# Construcción de los números enteros

Ana Ofelia Negrete Fernández

14 de julio de 2021

## 1. Introducción

Las ecuaciones de la forma $a = b + x$ no siempre tienen solución en $\mathbb{N}$; tómese cualquier $a < b$, con $a, b \in \mathbb{N}$. Por ejemplo, no existe ninguna $x \in \mathbb{N}$ tal que $3 = 5 + x$. Ello es motivación suficiente para querer construir un conjunto de números, denotado $\mathbb{Z}$, donde toda ecuación que tenga esa forma sí sea cerrada en ese conjunto. Es decir, "para cualquier $a, b, x \in \mathbb{N}$ tal que $a = b + x$, se cumplirá que $b + x \in \mathbb{Z}$."

Más intuitivamente, $\mathbb{N}$ está conformado por el cero y demás números estrictamente positivos, pero en ocasiones eso no basta para realizar algunas cuentas. Consideremos el siguiente problema:

Una rana está en una posición inicial 0 y salta dos unidades hacia la derecha. A continuación salta 3 unidades hacia la izquierda. Luego vuelve a saltar dos unidades hacia la derecha y seguido de esto vuelve a saltar 3 unidades a la izquierda. Una última vez, la rana salta 2 unidades a la derecha seguidas de 3 unidades a la izquierda. ¿En qué posición se encuentra la rana ahora?

Respuesta: ¡Está en la posición -3! El cual es un número negativo que no vive en $\mathbb{N}$.

En esta entrada de blog, dado que ya conocemos $\mathbb{N}$, lo usaremos para construir a $\mathbb{Z}$, el conjunto de los números enteros, de la manera más formal posible. Es decir, veremos que:

1. Un número entero es una clase de equivalencia
$$[(a,b)]_\sim := \Big\{(c,d) \in \mathbb{N} \times \mathbb{N} : \Big(a + d = b + c\Big) \;\; \wedge \;\; \Big((a,b) \in \mathbb{N} \times \mathbb{N}\Big)\Big\}.$$
2. El conjunto de los números enteros será la colección de todas las clases de equivalencia arriba mencionadas;
$$\mathbb{Z} := \Big\{[(a,b)]_\sim : (a,b) \in \mathbb{N} \times \mathbb{N}\Big\}.$$
3. $\mathbb{Z}$ es un dominio entero, con las propiedades usuales para la suma y producto de sus elementos.

## 2. ¿Qué es un número entero?

Comencemos tomando una pareja ordenada $(a, b) \in \mathbb{N} \times \mathbb{N}$, para la cual, la ecuación

$$a = b + x \tag{1}$$

tenga solución en $\mathbb{N}$. Es decir, $a \geq b$. Observemos luego que hay varias parejas $(c, d)$ distintas de $(a, b)$, para las que una misma $x \in \mathbb{N}$ resuelve $a = b + x$ y $c = d + x$ respectivamente; por ejemplo, elíjanse $a = 7$, $b = 3$, $c = 15$ y $d = 11$.

Entonces, $7 > 3$ y
$$7 = 3 + 4.$$

También, $15 > 11$ y
$$15 = 11 + 4.$$

Muchas más parejas de naturales pueden encontrarse tales que la $x$ sea el mismo número en todas las ecuaciones representadas por su pareja ordenada asociada. Entre ellas, $(5, 1)$, $(31, 27)$, $(100, 96)$, etc.

Buscamos que un número entero sea la clase de equivalencia cuyos elementos sean todas las parejas $(c, d) \in \mathbb{N}\times\mathbb{N}$, para las que una misma $x \in \mathbb{N}$ resuelva $c = d+x$. De ellas se eligirá un representante $(a, b)$ que dará nombre a cada clase, pero más importante es distinguir que todo elemento de cada clase refiere a un mismo número entero.

La siguiente proposición nos permite describir quiénes son todas las parejas $(c, d) \in \mathbb{N} \times \mathbb{N}$ que pertenecen a una misma clase:

**Proposición.** Sean $(a, b) \in \mathbb{N} \times \mathbb{N}$ y $(c, d) \in \mathbb{N} \times \mathbb{N}$. $a = b+x$ y $c = d+x$ tienen la misma solución si y sólo si $a + d = b + c$.

*Dem.-*

$\Longrightarrow$) Tenemos que

$$\begin{aligned} a &= b + x \\ d + x &= c \end{aligned}$$

Sumando, obtenemos
$$a + (d + x) = (b + x) + c.$$

Así,

$$\begin{aligned} a + (d + x) &= (b + x) + c \\ (a + d) + x &= b + x + c \\ (a + d) + x &= b + c + x \\ (a + d) &= (b + c) \\ (a + d) + 0 &= (b + c) + 0 \\ a + d &= b + c, \end{aligned}$$

operaciones correspondientes a la asociatividad, conmutatividad, ley de la cancelación en $\mathbb{N}$ y existencia del neutro aditivo en $\mathbb{N}$.

$\Longleftarrow$) Sea $k \in \mathbb{N}$ solución de $a = b + x$. Es decir, $a = b + k$.

Entonces,

$$\begin{aligned} a + d &= (b + k) + d \\ &= b + (k + d) \\ &= b + c. \end{aligned}$$

Así,

$$\begin{aligned}0+(k+d) &= (b-b)+(k+d)\\ &= (b-b)+c\\ &= 0+c\end{aligned}$$

Por lo tanto,

$$c = d+k.$$

Se ha demostrado que $k$ también es solución de $c = d+x$.

$\square$

La proposición anterior nos permite definir, para $w, z \in \mathbb{N}^2$ tales que $w = (a,b)$ y $z = (c,d)$, a la relación

$$w \sim z \text{ si y sólo si } a+d = b+c, \tag{2}$$

que ahora demostraremos, es de equivalencia.

**Proposición.** (2) es una relación de equivalencia.

*Dem.-*

1. Veamos que, para toda $w \in \mathbb{N}^2$, $w \sim w$: Sea $w = (a,b)$. Por la conmutatividad en $\mathbb{N}$, $a+b = b+a$. Así, $(a,b) \sim (a,b)$.
2. Veamos que, para cualquier $w, z \in \mathbb{N}^2$, si $w \sim z$, entonces $z \sim w$: Sean $w = (a,b)$ y $z = (c,d)$. Ya que $w \sim z$, entonces $a+d = b+c$. Nuevamente por la conmutatividad de $\mathbb{N}$, se desprende que $c+b = d+a$. De donde $z \sim w$.
3. Veamos que, para cualquier $w, w', z \in \mathbb{N}^2$ tales que $w \sim w'$ y $w' \sim z$, se obtiene que $w \sim z$: Sean $w = (a,b)$, $w' = (a',b')$ y $z = (c,d)$. $a+b' = b+a'$, pues $w \sim w'$. También, $a'+d = b'+c$, pues $w' \sim z$. Y sumando

$$\begin{aligned}a+b' &= b+a'\\ a'+d &= b'+c,\end{aligned}$$

se obtiene

$$a+d+(b'+a) = b+c+(b'+a').$$

De donde

$$\begin{aligned}a+d+(b'+a)-(b'+a) &= b+c+(b'+a')-(b'+a)\\ a+d+0 &= b+c+0\\ a+d &= b+c.\end{aligned}$$

De la última igualdad se deduce que $w \sim z$.

$\square$

Con sólo estas dos proposiciones ya debería quedar más claro de dónde sale la noción formal de número entero que es:

**Definición.** Un número entero es una clase de equivalencia $[(a,b)]_\sim$ definida por

$$[(a,b)]_\sim := \Big\{(c,d) \in \mathbb{N}^2 : a+d = b+c\Big\}. \tag{3}$$

## 3. El conjunto de los números enteros y su suma

Obviamente, en (1), la $x$ puede tomar cualquier valor $k \in \{1, \dots, n\}$, por lo que habrán infinitas clases como (3), y distintas.

Más aún, ya que la relación es de equivalencia y una relación de equivalencia induce una partición (resultado que se demostró en Álgebra Superior I), determinamos que existe una colección que tiene todas las clases del tipo (3), y donde ellas particionan tal conjunto, al cual se le llamará $\mathbb{Z}$.

**Definición.** Para $(a, b) \in \mathbb{N}^2$, el conjunto de los números enteros será la colección de todas las clases de equivalencia arriba mencionadas;

$$\mathbb{Z}/\sim := \Big\{ [(a,b)]_\sim : (a,b) \in \mathbb{N} \times \mathbb{N} \Big\}. \tag{4}$$

De ahora en adelante, abreviaremos la notación de clase de equivalencia por $[(a, b)]$ (sin la tilde), para facilitar las demostraciones. Otra notación usada comúnmente en la literatura es $\overline{(a, b)}$.

Ahora definimos la suma de dos enteros, como sigue:

**Definición.** La suma en los enteros es la función $\widehat{+} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que

$$[(a,b)] \ \widehat{+} \ [(c,d)] = [(a+c, b+d)].$$

La suma arriba dada indica que,

para $a = b + x$ y $c = d + y$, sumar ambas ecuaciones corresponde a sumar enteros:

$$a + c = (b + d) + (x + y) \equiv [(a + c, b + d))].$$

A continuación mostramos que la suma de dos enteros es la misma, sin importar quién sea el representante elegido para cada clase:

**Proposición.** La suma en los enteros está bien definida.

*Dem.-* Sean $w, w', z, z' \in \mathbb{Z}$ tales que $w \sim w'$ y $z \sim z'$. En otras palabras, $w = (a, b)$ y $w' = (f, g)$ pertenecen a la misma clase de equivalencia. Asímismo, $z = (c, d)$ y $z' = (h, i)$ pertenecen a una misma clase de equivalencia.

Queremos demostrar que $w + z = w' + z'$. O lo que es mismo, queremos ver que:

$$[(a,b)] \ \widehat{+} \ [(c,d)] = [(a+c, b+d)] = [(f+h, g+i)] = [(f,g)] \ \widehat{+} \ [(h,i)]$$

Ya que $w \sim w'$, entonces $a + g = b + f$.

Ya que $z \sim z'$, entonces $c + i = d + h$.

Sumando las ecuaciones, obtenemos que

$$(a + c) + (g + i) = (b + d) + (f + h),$$

lo que significa que, como se quería, $(a + c, b + d) \sim (f + h, g + i)$. Es decir, pertenecen a la misma clase de equivalencia. Por lo tanto, $[(a + c, b + d)] = [(f + h, g + i)]$.

$\square$

## 4. $\mathbb{Z}$ es un dominio entero

Informalmente -desde la escuela primaria-, ya sabíamos que los enteros operan bajo ciertas reglas de suma y multiplicación de sus elementos, y que antes eran tomadas como axiomas; no teníamos que demostrarlas para poder usarlas. Éstas son:

- $r \ \widehat{+} \ s = s \ \widehat{+} \ r \quad \forall \ r, s \in \mathbb{Z}$ (conmutatividad de la suma),
- $(r \ \widehat{+} \ s) \ \widehat{+} \ t = r \ \widehat{+} \ (s \ \widehat{+} \ t) \quad \forall \ r, s, t \in \mathbb{Z}$ (asociatividad de la suma),
- $\exists 0 \in \mathbb{Z}$ tal que $r \ \widehat{+} \ 0 = r \quad \forall \ r \in \mathbb{Z}$ (existencia del neutro aditivo),
- $r \ \widehat{+} \ (-r) = 0 \quad \forall \ r \in \mathbb{Z}$ (existencia del inverso aditivo),
- $r \star s = s \star r \quad \forall \ r, s \in \mathbb{Z}$ (conmutatividad del producto),
- $(r \star s) \star t = r \star (s \star t) \quad \forall \ r, s, t \in \mathbb{Z}$ (asociatividad del producto),
- $\exists 1 \in \mathbb{Z}$ tal que $r \star 1 = r \quad \forall \ r \in \mathbb{Z}$ (existencia del neutro multiplicativo),
- $r \star (s \ \widehat{+} \ t) = (r \star s) \ \widehat{+} \ (r \star t) \quad \forall r, s, t \in \mathbb{Z}$ (ley distributiva 1)
- $(s \ \widehat{+} \ t) \star r = (s \star r) \ \widehat{+} \ (t \star r) \quad \forall r, s, t \in \mathbb{Z}$ (ley distributiva 2).

Se te deja como ejercicio a tí lector, demostrar la conmutatividad, asociatividad, existencia del neutro aditivo y del inverso aditivo en $\mathbb{Z}$. Es muy fácil hacerlo; simplemente hay que utilizar la definición de entero y de suma en los enteros.

Es decir, lo que en la lista ha tomado el nombre de $r, s,$ o $t$, son cada uno, *clases de equivalencia*. Así, se pudieran especificar $r = [(a, b)]$, $s = [(c, d)]$ y $t = [(e, f)]$ y partir de ello para traducir las propiedades respectivas de la suma a su expresión más formal. Luego demostrarlas usando las definiciones que ya dimos.

Poner un acento circunflejo sobre el signo de suma y usar el símbolo $\star$ en el caso del producto es simplemente una notación que sirve para diferenciar la suma y producto de números naturales (ya elegimos que fueran $+$ y $\cdot$ respectivamente). La notación no debería causar miedo alguno; puede pensarse como la suma y producto a la que ya estamos acostumbrados para sumar y multiplicar enteros.

Para las siguientes entradas, los símbolos se simplificarán; esto con la finalidad de facilitar la escritura (y lectura), pero siempre hay que saber diferenciar en dónde y respecto a quién se están efectuando las operaciones.

Podemos adelantar que los enteros dotados con la operación suma, y denotados por $(\mathbb{Z}, \widehat{+})$, es un **grupo abeliano**. Esta estructura algebraica es muy importante irla conociendo, y basta probar todas las propiedades de la suma en los enteros, para que también hayas demostrado que $(\mathbb{Z}, \widehat{+})$ es un grupo abeliano.

Añadiendo una operación más a $\mathbb{Z}$ (en este caso, el producto en $\mathbb{Z}$) y con la que se cumplan el resto de las propiedades de la lista, podemos decir que $(\mathbb{Z}, \widehat{+}, *)$ es un **anillo conmutativo con unitario** (refiriéndose al neutro multiplicativo). No daré la definición de anillo conmutativo con unitario en esta entrada; más bien pretendo hacer ver que $(\mathbb{Z}, \widehat{+}, *)$, con su suma y producto, forman un caso particular de esa definición. En alguna próxima publicación, se verá el producto en $\mathbb{Z}$ y una vez que se sepa cómo está definido éste, se podrán demostrar el resto de las propiedades de la lista. Una vez que demuestres todas las propiedades, también habrás mostrado que $(\mathbb{Z}, \widehat{+}, *)$ es un anillo conmutativo con unitario. E invito al lector entusiasta a investigar por su cuenta las definiciones formales de grupo abeliano, y anillo conmutativo con unitario.

Finalicemos este texto proporcionando dos últimas definiciones:

**Definición.** Sea $A$ un anillo, y sean $m, n \neq 0_A$, que además satisfacen que

$$m \cdot n = 0_A.$$

Entonces a $m$ y $n$ se les llama **divisores de cero**; donde $m$ es el *divisor izquierdo de cero* y $n$ es el *divisor derecho de cero*. $0_A$ se refiere al elemento 0 del anillo.

**Definición.** Un **dominio entero** es un anillo conmutativo con unitario sin divisores de cero.

¿El conjunto de los enteros tiene divisores de cero? No. Esto quiere decir que $\mathbb{Z}$ es un dominio entero.

¿Puedes dar un ejemplo de un anillo $(A, +, \star)$, conmutativo y con unitario, que sí tenga divisores de cero?

# 5. Ejercicios

1. Demuestra la conmutatividad, asociatividad, existencia del neutro aditivo y del inverso aditivo en $\mathbb{Z}$.
2. Investigar las definiciones formales de grupo, grupo abeliano, anillo, anillo conmutativo y anillo conmutativo con unitario.
3. Demuestra que $\mathbb{Z}$ es un dominio entero.
4. Da un ejemplo de un anillo $(A, +, \star)$, conmutativo y con unitario, que sí tenga divisores de cero.