# ALGORITMO DE EUCLIDES Y ALGUNAS APLICACIONES

Isabel Dotti - Alicia García

El objetivo de este trabajo es presentar el algoritmo de división en los enteros y algunas aplicaciones que ilustren su importancia y belleza.

Debido a que estamos plenamente convencidas, de que la mejor manera de estimular y lograr el aprendizaje de la matemática es a través de planteos y soluciones de problemas, dedicamos gran parte de estas notas a la presentación y solución de algunos de ellos.

Si bien no contamos con suficiente experiencia docente primaria y secundaria, creemos que los resultados y ejemplos que aparecen son fácilmente adaptables para ser accesibles e interesantes a los alumnos.

En el desarrollo, $\mathbf{Z}$ denotará el conjunto de números enteros y $\mathbf{N}$ el de los naturales.

Algoritmo de división en $\mathbb{Z}$ (Algoritmo de Euclides)

*Teorema 1:* Sean a y b enteros $b > 0$. Entonces

i) existen enteros q y r tales que:

$$a = bq + r \quad \text{con} \quad 0 \leq r < b$$

ii) Si $a = bq + r$ con $0 \leq r < b$

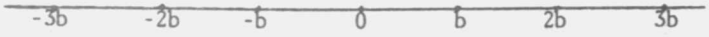
y $a = bq' + r'$ con $0 \leq r' < b$

entonces

$$q = q' \quad y \quad r = r'$$

q y r se denominan respectivamente el cociente y el resto de la división de a por b. (La parte (i) asegura la existencia de cociente q y resto r y la parte (ii) da la unicidad de q y r).

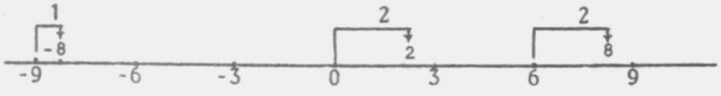
*Demostración:* Imaginemos los números enteros representados sobre el eje real. Los múltiplos enteros de b (los números de la forma bq con $q \in \mathbb{Z}$) serán




El punto que representa al número entero a debe caer en alguno de los intervalos que determinan dos múltiplos consecutivos de b. Elijamos $q \in \mathbb{Z}$ tal que $bq \leq a < b(q+1)$, entonces $a = bq + r$ siendo $0 \leq r < b$ = amplitud de cada intervalo.

Ejemplo:

b = 3




| | | |
|---|---|---|
| a = 8 | 8 = 6 + 2 = 3.2 + 2 | (q = 2, r = 2) , |
| a = -8 | -8 = -9 + 1 = 3(-3)+1 | (q = -3, r = 1) , |
| a = 9 | 9 = 3.3 | (q = 3, r = 0) , |
| a = 2 | 2 = 3.0 + 2 | (q = 0, r = 2) . |

Para quien no le satisfaga el argumento anterior, que lo destacamos por su gran intuitividad (¿no es acaso ésta la forma en que vemos los enteros?), daremos una demostración analítica. Para esto, nos apoyaremos en el *Principio de Buena Ordenación* del conjunto $N_0 = \{k \in \mathbb{Z} / k \geq 0\}$ . Este dice que cualquier subconjunto no vacío de $N_0$ tiene primer elemento.

i) Formemos el conjunto $S = \{a-kb: \ k \in \mathbb{Z} \ \text{y} \ a - kb \geq 0\}$.

Como $b \in \mathbb{Z}$ y $b > 0$ resulta $b \geq 1$, entonces $-|a|b \leq -|a| \leq a$ y por lo tanto $a-(-|a|b) \geq 0$ lo cual prueba que $S \neq \phi$.

Claramente $S \subset N_o$. Como $N_o$ está bien ordenado, existe un elemento mínimo en S que denotaremos por r. Notemos que:

$$r = a - qb \quad \text{para algún } q \in \mathbb{Z}$$

$$r \geq 0$$

$$r \leq a - kb \quad \forall k \in \mathbb{Z} \ \text{tal que} \ a - kb \geq 0.$$

Veremos ahora que $r < b$. Si $r \geq b$, $r - b \geq 0$;

$a - (q + 1)b = (a - qb) - b = r - b \geq 0$ y en consecuencia

$a - (q+1)b = r - b \in S$. Como $b > 0$, $-b < 0$ y $r - b < r$ con lo cual llegamos a una contradicción (por ser r el elemento mínimo de S) que provino de suponer $r \geq b$. Resulta entonces $r < b$.

ii) Sea $a = qb + r$ con $0 \leq r < b$

$a = q'b + r'$ con $0 \leq r' < b$.

Restando las dos igualdades anteriores obtenemos

$$(q - q')b = r - r'$$

por lo tanto sus valores absolutos son iguales, o sea

$$|q - q'| \ b = |r - r'| .$$

Si $q \neq q'$, $|q - q'| \geq 1$ y de la última igualdad concluímos

$$|r - r'| \geq b \quad (*)$$

Como $r' \geq 0$, $r - r' \leq r < b$, o sea

$$r - r' < b \quad (**)$$

Por ser $r' < b \leq b + r$ resulta

$$-b < r - r' \quad (***)$$

(**) y (***) equivalen a

$$|r - r'| < b$$

lo cual contradice (*). Por lo tanto debe ser $q = q'$ ; usando las expresiones de a es inmediato que $r = r'$ .

*Observación 2:* Notemos que si a y b son enteros, $b < 0$ entonces $-b > 0$ y por el teorema 1 existen únicos enteros q y r tales que

$$a = (-b)q + r \qquad \text{con} \qquad 0 \leq r < -b.$$

Del teorema 1 y de la observación 2 resulta probado el siguiente:

*Teorema 3:* Sean a y b enteros, $b \neq 0$. Entonces:

i) Existen enteros q y r tales que

$$a = bq + r \qquad \text{con} \qquad 0 \leq r < |b|$$

ii) Si además, $a = bq' + r'$ con $0 \leq r' < |b|$ entonces $q = q'$ y $r = r'$.

En las condiciones del teorema anterior se dice que b *divide al número* a o que a *es múltiplo de b* (se denota por $b|a$ ó $a \doteq b$) si el resto r en la división de a por b es 0.

Con los siguientes ejemplos y problemas ilustraremos el contenido y la importancia del teorema 3.

*Ejemplo:*

Si $a = 219$ , $b = 15 \Rightarrow q = 14$ y $r = 9$.

Si $a = 219$ , $b = -15 \Rightarrow q = -14$ y $r = 9$.

Si $a = -219$ , $b = 15 \Rightarrow q = -15$ y $r = 6$.

Si $a = -219$ , $b = -15 \Rightarrow q = 15$ y $r = 6$.

*Problema 4:* El cociente y el resto de la división de a por 7 son q y 5 respectivamente. ¿Cuál es el cociente y el resto de la división de a-15 por 7?

*Solución:* Si $a = 7q + 5$ entonces $a - 15 = 7q + 5 - 15 = 7q - 10$.

Como $-10 = 7(-2) + 4$ resulta

$$a - 15 = 7q + 7.(-2) + 4 = 7(q-2) + 4.$$

Concluímos así, que el cociente es q-2 y el resto es 4.

*Problema 5:* El cociente y el resto de la división de a por 11 es 21 y r respectivamente. ¿Qué se puede decir del cociente y el resto de la división de a + 701 por 11?

*Solución:* $a = 11.21 + r$ con $0 \leq r < 11$

$701 = 11.63 + 8$

entonces, $a + 701 = 11(21 + 63) + r + 8$, o sea

$$a + 701 = 11.84 + r + 8 .$$

Como r + 8 es la suma de dos restos en la división por b = 11, siempre es menor que 2b. Entonces basta considerar los casos:

i) $0 \leq r + 8 < b = 11$,

ii) $b = 11 \leq r + 8 < 2b = 22$ .

En el primer caso, es claro que el cociente será 84 y el resto r + 8.

En el segundo caso,

$r + 8 = 11 + (r + 8 - 11) = 11 + (r - 3)$ donde $0 \leq r - 3 < 11$ y así

$a + 701 = 11.85 + (r - 3)$

resultando el cociente 85 y el resto r - 3.

*Problema 6:* (descomposición b-ádica). Sean a y b enteros, $a \geq 0$ y $b > 1$. ¿Existen enteros $c_i$ y $m \geq 0$ tales que $0 \leq c_i < b$ y $a = \sum_{i=0}^{m} c_i b^i$ ?

*Solución:* Pensemos primero en un ejemplo con a = 2.537 y b = 10.

$a = 2.530 + 7 = 253 \times 10 + 7 = (250 + 3) \times 10 + 7 =$

$= (25 \times 10 + 3) \times 10 + 7 = [(20 + 5) \times 10 + 3] \times 10 + 7 =$

$= [(2 \times 10 + 5) \times 10 + 3] \times 10 + 7 = 2 \times 10^3 + 5 \times 10^2 + 3 \times 10 + 7$

Lo que hicimos en este ejemplo se puede generalizar fácilmente. En efecto (usaremos repetidas veces el algoritmo de división):

$$a = bq_1 + r_1 \qquad \text{con} \qquad 0 \leq r_1 < b.$$

Notemos que por ser $a \geq 0$ y $b > 1$ resulta

$$0 \leq q_1 < a$$

Si $q_1 < b$ entonces tenemos la solución del problema con $m = 1$, $c_0 = r_1$ y $c_1 = q_1$.

Si $q_1 \geq b$ entonces $q_1 = bq_2 + r_2$ con $0 \leq r_2 < b$, resultando $0 \leq q_2 < q_1$.

Además,

$$a = b(bq_2 + r_2) + r_1 = b^2q_2 + br_2 + r_1.$$

Si $q_2 < b$ entonces $m = 2$, $c_0 = r_1$, $c_1 = r_2$, $c_2 = q_2$ es la solución buscada.

Si $q_2 \geq b$ iteramos el proceso. Este proceso concluye en un número finito de pasos puesto que, en el i-ésimo paso

$$0 \leq q_i < q_{i-1} \text{ (entendemos } q_0 = a)$$

y por lo tanto existe m tal que $q_m < b \leq q_{m-1}$.

*Ejercicio 7:* Probar que el m y los $c_i$ del problema anterior son únicos (de allí que se llama a la descomposición anterior, representación b-ádica del número a).

(Ayuda: Suponer dos descomposiciones de a y usar adecuadamente la unicidad del cociente y resto).

*Congruencias*

Sean a, b, $m \in \mathbf{Z}$, $m > 0$. Se dice que a *es congruente a* b *módulo* m, $a \equiv b(m)$, si $m \mid a-b$.

*Ejemplos:* a) $21 \equiv 9(6)$ b) $-5 \equiv 7(3)$

c) Los números pares son aquellos que son congruentes a 0 o módulo 2.

A continuación deduciremos, de la definición de congruencia, varias propiedades que serán de suma utilidad en el tratamiento de muchos problemas como veremos luego.

*Proposición 8:* Si a, b, c, d y m son números enteros y $m > 0$, entonces se cumple:

(i) $a \equiv a(m)$,

(ii) $a \equiv b(m) \iff b \equiv a(m)$,

(iii) $a \equiv b(m)$ y $b \equiv c(m) \Rightarrow a \equiv c(m)$,

(iv) $a \equiv 0(m) \iff m|a$,

(v) $a \equiv b(m)$ y $c \equiv d(m) \Rightarrow a+c \equiv b+d(m)$ y $ac \equiv bd(m)$. En particular si $n \geq 0$, $n \in \mathbb{Z}$ y $a \equiv b(m)$ entonces $na \equiv nb(m)$ y $a^n \equiv b^n(m)$,

(vi) $a \equiv b(m) \iff$ a y b tienen el mismo resto en la división entera por m.

*Demostración:* La demostración de las 4 primeras propiedades es inmediata y queda como ejercicio para el lector (Por las 3 primeras, la relación de congruencia es de equivalencia y por lo tanto produce una partición en $\mathbb{Z}$ que veremos en observación 22).

Supongamos que $a \equiv b(m)$ y $c \equiv d(m)$. Entonces existen $k, \ell \in \mathbb{Z}$ tales que:

$$(a+c) - (b+d) = (a-b) + (c-d) = mk + m\ell = m(k+\ell),$$

$$ac - bd = c(a-b) + b(c-d) = cmk + bm\ell = m(ck + b\ell)$$

lo cual prueba (v).

Veamos (vi): Sean

$$a = q_a\, m + r_a \qquad 0 \leq r_a < m,$$
$$b = q_b\, m + r_b \qquad 0 \leq r_b < m$$

y supongamos que $r_a \geq r_b$. Entonces $a - b = (q_a - q_b)m + r_a - r_b$ donde $0 \leq r_a - r_b < m$.

Por lo tanto $m|a-b \iff m|(q_a-q_b)m + r_a-r_b \iff m|r_a-r_b \iff r_a-r_b = 0$ (esto último resulta por ser 0 el único múltiplo de m no negativo y menor que m).

Si $r_a \leq r_b$ consideramos $b - a$ y repetimos el argumento anterior.

*Ejemplo:* Queremos determinar todos los $a \in \mathbf{Z}$ tales que $a \equiv 3\ (5)$. Usando 8 (vi), $a \equiv 3\ (5) \iff$ a y 3 tienen el mismo resto en la división por 5, o sea $a = q\,5 + 3$ con $q \in \mathbf{Z}$


Notar que $\{a \in \mathbf{Z}: a \equiv 3\ (5)\} = \{a \in \mathbf{Z}: a \equiv 8\ (5)\} =$
$\{a \in \mathbf{Z}: a \equiv b\ (5)$ y $b \equiv 3\ (5)\}$.

*Problema 9:* El resto de la división de a por 7 es 5. ¿Cuál es el resto de la división de a - 15 por 7?

*Solución:* Por 8 (vi), debemos encontrar r tal que $0 \leq r < 7$ y $a \equiv 15 \equiv r(7)$.

Como $a \equiv 5\ (7)$ (ver 8 (vi)) y $-15 \equiv -8\ (7)$, resulta de 8 (v) que $a - 15 \equiv -3\ (7)$. Usando que $-3 \equiv 4\ (7)$ y 8 (iii) obtenemos $r = 4$.

Notemos que ésta es otra forma de resolver parte del problema 4.

*Problema 10:* ¿Cuál es el último dígito de $18^{7}$?

*Solución:* Usando el problema 6,

$183^7 = c_n\, 10^n + c_{n-1}\, 10^{n-1} + \ldots + c_1\, 10 + c_o = 10\, k + c_o$ donde

$0 \leqslant c_i < 10 \quad i = 1, \ldots, n.$

Encontrar la cifra de las unidades de $183^7$ equivale a determinar $c_o$. Por lo tanto, $c_o$ debe satisfacer

$$183^7 \equiv c_o \ (10) \qquad y \qquad 0 \leqslant c_o < 10.$$

Como $183 \equiv 3\ (10)$ resulta, de 8 (v), $183^7 \equiv 3^7\ (10)$ con lo cual se ha simplificado el problema puesto que de $3^4 \equiv 1\ (10)$ y $3^3 \equiv 7\ (10)$ se obtiene $3^7 \equiv 7\ (10)$. Como consecuencia $c_o = 7$.

*Ejercicio 11:* ¿Cuáles son las cifras de las decenas de los números $183^7$ y $523^4.52^3$ ?

*Problema 12:* ¿Por qué para saber si un número es múltiplo de 2 basta con considerar su último dígito?

*Solución:* Notemos que si $a \in \mathbf{Z}$ y $a = \dot{k}$, entonces $-a = \dot{k}$. Por lo tanto bastará analizar el caso $a \geqslant 0$.

De 6, $a = a_n\, 10^n + a_{n-1}\, 10^{n-1} + \ldots + a_1\, 10 + a_o$ con $0 \leqslant a_i < 10$.

Como $10 \equiv 0\ (2)$, resulta de 8 (v) $10^n \equiv 0\ (2)$ y $a_n\, 10^n \equiv a_n 0\ (2)$, $\forall\, n \in \mathbf{N}$. Usando nuevamente 8 (v) $a_n\, 10^n + \ldots + a_1\, 10 + a_o \equiv 0 + \ldots + 0 + a_o\ (2)$, por lo tanto $a \equiv a_0 (2)$. De 8 (vi), a y $a_0$ tienen el mismo resto en la división por 2 y en consecuencia:

$$a = \dot{2} \iff a_o = \dot{2}$$

La última equivalencia es lo que conocemos como *regla de divisibilidad* por 2.

*Problema 13:* Hallar una regla de divisibilidad por 3.

*Solución:* Como $10 \equiv 1\ (3)$, entonces $10^n \equiv 1\ (3)$ para cualquier

$n \in \mathbb{N}$. Por lo tanto $a_n\, 10^n \equiv a_n\ (3)$ $\forall\, n \in \mathbb{N}$ y en consecuencia:

$a = a_n\, 10^n + a_{n-1}\, 10^{n-1} + \ldots + a_1\, 10 + a_0 \equiv a_n + a_{n-1} + \ldots + a_1 + a_0\ (3)$.

De 8 (vi) concluímos que $a = \dot{3}$ (o sea el resto de la división de a por 3 es 0) sí y sólo si $a_n + a_{n-1} + \ldots + a_0 = \dot{3}$.

*Problema 14:* Hallar una regla de divisibilidad por 8.

*Solución:* $10 \equiv 2\ (8)$; $10^2 = 10.10 \equiv 4\ (8)$; $10^3 = 10.10^2 \equiv 0\ (8)$; $10^n = 10^{n-3}\, 10^3 \equiv 0\ (8)$ si $n \geqslant 4$. Por lo tanto,

$$a = a_n\, 10^n + \ldots + a_1\, 10 + a_0 \equiv 4\, a_2 + 2\, a_1 + a_0\ (8).$$

Es simple ahora formular la regla buscada.

*Ejercicio 15:* Hallar reglas de divisibilidad por 4, 5, 6, 7, 9, 11, 13.

*Ejercicio 16:* Sea $m \in \mathbb{N}$. ¿Cuál es el número máximo de potencias naturales de 10 que hay que analizar para hallar una regla de divisibilidad por m?.

Notar que para cualquier $m \in \mathbb{N}$ existe una tal regla.

*Ejercicio 17:* Sea a un entero par múltiplo de un número impar n. Probar que a es múltiplo de 2 n.

*Observación 18:* (Prueba del nueve). Es muy común, sobre todo en la escuela primaria, enseñar la "prueba del 9" para que los alumnos verifiquen si realizaron correctamente una multiplicación entre números naturales. Recordemos dicha prueba:

$$\begin{array}{r} 731 \\ \times\ 46 \\ \hline 4386 \\ 2924 \\ \hline 33626 \end{array} \qquad \begin{array}{ccc} & 2 & \\ 2 & & 2 \\ & 1 & \end{array}$$

¿Qué hemos hecho?. Dados $a_1$ y $a_2$ números naturales,

$$\begin{array}{r} a_1 \\ \times\ a_2 \\ \hline a_3 \end{array} \qquad \begin{array}{ccc} & a'_1 & \\ x & & a'_3 \\ & a'_2 & \end{array}$$

donde $a'_1$, $a'_2$ , $a'_3$ y x son números enteros tales que $0 \leq a'_i < 9$ $i = 1, 2, 3$, $0 \leq x < 9$ y $x \equiv a'_1 a'_2 (9)$.

Si se ha realizado correctamente la multiplicación entonces $x = a'_3$ . En efecto: si $a_1 \equiv a'_1 (9)$ y $a_2 \equiv a'_2 (9)$ , entonces por 8 (v) $a_3 = a_1 a_2 \equiv a'_1 a'_2 (9)$. Luego los restos de las divisiones de $a_3$ y $a'_1 a'_2$ por 9 deben coincidir, o sea $x = a'_3$ .

Debemos destacar que *productos incorrectos pueden ocasionar pruebas correctas*. Para ilustrar veamos que en cualquiera de los 3 casos siguientes se satisface la regla y sólo una de las igualdades es correcta:

$734 \times 21 = 15414$; $734 \times 21 = 14514$; $734 \times 21 = 15594$.

Por lo tanto, la conocida prueba sólo nos asegura que si $x \neq a'_3$ entonces el resultado de la multiplicación es incorrecto.

*Problema 19:* El producto entre un número natural de 3 cifras y 3 termina en 785. ¿Cuál es el número?

*Solución:* Sea $x = a\,10^2 + b\,10 + c$ el número que queremos determinar. Como $3x = 3a\,10^2 + 3b\,10 + 3c$, resulta $3c \equiv 5 (10)$ y por lo tanto $c = 5$ (considerando todos los c tales que $0 \leq c \leq 9$, $c = 5$ es el único que satisface lo deseado). Entonces $3x = 3a\,10^2 + (3b + 1)10 + 5$.

Análogamente, $3b + 1 \equiv 8(10)$ obteniendo $b = 9$ y $3a + 2 \equiv 7(10)$ resultando $a = 5$. Por lo tanto $x = 595$ satisface lo propuesto.

¿Tiene este problema otra solución?. La respuesta es negativa puesto que los números a, b y c anteriores estuvieron unívocamente determinados.

*Otra solución:* Como $x < 1000$, $3x < 3000$; por hipótesis

$3x = 10^3\,d + 785 = d\,785$. Luego los d posibles son 0,1 y 2 obte-

niendo 785, 1785 y 2785 de los cuales 1785 es el único múltiplo de 3. En consecuencia $x = 1785 \div 3 = 595$ es la única solución del problema.

*Problema 20:* ¿Existe un número de 3 cifras tal que al multiplicarlo por 6 resulte un número que termine en 542?. ¿Es único?

*Solución:* Los ejemplos $757 \times 6 = 4542$ y $257 \times 6 = 1542$ resuelven el problema.

¿Son éstas las 2 únicas soluciones?

*Problema 21:* Sean n y m enteros positivos distintos ¿Son $2^{2^n} + 1$ y $2^{2^m} + 1$ coprimos?

*Solución:* Sea $d > 0$ un divisor común de $2^{2^n} + 1$ y $2^{2^m} + 1$. Entonces:

$$(*) \qquad \begin{aligned} 2^{2^n} &\equiv -1 \ (d) \\ 2^{2^m} &\equiv -1 \ (d) \end{aligned}$$

Si $n < m$, $2^{2^m} = 2^{2^n \cdot 2^{m-n}} = (2^{2^n})^{2^{m-n}} \equiv (-1)^{2^{m-n}}$ (d) (por *). Como $2^{m-n}$ es par $(m-n > 0)$, $2^{2^m} \equiv 1$ (d) y usando (*) resulta $1 \equiv -1$(d), o sea $2 \equiv 0$(d). Entonces $2 = kd$ y por lo tanto $d = 1$ o $d = 2$. Como d es divisor de $2^{2^n} + 1$ (impar) sólo puede ser $d = 1$.

Concluímos que $2^{2^n} + 1$ y $2^{2^m} + 1$ son coprimos cuando $n \neq m$.

*Nota:* En el artículo "Cinco pruebas para un teorema de Euclides" O. Cámpoli, Revista de Educación Matemática, Vol. 1 N° 2 1982, hay otra prueba de este hecho, del cual resulta en forma inmediata la existencia de infinitos números primos.

*Proposición 22:* Sea $m > 0$ y $A_r = \{a \in \mathbb{Z}: a \equiv r(m)\}$. Entonces

i) $\bigcup_{r \in \mathbb{Z}} A_r = \mathbb{Z}$

ii) $A_r \cap A_s = \phi$ ó $A_r = A_s$

*Demostración:*

i) Sea $a \in \mathbb{Z}$. Por el teorema 1, $a = qm + r$ con $0 \leq r < m$ y por lo tanto $a \equiv r(m)$, o sea $a \in A_r$. Hemos probado que $\mathbb{Z} \subset \bigcup_{r \in \mathbb{Z}} A_r$ y como la otra inclusión es obvia concluímos que $\bigcup_{r \in \mathbb{Z}} A_r = \mathbb{Z}$.

ii) Supongamos que $A_r \cap A_s \neq \phi$ y sea $a \in A_r \cap A_s$. Entonces $a \equiv r(m)$ y $a \equiv s(m)$; por lo tanto $r \equiv s(m)$. Esto último nos permite probar que $A_r = A_s$.

En efecto, si $b \in A_r$, $b \equiv r(m)$ y por lo tanto $b \equiv s(m)$, o sea $b \in A_s$. En forma análoga se prueba que $A_s \subset A_r$.

*Observación 23:*

i) Si $0 \leq r < m$ entonces $r \in A_r$ puesto que r será el resto de la división entera de r por m.

ii) $\{A_0, A_1, \ldots, A_{m-1}\}$ es una partición de $\mathbb{Z}$.

Notemos que en 22(i) hemos probado que $\mathbb{Z} \subset \bigcup_{r=0}^{m-1} A_r$ y por lo tanto $\mathbb{Z} = \bigcup_{r=0}^{m-1} A_r$.

Sea $a \equiv r(m)$ y $a \equiv s(m)$ con $0 \leq r, s < m$. Por el teorema 1, $r = s$ con lo cual concluímos que si $A_r \cap A_s \neq \phi$ entonces $A_r = A_s$.

Es usual denotar $[r] = A_r$ y llamar $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. $\mathbb{Z}_m$ nos proporcionará un ejemplo de conjunto finito (de m elementos) donde es posible definir algunas estructuras algebraicas.

Definimos en $\mathbb{Z}_m$ las siguientes operaciones:

$[a] + [b] = [a+b]$ (= resto de la división de $a + b$ por m)

$[a] \cdot [b] = [ab]$ (= resto de la división de ab por m)

Con estas operaciones resulta:

*Proposición 24:* $(\mathbb{Z}_m, +)$ es grupo abeliano y $(\mathbb{Z}_m, +, .)$ es anillo conmutativo con unidad $(= [1])$.

*Demostración:* ejercicio.

*Problema 25:* ¿Es $(\mathbb{Z}_m, +, .)$ cuerpo?

*Solución:* Notemos que, por 24, sólo necesitamos ver si cada $[a] \neq [0]$ tiene inverso respecto de la operación $\cdot$ (que denotaremos por $[a]^{-1}$). Como $[1]^{-1} = [1]$ podemos además considerar $[a] \neq [1]$.

Como $\mathbb{Z}_2 = \{[0], [1]\}$ resulta inmediato que $\mathbb{Z}_2$ es cuerpo.

$\mathbb{Z}_3 = \{[0], [1], [2]\}$ y $[2] . [2] = [4] = [1]$ resulta $[2]^{-1} = [2]$ y $\mathbb{Z}_3$ cuerpo.

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Podemos hacer la siguiente tabla:

| . | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [2] |
| [3] | [0] | [3] | [2] | [1] |

De lo cual concluímos que $[3]^{-1} = [3]$ y que no existe $[2]^{-1}$ (observar la 4ta fila de la tabla), por lo tanto $\mathbb{Z}_4$ no es cuerpo.

De los ejemplos analizados resulta que no es posible dar respuesta afirmativa ni negativa al problema planteado. Sin embargo, notemos que para el caso m = 4 el elemento [2], que no tiene inverso, satisface $[2] . [2] = [0]$. Como $[3] . [4] = [0]$ en $\mathbb{Z}_{12}$, no existe $[3]^{-1}$ y $[4]^{-1}$ en $\mathbb{Z}_{12}$ (supongamos que existe $[3]^{-1}$, entonces $[3]^{-1} . [3] . [4] = [3]^{-1} . [0]$ y por lo tanto $[4] = [0]$ en $\mathbb{Z}_{12}$ lo cual es una contradicción). Esto motiva el siguiente *hecho general:*

"Si m no es primo entonces $\mathbb{Z}_m$ no es cuerpo".

*Prueba*: Como m no es primo, existen $m_1$ y $m_2$ tales que $m = m_1 m_2$ y $1 < m_i < m$ $i = 1, 2$. Entonces, $[0] = [m] = [m_1 m_2] = [m_1].[m_2]$ de lo cual concluímos que $\mathbb{Z}_m$ no es cuerpo puesto que $[m_1]$ ($[m_2]$) no tiene inverso multiplicativo (repetir argumento utilizado en el caso m = 12).

*Nota:* Sugerimos la lectura del artículo "¿Qué día de la semana fue el 1 de enero de 1901? ¿Qué día de la semana será el 1 de enero del 2001? Enzo R. Gentile, Revista de Educación Matemática, Vol. 1, N° 3, 1982. En este trabajo se encuentra una interesante aplicación de congruencia modulo 7.

Facultad de Matemática, Astronomía y Física
Universidad Nacional de Córdoba.