Máximo Común Divisor

Ana Ofelia Negrete Fernández

27 de julio 2021

1. Introducción

En esta entrada primero veremos qué significa que un entero a divida a otro entero b.

Luego nos servirá recordar lo que es un ideal en $\mathbb{Z}$ para definir al "generado de m y n," como sigue:

$$\langle\{m, n\}\rangle = \{nz_1 + mz_2 : z_1, z_2 \in \mathbb{Z}\}.$$

A partir de lo cual definiremos al máximo común divisor de dos enteros m y n como aquél $d \geq 0$, $d \in \mathbb{Z}$, tal que

$$d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z},$$

y que observaremos, $d\mathbb{Z}$ y $\langle\{m, n\}\rangle$ son el mismo conjunto.

En particular si $d = 1$, tendremos $\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$. Cuando esto ocurre decimos que m y n son primos relativos.

Finalmente demostraremos algunos teoremas que hagan uso de estos cuatro nuevos conceptos.

2. Divisibilidad e ideales en $\mathbb{Z}$

Definición (a divide a b). Definimos la relación "divide a" en $\mathbb{Z}$ así:

$$a \mid b \text{ si y sólo si } \exists x \in \mathbb{Z} \text{ tal que } ax = b.$$

Que es a equivalente decir: "a divide a b si y sólo si $b \in a\mathbb{Z}$," o que "b es múltiplo de a."

Definición (Resta en $\mathbb{Z}$). En el conjunto de los enteros, restar dos números w y z se define de la siguiente manera:

$$w - z = w + (-z).$$

La resta en $\mathbb{Z}$ no es conmutativa, pues eligiendo z un entero y $-z$ su inverso, obtenemos que $z - (-z) = z + [-(-z)] = z + z = 2z \neq -z - z = -z + (-z) = -2z$.

Tampoco es asociativa, pues eligiendo $x = -z$, $y = z$, $w = -z$ números enteros, se tendrá que

$$x - (y - w) = -3z \neq -z = (x - y) - w.$$

Un conjunto S es cerrado bajo la resta si al tomar dos elementos en S y restarlos, el resultado también está en S. En particular para $S = \mathbb{Z}$ sucederá que la única condición necesaria para que ciertos subconjuntos de $\mathbb{Z}$ sean ideales será pedirles que sean cerrados bajo la resta.

Demostremos entonces que:

Proposición 1. Si un subconjunto de $\mathbb{Z}$ cerrado bajo la resta tiene algún elemento distinto de 0, entonces también tiene un elemento positivo.

Dem.- Sea $S \subseteq \mathbb{Z}$ un subconjunto distinto del vacío y cerrado bajo la resta. Tomemos $z \in S$. Ya que S es un entero cerrado bajo la resta, $z - z = z + (-z) = 0$. Por lo que $0 \in S$. Y como 0 y z están en S que es cerrado bajo la resta, $0 - z = 0 + (-z) = -z$. Es decir, el inverso de z también está en S y necesariamente alguno de ellos, z o $-z$ será positivo.

□

Proposición 2. Si un subconjunto S de $\mathbb{Z}$ es cerrado bajo la resta, entonces S es cerrado bajo la suma.

Dem.- Si $S = \emptyset$, decir que $S \subseteq \mathbb{Z}$ es cerrado bajo la resta es una proposición falsa, pues no existen elementos en S, y de una hipótesis falsa podemos concluir lo que queramos; en particular, que S es cerrado bajo la suma.

Si, $S \neq \emptyset$, de la proposición anterior sabemos que S tiene al menos dos elementos z_1 y z_2. Y sólo es cuestión de expresar la suma de ellos como una resta:

$$z_1 + z_2' = z_1 + (-z_2),$$

lo cual es posible porque, también de la proposición anterior se tiene que $-z_2 \in S$.

□

Proposición 3. Si un subconjunto S de $\mathbb{Z}$ es cerrado bajo la resta, entonces cuando $x \in S$, todo múltiplo de x también está en S. Es decir, que

$$x \in S \implies \mathbb{Z}x \subseteq S.$$

Dem.- Sea S un subconjunto de $\mathbb{Z}$ distinto del vacío y cerrado bajo la resta. Primero veremos que los múltiplos positivos de x pertenecen a S y lo haremos por inducción.

Sea $x \in S$. Por la proposición anterior, $0 \in S$ y esto es la base de inducción.

Supongamos que el enunciado se cumple para nx, es decir, asumamos $nx \in S$. Tenemos entonces que $(n+1)x = nx + x$ está en S, pues $x \in S$ y un subconjunto cerrado bajo la resta es cerrado bajo la suma. Concluimos que todo $nx \in S$ si $n \geq 0$.

Pero para cada $nx \in S$, su inverso aditivo también está en S. Lo que termina de demostrar el resultado.

□

Definición (Ideal en $\mathbb{Z}$). Un subconjunto I de $\mathbb{Z}$ no vacío y cerrado bajo la resta se llama un ideal de $\mathbb{Z}$.

La definición de ideal en $\mathbb{Z}$ que acabamos de dar es exclusiva para el conjunto de los enteros, pues de la entrada de blog anterior sabemos que en general, para que un conjunto I sea ideal se requiere que I sea subanillo de un anillo A, también que I sea subgrupo de A con la operación suma y que se absorba la multiplicación; es decir, para cualquier $a \in A$ e $i \in I$ se tendrá que $aI \in I$.

Esta definición simplificada de ideal en los enteros es interesante porque nos hace dar cuenta de que sólo hay que pedir que I subconjunto de $\mathbb{Z}$ sea cerrado bajo la resta y de ello se implican los requerimientos para la definición de ideal en general. Muestra tú mismx este hecho.

También intenta demostrar lo siguiente:

Proposición 4. Si un subconjunto $S \neq \emptyset$ de $\mathbb{Z}$ es cerrado bajo la resta, entonces existe $n \in \mathbb{N}$ tal que $S = n\mathbb{Z}$.

La proposición anterior equivale a decir que todos los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, cosa que ya habíamos mostrado anteriormente; claro que en aquél caso explícitamente usamos la definición

de ideal y el hecho de que todos los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$. Aquí no sería necesaria la teoría algebraica adicional.

Subconjuntos de $\mathbb{Z}$ que no son de la forma $n\mathbb{Z}$ **no** serían ideales. Es lo que nos dice también la proposición.

Ejemplo. $\{1\}$ es subconjunto de $\mathbb{Z}$ pero su inverso aditivo no está en el conjunto.

Ejemplo. $\mathbb{N}$ es subconjunto de $\mathbb{Z}$ pero no es cerrado bajo la resta.

Teorema 1. Si $\{S_i\}_{i\in\mathbb{N}}$ es una familia de subconjuntos no vacíos de $\mathbb{Z}$ cerrados bajo la resta, entonces $\bigcap\{S_i\}_{i\in\mathbb{N}}$ también es un subconjunto no vacío cerrado bajo la resta.

Dem.- Tenemos que $0 \in S_i$ para toda $i \in \mathbb{N}$, por la proposición 1. Así, $0 \in \bigcap S_i$.

Análogamente, si $m, n \in \bigcap S_i$, entonces, como cada S_i es cerrado bajo la resta, $m - n \in S_i\ \forall i \in \mathbb{N}$. Como $m - n$ está en todos los S_i, entonces $m - n \in \bigcap S_i$.

Del teorema 1 se concluye que para cada subconjunto S de $\mathbb{Z}$ cerrado bajo la resta, existe un conjunto que lo contiene, con la propiedad de ser mínimo. Podría ser él mismo o no. Este hecho se denota

$$\langle S\rangle = \bigcap\{Y : S \subseteq Y,\ \ Y \neq \emptyset,\ \text{ y } Y \text{ es cerrado bajo la resta}\}.$$

Asimismo, no todo subconjunto de $\mathbb{Z}$ es cerrado bajo la resta, pero está contenido en uno que sí lo es. Por ejemplo, $\{1\} \subset \langle 1\rangle = 1 \cdot \mathbb{Z}$. Y $\mathbb{N} \subset \langle \mathbb{N}\rangle = \mathbb{Z}$. También,

- $\langle \emptyset\rangle = \{0\} = 0 \cdot \mathbb{Z}$.
- $\langle \{21, 14\}\rangle = 7\mathbb{Z}$.

Del último ejemplo vemos que, aunque $\mathbb{Z}$ es un conjunto cerrado bajo la resta que contiene a $\langle \{21, 14\}\rangle$, no es el mínimo que lo contiene.

Además, se puede demostrar más rigurosamente que $\langle \{21, 14\}\rangle = 7\mathbb{Z}$ por doble contención de conjuntos:

Por un lado, $21 = 7 \cdot 3$ y $14 = 7 \cdot 2$, por lo que $21 \in 7\mathbb{Z}$ y $14 \in 7\mathbb{Z}$. Ya que $7\mathbb{Z}$ es cerrado bajo la resta, entonces $\langle \{21, 14\}\rangle \subseteq 7\mathbb{Z}$, usando el teorema 1. Por otro lado, $7 \in 7\mathbb{Z}$ y $7 = 21 - 14$. Así, $7z = 21z - 14z$. Como a todo $7z \in 7\mathbb{Z}$ lo podemos escribir como una combinación lineal de 21 y 14, se concluye que $7z \in \langle \{21, 14\}\rangle$. Lo que significa que $7\mathbb{Z} \subseteq \langle \{21, 14\}\rangle$.

En general, demostraremos por doble contención de conjuntos, que

$$\langle \{m, n\}\rangle = \{mz_1 + nz_2 : z_1, z_2 \in \mathbb{Z}\}.$$

Dem.- Sea $S = \{m, n\}$. Para ver que $\langle \{m, n\}\rangle \subseteq \{mz_1 + nz_2 : z_1, z_2 \in \mathbb{Z}\}$, notemos que el lado derecho es un conjunto cerrado bajo la resta, pues podemos reescribir mz_1+nz_2 como $mz_1-n(-z_2)$. Además, $\{mz_1 + nz_2 : z_1, z_2 \in \mathbb{Z}\}$ contiene a m y n, pues $m = m \cdot 1 + n \cdot 0$ y $n = m \cdot 0 + n \cdot 1$. Y con esto también garantizamos que el conjunto es distinto del vacío. De la definición de $\langle S\rangle$, todos las colecciones que tengan estas características contienen a $\langle S\rangle$.

Asímismo, todo $m\cdot z_1+n\cdot z_2 \in \{mz_1+nz_2 : z_1, z_2 \in \mathbb{Z}\}$ está en $\langle S\rangle$, ya que como este es un conjunto cerrado bajo la resta en los enteros, la proposición 3 nos dice que todo $m\mathbb{Z}$ y todo $n\mathbb{Z}$ están en $\langle S\rangle$, y por la proposición 2, la suma $m\mathbb{Z} + n\mathbb{Z}$ también lo estará. En particular, $m \cdot z_1 + n \cdot z_2 \in \langle S\rangle$. Esto demostraría la contención inversa.

□

3. Definición de máximo común divisor

Por la proposición 4, afirmamos que existe $d \geq 0$ tal que

$$\langle \{m, n\} \rangle = d\mathbb{Z}.$$

Así es como podremos definir al máximo común divisor.

Definición (Máximo común divisor). El entero $d \geq 0$ tal que

$$d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$$

se llama el máximo común divisor de n y m. Lo denotaremos por (m, n).

Coloquialmente, decimos que el máximo común divisor de dos enteros es el mayor número que divide a ambos. Por ejemplo, el máximo común divisor de 30 y 50 es 10. Pues $30 = 2 \cdot 3 \cdot 5$ y $50 = 2 \cdot 5^2$. Es decir, para calcular el el MCD de 30 y 50 se descomponen ambos números en su factorización en primos (podemos usar el algoritmo que aprendimos en la primaria). Todos los divisores de 30 y 50 son esos números primos que los factorizan, al igual que los productos de ellos y de sus potencias.

El libro de Álgebra Superior de Rincón, Bravo, Rincón en el que estamos basándonos, pide demostrar que $(0, 0) = 0$:

Notamos que el máximo común divisor de $m = 0$ y $n = 0$ es $(0, 0) = 0 \cdot \mathbb{Z} + 0 \cdot \mathbb{Z} = 0 = d\mathbb{Z}$. Como $\mathbb{Z}$ no siempre es cero, d debe de serlo. Pero ¡cuidado! pues hay otros cursos y libros que especifican al máximo común divisor de cero como indefinido.

Teorema 2. Si $n \neq 0$ o $m \neq 0$, y $\langle \{m, n\} \rangle = d\mathbb{Z}$, $d \geq 0$, entonces d tiene las siguientes propiedades:

- $d > 0$.
- $(d \mid n) \wedge (d \mid m)$.
- $(k \mid n) \wedge (k \mid m) \implies (k \mid d)$.

Dem.- Si $m \neq 0$ o $n \neq 0$, necesariamente $d \neq 0$. Pero ya que $d \neq 0$ y $d \geq 0$, entonces $d > 0$.

$\langle \{m, n\} \rangle$ contiene a m por definición de "generado de m y n". Así, existe $z \in \mathbb{Z}$ tal que $dz = m$, usando que $\langle \{m, n\} \rangle = d\mathbb{Z}$. Se implica que $d \mid m$. Y por un razonamiento análigo, $d \mid n$.

Si $k \mid n$ y $k \mid m$, entonces $n \in k\mathbb{Z}$ y $m \in k\mathbb{Z}$. De este modo, $k\mathbb{Z}$ es un ideal que contiene a m y n. Por lo que también contiene a $\langle \{m, n\} \rangle = d\mathbb{Z}$. Así, existe un $z \in \mathbb{Z}$ tal que $k \cdot z = d \cdot 1 = d$. De donde $k \mid d$.

□

A continuación definimos a los números que son primos relativos y demostramos un teorema para ellos.

Definición (Primos relativos). Decimos que dos enteros m, n son primos relativos si $(n, m) = 1$.

Teorema 3. Dos enteros m, n son primos relativos si y sólo si existen x y y enteros tales que $xm + yn = 1$.

Dem.- La ida del teorema es una consecuencia inmediata de la definición de máximo común divisor, pues $1\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ implica que, eligiendo $1 \in \mathbb{Z}$ del lado izquierdo, necesariamente habrá alguna pareja de enteros x, y tales que $1 \cdot 1 = 1 = mx + ny$.

Tomemos ahora $mx + ny = 1$. Para z arbitraria se cumplirá que $zmx + zny = z$. Es decir, $m(zx) + n(zy) = 1z$. Como sucede para toda z, $m\mathbb{Z} + n\mathbb{Z} = 1 \cdot \mathbb{Z}$. Por lo que m y n son primos relativos.

□

El teorema anterior es relevante pues al hacer demostraciones será más usual describir a dos numeros que son primos relativos mediante una combinación lineal del tipo $xn + yn = 1$, en vez de usar la definición de máximo común divisor.

Ahora veamos otro teorema útil.

Teorema 4. Sean $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ y $(a, b) = 1$ entonces $a \mid c$.

Dem.- Como a divide a bc, existe $x \in \mathbb{Z}$ tal que $ax = bc$. Multiplicamos esta ecuación por m adecuada:

$$amx = bmc.$$

Luego, existen m, n enteros tales que $bm + an = 1$, pues a, b son primos relativos. Así, $bm = 1 - an$.

Sustituyendo en $amx = bmc$, tenemos que $amx = (1 - an)c$. De donde

$$amx(1 + an) = (1 + an)(1 - an)c = c - c(an)^2,$$

lo que implica

$$a\Big[mx(1 + an) + (ca)n^2\Big] = c.$$

□

Teorema 5. Sean $a, b, c \in \mathbb{Z}$. Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, entonces $ab \mid c$.

Dem.- Ya que (a, b) son primos relativos, existen $m, n \in \mathbb{Z}$ tales que $am + bn = 1$ y multiplicamos esta ecuación por c:

$$cam + cbn = c.$$

Luego, existen $q, r \in \mathbb{Z}$ tales que $aq = c$ y $br = c$, pues a divide a c y b divide a c. Y sustituyendo en $cam + cbn = c$ tenemos:

$$bram + aqbn = ab(rm + qn) = c,$$

de donde $ab \mid c$.

□

4. Ejercicios

1. Demuestra que dos enteros consecutivos siempre son primos relativos.
2. Demuestra que si $(a, b) = 1$, entonces $(a^n, b^m) = 1$.
3. Demuestra que si $(a, b) = 1$, entonces $(a^n, b^m) = 1$.
4. Demuestra que para $d = (a, b)$, si $d = ra + sb$, entonces $(r, s) = 1$.
5. Demuestra que si $(a, m) = 1 = (b, m)$, entonces $(ab, m) = 1$.
6. Demuestra que si $(a, b) = d$, entonces $(ad, bd) = 1$.