Factorización y dominios euclídeos

M. Bullejos Lorenzo, P. Carrasco Carrasco, P. A. García Sánchez,
A. Martínez Cegarra, E. Miranda Palacios, A. Rodríguez Garzón,
y los alumnos de Álgebra I de doble grado Matemáticas e Informática

15 de enero de 2019

Índice

1. Factorización

Sea A un dominio de integridad y sean $a, b \in A$.

Definición 1.1. Decimos que b *es un múltiplo de* a y que a *divide a* b si existe un $c \in A$ tal que $ac = b$. Se representa por $a \mid b$.

Todo divisor de 1 se llama *unidad* del anillo A.

Dos elementos $a, b \in A$ se llaman *asociados* si a divide a b y b divide a a.

Para un anillo A, el conjunto de divisores de uno constituye un grupo multiplicativo que se llama *grupo de las unidades* y se representa por $A^\times$.

Ejemplo 1.2. $\mathbb{Z}^\times = \{1, -1\}$.
$\mathbb{J}^\times = \{1, i, -1, -i\}$.
$\mathbb{Z}[\sqrt{2}]^\times = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z},\ a^2 - 2b^2 = \pm 1\}$.

Lema 1.3. *En un dominio de integridad A dos elementos $a, b \in A$ son asociados si y sólo si existe una unidad $u \in A$ tal que $a = bu$.*

Definición 1.4. Un elemento $a \in A$ es un *irreducible* o *átomo* de A si no es una unidad y si $a = bc$ implica que b o c es una unidad.

Ejemplo 1.5. En $\mathbb{Z}$ las unidades son 1 y -1 y los irreducibles son los primos y sus negativos.

Sea A un dominio de integridad y sean $a, b \in A$.

Definición 1.6. Un *máximo común divisor* de a y b es un elemento $d \in A$ que verifica dos propiedades:

1. $d \mid a$ y $d \mid b$.
2. Para $c \in A$, $c \mid a$ y $c \mid b$ implica $c \mid d$.

Se suele representar $d = (a, b) = \text{m. c. d.}(a, b)$.

Lema 1.7. *Dos máximos comunes divisores d, d' de a y b son asociados.*

Definición 1.8. Dos elementos $a, b \in A$ son *primos relativos* si $\text{m. c. d.}(a, b) = 1$.

Proposición 1.9. *Sea A un dominio de integridad y sean $a, b, c \in A$. Las siguientes reglas se verifican siempre que existan los máximos comunes divisores implicados:*

1. $(a, b) = (b, a)$
2. $((a, b), c) = (a, (b, c))$
3. $(ac, bc) = (a, b)c$
4. (a, b) *es asociado de a si y sólo si $a \mid b$.*
5. $(a, 0) = a$.

Demostración. 1. Por definición, es independiente el orden de los elementos a la hora de calcular su máximo común divisor.

2. Veamos en primer lugar que $((a,b),c) \mid a$ y que $((a,b),c) \mid (b,c)$. Por definición, se verifica que:

$$((a,b),c) \mid (a,b),\ ((a,b),c) \mid c.$$

Pero, además, que $(a,b) \mid a$ y $(a,b) \mid b$, luego, por transitividad, tenemos también que:

$$((a,b),c) \mid a,\ ((a,b),c) \mid b.$$

Haciendo uso además de que $((a,b),c) \mid c$, como hemos visto anteriormente, llegamos a que $((a,b),c) \mid (b,c)$.

Por otra parte, veamos que si cierto $k \in A$ verifica $k \mid a$ y $k \mid (b,c)$, entonces se da que $k \mid ((a,b),c)$. Como $(b,c) \mid b$ y $(b,c) \mid c$, tenemos por transitividad que $k \mid b$ y $k \mid c$, y usando todo esto, llegamos a que:

$$k \mid (a,b) \text{ y } k \mid c, \text{ por tanto, } k \mid ((a,b),c).$$

3. □

Definición 1.10. Sea A un dominio de integridad. Un *mínimo común múltiplo* de a y b es un elemento $m \in A$ que verifica dos propiedades:

1. $a \mid m$ y $b \mid m$.
2. Para $c \in A$, $a \mid c$ y $b \mid c$ implica $m \mid c$.

Se suele representar $m = [a,b] = \text{m. c. m.}(a,b)$.

Lema 1.11. *Dos mínimos comunes múltiplos m, m' de a y b son asociados.*

Proposición 1.12. *Sea A un dominio de integridad y sean $a, b, c \in A$. Las siguientes reglas se verifican siempre que existan los mínimos comunes múltiplos implicados.*

1. $[a,b] = [b,a]$,
2. $[[a,b],c] = [a,[b,c]]$,
3. $[ac,bc] = [a,b]c$,
4. $[a,b]$ *es asociado de* a *si y sólo si* $b \mid a$,
5. $[a,1] = a$.

Proposición 1.13. *Sea A un dominio de integridad y sean a, b dos elementos de A que tienen un mínimo común múltiplo m. Entonces $m = 0$ si y sólo si $a = 0$ o $b = 0$. Si $m \neq 0$, el elemento $d = ab/m$ es un máximo común divisor de a y b.*

Demostración. Sea $ab \neq 0$. El producto ab es un múltiplo de a y b, luego $m \mid ab$. Sea $ab = md$. En particular $m \neq 0$. Además $m = ab_1 = a_1 b$, así que $ab = ab_1 d = a_1 bd$. Como A es un dominio de integridad, $b = b_1 d$ y $a = a_1 d$, luego d divide a a y b. Sea d_1 otro divisor común de a y b. Llamamos $m_1 = ab/d_1$. Es fácil ver que m_1 es un múltiplo común de a y b, luego existe $c \in A$ tal que $m_1 = mc$. De donde $md = ab = m_1 d_1 = mcd_1$. Luego $d = cd_1$ y d_1 es un divisor de d. □

El enunciado recíproco es falso.

Ejemplo 1.14. Sea A el subanillo de $\mathbb{Z}[X]$ formado por los polinomios con coeficiente de X par. Los elementos 2 y $2X$ tienen un máximo común divisor en A, pero no tienen mínimo común múltiplo.

Sin embargo es cierto cuando *todos* los pares tienen un máximo común divisor.

Proposición 1.15. *Sea A un dominio de integridad en el que todo par de elementos tiene un máximo común divisor. Entonces todo par de elementos tiene un mínimo común múltiplo.*

Demostración. Sean $a, b \in A$, $ab \neq 0$. Sea $d = \text{m. c. d.}(a, b)$, así que $a = a_1 d$ y $b = b_1 d$ con $a_1, b_1 \in A$. Sea $m = ab/d = a_1 b_1 d = ab_1 = a_1 b$. Evidentemente $a \mid m$ y $b \mid m$. Sea m_1 un múltiplo común arbitrario de a, b y sea $k = \text{m. c. d.}(m, m_1)$. Como a y b son divisores de m y m_1, necesariamente a y b dividen a k. Sea $m = kd_1$ y sea $k = au = bv$. Sustituyendo obtenemos $a_1 b = m = kd_1 = bvd_1$. Simplificando nos queda $a_1 = vd_1$ y por tanto $a = a_1 d = v(d_1 d)$. Similarmente $b = u(d_1 d)$. Por tanto $(d_1 d)$ divide a $\text{m. c. d.}(a, b) = d$. Sea $d = cd_1 d$. Simplificando nos queda $1 = cd_1$, por lo que d_1 es una unidad y k, m son asociados, así que m divide a m_1.Luego $m = \text{m. c. m.}(a, b)$. □

1.1. Dominios de factorización única

El *teorema fundamental de la aritmética* dice que todo entero se factoriza en irreducibles de forma esencialmente única. La unicidad de la factorización resulta ser muy útil, lo que motiva la siguiente definición.

Definición 1.16. Un *dominio de factorización única* (abreviadamente, un DFU) o *dominio factorial* es un dominio de integridad en el que todo elemento no nulo ni unidad se puede escribir como un producto de irreducibles y además verifica que dadas dos factorizaciones en irreducibles del mismo elemento

$$a = p_1 \dots p_n = q_1 \dots q_m,$$

entonces $n = m$ y existe una permutación $\sigma \in S_n$ tal que p_i es asociado de $q_{\sigma(i)}$ para $i = 1, \dots, n$.

Ejemplo 1.17. $\mathbb{Z}$ es un dominio de factorización única por el teorema fundamental de la aritmética.

Ejemplo 1.18. Todo cuerpo es un dominio de factorización única de manera trivial.

Más adelante veremos que los anillos de polinomios con coeficientes en un dominio de factorización única también son dominio de factorización única.

Sea A un dominio de factorización única y sea $\mathcal{P}$ un conjunto de irreducibles tal que todo irreducible de A está asociado exactamente a un irreducible de $\mathcal{P}$. (en muchos ejemplos interesantes $\mathcal{P}$ es infinito, pero esto no es esencial). Todo elemento a de A se escribe de manera única como $a = up_1^{k_1} \dots p_n^{k_n}$ donde u es una unidad y los p_i son elementos de $\mathcal{P}$.

Lema 1.19. *Sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ elementos de A. Entonces $a \mid b$ si y sólo si $k_1 \leq t_i$ para $i = 1, \dots, n$.*

Proposición 1.20. *Sea A un dominio de factorización única, sean $a, b \in A$ y sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ las factorizaciones en irreducibles. Entonces* $\text{m. c. d.}(a, b) = up_1^{l_1} \dots p_n^{l_n}$ *donde $l_i = \text{mín}(k_i, t_i)$ para $i = 1, \dots, n$.*

Proposición 1.21. *Sea A un dominio de factorización única Sean $a = up_1^{k_1} \dots p_n^{k_n}$ y $b = up_1^{t_1} \dots p_n^{t_n}$ las factorizaciones en irreducibles. Entonces* $\text{m. c. m.}(a, b) = up_1^{s_1} \dots p_n^{s_n}$ *donde $s_i = \text{máx}(k_i, t_i)$ para $i = 1, \dots, n$.*

Vamos a establecer dos caracterizaciones de los dominios de factorización única.

Definición 1.22. Sea A un dominio de integridad y p un elemento suyo; p es un *elemento primo* de A si no es cero ni unidad y para $a, b \in A$ se verifica que $p \mid ab$ si y sólo si $p \mid a$ o $p \mid b$.

Ejemplo 1.23. Los primos de $\mathbb{Z}$ son los números primos y sus opuestos.

Lema 1.24. *Sea p un primo de A y sean $a_1, \dots, a_n \in A$. Entonces p divide al producto $a_1 \dots a_n$ si y sólo si existe un i tal que $p \mid a_i$.*

Lema 1.25. *Todo primo es un irreducible.*

Teorema 1.26. *Un dominio de integridad A es un dominio de factorización única si y sólo si*

1. *todo elemento no nulo ni unidad descompone como producto de irreducibles,*
2. *todo irreducible es primo.*

Demostración. Sea A un dominio de factorización única y sea $u \in A$ irreducible Sean $a, b \in A$ tales que $u \mid ab$. Entonces existe un $c \in A$ tal que $uc = ab$. Sean $a = u_1 \dots u_n$, $b = u_{n+1} \dots u_m$ y $c = v_1 \dots v_k$ factorizaciones en irreducibles Sustituyendo nos queda $uv_1 \dots v_k = u_1 \dots v_m$. Estas son dos factorizaciones en irreducibles. Como A es factorial, $k + 1 = m$ y existe un u_j asociado con u. Si $j \leq n$, resulta que $u \mid a$ y si $j > n$ queda que $u \mid b$. Luego u es primo.

A la inversa, sea A un dominio de integridad verificando las condiciones del enunciado y sean $a = p_1 \dots p_n = q_1 \dots q_m$ dos factorizaciones en irreducibles. Si n=1, $p_1 = q_1 \dots q_m$ y como p_1 es irreducible, necesariamente $m = n$ y $p_1 = q_1$.

Sea ahora $n > 1$ y supongamos que la factorización es única siempre que uno de los productos tenga menos de n factores. Como $p_1 \mid q_1 \dots q_m$ y p_1 es primo, existe un q_j tal que $p_1 \mid q_j$ y como q_j es irreducible, $q_j = p_1 u$ con u invertible. Por sencillez suponemos que $j = 1$. Nos queda $p_1 \dots p_n = p_1(uq_2) \dots q_m$ y simplificando $p_2 \dots p_n = (uq_2) \dots q_m$. Pero ahora el primer miembro tiene $n-1$ factores. Por la hipótesis de inducción, $n - 1 = m - 1$ y existe una permutación $i \mapsto j$ ta que p_i y q_j son asociados. □

Teorema 1.27. *Un dominio de integridad A es un dominio de factorización única si y sólo si*

1. *todo elemento no nulo ni unidad descompone como producto de irreducibles,*
2. *todo par de elementos tiene máximo común divisor.*

Demostración. La primera condición es la misma en ambos casos. Sea A un dominio de factorización única. Por la proposición 1.20 todo par de elementos tiene un máximo común divisor.

A la inversa, supongamos que todo par de elementos tiene un máximo común divisor. Sea $u \in A$ un irreducible arbitrario y sean $a, b \in A$ tales que $u \nmid a$ y $u \nmid b$, es decir que $\text{m. c. d.}(u, a) = 1 = \text{m. c. d.}(u, b)$. Por la proposición 1.9, $b = (ub, ab)$ y $1 = (u, b) = (u, (ub, ab)) = ((u, ub), ab) = (u(1, b), ab) = (u, ab)$. El contrarrecíproco nos dice que $(u, ab) = u$ implica $(u, a) = u$ ó $(u, b) = u$ □

Las proposiciones 1.20 y 1.21 suministran una forma cómoda de calcular el máximo común divisor y el mínimo común múltiplo. La pega es que presuponen que A es un dominio de factorización única y que a y b han sido factorizados en A. Pero el proceso de factorizar completamente un elemento normalmente es largo y penoso. Para $\mathbb{Z}$, $K[X]$ y otros dominios de integridad existe un método más directo y efectivo de calcular el máximo común divisor usando un algoritmo de división con resto. Esto motiva la definición de dos nuevas clases de anillos: Los dominios de ideales principales y los dominios euclídeos.

1.2. Dominios de ideales principales

Definición 1.28. Un *dominio de ideales principales* (abreviado por D.I.P) es un dominio de integridad en el que todo ideal es principal.

Lema 1.29. *En un dominio de ideales principales A toda cadena ascendente de ideales*

$$(a_1) \subset (a_2) \subset \dots$$

es estacionaria, es decir que existe un n tal que $(a_n) = (a_{n+1}) = \dots$.

Demostración. Sea $I = \cup_i (a_i)$. Es fácil comprobar que I es un ideal de A, luego existe un $b \in I$ tal que $I = (b)$. Como I es la unión de los ideales (a_i), existe un n tal que $b \in (a_n)$, es decir que $b = ca_n$ es un múltiplo de a_n. Para cualquier m tenemos que $a_m \in I$, luego $a_m = d_m b$ es un múltiplo de b. Sustituyendo tenemos que $a_m = d_m c a_n \in (a_n)$ y por tanto $(a_m) \subset (a_n)$ para todo m. Luego $(a_m) = (a_n)$ para todo $m \geq n$. □

Proposición 1.30. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. 1. *Todo elemento de un dominio de ideales principales se descompone como producto de irreducibles:*

Sea A un dominio de ideales principales arbitrario y sea $a_1 \in A$ cualquier elemento que no es invertible. Si a_1 es irreducible, tenemos una factorización $a_1 = p_1$. Si a_1 es reducible existe una factorización $a_1 = a_2 b_1$ con a_2 y b_1 no invertibles, y por tanto $(a_1) \subsetneq (a_2)$. Si a_2 es reducible, repetimos el razonamiento y obtenemos un a_3 no invertible tal que $(a_1) \subsetneq (a_2) \subsetneq (a_3)$. Por el lema anterior, este proceso no puede ser infinito. Luego llegamos a una factorización $a_1 = p_1 a_2$ con p_1 irreducible.

Si a_2 es irreducible o invertible, tenemos una factorización de a_1 en irreducibles. En otro caso, repetimos el proceso y obtenemos $a_2 = p_2 a_3$ con p_2 irreducible y $a_1 = p_1 p_2 a_3$. Otra vez tenemos una cadena ascendente de ideales $(a_1) \subsetneq (a_2) \subsetneq (a_3) \ldots$. Por el lema anterior, esta cadena es estacionaria. Luego existe un n tal que $a_1 = p_1 \ldots p_n$ es una factorización de a_1 como producto de irreducibles.

2. *En un dominio de ideales principales A todo par de elementos tiene un máximo común divisor:*

Sean $a, b \in A$ arbitrarios y sea $I = (a, b)$ el ideal generado por ellos. Por ser A un dominio de ideales principales, existe un $d \in I$ tal que $(a, b) = (d)$. Los elementos a, b están en $I = (d)$ luego $d \mid a$ y $d \mid b$. Además existen $u, v \in A$ tales que $d = ua + vb$. Sea c un divisor común de a y b, así que $a = a_1 c$ y $b = b_1 c$. Luego $d = ua_1 c + vb_1 c = (ua_1 + vb_1)c$ es un múltiplo de c.

□

Corolario 1.31 (Identidad de Bézout)**.** *Sea A un dominio de ideales principales. Para cualesquiera $a, b \in A$ existen $u, v \in A$ tales que*

$$d = \text{m. c. d.}(a, b) = ua + vb.$$

2. Definiciones de dominio euclídeo y resultados básicos

Definición 2.1. 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 2.2. 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 2.3. *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 2.4. 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 2.5. *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 2.6 (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 2.3. Tras un número finito de pasos tenemos un resto cero:

$$\begin{aligned}
a &= bq_1 + r_1 && \phi(r_1) < \phi(b)\\
b &= r_1q_2 + r_2 && \phi(r_2) < \phi(r_1)\\
&\dots && \dots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n && \phi(r_n) < \phi(r_{n-1})\\
r_{n-1} &= r_nq_n && r_{n+1} = 0
\end{aligned}$$

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

$$r_n = au + bv. \tag{2.1}$$

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 2.1 cualquier divisor de a y b también divide a r_n. Luego $d = r_n = \text{m. c. d.}(a, b)$ □

Corolario 2.7. *En un anillo euclídeo dos elementos cualesquiera tienen un mínimo común múltiplo.*

Corolario 2.8. *En un dominio euclídeo todo irreducible es primo.*

Corolario 2.9. *Todo dominio euclídeo es un dominio de factorización única.*

Corolario 2.10. *Para cualquier cuerpo K el anillo de polinomios $K[X]$ es un dominio de factorización única.*

3. Ejemplos: Anillos cuadráticos

3.1. 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 $u = 0$.

3.2. 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 3.1. *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 3.2. *Un elemento $x = a + b\omega \in \mathcal{O}$ es invertible en $\mathcal{O}$ si y sólo si $N(x) = \pm 1$.*

Ejemplo 3.3. 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 3.4 (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 3.5 (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 3.6. *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 3.7. *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 3.8. *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 3.9. *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.*

3.3. 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 3.10. *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 3.11. *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 3.12. *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

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

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

4. 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.

4.1. Factorización en primos

Ejemplo 4.1. 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 3.9, 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 4.2. 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 4.3. 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

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

4.2. 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 4.4. 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 4.5. 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 4.6. 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.$(a, b) = \frac{-1+\sqrt{-11}}{2} = b \cdot 1 + a \cdot (-1)$,

4.3. 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

$$ax + by = c. \tag{4.1}$$

Teorema 4.7. *1. La ecuación 4.1 tiene solución si y sólo si* $\text{m. c. d.}(a, b) \mid c$.

2. Una solución particular de 4.1 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 4.1. 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 4.8. 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.

4.4. Resolución de ecuaciones en congruencias

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

Definición 4.9. 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 4.10. *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 4.11. *La relación $a \equiv b \pmod{m}$ es una relación de equivalencia.*

Proposición 4.12. *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 4.13. *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 4.13 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 4.14. 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 4.15. *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 4.16. 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 4.17. *Sea A un dominio euclídeo y sean $a, b, m, n \in A$. Dos congruencias simultáneas*

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n} \tag{4.2}$$

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

Ejemplo 4.18. 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

$$t_1\cdot(1+\sqrt{-2}) \equiv -2+\sqrt{-2} \pmod{(3+\sqrt{-2})}. \tag{4.3}$$

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 4.3 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 4.19. 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 4.20. *Sea A un dominio euclídeo y sean $a_i, m_i \in A$ para $i = 1, \ldots, r$. Un sistema de r congruencias simultáneas*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, r \tag{4.4}$$

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

$$a_i \equiv a_j \pmod{(m_i, m_j)}, \tag{4.5}$$

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

Ejemplo 4.21. 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 4.22. 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

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

Índice alfabético