Tema 5

Dominios Euclídeos

Hay un tipo de dominios de integridad, los llamados "*Dominios Euclídeos*" (DE, por acortar), donde se dispone de una herramienta eficaz para saber si un elemento a divide a otro b; esto es, si la ecuación $ax = b$ tiene solución y, en su caso, resolverla.

Definición 5.0.1. *Sea A un DI. Se dice que A es un DE, si es especificada una aplicación $\rho : A - \{0\} \to \mathbb{N} = \{0, 1, ...\}$, que llamaremos la "*función euclídea*", tal que*

1. *$\rho(ab) \geq \rho(a)$, $\forall\, a, b \in A$, $a, b \neq 0$.*

2. *$\forall\, a, b \in A$, con $b \neq 0$, $\exists\, q, r \in A$ tal que $a = bq + r$, donde $r = 0$ o $\rho(r) < \rho(b)$.*

Nos referimos a "q" y a "r" como un cociente y un resto de dividir a entre b (¡no exigimos su unicidad!).

Proposición 5.0.2. *Sea A es un DE, para $a, b \in A - \{0\}$ son equivalentes:*

1. *$b|a$.*

2. *Todo resto de dividir a entre b es 0.*

3. *0 es un resto de dividir a entre b.*

Demostración.
(1) $\Rightarrow$ (2):
Si $b|a$ existe $c \in A$ tal que $a = bc$. Supongamos que $a = bq + r$ con $r = 0$ o $\rho(r) < \rho(b)$. Hemos de ver que necesariamente $r = 0$. En efecto, en otro caso, tenemos $r = a - bq = bc - bq = b(c - q)$ y, en particular, $c - q \neq 0$. pero entonces $\rho(r) = \rho(b(c - q)) \geq \rho(b)$, lo que supone una contradicción a que $\rho(r) < \rho(b)$.
Las implicaciones (2) $\Rightarrow$ (3) y(3) $\Rightarrow$ (1) son inmediatas. ■

Observación 5.0.1. Claramente $\mathbb{Z}$, por el Teorema de Euclides, es un DE con función euclídea el valor absoluto $|\ | : \mathbb{Z} \to \mathbb{N}$ (que en este caso está definida incluso para el 0). Vemos ahora que los anillos de polinomios $K[x]$, con K un cuerpo, son también DE.

Teorema 5.0.3. *Sea K un cuerpo. Para cualesquiera polinomios $f(x), g(x) \in K[x]$, con $g(x) \neq 0$, existen dos únicos polinomios $q(x), r(x) \in K[x]$ tales que $f(x) = g(x)q(x) + r(x)$ donde $r(x) = 0$ o $gr(r(x)) < gr(g(x))$.*

Demostración.

Probemos primero la unicidad: Supongamos $f(x) = g(x)q(x)+r(x)$ donde $r(x) = 0$ o $gr(r(x)) < gr(g(x))$ y $f(x) = g(x)q'(x) + r'(x)$, donde $r'(x) = 0$ o $gr(r'(x)) < gr(g(x))$. Y Supongamos que fuera $r(x) \neq r'(x)$. Entonces $r(x) - r'(x) \neq 0$ y claramente $gr(r(x) - r'(x)) < gr(g(x))$. Además, como $r(x) - r'(x) = g(x)(q'(x) - q(x)) \neq 0$, también es $q'(x) - q'(x) \neq 0$, y tendríamos también que $gr(r(x)-r'(x)) = gr(g(x))+gr(q'(x)-q(x)) \geq gr(g(x))$, lo que supone una contradicción. Luego $r(x) = r'(x)$ y, entonces, también $q(x) = q'(x)$.

Veamos ahora la existencia: Es claro que podemos reducirnos al caso en que $f(x) \neq 0$ y $gr(f(x)) \geq gr(g(x))$ (en otro caso $q(x) = 0$ y $r(x) = f(x)$ serían los cocientes y el resto). Supongamos que $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$, con $a_n \neq 0$ y $b_m \neq 0$, de manera que $n = gr(f(x)) \geq m = gr(g(x))$. Y haremos la demostración por inducción en n, el grado de $f(x)$.

Si $n = 0$, como $m \leq n$, será también $m = 0$, así que $f(x) = a_0 \in K$ y $g(x) = b_0 \in K$. La igualdad $a_0 = b_0(b_0^{-1}a_0) + 0$ nos dice que el cociente es $b_0^{-1}a_0$ y el resto 0.

Supuesto $n > 0$, y realizada la hipótesis de inducción, construyamos el polinomio

$$\begin{aligned} f_1(x) &= f(x) - a_n b_m^{-1} x^{n-m} g(x) \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}) \end{aligned}$$

que claramente resulta de grado menor que n. Por hipótesis de inducción, existen polinomios $q_1(x)$ y $r(x)$ con $f_1(x) = g(x)q_1(x) + r(x)$, donde bien es $r(x) = 0$ o $gr(r_1(x)) < gr(g(x))$. Pero entonces tenemos la igualdad

$$\begin{aligned} f(x) &= f_1(x) + a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &= g(x)(q_1(x) + a_n b_m^{-1} x^{n-m}) + r(x) = g(x)q(x) + r(x), \end{aligned}$$

y concluimos que el cociente es $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ y el resto $r(x)$. ■

Tenemos entonces que

Teorema 5.0.4. *el anillo $K[x]$ es un DE con función euclídea la función grado.*

No siempre hay unicidad de cocientes y restos. En los siguentes ejemplos de DE, los anillos de enteros cuadráticos, $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{3}]$, tal cosa no ocurre.

Teorema 5.0.5. *Para $n = -2, -1, 2, 3$ los anillos $\mathbb{Z}[\sqrt{n}]$ son DE, con función euclídea definida por $\rho(\alpha) = |N(\alpha)|$.*

Demostración.

Recordar que, para cualquier $a + b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$, su norma es

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2,$$

que un racional, pero entero si a y b lo son.

Sean $\alpha = a + b\sqrt{n}, \beta = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, dos enteros cuadráticos no nulos. La primera condición de DE es fácil de probar:

$$|N(\alpha\beta)| = |N(\alpha)|\,|N(\beta)| \geq |N(\alpha)| \quad \text{(pues } |N(\beta)| \geq 1)$$

Para la segunda condición, supongamos que $|\mathbb{N}(\alpha)| \geq |\mathbb{N}(\beta)|$. Hemos de probar que existen $q = q_1 + q_2\sqrt{n}$ y $r = r_1 + r_2\sqrt{n}$ en $\mathbb{Z}[\sqrt{n}]$ tal que $\alpha = \beta q + r$, donde bien es $r = 0$ o $|N(r)| < |N(\beta)|$ en otro caso. Para ello, procedemos como sigue.

Recordar que el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ es $\mathbb{Q}[\sqrt{n}]$. Consideramos entonces la fracción $\frac{\alpha}{\beta}$ y la expresamos como un elemento de $\mathbb{Q}[\sqrt{n}]$, mediante el procedimiento de "*racionalizar*":

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{1}{N(\beta)}(a+b\sqrt{n})(c-d\sqrt{n}) = \frac{1}{N(\beta)}\Big((ac-bdn)+(cb-ad)\sqrt{n}\Big)\\ &= \frac{ac-bdn}{N(\beta)} + \frac{cb-ad}{N(\beta)}\sqrt{n} = a_1 + a_2\sqrt{n},\end{aligned}$$

donde, claramente, $a_1, a_2 \in \mathbb{Q}$. Seleccionamos enteros $q_1, q_2 \in \mathbb{Z}$ con la condición de que $|a_1 - q_1| \leq \frac{1}{2}$, $|a_2 - q_2| \leq \frac{1}{2}$. Llamamos entonces $q = q_1 + q_2\sqrt{n}$ y $r = \alpha - \beta q$. Claramente $q, r \in \mathbb{Z}[\sqrt{n}]$ y $\alpha = \beta q + r$. Bastará que probemos que, si $r \neq 0$, entonces $|N(r)| < |N(\beta)|$. Para ello, trabajando en el cuerpo de fracciones $\mathbb{Q}[\sqrt{n}]$, notemos que

$$\begin{aligned}|N(r)| = |N(\alpha - \beta q)| &= \Big|N\Big(\beta\Big(\frac{\alpha}{\beta} - q\Big)\Big)\Big| = |N(\beta)|\,\Big|N\Big(\frac{\alpha}{\beta} - q\Big)\Big|\\ &= |N(\beta)|\,\big|N\big((a_1-q_1)+(a_2-q_2)\sqrt{n}\big)\big|\\ &= |N(\beta)|\,\big|(a_1-q_1)^2 - n(a_2-q_2)^2\big| = |N(\beta)|\,|A|.\end{aligned}$$

donde hemos denotado $A = (a_1 - q_1)^2 - n(a_2 - q_2)^2$. Y será suficiente probar que $|A| < 1$. Vemos esto en cada caso $n = -1, -2, 2, 3$:

- Si $n = -1$, $A = (a_1 - q_1)^2 + (a_2 - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$.
- Si $n = -2$, $A = (a_1 - q_1)^2 + 2(a_2 - q_2)^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$.
- Si $n = 2$, $A = (a_1 - q_1)^2 - 2(a_2 - q_2)^2$, donde $0 \leq (a_1 - q_1)^2 \leq \frac{1}{4}$ y $0 \leq 2(a_2 - q_2)^2 \leq \frac{1}{2}$. Entonces $-\frac{1}{2} \leq A \leq \frac{1}{4}$ y $|A| \leq \frac{1}{2} < 1$.
- Si $n = 3$, $A = (a_1 - q_1)^2 - 3(a_2 - q_2)^2$, donde $0 \leq (a_1 - q_1)^2 \leq \frac{1}{4}$ y $0 \leq 3(a_2 - q_2)^2 \leq \frac{3}{4}$. Entonces $-\frac{3}{4} \leq A \leq \frac{1}{4}$ y $|A| \leq \frac{3}{4} < 1$.

■

Ejemplo de no unicidad en los cocientes y restos.

En el anillo $\mathbb{Z}[i]$, se verifica que $11 + 7i = (2i)(3 - 5i) + (1 + i)$, donde $N(1 + i) = 2 < 4 = N(2i)$. Luego $3 - 5i$ y $1 + i$ son un cociente y un resto de dividir $11 + 7i$ entre $2i$. Pero también $11 + 7i = (2i)(4 - 6i) + (-1 - i)$, donde $N(-1 - i) = 2 < 4 = N(2i)$. Luego $4 - 6i$ y $-1 - i$ son también un cociente y un resto de dividir $11 + 7i$ entre $2i$.

Ejercicios.

1. Con un recipiente de 67 litros ¿podré rellenar con precisión un depósito de 1207 litros? (No. La ecuación $67x = 1207$ no tiene solución, pues $1207 = 67 \cdot 18 + 1$ y 67 no divide a 1208).
2. ¿Es $f(x) = 2x^4 - 3x^3 + 6x + 10$ divisor de $g(x) = 6x^6 - 9x^5 + 2x^4 + 15x^3 + 30x^2 + 6x + 10$ en el anillo $\mathbb{Q}[x]$? (Si, $g(x) = f(x)(3x^2 + 1)$.
3. ¿Es $f(x) = 2x^4 - 3x^2 + 6x + 10$ divisor de $g(x) = 6x^6 - 9x^5 + 2x^4 + 15x^3 + 30x^2 + 8x + 10$ en el anillo $\mathbb{Q}[x]$? (No, $g(x) = f(x)(3x^2 + 1) + 2x$.)
4. ¿Es $f(x) = 1 + 3x^2$ divisor de $g(x) = 2 + 3x + 4x^3 + 2x^4$ en el anillo $\mathbb{Z}_5[x]$? (Si, $g(x) = f(x)(2 + 3x + 4x^2)$.

5. Resolver la ecuación $(7+2\sqrt{2})x = 4+7\sqrt{2}$.

6. Resolver la ecuación $3i\,x = 11+7i$ en $\mathbb{Z}[i]$.

7. ¿Podremos rellenar con precisión un depósito de 538.833 litros usando un recipiente de 371? En caso afirmativo ¿Cuantas veces usaremos el recipiente?

8. Determinar, si existe, un polinomio $f(x) \in \mathbb{Q}[x]$ tal que
$$\Big(\frac{3}{5}x^3+\frac{1}{2}x+\frac{2}{3}\Big)f(x) = \frac{9}{20}x^5+\frac{147}{40}x^3+\frac{1}{2}x^2+\frac{11}{4}x+\frac{11}{3}.$$

9. Calcular el cociente y el resto de dividir, en el anillo $\mathbb{Q}[x]$, el polinomio $\frac{9}{20}x^5+\frac{147}{40}x^3+\frac{1}{2}x^2+\frac{17}{4}x+\frac{17}{3}$ entre el polinomio $\frac{3}{5}x^3+\frac{1}{2}x+\frac{2}{3}$.

10. Determinar, si existe, un polinomio $f(x) \in \mathbb{Z}_3[x]$ tal que
$$(2x^2+x+2)f(x) = 2x^7+x^6+2x^4+2.$$

11. En el anillo $\mathbb{Z}[i]$, calcular cociente y resto de dividir $1+15i$ entre $3+5i$.

12. ¿Es $2+5\sqrt{3}$ un divisor de $39-9\sqrt{3}$ en el anillo $\mathbb{Z}[\sqrt{3}]$?

5.1 Máximo común divisor

Nos vamos a continuación abordar las ecuaciones de la forma $ax+by=c$ en el contexto de Dominios Euclídeos. Estas son ecuaciones clásicamente estudiadas en el contexto del anillo $\mathbb{Z}$ de los números enteros, donde surgen de forma muy natural. Por ejemplo, con recipientes de 6 y 15 litros, ¿podré rellenar con precisión un depósito de 39 litros?. Si x es el número de veces que uso el recipiente de 6 e y el de 15, será por que $6x+9y=39$, y así trasformamos el problema en una ecuación diofántica (Se puede hacer, usando 4 veces el de 6 y una vez el de 15). Para estudiar y resolver tales ecuaciones será fundamental el concepto de máximo común divisor, que presentamos a continuación.

En lo que sigue A es un DI.

Definición 5.1.1. *Dados dos elementos $a,b \in A$, decimos que un elemento $d \in A$ es un máximo común divisor (mcd, para acortar) de a y b, y escribiremos $d = mcd(a,b)$ o bien $d=(a,b)$ (si en el contexto no hay confusión), si tiene las siguientes dos propiedades:*

1. *$d|a \wedge d|b$.*
2. *Si $c|a \wedge c|b$, entonces $c|d$.*

Ambas condiciones en conjunto significan que los divisores de d son exactamente los divisores comunes a a y b.

El mcd de dos elementos en un DI, si existe, no es único. Si $d=(a,b)$, claramente lo es también cualquier asociado con d (pues tienen los mismos divisores). Y recíprocamente, si también $d'=(a,b)$ entonces d y d' tienen los mismos divisores, y en particular, se dividen mutuamente, luego d y d' son asociados. Así que d es único salvo asociados. Con esta salvedad, hablaremos de que "*d es el mcd de a y b*", abusando del artículo determinado.

Definición 5.1.2. *Decimos que a y b son "* primos relativos *" o "* primos entre sí *", si $(a,b)=1$.*

Notemos que el concepto de mcd se extiende sin dificultad a un conjunto finito de elementos $a_1, ..., a_n \in A$: d es un mcd de ellos, cosa que escribiremos poniendo $d = mcd(a_1, ..., a_n)$ o bien $d = (a_1, ..., a_n)$, si:

1. $d|a_i \ \forall i = 1, ...n$ y,
2. si un $c|a_i \ \forall i = 1, ...n$, entonces $c|d$.

Las siguientes son propiedades generales, que se satisfacen siempre que existan los máximos comunes divisores que se ven involucrados en los enunciados (las igualdades hay que leerlas "salvo asociados"):

1. $(a, b) = (b, a)$.
2. Si a y a' son asociados, entonces $(a, b) = (a', b)$.
3. $(a, b) = a \Leftrightarrow a|b$. En particular $(a, 0) = a$, $(a, 1) = 1$.
4. $((a, b), c) = (a, b, c) = (a, (b, c))$.
5. $(ac, bc) = (a, b)c$.

   Podemos limitarnos al caso en que $a, b, c \neq 0$. Sea $d = (a, b)$ y $(ac, bc) = e$. Como $dc|ac \wedge dc|bc$, será $dc|e$. Supongamos que $e = dcu$. Por otra parte, como $dcu|ac$ y $dcu|bc$, resulta que $du|a$ y $du|b$, de donde $du|d$. Por tanto será $d = duv$, lo que implica que $1 = uv$ ($d \neq 0$ pues $a \neq 0$ es un múltiplo suyo). Así que $u \in U(A)$ y e es asociado con dc, luego dc es también el mcd de ac y bc, pues e lo es. En conclusión $(a, b)c = (ac, bc)$.
6. Si $d = (a, b)$, y $a = da'$ y $b = db'$ entonces $(a', b') = 1$.

   Como $d(a'b') = (da', db') = (a, b) = d = d \cdot 1$, basta simplificar por d.
7. Si $a|bc$ y $(a, b) = 1$, entonces $a|c$.

   Pongamos $bc = ax$. Entonces $c = c1 = c(a, b) = (ac, bc) = (ac, ax) = a(c, x)$.
8. Si $(a, b) = 1$, entonces $a|c \wedge b|c \Rightarrow ab|c$.

   Pongamos $c = bx$. Como $a|bx$ y $(a, b) = 1$, será $a|x$. Pongamos $x = ay$. Entonces $c = aby$.
9. $(a, b) = 1 \wedge (a, c) = 1 \Leftrightarrow (a, bc) = 1$.

   $\Rightarrow$]: $c = c1 = c(a, b) = (ac, bc)$. Entonces

   $$1 = (a, c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc).$$

   $\Leftarrow$]: $1 = (a, bc) = ((a, ac), bc) = (a, (ac, bc)) = (a, (a, b)c)$. Como (a, b) es un divisor común a a y a $(a, b)c$, será (a, b) un divisor de uno, o sea una unidad. Luego $(a, b) = 1$. De la primera igualdad, $1 = (a, (a, b)c)$, se sigue que también $(a, c) = 1$.
10. $(a, b) = (a - qb, b)$.

    Si $c|a \wedge c|b$, entonces $c|a - qb \wedge a|b$. Si $c|a - qb \wedge c|b$, entonces $c|a - qb + qb = b \wedge c|b$. Luego los divisores comunes a a y b son los mismos que los divisores comunes a $a - qb$ y b. Tendrán por tanto el mismo mcd.

11. Si p es irreducible, entonces $(p,a) = \begin{cases} p & \text{si } p|a, \\ 1 & \text{en otro caso.} \end{cases}$

Observación 5.1.1. No siempre existe el mcd de dos cualesquiera elementos en un DI.

EJEMPLO. *En* $\mathbb{Z}[\sqrt{-5}]$ *no existe* $(2+2\sqrt{-5},6)$.

En efecto. Observamos primero que, en este anillo, 3 es irreducible. Supongamos que por el contrario que $3 = \alpha\beta$, donde ni α ni β son unidades. O sea que $N(\alpha) \neq 1 \neq N(\beta)$. Entonces, la igualdad $N(3) = 9 = N(\alpha)N(\beta)$, obligaría a que $N(\alpha) = 3 = N(\beta)$. Pero, para cualesquiera $a, b \in \mathbb{Z}$,

$$N(a + b\sqrt{-5}) = 3 \Leftrightarrow a^2 + 5b^2 = 3$$

y no existen números enteros a y b de forma que se verifique tal igualdad.

Observamos ahora que 3 no divide a $1+\sqrt{-5}$, pues $N(3) = 9$ no es un divisor en $\mathbb{Z}$ de $N(1+\sqrt{-5}) = 1 + 25 = 26$. Entonces $(3, 1+\sqrt{-5}) = 1$.

Supongamos ahora que existiera $(2+2\sqrt{-5},6)$. Tendía que ser entonces

$$(2+2\sqrt{-5},6) = 2(1+\sqrt{-5},3) = 2 \cdot 1 = 2.$$

Pero ocurre que $1+\sqrt{-5} \,|\, 2+2\sqrt{-5}$ (pues $2+2\sqrt{-5} = 2(1+\sqrt{-5})$) y $1+\sqrt{-5}\,|6$ (pues $6 = N(1+\sqrt{-5}) = (1+\sqrt{-5})(1-\sqrt{-5})$), y tendría que ocurrir que $1+\sqrt{-5}\,|2$. Pero esto es falso, $N(1+\sqrt{-5}) = 6$, $N(2) = 4$ y 6 no es un divisor de 4 en $\mathbb{Z}$.

Hay dominios de integridad, sin embargo, donde la existencia de mcd está garantizada. Es el caso de los DE. Para probarlo, comenzamos con la siguiente

Proposición 5.1.3. *En un DE, todo ideal es principal.*

Demostración. Sea A un DE, e I un ideal suyo. Siempre $0 \in I$ (pues si $x \in I$, entonces $0 = 0x \in I$). Si $I = \{0\}$, entonces $I = 0A$ y es principal generado por el cero.

Supuesto I con elementos no nulos, consideremos

$$R = \{\rho(b) \mid b \in I, b \neq 0\} \subseteq \mathbb{N}.$$

Este conjunto no vacío de naturales tendrá un mínimo, digamos dado por $\rho(m)$. Como $m \in I$ e I es cerrado para múltiplos, será $mA \subseteq I$. Veamos que $I \subseteq mA$. En otro caso, tendríamos un $a \in I$ tal que m no divide a a. Pongamos $a = bm + r$ donde $r = 0$ o $\rho(r) < \rho(m)$. Claramente, no puede ser $r = 0$, o sea que $r \neq 0$ y $\rho(r) < \rho(m)$. Pero esto no es posible ya que $r = a + (-b)m \in I$, luego $\rho(r) \in R$, y $\rho(m)$ es mínimo en R. ■

Teorema 5.1.4. *Si A es un DE, existe el mcd de cualesquiera dos elementos. Además, si $d = (a,b)$, siempre es posible encontrar dos elementos $u, v \in A$ tales que*

$$d = au + bv,$$

*que son llamados "*coeficientes de Bezout de a y b*".*

Demostración. Dados $a, b \in A$, consideremos

$$I = aA + bA = \{ax + by \mid x, y \in A\}.$$

Es un ideal de A y será principal. Supongamos que $I = dA$. Como $a, b \in I = dA$, será $d|a$ y $d|b$. Además, como $d \in I$, será $d = au + bv$ para ciertos $u, v \in A$. Por otro lado, si $c|a$ y $c|b$ entonces $c|au + bv = d$. Luego $d = (a,b)$ y u, v son coeficientes de Bezout. ■

En un DE tenemos un algoritmo para el cálculo de mcd y coeficientes de Bezout. Es conocido como el ALGORITMO EXTENDIDO DE EUCLIDES, y es como sigue:

Si uno de los elementos involucrados es nulo, la cuestión es fácil:

$$(a, 0) = a = 1 \cdot a + 0 \cdot 0.$$

Supongamos entonces que $a, b \neq 0$, y podemos suponer entonces que $\rho(a) \geq \rho(b)$ (recordar que $(a, b) = (b, a)$. El algoritmo consiste en construir, recursivamente, una sucesión de elementos del anillo $r_1, r_2, \ldots, r_n$ partiendo de $r_1 = a$ y $r_2 = b$, por el siguiente procedimiento:

Si $r_i \neq 0$ entonces r_{i+1} es un resto de dividir r_{i-1} entre r_i.

Así, r_3 es el resto de dividir $r_1 = a$ entre $r_2 = b$. Si $r_3 \neq 0$, entonces r_4 es el resto de dividir r_2 entre r_3, etc.

Puesto que para todo i, $\rho(r_{i+1}) < \rho(r_i)$, la sucesión de números naturales $\rho(r_2) = \rho(b)$, $\rho(r_3)$, ..., $\rho(r_i)$, ... es estrictamente decreciente, y esta no puede continuar indefinidamente; esto es, habrá un $n \geq 1$ tal que $r_{n+1} = 0$. Pues bien, aseguramos que entonces

$$r_n = (a, b),$$

esto es el último de los restos no nulos obtenidos en tal sucesión es el mcd de a y b. En efecto, probamos por inducción que, para todo $i = 1, 2, ..., n$, se verifica que $(a, b) = (r_i, r_{i+1})$. Para $i = 1$, esto es obvio, pues $r_1 = a$ y $r_2 = b$. Supongamos que $i > 1$ y que $(a, b) = (r_{i-1}, r_i)$. Si q_i es el cociente de dividir r_{i-1} entre r_i, será $r_{i+1} = r_{i-1} - r_i q_i$. Entonces

$$(a, b) = (r_{i-1}, r_i) = (r_i, r_{i-1} - r_i q_i) = (r_i, r_{i+1}).$$

Finalmente, $(a, b) = (r_{n-1}, r_n) = r_n$, ya que $r_n | r_{n-1}$ al ser $r_{n+1} = 0$.

Vamos ahora que podemos encontrar, para todo $i = 1, ..., n$, elementos $u_i, v_i \in A$ tal que $r_i = au_i + bv_i$, por la reglas recursivas

- $u_1 = 1$, $v_1 = 0$.
- $u_2 = 0$, $v_1 = 1$.

y para $i \geq 2$,

- $u_{i+1} = u_{i-1} - q_i u_i$, $u_{i+1} = u_{i-1} - q_i u_i$.

En efecto, para $i = 1$ e $i = 2$, es obvio que $r_i = au_i + bu_i$. Supongamos esto cierto hasta un $i \geq 2$. Entonces

$$r_{i+1} = r_{i-1} - q_i r_i = au_{i-1} + bv_{i-1} - q_i(au_i + bv_i) = a(u_{i-1} - q_i u_i) + a(v_{i-1} - q_i v_i) = au_{i+1} + bv_{i+1}.$$

En última instancia, tenemos que $r_n = (a, b) = au_n + bv_n$, y habremos encontrado unos coeficientes de Bezout: $u = u_n$, $v = v_n$.

Vamos a sintetizar los datos anteriores en una tabla que nos permitirá no solo calcular el mcd de dos elementos, sino también los coeficientes de Bezout

	a	1	0
	b	0	1
q_2	r_3	$u_3 = 1 - 0 \cdot q_2$	$v_3 = 0 - q_2 \cdot 1$
...	...	...	...
q_{i-2}	r_{i-1}	u_{i-1}	v_{i-1}
q_{i-1}	r_i	u_i	v_i
q_i	r_{i+1}	$u_{i+1} = u_{i-1} - u_i \cdot q_i$	$v_{i+1} = v_{i-1} - q_i \cdot v_i$
...	...	...	...

EJEMPLOS.

1. En $\mathbb{Z}$, calcular $(80, 30)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & 80 & 1 & 0 \\ & 30 & 0 & 1 \\ 2 & 20 & 1 & -2 \\ 2 & 10 & -1 & 3 \\ & 0 & & \end{array}$$

   nos indica que $(80, 20) = 10$ y $10 = (-1) \cdot 80 + 3 \cdot 30$.

2. En el anillo $\mathbb{Z}[i]$, calcular $(11+7i, 3+7i)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & 11+7i & 1 & 0 \\ & 3+7i & 0 & 1 \\ 1-i & 1+3i & 1 & -1+i \\ -2 & 1+i & -2 & 3-2i \\ & 0 & & \end{array}$$

   nos indica que $(11+7i, 3+7i) = 1+i$ y $1+i = (-2)(11+7i) + (3-2i)(3+7i)$.

3. En el anillo $\mathbb{Z}_2[x]$, calcular $(x^3+x^2+x+1, x^4+x^3+x+1)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & x^4+x^3+x+1 & 1 & 0 \\ & x^3+x^2+x+1 & 0 & 1 \\ x & x^2+1 & 1 & x \\ & 0 & & \end{array}$$

   nos indica que $(x^3+x^2+x+1, x^4+x^3+x+1) = x^2+1$ y $x^2+1 = 1 \cdot (x^4+x^3+x+1) + x \cdot (x^3+x^2+x+1)$.

4. En el anillo $\mathbb{R}[x]$, calcular $(x^5+x^4+2x^3+2x^2+x+1, x^4+x^3+2x^2+x+1)$ y unos correspondientes coeficientes de Bezout.
   La tabla

$$\begin{array}{cc|cc} & x^5+x^4+2x^3+2x^2+x+1 & 1 & 0 \\ & x^4+x^3+2x^2+x+1 & 0 & 1 \\ x & x^2+1 & 1 & -x \\ & 0 & & \end{array}$$

   nos indica que $(x^5+x^4+2x^3+2x^2+x+1, x^4+x^3+2x^2+x+1) = x^2+1$ y

   $x^2+1 = 1 \cdot (x^5+x^4+2x^3+2x^2+x+1) + (-x) \cdot (x^4+x^3+2x^2+x+1)$.

5.2 Ecuaciones diofánticas

En lo que sigue A es un DE.

Teorema 5.2.1. *Sea la ecuación $ax+by=c$, donde $a, b \neq 0$, y sea $d = (a, b)$.*

1. *La ecuación tiene solución si y solo si $d|c$.*

2. *Si (x_0, y_0) es una solución particular, entonces la solución general consiste de todos los pares (x, y), donde*

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

Demostración. Al mismo tiempo que lo demostramos, "aprenderemos" a resolver tales ecuaciones.

Pongamos $a = da'$ y $b = db'$. Si la ecuación tiene soluciones, digamos que (x, y) es una de ellas, entonces, como $d|a$ y $d|b$, será $d|ax + by = c$. Así que, si d no divide a c, la ecuación no tiene solución.

Supongamos ahora que $d|c$. Pongamos $c = dc'$. La ecuación se escribe entonces como $da'x + db'y = dc'$, o sea $d(a'x + b'y) = dc'$, que claramente es equivalente a la ecuación

$$a'x + b'y = c'$$

donde $(a', b') = 1$. Nos referimos a esta como la reducida de la original. La novedad es que los coeficientes son ahora primos relativos. Podemos entonces encontrar $u, v \in A$, tal que $1 = a'u + b'v$. Entonces $c' = a'(c'u) + b'(c'v)$, vemos así que la ecuación tiene solución, y que (x_0, y_0), con $x_0 = c'u$ e $y_0 = c'v$, es una solución particular.

Para determinar todas las soluciones, notemos que, para cualquier $k \in K$, $(x_0 + kb', y_0 - ka')$ es también una solución:

$$a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + ka'b' + b'y_0 - ka'b' = a'x_0 + b'y_0 = c'.$$

Y no hay más soluciones que esas: Si (x, y) fuese cualquier otra, de las igualdades $a'x + b'y = c' = a'x_0 + b'y_0$, se deduce que $a'(x - x_0) = b'(y_0 - y)$. Pero entonces $b'|a'(x - x_0)$ y, ya que $(a', b') = 1$, será $b'|(x - x_0)$. Así que, para algún $k \in A$, $x - x_0 = kb'$. Análogamente, $a'|b'(y_0 - y)$ y, ya que $(a', b') = 1$, será $a'|(y_0 - y)$, de donde concluimos que $y_0 - y = ha'$, para un cierto $h \in A$. Pero, sustituyendo en la igualdad $a'(x - x_0) = b'(y_0 - y)$, vemos que $a'b'k = a'b'h$, de donde concluimos que $h = k$. Así que

$$x = x_0 + kb' = x_0 + k\frac{b}{d},\ x = y_0 - ka' = y_0 - k\frac{a}{d}.$$

■

Ejercicios.

1. "Cuarenta y seis náufragos cansados arribaron a una bella isla. Allí encontraron ciento veintiséis montones de cocos, de no más de cincuenta cada uno, y catorce cocos sueltos, y se los repartieron equitativamente . . ." (cuento del año 850 a.c.). ¿Cuántos cocos había en cada montón?

2. Disponemos de 15 euros para comprar 40 sellos de correos, de 10, 40, y 60 céntimos y, al menos, necesitamos 2 de cada tipo ¿Cuántos sellos de cada clase podremos comprar?

3. Llueve y, en un mercadillo improvisado en Moscú, un paraguas nos cuesta 190 rublos. Disponemos solo de billetes de 3 rublos, y el vendedor solo de 5 rublos ¿Podremos hacer la compra-venta? ¿Cómo?

4. En una torre eléctrica, se nos ha roto una pata de 4 m de altura. Para equilibrarlo provisionalmente, disponemos de 7 discos de madera de 50 cm de grosor y de otros 12 de 30 cm. ¿Cuál de las siguientes afirmaciones es verdadera?

- ☐ No podremos equilibrar la torre.
- ☐ Podremos equilibrar la torre, y de una única manera.
- ☐ Podremos equilibrar la torre, y de dos únicas maneras.
- ☐ Podremos equilibrar la torre, y de más de 2 maneras distintas.

5. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{R}[x]$, de los polinomios $x^3 - 2x^2 - 5x + 6$ y $x^3 - 3x^2 - x + 3$. Encontrar todos los polinomios $f(x)$ y $g(x)$ en $\mathbb{R}[x]$, ambos de grado 3, tales que
$$(x^3 - 2x^2 - 5x + 6)f(x) + (x^3 - 3x^2 - x + 3)g(x) = x^3 - 6x^2 + 11x - 6.$$

6. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{Z}_3[x]$, de los polinomios $x^4 + x^3 - x - 1$ y $x^5 + x^4 - x - 1$.Encontrar todos los polinomios $f(x)$ y $g(x)$ en $\mathbb{Z}_3[x]$, con grado de $g(x)$ igual a 7, tales que
$$(x^4 + x^3 - x - 1)f(x) + (x^5 + x^4 - x - 1)g(x) = x^4 + x^2 + 1.$$

7. a) En el anillo $\mathbb{Z}[\sqrt{-2}]$, calcular
$$(2 - 3\sqrt{-2}, 1 + \sqrt{-2}),\ [2 - 3\sqrt{-2}, 1 + \sqrt{-2}].$$

8. En $\mathbb{Z}[\sqrt{3}]$, calcula $(3 + \sqrt{3}, 2)$ y $[3 + \sqrt{3}, 2]$.

9. Determina enteros de Gauss $x, y \in \mathbb{Z}[i]$, con $N(x) \leq 18$, tales que
$$4x + (3 + 3i)y = -1 + 5i.$$

10. Resolver la siguiente ecuación en el anillo $\mathbb{Z}[\sqrt{2}]$:
$$(4 + \sqrt{2})x + (6 + 4\sqrt{2})y = \sqrt{2}.$$

5.3 Mínimo común múltiplo

Sea A un DI.

Definición 5.3.1. *Dados dos elementos $a, b \in A$, decimos que un elemento $m \in A$ es un mínimo común múltiplo (mcm, para acortar) de a y b, y escribiremos $m = mcm(a, b)$ o bien $m = [a, b]$, si tiene las siguientes dos propiedades*

1. *$a|m \wedge b|m$.*
2. *Si $a|c \wedge b|c$, entonces $m|c$.*

Ambas condiciones en conjunto significan que los múltiplos de m son exactamente los múltiplos comunes a a y b.

Como el mcd, el mcm de dos elementos, si existe, no es único. Si $m = [a, b]$, claramente lo es también cualquier asociado con m (pues tienen los mismos múltiplos). Y recíprocamente, si también $m' = [a, b]$ entonces m y m' tienen los mismos multiplos, y en particular, lo son uno del otro o, en otras palabras, se dividen mutuamente, luego m y m' son asociados. Así que m es único salvo asociados. Con esta salvedad, hablaremos de que "*m es el mcm de a y b*", abusando del artículo determinado.

Notemos que el concepto se extiende sin dificultad a un conjunto finito de elementos $a_1, ..., a_n \in A$: m es un mcm de ellos, cosa que escribiremos poniendo $m = mcm[a_1, ..., a_n]$ o bien $m = [a_1, ..., a_n]$, si:

1. $a_i|m\ \forall i = 1, ...n$ y,
2. si para un $c \in A$, $a_i|c\ \forall i = 1, ...n$, entonces $m|c$.

Las siguientes son propiedades generales, que se satisfacen siempre que existan los máximos comunes divisores que se ven involucrados en los enunciados (las igualdades hay que leerlas "salvo asociados"):

1. $[a, b] = [b, a]$.
2. Si a y a' son asociados, entonces $[a, b] = [a', b]$.
3. $[a, b] = a \Leftrightarrow b|a$. En particular $[a, 0] = 0$, $[a, 1] = a$.
4. $[[a, b], c] = [a, b, c] = [a, [b, c]]$.
5. $[ac, bc] = [a, b]c$.

   Si $c = 0$, es obvio. Supongamos $c \neq 0$. Como $c|ac$, será $c|[ac, bc]$, ya que este último es un múltiplo de ac. Pongamos $[ac, bc] = cq$. Sea $m = [a, b]$. Como $a|m$ y $b|m$, también $ac|mc$ y $ab|mc$, por tanto que $cq = [ac, bc]|mc$, de donde concluimos que $q|m$. Por otra parte, como $ac|cq = [ac, bc]$ y $bc|cq = [ac, bc]$, será $a|q$ y $b|q$, de modo que $m|q$. Luego m es asociado a q, y $q = [a, b]$. Así que $[ac, bc] = c[a, b]$.

La siguiente es muy relevante,

Teorema 5.3.2. *En un DE existe mcm de todo par de elementos. Además, para cualquier par de elementos a, b, se tiene que*

$$(a, b)[a, b] = ab.$$

Demostración. Sean $a, b \in A$. El subconjunto $aA \cap bA$ de los múltiplo comunes es un ideal. Será principal. Supongamos $aA \cap bA = mA$. Como $m \in aA$ y $m \in bA$, es $a|m$ y $b|m$. Si $a|c$ y $b|c$, entonces $c \in aA \cap bA = mA$, luego $m|c$ y $m = [a, b]$.

Para lo segundo, probamos primero que, si $(a, b) = 1$, entonces $[a, b] = ab$: Claramente $a|ab$ y $b|ab$. Si $a|c$ y $b|c$, como $(a, b) = 1$, sabemos que entonces $ab|c$.

Supongamos ahora que $(a, b) = d$. Pongamos $a = da'$ y $b = db'$, con lo que $(a', b') = 1$ y, por lo ya probado $[a', b'] = a'b'$. Pero entonces

$$(a, b)[a, d] = d[a'd, b'd] = d^2[a', b'] = d^2a'b' = (da')(db') = ab.$$

■

Observación 5.3.1. En el tema anterior definimos operaciones con ideales, aunque dejamos hacer el cálculo explícito de la suma y la intersección de ideales. Después de los Teoremas 5.1.4 y 5.3.2 tenemos que en un DE A:

- $aA + bA = (a, b)A$.
- $aA \cap bA = [a, b]A$.
- $aA \cdot bA = abA$.

5.4 Congruencias en DE

Recordemos que si $I \leq A$ es un ideal, decimos que un elemento "*a es congruente con un elemento b módulo I*", y escribimos

$$a \equiv b \mod I \qquad \text{o bien} \qquad a \equiv_I b,$$

si $a - b \in I$.

Si A es un DE, entonces todo ideal es principal, en el caso $I = mA$ hablamos simplemente de "*ser congruente módulo m*", y escribimos

$$a \equiv b \mod m \qquad \text{o bien} \qquad a \equiv_m b,$$

para significar que $a - b \in mA$ o equivalentemente, que $m|a-b$, esto es, que existe un $k \in A$ tal que $a - b = km$ o, equivalentemente, tal que $a = b + km$.

Cuando A es un Dominio Euclídeo y $m \in A$, $m \neq 0$, ser congruente módulo m está muy relacionado con lo que ocurre con el resto de dividir por m. Destacamos las siguientes propiedades:

1. Todo elemento del anillo es congruente con cualquiera de sus restos de división por el módulo m.

2. *$a \equiv_m b$ si y solo si a y b tienen un mismo resto al dividirlos por m.*
   Si $a \equiv_m b$, entonces $a = b + mk$ para un k. Si $b = mq + r$, con $r = 0$ o $\rho(r) < \rho(m)$, entonces $a = m(q+k)+r$ y r es también un resto de dividir a entre m. Reciprocamente, si $a = mp + r$ y$b = mq + r$, con $r = 0$ o $\rho(r) < \rho(m)$, entonces $a = b + m(p - q)$ y $a \equiv_m b$.

3. *Si $ac \equiv_m bc$ y $(c, m) = 1$, entonces $a \equiv_m b$.*

4. *Si $c \neq 0$, entonces $ac \equiv_{mc} bc \Leftrightarrow a \equiv_m b$.*

Ejemplos.

1. (a) $30 \equiv 6 \mod (8)$, pues $8|30 - 6 = 24$. Entonces $(+100)$ $130 \equiv 106 \mod (8)$ y (-5) $25 \equiv 1 \mod (8)$.
   (b) $166 \equiv 102 \mod (8) \Leftrightarrow 66 \equiv 2 \mod (8) \Leftrightarrow 64 \equiv 0 \mod (8) \Leftrightarrow 8|64$, ¡Sí!.
   (c) Que $30 \equiv 6 \mod (8)$ no implica que $(:6)5 \equiv 1 \mod (8)$, lo que es falso, pues $(6, 8) \neq 1$. Pero si implica que $10 \equiv 2 \mod (8)$, pues $(3, 8) = 1$.

2. *Calcular los restos módulo 7 de las potencias naturales de 2.*
   Calculemos las primeras potencias

   $$2^0 = 1 \equiv_7 1; \qquad 2^1 = 2 \equiv_7 2; \qquad 2^2 = 4 \equiv_7 4; \qquad 2^3 = 8 \equiv_7 1.$$

   Ya hay una repetición. Ya se van a repetir todas: Si $n \equiv 0 \mod (3)$, entonces $n = 3k$, y $2^n = (2^3)^k \equiv_7 1^k = 1$; luego el resto de dividir 2^n entre siete será 1. Si $n \equiv 1 \mod (3)$, entonces $n = 3k + 1$, y $2^n = (2^3)^k 2 \equiv_7 1^k 2 = 2$; luego el resto de dividir 2^n entre siete será 2. Si $n \equiv 2 \mod (3)$, entonces $n = 3k + 2$, y $2^n = (2^3)^k 2^2 \equiv_7 1^k 4 = 4$; luego el resto de dividir 2^n entre siete será 4. Como todo número es congruente con 0, 1 o 2 módulo 3 (su resto al dividirlo 3), ya los tenemos todos.

Por ejemplo, ¿Qué resto da 2^{350} al dividirlo por 7? Será 4, pues

$$350 = 10 \cdot 35 = 10 \cdot 5 \cdot 7 \equiv_7 1 \cdot 2 \cdot 1 = 2.$$

3. Calcular el resto de dividir $100^{1034} + 30^{3147}125^{311}$ entre 7.

   Como $100 = 2 \cdot 50 \equiv_7 2 \cdot 1 = 2$, $100^{1034} \equiv_7 2^{1035}$. Como $1034 = 1000 + 34 \equiv_3 1 + 1 = 2$, concluimos que $100^{1034} \equiv_7 4$.

   Como $30^{3147} \equiv_7 2^{3147} = 2^{15} \equiv_7 2^{3\cdot 1049} \equiv_7 1$, y $125^{311} = (5^3)^{311} \equiv_7 ((-2)^3)^{311} = -(2^3)^{311} \equiv_7 (-1)^{311} = -1$, concluimos que

   $$100^{1034} + 30^{3147} + 125^{311} \equiv_7 4 + 1 - 1 = 4.$$

4. Argumentar que un número natural es congruente módulo 3 con la suma de sus cifras. En particular divisible por 3 si y solo si lo es la suma de sus cifras.

   Si $n = a_m a_{m-1} \cdots a_1 a_0$, con $0 \leq a_i \leq 9$, $a_m \neq 0$, entonces $n = a_0 + a_1 10 + a_2 10^2 + \cdots + a_m 10^m$ y, como $10 \equiv_3 1$, $n \equiv_3 a_0 + a_1 + \cdots + a_m$.

4. Calcular el resto de dividir 13912 entre 3.

   $13913 \equiv_3 17 \equiv_3 8 \equiv_3 2$.

La siguiente observación es general para potencias en congruencias entre números enteros.

Lema 5.4.1. *Si* $a^e \equiv a^{e+k} \mod (m)$, *entonces, para cualquier* $n \geq 0$,

$$a^{e+n} \equiv a^{e+r} \mod (m)$$

donde r *es el resto de dividir* n *entre* k. *Par tanto, las potencias de* a *son congruentes, módulo* m, *con* $1 = a^0, a, a^2, \ldots, a^e, a^{e+1}, \ldots, a^{e+k-1}$.

En particular, si $e = 0$, *esto es, si* $a^k \equiv 1 \mod (m)$, *entonces, para cualquier* $n \geq 0$,

$$a^n \equiv a^r \mod (m)$$

donde r *es el resto de dividir* n *entre* k. *Par tanto, las potencias de* a *son congruentes, módulo* m, *con* $1, a, a^2, \ldots, a^{k-1}$.

Demostración. Vemos primero, por inducción en $q \geq 0$, que $a^{e+qk} \equiv a^e \mod (m)$. Para $q = 0$ es evidente. Entonces, supuesto para q,

$$a^{e+k(q+1)} = a^{e+kq}a^k \equiv_m a^e a^k \equiv_m a^{e+k} \equiv_m a^e.$$

Entonces, si $n = kq + r$, con $0 \leq r < k$, $a^{e+n} = a^{e+kq+r} = a^{e+kq}a^r \equiv_m a^e a^r = a^{e+r}$. ■

EJEMPLO. *Calcular el resto de* $2^{(47^{51})}$ *módulo* 14.

Empezamos las primeras potencias de 2: $2^0 \equiv_{14} 1$, $2^1 \equiv_{14} 2$, $2^3 \equiv_{14} 8$, $2^4 \equiv_{14} 16 \equiv_{14} 2$. Así que $2^1 \equiv_{14} 2^{1+3}$, luego, para cualquier $n \geq 0$, $2^{n+1} \equiv_{14} 2^{r+1}$, si r es el resto de dividir n entre 3. Calculemos entonces el resto de dividir $47^{51} - 1$ entre 3:

$$47^{51} - 1 \equiv_3 11^{51} - 1 \equiv_3 2^{51} - 1 \equiv_3 (-1)^{51} - 1 \equiv_3 -2 \equiv_3 1.$$

Luego, $2^{(47^{51})} \equiv_{14} 2^{1+1} = 4$.

5.4.1 La ecuación básica $ax \equiv b \mod m$

Nos situamos en el contexto de ser A un DE.

Teorema 5.4.2. *Sea la ecuación $ax \equiv b \mod m$, con $m \neq 0$, y supongamos que $d = (a, m)$.*

1. *La ecuación tiene solución si y solo si $d|b$.*
2. *Si $d|b$, y $a = da'$, $b = db'$ y $m = dm'$, la ecuación es equivalente a la ecuación "reducida"*
$$a'x \equiv b' \mod (m').$$
3. *Si $d|b$, y x_0 es cualquier solución particular, la ecuación original es equivalente a la ecuación*
$$x \equiv x_0 \mod (m').$$
Esto es, la solución general es $x = x_0 + km'$, $k \in A$.
4. *Hay una solución x_0 tal que $x_0 = 0$ o, en otro caso, $\rho(x_0) < \rho(m')$, la que llamaremos "solución óptima".*

Demostración.

1. La ecuación tiene solución si y solo si existe un y tal que $ax - my = b$, ecuación diofántica que tiene solución si y solo si $d|b$.
2. Un x verifica la ecuación si y solo si verifica que $da'x \equiv db' \mod dm'$, lo que se verifica si y solo si $a'x \equiv b' \mod m'$.
3. Como $(a', m') = 1$, podemos encontrar u, v tal que $1 = a'u + m'v$. Entonces $a'u \equiv 1 \mod m'$ y, por tanto, $a'b'u \equiv b' \mod m'$. Luego $x_0 = b'u$ es una solución particular. Si x es cualquier elemento con $x \equiv x_0 \mod m'$, entonces $a'x \equiv a'x_0 \mod m'$ y, por tanto, también $a'x \equiv b' \mod m'$. Y, reciprocamente, si $a'x \equiv b' \mod m'$, entonces $a'x \equiv a'x_0 \mod m'$. Como $(a', m') = 1$, necesariamente será $x \equiv x_0 \mod m'$.
4. Si x_0' es un resto de dividir cualquier solución particular previamente obtenida x_0 entre m', tendremos que $x_0 \equiv x_0' \mod m'$, entonces también que $a'x_0' \equiv b' \mod m'$, donde $x_0' = 0$ o $\rho(x_0') < \rho(m')$.

■

Observación 5.4.1. Si en la ecuación reducida $a'x \equiv b' \mod m'$, existe un c tal que $c|a'$ y $c|b'$, y ponemos $a' = ca''$ y $b' = cb''$, entonces la ecuación se escribe como $ca''x \equiv cb'' \mod m'$ y es equivalente, ya que $(c, m') = 1$, a la ecuación

$$a''x \equiv b'' \mod m'.$$

Ejemplos.

1. Resolver la ecuación en $\mathbb{Z}$: $60x \equiv 90 \mod 105$.

Como $(60, 105) = 5(12, 21) = 15(4, 7) = 15$ y $90 = 15 \cdot 6$, la ecuación tiene solución. Esta resulta equivalente a s "reducida": $4x \equiv 6 \mod 7$. Como $1 = 7 \cdot (-1) + 4 \cdot 2$, resulta que $4 \cdot \equiv 1 \mod (7)$ y entonces $4 \cdot 12 \equiv 6 \mod (7)$. Luego 12 es una solución particular y $12 \equiv 5 \mod 7$, 5 es la óptima. La ecuación original es equivalente a $x \equiv 5 \mod 7$ y la solución general óptima $x = 5 + 7k$, $k \in \mathbb{Z}$.

2. Resolver la ecuación en $\mathbb{Z}$: $1100x \equiv 660 \mod 140$.

La ecuación es equivalente a $110x \equiv 66 \mod 14$; también a $55x \equiv 33 \mod 7$, a $5x \equiv 3 \mod 7$, a $-2x \equiv -4 \mod 7$, y a $x \equiv 2 \mod 7$.

3. Resolver la ecuación en $\mathbb{Z}[\sqrt{2}]$: $(2+\sqrt{2})x \equiv 3-\sqrt{2} \mod 3$.

La tabla

$$\begin{array}{ccc|cc} & 3 & & 1 & 0 \\ & 2+\sqrt{2} & & 0 & 1 \\ 3-\sqrt{2} & -1-\sqrt{2} & & 1 & -3+\sqrt{2} \\ & 0 & & & \end{array},$$

nos indica que $(2+\sqrt{2}, 3) = -1-\sqrt{2}$, que es unidad con $(-1-\sqrt{2})^{-1} = 1-\sqrt{2}$.

De la igualdad $-1-\sqrt{2} = 3\cdot(1)+(2+\sqrt{2})(-3+\sqrt{2})$, obtenemos que $(2+\sqrt{2})(-3+\sqrt{2}) \equiv -1-\sqrt{2} \mod (3)$ y, multiplicando por $1-\sqrt{2}$, que $(2+\sqrt{2})(-5+4\sqrt{2}) \equiv 1 \mod 3$. Entonces, multiplicando por $3-\sqrt{2}$, obtenemos que $(2+\sqrt{2})(-23+17\sqrt{2}) \equiv 3-\sqrt{2} \mod 3$, y una solución particular es $-23+17\sqrt{2}$. Sus resto al dividirlo por 3 es $1-\sqrt{2}$, la ecuación original es equivalente a $x \equiv 1-\sqrt{2} \mod (3)$.

El estudio de estas ecuaciones tiene su repercusión en el estudio de unidades de anillos cocientes de un DE.

Teorema 5.4.3. *Sea A un DE y $m \in A$, no nulo ni unidad.*

1. *Un elemento $\bar{a} \in A/mA$ es una unidad si y solo si $(a, m) = 1$.*
2. *El anillo cociente A/mA es un DI $\Leftrightarrow$ es un cuerpo $\Leftrightarrow$ m es irreducible.*

Demostración.

1. El elemento $\bar{a}$ es una unidad en A/mA si y solo si $\exists x \in A$ tal que $\bar{a}\bar{x} = \bar{1}$; esto es, si y solo si la congruencia $ax \equiv 1 \mod m$ tiene solución, lo que sabemos ocurre si y solo si $(a, m) = 1$. Notemos que, en tal caso, $\bar{a}^{-1} = \bar{x}$, donde $ax \equiv 1 \mod m$.
2. Supongamos que m es irreducible. Si $\bar{a} \in A/mA$ no es nulo, o sea $\bar{a} \neq \bar{0}$, entonces a no es múltiplo de m y es $(a, m) = 1$. Luego $\bar{a} \in U(A/mA)$ por (1). Ya sabemos que si A/mA es cuerpo entonces es un DI. Finalmente, si m no es irreducible, será $m = ab$ en A, donde ninguno es múltiplo de m. Pero entonces, en A/mA $0 = \bar{m} = \bar{a}\bar{b}$ con $\bar{a} \neq \bar{0} \neq \bar{b}$ y, por tanto, A/mA no es DI.

■

Podemos particularizar el Teorema 5.4.3 al caso de DE ya estudiados, recordar que habíamos identificado el anillo de restos módulo n, $\mathbb{Z}_n$ con el anillo cociente $\mathbb{Z}/n\mathbb{Z}$.

Corolario 5.4.4.

(*i*) *$\mathbb{Z}_n$ es un cuerpo $\Leftrightarrow$ n es un irreducible.*

(*ii*) *$K[x]/\langle f\rangle$ es un cuerpo $\Leftrightarrow$ f es un polinomio irreducible.*

(*iii*) *Si $n = -2, -1, 2, 3$ y $\alpha \in \mathbb{Z}[\sqrt{n}]$, entonces $\mathbb{Z}[\sqrt{n}]/\langle\alpha\rangle$ es un cuerpo $\Leftrightarrow$ α es irreducible.*

Observación 5.4.2.

Si $p \geq 2$ es un irreducible de $\mathbb{Z}$ y $f = a_0 + a_1x + \cdot + a_nx^n$, con $a_n \neq 0$ es un irreducible de $\mathbb{Z}_p[x]$, el cuerpo $Z_p[x]/\langle f\rangle$ tiene exactamente p^n elementos, en efecto:

Si $\bar{g} \in \mathbb{Z}_p[x]/\langle f\rangle$, y $r = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ es el resto de dividir g entre f, entonces $\bar{g} = \bar{r}$. Así, toda clase de congruencia en $\mathbb{Z}_p[x]/\langle f\rangle$ está representada por un polinomio de la

forma $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, esto es, de grado menor que n. Dos polinomios de estos no pueden ser congruentes módulo f, pues este tiene grado n. Así que en $\mathbb{Z}_p[x]/\langle f\rangle$ hay tantos elementos distintos como polinomios en $Z_p[x]$ de la forma $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. En total p^n. Se denota a este cuerpo $\mathbb{F}_{p^n}$, y os menciono aquí que en cursos superiores veréis el Teorema de Moore, que asegura que, salvo isomorfismo, *estos son los únicos cuerpos finitos que existen.*

5.4.2 Sistemas de 2 congruencias en un DE

Vamos a estudiar el sistema de congruencias

$$\begin{cases} a_1x \equiv b_1 \mod m_1 \\ a_2x \equiv b_2 \mod m_2 \end{cases}$$

Puesto que cada ecuación ha de tener solución, un tal sistema será siempre equivalente a uno de la forma

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases} \tag{5.1}$$

cuya discusión nos lleva a la siguiente conclusión.

Teorema 5.4.5. *El sistema* (5.1) *tiene solución si y solo si* $a \equiv b \mod (m,n)$.

En tal caso, existe una solución x_0 *tal que, si* $x_0 \neq 0$, *entonces* $\rho(x_0) < \rho([m,n])$, *a la llamamos solución "*óptima*", y la solución general es*

$$x = x_0 + k[m,n] \qquad (k \in A).$$

Esto es, el sistema de ecuaciones original es equivalente a la ecuación

$$x \equiv x_0 \mod [m,n].$$

Demostración. Para que una solución $x = a + tm$ de la primera en (5.1) lo sea también de la segunda será por que $mt \equiv b - a \mod n$; y un tal t existe si y solo si $(m,n)|b-a$. Esto es, si y solo si $a \equiv b \mod (m,n)$. Además, si t_0 es cualquier solución particular de esta última, la solución general de esta será de la forma $t = t_0 + k\frac{n}{(m,n)}$, con $k \in A$. Luego la general del sistema es

$$x = a + tm = a + \Big(t_0 + k\frac{n}{(m,n)}\Big)m = a + t_0m + k[m,n] \qquad (k \in A).$$

En otros términos, el sistema es equivalente a la simple ecuación $x \equiv (a + t_0m) \mod [m,n]$. Si consideremos entonces x_0 el resto de dividir $a + t_0m$, concluimos que, la solución general es

$$x \equiv x_0 \mod [m,n]$$

donde $x_0 = 0$ o $\rho(x_0) < \rho([m,n])$. ■

Ejemplo. Tengo depósitos cuya capacidad no excede de 100 litros. Al llenar 6 de ellos con bidones de 11 litros, me sobraron 8. Al llenar 5 con bidones de 23, me sobraron 15 ¿qué capacidad tienen mis depósitos?.

El sistema a resolver es

$$\begin{cases} 6x \equiv 8 \mod 11 \\ 5x \equiv 15 \mod 23 \end{cases} \sim \begin{cases} x \equiv 5 \mod 11 \\ x \equiv 3 \mod 23 \end{cases}.$$

Buscamos los $x = 5 + 11t$ tales que $5 + 11t \equiv 3 \mod 23$, o sea, tales que $11t \equiv -2 \mod 23$. Multiplicando por 2, está ecuación es equivalente a $-t \equiv -4 \mod 23$, o sea a $t \equiv 4 \mod 23$. Una solución particular es $x_0 = 5 + 44 = 49$ y la general $x \equiv 49 \mod [11,23]$; esto es, $x \equiv 49 \mod (253)$, o $x = 49 + 253k$, $k \in \mathbb{Z}$. Total: 49 litros es la capacidad de mis depósitos.

5.4.3 Sistemas de r congruencias

Para resolver un sistema con $r \geq 3$ ecuaciones

$$\begin{cases} a_1 x \equiv b_1 & \mod m_1 \\ a_2 x \equiv b_2 & \mod m_2 \\ a_3 x \equiv b_3 & \mod m_3 \\ \cdots & \\ a_r x \equiv b_r & \mod m_r \end{cases}$$

procedemos como sigue. Resolvemos primero cada una, y el sistema, si todas tienen solución, se re-escribirá en la forma

$$\begin{cases} x \equiv c_1 & \mod m_1 \\ x \equiv c_2 & \mod m_2 \\ x \equiv c_3 & \mod m_3 \\ \cdots & \\ x \equiv c_r & \mod m_r \end{cases}$$

Resolvemos entonces el sistema formado por las dos primeras. Si tiene solución, este sistema resultará equivalente a una simple ecuación de la forma $x \equiv c \mod m$. Luego el sistema original de r ecuaciones será equivalente al sistema formado por las $r-1$ ecuaciones

$$\begin{cases} x \equiv c & \mod m \\ x \equiv c_3 & \mod m_3 \\ \cdots & \\ x \equiv c_r & \mod m_r \end{cases}$$

y reiteramos el proceso, resolviendo el sistema de las dos primeras, hasta concluir con una sola, que será de la forma $x \equiv d \mod n$, que ya expresará la solución general del sistema inicial: $x = d + kn$, con $k \in A$.

Ejemplo. Determinar los polinomios $f \in \mathbb{Q}[x]$ tales que

1. $gr(f) \leq 3$.
2. $f(1) = 8$,
3. $f(-1) = 2$,
4. El resto de dividir f entre $x^2 + 1$ es $x + 1$.

Recordemos el teorema de Ruffini: Si $f \in K[x]$ y $a \in K$, entonces $f(a)$ es el resto de dividir f entre $x - a$". En efecto, será $f = q(x-a) + r$, donde $r \in K$. Pero entonces $f(a) = r$.

En otras palabras, el Teorema de Ruffini nos dice que $f \equiv f(a) \mod (x-a)$, para cualquier $a \in K$.

Buscamos entonces los polinomios de grado 3 que satisfacen el sistema

$$\begin{cases} f \equiv 8 & \mod (x-1), \\ f \equiv 2 & \mod (x+1) \\ f \equiv x+1 & \mod (x^2+1). \end{cases}$$

Procedemos: $f = 8 + t(x-1)$; $8 + t(x-1) \equiv 2 \mod (x+1)$; $(x-1)t \equiv -6 \mod (x+1)$; De la tabla

$x-1$	1	0
$x+1$	0	1
-2	1	-1
0		

,

obtenemos que $-2 = (x-1) \cdot 1 + (x+1) \cdot (-1)$. Luego $(x-1) \cdot 1 \equiv -2 \mod (x+1)$, y $(x-1) \cdot (-\frac{1}{2}) \equiv 1 \mod (x+1)$. Entonces, $(x-1)(-\frac{1}{2})(-6) \equiv (-6) \mod (x+1)$ y una solución particular es $t_0 = 3$. El sistema formado por las dos primeras ecuaciones es equivalente a la ecuación $f \equiv 8 + 3(x-1) \mod (x^2-1)$; esto es $f \equiv 3x + 5 \mod (x^2-1)$.

La solución general de la última es $f = (x+1) + t(x^2+1)$, y nos planteamos entonces la ecuación

$$(x+1) + t(x^2+1) \equiv 3x + 5 \mod (x^2-1)$$

o, equivalentemente,

$$(x^2+1)t \equiv 2x + 4 \mod (x^2-1).$$

De la tabla

x^2+1	1	0
x^2-1	0	1
2	1	-1
0		

obtenemos $2 = (x^2+1)\cdot 1 + (x^2-1)\cdot(-1)$ y $1 = (x^2+1)\cdot(\frac{1}{2}) + (x^2-1)\cdot(-\frac{1}{2})$. Así que $(x^2+1)\cdot\frac{1}{2} \equiv 1 \mod (x^2-1)$ y $(x^2+1)\cdot(x+2) \equiv 2x+4 \mod (x^2-1)$. Luego una solución particular es $t_0 = x+2$ y $f_0 = (x+1) + (x+2)(x^2+1) = x^3 + 2x^2 + 2x + 3$ es una solución particular al sistema de las dos ecuaciones. El sistema general es entonces equivalente a $f \equiv x^3 + 2x^2 + 2x + 3 + \mod (x^4+1)$. En definitiva, el polinomio buscado es $f = x^3 + 2x^2 + 2x + 3$.

5.5 Complementos sobre $\mathbb{Z}_n$

5.5.1 La ecuación $ax = b$ en $\mathbb{Z}_n$

Sea $n \geq 2$ un entero, y consideremos la ecuación $ax = b$ en el anillo $\mathbb{Z}_n$, donde $a \neq 0$.

El conjunto de sus soluciones será

$$\begin{aligned}\{x \in \mathbb{Z};\ 0 \leq x < n,\ ax = b \text{ en } \mathbb{Z}_n\} &= \{x \in \mathbb{Z};\ 0 \leq x < n,\ \overline{ax} = \bar{b} \text{ en } \mathbb{Z}/n\mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid 0 \leq x < n,\ ax \equiv b \mod n\}\end{aligned}$$

Si $d = (a,n)$ no divide a b, la ecuación no tiene solución.

Supongamos que $d|b$, sabemos que la ecuación $ax \equiv b \mod n$ tiene solución, y más aun, que tiene una solución x_0 óptima, satisfaciendo que $0 \leq x_0 < n' = \frac{n}{d}$. Además todas las soluciones de la congruencia $ax \equiv b \mod n$ son entonces los $x = x_0 + kn'$, con $k \in \mathbb{Z}$. Concluimos entonces

Proposición 5.5.1. *Si $d|b$ hay d diferentes soluciones de la ecuación $ax = b$ en $\mathbb{Z}_n$ que son:*

$$\{x_0, x_0 + n', x_0 + 2n', \ldots, x_0 + (d-1)n'\}.$$

Demostración. Estas son efectivamente soluciones de la congruencia $ax \equiv b \mod (n)$, y para cualquier $0 \leq k < d$, se satisface que $x_0 + kn' < n' + (d-1)n' = dn' = n$. Y no hay más, pues para cualquier $k \in \mathbb{Z}$, si $k < 0$, entonces $x_0 + kn' < 0$; y si $k \geq d$, entonces $x_0 + kn' \geq x_0 + dn' \geq dn' = n$.

Observar también que, si $(a,n) = 1$, la ecuación $ax = 1$ en $\mathbb{Z}_n$ siempre tiene solución, y esta es única es única: $x_0 = a^{-1}$. ■

Ejemplo. *Resolver la ecuación $12x = 18$ en $\mathbb{Z}_{30}$.* Como $(12,30) = 6(2,5) = 6$ y $6/18$, la ecuación tiene 6 soluciones. Para buscarlas consideramos la ecuación $12x \equiv 18 \mod (30)$, que reduce a $2x \equiv 3 \mod (5)$. Fácilmente se ve que $x_0 = 4$ es la solución óptima. Pero podemos llegar a ella aplicando el procedimiento ortodoxo:

5	1	0
2	0	1
1	1	-2

así que $1 = 1 \cdot 5 + 2 \cdot (-2)$, de donde $2 \cdot (-2) \equiv 1 \mod (5)$, o lo que es lo mismo $2 \cdot 3 \equiv 1 \mod (5)$. Entonces $2 \cdot 9 \equiv 3 \mod (5)$ y $2 \cdot 4 \equiv 3 \mod (5)$. Luego $x_0 = 4$ es solución y óptima. El conjunto de todas las soluciones sería

$$\{4 + k5, k = 0, \dots 4\} = \{4, 9, 14, 19, 24, 29\}.$$

5.5.2 La función φ de Euler

Se define como la aplicación

$$\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\},$$

que asigna como imagen de cada numero natural $n \geq 1$ el número natural

$$\varphi(n) = |\{m \mid 1 \leq m \leq n, (m, n) = 1\}|.$$

Como ejemplo, tenemos que

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2, ...$$

y vemos que no sigue una pauta clara. Las siguientes observaciones van dirigidas a mostrar como se puede calcular $\varphi(n)$, para los diferentes n.

En principio, $\varphi(n)$ tiene la siguiente interpretación.

Proposición 5.5.2. *para cada $n \geq 2$,*

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

Demostración. $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid \exists x \in \mathbb{Z}_n \text{ con } ax = 1\} = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$. ■

Lema 5.5.3. *Sea $f : A \cong B$ es un isomorfismo de anillos, entonces la aplicación restringida $f : U(A) \to U(B)$, que asigna a cada unidad a su imagen por f, $f(a)$, es una biyección.*

Demostración. La aplicación $f : U(A) \to U(B)$ es claramente inyectiva. Si $b \in U(B)$, existirán un $a, a' \in A$ tales que $f(a) = b$ y $f(a') = b^{-1}$. Pero entonces $f(aa') = f(a)f(a') = bb^{-1} = 1 = f(1)$, luego $aa' = 1$, pues f es inyectiva. Entonces $a \in U(a)$ y $f(a)) = b$. ■

Si A y B son anillos conmutativos, se define su "*anillo producto*" como el producto cartesiano $A \times B$, con las operaciones

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b)(a', b') = (aa', bb').$$

La verificación de los axiomas es fácil. Su cero es el par $(0, 0)$, y su uno el par $(1, 1)$. El opuesto de un par (a, b) es el par $(-a, -b)$. Además,

Lema 5.5.4. $U(A \times B) = U(A) \times U(B)$.

Demostración. Para cada $(a, b) \in A \times B$, se tiene que

$$\begin{aligned}(a, b) \in U(A \times B) &\Leftrightarrow \exists (a', b') \mid (aa', bb') = (1, 1) \Leftrightarrow a \in U(A) \wedge b \in U(B) \\ &\Leftrightarrow (a, b) \in U(A) \times U(B).\end{aligned}$$

■

Lema 5.5.5 (Teorema Chino del resto)**.**
Si $m, n \geq 2$, son enteros con $(m, n) = 1$, entonces hay un isomorfismo

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

que hace corresponder a cada $k \in \mathbb{Z}_{mn}$ su par de restos $(R_m(k), R_n(k))$ al ser dividido por m y n respectivamente.

Demostración. Sea $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ la aplicación que asigna a cada $x \in \mathbb{Z}$ el par $(R_m(x), R_n(x))$ de sus restos en $\mathbb{Z}_m$ y $\mathbb{Z}_n$ respectivamente. Es fácil ver que R es un homomorfismo de anillos, desde que $R_m : \mathbb{Z} \to \mathbb{Z}_m$ y $R_n : A \to A_n$ lo son.

Veamos que es un epimorfismo:

Para cualquier $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, el sistema de ecuaciones en congruencias en $\mathbb{Z}$

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

tiene solución, pues $(m, n) = 1 | a - b$. Existe por tanto un $x \in A$ satisfaciendo ambas congruencias. Pero entonces $R_m(x) = a$ y $R_n(x) = b$; esto es $f(x) = (a, b)$.

El núcleo de f consiste de todos los $x \in \mathbb{Z}$ tal que $R_m(x) = 0$ y $R_n(x) = 0$, esto es, tales que $x \equiv 0 \mod m$ y $x \equiv 0 \mod m$. En otras palabras, los $x \in \mathbb{Z}$ tales que $m|x$ y $n|x$, que es lo mismo que decir que $[m, n] = mn|x$. Así que $Ker(f) = mn\mathbb{Z}$ es el ideal de los múltiplos de mn. El Primer Teorema de Isomorfía, nos asegura entonces que f induce in isomorfismo

$$\bar{f} : \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}_m \times \mathbb{Z}_n,$$

definido por $\bar{f}(\bar{x}) = f(x) = (R_m(x), R_n(x))$. Componiendo este con el isomorfismo $\mathbb{Z}_{mn} \cong \mathbb{Z}/mn\mathbb{Z}$, que asigna a cada $x \in \mathbb{Z}_{mn}$ su clase de congruencia $\bar{x}$ en $\mathbb{Z}/mn\mathbb{Z}$, obtenemos el isomorfismo buscado $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, que asigna a cada $x \in \mathbb{Z}_{mn}$ el par de restos $(R_m(x), R_n(x))$. ■

Lema 5.5.6. *Si $m, n \geq 2$ son enteros con $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración. Para tales enteros m, n se tiene que
$\varphi(mn) = |U(\mathbb{Z}_{mn}| = |U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| = |U(\mathbb{Z}_m)||U(\mathbb{Z}_n)| = \varphi(m)\varphi(n)$. ■

Lema 5.5.7. *Si $p \geq 2$ es un número irreducible, para cada $e \geq 1$,*

$$\varphi(p^e) = p^e\Big(1 - \frac{1}{p}\Big).$$

Demostración. Para cualquier natural m, si p/m, entonces $p/(p^e, m)$ y, por tanto, $(p^e, m) \neq 1$. En otro caso, si p no divide a m, entonces ninguna potencia de p lo hace. Como os únicos divisores de p^e son, salvo signo, potencias de p, el único divisor común a p^e y m es 1, salvo el signo, y $(p^e, m) = 1$. Por tanto, los naturales m con $1 \leq m \leq p^e$ y $(p^e, m) \neq 1$, son los de la forma kp, con $p = 1 \cdot p \leq kp \leq p^e = p^{e-1}p$, esto es, con $1 \leq k \leq p^{e-1}$. El número de estos es p^{e-1} y, en consecuencia, los naturales m con $1 \leq m \leq p^e$ y $(p^e, m) = 1$ están en número

$$p^e - p^{e-1} = p^{e-1}(p - 1) = p^e\Big(1 - \frac{1}{p}\Big).$$

■

Teorema 5.5.8. *Si $p_1, \cdots, p_r$ son los diferentes irreducibles que dividen al natural $n \geq 2$, entonces*

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big).$$

Demostración. Sea $n = p_1^{e_1}\cdots p_r^{e_r}$, la factorización de n en producto de irreducibles, con $p_i \neq p_j$. Hagamos inducción en r. Si $r = 1$, la fórmula ha sido probada antes. Supuesto $r > 1$, hacemos hipótesis de inducción. Sea $m = p_2^{e_1}\cdots p_r^{e_r}$. Entonces $(p_1^{e_1}, m) = 1$ y, por tanto,

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(m) = p_1^{e_1}\Big(1 - \frac{1}{p_1}\Big)m\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big) = n\Big(1 - \frac{1}{p_1}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big).\square$$

■

Ejemplo.

$$\varphi(10) = 10\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{5}\Big) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4.$$

$$\varphi(36) = 36\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$

Concluimos con la siguiente consecuencia

Teorema 5.5.9 (Fermat)**.** *Sea $n \geq 2$ un entero.*

1. *Para cualquier $a \in \mathbb{Z}$ tal que $(a, n) = 1$, se verifica que $a^{\varphi(n)} \equiv 1 \mod (n)$.*
2. *Si p es irreducible, para cualquier $a \in \mathbb{Z}$ que no es divisible por p se tiene que $a^{p-1} \equiv 1 \mod (p)$ y $a^p \equiv a \mod (p)$.*
3. *Para cualquier $r \in U(\mathbb{Z}_n)$, es decir, tal que $(r, n) = 1$, se verifica que $r^{\varphi(n)} = 1$ en el anillo $\mathbb{Z}_n$. Entonces $r^{-1} = r^{\varphi(n)-1}$.*
4. *Si $n = p$ es irreducible, para cualquier r en el cuerpo $\mathbb{Z}_p$ se tiene que $r^{p-1} = 1$ y $r^p = r$.*

Demostración.

(3) Tenemos que $r \in U(\mathbb{Z}_n)$. Sea $x = \prod_{m\in U(\mathbb{Z}_n)} m$, el producto en $\mathbb{Z}_n$ de todas sus unidades. La aplicación $f : U(\mathbb{Z}_n) \to U(\mathbb{Z}_n)$ tal que $f(m) = rm$, es claramente inyectiva y, entonces, biyectiva. Así que $U(\mathbb{Z}_n) = \{rm, m \in U(\mathbb{Z}_n)\}$. Por tanto

$$x = \prod_{m\in U(\mathbb{Z}_n)} m = \prod_{m\in U(\mathbb{Z}_n)} rm = r^{\varphi(n)} \prod_{m\in U(\mathbb{Z}_n)} m = r^{\varphi(n)}x.$$

Como x es una unidad, eso implica que $r^{\varphi(n)} = 1$.

(1) Consideremos el isomorfismo $\bar{R} : \mathbb{Z}/n \cong \mathbb{Z}_n$, $\bar{a} \mapsto R(a)$. Como $\bar{a} \in U(\mathbb{Z}/n)$, será $R(a) \in U(\mathbb{Z}_n)$. Entonces $R(\overline{a^{\varphi(n)}}) = R(a)^{\varphi(n)} = 1$. Luego $a^{\varphi(n)} \equiv_m 1$.

(2) y (4) son consecuencia directa de (1) y (3).

■

EJEMPLOS.

1. *Calcular* $3^{(3^{100})}$ *en* $\mathbb{Z}_{100}$.

Como $(3, 100) = 1$ y $\varphi(100) = 40$, podemos asegurar que $3^{40} \equiv 1 \mod (100)$. Busquemos el resto de dividir 3^{100} por 40: Como $(3, 40) = 1$ y $\varphi(40) = 16$, tenemos que $3^{16} \equiv 1 \mod (40)$. Como $100 = 10 \cdot 10 \equiv_{16} (-6)(-6) = 36 \equiv_{16} 4$, podemos asegurar que $3^{100} \equiv_{40} 3^4 = 81 \equiv_{40} 1$. Finalmente entonces, $3^{(3^{100})} \equiv_{100} 3^1 = 3$. □

2. *Calcular el resto de dividir* $24^{(47)^{51}}$ *entre* 14.

Puesto que $24 \equiv 10 \mod (14)$, la cuestión es lo mismo que calcular $10^{(47)^{51}}$ en $\mathbb{Z}_{14}$. Notemos que $10^{(47)^{51}} = 5^{(47^{51})}2^{(47^{51})}$, y podemos trabajar con cada factor por separado.

Como $(5, 14) = 1$, y $\varphi(14) = 6$, será $5^6 \cong_{14} 1$. Entonces, Si r es el resto de dividir 47^{51} entre 6, será $5^{(47)^{51}} \equiv_{14} 5^r$. Ahora, $47^{51} \equiv_6 5^{51}$. Ademas, como $(5, 6) = 1$ y $\varphi(6) = 2$, tendremos que $5^2 \equiv_6 1$. Entonces, como $51 \equiv_2 1$, será $5^{51} \equiv_6 5$. Por tanto

$$5^{(47^{51})} \equiv_{14} 5^5 \equiv_{14} (5^2)^2 5 \equiv_{14} (-3)^2 5 \equiv_{14} 9 \cdot 5 \equiv_{>14} (-5)5 \equiv_{14} -25 \equiv_{14} 3.$$

Para calcular el resto de $2^{(47^{51})}$ módulo 14, empezamos las primeras potencias de 2: $2^0 \equiv_{14} 1$, $2^1 \equiv_{14} 2$, $2^3 \equiv_{14} 8$, $2^4 \equiv_{14} 16 \equiv_{14} 2$. Así que $2^1 \equiv_{14} 2^{1+3}$, luego, para cualquier $n \geq 0$, $2^{n+1} \equiv_{14} 2^{r+1}$, si r es el resto de dividir n entre 3. Calculemos entonces el resto de dividir $47^{51} - 1$ entre 3:

$$47^{51} - 1 \equiv_3 11^{51} - 1 \equiv_3 2^{51} - 1 \equiv_3 (-1)^{51} - 1 \equiv_3 -2 \equiv_3 1.$$

Luego, $2^{(47^{51})} \equiv_{14} 2^{1+1} = 4$.

En definitiva, $24^{(47)^{51}} \equiv_{14} 3 \cdot 4 = 12$. □

Ejercicio 1 Resuelve las ecuaciones siguientes

1. $12x = 8$ en el anillo $\mathbb{Z}_{20}$.
2. $19x = 42$ en $\mathbb{Z}_{50}$.
3. $9x = 4$ en $\mathbb{Z}_{1453}$.
4. $5^{30}x = 2$ en $\mathbb{Z}_7$.
5. $20x = 984$ en $\mathbb{Z}_{1984}$.

Ejercicio 2 Determina, si existen, los inversos de

1. 15 en $\mathbb{Z}_{16}$.
2. 9 en $\mathbb{Z}_{20}$.
3. 12 en $\mathbb{Z}_{21}$.
4. 22 en $\mathbb{Z}_{31}$.

Ejercicio 3 Determina cuántas unidades tienen los anillos

1. $\mathbb{Z}_{125}$.
2. $\mathbb{Z}_{72}$.
3. $\mathbb{Z}_{88}$.
4. $\mathbb{Z}_{1000}$.

Ejercicio 4 Determina si la igualdad $a = b$ es cierta en los siguientes casos:

1. $a = 9^{(55^9)}$ y $b = 7^{(70^{55})}$, en el anillo $\mathbb{Z}_{21}$.
2. $a = 2^{(5^{70})}$ y $b = 5^{(70^2)}$, en el anillo $\mathbb{Z}_{21}$.
3. $a = 12^{(55^{70})}$ y $b = 10^{(70^{55})}$, en el anillo $\mathbb{Z}_{22}$.
4. $a = 5^{(5^{70})} \cdot 11^{(5^{70})}$ y $b = 10^{(70^{22})}$, en el anillo $\mathbb{Z}_{22}$.

Ejercicio 5 Determinar los inversos que se proponen (si existen)

1. $\overline{x^2 + x + 1}^{\,-1}$ en el anillo $\mathbb{Z}_3[x]/x^3 + 2x + 1$.
2. $\overline{x + 1}^{\,-1}$ en el anillo $\mathbb{R}[x]/x^3 - 2x - 3$.
3. $\overline{x^2 + x}^{\,-1}$ en el anillo $\mathbb{Z}_2[x]/x^2 + 1$.
4. $\overline{x^3 + x + 1}^{\,-1}$ en el anillo $\mathbb{Z}_2[x]/x^2 + x + 1$.

Ejercicio 5 Determinar los inversos que se proponen (si existen)

1. $\overline{1 + i}^{\,-1}$ en el anillo $\mathbb{Z}[i]/3 + 2i$.
2. $\overline{2 - \sqrt{2}}^{\,-1}$ en el anillo $\mathbb{Z}[\sqrt{2}]/3$.
3. $\overline{3 + 3i\sqrt{2}}^{\,-1}$ en el anillo $\mathbb{Z}[i\sqrt{2}]/4 - 2i\sqrt{2}$.
4. $\overline{1 + \sqrt{3}}^{\,-1}$ en el anillo $\mathbb{Z}[\sqrt{3}]/\sqrt{3}$.