Tema 1: Números enteros

TEORÍA

Índice

En Informática es frecuente el empleo de operaciones y herramientas matemáticas basadas en la divisibilidad de números enteros y en la aritmética modular. En este primer tema estudiaremos los resultados matemáticos más relevantes como introducción a dichas herramientas.

1. Divisibilidad en $\mathbb{Z}$

1.1. Teorema de la división euclídea

Empezamos repasando el resultado básico en el que se apoya la definición de divisibilidad, y algunos de los algoritmos que emplearemos: el teorema de la división euclídea. Veremos dos versiones de este teorema, según realicemos la división restringiéndonos al conjunto de los números naturales o al conjunto de los enteros.

En estos apuntes nos convendrá definir los *números naturales* como los números enteros positivos junto con el cero

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\},$$

mientras que en los *números enteros* añadiríamos a los naturales sus opuestos

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

Teorema 1.1 (**Teorema de la división euclídea en** $\mathbb{N}$)**.** *Dados dos números naturales D y d, con $d \neq 0$, existe un único par de números naturales c y r para el que se cumplan a la vez las dos condiciones siguientes:*

i) $D = d \cdot c + r$,

ii) $0 \leq r < d$.

Definición 1.2. El proceso de cálculo de los valores de c y r del Teorema 1.1 se denomina *división euclídea* (por defecto) del *dividendo* D entre el *divisor* d. Los números naturales c y r se denominan respectivamente *cociente* y *resto* de la división euclídea de D entre d.

Ejemplo 1.3. Al realizar la división euclídea del dividendo $D = 14$ entre el divisor $d = 3$, obtendremos que el cociente es $c = 4$ y que el resto es $r = 2$, porque estos valores son los únicos números naturales que cumplen que $14 = 3 \cdot c + r$ siendo $0 \leq r < 3$.

Teorema 1.4 (**Teorema de la división euclídea en** $\mathbb{Z}$)**.** *Dados dos números enteros D y d, con $d \neq 0$, existe un único par de números enteros c y r para el que se cumplan a la vez las dos condiciones siguientes:*

i) $D = d \cdot c + r$,

ii) $0 \leq r < |d|$.

Ejercicio 1.5. Realizar la división euclídea de D entre d en cada uno de los siguientes casos:

a) $D = -14$, $d = 3$, *b)* $D = 14$, $d = -3$, *c)* $D = -14$, $d = -3$.

Definición 1.6. Dados dos números enteros d y m, diremos que d *divide* a m (o que d es *divisor* de m, o que m es *múltiplo* de d) si existe un $c \in \mathbb{Z}$ tal que

$$m = d \cdot c.$$

Observación 1.7. Si $d \neq 0$, esto es equivalente a que el resto r de la división euclídea de m entre d sea 0.

Ejemplo 1.8. Escribiremos $d|m$ si d divide a m, y $d \nmid m$ en caso contrario:

$$3|12, \qquad 3 \nmid 14, \qquad 3|3, \qquad 3|0, \qquad 0 \nmid 3.$$

Propiedades 1.9. *Para todo $a, b, c, d, \lambda, \mu \in \mathbb{Z}$ se cumple que:*

1) $a|0$,

2) $0 \nmid a$ *si* $a \neq 0$,

3) $a|a$,

4) $(a|b) \wedge (b|c) \Longrightarrow a|c$,

5) $(a|b) \wedge (b|a) \Longrightarrow a = \pm b$,

6) $(d|a) \wedge (d|b) \Longrightarrow d|(\lambda a + \mu b)$.

Notación 1.10. El conjunto de divisores de un número entero m lo denotaremos por

$$\mathrm{Div}(m) := \{d \in \mathbb{Z} \ / \ d|m\}.$$

Ejemplo 1.11. $\mathrm{Div}(4) = \{-4, -2, -1, 1, 2, 4\}$.

Ejercicio 1.12. Construir los conjuntos $\mathrm{Div}(12)$ y $\mathrm{Div}(-12)$.

Propiedades 1.13. *Para cada $m \in \mathbb{Z}$ se cumple que:*

1) $\mathrm{Div}(m) = \mathrm{Div}(-m)$,

2) $\mathrm{Div}(1) = \{1, -1\}$,

3) $\{1, -1, m, -m\} \subseteq \mathrm{Div}(m)$.

1.2. Números primos y factorización de números compuestos

Definición 1.14. Se dice que un número entero m, distinto de 0, 1 y -1, es un número *primo* si sus únicos divisores son 1, -1, m y $-m$. En caso contrario se dice que es *compuesto*.

Ejemplo 1.15. Los veinte primeros números primos positivos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67 y 71.

Observación 1.16. Todo número $m \in \mathbb{Z} - \{-1, 0, 1\}$ tiene al menos cuatro divisores enteros: 1, -1, m y $-m$. Si m es compuesto, entonces poseerá algún divisor a mayores de estos cuatro. Dichos divisores de m distintos de 1, -1, m y $-m$ se denominan *divisores propios* de m.

Ejemplo 1.17. El número 12 es compuesto pues tiene divisores propios, como por ejemplo el 6.

El siguiente resultado nos garantiza que siempre podremos trabajar con números primos tan grandes como queramos, pues el conjunto de números primos es ilimitado.

Teorema 1.18 (Euclides). *El conjunto de los números primos tiene infinitos elementos.*

Demostración (por reducción al absurdo): Supongamos que el conjunto de números primos positivos es finito, y sea $P = \{p_1, \cdots, p_r\}$ dicho conjunto. Consideramos el número natural $n = p_1 \cdot \ldots \cdot p_r + 1$. Se tiene que n es distinto de 1, y que $n \notin P$, pues n es mayor que cualquiera de los elementos de P. Luego n es compuesto, y ha de ser múltiplo de algún número primo $p_i \in P$. Como $p_i | n$ y $p_i | p_1 \cdot \ldots \cdot p_r$, entonces, $p_i | 1$ al ser $1 = n - p_1 \cdot \ldots \cdot p_r$. Pero es absurdo que $p_i | 1$ pues $p_i \neq \pm 1$ al ser p_i primo. Por lo tanto la suposición inicial no puede ser cierta, y han de existir infinitos números primos positivos.

□

La factorización única de enteros que se establece en el siguiente teorema es clave para varios resultados posteriores.

Teorema 1.19 (Teorema fundamental de la aritmética). *Dado un número entero m, distinto de 0, 1 y -1, existe una única factorización de m de la forma*

$$m = (\pm 1) \cdot p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k},$$

donde $p_1, p_2, \cdots, p_k$ son primos positivos tales que $p_1 < p_2 < \cdots < p_k$, y los números $r_1, \cdots, r_k$ son enteros positivos.

Ejemplo 1.20. Consideremos por ejemplo el número $m = 504$. Para obtener su factorización única como producto de primos utilizamos la reglas de divisibilidad entre 2 y 3:

$$\begin{array}{r|l} 504 & 2 \\ 252 & 2 \\ 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

Luego la factorización es $504 = 2^3 \cdot 3^2 \cdot 7$. En este caso el número de factores primos positivos distintos es $k = 3$: éstos son $p_1 = 2$, $p_2 = 3$ y $p_3 = 7$, que aparecen con multiplicidades $r_1 = 3$, $r_2 = 2$ y $r_3 = 1$.

Ejercicio 1.21. Hallar la factorización única como producto de primos de:

a) $m = 2016$, *b)* $m = -504$.

Observación 1.22. Para calcular la factorización de un número m debemos localizar los números primos que dividen a m y el orden de la potencia de ese primo en la factorización. A medida que crece el número de dígitos de m la complejidad que ofrece el problema de factorización de m aumenta en general de forma exponencial. Por otra parte, factorizar enteros negativos no supone mayor dificultad que la de sus opuestos, pues sus factorizaciones únicas son las mismas añadiendo un factor -1 al inicio.

Uno de los resultados más básicos empleados en la factorización en primos de un número compuesto es el siguiente:

Proposición 1.23. *El menor divisor propio positivo de un número natural compuesto m es menor o igual que $\sqrt{m}$.*

Demostración: Sea d el menor divisor propio positivo de m. Existirá un $c \geq d$ tal que $m = d \cdot c$. Luego $m = d \cdot c \geq d \cdot d = d^2$, de donde se obtiene que $\sqrt{m} \geq d$.

□

Ejemplo 1.24. Averigüemos si el número 127 es primo o compuesto. Como $\lfloor \sqrt{127} \rfloor = 11$, en caso de ser el número 127 compuesto, su menor divisor propio sería el 2, el 3, el 5, el 7 o el 11. Como ninguno de estos números divide a 127, deducimos que 127 tiene que ser primo.

Ejercicio 1.25. Teniendo en cuenta que $\lfloor \sqrt{291} \rfloor = 17$ y $\lfloor \sqrt{97} \rfloor = 9$, hallar la factorización única como producto de primos de 291 y de 97.

Si conocemos la factorización de un número como producto de primos, entonces sabremos cuáles son todos sus divisores:

Proposición 1.26. *Si la factorización de un número compuesto m es*

$$m = (\pm 1) \cdot p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$$

entonces los divisores de m son los números de la forma $(\pm 1) \cdot p_1^{j_1} \cdot \ldots \cdot p_k^{j_k}$, con $0 \leq j_i \leq r_i$ para cada i.

Demostración: Se deduce del Teorema Fundamental de la Aritmética: si $a|m$ entonces $m = a \cdot c$ para algún entero c. La factorización única de m se ha de obtener juntando los factores primos de las factorizaciones únicas de a y c. Por tanto si a tiene un factor que sea potencia de primo $p_i^{l_i}$ entonces en la factorización de m también ha de aparecer al menos l_i veces el primo p_i. □

Ejemplo 1.27. Para generar todos los divisores positivos del número $504 = 2^3 \cdot 3^2 \cdot 7$, basta calcular todos los números de la forma $2^a \cdot 3^b \cdot 7^c$ donde $a \in \{0, 1, 2, 3\}$, $b \in \{0, 1, 2\}$ y $c \in \{0, 1\}$. Cada elección nos daría un número distinto pues tendría una factorización en primos distinta. El número total de posibilidades es $4 \times 3 \times 2 = 24$. Luego el número total de divisores, incluyendo los positivos y los negativos, es de 48.

Ejercicio 1.28. Describir los divisores de los siguientes números:

a) $m = 2016$, *b)* $m = -504$.

1.3. Máximo común divisor

Dados dos números enteros a y b, llamamos *máximo común divisor* de a y b al mayor divisor común positivo de ambos. Habitualmente lo denotamos por $\text{mcd}(a, b)$ y lo calculamos como el producto de los factores primos comunes con menor exponente que aparecen en las factorizaciones únicas de a y b.

Ejemplo 1.29. $\text{mcd}(504, 140) = \text{mcd}(2^3 \cdot 3^2 \cdot 7,\ 2^2 \cdot 5 \cdot 7) = 2^2 \cdot 7 = 28$.

Ejercicio 1.30. Calcular:

a) $\text{mcd}(196, -35000)$, *b)* $\text{mcd}(-6, -8)$, *c)* $\text{mcd}(5, 0)$, *d)* $\text{mcd}(5, 1)$.

Observación 1.31. Como todos los números enteros dividen al 0, y no existe un número entero máximo, no se puede definir el $\text{mcd}(0, 0)$.

Propiedades 1.32. *Si a y b son dos números enteros no simultáneamente nulos y $k \in \mathbb{Z} - \{0\}$, entonces:*

1) $\text{mcd}(a, b) = \text{mcd}(b, a)$,

2) $\text{mcd}(a, b) = \text{mcd}(-a, b) = \text{mcd}(a, -b)$,

3) $\text{mcd}(a, 1) = 1$,

4) $\text{mcd}(a, 0) = |a|$,

5) $a|b \Longrightarrow \text{mcd}(a, b) = |a|$,

6) $\text{mcd}(k \cdot a, k \cdot b) = |k| \cdot \text{mcd}(a, b)$.

Ejemplo 1.33. $\text{mcd}(36, 63) = \text{mcd}(9 \cdot 4, 9 \cdot 7) = 9 \cdot \text{mcd}(4, 7) = 9 \cdot 1 = 9$.

Definición 1.34. Cuando el máximo común divisor de dos números enteros es 1 se dice que los números son *primos entre sí.*

Ejemplo 1.35. Los números 4 y 21 son primos entre sí.

1.4. Algoritmo de Euclides

Veremos en esta sección un algoritmo que es computacionalmente eficiente para calcular el máximo común divisor de dos enteros sin tener que factorizarlos. Dicho algoritmo se basa en el siguiente resultado:

Lema 1.36. *Si* $D = d \cdot c + r$ *entonces* $\mathrm{mcd}(D, d) = \mathrm{mcd}(d, r)$.

Demostración: Se deduce de que los divisores comunes de D y d coinciden exactamente con los divisores comunes de d y r, esto es, $\mathrm{Div}(D) \cap \mathrm{Div}(d) = \mathrm{Div}(d) \cap \mathrm{Div}(r)$: Por una parte, $\mathrm{Div}(D) \cap \mathrm{Div}(d) \subseteq \mathrm{Div}(d) \cap \mathrm{Div}(r)$ ya que si un entero k es divisor común de D y d también lo será de r, pues $r = D - d \cdot c$ es diferencia de múltiplos de k. Por otra parte, $\mathrm{Div}(d) \cap \mathrm{Div}(r) \subseteq \mathrm{Div}(D) \cap \mathrm{Div}(d)$ ya que si un entero k es divisor común de d y r también lo será de D, al ser $D = d \cdot c + r$ una suma de múltiplos de k.

□

Ejemplo 1.37. Calculemos el $\mathrm{mcd}(174, 63)$ empleando el Lema 1.36. Como $174 = 63 \cdot 2 + 48$ deducimos que

$$\mathrm{mcd}(174, 63) = \mathrm{mcd}(63, 48).$$

Es decir, hemos reducido el cálculo del $\mathrm{mcd}(174, 63)$ a calcular el mcd más sencillo $\mathrm{mcd}(63, 48)$. Este otro mcd se puede simplificar aplicando de nuevo el Lema 1.36 con la división $63 = 48 \cdot 1 + 15$, con lo que

$$\mathrm{mcd}(63, 48) = \mathrm{mcd}(48, 15).$$

Reiterando este procedimiento, como $48 = 15 \cdot 3 + 3$, deducimos que

$$\mathrm{mcd}(48, 15) = \mathrm{mcd}(15, 3).$$

Reiterando de nuevo, como $15 = 3 \cdot 5 + 0$, deducimos que

$$\mathrm{mcd}(15, 3) = \mathrm{mcd}(3, 0),$$

que es 3. En conclusión, el $\mathrm{mcd}(174, 63) = 3$, que es igual al último resto no nulo obtenido en esta sucesión de divisiones euclídeas.

El procedimiento seguido en este ejemplo se conoce como *algoritmo de Euclides* para el cálculo del mcd. Pasamos a describir con detalle su notación estándar:

Algoritmo de Euclides. *Dados dos enteros positivos* a *y* b*, con* $a > b$*, para calcular el* $\mathrm{mcd}(a, b)$ *llevamos a cabo las siguientes etapas:*

etapa 0) *Definimos* $r_0 := a$.

etapa 1) *Definimos* $r_1 := b$.

etapa i) *Para valores* $i \geq 2$ *se realiza la división euclidea de* r_{i-2} *entre* r_{i-1}*, denotando el cociente y el resto de esta división por* c_i *y* r_i *respectivamente:*

$$r_{i-2} = r_{i-1} \cdot c_i + r_i.$$

Pararemos el algoritmo en la etapa en la que $r_i = 0$. En ese momento concluiremos que $\mathrm{mcd}(a, b) = r_{i-1}$.

Notación 1.38. Habitualmente dispondremos las cuentas realizadas al aplicar el algoritmo de Euclides en una tabla. Por ejemplo, para calcular el $\mathrm{mcd}(174, 63)$ escribiremos:

i	división euclídea	r_i
0		174
1		63
2	$174 = 63 \cdot 2 + 48$	48
3	$63 = 48 \cdot 1 + 15$	15
4	$48 = 15 \cdot 3 + 3$	3
5	$15 = 3 \cdot 5 + 0$	0

Concluimos que el $\mathrm{mcd}(174, 63)$ es igual a 3, que es el último resto r_i no nulo.

Ejercicio 1.39. Emplear el Algoritmo de Euclides para calcular:

a) $\mathrm{mcd}(92, 36)$, *b)* $\mathrm{mcd}(12, -18)$, *c)* $\mathrm{mcd}(-342, 195)$.

El siguiente resultado es una sencilla consecuencia del algortimo de Euclides, que emplearemos más adelante tanto para calcular inversos modulares como para resolver ecuaciones diofánticas.

Teorema 1.40 (Identidad de Bézout). *Dados dos enteros a y b no simultáneamente nulos, existen dos enteros λ y μ tales que* $\lambda \cdot a + \mu \cdot b = \mathrm{mcd}(a, b)$.

Demostración: Se deduce de que en las divisiones del algoritmo de Euclides, cada resto r_i es combinación lineal de los dos anteriores:

$$r_i = r_{i-2} + (-c_i) \cdot r_{i-1}.$$

Mediante la sucesiva sustitución de unas expresiones en otras se puede escribir el último resto no nulo (que es $\mathrm{mcd}(a, b)$) como combinación lineal de los dos primeros (a y b).

□

Ejemplo 1.41. Para expresar el $\mathrm{mcd}(174, 63)$, que es 3, como combinación lineal de 174 y 63 empezamos despejando los restos no nulos del algoritmo de Euclides en las divisiones de cada etapa, en sentido ascendente:

$$3 = 48 + (-3) \cdot 15,$$
$$15 = 63 + (-1) \cdot 48,$$
$$48 = 174 + (-2) \cdot 63.$$

De esta forma conseguimos expresar cada resto como combinación lineal de los dos restos que le preceden. A continuación sustituimos sucesivamente cada una de estas expresiones de los restos en la igualdad del primero hasta tenerlo expresado como combinación lineal de 174 y 63:

$$\begin{array}{rclcl} 3 & = & 48 + (-3) \cdot 15 & = & 48 + (-3) \cdot (63 + (-1) \cdot 48) \\ & = & (-3) \cdot 63 + 4 \cdot 48 & = & (-3) \cdot 63 + 4 \cdot (174 + (-2) \cdot 63) \\ & = & 4 \cdot 174 + (-11) \cdot 63. & & \end{array}$$

En conclusión, el $\mathrm{mcd}(174, 63) = 3$ es igual a $\lambda \cdot 174 + \mu \cdot 63$, siendo $\lambda = 4$ y $\mu = -11$.

Existe la posibilidad de realizar una pequeña modificación al Algoritmo de Euclides para el $\mathrm{mcd}(a,b)$ que nos permitirá calcular directamente los valores de λ y μ de la Identidad de Bézout. Incluso nos permitirá expresar cada uno de los restos del Algoritmo de Euclides como combinación lineal de los valores iniciales a y b.

Algoritmo de Euclides extendido. *Dados dos enteros positivos a y b, con $a > b$, para calcular el $\mathrm{mcd}(a,b)$ y los valores λ y μ de la Identidad de Bézout llevamos a cabo las siguientes etapas:*

etapa 0) *Definimos $r_0 := a$, $\lambda_0 := 1$, $\mu_0 := 0$.*

etapa 1) *Definimos $r_1 := b$, $\lambda_1 := 0$, $\mu_1 := 1$.*

etapa i) *Para valores $i \geq 2$ se calculan c_i y r_i como en el Algoritmo de Euclides:*

$$r_{i-2} = r_{i-1} \cdot c_i + r_i.$$

Además definiremos:

$$\lambda_i := \lambda_{i-2} - c_i \cdot \lambda_{i-1}$$

$$\mu_i := \mu_{i-2} - c_i \cdot \mu_{i-1}$$

Pararemos el algoritmo en la etapa en la que $r_i = 0$. En ese momento concluiremos que $\mathrm{mcd}(a,b) = r_{i-1} = \lambda_{i-1} \cdot a + \mu_{i-1} \cdot b$.

Notación 1.42. También emplearemos el formato de tabla para mostrar las cuentas realizadas al aplicar el algoritmo de Euclides extendido. Por ejemplo, para el $\mathrm{mcd}(174, 63)$ escribiremos:

i	división euclídea	r_i	λ_i	μ_i
0		174	1	0
1		63	0	1
2	$174 = 63 \cdot 2 + 48$	48	1	-2
3	$63 = 48 \cdot 1 + 15$	15	-1	3
4	$48 = 15 \cdot 3 + 3$	3	4	-11
5	$15 = 3 \cdot 5 + 0$	0		

Para cada etapa i se cumple que $r_i = \lambda_i \cdot a + \mu_i \cdot b$. En concreto, en la etapa $i = 4$ obtenemos la Identidad de Bézout del $\mathrm{mcd}(174, 63) = 3$:

$$4 \cdot 174 + (-11) \cdot 63 = 3.$$

Ejercicio 1.43. Emplear el Algoritmo de Euclides extendido para obtener la Identidad de Bézout de los siguientes mcd:

a) $\mathrm{mcd}(92, 36)$, *b)* $\mathrm{mcd}(12, -18)$, *c)* $\mathrm{mcd}(-342, 195)$.

1.5. Resolución de ecuaciones diofánticas lineales

Habitualmente se llama *ecuación diofántica* a toda ecuación polinómica de dos o más variables, con coeficientes y término independiente enteros, y de la que se buscan soluciones enteras.

Ejemplo 1.44. La ecuación $3X - Y^2 = 11$ se entiende que es una ecuación diofántica siempre que aparezca enmarcada en un problema en el que se busquen soluciones enteras suyas.

Definición 1.45. Llamamos *ecuación diofántica lineal* a una ecuación diofántica E de la forma

$$aX + bY = c.$$

Su conjunto de soluciones será

$$\mathrm{Sol}(E) := \{(x, y) \in \mathbb{Z}^2 \ / \ ax + by = c\}.$$

Proposición 1.46. $\mathrm{Sol}(E) \neq \emptyset \iff \mathrm{mcd}(a, b)|c$.

Demostración: Denotemos $d := \mathrm{mcd}(a, b)$.

"$\Longrightarrow$"

Si (x_0, y_0) es una solución entonces $ax_0 + by_0 = c$. Como $d|a$ y $d|b$ entonces d divide a cualquier combinación lineal de a y b, en particular $d|c$.

"$\Longleftarrow$"

Si $d|c$, entonces existe un entero k tal que $c = dk$. Por otro lado por la identidad de Bézout (Teorema 1.40), existen enteros λ y μ tales que $\lambda a + \mu b = d$. Si multiplicamos la igualdad por k se tiene $\lambda ka + \mu kb = dk = c$, luego una solución para la ecuación E es $(x_0, y_0) = (\lambda k, \mu k)$. □

Ejemplo 1.47. La ecuación diofántica lineal $6X + 8Y = 3$ no posee ninguna solución pues $\mathrm{mcd}(6, 8) \nmid 3$.

Ejemplo 1.48. La ecuación diofántica lineal $6X + 8Y = 22$ sí que tiene soluciones pues $\mathrm{mcd}(6, 8)|22$. Además la ecuación es equivalente a $3X + 4Y = 11$, obtenida dividiéndola por el máximo común divisor de los coeficientes $\mathrm{mcd}(6, 8) = 2$. Esta nueva ecuación, en la que los coeficientes son primos entre sí, se suele denominar *ecuación diofántica lineal reducida*.

Observación 1.49. Toda ecuación diofántica lineal que tenga solución se puede escribir de forma equivalente como ecuación diofántica lineal reducida (obtenida dividiéndola por el máximo común divisor de los coeficientes).

Definición 1.50. Llamamos *ecuación diofántica lineal homogénea* a una ecuación diofántica lineal E de la forma

$$aX + bY = 0.$$

Ejemplo 1.51. La ecuación diofántica lineal $3X + 4Y = 0$ es homogénea.

El siguiente resultado es de utilidad para resolver ecuaciones diofánticas lineales homogéneas que sean reducidas:

Lema 1.52 (**Lema de Euclides**). *Sean a, b y c tres números enteros con a y b no simultáneamente nulos. Entonces, si $a|bc$ y $\mathrm{mcd}(a,b)=1$ entonces $a|c$.*

Demostración: Como $\mathrm{mcd}(a,b)=1$, aplicando la identidad de Bézout (Teorema 1.40) deducimos que existen $\lambda,\mu\in\mathbb{Z}$ tales que $1=\lambda a+\mu b$. Si multiplicamos la igualdad por c se tiene $c=\lambda ac+\mu bc$. Como $a|bc$, se tiene que μbc es múltiplo de a, y también lo será $c=\lambda ac+\mu bc$ por ser suma de múltiplos de a.

□

Ejemplo 1.53. Si (x,y) es una solución de la ecuación diofántica lineal homogénea reducida $3X+4Y=0$, entonces $3x=-4y$, y por tanto $4|3x$. Como $\mathrm{mcd}(4,3)=1$, deducimos del Lema de Euclides que $4|x$, es decir $x=4t$ para algún $t\in\mathbb{Z}$. Sustituyendo en $3x=-4y$ obtenemos que $12t=-4y$, esto es $y=-3t$. Además observamos que para todo $t\in\mathbb{Z}$ el par $(x,y)=(4t,-3t)$ es solución de $3X+4Y=0$, ya que

$$3\cdot 4t+4\cdot(-3t)=12t-12t=0.$$

En resumen, si $E\equiv 3X+4Y=0$,

$$\mathrm{Sol}(E)=\{(4t,-3t)\ /\ t\in\mathbb{Z}\}.$$

Proposición 1.54. *Sea $E\equiv aX+bY=0$ una ecuación diofántica lineal homogénea. Si E es reducida, entonces*

$$\mathrm{Sol}(E)=\{(bt,-at)\ /\ t\in\mathbb{Z}\}.$$

El *método lineal* de resolución de ecuaciones diofánticas lineales se basa en el siguiente teorema:

Teorema 1.55 (**Método Lineal**). *Sea $E\equiv aX+bY=c$ una ecuación diofántica lineal, y denotemos por E_h la ecuación diofántica homogénea asociada $E_h\equiv aX+bY=0$. Entonces todas las soluciones de E se pueden obtener a partir de una particular suya, sumándole soluciones de la homogénea E_h.*

Demostración: Sea (x_p,y_p) una solución particular de E. Se cumplirá que $ax_p+by_p=c$. Veamos que para un par $(x,y)\in\mathbb{Z}^2$,

$$(x,y)\text{ es solución de }E\overset{?}{\Longleftrightarrow}(x,y)-(x_p,y_p)\text{ es solución de }E_h:$$

(x,y) es solución de $E\Longleftrightarrow ax+by=c\Longleftrightarrow ax+by=ax_p+by_p\Longleftrightarrow$
$a(x-x_p)+b(y-y_p)=0\Longleftrightarrow(x,y)-(x_p,y_p)$ es solución de E_h.

□

Ejemplo 1.56. Para hallar las soluciones de la ecuación diofántica $6X+8Y=22$ por el método lineal, procederíamos a sumar una solución particular suya con soluciones de su ecuación homogénea asociada $6X+8Y=0$.

Para calcular una solución particular de $6X+8Y=22$ podemos hallar la identidad de Bézout para el $\mathrm{mcd}(6,8)$ usando el Algoritmo de Euclides que es $6\cdot(-1)+8\cdot 1=2$, de donde $6\cdot(-11)+8\cdot 11=22$. Luego una solución particular de $6X+8Y=22$ es

$$(x_p,y_p)=(-11,11).$$

Por otra parte, las soluciones de la ecuación homogénea $6X + 8Y = 0$, coincidirán con las de su ecuación reducida $3X + 4Y = 0$, halladas en el Ejemplo 1.53:

$$(x_h, y_h) = (4t, -3t), \text{ con } t \in \mathbb{Z}.$$

Cada solución de $E \equiv 6X + 8Y = 22$ se obtiene como suma de la solución particular (x_p, y_p) con una de las soluciones (x_h, y_h) de la ecuación homogénea:

$$\text{Sol}(E) = \{(-11 + 4t, 11 - 3t) \ / \ t \in \mathbb{Z}\}.$$

Ejercicio 1.57. Emplear el método lineal para hallar las soluciones de la ecuación diofántica $92X + 36Y = 8$.

2. Aritmética modular

A lo largo de esta sección, m denotará un numero entero fijado, $m \geq 2$, llamado *módulo*.

2.1. Números enteros modulares

Definición 2.1. Dados $a, b \in \mathbb{Z}$, diremos que a *es congruente con* b *módulo* m si $m|(a - b)$.

Notación 2.2. Si a es congruente con b módulo m escribiremos $a \equiv b \,(\text{mod } m)$.

Ejemplo 2.3. Ejemplos de congruencias:

$$16 \equiv 4 \,(\text{mod } 12), \qquad 127 \equiv 67 \,(\text{mod } 10), \qquad 48 \equiv 48 \,(\text{mod } 21).$$
$$18 \equiv 0 \,(\text{mod } 9), \qquad -5 \equiv 37 \,(\text{mod } 2),$$

Propiedades 2.4. *Para todo* $a, b, c \in \mathbb{Z}$ *se cumplen las siguientes propiedades:*

reflexiva) $a \equiv a \,(\text{mod } m)$,

simétrica) $[a \equiv b \,(\text{mod } m)] \Longrightarrow [b \equiv a \,(\text{mod } m)]$,

transitiva) $[a \equiv b \,(\text{mod } m)] \wedge [b \equiv c \,(\text{mod } m)] \Longrightarrow [a \equiv c \,(\text{mod } m)]$.

Proposición 2.5. *La relación de congruencia módulo* m *es una relación de equivalencia sobre el conjunto* $\mathbb{Z}$.

Notación 2.6. Dada una relación de equivalencia R sobre un conjunto A, para cada elemento de $a \in A$ se define su *clase de equivalencia* como el conjunto de elementos con los que está relacionado:

$$\overline{a} := \{b \in A \ / \ aRb\}.$$

Otra notación habitual para la clase de equivalencia de a es $[a]$.
Al conjunto $\{\overline{a} \ / \ a \in A\}$ de clases de equivalencia formadas bajo una relación se le suele llamar *conjunto cociente*.

Ejemplo 2.7. Para $m = 3$ tendremos una relación de equivalencia "$\equiv \pmod 3$" sobre el conjunto $\mathbb{Z}$ denominada *relación de congruencia módulo* 3, y definida por:

$$[a \equiv b \,(\mathrm{mod}\ 3)] \ :\Longleftrightarrow 3|(a-b),$$

para elementos $a, b \in \mathbb{Z}$. En la relación de congruencia, las clases de equivalencia suelen llamarse *clases de congruencia*. Por ejemplo, para $m = 3$, las clases de congruencia serían de este tipo:

$$\overline{a} = \{b \in \mathbb{Z} \ / \ a \equiv b \,(\mathrm{mod}\ 3)\} = a + 3\mathbb{Z},$$

donde $3\mathbb{Z}$ denota el conjunto de múltiplos de 3. En este caso habrá en total 3 clases de congruencia distintas:

$$\overline{0} = 3\mathbb{Z} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\},$$

$$\overline{1} = 1 + 3\mathbb{Z} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\},$$
$$\overline{2} = 2 + 3\mathbb{Z} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}.$$

Observación 2.8. En general hay m clases de congruencia módulo m distintas. Se suelen considerar los números 0, 1, 2, $\cdots$, $m-1$ como representantes de cada una de ellas:

$$\overline{0} = m\mathbb{Z}, \qquad \overline{1} = 1 + m\mathbb{Z}, \qquad \overline{2} = 2 + m\mathbb{Z}, \qquad \cdots \qquad \overline{m-1} = (m-1) + m\mathbb{Z}.$$

Notación 2.9. Denotaremos el conjunto cociente para la relación de congruencia módulo m por $\mathbb{Z}_m$:

$$\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}.$$

Otras notaciones habituales para el conjunto $\mathbb{Z}_m$ son $\mathbb{Z}/_{m\mathbb{Z}}$, o también $\mathbb{Z}/_{(m)}$.

Ejemplo 2.10. El conjunto cociente para la relación de congruencia módulo 7 es:

$$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{6}\},$$

donde $\overline{0} = 7\mathbb{Z}$, $\overline{1} = 1 + 7\mathbb{Z}$, $\overline{2} = 2 + 7\mathbb{Z}$, $\cdots$, $\overline{6} = 6 + 7\mathbb{Z}$.

Observación 2.11. En las relaciones de equivalencia se cumple que si dos elementos están relacionados, entonces sus clases de equivalencia son iguales. Por tanto, si $a \equiv b \,(\mathrm{mod}\ m)$ entonces $\overline{a} = \overline{b}$ en $\mathbb{Z}_m$.

Por ejemplo, como $11 \equiv 2 \,(\mathrm{mod}\ 3)$ entonces $\overline{11} = \overline{2}$.

Cualquier elemento b de una clase de equivalencia $\overline{a}$ se dice que es un *representante* de $\overline{a}$. Un representante de la clase $\overline{2}$ sería por ejemplo el 11, ya que $11 \in \overline{2}$, o lo que es lo mismo $\overline{11} = \overline{2}$.

El siguiente resultado nos proporciona un método sencillo para encontrar el representante comprendido entre 0 y $m-1$ de una clase de congruencia módulo m dada. Dicho método consiste simplemente en calcular el resto de la división por m de un representante D cualquiera de la clase. Dicho resto se suele denominar el *resto módulo m de D*.

Lema 2.12. *Si $D = d \cdot c + r$ entonces $D \equiv r \,(\mathrm{mod}\ d)$. Por tanto $\overline{D} = \overline{r}$ en $\mathbb{Z}_d$.*

Demostración: Se deduce de que $d|d \cdot c$ y $d \cdot c = D - r$.

□

Ejemplo 2.13. Si queremos hallar el representante comprendido entre 0 y 2 de la clase $\overline{94}$ módulo 3 (i.e. el resto módulo 3 de 94), habremos de calcular el resto de dividir 94 entre 3:

$$94 = 3 \cdot 31 + 1.$$

Concluimos que al ser $94 \equiv 1 \,(\mathrm{mod}\ 3)$, se cumple que $\overline{94} = \overline{1}$ en $\mathbb{Z}_3$ y por tanto ese representante buscado de $\overline{94}$ es el 1.

En $\mathbb{Z}_m$ podemos caracterizar los elementos de la misma clase usando restos de la división euclídea entre m:

Proposición 2.14. *$a \equiv b \,(\mathrm{mod}\ m)$ si y sólo si los restos módulo m de a y b coinciden.*

Demostración: Denotemos por r_a y r_b los restos de dividir a y b entre m, respectivamente. Del Lema 2.12, deducimos que $\overline{a} = \overline{r_a}$ y $\overline{b} = \overline{r_b}$ en $\mathbb{Z}_m$. Probaremos que

$$[\overline{a} = \overline{b}] \overset{?}{\Longleftrightarrow} [r_a = r_b]$$

"$\Longrightarrow$"

Si $\overline{a} = \overline{b}$, entonces $\overline{r_a} = \overline{a} = \overline{b} = \overline{r_b}$. Como $0 \leq r_a, r_b \leq m - 1$, y cualquier clase de congruencia sólo tiene un posible representante que este comprendido entre 0 y $m - 1$, deducimos que los representantes r_a y r_b de las clases $\overline{r_a} = \overline{r_b}$ han de ser iguales.

"$\Longleftarrow$"

Si $r_a = r_b$ entonces $\overline{r_a} = \overline{r_b}$, y $\overline{a} = \overline{r_a} = \overline{r_b} = \overline{b}$.

□

Ejemplo 2.15. ¿Es cierto que $\overline{84} = \overline{57}$ en $\mathbb{Z}_3$?

Claramente 84 y 57 son ambos múltiplos de 3, y al dividirlos por 3 el resto será 0 en ambos casos. Luego $84 \equiv 57 \,(\mathrm{mod}\ 3)$, y por tanto $\overline{84} = \overline{57}$ en $\mathbb{Z}_3$.

Ejercicio 2.16. ¿Es cierto que los restos de dividir 2016 y 2002 entre 7 coinciden?

2.2. Estructura de anillo

Definición 2.17. Un *anillo* $(A, +, \cdot)$ es un conjunto A con al menos dos elementos $0 \in A$ y $1 \in A$, junto con dos operaciones $+ : A \times A \Rightarrow A$ (*suma*) y $\cdot : A \times A \Rightarrow A$ (*producto*), cumpliendo para cada $x, y, z \in A$ las siguientes propiedades:

A1) *Asociativa* de la suma: $(x + y) + z = x + (y + z)$.

A2) 0 es el *elemento neutro* de la suma: $x + 0 = x, \quad 0 + x = x$.

A3) Cada $x \in A$ posee un *elemento opuesto* $-x$ para la suma: $x + (-x) = 0, \quad (-x) + x = 0$.

A4) *Conmutativa* de la suma: $x + y = y + x$.

A5) *Asociativa* del producto: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

A6) 1 es el *elemento neutro* del producto: $x \cdot 1 = x, \quad 1 \cdot x = x$.

A7) *Distributiva*: $x \cdot (y + z) = (x \cdot y) + (x \cdot z), \quad (y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

Definición 2.18. Un anillo $(A, +, \cdot)$ se dice que es *conmutativo* si además cumple para cada $x, y \in A$ la siguiente propiedad:

A8) *Conmutativa* del producto: $x \cdot y = y \cdot x$.

Ejemplo 2.19. Son ejemplos de anillo conmutativo:

$$(\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot).$$

La siguiente propiedad de la relación de congruencia nos permitirá definir una estructura de anillo en $\mathbb{Z}_m$.

Propiedades 2.20. *Si* $a_1 \equiv b_1 \pmod m$ *y* $a_2 \equiv b_2 \pmod m$*, entonces:*

1) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$,

2) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$.

Demostración: Como $m|(a_1 - b_1)$ y $m|(a_2 - b_2)$ también:

1) m divide a la suma $(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$, y

2) m divide a $a_1 \cdot a_2 - b_1 \cdot b_2$, ya que $a_1 \cdot a_2 - b_1 \cdot b_2 = a_1 \cdot a_2 - b_1 \cdot b_2 + (b_1 \cdot a_2 - b_1 \cdot a_2) = (a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2)$, que es suma de múltiplos de m.

Observación 2.21. En el conjunto $\mathbb{Z}_m$ se pueden definir las siguientes operaciones:

$$\begin{array}{rcl} + : \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a+b} \end{array} \qquad \begin{array}{rcl} \cdot : \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{ab} \end{array}$$

Estas operaciones están bien definidas: las Propiedades 2.20 nos garantizan que la suma y producto de clases no dependen de los representantes de las clases escogidos.

Ejemplo 2.22. ¿Cuánto vale $\overline{5} \cdot \overline{3} + \overline{7}^2 \cdot \overline{6}$ en $\mathbb{Z}_{11}$? Para facilitar las cuentas, tras cada operación expresamos cada clase usando un representante comprendido entre 0 y 10:

$$\overline{5} \cdot \overline{3} + \overline{7}^2 \cdot \overline{6} = \overline{15} + \overline{49} \cdot \overline{6} = \overline{4} + \overline{5} \cdot \overline{6} = \overline{4} + \overline{30} = \overline{4} + \overline{8} = \overline{12} = \overline{1}.$$

Proposición 2.23. $(\mathbb{Z}_m, +, \cdot)$ *es un anillo conmutativo.*

Demostración: (Ejercicio) Los elementos neutros de suma y producto son el $\overline{0}$ y el $\overline{1}$ respectivamente. El elemento opuesto de un elemento $\overline{a} \in \mathbb{Z}_m$ es el elemento $\overline{-a} \in \mathbb{Z}_m$.

Ejemplo 2.24. Las tablas de sumar y multiplicar en $\mathbb{Z}_4$ son:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Obsérvese que los elementos neutros de suma y producto son el $\overline{0}$ y el $\overline{1}$ respectivamente, y que los opuestos de $\overline{0}$, $\overline{1}$, $\overline{2}$ y $\overline{3}$ son respectivamente $\overline{-0} = \overline{0}$, $\overline{-1} = \overline{3}$, $\overline{-2} = \overline{2}$ y $\overline{-3} = \overline{1}$.

2.3. Estructura de cuerpo

Algunos anillos tienen a mayores una estructura algebraica de *cuerpo*, dependiendo de si sus elementos no nulos tienen elemento inverso para el producto, o no.

Definición 2.25. Sea $(A, +, \cdot)$ un anillo, y $a \in A$. Se dice que a es una *unidad* de A si a tiene *elemento inverso* para el producto, esto es, existe un elemento $a^{-1} \in A$ tal que

$$a \cdot a^{-1} = 1, \qquad a^{-1} \cdot a = 1$$

Notación 2.26. Denotaremos por A^* el conjunto de unidades de un anillo A.

Ejemplo 2.27. $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{\overline{0}\}$, ya que:

- el $\overline{1}$ es unidad, siendo $\overline{1}^{-1} = \overline{1}$, porque $\overline{1} \cdot \overline{1} = \overline{1}$,
- el $\overline{2}$ es unidad, siendo $\overline{2}^{-1} = \overline{3}$, porque $\overline{2} \cdot \overline{3} = \overline{1}$ y $\overline{3} \cdot \overline{2} = \overline{1}$,
- el $\overline{3}$ es unidad, siendo $\overline{3}^{-1} = \overline{2}$, porque $\overline{3} \cdot \overline{2} = \overline{1}$ y $\overline{2} \cdot \overline{3} = \overline{1}$,
- el $\overline{4}$ es unidad, siendo $\overline{4}^{-1} = \overline{4}$, porque $\overline{4} \cdot \overline{4} = \overline{1}$.

Proposición 2.28. *Si $(A, +, \cdot)$ es un anillo se cumple que:*

1) Si a es unidad, entonces sólo posee un elemento inverso a^{-1},

2) Si a es unidad, entonces a^{-1} también lo es, y $(a^{-1})^{-1} = a$,

3) 1 es unidad, pero 0 no lo es.

Ejercicio 2.29. ¿Cuáles son las unidades de $\mathbb{Z}_4$?

Proposición 2.30. *Para un $a \in \mathbb{Z}_m$ se cumple:*

$$\overline{a} \text{ es una unidad } \Longleftrightarrow \operatorname{mcd}(a, m) = 1.$$

Además, en este caso, si $\lambda a + \mu m = 1$ entonces $\overline{a}^{-1} = \overline{\lambda}$.

Demostración:

"$\Longrightarrow$"

Si $\overline{a}^{-1} = \overline{b}$, entonces $\overline{a} \cdot \overline{b} - \overline{1} = \overline{0}$, luego $m|(a \cdot b - 1)$. Por tanto existe $c \in \mathbb{Z}$ tal que $a \cdot b - 1 = c \cdot m$. De ahí que si k es divisor común de a y de m lo es también de $1 = a \cdot b - c \cdot m$, luego $\operatorname{mcd}(a, m) = 1$.

"$\Longleftarrow$"

Si $\operatorname{mcd}(a, m) = 1$, entonces por la identidad de Bézout (Teorema 1.40) existen $\lambda, \mu \in \mathbb{Z}$ tales que $\lambda a + \mu m = 1$. Luego $m|(\lambda a - 1)$ y $\overline{\lambda a - 1} = \overline{0}$. Por tanto $\overline{a} \cdot \overline{\lambda} = \overline{\lambda} \cdot \overline{a} = \overline{1}$ y $\overline{a}^{-1} = \overline{\lambda}$. □

Ejemplo 2.31. Son unidades de $\mathbb{Z}_8$ aquellos $\overline{a} \in \mathbb{Z}_8$ tales que $\operatorname{mcd}(a, 8) = 1$, esto es, $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. No serían unidades el $\overline{0}$, el $\overline{2}$, el $\overline{4}$ y el $\overline{6}$.

Ejemplo 2.32. ¿Es $\overline{24} \in \mathbb{Z}_{35}$ una unidad? ¿En tal caso cuál es su inverso?

Aplicando el algoritmo de Euclides extendido para el mcd$(35, 24)$:

i	división	r_i	λ_i	μ_i
0		35	1	0
1		24	0	1
2	$35 = 24 \cdot 1 + 11$	11	1	-1
3	$24 = 11 \cdot 2 + 2$	2	-2	3
4	$11 = 2 \cdot 5 + 1$	1	11	-16
5	$2 = 1 \cdot 2 + 0$	0		

deducimos que el mcd$(35, 24) = 1$, y por tanto $\overline{24}$ es una unidad en $\mathbb{Z}_{35}$.

Para calcular $\overline{24}^{-1}$ realizamos los siguientes pasos: en la identidad de Bézout

$$1 = 11 \cdot 35 + (-16) \cdot 24,$$

tomamos clases en $\mathbb{Z}_{35}$

$$\overline{1} = \overline{11} \cdot \overline{35} + \overline{-16} \cdot \overline{24},$$

con representantes entre $\overline{0}$ y $\overline{34}$

$$\overline{1} = \overline{11} \cdot \overline{0} + \overline{19} \cdot \overline{24},$$

de ahí que

$$\overline{1} = \overline{19} \cdot \overline{24},$$

y $\overline{24}^{-1} = \overline{19}$.

Definición 2.33. Sea $(A, +, \cdot)$ un anillo conmutativo. Se dice que $(A, +, \cdot)$ es un *cuerpo* si todos sus elementos distintos de 0 son unidades de A.

Ejemplo 2.34. Son ejemplos de cuerpo:

$$(\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot).$$

Sin embargo $(\mathbb{Z}, +, \cdot)$ no es un cuerpo, pues sus únicas unidades son el 1 y el -1.

Proposición 2.35. $(\mathbb{Z}_m, +, \cdot)$ *es un cuerpo si y sólo si* m *es primo.*

Demostración: $\mathbb{Z}_m$ es cuerpo si, y sólo si, todo elemento no nulo tiene inverso, es decir, mcd$(a, m) = 1$ para todo $a \in \{1, \cdots, m-1\}$. Esto es equivalente a que m no tenga ningún divisor positivo salvo 1 y m.

□

Ejemplo 2.36. $(\mathbb{Z}_2, +, \cdot)$, $(\mathbb{Z}_3, +, \cdot)$ y $(\mathbb{Z}_5, +, \cdot)$ son cuerpos.

Sin embargo no lo es $(\mathbb{Z}_{35}, +, \cdot)$, ya que por ejemplo $\overline{7}$ no es unidad por ser mcd$(7, 35) \neq 1$.

2.4. Resolución de ecuaciones en congruencias

Las ecuaciones en congruencias son ecuaciones el símbolo de igualdad se sustituye por el de congruencia módulo m. Estudiaremos la resolución de congruencias lineales $aX \equiv b\,(\mathrm{mod}\ m)$, que en general se pueden resolver de dos formas: una traduciéndola a ecuación diofántica lineal ($aX - b = mY$) y otra traduciéndola a ecuación lineal ($\overline{a}\overline{X} = \overline{b}$) en $\mathbb{Z}_m$.

Observación 2.37. De la Proposición 1.46 deducimos que la ecuación $aX \equiv b\,(\mathrm{mod}\ m)$ tiene solución exactamente cuando $\mathrm{mcd}(a, m)|b$.

Ejemplo 2.38. La ecuación $2X \equiv 1\,(\mathrm{mod}\ 6)$ no tiene solución, pues $\mathrm{mcd}(2, 6) = 2 \nmid 1$.

Ejemplo 2.39. La ecuación $4X \equiv 2\,(\mathrm{mod}\ 6)$ sí que tiene solución, pues $\mathrm{mcd}(4, 6) = 2|2$.

Observación 2.40. En el caso en que la ecuación $aX \equiv b\,(\mathrm{mod}\ m)$ tiene solución, si además se cumple que $\mathrm{mcd}(a, m) = 1$, entonces $\overline{a}$ es unidad de $\mathbb{Z}_m$. Esto facilita la resolución de la congruencia si la traducimos a la ecuación $\overline{a}\overline{X} = \overline{b}$ en el anillo $\mathbb{Z}_m$ ya que entonces $\overline{a}^{-1} \cdot \overline{a}\overline{X} = \overline{a}^{-1} \cdot \overline{b}$, y

$$\overline{X} = \overline{a}^{-1} \cdot \overline{b}.$$

Ejemplo 2.41. La ecuación $24X \equiv 7\,(\mathrm{mod}\ 35)$ tiene solución, ya que $\mathrm{mcd}(24, 35) = 1|7$. Como sabemos además que $\overline{24}^{-1} = \overline{19}$ en $\mathbb{Z}_{35}$ (Ejemplo 2.32), nos convendrá traducir la congruencia a la ecuación lineal $\overline{24} \cdot \overline{X} = \overline{7}$ en el anillo $\mathbb{Z}_{35}$, ya que entonces:

$$\overline{X} = \overline{24}^{-1} \cdot \overline{7} = \overline{19} \cdot \overline{7} = \overline{133} = \overline{28}.$$

Luego las soluciones de la congruencia $24X \equiv 7\,(\mathrm{mod}\ 35)$ se corresponderán con aquellos enteros X que pertenezcan a la clase de congruencia $\overline{28}$ de $\mathbb{Z}_{35}$. Es decir, son los elementos del conjunto

$$\{28 + 35z \ /\ z \in \mathbb{Z}\}.$$

Observación 2.42. Si la ecuación $aX \equiv b\,(\mathrm{mod}\ m)$ tiene solución pero $\overline{a}$ no es unidad de $\mathbb{Z}_m$, lo adecuado será traducir la congruencia a ecuación diofántica lineal $aX - b = mY$ con el objetivo de reducirla.

Ejemplo 2.43. Hallemos las soluciones de la congruencia $4X \equiv 2\,(\mathrm{mod}\ 6)$. En este caso $\overline{4}$ no es unidad de $\mathbb{Z}_6$, por lo que no es posible despejar $\overline{X}$ en la ecuación $\overline{4} \cdot \overline{X} = \overline{2}$ de $\mathbb{Z}_6$. Sin embargo, si traducimos la congruencia a ecuación diofántica lineal $4X - 2 = 6Y$, ésta la podemos reducir a $2X - 1 = 3Y$, que reinterpretada como congruencia sería

$$2X \equiv 1\,(\mathrm{mod}\ 3),$$

que se puede resolver fácilmente entendida como la ecuación $\overline{2} \cdot \overline{X} = \overline{1}$ en $\mathbb{Z}_3$, ya que $\overline{2}^{-1} = \overline{2}$ en $\mathbb{Z}_3$. Por tanto

$$\overline{X} = \overline{2}^{-1} \cdot \overline{1} = \overline{2} \cdot \overline{1} = \overline{2}.$$

Luego las soluciones de la congruencia $4X \equiv 2\,(\mathrm{mod}\ 6)$ se corresponderán con aquellos enteros X que pertenezcan a la clase de congruencia $\overline{2}$ de $\mathbb{Z}_3$. Es decir, son los elementos del conjunto

$$\{2 + 3z \ /\ z \in \mathbb{Z}\}.$$

Veamos ahora un método específico para resolver, bajo ciertas condiciones, sistemas de ecuaciones en congruencias lineales.

Teorema 2.44 (**Teorema chino del resto**). *Sean $m_1, \cdots, m_r$ números enteros mayores o iguales a 2, que son primos entre sí tomados de dos en dos. El sistema*

$$\begin{cases} X \equiv a_1 \,(\mathrm{mod}\, m_1) \\ X \equiv a_2 \,(\mathrm{mod}\, m_2) \\ \quad \vdots \\ X \equiv a_r \,(\mathrm{mod}\, m_r) \end{cases}$$

tiene una única solución módulo m: los enteros X tales que $X \equiv a \,(\mathrm{mod}\, m)$, donde

- $m = m_1 \cdot \ldots \cdot m_r$,
- $M_k = \dfrac{m}{m_k}$,
- $\overline{y_k} = \overline{M_k}^{-1}$ *en* $\mathbb{Z}_{m_k}$,
- $a = a_1 M_1 y_1 + \ldots + a_r M_r y_r$.

Ejemplo 2.45. Supongamos que queremos resolver el sistema

$$\begin{cases} X \equiv 2 \,(\mathrm{mod}\, 3) \\ X \equiv 3 \,(\mathrm{mod}\, 5) \\ X \equiv 2 \,(\mathrm{mod}\, 7) \end{cases}$$

Estamos en las condiciones del Teorema chino del resto, pues los modulos de las congruencias $m_1 = 3$, $m_2 = 5$ y $m_3 = 7$ son primos entre sí dos a dos.

Calculamos los valores de m, M_k, y_k y a:

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$,
$M_1 = \dfrac{m}{m_1} = 35$, $M_2 = \dfrac{m}{m_2} = 21$ y $M_3 = \dfrac{m}{m_3} = 15$,
$\overline{y_1} = \overline{M_1}^{-1} = \overline{35}^{-1} = \overline{2}^{-1} = \overline{2}$ en $\mathbb{Z}_{m_1} = \mathbb{Z}_3$,
$\overline{y_2} = \overline{M_2}^{-1} = \overline{21}^{-1} = \overline{1}^{-1} = \overline{1}$ en $\mathbb{Z}_{m_2} = \mathbb{Z}_5$,
$\overline{y_3} = \overline{M_3}^{-1} = \overline{15}^{-1} = \overline{1}^{-1} = \overline{1}$ en $\mathbb{Z}_{m_3} = \mathbb{Z}_7$,
$a = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$.

A menudo expresamos estas cuentas en formato tabla:

m_k	3	5	7	$m = 105$
a_k	2	3	2	
M_k	35	21	15	
y_k	2	1	1	
$a_k M_k y_k$	140	63	30	$a = 233$

Las soluciones serán valores de X tales que

$$X \equiv 233 \,(\mathrm{mod}\, 105).$$

Como $233 \equiv 23 \,(\mathrm{mod}\, 105)$, el conjunto de soluciones es $\{23 + 105t \;/\; t \in \mathbb{Z}\}$.

2.5. Restos potenciales modulares

Definición 2.46. Sea $a \in \mathbb{Z}$. Llamamos *sucesión de restos potenciales de a módulo m* a una sucesión de enteros $\{y_0, y_1, y_2, \cdots\}$ todos ellos comprendidos entre 0 y $m-1$, tales que y_k es el resto módulo m de a^k:

$$y_k \equiv a^k \,(\text{mod } m).$$

Observación 2.47. Básicamente, con la sucesión de restos potenciales de a módulo m estamos calculando los representantes entre 0 y $m-1$ de cada potencia $\overline{a}^k$ en $\mathbb{Z}_m$. Esta sucesión siempre empezará con $y_0 = 1$, ya que $\overline{a}^0 = \overline{1}$. Además, como los elementos de la sucesión pertenecen a un conjunto finito $\{0, 1, 2, \cdots, m-1\}$, en ella siempre va a haber repeticiones. Tras la primera repetición, los siguientes elementos se repiten de forma cíclica: si dos potencias $\overline{a}^k = \overline{a}^r$ son iguales, entonces las siguientes también lo son:

$$\overline{a}^{k+j} = \overline{a}^k \cdot \overline{a}^j = \overline{a}^r \cdot \overline{a}^j = \overline{a}^{r+j}.$$

Ejemplo 2.48. Calculemos la sucesión de restos potenciales de 10 módulo 7. Como $10 \equiv 3 \,(\text{mod } 7)$, podemos reducir el problema a calcular los restos potenciales de 3 módulo 7, ya que $10^k \equiv 3^k \,(\text{mod } 7)$. Se tiene que:

$$\begin{array}{ll} 3^0 \equiv 1 \,(\text{mod } 7), & 3^4 \equiv 4 \,(\text{mod } 7), \\ 3^1 \equiv 3 \,(\text{mod } 7), & 3^5 \equiv 5 \,(\text{mod } 7), \\ 3^2 \equiv 2 \,(\text{mod } 7), & 3^6 \equiv 1 \,(\text{mod } 7), \\ 3^3 \equiv 6 \,(\text{mod } 7), & \end{array}$$

luego la secuencia de restos es $\{1, 3, 2, 6, 4, 5, 1, 3, 2, \cdots\}$.

Ejercicio 2.49. Calcular las sucesiones de restos potenciales siguientes:

a) de 2 módulo 5, *b*) de 2 módulo 12, *c*) de 6 módulo 12.

Existen algunas potencias cuya obtención no requiere ningún cálculo, son conocidas a priori. Son potencias cuyo exponente está relacionado con la *función φ de Euler* definida a continuación:

Definición 2.50. Se define $\varphi(m)$ como la cantidad de unidades que tiene el anillo $\mathbb{Z}_m$.

Ejemplo 2.51. Como en $\mathbb{Z}_5$ hay cuatro unidades (Ejemplo 2.27), se tiene que $\varphi(5) = 4$.

Las siguientes propiedades permiten calcular con facilidad $\varphi(m)$ para cualquier entero $m \geq 2$ del que conozcamos su factorización única como producto de primos:

Propiedades 2.52. *La función φ de Euler cumple las siguientes propiedades*

1. *Si p es primo positivo, entonces* $\begin{cases} \varphi(p) = p - 1 \\ \varphi(p^r) = p^r - p^{r-1} \end{cases}$
2. *Si a y b son primos entre sí, entonces $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*

Ejemplo 2.53. Como $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$, en $\mathbb{Z}_8$ hay cuatro unidades. Son aquellas $\overline{a} \in \mathbb{Z}_8$ tales que $\text{mcd}(a, 8) = 1$, esto es, $\overline{1}$, $\overline{3}$, $\overline{5}$ y $\overline{7}$.

Ejemplo 2.54. Como $\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = (2-1) \cdot (3-1) = 1 \cdot 2 = 2$, en $\mathbb{Z}_6$ hay dos unidades. Son aquellas $\overline{a} \in \mathbb{Z}_6$ tales que $\text{mcd}(a, 6) = 1$, esto es, $\overline{1}$ y $\overline{5}$.

Corolario 2.55. *Si* $m = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_s^{r_s}$, *entonces*

$$\varphi(m) = (p_1^{r_1} - p_1^{r_1-1}) \cdot (p_2^{r_2} - p_2^{r_2-1}) \cdot \ldots \cdot (p_s^{r_s} - p_s^{r_s-1}).$$

Ejemplo 2.56. Como $\varphi(72) = \varphi(2^3 \cdot 3^2) = (2^3 - 2^2) \cdot (3^2 - 3^1) = 4 \cdot 6 = 24$, en $\mathbb{Z}_{72}$ hay 24 unidades. Son aquellas $\overline{a} \in \mathbb{Z}_{72}$ tales que $\text{mcd}(a, 72) = 1$, esto es, $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$,$\cdots$.

Ejercicio 2.57. ¿Cuántas unidades hay en el anillo $\mathbb{Z}_{2016}$?

La Congruencia de Euler nos proporciona un método sencillo para el cálculo de potencias a^k módulo m, cuando a es primo con m y además se conoce el valor $\varphi(m)$. En ese caso el exponente k se podrá reducir módulo $\varphi(m)$, pues:

Teorema 2.58 (Congruencia de Euler). *Si* a *es un entero tal que* $\text{mcd}(a, m) = 1$, *entonces* $a^{\varphi(m)} \equiv 1 \,(\text{mod } m)$.

Corolario 2.59 (Pequeño teorema de Fermat). *Si* p *es un número primo y* a *es un entero que no es múltiplo de* p, *entonces* $a^{p-1} \equiv 1 \,(\text{mod } p)$.

Observación 2.60. Obsérvese que si a es un entero tal que $\text{mcd}(a, m) = 1$, las potencias de a cuyo exponente es un múltiplo de $\varphi(m)$ también serán congruentes con 1 módulo m:

$$a^{\varphi(m)\cdot c} = (a^{\varphi(m)})^c \equiv 1^c \equiv 1 \,(\text{mod } m)$$

Por tanto, si queremos calcular el resto de la división de una potencia a^k entre m, una buena estrategia para simplificar las cuentas sería dividir k entre $\varphi(m)$, de modo que $k = \varphi(m) \cdot c + r$, con $r < \varphi(m)$. De este modo

$$a^k = a^{\varphi(m)\cdot c + r} = a^{\varphi(m)\cdot c} \cdot a^r \equiv 1 \cdot a^r \equiv a^r \,(\text{mod } m),$$

y reducimos el problema a calcular el resto de la potencia más sencilla a^r.

Ejemplo 2.61. Si queremos calcular el resto de la división de 3^{47} entre 23, como 23 es primo, podemos usar el Pequeño Teorema de Fermat para simplificar el cálculo. Ese teorema nos asegura que

$$3^{22} \equiv 1 \,(\text{mod } 23).$$

Como $47 = 22 \cdot 2 + 3$,

$$3^{47} = 3^{22\cdot 2+3} = (3^{22})^2 \cdot 3^3 \equiv 1^2 \cdot 27 \equiv 27 \equiv 4 \,(\text{mod } 23).$$

Luego el resto de la división de 3^{47} entre 23 es 4.