# La aritmética modular (parte 1)
# Disquisición informal: "la aritmética del reloj"

27 de noviembre de 2018

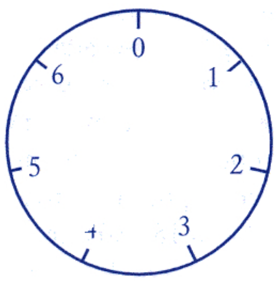
## Índice



## 1. "Empaquetando" enteros no negativos

Consideremos un conjunto finito de números del tipo $\{0, 1, 2, 3, \ldots, n-1\}$ dispuestos en círculo, de manera bastante similar a las horas de un reloj. Por ejemplo, la siguiente figura muestra un reloj que sólo tiene los 7 números del 0 al 6 (un reloj "módulo 7"). Veremos a continuación una manera, distinta de la usual, de "sumar" elementos del conjunto $\{0, 1, 2, 3, 4, 5, 6\}$.

Para calcular 2 + 3, avanzamos primero 2 lugares (en sentido horario y empezando en "0") y luego avanzamos 3 lugares, hasta llegar a 5. Es la misma respuesta que en aritmética "normal".




Sin embargo para calcular 2 + 6, avanzamos primero 2 lugares y luego 6, acabando esta vez en el 1, que no es el resultado que obtendríamos en aritmética "normal". Para representar este tipo de operación suele emplearse la siguiente notación:

- $2+3 \equiv 5 \ (mod\ 7)$, y se lee "2+3 es congruente con 5 módulo 7"

- $2+6 \equiv 1 \ (mod\ 7)$, y se lee "2+6 es congruente con 1 módulo 7"

Dos números enteros (no negativos, por ahora) se dirá que *son congruentes módulo 7* si, al avanzar en un reloj "módulo 7" tantas posiciones (empezando por la posición "0" y en sentido horario) como indican los números, en ambos casos terminamos en la misma posición. Así pues, por ejemplo, $8 \equiv 1 \ (mod\ 7)$, $8 \equiv 15 \ (mod\ 7)$, $9 \equiv 2 \ (mod\ 7)$, $9 \equiv 23 \ (mod\ 7)$ y también $7 \equiv 0 \ (mod\ 7)$.

Detengámonos un momento: ¿cuál es la razón de que dos números sean congruentes módulo 7? ¿Qué tienen en común? Tomemos, como ejemplo, 9 y 23, que son congruentes módulo 7 (efectúa ambos recorridos sobre el reloj y comprueba que se va a parar a la misma posición).

- Si avanzamos (desde "0" y en sentido horario) 9 posiciones veremos que damos una vuelta entera al reloj y seguimos 2 posiciones más.

- Si avanzamos (desde "0" y en sentido horario) 23 posiciones veremos que damos 3 vueltas enteras al reloj, y seguimos 2 posiciones más.

¿Cómo podríamos obtener otros números que sean congruentes con ellos? Está claro que dando varias vueltas al reloj (es decir, tomando un múltiplo de 7) y avanzando 2 posiciones más (es decir, sumando 2). Por ejemplo: $5 \cdot 7 + 2 = \mathbf{37}$, $10 \cdot 7 + 2 = \mathbf{72}$, $501 \cdot 7 + 2 = \mathbf{3509}$ y también... por supuesto... $0 \cdot 7 + 2 = \mathbf{2}$. Fíjate que lo que tienen en común todos estos números es que, **al dividirlos entre 7, el resto de esta división es en todos los casos el mismo (2).** Un poco de reflexión nos llevará a la conclusión de que ésta es la única manera de generar números congruentes (módulo 7) a uno dado. Es decir:

> Dos enteros no negativos son congruentes módulo 7 si y sólo si los restos de sus divisiones entre 7 son iguales.

**Ejercicio 1.** Determina si los siguientes pares de números son congruentes módulo 7. En los casos afirmativos calcula un número entre 0 y 6 que sea congruente con ellos.

(a) $59$ y $38$.

(b) $69$ y $41$.

(c) $82$ y $71$.

Fíjate en lo siguiente:

> Dado un número entero no negativo cualquiera $a$ **sólo hay un número entre 0 y 6 que sea congruente con $a$ módulo 7** (es el número de avances que "sobran" después de haber dado varias vueltas completas al reloj; es decir, es el **resto** de la división entre 7).

Dado un número entero no negativo $a$, denotaremos (de momento) por $\overline{a}$ (o también por $[a]$) al conjunto de todos los enteros no negativos que son congruentes con $a$ módulo 7. A estos conjuntos los llamaremos **clases de congruencia módulo 7**.

**Ejemplo 1.** Calculemos la **clase del 12**, es decir, $\overline{12}$. El resto de la división de 12 entre 7 es 5. Por tanto, pertenecerán a $\overline{12}$ todos los enteros no negativos cuyo resto al dividirlos entre 7 sea también 5. Éstos son: $5, 12, 19, 26, 33, \ldots$. (es decir, $5+0\cdot 7, 5+1\cdot 7, 5+2\cdot 7, 5+3\cdot 7, 5+4\cdot 7, \ldots$). Por tanto:

$$\overline{12} = \{5 + k \cdot 7 \mid k \text{ es un entero no negativo}\} = \{5, 12, 19, 26, 33, \ldots\}.$$

¿Cuál será la clase de un elemento que esté en $\overline{12}$, por ejemplo 19? Pues la clase $\overline{19}$ estará formada por todos aquellos enteros no negativos cuyo resto al dividirlos entre 7 sea **el mismo que el resto resultante al dividir 19 entre 7**. Como este resto es 5, está claro que: **¡los elementos de la clase del 19 <u>son los mismos</u> que los elementos de la clase del 12!** Luego $\overline{12} = \overline{19}$. Y también, claro está (por el mismo motivo):

$$\overline{5} = \overline{12} = \overline{19} = \overline{26} = \overline{33} = \cdots .$$

Todos los números en $\{\mathbf{5}, 12, 19, 26, 33, \ldots\}$ **tienen la misma clase** de congruencia módulo 7. Hemos "empaquetado" todos estos números **en una clase de congruencia**. Y fíjate en que **<u>sólo uno</u> de los elementos de la clase está entre 0 y 6**: el 5. A éste lo vamos a llamar **representante principal** de la clase.

Pensando un poco te darás cuenta de que, trabajando con un "reloj módulo 7", podemos formar **7 clases de congruencia** distintas, correspondientes a todos **representantes principales** posibles (que son 0, 1, 2 ,3, 4, 5 y 6):

$$\overline{0} = \{0, 7, 14, 21, \ldots\}$$
$$\overline{1} = \{1, 8, 15, 22, \ldots\}$$
$$\overline{2} = \{2, 9, 16, 23, \ldots\}$$
$$\overline{3} = \{3, 10, 17, 24, \ldots\}$$
$$\overline{4} = \{4, 11, 18, 25, \ldots\}$$
$$\overline{5} = \{5, 12, 19, 26, \ldots\}$$
$$\overline{6} = \{6, 13, 20, 27, \ldots\}$$

Fíjate que su unión es el conjunto de los enteros no negativos y, además, son disjuntas dos a dos (es decir, constituyen una **partición** del conjunto de los enteros no negativos). Dicho de otro modo:

| Todo entero no negativo está en una, y sólo en una, clase de congruencia. |
|---|

**Ejercicio 2.** Calcula, los representantes principales de las siguientes clases de congruencia módulo 7: $\overline{123}, \overline{56}, \overline{49}, \overline{111}, \overline{82}$. ¿Hay algunas de estas clases que sean iguales?

## 2. Generalización: "empaquetando" enteros (negativos y no negativos)

Lo que hemos hecho hasta ahora es "empaquetar" los enteros no negativos $a$ según la posición final cuando avanzamos $a$ posiciones en el "reloj módulo 7" (partiendo de "0" y en sentido horario). Pero, ¿por qué restringirnos a los enteros no negativos? ¿Por qué no considerar **todos** los enteros? La generalización es muy fácil:

> Podemos interpretar que, cuando tenemos un número entero negativo $-a$, avanzamos $a$ posiciones en el reloj **pero en sentido anti-horario.**

Por ejemplo, si avanzamos -8 posiciones (es decir, 8 posiciones en sentido anti-horario empezando desde "0") acabaremos en la posición 6. Por tanto, diremos que **-8 es congruente con 6** módulo 7, es decir, $-8 \equiv 6 \ (mod\ 7)$.

Con esta ampliación del concepto de congruencia, podemos ahora tratar de "empaquetar" **todos** los números enteros en clases de congruencia (y no sólo los no negativos):

> Dos números enteros **cualesquiera** $a$ y $b$ se dirán que *son congruentes módulo 7*, y lo escribiremos $a \equiv b \ (mod\ 7)$, si la posición ocupada en el "reloj módulo 7" después de avanzar $a$ posiciones es la misma que después de avanzar $b$ posiciones (entendiéndose en sentido horario si el número es positivo y en sentido anti-horario si es negativo).

> Dado un entero **arbitrario** $a$, llamaremos *clase de congruencia* de $a$ (módulo 7) (y la denotaremos por $\overline{a}$ o por $[a]$) al conjunto de todos los enteros que son congruentes con $a$ módulo 7.

**Ejemplo 2.** Ya sabemos que los enteros no negativos que están en la clase de congruencia de $2$ son: $2, 9, 16, 23, \ldots$, pero ahora debemos añadir también $2-7=-5,\ 2-2\cdot 7=-12,\ 2-3\cdot 7=-19, \ldots$. Es decir:

$$\overline{2} = \{2 + k \cdot 7 \mid k \text{ es un número entero}\} = \{\ldots, -19, -12, -5, 2, 9, 16, 23, \ldots\}.$$

Fíjate en que **sigue habiendo un único representante principal** en cada clase.

**Ejercicio 3.** Completa los huecos en las siguientes clases de congruencia módulo 7:

$$\overline{0} = \{\ldots, \_, \_, \_, 0, 7, 14, 21, \ldots\}$$
$$\overline{1} = \{\ldots, \_, \_, \_, 1, 8, 15, 22, \ldots\}$$
$$\overline{2} = \{\ldots, \_, \_, \_, 2, 9, 16, 23, \ldots\}$$
$$\overline{3} = \{\ldots, \_, \_, \_, 3, 10, 17, 24, \ldots\}$$
$$\overline{4} = \{\ldots, \_, \_, \_, 4, 11, 18, 25, \ldots\}$$

$$\overline{5} = \{\ldots, \_, \_, \_, 5, 12, 19, 26, \ldots\}$$
$$\overline{6} = \{\ldots, \_, \_, \_, 6, 13, 20, 27, \ldots\}$$

**Observación:** El "truco" de dividir entre 7 y tomar el resto para calcular un representante principal **no vale** en el caso de números negativos. Por ejemplo, $-8 \equiv \underline{6}$ $(mod\ 7)$ y el resto que se obtiene al dividir $8$ entre 7 es $\underline{1}$.

La siguiente propiedad nos da un criterio fácil para determinar si dos números enteros cualesquiera son congruentes módulo 7:

**Proposición 1.** Dos números enteros $a$ y $b$ son congruentes módulo 7 si y sólo si $a - b$ es un múltiplo de 7.

Por tanto:

| |
|---|
| para saber si dos números enteros son congruentes módulo 7 sólo hay que estudiar si su diferencia es un múltiplo de 7. |

Por ejemplo, $-1236$ y $47673$ son congruentes módulo 7 porque $-1236 - 47673 = -48909 = 7 \cdot (-6987)$. Por supuesto, también podemos restar a la inversa: $47673 - (-1236) = 48909 = 7 \cdot 6987$.

Aunque hemos estudiado la congruencia módulo 7, adaptada a un "reloj módulo 7", podemos considerar también un reloj "módulo 3", o "módulo 22", o... "módulo n" en general, siendo $n$ un número natural. Todo funciona **exactamente igual** (sólo hay que sustituir, en el desarrollo anterior, el 7 por $n$).

**Ejercicio 4.** Considera un "reloj módulo 4".

(b) Escribe todas las clases de congruencia módulo 4. ¿Cuántas hay?

(a) ¿Son ciertas o falsas las siguientes congruencias: $5 \equiv 17$ $(mod\ 4)$, $19 \equiv 43$ $(mod\ 4)$, $-9 \equiv 7$ $(mod\ 4)$?