SISTEMAS NUMÉRICOS

Renato A. Lewin

Cuarta Versión
Marzo de 2019

Índice general

Capítulo 1

Los Números Enteros

Los números naturales cumplen eficientemente con las funciones descritas en la sección anterior, sin embargo tienen una estructura insuficiente como para desarrollar una aritmética interesante. La principal deficiencia es que en los números naturales a veces se puede definir la resta y a veces no. Si $n \geq m$ entonces tiene sentido definir la diferencia o resta $n - m$ como aquel único natural d tal que $m + d = n$, o sea aquel número que sumado al menor nos da el mayor. En el Teorema **??** del capítulo anterior hemos probado que tal número existe. Intuitivamente, $n - m$ es lo que le falta a m para llegar a n.

Podemos pensar, siguiendo nuestras naturales intuiciones, que los enteros negativos pueden resultar de "restar" un natural mayor de uno menor. Por ejemplo, el entero negativo -5 resulta de "restar" 6 de 1, porque por analogía con la definición anterior, -5 sería el "número"que sumado al 6 nos da 1. Hemos escrito restar entre comillas porque tal operación es una intuición que no está definida en esta situación. Algo similar puede decirse de la palabra "número" aplicada a -5.

Entonces nos damos cuenta del siguiente hecho: si -5 es el "número"que sumado al 6 nos da 1, entonces también -5 es el "número" que sumado al 7 nos da 2 y -5 es el "número" que sumado al 8 nos da 3, etc.

Un caso particular importante es aquél en el que $n = m$. En este caso"lo que falta a 5 para llegar a 5" es ... ¡Nada! Denotamos 0 a este nuevo "número".

Podemos pensar que los números naturales representan de la manera obvia a cada escalón de una escalera. Si estoy en el tercer escalón y quiero llegar al quinto, entonces $5 - 3$ representa cuánto debo subir, en este caso 2. Si en cambio tengo que ir del quinto escalón al tercero, entonces lo que necesito es bajar 2 escalones. En esta metáfora "escalerística", el nivel del suelo puede ser representado por el cero. Se puede también presentar la necesidad de bajar escalones hacia el subterráneo. Podemos llamar -1 al primer escalón hacia

abajo, ya que para llegar del nivel 0, el suelo, debo bajar 1. Similarmente, -2, -3, etc., representarían los escalones siguientes hacia el subterráneo.

1.1. Los axiomas

Basados en las intuiciones anteriores, queremos contar con un conjunto que contenga a los números naturales y a todos los objetos que nuestra intuición nos dice que deben existir para extender la resta a todos los pares de números pero conservando las propiedades de la suma y el producto que, según vimos antes, tienen los números naturales. A este conjunto lo llamaremos los *números enteros* y lo denotaremos $\mathbb{Z}$.

Resumamos aquí las propiedades algebraicas de los naturales que queremos preservar y que asumiremos como axiomas.

Axiomas:

1. $(a+b)+c = a+(b+c)$
2. $a+b = b+a$
3. $(a\,b)\,c = a\,(b\,c)$
4. $a \cdot b = b \cdot a$,
5. $a \cdot 1 = a$,

   Decimos que 1 es *neutro con respecto al producto* o *neutro multiplicativo*.
6. $a\,(b+c) = a\,b + a\,c$

Considerando lo que nos sugiere la metáfora de la escalera, agregaremos dos condiciones. La primera tiene que ver con el 0 y cómo operamos con él.

El conjunto $\mathbb{Z}$ debe contener un elemento que denotamos 0 y que cumple con el siguiente axioma.

Axioma 7. En $\mathbb{Z}$ existe un elemento denotado 0, tal que para todo $\mathbf{a \in \mathbb{Z}}$, $\mathbf{a + 0 = a}$.

Decimos que 0 es *neutro con respecto a la suma* o que es un *neutro aditivo*. Nótese que por la conmutatividad de la suma, $0 + a = a + 0 = a$.

Teorema 1.1. *El 0 es el único número entero con la propiedad de ser neutro con respecto a la suma, es decir, si existiera otro entero c tal que para todo entero m, $m + c = m$. Entonces $c = 0$.*

Demostración. Supongamos que c tiene la propiedad indicada, entonces en particular la aplicamos a $m = 0$, o sea,

$$\begin{aligned} 0 &= 0 + c && \textit{propiedad de c}, \\ &= c + 0 && \textit{conmutatividad}, \\ &= c && \textit{axioma 7}. \end{aligned}$$

□

> *La demostración anterior ilustra cómo se demuestra que un objeto que tiene alguna propiedad es único. Suponemos que hay otro con la mismas características y demostramos, usando nuestra teoría, que deben ser iguales.*

Este axioma más el teorema de unicidad pueden pensarse como una definición del cero en el sentido de que, sin importar qué es, un objeto con esa propiedad queda totalmente determinado.

La segunda condición tiene que ver con los inversos aditivos y la resta.

Axioma 8. Para todo entero a existe un entero b tal que a + b = 0.

Decimos que b es *inverso de a con respecto a la suma* o que es b es un *inverso aditivo* de a. Nótese que por la conmutatividad de la suma, $b + a = a + b = 0$.

Teorema 1.2. *Para cada a, el inverso aditivo de a es único.*

Demostración. Supongamos que b y c son dos inversos aditivos de a. Entonces

$$\begin{aligned} b &= b + 0 && \textit{propiedad de } 0, \\ &= b + (a + c) && c \textit{ es inverso de } a, \\ &= (b + a) + c && \textit{asociatividad}, \\ &= 0 + c && b \textit{ es inverso de } a, \\ &= c && \textit{propiedad de } 0. \end{aligned}$$

□

Al igual que en el caso del cero, el axioma 8 más el teorema de unicidad pueden pensarse como una definición del inverso aditivo de un número, ya que queda totalmente determinado por ellos. Si cada entero tiene un único inverso aditivo, entonces puedo ponerle un nombre sin temer confundirlo con otro elemento. Para cada entero a denotaremos $-a$ a su inverso aditivo. Como los naturales están contenidos en los enteros, el inverso de 5 es -5, el de 18 es -18, etc. Surge inmediatamente la pregunta ¿y cuál es el inverso de -5?, y también, ¿cuál es el inverso de 0?

¡Cuidado! Corremos aquí el peligro de suponer que el inverso de -5 es 5, porque eso es lo que sabemos desde la escuela secundaria. Pero como hemos dicho,

queremos justificar lo que aprendimos allí. Hasta lo que sabemos aquí, el inverso de -5 es $-(-5)$. Por supuesto, $-(-5) = 5$, pero esto y otras propiedades de los inversos debemos probarlo.

Definición 1.3. Llamamos conjunto de los números enteros a

$$\mathbb{Z} = \{\cdots -4, -3, -2, -1, 0, 1, 2, 3 \cdots\}.$$

Es decir, los enteros son los números naturales, sus inversos aditivos y el cero.

Teorema 1.4. *Las siguientes afirmaciones se cumplen para todos los números enteros a, b.*

1. $-0 = 0$
2. $-(-a) = a$
3. *Si* $a + c = b + c$, *entonces* $a = b$.

   Esto es lo que hemos llamado ley de cancelación de la suma.
4. $a \cdot 0 = 0 \cdot a = 0$
5. $a(-b) = (-a)b = -(ab)$
6. $(-a)(-b) = ab$
7. $-(a + b) = (-a) + (-b)$

Demostración. 1. Tenemos por un lado que $0 + 0 = 0$ porque esa es la propiedad del cero. Por otra parte, $0 + (-0) = 0$, porque esa es la definición del inverso aditivo. Pero hay un único número con la propiedad de ser el inverso aditivo de 0, luego $0 = -0$

2. Tenemos por un lado que $(-a) + a = 0$ porque esa es la propiedad del inverso aditivo de a (y conmutatividad). Por otra parte, $0 + (-0) = 0$, porque esa es la definición del inverso aditivo. Entonces vemos $0 = 0 + (-0) = -0$.

3.

$$\begin{aligned}
a + c &= b + c && \text{es nuestra suposición} \\
(a + c) + (-c) &= (b + c) + (-c) && \text{sumamos el inverso de } c, \\
a + (c + (-c)) &= b + (c + (-c)) && \text{asociatividad} \\
a + 0 &= b + 0 && \text{propiedad de los inversos} \\
a &= b && \text{propiedad de } 0.
\end{aligned}$$

4.

$$\begin{aligned} 0 &= 0+0 && \textit{propiedad de } 0 \\ a\cdot 0 &= a\,(0+0) && \textit{multiplicamos por } a, \\ a\cdot 0 &= a\cdot 0 + a\cdot 0 && \textit{distributitividad} \\ 0 + a\cdot 0 &= a\cdot 0 + a\cdot 0 && \textit{propiedad de } 0 \\ 0 &= a\cdot 0 && \textit{cancelamos } a\cdot 0. \end{aligned}$$

5.

$$\begin{aligned} ab + a(-b) &= a(b+(-b)\,) && \textit{distributitividad} \\ &= a\cdot 0 && \textit{propiedad de los inversos}, \\ &= 0 && \textit{más arriba} \end{aligned}$$

Por lo tanto $a(-b)$ tiene la misma propiedad que define al inverso aditivo de ab, luego tiene que ser igual a él, o sea $a(-b) = -(ab)$. La otra identidad se demuestra de la misma manera o usando la conmutatividad del producto.

6.

$$\begin{aligned} -(ab) + (-a)(-b) &= (-a)\,b + (-a)(-b) && \textit{5 anterior}, \\ &= -a(b+(-b)\,) && \textit{distributitividad}, \\ &= (-a)\,0 && \textit{propiedad de los inversos}, \\ &= 0 && \textit{4 anterior}. \end{aligned}$$

O sea, $(-a)(-b)$ tiene la propiedad del único inverso aditivo de $-(ab)$, pero como vimos en 2., el inverso del inverso de un número es él mismo, luego $(-a)(-b) = ab$.

7.

$$\begin{aligned} (a+b) + ((-a)+(-b)) &= ((a+b)+(-a)) + (-b) && \textit{asociatividad}, \\ &= ((a+(-a))+b) + (-b) && \textit{asoc. y conmut.}, \\ &= (a+(-a)) + (b+(-b)) && \textit{asociatividad}, \\ &= 0+0 && \textit{prop. inversos}, \\ &= 0 && \textit{prop. del 0}. \end{aligned}$$

O sea, $(-a)+(-b)$ tiene la propiedad del único inverso aditivo de $a+b$, luego son iguales, o sea, $-(a+b) = (-a)+(-b)$. □

Desde el punto de vista del razonamiento abstracto es importante notar que en las demostraciones anteriores no hemos hecho ninguna alusión a nuestros conocimientos anteriores o intuitivos acerca de los números enteros, sean estos positivos o negativos.

¡Cuidado! Un error frecuente es suponer que $-n$ representa siempre un número negativo, no es así, sólo representa el inverso aditivo de un número. Si este es negativo, su inverso será positivo, por ejemplo, si $n = -7$, entonces $-n = 7$. En estricto rigor, no podemos hablar de números positivos o negativos, porque

no hemos dicho cuáles enteros son positivos y cuáles negativos. Estos conceptos están relacionados con el orden que no ha sido aún definido.

El teorema anterior nos dice la verdadera razón por la cual los números enteros negativos se multiplican como aprendimos en el colegio:

No puede ser de otra manera, dado que impusimos la condición de que las operaciones deben tener las mismas propiedades que los números naturales.

Una metáfora cinemática[1] A veces resulta difícil explicar por qué el producto de dos números negativos es positivo. Como vemos, esto es el resultado natural de imponer ciertas propiedades a las operaciones. Sin embargo resulta contraintuitivo y los profesores a menudo inventan metáforas para explicarlo, las que incluyen amigos, enemigos, enemigos de los enemigos, etc., pero que resultan poco convincentes.

Sin embargo hay una interpretación proveniente de la física que es muy intuitiva y quepuede servir para motivar en los alumnos. Supongamos que una persona camina de izquierda a derecha con una velocidad de 3 Km/hr. Si lo hace por dos horas habrá recorrido una distancia de $6 = 3 \cdot 2$ kilómetros hacia la derecha, lo que convencionalmente se interpreta como positivo. Pero, ¿dónde estaba hace dos horas? Estaba a 6 kilómetros a la izquierda, ¿no?, es decir a -6 kilómetros, ya que es un camino en el sentido opuesto al positivo. Debemos ponernos de acuerdo en que "hace dos horas" es lo mismo que decir que el tiempo transcurrido es -2 horas. En otras palabras, el camino recorrido sería $3 \cdot (-2) = -6$.

Pensemos ahora en otra persona que camina también a 3 Km/hr pero de derecha a izquierda. Consideramos entonces que su velocidad es negativa, es decir, -3 Km/hr. Después de dos horas, este caminante estará a 6 kilómetros hacia la izquierda, es decir, $(-3) \cdot 2 = -6$.

La pregunta interesante es, nuevamente, ¿dónde estaba hace dos horas? La respuesta es que estaba 6 kilómetros hacia la derecha, es decir, $(-3) \cdot (-2) = 6$. □

Una consecuencia importante del teorema anterior es que en nuestra definición de número entero hemos puesto exactamente el mínimo necesario. En efecto, de *1* se desprende que basta con agregar 0, y no es necesario agregar un inverso aditivo de 0, o sea -0, ya que 0 es su propio inverso aditivo. De la misma manera, de *2* se desprende que no es necesario agregar inversos aditivos de los inversos aditivos. Por último, de *4–7* se desprende que las sumas y productos de lo que hemos llamado números enteros son, a su vez, números enteros, es decir, se trata de un conjunto cerrado bajo todas las operaciones.

[1] Esta idea la he tomado de *Matemática...¿estás ahí? Episodio 3*, de Adrián Paenza. Este libro y los dos primeros "Episodios" pueden descargarse de la web.

Definimos también la *resta de dos enteros* como

$$a - b = a + (-b)\,.$$

Es importante hacer notar que, en principio, esta definición nada tiene que ver con la resta de los números naturales que definimos en el capítulo anterior. Sin embargo, el siguiente cálculo nos demuestra que no son tan distintas.

$$\begin{aligned} b + (a - b) &= b + (a + (-b)) && \textit{definición},\\ &= (b + a) + (-b) && \textit{asociatividad},\\ &= (a + b) + (-b) && \textit{conmutatividad},\\ &= a + (b + (-b)) && \textit{asociatividad},\\ &= a + 0 && \textit{propiedad del inverso},\\ &= a && \textit{propiedad del } 0. \end{aligned}$$

Obsérve que si a y b son naturales con $a > b$, entonces $a - b$ representa aquel único número que sumado a b nos da a, o sea, es "lo que falta a b para llegar a a", que es una interpretación intuitiva de la resta en los naturales.

Ejemplo 1.5. Demuestre que para todo a, b, c, $(a + c) - (b + c) = a - b$.

Demostración.

$$\begin{aligned} (a + c) - (b + c) &= (a + c) + (-(b + c)) && \textit{definición},\\ &= (a + c) + ((-b) + (-c)) && \textit{Teorema 1.4, 7},\\ &= ((a + c) + (-b)) + (-c) && \textit{asociatividad},\\ &= ((a + (-b)) + c) + (-c) && \textit{asociat. y conmut.},\\ &= (a + (-b)) + (c + (-c)) && \textit{asociat. y conmut.},\\ &= (a + (-b)) + 0 && \textit{propiedad del inverso},\\ &= (a + (-b)) && \textit{propiedad del } 0,\\ &= a - b && \textit{definición}. \end{aligned}$$

□

Esta propiedad tiene una aplicación al cálculo mental. Supongamos que debemos restar $157 - 98$. Entonces según la propiedad, sumamos 2 al minuendo y al sustraendo y restamos obteniendo la misma diferencia, o sea, $159 - 100 = 59$, ¿no es más fácil?

El Teorema 1.4 nos dice también cómo se suman y cómo se multiplican los números enteros a partir de cómo se operan los naturales y también como se opera con el 0 pero, ¿cómo se operan sus inversos?

Supongamos sin pérdida de generalidad que los naturales n y m verifican $n \leq m$. Entonces

$$\begin{aligned} (-n) + m &= m - n\\ n + (-m) &= -(m - n)\\ (-n) + (-m) &= -(n + m) \end{aligned}$$

Las operaciones del lado derecho son entre números naturales y están bien definidas. Lo que hemos hecho notar es que las sumas de enteros siempre pueden reducirse a sumas o restas de naturales. Esto nos da una justificación de la "ley de los signos" que aprendimos en el colegio.

El caso del producto es más fácil aún. Si m y n representan naturales, entonces según el Teorema 1.4, *5* y *6*,

$$\begin{aligned} (-n)\,m &= -(n\,m) \\ n\,(-m) &= -(n\,m) \\ (-n)\,(-m) &= n\,m \end{aligned}$$

De esta manera, estamos seguros de que las operaciones verifican las propiedades indicadas, asociatividad, conmutatividad y distributividad *porque* se definieron a partir de ellas.

Corolario 1.6. *Si* $a\,b = 0$*, entonces o bien* $a = 0$ *o bien* $b = 0$*.*

Demostración. Basta notar que la multiplicación de enteros distintos de cero se reduce siempre a un producto de números naturales o de sus inversos, y el producto de dos naturales no es nunca cero.

> *Hemos usado sin mencionarlo el principio de contraposición. Si* $a \neq 0$ *y* $b \neq 0$*, entonces* $a\,b \neq 0$

□

Corolario 1.7. Ley de Cancelación *Si* $a \neq 0$ *y* $a\,b = a\,c$*, entonces* $b = c$*.*

Demostración. Supongamos que

$$\begin{aligned} a\,b &= a\,c && \\ a\,b - a\,c &= a\,c - a\,c && \text{restamos } a\,c, \\ a(b-c) &= 0 && \text{distributividad e inverso}, \end{aligned}$$

luego, por el corolario anterior, como $a \neq 0$, debemos tener que $b - c = 0$, o sea, $b = c$ que es lo que queríamos.

> *Hemos usado otra regla lógica habitual. Si sabemos que una disyunción es cierta,* (o *bien* $a = 0$ *o bien* $b - c = 0$) *y además sabemos que una de ellas es falsa* ($a \neq 0$)*, entonces la otra* ($b - c = 0$) *debe ser verdadera.*

□

Para resumir, lo que hemos hecho en esta sección es definir un conjunto que:

- Contiene a los números naturales.

- Está dotado de dos operaciones, suma y resta que extienden las de los números naturales. Es decir la suma de los naturales se hace tal como se hacía antes, sólo agregamos las nuevas posibilidades.
- Estas operaciones tienen las mismas propiedades que aquellas de los números naturales.
- En este conjunto la resta está definida para todo par de elementos y tiene el mismo significado intuitivo que en los números naturales.
- Contiene un elemento que actúa como neutro para la suma.
- Basados sólo en los axiomas 1 a 8, hay muchos conjuntos posibles con las propiedades anteriores, sin embargo es intuitivamente cierto que hemos incluido el mínimo necesario para obtener lo que nos propusimos, luego $\mathbb{Z}$ debe estar contenido en todo tal conjunto. Es decir, $\mathbb{Z}$ es el conjunto más pequeño que cumple con las condiciones anteriores. Esto no lo demostraremos formalmente aquí.

1.1.1. Orden

Los números enteros pueden ser ordenados de la siguiente manera.

$$a <_{\mathbb{Z}} b \quad \text{si y sólo si} \quad b - a \in \mathbb{N}.$$

Usaremos también la notación

$$a \leq_{\mathbb{Z}} b \quad \text{si y sólo si} \quad a <_{\mathbb{Z}} b \quad \text{ó} \quad a = b$$

A los números naturales les llamamos enteros positivos, a los inversos de los números naturales les llamamos enteros negativos.

Ejemplos 1.8.

1. Si m, $n \in \mathbb{N}$, entonces $m \leq_{\mathbb{Z}} n$ es lo mismo que $m \leq n$, donde este segundo orden es el de los números naturales.
2. $-9 <_{\mathbb{Z}} 3$ porque $3 - (-9) = 3 + 9 = 12 \in \mathbb{N}$. Más generalmente, si m, $n \in \mathbb{N}$, entonces $-m \leq_{\mathbb{Z}} n$, porque $n - (-m) = n + m \in \mathbb{N}$, es decir, cualquier entero negativo es menor que cualquier entero positivo.
3. El 0 no es positivo ni negativo. Es fácil ver que para cualquier entero positivo n, $0 <_{\mathbb{Z}} n$ y que para cualquier entero negativo m, $m <_{\mathbb{Z}} 0$, en otras palabras, los enteros positivos son aquellos mayores que el cero, los enteros negativos son los menores que el cero, tal como sabemos que tiene que ser.

4. Obsérvese que $a <_{\mathbb{Z}} 0$ si y sólo si $0 <_{\mathbb{Z}} -a$.

Debemos ahora demostrar que $\leq_{\mathbb{Z}}$ es un orden.

Teorema 1.9. *La relación $\leq_{\mathbb{Z}}$ es un orden total, discreto, sin primer ni último elemento.*

Demostración. La relación $\leq_{\mathbb{Z}}$ es obviamente reflexiva.

Para verificar la antisimetría usaremos el método de la contradicción. Para ello supongamos que $m \leq_{\mathbb{Z}} n$ y $n \leq_{\mathbb{Z}} m$, pero que $n \neq m$.

Esto significa que $n - m \in \mathbb{N}$ y $m - n \in \mathbb{N}$. Entonces como la suma de números naturales es un número natural,

$$(n - m) + (m - n) = (n - n) + (m - m) = 0 \in \mathbb{N}\,,$$

por la conmutatividad y asociatividad de la suma. Esto es una contradicción, por lo tanto si $m \leq_{\mathbb{Z}} n$ y $n \leq_{\mathbb{Z}} m$, entonces $n = m$.

Verificamos la transitividad. Supongamos que $n \leq_{\mathbb{Z}} m$ y $m \leq_{\mathbb{Z}} p$.

Si $n = m$ o bien $m = p$, entonces reemplazando adecuadamente, $n \leq_{\mathbb{Z}} p$. Podemos suponer que los tres números son distintos. En tal caso, tenemos $m - n \in \mathbb{N}$ y $p - m \in \mathbb{N}$. Nuevamente notamos que la suma de naturales es un natural luego

$$(m - n) + (p - m) = (m - m) + (p - n) = p - n \in \mathbb{N}\,,$$

es decir $n \leq_{\mathbb{Z}} p$, que es lo que queríamos demostrar.

Veremos ahora que el orden $\leq_{\mathbb{Z}}$ es un orden total. Sean m y n dos enteros distintos. Hay dos posibilidades, o bien $n - m$ es un natural, o bien no lo es.

Si $n - m \in \mathbb{N}$ entonces $m \leq_{\mathbb{Z}} n$. Si $n - m \notin \mathbb{N}$, entonces $n - m = -p$ para algún $p \in \mathbb{N}$. Pero entonces $m - n = -(n - m) = p \in \mathbb{N}$, es decir, $n \leq_{\mathbb{Z}} m$. En resumen se cumple una (y sólo una) de las siguientes:

$$m <_{\mathbb{Z}} n\ ,\ \text{o bien}\ \ m = n\ ,\ \text{o bien}\ \ n <_{\mathbb{Z}} m\,,$$

es decir el orden es total.

El orden $\leq_{\mathbb{Z}}$ es discreto porque dado cualquier entero $n \in \mathbb{Z}$, su sucesor inmediato es $n+1$. En efecto, si existiera m tal que $n <_{\mathbb{Z}} m <_{\mathbb{Z}} n+1$, entonces sumando $-n + 1$

$$1 = n - n + 1 <_{\mathbb{Z}} m - n + 1 <_{\mathbb{Z}} (n + 1) - n + 1 = 2\,,$$

y tendríamos que el número natural $m-n+1$ estaría entre 1 y el 2, lo que es una contradicción.

Por último, es claro que $\leq_{\mathbb{Z}}$ no tiene primer ni último elemento porque dado cualquier entero n hay uno más grande, por ejemplo $n+1$ y también uno más chico, por ejemplo, $n-1$. □

1.2. La División

Si bien la división tiene sentido para los números naturales, hemos postergado su estudio hasta aquí debido a que la mayoría de los resultados sobre divisibilidad se expresan mejor cuando contamos con toda la potencia de los números enteros, en particular, de la resta como operación no restringida a ciertos casos particulares.

1.2.1. Divisibilidad

Definición 1.10. Sean a y b dos enteros con $a \neq 0$. Decimos que a *divide* a b si existe un entero n tal que $na = b$. También decimos que b es un *múltiplo* de a. Denotamos este hecho por $a \mid b$. Si a no divide a b escribiremos $a \nmid b$.

Para cualquier entero a, su valor absoluto se define como

$$|a| = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

Teorema 1.11. *Si a, b y c son enteros, entonces:*

1. *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
2. *Si $a \mid b$ y $a \mid c$, entonces $a \mid mb + nc$, para cualquier par de enteros m, n.*
3. *Si $a \mid b$ y $b \neq 0$, entonces $0 < |a| \leq |b|$.*
4. *Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.*

Demostración. 1. $b = ma$ y $c = nb$, luego $c = n(ma) = (nm)a$, es decir $a|c$.

2. $b = pa$ y $c = qa$, luego $mb + nc = m(pa) + m(qa) = (mp + nq)a$, es decir $a|mb + nc$.

3. $b = ma \neq 0$, luego $a \neq 0$ y $m \neq 0$. Por lo tanto, $|a| \geq 1, |m| \geq 1$ y $|b| = |ma| = |m||a| \geq 1\,|a| = |a| \geq 1 > 0$.

4. Como $a \mid b$, por (3), $0 < |a| \leq |b|$. Análogamente, $0 < |b| \leq |a|$. Luego $|a| = |b|$ y por lo tanto $a = \pm b$. □

El siguiente teorema es el más importante sobre divisibilidad. Préstese especial atención a su demostración porque es interesante en sí misma como método de demostración.

Teorema 1.12. El Algoritmo de la División.
Sean a y b dos enteros, $b > 0$. Entonces existen dos enteros q y r tales que $a = bq + r$ y $0 \leq r < b$. Los enteros q y r son únicos.

Demostración. Si $a = 0$ el teorema se cumple trivialmente con $q = r = 0$. Este es un caso particular de aquel en el que a es un múltiplo de b, o sea, $a = bq + 0$ y el teorema se cumple. Obsérvese que en este caso $r = 0$.

Podemos entonces suponer que a no es un múltiplo de b. Consideremos el conjunto

$$A = \{a - bn : n \in \mathbb{Z} \text{ y } a - bn \geq 0\}.$$

Vemos que $0 \notin A$ ya que a no es un múltiplo de b. También es inmediato ver que A es un conjunto no vacío de enteros positivos, porque si $a > 0$, entonces $a - b \cdot 0 = a \in A$. Por otra parte, si $a < 0$, entonces $a - 2\,b\,a = a(1 - 2\,b) > 0$, porque tanto a como $1 - 2\,b$ son números negativos, luego $-a \in A$.

Por el principio de Buen Orden, A debe tener un menor elemento. Llamémoslo r. Como $r \in A$ debe existir un entero q tal que $r = a - bq$, i.e., $a = bq + r$.

Supongamos que $r \geq b$. Entonces $r - b = a - bq - b = a - b(q + 1) \geq 0$, luego $r - b \in A$, pero $0 \leq r - b < r$, contradiciendo la minimalidad de r. Por lo tanto $0 \leq r < b$. (Como vimos arriba, $r = 0$ si y sólo si a es un múltiplo de b).

Finalmente, para probar la unicidad de q y r, supongamos que q' y r' son números tales que $a = bq' + r'$ y $0 \leq r' < b$. Entonces $bq + r = bq' + r'$, luego $b(q - q') = r' - r$, o sea, $b \mid (r' - r)$. Si $r \neq r'$, por Teorema 1.11 (*3*), $|r' - r| \geq |b| = b > 0$. Pero esto es imposible ya que $-b < r' - r < b$. Luego $r = r'$. Pero entonces $b(q - q') = 0$ y como $b \neq 0$, tenemos $q = q'$.

Por inducción: Haremos inducción sobre a.
(*i*) Si $a = 1$, entonces, como $1 \leq_{\mathbb{Z}} b$ tenemos dos casos.
Si $b = 1$, entonces $b \cdot 1 + 0 = 1 = a$, es decir $q = 1$ y $r = 0$.
Si $1 <_{\mathbb{Z}} b$, entonces $a = 1 = d \cdot 0 + 1$, es decir, $q = 0$ y $r = 1$.
En ambos casos los números q y r son únicos y r verifica que $0 \leq_{\mathbb{Z}} r <_{\mathbb{Z}} b$.
(*ii*) Supongamos que la condición se verifica para a. Entonces existen q y r con $0 \leq_{\mathbb{Z}} r <_{\mathbb{Z}} b$, tales que

$$a + 1 = (bq + r) + 1 = bq + (r + 1)\,.$$

Nuevamente tenemos dos casos.

Si $r+1 <_{\mathbb{Z}} b$, entonces hacemos $q' = q$ y $r' = r+1$.
Si $r+1 = b$, entonces factorizando por b, hacemos $q' = q+1$ y $r' = 0$.
En cualquiera de los dos casos q' y r' verifican la propiedad.

□

Ejemplos 1.13.

1. Demuestre que si a y b son impares entonces a^2+b^2 es par pero no es divisible por 4.

   Como a es impar, $a = 2k+1$ para cierto k igualmente $b = 2j+1$ entonces $a^2+b^2 = (2k+1)^2+(2j+1)^2 = 4k^2+4k+1+4j^2+4j+1 = 4(k^2+j^2+k+j)+2$ es par, pero al dividirse por 4 deja resto 2, luego a^2+b^2 no es divisible por 4.

2. Dado cualquier entero n, n^3-n es divisible por 6.

   Observemos que $N = n^3-n = (n-1)\,n\,(n+1)$, es decir, el producto de tres números consecutivos. Resolveremos este problema haciendo un uso típico del teorema de la división (hay otras soluciones más elegantes). Por el axioma de la división n debe ser de la forma $n = 6k+r$ con $r \in \{0,1,2,3,4,5\}$. Es cosa de analizar los seis casos.

   Si $n = 6k$, entonces $N = (6k-1)6k(6k+1)$ es obviamente múltiplo de 6.

   Si $n = 6k+1$, entonces $N = 6k(6k+1)(6k+2)$ es también obviamente múltiplo de 6.

   Si $n = 6k+2$, entonces $N = (6k+1)(6k+2)(6k+3) = 6(6k+1)(3k+1)(2k+1)$ es múltiplo de 6.

   Si $n = 6k+3$, entonces $N = (6k+2)(6k+3)(6k+4) = 6(3k+1)(2k+1)(6k+4)$ es múltiplo de 6.

   Si $n = 6k+4$, entonces $N = (6k+3)(6k+4)(6k+5) = 6(2k+1)(2k+2)(6k+5)$ es múltiplo de 6.

   Si $n = 6k+5$, entonces $N = (6k+4)(6k+5)(6k+6) = 6(6k+4)(6k+5)(k+1)$ es múltiplo de 6.

Definición 1.14.

1. Un entero positivo $p \neq 1$ se dice *primo* si sus únicos divisores son ± 1 y $\pm p$.

2. Sean a, b dos enteros no ambos nulos. El mayor entero que divide tanto a a como a b se llama el *máximo común divisor* de a y b. El máximo

común divisor de a y b se denota $MCD\{a, b\}$. (En muchos libros el máximo común divisor se denota (a, b)).

Similarmente definimos $MCD\{a_1, a_2, \ldots, a_n\}$, el máximo común divisor de

$a_1, a_2, \ldots, a_n$, como el mayor entero que divide a todos esos números.

3. Dos enteros se dicen *primos relativos* si su máximo común divisor es 1.

A priori no es obvio que el máximo común divisor de dos números deba existir, sin embargo esto es consecuencia inmediata del próximo teorema.

Teorema 1.15. *Dados dos enteros a y b no ambos nulos, su máximo común divisor $MCD\{a, b\}$ es el menor entero positivo que se puede escribir como suma de multiplos de a y de b.*

Demostración. Supongamos sin pérdida de generalidad que $a \neq 0$ y consideremos el conjunto $A = \{ma + nb : m, n \in \mathbb{Z} \text{ y } ma + nb > 0\}$. A no es vacío ya que $0 < |a| = \pm 1 \cdot a + 0 \cdot b \in A$. Veremos ahora dos demostraciones de que este conjunto tiene un menor elemento.

Demostración usando el Principio del Buen Orden

Por el Principio de Buen Orden, A tiene un menor elemento, al que llamaremos d. Como $d \in A$, $d > 0$ y existen enteros m, n tales que $d = ma + nb$.

Demostración usando el Principio de Inducción

Supongamos que no existe el menor entero positivo que es combinación de a y de b, es decir el conjunto A del párrafo anterior no tiene menor elemento. Consideremos la propiedad

$$P(n) : 1 \notin A, 2 \notin A, \ldots, n \notin A\,.$$

(i) Es claro que $P(1)$ es cierta porque, si $1 \in A$, 1 tendría que ser el menor elemento de A.
(ii) Para el paso de inducción, supongamos que $1 \notin A, 2 \notin A, \ldots, n \notin A$. Entonces es inmediato que $n + 1 \notin A$, de lo contrario, $n + 1$ sería el menor elemento de A, contradiciendo nuestra hipótesis.

Por el Principio de inducción, todos los naturales verifican la propiedad P. Pero esto quiere decir que A es vacío, lo que como vimos, no es así. Por lo tanto debe existir d que es combinación de a y b.

Ahora veremos que éste es el máximo común divisor de a y b. Primero veamos que efectivamente d es un divisor de ambos números.

Por el algoritmo de la división, $a = qd + r$, con $0 \leq r < d$. Entonces,

$$r = a - qd = a - q(ma + nb) = (1 - mq)a - nqb.$$

Si $r > 0$, entonces $r \in A$, pero $r < d$, lo que contradice la minimalidad de d. Por lo tanto $r = 0$ y $d \mid a$.

Análogamente podemos demostrar que $d \mid b$, por lo tanto d es un divisor común de a y de b.

Para verificar que d es el mayor divisor común, sea $s \geq 1$ otro divisor común. Por el Teorema 1.11.*2*, $s \mid ma + nb$, para cualquier $m, n \in \mathbb{Z}$, en particular, $s \mid d$, luego por 1.11.*3*, $0 < s \leq d$.

□

La propiedad anterior se puede extender a cualquier cantidad finita de números.

Corolario 1.16. *El máximo común divisor de $a_1, a_2, \ldots, a_n$ es el menor entero positivo que puede escribirse como suma de múltiplos de los números $a_1, a_2, \ldots, a_n$.*

Observación 1.17.

1. a y b son relativamente primos si y sólo si existen $m, n \in \mathbb{Z}$ tales que $1 = ma + nb$.

2. El máximo común divisor de $a_1, a_2, \ldots, a_n$ divide a $a_1, a_2, \ldots, a_n$. Si $s \mid a_1$, $s \mid a_2, \ldots, s \mid a_n$, entonces $s \mid MCD\{a_1, a_2, \ldots, a_n\}$.

Corolario 1.18. *Si $d = MCD\{a, b\}$, entonces $MCD\{\frac{a}{d}, \frac{b}{d}\} = 1$. (I.e. $\frac{a}{d}$ y $\frac{b}{d}$ son relativamente primos. ¡Obsérvese que ($\frac{a}{d}$ y $\frac{b}{d}$) son enteros!).*

El siguiente es un importante teorema, a veces conocido como Lema de Euclides. Responde parcialmente la pregunta: Si un número divide a un producto, ¿debe dividir a alguno de sus factores? En general no, por ejemplo, $6 \mid 12 = 3 \cdot 4$, sin embargo $6 \nmid 3$ y $6 \nmid 4$.

Teorema 1.19. *Si p es un número primo y $p \mid bc$, entonces $p \mid b$ ó $p \mid c$.*

Esto se puede generalizar fácilmente por inducción a:

Corolario 1.20. *Si p es un número primo y $p \mid a_1 a_2 \cdots a_n$, entonces $p \mid a_k$, para algún $k \leq n$.*

El Teorema 1.19 es un caso particular del próximo teorema que responde la pregunta anterior en forma más general.

Corolario 1.21. *Si $MCD\{a, b\} = 1$ y $a \mid bc$, entonces $a \mid c$.*

Demostración. Si $a \mid bc$, entonces $bc = ak$ para algún k, y como $1 = ma + nb$, multiplicando ambos miembros por c,

$$c = mac + nbc = mac + nak = a(mc + nk).$$

□

El siguiente ejemplo es un pequeño lema que usaremos en el próximo apartado. Ilustra cómo se usa la descomposición del máximo común divisor de dos números como combinación de ellos.

Ejemplo 1.22. Si $a = bq + r$ y $b \neq 0$, entonces $MCD\{a, b) = MCD\{b, r)$.

Demostración. $MCD\{a, b\} = ma + nb = m(bq + r) + nb = (mq + n)b + mr$, es decir, $MCD\{a, b\}$ es una suma de múltiplos de b y de r, luego por el teorema 1.15, $MCD\{a, b\} \mid MCD\{b, r\}$.

De una manera similar demostramos que $MCD\{b, r\} \mid MCD\{a, b\}$. □

1.2.2. El Algoritmo de Euclides

Existe un método para calcular el máximo común divisor de dos números, tal método se denomina el *Algoritmo de Euclides*.

Sean a y b dos números no ambos nulos, digamos, $b > 0$. Entonces, por el algoritmo de la división, existen q y r tales que $a = bq + r$, con $0 \leq r < b$.

Si $r = 0$, entonces $b \mid a$, $MCD\{a, b\} = b$ y hemos terminado.

Si $r > 0$, entonces existen q_1 y r_1 tales que $b = rq_1 + r_1$, con $0 \leq r_1 < r$.

Si $r_1 = 0$, entonces $MCD\{b, r\} = r$ y por el lema que demostramos en el Ejemplo 1.22, $MCD\{a, b\} = r$ y nuevamente hemos terminado.

Si $r_1 > 0$, entonces existen q_2 y r_2 tales que $r = r_1q_2 + r_2$ y $0 \leq r_2 < r_1$.

Este proceso se puede continuar indefinidamente de tal manera que en cada paso, si obtenemos un resto cero, nos detenemos y si no, aplicamos el algoritmo de la división una vez más. Es importante notar que en cada aplicación del algoritmo de la división, el resto obtenido es estrictamente menor que el de la aplicación precedente. Vale decir, tenemos $r > r_1 > r_2 > \cdots > r_n > \cdots \geq 0$.

Pero tiene que existir un n tal que $r_n = 0$, ya que si no, habría una cadena descendente infinita de números naturales, lo que contradice el Principio de Buen Orden. Pero si $r_n = 0$, $r_{n-1} \mid r_{n-2}$ en cuyo caso $MCD\{r_{n-2}, r_{n-1}\} = r_{n-1}$ y aplicando el Corolario 1.22 varias veces,

$$MCD\{a, b\} = MCD\{r, r_1\} = MCD\{r_1, r_2\} = \cdots = MCD\{r_{n-2}, r_{n-1}\} = r_{n-1}.$$

Vale decir, el máximo común divisor de a y de b es el resto inmediatamente anterior al resto que se anula.

Ejemplo 1.23. Calculemos el máximo común divisor de 454 y 136.

$$\begin{aligned} 454 &= 136 \cdot 3 + 46 \\ 136 &= 46 \cdot 2 + 44 \\ 46 &= 44 \cdot 1 + 2 \\ 44 &= 2 \cdot 22 + 0 \end{aligned}$$

Es decir, el máximo común divisor de 454 y 136 es 2.

Para calcular el máximo común divisor de tres o más números, aplicamos el Corolario **??** y el algoritmo de Euclides.

Definición 1.24. El *mínimo común múltiplo* de dos enteros no nulos a y b es el menor entero positivo que es múltiplo de a y de b. Se le denotará por $mcm\{a, b\}$). (Algunos libros usan la notación $[a, b]$).

Como en el caso del máximo común divisor, el mínimo común múltiplo de dos números siempre existe. En este caso, en virtud del Principio de Buen Orden.

Teorema 1.25. *Si m es un múltiplo común de a y de b, entonces $mcm\{a, b\} \mid m$.*

Demostración. Por el algoritmo de la división, $m = mcm\{a, b\}\, q + r$, con $0 \leq r < mcm\{a, b\}$. Pero $a \mid m$ y $a \mid mcm\{a, b\}$, luego $a \mid r = m - mcm\{a, b\}\, q$.

Similarmente, $b \mid r$, o sea, r es un múltiplo común de a y de b. Si $r > 0$, entonces $mcm\{a, b\}$ no sería el mínimo común múltiplo de a y de b. Por lo tanto $r = 0$ y $mcm\{a, b\} \mid m$. □

Teorema 1.26. *Si a y b son enteros no nulos,*

$$mcm\{a, b\} = \frac{|ab|}{MCD\{a, b\}}.$$

Demostración. Sean $d = MCD\{a, b\}$ y $m = mcm\{a, b\}$. Entonces

$$\frac{|ab|}{d} = \frac{|a|}{d}|b| = |a|\frac{|b|}{d}\,.$$

Pero $\frac{|a|}{d}$ y $\frac{|b|}{d}$ son enteros, luego $\frac{|ab|}{d}$ es un múltiplo de a y de b, luego $m \mid \frac{|ab|}{MCD\{a,b\}}$.

Por otra parte, $|ab|$ es un múltiplo común de a y b, luego $m \mid |ab|$ y, en particular, $\frac{|ab|}{m}$ es un entero.

Ahora bien, $m = ka$, luego

$$k\frac{|ab|}{m} = \frac{k|a|}{m}|b| = \pm b,$$

o sea,

$$\frac{|ab|}{m} \mid b.$$

Análogamente, $\frac{|ab|}{m} \mid a$. Es decir, $\frac{|ab|}{m}$ es divisor común de a y de b, luego $\frac{|ab|}{m} \mid d$ y por el Teorema 1.11,*3*, $\frac{|ab|}{m} \leq d$. Por lo tanto $\frac{|ab|}{d} = m$. □

El siguiente teorema conocido también como teorema de factorización única, es la piedra angular de toda la teoría de números.

Teorema 1.27. El Teorema Fundamental de la Aritmética.
Todo número entero mayor que 1 *o bien es un número primo o bien se puede factorizar como producto de números primos. Más aún, tal factorización es única salvo por el orden de los factores.*

Demostración. Supongamos que el teorema no es cierto, es decir, existe un entero positivo mayor que 1 que no es primo y que no se descompone como producto de primos. Sea n el más pequeño tal número. Este debe existir por el Principio de Buen Orden.

Como n no es primo, debe tener divisores no triviales. Sea $n = ab$, donde a y b son distintos de ± 1 y de $\pm n$. Sin pérdida de generalidad podemos suponer que a y b son positivos. Además sabemos que $a < n$ y $b < n$. Pero entonces, como n es minimal para la propiedad indicada, tanto a como b son o bien primos, o bien producto de primos y por lo tanto, en cualquier caso, n es producto de números primos, contradiciendo la suposición original. Luego ésta es falsa.

Para demostrar la unicidad de la descomposición, supongamos que existen enteros que tienen más de una descomposición. Sea n ahora el menor entero positivo tal que la factorización no es única. Es decir,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ son números primos. Entonces $p_1 | q_1 q_2 \cdots q_s$ y por el Corolario 1.20, para algún j, $1 \leq j \leq s$, $p_1 | q_j$. Pero como ambos son primos, $p_1 = q_j$. Podemos suponer (reordenando) que $j = 1$, luego

$$n' = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s,$$

pero $n' < n$, luego n' verifica la condición de unicidad de la factorización, por lo tanto $r = s$ y reordenando, $p_i = q_i$, para $1 \leq i \leq r$, por lo tanto la descomposición de n es única. □

Observación 1.28. Obviamente no todos los primos que aparecen en la descomposición de un número tienen que ser distintos. En general todo entero $n > 1$ se puede escribir como

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m},$$

donde los p_k son primos, los k_i son enteros positivos. El número k_i suele llamarse la *multiplicidad* de p_i en la descomposición de n.

Este teorema tiene muchas aplicaciones, la más elemental es probablemente el algoritmo para calcular máximo común divisor y mínimo común múltiplo de dos o más números:

El máximo común divisor de dos números es el producto de todos los primos (considerando su multiplicidad) que se repiten en la factorización de ambos números.

El mínimo común múltiplo de dos números es el producto de las máximas potencias de cada primo que aparece en la descomposición de alguno de los números.

Ejemplo 1.29. Calcular el máximo común divisor y el mínimo común múltiplo de 48 y 180.

Como $48 = 2^4 \cdot 3$ y $180 = 2^2 \cdot 3^2 \cdot 5$,

$$(48, 180) = 2^2 \cdot 3 = 12 \text{ y } [48, 180] = 2^4 \cdot 3^2 \cdot 5 = 720.$$

Este algoritmo puede generalizarse a cualquier cantidad de números.

Podemos dar una fórmula general para calcular el máximo común divisor y el mínimo común múltiplo de dos números basada en la descomposición en números primos. Consideremos las descomposiciones

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{y} \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

de los números n y m, donde $0 \leq \alpha_i$ y $0 \leq \beta_i$, para $1 \leq i \leq k$, en las que si algún primo p_i no aparece en ambas descomposiciones hacemos $\alpha_i = 0$ ó $\beta_i = 0$, según corresponda. Entonces

$$MCD\{n, m\} = p_1^{min\{\alpha_1, \beta_1\}} p_2^{min\{\alpha_2, \beta_2\}} \cdots p_k^{min\{\alpha_k, \beta_k\}},$$

$$mcm\{n, m\} = p_1^{max\{\alpha_1, \beta_1\}} p_2^{max\{\alpha_2, \beta_2\}} \cdots p_k^{max\{\alpha_k, \beta_k\}}.$$

Ejemplo 1.30. Podemos usar la descomposición en factores primos para dar una demostración de que $\sqrt{2}$ no es racional. En efecto, supongamos que $\sqrt{2} = \frac{n}{m}$, donde m y n son primos relativos. Usemos las descomposiciones

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad \text{y} \quad m = q_1^{j_1} q_2^{j_2} \cdots q_t^{j_t}.$$

Vemos que como m y n son primos relativos, los primos p_i y q_i son todos distintos. Entonces, elevando al cuadrado tendríamos

$$2\, q_1^{2j_1} q_2^{2j_2} \cdots q_t^{2j_t} = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}.$$

Si 2 aparece entre los p_i , lo cancelamos, si no aparece, nada podemos cancelar. En cualquier caso, tendríamos un número con dos descomposiciones distintas, lo que es imposible.

□

Terminamos esta sección con el siguiente corolario, uno de los más famosos y hermosos resultados de Euclides.

Corolario 1.31. *Existen infinitos números primos.*

Demostración. Supongamos que existe solamente una cantidad finita de primos p_1, p_2,..., p_n. Consideremos ahora el número

$$m = p_1 p_2 \cdots p_n + 1.$$

Obviamente m es mayor que todos los primos, luego no es primo. Por otra parte, m no es divisible por p_1, ni por p_2, ..., ni por p_n, o sea, m no es divisible por ningún primo. Pero por el teorema 1.27, m debe ser divisible por algún primo, lo cual es una contradicción, por lo tanto la lista finita debe ser incompleta. □

1.3. Ejercicios

Operatoria y orden

1. Demuestre que la distributividad en el otra dirección $(b + c) \cdot a = b \cdot a + c \cdot a$ se desprende del axioma 6.

2. Explique cómo se relacionan las operaciones de los números enteros con aquellas de los números naturales.

3. *a*) De acuerdo con las "regla de los signos", en el colegio nos enseñaron que para calcular $2 \cdot (-3)$ multiplicamos los dos números sin considerar el signo, es decir, $2 \cdot 3 = 6$, y después ponemos el signo menos delante del resultado, de modo que $2 \cdot (-3) = -6$.

   Justifique este procedimiento usando los axiomas o teoremas sobre números enteros

   b) Haga lo mismo para justificar que $2 + (-3) = -1$.

4. Demuestre las siguientes propiedades de los números enteros usando solo los axiomas.

   a) El neutro aditivo 0 es único

   b) Si $x + y = x + z$, entonces $y = z$

c) $x \cdot 0 = 0$

d) Si $x \neq 0$ e $y \neq 0$, entonces $xy \neq 0$

e) Si $xy = 0$, entonces $x = 0$ o $y = 0$

f) El inverso aditivo de un número es único

g) $-0 = 0$

h) $-(-x) = x$

i) $-(x + y) = -x - y$

j) $-(x - y) = y - x$

k) Si $xy = xz$ y $x \neq 0$, entonces $y = z$.

l) El cero no tiene inverso multiplicativo

m) $(-1)(-1) = 1$

n) $(-1)x = -x$

ñ) $(-x)(-y) = xy$

o) $-(xy) = (-x)y = x(-y)$

5. Demuestre usando los axiomas y los teoremas demostrados que para cualesquiera números enteros m, n y p

   a) $(m + n)^2 = (m^2 + 2m \cdot n) + n^2$

   b) $(m + n)(m - n) = m^2 - n^2$

   c) $(m + n)(p + m) = (m^2 + m(n + p)) + n \cdot p$

   d) $(m + 1)(n + 1) = ((m \cdot n + m) + n) + 1$

   Este ejercicio no busca ver si Ud. sabe la fórmula del cuadrado del binomio, o de la suma por la diferencia de dos números, etc., eso se da por descontado. La idea es que muestre cómo se justifica cada paso algebraico a partir de los axiomas o de teoremas ya demostrados.

6. Demuestre:

   a) Cualquier número entero n, verifica $0 \leq_{\mathbb{Z}} n^2$.

   b) Para cualesquiera números enteros a y b, se verifica $2\,a \cdot b \leq_{\mathbb{Z}} a^2 + b^2$.

Divisibilidad

1. Demuestre que el mínimo común múltiplo de dos números siempre existe.

2. Demuestre que si $(a, m) = 1$ y $(b, m) = 1$, entonces $(ab, m) = 1$.

3. Demuestre o de un contraejemplo

   a) Si $a \mid a+b$, entonces $a \mid b$.

   b) Si $a^2 \mid b^2$, entonces $a \mid b$.

   Inténtelo primero sin usar el teorema de descomposición prima. Luego hágalo haciendo uso del teorema.

   c) Si $a \mid b^2$, entonces $a^2 \mid b^2$.

   d) Si $d = (a, b)$, $a \mid c$ y $b \mid c$, entonces $ab \mid dc$.

4. Demuestre los criterios de divisibilidad que aprendió en el colegio. Recordemos que si un entero se escribe en notación decimal como

$$a_n a_{n-1} \cdots a_2 a_1 a_0,$$

   a_0 es su *dígito de las unidades*, a_1 es su *dígito de las decenas*, etc.

   a) Un número es divisible por 2 si $2 \mid a_0$.

   b) Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.

   c) Un número es divisible por 4 si $4 \mid a_1 a_0$. También es divisible por 4 si $4 \mid 2a_1 + a_0$.

   d) Un número es divisible por 5 si su dígito de las unidades es 5 o 0.

   e) Un número es divisible por 6 si es divisible por 2 y por 3.

   f) Un número es divisible por 7 si

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$$

   es divisible por 7.

   g) Un número es divisible por 7 si

$$a_n a_{n-1} \ldots a_1 + 2a_0$$

   es divisible por 7.

   h) Un número es divisible por 8 si $8 \mid a_2 a_1 a_0$. También es divisible por 8 si $8 \mid 4a_2 + 2a_1 + a_0$.

   i) Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.

   j) Un número es divisible por 11 si

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$$

   es divisible por 11.

5. Invente criterios de divisibilidad para otros números mas grandes.

6. Demuestre que el cuadrado de cualquier número entero puede tener la forma $3k$ o bien $3k+1$, pero no puede tener la forma $3k+2$.

7. Demuestre que no existen enteros a y b tales que $(a,b) = 7$ y $2a+b = 50$.

8. Probar que si a y b son impares, entonces a^2+b^2 no puede ser un cuadrado perfecto.

9. Demuestre que si $(a,b) = 1$, entonces $(a+b, ab) = 1$.

1.4. APÉNDICE: La construcción de los números enteros

Como dijimos en el Prefacio, existe otra manera de entender los números, esta es, construyéndolos como objetos a partir de otros que ya se han construidos antes. Esto se puede hacer, por ejemplo, dentro de la teoría de conjuntos[2].

La construcción clásica de los enteros se atribuye a Karl Weierstrass (1815–1897], a mediados del siglo XIX, supone como punto de partida la existencia del conjunto $\mathbb{N}$ de los números naturales. La intuición detrás de esta está insinuada en la introducción de este capítulo, a partir de la noción de diferencia de dos números.

Una de las interpretaciones de las diferencia entre dos números naturales es *aquello que falta al menor para alcanzar al mayor*, de esta manera, cada número, por ejemplo el 5, es aquello que le falta al 1 para llegar a 6 pero también lo que le falta al 2 para llegar a 7, etc.

Esta idea es particularmente útil para extender la diferencia a cualquier par de números. Podemos pensar en aquel número que *le falta* al 6 para llegar al 1 como un número negativo, el número de pasos hacia la izquierda que debemos dar sobre la recta numérica para llegar del más grande al más pequeño.

Tenemos entonces que se define en forma más o menos natural una relación entre los pares ordenados de números naturales. Por ejemplo los pares $(6,1), (7,2), (8,3), \ldots (n+5, n) \ldots$ tienen algo en común, a saber, la diferencia entre la primera y la segunda componente es 5.

Esto tiene sentido solo si la primera componente del par es mayor que la segunda, pero como indicamos más arriba, podemos extender esta idea al caso en que ocurre lo opuesto o en el que ambas componentes son iguales. De esta manera, los pares $(3,6), (8,11), (17,20) \ldots (n, n+3) \ldots$ comparten que la

[2]Para un tratamiento detallado de los contenidos y demostraciones de los teoremas de toda esta sección ver, por ejemplo, [**?**].

diferencia entre la segunda y la primera componentes es 3 en todos los casos. Algo análogo ocurre con los pares $(1,1),(7,7),(13,13),\ldots(n,n)\ldots$, en los que todas las diferencias son cero.

Lo interesante es que esta relación se puede definir para todos los pares de números naturales de una manera uniforme sin recurrir a la resta. La idea es que, si bien lo que comparten todos esos pares es que "su diferencia" es la misma, esto se puede expresar en términos de la suma.

Sea $\sim$ la relación definida sobre $\mathbb{N}\times\mathbb{N}$, el conjunto de los pares ordenados de números naturales, definida por

$$(n,m) \sim (p,q) \quad \text{si y solo si} \quad n+q = p+m\,.$$

Obsérvese que en este caso si $(n,m) \sim (p,q)$, entonces "$n-m=p-q$", lo que concuerda con la intuición anterior. Ponemos comillas porque en la mitad de los casos estas restas no tienen sentido.

Lo siguiente es hacer notar que esta es una relación de equivalencia y que, como tal, genera una partición del conjunto $\mathbb{N}\times\mathbb{N}$.

Si denotamos $[(n,m)]_\sim$ a la clase de equivalencia del par (n,m), entonces definimos el conjunto $\mathbb{Z}$ de los *números enteros*

$$\mathbb{Z} = \{\,[(n,m)]_\sim \;:\; n,m\in\mathbb{N}\}\,.$$

1.4.1. Operaciones en los números enteros

Definición 1.32. La suma de dos enteros $[(n,m)]_\sim$ y $[(p,q)]_\sim$ es el entero

$$[(n,m)]_\sim \oplus [(p,q)]_\sim = [(n+p,m+q)]_\sim\,.$$

El producto o multiplicación de dos enteros $[(n,m)]_\sim$ y $[(p,q)]_\sim$ es el entero

$$[(n,m)]_\sim \odot [(p,q)]_\sim = [(np+mq,mp+nq)]_\sim\,.$$

Hemos usado los símbolos $\oplus$ y $\odot$ para representar la suma y el producto de enteros, reservando los símbolos $+$ y $\cdot$ para las correspondientes operaciones entre números naturales. De esta manera enfatizamos que las operaciones con números naturales y con números enteros son, en este contexto, cosas muy distintas.

Debe verificarse que estas operaciones están bien definidas, es decir, que no dependen del representante de la clase de equivalencia que se haya elegido.

1.4.2. Orden en los números enteros

Los número enteros pueden ser ordenados de la siguiente manera.

$$[(n,m)]_\sim \leq_{\mathbb{Z}} [(p,q)] \quad \text{si y solo si} \quad n+q \leq p+m\,.$$

Obsérvese que la primera relación, $\leq_{\mathbb{Z}}$ es entre números enteros y la segunda $\leq$, es entre números naturales. Usaremos también la notación

Por ejemplo, $[(1,4)] \leq_{\mathbb{Z}} [(3,2)]$ porque $1+2 \leq 3+4$.

Como en el caso de las operaciones, se debe verificar que esta relación está bien definida para las clases de equivalencia.

1.4.3. Los Enteros y los Naturales

En nuestras intuiciones y en la construcción axiomática hecha en este capítulo, los números naturales están contenidos en los enteros, coincidiendo con los enteros positivos. Es claro que en esta construcción esto no sucede. Sería difícil confundir el número natural 1 con el entero que hace el papel de 1 en $\mathbb{Z}$, a saber, $[(2,1)]_\sim = \{(n+2,1) \ : \ n \in \mathbb{N}\}$, ¡el segundo es un conjunto infinito de pares ordenados números naturales! Sin embargo, las intuiciones descritas al comienzo de esta sección nos dan una idea de cómo pueden verse los números naturales reflejados dentro del conjunto de los números enteros.

Estudiemos un poco la estructura de cada uno de los conjuntos $[(n,m)]_\sim$ a los que hemos llamado número entero.

Si $n > m$, existe un par de la forma $(r+1,1)$ tal que $(r+1,1) \in [(n,m)]_\sim$. A su vez, si $n < m$, existe un par de la forma $(1,r+1)$ tal que $(1,r+1) \in [(n,m)]_\sim$. En cada caso, estos números naturales r son obviamente únicos. Es habitual elegir como representante de cada clase a este elemento distinguido.

Existe una obvia inyección de $\mathbb{N}$ en $\mathbb{Z}$, a saber

$$\begin{array}{rccl} F \ : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & [(n+1,1)]_\sim \end{array}$$

El conjunto $F[\mathbb{N}] = \{[(n+1,1)]_\sim \ : \ n \in \mathbb{N}\} \subseteq \mathbb{Z}$ es una especie de copia de los naturales dentro de los enteros que se comporta exactamente igual a los naturales, de manera que, con un abuso de lenguaje, podemos decir que los naturales coinciden con los enteros positivos y denotar a los enteros como sigue:

$$[(n,m)]_\sim = \begin{cases} r & , \text{ si } (r+1,1) \in [(n,m)]_\sim \\ 0 & , \text{ si } n = m \\ -r & , \text{ si } (1,r+1) \in [(n,m)]_\sim\,, \end{cases}$$

Por ejemplo, $-2 = \{(1,3),(2,4),(3,5),\cdots\}$ y $2 = \{(3,1),(4,2),(5,3),\cdots\}$. Por comodidad usamos el mismo símbolo, "2", para denotar tanto al número entero dos como al número natural dos. Obsérvese también que $0 = [(n,n)]_\sim$.

Comprobar que esta copia de los números naturales dentro de los enteros efectivamente se comporta como los números naturales es un ejercicio elemental, si bien algo tedioso.

Por ejemplo, si sumamos los enteros positivos n y m, tenemos

$$n \oplus m = [(n+1,1)]_\sim \oplus [(m+1,1)]_\sim = [(n+1+m+1,1+1)]_\sim = [((n+m)+1,1)]_\sim ,$$

es decir,

$$F(n) \oplus F(m) = F(n+m) .$$

También,

$$\begin{array}{lll} n \leq_{\mathbb{Z}} m & \text{si y solo si} & [(n+1,1)]_\sim \leq_{\mathbb{Z}} [(m+1,1)]_\sim \\ & \text{si y solo si} & n+1 \leq m+1 \\ & \text{si y solo si} & n \leq m \end{array}$$

Para terminar esta sección, debe enfatizarse que el propósito de esta hermosa construcción es proporcionar a los números enteros de un andamiaje lógico riguroso. Se trata de un modelo de los números enteros, lo que quiera que estos sean, dentro de la teoría de conjuntos, sus creadores jamás pensaron que estos raros conjuntos fueran "los números" enteros. Tampoco se pensó que estas construcciones tan abstractas tuvieran un potencial didáctico, para que las personas aprendieran acerca de los números enteros. En las décadas de los 70 y 80 del siglo XX, una interpretación errada de estas ideas llevó a muchos especialistas en educación de la matemática y también a matemáticos a proponer la enseñanza de los números y sus operaciones a través de estas clases de equivalencia. El resultado, como cabía esperar, fue desastroso.

Índice alfabético