Índice

1. Definiciones y resultados básicos

Definición 1.1. Sea A un dominio de integridad. Una *función euclídea* es una función $\phi : A - \{0\} \to \mathbb{Z}^+$ que verifica

1. Para cualesquiera $a, b \in A$ con $ab \neq 0$ se tiene $\phi(ab) \geq \phi(a)$.
2. Para cualesquiera $a, b \in A$ con $b \neq 0$ existen $q, r \in A$ tales que $a = bq + r$ y o bien $\phi(r) < \phi(b)$ o bien $r = 0$.

Un dominio de integridad que tenga una función euclídea se llama *dominio euclídeo*.

Ejemplo 1.2. El anillo $\mathbb{Z}$ de los enteros es un dominio euclídeo tomando la función $\phi(n) = |n|$.

Generalmente para verificar que un anillo es euclídeo es más conveniente reemplazar la segunda condición por otra:

Lema 1.3. *La segunda condición de la definición de función euclídea es equivalente a la siguiente: Para cualesquiera $a, b \in A$ si $\phi(a) \geq \phi(b)$ existe un $c \in A$ tal que $\phi(a - bc) < \phi(a)$ o $a = bc$.*

Ejemplo 1.4. Sea K un cuerpo arbitrario. El anillo de polinomios $K[X]$ es un anillo euclídeo para la función $\phi(f) = gr(f)$.

La siguiente propiedad es la que hace muy fácil trabajar con los anillos euclídeos:

Teorema 1.5. *Todo anillo euclídeo es un dominio de ideales principales.*

Demostración. Sea A un dominio euclídeo y sea I un ideal de A. Si $I \neq 0$ existe un $a \in I$, $a \neq 0$, con $\phi(a)$ mínimo. Entonces $(a) \subset I$.

Supongamos que $(a) \subsetneq I$. Sea $b \in I$, $b \notin (a)$. Dividimos $b = qa + r$. Ahora $r = b - qa \in I$, $r \neq 0$ y $\phi(r) < \phi(a)$ en contradicción con la elección de a. Luego $(a) = I$. □

Corolario 1.6 (Teorema de Bézout). *En un anillo euclídeo A dos elementos cualesquiera $a, b \in A$ tienen un máximo común divisor d y existen $u, v \in A$ tales que*

$$d = au + bv$$

Demostración alternativa (Algoritmo extendido de Euclides): Sea $\phi(a) \geq \phi(b)$ y aplicamos repetidamente la propiedad 1.3. Tras un número finito de pasos tenemos un resto cero:

$$\begin{aligned}
a &= bq_1 + r_1 && \phi(r_1) < \phi(b) \\
b &= r_1 q_2 + r_2 && \phi(r_2) < \phi(r_1) \\
&\dots && \dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && \phi(r_n) < \phi(r_{n-1}) \\
r_{n-1} &= r_n q_n && r_{n+1} = 0
\end{aligned}$$

porque $\phi(b) > \phi(r_1) > \dots$ es una sucesión estrictamente decreciente de números no negativos que debe pararse y esto sólo puede ocurrir cuando un resto es cero.

De la primera ecuación vemos que r_1 es de la forma $ax + by$ con $x, y \in A$. Por inducción lo mismo se verifica para todo r_i: Sean

$$\begin{aligned}
r_{i-2} &= ax' + by' \\
r_{i-1} &= ax + by
\end{aligned}$$

Entonces $r_i = -r_{i-1} q_i + r_{i-2} = a(x' - xq_i) + b(y' - yq_i)$. En particular

$$r_n = au + bv \tag{1.1}$$

Además r_n divide a r_n y a r_{n-1}, luego divide a r_{n-2}. Por inducción obtenemos que r_n divide a y b. Pero de la expresión 1.1 cualquier divisor de a y b también divide a r_n. Luego $d = r_n = \text{m. c. d.}(a, b)$ □

Corolario 1.7. *En un anillo euclídeo dos elementos cualesquiera tienen un mínimo común múltiplo.*

Corolario 1.8. *En un dominio euclídeo todo irreducible es primo.*

Corolario 1.9. *Todo dominio euclídeo es un dominio de factorización única.*

Corolario 1.10. *Para cualquier cuerpo K el anillo de polinomios $K[X]$ es un dominio de factorización única.*

2. Ejemplos: Anillos cuadráticos

2.1. Cuerpos cuadráticos de números

Sea D un número racional que no es un cuadrado perfecto en $\mathbb{Q}$. Definimos el subconjunto de $\mathbb{C}$

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Está claro que este subconjunto es cerrado para la resta y la identidad

$$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D})$$

muestra que también es cerrado para la multiplicación. Por tanto $\mathbb{Q}[\sqrt{D}]$ es un subanillo de $\mathbb{C}$ (e incluso de $\mathbb{R}$ cuando $D > 0$), así que en particular es un anillo conmutativo. Es fácil comprobar que la hipótesis de que D no es un cuadrado implica que todo elemento de $\mathbb{Q}[\sqrt{D}]$ se escribe de manera única como $a + b\sqrt{D}$. También implica que si a, b no son ambos cero, entonces $a^2 - b^2D \neq 0$ y como $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$ tenemos que

$$(a + b\sqrt{D})^{-1} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

Esto demuestra que todo elemento no nulo de $\mathbb{Q}[\sqrt{D}]$ tiene un inverso en $\mathbb{Q}[\sqrt{D}]$ y por tanto $\mathbb{Q}[\sqrt{D}]$ es un cuerpo, que se llama *cuerpo cuadrático*.

El número racional D puede expresarse como $D = f^2D'$ para algún $f \in \mathbb{Q}$ y un único $D' \in \mathbb{Z}$ que no sea divisible por el cuadrado de ningún entero mayor que 1, es decir que o bien $D' = -1$ o bien $D' = \pm p_1 \dots p_t$ donde los p_i son primos distintos de $\mathbb{Z}$. (Por ejemplo, $8/5 = (2/5)^2 \cdot 10$). Al entero D' le llamamos *parte libre de cuadrados de* D. Entonces $\sqrt{D} = f\sqrt{D'}$ y por tanto $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$. Luego *no se pierde generalidad si se supone que D es un entero libre de cuadrados en la definición del cuerpo cuadrático* $\mathbb{Q}[\sqrt{D}]$.

La aplicación $N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ definida por $N(a + b\sqrt{D}) = (a + b\sqrt{D})\sigma(a + b\sqrt{D}) = a^2 - b^2D$ (σ es el conjugado) se llama *norma del cuerpo* $\mathbb{Q}[\sqrt{D}]$ (Por ejemplo, si $D < 0$ la norma $N(z)$ es sencillamente el cuadrado del módulo del número complejo z). La aplicación norma verifica las siguientes propiedades:

1. $N(uv) = N(u)N(v)$ para cualesquiera $u, v \in \mathbb{Q}[\sqrt{D}]$.
2. $N(u) = 0$ si y sólo si $u = 0$.

2.2. Anillos cuadráticos de enteros

Sea D un entero libre de cuadrados. Es inmediato que el conjunto

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$$

es cerrado para la resta y el producto y contiene al número 1, luego es un subanillo del cuerpo cuadrático $\mathbb{Q}[\sqrt{D}]$.

En el caso en que $D \equiv 1 \pmod 4$, el conjunto ligeramente mayor

$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{c + b\frac{1+\sqrt{D}}{2} \mid c, b \in \mathbb{Z}\right\}$$
$$= \left\{\frac{a + b\sqrt{D}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}$$

también es un subanillo: Es inmediato que es cerrado para la resta y el 1 y el cálculo

$$(c + b\frac{1+\sqrt{D}}{2})(c_1 + b_1\frac{1+\sqrt{D}}{2}) = (cc_1 + bb_1\frac{D-1}{4}) + (cb_1 + c_1b + bb_1)\frac{1+\sqrt{D}}{2}$$

muestra que es cerrado para la multiplicación, ya que $(D-1)/4 \in \mathbb{Z}$.

Para unificar los dos casos, llamamos

$$\omega = \begin{cases} \sqrt{D} & \text{si } D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

y definimos

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

El anillo $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$ se llama *anillo de enteros del cuerpo cuadrático* $\mathbb{Q}[\sqrt{D}]$. La terminología proviene de que los elementos de $\mathcal{O}$ tienen muchas propiedades respecto a $\mathbb{Q}[\sqrt{D}]$ que son análogas a las de los enteros de $\mathbb{Z}$ respecto al cuerpo $\mathbb{Q}$ (En cursos posteriores se verá que $\mathcal{O}$ es la *clausura entera* de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{D}]$). La más sencilla de estas propiedades es la siguiente.

Lema 2.1. *El cuerpo* $\mathbb{Q}[\sqrt{D}]$ *es el cuerpo de fracciones del dominio de integridad* $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$.

En el caso particular $D = -1$ obtenemos el anillo $\mathbb{J} = \mathbb{Z}[i]$ de los *enteros de Gauss*, que son los números complejos $a + bi \in \mathbb{C}$ con a y b enteros. Estos números fueron estudiados primero por Gauss alrededor del año 1800 para demostrar la *ley de reciprocidad bicuadrática*, que trata de las relaciones que existen entre las cuartas potencias módulo primos.

En los anillos $\mathcal{O}$ se utiliza la norma para caracterizar las unidades.

Lema 2.2. *Un elemento $x = a + b\omega \in \mathcal{O}$ es invertible en $\mathcal{O}$ si y sólo si $N(x) = \pm 1$.*

Ejemplo 2.3. Cuando $D = -1$, las unidades del anillo de enteros de Gauss son cuatro: $\pm 1, \pm i$ (que son las *raíces cuartas de la unidad*).

Cuando $D = -3$, las unidades del anillo $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ son los $a + b\omega$ tales que $a^2 + ab + b^2 = 1$, es decir los seis elementos $\pm 1, (\pm 1 \pm \sqrt{-3})/2$, que son las *raíces sextas de la unidad*.

Para cualquier otro $D < 0$, $D \neq -1, -3$, las unidades del anillo $\mathcal{O}$ son $1, -1$.

Cuando $D > 0$, se puede demostrar que el grupo de las unidades $\mathcal{O}^\times$ es siempre infinito. Por ejemplo, cuando $D = 2$ el grupo de las unidades es $\mathcal{O}^\times = \{\pm(1 + \sqrt{2})^k \mid k \in \mathbb{Z}\}$.

También utilizamos la norma para buscar irreducibles y primos en $\mathcal{O}$.

Lema 2.4 (Condición suficiente de irreducibilidad). *Sea $u = a + b\sqrt{D}$ tal que $N(u) = \pm p$, con p primo en $\mathbb{Z}$. Entonces u es irreducible.*

Demostración. Sea $u = vw$. Entonces $N(v)N(w) = N(u) = \pm p$, así que o bien $N(v) = \pm 1$ (en cuyo caso v es invertible) o bien $N(w) = \pm 1$ (en cuyo caso w es invertible). □

Lema 2.5 (Condición necesaria de primalidad). *Sea $u = a + b\sqrt{D}$ primo en $\mathcal{O}$. Entonces $N(u) = \pm p$ o $\pm p^2$ con p primo en $\mathbb{Z}$.*

Si u es primo en $\mathcal{O}$, u es asociado con p si y sólo si $N(u) = \pm p^2$.

Demostración. Sabemos que $N(u) = u\sigma(u)$, así que u divide al entero racional $N(u)$. Descomponemos en primos en $\mathbb{Z}$: $N(u) = p_1 \dots p_t$. Por ser u primo debe dividir a uno de los factores $p = p_i$. Luego el entero racional $N(u)$ divide a $N(p) = p^2$. Como $N(u) \neq \pm 1$, sólo quedan las posibilidades del enunciado.

Sea $p = uv$. Se verifica que $p^2 = N(p) = N(u)N(v)$, así que v es invertible si y sólo si $N(u) = \pm p^2$. □

Corolario 2.6. *Sea $D < 0$, $D \neq -1, -3$. Si $u = a + b\omega$ es primo y $b \neq 0$, necesariamente $N(u) = p$ es un primo en $\mathbb{Z}$.*

Teorema 2.7. *Sea D un entero libre de cuadrados tal que $\mathcal{O}$ es un dominio de factorización única. Un elemento $u \in \mathcal{O}$ es primo si y sólo si es de uno de los siguientes tipos:*

- *$u = \epsilon p$ con ϵ invertible y $p \in \mathbb{Z}$ irreducible en $\mathcal{O}$.*
- *$u = a + b\omega$ con $N(u) = \pm p$ y p primo en $\mathbb{Z}$.*

Podemos enunciar explícitamente los primos de un anillo cuadrático euclídeo.

Teorema 2.8. *Sea D un entero libre de cuadrados tal que $\mathcal{O}$ es un dominio de factorización única.*

1. *Todo primo u de $\mathcal{O}$ divide a un único primo p de $\mathbb{Z}$.*

2. *Sea p un primo de $\mathbb{Z}$ tal que $p \nmid 2D$.*

   a) *$p = uv$ es el producto de dos primos no asociados de $\mathcal{O}$ si y sólo si existe un $a \in \mathbb{Z}$ tal que $a^2 \equiv D \pmod{p}$.*

   b) *p es primo en $\mathcal{O}$ si y sólo si para todo $a \in \mathbb{Z}$ se verifica $a^2 \not\equiv D \pmod{p}$.*

3. a) *Sea $D \equiv 1 \pmod{8}$. Entonces $2 = uv$ es el producto de dos primos no asociados de $\mathcal{O}$.*

   b) *Sea $D \equiv 5 \pmod{8}$. Entonces 2 es primo en $\mathcal{O}$*

   c) *Sea $D \equiv 2, 3 \pmod{4}$. Entonces $2 = \epsilon u^2$ es asociado al cuadrado de un primo de $\mathcal{O}$.*

4. *Sea $p \mid D$. Entonces $p = \epsilon u^2$ es asociado al cuadrado de un primo de $\mathcal{O}$.*

Corolario 2.9. *Sea $\mathbb{J} = \mathbb{Z}[i]$ el anillo de los enteros de Gauss y sea $p \in \mathbb{Z}$ un primo.*

1. *$p = (a + bi)(a - bi)$ es el producto de dos primos de $\mathbb{J}$ no asociados si y sólo si $p \equiv 1 \pmod{4}$.*

2. *p es primo en $\mathbb{J}$ si y sólo si $p \equiv 3 \pmod{4}$.*

3. *El elemento $1 + i$ es primo en $\mathbb{J}$ y $2 = -i(1 + i)^2$.*

4. *Todo primo de $\mathbb{J}$ es de uno de los tipos anteriores.*

2.3. Anillos cuadráticos euclídeos

Los anillos $\mathcal{O}$ no son todos euclídeos, ni siquiera son dominios de factorización única. Pero vamos a ver que algunos de ellos son euclídeos respecto a la función $\phi : \mathcal{O} \to \mathbb{Z}$ definida por $\phi(u) = |N(u)|$ (valor absoluto de la norma).

En primer lugar, para cualquier par de elementos $u, v \in \mathcal{O}$ siempre se verifica que $\phi(uv) = \phi(u)\phi(v) \geq \phi(u)$ que es la primera condición de la definición de dominio euclídeo.

La segunda condición de dicha definición dice:

Para $u, v \in \mathcal{O}$ con $v \neq 0$ existen $q, r \in \mathcal{O}$ tales que $u = vq + r$ y o bien $\phi(r) < \phi(v)$ o bien $r = 0$.

Dividiendo por v y teniendo en cuenta que $\mathbb{Q}[\sqrt{D}]$ es el cuerpo de fracciones de $\mathcal{O}$, esta condición se traduce en:

Para todo $x \in \mathbb{Q}[\sqrt{D}]$ existe $q \in \mathcal{O}$ tal que o bien $|N(x - q)| < 1$ o bien $x = q$.

Con esta condición podemos demostrar:

Proposición 2.10. *Sea $D = -2, -1$ o 2. Entonces $\mathcal{O}$ es euclídeo respecto a la función ϕ.*

Demostración. Nótese que los tres valores del enunciado son exactamente los D libres de cuadrados con $|D| < 3$.

Sea $x = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Elegimos $q_1, q_2 \in \mathbb{Z}$ tales que $|a - q_1| \leq 1/2$ y $|b - q_2| \leq 1/2$ y llamamos $q = q_1 + q_2\sqrt{D}$. Entonces

$$\phi(x-q) = |N(x-q)| = |(a-q_1)^2 - (b-q_2)^2 D| \leq (a-q_1)^2 + (b-q_2)^2|D| < 1/4 + (1/4)\cdot 3 = 1,$$

y por tanto $\mathbb{Z}[\sqrt{D}]$ es euclídeo.

Obsérvese que una vez conocido el cociente de dos elementos $u, v \in \mathcal{O}$, el resto se obtiene como $r = u - vq$. □

Proposición 2.11. *Sea $D = -11, -7, -3$ o 5. Entonces $\mathcal{O}$ es euclídeo respecto a la función ϕ.*

Demostración. Los valores del enunciado son exactamente los D libres de cuadrados con $D \equiv 1 \pmod 4$ y $|D| < 12$.

Sea $x = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Elegimos $2q_1, 2q_2 \in \mathbb{Z}$ tales que $|b - q_2| \leq 1/4$, $2q_1 \equiv 2q_2 \pmod 2$ y $|a - q_1| \leq 1/2$ y llamamos $q = q_1 + q_2\sqrt{D}$. Entonces

$$\phi(x-q) = |N(x-q)| = |(a-q_1)^2 - (b-q_2)^2 D| \leq (a-q_1)^2 + (b-q_2)^2|D| < 1/4 + (1/16)\cdot 12 = 1,$$

y por tanto $\mathbb{Q}[\sqrt{D}]$ es euclídeo.

Como antes, una vez conocido el cociente de dos elementos $u, v \in \mathcal{O}$, el resto se obtiene como $r = u - vq$. □

Existen más anillos cuadráticos euclídeos. En concreto la lista completa es la siguiente.

Teorema 2.12. *El anillo $\mathcal{O}$ es euclídeo respecto a la función ϕ anterior si y sólo si D es uno de los valores*

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

Esta lista no agota todos los anillos cuadráticos euclídeos, porque la función respecto a la que $\mathcal{O}$ es euclídeo no tiene porqué ser el valor absoluto de la norma. Se demuestra que para $D < 0$ el anillo $\mathcal{O}$ es euclídeo respecto a alguna función ϕ si y sólo si $D = -11, -7, -3, -2, -1$, pero es una conjetura que el conjunto de valores $D > 0$ para los que $\mathcal{O}$ es euclídeo es infinito. Por ejemplo para $D < 100$ el anillo $\mathcal{O}$, además de para los valores citados en el teorema anterior, también es euclídeo respecto a alguna función ϕ para los valores

$$D = 14, 22, 23, 31, 35, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97$$

Naturalmente para estos valores la función ϕ no es el valor absoluto de la norma.

3. Aritmética en dominios euclídeos

Los métodos y resultados que hemos estudiado para $\mathbb{Z}$ que se basan en el algoritmo de la división con resto se trasladan *mutatis mutande* a los anillos cuadráticos. En esta sección vamos a ver ejemplos de estos métodos en anillos cuadráticos euclídeos.

3.1. Factorización en primos

Ejemplo 3.1. Vamos a obtener la descomposición en primos de $u = 11 + 7i \in \mathbb{Z}[i]$:

En primer lugar calculamos y factorizamos en $\mathbb{Z}$ la norma de u:

$$N(u) = 11^2 + 7^2 = 121 + 49 = 170 = 2 \cdot 5 \cdot 17.$$

Por el corolario 2.9, el elemento u descompone como producto de un primo de norma 2, otro de norma 5 y un tercero de norma 17. Para cada uno de los valores 5 y 17 existen exactamente dos primos con dicha norma, y sólo hay un primo con norma 2. En total hay que probar como máximo cinco divisores. Empezamos sobre seguro, calculando el cociente de u por el único primo (salvo asociados) de norma 2:

$$\frac{11+7i}{1+i} = \frac{(11+7i)(1-i)}{(1+i)(1-i)} = \frac{11-11i+7i+7}{2} = 9-2i$$

así que $u = (1+i)(9-2i)$. Probamos a dividir el cociente $9-2i$ por uno de los primos de norma 5:

$$\frac{9-2i}{2+i} = \frac{(9-2i)(2-i)}{(2+i)(2-i)} = \frac{18-9i-4i-2}{5} = \frac{16-11i}{5}$$

que no pertenece a $\mathbb{Z}[i]$. Luego $(2+i) \nmid (9-2i)$.

Probamos ahora con el otro primo de norma 5:

$$\frac{9-2i}{2-i} = \frac{(9-2i)(2+i)}{(2-i)(2+i)} = \frac{18+9i-4i+2}{5} = \frac{20+5i}{5} = 4+i.$$

Este cociente pertenece a $\mathbb{Z}[i]$ y además es un primo de norma 17. Tenemos que $9-2i = (2-i)(4+i)$, luego la descomposición en primos del elemento dado es

$$11+7i = (1+i)(2-i)(4+i).$$

Ejemplo 3.2. Sea ahora $u = 4 + 7\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Su norma vale $N(u) = 4^2 - 7^2 2 = 16 - 98 = -2 \cdot 41$, luego el elemento u descompone como producto de un elemento de norma 2 y otro de norma 41, $u = \sqrt{2}(7 + 2\sqrt{2})$.

Ejemplo 3.3. Sea $u = 4 - 5\sqrt{-3} \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Calculamos la norma: $N(u) = 4^2 + 5^2 3 = 16 + 75 = 91 = 7 \cdot 13$.

En $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ existen dos primos de norma 7 (que se obtienen resolviendo la ecuación $a^2 + 3b^2 = 7$), a saber $2 + \sqrt{-3}$ y $2 - \sqrt{-3}$. Probamos a dividir por el primero:

$$\frac{4 - 5\sqrt{-3}}{2 + \sqrt{-3}} = \frac{(4 - 5\sqrt{-3})(2 - \sqrt{-3})}{(2 + \sqrt{-3})(2 - \sqrt{-3})} = \frac{8 - 4\sqrt{-3} - 10\sqrt{-3} - 15}{7}$$

$$= \frac{-7 - 14\sqrt{-3}}{7} = -1 - 2\sqrt{-3},$$

así que la factorización en primos es

$$4 - 5\sqrt{-3} = (2 + \sqrt{-3})(-1 - 2\sqrt{-3}).$$

3.2. Cálculo del máximo común divisor

Igual que en $\mathbb{Z}$, en cualquier anillo euclídeo tenemos dos métodos para calcular el máximo común divisor: Uno es factorizar en primos cada elemento dado y formar "el producto de los factores comunes elevados al menor exponente".

Ejemplo 3.4. Sean $a = 1 + 3i$, $b = 3 + 4i$ dos elementos de $\mathbb{Z}[i]$. Buscamos sus respectivas factorizaciones en primos:

$$N(a) = 1^2 + 3^2 = 10 = 2 \cdot 5, \qquad \frac{1 + 3i}{1 + i} = \frac{(1 + 3i)(1 - i)}{(1 + i)(1 - i)} = 2 + i,$$

$$N(b) = 3^2 + 4^2 = 25 = 5^2, \qquad \frac{3 + 4i}{2 + i} = \frac{(3 + 4i)(2 - i)}{(2 + i)(2 - i)} = 2 + i,$$

así que $a = (1 + i)(2 + i)$, $b = (2 + i)^2$, m. c. d.$(a, b) = 2 + i$ y m. c. m.$(a, b) = (1 + i)(2 + i)^2 = -1 + 7i$.

El otro método es aplicar el algoritmo de Euclides (simple o extendido). El máximo común divisor será el último resto no nulo.

Ejemplo 3.5. Sean $a = 11 + 7i$, $b = 3 + 7i$ dos elementos de $\mathbb{Z}[i]$. Calculamos

$$\frac{11 + 7i}{3 + 7i} = \frac{(11 + 7i)(3 - 7i)}{(3 + 7i)(3 - 7i)} = \frac{82}{58} - \frac{56}{58}i$$

así que tomamos el cociente $q_1 = 1 - i$ y el resto $r_1 = a - bq_1 = 1 + 3i$. Dividimos ahora b por r_1:

$$\frac{3 + 7i}{1 + 3i} = \frac{(3 + 7i)(1 - 3i)}{(1 + 3i)(1 - 3i)} = \frac{24}{10} - \frac{2}{10}i.$$

El nuevo cociente será $q_2 = 2$ y el resto $r_2 = b - r_1 q_2 = 1 + i$. El siguiente paso es dividir r_1 por r_2:

$$\frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = 2 + i.$$

con lo que $q_3 = 2 + i$ y $r_3 = 0$. Luego m. c. d.$(a, b) = 1 + i$ (el último resto no nulo).

Para obtener los coeficientes de Bézout utilizamos el algoritmo extendido de Euclides:

q		u	v
	$11+7i$	1	0
	$3+7i$	0	1
$1-i$	$1+3i$	1	$-1+i$
2	$1+i$	-2	$3-2i$
$2+i$	0		

así que $(11 + 7i)(-2) + (3 + i)(3 - 2i) = 1 + i$.

Ejemplo 3.6. Vamos a calcular ahora el máximo común divisor de $a = (5 + \sqrt{-11})/2$ y $b = 2 + \sqrt{-11}$ en el anillo $A = \mathbb{Z}[(1 + \sqrt{-11})/2]$. Como $N(a) = (5^2 + 11)/4 = 9$ y $N(b) = 2^2 + 11 = 15$, empezamos dividiendo b entre a:

$$\frac{2+\sqrt{-11}}{(5+\sqrt{-11})/2} = \frac{2(2+\sqrt{-11})(5-\sqrt{-11})}{(5+\sqrt{-11})(5-\sqrt{-11})} = \frac{2(21+3\sqrt{-11})}{36} = \frac{7+\sqrt{-11}}{6},$$

así que el cociente es $q = 1$ y el resto $r = b - aq = (-1 + \sqrt{-11})/2$. Dividimos ahora a entre r:

$$\frac{(5+\sqrt{-11})/2}{(-1+\sqrt{-11})/2} = \frac{(5+\sqrt{-11})(-1-\sqrt{-11})}{(-1+\sqrt{-11})(-1-\sqrt{-11})} = \frac{6-6\sqrt{-11}}{12} = \frac{1-\sqrt{-11}}{2}$$

que pertenece a $\mathbb{Z}[(1 + \sqrt{-11})/2]$, así que $q_1 = (1 - \sqrt{-11})/2$ y $r_1 = 0$. Vamos a calcular los coeficientes de Bézout:

q		u	v
	$2+\sqrt{-11}$	1	0
	$\frac{5+\sqrt{-11}}{2}$	0	1
1	$\frac{-1+\sqrt{-11}}{2}$	1	-1
$\frac{1-\sqrt{-11}}{2}$	0		

luego m. c. d.$(a, b) = \frac{-1+\sqrt{-11}}{2} = b \cdot 1 + a \cdot (-1)$,

3.3. Resolución de ecuaciones lineales

En nuestra exposición de $\mathbb{Z}$ vimos cómo utilizar el algoritmo extendido de Euclides para resolver ecuaciones diofánticas lineales en dos incógnitas. Exactamente el mismo método se aplica para resolver ecuaciones lineales en anillos euclídeos. En concreto tenemos el siguiente teorema:

Sea A un anillo euclídeo y sean $a, b, c \in A$. Consideramos la ecuación

$$ax + by = c. \tag{3.1}$$

Teorema 3.7. *1. La ecuación 3.1 tiene solución si y sólo si* $\text{m. c. d.}(a, b) \mid c$.

2. Una solución particular de 3.1 se obtiene por el algoritmo extendido de Euclides.

3. Sea $d = \text{m. c. d.}(a, b)$ *y sea* (x_0, y_0) *una solución particular de 3.1. La solución general* (x, y) *viene dada por*

$$x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}$$

con $k \in A$ *arbitrario.*

Demostración. La demostración es idéntica a la realizada en el caso $A = \mathbb{Z}$, que se basaba sólo en la existencia del algoritmo de división con resto. □

Ejemplo 3.8. Consideramos la ecuación siguiente en $\mathbb{Z}[i]$:

$$4x + (3 + 3i)y = -1 + 5i.$$

Para discutirla y en su caso resolverla, calculamos el máximo común divisor de los coeficientes:

q	u	v
	$3 + 3i$	1	0
	4	0	1
$1 + i$	$-1 - i$	1	$-1 - i$
$-2 + 2i$	0		

luego el máximo común divisor es $-1 - i = (3 + 3i) - 4 \cdot (1 + i)$. Calculamos el cociente $(-1 + 5i)/(-1 - i) = -2 - 3i$ que pertenece a $\mathbb{Z}[i]$, luego la ecuación dada tiene solución. Una solución particular será

$$x_0 = -(1 + i)(-2 - 3i) = -1 + 5i, \qquad y_0 = -2 - 3i,$$

y la solución general es

$$x = -1 + 5i + k \cdot 3$$
$$y = -2 - 3i - k \cdot (2 - 2i),$$

con $k \in \mathbb{Z}[i]$ arbitrario.

3.4. Resolución de ecuaciones en congruencias

También podemos establecer en cualquier anillo euclídeo el concepto de congruencia módulo un elemento:

Definición 3.9. Sea A un anillo euclídeo y sea $m \in A$. Los elementos $a, b \in A$ se llaman *congruentes módulo* m si tienen el mismo resto al dividirlos por m. Esto se denota por $a \equiv b \pmod{m}$ o $a \equiv b \mod m$

Proposición 3.10. *Sean $a, b, m \in A$. Entonces $a \equiv b \pmod{m}$ si y sólo si $m \mid (a - b)$.*

Esta proposición nos dice que $a \equiv b \pmod{m}$ si y sólo si $a - b = mq$ para algún $q \in A$, lo que podemos escribir como $a = b + mq$. Esta observación proporciona un método muy útil de reemplazar una congruencia por una ecuación diofántica.

Proposición 3.11. *La relación $a \equiv b \pmod{m}$ es una relación de equivalencia.*

Proposición 3.12. *Sea $m \in A$. Cualesquiera $a, b, c, d \in A$ verifican las siguientes propiedades:*

1. *Si $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$, entonces $a + b \equiv c + d \pmod{m}$, $a - b \equiv c - d \pmod{m}$ y $ab \equiv cd \pmod{m}$.*
2. *Si $a + c \equiv a + d \pmod{m}$ entonces $c \equiv d \pmod{m}$. Si $ac \equiv ad \pmod{m}$ y $(a, m) = 1$ entonces $c \equiv d \pmod{m}$.*

Proposición 3.13. *Sean $a, m \in A$ con $m \neq 0$ y no invertible en A. Existe un elemento b tal que $ab \equiv 1 \pmod{m}$ si y sólo si* $\text{m. c. d.}(a, m) = 1$.

La proposición 3.13 muestra que la congruencia

$$ax \equiv 1 \pmod{m}$$

tiene solución si y sólo si $(a, m) = 1$. De hecho la demostración (omitida) de dicha proposición muestra que se obtiene una solución utilizando el algoritmo extendido de Euclides para expresar $1 = ab + mq$ con $b, q \in A$.

Definición 3.14. Dos soluciones r y s a la congruencia $ax \equiv b \pmod{m}$ son distintas módulo m si r y s no son congruentes módulo m.

Teorema 3.15. *La congruencia $ax \equiv b \pmod{m}$ tiene solución si y sólo si b es divisible por $d = \text{m. c. d.}(a, m)$. Si $d \mid b$, todas las soluciones son congruentes módulo m/d.*

Ejemplo 3.16. Consideramos $A = \mathbb{Z}[\sqrt{2}]$. Vamos a resolver la congruencia

$$(2+\sqrt{2})x \equiv 3-\sqrt{2} \pmod{3}.$$

Para ello calculamos el máximo común divisor de $2+\sqrt{2}$ y 3:

q		u	v
	3	1	0
	$2+\sqrt{2}$	0	1
$3-\sqrt{2}$	$-1-\sqrt{2}$	1	$-3+\sqrt{2}$
$-\sqrt{2}$	0		

así que un máximo común divisor es $-1-\sqrt{2} = 3\cdot 1 + (2+\sqrt{2})\cdot(-3+\sqrt{2})$. Ahora $(3-\sqrt{2})/(-1-\sqrt{2}) = 5-4\sqrt{2}$, luego la solución de la congruencia dada es $x \equiv (-3+\sqrt{2})(5-4\sqrt{2}) \equiv -23+17\sqrt{2} \equiv 1-\sqrt{2} \pmod{3}$. Obsérvese que $-1-\sqrt{2}$ es invertible en $\mathbb{Z}[\sqrt{2}]$ (su inverso es $1-\sqrt{2}$), así que $2+\sqrt{2}$ y 3 son primos relativos y la solución es única módulo 3.

Teorema 3.17. *Sea A un dominio euclídeo y sean $a, b, m, n \in A$. Dos congruencias simultáneas*

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n} \tag{3.2}$$

tienen solución si y sólo si $a \equiv b \pmod{(m,n)}$. En este caso la solución es única módulo $[m,n]$.

Ejemplo 3.18. Vamos a resolver en $A = \mathbb{Z}[\sqrt{-2}]$ el sistema de congruencias

$$x \equiv 2 \pmod{(1+\sqrt{-2})}$$
$$x \equiv \sqrt{-2} \pmod{(3+\sqrt{-2})}$$

La solución general de la primera congruencia es $x = 2 + t_1\cdot(1+\sqrt{-2})$. Lo sustituimos en la segunda:

$$2 + t_1\cdot(1+\sqrt{-2}) \equiv \sqrt{-2} \pmod{(3+\sqrt{-2})}.$$

Trasponiendo términos nos queda

$$t_1\cdot(1+\sqrt{-2}) \equiv -2+\sqrt{-2} \pmod{(3+\sqrt{-2})}. \tag{3.3}$$

Aplicamos ahora el algoritmo de Euclides extendido:

q	u	v
	$3+\sqrt{-2}$	1	0
	$1+\sqrt{-2}$	0	1
$2-\sqrt{-2}$	-1	1	$-2+\sqrt{-2}$

así que $(3+\sqrt{-2})\cdot 1+(1+\sqrt{-2})(-2+\sqrt{-2})=-1$. Luego la solución de 3.3 es $t_1=(-2+\sqrt{-2})(2-\sqrt{-2})+u\cdot(3+\sqrt{-2})=-2+4\sqrt{-2}+t\cdot(3+\sqrt{-2})$. Sustituyendo en la primera solución obtenemos la solución general del sistema:

$$\begin{aligned} x &= 2+(1+\sqrt{-2})(-2+4\sqrt{-2}+t\cdot(3+\sqrt{-2})) \\ &= -8+2\sqrt{-2}+t\cdot(1+4\sqrt{-2}). \end{aligned}$$

Ejemplo 3.19. Vamos ahora a resolver el sistema

$$\begin{aligned} x &\equiv 1+2\sqrt{-2} \pmod{(2-3\sqrt{-2})}, \\ x &\equiv 3 \pmod{(1+\sqrt{-2})}. \end{aligned}$$

Desarrollamos el algoritmo extendido de Euclides:

q	u	v
	$2-3\sqrt{-2}$	1	0
	$1+\sqrt{-2}$	0	1
$-1-2\sqrt{-2}$	-1	1	$1+2\sqrt{-2}$

así que $(2-3\sqrt{-2})\cdot 1+(1+\sqrt{-2})(1+2\sqrt{-2})=-1$ y los módulos de las congruencias son primos relativos. Luego el sistema de ecuaciones tiene solución.

La solución general de la primera ecuación es

$$x=(1+\sqrt{-2})+(2-3\sqrt{-2})t_1.$$

Sustituyendo en la segunda y trasponiendo términos nos queda la ecuación

$$(2-3\sqrt{-2})t_1\equiv 3-(1+2\sqrt{-2})=2-2\sqrt{-2} \pmod{(1+\sqrt{-2})}.$$

Por el algoritmo de Euclides calculado tenemos que

$$t_1 \equiv -1 \cdot (2 - 2\sqrt{-2}) = -2 + 2\sqrt{-2} \pmod{(1 + \sqrt{-2})}.$$

Sustituyendo en la solución de la primera obtenemos la solución general del sistema:

$$\begin{aligned} x &= (1 + \sqrt{-2}) + (2 - 3\sqrt{-2})((-2 + 2\sqrt{-2}) + (1 + \sqrt{-2})t), \\ &= (9 + 11\sqrt{-2}) + (8 - \sqrt{-2})t. \end{aligned}$$

Teorema 3.20. *Sea A un dominio euclídeo y sean $a_i, m_i \in A$ para $i = 1, \ldots, r$. Un sistema de r congruencias simultáneas*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, r \tag{3.4}$$

tiene solución si y sólo si para todo par de índices i, j se verifica

$$a_i \equiv a_j \pmod{(m_i, m_j)}, \tag{3.5}$$

y en este caso la solución es única módulo $M_r = [m_1, \ldots, m_r]$.

Ejemplo 3.21. Vamos a tomar$A = \mathbb{Z}[i]$, el anillo de los enteros de Gauss y consideramos el sistema de congruencias:

$$\begin{aligned} x &\equiv i \pmod{3}, \\ x &\equiv 2 \pmod{(2 + i)}, \\ x &\equiv 1 + i \pmod{(3 + 2i)}, \\ x &\equiv 3 + 2i \pmod{(4 + i)}. \end{aligned}$$

El máximo común divisor de los dos primeros módulos es $3 \cdot (-i) + (2 + i)(1 + i) = 1$. La solución general de la primera ecuación es

$$x = i + 3t_1$$

Sustituyendo en la segunda ecuación nos queda $3t_1 \equiv 2 - i \pmod{(2 + i)}$. Luego $t_1 \equiv -i \cdot (2 - i) = -1 - 2i \pmod{(2 + i)}$ y la solución general de las dos primeras ecuaciones es

$$\begin{aligned} x &= i + 3(-1 - 2i + (2 + i)t_2 \\ &= -3 - 5i + (6 + 3i)t_2. \end{aligned}$$

Sustituimos en la tercera ecuación y despejamos: $(6+3i)t_2 \equiv 4+6i \pmod{(3+2i)}$. El algoritmo extendido de Euclides muestra que $(6+3i)i + (3+2i)(-2i) = 1$ por lo que $t_2 \equiv i(4+6i) \pmod{(3+2i)}$. La solución general de las tres primeras ecuaciones es ahora

$$\begin{aligned} x &= -3-5i + (6+3i)(i(4+6i) + (3+2i)t_3) \\ &= -51 + i + (12+21i)t_3. \end{aligned}$$

Finalmente sustituimos este valor en la cuarta ecuación y despejamos:

$$(12+21i)t_3 \equiv 54+i \pmod{(4+i)}$$

La aplicación correspondiente del algoritmo de Euclides nos da $(-i)(12+21i) + (-4+4i)(4+i) = 1$. Luego $t_3 \equiv (-i)(54+i) = 1-54i \pmod{(4+i)}$ y la solución general del sistema dado es

$$\begin{aligned} x &= -51 + i + (12+21i)((1-54i) + (4+i)t) \\ &= 1095 - 626i + (27+96i)t \\ &= 24 - 14i + (27+96i)t, \end{aligned}$$

donde la última reducción se obtiene por el cambio $t \to t + (3+12i)$. (El algoritmo de división nos da $1095 - 626i = (27+96i)(-3-12i) + (24-14i)$).

Ejemplo 3.22. Cuando los módulos de un sistema de congruencias son primos relativos dos a dos, podemos emplear el algoritmo chino del resto. Volvamos a resolver el sistema del ejemplo anterior:

$$\begin{aligned} x &\equiv i \pmod{3}, \\ x &\equiv 2 \pmod{(2+i)}, \\ x &\equiv 1+i \pmod{(3+2i)}, \\ x &\equiv 3+2i \pmod{(4+i)}. \end{aligned}$$

Formamos el producto de todos los módulos $M = 3(2+i)(3+2i)(4+i) = 27+96i$ y cada uno de los cocientes $M_1 = M/3 = 9+32i$, $M_2 = M/(2+i) = 30+33i$, $M_3 = M/(3+2i) = 21+18i$ y $M_4 = M/(4+i) = 12+21i$. El algoritmo de Euclides para cada uno de los cuatro casos nos da

$$\begin{aligned} i(9+32i) + (11-3i)3 &= 1, \\ (-1)(30+33i) + (19+7i)(2+i) &= 1, \\ 2(21+18i) + (-15-2i)(3+2i) &= 1, \\ (-i)(12+21i) + (-4+4i)(4+i) &= 1. \end{aligned}$$

El teorema chino del resto nos dice que la solución del sistema dado es

$$\begin{aligned} x &\equiv i \cdot i(9+32i) + 2 \cdot (-1)(30+33i) \\ &\quad + (1+i) \cdot 2(21+18i) + (3+2i) \cdot (-i)(12+21i) \\ &\equiv 24 - 14i \pmod{(27+96i)}. \end{aligned}$$

4. Ejercicios

Ejercicio 1. Calcular en $\mathbb{Z}[i]$ todos los elementos z que cumplan $N(z) \leq 5$, ¿cuales de ellos son irreducibles?.

Ejercicio 2. Calcula $\mathcal{U}(R)$ las unidades del anillo R en los casos $R = \mathbb{Z}[i]$ y $R = \mathbb{Z}[\sqrt{-5}]$.

Ejercicio 3. Comprobar que los elementos $2, 3, 4+\sqrt{10}, 4-\sqrt{10}$ son irreducibles en $\mathbb{Z}[\sqrt{10}]$ pero no son primos. Como consecuencia deducir que $\mathbb{Z}[\sqrt{10}]$ no es un DFU encontrando dos factorizaciones de 6 distintas.

Ejercicio 4. Demostrar que los elementos 2, 7, $1+\sqrt{-13}$ y $1-\sqrt{-13}$ son irreducibles no asociados en $\mathbb{Z}[\sqrt{-13}]$. Encontrar dos factorizaciones distintas en irreducibles de 14 y a partir de ella concluir que en $\mathbb{Z}[\sqrt{-13}]$ hay elementos irreducibles que no son primos. ¿Es $\mathbb{Z}[\sqrt{-13}]$ un dominio euclídeo?.

Ejercicio 5. En el anillo $\mathbb{Z}[i]$ calcular el máximo común divisor y el mínimo común múltiplo de $a = 2i$ y $b = 3-7i$. Calcular además elementos u y v tales que $ua + vb = \text{mcd}(a, b)$.

Ejercicio 6. Calcular las unidades de $\mathbb{Z}\sqrt{-3}$ y demostrar que este anillo no es un DFU viendo que $4 = 2{,}2 = (1+\sqrt{-3})(1-\sqrt{-3})$ son dos factorizaciones en irreducibles distintas del elemento 4. Razonar que los elementos en las factorizaciones no son primos.

Ejercicio 7. En el anillo $\mathbb{Z}[i]$ calcular elementos u y v tales que

$$(2+5i)u + (3-4i)v = 1+i.$$

Ejercicio 8. Da la solución general, si existe, de la ecuación diofántica en $\mathbb{Z}[i]$,

$$4x + (3+3i)y = -1+5i\ .$$

Ejercicio 9. Factoriza $15+42i$ y $9-2i$ en $\mathbb{Z}[i]$. Calcula $mcd(15+42i, 9-2i)$.

Ejercicio 10. En $\mathbb{Z}[\sqrt{3}]$ factoriza $3+\sqrt{3}$ en irreducibles y calcula $\text{mcd}(3+\sqrt{3}, 2)$ y $\text{m.c.m.}(3+\sqrt{3}, 2)$.

Ejercicio 11. Demuestra que los elementos $2, 1+\sqrt{-7}, 1-\sqrt{-7}$ de $\mathbb{Z}[\sqrt{-7}]$ son irreducibles pero no son primos y encuentra dos factorizaciones que no sean esencialmente idénticas de 8 en irreducibles. ¿Que se puede concluir entonces de las propiedades aritméticas de $\mathbb{Z}[\sqrt{-7}]$?

Ejercicio 12. Sea $a+bi \in \mathbb{Z}[i]$ un elemento tal que $ab \neq 0$. Probar que es primo si y solo si $a2+b2$ es un primo.

Ejercicio 13. En el anillo $\mathbb{Z}[i]$ se consideran los elementos $x = 1+3i$, $y = 3+4i$. Factorizar x e y como producto de irreducibles y calcular su m.c.d. y su m.c.m.

Ejercicio 14. En el anillo $\mathbb{Z}[i]$ resolver el siguiente sistema de congruencias

$$\left.\begin{array}{rcccc} x & \equiv & i & \mod & 3 \\ x & \equiv & 2 & \mod & 2+i \\ x & \equiv & 1+i & \mod & 3+2i \\ x & \equiv & 3+2i & \mod & 4+i \end{array}\right\}$$

Ejercicio 15. Resolver, dando la solución general, el siguiente sistema de congruencias en $\mathbb{Z}[i]$:

$$\left.\begin{array}{rcccc} x & \equiv & 1 & (\mod & 1+2i) \\ x & \equiv & 1-i & (\mod & 1+3i) \\ x & \equiv & 2i & (\mod & 3+2i) \end{array}\right\}$$

Ejercicio 16. Demostrar que la aplicación $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_2$ dada por $f(a+bi) = [a-b]_2$ es un homomorfismo de anillos. Calcular $Ker(f)$, dando su generador, e $Im(f)$.

Ejercicio 17. Calcular en $\mathbb{Z}[\sqrt{-2}]$ el m.c.d. y el m.c.m. de los elementos 3 y $2+\sqrt{-2}$.

Ejercicio 18. En el anillo $\mathbb{Z}[\sqrt{-2}]$ resolver el siguiente sistema de congruencias

$$\left.\begin{array}{rcccc} x & \equiv & 1+2\sqrt{-2} & \mod & 2-3\sqrt{-2} \\ x & \equiv & 3 & \mod & 1+\sqrt{-2} \end{array}\right\}$$

Ejercicio 19. Sea $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z} \text{ y } \omega = (-1+i\sqrt{3})/2\}$. Demuestra que es un dominio de integridad y calcula sus unidades.

Ejercicio 20. En el anillo $\mathbb{Z}[\sqrt{5}]$ comprobar que $4 = 2 \cdot 2$ y $4 = (1+\sqrt{5})(-1+\sqrt{5})$ son dos factorizaciones en irreducibles no equivalentes, ¿es $(1+\sqrt{5})$ primo?

Ejercicio 21. Sea $S = \{a + bi \,/\, a, b \in \mathbb{Z}, b \text{ es par}\}$.

- Demostrar que S es un subanillo de $\mathbb{Z}[i]$.
- Demostrar que S no es un ideal de $\mathbb{Z}[i]$.
- ¿Cuantos elementos tiene el anillo cociente $\mathbb{Z}[i]/(3+i)\mathbb{Z}[i]$?. Razonar la respuesta.

Ejercicio 22. Si D y D' son DIP, demostrar que todo ideal de $D \times D'$ es principal aunque $D \times D'$ no es un DIP. En el caso en que $D = D' = \mathbb{Z}$ determinar el ideal generado por los elementos (a, b) y (c, d).

Ejercicio 23. Factorizar en irreducibles los siguientes elementos: $11 + 7i$ en $\mathbb{Z}[i]$; $4 + 7\sqrt{2}$ 2n $\mathbb{Z}[\sqrt{2}]$; $4 - \sqrt{-3}$ en $\mathbb{Z}[\sqrt{-3}]$.

Ejercicio 24. Hallar el m.c.d. y las expresiones de Bézout para las siguientes parejas de elementos de $\mathbb{Z}[i]$: $11 + 7i$ y $3 + 7i$; $8 + 6i$ y $5 - 15i$; $16 + 7i$ y $10 - 5i$.

Ejercicio 25. i) Encontrar u y v en $\mathbb{Z}[i]$ tales que

$$4u + (3 + 3i)v = -1 + 5i$$

.

ii) ¿Son ciertos los isomorfismos siguientes?:

$$\frac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{Z}_2 \;\; ; \;\; \frac{\mathbb{Z}[i]}{(i)} \cong \mathbb{Z} \, .$$

iii) En $\mathbb{Z}[\sqrt{-2}]$ calcular el máximo común divisor y el mínimo común múltiplo de $2 + \sqrt{-2}$ y 3.

Ejercicio 26. i) Resolver el siguiente sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$ y dar una solución de norma mayor que 7:

$$x \equiv 2 \,(\text{ mód } 1 + \sqrt{-2}) \;\; ; \;\; x \equiv \sqrt{-2} \,(\text{ mód } 3 + \sqrt{-2})$$

ii) Dar la solución general de la ecuación en $\mathbb{Z}$ $6783x + 613y = 3$.

iii) Calcular $\text{mcd}(-1 + 3i, 2)$ en $\mathbb{Z}[i]$.

iv) Descomponer $-3 + 9i$ en factores primos en $\mathbb{Z}[i]$.

Ejercicio 27. i) Calcular $\text{mcd}(18 - i, 11 + 7i)$ en $\mathbb{Z}[i]$.

ii) Verificar que $4 = 2{,}2 = (1+\sqrt{-3})(1-\sqrt{-3})$ es un ejemplo de factorización no única en elementos irreducibles en $\mathbb{Z}[\sqrt{-3}]$.

Ejercicio 28. El número de páginas de un libro es mayor que 400 y menor que 500. Si se cuentan de 2 en 2 sobra una página; si se cuentan de 3 en 3 sobran dos, si se cuentan de 5 en 5 sobran cuatro y si se cuentan de 7 en 7 sobran seis ¿Cuantas páginas tiene el libro?.

Ejercicio 29. Resolver en $\mathbb{Z}$ el siguiente sistema de congruencias: $x \equiv 1(\text{ mód } 2); x \equiv 2(\text{ mód } 3); x \equiv 2(\text{ mód } 5); x \equiv 10(\text{ mód } 11); x \equiv 10(\text{ mód } 49)$.

Ejercicio 30. Resolver en $\mathbb{Z}[\sqrt{-2}]$ el siguiente sistema de congruencias:
$x \equiv 1+2\sqrt{-2}(\text{ mód } 2-3\sqrt{-2}); x \equiv 3(\text{ mód } 1+\sqrt{-2})$.

Resolver en $\mathbb{Z}$ la congruencia $3293x \equiv 222(\text{ mód } 8991)$ y en $\mathbb{Z}[\sqrt{2}]$ la congruencia $(2+\sqrt{2})x \equiv 3-\sqrt{2}(\text{ mód } 3)$.

Ejercicio 31. Después de que una banda de 17 piratas dividiera sus doblones en partes iguales resultó que sobraban 3 doblones que decidieron dar a su cocinero chino Wun Tu; pero en una disputa murieron 6 de los piratas después de lo cual decidieron nuevamente dividir su fortuna entre los que quedaban sobrando 4 doblones que en su momento daría a Wun Tu. Pero tuvieron un accidente y sólo quedaron 6 de los piratas, el tesoro y el cocinero chino; esta vez un reparto equitativo dió un resto de 5 doblones. Cansado de la tacañería de sus amos el buen Wun Tu aprovechó su posición de cocinero para preparar un "sabroso.^{es}tofado de setas venenosas con las que eliminó a toda la banda de forma que el tesoro pasó a ser de su propiedad. Sabiendo que el número de doblones estaba comprendido entre 1000 y 2000 y que el cocinero calzaba un número 42, calcular el número de monedas que se quedó Wun Tu.

5. Anillos y extensiones cuadráticas usando GAP

5.1. Divisores de cero

Podemos utilizar el mismo procedimiento usado anteriormente para calcular las unidades en $\mathbb{Z}_{10}$, para determinar los divisores de cero de $\mathbb{Z}_{10}$.

```
gap> Filtered([1..9],n->ForAny([1..9],m->n*m mod 10=0));
[ 2, 4, 5, 6, 8 ]
```

Por tanto, como ya sabemos $\mathbb{Z}_{10}$, no es un dominio de integridad. En GAPpodemos usar la siguiente orden para comprobarlo directamente sin calcular sus divisores de cero.

```
gap> IsIntegralRing(ZmodnZ(10));
false
```

Veamos ahora cómo podemos calcular los divisores de cero del anillo

$$\mathbb{Z}_2[i] = \{a + bi | a, b \in \mathbb{Z}_2\}.$$

Primero calculamos los elementos de $\mathbb{Z}_2[i]$. Como i es la raíz cuarta de la unidad, usamos `E(4)` para representarlo.

```
gap> l:=Cartesian([0..1],[0..1]);
[ [ 0, 0 ], [ 0, 1 ], [ 1, 0 ], [ 1, 1 ] ]
gap> z2i:=Set(l,n->n[1]+n[2]*E(4));
[ 0, 1, E(4), 1+E(4) ]
```

Nos quedamos con los elementos no nulos.

```
gap> last{[2..4]};
[ 1, E(4), 1+E(4) ]
```

Seleccionamos (`Filtered`) ahora aquellos para los que exista (`ForAny`) un elemento no nulo que multiplicado por él de cero.

```
gap> Filtered(last,n->ForAny(last,m->EuclideanRemainder(n*m,2)=0));
[ 1+E(4) ]
```

Lo que indica que $1 + i$ es el único divisor de cero no nulo de $\mathbb{Z}_2[i]$. Nótese que para hacer las cuentas módulo 2, hemos usado el comando `EuclideanRemainder`, ya que con los enteros de Gauss no podemos utilizar `mod`.

5.2. Unidades

GAPtiene un comando para determinar el grupo de unidades de un anillo. Usémoslo para ver las unidades de $\mathbb{Z}_{10}$.

```
gap> Units(ZmodnZ(10));
<group with 1 generators>
```

Como la salida es un grupo, para ver sus elementos lo pasamos a lista y luego cada elemento lo representamos como un entero.

```
gap> List(last,Int);
[ 1, 3, 7, 9 ]
```

También podemos optar por la fuerza bruta, y ver para qué enteros entre 1 y 9, existe otro de forma que su producto de 1 módulo 10.

```
gap> Filtered([1..9],n->ForAny([1..9],m->n*m mod 10=1));
[ 1, 3, 7, 9 ]
```

Además GAPtiene un comando para determinar si un anillo es o no un cuerpo.

```
gap> IsField(ZmodnZ(5));
true
```

5.3. Enteros de Gauss

Ya hemos visto en prácticas anteriores cómo factorizar enteros de Gauss. También vimos cómo calcular el cociente y resto de dos enteros cualesquiera, así como su máximo común divisor y los coeficientes de Bézout correspondientes. Por desgracia, como hemos visto anteriormente, la función `mod` no se puede utilizar con los enteros de Gauss. Podemos usar en su lugar, `EuclideanRemainder` y `EuclideanQuotient` para el cociente, o bien, `QuotientRemainder` si queremos obtener ambas cantidades a la vez.

```
gap> (9+7*E(4)) mod (1+E(4));
Error, no method found! For debugging hints type ?Recovery from NoMethodFound
Error, no 1st choice method found for 'MOD' on 2 arguments called from
<function>( <arguments> ) called from read-eval-loop
Entering break read-eval-print loop ...
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue

gap> (9+7*E(4))/(1+E(4));
8-E(4)

gap> QuotientRemainder(9+7*E(4),1+E(4));
[ 8-E(4), 0 ]

gap> QuotientRemainder(9+7*E(4),3+E(4));
[ 3+E(4), 1+E(4) ]
gap> (9+7*E(4))/(3+E(4));
17/5+6/5*E(4)
```

Para el máximo común divisor y coeficientes de Bézout, podemos usar las funciones que conocemos para enteros.

```
gap> Gcd(2*E(4),3-7*E(4));
1+E(4)
gap> GcdRepresentation(2*E(4),3-7*E(4));
[ 2-4*E(4), -E(4) ]
```

Para encontrar los enteros de Gauss de norma menor o igual que cinco que sean irreducibles, podemos usar la función `Norm`. Primero generamos los posibles candidatos, que tienen que tener parte real e imaginaria menor o igual que 2 en valor absoluto.

```
gap> elementos:=List(Cartesian([-2..2],[-2..2]),n->n[1]+E(4)*n[2]);
[ -2-2*E(4), -2-E(4), -2, -2+E(4), -2+2*E(4), -1-2*E(4), -1-E(4), -1,
  -1+E(4), -1+2*E(4), -2*E(4), -E(4), 0, E(4), 2*E(4), 1-2*E(4), 1-E(4), 1,
  1+E(4), 1+2*E(4), 2-2*E(4), 2-E(4), 2, 2+E(4), 2+2*E(4) ]
```

Seleccionamos ahora aquellos con norma menor o igual que cinco.

```
gap> Filtered(elementos,n->(Norm(n)<=5));
[ -2-E(4), -2, -2+E(4), -1-2*E(4), -1-E(4), -1, -1+E(4), -1+2*E(4), -2*E(4),
  -E(4), 0, E(4), 2*E(4), 1-2*E(4), 1-E(4), 1, 1+E(4), 1+2*E(4), 2-E(4), 2,
  2+E(4) ]
```

Si escribimos,

```
gap> Filtered(last,IsPrime);
[ -2-E(4), -2, -2+E(4), -1-2*E(4), -1-E(4), -1+E(4), -1+2*E(4), 1-2*E(4),
  1-E(4), 1+E(4), 1+2*E(4), 2-E(4), 2, 2+E(4) ]
```

la salida no es la correcta, ya que por ejemplo nos aparecen 2 y -2, que sabemos que no son irreducibles en $\mathbb{Z}[i]$. Esto se debe a que no hemos especificado el anillo en la orden `IsPrime`.

```
gap> Filtered(last,n->IsPrime(GaussianIntegers,n));
[ -2-E(4), -2+E(4), -1-2*E(4), -1-E(4), -1+E(4), -1+2*E(4), 1-2*E(4), 1-E(4),
  1+E(4), 1+2*E(4), 2-E(4), 2+E(4) ]
```

Si queremos saber cuántos tenemos salvo asociados, usamos la función `StandardAssociate` (que da un asociado estándar a cada elemento de $\mathbb{Z}[i]$) junto con la operación `Set` para eliminar repetidos.

```
gap> Set(last,StandardAssociate);
[ 1+E(4), 1+2*E(4), 2+E(4) ]
```

Obsérvese que la salida es la misma si hacemos lo siguiente (+por qué?).

```
gap> elementos:=List(Cartesian([0..2],[0..2]),n->n[1]+E(4)*n[2]);
[ 0, E(4), 2*E(4), 1, 1+E(4), 1+2*E(4), 2, 2+E(4), 2+2*E(4) ]
gap> Filtered(elementos,n->(Norm(n)<=5));
[ 0, E(4), 2*E(4), 1, 1+E(4), 1+2*E(4), 2, 2+E(4) ]
gap> Filtered(last,n->IsPrime(GaussianIntegers,n));
[ 1+E(4), 1+2*E(4), 2+E(4) ]
```

5.4. Operaciones en $\mathbb{Z}[\sqrt{(d)}]$, $d \in \{-1, 2, -2, 3\}$

Si introducimos la expresión

```
gap> (1+2*Sqrt(3))*(Sqrt(3));
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
```

obtenemos una salida un poco difícil de tratar. Es por eso que vamos a definir nuestros propios productos, cociente y resto. Vamos representar un entero $a + b\sqrt{d}$ en $\mathbb{Z}[d]$ (con d libre de cuadrados) mediante una lista $[a, b]$, y pasaremos d como argumento extra en nuestras funciones. Así la función producto podría definirse como sigue.

```
por:=function(x,y,d)
    return [x[1]*y[1]+d*x[2]*y[2],x[1]*y[2]+x[2]*y[1]];
end;

gap> por([1,2],[0,1],3);
[ 6, 1 ]

gap> (1+2*Sqrt(3))*(Sqrt(3));
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
gap> 6+Sqrt(3);
-6*E(12)^4-E(12)^7-6*E(12)^8+E(12)^11
```

Para hacer el cociente, necesitamos la norma. Vamos a definir una función para tal efecto, aunque como explicamos después, también se puede hacer definiendo el cuerpo $\mathbb{Q}(\sqrt{(d)})$.

```
norma:=function(x,d)
    return AbsInt(x[1]^2-d*x[2]^2);
end;

gap> norma([4,1],3);
13
gap> F:=Field(Sqrt(3));
NF(12,[ 1, 11 ])
gap> Norm(F,4+Sqrt(3));
13
```

Hay que tener cuidado con especificar en qué cuerpo estamos si usamos `Norm` para no obtener resultados no deseados.

```
gap> Norm(4+Sqrt(3));
169
```

Como hemos visto en teoría, para dividir, necesitamos aproximarnos a un racional lo mejor que podamos con un entero. Para ello introducimos una función de redondeo.

```
redondeo:=function(x)
    if ((x-Int(x))<(Int(x)+1-x)) then
        return Int(x);
    fi;
    return Int(x)+1;
end;

gap> redondeo(2/3);
1
gap> redondeo(1/3);
0
```

Usando la función auxiliar

```
conjugado:=function(x)
    return [x[1],-x[2]];
end;
```

podemos definir la función cociente de la siguiente forma.

```
cociente:=function ( x, y, d )
    return List( por( x, conjugado( y ), d ) / norma( y, d ), redondeo );
end;

gap> cociente([11,7],[1,1],-1);
[ 9, -2 ]
gap> (11+7*E(4))/(1+E(4));
9-2*E(4)
```

Por tanto, una función resto ya es bastante fácil de obtener.

```
resto:=function(x,y,d)
    return x-por(y,cociente(x,y,d),d);
end;

gap> resto([11,7],[1,1],-1);
[ 0, 0 ]
gap> EuclideanRemainder(11+7*E(4),1+E(4));
0
```

6. Aritmética en extensiones cuadráticas de $\mathbb{Z}$ con MATHEMATICA

6.1. Generalidades

Las siguientes funciones calculan unidades y divisores de $\mathbb{Z}_n$. Utilizamos la función **Range** y otras funciones conocidas. Notemos que, por ejemplo,

```
Range[1, 10]
```

$$\{1,2,3,4,5,6,7,8,9,10\}$$

Entonces

```
unidadesZ[n_]:=Select[Range[1,n-1],GCD[#,n]==1&]
divisoresdeceroZ[n_]:=Select[Range[1,n-1], MemberQ[Mod[#Range[1,n-1],n], 0]&]
```

Así

```
divisoresdeceroZ[10]
```

Out[4] = $\{2,4,5,6,8\}$

mientras que

```
unidadesZ[4]
```

$$\{1,3\}$$

6.2. El anillo de los enteros de Gauss $\mathbb{Z}[i]$

Comenzaremos con el anillo de enteros de Gauss y en la siguiente sección analizaremos otros dominios cuadráticos.

Destacamos en principio que Mathematica trabaja con enteros de Gauss usando las mismas funciones que con enteros racionales, salvo en algunos casos en los que hay que añadir el parámetro `GaussianIntegers -> True`.

Así, directamente, podemos calcular con enteros de Gauss, resto, cociente y máximo común divisor y coeficientes de Bezout utilizando los mismos comandos ya aprendidos en la aritmética entera. Igualmente, podemos factorizar un entero de Gauss en primos.

Ejemplos

```
Mod[9+7I,1+I]
```

$$0$$

```
Mod[1+2I,1+I]
```

$$-1$$

```
Quotient[9+7I,1+I]
```

$$8-I$$

```
Quotient[1+2I,1+I]
```

$$2$$

```
ExtendedGCD[1+2I,1+I]
```

$$\{1,\{-1,2\}\}$$

```
ExtendedGCD[2I,3-7I]
```

$$\{1+I,\{2-4I,-I\}\}$$

```
FactorInteger[8+10I,GaussianIntegers->True]
```

$$\{\{-I,1\},\{1+I,2\},\{4+5I,1\}\}$$

6.2.1. Algunas funciones básicas

Las funciones `Re` e `Im` aplicadas a un número complejo devuelven respectivamente la parte real y la imaginaria de dicho número.

Ejemplos:

```
Re[2+3I]
```

$$2$$

```
Im[2+3I]
```

$$3$$

La función `Round` aplicada a un número complejo devuelve el entero de Gauss más cercano a él.

Ejemplo:

```
Round[3/5+9/7I]
```

$$1 + I$$

Usando la función `FactorInteger` podemos definir una función que factoriza un entero de gauss en primos:

```
factoriza[x_]:=FactorInteger[x, GaussianIntegers-> True]
```

Ejemplo

```
factoriza[1+3I]
```

$$\{\{1 + I, 1\}, \{2 + I, 1\}\}$$

La función `Norm` devuelve la raíz cuadrada de la norma del entero de Gauss.
Ejemplo

```
Norm[1+2I]
```

$$\sqrt{5}$$

6.2.2. Usando la función `Norm` seleccionar enteros de Gauss de norma menor que 5

.
Para ello, empezamos buscando candidatos con norma menor que 5 poniendo

```
n5=Table[a+b I,{a,0,2},{b,0,2}]
```

$$\{\{0, I, 2I\}, \{1, 1+I, 1+2I\}, \{2, 2+I, 2+2I\}\}$$
$$\{\{0, I, 2I\}, \{1, 1+I, 1+2I\}, \{2, 2+I, 2+2I\}\}$$

Convertimos la tabla en una lista

```
n5lista=Flatten[n5]
```

$$\{0, I, 2I, 1, 1+I, 1+2I, 2, 2+I, 2+2I\}\{0, I, 2I, 1, 1+I, 1+2I, 2, 2+I, 2+2I\}$$

Y en esta lista seleccionamos los elementos que tienen norma menor que 5 (según nuestra definición de norma)

```
n5listamenor=Select[n5lista,Norm[#]^2<=5&]
```

$\{0, I, 2I, 1, 1+I, 1+2I, 2, 2+I\}$ 0,I,2 I,1,1+I,1+2 I,2,2+I

Usando la función `PrimeQ` podemos definir una función que nos dice si un entero de Gauss es primo,

```
primo[x_]:=PrimeQ[x,GaussianIntegers-> True]
```

Ejemplo

```
primo[2+I]
```

True

Ahora podemos seleccionar en nuestra lista los elementos que son primos poniendo

```
Select[n5listamenor,primo]
```

$\{1+I, 1+2I, 2+I\}\{1+I, 1+2I, 2+I\}$

6.2.3. Las funciones cociente, módulo y gextendidomcd

Definimos a continuación funciones alternativas a las predefinidas para calcular cociente, resto, máximo comun divisor y coeficientes de Bezout.

Par definir una función `cociente[x,y]` que devuelva el cociente en $\mathbb{Z}[i]$ de los elementos x e y.

```
cociente[x_,y_]:=Round[x/y]
```

Ejemplo

```
cociente[3+2I,2+I]
```

2

```
Quotient[3+2I,2+I]
```

```
2
```

Para definir una función modulo[x,y] que devuelva el resto de la división de x por y.

```
modulo[x_,y_]:= x-y*cociente[x,y]
```

Ejemplo

```
modulo[5+7I,2+3I]
```

$$1+I$$

```
Mod[5+7I,2+3I]
```

$$1+I$$

Para definir una función auxiliar gextendidomcd[x,y,u0,u1,v0,v1] que calcule el máximo común divisor de x e y y los coeficientes de Bezout:

```
 gextendidomcd[x_,0,u0_,u1_,v0_,v1_]:={x,{u0,v0}}
gextendidomcd[x_,y_,u0_,u1_,v0_,v1_]:=gextendidomcd[y, \
modulo[x,y],u1,u0-u1*cociente[x,y],v1,v0-v1*cociente[x,y]]
```

Ejemplo

```
gextendidomcd[5+7I,3+2I,1,0,0,1]
```

$\{1, \{1, -2 - I\}\}$

```
ExtendedGCD[5+7I,3+2I,1,0,0,1]
```

$\{1, \{1, -2 - I\}\}$

6.3. Congruencias y Sistemas de congruencias

Queremos definir una función que calcule las soluciones de la ecuación $ax \equiv b \pmod{n}$ (donde $a, b, n \in \mathbb{Z}[i]$)

Recordamos que la congruencia anterior tiene solución si y solo si $d = \text{m.c.d.}(a, n)$ divide a b. En este caso, si escribimos $d = ua + vn$ con $b = db'$, sabemos que una solución de la congruencia es $x = ub'$. Entonces ponemos

```
Solucion[a_,b_,n_]:= With[{d=GCD[a,n]}], ExtendedGCD[a,n][[2,1]]*b/d /; Mod[b,GCD[a,n]] == 0
        Solucion[_,_,_]:= Print["La congruencia no tiene solucion"]]
```

o alternativamente usando la función auxiliar antes definida

```
 solucion[a_,b_,n_]:=If[modulo[b,gextendidomcd[a,n,1,0,0,1][[1]]]==0,\
gextendidomcd[a,n,1,0,0,1][[2,1]]*cociente[b,gextendidomcd[a,n,1,0,0,\
1][[1]]], Print["La congruencia no tiene solucion"]]
```

Así, si buscamos la solución de la congruencia $(6 + 2I)x \equiv 1 + I \pmod{4 + 10I}$

```
Solucion[6+2I,1+I,4+10I]
```

La congruencia no tiene solucion

o bien

```
solucion[6+2I,1+I,4+10I]
```

La congruencia no tiene solucion

Notemos que

```
GCD[6+2 I, 4+10 I]
```

Out[40] = 2

y que

```
Mod[1 + I, 2]
```

Out[41] = $1 + i$

por lo que $1 + I$ no es divisible por 2
Por otro lado

```
Solucion[6 + 2 I, 2 - 2 I, 4 + 10 I]
```

Out[42] = $2i$

o bien

```
solucion[6 + 2 I, 2 - 2 I, 4 + 10 I]
```

Out[43] = $2i$

Comprobamos el resultado haciendo

```
Mod[(6 + 2 I) 2 I - (2 - 2 I), 4 + 10 I]
```

Out[44] = 0

Para definir una función que calcule las soluciones de un sistema de dos congruencias

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \end{aligned}$$

recordamos que dicho sistema tiene solución si y solo si $b_1 \equiv b_2 \pmod{\text{m.c.d.}(n_1, n_2)}$, en cuyo caso, para obtener una solución resolvemos primero la ecuación $n_1 t \equiv b_2 - b_1 \pmod{n_2}$. Si t_0 es una solución de esta ecuación, entonces una solución del sistema estará dada por $x_0 = b_1 + t_0 n_1$. Tomamos:

```
Sistema[{b1_,b2_},{n1_,n2_}]:= b1 + n1*solucion[n1,b2-b1,n2] /; Mod[b1-b2, GCD[n1,n2]] == 0
        Sistema[_,_] := Print["El sistema no tiene solucion"]]
```

o alternativamente

```
sistema[{b1_,b2_},{n1_,n2_}]:= \
If[modulo[b1-b2,gextendidomcd[n1,n2,1,0,0,1][[1]]]==0,b1+n1*solucion[\
n1,b2-b1,n2],Print["El sistema no tiene solucion"]]
```

Así, si buscamos la solución del sistema

$$x \equiv 3 + 2I \pmod{2 + 4I}$$
$$x \equiv 1 + I \pmod{2 + I}$$

```
Sistema[{3+2I,1+I},{2+4I,2+I}]
```

$3 + 12I$

o bien

```
sistema[{3+2I,1+I},{2+4I,2+I}]
```

$3 + 12I$

Comprobamos

```
Mod[3 + 12 I - (3 + 2 I, I + I), {2 + 4 I, 2 + I }]
```

Out[50] = $\{0, 0\}$

Por otro lado para el sistema

$$x \equiv 1 + I \pmod{2 + 2I}$$
$$x \equiv 1 + 2I \pmod{4 + 8I}$$

tenemos

```
Sistema[{1+I,1+2I},{2+2I,4+8I}]
```

El sistema no tiene solucion

o bien

```
sistema[{1+I,1+2I},{2+2I,4+8I}]
```

El sistema no tiene solucion

Esta función nos permite definir a continuación, por recurrencia, una función que devuelve la solución de un sistema general de congruencias.

Para definir una función que recursivamente calcule las soluciones de un sistema de r congruencias en $\mathbb{Z}[i]$

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

```
SCongruencias[{a1_,a2_},{n1_,n2_}]:=Sistema[{a1,a2},{n1,n2}]
SCongruencias[{a1_,a2_,a3__},{n1_,n2_,n3__}]:=SCongruencias[{Sistema[{\
a1,a2},{n1,n2}],a3},{n1*n2/GCD[n1,n2],n3}]
```

o bien

```
sCongruencias[{a1_,a2_},{n1_,n2_}]:=sistema[{a1,a2},{n1,n2}]
sCongruencias[{a1_,a2_,a3__},{n1_,n2_,n3__}]:=sCongruencias[{sistema[{\
a1,a2},{n1,n2}],a3},{n1*n2/gextendidomcd[n1,n2,1,0,0,1][[1]],n3}]
```

Así, si buscamos la solución del sistema

$$\begin{aligned} x &\equiv 213 + I \pmod{3 + 2I} \\ x &\equiv 1 + 15I \pmod{1 + 2I} \\ x &\equiv 7 + 5I \pmod{2 + I} \end{aligned}$$

```
SCongruencias[{213+I,1+15I,7+5I}, {3+2I,1+2I,2+I}]
```

Out[57] = $1899 - 4439I$

o bien

```
sCongruencias[{213+I,1+15I,7+5I}, {3+2I,1+2I,2+I}]
```

Out[58] = $1899 - 4439I$

Comprobamos

```
Mod[% - {213 + I, 1 + 15 I, 7 + 5 I}, {3 + 2 I, 1 + 2 I, 2 + I}]
```

Out[59] = $\{0, 0, 0\}$

6.4. Los dominios cuadráticos $\mathbb{Z}[\sqrt{d}]$, $d \in \{-1, -2, 2, 3\}$

Notemos que, para los valores apuntados $d \in \{-1, -2, 2, 3\}$, los dominios $\mathbb{Z}[\sqrt{d}]$ son dominios euclideos con función euclidea definida por la norma que mas abajo recordamos.

El elemento $a + b\sqrt{d}$ lo vamos a representar por $\{a, b\}$. Empezamos definiendo las funciones elementales de producto y norma:

```
por[{x_,y_},{z_,t_},d_]:={x z+ d y t,x t +y z}
```

Ejemplo: El producto $(1 + 2\sqrt{-2})(2 + \sqrt{-2})$ lo obtenemos poniendo

```
por[{1,2},{2,1},-2]
```

$\{-2, 5\}$

Así que la solución es $-2+5\sqrt{-2}$
En cuanto a la norma, definimos

```
norma[{x_,y_},d_]:=x^2-d y^2
```

Ejemplo

```
norma[{2,1},-2]
```

```
6
```

```
norma[{2,-1},3]
```

```
1
```

Para definir el cociente, usamos la función de redondeo una vez que hemos multiplicado por el conjugado así que ponemos

```
cociente[{x_,y_},{z_,t_},d_]:=Round[por[{x,y},{z,-t},d]/norma[{z,t},d]\
];
```

Ejemplo: El cociente $(-2+5\sqrt{[-2)}/(1+3\sqrt{-2})$ lo obtenemos poniendo

```
cociente[{-2,5},{1,3},-2]
```

$$\{1, 1\}$$

Una vez que tenemos el cociente, el resto lo obtenemos con la función.

```
resto[{x_,y_},{z_,t_},d_]:={x,y}-por[{z,t},cociente[{x,y},{z,t},d],d]
```

Así, el resto de dividir $2 + 5\sqrt{3}$ entre $4 - 3\sqrt{3}$ lo obtenemos poniendo

```
resto[{2,5},{4,-3},3]
```

$$\{4, -2\}$$

mientras que

```
resto[{11,7},{3,7},-1]
```

$$\{1, 3\}$$

Se propone como ejercicio final encontrar solución a los ejercicios propuestos en la sección 4 que puedan ser resueltos utilizando las funciones definidas en esta práctica.

Índice alfabético