$ o de $k[x]$).

Ejercicio 5. Demuestre que en $\mathbb{Z}[i]$ todo irreducible es primo. (Sugerencia: imite la demostración que se da en el caso de $\mathbb{Z}$ o de $k[x]$).

El fin de la historia

Ahora podemos juntar todo lo que hemos visto. Si un primo termina en binario en 01, entonces hay un entero $\alpha < p$ tal que $p \mid \alpha^2 + 1$. Pasando a $\mathbb{Z}[i]$ esto significa que $p \mid (\alpha - i)(\alpha + i)$.

Lo que queremos probar es que p es una suma de dos cuadrados. Según vimos en una sección anterior, eso equivale a probar que p no es irreducible en $\mathbb{Z}[i]$. Como en $\mathbb{Z}[i]$ irreducible implica primo, si p fuera irreducible debería ocurrir que $p \mid (\alpha - i)$ o bien $p \mid (\alpha + i)$. Sin embargo ninguna de estas cosas es posible. Por ejemplo, si p dividiera a $\alpha + i$ tendríamos:

$$\alpha + i = p(a + bi) = pa + pbi.$$

Comparando las partes imaginarias eso implicaría que $1 = pb$, lo que es imposible.

Ejercicio 6. Demuestre que si p es un primo entero de la forma $4k + 1$, entonces $p = (a + bi)(a - bi)$ con $(a + bi)$ y $(a - bi)$ irreducibles en $\mathbb{Z}[i]$.

(*) Ejercicio 7. Escriba un algoritmo que tome como entradas enteros primos p y, en el caso de tratarse de números de la forma $4k+1$, entregue como resultado un par de enteros a y b tales que $a^2 + b^2 = p$. (Para resolver este ejercicio usted va a necesitar división con cociente y resto y algoritmo de Euclides para enteros de Gauss).