

3. Aritmética modular

□ 1. Ecuaciones diofánticas

Los alumnos de la Escuela 314 hacen una colecta para reunir fondos para ayudar a una escuela de frontera. Para esto, ofrecen bonos contribución de dos tipos: bonos de \$15 y bonos de \$8.

Martín se lleva un piloncito de bonos de \$15 y otro de bonos de \$8. Después de vender varios bonos recaudó \$100, pero no recuerda cuántos bonos vendió de cada clase (ni sabe cuántos bonos tenía cada uno de sus piloncitos al comienzo). ¿Puede Martín determinar cuántos bonos vendió de cada tipo?

Para tratar de determinar estas cantidades, Martín observa que:

- si no hubiera vendido ningún bono de \$15, los \$100 provendrían de vender bonos de \$8; es decir, si vendió una cantidad y de bonos de \$8 sería $\$100 = \$8 \cdot y$, pero esto no puede ser porque 100 no es múltiplo de 8;
- si hubiera vendido un solo bono de \$15, entonces los $\$100 - \$15 = \$85$ restantes provendrían de vender bonos de \$8, pero 85 tampoco es múltiplo de 8;
- si hubiera vendido 2 bonos de \$15, los $\$100 - 2 \cdot \$15 = \$70$ restantes provendrían de vender bonos de \$8, pero 70 no es múltiplo de 8;
- no puede ser que haya vendido 3 bonos de \$15, porque $\$100 - 3 \cdot \$15 = \$55$ y 55 tampoco es múltiplo de 8;
- es posible que haya vendido 4 bonos de \$15, ya que $\$100 - 4 \cdot \$15 = \$40 = 5 \cdot \8 . Esto significa que además habría vendido 5 bonos de \$8;
- razonando de la misma manera deduce que no puede ser que haya vendido ni 5 ni 6 bonos de \$15. Además, seguro que no vendió más de 7 de estos bonos, pues $7 \cdot \$15 = \105 y sólo recaudó \$100.

Martín concluye entonces que los \$100 fueron recaudados mediante la venta de 4 bonos de \$15 y 5 bonos de \$8.

Podemos plantear el problema de Martín mediante una igualdad de números enteros: si Martín vendió x bonos de \$15 e y bonos de \$8, entonces la cantidad de dinero que recaudó es:

$$15 \cdot x + 8 \cdot y = 100$$

Esto es, las cantidades de bonos de cada tipo $x, y \in \mathbb{N}_0$ que puede haber vendido Martín son las soluciones en los números enteros no negativos para esta ecuación. A continuación vamos a ver cómo es posible resolver este tipo de ecuaciones sistemáticamente.

Más precisamente, *dados* $a, b, c \in \mathbb{Z}$, con a y b no nulos, nos interesa hallar las soluciones en los números enteros de la ecuación:

$$a \cdot x + b \cdot y = c \quad (2)$$

es decir, los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ para los cuales se cumple la igualdad.

Estas ecuaciones son una clase particular de las que se conocen como ecuaciones diofánticas⁴, que son ecuaciones con coeficientes enteros de las que se buscan soluciones en el conjunto de los números enteros.

Una ecuación de este tipo no siempre tiene solución; por ejemplo, la ecuación $12 \cdot x + 14 \cdot y = 123$ no tiene solución, porque para todo par de números $x, y \in \mathbb{Z}$, el resultado de $12 \cdot x + 14 \cdot y$ es un entero par:

$$12 \cdot x + 14 \cdot y = 2 \cdot (6 \cdot x + 7 \cdot y)$$

mientras que 123 es impar.

De la misma manera que en el ejemplo, vemos que si $d \in \mathbb{Z}$ es un divisor común de a y b , tenemos que $d \mid a \cdot x + b \cdot y$ para cualesquiera $x, y \in \mathbb{Z}$. Entonces, si $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación (2), resulta que $d \mid c$. Esto nos dice que para que la ecuación (2) tenga soluciones es necesario que todo divisor común de a y b sea también divisor de c .

Esta última condición es a su vez equivalente a que $(a : b)$ divida a c . En efecto, si todo divisor común de a y b divide a c , en particular lo divide su máximo común divisor $(a : b)$. Recíprocamente, si $(a : b)$ divide a c , como cualquier divisor común de a y b divide a $(a : b)$, por la transitividad de la divisibilidad, también divide a c .

Concluimos que:

Si $(a : b) \nmid c$, la ecuación $a \cdot x + b \cdot y = c$ no tiene soluciones en \mathbb{Z} .

Analícemos ahora en detalle un ejemplo en el que $(a : b) \mid c$.

EJEMPLO. Consideremos la ecuación $50 \cdot x + 630 \cdot y = 10$. Como vimos en la sección 5 del capítulo 2, esta ecuación tiene solución, ya que $10 = (50 : 630)$ es combinación lineal entera de 50 y 630:

$$50 \cdot (-25) + 630 \cdot 2 = 10$$

es decir $(x, y) = (-25, 2)$ es una solución.

A partir de esta solución podemos ver, por ejemplo, que la ecuación $50 \cdot x + 630 \cdot y = 20$ también tiene solución. Para obtener como resultado el doble de 10, basta duplicar los valores de x e y (o lo que es lo mismo, multiplicar por 2 la igualdad anterior):

$$50 \cdot (-25) \cdot 2 + 630 \cdot 2 \cdot 2 = 10 \cdot 2$$

⁴ El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra Aritmética.

o sea, que $(x, y) = ((-25) \cdot 2, 2 \cdot 2) = (-50, 4)$ es solución de esta nueva ecuación. De la misma manera, para cualquier $q \in \mathbb{Z}$ resulta que la ecuación $50 \cdot x + 630 \cdot y = 10 \cdot q$ tiene como solución a $(x, y) = (-25 \cdot q, 2 \cdot q)$, ya que:

$$50 \cdot (-25) \cdot q + 630 \cdot 2 \cdot q = 10 \cdot q$$

En general, sabemos que para cualesquiera $a, b \in \mathbb{Z}$ no simultáneamente nulos, $(a : b)$ es combinación lineal entera de a y b , es decir, existen números enteros s y t tales que:

$$a \cdot s + b \cdot t = (a : b)$$

Esto nos dice que la ecuación $a \cdot x + b \cdot y = (a : b)$ siempre tiene solución. Más aún, a partir de la igualdad de arriba vemos que, si $c = (a : b) \cdot q$, la ecuación (2) tiene como una solución a $(x, y) = (s \cdot q, t \cdot q)$, ya que:

$$a \cdot \underbrace{s \cdot q}_x + b \cdot \underbrace{t \cdot q}_y = (a \cdot s + b \cdot t) \cdot q = (a : b) \cdot q$$

Tenemos entonces también que:

Si $(a : b) \mid c$, la ecuación $a \cdot x + b \cdot y = c$ tiene soluciones en \mathbb{Z} .

Resumiendo, hemos probado la siguiente proposición:

PROPOSICIÓN 3.1. Sean $a, b, c \in \mathbb{Z}$ con a y b no nulos. La ecuación diofántica $a \cdot x + b \cdot y = c$ tiene soluciones en \mathbb{Z} si y solo si $(a : b)$ divide a c .

Veamos cómo son **todas** las soluciones de (2) cuando $(a : b)$ divide a c . En primer lugar, podemos dividir ambos miembros de (2) por $(a : b)$, obteniendo la nueva ecuación:

$$\frac{a}{(a : b)} \cdot x + \frac{b}{(a : b)} \cdot y = \frac{c}{(a : b)}$$

Esta ecuación tiene las mismas soluciones en $\mathbb{Z} \times \mathbb{Z}$ que la original (se puede pasar de una ecuación a la otra simplemente multiplicando o dividiendo por $(a : b)$). Si llamamos

$\alpha = \frac{a}{(a:b)}$, $\beta = \frac{b}{(a:b)}$ y $\gamma = \frac{c}{(a:b)}$, que son enteros, nos queda la ecuación:

$$\alpha \cdot x + \beta \cdot y = \gamma$$

donde ahora $(\alpha : \beta) = 1$ (observar que α y β son coprimos porque hemos suprimido todos los factores comunes de a y b). Supongamos que (x_0, y_0) es una solución de esta ecuación. Si (x, y) es otra solución, vale que $\alpha \cdot x + \beta \cdot y = \gamma = \alpha \cdot x_0 + \beta \cdot y_0$; entonces:

$$\alpha \cdot (x - x_0) = -\beta \cdot (y - y_0)$$

De esta igualdad deducimos que $\beta \mid \alpha \cdot (x - x_0)$ y, como $(\alpha : \beta) = 1$, entonces $\beta \mid x - x_0$ (ver la Proposición 2.4 del capítulo 2); luego, existe $k \in \mathbb{Z}$ tal que $x - x_0 = k \cdot \beta$. Reemplazando en la igualdad de arriba, nos queda que $\alpha \cdot k \cdot \beta = -\beta \cdot (y - y_0)$, de donde se desprende que $y - y_0 = -\alpha \cdot k$. En conclusión, toda solución (x, y) de la ecuación diofántica considerada es

de la forma $x = x_0 + k \cdot \beta, y = y_0 - k \cdot \alpha$, con $k \in \mathbb{Z}$.

TEOREMA 3.2. Sean $a, b, c \in \mathbb{Z}$, con a y b no nulos. Si $(a : b) \mid c$, entonces las soluciones de la ecuación diofántica $a \cdot x + b \cdot y = c$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tales que

$$x = x_0 + k \cdot \frac{b}{(a : b)}, \quad y = y_0 - k \cdot \frac{a}{(a : b)}, \quad \text{con } k \in \mathbb{Z}$$

donde (x_0, y_0) es una solución particular de la ecuación.

EJEMPLO. Volvamos al problema planteado al comienzo de esta sección: Martín vendió x bonos de \$15 e y bonos de \$8, y busca determinar los valores de x e y sabiendo que recaudó \$100, es decir, que:

$$15 \cdot x + 8 \cdot y = 100$$

Como $(15 : 8) = 1$, sabemos que la ecuación tiene soluciones. Comenzaremos buscando todas las soluciones en $\mathbb{Z} \times \mathbb{Z}$, y luego determinaremos las soluciones en $\mathbb{N}_0 \times \mathbb{N}_0$, que son las que le interesan a Martín.

En primer lugar, escribimos $1 = (15 : 8)$ como combinación lineal entera de 15 y 8. Para esto, utilizamos la información dada por el algoritmo de Euclides:

$$\begin{aligned} 15 &= 1 \cdot 8 + 7 &\longrightarrow 7 &= 15 - 1 \cdot 8 \\ 8 &= 1 \cdot 7 + 1 &\longrightarrow 1 &= 8 - 1 \cdot 7 \\ 7 &= 7 \cdot 1 &&= 8 - 1 \cdot (15 - 1 \cdot 8) \\ &&&= 15 \cdot (-1) + 8 \cdot 2 \end{aligned}$$

Ahora tomamos la identidad obtenida:

$$15 \cdot (-1) + 8 \cdot 2 = 1$$

y la multiplicamos por 100 para conseguir una solución de la ecuación original:

$$\begin{aligned} 15 \cdot (-1) \cdot 100 + 8 \cdot 2 \cdot 100 &= 100 \\ 15 \cdot (-100) + 8 \cdot 200 &= 100 \end{aligned}$$

Tenemos así una solución particular de la ecuación: $(x_0, y_0) = (-100, 200)$.

Por el Teorema 3.2, todas las soluciones enteras de la ecuación $15 \cdot x + 8 \cdot y = 100$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ donde:

$$x = -100 + k \cdot 8, \quad y = 200 - k \cdot 15, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, nos interesan aquellas soluciones en las cuales $x \geq 0$ e $y \geq 0$:

$$\begin{aligned} x \geq 0 &\iff -100 + k \cdot 8 \geq 0 \iff k \cdot 8 \geq 100 \iff k \geq 13 \quad (\text{porque } k \in \mathbb{Z}) \\ y \geq 0 &\iff 200 - k \cdot 15 \geq 0 \iff 200 \geq k \cdot 15 \iff 13 \geq k \quad (\text{porque } k \in \mathbb{Z}) \end{aligned}$$

De estas desigualdades deducimos que la única solución $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ se obtiene para $k = 13$:

$$\begin{aligned} x &= -100 + 13 \cdot 8, & y &= 200 - 13 \cdot 15 \\ &= 4 & &= 5 \end{aligned}$$

con lo cual, si recaudó \$100, Martín tiene que haber vendido 4 bonos de \$15 y 5 bonos de \$8.

EJERCICIO 3.1. Hallar todas las soluciones enteras de la ecuación $84 \cdot x + 270 \cdot y = 66$

□ 2. Congruencias

En esta sección vamos a presentar una noción de congruencia⁵ en el conjunto \mathbb{Z} , que resulta muy útil a la hora de trabajar con propiedades de divisibilidad sobre los números enteros.

Dado $m \in \mathbb{N}$, decimos que $a, b \in \mathbb{N}$ son *congruentes módulo m* , y escribimos $a \equiv b \pmod{m}$ o simplemente $a \equiv_{(m)} b$, si $m \mid a - b$. Si a y b no son congruentes módulo m , escribimos $a \not\equiv b \pmod{m}$.

Por ejemplo,

- $11 \equiv 5 \pmod{3}$, pues $3 \mid 11 - 5 = 6$,
- $11 \not\equiv -2 \pmod{4}$, pues $4 \nmid 11 - (-2) = 13$,
- $a \equiv b \pmod{1}$ para cualesquiera $a, b \in \mathbb{Z}$, ya que todo número entero es múltiplo de 1.

Observemos que, cualquiera sea $m \in \mathbb{N}$, tenemos que:

$$a \equiv 0 \pmod{m} \iff m \mid a.$$

Antes de continuar, analicemos más en detalle el caso $m = 2$.

Tenemos que $a \equiv b \pmod{2}$ si y sólo si $2 \mid a - b$. Si a es par, entonces $a = 2 \cdot \alpha$ para algún $\alpha \in \mathbb{Z}$, con lo cual $a - b = 2 \cdot \alpha - b$ es múltiplo de 2 si y sólo si b lo es, o sea, si y sólo si b es par. De la misma manera, si a es impar vemos que $2 \mid a - b$ si y sólo si b también es impar. En otras palabras:

$$a \equiv b \pmod{2} \iff a \text{ y } b \text{ son ambos pares o ambos impares.}$$

Esto nos dice que la congruencia módulo 2 *parte* al conjunto de los números enteros en dos subconjuntos: el de los enteros pares y el de los enteros impares. En cada uno de estos subconjuntos, dos elementos cualesquiera están relacionados, y un elemento de uno de estos conjuntos no está relacionado con uno del otro (es decir, un entero par es congruente a todo entero par y no es congruente a ningún impar, y un entero impar es congruente a cualquier impar, pero a ningún par). Podemos formalizar esto, mediante el concepto de relación de equivalencia.

Para $m \in \mathbb{N}$ fijo, consideremos la relación \mathcal{R} en \mathbb{Z} definida por

$$a \mathcal{R} b \iff a \equiv b \pmod{m}$$

⁵ Esta noción fue introducida por Carl Friedrich Gauss en su libro *Disquisitiones Arithmeticae* publicado en 1801.

Esta relación satisface:

- i) \mathcal{R} es reflexiva: $a \equiv a \pmod{m}$ para todo $a \in \mathbb{Z}$, ya que $m \mid a - a = 0$.
- ii) \mathcal{R} es simétrica: si $a \equiv b \pmod{m}$, entonces $m \mid a - b = -(b - a)$, con lo que también vale que $m \mid b - a$, es decir, que $b \equiv a \pmod{m}$.
- iii) \mathcal{R} es transitiva: si $a\mathcal{R}b$ y $b\mathcal{R}c$, es porque $m \mid a - b$ y $m \mid b - c$; pero entonces $m \mid (a - b) + (b - c) = a - c$, lo que dice que $a \equiv c \pmod{m}$.

Por lo tanto, \mathcal{R} es una relación de equivalencia. Como vimos en la sección 3 del capítulo 0, \mathcal{R} nos da una partición del conjunto \mathbb{Z} en subconjuntos disjuntos – las clases de equivalencia – tales que, dentro de cada uno de ellos, dos elementos cualesquiera están relacionados (en nuestro caso, son congruentes módulo m) y dos elementos de subconjuntos distintos no están relacionados.

Como vimos anteriormente, para $m = 2$ la relación de congruencia parte al conjunto \mathbb{Z} en 2 subconjuntos, $\{a \in \mathbb{Z} \mid a \text{ es par}\}$ y $\{a \in \mathbb{Z} \mid a \text{ es impar}\}$. El primero de ellos es la clase de equivalencia $[0]$ y el segundo, es la clase de equivalencia $[1]$. En el caso general, fijado $m \in \mathbb{N}$, la relación de congruencia módulo m parte al conjunto de los números enteros en m clases de equivalencia. La siguiente propiedad de la congruencia nos dice cómo son estas m clases.

PROPOSICIÓN 3.3. *Sea $m \in \mathbb{N}$. Para cada $a \in \mathbb{Z}$, si r es el resto de la división de a por m , vale $a \equiv r \pmod{m}$. Más aún, este resto es el único entero r tal que $0 \leq r < m$ que es congruente con a módulo m .*

DEMOSTRACIÓN. Si r es el resto de la división de a por m , existe un entero q tal que $a = m \cdot q + r$. Entonces $a - r = m \cdot q$, con lo que $m \mid a - r$ y, por lo tanto, $a \equiv r \pmod{m}$.

Por otro lado, si $a \equiv r \pmod{m}$, sabemos que $m \mid a - r$. Entonces existe $q \in \mathbb{Z}$ tal que $a - r = m \cdot q$; luego $a = m \cdot q + r$. Si vale $0 \leq r < m$, por la unicidad en el algoritmo de división, r es el resto de la división de a por m .

Como consecuencia de este resultado, fijado $m \in \mathbb{N}$, dos enteros distintos r_1 y r_2 con $0 \leq r_1, r_2 < m$ no son congruentes módulo m , es decir, las clases de equivalencia $[r_1]$ y $[r_2]$ son distintas. Además, todo entero a resulta congruente a su resto r en la división por m , y entonces $a \in [r]$. Luego, el conjunto de los enteros se parte como sigue:

$$\mathbb{Z} = [0] \cup [1] \cup \dots \cup [m - 1]$$

Volveremos sobre esta propiedad importante de la congruencia en la sección 4.

Algunas propiedades fundamentales de la congruencia son las siguientes:

PROPIEDADES 3.4. *Sea $m \in \mathbb{N}$. Entonces:*

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 $a \equiv b \pmod{m}$, entonces $c \cdot a \equiv c \cdot b \pmod{m}$ para todo $c \in \mathbb{Z}$;

3. si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;
4. si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$ para todo $k \in \mathbb{N}$;
5. si $c \cdot a \equiv c \cdot b \pmod{m}$ y $(c : m) = 1$, entonces $a \equiv b \pmod{m}$;
6. si $d \mid m$ y $a \equiv b \pmod{m}$, entonces $a \equiv b \pmod{d}$.

DEMOSTRACIÓN. Para demostrar estas propiedades se usan básicamente las propiedades de la divisibilidad vistas en el capítulo 2.

1. Por la definición de congruencia, tenemos que $m \mid a_1 - b_1$ y $m \mid a_2 - b_2$. Entonces, $m \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$; luego, $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
2. Tenemos que $m \mid a - b$, entonces también $m \mid c \cdot (a - b) = c \cdot a - c \cdot b$, con lo que $c \cdot a \equiv c \cdot b \pmod{m}$.
3. Por la propiedad anterior, como $a_1 \equiv b_1 \pmod{m}$, multiplicando por a_2 , resulta que $a_1 \cdot a_2 \equiv b_1 \cdot a_2 \pmod{m}$; análogamente, multiplicando por b_1 la congruencia $a_2 \equiv b_2 \pmod{m}$, obtenemos que $b_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ y finalmente, por la transitividad, concluimos que $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.
4. Se prueba por inducción aplicando la propiedad 3.
5. Por hipótesis, $m \mid c \cdot a - c \cdot b = c \cdot (a - b)$. Y como c y m son coprimos, por la Proposición 2.4 del capítulo 2, resulta que $m \mid a - b$, es decir, que $a \equiv b \pmod{m}$.
6. Como $d \mid m$ y $m \mid a - b$, la transitividad de la divisibilidad implica que $d \mid a - b$, o sea que $a \equiv b \pmod{d}$.

EJEMPLO. Veamos, utilizando la noción de congruencia y sus propiedades, que si $a, b, c \in \mathbb{Z}$ son tales que $a^2 + b^2 = c^2$, entonces $3 \mid a$ o $3 \mid b$.

Si 3 no divide a a ni a b , entonces tanto a como b tienen resto 1 ó 2 en la división por 3. Ahora bien, $1^2 = 1 \equiv_{(3)} 1$ y $2^2 = 4 \equiv_{(3)} 1$. Entonces, por la propiedad 4 anterior, tenemos que $a^2 \equiv 1 \pmod{3}$ y $b^2 \equiv 1 \pmod{3}$; luego, por la propiedad 1,

$$\begin{aligned} a^2 + b^2 &\equiv 1 + 1 \pmod{3} \\ &\equiv 2 \pmod{3} \end{aligned}$$

Esto implica que $c \in \mathbb{Z}$ debería cumplir que:

$$c^2 \equiv 2 \pmod{3}$$

Pero esto no puede ocurrir, puesto que si $c \equiv 0 \pmod{3}$, entonces $c^2 \equiv 0 \pmod{3}$ y, al igual que antes, si $c \equiv 1$ ó $2 \pmod{3}$, entonces $c^2 \equiv 1 \pmod{3}$.

EJEMPLO. Calcular la cifra de las unidades en el desarrollo decimal de 33^{666} .

Calculando las primeras potencias de 33:

$$\begin{aligned} 33^0 &= \underline{1} \\ 33^1 &= \underline{33} \\ 33^2 &= \underline{1.089} \\ 33^3 &= \underline{35.937} \\ 33^4 &= \underline{1.185.921} \\ 33^5 &= \underline{39.135.393} \\ \dots &\dots \dots \end{aligned}$$

vemos que las cifras de las unidades son 1, 3, 9, 7, 1, 3, ... Uno podría conjeturar que seguirá siempre así, repitiéndose la secuencia 1, 3, 9, 7 sucesivamente y, a partir de esto, tratar de determinar la cifra de las unidades pedidas.

Para formalizar esta idea utilizaremos congruencias. La observación fundamental es que si el desarrollo decimal de 33^{666} es $(n_s \dots n_1 n_0)_{10}$, entonces:

$$\begin{aligned} 33^{666} &= n_s \cdot 10^s + \dots + n_1 \cdot 10 + n_0 \\ &= 10 \cdot (n_s \cdot 10^{s-1} + \dots + n_1) + n_0 \quad \text{y } 0 \leq n_0 < 10 \end{aligned}$$

de donde deducimos que la cifra n_0 de las unidades es el *resto del número en la división por 10*. Para hallarlo, aplicaremos el resultado visto en la Proposición 3.3, o sea, buscaremos el único entero n_0 con $0 \leq n_0 < 10$ tal que $33^{666} \equiv n_0 \pmod{10}$.

Según los cálculos hechos al comienzo:

$$33^4 \equiv 1 \pmod{10}$$

Entonces, por la propiedad 4 de las Propiedades 3.4, para todo $k \in \mathbb{N}$, vale:

$$(33^4)^k \equiv 1^k \pmod{10}, \quad \text{o sea, } 33^{4 \cdot k} \equiv 1 \pmod{10}$$

Dividamos entonces al exponente 666 por 4: como $666 = 4 \cdot 166 + 2$, deducimos que:

$$\begin{aligned} 33^{666} &= 33^{4 \cdot 166 + 2} \\ &= 33^{4 \cdot 166} \cdot 33^2 \\ &\equiv_{(10)} 1 \cdot 9 \\ &= 9 \end{aligned}$$

donde la congruencia es consecuencia de la propiedad 3 de las Propiedades 3.4. En consecuencia, la cifra de las unidades en el desarrollo decimal de 33^{666} es 9.

Observemos que, aplicando estas mismas propiedades, podemos determinar la cifra de las unidades de 33^n para $n \in \mathbb{N}$ arbitrario: dado $n \in \mathbb{N}$, por el algoritmo de división, existen enteros k y r tales que $n = 4 \cdot k + r$ y $0 \leq r < 4$, con lo cual:

$$\begin{aligned} 33^n &= 33^{4 \cdot k + r} \\ &= \underbrace{33^{4 \cdot k}}_{\equiv_{(10)} 1} \cdot 33^r \\ &\equiv_{(10)} 33^r \end{aligned}$$

Concluimos entonces que la cifra de las unidades de 33^n coincide con la de 33^r , donde r es el resto de la división de n por 4; por lo tanto, de acuerdo a los cálculos hechos al comienzo, esta cifra es 1, 3, 9, 7 si $r = 0, 1, 2, 3$ respectivamente.

Como aplicación de las propiedades de la congruencia podemos deducir los conocidos *criterios de divisibilidad*. Comencemos analizando el criterio de divisibilidad por 9 que nos dice que “*un número natural n es múltiplo de 9 si y sólo si la suma de todos sus dígitos es múltiplo de 9*”. Observamos que si el desarrollo decimal de n es $(n_s \dots n_1 n_0)_{10}$, entonces

$$n = n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0$$

Queremos ver cuándo n es divisible por 9 o, equivalentemente, $n \equiv 0 \pmod{9}$. La clave para esto es observar que $10 \equiv 1 \pmod{9}$. Usando la propiedad 4 de las Propiedades 3.4, deducimos que $10^k \equiv 1 \pmod{9}$ para todo $k \in \mathbb{N}$ y, por lo tanto, de la escritura anterior de n , aplicando las propiedades 3 y 1, concluimos que:

$$\begin{aligned} n &= n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0 \\ &\equiv_{(9)} n_s \cdot 1 + \cdots + n_1 \cdot 1 + n_0 \\ &= n_s + \cdots + n_1 + n_0 \end{aligned}$$

En definitiva:

$$\text{si } n = (n_s \dots n_1 n_0)_{10}, \text{ entonces } n \equiv n_s + \cdots + n_1 + n_0 \pmod{9}$$

con lo cual, los enteros n y $n_s + \dots + n_1 + n_0$ tienen el mismo resto en la división por 9 (o sea, para conocer el resto de un número natural en la división por 9, basta sumar sus dígitos y calcular el resto en la división por 9 del número obtenido). En particular, n es múltiplo de 9 si y solo si $n_s + \dots + n_1 + n_0$ lo es.

EJERCICIO 3.2. Enunciar y probar la validez de los criterios de divisibilidad por 3, 4, 5, 8 y 11.

Sugerencias para la divisibilidad por 4 y 8: observar que $10^2 \equiv 0 \pmod{4}$ y que $10^3 \equiv 0 \pmod{8}$.

Sugerencias para la divisibilidad por 11: tener en cuenta que $10 \equiv -1 \pmod{11}$ y que $(-1)^k$ es 1 si k es par o -1 si k es impar. Proceder luego en forma análoga a lo que hicimos para analizar divisibilidad por 9.

Una aplicación de la congruencia: el ISSN de las publicaciones. El ISSN (*International Standard Serial Number*) es un número de ocho dígitos que se usa para identificar publicaciones periódicas, tanto impresas como electrónicas. Cada publicación periódica (por ejemplo, las revistas) tiene asignado un ISSN único.

Los siete primeros dígitos de los ISSN son asignados secuencialmente a las publicaciones, independientemente del país de origen, el idioma, etc. (es decir, el ISSN no contiene información en sí mismo).

El octavo dígito de un ISSN es un *dígito de control* y para determinarlo se utiliza aritmética modular: Si los primeros siete dígitos del ISSN son $d_1 d_2 d_3 d_4 d_5 d_6 d_7$, el octavo dígito d_8 se determina de manera que:

$$8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7 + d_8$$

sea múltiplo de 11. Para esto, se calcula $8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7$ módulo 11 y se elige d_8 convenientemente.

Por ejemplo, la revista *Journal of Algebra* tiene ISSN: 0021-8693. Esto significa que se le asignaron los 7 dígitos 0021869 y luego el dígito de control. Teniendo en cuenta que:

$$\begin{aligned}
8 \cdot 0 + 7 \cdot 0 + 6 \cdot 2 + 5 \cdot 1 + 4 \cdot 8 + 3 \cdot 6 + 2 \cdot 9 &= 0 + 0 + 12 + 5 + 32 + 18 + 18 \\
&\equiv_{(11)} 1 + 5 + (-1) + 7 + 7 \\
&\equiv_{(11)} 8
\end{aligned}$$

Si elegimos $d_8 = 3$, resulta que:

$$\begin{aligned}
8 + d_8 &= 11 \\
&\equiv 0 \pmod{11}.
\end{aligned}$$

Sin embargo, el dígito de control no siempre es un número entre 0 y 9. Por ejemplo, para la revista *Trends in Microbiology* se tiene que ISSN: 0966-842X. ¿A qué se debe la “X”? Procediendo como en el ejemplo anterior, se calcula:

$$\begin{aligned}
8 \cdot 0 + 7 \cdot 9 + 6 \cdot 6 + 5 \cdot 6 + 4 \cdot 8 + 3 \cdot 4 + 2 \cdot 2 &= 63 + 36 + 30 + 32 + 12 + 4 \\
&\equiv_{(11)} (-3) + 3 + 8 + (-1) + 1 + 4 \\
&\equiv_{(11)} 1
\end{aligned}$$

con lo cual, d_8 debe cumplir:

$$1 + d_8 \equiv 0 \pmod{11}$$

Ahora bien, el menor número natural que verifica esta igualdad es $d_8 = 10$. Cuando esto sucede, el dígito de control se escribe “X”.

□ 3. Ecuaciones de congruencia

Martín compró unas cajas de chocolates para repartir entre sus 19 compañeros de división de la Escuela 314. Como eran menos de 19 cajas, para darle la misma cantidad de chocolates a cada uno, las abrió y repartió el contenido entre sus compañeros. Luego de hacer esto, le quedaron 5 chocolates. Sabiendo que cada caja tenía 12 chocolates, ¿cuántas cajas repartió Martín?

Para responder esta pregunta, observemos que si Martín repartió una cantidad x de cajas de chocolates, entonces la cantidad total de chocolates repartidos es $12 \cdot x$. Al repartir estos chocolates entre sus 19 compañeros le quedaron 5. En términos de divisibilidad, esto significa que $12 \cdot x$ tiene resto 5 en la división por 19 y, en términos de congruencias, que:

$$12 \cdot x \equiv 5 \pmod{19}$$

Como sabemos que $1 \leq x < 19$, podemos determinar la cantidad x de cajas repartidas por Martín verificando, para cada posible valor de x , si esta condición se cumple o no.

- Si $x = 1$, serían $12 \cdot 1 = 12$ chocolates, y $12 \not\equiv 5 \pmod{19}$. Concluimos que Martín no repartió una sola caja.
- Si $x = 2$, serían $12 \cdot 2 = 24$ chocolates, y $24 \equiv 5 \pmod{19}$. Entonces es posible que Martín haya repartido 2 cajas de chocolates.
- Si $x = 3$, serían $12 \cdot 3 = 36$ chocolates, y $36 \equiv 17 \not\equiv 5 \pmod{19}$. Entonces, Martín no repartió 3 cajas.
- ...

Haciendo esta misma verificación para $x = 4, 5, \dots, 17, 18$, se ve que en ningún otro caso la cantidad total de chocolates resulta tener resto 5 en la división por 19. Concluimos entonces que Martín repartió 2 cajas de chocolates entre sus compañeros.

Para resolver el problema anterior, lo que hicimos fue buscar un entero x que sea solución de la ecuación $12 \cdot x \equiv 5 \pmod{19}$. Teniendo en cuenta que el valor buscado estaba comprendido entre 1 y 18, nos bastó con verificar cada uno de estos 18 casos. Pero esta verificación puede resultar ser muy larga si las cantidades involucradas son más grandes.

En lo que sigue estudiaremos *ecuaciones lineales de congruencia*. Se trata de ecuaciones del tipo:

$$a \cdot x \equiv b \pmod{m}$$

donde $m \in \mathbb{N}$ y $a, b \in \mathbb{Z}$, $a \neq 0$, están fijos y $x \in \mathbb{Z}$ es la incógnita.

Comencemos resolviendo la ecuación que apareció en el problema de las cajas de chocolates de Martín.

EJEMPLO. Hallar todos los $x \in \mathbb{Z}$ tales que $12 \cdot x \equiv 5 \pmod{19}$.

La condición $12 \cdot x \equiv 5 \pmod{19}$ es equivalente a que $19 \mid 12 \cdot x - 5$, es decir, a que exista $y \in \mathbb{Z}$ tal que:

$$12 \cdot x - 5 = 19 \cdot y$$

o, lo que es lo mismo, tal que:

$$12 \cdot x - 19 \cdot y = 5.$$

Ahora, ésta es una ecuación diofántica como las que estudiamos en la sección 1 de este capítulo y que ya sabemos resolver. Procediendo como vimos allí, resulta que $(40, 25)$ es una solución de esta ecuación y luego, todas sus soluciones son los pares de números enteros (x, y) de la forma $(x, y) = (40 + 19 \cdot k, 25 + 12 \cdot k)$ con $k \in \mathbb{Z}$.

En particular, lo que nos interesa para nuestro problema es que x es de la forma $x = 40 + 19 \cdot k$, que podemos reescribir usando la notación de congruencias como $x \equiv 40 \pmod{19}$, o bien (teniendo en cuenta que $40 \equiv 2 \pmod{19}$), como:

$$x \equiv 2 \pmod{19}$$

Observemos que esta ecuación tiene una única solución módulo 19, es decir, que existe un único x_0 solución de la ecuación que satisface $0 \leq x_0 < 19$ (en este caso $x_0 = 2$).

En el caso general, se puede proceder de la misma manera para llevar una ecuación de congruencias a una ecuación diofántica; para $x \in \mathbb{Z}$, vale que:

$$\begin{aligned} a \cdot x \equiv b \pmod{m} &\iff m \mid a \cdot x - b \iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - b = m \cdot y \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - m \cdot y = b \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } (x, y) \text{ es solución de } a \cdot x - m \cdot y = b \end{aligned}$$

Se resuelve la ecuación diofántica así obtenida y a partir de sus soluciones se obtienen, como en el ejemplo, las soluciones de la ecuación de congruencia original.

La equivalencia anterior entre ecuación de congruencia y ecuación diofántica nos provee un criterio para determinar cuándo una ecuación de congruencia tiene solución (ver en la Proposición 3.1 la condición que dedujimos para que la ecuación diofántica tenga soluciones):

$$a \cdot x \equiv b \pmod{m} \text{ tiene solución} \iff (a : m) \mid b$$

En particular, si a y m son coprimos, la ecuación $a \cdot x \equiv b \pmod{m}$ tiene solución para todo $b \in \mathbb{Z}$. En este caso, las soluciones de la ecuación diofántica $a \cdot x - m \cdot y = b$ son de la forma $(x_0 + m \cdot k, y_0 + a \cdot k)$, donde (x_0, y_0) es una solución particular. Entonces las soluciones a la ecuación de congruencia son todos los x de la forma $x = x_0 + m \cdot k$ con $k \in \mathbb{Z}$, lo que podemos reescribir como:

$$x \equiv x_0 \pmod{m}$$

En el caso general, si $(a : m) \mid b$, las soluciones de $a \cdot x \equiv b \pmod{m}$ son las mismas que las de:

$$\frac{a}{(a : m)} \cdot x \equiv \frac{b}{(a : m)} \pmod{\frac{m}{(a : m)}}$$

(Observar que ya vimos que las ecuaciones diofánticas asociadas a estas dos ecuaciones de congruencia tienen las mismas soluciones).

EJEMPLO. Hallar todas las soluciones de la ecuación $24 \cdot x \equiv 10 \pmod{38}$.

Como $(24 : 38) = 2$ divide a 10, esta ecuación tiene soluciones en \mathbb{Z} . Para hallarlas, podemos resolver la ecuación de congruencia más simple que se obtiene dividiendo la ecuación dada por 2 = $(24 : 38)$, es decir:

$$\frac{24}{2} \cdot x \equiv \frac{10}{2} \pmod{\frac{38}{2}} \iff 12 \cdot x \equiv 5 \pmod{19}$$

Pero esta ecuación es la que resolvimos en el ejemplo anterior. Concluimos entonces que las soluciones de $24 \cdot x \equiv 10 \pmod{38}$ son los $x \in \mathbb{Z}$ tales que:

$$x \equiv 2 \pmod{19}$$

La ecuación planteada en el ejemplo que acabamos de resolver es una ecuación de congruencia módulo 38, mientras que la caracterización que dimos para sus soluciones es módulo 19, que es un *divisor* de 38. Esto ocurre en general: dada la ecuación de congruencia $a \cdot x \equiv b \pmod{m}$, si $(a : m) \mid b$, existe un único entero x_0 , con $0 \leq x_0 < \frac{m}{(a : m)}$, tal que las soluciones de la ecuación son los enteros x que cumplen:

$$x \equiv x_0 \pmod{\frac{m}{(a : m)}}$$

EJERCICIO 3.3. Hallar, cuando existan, todas las soluciones a las siguientes ecuaciones lineales de congruencias:

- (a) $17 \cdot x \equiv 20 \pmod{45}$
- (b) $84 \cdot x \equiv 66 \pmod{270}$
- (c) $28 \cdot x \equiv 30 \pmod{60}$

EJERCICIO 3.4. Hallar todos los enteros a tales que el resto de dividir a $45 \cdot a$ por 27 es 9.

□ 4. El anillo de enteros módulo m

Como vimos en la sección 2 de este capítulo, la relación de congruencia módulo un número natural fijo m parte al conjunto de los enteros en m clases de equivalencia:

$$\mathbb{Z} = [0] \cup [1] \cup \dots \cup [m-1]$$

donde, para cada $0 \leq r < m$, la clase $[r]$ contiene a todos los enteros que tienen resto r en la división por m .

Escribiremos el conjunto de clases de equivalencia en la congruencia módulo m como \mathbb{Z}_m , es decir:

$$\mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$$

Gracias a las propiedades 3.4, en particular a las propiedades 1 y 3, a partir de la suma y producto de números enteros se pueden definir dos operaciones en \mathbb{Z}_m , suma y producto, de la siguiente forma:

$$\begin{aligned} [a] +_m [b] &= [a + b] \\ [a] \cdot_m [b] &= [a \cdot b] \end{aligned}$$

Observemos que la propiedad “ $a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ ” nos dice que el resultado de $[a] +_m [b]$ será el mismo sin importar qué elementos de las clases de equivalencia $[a]$ y $[b]$ consideremos para hacer la cuenta (y lo mismo nos dice la propiedad sobre el producto). En general, representamos cada clase de equivalencia módulo m por su único elemento comprendido entre 0 y $m-1$ (como hicimos más arriba).

Por ejemplo:

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

Calculemos algunas sumas y productos en \mathbb{Z}_6 .

- $[1] +_6 [3] = [1 + 3] = [4]$.
- $[2] +_6 [4] = [2+4] = [6] = [0]$. En consecuencia, $[4]$ es el inverso de $[2]$ para la suma en \mathbb{Z}_6 .
- $[3] \cdot_6 [5] = [3 \cdot 5] = [15] = [3]$, ya que $15 \equiv 3 \pmod{6}$.
- $[5] \cdot_6 [5] = [25] = [1]$, ya que $25 \equiv 1 \pmod{6}$. Entonces, $[5]$ es inverso de sí mismo para el producto en \mathbb{Z}_6 .

Podemos resumir las operaciones de suma y producto en \mathbb{Z}_6 por medio de las siguientes tablas:

$+_6$	[0]	[1]	[2]	[3]	[4]	[5]	\cdot_6	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[0]	[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[3]	[4]	[5]	[0]	[1]	[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[4]	[5]	[0]	[1]	[2]	[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[5]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[5]	[4]	[3]	[2]	[1]

Veamos algunas propiedades que cumplen las operaciones de suma y producto en \mathbb{Z}_m . En primer lugar, observamos que la asociatividad y conmutatividad de la suma y el producto en \mathbb{Z} hacen que $+_m$ y \cdot_m sean también *asociativas* y *conmutativas*. Por ejemplo:

$$\begin{aligned}
 ([a] +_m [b]) +_m [c] &= [a + b] +_m [c] \\
 &= [(a + b) + c] \\
 &= [a + (b + c)] \\
 &= [a] +_m [b + c] \\
 &= [a] +_m ([b] +_m [c])
 \end{aligned}$$

(Análogamente se puede ver que \cdot_m es asociativa y que $+_m$ y \cdot_m son conmutativas).

Las clase [0] es el elemento neutro de $+_m$ y [1] es el elemento neutro de \cdot_m . Por otra parte, todo elemento de \mathbb{Z}_m tiene un inverso para $+_m$, ya que $[a] +_m [-a] = [0]$; es decir, $[-a]$ es el inverso aditivo de $[a]$. Observemos que, sin embargo, no es cierto que todo elemento de \mathbb{Z}_m tenga inverso para \cdot_m . Por ejemplo, mirando la tabla de \cdot_6 , es claro que [2] no tiene inverso para \cdot_6 , puesto que $[2] \cdot_6 [a] \neq [1]$ para todo a .

Finalmente, al igual que ocurre en \mathbb{Z} , las operaciones $+_m$ y \cdot_m están relacionadas mediante la propiedad *distributiva* del producto sobre la suma:

$$\begin{aligned}
 [a] \cdot_m ([b] +_m [c]) &= [a] \cdot_m ([b + c]) \\
 &= [a \cdot (b + c)] \\
 &= [a \cdot b + a \cdot c] \\
 &= [a \cdot b] +_m [a \cdot c] \\
 &= ([a] \cdot_m [b]) +_m ([a] \cdot_m [c])
 \end{aligned}$$

Tenemos entonces que \mathbb{Z}_m con las operaciones $+_m$ y \cdot_m definidas arriba es un *anillo conmutativo con unidad*⁶ para cada $m \geq 2$.

OBSERVACIÓN. El producto de números enteros tiene la propiedad de que si $a, b \in \mathbb{Z}$ y $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$. Esto no ocurre en general en \mathbb{Z}_m : mirando la tabla de \cdot_6 vemos que, en \mathbb{Z}_6 , $[2] \cdot_6 [3] = [0]$, pero $[2] \neq [0]$ y $[3] \neq [0]$. Más aún, para cada $m \in \mathbb{N}$ compuesto, si $m = m_1 \cdot m_2$ con $m_1 > 1$ y $m_2 > 1$, resulta que $[m_1] \neq [0]$, $[m_2] \neq [0]$, pero $[m_1] \cdot_m [m_2] = [m_1 \cdot m_2] = [0]$.

⁶ El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra *Aritmética*.

La propiedad vale en \mathbb{Z}_p si p es primo, ya que $[a] \cdot [b] = [a \cdot b] = [0]$ si y sólo si $p \mid a \cdot b$, y esto ocurre si y sólo si $p \mid a$ o $p \mid b$, o sea, si y sólo si $[a] = [0]$ o $[b] = [0]$ en \mathbb{Z}_p .

EJERCICIO 3.5. Escribir las tablas de suma y producto en \mathbb{Z}_2 , \mathbb{Z}_4 y \mathbb{Z}_7 .

La “prueba del 9”. Una herramienta que puede utilizarse para detectar errores cuando se efectúan operaciones con números enteros utilizando su desarrollo decimal es la llamada *prueba del 9*.

La idea básica consiste en reemplazar cada número natural involucrado en las operaciones por un único dígito, hacer luego la cuenta original con estos dígitos, y comparar el dígito así obtenido con el asociado al resultado original. El dígito que se le asigna a un número natural se obtiene por medio del siguiente procedimiento:

1. se calcula la suma de los dígitos del número sin tener en cuenta los 9;
2. si el resultado obtenido es mayor o igual que 9, se vuelve a sumar sus dígitos sin considerar los 9;
3. se sigue así reemplazando un número por la suma de sus dígitos hasta obtener un único dígito que, si es 9, se reemplaza por 0.

Este procedimiento se basa en la propiedad “Si $n = (n_s \dots n_1 n_0)_{10}$, entonces $n \equiv n_s + \dots + n_1 + n_0 \pmod{9}$ ”. Utilizando esta propiedad, no es difícil convencerse de que el dígito asociado a cada número es simplemente su resto en la división por 9 y, por lo tanto, representa la misma clase de equivalencia en \mathbb{Z}_9 . Al efectuar la operación indicada con los dígitos obtenidos y volver a transformar el resultado en un dígito, no estamos haciendo otra cosa que calcular el resultado de la operación en \mathbb{Z}_9 .

Por ejemplo, si hacemos la suma $192.545 + 258.672$ y el resultado nos da 451.217 , para ver si hay un error calculamos:

- $192.545 \rightarrow 1 + 2 + 5 + 4 + 5 = 17 \rightarrow 1 + 7 = 8$
- $258.672 \rightarrow 2 + 5 + 8 + 6 + 7 + 2 = 30 \rightarrow 3$

Ahora efectuamos la suma de los dígitos obtenidos para los sumandos: $8 + 3 = 11$, reemplazamos el resultado por un único dígito $11 \rightarrow 1 + 1 = \boxed{2}$ y lo comparamos con el dígito asociado a la suma:

- $451.217 \rightarrow 4 + 5 + 1 + 2 + 1 + 7 = 20 \rightarrow 2 + 0 = \boxed{2}$

De esta manera obtenemos:

$$\begin{array}{r} + \quad 192.545 \rightarrow \quad \quad + \quad 8 \\ + \quad 258.672 \rightarrow \quad \quad + \quad 3 \\ \hline 451.217 \rightarrow \boxed{2} = \boxed{2} \end{array}$$

Como en este caso el resultado era el correcto, ambos dígitos coinciden. Sin embargo, el hecho de que la igualdad de los dígitos se cumpla no significa que la cuenta esté bien;

por ejemplo:

$$\begin{array}{r} + \quad 192.545 \rightarrow \quad \quad + \quad 8 \\ + \quad 258.672 \rightarrow \quad \quad + \quad 3 \\ \hline 451.\underline{127} \rightarrow \quad \boxed{2} = \boxed{2} \end{array}$$

Tiene dos dígitos del resultado con errores.

Ahora, si los dígitos obtenidos en la prueba del 9 difieren, podemos asegurar que ha ocurrido un error, ya que lo que estamos haciendo es calcular de dos maneras distintas la suma en \mathbb{Z}_9 .

$$\begin{array}{r} + \quad 192.545 \rightarrow \quad \quad + \quad 8 \\ + \quad 258.672 \rightarrow \quad \quad + \quad 3 \\ \hline 451.117 \rightarrow \quad \boxed{1} \neq \boxed{2} \end{array}$$

En este caso, el haber obtenido como resultados $1 \neq 2$ nos dice que hemos cometido un error (aunque no podemos saber en cuál de los dígitos).

Análogamente, podemos aplicar el procedimiento en el caso del producto de números naturales. Si multiplicamos, por ejemplo, 192.545×258.672 y obtenemos por resultado $49.807.100.240$, podemos darnos cuenta de que hay un error de la siguiente manera: el dígito asociado a 192.545 es 8 y el asociado a 258.672 es 3 ; haciendo la operación con estos dígitos obtenemos:

$$8 \cdot 3 = 24 \rightarrow 2 + 4 = \boxed{6}$$

mientras que, para el resultado de la cuenta original, tenemos que:

$$49.807.100.240 \rightarrow 4 + 8 + 7 + 1 + 2 + 4 = 26 \rightarrow 2 + 6 = \boxed{8}$$

Como los dígitos calculados no coinciden, concluimos que hubo un error en la cuenta. (De hecho, el resultado correcto de esta multiplicación es $49.806.000.240$.)

□ 5. Ecuaciones en \mathbb{Z}_m

Las ecuaciones de congruencia que estudiamos en la sección 3 pueden reinterpretarse como ecuaciones en \mathbb{Z}_m , simplemente observando que:

$$a \cdot x \equiv b \pmod{m} \iff [a] \cdot_m [x] = [b] \text{ en } \mathbb{Z}_m.$$

En lo que sigue, si queda claro en el contexto, escribiremos simplemente a para representar al elemento $[a] \in \mathbb{Z}_m$ y dejaremos de escribir los subíndices en la suma y el producto de \mathbb{Z}_m , es decir, escribiremos $+$ en lugar de $+_m$ y \cdot en lugar de \cdot_m .

Ahora la ecuación $[a] \cdot_m [x] = [b]$ queda simplemente:

$$a \cdot x = b \text{ en } \mathbb{Z}_m$$

que tiene una forma más familiar. ¿Cómo resolvemos esta ecuación? En la sección 3 vimos cómo hacer esto en el caso general (resolvimos la ecuación de congruencia). Lo que pretendemos aquí es mostrar un camino alternativo utilizando las operaciones en \mathbb{Z}_m .

La idea para “despejar” x en una ecuación del tipo $a \cdot x = b$ es “pasar dividiendo” el coeficiente a . Formalmente, esto significa *multiplicar ambos miembros* de la ecuación por el *inverso multiplicativo* de a :

Si a^{-1} es un elemento tal que:

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

entonces:

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

O, equivalentemente:

$$x = a^{-1} \cdot b$$

Reemplazando este valor de x en la ecuación vemos que, en efecto, es una solución, ya que:

$$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$$

Así, si queremos resolver, por ejemplo, la ecuación $5 \cdot x = 4$ en \mathbb{Z}_7 , como $3 \cdot 5 = 1$ en \mathbb{Z}_7 (o sea, 3 es el inverso multiplicativo de 5 en \mathbb{Z}_7), tenemos que:

$$5 \cdot x = 4 \text{ en } \mathbb{Z}_7 \implies \underbrace{3 \cdot 5}_{=1} \cdot x = 3 \cdot 4 \text{ en } \mathbb{Z}_7 \implies x = 5 \text{ en } \mathbb{Z}_7$$

y ésta es la (única) solución de la ecuación en \mathbb{Z}_7 .

Esto nos dice que cuando $a \in \mathbb{Z}_m$ tiene inverso multiplicativo $a^{-1} \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene una única solución, $x = a^{-1} \cdot b$. En cambio, si $a \in \mathbb{Z}_m$ no tiene inverso multiplicativo, la ecuación $a \cdot x = b$ puede no tener soluciones o tener más de una solución. Por ejemplo, la ecuación $2 \cdot x = 1$ en \mathbb{Z}_4 no tiene solución, ya que es equivalente a la ecuación de congruencias $2 \cdot x \equiv 1 \pmod{4}$ y $(2 : 4) = 2$, que no divide a 1. Consideremos, por otro lado, la ecuación:

$$2 \cdot x = 2 \text{ en } \mathbb{Z}_4$$

A simple vista, deducimos que $x = 1 \in \mathbb{Z}_4$ es una solución de esta ecuación. Pero no es la única: $x = 3 \in \mathbb{Z}_4$ también lo es.

Ya vimos que, para un número natural m cualquiera, no todo elemento de \mathbb{Z}_m tiene inverso multiplicativo. Por ejemplo: recién vimos que $2 \in \mathbb{Z}_4$ no tiene inverso multiplicativo. Tratemos de caracterizar los elementos que sí tienen inverso.

Sea $m \in \mathbb{N}$ fijo. Dado $a \in \mathbb{Z}_m$, un inverso multiplicativo para a en \mathbb{Z}_m es un elemento $x \in \mathbb{Z}_m$ tal que:

$$a \cdot x = 1 \text{ en } \mathbb{Z}_m \text{ o, equivalentemente, } a \cdot x \equiv 1 \pmod{m}$$

Sabemos que esta última ecuación tiene solución si y sólo si $(a : m)$ divide a 1; pero para que esta condición valga, necesariamente debe ser $(a : m) = 1$. En definitiva:

$a \in \mathbb{Z}_m$ tiene inverso multiplicativo si y sólo si $(a : m) = 1$.

Por ejemplo:

- en \mathbb{Z}_6 los únicos elementos que tienen inverso multiplicativo son $a = 1$ y $a = 5$, ya que 1 y 5 son los únicos enteros comprendidos entre 0 y 5 que son coprimos con 6 (comparar con la tabla de \cdot_6 en la sección 4);
- todos los elementos de \mathbb{Z}_7 , salvo el 0, tienen inverso multiplicativo, porque $(a : 7) = 1$ para todo $1 \leq a \leq 6$;
- en \mathbb{Z}_8 , los elementos que tienen inverso multiplicativo son las clases de los números impares, es decir, 1, 3, 5 y 7.

Es claro que $0 \in \mathbb{Z}_m$ no puede tener inverso multiplicativo para ningún $m \geq 2$, puesto que $0 \cdot x = 0 \neq 1$ para cualquier $x \in \mathbb{Z}_m$. Pero, por ejemplo, en \mathbb{Z}_7 , todo elemento $a \neq 0$ tiene inverso multiplicativo. Nos preguntamos, ¿cómo son los $m \in \mathbb{N}$ para los cuales todo elemento $a \in \mathbb{Z}_m$, $a \neq 0$, tiene inverso multiplicativo? Por lo que vimos antes, esto es equivalente a que $(a : m) = 1$ para todo a tal que $1 \leq a \leq m - 1$. Esto ocurre si m es *primo*: en este caso, los únicos divisores positivos de m son 1 y m , con lo cual, si $1 \leq a \leq m - 1$, el único posible divisor positivo común de a y m es 1; luego, $(a : m) = 1$. Por otro lado, si m no es primo, entonces m puede escribirse como un producto de dos números naturales menores que m , es decir, $m = a \cdot a'$ con $1 < a, a' < m$. Entonces $a \in \mathbb{Z}_m$ es no nulo y no tiene inverso multiplicativo, ya que $(a : m) = a \neq 1$.

Un anillo conmutativo con unidad en el que todo elemento no nulo tiene inverso multiplicativo se llama un *cuerpo*. El razonamiento anterior prueba que:

TEOREMA 3.5. \mathbb{Z}_m es un cuerpo si y sólo si $m \in \mathbb{N}$ es primo.

EJERCICIO 3.6.

1. Hallar los inversos multiplicativos de todos los elementos no nulos de \mathbb{Z}_7 .
2. Determinar todos los elementos de \mathbb{Z}_{14} que tienen inverso multiplicativo y hallar dichos inversos.

Volviendo a las ecuaciones lineales, el resultado anterior nos dice que, si m es primo y $a \neq 0 \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene una única solución en \mathbb{Z}_m . Cuando m no es primo, la ecuación $a \cdot x = b$ tiene solución en \mathbb{Z}_m si y sólo si $(a : m) \mid b$. En caso que esto ocurra, existe un único entero x_0 con $0 \leq x_0 < \frac{m}{(a:m)}$ tal que las soluciones son todos los enteros x que cumplen $x \equiv x_0 \pmod{\frac{m}{(a:m)}}$, es decir, los enteros de la forma $x = x_0 + k \cdot \frac{m}{(a:m)}$ con $k \in \mathbb{Z}$. No es difícil ver que:

$$x_0, x_0 + \frac{m}{(a : m)}, x_0 + 2 \cdot \frac{m}{(a : m)}, \dots, x_0 + ((a : m) - 1) \cdot \frac{m}{(a : m)}$$

pertencen a clases de equivalencia distintas en \mathbb{Z}_m y que cualquier otro entero de la forma $x_0 + k \cdot \frac{m}{(a:m)}$ pertenece a la clase de alguno de ellos. Concluimos que:

Si $(a : m) \mid b$, la ecuación $a \cdot x = b$ tiene exactamente $(a : m)$ soluciones distintas en \mathbb{Z}_m , que son de la forma

$$x_0 + k \cdot \frac{m}{(a : m)} \quad \text{con } 0 \leq k < (a : m)$$

para algún x_0 tal que $0 \leq x_0 < \frac{m}{(a:m)}$

EJERCICIO 3.7. Para cada una de las siguientes ecuaciones, determinar si tiene soluciones y, en caso afirmativo, hallarlas:

- $5 \cdot x = 4$ en \mathbb{Z}_{14}
- $6 \cdot x = 10$ en \mathbb{Z}_{21}
- $20 \cdot x = 12$ en \mathbb{Z}_{24}

□ 6. Teorema chino del resto

Lorena y sus amigas juegan al *Corazones*, que es un juego de cartas que se juega con un mazo de cartas francesas, sin los comodines (son 52 cartas). No vamos a entrar en los detalles del juego, simplemente diremos que al comienzo de cada mano de *Corazones* se reparten las cartas de manera que todos los jugadores tengan la misma cantidad (eventualmente pueden sobrar algunas).

En el caso de Lorena y sus amigas, aunque ellas no lo saben, al mazo de cartas con el que están jugando le faltan algunas cartas. En la primera mano juegan 5 de las amigas; Lorena reparte todas las cartas que puede y le sobran 2. En la mano siguiente, juegan 4 y sobran 3 cartas (estaban un poco distraídas y no se dieron cuenta de que esto no puede ser). Finalmente, juegan una última mano entre 3 de las amigas y al repartir las cartas sobran 2. En este momento Lorena, que no estaba jugando porque había salido última en la mano anterior, se da cuenta de que no puede ser que sobren 2 cartas (¿cómo lo supo?).

Lorena se pregunta cuántas cartas faltan en el mazo y decide intentar calcular este número sin interrumpir el juego (o sea, ¡sin contar las cartas!). Haciendo memoria sobre lo que ocurrió en las manos anteriores, razona como sigue:

Si x es la cantidad de cartas que hay en el mazo, entonces

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \end{cases}$$

Como la cantidad de cartas es $x \leq 52$, por la condición $x \equiv 2 \pmod{5}$, Lorena deduce que:

$$x \in \{2, \underline{7}, 12, 17, 22, \underline{27}, 32, 37, 42, \underline{47}, 52\}$$

De entre estos posibles valores, se queda con los que además cumplen que $x \equiv 3 \pmod{4}$, es decir

$$x \in \{7, 27, \underline{47}\}$$

y de estos, busca los que cumplen que $x \equiv 2 \pmod{3}$. El único valor con esta propiedad resulta ser:

$$x = 47$$

Lorena concluye que están jugando con 47 cartas, es decir, que faltan 5 en el mazo.

El problema general que trataremos en esta sección es el de la resolución de *sistemas de ecuaciones de congruencias*. Más precisamente, dados $m_1, m_2, \dots, m_n \in \mathbb{N}$ y $a_1, a_2, \dots, a_n \in \mathbb{Z}$, se busca hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv a_1 & (\text{mód } m_1) \\ x \equiv a_2 & (\text{mód } m_2) \\ \vdots \\ x \equiv a_n & (\text{mód } m_n) \end{cases} \quad (3)$$

Un sistema de ecuaciones de este tipo no siempre tiene solución; por ejemplo, el sistema:

$$\begin{cases} x \equiv 1 & (\text{mód } 2) \\ x \equiv 4 & (\text{mód } 6) \end{cases}$$

no tiene soluciones. En efecto, la condición $x \equiv 4 \pmod{6}$ implica que $x \equiv 4 \pmod{2}$ (por la propiedad 6 de la Proposición 3.4). O sea, un entero x que satisface la segunda ecuación debe ser par. Pero la primera condición, $x \equiv 1 \pmod{2}$, pide que x sea impar.

Una situación en la que podemos asegurar que el sistema de ecuaciones de congruencias sí tiene soluciones es cuando los módulos m_1, \dots, m_n son coprimos de a pares, es decir, si dos cualesquiera de ellos son coprimos.

TEOREMA 3.6 (Teorema chino del resto⁷). *Sean $m_1, m_2, \dots, m_n \in \mathbb{N}$ coprimos de a pares, y sean $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Entonces existe un único $x_0 \in \mathbb{Z}$ con $0 \leq x_0 < m_1 \cdot m_2 \cdot \dots \cdot m_n$ que es solución del sistema de ecuaciones:*

$$\begin{cases} x \equiv a_1 & (\text{mód } m_1) \\ x \equiv a_2 & (\text{mód } m_2) \\ \vdots \\ x \equiv a_n & (\text{mód } m_n) \end{cases}$$

y, además, un entero x es solución de las ecuaciones si y sólo si:

$$x \equiv x_0 \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_n}$$

DEMOSTRACIÓN. Existencia. Haremos la demostración por inducción en n , la cantidad de ecuaciones del sistema. Para $n = 1$ no hay nada que hacer, ya que el sistema es en realidad una única ecuación de congruencia.

Supongamos que el enunciado vale para sistemas de n ecuaciones y consideremos un sistema de $n + 1$ ecuaciones:

$$\begin{cases} x \equiv a_1 & (\text{mód } m_1) \\ \vdots \\ x \equiv a_n & (\text{mód } m_n) \\ x \equiv a_{n+1} & (\text{mód } m_{n+1}) \end{cases}$$

⁷ El origen de este teorema es un problema similar al que planteamos al comienzo de esta sección que aparece en el Manual Matemático escrito por Sun Zi alrededor del año 300. Un método para resolver este problema en el caso general fue dado en el Tratado de Matemática en Nueve Secciones, escrito por Qin Jiushao en 1247.

con $(m_i, m_j) = 1$ para todo $i \neq j$. Por la hipótesis inductiva, el sistema formado por las primeras n ecuaciones es equivalente a una única ecuación de congruencia:

$$x \equiv A \pmod{m_1 \cdots m_n}$$

para un (único) entero A con $0 \leq A < m_1 \cdots m_n$. Esto dice que los enteros x que cumplen las primeras n ecuaciones son aquéllos de la forma $x = M \cdot Q + A$ con $Q \in \mathbb{Z}$, donde $M = m_1 \cdots m_n$.

Las soluciones del sistema original son los x de esta forma que además cumplen la última ecuación; o sea $x = M \cdot Q + A$ para $Q \in \mathbb{Z}$ tal que $M \cdot Q + A \equiv a_{n+1} \pmod{m_{n+1}}$. Ahora, esta última condición es equivalente a la ecuación de congruencia:

$$M \cdot Q \equiv a_{n+1} - A \pmod{m_{n+1}}$$

Como por hipótesis $(m_i, m_{n+1}) = 1$ para cada $1 \leq i \leq n$, entonces $M = m_1 \cdots m_n$ resulta también coprimo con m_{n+1} y, por lo tanto, la ecuación anterior tiene solución. Más aún, las soluciones son de la forma:

$$Q \equiv q \pmod{m_{n+1}}$$

para un único q con $0 \leq q < m_{n+1}$, es decir, de la forma $Q = m_{n+1} \cdot k + q$ con $k \in \mathbb{Z}$. En definitiva, las soluciones del sistema son los $x \in \mathbb{Z}$ tales que:

$$\begin{aligned} x &= M \cdot Q + A \\ &= M \cdot (m_{n+1} \cdot k + q) + A \\ &= M \cdot m_{n+1} \cdot k + M \cdot q + A \\ &= (m_1 \cdots m_n \cdot m_{n+1}) \cdot k + (M \cdot q + A) \end{aligned}$$

Llamando $x_0 = M \cdot q + A$, esto es equivalente a la ecuación:

$$x \equiv x_0 \pmod{m_1 \cdots m_n \cdot m_{n+1}}$$

Como $0 \leq q \leq m_{n+1} - 1$ y $0 \leq A \leq M - 1$, resulta que

$$0 \leq x_0 \leq M \cdot (m_{n+1} - 1) + M - 1 = M \cdot m_{n+1} - 1 = m_1 \cdots m_n \cdot m_{n+1} - 1.$$

Unicidad. Supongamos que $0 \leq x_0 < x'_0 < m_1 \cdots m_n$ son dos soluciones del sistema dado. Entonces $x_0 \equiv x'_0 \pmod{m_i}$ para cada $1 \leq i \leq n$ (ya que ambos son congruentes a a_i); es decir, $m_i \mid x'_0 - x_0$ para todo $1 \leq i \leq n$. En otras palabras, $x'_0 - x_0$ es un múltiplo común de m_1, \dots, m_n . Pero como m_1, \dots, m_n son coprimos de a pares, su mínimo común múltiplo es $m_1 \cdots m_n$; luego, $x'_0 - x_0$ es múltiplo de $m_1 \cdots m_n$. Como $0 \leq x'_0 - x_0 < m_1 \cdots m_n$, esto implica que necesariamente $x'_0 - x_0 = 0$, es decir, $x'_0 = x_0$.

El teorema nos asegura que, si los módulos son coprimos de a pares, vamos a encontrar una solución x_0 (y sólo una) para el sistema (3) que cumple $0 \leq x_0 < m_1 \cdot m_2 \cdots m_n$, y que todas las soluciones del sistema son los enteros de la forma $x = m_1 \cdot m_2 \cdots m_n \cdot k + x_0$ con $k \in \mathbb{Z}$.

Algoritmo para resolver el sistema (3) si m_1, \dots, m_n son coprimos de a pares.

- Definir $M_1 = m_1$ y $A_1 = a_1$. De la primera ecuación, $x \equiv a_1 \pmod{m_1}$, se deduce que las soluciones son de la forma $x = M_1 \cdot Q_1 + A_1$ con $Q_1 \in \mathbb{Z}$.
- Para $i = 1, \dots, n-1$:

resolver $M_i \cdot Q_i + A_i \equiv a_{i+1} \pmod{m_{i+1}}$

(donde la incógnita es Q_i). Sea $q_i \in \mathbb{Z}$ con $0 \leq q_i < m_{i+1}$ tal que las soluciones de esta ecuación son $Q_i \equiv q_i \pmod{m_{i+1}}$:

definir $M_{i+1} = M_i \cdot m_{i+1}$, $A_{i+1} = M_i \cdot q_i + A_i$

Entonces las soluciones del sistema formado por las primeras $i+1$ ecuaciones son de la forma $x = M_{i+1} \cdot Q_{i+1} + A_{i+1}$ con $Q_{i+1} \in \mathbb{Z}$.

- Dar como respuesta $x \equiv A_n \pmod{M_n}$.

Saber que hay una solución en un rango acotado nos permite hallarla por búsqueda exhaustiva (si es que el rango no es demasiado grande). Como Lorena en el ejemplo, buscamos todos los enteros x con $0 \leq x < m_1 \cdot m_2 \dots m_n$ tales que $x \equiv a_1 \pmod{m_1}$; de estos nos quedamos con aquellos que también cumplen que $x \equiv a_2 \pmod{m_2}$, y seguimos así, agregando en cada paso una restricción, hasta llegar a tener un único elemento en la lista. Sin embargo, para valores grandes de m_1, \dots, m_n esta búsqueda puede volverse tediosa. Resulta entonces más conveniente proceder resolviendo las ecuaciones sucesivamente.

EJEMPLO. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 14 \pmod{49} \\ x \equiv 17 \pmod{45} \end{cases}$$

Como $(49 : 45) = 1$, el Teorema chino del resto asegura que el sistema tiene soluciones y que tiene

una única solución x_0 con $0 \leq x_0 < 49 \cdot 45 = 2.205$. Buscaremos la solución resolviendo sucesivamente las ecuaciones.

Las soluciones de la primera ecuación, $x \equiv 14 \pmod{49}$, son todos los enteros x de la forma:

$$x = 49 \cdot q + 14, \quad \text{con } q \in \mathbb{Z}$$

De entre todos los posibles q , nos interesan aquéllos que hacen que se cumpla la segunda ecuación, $x \equiv 17 \pmod{45}$; en términos de q , esto es que $49 \cdot q + 14 \equiv 17 \pmod{45}$. En definitiva, nos queda una ecuación lineal de congruencia; basta determinar los $q \in \mathbb{Z}$ tales que:

$$49 \cdot q \equiv 3 \pmod{45}.$$

Acá vemos la importancia de que $(49 : 45) = 1$, que es lo que nos asegura que esta ecuación, y por lo tanto también el sistema original, tiene solución. Reduciendo módulo 45, la ecuación anterior queda $4 \cdot q \equiv 3 \pmod{45}$ y vemos que una solución es $q_0 = 12$ (en el caso general, resolvemos la ecuación de congruencia como vimos en la sección 3); luego todas sus soluciones son los $q \equiv 12 \pmod{45}$, es decir:

$$q = 45 \cdot k + 12, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, concluimos que las soluciones del sistema son todos los enteros x de la forma $x = 49 \cdot q + 14 = 49 \cdot (45 \cdot k + 12) + 14 = 49 \cdot 45 \cdot k + 602 = 2.205 \cdot k + 602$, con $k \in \mathbb{Z}$.

En el caso de un sistema de ecuaciones de congruencia en el que los módulos no son coprimos, lo que puede hacerse es tratar de reducirlo a otro en el que sí lo sean. Para hacer esto, la observación fundamental es que si $m = m_1 \cdot m_2 \dots m_r$ con m_1, \dots, m_r coprimos de a pares, entonces:

$$x \equiv a \pmod{m} \iff \begin{cases} x \equiv a & (\text{mód } m_1) \\ \vdots \\ x \equiv a & (\text{mód } m_r) \end{cases}$$

EJEMPLO. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 3 & (\text{mód } 12) \\ x \equiv 9 & (\text{mód } 14) \end{cases}$$

Tenemos que:

$$\begin{aligned} x \equiv 3 \pmod{12} &\iff \begin{cases} x \equiv 3 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases} \iff \begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases} \\ x \equiv 9 \pmod{14} &\iff \begin{cases} x \equiv 9 & (\text{mód } 2) \\ x \equiv 9 & (\text{mód } 7) \end{cases} \iff \begin{cases} x \equiv 1 & (\text{mód } 2) \\ x \equiv 2 & (\text{mód } 7) \end{cases} \end{aligned}$$

Aquí los módulos no son coprimos de a pares, $(4 : 2) = 2$, pero vemos que la validez de la segunda ecuación implica la de la tercera. Luego, podemos suprimir esta última y resolver el sistema que queda:

$$\begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \\ x \equiv 2 & (\text{mód } 7) \end{cases} \iff x \equiv 51 \pmod{3 \cdot 4 \cdot 7}$$

Concluimos que las soluciones del sistema dado son los enteros de la forma $x = 84 \cdot k + 51$ con $k \in \mathbb{Z}$.

EJERCICIO 3.8. Un grupo de amigos va a cenar a una pizzería. Cuando llega la cuenta, en la mesa son 10 personas; si todos ponen la misma cantidad (entera) de dinero, recolectan \$6 más que lo que debían pagar. En ese momento vuelve a la mesa Martín (es decir, en realidad eran 11 amigos y no 10). Reparten entonces los gastos entre los 11, y sobran \$10. Sabiendo que juntaron más de \$100, ¿cuánto es lo mínimo que puede haberles costado la cena?

EJERCICIO 3.9.

- Hallar todos los enteros que tienen resto 1 en la división por 3, resto 2 en la división por 5 y resto 5 en la división por 7.
- Hallar, si existen, todos los enteros que tienen resto 8 en la división por 12 y resto 6 en la división por 20.

□ 7. Pequeño teorema de Fermat

Como vimos en uno de los ejemplos de la sección 2, los restos de dividir las sucesivas potencias de un entero a por un entero m se repiten en algún momento (porque hay sólo una cantidad finita de restos posibles, mientras que consideramos infinitas potencias). Para simplificar los cálculos, es útil conocer un exponente donde ocurre esta repetición. El *pequeño teorema de Fermat*⁸ es un

⁸ Este teorema fue enunciado originalmente por Pierre de Fermat en una carta en 1640. Aunque se supone que Leibniz lo demostró unos pocos años después, fue recién en 1736 que Euler publicó la primera demostración. Más adelante, en 1760, Euler también probó una generalización del teorema.

resultado fundamental que nos da esa información.

TEOREMA 3.7 (Pequeño teorema de Fermat). *Sea $p \in \mathbb{N}$ un primo. Para cada $a \in \mathbb{Z}$ que no es múltiplo de p , vale que $a^{p-1} \equiv 1 \pmod{p}$. Más aún, para todo $a \in \mathbb{Z}$ vale que $a^p \equiv a \pmod{p}$.*

DEMOSTRACIÓN. Sea $a \in \mathbb{Z}$ no divisible por p . Sea $[a] \in \mathbb{Z}_p^*$ la clase de equivalencia de a . Tenemos que $[a] \neq [0]$. Consideremos el conjunto \mathbb{Z}_p^* de todos los elementos no nulos de \mathbb{Z}_p ,

$$\mathbb{Z}_p^* = \{[1], [2], \dots, [p-1]\}$$

Vamos a multiplicar cada elemento de \mathbb{Z}_p^* por $[a]$ y a mirar el conjunto obtenido de esta manera. Observemos que si $[b], [c] \in \mathbb{Z}_p^*$ y $[a] \cdot [b] = [a] \cdot [c]$, necesariamente $[b] = [c]$ porque podemos multiplicar ambos miembros de la primera igualdad por el inverso multiplicativo de $[a]$; en particular, $[a] \cdot [b] \neq 0$ si $[b] \neq 0$. Entonces, deducimos que el conjunto:

$$[a] \cdot \mathbb{Z}_p^* = \{[a] \cdot [1], [a] \cdot [2], \dots, [a] \cdot [p-1]\}$$

está formado por $p-1$ elementos del conjunto \mathbb{Z}_p^* *distintos entre sí*. Como \mathbb{Z}_p^* tiene a su vez $p-1$ elementos, concluimos que $[a] \cdot \mathbb{Z}_p^*$ contiene a *todos* los elementos de \mathbb{Z}_p^* , es decir, que $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$.

Multiplicando los elementos de $[a] \cdot \mathbb{Z}_p^*$ obtenemos, por un lado:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \dots \cdot ([a] \cdot [p-1]) &= [a]^{p-1} \cdot ([1] \cdot [2] \cdot \dots \cdot [p-1]) \\ &= [a]^{p-1} \cdot [1 \cdot 2 \cdot \dots \cdot (p-1)] \end{aligned}$$

Por otra parte, como $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$, el producto de estos elementos es el producto de los elementos de \mathbb{Z}_p^* (eventualmente hecho en otro orden), o sea:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \dots \cdot ([a] \cdot [p-1]) &= [1] \cdot [2] \cdot \dots \cdot [p-1] \\ &= [1 \cdot 2 \cdot \dots \cdot (p-1)] \end{aligned}$$

Igualando ambas expresiones para el producto, resulta que:

$$[a]^{p-1} \cdot [1 \cdot 2 \cdot \dots \cdot (p-1)] = [1 \cdot 2 \cdot \dots \cdot (p-1)]$$

Como p no divide a $1 \cdot 2 \cdot \dots \cdot (p-1)$, puesto que es primo y no divide a ninguno de los factores, tenemos que $[1 \cdot 2 \cdot \dots \cdot (p-1)] \neq [0]$, con lo que tiene inverso multiplicativo en \mathbb{Z}_p , y, multiplicando la igualdad anterior por dicho inverso, deducimos que:

$$[a]^{p-1} = 1$$

o, en términos de congruencias:

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

Para terminar, observemos que multiplicando ambos miembros de esta congruencia por a obtenemos que:

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

Pero esta igualdad vale también cuando $p \mid a$, ya que en este caso $a \equiv 0 \pmod{p}$ y también $a^p \equiv 0 \pmod{p}$.

OBSERVACIÓN. Sea $p \in \mathbb{N}$ primo y sea $a \in \mathbb{Z}$ no divisible por p . Entonces $a^n \equiv a^m \pmod{p}$ si n y m son números naturales tales que $n \equiv m \pmod{p-1}$. En particular, si r_{p-1} es el resto en la división de n por $p-1$, entonces $a^n \equiv a^{r_{p-1}} \pmod{p}$.

En efecto, suponiendo que $n \geq m$, si $n \equiv m \pmod{p-1}$, tenemos que $n = m + k \cdot (p-1)$ para algún $k \in \mathbb{N}_0$; luego:

$$\begin{aligned} a^n &= a^{m+k \cdot (p-1)} \\ &= a^m \cdot (a^{p-1})^k \\ &\equiv a^m \cdot 1^k \\ &\equiv a^m \pmod{p}. \end{aligned}$$

donde la anteúltima congruencia es consecuencia del pequeño teorema de Fermat.

EJEMPLO. Hallar el resto en la división de $3^{1.423}$ por 11.

Por la Proposición 3.3, sabemos que el resto buscado es el único entero r con $0 \leq r < 11$ tal que $3^{1.423} \equiv r \pmod{11}$. Ahora, por la observación anterior, como $1.423 \equiv 3 \pmod{10}$ tenemos que:

$$\begin{aligned} 3^{1.423} &\equiv 3^3 \\ &\equiv 5 \pmod{11} \end{aligned}$$

Luego, $r = 5$.

Mencionemos, para concluir esta sección, que como consecuencia del pequeño teorema de Fermat podemos obtener una expresión explícita para los inversos multiplicativos de los elementos de \mathbb{Z}_p , si $p \in \mathbb{N}$ es primo: *el inverso multiplicativo de un elemento $a \in \mathbb{Z}_p$, $a \neq 0$, es $a^{p-2} \in \mathbb{Z}_p$* . En efecto, tenemos que $a \cdot a^{p-2} = a^{p-1} = 1$ en \mathbb{Z}_p , con lo que $a^{-1} = a^{p-2}$ en \mathbb{Z}_p .

EJERCICIO 3.10. Hallar el resto en la división de a por m en los siguientes casos:

- $a = 129^{111}$, $m = 7$.
- $a = 129^{111}$, $m = 35$. (Sugerencia: calcular el resto en la división por 5 y por 7 y usar el teorema chino del resto).

□ 8. Aplicación: Tests de primalidad

Un *test de primalidad* es un procedimiento para determinar si un entero dado es primo o no lo es.

Dado $n \in \mathbb{N}$ un posible test de primalidad consiste en verificar si n es divisible por algún entero m tal que $2 \leq m \leq \sqrt{n}$. Si algún $m_0 \in \mathbb{N}$ con $2 \leq m_0 \leq \sqrt{n}$ divide a n , es claro que n es compuesto (hemos encontrado un divisor propio de n). De lo contrario, podemos asegurar que n es primo por el Lema 2.8 del capítulo 2. Este procedimiento nos permite decidir con certeza si n es primo.

Sin embargo, para valores grandes de n , la cantidad de operaciones a realizar (y por consiguiente, el tiempo que lleva hacerlas) puede resultar demasiado grande a los fines prácticos.

El pequeño teorema de Fermat ha dado lugar a tests de primalidad *probabilísticos* alternativos. La idea es que el método no nos permite determinar con certeza si n es primo, sino que podemos saberlo pero con cierta probabilidad de error.

8.1. Test de primalidad de Fermat

Este procedimiento funciona como explicamos a continuación:

- dado $n \in \mathbb{N}$, se elige al azar un entero a tal que $2 \leq a \leq n - 1$ y se calcula $a^{n-1} \pmod{n}$;
- si $a^{n-1} \not\equiv 1 \pmod{n}$, la respuesta es que n es compuesto;
- si $a^{n-1} \equiv 1 \pmod{n}$, la respuesta es que n probablemente sea primo.

Observemos que en caso que $a^{n-1} \not\equiv 1 \pmod{n}$, podemos estar seguros de que a **no** es primo, porque el pequeño teorema de Fermat nos dice que de serlo, debería ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ sin importar qué valor de a hayamos elegido.

Ahora bien, si n es compuesto puede ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ para algún a tal que $2 \leq a \leq n - 1$. Por ejemplo, para $n = 91 = 7 \cdot 13$ (¡que no es primo!) y $a = 3$ se tiene que $3^{90} = (3^6)^{15} = 729^{15} \equiv_{(91)} 1^{15} \equiv_{(91)} 1$. Es por este motivo que no podemos estar seguros de que n sea primo si la congruencia vale.

Sin embargo, si existe algún a coprimo con n tal que $a^{n-1} \not\equiv 1 \pmod{n}$, entonces lo mismo ocurre para al menos la mitad de los posibles $2 \leq a \leq n - 1$. Esto se debe a que, si a_1, \dots, a_s son todas las bases para las cuales $a_i^{n-1} \equiv 1 \pmod{n}$, entonces $(a \cdot a_i)^{n-1} = a^{n-1} \cdot a_i^{n-1} \equiv_{(n)} a^{n-1} \cdot 1 \equiv_{(n)} a^{n-1} \not\equiv_{(n)} 1$ y, además, $a \cdot a_1, \dots, a \cdot a_s$ son todos distintos módulo n , ya que a es coprimo con n . Así, hay una probabilidad menor que $1/2$ de que eligiendo a al azar se verifique $a^{n-1} \equiv 1 \pmod{n}$. Si el proceso se repite k veces, la probabilidad de que en todos los casos resulte $a^{n-1} \equiv 1 \pmod{n}$ es $1/2^k$ (¡muy chica si k es grande!).

El problema es que hay enteros compuestos n para los cuales $a^{n-1} \equiv 1 \pmod{n}$ para *todo* a coprimo con n . Estos enteros se conocen como *números de Carmichael* y el hecho de que sean compuestos los hace difícil de detectar para el test de Fermat (sólo nos damos cuenta de que n es compuesto si justo elegimos un a tal que $(a : n) \neq 1$).

El menor de estos números⁹ es $n = 561$; veamos que tiene la propiedad mencionada, es decir que:

$$a^{560} \equiv 1 \pmod{561}$$

⁹ Este número fue encontrado por Carmichael en 1910, de ahí el nombre que reciben los enteros con esta propiedad.

para todo $a \in \mathbb{Z}$ con $(a : 561) = 1$. Como $561 = 3 \cdot 11 \cdot 17$, para probar lo anterior basta ver que:

$$\begin{cases} a^{560} \equiv 1 & (\text{mód } 3) \\ a^{560} \equiv 1 & (\text{mód } 11) \\ a^{560} \equiv 1 & (\text{mód } 17) \end{cases}$$

Estas congruencias son consecuencia del pequeño teorema de Fermat: en efecto, si $(a : 561) = 1$, tenemos que a no es múltiplo de 3 ni de 11 ni de 17, y el teorema asegura entonces que:

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}$$

con lo cual:

$$\begin{aligned} a^{560} &= (a^2)^{280} & a^{560} &= (a^{10})^{56} & a^{560} &= (a^{16})^{35} \\ &\equiv 1 \pmod{3}, & &\equiv 1 \pmod{11}, & &\equiv 1 \pmod{17} \end{aligned}$$

8.2. Test de primalidad de Miller-Rabin

Este procedimiento alternativo para determinar si un entero dado es primo o no se basa en el pequeño teorema de Fermat más el hecho fundamental de que:

$$x^2 \equiv 1 \pmod{p} \iff x \equiv 1 \pmod{p} \quad \text{o} \quad x \equiv -1 \pmod{p}.$$

Esta equivalencia vale ya que, si p es primo, entonces $p \mid x^2 - 1 = (x - 1) \cdot (x + 1)$ si y sólo si $p \mid x - 1$ o $p \mid x + 1$ (recordar que un número primo divide a un producto si y sólo si divide a alguno de los factores). Más precisamente, ambos resultados se combinan en la siguiente propiedad:

PROPOSICIÓN 3.8. *Sea p un primo positivo impar. Factoricemos $p - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar. Entonces, para cada $a \in \mathbb{Z}$ que no es múltiplo de p se tiene que:*

$$a^t \equiv 1 \pmod{p} \quad \text{o} \quad a^{t \cdot 2^k} \equiv -1 \pmod{p} \quad \text{para algún } 0 \leq k < r$$

DEMOSTRACIÓN. Por el pequeño teorema de Fermat, sabemos que $a^{t \cdot 2^r} \equiv 1 \pmod{p}$. Como $r \geq 1$ porque $p - 1$ es par, podemos escribir $a^{t \cdot 2^r} = (a^{t \cdot 2^{r-1}})^2$ con $r - 1 \in \mathbb{N}_0$, y tenemos que:

$$(a^{t \cdot 2^{r-1}})^2 \equiv 1 \pmod{p}$$

Por lo que observamos más arriba, esto equivale a que:

$$a^{t \cdot 2^{r-1}} \equiv 1 \pmod{p} \quad \text{o} \quad a^{t \cdot 2^{r-1}} \equiv -1 \pmod{p}$$

Si $a^{t \cdot 2^{r-1}} \equiv -1 \pmod{p}$, se verifica la segunda condición del enunciado con $k = r - 1$. De lo contrario, resulta que $a^{t \cdot 2^{r-1}} \equiv 1 \pmod{p}$. Si $r - 1 = 0$, esto es simplemente la primera de las condiciones del enunciado. Finalmente, si $r - 1 \geq 1$, repitiendo el razonamiento anterior para $a^{t \cdot 2^{r-1}}$, deducimos que $a^{t \cdot 2^{r-2}} \equiv 1 \pmod{p}$ o $a^{t \cdot 2^{r-2}} \equiv -1 \pmod{p}$.

Siguiendo de la misma manera, o bien se llega en algún momento a un k con $0 \leq k \leq r - 1$ tal que $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, o bien resulta que $a^t \equiv 1 \pmod{p}$.

El *test de primalidad de Miller-Rabin* funciona entonces como sigue:

- dado $n \in \mathbb{N}$ impar, se escribe $n - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar;
- se elige a tal que $2 \leq a \leq n - 1$ al azar;
- se calcula $a^t \pmod{n}$. Si $a^t \equiv 1 \pmod{n}$ o $a^t \equiv -1 \pmod{n}$, decimos que *n probablemente sea primo*;
- si no, se calculan sucesivamente $a^{t \cdot 2} = (a^t)^2, a^{t \cdot 2^2} = (a^{t \cdot 2})^2, \dots, a^{t \cdot 2^k} = (a^{t \cdot 2^{k-1}})^2, \dots \pmod{p}$ hasta obtener como resultado -1 , o bien hasta llegar a $a^{t \cdot 2^{r-1}}$. Si en algún paso el resultado es $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, decimos que *n probablemente sea primo*. De lo contrario, tenemos que:

$$a^t \not\equiv 1 \pmod{n} \quad \text{y} \quad a^{t \cdot 2^k} \not\equiv -1 \text{ para todo } 0 \leq k \leq r - 1$$

y, por la proposición anterior, podemos asegurar que *n es compuesto*.

Se puede ver que si n es compuesto, la propiedad:

$$a^t \equiv 1 \pmod{n} \quad \text{o} \quad a^{t \cdot 2^k} \equiv -1 \pmod{n} \text{ para algún } 0 \leq k < r$$

se cumple a lo sumo para la cuarta parte de los a tales que $1 \leq a \leq n - 1$. Es decir, que la probabilidad de que para un n compuesto el test diga que n probablemente sea primo es a lo sumo $1/4$. Esto nos dice que repitiendo el test para distintos valores de a podemos hacer que la probabilidad de obtener una respuesta incorrecta sea muy chica.

EJEMPLO. Apliquemos el test de Miller-Rabin a $n = 561$.

- Escribimos $n - 1 = 560 = 35 \cdot 2^4$.
- Elegimos a tal que $2 \leq a \leq 560$, por ejemplo, $a = 2$.
- Calculamos $2^{35} \equiv 263 \pmod{561}$. Como $2^{35} \not\equiv 1 \pmod{561}$ y $2^{35} \not\equiv -1 \pmod{561}$, continuamos.
- Elevamos al cuadrado sucesivamente:
 - $(2^{35})^2 \equiv 263^2 \equiv 166 \not\equiv -1 \pmod{561}$
 - $(2^{35})^{2^2} \equiv 166^2 \equiv 67 \not\equiv -1 \pmod{561}$
 - $(2^{35})^{2^3} \equiv 67^2 \equiv 1 \not\equiv -1 \pmod{561}$
- Concluimos que 561 es *compuesto*.

□ 9. Aplicación: criptografía

La *criptografía* se encarga de estudiar cómo enviar mensajes de manera *secreta*. El

objetivo es que solamente el receptor a quien queremos enviarle el mensaje pueda leerlo y entenderlo, es decir, que si otra persona (en particular, alguien que nosotros no queremos que lea el mensaje) logra acceder a la información, no pueda interpretarla.

Para esto se utilizan distintos *métodos de encriptación* y, esencialmente, el proceso funciona como explicamos a continuación:

- el emisor *encripta* el mensaje, es decir, convierte la información original o *texto plano* en *texto cifrado*, que en apariencia no tiene sentido,
- se transmite el texto cifrado,
- el receptor *desencripta* el mensaje recibido, es decir, lo vuelve a su forma original.

Lo importante en este esquema es que si el texto cifrado es interceptado por quien no es el receptor, sea muy difícil o mejor aún, imposible, de descifrar.

Procedimientos de este tipo se han utilizado desde la antigüedad: por ejemplo, se cuenta que Julio César utilizaba un esquema de encriptación basado en una tabla como la siguiente:

0	A	D
1	B	E
2	C	F
3	D	G
4	E	H
5	F	I
6	G	J
7	H	K
8	I	L
9	J	M
10	K	N
11	L	O
12	M	P

13	N	Q
14	O	R
15	P	S
16	Q	T
17	R	U
18	S	V
19	T	W
20	U	X
21	V	Y
22	W	Z
23	X	A
24	Y	B
25	Z	C

La segunda columna de estas tablas contiene, ordenadas, las 26 letras del alfabeto. La tercera columna, también contiene todo el alfabeto ordenado, pero comenzando desde la letra D y volviendo a comenzar con la A una vez que se termina. Para encriptar una palabra, se reemplaza cada una de sus letras por la ubicada a su lado en la tabla anterior. Por ejemplo, la palabra

ATAQUE

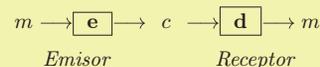
se codifica como

DWDTXH.

Para desencriptar se utiliza la tabla de manera inversa: se lee en la tercera columna y se busca su interpretación en la segunda.

El mecanismo para encriptar resulta ser simplemente reemplazar cada letra por la que está tres lugares más adelante en el alfabeto, leyéndolo en forma circular (o sea, “a b c ... x

El texto plano del mensaje m es encriptado por el emisor usando un método e ; el resultado es el texto cifrado c que se transmite al receptor, quien lo desencripta por medio de d para recuperar el mensaje original m .



y z a b ...”), y para descryptar, reemplazar cada letra por la que está tres lugares antes.

Podemos interpretar esto en términos matemáticos como sigue: representamos cada letra por un elemento $x \in \mathbb{Z}_{26}$ (el número ubicado en la primera columna de las tablas) y para encriptarla calculamos:

$$e(x) = x + 3 \quad \text{en } \mathbb{Z}_{26}$$

y escribimos la letra representada por el elemento obtenido. Por ejemplo:

- la letra Q corresponde al elemento $16 \in \mathbb{Z}_{26}$; para encriptar, calculamos $16 + 3 = 19$ en \mathbb{Z}_{26} y buscamos a qué letra corresponde: la T;
- la letra Y corresponde a $24 \in \mathbb{Z}_{26}$; para encriptar, calculamos $24 + 3 = 1$ en \mathbb{Z}_{26} y buscamos a qué letra corresponde el resultado: la B.

Para descryptar, reemplazamos cada letra por el elemento correspondiente $y \in \mathbb{Z}_{26}$ y calculamos:

$$d(y) = y - 3 \quad \text{en } \mathbb{Z}_{26}$$

Por ejemplo, para descryptar la letra C, que corresponde al elemento $2 \in \mathbb{Z}_{26}$, calculamos $2 - 3 = 25$ en \mathbb{Z}_{26} y buscamos a qué letra corresponde: la Z.

Es fácil generar nuevos métodos de encriptación que funcionen de esta manera, observando que e y d no son otra cosa que una función biyectiva $e : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$ y su inversa $d = e^{-1}$. Por ejemplo, podríamos tomar $e(x) = 3 \cdot x + 4$ y $d(y) = 9 \cdot y + 16$.

El inconveniente de los métodos de encriptación como éste, en los que cada letra se reemplaza siempre por el mismo símbolo, es que son fácilmente vulnerables. Dado un texto encriptado de esta manera, si se analiza la frecuencia con que aparecen los distintos caracteres es posible descubrir qué letras representan (por ejemplo, las vocales A y E aparecen con mucha frecuencia en un texto; lo mismo ocurre con consonantes como la S o la T).

Por este motivo, para aplicaciones en las que la seguridad es muy importante, se utilizan otros métodos más sofisticados. En lo que sigue, introduciremos el *algoritmo RSA*, ideado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Este procedimiento hace uso de dos claves: una *clave pública*, que puede ser conocida por todos y se utiliza para encriptar, y una *clave privada*, que sólo debe conocer quien recibirá el mensaje, y que se usa para descryptar. Al igual que el ejemplo básico que vimos antes, el algoritmo RSA se basa en cálculos de aritmética modular, en este caso, potenciación en lugar de suma.

Supongamos que Andrea le va a enviar un mensaje a Belén. Para armar las claves, Belén procede como sigue:

- genera dos primos grandes al azar $p \neq q$, aproximadamente del mismo tamaño;
- calcula $n = p \cdot q$ y $\varphi(n) = (p - 1) \cdot (q - 1)$;
- elige un entero e tal que:

$$1 < e < \varphi(n) \quad \text{y} \quad \text{mcd}(e, \varphi(n)) = 1$$

El par (e, n) es la clave pública que Belén da a conocer.

- calcula el inverso de e en $\mathbb{Z}_{\varphi(n)}$, es decir, obtiene el único d con:

$$1 < d < \varphi(n) \quad \text{y} \quad e \cdot d \equiv 1 \pmod{\varphi(n)}$$

El par (d, n) es la clave privada que Belén guarda en secreto.

Ahora, para mandar el mensaje, Andrea lo representa por un número m con $1 \leq m \leq n - 1$ y coprimo con n (si el mensaje es largo, lo separa en partes y lo representa por varios números), y luego lo encripta usando la clave pública de Belén:

$$\mathbf{e}(m) = m^e \quad \text{en } \mathbb{Z}_n$$

Finalmente, envía el resultado $c = \mathbf{e}(m)$ a Belén.

Belén recibe c y lo desencripta usando la clave privada que sólo ella conoce:

$$\mathbf{d}(c) = c^d \quad \text{en } \mathbb{Z}_n$$

EJEMPLO. Supongamos que Andrea quiere mandarle el mensaje $m = 87$ a Belén. En primer lugar, Belén genera las claves:

- elige $p = 11$, $q = 17$;
- calcula $n = 11 \cdot 17 = 187$ y $\varphi(n) = 10 \cdot 16 = 160$;
- elige un entero e tal que $1 < e < 160$ y $\text{mcd}(e, 160) = 1$, por ejemplo $e = 7$. Hace pública la clave $(7, 187)$;
- busca el inverso de $e = 7$ en \mathbb{Z}_{160} , es decir, resuelve:

$$7 \cdot d \equiv 1 \pmod{160}$$

obteniendo $d = 23$ (ya que $7 \cdot 23 = 161 \equiv 1 \pmod{160}$). Entonces $(23, 187)$ es la clave que Belén se guarda para desencriptar el mensaje de Andrea.

Una vez que tiene la clave $(e, n) = (7, 187)$, Andrea encripta su mensaje $m = 87$ calculando:

$$m^e = 87^7 \quad \text{en } \mathbb{Z}_{187}$$

Para esto, haciendo las cuentas en \mathbb{Z}_{187} , calcula:

$$87^2 = 7.569 = 89$$

$$87^4 = (87^2)^2 = 89^2 = 7.921 = 67$$

$$87^7 = 87^{1+2+4} = 87^1 \cdot 87^2 \cdot 87^4 = 87 \cdot 89 \cdot 67 = 43$$

Envía entonces $\mathbf{e}(87) = 43$.

Finalmente, Belén descripta la información recibida usando su clave privada $(d, n) = (23, 187)$, nuevamente calculando en \mathbb{Z}_{187} :

$$\begin{aligned} 43^2 &= 1.849 = 166 \\ 43^4 &= (43^2)^2 = 166^2 = 27.556 = 67 \\ 43^8 &= (43^4)^2 = 67^2 = 4.489 = 1 \\ 43^{16} &= (43^8)^2 = 1^2 = 1 \\ 43^{23} &= 11^{16+4+2+1} = 11^{16} \cdot 11^4 \cdot 11^2 \cdot 11 = 1 \cdot 67 \cdot 166 \cdot 43 = 87 \end{aligned}$$

Obtiene de esta manera, $\mathbf{d}(43) = 87$, que es el mensaje original que Andrea quería enviarle.

Veamos que en cualquier caso, si Belén recibe c , entonces $\mathbf{d}(c) = m$, el mensaje original. Es decir, Belén siempre descifra correctamente el mensaje. Recordando que $c = \mathbf{e}(m)$, esto es equivalente a verificar que:

$$\mathbf{d}(\mathbf{e}(m)) = m$$

Ahora bien, $\mathbf{d}(\mathbf{e}(m)) = (\mathbf{e}(m))^d = (m^e)^d = m^{e \cdot d}$ en \mathbb{Z}_n ; con lo cual, debemos ver que:

$$m^{e \cdot d} = m \text{ en } \mathbb{Z}_n$$

o equivalentemente, que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

Para esto utilizaremos el pequeño teorema de Fermat. En primer lugar, recordemos que como $n = p \cdot q$ con p y q primos distintos (y por lo tanto, enteros coprimos), vale que:

$$m^{e \cdot d} \equiv m \pmod{n} \iff \begin{cases} m^{e \cdot d} \equiv m \pmod{p} \\ m^{e \cdot d} \equiv m \pmod{q} \end{cases}$$

La elección de las claves d y e se hizo de manera que $e \cdot d \equiv 1 \pmod{\varphi(n)}$, donde $\varphi(n) = (p-1) \cdot (q-1)$. Entonces, existe $k \in \mathbb{Z}$ tal que $e \cdot d = 1 + (p-1) \cdot (q-1) \cdot k$, y, por lo tanto:

$$m^{e \cdot d} = m^{1+(p-1) \cdot (q-1) \cdot k} = m \cdot (m^{p-1})^{(q-1) \cdot k}$$

Mirando ahora módulo p y teniendo en cuenta que, por el pequeño teorema de Fermat, vale $m^{p-1} \equiv 1 \pmod{p}$ (observar que p no divide a m , ya que $(m : n) = 1$), resulta que $m^{e \cdot d} \equiv m \pmod{p}$. De la misma manera, $m^{e \cdot d} \equiv m \pmod{q}$. En consecuencia, tenemos que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

¿Por qué es difícil descifrar el mensaje para alguien que intercepta el envío de Andrea? Observemos que para hallar m a partir de $c = m^e$ es suficiente conocer d (así es como Belén descifrará el mensaje). Pero para calcular d , lo que se hizo fue buscar el inverso de e módulo $\varphi(n)$. Esto es fácil de hacer conociendo $\varphi(n)$, pero quien intercepte el mensaje, lo que conoce es la clave pública (e, n) , es decir, conoce n , pero no $\varphi(n)$. Nuevamente, $\varphi(n) = (p-1) \cdot (q-1)$ es fácil de calcular una vez que conocemos p y q , es decir, una vez que factorizamos n . Y aquí está el problema: *factorizar números naturales grandes es difícil*. Por difícil entendemos que requiere de *mucho* tiempo: se cree que la cantidad de tiempo necesaria para factorizar un número natural crece casi exponencialmente a medida que

aumenta el tamaño de n . Por este motivo, en la actualidad se utilizan números de más de 300 dígitos en el algoritmo RSA.

No está probado que para ser capaz de descifrar mensajes (es decir, recuperar m conociendo $c = m^e$ en \mathbb{Z}_n y la clave pública (e, n)) sea necesario conocer la factorización de $n = p \cdot q$. Sin embargo, hasta el momento, no han surgido alternativas más eficientes y, más aún, existe un método probabilístico para factorizar $n = p \cdot q$ basado en poder descifrar mensajes de RSA. Por todo esto, el algoritmo RSA es uno de los métodos más utilizados en la actualidad en las aplicaciones donde realmente es necesario transmitir información de manera segura; de hecho, se usa a diario en Internet cuando se visita una página segura que requiere una clave para ingresar (como la de un banco).