Semana 6: Divisibilidad

1. Definiciones

Hemos establecido ya algunas propiedades de los números enteros, en particular, establecimos su clasificación como un anillo y un dominio entero. Como se comentó, estas propiedades son suficientes para probar cualquier verdad conocida acerca de los números enteros. Con esto en mente, comencemos a plantear algunos definiciones básicas de un área de la matemática conocida como «Teoría de Números».

Definición 6.1. Para dos enteros a y b, diremos que *a es divisor de b*, en símbolos $a|b$, si existe un entero q de forma que

$$b = qa.$$

Por ejemplo, 6 es divisor de 12 pues $6 \cdot 2 = 12$, lo mismo que 3 al tener $3 \cdot 4 = 12$. De igual forma, es falso que 3 es divisor de 7, a razón que no existe un número entero q de forma que $3q = 7$, lo anterior se expresa usualmente como $a \nmid b$, lo cual se lee «a no es divisor de b». Existen algunas otras formas de enunciar que a es divisor de b, entre ellas encontramos:

- a divide a b.
- a es factor de b.
- b es múltiplo de a.
- b es divisible entre a.

Debemos notar que la anterior definición no tiene un vínculo directo con la operación inversa del producto[1], por ejemplo, tendría perfecto sentido preguntar si existe un entero a de forma que $0 \mid a$. Si lo anterior fuera cierto deberíamos garantizar la existencia de un número k de forma que

$$a = k \cdot 0 = 0;$$

podemos entonces concluir que $0 \mid a$ si y sólo si $a = 0$. Este hecho deriva en que podamos enunciar sin problema alguno $0 \mid 0$, lo cual, si pensamos el concepto de divisibilidad como una operación inversa, podría ser problemático. Esto último parece razón suficiente para desvincular los conceptos y darse cuenta que el concepto de divisibilidad es en realidad un predicado y no una operación entre números enteros.

[1] En este punto desconocemos cual es la operación inversa del producto. Sin embargo, somos capaces de distinguir que se trata de "la división de enteros". De esta forma, en el conjunto de los racionales, el número $12/3 = 4$ mientras que $7/3$ resulta un número que no es entero que podríamos denominar *puramente racional*.

De forma similar, podemos preguntarnos en que casos a divide a 1. Para responder esto necesitamos indagar en casos existe un entero q de forma que

$$1 = aq.$$

Aunque es sencillo encontrar los únicos números posibles, es interesante dotar a la pregunta de un poco de terminología antes de responderla.

Definición 6.2. Sean a un entero cualquiera. Si existe un entero q de forma que $aq = 1$, entonces q se dirá *un inverso mutliplicativo de a*. Además, a un entero que tenga un inverso multiplicativo, se llamará *una unidad* .

No es difícil notar que, si un entero posee un inverso multiplicativo, entonces este es único. Sin embargo, los números que poseen inversos multiplicativos, o en nuestra terminología, las unidades, no son realmente diversos.

Lema 6.1. *Sea a un entero cualquiera. Entonces, la existencia de un entero q de forma que $aq = 1$, implica que $a = 1$ o $a = -1$.*

Demostración. Por hipótesis, existe un entero q que satisface $aq = 1$. Comencemos notando es imposible tener $a = 0$. En efecto, si éste fuera el caso debemos tener $aq = 0$ y de esta forma debemos concluir que $a \neq 0$ al considerar $1 \neq 0$. De manera similar podemos concluir que $q \neq 0$.

Si ahora suponemos $a > 1$, como $aq = 1$ debemos tener que $q > 0$. También, $q > 1$ pues si $q = 1$, entonces $a = aq = 1$ lo cual contradice nuestra suposición. En resumen, si $a > 1$, entonces $q > 1$ y además $aq > 1$ lo cual es imposible pues por hipótesis $aq = 1$; por contradicción podemos concluir que $a \leq 1$. Con un argumento similar podemos descartar $a < -1$, obteniendo así que $-1 \leq a \leq 1$. Además, la discusión del primer párrafo asegura que $a \neq 0$ con lo concluimos que $a = 1$ o $a = -1$ como afirma el lema. ■

Corolario 6.2. *Las únicas unidades en $\mathbb{Z}$ son 1 y -1.*

Estos resultados responden a nuestro objetivo: ¿Cuáles enteros son divisores de 1? Solamente 1 y -1. Es un halago lo simple que resulta $\mathbb{Z}$ respecto a las unidades, esto nos permite realizar algunas observaciones del concepto en cuestión.

Teorema 6.3. *Para cualesquiera enteros a y b*

1. *$a \mid a$.*
2. *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *Para enteros $a \neq 0$ y $b \neq 0$, si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$.*

Demostración. Notemos primero que $a \cdot 1 = a$, por lo que en verdad a es divisor de a. De esto sigue 1. Supongamos, ahora que existen números q_1 y q_2 que satisfacen $aq_1 = b$ y $bq_2 = c$. En ese caso tenemos

$$c = bq_2 = (q_1q_2)a.$$

La existencia del número q_1q_2 garantiza la divisibilidad de c por a de lo que sigue 2. Por último, supongamos que q_1 y q_2 son enteros de forma que $aq_1 = b$ y $bq_2 = a$, en ese caso

$$a(q_1q_2) = bq_2 = a,$$

como $a \neq 0$, la ley de cancelación garantiza que $q_1q_2 = 1$, lo cual sucede solamente si $q_2 = 1$ o $q_2 = -1$ por lo que $a = b$ o $a = -b$. ■

Debemos notar que el teorema anterior no da información acerca de la relación que hemos definido sobre los enteros. La primera propiedad muestra que es reflexiva, la segunda que es transitiva y la tercera que está cerca de ser simétrica salvo unidades.

Teorema 6.4. *Sean a, b, u y v de forma que u y v son unidades. Entonces, $a \mid b$ si y sólo si $u \cdot a \mid v \cdot b$.*

Demostración. Supongamos primero que a es divisor de b. En ese caso existe un entero q de forma que $aq = b$. Como u es unidad, debe existir u_1 de forma que $uu_1 = 1$ y consecuencia

$$b = aq = (uu_1)aq = ua(qu_1),$$

de lo que podemos concluir que ua divide a b. Debemos observar por definición que también b es divisor de vb y usando que la divisibilidad es transitiva, ua resulta también divisor de vb.

Supongamos ahora que ua es divisor de vb. En ese caso existe un entero q que satisface $vb = uaq$. Como v es unidad, debe existir v_1 de forma que $v_1v = 1$ con lo que podemos concluir

$$b = (v_1v)b = v_1uaq = a(v_1uq).$$

En otras palabras a es divisor de b como buscábamos. ∎

Existen por supuesto muchas otras propiedades que hablan de la divisibilidad en términos de los enteros como conjunto. Sin embargo, es importante vincular el concepto con la estructura que hemos articulado en $\mathbb{Z}$.

2. Propiedades de estructura

Comenzaremos preguntándonos qué relación guardan el orden de los enteros y la divisibilidad. De manera intuitiva podemos razonar como sigue: Si $b = qa$ teniendo a y q como enteros positivos, el producto entre ambos debe resultar se un número más grande o igual a cualquiera a o q. Por ejemplo, sabemos que 6 es un múltiplo de 3, además $3 < 6$ y de la misma forma 8 es múltiplo de 2 y $2 < 8$. Para los enteros negativos, funciona de manera inversa, por ejemplo -8 es múltiplo de -2 pero $-8 < -2$. Exploraremos ahora el caso general.

Definición 6.3. Para un entero a, definimos *el valor absoluto de a*, como

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

La definición anterior nos permite interpretar el teorema 6.4 evitando la terminología de unidades e intercambiarla por el valor absoluto.

Lema 6.5. *Para enteros cualquiera a y b, $a|b$ si y sólo si $|a| \mid |b|$.*

Teorema 6.6. *Para enteros $a \neq 0$ y $b \neq 0$, si $a|b$ entonces, $|a| \leq |b|$.*

Demostración. Considerando el lema 6.5 podemos afirmar que $|a| \mid |b|$ o, siguiendo la definición, existe un entero q de forma que

$$|b| = q|a|.$$

Lo primero que hay que notar es que q no puede ser 0, si lo fuera estaríamos obligados concluir que $|b| = 0$ lo que es una contradicción con la hipótesis. Además, q no puede ser negativo, pues si lo fuera al ser $|a| > 0$, deberíamos tener $|b| < 0$ lo cual es de nueva cuenta contradictorio. En resumen, debemos tener $q > 0$, o en otras palabras $q \geq 1$. De esta desigualdad, podemos desprender de inmediato el resultado

$$|a| \leq q|a| = |b|. \qquad \blacksquare$$

Exploremos ahora la relación que guarda la divisibilidad con la suma. De nueva cuenta, comenzaremos con algunos ejemplos. Para determinar si un número a es múltiplo de 3, podemos proponer crear una lista donde aparezcan los números 3, 6, 9, 12,... Los elementos de esta lista se puede escribir de forma recursiva como

$$a_0 = 3$$

$$a_{i+1} = a_i + 3.$$

Basta entonces revisar esta lista hasta que aparezca un número más grande o igual que a para determinar si es o no múltiplo de 3. La relevancia de este método reside es su expresión recursiva que es capaz de construir cualquier múltiplo de 3 como una suma finita, i.e.,

$$a = 3 + 3 + \cdots + 3.$$

Podemos indagar ahora sobre el vínculo que buscamos: ¿qué pasa con la suma de dos múltiplos de 3? En realidad no es difícil responder usando nuestro argumento intuitivo: si tenemos números que se puedan expresar como sumas de una cantidad fija de 3, su suma va a ser simplemente otra suma de una cantidad fija de 3 (aunque esta vez más larga) por lo que podemos concluir que *la suma de múltiplos de 3 es un múltiplo de 3*. Una versión general de este resultado, mostraría la relación que guarda la suma en los enteros y la divisibilidad. Formulemos ahora el enunciado y un argumento preciso que lo justifique.

Teorema 6.7. *Sean a, b y d enteros cualquiera. En ese caso, si $d \mid a$ y $d \mid b$ entonces $d \mid a + b$.*

Demostración. Por hipótesis deben existir enteros p y q que satisfacen $a = pd$ $b = qd$ por lo que

$$a + b = pd + qd = (p + q)d,$$

de lo que podemos concluir que $a + b$ es un múltiplo de d como esperábamos. $\blacksquare$

Por supuesto, podríamos dar una versión del teorema anterior para la multiplicación, pero la definición de divisibilidad se recarga tanto en el producto en los enteros que debe parecer lo suficientemente obvia. Buscar la prueba, sin embargo, es un interesante ejercicio (6.10).

Teorema 6.8. *Sean a, b y d enteros cualquiera. Si $d \mid a$, entonces $d \mid ab$.*

Podemos desprender de inmediato un corolario de los teoremas 6.7 y 6.8 sobre las condiciones que han de imponerse para garantizar la divisibilidad de una combinación de sumas y productos. El resultado, debe notarse, es una consecuencia directa de los teoremas mencionados.

Corolario 6.9. *Sean a, b y d enteros cualquiera. Si $d \mid a$ y $d \mid b$, entonces $d \mid sa + tb$, para cualesquier pareja de enteros s y t.*

Podemos llevar estos teoremas un poco más lejos motivados por el hecho que una suma puede involucrar varios términos. Habrá que precisar primero lo que entendemos por una *combinación de números*. Comencemos aclarando el término.

Definición 6.4. Sean a y b dos enteros cualesquiera. Un entero se dice *una combinación lineal de a y b* siempre que existan números s y t de forma que dicho número, se pueda expresar como

$$sa + tb.$$

Aunque la anterior definición parece abstracta, no es para nada complicada. Pensemos como ejemplo en el número 12, el cual podemos escribir como

$$12 = 3 \cdot 2 + 2 \cdot 3$$

por lo que podemos concluir que *12 es una combinación lineal de 2 y 3*. De la misma forma 15 se puede expresar como

$$15 = 1 \cdot 1 + 7 \cdot 2$$

teniendo esto como consecuencia que *15 es una combinación lineal de 1 y 2*. Esta terminología resulta útil al proporcionar una forma de expresarnos quitando algunas particularidades del camino: no nos importan quienes sean los números s y t en la definición, sólo que existan.

En este punto podemos vernos tentados a pensar que dados un par de números, cualquier otro número se puede expresar como una combinación lineal de estos. El siguiente teorema tendrá como consecuencia que esto no es así y de paso, nos permitirá dar una caracterización de la divisibilidad de una combinación lineal.

Teorema 6.10. *Sean a, b y d enteros cualquiera. Entonces, d divide a los enteros a y b si y sólo si d divide a cualquier combinación lineal de a y b.*

Demostración. Del corolario 6.9 podemos concluir que si d divide a ambos, a y b, d debe dividir a cualquier combinación lineal de estos, lo que garantiza la condición es necesaria.

Si d divide a cualquier combinación lineal de a y b, debe, en particular, dividir a las combinaciones

$$a = 1 \cdot a + 0 \cdot b$$

y

$$b = 0 \cdot a + 1 \cdot b.$$

Esto es, d divide a los números a y b probando con esto que la condición es suficiente. ■

Volvemos ahora a la pregunta del párrafo anterior. Dados dos números, se puede expresar cualquier otro como la combinación lineal de esos dos. El teorema nos permite responder no. Consideremos por ejemplo el número 13, ¿será el 13 una combinación lineal de 6 y 9? En otras palabras, ¿existirán enteros s y t de forma que $13 = s \cdot 6 + t \cdot 9$? Supongamos que existen, como $3 \mid 6$ y $3 \mid 9$, el teorema anterior afirma que 13 debería ser un múltiplo de 3, lo cual es evidentemente absurdo. Debemos entonces concluir que es imposible expresar 13 como una combinación lineal de 6 y 9. Podemos presentar este criterio de manera general, usando este mismo argumento, obteniendo con esto una regla que decide cuándo es posible expresar un número como una combinación lineal usando como condiciones enunciados que involucren divisibilidad.

Corolario 6.11. *Para cualesquiera números a, b y c, si existe un número d de forma que $d \mid a$ y $d \mid b$ pero $d \nmid c$, entonces c no es una combinación lineal de a y b.*

Demostración. Usando el mismo argumento que en el caso particular podemos garantizar este caso general. Supongamos entonces que c es una combinación lineal de a y b en ese caso, al d dividir a ambos números a y b, el teorema 6.10 garantiza que d debe dividir de igual forma a c, lo cual contradice una de las hipótesis. En ese caso, c no puede ser una combinación lineal de a y b. ■

3. El teorema de la división

Esta sección pretende proveer los pormenores de un resultado con el nos hemos enfrentado en muchas ocasiones durante nuestra educación básica: La división. Quizá no sea posible reconocer el enunciado a simple vista, pero debe ser por todos conocido. Es importante recalcar el objetivo de este algoritmo: Encontrar el cociente y el residuo dados dos números. Estamos ahora en el borde de conectar una idea intuitiva que por algún tiempo hemos aceptado sin cuestionarnos realmente su significado. Para crear un algoritmo, debemos tener ciertas garantías que no pueden ser menospreciadas. Por ejemplo, el algoritmo parece garantizar que siempre existen un cociente y un residuo, ¿existirán siempre? Y si lo hacen, ¿podrá existir otro par de números que sean cociente y residuo de la misma división? Estas preguntas nos deben llevar primero a identificar con precisión que son el cociente y el residuo de una división. El siguiente lema tiene como objetivo dar una respuesta parcial.

Lema 6.12. *Para cualesquiera dos enteros no negativos a y b, con $b \neq 0$, existen un único par de enteros q y r, que satisfacen $0 \leq r < b$ y*

$$a = qb + r.$$

Demostración. Comencemos definiendo el conjunto

$$Q = \{n \in \mathbb{Z} \mid a \geq nb\}.$$

Afirmamos que este conjunto está acotado superiormente, lo cual constituye la parte crucial en la demostración. En efecto, como $b \neq 0$ entonces $b \geq 1$. En ese caso, si $n > a$ entonces,

$$nb \geq n > a$$

y en consecuencia $n \notin Q$. En otras palabras, si $n \in Q$, entonces $n \leq a$. Esto prueba nuestra afirmación al ser a una cota superior de Q.

Sabemos que en $\mathbb{Z}$ cualquier conjunto acotado superiormente tiene un máximo. Esto nos permite realizar la elección de los números que afirma el teorema de la siguiente manera: Tomamos $q = \max Q$ y $r = a - qb$. Por la forma en que tomamos estos números, es inmediato que

$$a = qb + r,$$

hace falta probar la desigualdad que define a r. Por la naturaleza del conjunto Q, se debe tener $r \geq 0$. Por otro lado, afirmamos que $r < b$. En efecto, si no fuera el caso, entonces $r \geq b$ y

$$a - (q+1)b = a - qb - b = r - b \geq 0.$$

Lo anterior implicaría que $q+1 \in Q$ en contradicción con la elección que hicimos de q (el máximo del conjunto Q). En consecuencia, $r < b$ como afirmamos.

Supongamos ahora que q_1 y r_1 son números tales que $a = q_1 b + r_1$ y $0 \leq r_1 < b$. En ese caso,

$$qb + r = a = q_1 b + r_1$$

y en consecuencia

$$(q - q_1)b = r_1 - r$$

por lo que $b \mid r_1 - r$. Además, $0 \leq r < b$ y $0 \leq r_1 < b$, por lo que $-b < r_1 - r < b$ o en otras palabras $|r_1 - r| < b$. Entonces, según el teorema 6.6, si $r_1 \neq r$ debemos tener que $b \leq |r_1 - r|$ lo cual es una contradicción, luego $r_1 = r$ y como $b \neq 0$ esto implica de igual forma que $q_1 = q$, mostrando con esto que los elementos q y r son lo únicos con las propiedades que buscamos. ■

El lema anterior sólo considera el caso para los naturales y sorprendentemente esto es suficiente para afirmar el resultado para los enteros. El siguiente teorema se presenta sin prueba, esperando que el lector suministre una, usando algunos ejemplos presentados posterior al teorema.

Teorema 6.13 (de la división)**.** *Para cualesquiera dos enteros a y $b \neq 0$ existe un único par de enteros q y r que satisfacen $0 \leq r < |b|$ y*

$$a = qb + r.$$

Definición 6.5. A los números q y r descritos en el teorema anterior, se les denominan *cociente* y *residuo* de la división de a entre b.

Presentamos ahora un par de ejemplos que nos permitirán delinear como es que el lema 6.12 implica el teorema de la división. Tomemos sobre el lema anterior $a = 9$ y $b = 2$, tenemos

$$9 = 4 \cdot 2 + 1,$$

por lo que debemos concluir que $q = 2$ y $r = 1$. Ahora, esto nos permite afirmar que

$$-9 = -4 \cdot 2 - 1$$

expresión que nos incita tomar el residuo de dividir -9 entre -2 como -1; sin embargo, el teorema indica que el residuo debe ser no negativo. Para solucionar esto, sumamos y restamos $|b| = 2$ al lado derecho de la igualdad anterior,

$$-9 = (-4 \cdot 2 - 2) + (2 - 1) = 5 \cdot (-2) + 1$$

y en ese caso podemos concluir que el cociente y el residuo de dividir -9 entre -2 resulta 5 y 1 respectivamente. Este ejemplo ilustra como dividir dos enteros negativos.

Consideremos ahora que al dividir -12 entre 7. Comenzamos explorando que pasa con la división asociada sus valores absolutos, i.e., a 12 y 7; para estos valores tenemos

$$12 = 1 \cdot 7 + 5.$$

En ese caso, procedemos de manera muy similar al ejemplo anterior. Primero,

$$-12 = -1 \cdot 7 - 5$$

y sumando y restando 7 de ambos al lado derecho de la igualdad

$$-12 = (-1 \cdot 7 - 7) + (7 - 5) = -2 \cdot 7 + 2$$

lo que exhibe el cociente y el residuo de la división resultan los números -2 y 2 respectivamente.

Estos dos ejemplos deben de dar una idea que en que algunos de los números involucrado sea negativo, se pueden resolver usando el valor absoluto y el lema 6.12. Esto se probará en el ejercicio 6.12.

El teorema de la división es un resultado importante, tanto por su generalización como su importancia en teoría de números, para ver al resultado en acción es importante realizar los ejercicios 6.13 y 6.14 en los cuales se deberá ocupar en citado teorema. Para concluir esta sección, escribiremos un resultado absolutamente inmediato que vincula la división con la divisibilidad.

Proposición 6.14. *Para cualesquiera números, a es múltiplo de b si y sólo si el residuo que resulta de dividir a entre b es 0.*

4. Máximo común divisor

El siguiente paso en nuestra exploración de la divisibilidad, consiste en determinar algunas caracterizaciones de un divisor de un par de números. Comencemos introduciendo algunas definiciones.

Definición 6.6. Sean a y b enteros cualesquiera. *Un divisor común de a y b* es un entero d de forma que d es divisor de a y d es divisor de b.

Esta definición de divisor común nos permite afirmar que a cada par de enteros a y b tiene al menos un divisor común: $d = 1$. Además, si d es un divisor común de estos números, debe satisfacer $|d| \leq |a|$ y $|d| \leq |b|$ (teorema 6.6), por lo que

$$d \leq |d| \leq \text{mín}\left\{|a|, |b|\right\}.$$

Esto se puede traducir afirmando que el conjunto de divisores comunes de a y b es no vacío y acotado superiormente, por lo que presenta un máximo.

Definición 6.7. El máximo común divisor de dos enteros a y b se denotará como (a, b).

Es quizá importante notar que si $a \mid b$, entonces a es un divisor común y además $(a, b) = a$. En particular, $(a, 0) = (0, a) = a$. Además, $(a, b) = 0$ si y sólo si $a = b = 0$. En realidad, lo anterior puede considerarse patologías y en general nos bastará estudiar los casos $a > 0$ y $b > 0$ pues

$$(a, b) = (|a|, |b|)$$

Teorema 6.15 (Identidad de Bézout)**.** *Sean a y b enteros cualesquiera. Entonces, el máximo común divisor es una combinación lineal de a y b, i.e., existen enteros s y t que satisfacen*

$$(a, b) = sa + tb.$$

Demostración. Si a o b fueran 0, el resultado es inmediato. Supongamos entonces que ambos son distintos de 0 y consideremos el conjunto I de números enteros formado por las combinaciones lineales de a y b, i.e.,

$$I = \{xa + yb \mid x, y \in \mathbb{Z}\}.$$

Debemos notar que tanto $-a$ como a son miembros de I, lo que nos lleva a concluir que I contiene al menos un elemento positivo. Tomamos entonces $P = I \cup \mathbb{Z}^+$ como el conjunto de enteros positivos que pertenecen a I. Según la discusión anterior, P es no vacío por lo que debe presentar un elemento mínimo. Tomemos entonces $d = \text{mín}\, P$. Afirmamos que d es el máximo común divisor.

Para probar nuestra afirmación, comenzaremos mostrando que d es un divisor común. Como d un elemento de I, deben existir enteros s y t de forma que

$$d = sa + tb.$$

Ahora, de acuerdo con el teorema de división existen números q y r de forma que $0 \leq r < d$ y

$$a = qd + r.$$

Vamos a descartar la posibilidad de tener $r > 0$. Para esto, debemos notar primero que

$$r = a - qd = a - q(as + bt) = (1 - qs)a + (-qt)b,$$

por lo que r es una combinación lineal de a y b y en consecuencia $r \in I$. Si $r > 0$ entonces $r \in P$ pero $r < d$, lo que es una contradicción con nuestra elección de d como el mínimo del conjunto P. Debemos entonces concluir que $r = 0$ implicando esto que $d \mid a$. Un argumento análogo sirve para concluir que $d \mid b$ mostrando que d es un divisor común de a y b como ase afirmó.

Finalmente, si c es cualquier otro divisor común de a y b, de acuerdo al corolario 6.9, c divide a cualquier combinación lineal y en consecuencia $c \mid d$, esto a su vez implica que $c \leq |c| \leq d$. Esto muestra que d es el máximo de entre todos los divisores comunes. ■

Corolario 6.16. *Sea d un entero no negativo de forma que sea un divisor común de los enteros a y b. Entonces, d es el máximo común divisor de a y b si y sólo si para todo divisor común c de a y b, $c \mid d$.*

Demostración. La prueba de la necesidad es resultado del teorema pues si tomamos $(a, b) = sa + tb$, cualquier divisor común de a y b dividirá también a (a, b) al ser éste una combinación lineal de los números involucrados.

Para demostrar que la condición es suficiente, supongamos que d es un entero no negativo que tiene la propiedad de ser un divisor común y múltiplo de cualquier divisor común de a y b. En particular, satisface $(a, b) \mid d$. Si $(a, b) = 0$, entonces $d = 0$ y habremos terminado. Si no lo fuera, entonces $(a, b) = |(a, b)| \leq d$ y además $d \leq (a, b)$ por la definición de máximo común divisor. En consecuencia, $d = (a, b)$, como afirma el corolario. ■

Habrá que tener cuidado en la lectura del corolario anterior, no todo divisor común que sea múltiplo de todos los divisores comunes es el máximo común divisor. Por ejemplo -3 es un divisor común de 6 y 9 y tiene la propiedad de ser múltiplo de cualquier divisor común sin éste ser el máximo. Para que el corolario sea válido, el número a evaluarse ha de ser no negativo. En realidad, el corolario tiene una consecuencia que pasa muchas veces desapercibida: El máximo común divisor no puede ser negativo.

Ejercicios

Ejercicio 6.1. Encuentra todos los divisores de 16 y 25.

Ejercicio 6.2. Prueba que 52 no es combinación lineal de 20 y 15.

Ejercicio 6.3. Encuentra un entero que no sea combinación lineal de 30 y 70.

Ejercicio 6.4. Para un entero n cualquiera, prueba lo siguiente:

1. Si c es un entero impar, entonces no es combinación lineal de 98 y 102
2. Si $c = 3n + 1$ entonces c no es combinación lineal de 45 y 1251.
3. Si $c = 30n + 6$, entonces c no es combinación lineal de 1020 y 210.

Ejercicio 6.5. Encuentra el cociente y residuo resultado de dividir a entre b para los siguiente valores.

1. $a = 0$ y $b = -3$.
2. $a = 12$ y $b = 59$.
3. $a = 59$ y $b = 12$.
4. $a = -59$ y $b = -12$.

Ejercicio 6.6. Demuestra que para cualquier entero a, debemos tener $a \mid 0$.

Ejercicio 6.7. Demuestra que para cualquier entero a, debemos tener $1 \mid a$.

Ejercicio 6.8. Prueba que si c es combinación lineal de a y b entonces cualquier múltiplo de c también lo es.

Ejercicio 6.9. Demuestra que si d es una combinación lineal de a y b, y b es una combinación lineal de a y c, entonces d es una combinación lineal de a y c.

Ejercicio 6.10. Prueba el teorema 6.8.

Ejercicio 6.11. Vamos a proveer una generalización del teorema 6.10. Para conseguirlo vamos a necesitar definir lo siguiente: Sea una sucesión de enteros $a_1, a_2, \ldots, a_{n-1}$ y a_n. Entonces a cualquier número que se pueda expresar por

$$r_1 a_1 + \cdots + r_n a_n,$$

para algunos enteros $r_1, r_2 \ldots r_{n-1}$ y r_n, se le llamará *combinación lineal de* $a_1, a_2, \ldots, a_{n-1}$ *y* a_n. Usando esto, prueba el siguiente teorema. (Sugerencia: Usa inducción sobre el tamaño de la sucesión).

Teorema 6.17. *Un entero d divide a los enteros* $a_1, a_2, \ldots a_{n-1}$ *y* a_n *si y sólo si d divide a cualquier combinación lineal de ellos.*

Ejercicio 6.12. Para proveer la demostración del teorema 6.13, considera los siguientes casos y utiliza el lema 6.12 de alguna forma en cada uno.

1. $a \geq 0$ y $b < 0$.
2. $a < 0$ y $b > 0$.
3. $a < 0$ y $b < 0$.

Ejercicio 6.13. Muestra que el conjunto de tres enteros consecutivos posee un múltiplo de 3.

Ejercicio 6.14. Muestra que el conjunto de m enteros consecutivos posee un múltiplo de m.

Ejercicio 6.15. Muestra que para cualesquiera dos enteros

$$(a, b) = (|a|, |b|).$$

Ejercicio 6.16. Asume que $d = sa + tb$ es una combinación lineal de a y b. Muestra que tantas parejas de enteros s_k y t_k como naturales de forma que

$$d = s_k a + t_k b$$

Para entregar: Ejercicio 6.12

Referencias

[Chi95] Childs, Lindsay N.: *A concrete introduction to higher algebra*. Springer, 2ª edición, 1995.

[CLRT90] Cárdenas, Humberto, Luis, Emilio, Raggi, Francisco y Tomás, Francisco: *Álgebra Superior*. Editorial Trillas, 1990.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.