Algoritmo de la división

Ana Ofelia Negrete Fernández

17 de Julio 2021

1. Introducción

El algoritmo de la división nos dice que siempre que intentemos dividir dos enteros a, b, la división será exacta o en otro caso, existirá un residuo. También nos dice que siempre vamos a poder hacer esta operación para cualesquiera dos enteros y el resultado será único.

Por ejemplo, tomemos $a = 2$, $b = 3$. Entonces $2 \div 3 = 3 \cdot 0 + 2$.

Alguien diría que dividir 2 entre 3 da cero, "pues el 3 es mayor que 2 y no hay modo de hacer caber el 3 en el 2." Y en efecto, el resultado es 0, pero hay un residuo que no se mencionó. El residuo es, en este caso, 2.

O podríamos elegir $a = 3$ y $b = 2$. Tendríamos que $3 \div 2 = 2 \cdot 1 + 1$.

Si nos preguntáramos: ¿Cuántos equipos de 2 personas se pueden formar si hay 3 personas en total? La respuesta sería: Podríamos formar dos equipos de 2 personas cada uno, y dejar a alguien fuera.

Mejor quizá, sabiendo esto, diríamos: "Hagamos un equipo de 2 personas y otro de 3, porque no queremos que nadie se quede fuera."

Así, el algoritmo de la división dice más precisamente: Dados $a, b \in \mathbb{Z}$, es posible encontrar q y r únicos, tales que $a = bq + r$, con $0 \leq r < |b|$. A q se le llama cociente y a r le llamamos residuo.

Que no espante el valor absoluto que se le añade a la b. Esto se irá explicando en el presente texto, y más aún, antes de demostrar el teorema daremos previamente una intuición numérica para que sí entendamos la demostración del algoritmo de la división en $\mathbb{Z}$. Esta receta de "algoritmo de la división" después se extiende hacia otras estructuras numéricas.

2. Intuición para entender el algoritmo de la división en $\mathbb{Z}$

Comencemos planteando el problema de encontrar q y r enteros tales que $3531 = 8q + r$, para $0 \leq r < 8$.

Ya que r debe ser un número muy pequeño entre 0 y 8, podemos ir dando valores a r hasta encontrar un q que divida exactamente a 8, observando que $3531 - 8q = r$.

Si $r = 0$, habríamos de verificar si 3531 es múltiplo de 8. No es el caso, pues $8 \cdot 66 + 3 = 531$ (es un criterio de divisibilidad del 8, que si 8 no divide al número formado por las últimas tres cifras de $x \in \mathbb{Z}$, entonces 8 no divide a x).

Si $r = 1$, entonces querríamos ver si $8q = 3530$, pero 3530 tampoco es múltiplo de 8, pues $530 = 8 \cdot 66 + 2$.

Si $r = 2$, buscaríamos si $8q = 3529$, pero $529 = 8 \cdot 66 + 1$.

Finalmente, si $r = 3$, entonces $3531 - 8q = r \implies 8q = 3528$, pues como $8 \cdot 66 = 528$ -es decir, 528 sí es múltiplo de 8-, entonces 3528 también es múltiplo de 8. En efecto, $8 \cdot 441 = 3528$.

Hemos encontrado $q = 441$, $r = 3$, para los que $3531 = 8q + r$, con lo que terminamos el problema.

Geométricamente, esto significa que 3531, en la recta de los números enteros, estará situado entre dos múltiplos de 8, a saber, $8 \cdot 441$ y $8 \cdot 442$:

$$\ldots < 8 \cdot 441 < 3531 < 8 \cdot 442 < \ldots.$$

Más precisamente, como 3531 es un entero positivo, el problema consistió en encontrar el múltiplo de 8 más cercano por la izquierda y añadir 3 unidades; también dicho, "3531 está a 3 unidades de distancia de ser un múltiplo de 8 por la izquierda:"

$$8 \cdot 441 < 8 \cdot 441 + 1 < 8 \cdot 441 + 2 < 3531 < 8 \cdot 441 + 4 < 8 \cdot 441 + 5 < 8 \cdot 441 + 6 < 8 \cdot 441 + 7 < 8 \cdot 442.$$

Generalizando aún más, podemos tomar algún entero b (no necesariamente el 8) y siempre podremos situar a otro $a \in \mathbb{Z}$ en la recta numérica, de tal modo que este sea múltiplo de b o esté entre dos múltiplos de b que sean consecutivos, obteniendo

$$qb \leq a < (q+1)b, \qquad q \in \mathbb{Z}.$$

Los múltiplos de b en la recta numérica se verían así:

$$\ldots - 4b, -3b, -2b, -b, 0, b, 2b, 3b, 4b, \ldots$$

De tal modo que q sería el mayor múltiplo de b más cercano a a, sin excederse de a.

3. Demostración del algoritmo de la división en $\mathbb{Z}$

Previamente a enunciar el teorema del algoritmo de la división, recordemos que, en la sección de números naturales se demostró el principio del buen orden:

Principio del buen orden (PBO). Todo subconjunto no vacío de $\mathbb{N}$ tiene un primer elemento (es decir, un elemento menor que todos los demás).

En otras palabras, el principio del buen orden nos decía que $\mathbb{N}$ es un conjunto bien ordenado. También, el principio del orden es equivalente al principio de inducción matemática, de modo que, en los axiomas de Peano, se pueden intercambiar el principio de inducción por el principio del buen orden (aunque suele ser más fácil demostrar hechos usando inducción).

También usaremos la función valor absoluto al enunciar el algoritmo de la división:

Definición (Valor absoluto). Si $b \in \mathbb{Z}$, definimos el valor absoluto de b, denotado $|b|$, como sigue:

$$|b| = \begin{cases} b & \text{si } b \geq 0 \\ -b & \text{si } b < 0. \end{cases} \tag{1}$$

En el algoritmo de la división nos darán dos números enteros a y b. Para la restricción $0 \leq r \leq |b|$, sucederá que, no importa si b sea un número positivo o negativo, nosotros nos fijaremos en el número siempre positivo que resulta de aplicarle valor absouluto a b. $|b|$ siempre es un número positivo. Lo que hace que esa desigualdad tenga sentido.

Ya con esto, podemos enunciar y demostrar el...

Teorema (Algoritmo de la división en $\mathbb{Z}$). Sean $a, b \in \mathbb{Z}$. Existen q y r enteros únicos tales que

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

Demostración.- Primero hay que demostrar que siempre existen q y r enteros que satisfacen las condiciones que queremos.

Si $a = 0$, elegimos $q = 0 = r$. En otro caso, consideremos a S un subconjunto de enteros no negativos,

$$S = \{a - bq \ : \ q \in \mathbb{Z} \quad \text{y} \quad a - bq \geq 0\}.$$

Primero hay que demostrar que $S \neq \emptyset$, para aplicar el principio del buen orden.

Si $a \geq 0$, podemos elegir $q = 0$. Así, $a \in S$, lo que implica $S \neq \emptyset$.

Si $a < 0$, tomando $q = a$ tenemos que $a - ab = a(1 - b)$. Como $a < 0$, entonces $1 - b \leq 0$ ya que $a - ab$ debe ser positivo o cero. Concluimos que $a(1 - b) \in S$ y con esto, $S \neq \emptyset$.

Así, por el principio del buen orden, en S existe un elemento mínimo.

Sea $a - bq = r$ tal elemento. Hay que verificar que se cumple que $0 \leq r < |b|$

Como $r \in S$, entonces $r \geq 0$.

Ahora supongamos por contradicción, que $r \geq |b|$. Eso significa que

$$\begin{aligned} r &> r - |b| \\ &= a - bq - |b| \\ &\geq 0, \end{aligned}$$

lo que significa que hemos encontrado un elemento más pequeño en S, a saber, $a - bq - |b|$ y diferente de r. Pero eso contradice el hecho de que r era por hipótesis, el elemento mínimo en S. Concluimos entonces, que es imposible que $r \geq |b|$. Es decir, forzosamente $r < |b|$.

Con esto queda demostrada la existencia de los enteros q y r, tales que $a = bq + r$, con $0 \leq r < |b|$. Falta ver la unicidad:

Supongamos que existen q' y r' enteros que cumplen

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

y tales que $q \neq q'$, y $r \neq r'$.

Demostramos primero que $r = r'$.

Aquí cabe recordar, para evitar confusiones, que para demostrar la unicidad, se suele SUPONER qué pasaría si existieran elementos r y r' distintos (la demostración es por contradicción), lo que nos llevará, mediante una cadena de pasos lógicos, a que $r = r'$, lo cual contradecirá la hipótesis. Así, se concluirá que r es único.

Ya que estamos suponiendo por contradicción, que $r \neq r'$, entonces alguno de ellos es menor que el otro. Elijamos $0 \leq r' < r$, sin pérdida de generalidad.

Tenemos por un lado, que $0 \leq r - r' < r < |b|$.

Luego, como $bq' + r' = a = bq + r$, entonces

$$0 = a - a = bq + r - (bq' + r') = bq + r - bq' - r',$$

lo que implica que

$$\begin{aligned} bq' - bq &= r - r' \qquad (1) \\ \implies b(q' - q) &= r - r'. \end{aligned}$$

Ya que q' es distinto de q (lo supusimos), entonces $q' - q \neq 0$. Como $r - r' > 0$, también tenemos que $b(q' - q) > 0$, de donde $q' - q > 0$. Así, $b(q' - q) \geq |b|$. Y esto implica que $r - r' \geq |b|$. Una contradicción, pues ya teníamos que $r - r' < |b|$.

Así, concluimos que $r' = r$. Ahora usamos este hecho para demostrar que $b' = b$:

$r = r'$ implica que $r - r' = 0$. De este modo, sustituyendo en (1) obtenemos $bq' - bq = 0$. De la ley de la cancelación en $\mathbb{Z}$, se deslinda $q' = q$.

Esto termina de demostrar que q y r son únicos.

□

Ejercicios.

1. Encuentra q y r enteros tales que $-1873 = 31q + r$.
2. En general, ¿cómo se calcula q, para $a < 0$?
3. Demuestra que 8 divide a $x \in \mathbb{Z}$ si y sólo si 8 divide al número formado por las últimas 3 cifras de x.
4. Sea a un entero positivo. Muestra que es posible escribir $b = r_m 8^m + \ldots + r_1 8 + r_0$, donde $r_m > 0$ y $0 \leq r_1 < 8$, para $i \in \{0, \ldots, m\}$. A esto se le llama base 8 o representación octal de b.