Congruencias

Definición de congruencia. Primeras propiedades

Definición. *Un entero a es* **congruente** *con un entero a'* **módulo** *un entero m si $a - a'$ es múltiplo de m; en este caso se escribe $a \equiv a' \pmod{m}$, y su negación: $a \not\equiv a' \pmod{m}$.*

Así:

$$a \equiv a' \pmod{m} \iff \text{existe } z \in \mathbf{Z} \text{ tal que } a - a' = mz \ ;$$

o bien:

$$a \equiv a' \pmod{m} \iff a - a' \in (m) \ ,$$

donde (m) denota al conjunto (ideal) de los múltiplos de m.

Ejemplos

$14 \equiv 2 \pmod{12}$, $\quad 4 \equiv 19 \pmod{5}$, $\quad 12 \equiv 12 \pmod{0}$,
$13 \equiv -2 \pmod{3}$, $\quad 7 \not\equiv 4 \pmod{2}$, $\quad 13 \not\equiv 12 \pmod{0}$.

Cada entero m determina así una relación binaria en el conjunto $\mathbf{Z}$ de los enteros, llamada la **congruencia módulo** m. Se estudiarán algunas propiedades notables de estas congruencias; en primer lugar veamos algunas reducciones.

(1) Si a y b son enteros, entonces las relaciones $a \equiv b \pmod{0}$ y $a = b$ son equivalentes, de modo que la relación de congruencia módulo cero es precisamente la relación de identidad o igualdad en el conjunto $\mathbf{Z}$ de los enteros.

(2) Cualquiera que sea $m \in \mathbf{Z}$, la relación $a \equiv b \pmod{m}$ equivale a la relación $a \equiv b \pmod{-m}$; esto es, las congruencias con repecto a un módulo m y su opuesto $-m$ son idénticas.

(3) La relación $a \equiv b \pmod{1}$ es válida cualesquiera que sean los enteros a y b.

Debido a **(1)**, **(2)** y **(3)** se suele imponer la restricción $m > 1$.

De la definición de congruencia se deriva directamente el siguiente criterio para decidir si dos enteros son congruentes módulo un entero $m \neq 0$: Sean a, a' enteros, y sea $r_m(a - a')$ el resto de dividir $a - a'$ entre m

si $r_m(a - a') = 0$, entonces $a \equiv a' \pmod{m}$
si $r_m(a - a') \neq 0$, entonces $a \not\equiv a' \pmod{m}$

Proposición. *Sea m un entero, se cumplen las propiedades:*

1. $a \equiv a \pmod{m}$, *para todo entero a;*
2. *para todo $a, b \in \mathbf{Z}$, si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$; y*
3. *para todo $a, b, c \in \mathbf{Z}$, si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.*

Demostración. Es comprobación rutinaria, pero cabe señalar que

1. es consecuencia de que $0 \in (m)$;
2. es consecuencia de que si $d \in (m)$, entonces $-d \in (m)$; y
3. es consecuencia de que si $d, d' \in (m)$, entonces $d + d' \in (m)$.

Para cada entero m, la congruencia módulo m es una relación de equivalencia en el conjunto $\mathbf{Z}$ de los enteros; la clase de equivalencia de un entero a con respecto a la congruencia módulo m se denomina la **clase de congruencia de** a **módulo** m; se representará la clase de congruencia de a módulo m mediante la notación $[a]_m$:

$$[a]_m = \{a' \in \mathbf{Z} \mid a' \equiv a \pmod{m}\}$$

Un entero a' pertenece a la clase $[a]_m$ si, y sólo si, $a' - a$ es múltiplo de m; y esto se cumple si, y sólo si, $a' = a + mz$ para algún entero z. Se obtiene así una descripción explícita de la clase de congruencia de a módulo m:

$$[a]_m = \{a + mz \mid z \in \mathbf{Z}\}.$$

El conjunto cociente (conjunto de todas las clases de congruencia módulo m) se denotará, provisionalmente, $\mathbf{Z}/\!\equiv_m$.

Ejemplo. Veamos cómo son, explícitamente, las clases de congruencia módulo 5.
Comencemos por la clase de 0:
$[0]_5 = \{0 + 5z \mid z \in \mathbf{Z}\} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$;
escojamos un entero fuera de esta clase, digamos 1:
$[1]_5 = \{1 + 5z \mid z \in \mathbf{Z}\} = \{\ldots, -19, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}$;
escojamos un entero fuera de las clases anteriores, por ejemplo 2:
$[2]_5 = \{2 + 5z \mid z \in \mathbf{Z}\} = \{\ldots, -18, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$;
escojamos un entero fuera de las clases anteriores, por ejemplo 3:
$[3]_5 = \{3 + 5z \mid z \in \mathbf{Z}\} = \{\ldots, -17, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$;
escojamos un entero fuera de las clases anteriores, digamos 4:
$[4]_5 = \{4 + 5z \mid z \in \mathbf{Z}\} = \{\ldots, -16, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$;
como no es posible escoger un entero fuera de estas clases (¿justificación?), y estas clases son distintas dos a dos, se concluye que $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$ son exactamente las distintas clases de congruencia módulo 5. Se obtiene así una partición del conjunto $\mathbf{Z}$ de los enteros en cinco clases de congruencia módulo 5, y el conjunto cociente es

$$\mathbf{Z}/\!\equiv_5 \;=\; \Big\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\Big\}.$$

Ejercicio. Describir explícitamente las clases de congruencia módulo m y el correspondiente conjunto cociente $\mathbf{Z}/\equiv_m$ en cada uno de los siguientes casos:

(1) $m = 6$,	**(2)** $m = -6$,
(3) $m = 3$,	**(4)** $m = 2$,
(5) $m = 1$,	**(6)** $m = 0$.

La relación de congruencia módulo m, para un entero positivo m, está íntimamente conectada con los restos módulo m según se expone a continuación.

Proposición. *Sea m un entero positivo, y sean a y a' enteros cualesquiera. Se cumplen:*

(1) $a \equiv a' \pmod{m}$ *si y sólo si* $r_m(a - a') = 0$

(2) $a \equiv r_m(a) \pmod{m}$

(3) $a = r_m(a)$ *si, y sólo si,* $0 \le a < m$.

(4) $a \equiv a' \pmod{m}$ *si, y sólo si,* $r_m(a) = r_m(a')$

(5) $[a]_m = [r_m(a)]_m$

(6) *Si* $a \ne a'$ *y* $0 \le a, a' < m$, *entonces* $[a]_m \ne [a']_m$

Demostración. Usando la propiedad de la división, y teniendo en cuenta que se supone $m > 0$, pongamos

$$a = mq_m(a) + r_m(a), \qquad 0 \le r_m(a) < m, \tag{1}$$

$$a' = mq_m(a') + r_m(a'), \quad 0 \le r_m(a') < m \tag{2}$$

(1) $a \equiv a' \pmod{m}$ equivale a $a - a' = mk$ para algún entero k que, a su vez, equivale a $r_m(a - a') = 0$.

(2) Como $a - r_m(a) = mq_m(a)$, resulta $a \equiv r_m(a) \pmod{m}$.

(3) Si $a = r_m(a)$, entonces $0 \leq r_m(a) = a < m$. Recíprocamente, si $0 \leq a < m$, entonces de la igualdad $a = m0 + a$ y de la unicidad del resto se sigue que $a = r_m(a)$.

(4) Suponer $a \equiv a' \pmod{m}$, hay un entero z tal que $a = a' + mz$, de [2] se obtiene $a = mq_m(a') + r_m(a') + mz = m(q_m(a') + z) + r_m(a')$; comparando esta expresión con [1] y por unicidad del resto, se concluye que $r_m(a) = r_m(a')$. Recíprocamente, suponer $r_m(a) = r_m(a')$, restando [1] y [2] miembro a miembro se obtiene $a \equiv a' \pmod{m}$.

(5) Es consecuencia de (2).

(6) Por (3), $r_m(a) = a \neq a' = r_m(a')$; por (4), $a \not\equiv a' \pmod{m}$, de donde $[a]_m \neq [a']_m$.

Si $a, a' \in [a]_m$, entonces $a \equiv a' \pmod{m}$ y, por (4), $r_m(a) = r_m(a')$. Para cada elemento $[a]_m \in \mathbf{Z}/\equiv_m$ pongamos $r([a]_m) = r_m(a)$, queda definida una aplicación r del conjunto cociente $\mathbf{Z}/\equiv_m$ en el subconjunto $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ de $\mathbf{Z}$. La aplicación r es biyectiva (¿demostración?). En consecuencia el conjunto $\mathbf{Z}/\equiv_m$ es finito y se tiene $\#(\mathbf{Z}/\equiv_m) = m$; esto es, hay exactamente m clases de congruencia módulo m. Cada clase de conguencia $[a]_m \in \mathbf{Z}/\equiv_m$ posee exactamente un *representante* en $\mathbf{Z}_m$, con lo que el conjunto $\mathbf{Z}_m$ es un sistema completo de representantes de las clases de congruencia módulo m.

Adición y multiplicación de clases de congruencia

En el siguiente enunciado se expone el comportamiento de la relación de congruencia módulo un entero m con respecto a las operaciones de adición y de multiplicación en el conjunto $\mathbf{Z}$ de los enteros:

Proposición. *Sea m un entero.*
(1) *Si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.*
(2) *Si $a_1 \equiv b_1 \pmod{m}$, entonces $-a_1 \equiv -b_1 \pmod{m}$.*
(3) *Si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.*

Demostración.
(1) Suponer que $a_1 = b_1 + k_1 m$ y $a_2 = b_2 + k_2 m$ para enteros k_1 y k_2, sumando miembro a miembro ambas igualdades se obtiene $a_1 + a_2 = b_1 + b_2 + (k_1 + k_2)m$.
(2) Suponer que $a_1 = b_1 + k_1 m$, multiplicando los dos miembros por -1 se obtiene $-a_1 = -b_1 + (-k_1)m$.
(3) Suponer que $a_1 = b_1 + k_1 m$ y $a_2 = b_2 + k_2 m$ para enteros k_1 y k_2, multiplicando miembro a miembro se obtiene $a_1 a_2 = b_1 b_2 + (b_1 k_2 + k_1 b_2 + k_1 k_2 m)m$.

Este *"buen comportamiento"* de la congruencia módulo un entero m en $\mathbf{Z}$ respecto de las operaciones de adición y de multiplicación permite definir operaciones de adición y de multiplicación en el conjunto cociente $\mathbf{Z}/\equiv_m$, heredadas de aquellas:

$$\begin{array}{ccc} \mathbf{Z}/\equiv_m \times \mathbf{Z}/\equiv_m & \rightarrow & \mathbf{Z}/\equiv_m \\ ([a]_m, [b]_m) & \mapsto & [a]_m + [b]_m = [a+b]_m \end{array}$$

$$\begin{array}{ccc} \mathbf{Z}/\equiv_m \times \mathbf{Z}/\equiv_m & \rightarrow & \mathbf{Z}/\equiv_m \\ ([a]_m, [b]_m) & \mapsto & [a]_m [b]_m = [ab]_m \end{array}$$

Nota. La definición de $[a]_m + [b]_m$ deberá entenderse en el sentido siguiente: Escoger representantes arbitrarios $a_1 \in [a]_m$ y $b_1 \in [b]_m$, calcular $a_1 + b_1$ en $\mathbf{Z}$, y poner la clase de congruencia $[a_1 + b_1]_m$ como resultado de la suma; si se eligiesen otros representantes, digamos $a_2 \in [a]_m$ y $b_2 \in [b]_m$, se calcularía $a_2 + b_2$ en $\mathbf{Z}$, y se obtendría la clase $[a_2 + b_2]_m$. La propiedad **(1)** asegura que $[a_1 + b_1]_m = [a_2 + b_2]_m$. Análogas consideraciones para la definición de $[a]_m [b]_m$.

Ejemplos

1. Consideremos el módulo $m = 12$. Se tienen las siguientes relaciones en $\mathbf{Z}/\equiv_{12}$:
$[3]_{12} + [7]_{12} = [10]_{12}$,
$[15]_{12} + [-5]_{12} = [10]_{12} = [3]_{12} + [7]_{12}$.

   $[8]_{12} + [9]_{12} = [17]_{12} = [5]_{12}$,
$[20]_{12} + [21]_{12} = [41]_{12} = [5]_{12} = [8]_{12} + [9]_{12}$.

   $[3]_{12}[7]_{12} = [21]_{12} = [9]_{12}$,
$[-9]_{12}[7]_{12} = [-63]_{12} = [9]_{12} = [3]_{12}[7]_{12}$.

   $[8]_{12}[9]_{12} = [72]_{12} = [0]_{12}$,
$[20]_{12}[-3]_{12} = [-60]_{12} = [0]_{12} = [8]_{12}[9]_{12}$.

2. Las *tablas de sumar y de multiplicar* módulo 5; esto es, en $\mathbf{Z}/\equiv_5$:

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

$\times$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

3. Las *tablas de sumar y de multiplicar* módulo 6; esto es, en $\mathbf{Z}/\equiv_6$:

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$\times$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Ejercicios

1. Construir, como se ha hecho en los ejemplos, las tablas de sumar y de multiplicar para cada uno de los módulo 2, 3, 4, 7 y 12.
2. En los ejemplos y ejercicios precedentes se han construido las tablas de multiplicación de $\mathbf{Z}/\equiv_m$, para $m = 2, 3, 4, 5, 6, 7$ y 12. Observando dichas tablas, señalar en cada uno de los correspondientes sistemas $(\mathbf{Z}/\equiv_m\ ,\ .)$ aquellos elementos a tales que $ab = 0$ para algún b. Analogamente, señalar aquellos elementos u tales que $uv = 1$ para algún v.

Propiedades. Sea m un entero, las operaciones de adición y de multiplicación en el conjunto $\mathbf{Z}/\equiv_m$ cumplen las siguientes propiedades

- Adición:
  - Asociativa: para todo $[a]_m, [b]_m, [c]_m \in \mathbf{Z}/\equiv_m$

$$\Big([a]_m + [b]_m\Big) + [c]_m = [a]_m + \Big([b]_m + [c]_m\Big)$$

- Conmutativa: para todo $[a]_m, [b]_m \in \mathbf{Z}/\equiv_m$

$$[a]_m + [b]_m = [b]_m + [a]_m$$

- Existencia de cero: hay un (único) elemento $[z]_m \in \mathbf{Z}/\equiv_m$ tal que

$$[a]_m + [z]_m = [a]_m \ \text{ para todo } \ [a]_m \in \mathbf{Z}/\equiv_m$$

  Se tiene $[z]_m = [0]_m$

- Existencia de opuestos: para cada $[a]_m \in \mathbf{Z}/\equiv_m$ hay un (único) elemento $[a']_m \in \mathbf{Z}/\equiv_m$ tal que

$$[a]_m + [a']_m = 0$$

  Se tiene $[a']_m = [-a]_m$

• Multiplicación:

- Asociativa: para todo $[a]_m, [b]_m, [c]_m \in \mathbf{Z}/\equiv_m$

$$\Big([a]_m[b]_m\Big)[c]_m = [a]_m\Big([b]_m[c]_m\Big)$$

- Conmutativa: para todo $[a]_m, [b]_m \in \mathbf{Z}/\equiv_m$

$$[a]_m[b]_m = [b]_m[a]_m$$

- Existencia de unidad: hay un (único) elemento $[u]_m \in \mathbf{Z}/\equiv_m$ tal que

$$[a]_m[u]_m = [a]_m \ \text{ para todo } \ [a]_m \in \mathbf{Z}/\equiv_m$$

  Este elemento es $[u]_m = [1]_m$

• Multiplicación y adición:

- Distributiva (de la multiplicación respecto de la adición): para todo $[a]_m, [b]_m, [c]_m \in \mathbf{Z}/\equiv_m$

$$[a]_m\Big([b]_m + [c]_m\Big) = \Big([a]_m[b]_m\Big) + \Big([a]_m[c]_m\Big)$$

La demostración de estas propiedades es sencilla y se obtiene directamente a partir de las definiciones de las respectivas operaciones y de las correspondientes propiedades en el anillo $\mathbf{Z}$ de los enteros. Se deja como ejercicio simple al lector interesado.

Notas.

- Por cumplirse las propiedades anteriores se dice que la terna $(\mathbf{Z}/\equiv_m, +, .)$, formada por el conjunto $\mathbf{Z}/\equiv_m$ y las operaciones de adición y de multiplicación definidas en él, es un anillo conmutativo.
- Otros ejemplos de anillos conmutativos son $(\mathbf{Z}, +, .)$, $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$.
- La terna $(\mathrm{M}_2(\mathbf{Q}), +, .)$, formada por las matrices 2×2 sobre los racionles con la adición y la multiplicación de matrices, es un ejemplo de anillo no conmutativo.
- Como en todo anillo, se tiene la siguiente propiedad:

$$[a]_m[0]_m = [0]_m = [0]_m[a]_m \quad \text{ para todo } \quad [a]_m \in \mathbf{Z}/\equiv_m$$

Definición. *El conjunto $\mathbf{Z}/{\equiv_m}$ junto con las operaciones de adición y multiplicación definidas previamente se denomina el* **anillo de clases de restos módulo** m.

Unidades y divisores de cero

En el conjunto $\mathbf{Z}/{\equiv_{12}}$ de las clases de congruencia módulo 12, y para la operación de multiplicación, se observan las siguientes *anomalías* aparentes:

$$[2]_{12}[6]_{12} = [0]_{12}; \quad [3]_{12}[8]_{12} = [0]_{12}; \quad [8]_{12}[9]_{12} = [0]_{12}$$

Esto es, el producto de dos elementos no nulos puede ser cero. Sin embargo, hay elementos $[a]_{12}$ en $\mathbf{Z}/{\equiv_{12}}$ tales que $[a]_{12}[b]_{12} = [0]_{12}$ sólo si $[b]_{12} = [0]_{12}$. Por ejemplo, el lector puede comprobar directamente que $[5]_{12}[b]_{12} = [0]_{12}$ sólo si $[b]_{12} = [0]_{12}$.
Se producen situaciones análogas para los módulos $m = 4, 6, 8$:

$$[2]_4[2]_4 = [0]_4; \quad [2]_6[3]_6 = [0]_6; \quad [2]_8[4]_8 = [0]_8$$

Sin embargo, para los módulos $m = 2, 3, 5$ ó 7 el lector puede comprobar directamente que un producto de dos factores es cero únicamente si (al menos) uno de ellos lo es:

Para $m = 2, 3, 5$ ó 7 se tiene

$$[a]_m[b]_m = [0]_m$$

si, y sólo si,

$$[a]_m = [0]_m \quad \text{ó} \quad [b]_m = [0]_m$$

Pasemos a estudiar estas situaciones.

Definición. *Sea m un entero, $m > 1$. Un elemento $[u]_m$ del anillo $\in \mathbf{Z}/{\equiv_m}$ es una* **unidad** *si hay un elemento $[v]_m \in \mathbf{Z}/{\equiv_m}$ tal que*

$$[u]_m[v]_m = [1]_m$$

Ejemplos.

(1) En el anillo $\mathbf{Z}/{\equiv_{12}}$, los siguientes elementos son unidades:

$$[1]_{12},\ [5]_{12},\ [7]_{12},\ [11]_{12}$$

En efecto:

$$[1]_{12}[1]_{12} = [1]_{12}, \quad [5]_{12}[5]_{12} = [1]_{12}, \quad [7]_{12}[7]_{12} = [1]_{12}, \quad [11]_{12}[11]_{12} = [1]_{12}$$

(2) En el anillo $\mathbf{Z}/{\equiv_9}$, los siguientes elementos son unidades:

$$[1]_9,\ [2]_9,\ [4]_9,\ [5]_9,\ [7]_9,\ [8]_9$$

En efecto:

$$[1]_9[1]_9 = [1]_9, \quad [2]_9[5]_9 = [1]_9, \quad [4]_9[7]_9 = [1]_9, \quad [8]_9[8]_9 = [1]_9$$

Ejercicios.

1. Comprobar que en el anillo $\mathbf{Z}/{\equiv_{12}}$ los siguientes elementos no son unidades:

$$[0]_{12},\ [2]_{12},\ [3]_{12},\ [4]_{12}, [6]_{12},\ [8]_{12},\ [10]_{12}$$

2. Comprobar que en el anillo $\mathbf{Z}/{\equiv_9}$ los siguientes elementos no son unidades:

$$[0]_9,\ [3]_9,\ [6]_9$$

Veamos una caracterización útil de las unidades de los anillos $\mathbf{Z}/{\equiv_m}$ para cualquier entero $m > 0$.

Proposición. *Sea m un entero, $m > 1$. Un elemento $[u]_m$ del anillo $\mathbf{Z}/\equiv_m$ es una unidad si, y sólo si,* $\mathrm{mcd}(u, m) = 1$.

Demostración. Suponer que $[u]_m$ es una unidad en $\mathbf{Z}/\equiv_m$ y sea $[v]_m$ un elemento de $\mathbf{Z}/\equiv_m$ tal que $[u]_m[v]_m = [1]_m$; entonces $[uv]_m = [1]$; esto es, $uv \equiv 1 \pmod{m}$; por tanto hay un entero z tal que $uv + mz = 1$; de ahí que $\mathrm{mcd}(u, m) = 1$. Recíprocamente, suponer que $\mathrm{mcd}(u, m) = 1$; por la identidad de Bezout hay enteros v, z tales que $1 = uv + mz$, de donde

$$[1]_m = [uv + mz]_m = [u]_m[v]_m + [m]_m[z]_m = [u]_m[v]_m$$

por tanto $[u]_m$ es una unidad.

Ejercicio. Probar que si a y a' son representantes de una misma clase $[a]_m$ módulo m, entonces $\mathrm{mcd}(a, m) = \mathrm{mcd}(a', m)$.

Proposición. *Si $[u]_m$ es una unidad del anillo $\mathbf{Z}/\equiv_m$, entonces sólo hay un elemento $[v]_m \in \mathbf{Z}/\equiv_m$ que cumpla*

$$[u]_m[v]_m = [1]_m$$

Demostración. Si $[v']_m \in \mathbf{Z}/\equiv_m$ también cumple

$$[u]_m[v']_m = [1]_m$$

entonces se tiene

$$[v']_m = [1]_m[v']_m = ([v]_m[u]_m)[v']_m = [v]_m([u]_m[v']_m) = [v]_m[1]_m = [v]_m$$

Definición. *Sea $[u]_m$ una unidad en el anillo $\mathbf{Z}/\equiv_m$. El único elemento $[v]_m$ en $\mathbf{Z}/\equiv_m$ que cumple*

$$[u]_m[v]_m = [1]_m$$

se denomina el **inverso** *de $[u]_m$ (el inverso de u módulo m). Se escribe $[v]_m = [u]_m^{-1}$.*

Algoritmo INVMOD (Cálculo de inversos modulares; esto es, de inversos en el anillo $\mathbf{Z}/\equiv_m$)

Entrada: $u \in \mathbf{Z}$, un representante de $[u]_m$, y m un entero, $m > 1$.
Salida: el representante canónico de $[u]_m^{-1}$ si $[u]_m$ es una unidad; ERROR en otro caso.

INVMOD(u, m)

1 $(d, v, z) \leftarrow$ MCDEX(u, m) // (d, v, z) es tal que $d = \mathrm{mcd}(u, m)$ y $d = uv + mz$
2 **Si** $d \neq 1$ **entonces parar** y **anunciar** ERROR
3 **Si** $d = 1$ **entonces devolver** RESTO(v, m)

Ejemplos.

(1) Calcular el inverso de $[7]_{12}$ en el anillo $\mathbf{Z}/\equiv_{12}$.
El algoritmo extendido de Euclides (MCDEX) aplicado al par $(7, 12)$ proporciona como salida la terna $(1, -5, 3)$, de modo que $\mathrm{mcd}(7, 12) = 1$ y $1 = 7 \times (-5) + 12 \times 3$. Por tanto $[7]_{12}$ es una unidad en $\mathbf{Z}/\equiv_{12}$ y $[7]_{12}^{-1} = [-5]_{12} = [7]_{12}$

(2) Calcular el inverso de $[81]_{152}$ en el anillo $\mathbf{Z}/\equiv_{152}$.
El algoritmo extendido de Euclides (MCDEX) aplicado al par $(81, 152)$ proporciona como salida la terna $(1, -15, 8)$, de modo que $\mathrm{mcd}(81, 152) = 1$ y $1 = 81 \times (-15) + 152 \times 8$. Por tanto $[81]_{152}$ es una unidad en $\mathbf{Z}/\equiv_{152}$ y $[81]_{152}^{-1} = [-15]_{152} = [137]_{152}$

---

(3) Calcular el inverso de $[1287]_{1768}$ en el anillo $\mathbf{Z}/\equiv_{1768}$.

El algoritmo extendido de Euclides (MCDEX) aplicado al par $(1287, 1768)$ proporciona como salida la terna $(13, 11, -8)$, de modo que $\mathrm{mcd}(1287, 1768) = 13$; por tanto $[1287]_{1768}$ no es una unidad en el anillo $\mathbf{Z}/\equiv_{1768}$

Notas de programación

- Un programa en Maple que implementa el cálculo de inversos modulares.

```
invmod := proc(u::integer, m::integer)
local M, lista_mcdex;
    if m = 0 or m = 1 then
        ERROR("El modulo debe ser distinto de cero y de uno")
    fi;
    `mod` := modp;
    M := abs(m);
    lista_mcdex := mcdex(u, M);
    if op(1, lista_mcdex) <> 1 then ERROR(
        cat("No existe el inverso de ", u, " modulo ", m))
    fi;
    op(2, lista_mcdex) mod M
end;
```

Proposición. *Sea m un entero, $m > 1$.*

1. *El producto $[u]_m[v]_m$ de unidades $[u]_m$ y $[v]_m$ en el anillo $\mathbf{Z}/\equiv_m$ es también una unidad y se verifica*

$$([u]_m[v]_m)^{-1} = [u]_m^{-1}[v]_m^{-1}$$

2. *El elemento unidad $[1]_m$ es una unidad en el anillo $\mathbf{Z}/\equiv_m$ y se verifica*

$$[1]_m^{-1} = [1]_m$$

3. *El inverso $[u]_m^{-1}$ de una unidad $[u]_m$ en el anillo $\mathbf{Z}/\equiv_m$ es también una unidad y se verifica*

$$([u]_m^{-1})^{-1} = [u]_m$$

Demostración. Es sencilla y se deja como ejercicio.

Vamos a simplificar la notación. Desde ahora, y como es práctica habitual en Algebra, se pondrá $\mathbf{Z}_m$ para denotar al anillo $\mathbf{Z}/\equiv_m$ de clases de restos módulo un entero m.

Se denota mediante $U(\mathbf{Z}_m)$ al conjunto de las unidades del anillo $\mathbf{Z}_m$, $m > 1$. Teniendo en cuenta la caracterización de las unidades de los anillos $\mathbf{Z}_m$, se tienen los siguientes ejemplos:

$$\begin{array}{lcl}
U(\mathbf{Z}_2) & = & \{[1]_2\} \\
U(\mathbf{Z}_3) & = & \{[1]_3, [2]_3\} \\
U(\mathbf{Z}_4) & = & \{[1]_4, [3]_4\} \\
U(\mathbf{Z}_5) & = & \{[1]_5, [2]_5, [3]_5, [4]_5\} \\
U(\mathbf{Z}_6) & = & \{[1]_6, [5]_6\} \\
U(\mathbf{Z}_7) & = & \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\} \\
U(\mathbf{Z}_8) & = & \{[1]_8, [3]_8, [5]_8, [7]_8\} \\
U(\mathbf{Z}_9) & = & \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\} \\
U(\mathbf{Z}_{10}) & = & \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} \\
U(\mathbf{Z}_{11}) & = & \{[1]_{11}, [2]_{11}, [3]_{11}, [4]_{11}, [5]_{11}, [6]_{11}, [7]_{11}, [8]_{11}, [9]_{11}, [10]_{11}\} \\
U(\mathbf{Z}_{12}) & = & \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}
\end{array}$$

Dado que el producto de dos unidades en $\mathbf{Z}_m$ es una unidad, la operación de multiplicación en $\mathbf{Z}_m$ induce, por restricción, una operación binaria interna en el conjunto $U(\mathbf{Z}_m)$ de las unidades:

$$\begin{array}{rccc} \times : & U(\mathbf{Z}_m) \times U(\mathbf{Z}_m) & \to & U(\mathbf{Z}_m) \\ & ([u]_m, [v]_m) & \mapsto & [u]_m[v]_m \end{array}$$

Proposición. *Sea m un entero, $m > 1$. El par $\big(U(\mathbf{Z}_m), \times\big)$ de las unidades del anillo $\mathbf{Z}_m$ con la multiplicación es un grupo conmutativo.*

Para cada entero $m > 1$ se denota por $\varphi(m)$ el número de elementos del grupo $U(\mathbf{Z}_m)$ de las unidades del anillo $\mathbf{Z}_m$. Se pone $\varphi(1) = 1$ y $\varphi(0) = 0$. Queda así definida una función

$$\begin{array}{rccc} \varphi : & \mathbf{N} & \to & \mathbf{N} \\ & m & \mapsto & \varphi(m) \end{array}$$

que se denomina la **función de Euler**. En la tabla adjunta se muestran los valores $\varphi(m)$ de la función de Euler para m en el rango 0 a 12:

m	0	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(m)$	0	1	1	2	2	4	2	6	4	6	4	10	4

Proposición. *Para todo número natural m, $\varphi(m)$ coincide con el número de enteros positivos menores que o iguales a m y primos con m:*

$$\varphi(m) = \mathrm{Card}\big(\{i \in \mathbf{N} \mid 0 < i \leq m \;\; y \;\; \mathrm{mcd}(i, m) = 1\}\big)$$

Veamos algunas propiedades de la función de Euler.

Proposición.

1. *Un entero $p > 1$ es primo si, y sólo si,*

$$\varphi(p) = p - 1$$

2. *Para todo primo p y todo entero positivo e se tiene*

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

3. *Si m y n son enteros positivos primos entre sí, entonces $\varphi(mn) = \varphi(m)\varphi(n)$*

4. *Sea n un entero, $n > 1$, y sea*

$$n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} = \prod_{i=1}^{n} p_i^{e_i}$$

la factorización de n en producto de primos distintos elevados a exponentes positivos, entonces

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \dots \Big(1 - \frac{1}{p_s}\Big) = n \prod_{i=1}^{s} \Big(1 - \frac{1}{p_1}\Big)$$

Demostración. ... ...

Lema. *Sea $G = (G, .)$ un grupo. Para cada elemento $g \in G$ la aplicación*

$$\begin{array}{rccc} t_g : & G & \to & G \\ & x & \mapsto & gx \end{array}$$

es biyectiva.

Demostración. Considerar la aplicación $t_{g^{-1}}$. Se tiene

$$t_g \circ t_{g^{-1}} = 1_G = t_{g^{-1}} \circ t_g \ ;$$

donde 1_G denota la apliceción identidad de G en G

$$\begin{array}{cccc} 1_G : & G & \to & G \\ & x & \mapsto & x \end{array}$$

Proposición. *Sea $G = (G, .)$ un grupo abeliano de orden finito n. Para cada elemento $g \in G$ se tiene*

$$g^n = e, \quad \textit{donde } e \textit{ denota el elemento unidad del grupo } G$$

Demostración. Suponer que $G = \{g_1, g_2, \ldots, g_i, \ldots, g_n\}$ y sea g un elemento de G (i.e., g es uno de los g_i). Por el Lema anterior se tiene

$$\prod_{i=1}^{n} g_i = \prod_{i=1}^{n} (g g_i) = g^n \prod_{i=1}^{n} g_i$$

Multiplicando ambos miembros por el inverso de $\prod_{i=1}^{n} g_i$ se obtiene la afirmación.

Teorema de Euler. *Sea m un entero, $m > 1$. Para todo entero a primo con m se verifica*

$$([a]_m)^{\varphi(m)} = [1]_m$$

Teorema de Fermat. *Sea p un número primo. Para todo entero a tal que $p \not| \, a$ se tiene*

$$([a]_p)^{p-1} = [1]_p$$

Notas y ejemplos.

- En términos de congruencias el Teorema de Euler se expresa:
  Teorema de Euler. *Sea m un entero, $m > 1$. Para todo entero a primo con m se verifica*

  $$a^{\varphi(m)} \equiv 1 \pmod{m}$$

- En términos de congruencias el Teorema de Fermat se expresa:
  Teorema de Fermat. *Sea p un número primo. Para todo entero a tal que $p \not| \, a$ se tiene*

  $$a^{p-1} \equiv 1 \pmod{p}$$

- Como consecuencia del punto anterior se tiene: *Si p es un número primo y a es un entero cualquiera, entonces*

  $$a^p \equiv a \pmod{p}$$

- Un algoritmo eficiente para calcular potencias. Teniendo en cuenta la definición de potencias de exponente no negativo:

  $$\begin{array}{lcl} a^0 & = & 1 \\ a^{n+1} & = & a \times a^n, \quad \text{para todo } n \in \mathbf{N} \end{array}$$

Se obtiene la propiedad

$$a^{2n} = (a^2)^n, \quad \text{para todo } n \in \mathbf{N}$$

que se utiliza en el siguiente algoritmo

Algoritmo POTENCIA (Cálculo de potencias de exponente entero no negativo)

Entrada: $B \in \mathbf{Z}, E \in \mathbf{N}$.
Salida: B^E .

POTENCIA(B, E)

$(b, e, p) \leftarrow (B, E, 1)$
mientras $e \neq 0$
  hacer
    si ES_PAR(e) **entonces** $(b, e) \leftarrow (b \times b, e/2)$
    si ES_IMPAR(e) **entonces** $(e, p) \leftarrow (e - 1, b \times p)$
devolver p

- Un programa en Maple que implementa el algoritmo anterior para el cálculo de potencias modulares:

```
potmod := proc(B::integer, E::integer, m::integer)
local b, e, p;
   if E < 0 then ERROR("El exponente debe ser no negativo") fi;
   if m < 2 then ERROR("Por convenio el modulo debe ser mayor que 1") fi;
   b, e, p := B, E, 1;
   do
     if e = 0 then RETURN(p) fi;
     if type(e, even)
       then b, e := b*b mod m, e/2
       else e, p := e-1, p*b mod m
     fi
   od;
end;
```

En todo grupo $G = (G, .)$ el elemento unidad e coincide con su inverso. Nótese que para todo $g \in G$, la relación $g = g^{-1}$ equivale a la relación $g^2 = e$. Veamos cuáles son los elementos del grupo $U(\mathbf{Z}_p)$, con p un entero primo, que coinciden con su inverso.

Proposición. *Sea p un número primo. Los únicos elementos del grupo $U(\mathbf{Z}_p)$ que coinciden con su inverso son $[1]_p$ y $[p-1]_p$ $\big(= [-1]_p\big)$.*

Demostración. Obviamente

$$[1]_p^2 = [1]_p \quad \text{y} \quad [p-1]_p^2 = [-1]_p^2 = [1]_p$$

Recíprocamente, sea $[u]_p$ un elemento de $U(\mathbf{Z}_p)$ tal que $[u]_p^2 = [1]_p$, entonces $u^2 \equiv 1 \pmod{p}$, por tanto $p \,|(u^2 - 1) = (u-1)(u+1)$. Como, por hipótesis p es primo, se sigue que $p \,|(u-1)$ ó $p \,|(u+1)$; esto es, $u \equiv 1 \pmod{p}$ ó $u \equiv -1 \pmod{p}$, de donde se sigue directamente la afirmación del enunciado.

Usando este resultado se puede probar fácilmente el

Teorema de Wilson. *Para todo primo p se cumple*

$$[(p-1)!]_p = [p-1]_p \ \big(= [-1]_p\big)$$

Demostración. El caso $p = 2$ se comprueba fácilmente de modo directo. Suponer que p es un primo mayor que 2. Cada elemento $[i]_p$, $1 \le i \le p-1$ posee inverso; y se tiene:

$$[i]_p^{-1} \neq [i]_p, \quad \text{para todo } i,\ 2 \le i \le p-2$$

por tanto

$$\prod_{i=2}^{p-2}[i]_p = [1]_p$$

(pues cada factor $[i]_p$ "se va" con su inverso, ya que $[i]_p \neq [i]_p^{-1}$). Por tanto

$$[(p-1)!]_p = \prod_{i=1}^{p-1}[i]_p = [1]_p\Big(\prod_{i=2}^{p-2}[i]_p\Big)[p-1]_p = [1]_p[p-1]_p = [p-1]_p$$

lo que completa la demostración.

Nota. En términos de congruencias el Teorema de Wilson se expresa: *Para todo primo p se cumple*

$$(p-1)! \equiv -1 \pmod p$$

El teorema chino de los restos.

En esta sección se estudia el siguiente problema:

Dados

un entero positivo n,

una sucesión $m_1, m_2, \ldots, m_n$ de enteros positivos primos entre sí dos a dos; esto es,

$$\mathrm{mcd}(m_i, m_j) = 1, \ (i \neq j) \ ,$$

y una sucesión $a_1, a_2, \ldots, a_n$ de enteros.

- *Decidir si hay algún entero x que cumpla las n congruencias simultáneas:*

$$\begin{array}{c} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x \equiv a_n \pmod{m_n} \end{array}$$

- *En caso de respuesta afirmativa, describir todas las soluciones, y dar un método efectivo que permita calcularlas.*

Distingamos tres casos:

Caso 1. Suponer que $n = 1$; es decir, que se tiene una única congruencia:

$$x \equiv a_1 \pmod{m_1} \ .$$

En este caso el propio a_1 es una solución y el conjunto de las soluciones es la clase de congruencia de a_1 módulo m_1. Se puede tomar también como solución el resto r_1 de dividir a_1 entre m_1, porque $r_1 \equiv a_1 \pmod{m_1}$. El conjunto de todas las soluciones es la clase de congruencia

$$[a_1]_m = [r_1]_m = \{r_1 + m_1 t_1 \mid t_1 \in \mathbf{Z}\}$$

Ejemplo 1. Una solución de la ecuación $x \equiv 12 \pmod 8$ es $x = 12$. También el resto, 4, de dividir 12 entre 8 es una solución. El conjunto de todas las soluciones es

$$[12]_8 = [4]_8 = \{4 + 8t \mid t \in \mathbf{Z}\}$$

Caso 2. Suponer que $n = 2$; es decir, que se tienen dos congruencias:

$$x \equiv a_1 \pmod{m_1} \qquad [1]$$

$$x \equiv a_2 \pmod{m_2} \qquad [2]$$

con

$$\text{mcd}(m_1, m_2) = 1 \qquad [3]$$

Búsqueda de una solución. Si un entero x verifica [1], entonces debe ser

$$x = a_1 + m_1 t_1, \quad \text{para algún entero } t_1$$

De [2] se obtiene

$$a_1 + m_1 t_1 \equiv a_2 \pmod{m_2};$$

esto es,

$$a_1 + m_1 t_1 = a_2 + m_2 t_2, \quad \text{para algún entero } t_2$$

o bien,

$$m_1 t_1 - m_2 t_2 = a_2 - a_1, \quad \text{para algún entero } t_2 \qquad [4]$$

Por [3], existen enteros c_1, c_2 tales que

$$m_1 c_1 + m_2 c_2 = 1$$

de donde, multiplicando ambos miembros por $a_2 - a_1$,

$$m_1 c_1 (a_2 - a_1) - m_2 c_2 (a_1 - a_2) = a_2 - a_1 \qquad [5]$$

Comparando [4] y [5], tomemos $t_1 = c_1(a_2 - a_1)$; se obtiene, de [1],

$$x = a_1 + m_1 c_1 (a_2 - a_1)$$

Se comprueba que el entero $x = a_1 + m_1 c_1 (a_2 - a_1)$ verifica las condiciones [1] y [2] (¡hágase esta comprobación!). Por tanto $a_1 + m_1 c_1 (a_2 - a_1)$ es una solución común a las ecuaciones [1] y [2].

Descripción de todas las soluciones. Si x, x' son enteros que cumplen ambos las ecuaciones [1] y [2], entonces

$$x' \equiv x \pmod{m_1}$$

y

$$x' \equiv x \pmod{m_2}$$

de ahí que $x' - x$ es múltiplo de m_1 y de m_2 y, teniendo en cuenta que $\text{mcd}(m_1, m_2) = 1$, se concluye que $x' - x$ es múltiplo de $m_1 m_2$; esto es,

$$x' \equiv x \pmod{m_1 m_2}$$

esto es, dos soluciones comunes a [1] y [2] son congruentes módulo $m_1 m_2$.

Recíprocamente, si x es una solución común a [1] y a [2], y x' es un entero tal que

$$x' \equiv x \pmod{m_1 m_2}$$

entonces

$$x' = x + m_1 m_2 t \quad \text{para algún } t \in \mathbf{Z}$$

de donde se sigue
$$x' \equiv x \pmod{m_1}$$
y
$$x' \equiv x \pmod{m_2}$$
Por tanto x' es también una solución común a [1] y a [2], ya que se cumple
$$x' \equiv a_1 \pmod{m_1}$$
y
$$x' \equiv a_2 \pmod{m_2}$$

En consecuencia, el conjunto de las soluciones comunes a las ecuaciones en congruencias [1] y [2] coincide con el conjunto de las soluciones de la congruencia simple
$$x \equiv a_1 + m_1c_1(a_2 - a_1) \pmod{m_1m_2}$$

Proposición. *Sean m_1 y m_2 enteros positivos primos entre sí. Sean a_1 y a_2 enteros cualesquiera. Se tienen los hechos siguientes:*

1. *Hay soluciones comunes a las congruencias*
$$x \equiv a_1 \pmod{m_1} \qquad [1]$$
$$x \equiv a_2 \pmod{m_2} \qquad [2]$$
2. Si c_1 y c_2 son enteros tales que $m_1c_1 + m_2c_2 = 1$, entonces $a_1 + m_1c_1(a_2 - a_1)$ es una solución común a [1] y [2].
3. El sistema formado por las congruencias [1] y [2] es equivalente a la congruencia simple
$$x \equiv a_1 + m_1c_1(a_2 - a_1) \pmod{m_1m_2}$$

Notas y ejemplos.

- El algoritmo extendido de Euclides aplicado al par m_1, m_2 permite calcular eficientemente un par c_1, c_2 de enteros que cumplan $m_1c_1 + m_2c_2 = 1$
- Ejemplo. Hallar todos los enteros x que cumplan las dos congruencias
$$\begin{array}{ccc} x & \equiv & 3 \pmod{4} \\ x & \equiv & 8 \pmod{15} \end{array}$$
Solución: Se tiene (directamente, por simple inspección en un caso sencillo como éste)
$$4 \times 4 + 15 \times (-1) = 1$$
Una solución particular es
$$3 + 4 \times 4 \times 5 = 83$$
Por tanto la solución general es
$$x \equiv 83 \pmod{60}$$
O bien
$$x \equiv 23 \pmod{60}$$