**Forum Docentis - Sección AP, Vol. 2023, Núm. 1 (2023)**
**ISSN: 2952-3052**
**doi: https://doi.org/10.33732/FD.v2023.n1.16**
Recepción: 23/09/2023, Aceptación: 26/10/2023

# Aritmética Modular y Aplicaciones

Elena Castilla[1], Pedro J. Chocano[1]*

[1]*Departamento de Matemática Aplicada, CC. e Ingeniería de los Materiales y Tec. Electrónica, URJC, España*
***Autor de correspondencia**: pedro.chocano@urjc.es

**Resumen**
En este artículo hacemos una introducción a la aritmética modular. Para ello empezamos repasando cuestiones básicas como la divisibilidad y el máximo común divisor, así como la identidad de Bézout. Explicamos los conceptos más importantes de aritmética modular y de aritmética en $\mathbb{Z}_m$. Finalmente, damos algunos sencillos ejemplos de aplicaciones de la aritmética modular en diferentes campos, como el álgebra, la criptografía o la simulacíon estadística.

**Palabras clave**
Aritmética Modular — Divisibilidad — Generación de números aleatorios


*Cómo citar este artículo: Elena Castilla, Pedro J. Chocano; Aritmética Modular y Aplicaciones; Forum Docentis - AP vol. 2023, (1), e16, 2023*

## Índice

## Introducción

En estas breves notas, pensadas para un curso de unas 5 horas en grados de ingeniería o informática, se pretende dar una introducción rápida a algunas cuestiones de aritmética modular haciendo, al final de las mismas, especial énfasis en aplicaciones sencillas que sirvan de motivación al lector para que profundice más a fondo en algunos detalles y contenidos que se escapan por cuestiones de tiempo.

No se asumen conocimientos previos por parte del lector. Empezaremos recordando cuestiones básicas como la divisibilidad y el concepto de máximo común divisor para a continuación introducir la identidad de Bézout, resultado fundamental para abordar el estudio de ecuaciones diofánticas y congruencias lineales. Finalmente se introducen algunas aplicaciones a criptografía o métodos de simulación, entre otros.

## 1. Divisibilidad y Máximo Común Divisor

### 1.1 Divisibilidad

**Definición 1.1** (Divisibilidad)**.** Dados dos números enteros $a$ y $b$ (con $a$ distinto de 0), se dice que $a$ divide a $b$, y lo escribimos como $a|b$, si existe un $c \in \mathbb{Z}$ tal que $b = ac$. También se dice que $a$ es un factor o divisor de $b$, y que $b$ es un múltiplo de $a$.

Veamos en la siguiente proposición algunas propiedades sencillas.

**Proposición 1.1.** *Sean $a, b, c \in \mathbb{Z}$, tenemos:*

- $1|a$.
- $a|0$.
- *Si $a|b$ y $a|c$, entonces $a|(b + c)$.*
- *Si $a|b$ y $b|a$, entonces $a = b$ o bien $a = -b$.*

**Definición 1.2** (Número primo)**.** Diremos que un número $p \in \mathbb{N}$ es primo si el único divisor de $p$ es 1.

Los números primos tienen gran importancia en áreas como la criptografía. Sin embargo, encontrar números primos no es, en general, un problema sencillo. Como curiosidad, a septiembre de 2023, el número primo más grande encontrado (en diciembre de 2018 [1]) es $2^{82,589,933} - 1$. Un método clásico para encontrar todos los números primos más pequeños que un número $n$ fijado, con el que posiblemente el lector ya esté familiarizado, es la **criba de Eratóstenes**:

Paso 1 Escribimos en orden todos los números comprendidos entre 2 y $n$.

Paso 2 Tomamos el primer número que no se encuentre tachado como número primo.

Paso 3 Tachamos todos los números que sean múltiplos del número que hemos marcado como primo.

Paso 4 Si el cuadrado del primer número que no ha sido tachado es inferior a $n$, entonces se repite el segundo paso. Si no, el algoritmo termina, y todos los enteros no tachados son declarados primos.

A continuación mostramos un listado de los números primos que hay entre 1 y 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

### 1.2 Máximo Común Divisor

**Definición 1.3.** Dados dos enteros $a$ y $b$ distintos de 0, decimos que el entero $d > 1$ es un máximo común divisor de $a$ y $b$, ó $mcd(a, b)$, de $a$ y $b$ si $d|a$, $d|b$ y para cualquier otro $c \in \mathbb{Z}$ tal que $c|a$ y $c|b$ se tiene que $c|d$.

[1] "GIMPS Project Discovers Largest Known Prime Number: 282,589,933-1". Mersenne Research, Inc. 21 December 2018. Retrieved 21 December 2018. https://www.mersenne.org

Es común asumir que dados dos enteros distintos de cero siempre existe el máximo común divisor. Sin embargo, demostrarlo no es trivial, pues involucra el *principio de buena ordenación*. En estas breves notas no lo probaremos pero animamos al lector interesado que consulte [1] para ver una demostración completa. Recogemos en la siguiente proposición algunas propiedades básicas del máximo común divisor.

**Proposición 1.2.** *Sean $a$, $b$, $c$, $k$ enteros.*

1. $\mathrm{mcd}(ka, kb) = |k|\mathrm{mcd}(a, b)$.
2. *Si* $a|bc$ *y* $\mathrm{mcd}(a, b) = 1$, *entonces* $a|c$.
3. $\mathrm{mcd}(a, b) = d$ *sí y sólo sí* $d|a$, $d|b$ *y* $\mathrm{mcd}(a/d, b/d) = 1$.

*Demostración.*

1. Supongamos que $c = \mathrm{mcd}(a, b)$ y $d = \mathrm{mcd}(ka, kb)$, luego $c|a$ y $c|b$, y por tanto, $kc|ka$ y $kc|kb$. Por definición de máximo común divisor tenemos que $kc|d$. Esto nos dice que $d = kce$ para cierto entero $e$. Por otro lado, $kce|ka$ y $kce|kb$, lo que implica que $ce|a$ y $ce|b$. De nuevo usando la definición de máximo común divisor, tenemos que $c|ce$ lo que significa que $e = 1$ y que $\mathrm{mcd}(ka, kb) = |k|\mathrm{mcd}(a, b)$.
2. Trivial.
3. Basta con aplicar la primera propiedad. Tenemos que $d \cdot \mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \mathrm{mcd}\left(d\frac{a}{d}, d\frac{b}{d}\right) = \mathrm{mcd}(a,b)$. Esto nos dice que $\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \mathrm{mcd}(a,b)/d$. Por tanto, $1 = \mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right)$ si y solo si $\mathrm{mcd}(a, b) = d$.

□

Por ahora, solamente hemos enunciado propiedades, pero dados dos enteros no sabemos calcular el máximo común divisor. La próxima proposición será fundamental para el desarrollo de un algoritmo que nos permita tal fin.

**Proposición 1.3.** *Sean $a$, $b$ enteros positivos no nulos. Entonces* $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$ *donde $r$ es el único* $0 < r < b$ *tal que existe un entero $q$ con $a = bq + r$ (esto significa que $r$ es el resto de la división de $a$ por $b$).*

*Demostración.* Supongamos que $d|a$, $b$, luego $a = da'$ y $b = db'$ para ciertos enteros positivos $a'$ y $b'$. Por otro lado, como $a = bq + r$ tenemos que $r = a - bq = d(a' - b' q)$. Por tanto, $d|b$, $r$. En concreto, como $\mathrm{mcd}(a, b)|a$, $b$, acabamos de probar que $\mathrm{mcd}(a, b)|\mathrm{mcd}(b, r)$. Supongamos ahora que $d|b$, $r$, así que también tenemos que $d|bq$. Usando las propiedades de divisibilidad tenemos que $d|(bq + r)$, pero $a = bq + r$, luego $d|a$. En concreto, tenemos que $\mathrm{mcd}(b, r)|a$, $b$ y esto implica que $\mathrm{mcd}(b, r)|\mathrm{mcd}(a, b)$. □

Esta proposición nos indica que es igual de válido calcular el $\mathrm{mcd}(a, b)$ que el $\mathrm{mcd}(b, r)$, con la ventaja de que $r$ es un entero de menor tamaño que el original $a$. El algoritmo de Euclides utilizará esta propiedad para el cálculo recursivo del máximo común divisor de dos números enteros.

**Algoritmo de Euclides:** Dados dos enteros $a$ y $b$, el algoritmo de Euclides para encontrar $\mathrm{mcd}(a, b)$ es como sigue:

Paso 1 Si $a = 0$ entonces $\mathrm{mcd}(a, b) = b$, ya que el $\mathrm{mcd}(0, b) = b$, y podemos detenernos.

Paso 2 Si $b = 0$ entonces $\mathrm{mcd}(a, b) = a$, ya que el $\mathrm{mcd}(a, 0) = a$, y podemos detenernos.

Paso 3 Escribe $a$ como cociente por $b$: $a = bq + r$.

Paso 4 Encuentra $\mathrm{mcd}(b, r)$. Para ello repite los anteriores pasos cambiando $a$ por $b$ y $b$ por $r$.

**Ejemplo 1.4.** *Calculemos* $\mathrm{mcd}(42, 24)$. *Dado que ninguno de los términos es cero, aplicamos el Paso 3 del algoritmo:*

$$42 = 24 \times 1 + 18.$$

*Si usamos la Proposición 1.3, es decir, el Paso 3, tenemos que* $\mathrm{mcd}(42, 24) = \mathrm{mcd}(24, 18)$. *De nuevo como* 24 *y* 18 *son distintos de cero volvemos al Paso 3:*

$$24 = 18 \times 1 + 6.$$

*Por el Paso 4 tenemos* mcd(24, 18) = mcd(18, 6). *Volvemos de nuevo al Paso 3:*

$$18 = 6 \times 3 + 0.$$

*Aplicando el Paso 4,* mcd(18, 6) = mcd(6, 0). *Por el Paso 2 podemos detener el algoritmo y hemos llegado a que* mcd(42, 24) = 6.

### 1.3 Identidad de Bézout

En esta sección vamos a enunciar un resultado fundamental que necesitaremos más adelante. La demostración del resultado no es complicada e instamos al lector interesado que la vea con detalles por ejemplo en [2].

**Teorema 1.5** (Identidad de Bézout)**.** *Sean $a$ y $b$ números enteros con $d$ =* mcd($a$, $b$). *Entonces existen enteros $x$ e $y$ tales que $d = ax + by$.*

Veamos cómo obtener los enteros $x$ e $y$ de la identidad de Bézout. Para ello, solamente tenemos que aplicar el algoritmo de Euclides para calcular el máximo común divisor y deshacer las operaciones. Veamos un sencillo ejemplo a modo de ilustración.

**Ejemplo 1.6.** *Vamos a encontrar una identidad de Bézout para* 42 *y* 24. *Previamente, habíamos obtenido que* mcd(42, 24) = 6. *Así pues, el objetivo es encontrar enteros $x$ e $y$ tales que* $6 = 42x + 24y$. *Escribimos las distintas iteraciones del Paso 3 de algoritmo de Euclides.*

$$42 = 24 \times 1 + 18 \tag{1}$$
$$24 = 18 \times 1 + 6 \tag{2}$$
$$18 = 6 \times 3 + 0 \tag{3}$$

*Si en la ecuación (2) despejamos el* 6 *tenemos:*

$$6 = 24 - 18 \times 1.$$

*Ahora vamos a despejar* 18 *de la ecuación (1)*

$$18 = 42 - 24 \times 1$$

*y vamos sustituir el* 18 *que acabamos de obtener en la forma que teníamos de expresar* 6*:*

$$6 = 24 - (42 - 24) = 2 \times 24 - 42.$$

*De esta manera acabamos de obtener que $x = 2$ e $y = -1$.*

De manera general tenemos que dados dos números enteros $a$ y $b$ tales que ni $a$ divide a $b$, ni $b$ divide a $a$, si aplicamos el algoritmo de Euclides obtenemos denotando por $r_0 = a$ y $r_1 = b$ la siguiente secuencia de restos:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
r_1 &= r_2 q_2 + r_3 \\
r_2 &= r_3 q_3 + r_4 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k \\
r_{k-1} &= r_k q_k
\end{aligned}$$

Tenemos que $r_k$ = mcd($a$, $b$). Despejando $r_k$ en la penúltima ecuación, a continuación sustituyendo $r_{k-1}$ por el resultado de despejarlo en la antepenúltima igualdad, y recorriendo todo el camino otra vez desde abajo hasta arriba obtenemos una identidad de Bézout.

## 2. Aritmética Modular

**Definición 2.1.** Sean $a$ y $b$ enteros y $m$ un entero positivo. Se dice que $a$ es congruente a $b$ módulo $m$, y se expresa

$$a \equiv b \pmod{m},$$

si $(a - b)$ es múltiplo de $m$. Es decir, da resto $b$ si dividimos $a$ entre $m$.

**Ejemplo 2.1.** *Veamos algunos sencillos ejemplos de congruencias:*

$5 \equiv 1 \pmod 2$ $\quad$ $5 \equiv -1 \pmod 3$ $\quad$ $100 \equiv 24 \pmod{76}$

$5 \equiv 2 \pmod 3$ $\quad$ $23 \equiv 1 \pmod{11}$ $\quad$ $6 \equiv 0 \pmod 2$

**Propiedades:** Sean $a, b, c \in \mathbb{Z}$ y $m$ un entero positivo, entonces se cumple

- **Reflexividad**: $a \equiv a \pmod m$.
- **Simetría**: Si $a \equiv b \pmod m$, entonces $b \equiv a \pmod m$.
- **Transitividad**: Si $a \equiv b \pmod m$ y $b \equiv c \pmod m$, entonces $a \equiv c \pmod m$.

Queda como un sencillo ejercicio para el lector probar las anteriores propiedades.

La relación de congruencia se trata por tanto de una relación de equivalencia en $\mathbb{Z}$, que descompone este conjunto en $m$ **clases de equivalencia**:

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

donde $[i] = \{k \in \mathbb{Z} \mid k \equiv i \pmod m\}$ para $i = 0, \ldots, m - 1$. Por tanto, la clase $[i]$ está representando el conjunto de números que tienen por resto $i$ al dividir por $m$. Cuando tenemos una relación de equivalencia y consideramos sus clases, estamos de alguna manera clasificando a los elementos del conjunto original siguiendo alguna propiedad concreta que viene determinada por la relación. A pesar de que $[i]$ es un conjunto con infinitos elementos vamos a tratarlo como si se tratara de un único elemento y cuando no haya dudas en la notación simplemente denotaremos a los elementos de $\mathbb{Z}_m$ como $\{0, 1, \ldots, m - 1\}$.

**Ejemplo 2.2.** *Supongamos que tomamos la relación de congruencia con $m = 2$. En ese caso, estamos distinguiendo si los números son pares e impares, $\mathbb{Z}_2 = \{0, 1\}$. La clase $0$ representa a los números pares y la clase $1$ representa los números impares.*

**Notación:** Como norma general, se tiende a expresar las congruencias con un elemento $0 \leq b \leq m$. Así, por ejemplo, aunque las identidades

$$5 \equiv 2 \pmod 3 \quad \text{y} \quad 5 \equiv -1 \pmod 3$$

son ambas ciertas, se prefiere la primera expresión. Podemos decir que, en $\mathbb{Z}_3$: $-1 = 2$ ó $3 = 0$.

A continuación enunciamos sin demostración algunas propiedades sencillas de demostrar que quedan como ejercicio propuesto.

**Proposición 2.3.** *Sean $a, b, c, d, \lambda \in \mathbb{Z}$ y $m, k \in \mathbb{N}$ tal que $a \equiv b \pmod m$ y $c \equiv d \pmod m$, entonces:*

- $\lambda a \equiv \lambda b \pmod m$.
- $a + c \equiv b + d \pmod m$.
- $ac \equiv bd \pmod m$.
- $a^k \equiv b^k \pmod m$.

**Proposición 2.4.** *Sean $a, b, c \in \mathbb{Z}$ y $m \in \mathbb{N}$ . Si $ac \equiv bc \pmod m$ y $\mathrm{mcd}(c, m) = 1$, entonces:*

$$a \equiv b \pmod m.$$

Hay distintas demostraciones del siguiente resultado, el lector interesado puede encontrar alguna de ellas en [1].

**Teorema 2.5** (Pequeño teorema de Fermat)**.** *Si $p$ es primo y $a$ no es múltiplo de $p$, entonces:*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4}$$

**Observación 2.6.** *La ecuación (4) se cumple si $p$ es primo, pero también puede darse en caso de no serlo. Por ejemplo:*

$$2^{340} \equiv 1 \pmod{341}, \quad \textit{pero 341 no es primo:}\ 341 = 31 \times 11.$$

Veamos cómo podemos utilizar los resultados previos en un problema de obtener restos.

**Ejemplo 2.7.** *Supongamos que queremos calcular el resto de dividir $2^{39}3^{38}$ entre 37, evidentemente sin usar calculadora. Este problema es equivalente a obtener $x$ donde*

$$2^{39}3^{38} \equiv x \pmod{37}.$$

*Tenemos que 37 es primo (ya lo vimos en la criba de Eratóstenes). Vamos a aplicar el pequeño teorema de Fermat dos veces. Sabemos que*

$$2^{36} \equiv 1 \pmod{37},$$

$$3^{36} \equiv 1 \pmod{37}.$$

*Aplicamos la primera propiedad de la Proposición 2.3 a la primera ecuación multiplicando por $2^3$ y lo mismo a la segunda ecuación multiplicando por $3^2$:*

$$2^{39} \equiv 2^3 \pmod{37},$$

$$3^{38} \equiv 3^2 \pmod{37}.$$

*Utilizando la propiedad 3 de la Proposición 2.3 a las dos anteriores congruencias tenemos:*

$$2^{39}3^{38} \equiv 3^2 2^3 \pmod{37}.$$

*Así pues, nuestro problema original se ha traducido en el problema de obtener el resto de dividir $3^2 2^3$ entre 37 que claramente es 35.*

*Otra manera sencilla de resolver el problema también puede ser considerando $2^{39}3^{38} = 2^3 3^2 (2^{36}3^{26}) = 2^3 3^2 6^{36}$. De nuevo podemos aplicar el pequeño teorema de Fermat:*

$$6^{36} \equiv 1 \pmod{37}.$$

*Y de nuevo, aplicando la primera propiedad de la proposición 2.3 tenemos:*

$$2^{39}3^{38} \equiv 2^3 3^2 6^{36} \equiv 3^2 2^3 \pmod{37}.$$

## 3. Aritmética en $\mathbb{Z}_m$

Hemos visto que $\mathbb{Z}_m$ era el resultado de clasificar o agrupar los números de $\mathbb{Z}$ en función del resto obtenido al dividir por $m$. Pero $\mathbb{Z}$ es un anillo conmutativo si consideramos la suma y producto usuales. Estas operaciones se trasladan de manera natural a $\mathbb{Z}_m$, es algo que ya vimos en la sección previa con la Proposición 2.3.

**Ejemplo 3.1.** *Tenemos que en $\mathbb{Z}_2$ la suma y producto nos queda como sigue:*

| + | 1 | 0 |
|---|---|---|
| 1 | 0 | 1 |
| 0 | 1 | 0 |

| × | 1 | 0 |
|---|---|---|
| 1 | 1 | 0 |
| 0 | 0 | 0 |

*Por tanto, si trabajásemos en* $\mathbb{Z}_2$*, sí que se cumple uno de los errores más comunes entre los estudiantes de escribir* $(a+b)^2 = a^2 + b^2$*. Ya que en* $\mathbb{Z}_2$ *el término* $2ab$ *es congruente con* $0$ *módulo* $2$*.*

**Ejemplo 3.2.** *Otro sencillo ejemplo con aritmética modular lo encontramos en el día a día con las horas. Si tenemos un reloj digital, cuando vemos que la hora marca las* 15*, no decimos las* 15 *sino las* 3*. Esto se debe a que de manera inconsciente estamos trabajando en* $\mathbb{Z}_{12}$ *y lo que acabamos de hacer es obtener el resto de dividir* 15 *entre* 12*.*

En $\mathbb{Z}_m$, tenemos algunas peculiaridades que no ocurren en $\mathbb{Z}$. Por ejemplo, en $\mathbb{Z}$, $a \times b = 0$ si y solo si alguno de los dos términos es cero. Sin embargo, en $\mathbb{Z}_{12}$, tenemos que $3 \times 4 = 0$, pero ninguno de los dos términos es cero. Además, mientras que en $\mathbb{Z}$ no tenemos inversos para el producto (nos tendríamos que ir a el conjunto de los racionales $\mathbb{Q}$), si consideramos $\mathbb{Z}_3$ tenemos que $2 \times 2 = 1$. Estas cuestiones motivan las dos siguientes definiciones:

**Definición 3.1.** Diremos *que* $a \in \mathbb{Z}_m$ es un divisor de cero si ex*iste* $x \in \mathbb{Z}_m$ distinto de 0 tal que $a \times x = 0$.

Por ejemplo, en $\mathbb{Z}_{12}$ tenemos que 3 es un divisor de cero. Veamos una caracterización muy útil que emplea herramientas previas:

**Teorema 3.3.** *Supongamos que* $a \in \mathbb{Z}_m$*. Tenemos que* $a$ *es divisor de cero si y solo si* $\mathrm{mcd}(a, m) \neq 1$.

**Definición 3.2.** Diremos que $a \in \mathbb{Z}_m$ es un elemento invertible de $\mathbb{Z}_m$ si existe $b \in \mathbb{Z}_m$ tal que $ab = 1$.

Por ejemplo, en $\mathbb{Z}_7$ tenemos que 2 es un elemento invertible porque $2 \times 4 = 1$. De nuevo, enunciamos una importante caracterización:

**Teorema 3.4.** *Supongamos que* $a \in \mathbb{Z}_m$*. Tenemos que* $a$ *es invertible si y solo si* $\mathrm{mcd}(a, m) = 1$.

Cuando trabajamos con los números reales el tipo de ecuaciones más sencillas a resolver son las de la forma $ax + b = 0$. Veamos su equivalente en $\mathbb{Z}_m$.

**Definición 3.3.** Llamaremos congruencia lineal a una ecuación de la forma

$$ax \equiv b \pmod{m},$$

donde $a,\ b \in \mathbb{Z}$, $a \neq 0$ y $m \in \mathbb{N}$.

Una observación interesante es que si $\alpha$ es solución a una congruencia lineal y $\beta \equiv \alpha \pmod{m}$, entonces $\beta$ también es solución.

**Ejemplo 3.5.** $2x \equiv 1 \pmod 6$ *no tiene solución en* $\mathbb{Z}_6$*. Mientras que* $2x \equiv 2 \pmod 8$ *tiene dos soluciones en* $\mathbb{Z}_8$ *(*$x = 1$ *y* $x = 5$*).*

Con el siguiente resultado vamos a caracterizar cuándo una congruencia lineal tiene solución. Además, en la propia demostración vamos a ver los pasos a seguir para poder hallarla.

**Teorema 3.6.** *La congruencia lineal* $ax \equiv b \pmod m$ *tiene solución si y solo si* $\mathrm{mcd}(a, m) | b$.

*Demostración.* Supongamos primero que la congruencia tiene solución y la denotaremos por $\alpha$, esto significa que $m | a\alpha - b$ y a su vez que existe $k$ tal que $km = a\alpha - b$. Despejando $b$, tenemos $b = a\alpha - km$ como $\mathrm{mcd}(a, m) | a\alpha$ y $\mathrm{mcd}(a, m) | km$, entonces $\mathrm{mcd}(a, m) | b$. Supongamos ahora que $\mathrm{mcd}(a, m) | b$ y veamos que hay solución. Como $d = \mathrm{mcd}(a, m) | b$, tenemos que $b = db'$ para cierto entero $b'$. Usando la identidad de Bézout sabemos que existen enteros $u$ y $v$ tales que $d = au + mv$. Multiplicando esta última igualdad por $b'$ tenemos

$$b = db' = b'au + b'mv.$$

Esto significa que $b \equiv b'ua \pmod m$ y $b'u$ es solución. □

**Ejemplo 3.7.** *En este ejemplo veremos cómo usar la identidad de Bézout para hallar una solución a una congruencia lineal. Considera la congruencia lineal definida por*

$$56x \equiv 42 \pmod{105}.$$

*Aplicamos el algoritmo de Euclides para calcular* mcd(105, 56):

$$105 = 56 \times 1 + 49$$
$$56 = 49 \times 1 + 7$$
$$49 = 7 \times 7 + 0$$

*Tenemos pues que* mcd(105, 56) = 7. *Vamos a hallar una identidad de Bézout. Despejando, tenemos que* $7 = 56 - 49 \times 1$ *y* $49 = 105 - 56 \times 1$. *Finalmente:* $7 = 56 - 105 + 56 = 2 \times 56 + (-1)105$. *Multiplicando dicha identidad por* $42/7 = 6$ *tenemos*

$$42 = 12 \times 56 - 5 \times 105,$$

*lo que me da la solución* $x = 12$.

Observa que si en la congruencia $ax \equiv b \pmod{m}$ tenemos que mcd$(a, m) = 1$, entonces hay solución. Además, como mcd$(a, m) = 1$, significa que $a$ es invertible. Así que el problema de resolver la congruencia se puede convertir en un problema de encontrar el inverso de $a$. También al revés, el problema de encontrar el inverso de un elemento $a$ se puede ver como el de resolver la congruencia lineal $ax \equiv 1 \pmod{m}$.

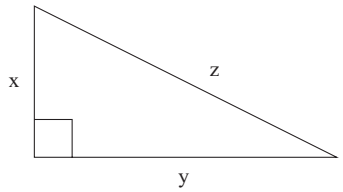
## 4. Aplicaciones

### 4.1 Ecuaciones diofánticas

Las ecuaciones diofánticas son ecuaciones en dos o más variables con coeficientes reales donde se buscan soluciones que sean números enteros de manera que la solución no sea trivial (por ejemplo todo ceros). Posiblemente una de las ecuaciones diofánticas más importantes sea la generalización de la ecuación pitagórica ( $x^2 + y^2 = z^2$) dada por:

$$x^n + y^n = z^n.$$

Nótese que para el caso $n = 2$ tenemos infinitas soluciones si tenemos en cuenta un resultado básico de geometría: Teorema de Pitágoras. Este teorema nos dice que en un triángulo rectángulo, la hipotenusa al cuadrado es igual a la suma de los catetos al cuadrado.




El problema general planteado previamente con $n \geq 3$ es lo que se conoce como *el último teorema de Fermat*. Dicho problema fue planteado en 1637 por el matemático francés Pierre de Fermat y no fue hasta 1994 cuando Andrew Wiles consiguió demostrar que no hay soluciones triviales para $n \geq 3$. Se recomienda al lector interesa- do en dicho problema el libro divulgativo [3] donde se hace un repaso general a la apasionante historia de este problema.

En esta sección abordaremos una familia de ecuaciones diofánticas muy sencillas

$$ax + my = b,$$

donde $a, b, m \in \mathbb{Z}$. Realmente el problema de encontrar $x$ e $y$ se puede abordar como el problema de encontrar soluciones a una congruencia lineal. Veamos cómo ambos problemas son equivalentes:

- Si $ax \equiv b \pmod{m}$ tiene solución, significa que existe $x$ tal que $ax - b = -my$ para cierto $y \in \mathbb{Z}$ pues que haya solución implica que $m$ divide a $ax - b$. En concreto, tenemos $ax + my = b$.
- Por otro lado, supongamos que $ax + my = b$ tiene solución. Esto significa que $ax - b$ es divisible por $m$ y en concreto $ax \equiv b \pmod{m}$.

Por tanto, podemos establecer

**Teorema 4.1.** *La ecuación diofántica* $ax + my = b$ *tiene solución si y solamente si* $\text{mcd}(a, m)|b$.

Además, para encontrar la solución basta con proceder como hicimos previamente para resolver una congruencia lineal, pero teniendo en cuenta los dos términos encontrados en la identidad de Bézout.

**Ejemplo 4.2.** *Considera la ecuación diofántica dada por*

$$42 = 56x + 105y.$$

*Como* $\text{mcd}(56, 105) = 7|42$, *tenemos que dicha ecuación tiene solución. Si repetimos los pasos seguidos en el Ejemplo 3.7 llegamos a que*

$$42 = 12 \times 56 - 5 \times 105$$

*y por tanto una solución es* $x = 12$ *e* $y = -5$.

Una vez se han estudiado las ecuaciones más sencillas el paso natural es estudiar sistemas de congruencias lineales. Para aquellos interesados en profundizar en esta cuestión recomendamos [1].

### 4.2 Reglas de divisibilidad

Vamos a ver algunas reglas de divisibilidad conocidas. Para ello, nos apoyaremos en el siguiente teorema de sencilla demostración:

**Teorema 4.3.** *Si* $p(x)$ *es un polinomio con coeficientes en* $\mathbb{Z}$ *y tenemos dos enteros* $a$ *y* $b$ *tales que* $a \equiv b \pmod m$ *para algún entero positivo* $m$, *entonces* $p(a) \equiv p(b) \pmod m$.

Si $n = a_k a_{k-1} \ldots a_1 a_0$ es la expresión decimal de $n$, entonces $n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$. Esta última expresión la podemos ver como un polinomio evaluado en 10, es decir, $p(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ y $n = p(10)$.

**Criterio de divisibilidad por 9** Como $10 \equiv 1 \pmod 9$, usando el anterior teorema tenemos que

$$n = p(10) \equiv p(1) = a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod 9.$$

Por tanto, $n$ es divisible por 9 si la suma de sus cifras es múltiplo de 9.

**Criterio de divisibilidad por 11** Podemos repetir el mismo esquema usado previamente, tenemos que $10 \equiv -1 \pmod{11}$ y entonces

$$n = p(11) \equiv p(1) = a_k(-1)^k + a_{k-1}(-1)^{k-1} + \ldots - a_1 + a_0 \pmod{11}.$$

Por tanto, $n$ es divisible por 11 si lo es la suma alternada de sus cifras.

Queda como ejercicio para el lector que obtenga otras reglas de divisibilidad que conozca aplicando este esquema.

### 4.3 Letra del DNI

Si el lector alguna vez se ha preguntado de donde se obtiene la letra final de su DNI, esta se obtiene tras un pequeño ejercicio con congruencias. En concreto, ha de dividirse el número completo del DNI entre 23. El resto de la división (que siempre estará comprendido entre 0 y 22) será el que se obtenga para obtener la letra según la siguiente tabla:

| **RESTO** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **LETRA** | T | R | W | A | G | M | Y | F | P | D | X | |
| **RESTO** | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| **LETRA** | B | N | J | Z | S | Q | V | H | L | C | K | E |

### 4.4 Criptografía

En este apartado vamos a ver, a modo de ejemplo, una de las técnicas de cifrado en criptografía más usadas, el cifrado César o *cifrado por desplazamiento*:

**Cifrado César** Consideramos el alfabeto español, con 27 símbolos. Otorgamos a cada una en orden un número: $A = 0$, $B = 1$, $C = 2$,..., $Z = 26$. Codificamos la letra $x$ con un desplazamiento $n$ como sigue

$$E_n(x) = x + n \pmod{27}.$$

La descodificación de una letra será deshacer este proceso, simplemente valdría con

$$D_n(x) = x - n \pmod{27}.$$

Evidentemente, este es un tipo de codificación demasiado simple y muy poco seguro, pero bastante ilustrativo. Veamos un sencillo ejemplo, tomemos un desplazamiento de $n = 4$. De esta manera tenemos que la palabra "HOLA" queda codificada como "LSOE". Como ejercicio descodifica la siguiente palabra donde hemos tomado $n = 2$ "XCKUCUWURGPFGT" (Consejo: hay calculadoras en línea [2] que resuelven el problema conociendo el desplazamiento $n$).

### 4.5 Generación de números aleatorios

El desarrollo de los métodos de simulación así como la aparición de ordenadores de alta velocidad a mitad del siglo XX, promovió el desarrollo de métodos de generación de números pseudoaleatorios. A continuación presentamos el generador congruencial lineal introducido por Lehmer en el 1951 [4].

**Método congruencial para la generación de números aleatorios** Dados $a,\ b,\ m \in \mathbb{N}$:

Paso 1 Elegir un número $x_0$ inicial (semilla).

Paso 2 Para $i \geq 1$ obtener de manera recursiva

$$x_i \equiv ax_{i-1} + b \pmod{m}. \tag{5}$$

Si además queremos que los números se encuentren en el intervalo $[0,\ 1]$ (muy útil en caso de querer simular más adelante otras distribuciones estadísticas), debemos dividir la secuencia de números obtenidos entre $m$,

$$u_i = \frac{x_i}{m}.$$

Si $b = 0$, se dice que es un *generador multiplicativo*, en caso contrario se dice que es un *generador mixto*. Por otra parte, aunque hablemos de generar números "aleatorios", estos quedan completamente determinados por nuestro algoritmo. La pseudoaleatoriedad de los métodos congruenciales se refleja en la siguiente proposición:

**Proposición 4.4.** *Si se aplica un método congruencial como el definido en (5), se verifica*

$$x_i \equiv a^i x_0 + b\frac{a^i - 1}{a - 1} \pmod{m}.$$

Un gran inconveniente de este método es que los valores $u_i$ sólo pueden tomar valores $i/m$, $i = 0, \ldots, m$. Además, es inevitable que se produzcan ciclos, ya que el periodo nunca puede exceder al módulo. Así, se tiene que tomar un valor suficiente grande de $m$ para que el conjunto de posibles valores de la sucesión se asemeje a la de una variable continua uniforme en el intervalo $[0,\ 1]$ y que el ciclo no sea demasiado corto. En concreto, el siguiente teorema nos dice cómo elegir los parámetros para que el ciclo sea completo.

**Teorema 4.5.** *Un generador congruencial tiene periodo completo si y sólo si se cumplen las siguientes condiciones:*

1. *m y b son primos entre sí.*

[2] https://julioc1984.tumblr.com/cifradocesar

*2. Si $q$ es un número primo que divide a $m$, entonces $q$ divide a $(a-1)$.*

*3. Si 4 divide a $m$, entonces 4 divide a $(a-1)$.*

Recomendamos [5] al lector interesado en otros aspectos y cuestiones relacionados con la simulación para que pueda comprobar el impacto que tiene la generación de números aleatorios en las matemáticas actuales.

## 5. Ejercicios

1. Escribe un programa para cada una de las siguientes tareas:

   *a*) Calcular el máximo común divisor entre dos números enteros.

   *b*) Dados dos números enteros, calcular una identidad de Bézout.

   *c*) Dada una congruencia lineal, determinar si existe solución y en caso de que existe hallar una posible solución.

   *d*) Dada una ecuación diofántica, hallar una solución en caso de que exista.

2. Mediante el algoritmo de Euclides, calcular el máximo común divisor de los siguientes pares de números

   *a*) $m$mcd$(721,\ 448)$.

   *b*) mcd$(25134,\ 19185)$.

3. Demostrar que sean $a,\ b,\ c,\ d,\ \lambda \in \mathbb{Z}$ y $m \in \mathbb{N}$ tal que $a \equiv b \pmod m$ y $c \equiv d \pmod m$, entonces:

   *a*) $\lambda a \equiv \lambda b \pmod m$.

   *b*) $a + c \equiv b + d \pmod m$.

   *c*) $ac \equiv bd \pmod m$.

4. Calcular el resto de la división $2^{98}$ por 101.

5. Demostrar que los posibles restos de la división por 7 de un cubo perfecto son 0, 1 ó 6.

6. Si $p$ es primo demuestra que $(x + y)^p = x^p + y^p$ en $\mathbb{Z}_p$.

7. Si $x \in \mathbb{Z}$, entonces $4x^2 + x + 3$ no es divisible por 5.

8. Resuelve la congruencia $6x + 1 \equiv 2(x + 2) \pmod 7$.

9. ¿Qué elementos tienen inverso en $\mathbb{Z}_{12}$?

10. Encuentra, si es posible, el inverso de 47 en $\mathbb{Z}_{61}$.

## Referencias

[1]D. M. Burton, *Elementary Number Theory*, 7.ª ed. (McGraw Hill, 2010).

[2]T. M. Apostol, *Introduction to Analytic Number Theory* (Springer, 1976).

[3]S. Singh, *Fermat's Last Theorem* (Harper Collins, 1997).

[4]D. H. Lehmer, "Mathematical models in large-scale computing units", Ann. Comput. Lab.(Harvard University) **26**, 141-146 (1951).

[5]E. Castilla y P. J. Chocano, "Introducción al Método de Montecarlo", Gaceta de la Real Sociedad Matemática Española **26**, 87-109 (2023).